ISSN 0042-8469
e-ISSN 2217-4753
УДК 623 + 355/359

Вол. 70, бр. 3

2022

НАУЧНИ ЧАСОПИС МИНИСТАРСТВА ОДБРАНЕ И ВОЈСКЕ СРБИЈЕ

ВОЈНОТЕХНИЧКИ ГЛАСНИК

3 2022 ВОЈНОТЕХНИЧКИ ГЛАСНИК

втг.мо.упр.срб

www.vtg.mod.gov.rs

ВОЕННО-ТЕХНИЧЕСКИЙ ВЕСТНИК 2022 3

РЕПУБЛИКА СРБИЈА
МИНИСТАРСТВО ОДБРАНЕ

УНИВЕРЗИТЕТ ОДБРАНЕ
2011

ISSN 0042-8469
e-ISSN 2217-4753
УДК 623 + 355/359

Том 70, № 3

2022

ВТГ

70 С 1953 г.
ВТГ
ЛЕТ

НАУЧНЫЙ ЖУРНАЛ МИНИСТЕРСТВА ОБОРОНЫ
И ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ СЕРБИЯ

ВОЕННО-ТЕХНИЧЕСКИЙ ВЕСТНИК

втг.мо.упр.срб

www.vtg.mod.gov.rs

ISSN 0042-8469
e-ISSN 2217-4753
UDC 623 + 355/359

Vol. 70, Issue 3
2022

SCIENTIFIC JOURNAL OF THE MINISTRY OF DEFENCE AND THE SERBIAN ARMED FORCES

MILITARY TECHNICAL COURIER

MILITARY TECHNICAL COURIER
2022
3

втг.мо.упр.срб
www.vtg.mod.gov.rs

ISSN 0042-8469
e-ISSN 2217-4753
UDC 623 + 355/359

НАУЧНИ ЧАСОПИС МИНИСТАРСТВА ОДБРАНЕ И ВОЈСКЕ СРБИЈЕ

ВОЈНОТЕХНИЧКИ ГЛАСНИК

ВОЛУМЕН 70 • БРОЈ 3 • ЈУЛ–СЕПТЕМБАР 2022.

NAUČNI ČASOPIS MINISTARSTVA ODBRANE I VOJSKE SRBIJE

VOJNOTEHNIČKI GLASNIK

VOLUMEN 70 • BROJ 3 • JUL–SEPTEMBAR 2022.

втг.мо.упр.срб
www.vtg.mod.gov.rs
COBISS.SR-ID: 4423938
COBISS.SR-ID: 181287436
DOI: 10.5937/VojnotehnickiGlasnik

ISSN 0042-8469
e-ISSN 2217-4753
UDC 623 + 355/359

НАУЧНЫЙ ЖУРНАЛ МИНИСТЕРСТВА ОБОРОНЫ И ВООРУЖЁННЫХ СИЛ РЕСПУБЛИКИ СЕРБИЯ

ВОЕННО-ТЕХНИЧЕСКИЙ ВЕСТНИК

ТОМ 70•НОМЕР ВЫПУСКА 3•ИЮЛЬ–СЕНТЯБРЬ 2022.

SCIENTIFIC JOURNAL OF THE MINISTRY OF DEFENCE AND SERBIAN ARMED FORCES

MILITARY TECHNICAL COURIER

VOLUME 70•ISSUE 3•JULY-SEPTEMBER 2022

втг.мо.упр.срб
www.vtg.mod.gov.rs
COBISS.SR-ID: 4423938
COBISS.SR-ID: 181287436
DOI: 10.5937/VojnotehnickiGlasnik

ВЛАСНИЦИ:
Министарство одбране и Војска Србије

ИЗДАВАЧ:
Универзитет одбране у Београду, Војна академија

УРЕДНИШТВО: странице чланова уредништва у ORCID iD-у, Google Scholar-у, Web of Science ResearcherID-у, Scopus Author ID-у и РИНЦ-у доступни су на http://www.vtg.mod.gov.rs/urednistvo.html

Главни и одговорни уредник
Др Драган Памучар, Универзитет одбране у Београду, Војна академија, Београд, Србија,
e-mail: dragan.pamucar@va.mod.gov.rs

Уредник за област математике, механике и рачунарских наука
Др Драган Трифковић, Универзитет одбране у Београду, Војна академија, Београд, Србија

Уредник за област електронике, телекомуникација и информационих технологија
Др Бобан Бонџулић, Универзитет одбране у Београду, Војна академија, Београд, Србија

Уредник за област машинства
Др Бранимир Крстић, Универзитет одбране у Београду, Војна академија, Београд, Србија

Уредник за област материјала и хемијских технологија
Др Радован Каркалић, Универзитет одбране у Београду, Војна академија, Београд, Србија

Технички уредник
Мр Небојша Гаћеша, Универзитет одбране у Београду, Војна академија, Београд, Србија,
e-mail: nebojsa.gacesa@mod.gov.rs, tel. 011/3603-260, 066/87-00-123

СОБСТВЕННИКИ: Министерство обороны и Вооружённые силы Республики Сербия

ИЗДАТЕЛЬСТВО: Университет обороны в г. Белград, Военная академия

OWNERS:
Ministry of Defence and Serbian Armed Forces

PUBLISHER:
University of Defence in Belgrade, Military Academy

EDITORIAL TEAM: the pages of the Editorial Team's members in ORCID iD, Google Scholar, Web of Science ResearcherID, Scopus Author ID, and РИНЦ can be accessed at http://www.vtg.mod.gov.rs/editorial-team.html
Editor in chief
Dr. Dragan Pamučar, University of Defence in Belgrade, Military Academy, Belgrade, Serbia,
e-mail: dragan.pamucar@va.mod.gov.rs
Editor for Mathematics, Mechanics and Computer Science
Dr. Dragan Trifković, University of Defence in Belgrade, Military Academy, Belgrade, Serbia
Editor for Electronics, Telecommunications and Information Technology
Dr. Boban Bondžulić, University of Defence in Belgrade, Military Academy, Belgrade, Serbia
Editor for Mechanical Engineering
Dr. Branimir Krstić, University of Defence in Belgrade, Military Academy, Belgrade, Serbia
Editor for Materials and Chemical Technologies
Dr. Radovan Karkalić, University of Defence in Belgrade, Military Academy, Belgrade, Serbia
Technical editor
Nebojša Gaćeša, MSc, University of Defence in Belgrade, Military Academy, Belgrade, Serbia,
e-mail: nebojsa.gacesa@mod.gov.rs, tel. +381 11 3603 260, +381 66 87 00 123

САДРЖАЈ

ОРИГИНАЛНИ НАУЧНИ РАДОВИ

ПРЕГЛЕДНИ РАДОВИ

СОДЕРЖАНИЕ

ОРИГИНАЛЬНЫЕ НАУЧНЫЕ СТАТЬИ

ОБЗОРНЫЕ СТАТЬИ

CONTENTS

ORIGINAL SCIENTIFIC PAPERS

REVIEW PAPERS

FIXED POINT THEOREM IN A PARTIAL b-METRIC SPACE APPLIED TO QUANTUM OPERATIONS

Rakesh Tiwari[a], *Mohammad Saeed* Khan[b], *Shoba* Rani[c], *Nicola* Fabiano[d]

[a] Government V. Y. T. Post-Graduate Autonomous College,
Department of Mathematics, Durg, Chhattisgarh, Republic of India,
e-mail: rtiwari@govtsciencecollegedurg.ac.in,
ORCID iD: https://orcid.org/0000-0002-6112-0116

[b] Sefako Makgatho Health Sciences University,
Department of Mathematics and Applied mathematics,
Ga-Rankuwa, Republic of South Africa,
e-mail: drsaeed9@gmail.com,
ORCID iD: https://orcid.org/0000-0003-0216-241X

[c] Government V. Y. T. Post-Graduate Autonomous College,
Department of Mathematics, Durg, Chhattisgarh, Republic of India,
e-mail: shobharaniy89@gmail.com,
ORCID iD: https://orcid.org/0000-0001-9143-5410

[d] University of Belgrade, “Vinča” Institute of Nuclear Sciences - National Institute of the Republic of Serbia, Belgrade, Republic of Serbia,
e-mail: nicola.fabiano@gmail.com, **corresponding author**,
ORCID iD: https://orcid.org/0000-0003-1645-2071

DOI: 10.5937/vojtehg70-37109;https://doi.org/10.5937/vojtehg70-37109

FIELD: Mathematics
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: A fixed point theorem of an order-preserving mapping on a complete partial b-metric space satisfying a contractive condition is constructed.

Methods: Extension of the results of Batsari et al.

Results: The fidelity of quantum states is used to construct the existence of a fixed quantum state.

Conclusions: The fixed quantum state is associated to an order-preserving quantum operation.

Key words: partial b-metric space, order-preserving mapping, quantum operation, fidelity of quantum state, Bloch vector.

Introduction and preliminaries

A partial metric space is a generalized metric space in which each object does not necessarily have a zero distance from itself (Aamri & El Moutawakil, 2002). Another angle of fixed point research emerged with the approach of the Knaster-Tarski fixed point theorem (Knaster, 1928; Tarski, 1955). The idea was first initiated from Knaster and Tarski in 1927 (Knaster, 1928), and later Tarski found some improvement of the work in 1939, which he discussed in some public lectures between 1939 and 1942 (Tarski, 1955, 1949). Finally, in 1955, Tarski (Tarski, 1955) published the comprehensive results together with some applications. A different property of this theorem is that it involves an order relation defined on the space of consideration. Indeed, the order relation serves as an alternative to the continuity and contraction of the mappings as found in the Brouwer (Brouwer, 1911) and Banach (Banach, 1922) fixed point theorems, respectively, see (Tarski, 1955).

After the approach of the Brouwer (Brouwer, 1911), Banach (Banach, 1922) and Knaster-Tarski (Tarski, 1955) fixed point theorems, many researchers become involved in extension (Browder, 1959; Leray & Schauder, 1934; Schauder, 1930), generalization (Batsari et al, 2018; Browder, 1959; Du et al, 2018) and improvements (Batsari et al, 2018; Batsari & Kumam, 2018; Kannan, 1972; Khan et al, 1984) of the theorems using different spaces and functions. In the way of generalizing spaces was Bourbaki-Bakhtin-Cezerwik's b-metric space (Bakhtin, 1989; Bourbaki, 1974; Czerwik, 1993), Matthews's partial metric space (Matthews, 1994) and Shukla's Partial b-metric space (Shukla, 2014).

In the area of the quantum information theory, a qubit is seen as a quantum system, whereas a quantum operation can be inspected as the measurement of a quantum system; it describes the development of the system through the quantum states. Measurements have some errors which can be corrected through quantum error correction codes. The quantum error correction codes are easily developed through the information-preserving structures with the help of the fixed points set of the associated quantum operation. Therefore, the study of quantum operations is necessary in the field of the quantum information theory, at least in developing the error correction codes, knowing the state of the system (qubit) and the description of energy dissipation effects due to loss of energy from a quantum system (Nielsen & Chuang, 2000).

In 1951, Luders (Lüders, 1950) discussed the compatibility of quantum states in measurements (quantum operations). He also proved that the compatibility of quantum states in measurements is equivalent to the commutativity of the states with each quantum effects in the measurement.

In 1998, Busch et al. (Busch & Singh, 1998) generalized the Luders theorem. He also showed that a state is unchanged under a quantum operation if the state commutes with every quantum effect that relates the quantum operation. In 2002, Arias et al. (Arias et al, 2002) studied the fixed point sets of a quantum operation and gave some conditions for which the set is equal to a commutate set of the quantum effects that described the quantum operation. In 2011, Long and Zhang (Zhang & Ji, 2012) deliberated the fixed point set for quantum operations, they presented some necessary and sufficient conditions for the existence of a non-trivial fixed point set. Similarly, in 2012, Zhang and Ji (Long & Zhang, 2011) deliberated the existence of a non-trivial fixed point set of a generalized quantum operation. In 2016, Zhang and Si (Zhang & Si, 2016) explored the conditions for which the fixed point set of a quantum operation $(\phi_{\mathcal{A}})$ with respect to a row contraction $\mathcal{A}$ equals to the fixed point set of the power of the quantum operation $(\phi^{j}_{\mathcal{A}})$ for some $1 \leq j < +\infty$. Other useful references are (Agarwal et al, 2015; Debnath et al, 2021; Kirk & Shahzad, 2014).

Definition 1. (Shukla, 2014) A **partial b-metric** on the set X is a function $p_s : X \times X \to \mathbb{R}_+$ such that,
(1) For all $x, y \in X,\ x = y$ iff $p_s(x,x) = p_s(x,y) = p_s(y,y)$
(2) For all $x, y \in X,\ p_s(x,x) \leq p_s(x,y)$
(3) For all $x, y \in X,\ p_s(x,y) = p_s(y,x)$
(4) There exists a real number $s \geq 1$ such that, for all $x, y, z \in X,\ p_s(x,z) \leq s[p_s(x,y) + p_s(y,z)] - p_s(y,y)$.
(X, p_s) denotes the partial b-metric space. Note that every partial metric is

a partial b-metric with $s = 1$. Also, every b-metric is a partial b-metric with $p_s(x, x) = 0, \text{ for all } x, y \in X$.

A sequence $\{x_n\}$ in the space (X, p_s) converges with respect to the topology τ_b to a point $x \in X$, if and only if

$$\lim_{n\to+\infty} p_s(x_n, x) = p_s(x, x). \tag{1}$$

The sequence $\{x_n\}$ is Cauchy in (X, p_s) if the below limit exists and is finite

$$\lim_{n,m\to+\infty} p_s(x_n, x_m) < +\infty. \tag{2}$$

A partial b-metric space (X, p_s) is complete, if every Cauchy sequence $\{x_n\}$ in (X, p_s) converges to a point $x \in X$ such that,

$$\lim_{n,m\to+\infty} p_s(x_n, x_m) = p_s(x, x). \tag{3}$$

DEFINITION 2. A mapping T is said to be order-preserving on X, whenever $x \preceq y$ implies $T(x) \preceq T(y) \text{ for all } x, y \in X$.

Main result

The objective of this work is to establish a fixed point theorem in a complete partial b-metric space.

THEOREM 1. Let (X, p_s) be a complete partial b-metric space with $s \geq 1$ and associated with a partial order $\preceq$. Suppose an order preserving mapping $T : X \to X$ satisfies

$$\begin{aligned} p_s(T(x), T(y)) \leq{} & \alpha \max\{p_s(x, y), p_s(x, T(y)), p_s(y, T(x))\} \\ & + \frac{\beta}{2} \min\{p_s(x, T(y)) + p_s(y, T(x)), p_s(x, T(x)) + p_s(y, T(y))\} \end{aligned} \tag{4}$$

for all comparable $x, y \in X$, where $\alpha, \beta \in [0, \theta]$ and $\theta = \min\{\frac{1}{s^3}, \frac{2}{s+1}\}$. If there exists $x_0 \in X$ such that $x_0 \preceq T(x_0)$, then T has a unique fixed point $\hat{x} \in X$ such that $p_s(\hat{x}, \hat{x}) = 0$.

Proof. Suppose $x_0 \neq T(x_0)$, define a sequence $\{x_n\} \subseteq X$ by $x_n = T^n(x_0)$ and let $q_n = p_s(x_n, x_{n+1})$. It is clear that if $x_n = x_{n+1}$ for some natural number n, then x_n is a fixed point of T, i.e., $x_{n+1} = T(x_n) = x_n$. Let $x_{n+1} \neq x_n$ for all $n \in N$. Then, we proceed as follows:

$$\begin{aligned}
q_n = {} & p_s(x_n, x_{n+1}) = p_s(T(x_{n-1}), T(x_n)) \\
\leq {} & \alpha \max\{p_s(x_{n-1}, x_n), p_s(x_{n-1}, T(x_n)), p_s(x_n, T(x_{n-1}))\} \\
& + \frac{\beta}{2} \min\{p_s(x_{n-1}, T(x_n)) + \\
& p_s(x_n, T(x_{n-1})), p_s(x_{n-1}, T(x_{n-1})) + p_s(x_n, T(x_n))\} \\
= {} & \alpha \max\{p_s(x_{n-1}, x_n), p_s(x_{n-1}, x_{n+1}), p_s(x_n, x_n)\} \\
& + \frac{\beta}{2} \min\{p_s(x_{n-1}, x_{n+1}) + p_s(x_n, x_n), p_s(x_{n-1}, x_n) + p_s(x_n, x_{n+1})\} \\
= {} & \alpha \max\{p_s(x_{n-1}, x_n), s[p_s(x_{n-1}, x_n) + p_s(x_n, x_{n+1})]\} \\
& + \frac{\beta}{2} [\frac{s[p_s(x_{n-1}, x_n) + p_s(x_n, x_{n+1})] + p_s(x_{n-1}, x_n) + p_s(x_n, x_{n+1})}{2}] \\
= {} & \alpha(s[p_s(x_{n-1}, x_n) + p_s(x_n, x_{n+1})]) + \\
& \frac{\beta}{2}(s+1)[\frac{p_s(x_{n-1}, x_n) + p_s(x_n, x_{n+1})}{2}] \\
= {} & \alpha s + \frac{\beta(s+1)}{4}(p_s(x_{n-1}, x_n) + p_s(x_n, x_{n+1})) \\
= {} & \frac{4\alpha s + \beta s + \beta}{4}(p_s(x_{n-1}, x_n) + p_s(x_n, x_{n+1})) \\
= {} & \frac{4\alpha s + \beta s + \beta}{4}(q_{n-1} + q_n).
\end{aligned}$$

Thus, we have

$$q_n \leq \frac{4\alpha s + \beta s + \beta}{4}(q_{n-1} + q_n)$$

which implies

$$(\frac{4 - 4\alpha s - \beta s - \beta}{4})q_n \leq (\frac{4\alpha s + \beta s + \beta}{4})q_{n-1} \tag{5}$$

By simplifying (5), we have

$$q_n \leq (\frac{4\alpha s + \beta s + \beta}{4 - 4\alpha s - \beta s - \beta})q_{n-1} \tag{6}$$

For $\theta \in \min\{\frac{1}{s^3}, \frac{2}{s+1}\}$, we deduce that

$$0 \leq \frac{4\alpha s + \beta s + \beta}{4 - 4\alpha s - \beta s - \beta} \leq 1.$$

Therefore, from(6), we conclude that $p_s(x_n, x_{n+1}) = q_n \leq q_{n-1} = p_s(x_{n-1}, x_n)$. Thus, $\{q_n\}_{n=1}^{+\infty}$ is a monotone non-increasing sequence of real numbers and bounded below by 0. Therefore, $\lim_{n\to+\infty} q_n = 0$, see Chidume et al.(Chidume & Chidume, 2014).

Next, we show $\{x_n\}_{n=1}^{+\infty}$ is Cauchy. Let $x_n, x_m \in X$, for all $n, m \in \mathbb{N}$. Then,

$$\begin{aligned}
p_s(x_n, x_m) &= p_s(T^n x_0, T^m x_0)\\
&= p_s(T(x_{n-1}), T(x_{m-1}))\\
&= \alpha \max\{p_s(x_{n-1}, x_{m-1}), p_s(x_{n-1}, x_m), p_s(x_n, x_{m-1})\}\\
&+\frac{\beta}{2} \min p_s(x_{n-1}, x_m) + p_s(x_{m-1}, x_n), p_s(x_{n-1}, x_n) + p_s(x_{m-1}, x_m)\\
&= \alpha \max\{s(p_s(x_{n-1}, x_n) + p_s(x_n, x_{m-1})), p_s(x_{n-1}, x_m), p_s(x_n, x_{m-1})\}\\
&+\frac{\beta}{2}\{\frac{p_s(x_{n-1}, x_m) + p_s(x_{m-1}, x_n) + p_s(x_{n-1}, x_n) + p_s(x_{m-1}, x_m)}{2}\}\\
&= \alpha \max\{s(p_s(x_{n-1}, x_n) + s(p_s(x_n, x_m) + p_s(x_m, x_{m-1}))), p_s(x_{n-1}, x_n)\\
&+p_s(x_{m-1}, x_m)\} + \frac{\beta}{4}(s(p_s(x_{n-1}, x_n) + p_s(x_n, x_m)) + s(p_s(x_{m-1}, x_m)\\
&+p_s(x_m, x_n)) + p_s(x_{n-1}, x_n) + p_s(x_{m-1}, x_m)\\
&= \alpha s(p_s(x_{n-1}, x_n) + s(p_s(x_n, x_m) + p_s(x_m, x_{m-1}))\\
&+\frac{\beta}{4}(sp_s(x_{n-1}, x_n) + 2sp_s(x_n, x_m) + sp_s(x_{m-1}, x_m)\\
&+p_s(x_{n-1}, x_n) + p_s(x_{m-1}, x_m))\\
&\leq (\alpha s + \frac{s\beta}{4} + \frac{\beta}{4})p_s(x_{n-1}, x_n) + (\alpha s^2 + \frac{s\beta}{2})p_s(x_n, x_m)\\
&+(\alpha s^2 + \frac{s\beta}{4} + \frac{\beta}{4})p_s(x_{m-1}, x_m), \qquad (7)
\end{aligned}$$

implies that

$$\begin{aligned}
(1 - (\alpha s^2 + \frac{s\beta}{2}))p_s(x_n, x_m) &\leq (\alpha s + \frac{s\beta}{4} + \frac{\beta}{4})p_s(x_{n-1}, x_n) +\\
&(\alpha s^2 + \frac{s\beta}{4} + \frac{\beta}{4})p_s(x_{m-1}, x_m)\\
&\leq \frac{2}{2 - 2\alpha s^2 - s\beta}((\alpha s + \frac{s\beta}{4} + \frac{\beta}{4})p_s(x_{n-1}, x_n)\\
&+(\alpha s^2 + \frac{s\beta}{4} + \frac{\beta}{4})p_s(x_{m-1}, x_m)). \qquad (8)
\end{aligned}$$

Now, taking the limit as $n, m \to +\infty$ in (7), we have

$$\lim_{n,m\to+\infty} p_s(x_n, x_m) = 0.$$

Therefore, $\{x_n\}$ is a Cauchy sequence in X. For X being complete, there exists $\hat{x} \in X$ such that

$$\lim_{n\to+\infty} p_s(x_n, \hat{x}) = \lim_{n,m\to+\infty} p_s(x_n, x_m) = p_s(\hat{x}, \hat{x}) = 0.$$

Now, we proceed to prove the existence of the fixed point of T satisfying (1). Let $x_0 \in X$ be such that $x_0 \preceq T(x_0)$. If $T(x_0) = x_0$ then, x_0 is a fixed point of T. Recall that, T is order-preserving and $x_0 \preceq T(x_0)$ then, we have $x_0 \preceq T(x_0) = x_1$, $x_1 \preceq T(x_1) = x_2$, $x_2 \preceq T(x_2) = x_3$, $\cdots$, $x_n \preceq T(x_n) = x_{n+1}$. By transitivity of $\preceq$, we have $x_0 \preceq x_1 \preceq x_2 \preceq x_3 \preceq \cdots \preceq x_n \preceq x_{n+1} \preceq \cdots$.
For showing $\hat{x} \in X$ is a fixed point of T, we proceed as follows:

$$\begin{aligned} p_s(\hat{x}, T(\hat{x})) &\le s[p_s(\hat{x}, x_{n+1}) + p_s(x_{n+1}, T(\hat{x})] - p_s(x_{n+1}, x_{n+1}) \\ &\le s[p_s(\hat{x}, x_{n+1}) + p_s(T(x_n), T(\hat{x})] \\ \le s\big[&p_s(\hat{x}, x_{n+1}) + \alpha \max\{p_s(x_n, \hat{x}), p_s(x_n, T(\hat{x})), p_s(\hat{x}, T(x_n))\} \\ +\frac{\beta}{2}\min\{&p_s(x_n, T(\hat{x})) + p_s(\hat{x}, T(x_n)), p_s(x_n, T(x_n)) + p_s(\hat{x}, T(\hat{x}))\}\big] \\ \le s\big[&p_s(\hat{x}, x_{n+1}) + \alpha \max\{p_s(x_n, \hat{x}), p_s(x_n, T(\hat{x})), p_s(\hat{x}, T(x_n))\} \\ +\frac{\beta}{4}(&p_s(x_n, T(\hat{x})) + p_s(\hat{x}, T(x_n)) + p_s(x_n, T(x_n)) + p_s(\hat{x}, T(\hat{x})))\big]. \end{aligned} \tag{9}$$

Case I: Suppose $\max\{p_s(x_n, \hat{x}), p_s(x_n, T(\hat{x})), p_s(\hat{x}, T(x_n))\} = p_s(x_n, \hat{x})$. Then, from inequality (9), we have

$$\begin{aligned} p_s(\hat{x}, T(\hat{x})) &\le s\big[p_s(\hat{x}, x_{n+1}) + \alpha p_s(x_n, \hat{x}) \\ +\frac{\beta}{2}&\Big(\frac{p_s(x_n, T(\hat{x})) + p_s(\hat{x}, T(x_n)) + p_s(x_n, T(x_n)) + p_s(\hat{x}, T(\hat{x}))}{2}\Big)\big] \\ &\le sp_s(\hat{x}, x_{n+1}) + s\alpha p_s(x_n, \hat{x}) + \frac{s\beta}{4}(s(p_s(x_n, \hat{x}) + p_s(\hat{x}, T(\hat{x}))) \\ &+p_s(\hat{x}, x_{n+1}) + p_s(x_n, x_{n+1}) + p_s(\hat{x}, T(\hat{x}))) \\ &= (s + \frac{s\beta}{4})p_s(\hat{x}, x_{n+1}) + (s\alpha + \frac{s^2\beta}{4})p_s(x_n, \hat{x}) \\ &+(\frac{s^2\beta}{4} + \frac{s\beta}{4})p_s(\hat{x}, T(\hat{x}) + \frac{s\beta}{4}p_s(x_n, x_{n+1}). \end{aligned}$$

From the above inequality, we have

$$(1-\frac{s^2\beta}{4}-\frac{s\beta}{4})p_s(\hat{x},T(\hat{x}))\leq(s+\frac{s\beta}{4})p_s(\hat{x},x_{n+1})+$$
$$(s\alpha+\frac{s^2\beta}{4})p_s(x_n,\hat{x})+\frac{s\beta}{4}p_s(x_n,x_{n+1}),$$

which implies

$$\begin{aligned}p_s(\hat{x},T(\hat{x}))\leq\frac{4}{4-s^2\beta-s\beta}\big[(s+\frac{s\beta}{4})p_s(\hat{x},x_{n+1})+\\ (s\alpha+\frac{s^2\beta}{4})p_s(x_n,\hat{x})+\frac{s\beta}{4}p_s(x_n,x_{n+1})\big].\end{aligned}\tag{10}$$

We can observe that for $\beta\in\min\{\frac{1}{s^3},\frac{2}{s+1}\}$,

$$\begin{aligned}4-s^2\beta-s\beta&=4-s^2\beta-s\beta\\&=4-s\beta(s+1).\end{aligned}\tag{11}$$

If $\beta=\frac{1}{s^3}$, then, from equality (11) we have

$$\begin{aligned}4-s^2\beta-s\beta&=4-s\beta(s+1)\\&=4-s(s+1)\frac{1}{s^3}\\&=4-\frac{s+1}{s^2}\\&>0\ \text{ for all } s\geq1.\end{aligned}\tag{12}$$

Similarly, if $\beta=\frac{2}{s+1}$, then, from equality (11),

$$\begin{aligned}4-s^2\beta-s\beta&=4-s\beta(s+1)\\&=4-(s+1)s\frac{2}{s+1}\\&\leq4-s(s+1)\frac{1}{s^3}\\&>0\ \text{ for all } s\geq1.\end{aligned}\tag{13}$$

From equalities (12) and (13), we conclude that the right-hand side of (10) is non-negative.

Case II: Suppose $\max\{p_s(x_n,\hat{x}), p_s(x_n,T(\hat{x})), p_s(\hat{x},T(x_n))\} = p_s(x_n,T(\hat{x}))$. Then, from inequality (9),
we have

$$\begin{aligned}
p_s(\hat{x},T(\hat{x})) &\le s\big[p_s(\hat{x},x_{n+1}) + \alpha p_s(x_n,T(\hat{x})) \\
&+\frac{\beta}{2}(\frac{p_s(x_n,T(\hat{x})) + p_s(\hat{x},T(x_n)) + p_s(x_n,T(x_n)) + p_s(\hat{x},T(\hat{x}))}{2})\big] \\
&\le s\big[p_s(\hat{x},x_{n+1}) + \alpha s(p_s(x_n,\hat{x}) + p_s(\hat{x},T(\hat{x}))) \\
&+\frac{\beta}{4}(s(p_s(x_n,\hat{x}) + p_s(\hat{x},T(\hat{x}))) + p_s(\hat{x},x_{n+1}) + p_s(x_n,x_{n+1}) + p_s(\hat{x},T(\hat{x})))\big] \\
&\le (s+\frac{\beta}{4}s)p_s(\hat{x},x_{n+1}) + (s^2\alpha + \frac{\beta}{4}s^2)p_s(x_n,\hat{x}) \\
&+(s^2\alpha + \frac{\beta}{4}s^2 + \frac{\beta}{4}s)p_s(\hat{x},T(\hat{x})) + \frac{\beta}{4}sp_s(x_n,x_{n+1}),
\end{aligned}$$

from the above inequality, we have

$$\begin{aligned}
(1 - s^2\alpha - \frac{\beta}{4}s^2 - \frac{\beta}{4}s)p_s(\hat{x},T(\hat{x})) \le\ & (s+\frac{\beta}{4}s)p_s(\hat{x},x_{n+1}) \\
&+(s^2\alpha + \frac{\beta}{4}s^2)p_s(x_n,\hat{x}) + \frac{\beta}{4}sp_s(x_n,x_{n+1}),
\end{aligned}$$

so that

$$\begin{aligned}
p_s(\hat{x},T(\hat{x})) \le\ & \frac{4}{4 - 4s^2\alpha - \beta s^2 - \beta s}\big[(s+\frac{\beta}{4}s)p_s(\hat{x},x_{n+1}) \\
&+(s^2\alpha + \frac{\beta}{4}s^2)p_s(x_n,\hat{x}) + \frac{\beta}{4}sp_s(x_n,x_{n+1})\big] \qquad (14)
\end{aligned}$$

from the fact that $\theta \in \min\{\frac{1}{s^3}, \frac{2}{s+1}\}$, we have if $\alpha > \beta$ then by (14), we have

$$\begin{aligned}
4 - 4s^2\alpha - \beta s^2 - \beta s &= 4 - 4s^2\beta + \beta s^2 + \beta s \\
&= 4 - (5s+1)s\beta. \qquad (15)
\end{aligned}$$

If $\beta = \frac{1}{s^3}$ by (15), we have

$$\begin{aligned}
4 - 4s^2\alpha - \beta s^2 - \beta s &= 4 - (5s+1)s\beta \\
&= 4 - (5s+1)s\frac{1}{s^3} \\
&\ge 0 \quad \text{for all } s \ge 1. \qquad (16)
\end{aligned}$$

If $\beta = \frac{2}{s+1}$ by (15), we have

$$\begin{aligned} 4 - 4s^2\alpha - \beta s^2 - \beta s &= 4 - (5s+1)s\beta \\ &= 4 - (5s+1)s\frac{2}{s+1} \\ &\leq 4 - (5s+1)s\frac{1}{s^3} \\ &\geq 0 \quad \text{for all } s \geq 1. \end{aligned} \tag{17}$$

From inequalities (16) and (17), we conclude that the right-hand side of (10) is non-negative.

If $\alpha < \beta$, then by (14), we have

$$\begin{aligned} 4 - 4s^2\alpha - \beta s^2 - \beta s &= 4 - 4s^2\alpha + \alpha s^2 + \beta s \\ &= 4 - 5s^2\alpha + s\alpha \\ &= 4 - (5s+1)s\alpha. \end{aligned} \tag{18}$$

Similarly for (18), we conclude that the right-hand side of (10) is non-negative.

Case III: Suppose $\max\{p_s(x_n,\hat{x}), p_s(x_n,T(\hat{x})), p_s(\hat{x},T(x_n))\} = p_s(\hat{x},T(x_n)))$. Then, from inequality (9), we have

$$\begin{aligned} p_s(\hat{x},T(\hat{x})) &\leq s\big[p_s(\hat{x},x_{n+1}) + \alpha p_s(\hat{x},T(x_n))) \\ &+\frac{\beta}{4}(p_s(x_n,T(\hat{x})) + p_s(\hat{x},T(x_n)) + p_s(x_n,T(x_n)) + p_s(\hat{x},T(\hat{x})))\big] \\ &\leq s\big[p_s(\hat{x},x_{n+1}) + \alpha s p_s(\hat{x},x_{n+1}) \\ &+\frac{\beta}{4}(s(p_s(x_n,\hat{x}) + p_s(\hat{x},T(\hat{x}))) + p_s(\hat{x},x_{n+1}) + p_s(x_n,x_{n+1}) + p_s(\hat{x},T(\hat{x})))\big] \\ &\leq \ (s + \alpha s + \frac{\beta}{4}s)p_s(\hat{x},x_{n+1}) + \frac{\beta}{4}s^2 p_s(x_n,\hat{x}) \\ &+(\frac{\beta}{4}s^2 + \frac{\beta}{4}s)p_s(\hat{x},T(\hat{x})) + \frac{\beta}{4}s p_s(x_n,x_{n+1}). \end{aligned}$$

By the simplification of the above equality, we have

$$\begin{aligned} p_s(\hat{x},T(\hat{x}) \leq \ &\frac{4}{4 - s^2\beta - s\beta}\big[(s + \alpha s + \frac{\beta}{4}s)p_s(\hat{x},x_{n+1}) \\ &+\frac{\beta}{4}s^2 p_s(x_n,\hat{x}) + \frac{\beta}{4}s p_s(x_n,x_{n+1})\big]. \end{aligned} \tag{19}$$

Note that, for any value of $\alpha, \beta \in [0, \theta)$ and $4 - s^2\beta - s\beta \geq 0$. Thus, the right-hand side of (10) is non-negative. Taking the limit as $n \to +\infty$ of both sides in the respective inequalities (10), (14) and (19), we conclude that

$$\begin{aligned} p_s(\hat{x}, T(\hat{x})) &= \lim_{n\to+\infty} p_s(\hat{x}, T(\hat{x})) \\ &= 0. \end{aligned}$$

Thus, $T(\hat{x}) = \hat{x}$.
Next, we prove that if $\hat{x} \in X$ is a fixed point of T, then $p_s(\hat{x}, \hat{x}) = 0$.
Suppose $p_s(\hat{x}, \hat{x}) \neq 0$. Then

$$\begin{aligned} p_s(\hat{x}, \hat{x}) &= p_s(T(\hat{x}, \hat{x})) \\ &\leq \alpha \max\{p_s(\hat{x}, \hat{x}), p_s(\hat{x}, \hat{x})), p_s(\hat{x}, \hat{x}))\} \\ &+ \frac{\beta}{2} \min\{p_s(\hat{x}, \hat{x})) + p_s(\hat{x}, T(\hat{x})), p_s(\hat{x}, \hat{x})) + p_s(\hat{x}, T(\hat{x}))\} \\ &= \alpha \max\{p_s(\hat{x}, \hat{x}), p_s(\hat{x}, \hat{x}), p_s(\hat{x}, \hat{x})\} \\ &+ \frac{\beta}{2} \min\{p_s(\hat{x}, \hat{x}) + p_s(\hat{x}, \hat{x}), p_s(\hat{x}, \hat{x}) + p_s(\hat{x}, \hat{x})\} \\ &= (\alpha + \beta) p_s(\hat{x}, \hat{x}) \\ &= \theta p_s(\hat{x}, \hat{x}) \\ &< p_s(\hat{x}, \hat{x}). \end{aligned}$$

This is contradicting the fact that $p_s(\hat{x}, \hat{x}) \neq 0$. Therefore, $p_s(\hat{x}, \hat{x}) = 0$.

Last, we will prove the uniqueness of the fixed point. Let $x_1, x_2 \in X$ be two distinct fixed points of T. Then

$$\begin{aligned} p_s(x_1, x_2) &= p_s(T(x_1), T(x_2)) \\ &\leq \alpha \max\{p_s(x_1, x_2), p_s(x_1, T(x_2)), p_s(x_2, T(x_1))\} \\ &+ \frac{\beta}{2} \min\{p_s(x_1, T(x_2)) + p_s(x_2, T(x_1)), p_s(x_1, T(x_1)) + p_s(x_2, T(x_2))\} \\ &= \alpha \max\{p_s(x_1, x_2), p_s(x_1, x_2), p_s(x_1, x_2)\} \\ &+ \frac{\beta}{2} \min\{p_s(x_1, x_2) + p_s(x_1, x_2), p_s(x_1, x_2) + p_s(x_1, x_2)\} \\ &= (\alpha + \beta) p_s(x_1, x_2) \\ &= \theta p_s(x_1, x_2) \\ &< p_s(x_1, x_2). \end{aligned}$$

This is a contradiction. Therefore, the fixed point is unique. □

REMARK 2. If we take $\alpha = \frac{\beta}{2}$ and $p_s(x, T(y)) + p_s(y, T(x)) \geq p_s(x, T(x)) + p_s(y, T(y))$ then we find Theorem 1 of Batsari et al. (Batsari & Kumam, 2020).

COROLLARY 3. Let (X, p) be a complete partial metric space associated with a partial order $\preceq$. Suppose an order-preserving mapping $T : X \to X$ satisfies

$$p_s(T(x), T(y)) \leq \alpha \max\{p_s(x, y), p_s(x, T(y)), p_s(y, T(x))\}$$
$$+\frac{\beta}{2} \min p_s(x, T(y)) + p_s(y, T(x)), p_s(x, T(x)) + p_s(y, T(y)) \tag{20}$$

for all comparable $x, y \in X$, where $\theta \in [0, 1]$. If there exists $x_0 \in X$ such that $x_0 \preceq T(x_0)$, then T has a unique fixed point $\hat{x} \in X$ and $p(\hat{x}, \hat{x}) = 0$.

Now we apply our main result similar to (Batsari & Kumam, 2020) as follows:

Application to quantum operations

In quantum systems, measurements can be seen as quantum operations (Seevinck, 2003). Quantum operations are very important in narrating quantum systems that collaborate with the environment.

Let $\mathcal{B}(H)$ be the set of bounded linear operators on the separable complex Hilbert space H; $\mathcal{B}(H)$ is the state space of consideration. Suppose $\mathcal{A} = \{A_i, A_i^* : i = 1, 2, 3, \dots\}$ is a collection of operators $A_i's \in \mathcal{B}(H)$ satisfying $\sum A_i A_i^* \leq I$. A map $\phi : \mathcal{B}(H) \to \mathcal{B}(H)$ of the form $\phi_{\mathcal{A}}(B) = \sum A_i B A_i^*$ is called a quantum operation (Arias et al, 2002), quantum operations can be used in quantum measurements of states. If the A_i's are self adjoint then, $\phi_{\mathcal{A}}$ is self-adjoint.

General quantum measurements that have more than two values are narrated by effect-valued measures (Arias et al, 2002). Denote the set of quantum effects by $\varepsilon(H) = \{A \in \mathcal{B}(H) : 0 \leq A \leq I\}$. Consider the discrete effect-valued measures narrated by a sequence of $E_i \in \varepsilon(H), i = 1, 2, \dots$ satisfying $E_i = I$ where the sum converges in the strong operator topology. Therefore, the probability that outcome i eventuates in the state ρ is $_\rho(E_i)$

and the post-measurement state given that i eventuates is $\frac{E_i^{\frac{1}{2}}\rho E_i^{\frac{1}{2}}}{tr\rho E_i}$ (Arias et al, 2002). Furthermore, the resulting state after the implementation of measurement without making any consideration is given by

$$\phi(\rho) = \sum E_i^{\frac{1}{2}}\rho E_i^{\frac{1}{2}} \tag{21}$$

If the measurement does not disturb the state ρ, then we have $\phi(\rho) = \rho$. Furthermore, the probability that an effect A eventuates in the state r given that the measurement was conducted is

$$P_{\phi(\rho)}(A) = tr\left[A\sum E_i^{\frac{1}{2}}\rho E_i^{\frac{1}{2}}\right] = tr\left(\sum E_i^{\frac{1}{2}}\rho E_i^{\frac{1}{2}}\rho\right) \tag{22}$$

If A is not interrupted by the measurement in any state we have

$$\sum E_i^{\frac{1}{2}}\rho E_i^{\frac{1}{2}} = A,$$

and by defining $\phi(A) = \sum E_i^{\frac{1}{2}}\rho E_i^{\frac{1}{2}}$, we end up with $\phi(A) = A$.

From now, we will be dealing with a bi-level $(|0\rangle, |1\rangle)$ single qubit quantum system where a quantum state $|\Psi\rangle$ can be narrated as

$$|\Psi\rangle = a|0\rangle + b|1\rangle,\ \text{with } a, b \in \mathbb{C} \ \text{ and } \ |a|^2 + |b|^2 = 1$$

see (Batsari & Kumam, 2020; Nielsen & Chuang, 2000). Considering the characterization of a bi-level quantum system by the Bloch sphere (Figure 1) above, a quantum state $(|\Psi\rangle)$ can be represented with the density matrix below (ρ),

$$|\Psi\rangle = \rho = \frac{1}{2}\begin{pmatrix} 1+\eta\cos\theta & \eta\cos\phi\sin\theta - i\eta\sin\phi\sin\theta \\ \eta\cos\phi\sin\theta + i\eta\sin\phi\sin\theta & 1-\eta\cos\theta \end{pmatrix},$$
$$\eta \in [0,1],\ 0 \leq \theta \leq \pi,\ and\ 0 \leq \phi \leq 2\pi. \tag{23}$$

Also, the density (ρ) matrix is,

$$\rho = \frac{1}{2}[I + \overline{r_\rho}.\overline{\sigma}] = \frac{1}{2}\begin{bmatrix} 1+r_z & r_x - ir_y \\ r_x + ir_y & 1-r_z, \end{bmatrix} \tag{24}$$

where $\overline{r_\rho} = [r_x, r_y, r_z]$ is the Bloch vector with $\|\overline{r_\rho}\| \leq 1$, and $\overline{\sigma} = [\sigma_x, \sigma_y, \sigma_z]$ where

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1, \end{pmatrix}$$

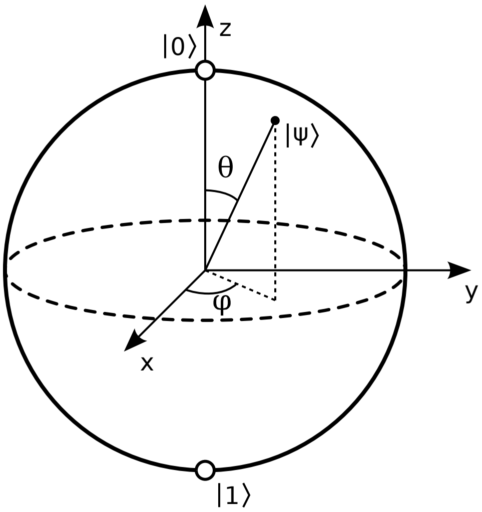


Figure 1 – Bloch sphere
Рис. 1 − Сфера Блоха
Слика 1 – Блохова сфера

Let ρ, σ be two quantum states in a bi-level quantum system. Then, the Bures fidelity (Bures, 1969) between the quantum states ρ and σ is defined as

$$F(\rho, \sigma) = [tr\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}]^2.$$

The Bures fidelity satisfies $0 \leq F(\rho, \sigma) \leq 1$, if $\rho = \sigma$ it takes the value 1 and 0 if ρ and σ have an orthogonal support (Nielsen & Chuang, 2000).

Now consider a two-level quantum system X represented with the collection of density matrices $\{\rho : \rho$ is as defined in Equation (24)$\}$. Define the function $p_s : X \times X \to \mathbb{R}_+$ as follows:

$$p_s(\rho, \delta) = \begin{cases} \max\{\|\overline{r_\rho}\|, \|\overline{r_\delta}\|\}e^{\frac{1}{6}(1-F(\rho,\delta))}, & \rho \neq \delta, \\ 0, & \rho = \delta. \end{cases}$$

It is easy to show that p_s is a b-metric on X with s taking the value 1 approximately. They also define an order relation $\preceq$ on X by

$$\rho \preceq \delta \text{ iff the line from the origin joining the point } \overline{r_\delta} \text{ passes through } \overline{r_\rho}. \tag{25}$$

It is easy to show that the order relation defined above is a partial order (Batsari & Kumam, 2020).
As in (Batsari & Kumam, 2020), we find the following corollary.

COROLLARY 4. Let (p_s, X) be a complete partial b-metric space associated with the above order $\preceq$. Suppose an order-preserving quantum operation $T : X \to X$ that satisfies conditions in Theorems 1. Then, T has a fixed point.

The following example validates our main result.

EXAMPLE 0.1. Consider the depolarizing quantum operation T on the Bloch sphere X; $T(\rho) = \frac{I}{2}p + (1-p)\rho$ with the depolarizing parameter $p \in [0, 1]$. Let the comparable quantum states satisfy (25).

We examine that $T : X \to X$ satisfies all the conditions of our theorem. Now, let $\rho, \delta \in X$. We show that T is order preserving with definition (25). For this, we will prove that if $\rho \preceq \delta$ then $T(\rho) \preceq T(\delta)$.

Therefore, as (Batsari & Kumam, 2020) using the Bloch sphere representation of states in a bi-level quantum system below

$$\rho = \frac{1}{2}\begin{pmatrix} 1+\mu\cos\theta & \mu\cos\phi\sin\theta - i\mu\sin\phi\sin\theta \\ \mu\cos\phi\sin\theta + i\mu\sin\phi\sin\theta & 1-\mu\cos\theta \end{pmatrix},$$
$$\mu \in [0,1],\ 0 \le \theta \le \pi,\ and\ 0 \le \phi \le 2\pi,$$

So,

$$T(\rho) = \frac{1}{2}\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} +$$
$$\frac{1-p}{2}\begin{pmatrix} 1+\mu\cos\theta & \mu\cos\phi\sin\theta - i\mu\sin\phi\sin\theta \\ \mu\cos\phi\sin\theta + i\mu\sin\phi\sin\theta & 1-\mu\cos\theta \end{pmatrix}$$
$$= \frac{1}{2}\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1+\mu\cos\theta & \mu\cos\phi\sin\theta - i\mu\sin\phi\sin\theta \\ \mu\cos\phi\sin\theta + i\mu\sin\phi\sin\theta & 1-\mu\cos\theta \end{pmatrix}$$
$$-\frac{1}{2}\begin{pmatrix} p+p\mu\cos\theta & p\mu\cos\phi\sin\theta - ip\mu\sin\phi\sin\theta \\ p\mu\cos\phi\sin\theta + ip\mu\sin\phi\sin\theta & p-p\mu\cos\theta \end{pmatrix}$$
$$= \frac{1}{2}\begin{pmatrix} 1+(1-p)\mu\cos\theta & (1-p)[\mu\cos\phi\sin\theta - i\mu\sin\phi\sin\theta] \\ (1-p)[\mu\cos\phi\sin\theta + i\mu\sin\phi\sin\theta] & 1-(1-p)\mu\cos\theta. \end{pmatrix}$$

Clearly, the angles θ and ϕ do not change by the depolarizing quantum operation T. Also, we can deduce that the distance of the quantum state ρ from the origin given by μ is greater than or equal to the distance of the new quantum state $T(\rho)$ from the origin given by $(1-p)\mu$, $p \in [0,1]$. Consequently, for any two quantum states which are comparable $\rho, \delta \in X(\rho \preceq \delta)$, with respective distances from the origin μ_ρ and μ_δ such that, $\mu_\rho \leq \mu_\delta$, the depolarizing quantum operation T constructs two quantum states $T(\rho), T(\delta) \in X$, have distances $(1-p)\mu_\rho$ and $(1-p)\mu_\delta$ from the origin for $p \in [0,1]$ respectively. Since $\mu_\rho \leq \mu_\delta$, then $(1-p)\mu_\rho \leq (1-p)\mu_\delta$, $\text{for all } p \in [0,1]$. Thus, $T(\rho) \preceq T(\delta)$, which proves T is order-preserving.

The fidelity of any two quantum states $\rho = \frac{1}{2}(I_2 + \vec{r_\rho} \cdot \vec{\sigma})$ and $\delta = \frac{1}{2}(I_2 + \vec{r_\delta} \cdot \vec{\sigma})$ is,

$$F(\rho,\delta) = \frac{1}{2}[1 + \vec{r_\rho} \cdot \vec{r_\delta} + \sqrt{1 - \|\vec{r_\rho}\|^2}\sqrt{1 - \|\vec{r_\rho}\|^2}] \tag{26}$$

see (Batsari & Kumam, 2020; Chen et al, 2002), where $\vec{r_\rho} \cdot \vec{r_\delta}$ is the inner dot product between the vectors $\vec{r_\rho}$ and $\vec{r_\delta}$. So, for any comparable quantum states $\rho = \frac{1}{2}(I_2 + \vec{r_\rho} \cdot \vec{\sigma})$ and $\delta = \frac{1}{2}(I_2 + \vec{r_\delta} \cdot \vec{\sigma}), \vec{r_\rho} \cdot \vec{r_\delta} = \|\vec{r_\rho}\|\|\vec{r_\delta}\| \cos\vartheta$ for ϑ being the angle between $\vec{r_\rho}$ and $\vec{r_\delta}$. Using Equation (26), we have,
(i). $F(\rho,\rho) = 1.$
(ii) $F(\rho, o) = \frac{1}{2}$; for ρ a pure state and o the completely mixed state.
(iii) $F(\rho, \rho-) = 0$; for ρ a pure state that is 180° separated from ρ,
see (Davies, 1976; Göhde, 1965). Thus, $1.000 \leq e^{\frac{1}{6}(1-F(\rho,\delta))} \leq 1.181$ for $\rho, \delta \in X$. Now, using $s = 1$ and $\theta \in [0,1]$ on Theorems 1. We have

$$\begin{aligned}
p_s(T(\rho),T(\delta)) &= \max\{\|\overline{r_\rho}\|, \|\overline{r_\delta}\|\}e^{\frac{1}{5}(1-F(T(\rho),T(\delta)))}\\
&= \frac{1}{4}\|\delta\|e^{\frac{1}{5}(1-F(T(\rho),T(\delta)))}\\
&\leq \frac{1}{4}(\|\delta\|e^{\frac{1}{5}(1-F(T(\rho),\delta))} + \|\rho\|e^{\frac{1}{5}(1-F(T(\rho),\rho))})\\
&= \frac{1}{2}(\frac{1}{2}(p_s(T(\rho),\delta) + p_s(T(\rho),\rho)))\\
&= \frac{1}{2}(\frac{1}{2}\max\{p_s(\rho,\delta), p_s(\rho,T(\delta)), p_s(T(\rho),\delta)\}\\
&+ \min\{\frac{p_s(\rho,T(\delta)) + p_s(T(\rho),\delta)}{2}, \frac{p_s(\rho,T(\rho)) + p_s(\delta,T(\delta))}{2}\}.
\end{aligned}$$

Taking $\alpha = \frac{1}{2}$ and $\beta = 1$, condition (1) in Theorem 1 is satisfied. So T has a unique fixed point in X.

References

Aamri, M. & El Moutawakil, D. 2002. Some new common fixed point theorems under strict contractive conditions. *Journal of Mathematical Analysis and Applications*, 270(1), pp.181-188. Available at: https://doi.org/10.1016/S0022-247X(02)00059-8.

Agarwal, R.P., Karapinar, E., O'Regan, D. & Roldán-López-de-Hierro, A.F. 2015. *Fixed point theory in metric type spaces*. Springer, Cham. Available at: https://doi.org/10.1007/978-3-319-24082-4. ISBN: 978-3-319-24082-4.

Arias, A., Gheondea, A. & Gudder, S. 2002. Fixed Points of Quantum Operations. *Journal of Mathematical Physics*, 43(12), pp.5872-5881. Available at: https://doi.org/10.1063/1.1519669.

Bakhtin, I. 1989. The contraction mapping principle in quasimetric spaces. *Func. An., Gos. Ped. Inst. Unianowsk*, 30, pp.26-37.

Banach, S. 1922. Sur les opérations dans les ensembles abstraits et leur applications aux équations intégrales. *Fundamenta Mathematicae*, 3, pp.133-181 (in French). Available at: https://doi.org/10.4064/fm-3-1-133-181.

Batsari, U.Y. & Kumam, P. 2018. A Globally Stable Fixed Point in an Ordered Partial Metric Space. In: Anh, L., Dong, L., Kreinovich, V. & Thach, N. (Eds.) *Econometrics for Financial Applications. ECONVN 2018. Studies in Computational Intelligence*, 760, pp.360-368. Springer, Cham. Available at: https://doi.org/10.1007/978-3-319-73150-6_29.

Batsari, U.Y. & Kumam, P. 2020. Some Generalised Fixed Point Theorems Applied to Quantum Operations. *Symmetry*, 12(5), art.ID:759. Available at: https://doi.org/10.3390/sym12050759.

Batsari, U.Y., Kumam, P. & Sitthithakerngkiet, K. 2018. Some globally stable fixed points in b-metric spaces. *Symmetry*, 10(11), art.ID:555. Available at: https://doi.org/10.3390/sym10110555.

Bourbaki, N. 1974. *Topologie Generale*. Paris, France: Herman. ISBN-13: 978-2705656928.

Brouwer, L.E.J. 1911. Über Abbildung von Mannigfaltigkeiten. *Mathematische Annalen*, 71, pp.97-115. Available at: https://doi.org/10.1007/BF01456931.

Browder, F.E. 1959. On a generalization of the Schauder fixed point theorem. *Duke Mathematical Journal*, 26(2), pp.291-303. Available at: https://doi.org/10.1215/S0012-7094-59-02629-8.

Bures, D. 1969. An Extension of Kakutanis Theorem on Infinite Product Measures to the Tensor Product of Semifinite w^*-Algebras. *Transactions of the American Mathematical Society*, 135, pp.199-212. Available at: https://doi.org/10.2307/1995012.

Busch, P. & Singh, J. 1998. Lüders Theorem for Unsharp Quantum Measurements. *Physics Letters A*, 249)(1-2), pp.10-12. Available at: https://doi.org/10.1016/S0375-9601(98)00704-X.

Chen, J-L., Fu, L., Ungar, A.A. & Zhao, X-G. 2002. Alternative fidelity measure between two states of an *N*-state quantum system. *Physical Review A*, 65(art.number:054304). Available at: https://doi.org/10.1103/PhysRevA.65.054304.

Chidume, C.E. & Chidume, C.O. 2014. *Foundations of Mathematical Analysis*. Ibadan, Nigeria: University of Ibadan, Ibadan University Press Publishing House. ISBN: 978-978-8456-32-2.

Czerwik, S. 1993. Contraction mappings in b-metric spaces. *Acta Mathematica et Informatica Universitatis Ostraviensis*, 1(1), pp.5-11 [online]. Available at: https://dml.cz/handle/10338.dmlcz/120469 [Accessed: 20 March 2022].

Davies, E.B. 1976. *Quantum Theory of Open Systems*. London, UK: Academic Press. ISBN-13: 978-0122061509.

Debnath, P., Konwar, N. & Radenović, S. 2021. *Metric Fixed Point Theory: Applications in Science, Engineering and Behavioural Sciences*. Springer Verlag, Singapore. Available at: https://doi.org/10.1007/978-981-16-4896-0 .

Du, W-S., Karapinar, E. & He, Z. 2018. Some Simultaneous Generalizations of Well-Known Fixed Point Theorems and Their Applications to Fixed Point Theory. *Mathematics*, 6(7), art.ID:117. Available at: https://doi.org/10.3390/math6070117.

Göhde, D. 1965. Zum Prinzip der Kontraktiveen abbildurg. *Mathematische Nachrichten*, 30(3-4), pp.251-258. Available at: https://doi.org/10.1002/mana.19650300312.

Kannan, R. 1972. Some results on fixed points - IV. *Fundamenta Mathematicae*, 74, pp.181-187. Available at: https://doi.org/10.4064/fm-74-3-181-187.

Khan, M.S., Swaleh, M. & Sessa, S. 1984. Fixed point theorems by altering distances between the points. *Bulletin of the Australian Mathematical Society*, 30(1), pp.1-9. Available at: https://doi.org/10.1017/S0004972700001659.

Kirk, W. & Shahzad, N. 2014. *Fixed Point Theory in Distance Spaces*. Springer International Publishing Switzerland. Available at: https://doi.org/10.1007/978-3-319-10927-5.

Knaster, B. 1928. Un theoreme sur les fonctions densembles. *Annales de la Société polonaise de mathématique*, 6, pp.133-134.

Leray, J. & Schauder, J. 1934. Topologie et equations fonctionnelles. *Annales scientifiques de l'École Normale Supérieure*, 51, pp.45-78. Available at: https://doi.org/10.24033/asens.836.

Long, L. & Zhang, S. 2011. Fixed points of commutative super-operators. *Journal of Physics A: Mathematical and Theoretical*, 44(9), art.ID:095201. Available at: https://doi.org/10.1088/1751-8113/44/9/095201.

Lüders, G. 1950. Über die Zustandsänderung durch den Meßprozeß. A*nnalen der physic*, 443(5-8), pp.322-328. Available at: https://doi.org/10.1002/andp.19504430510.

Matthews, S.G. 1994. Partial Metric Topology. *Annals of the New York Academy of Sciences*, 728(1) General Topology and Applications, pp.183-197. Available at: https://doi.org/10.1111/j.1749-6632.1994.tb44144.x.

Nielsen, M.A. & Chuang, I.L. 2000. *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press. Available at: https://doi.org/10.1017/CBO9780511976667.

Schauder, J. 1930. Der Fixpunktsatz in Funktionalraumen. *Studia Mathematica*, 2(1), pp.171-180 [online]. Available at: https://eudml.org/doc/urn:eudml:doc:217247 [Accessed: 22 March 2022].

Seevinck, M.P. 2003. *Quantum Operations and Measurement, 2nd ed*. Utrecht, The Netherlands: Utrecht University [online]. Available at: http://mpseevinck.ruhosting.nl/seevinck/lezingoviedo03a.pdf [Accessed: 22 March 2022].

Shukla S. 2014. Partial b-metric spaces and fixed point theorems. *Mediterranean Journal of Mathematics*, 11, pp.703-711. Available at: https://doi.org/10.1007/s00009-013-0327-4.

Tarski, A. 1955. A lattice-theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5(2), pp.285-309. Available at: https://doi.org/10.2140/pjm.1955.5.285.

Tarski, A.A. 1949. A fixpoint theorem for lattices and its applications (preliminary report). *Bulletin of the American Mathematical Society*, 1949(55), 1051-1052.

Zhang, H. & Ji, G. 2012. A Note on Fixed Points of General Quantum Operations. *Reports on Mathematical Physics*, 70(1), pp.111-117. Available at: https://doi.org/10.1016/S0034-4877(13)60016-6.

Zhang, H. & Si, H. 2016. Fixed Points Associated to Power of Normal Completely Positive Maps*. *Journal of Applied Mathematics and Physics*, 4(5), pp.925-929. Available at: https://doi.org/10.4236/jamp.2016.45101.

ТЕОРЕМА О ФИКСИРОВАННОЙ ТОЧКЕ В ЧАСТИЧНОМ b-МЕТРИЧЕСКОМ ПРОСТРАНСТВЕ С ПРИМЕНЕНИЕМ В КВАНТОВЫХ ОПЕРАЦИЯХ

Ракеш Тивари[а], *Мохаммад Саид* Кхан[б],
Шоба Рани[а], *Никола* Фабиано[в]

[а] Государственный автономный колледж последепипломного образования VYT , кафедра математики, г. Дург, Чхаттисгарх, Республика Индия

[б] Университет медицинских наук Сефако Макгато, кафедра математики и прикладной математики, г. Га-Ранкува, Южно-Африканская Республика [в] Белградский университет, Институт ядерных наук Винча - Национальный институт Республики Сербия, г. Белград, Республика Сербия, **корреспондент**

РУБРИКА ГРНТИ: 27.35.33 Математические модели электродинамики и оптики
27.35.57 Математические модели квантовой физики
27.39.27 Нелинейный функциональный анализ
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Сконструирована теорема о неподвижной точке с сохранением порядка в полном и частичном b-метрическом пространстве при выполнении условий сжатия.

Методы: В данной статье применен метод расширения результатов Батсари и др.

Результаты: Точность квантового состояния используется для построения неподвижного квантового состояния.

Выводы: Неподвижное квантовое состояние связано с квантовой операцией, сохраняющей порядок.

Ключевые слова: частичное b-метрическое пространство, отображение с сохранением порядка, квантовая операция, точность квантового состояния, вектор Блоха.

ТЕОРЕМА ФИКСНЕ ТАЧКЕ У ДЕЛИМИЧНОМ b-МЕТРИЧКОМ ПРОСТОРУ ПРИМЕЊЕНА НА КВАНТНЕ ОПЕРАЦИЈЕ

Ракеш Тивари[а], *Мохамед Саид* Кан[б],
Шоба Рани[а], *Никола* Фабиано[г]

[а] Државни колеџ за последипломске студије B.J.T, Департман за математику, Дург, Чатисгар, Република Индија

[б] Универзитет здравствених наука Сефако Макгато, Департман за математику и примењену математику, Га-Ранкува, Јужноафричка Република

[в] Универзитет у Београду, Институт за нуклеарне науке “Винча” - Национални институт Републике Србије, Београд, Република Србија, **аутор за преписку**

ОБЛАСТ: математика
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Конструисана је теорема фиксне тачке мапирања с очувањем редоследа на комплетном парцијалном b-метричком простору уз задовољавање контрактивног услова.

Методе: Примењен метод проширен је резултатима Батсарија и других.

Резултати: Верност квантног стања користи се за конструисање фиксног квантног стања.

Закључак: Фиксно квантно стање повезано је са квантном операцијом која чува редослед.

Кључне речи: парцијални b-метрички простор, мапирање с очувањем редоследа, квантна операција, верност квантног стања, Блохов вектор.

Paper received on / Дата получения работы / Датум пријема чланка: 22.03.2022. Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 21.06.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 23.06.2022.

PROPERTY P IN MODULAR METRIC SPACES

Ljiljana Paunović[a] , *Parveen* Kumar[b],
Savita Malik[c], *Manoj* Kumar[d]

[a] University in Priština-Kosovska Mitrovica,Teacher Education Faculty, Leposavić, Republic of Serbia,
e-mail: ljiljana.paunovic@pr.ac.rs, **corresponding author**,
ORCID iD: https://orcid.org/0000-0002-5449-9367

[b] Tau Devi Lal Govt. College for Women,
Murthal, Sonepat, Haryana, Republic of India,
e-mail: parveenyuvi@gmail.com,
ORCID iD: https://orcid.org/0000-0002-4361-477X

[c] Tau Devi Lal Govt. College for Women,
Murthal, Sonepat, Haryana, Republic of India,
e-mail: deswal.savita@gmail.com,
ORCID iD: https://orcid.org/0000-0003-2759-2432

[d] Baba Mastnath University, Faculty of Science, Department of Mathematics, Asthal Bohar, Rohtak, Haryana, Republic of India,
e-mail: manojantil18@gmail.com,
ORCID iD: https://orcid.org/0000-0003-4455-8690

DOI: 10.5937/vojtehg70-36958; https://doi.org/10.5937/vojtehg70-36958

FIELD: Mathematics
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: The aim of this paper is to present the concept of the generalized $\emptyset$ –weak contractive condition involving various combinations of d(x,y) in modular metric spaces.

Methods: Conventional theoretical methods of functional analysis.

Results: This study presents the result of (Murthy & Vara Prasad, 2013) for a single-valued mapping satisfying a generalized $\emptyset$ –weak contractive condition involving various combinations of d(x,y). It is generalized in the setting of modular metric spaces, and then it is proved that this single-valued map satisfies the property P. In the end, an example is given in support of the result.

Conclusion: With proper generalisations, it is possible to formulate well-known results of classical metric spaces to the case of modular metric spaces.

Key words: Fixed point, $\emptyset$ –weak contraction, modular metric spaces, property P.

Introduction

One of trends in mathematical research is to refine the frameworks of the known theorems and their results. For instance, Polish mathematician Banach observed the first metric fixed point results in the setting of complete normed spaces. An immediate extension of this theorem was given by Caccioppoli who observed the characterization of the Banach fixed point theorem in the context of complete metric spaces. Afterwards, for various abstract spaces, several analogs of the Banach contraction principle have been reported. Among them, we can underline some of interesting abstract structures such as modular metric space, partial metric space, *b*-metric space, fuzzy metric space, probabilistic metric space, *G*-metric space, etc.

This paper will be restricted to the recently introduced generalization of a metric space, namely, a modular metric space. Chistyakov introduced the notion of modular metric spaces (Chistyakov, 2010a, 2010b) inspired partly by the classical linear modulars on function spaces. Informally speaking, whereas a metric on a set represents the nonnegative finite distances between any two points of the set, a modular on a set attributes a nonnegative (possibly, infinite valued) “field of (generalized) velocities”: to each “time” λ>0 the absolute value of an average velocity $w_\lambda(x,y)$ is associated in such a way that in order to cover the “distance” between the points x, $y \in \psi$, it takes time λ to move from x to y with the velocity $w_\lambda(x,y)$. But the way we approached the concept of modular metric spaces is different. Indeed, we look at these spaces as a nonlinear version of the classical modular spaces introduced by H. Nakano (Nakano, 1950) on vector spaces and modular function spaces introduced by (Musielak, 1983) and (Orlicz, 1988a, 1988b). More about modular metric spaces can be read in (Hussain et al, 2011), (Paknazar & De la Sen, 2017) and (Paknazar & De la Sen, 2020).

In the formulation given by (Khamsi, 1996) and (Kozlowski, 1988), a modular on a vector space ψ is a function $m : \psi \to [0,+\infty)$ satisfying:
(1) $m(x) = 0$ if and only if $x = 0$,
(2) $m(ax) = m(x)$ for every $a \in R$ with $|a| = 1$,
(3) $m(ax + by) \leq m(x) + m(y)$ if $a, b \geq 0$ and $a + b = 1$.

A modular m is said to be convex if, instead of (3), it satisfies the stronger property:
(3*) $m(ax + by) \leq am(x) + bm(y)$ if $a, b \geq 0$ and $a + b = 1$.

Given a modular m on ψ, the modular space is defined by
ψ_m = $\{x \in \psi : m(ax) \to 0$ as $a \to 0\}$.

It is possible to define a corresponding F-norm (or a norm when m is convex) on the modular space. The Orlicz spaces L^{Φ} are examples of this construction (Rao & Ren, 2002). The modular metric approach is more natural and has not been used extensively. For more on the metric fixed point theory, the reader may consult the book (Khamsi & Kirk, 2001) and for modular function spaces (Chistyakov, 2010a, 2010b) and (Chistyakov, 2008). Some recent work in modular metric spaces has been presented in (Mongkolkeha et al, 2011) and (Padcharoen et al, 2016). It has been almost a century since several mathematicians improved, extended and enriched the classical Banach contraction principle (Banach, 1922) in different directions along with variety of applications. In the sequel, we recall some basic concepts about modular metric spaces.

Throughout this paper, $\mathbb{N}$ will denote the set of natural numbers.
Let ψ be a nonempty set. Throughout this paper, for a function
ω: $(0,+\infty) \times \psi \times \psi \to [0,+\infty)$, we write
$\omega_\lambda(x,y) = \omega(\lambda,x,y)$ for all $\lambda > 0$ and $x,y \in \psi$.

DEFINITION 1. (Chistyakov, 2006) Let ψ be a nonempty set. A function ω: $(0,+\infty) \times \psi \times \psi \to [0,+\infty)$ is said to be a metric modular on ψ if it satisfies, for all $x,y,z \in \psi$, the following conditions:
1) $\omega_\lambda(x,y) = 0$ for all $\lambda > 0$ if and only if $x = y$,
2) $\omega_\lambda(x,y) = \omega_\lambda(y,x)$ for all $\lambda > 0$,
3) $\omega_{\lambda+\mu}(x,y) \leq \omega_\lambda(x,z) + \omega_\mu(z,y)$ for all $\lambda,\mu > 0$.

If instead of (1) we have only the condition (1'):
$\omega_\lambda(x,x) = 0$ for all $x \in \psi$, $\lambda > 0$, then ω is said to be a pseudo modular (metric) on ψ.
An important property of the (metric) pseudo modular on the set ψ is that the mapping $\lambda \mapsto \omega_\lambda(x,y)$ is non increasing for all $x,y \in \psi$.

DEFINITION 2. (Chistyakov, 2006) Let ω be a pseudo modular on ψ. Fixed $x_0 \in \psi$. The set
$\psi_\omega = \psi_\omega(x_0) = \{x \in \psi : \omega_\lambda(x, x_0) \to 0$ as $\lambda \to +\infty\}$ is said to be a modular metric space (around x_0).

DEFINITION 3. (Padcharoen et al, 2016)Let ψ_ω be a modular metric space.

1) The sequence $\{x_\eta\}$ in ψ_ω is said to be ω-convergent to $x \in \psi_\omega$ if and only if there exists a number $\lambda > 0$, possibly depending on $\{x_\eta\}$ and x, such that $\lim\limits_{\eta \to +\infty} \omega_\lambda(x_\eta, x)$= 0.
2) The sequence $\{x_\eta\}$ in ψ_ω is said to be ω-Cauchy if there exists $\lambda > 0$, possibly depending on the sequence, such that $\omega_\lambda(x_m, x_\eta) \to 0$ as $m, \eta \to +\infty$.
3) A subset $C$of ψ_ω is said to be ω -complete if any ω-Cauchy sequence in C is a convergent sequence and its limit is in C.

DEFINITION 4.(Mongkolkeha et al, 2011) Let ω be a metric modular on ψ and ψ_ω be a modular metric space induced by ω. If ψ_ω is a ω-complete modular metric space and $\mathcal{T}$: $\psi_\omega \to \psi_\omega$be an arbitrary mapping, $\mathcal{T}$ is called a contraction if for each $x, y \in \psi_\omega$ and for all $\lambda > 0$ there exists $0 \leq \sigma < 1$ such that

$$\omega_\lambda(\mathcal{T}x, \mathcal{T}y) \leq \sigma \omega_\lambda(x, y)$$

Mongkolkeha et al, (2011) proved that if $\psi_\omega$is a ω - complete modular metric space, then contraction mapping $\mathcal{T}$ has a unique fixed point.

Main result

In this section, there is a generalization of the result proved by (Murthy & Vara Prasad, 2013):
Let $\mathcal{T}$ be a self-map of a complete metric space ψ satisfying:

(C_1) **:**

$$[1 + pd(x,y)]d^2(\mathcal{T}x, \mathcal{T}y) \leq pmax \left\{ \begin{array}{c} \frac{1}{2}[d^2(x,\mathcal{T}x)d(y,\mathcal{T}y) + d(x,\mathcal{T}x)d^2(y,\mathcal{T}y)], \\ d(x,\mathcal{T}x)d(x,\mathcal{T}y)d(y,\mathcal{T}x), \\ d(x,\mathcal{T}y)d(y,\mathcal{T}x)d(y,\mathcal{T}y) \end{array} \right\} + m(x,y) - \emptyset m(x,y).$$

Where,
(C_2) **:**

$$m(x,y) = \max \left\{ \begin{array}{c} d^2(x,y), d(x,\mathcal{T}x)d(y,\mathcal{T}y), d(x,\mathcal{T}y)d(y,\mathcal{T}x), \\ \frac{1}{2}[d(x,\mathcal{T}x)d(x,\mathcal{T}y) + d(y,\mathcal{T}x)d(y,\mathcal{T}y)] \end{array} \right\},$$

$p \geq 0$ is a real number and $\emptyset$: [0,+∞) → [0,+∞) is a continuous function with $\emptyset$ (t) = 0 ⇔t = 0 and $\emptyset(t) > 0$ for each $t > 0$.
Then $\mathcal{T}$ has a unique fixed point in ψ.

Now we will generalize the above result in the setting of modular metric spaces as follows:

Theorem 1. Let (ψ_ω, ω) be a complete modular metric space. Let $\mathcal{T}$ be a self-map of a complete modular metric space ψ_ω satisfying:
(C_3) **:**

$$[1 + p\omega_1(x,y)]\omega_1{}^2(\mathcal{T}x,\mathcal{T}y) \le pmax\left\{\begin{array}{c} \frac{1}{2}[\omega_1{}^2(x,\mathcal{T}x)\omega_1(y,\mathcal{T}y) + \omega_1(x,\mathcal{T}x)\omega_1{}^2(y,\mathcal{T}y)], \\ \omega_1(x,\mathcal{T}x)\omega_2(x,\mathcal{T}y)\omega_1(y,\mathcal{T}x), \\ \omega_2(x,\mathcal{T}y)\omega_1(y,\mathcal{T}x)\omega_1(y,\mathcal{T}y) \end{array}\right\} + m(x,y) - \emptyset m(x,y),$$

where,
(C_4) **:**

$$m(x,y) = \max\left\{\begin{array}{c} \omega_1{}^2(x,y), \omega_1(x,\mathcal{T}x)\omega_1(y,\mathcal{T}y), \omega_2(x,\mathcal{T}y)\omega_1(y,\mathcal{T}x), \\ \frac{1}{2}[\omega_1(x,\mathcal{T}x)\omega_2(x,\mathcal{T}y) + \omega_1(y,\mathcal{T}x)\omega_1(y,\mathcal{T}y)] \end{array}\right\}$$

$p \ge 0$ is a real number and $\emptyset$: [0, +∞) → [0, +∞) is a continuous function with $\emptyset$ (t) = 0 ⇔t = 0 and $\emptyset(t) > 0$ for each $t > 0$.
Then $\mathcal{T}$ has a unique common fixed point in ψ_ω.

Proof. Let $x_0 \in \psi_\omega$ be an arbitrary point. Then we can find x_1 such that $x_1 = \mathcal{T}(x_0)$. For this x_1, we can find $x_2 \in \psi_\omega$ such that $x_2 = \mathcal{T}(x_1)$.

In general, one can choose $\{x_{\eta+1}\}$ in ψ_ω such that
$x_{\eta+1} = \mathcal{T}(x_\eta),\ \eta = 0,1,2 \ldots$ (1)
We may assume that $x_\eta \neq x_{\eta+1}$ for each η.
Since if there exists η such that $x_\eta = x_{\eta+1}$ then $x_\eta = x_{\eta+1} = \mathcal{T}(x_\eta)$,
We write $\alpha_\eta = d(x_\eta, x_{\eta+1})$.
Firstly, we prove that α_η is a non - increasing sequence and converges to 0.

Case I. If η is even, taking $x = x_{2\eta}$ and $y = x_{2\eta+1}$ in (C_3), we get
$\left[1 + p\omega_1(x_{2\eta}, x_{2\eta+1})\right]\omega_1{}^2(\mathcal{T}x_{2\eta}, \mathcal{T}x_{2\eta+1})$

$$\leq pmax\left\{\begin{array}{c}\frac{1}{2}\left[\begin{array}{c}\omega_1{}^2(x_{2\eta},\mathcal{T}x_{2\eta})\omega_1(x_{2\eta+1},\mathcal{T}x_{2\eta+1})\\+\ \omega_1(x_{2\eta},\mathcal{T}x_{2\eta})\omega_1{}^2(x_{2\eta+1},\mathcal{T}x_{2\eta+1})\end{array}\right],\\ \omega_1(x_{2\eta},\mathcal{T}x_{2\eta})\omega_2(x_{2\eta},\mathcal{T}x_{2\eta+1})\omega_1(x_{2\eta+1},\mathcal{T}x_{2\eta}),\\ \omega_2(x_{2\eta},\mathcal{T}x_{2\eta+1})\omega_1(x_{2\eta+1},\mathcal{T}x_{2\eta})\omega_1(x_{2\eta+1},\mathcal{T}x_{2\eta+1})\end{array}\right\}$$

$$+\ m(x_{2\eta},x_{2\eta+1})-\emptyset m(x_{2\eta},x_{2\eta+1}), \qquad (2)$$

where,

$$m(x_{2\eta},x_{2\eta+1})=$$

$$\max\left\{\begin{array}{c}\omega_1{}^2(x_{2\eta},x_{2\eta+1}),\omega_1(x_{2\eta},\mathcal{T}x_{2\eta})\omega_1(x_{2\eta+1},\mathcal{T}x_{2\eta+1}),\\ \omega_2(x_{2\eta},\mathcal{T}x_{2\eta+1})\omega_1(x_{2\eta+1},\mathcal{T}x_{2\eta}),\\ \frac{1}{2}\left[\begin{array}{c}\omega_1(x_{2\eta},\mathcal{T}x_{2\eta})\omega_2(x_{2\eta},\mathcal{T}x_{2\eta+1})\\+\omega_1(x_{2\eta+1},\mathcal{T}x_{2\eta})\omega_1(x_{2\eta+1},\mathcal{T}x_{2\eta+1})\end{array}\right]\end{array}\right\}. \qquad (3)$$

Using (1) we get

$$[1+p\omega_1(x_{2\eta},x_{2\eta+1})]\omega_1{}^2(x_{2\eta+1},x_{2\eta+2})$$

$$\leq pmax\left\{\begin{array}{c}\frac{1}{2}\left[\begin{array}{c}\omega_1{}^2(x_{2\eta},x_{2\eta+1})\omega_1(x_{2\eta+1},x_{2\eta+2})\\+\ \omega_1(x_{2\eta},x_{2\eta+1})\omega_1{}^2(x_{2\eta+1},x_{2\eta+2})\end{array}\right],\\ \omega_1(x_{2\eta},x_{2\eta+1})\omega_2(x_{2\eta},x_{2\eta+2})\omega_1(x_{2\eta+1},x_{2\eta+1}),\\ \omega_2(x_{2\eta},x_{2\eta+2})\omega_1(x_{2\eta+1},x_{2\eta+1})\omega_1(x_{2\eta+1},x_{2\eta+2})\end{array}\right\}$$

$$+\ m(x_{2\eta},x_{2\eta+1})-\emptyset m(x_{2\eta},x_{2\eta+1})\ , \qquad (4)$$

where,

$$m(x_{2\eta},x_{2\eta+1})=\max\left\{\begin{array}{c}\omega_1{}^2(x_{2\eta},x_{2\eta+1}),\omega_1(x_{2\eta},x_{2\eta+1})\omega_1(x_{2\eta+1},x_{2\eta+2}),\\ \omega_2(x_{2\eta},x_{2\eta+2})\omega_1(x_{2\eta+1},x_{2\eta+1}),\\ \frac{1}{2}\left[\begin{array}{c}\omega_1(x_{2\eta},x_{2\eta+1})\omega_2(x_{2\eta},x_{2\eta+2})\\+\omega_1(x_{2\eta+1},x_{2\eta+1})\omega_1(x_{2\eta+1},x_{2\eta+2})\end{array}\right]\end{array}\right\} \qquad (5)$$

Now consider $\alpha_{2\eta}=\omega_1(x_{2\eta},x_{2\eta+1})$; then we have

$$[1+p\alpha_{2\eta}]\alpha_{2\eta+1}^2\leq pmax\left\{\frac{1}{2}\left[\alpha_{2\eta}^2\alpha_{2\eta+1}+\ \alpha_{2\eta}\alpha_{2\eta+1}^2\right],0,0\right\}+$$

$$m(x_{2\eta},x_{2\eta+1})-\emptyset m(x_{2\eta},x_{2\eta+1})\ , \qquad (6)$$

where, $m(x_{2\eta},x_{2\eta+1})=\max\left\{\alpha_{2\eta}^2,\alpha_{2\eta}\alpha_{2\eta+1},0,\frac{1}{2}\left[\alpha_{2\eta}\omega_2(x_{2\eta},x_{2\eta+2})+0\right]\right\}$.

By triangular inequality and using the property of $\emptyset$, we get

$$\omega_2(x_{2\eta},x_{2\eta+2})\leq\omega_1(x_{2\eta},x_{2\eta+1})+\omega_1(x_{2\eta+1},x_{2\eta+2})$$

$$= \alpha_{2\eta} + \alpha_{2\eta+1}, \tag{7}$$

and

$m(x_{2\eta}, x_{2\eta+1}) =$

$$m(x, \mathscr{y}) \leq \max\left\{\alpha_{2\eta}^2, \alpha_{2\eta}\alpha_{2\eta+1}, 0, \frac{1}{2}\left[\alpha_{2\eta}\left(\alpha_{2\eta} + \alpha_{2\eta+1}\right) + 0\right]\right\}. \tag{8}$$

If $\alpha_{2\eta} < \alpha_{2\eta+1}$, then (C_3) reduces to

$p\alpha_{2\eta+1}^2 \leq p\alpha_{2\eta+1}^2 - \emptyset\alpha_{2\eta+1}^2$, a contradiction.

Therefore, $\alpha_{2\eta+1}^2 \leq \alpha_{2\eta}^2 \Longrightarrow \alpha_{2\eta+1} \leq \alpha_{2\eta}$.

Case II. In a similar way, if η is odd, then we can obtain $\alpha_{2\eta+2} < \alpha_{2\eta+1}$. It follows that the sequence $\{\alpha_\eta\}$ is decreasing.

Let $\lim\limits_{\eta \to +\infty} \alpha_\eta = r,$ for some $r \geq 0$.

Suppose $r > 0$; then from the inequality (C_3) and (C_4), we have

$$\left[1 + p\omega_1\left(x_\eta, x_{\eta+1}\right)\right]{\omega_1}^2\left(\mathcal{T}x_\eta, \mathcal{T}x_{\eta+1}\right)$$

$$\leq pmax\left\{\begin{array}{c} \dfrac{1}{2}\left[\begin{array}{c} {\omega_1}^2\left(x_\eta, \mathcal{T}x_\eta\right)\omega_1\left(x_{\eta+1}, \mathcal{T}x_{\eta+1}\right) \\ +\omega_1\left(x_\eta, \mathcal{T}x_\eta\right){\omega_1}^2\left(x_{\eta+1}, \mathcal{T}x_{\eta+1}\right) \end{array}\right], \\ \omega_1\left(x_\eta, \mathcal{T}x_\eta\right)\omega_2\left(x_\eta, \mathcal{T}x_{\eta+1}\right)\omega_1\left(x_{\eta+1}, \mathcal{T}x_\eta\right), \\ \omega_2\left(x_\eta, \mathcal{T}x_{\eta+1}\right)\omega_1\left(x_{\eta+1}, \mathcal{T}x_\eta\right)\omega_1\left(x_{\eta+1}, \mathcal{T}x_{\eta+1}\right) \end{array}\right\}$$

$$+ m\left(x_\eta, x_{\eta+1}\right) - \emptyset m\left(x_\eta, x_{\eta+1}\right), \tag{9}$$

where, $m\left(x_\eta, x_{\eta+1}\right) =$

$$\max\left\{\begin{array}{c} {\omega_1}^2\left(x_\eta, x_{\eta+1}\right), \omega_1\left(x_\eta, \mathcal{T}x_\eta\right)\omega_1\left(x_{\eta+1}, \mathcal{T}x_{\eta+1}\right), \\ \omega_2\left(x_\eta, \mathcal{T}x_{\eta+1}\right)\omega_1\left(x_{\eta+1}, \mathcal{T}x_\eta\right), \\ \frac{1}{2}\left[\begin{array}{c} \omega_1\left(x_\eta, \mathcal{T}x_\eta\right)\omega_2\left(x_\eta, \mathcal{T}x_{\eta+1}\right) \\ +\omega_1\left(x_{\eta+1}, \mathcal{T}x_\eta\right)\omega_1\left(x_{\eta+1}, \mathcal{T}x_{\eta+1}\right) \end{array}\right] \end{array}\right\}. \tag{10}$$

Now by using (1) we get,

$$\left[1 + p\omega_1\left(x_\eta, x_{\eta+1}\right)\right]{\omega_1}^2\left(x_{\eta+1}, x_{\eta+2}\right)$$

$$\leq pmax\left\{\begin{array}{c} \dfrac{1}{2}\left[\begin{array}{c} {\omega_1}^2\left(x_\eta, x_{\eta+1}\right)\omega_1\left(x_{\eta+1}, x_{\eta+2}\right) \\ +\omega_1\left(x_\eta, x_{\eta+1}\right){\omega_1}^2\left(x_{\eta+1}, x_{\eta+2}\right) \end{array}\right], \\ \omega_1\left(x_\eta, x_{\eta+1}\right)\omega_2\left(x_\eta, x_{\eta+2}\right)\omega_1\left(x_{\eta+1}, x_{\eta+1}\right), \\ \omega_2\left(x_\eta, x_{\eta+2}\right)\omega_1\left(x_{\eta+1}, x_{\eta+1}\right)\omega_1\left(x_{\eta+1}, x_{\eta+2}\right) \end{array}\right\}$$

$$+ \ m\left(x_\eta, x_{\eta+1}\right) - \emptyset m\left(x_\eta, x_{\eta+1}\right), \tag{11}$$

where, $m(x_\eta, x_{\eta+1}) = \max \left\{ \begin{matrix} \omega_1{}^2(x_\eta, x_{\eta+1}), \omega_1(x_\eta, x_{\eta+1})\omega_1(x_{\eta+1}, x_{\eta+2}), \\ \omega_2(x_\eta, x_{\eta+2})\omega_1(x_{\eta+1}, x_{\eta+1}), \\ \frac{1}{2}\begin{bmatrix} \omega_1(x_\eta, x_{\eta+1})\omega_2(x_\eta, x_{\eta+2}) \\ +\omega_1(x_{\eta+1}, x_{\eta+1})\omega_1(x_{\eta+1}, x_{\eta+2}) \end{bmatrix} \end{matrix} \right\}$

Using the triangular inequality and the property of $\emptyset$, and taking the limit $\eta \to +\infty$, we get

$[1 + pr]r^2 \le pr^3 + r^2 - \emptyset(r^2).$ (12)

Then $\emptyset(r^2) \le 0$, since r is positive, then by the property of $\emptyset$, we get $r = 0$, and we conclude that

$\lim_{\eta \to +\infty} \alpha_\eta = \lim_{\eta \to +\infty} \omega_1(x_\eta, x_{\eta+1}) = r = 0$. (13)

Now we show that $\{x_\eta\}$ is a Cauchy sequence. For the given $\epsilon > 0$, we can find two sequences of positive integers $\{m(\sigma)\}$ and $\{\eta(\sigma)\}$ such that

$\omega_8(x_{m(\sigma)}, x_{\eta(\sigma)}) \ge \epsilon, \qquad \omega_{\frac{1}{4}}(x_{m(\sigma)}, x_{\eta(\sigma)-1}) < \epsilon$ (14)

and $\eta(\sigma) > m(\sigma) > \sigma$.

Now $\epsilon \le \omega_8(x_{m(\sigma)}, x_{\eta(\sigma)})$

$\le \omega_2(x_{m(\sigma)}, x_{\eta(\sigma)}) + \omega_1(x_{m(\sigma)}, x_{\eta(\sigma)})$

$\le \omega_{\frac{1}{2}}(x_{m(\sigma)}, x_{\eta(\sigma)-1}) + \omega_{\frac{1}{2}}(x_{\eta(\sigma)-1}, x_{\eta(\sigma)})$

$\le \omega_{\frac{1}{4}}(x_{m(\sigma)}, x_{\eta(\sigma)-1}) + \omega_{\frac{1}{2}}(x_{\eta(\sigma)-1}, x_{\eta(\sigma)})$

$\le \epsilon + \omega_{\frac{1}{2}}(x_{\eta(\sigma)-1}, x_{\eta(\sigma)})$

Letting $\sigma \to +\infty$, we get $\lim_{\sigma \to +\infty} \omega_2(x_{m(\sigma)}, x_{\eta(\sigma)}) = \lim_{\sigma \to +\infty} \omega_1(x_{m(\sigma)}, x_{\eta(\sigma)}) = \epsilon$

Again using the triangular inequality, we have

$\epsilon \le \omega_8(x_{m(\sigma)}, x_{\eta(\sigma)}) \le \omega_4(x_{m(\sigma)}, x_{\eta(\sigma)})$

$\le \omega_2(x_{\eta(\sigma)}, x_{\eta(\sigma)+1}) + \omega_2(x_{m(\sigma)}, x_{\eta(\sigma)+1})$. (15)

We get

$\epsilon - \omega_2(x_{\eta(\sigma)}, x_{\eta(\sigma)+1}) \le \omega_2(x_{m(\sigma)}, x_{\eta(\sigma)+1}) \le \omega_1(x_{m(\sigma)}, x_{\eta(\sigma)+1})$

$\le \omega_{\frac{1}{4}}(x_{m(\sigma)}, x_{\eta(\sigma)+1})$

$\le \omega_{\frac{1}{8}}(x_{m(\sigma)}, x_{\eta(\sigma)}) + \omega_{\frac{1}{8}}(x_{\eta(\sigma)}, x_{\eta(\sigma)+1})$.

Taking the limits as $\sigma \to +\infty$, we have

$\lim_{\sigma \to +\infty} \omega_1(x_{m(\sigma)}, x_{\eta(\sigma)+1}) = \lim_{\sigma \to +\infty} \omega_2(x_{m(\sigma)}, x_{\eta(\sigma)+1}) = \epsilon$. (16)

Now from the triangular inequality, we have

$\epsilon \le \omega_2(x_{m(\sigma)}, x_{\eta(\sigma)}) \le \omega_1(x_{m(\sigma)}, x_{m(\sigma)+1}) + \omega_1(x_{m(\sigma)+1}, x_{\eta(\sigma)})$

We get

ϵ -$\omega_1\left(x_{m(\sigma)}, x_{m(\sigma)+1}\right) \leq \omega_1\left(x_{m(\sigma)+1}, x_{\eta(\sigma)}\right)$
$\leq \omega_{\frac{1}{2}}\left(x_{\eta(\sigma)}, x_{m(\sigma)-1}\right) + \omega_{\frac{1}{2}}\left(x_{m(\sigma)+1}, x_{m(\sigma)-1}\right)$
$\leq \omega_{\frac{1}{2}}\left(x_{\eta(\sigma)}, x_{m(\sigma)-1}\right) + \omega_{\frac{1}{4}}\left(x_{m(\sigma)-1}, x_{m(\sigma)}\right) + \omega_{\frac{1}{4}}\left(x_{m(\sigma)}, x_{m(\sigma)+1}\right)$.
Letting $\sigma \rightarrow +\infty$, we have $\lim_{\sigma\rightarrow+\infty} \omega_1\left(x_{m(\sigma)+1}, x_{\eta(\sigma)}\right) = \epsilon$ (17)
Again, from the triangular inequality, we have

$$\omega_8\left(x_{m(\sigma)}, x_{\eta(\sigma)}\right) \leq \omega_4\left(x_{\eta(\sigma)}, x_{\eta(\sigma)+1}\right) + \omega_4\left(x_{\eta(\sigma)+1}, x_{m(\sigma)}\right)$$

We get
$\omega_8\left(x_{m(\sigma)}, x_{\eta(\sigma)}\right) \leq \omega_4\left(x_{\eta(\sigma)}, x_{\eta(\sigma)+1}\right) + \omega_2\left(x_{m(\sigma)+1}, x_{m(\sigma)}\right) + \omega_2\left(x_{m(\sigma)+1}, x_{\eta(\sigma)+1}\right)$
$\omega_8\left(x_{m(\sigma)}, x_{\eta(\sigma)}\right)$-$\omega_4\left(x_{\eta(\sigma)}, x_{\eta(\sigma)+1}\right)$-$\omega_2\left(x_{m(\sigma)+1}, x_{m(\sigma)}\right) \leq \omega_2\left(x_{m(\sigma)+1}, x_{\eta(\sigma)+1}\right)$
$\leq \omega_1\left(x_{m(\sigma)+1}, x_{m(\sigma)}\right) + \omega_1\left(x_{\eta(\sigma)+1}, x_{m(\sigma)}\right)$.
Letting $\sigma \rightarrow +\infty$, we have $\lim_{\sigma\rightarrow+\infty} \omega_2\left(x_{m(\sigma)+1}, x_{\eta(\sigma)+1}\right) = \epsilon$ (18)
Since $\omega_2\left(x_{m(\sigma)+1}, x_{\eta(\sigma)+1}\right) \leq \omega_1\left(x_{m(\sigma)+1}, x_{\eta(\sigma)+1}\right)$
$\leq \omega_{\frac{1}{2}}\left(x_{m(\sigma)+1}, x_{m(\sigma)}\right) + \omega_{\frac{1}{2}}\left(x_{m(\sigma)}, x_{\eta(\sigma)+1}\right) \leq \omega_{\frac{1}{2}}\left(x_{m(\sigma)}, x_{\eta(\sigma)+1}\right)$
$\leq \omega_{\frac{1}{4}}\left(x_{m(\sigma)}, x_{m(\sigma)-1}\right) + \omega_{\frac{1}{4}}\left(x_{m(\sigma)-1}, x_{\eta(\sigma)+1}\right)$
$\leq \omega_{\frac{1}{8}}\left(x_{m(\sigma)-1}, x_{\eta(\sigma)}\right) + \omega_{\frac{1}{8}}\left(x_{\eta(\sigma)+1}, x_{\eta(\sigma)}\right)$.
Letting $\sigma \rightarrow +\infty$, we have $\lim_{\sigma\rightarrow+\infty} \omega_1\left(x_{m(\sigma)+1}, x_{\eta(\sigma)+1}\right) = \epsilon$. (19)
On putting $x = x_{m(\sigma)}$ and $y = x_{\eta(\sigma)}$ in (C_3), we get

$$\left[1 + p\omega_1\left(x_{m(\sigma)}, x_{\eta(\sigma)}\right)\right]{\omega_1}^2\left(\mathcal{T}x_{m(\sigma)}, \mathcal{T}x_{\eta(\sigma)}\right)$$
$$\leq pmax\left\{\begin{matrix} \frac{1}{2}\begin{bmatrix} {\omega_1}^2\left(x_{m(\sigma)}, \mathcal{T}x_{m(\sigma)}\right)\omega_1\left(x_{\eta(\sigma)}, \mathcal{T}x_{\eta(\sigma)}\right) \\ +\omega_1\left(x_{m(\sigma)}, \mathcal{T}x_{m(\sigma)}\right){\omega_1}^2\left(x_{\eta(\sigma)}, \mathcal{T}x_{\eta(\sigma)}\right) \end{bmatrix}, \\ \omega_1\left(x_{m(\sigma)}, \mathcal{T}x_{m(\sigma)}\right)\omega_2\left(x_{m(\sigma)}, \mathcal{T}x_{\eta(\sigma)}\right)\omega_1\left(x_{\eta(\sigma)}, \mathcal{T}x_{m(\sigma)}\right), \\ \omega_2\left(x_{m(\sigma)}, \mathcal{T}x_{\eta(\sigma)}\right)\omega_1\left(x_{\eta(\sigma)}, \mathcal{T}x_{m(\sigma)}\right)\omega_1\left(x_{\eta(\sigma)}, \mathcal{T}x_{\eta(\sigma)}\right) \end{matrix}\right\}$$
$$+\ m\left(x_{m(\sigma)}, x_{\eta(\sigma)}\right) - \emptyset m\left(x_{m(\sigma)}, x_{\eta(\sigma)}\right) \qquad (20)$$

where,

$$m\left(x_{m(\sigma)},x_{\eta(\sigma)}\right) = \max\left\{\begin{array}{c} {\omega_1}^2\left(x_{m(\sigma)},x_{\eta(\sigma)}\right), \\ \omega_1\left(x_{m(\sigma)},\mathcal{T}x_{m(\sigma)}\right)\omega_1\left(x_{\eta(\sigma)},\mathcal{T}x_{\eta(\sigma)}\right), \\ \omega_2\left(x_{m(\sigma)},\mathcal{T}x_{\eta(\sigma)}\right)\omega_1\left(x_{\eta(\sigma)},\mathcal{T}x_{m(\sigma)}\right), \\ \frac{1}{2}\left[\begin{array}{c} \omega_1\left(x_{m(\sigma)},\mathcal{T}x_{m(\sigma)}\right)\omega_2\left(x_{m(\sigma)},\mathcal{T}x_{\eta(\sigma)}\right) \\ +\omega_1\left(x_{\eta(\sigma)},\mathcal{T}x_{m(\sigma)}\right)\omega_1\left(x_{\eta(\sigma)},\mathcal{T}x_{\eta(\sigma)}\right) \end{array}\right] \end{array}\right\}.$$

Using (1), we obtain

$$\left[1+p\omega_1\left(x_{m(\sigma)},x_{\eta(\sigma)}\right)\right]{\omega_1}^2\left(x_{m(\sigma)+1},x_{\eta(\sigma)+1}\right)$$
$$\leq p\max\left\{\begin{array}{c} \frac{1}{2}\left[\begin{array}{c} {\omega_1}^2\left(x_{m(\sigma)},x_{m(\sigma)+1}\right)\omega_1\left(x_{\eta(\sigma)},x_{\eta(\sigma)+1}\right) \\ +\omega_1\left(x_{m(\sigma)},x_{m(\sigma)+1}\right){\omega_1}^2\left(x_{\eta(\sigma)},x_{\eta(\sigma)+1}\right) \end{array}\right], \\ \omega_1\left(x_{m(\sigma)},x_{m(\sigma)+1}\right)\omega_2\left(x_{m(\sigma)},x_{\eta(\sigma)+1}\right)\omega_1\left(x_{\eta(\sigma)},x_{m(\sigma)+1}\right), \\ \omega_2\left(x_{m(\sigma)},x_{\eta(\sigma)+1}\right)\omega_1\left(x_{\eta(\sigma)},x_{m(\sigma)+1}\right)\omega_1\left(x_{\eta(\sigma)},x_{\eta(\sigma)+1}\right) \end{array}\right\}$$
$$+m\left(x_{m(\sigma)},x_{\eta(\sigma)}\right)-\emptyset m\left(x_{m(\sigma)},x_{\eta(\sigma)}\right) \qquad (21)$$

where,

$$m\left(x_{m(\sigma)},x_{\eta(\sigma)}\right) = \max\left\{\begin{array}{c} {\omega_1}^2\left(x_{m(\sigma)},x_{\eta(\sigma)}\right), \\ \omega_1\left(x_{m(\sigma)},x_{m(\sigma)+1}\right)\omega_1\left(x_{\eta(\sigma)},x_{\eta(\sigma)+1}\right), \\ \omega_2\left(x_{m(\sigma)},x_{\eta(\sigma)+1}\right)\omega_1\left(x_{\eta(\sigma)},x_{m(\sigma)+1}\right), \\ \frac{1}{2}\left[\begin{array}{c} \omega_1\left(x_{m(\sigma)},x_{m(\sigma)+1}\right)\omega_2\left(x_{m(\sigma)},x_{\eta(\sigma)+1}\right) \\ +\omega_1\left(x_{\eta(\sigma)},x_{m(\sigma)+1}\right)\omega_1\left(x_{\eta(\sigma)},x_{\eta(\sigma)+1}\right) \end{array}\right] \end{array}\right\}$$

Letting $\sigma \to +\infty$ and using (13) - (19), we get

$$[1+p\epsilon]\epsilon^2 \leq p\max\left\{\frac{1}{2}[0+0],0,0\right\}+\epsilon^2-\emptyset(\epsilon^2)$$
$$=\epsilon^2-\emptyset(\epsilon^2),$$

a contradiction.

Thus, $\{x_\eta\}$ is a Cauchy sequence in ψ_ω, since (ψ_ω,ω) is a complete modular metric space.

Therefore, $\{x_\eta\}$ converges to a point z and $x_{\eta+1}=\mathcal{T}(x_\eta)$ also converges to the same point z, $\lim\limits_{\eta\to\infty} x_\eta = z$. (22)

Now, we will prove that z is a fixed point of $\mathcal{T}$.

For this, let $x=x_\eta$ and $y=z$ in (C_3), we get

$$\left[1+p\omega_1\left(x_\eta,z\right)\right]{\omega_1}^2\left(\mathcal{T}x_\eta,\mathcal{T}z\right)$$

$$\leq pmax\begin{Bmatrix} \frac{1}{2}\left[\omega_1{}^2(x_\eta,\mathcal{T}x_\eta)\omega_1(z,\mathcal{T}z)+\omega_1(x_\eta,\mathcal{T}x_\eta)\omega_1{}^2(z,\mathcal{T}z)\right], \\ \omega_1(x_\eta,\mathcal{T}x_\eta)\omega_2(x_\eta,\mathcal{T}z)\omega_1(z,\mathcal{T}x_\eta), \\ \omega_2(x_\eta,\mathcal{T}z)\omega_1(z,\mathcal{T}x_\eta)\omega_1(z,\mathcal{T}z) \end{Bmatrix} + $$

$$+ m(x_\eta,z) - \emptyset m(x_\eta,z) \qquad (23)$$

where,

$$m(x_\eta,z)$$
$$= \max\begin{Bmatrix} \omega_1{}^2(x_\eta,z), \omega_1(x_\eta,\mathcal{T}x_\eta)\omega_1(z,\mathcal{T}z), \omega_2(x_\eta,\mathcal{T}z)\omega_1(z,\mathcal{T}x_\eta), \\ \frac{1}{2}\left[\omega_1(x_\eta,\mathcal{T}x_\eta)\omega_2(x_\eta,\mathcal{T}z)+\omega_1(z,\mathcal{T}x_\eta)\omega_1(z,\mathcal{T}z)\right] \end{Bmatrix}$$

Using (22) and (1), we have

$$[1+p\omega_1(z,z)]\omega_1{}^2(z,\mathcal{T}z)$$
$$\leq pmax\begin{Bmatrix} \frac{1}{2}[\omega_1{}^2(z,z)\omega_1(z,\mathcal{T}z)+\omega_1(z,z)\omega_1{}^2(z,\mathcal{T}z)], \\ \omega_1(z,z)\omega_2(z,\mathcal{T}z)\omega_1(z,z), \\ \omega_2(z,\mathcal{T}z)\omega_1(z,z)\omega_1(z,\mathcal{T}z) \end{Bmatrix}$$
$$+ m(x_\eta,z) - \emptyset m(x_\eta,z) \qquad (24)$$

where,

$$m(x_\eta,z) = \max\begin{Bmatrix} \omega_1{}^2(z,z), \omega_1(z,z)\omega_1(z,\mathcal{T}z), \omega_2(z,\mathcal{T}z)\omega_1(z,z), \\ \frac{1}{2}[\omega_1(z,z)\omega_2(z,\mathcal{T}z)+\omega_1(z,z)\omega_1(z,\mathcal{T}z)] \end{Bmatrix} = 0.$$

Hence, $\omega_1{}^2(z,\mathcal{T}z) \leq 0 \Longrightarrow \mathcal{T}z = z$.
So, $\mathcal{T}$ has a fixed point in ψ_ω.

Uniqueness:

To show that $\mathcal{T}$ can have only one common fixed point.
Suppose $x \neq y$ be two fixed points of $\mathcal{T}$.
Therefore, $x = \mathcal{T}x$ and $y = \mathcal{T}y$ from (C_3) ,we have

$$[1+p\omega_1(x,y)]\omega_1{}^2(x,y) \leq pmax\{0,0,0\} + m(x,y) - \emptyset m(x,y)$$
$$\leq (1-\emptyset)\omega_1{}^2(x,y)$$
$$\Longrightarrow \omega_1{}^2(x,y)\ [1+\omega_1(x,y)-1+\emptyset] \leq 0$$
$$\Longrightarrow \omega_1{}^2(x,y) = 0$$
$$\Longrightarrow x = y.$$

This completes the proof.

Corollary 1. Let $\mathcal{T}$ be a mapping of a complete modular metric space (ψ_ω,ω) into itself satisfying the condition

$$\omega_1{}^2(\mathcal{T}x,\mathcal{T}y) \leq m(x,y) - \emptyset m(x,y)$$

where,

$$m(x,y) = \max\left\{\begin{matrix} {\omega_1}^2(x,y), \omega_1(x,\mathcal{T}x)\omega_1(y,\mathcal{T}y), \\ \omega_2(x,\mathcal{T}y)\omega_1(y,\mathcal{T}x), \\ \frac{1}{2}[\omega_1(x,\mathcal{T}x)\omega_2(x,\mathcal{T}y) + \omega_1(y,\mathcal{T}x)\omega_1(y,\mathcal{T}y)] \end{matrix}\right\}.$$

For all $x, y \in \psi$ and $\emptyset\colon [0,+\infty) \to [0,+\infty)$ is a continuous function with $\emptyset(t) = 0 \Leftrightarrow t = 0$ and $\emptyset(t) > 0$ for each $t > 0$. Then $\mathcal{T}$ has a unique fixed point in ψ_ω.

Proof. Put $p = 0$ in Theorem 1 and we have the required result.

Example 1. Let ψ = $\mathbb{R}$. We define the mapping ω: (0,1) × $\mathbb{R}$ × $\mathbb{R}$ →[0,1] by $\omega_\lambda(x, y) = \frac{|x-y|}{1+\lambda}$ for all x, $y \in \mathbb{R}$ and λ> 0. Then it is obvious that $\mathbb{R}_\omega$ is a complete modular metric space. Define $\mathcal{T}$: $\mathbb{R}_\omega \to \mathbb{R}_\omega$ by $\mathcal{T}x = \frac{x}{4}$ and $\emptyset\colon [0,+\infty) \to [0,+\infty)$ by $\emptyset(t) = \frac{t}{3}$, for any values of $p > 0$ and $x, y \in \psi$. Then it is easy to verify the inequalities (C_3) and (C_4) hold.
Hence from Theorem 1, the mapping $\mathcal{T}$ has a unique fixed point 0.
Moreover, it is 0 ∈ $\mathbb{R}_\omega$.

Property P

In this section, we will show that the maps satisfying (C_3) and (C_4) possess the property P.

Let us denote the set of all fixed points of a self –mapping $\mathcal{T}$ from X into itself by F($\mathcal{T}$), that is, F($\mathcal{T}$)= { $z \in X$: $\mathcal{T}z = z$ }. It is clearly that if z is a fixed point of $\mathcal{T}$, then it is also a fixed point of $\mathcal{T}^n$ for each $n \in \mathbb{N}$, that is, F($\mathcal{T}$)⊂F($\mathcal{T}^n$) if F($\mathcal{T}$) ≠ ϕ. However, converse is false.

Indeed the mapping $\mathcal{T}$: $\mathbb{R}$ →$\mathbb{R}$ defined by $\mathcal{T}x = \frac{1}{2} - x$ has a unique fixed point, that is, F ($\mathcal{T}$) = $\left\{\frac{1}{4}\right\}$, but every $x \in \mathbb{R}$ is a fixed point for $\mathcal{T}^2$.
If F($\mathcal{T}$) = F($\mathcal{T}^n$), for each $n \in \mathbb{N}$, then we say that $\mathcal{T}^n$ has no periodic points.
(Jeong & Rhoades, 2005) examined a number of situations in which the fixed point sets for maps and their iterates are the same. They state that a map $\mathcal{T}$ has the property P if F($\mathcal{T}$) = F($\mathcal{T}^n$) for each $n \in \mathbb{N}$.

Theorem 2.

Under the condition of Theorem 1, $\mathcal{T}$ has the property P.

Proof. From Theorem 1, $\mathcal{T}$ has a fixed point. Therefore, $F(\mathcal{T}^n) \neq \phi$ for each $n \in \mathbb{N}$. Fix $n > 1$ and assume that $p \in F(\mathcal{T}^n)$.
We wish to show that $p \in F(\mathcal{T})$.
Suppose that $p \neq \mathcal{T}p$.
Using the inequality (C_3), we have

$$\begin{aligned}&[1 + p\omega_1(\mathcal{T}^{n-1}p, \mathcal{T}^n p)]{\omega_1}^2(\mathcal{T}\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^n p)\\ \leq\ & pmax\left\{\begin{matrix} \frac{1}{2}\begin{bmatrix}{\omega_1}^2(\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^{n-1}p)\omega_1(\mathcal{T}^n p, \mathcal{T}\mathcal{T}^n p) + \\ \omega_1(\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^{n-1}p){\omega_1}^2(\mathcal{T}^n p, \mathcal{T}\mathcal{T}^n p)\end{bmatrix}, \\ \omega_1(\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^{n-1}p)\omega_2(\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^n p)\omega_1(\mathcal{T}^n p, \mathcal{T}\mathcal{T}^{n-1}p), \\ \omega_2(\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^n p)\omega_1(\mathcal{T}^n p, \mathcal{T}\mathcal{T}^{n-1}p)\omega_1(\mathcal{T}^n p, \mathcal{T}\mathcal{T}^n p)\end{matrix}\right\}\\ &+\ m(\mathcal{T}^{n-1}p, \mathcal{T}^n p) - \emptyset m(\mathcal{T}^{n-1}p, \mathcal{T}^n p)\end{aligned}$$

where,

$$\begin{aligned}&m(\mathcal{T}^{n-1}p, \mathcal{T}^n p)\\ &= \max\left\{\begin{matrix}{\omega_1}^2(\mathcal{T}^{n-1}p, \mathcal{T}^n p), \omega_1(\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^{n-1}p)\omega_1(\mathcal{T}^n p, \mathcal{T}\mathcal{T}^n p), \\ \omega_2(\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^n p)\omega_1(\mathcal{T}^n p, \mathcal{T}\mathcal{T}^{n-1}p), \\ \frac{1}{2}\begin{bmatrix}\omega_1(\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^{n-1}p)\omega_2(\mathcal{T}^{n-1}p, \mathcal{T}\mathcal{T}^n p) \\ +\omega_1(\mathcal{T}^n p, \mathcal{T}\mathcal{T}^{n-1}p)\omega_1(\mathcal{T}^n p, \mathcal{T}\mathcal{T}^n p)\end{bmatrix}\end{matrix}\right\}\end{aligned}$$

$$\begin{aligned}&[1 + p\omega_1(\mathcal{T}^{n-1}p, \mathcal{T}^n p)]{\omega_1}^2(\mathcal{T}^n p, \mathcal{T}^{n+1}p)\\ &\leq pmax\left\{\begin{matrix}\frac{1}{2}\begin{bmatrix}{\omega_1}^2(\mathcal{T}^{n-1}p, \mathcal{T}^n p)\omega_1(\mathcal{T}^n p, \mathcal{T}^{n+1}p) + \\ \omega_1(\mathcal{T}^{n-1}p, \mathcal{T}^n p){\omega_1}^2(\mathcal{T}^n p, \mathcal{T}^{n+1}p)\end{bmatrix}, \\ \omega_1(\mathcal{T}^{n-1}p, \mathcal{T}^n p)\omega_2(\mathcal{T}^{n-1}p, \mathcal{T}^{n+1}p)\omega_1(\mathcal{T}^n p, \mathcal{T}^n p), \\ \omega_2(\mathcal{T}^{n-1}p, \mathcal{T}^{n+1}p)\omega_1(\mathcal{T}^n p, \mathcal{T}^n p)\omega_1(\mathcal{T}^n p, \mathcal{T}^{n+1}p)\end{matrix}\right\}\\ &\qquad + m(\mathcal{T}^{n-1}p, \mathcal{T}^n p) - \emptyset m(\mathcal{T}^{n-1}p, \mathcal{T}^n p)\end{aligned}$$

where,

$$\begin{aligned}&m(\mathcal{T}^{n-1}p, \mathcal{T}^n p)\\ &= \max\left\{\begin{matrix}{\omega_1}^2(\mathcal{T}^{n-1}p, \mathcal{T}^n p), \omega_1(\mathcal{T}^{n-1}p, \mathcal{T}^n p)\omega_1(\mathcal{T}^n p, \mathcal{T}^{n+1}p), \\ \omega_2(\mathcal{T}^{n-1}p, \mathcal{T}^{n+1}p)\omega_1(\mathcal{T}^n p, \mathcal{T}^n p), \\ \frac{1}{2}[\omega_1(\mathcal{T}^{n-1}p, \mathcal{T}^n p)\omega_2(\mathcal{T}^{n-1}p, \mathcal{T}^{n+1}p) + \omega_1(\mathcal{T}^n p, \mathcal{T}^n p)\omega_1(\mathcal{T}^n p, \mathcal{T}^{n+1}p)]\end{matrix}\right\}\end{aligned}$$

$$\begin{aligned}&[1 + p\omega_1(\mathcal{T}^{n-1}p, p)]{\omega_1}^2(p, \mathcal{T}p)\\ &\leq pmax\left\{\begin{matrix}\frac{1}{2}[{\omega_1}^2(\mathcal{T}^{n-1}p, p)\omega_1(p, \mathcal{T}p) + \omega_1(\mathcal{T}^{n-1}p, p){\omega_1}^2(p, \mathcal{T}p)], \\ \omega_1(\mathcal{T}^{n-1}p, p)\omega_2(\mathcal{T}^{n-1}p, \mathcal{T}p)\omega_1(p, p), \\ \omega_2(\mathcal{T}^{n-1}p, \mathcal{T}p)\omega_1(p, p)\omega_1(p, \mathcal{T}p)\end{matrix}\right\}\\ &+ m(\mathcal{T}^{n-1}p, p) - \emptyset m(\mathcal{T}^{n-1}p, p)\end{aligned}$$

where,

$$m(\mathcal{T}^{n-1}p,p) = \max\left\{\begin{matrix}\omega_1{}^2(\mathcal{T}^{n-1}p,p), \omega_1(\mathcal{T}^{n-1}p,p)\omega_1(p,\mathcal{T}p), \omega_2(\mathcal{T}^{n-1}p,\mathcal{T}p)\omega_1(p,p), \\ \frac{1}{2}[\omega_1(\mathcal{T}^{n-1}p,p)\omega_2(\mathcal{T}^{n-1}p,\mathcal{T}p) + \omega_1(p,p)\omega_1(p,\mathcal{T}p)]\end{matrix}\right\} = \omega_1{}^2(p,\mathcal{T}p).$$

If $\omega_1(\mathcal{T}^{n-1}p,p) \leq \omega_1(p,\mathcal{T}p)$ then
$\omega_1{}^2(p,\mathcal{T}p) \leq \omega_1{}^2(p,\mathcal{T}p)$ - $\emptyset\omega_1{}^2(p,\mathcal{T}p)$.
This implies that $p = \mathcal{T}p$, a contradiction.
Therefore, $p \in F(\mathcal{T})$ and $\mathcal{T}$has the property P.

References

Banach, S. 1922. Sur les opérations dans les ensembles abstraits et leur applications aux équations intégrales. *Fundamenta Mathematicae*, 3, pp.133-181 (in French). Available at: https://doi.org/10.4064/fm-3-1-133-181.

Chistyakov, V.V. 2010a. Modular metric spaces, I: Basic concepts. *Nonlinear Analysis: Theory, Methods and pplications*, 72(1), pp.1-14. Available at: https://doi.org/10.1016/j.na.2009.04.057.

Chistyakov, V.V. 2010b. Modular metric spaces, II: Application to superposition operators. *Nonlinear Analysis: Theory, Methods and Applications*, 72(1), pp.15-30. Available at: https://doi.org/10.1016/j.na.2009.04.018.

Chistyakov, V.V. 2006. Metric modulars and their application. *Doklady Mathematics*, 73(1), pp.32-35. Available at: https://doi.org/10.1134/S106456240601008X.

Chistyakov, V.V. 2008. Modular Metric Spaces Generated by F-Modular. *Folia Mathematica*, 15(1), pp.3-24 [online]. Available at: http://fm.math.uni.lodz.pl/artykuly/15/01chistyakov.pdf [Accessed: 10 March 2022].

Hussain, N., Khamsi, M. & Latif, A. 2011. Banach operator pairs and common fixed points in modular function spaces. *Fixed Point Theory and Applications*, art.number:75. Available at: https://doi.org/10.1186/1687-1812-2011-75.

Jeong, G.S. & Rhoades, B.E. 2005. Maps for which F($\mathcal{T}$) = F($\mathcal{T}^n$). *Demonstratio Mathematica*, 40(3), pp.671-680. Available at: https://doi.org/10.1515/dema-2007-0317.

Khamsi, M.A. 1996. A convexity property in Modular function spaces. *Mathematica Japonica*, 44(2), pp.269-279 [online]. Available at: http://69.13.193.156/publication/acpimfs.pdf [Accessed: 10 March 2022].

Khamsi, M.A. & Kirk, W.A. 2001. *An Introduction to Metric Spaces and Fixed Point Theory.* New York, NY, USA: John Wiley & Sons. Available at: ISBN: 978-0-471-41825-2.

Kozlowski, W.M. 1988. *Modular Function Spaces, Monographs and Textbooks in Pure and Applied Mathematics.* New York, NY, USA: Marce Dekker.

Mongkolkeha, C., Sintunavarat, W. & Kumam, P. 2011. Fixed point theorems for contraction mappings in modular metric spaces. *Fixed Point Theory and Applications,* art.number:93. Available at: https://doi.org/10.1186/1687-1812-2011-93.

Murthy, P.P. & Vara Prasad, K.N.V.V. 2013. Weak Contraction Condition Involving Cubic Terms of $d(x, y)$ under the Fixed Point Consideration. *Journal of Mathematics*, art.ID:967045. Available at: https://doi.org/10.1155/2013/967045.

Musielak, J. 1983. *Orlicz Spaces and Modular Spaces.* Berlin Heidelberg: Springer-Verlag. Available at: https://doi.org/10.1007/BFb0072210.

Nakano, H. 1950. *Modulared semi-ordered linear spaces.* Tokyo, Japan: Maruzen Co.

Orlicz, W. 1988a. *Collected Papers. Part I*. Warsaw Poland: PWN Polish Scientific Publishers.

Orlicz, W. 1988b. *Collected Papers. Part II*. Warsaw Poland: Polish Academy of Sciences.

Padcharoen, A., Gopal, D., Chaipunya, P. & Kumam, P. 2016. Fixed point and periodic point results for α-type F-contractions in modular metric spaces. *Fixed Point Theory and Applications*, art.number:39. Available at: https://doi.org/10.1186/s13663-016-0525-4.

Paknazar, M. & De la Sen, M. 2017. Best Proximity Point Results in Non-Archimedean Modular Metric Space. *Mathematics*, 5(2), art.number:23. Available at: https://doi.org/10.3390/math5020023.

Paknazar, M. & De la Sen, M. 2020. Some new approaches to modular and fuzzy metric and related best proximity results. *Fuzzy Sets and Systems*, 390, pp.138-159. Available at: https://doi.org/10.1016/j.fss.2019.12.012.

Rao, M.M. & Ren, Z.D. 2002. *Applications Of Orlicz Spaces (1st ed.)*. Boca Raton, FL, USA: CRC Press. Available at: https://doi.org/10.1201/9780203910863.

СВОЙСТВО P В МОДУЛЬНЫХ МЕТРИЧЕСКИХ ПРОСТРАНСТВАХ

Лиляна Паунович[а], *Парвин* Кумар[б],
Савита Малик[б], *Маной* Кумар[в]

[а] Приштинский университет– Косовска Митровица, Педагогический факультет, г. Лепосавич, Республика Сербия, **корреспондент**

[б] Тау Деви Лал – Государственный женский колледж, Муртхал, Сонипат, Харьяна, Республика Индия

[в] Университет Баба Мастнатх, Физико-математический факультет, департмент математики, Астхал Бохар, Рохтак, Харьяна, Республика Индия

РУБРИКА ГРНТИ: 27.01.00 Общие вопросы математики,
27.25.17 Метрическая теория функций,
27.39.27 Нелинейный функциональный анализ,
27.43.17 Математическая статистика
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Цель данной статьи заключается в представлении концепции обобщенного ∅-слабого сжимающего условия, включающего различные комбинации d(x,y) в модулярных метрических пространствах.

Методы: В данной статье применялись общепринятые теоретические методы функционального анализа.

Результаты: В данном исследовании представлен результат (Murthy & Vara Prasad, 2013) по однозначному отображению, соответствующему обобщенному ∅-слабому условию сокращения, включающему различные комбинации d(x,y). Оно обобщается в задании модулярных метрических пространств, а затем доказывается, что приведенное однозначное отображение отвечает свойству P. В заключении приводится пример, подтверждающий результаты.

Выводы: При соответствующих обобщениях можно сформулировать широко известные результаты классических метрических пространств для случая модулярных метрических пространств.

Ключевые слова: Фиксированная точка, ∅-слабое сжатие, модулярные метрические пространства, свойство P.

ОСОБИНА P У МОДУЛАРНИМ МЕТРИЧКИМ ПРОСТОРИМА

Љиљана Пауновић[а], *Парвин* Кумар[б],
Савита Малик[б], *Маној* Кумар[в]

[а] Универзитет у Приштини – Косовска Митровица, Учитељски факултет, Лепосавић, Република Србија, **аутор за преписку**

[б] Тау Деви Лал – Државни женски колеџ, Муртхал, Сонипат, Харијана, Република Индија

[в] Универзитет Баба Мастнатх, Природно-математички факултет, Департман за математику, Астхал Бохар, Рохтак, Харијана,Република Индија

ОБЛАСТ: математика
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Циљ овог рада јесте да представи концепт генерализованог ∅-слабог контрактивног услова који укључује различите комбинације d(x,y) у модуларним метричким просторима.

Методе: Конвенционалне теоријске методе функционалне анализе.

Резултати: Представљен је резултат (Murthy & Vara Prasad, 2013) за сингуларно пресликавање које задовољава уопштени ∅-слаби контрактивни услов који укључује различите комбинације d(x,y). Он је уопштен у постављању модуларних метричких простора.Такође, доказано је да ово сингуларно пресликавање задовољава својство P. На крају је наведен пример који подржава резултат.

Закључак: Уз одговарајуће генерализације могуће је формулисати добро познате резултате класичних метричких простора који се односе на случај модуларних метричких простора.

Кључне речи: фиксна тачка, ∅-слаба контракција, модуларни метрички простори, својство P.

Paper received on / Дата получения работы / Датум пријема чланка: 14.03.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 21. 06. 2022.
Paper accepted for publishingon / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 23. 06. 2022.

APPLICATION OF CHEBYSHEV'S INEQUALITY IN THE PRELIMINARY FEASIBILITY STUDY FOR CONSTRUCTING A SOLAR THERMAL POWER PLANT

Milan B. Pupčević[a], *Zoran* D. Mitrović[b]

[a] University of Banja Luka, Faculty of Mechanical Engineering,
Banja Luka, Republic of Srpska, Bosnia and Herzegovina,
e-mail: milan.pupcevic@mf.unibl.org, **corresponding author**,
ORCID iD: https://orcid.org/0000-0003-4494-302X

[b] University of Banja Luka, Faculty of Electrical Engineering,
Banja Luka, Republic of Srpska, Bosnia and Herzegovina,
e-mail: zoran.mitrovic@etf.unibl.org,
ORCID iD: https://orcid.org/0000-0001-9993-9082

DOI: 10.5937/vojtehg70-36734; https://doi.org/10.5937/vojtehg70-36734

FIELD: Mathematics
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: This paper examines some of the applications of Chebyshev's inequality. Using Chebyshev's inequality, the analysis of a preliminary feasibility study for constructing a solar thermal power plant in the Banja Luka area has been conducted. The goal of the preliminary analysis is to show, without financial investments, if there is a basis for the climate parameters measurement in the area.

Methods: For the known values of the arithmetic means and the standard deviations of the number of cloudy days, the probability of deviation of the number of cloudy days from the mean value was defined by applying Chebyshev's inequality.

Results: The diagram shows the values of the upper and lower limits of the number of cloudy days that deviate from the expected value with a probability of 50%.

Conclusion: The preliminary assessment of the justification of the realization of a solar thermal power plant justifies the measurements necessary for the analysis and detailed calculation of this type of a plant, because the annual interval of cloudy days is from 94 to 164, or from 26 to 44% in the year.

Key words: probability, random variable, dispersion, mean value, cloudy day, solar radiation, solar thermal power plants.

Introduction

Many natural phenomena cannot be described in exact ways by applying mathematical rules and schemes. There is not a possibility to unambiguously determine correlations and relations within them. These phenomena are known as random or stochastic and for the probability theory they are the main subject of study. One of the branches of mathematics which deals with the application of the probability theory basic results is mathematical statistics (Dekking et al, 2005; Aranđelović et al, 2011). The concept of probability is a completely determined mathematical concept, i.e. probability is a determined function defined by a set of random events. Random events show certain regularity in the frequency of their occurrence if they are observed on a large scale (Elazar, 1972).

All statistic principles are stable if they are related to mass occurrences. Random deviations from the mean value are negligible when observed on a large scale. This stability of mean values of mass occurrences is the essence of the concept of the law of large numbers (Lange, 2010). At a significant number of random occurrences, their mean result ceases to be random and could be predicted with a great precision, which is very useful at analyzing renewable energy sources systems, as they tend to have a random character (Yang et al, 2019; Wang et al, 2017; Hooshmand et al, 2012).

There are certain entry parameters needed when working on a feasibility study of the realization of a certain system. If detailed entry parameters are not available, and their collection demands measuring for a lengthy period of time, it is necessary to determine, according to the existing data, whether conducting the measurement would be justified (Bahmani et al, 2020). A feasibility study related to the construction of a solar thermal plant in the Banja Luka area needs to be based on relevant data related to solar radiation (direct, diffuse and reflected), obtained by long term measurements. Due to the lack of official data on the solar radiation for this area, the available data to be used for this purpose is the data on the number of cloudy days.

Solar thermal plants with parabolic trough collectors, unlike photovoltaic systems, do not use diffuse radiation. Based on the above mentioned, the goal of this paper is to estimate the annual number of cloudy days with a 50% probability, using Chebyshev’s inequality. If the preliminary estimation, which does not demand financial investment, leads to a conclusion that the number of cloudy days (with a 50% probability) is under

50% of the year, it is justifiable to invest and conduct measurements on which the feasibility study would be based.

Inequality in probability theory

It is impossible to predict which of possible values a random variable will have in a specific experiment. It depends on various random circumstances; however, common influence of various random circumstances can lead to the results that almost do not depend on the experiment (Simonović, 1986).

Probability (P) is a function that to each event (A) assigns a number $P(A) \in [0,1]$, and it is defined by a probability space. A probability space (Ω, F, P) consists of the sample space Ω, where the set F represents σ – algebra of the events defined on the space Ω. The function P: $F \rightarrow [0, 1]$ is the probability for Ω if it fulfills the following axioms:

- Non-negativity - $P(A) \geq 0$,
- Normalization - $P(\Omega) = 1$,
- Finite additivity - for the family of disjoint sets $\{A_i : i \in I\} \subseteq F, I \subseteq N$ it is as follows:

$$P\left(\bigcup_{i \in I} A_i\right) = \sum_{i \in I} P(A_i). \tag{1}$$

The conclusion is that the non-negativity and normalization axioms result in the following inequality: $0 \leq P(A) \leq 1$, for each $A \in F$.

The probability space where Ω is a discrete set (finite or countably infinite), and corresponding σ-algebra equals the power set of Ω, i.e. $F = P$ (Ω), is known as a discrete probability space (Jaoude, 2016).

In practice, it is important to know the conditions under which the common influence of various random circumstances leads to the results that almost do not depend on the case, as this enables the prediction of the occurrence's possible outcome (Simonović, 1986).

Definition: If on the probability space there is a continuous random variable X, with the density function *f*, and if the integral:

$$\int_{-\infty}^{+\infty} |x| \, f(x) dx, \tag{2}$$

is finite, then the random variable X has the expectation and the number:

$$EX = \int_{-\infty}^{+\infty} x \, f(x) dx, \tag{3}$$

and it is called the mathematical expectation of the random variable X (Maširević & Keglević, 2017).

In the case when Ω is a discrete set, and there is a random variable X on the discrete probability space, the mathematical expectation of the discrete random variable X can be defined as:

$$EX = \sum_{i \in I \subseteq N} x_i p_i. \tag{4}$$

Understanding the principle of mathematical expectation is only the first step in determining the parameters of a certain distribution. Dispersion (variance) is the next important parameter which represents the extent to which certain distribution deviates from its mean value. The order moment $k \in N,$ as the mathematical expectation $E(X^k)$ of the random variable X^k is defined by the following theorem which represents the basis for analyzing the dispersion concept.

Theorem: If for the random variable X there is a finite (absolute) order moment n, then there are all order moments $k<n$ (Aranđelović et al, 2011).

If the variance (expressed as $Var(X), \sigma_X^2, \sigma^2$) were defined as $E\left[X - E(X)\right]$, it would not be a valid choice as this value always equals zero, i.e. it is as follows:

$$E\left[X - E(X)\right] = E(X) - E\left[E(X)\right] = E(X) - E(X) = 0. \tag{5}$$

In addition, if the variance were defined as $E\left(\left|X - E(X)\right|\right)$, it has been proven that this measure would not have good characteristics important for probability theory. Better characteristics than the above mentioned are present at the random variable $\left[X - E(X)\right]^2$, i.e. the variance is defined as $E\left[X - E(X)\right]^2$, provided this expectation exists (Maširević & Keglević, 2017).

Based on the dispersion (2nd order moment) of the random variable X:

$$D(X) = E\left[X - E(X)\right]^2, \tag{6}$$

it follows that:

$$D(X) = E\left(X^2\right) - 2\left[E(X)\right]^2 + \left[E(X)\right]^2, \tag{7}$$

which results in the dispersion of random variables more suitable for practical calculation:

$$D(X)=E\left(X^{2}\right)-\left[E(X)\right]^{2}. \tag{8}$$

Dispersion represents the square degree of the deviation of X from its mean value, hence its root, denoted as a standard deviation of the random variable X (Aranđelović et al, 2011), is often considered, and represented as:

$$\sigma(X)=\sqrt{D(X)}=\sqrt{E\left(X^{2}\right)-\left[E(X)\right]^{2}}. \tag{9}$$

In probability theory, there is a saying that behind every limit theorem there is probability inequality, i.e. that a large number of inequalities has been discovered in very attempts to prove some of the fundamental theorems of probability theory. In this way, Chebyshev discovered his renowned inequality, later named Chebyshev's inequality after him, through which he proved the general form of the Law of large numbers. If we have a series of random variables $\left(X_{n}, n\in N\right)$ such that for each natural number n the random variables $X_{1},...,X_{n}$ are mutually independent and their variances are uniformly limited, then the probability that the realization of the random variables' $X_{1},...,X_{n}$ mean value differs from the expected mean in more than a randomly chosen small number has a tendency toward zero with the increasing number of random variables that are taken when calculating the mean. The inequality itself was first presented by French mathematician I.J. Bienaymé in 1853, and 14 years later was proven by Chebyshev (Stellato et al, 2017; Maširević & Keglević, 2017).

If the function of probability distribution is known, then the probability of an event $\{|X|\geq\varepsilon\}, \varepsilon>0,$ can be determined, where the upper limit of the probability is $P(|X|\geq\varepsilon)$(Mitrović, 2007).

Markov's inequality (Russian mathematician A.A. Markov, 1856-1922): Let X be a non-negative random variable, if there is $E\left(X^{k}\right), k\in N$, then:

$$P(X\geq\varepsilon)\leq\frac{E\left(X^{k}\right)}{\varepsilon^{k}} \text{ for each } \varepsilon>0. \tag{10}$$

Chebyshev's inequality: Also according to the author (Chen, 2011), if there is $Var(X),$ then:

$$P\left(\left|X-E(X)\right|\geq\varepsilon\right)\leq\frac{Var(X)}{\varepsilon^2}. \qquad (11)$$

Chebyshev's inequality

Pafnuty Lvovich Chebyshev (1821−1894) was a Russian mathematician. He graduated from the Moscow University where he also started his academic career. Later on he moved to Saint Petersburg where he founded one of the most significant Russian mathematical schools which today is named after him. The subject of his research was probability theory. He demonstrated the weak law of large numbers which eventually was named after him. Some of his students were famous mathematicians Markov, Lyapunov and Korkin (Medić, 2014).

Analyzing the sum of a large number of random variables and their arithmetic means, it can be noticed that partial damping of deviation at summing up causes a decrease in dispersion of the arithmetic mean and enables prediction of its possible outcome at an unlimited increase of the number of addends. Such principles and the conditions under which these principles occur constitute the content of a series of important theorems known under the common name of Law of large numbers, to which Chebyshev's as well as Bernoulli's theorems belong. Chebyshev's theorem is the most general law of large numbers, and Bernoulli's is the simplest. In order for these theorems to be proven, Chebyshev's inequality is needed, as it applies to both discrete and continuous random variables (Jaoude, 2016; Simonović, 1986).

Laws of large numbers are very useful when analyzing renewable energy sources systems, which can be said to have, to a great extent, a random character. An arithmetic mean, i.e. the mean value of many random occurrences ceases to be random and can be defined with a great certainty. These laws consider various forms of convergence of sequence of random variables towards mathematical expectation.

Supposing $E(X)=\mu$ is an arithmetic mean and σ is a standard deviation of a discrete random variable, Chebyshev formulated the following inequalities (Amidan et al, 2005; Biyya et al, 2017):

$$P\left(\left|X-\mu\right|>k\cdot\sigma=\varepsilon\right)<\frac{1}{k^2}=\frac{\sigma^2}{\varepsilon^2} \text{ and} \qquad (12)$$

$$P\left(\left|X-\mu\right|\leq k\cdot\sigma=\varepsilon\right)\geq 1-\frac{1}{k^2}=1-\frac{\sigma^2}{\varepsilon^2}, \qquad (13)$$

where k and ε are positive real numbers defined by the relation $k \cdot \sigma = \varepsilon$ from which follows:

$$\frac{1}{k^2} = \frac{\sigma^2}{\varepsilon^2}. \tag{14}$$

Based on the given inequalities, it can be said that probability, when the random variable is outside or inside of the following interval (Elazar, 1972):

$$\left[\mu - \varepsilon = \mu - k \cdot \sigma;\ \mu + \varepsilon = \mu + k \cdot \sigma\right], \tag{15}$$

is smaller than the above mentioned relation:

$$\frac{1}{k^2} = \frac{\sigma^2}{\varepsilon^2}, \tag{16}$$

or that it is not smaller than:

$$1 - \frac{1}{k^2} = 1 - \frac{\sigma^2}{\varepsilon^2}. \tag{17}$$

Chebyshev's inequality states that the probability of the random variable X to deviate from its expectation at its absolute value for greater than or equal to k standard deviations, is less than or equal to $1/k^2$ (Maširević & Keglević, 2017).

Chebyshev's inequality gives only the upper limit of the probability of the given deviation. The probability for a random variable to assume the value outside the interval $(\mu - 3\sigma, \mu + 3\sigma)$, is in practice generally far smaller than 1/9. If the distribution law is not known, and only μ and σ are, the given interval is considered to be an interval of practically possible values of the random variable X. The statistic rule stating that for normal distribution it is necessary that all the values lie within the three standard deviations of the arithmetic mean is called three sigma or 68-95-99.7 rule. More precisely, 68.27% of the values lie within one standard deviation of the mean, 95.45% of the values lie within two standard deviations of the mean and 99.73% of the values lie within three standard deviations of the mean, which can be presented as:

$$P(\mu - 3\sigma < X < \mu + 3\sigma) = 0{,}9973. \tag{18}$$

If a product whose unit of measurement is marked as J is analyzed, the values of the new components are grouped around J through a normal distribution. Any bigger deviation serves as information on the malfunctioning of the product which should be discarded.

In Figure 1, the values of the random variable X_i and its arithmetic mean μ are applied to the X axis. Based on the probability addition theorem, for any positive number ε , it can be written:

$$P\left(\left|X-\mu\right|>\varepsilon\right)=\sum_{\left|X_i-\mu\right|>\varepsilon} p_i, \qquad (19)$$

where $\left|X_i-\mu\right|>\varepsilon$ under the summation sign implies that the sum is spread across all the p_i values whose corresponding values X_i lie outside the $\overline{AB}$ straight line.

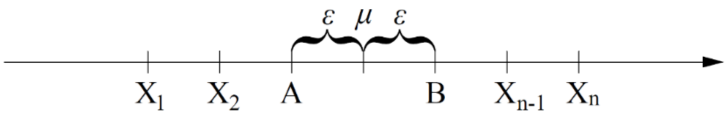


Figure 1 – X axis with random variables and the arithmetic value
Рис. 1 – Ось X со случайными переменными и средним арифметическим
Слика 1 –Оса X са случајним промјенљивим и аритметичком средином

Dispersion has the following form:

$$\sigma^2=E\left(X-\mu\right)^2=\sum_{i=1}^{n}\left(X_i-\mu\right)^2 p_i=\sum_{i=1}^{n}\left|X_i-\mu\right|^2 p_i. \qquad (20)$$

Considering that all the elements of the previous sum are positive, the sum can decrease if the values of X_i that lie outside the $\overline{AB}$ straight line are used:

$$\sigma^2>\sum_{\left|X_i-\mu\right|>\varepsilon}\left|X_i-\mu\right|^2 p_i. \qquad (21)$$

If the expression under the summation sign $\left|X_i-\mu\right|$ is replaced with ε , the sum will decrease even more:

$$\sigma^2>\sum_{\left|X_i-\mu\right|>\varepsilon}\varepsilon^2 p_i=\varepsilon^2\sum_{\left|X_i-\mu\right|>\varepsilon} p_i, \qquad (22)$$

as for all the elements of the sum it is:

$$\left|X_i-\mu\right|>\varepsilon. \qquad (23)$$

Based on the given relations:

$$P\left(\left|X-\mu\right|>\varepsilon\right)=\sum_{\left|X_i-\mu\right|>\varepsilon} p_i \quad \text{and} \quad \sigma^2>\sum_{\left|X_i-\mu\right|>\varepsilon}\varepsilon^2 p_i=\varepsilon^2\sum_{\left|X_i-\mu\right|>\varepsilon} p_i, \qquad (24)$$

a possible result is:

$$\sigma^2 > \varepsilon^2 P\left(\left|X-\mu\right| > \varepsilon\right), \tag{25}$$

which directly leads to the first Chebyshev's inequality (Elazar, 1972).

Chebyshev's inequality has a great theoretical value. Unfortunately, its practical value is limited as it gives only a rough (sometimes even trivial) probability estimation (Simonović, 1986).

For events that are said to be opposite, the following applies:

$$\left|X-\mu\right| \le \varepsilon \text{ and } \left|X-\mu\right| > \varepsilon, \tag{26}$$

and the sum of their probabilities equals one:

$$P\left(\left|X-\mu\right| \le \varepsilon\right) + P\left(\left|X-\mu\right| > \varepsilon\right) = 1. \tag{27}$$

Based on the above demonstrated and the first Chebyshev's inequality, the second Chebishev's inequality results (Elazar, 1972).

Preliminary feasibility study of solar thermal power plant construction using Chebyshev's inequality

Solar thermal power plants are sources of electrical energy generated by transforming solar energy into thermal energy by the process of heating a fluid or a solid substance and using the product in the circular process for generating electricity.

As all the forms of solar thermal plants need high temperatures to function, they have to have a system to concentrate a large area of sunlight onto a small surface. The oldest and the most commonly used type of plants of this sort are parabolic trough plants (Figure 2). They consist of long rows of parabolic mirrors (curved as a parabola) and a collector placed above them (Pupčević, 2016).

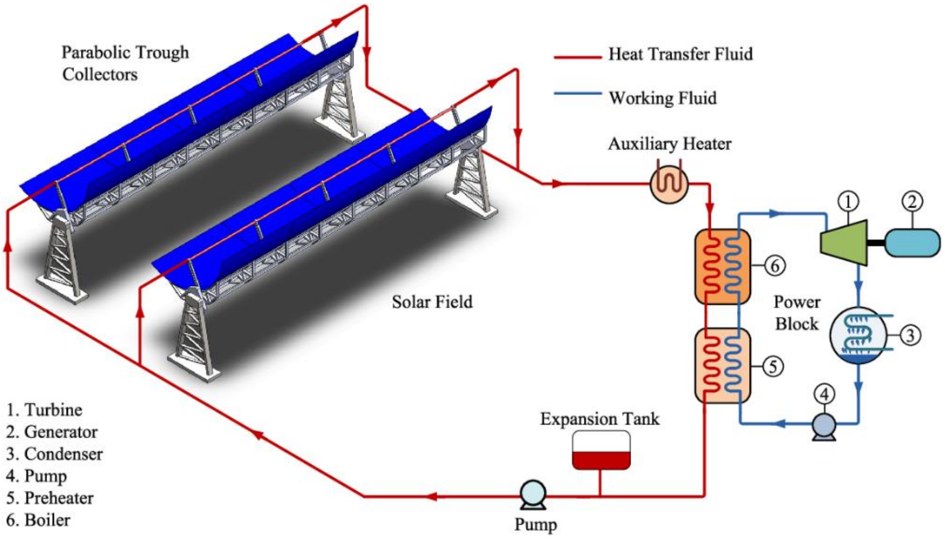


Figure 2 – Solar plant with parabolic troughs (Vasquez Padilla, 2011)
Рис. 2 – Солнечная электростанция с параболическими коллекторами (Vasquez Padilla, 2011)
Слика 2 – Соларна електрана са параболичним колекторима (Vasquez Padilla, 2011)

A form of this system, a single-axis tracking system, enables reflection of 98% of sunlight towards the focal point. The concentration ratio of the collector can be expressed by the equation:

$$k_k = \frac{A_o}{A_a} \tag{28}$$

where:

- A_o - area of the mirror collecting sunlight, and
- A_a - area of the tube - absorption.

As opposed to the flat plate solar collectors (where k_k =1 always), the systems of concentrated solar power can have this ratio up to tens of thousands.

The parabolic mirror is more curved in the centre than on the rims. This feature is necessary in order for the mirror to collect parallel sun rays into one focal point (Figure 3). Consequently, the cross section of the mirror has to have a parabolic shape with the vertex in the center of the mirror (Pupčević, 2016).

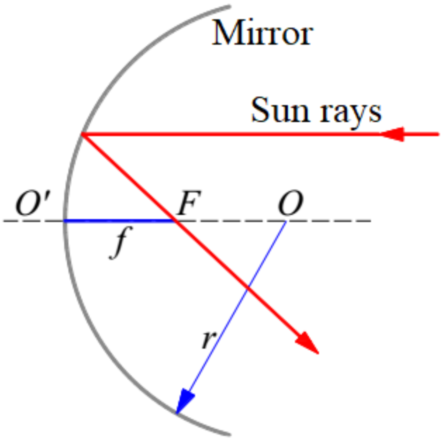


Figure 3 – Spherical mirror and its elements
Рис. 3 – Сферическое зеркало и его элементы
Слика 3 – Сферно огледало и његови елементи

The elements of spherical mirrors are:

- *O* - the center of the curvature is the center of the sphere of which the mirror is a part,
- *O′* - vertex of the mirror is its highest point,
- *r* - radius of the curvature is the radius of the sphere of which the mirror is a part,
- *OO′* - principal axis is an imaginary line passing through the vertex, focus and the centre of the mirror,
- *F* - focus is a point on the optical axis through which rays of light pass, and
- *f* - focal length is the distance between the vertex and the focus of the mirror.

The focal length equals a half of the curve radius (Han et al, 2021):

$$f = \frac{r}{2}\ [m]. \tag{29}$$

The efficiency of these plants increases with the installation of energy storing systems, which also contributes to their reliability. These systems rely on the storage of thermal energy into a material of high energy density. The heat storing systems collect the energy during sunny periods (Figure 4), and this energy is spent in the periods of low sun radiation or when there is not radiation at all.

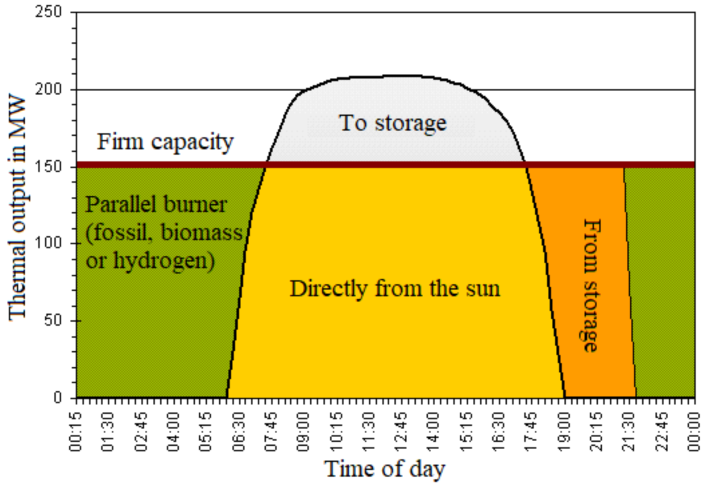


Figure 4 – Energy storing principle (Renewable Energy World, 2003)
Рис. 4 – Принцип накопления энергии (Renewable Energy World, 2003)
Слика 4 – Принцип складиштења енергије (Renewable Energy World, 2003)

Terrestrial radiation consists of:
- Z_d - direct radiation that comes to the Earth,
- Z_r - diffuse radiation, resulted from dispersion in the atmosphere,
- Z_o - reflected radiation from the Earth’s surface.

Terrestrial radiation (Figure 5) can be expressed as follows:

$$Z = Z_d + Z_r + Z_o. \tag{30}$$

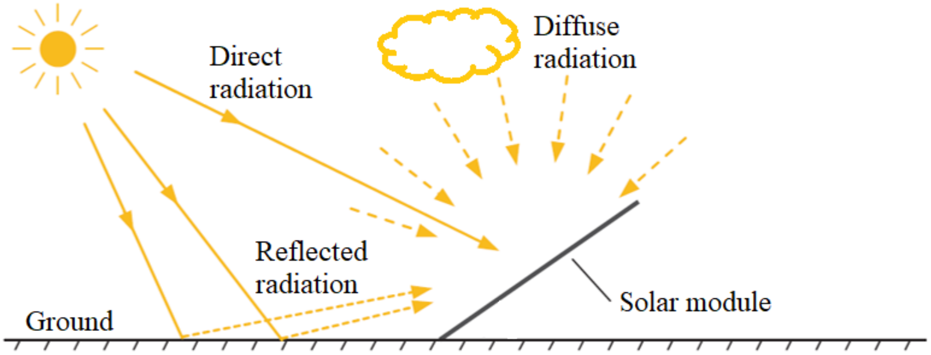


Figure 5 – Direct, diffuse and reflected solar radiation
Рис. 5 – Прямое, рассеянное и отраженное солнечное излучение
Слика 5 – Директно, дифузно и рефлектовано сунчево зрачење

When projecting and planning solar systems, it is necessary to know the exact values of different meteorological elements and parameters (Gomez-Munoz & Porta-Gandara, 2002). Concentrating collectors, in comparison to photovoltaic systems, use only direct solar radiation. Consequently, it can be said that cloudiness, as well as diffuse solar radiation, influence solar thermal plants to a great extent. The climate features of the Bosnia and Herzegovina area result from the influence of a complex climate system – from global, synoptic to mezzo and micro scales. The data necessary for a detailed solar thermal plant study are not available, as measurements have not been done. Measurements relevant for a detailed estimation would have to be taken several years in a row and they demand financial investments. For these reasons, the number of cloudy days in the Banja Luka area has been taken into account for the purposes of a preliminary analysis; more specifically, the data on the number of months a year (with a 50% probability) in which the number of cloudy days does not exceed half of the month.

In the Banja Luka area, it is cloudy or overcast on average for 128.5 days a year (Table 1). The annual number of cloudy days varies slightly less than the number of sunny days. According to the data, it ranges from 71 to 191 days. The winter period, especially January and December, is the period when almost every other day is cloudy.

Table 1 – Number of cloudy days in the Banja Luka area (Pupčević, 2016)
Таблица 1 – Количество пасмурных дней в Баня-Луке (Pupčević, 2016)
Табела 1 – Број облачних дана у Бања Луци (Pupčević, 2016)

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Oct	Nov	Dec	Year
Mid	15,8	12,8	12	10,6	9,1	8,7	6,6	6,7	7,7	9,9	14	14,5	128,5
Max	30	23	23	16	20	20	18	16	17	18	25	28	191
Min	4	0	2	1	3	2	2	1	1	3	6	1	71
σ	5,8	5,2	5,5	3,3	4,1	4,2	4,3	3,6	3,5	4,3	4,7	6,1	24,8

where:

- *Mid* - middle - expected value,
- *Max* - maximum monthly value,
- *Min* - minimum monthly value, and
- σ - standard deviation of monthly values.

Let X be a continuous random variable which denotes the average number of cloudy days per month. The middle, minimum and maximum values of the cloudy days are defined in the table above. According to the experience of the authors (Hajiagha et al, 2015; Crvenković & Rajter, 1999; Jovanović et al, 2008) and using Chebyshev's inequality:

$$P\left(\left|X-\mu\right|<k\cdot\sigma\right)=1-P\left(\left|X-\mu\right|\geq k\cdot\sigma\right)\geq 1-\frac{1}{k^2}, \qquad (31)$$

as well as based on the known expected values μ and the standard deviation σ, the probability of the number of cloudy days deviation from the mean value can be calculated. The minimum value of the number of cloudy days for January is 4, the maximum is 30 and the middle - expected value is μ =15.8 days. Taking into account the standard deviation σ = 5.8 and the deviation of 10 days, the result for January, as a critical month is as follows:

$$P\left(\left|X-15.8\right|<10\right)=P\left(\left|X-\mu\right|<k\cdot 5.8\right)\geq 1-\frac{1}{1.72^2}=0.664\,\text{implies}\,66.4\%. \qquad (32)$$

The conclusion that follows is that the probability of the number of cloudy days to deviate for January, for less than two deviations, equals at least 66%. It means that at least 66% of the realization of the random variable X is within the interval (5.8; 25.8).

Based on the above example, the deviation interval from the standard value at a 50% probability can be expressed in a different way:

$$P\left(\left|X-\mu\right|<k\cdot 5.8\right)\geq 1-\frac{1}{k^2}=0.5. \qquad (33)$$

From the above equation, k can be expressed as:

$$1-\frac{1}{k^2}=0.5 \text{ implies } k=\sqrt{2}, \qquad (34)$$

and the following correlation is defined:

$$\mathrm{P}\left(\left|\mathrm{X}-15.8\right|<\sqrt{2}\cdot 5.8\right)\geq 0.5 \text{ if and only if } \mathrm{P}\left(7.6<\mathrm{X}<24\right)\geq 0.5. \qquad (35)$$

The conclusion is that the number of cloudy days in January is under 24 and above 7.6 for the probability more than or equal to 50%.

The upper limit *(Xg)* and the lower limit *(Xd)* of the number of cloudy days per month that varies from the middle - expected value, with a 50% probability, is shown in Table 2.

Table 2 – The number of cloudy days per month with the outcome probability of 50%
Таблица 2 – Количество пасмурных дней в месяц с вероятностью исхода 50%
Табела 2 – Број облачних дана мјесечно са вјероватноћом исхода од 50%

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Oct	Nov	Dec	Year
μ	15.8	12.8	12	10.6	9.1	8.7	6.6	6.7	7.7	9.9	14	14.5	128.5
σ	5.8	5.2	5.5	3.30	4.1	4.2	4.3	3.6	3.5	4.3	4.7	6.1	24.8
k	1.41	1.41	1.41	1.41	1.41	1.41	1.41	1.41	1.41	1.41	1.41	1.41	1.41
$\lvert X\text{-}\mu\rvert$	8.20	7.35	7.78	4.67	5.80	5.94	6.08	5.09	4.95	6.08	6.65	8.63	35.07
Xg	24.00	20.15	19.78	15.27	14.90	14.64	12.68	11.79	12.65	15.98	20.65	23.13	163.57
Xd	7.60	5.45	4.22	5.93	3.30	2.76	2.00	1.61	2.75	3.82	7.35	5.87	93.43

Figure 6 shows the minimum (*Min*), maximum (*Max*) and middle (*Mid*) values of the cloudy days number for a period of 30 years. Using Chebyshev's inequality, the upper and the lower limits of the number of cloudy days with the deviation from the expected value with a 50% probability have been calculated.

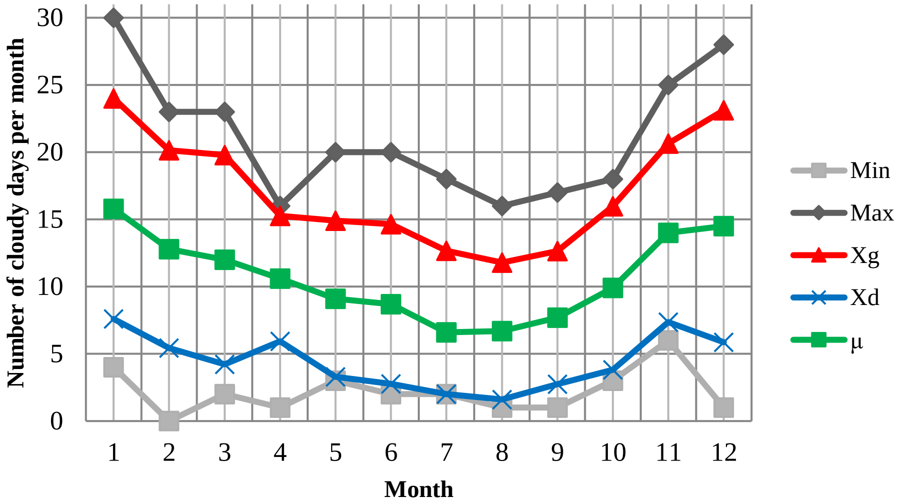


Figure 6 – Number of cloudy days per month (Min – Max) and the number of cloudy days interval around the average value with a 50% outcome probability.
Рис. 6 – Количество пасмурных дней в месяц (Мин–Макс) и интервал количества пасмурных дней около среднего значения с вероятностью результата 50%.
Слика 6 – Број облачних дана мјесечно (мин-макс) и интервал броја облачних дана око средње вриједности са вјероватноћом исхода од 50%

Conclusion

Although the estimations obtained from Chebyshev's inequality are generally quite rough, they are often used in practice for their simplicity and the quality of not depending on the values' layout. Chebyshev's inequality has a wide range of applications in cases where probability distribution is not known, while the mean value and the variance are.

The results of the analysis show that, in the worst case scenario, on an annual basis, the Banja Luka area has more than six months with the number of cloudy days that exceeds 15 days a month, (maximum, including April, although its value is higher for only 0.27 days than the upper limit value) with a 50% outcome probability. On the other hand, the measurements show that the minimum number of cloudy days per month does not exceed eight. The annual interval of cloudy days ranges from 94 to 164, i.e. 26 to 44% of the year. A very important fact is that the middle - expected value of cloudy days per month is less than 50% throughout the year. This lack of sunny days can be compensated by peak energy resources.

The preliminary feasibility study of solar thermal power plant construction in the Banja Luka area using Chebyshev's inequality justifies the measurements necessary for the analysis and detailed estimation of this type of a power plant.

References

Amidan, B.G., Ferryman, T.A. & Cooley, S.K. 2005. Data Outlier Detection using the Chebyshev Theorem. In: *IEEE Aerospace Conference*, Big Sky, MT, USA, pp.3814-3819, March 5-12. Available at: https://doi.org/10.1109/AERO.2005.1559688.

Aranđelović, I., Mitrović, D.Z. & Stojanović, V. 2011. *Verovatnoća i statistika*. Belgrade, Serbia: Zavod za udžbenike (in Serbian).

Bahmani, R., Karimi, H. & Jadid, S. 2020. Stochastic electricity market model in networked microgrids considering demand response programs and renewable energy sources. *International Journal of Electrical Power & Energy Systems,* 117(art.ID: 105606). Available at: https://doi.org/10.1016/j.ijepes.2019.105606.

Biyya, I., Aniba, G. & Maaroufi, M. 2017. Impact of Load and Renewable Energy Uncertainties on Single and Multiple Energy Storage Systems Sizing. In: *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, pp.1-5, April 23-26. Available at: https://doi.org/10.1109/ISGT.2017.8086031.

Chen, X. 2011. A New Generalization of Chebyshev Inequality for Random Vectors. *arXiv preprint* arXiv:0707.0805 [online]. Available at: https://arxiv.org/pdf/0707.0805.pdf [Accessed: 1 March 2022].

Crvenković, Z. & Rajter, D. 1999. *Zbirka rešenih zadataka iz verovatnoće i statistike*. Novi Sad, Serbia: University of Novi Sad (in Serbian).

Dekking, F.M., Kraaikamp, C., Lopuhaä, H.P. & Meester L.E. 2005. *A Modern Introduction to Probability and Statistics.* London: Springer-Verlag. Available at: https://doi.org/10.1007/1-84628-168-7.

Elazar, S. 1972. *Matematička statistika*. Sarajevo, Bosnia and Herzegovina: Zavod za izdavanje udžbenika (in Serbian).

Gomez-Munoz, V.M. & Porta-Gandara, M.A. 2002. Local wind patterns for modeling renewable energy systems by means of cluster analysis techniques. *Renewable Energy,* 25(2), pp.171-182. Available at: https://doi.org/10.1016/S0960-1481(01)00013-1.

Hajiagha, S.H.R., Hashemi, S.S., Mahdiraji, H.A. & Azaddel, J. 2015. Multi-period data envelopment analysis based on Chebyshev inequality bounds. *Expert*

Systems with Applications, 42(21), pp.7759-7767. Available at: https://doi.org/10.1016/j.eswa.2015.06.008.

Han, C-Y., Lo, W-T., Chen, K-H., Lee, J-Y., Yeh, C-H., Chen, J-H. 2021. Measurement of Focal Length and Radius of Curvature for Spherical Lenses and Mirrors by Using Digital-Grating Moiré Effect. *Photonics,* 8(7), art.number:252. Available at: https://doi.org/10.3390/photonics8070252.

Hooshmand, A., Poursaeidi M.H., Mohammadpour, J., Malki, H.A. & Grigoriads, K. 2012. Stochastic Model Predictive Control Method for Microgrid Management. In: *IEEE PES Innovative Smart Grid Technologies (ISGT)*, Washington, DC, USA, pp.1-7, January 16-20. Available at: https://doi.org/10.1109/ISGT.2012.6175660.

Jaoude, A.A. 2016. The paradigm of complex probability and Chebyshev's inequality. *Systems Science & Control Engineering*, 4(1), pp. 99-137. Available at: https://doi.org/10.1080/21642583.2016.1185044.

Jovanović, M., Merkle, M. & Mitrović, D.Z. 2008. *Vjerovatnoća i statistika-zbirka riješenih zadataka*. Banja Luka, Republic of Srpska, Bosnia and Herzegovina: Faculty of Electrical Engineering (in Serbian).

Lange, K. 2010. *Applied Probability*. New York, NY, USA: Springer. Available at: https://doi.org/10.1007/978-1-4419-7165-4.

Maširević, D.J. & Keglević, N. 2017. Chebyshev's and Markov's inequality in probability theory. *Osječki matematički list,* 17, pp.125-137 [online]. Available at: https://hrcak.srce.hr/file/285086 (in Serbian) [Accessed: 1 March 2022].

Medić, S. 2014. *Jensen and Chebyshev inequalities for interval-valued functions*. Ph.D. thesis. Novi Sad, Serbia: University of Novi Sad, Faculty of Science (in Serbian) [online]. Available at: https://nardus.mpn.gov.rs/handle/123456789/1892 [Accessed: 1 March 2022].

Mitrović, D.Z. 2007. *Primijenjena statistika – Teorija i zadaci*. Banja Luka, Republic of Srpska, Bosnia and Herzegovina: University of Banja Luka (in Serbian).

Pupčević, B.M. 2016. *Primjena reverzibilnog ciklusa centrifugalnog rashladnog uređaja za konverziju geotermalne i solarne energije u električnu.* MA thesis. Banja Luka, Republic of Srpska, Bosnia and Herzegovina: University of Banja Luka, Faculty of Mechanical Engineering (in Serbian).

-Renewable Energy World. 2003. Solar thermal power plants - Technology Fundamentals. *Renewable Energy World*, June, pp.109-113.

Simonović, V. 1986. *Uvod u teoriju verovatnoće i matematičku statistiku*. Belgrade, Serbia: Građevinska knjiga (in Serbian).

Stellato, B., Van Parys, B.P.G. & Goulart, P.J. 2017. Multivariate Chebyshev Inequality With Estimated Mean and Variance. *The American Statistician*, 71(2), pp.123-127. Available at: https://doi.org/10.1080/00031305.2016.1186559.

Vasquez Padilla, R. 2011. *Simplified Methodology for Designing Parabolic Trough Solar Power Plants*. Ph.D. thesis. University of South Florida, ProQuest Dissertations Publishing [online]. Available at: https://www.proquest.com/openview/9f7c10b791b1bef807d4fdb59eec0cee/1?pq-origsite=gscholar&cbl=18750 [Accessed: 1 March 2022].

Wang, R., Xiao, G., Wang, P., Cao, Y., Li&, G., Hao, J. & Zhu, K. 2017. Energy Generation Scheduling in Microgrids Involving Temporal-Correlated Renewable Energy. In: *GLOBECOM 2017 - 2017 IEEE Global Communications Conference,* Singapore, pp.1-6, December 4-8*.* Available at: https://doi.org/10.1109/GLOCOM.2017.8255069.

Yang, C., Liu, J., Zeng, Y. & Xie, G. 2019. Real-time condition monitoring and fault detection of components based on machine-learning reconstruction model. *Renewable Energy,* 133, pp.433-441. Available at: https://doi.org/10.1016/j.renene.2018.10.062.

ПРИМЕНЕНИЕ НЕРАВЕНСТВА ЧЕБЫШЕВА В ПРЕДВАРИТЕЛЬНОМ ТЕХНИКО-ЭКОНОМИЧЕСКОМ ОБОСНОВАНИИ СТРОИТЕЛЬСТВА СОЛНЕЧНОЙ ТЕПЛОВОЙ ЭЛЕКТРОСТАНЦИИ

Милан Б. Пупчевич[а], *Зоран* Д. Митрович[б]

[а] Университет в г.Баня-Лука, Факультет машиностроения,
г. Баня-Лука, Республика Сербская, Босния и Герцеговина,
корреспондент

[б] Университет в г. Баня-Лука, Электротехнический факультет,
г. Баня-Лука, Республика Сербская, Босния и Герцеговина

РУБРИКА ГРНТИ: 27.43.15 Теория вероятностей и случайные процессы
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: В данной статье описано применение неравенства Чебышева. Используя неравенство Чебышева, был проведен анализ предварительного технико-экономического обоснования строительства солнечной тепловой электростанции на территории Баня-Луки. Цель данного предварительного анализа состоит в том, чтобы без вложений доказать, существует ли основание для измерения климатических параметров в данном регионе.

Методы: Путем применения неравенства Чебышева для известных значений средних арифметических и стандартных отклонений в количестве пасмурных дней была определена вероятность отклонения количества пасмурных дней от среднего значения.

Результаты: На диаграмме показаны значения верхнего и нижнего пределов количества пасмурных дней, которые с вероятностью 50% не совпадают с ожидаемым значением.

Выводы: Предварительная оценка ТЭО по установке солнечной тепловой электростанции опрадывает измерения, необходимые для анализа и детального расчета данного типа установки, так *как годовой интервал пасмурных дней составляет от 94 до 164%, то есть от 26 до 44% в год.*

Ключевые слова: вероятность, случайная величина, дисперсия, среднее значение, пасмурный день, солнечная радиация, солнечные тепловые электростанции.

ПРИМЈЕНЕ НЕЈЕДНАКОСТИ ЧЕБИШЕВА У ПРЕЛИМИНАРНОЈ ОЦЈЕНИ ОПРАВДАНОСТИ РЕАЛИЗАЦИЈЕ СОЛАРНЕ ТЕРМАЛНЕ ЕЛЕКТРАНЕ

Милан Б. Пупчевић[а], *Зоран* Д. Митровић[б]

[а] Универзитет у Бањој Луци, Машински факултет,
Бања Лука, Република Српска, Босна и Херцеговина,
аутор за преписку

[б] Универзитет у Бањој Луци, Електротехнички факултет,
Бања Лука, Република Српска, Босна и Херцеговина

ОБЛАСТ: математика
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: У раду су представљене неке примјене неједнакости Чебишева. Помоћу неједнакости Чебишева анализирана је прелиминарна оцјена оправданости реализације соларне термалне електране на простору Бање Луке. Циљ ове прелиминарне анализе јесте да се докаже, без инвестиционих улагања, да ли су оправдана мјерења климатских параметара на том подручју.

Методе: За познате вриједности аритметичких средина и стандардних девијација броја облачних дана, примјеном Чебишевљеве неједнакости дефинисана је вјероватноћа одступања броја облачних дана од средње вриједности.

Резултати: На дијаграму су приказане вриједности горње и доње границе броја облачних дана које одступају од очекиване вриједности са вјероватноћом од 50%.

Закључак: Прелиминарна оцјена оправданости реализације соларне термалне електране оправдава мјерења која су неопходна за анализу и детаљни прорачун овакве врсте постројења, јер је годишњи интервал облачних дана од 94 до 164, односно од 26 до 44% периода године.

Кључне ријечи: вјероватноћа, случајна промјенљива, дисперзија, средња вриједност, облачан дан, соларно зрачење, соларне термалне електране.

Paper received on / Дата получения работы / Датум пријема чланка: 02. 03. 2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 21. 06. 2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 23. 06. 2022.

DOMINATION ON CACTUS CHAINS OF PENTAGONS

Miroslava Mihajlov Carević

Faculty for Business, Economics and Entrepeneurship,
Belgrade, Republic of Serbia,
e-mail: mm.carevic@vspep.edu.rs,
ORCID iD: https://orcid.org/0000-0001-6458-2044

DOI: 10.5937/vojtehg70-36576; https://doi.org/10.5937/vojtehg70-36576

FIELD: Materials and chemical technologies, Mathematics
ARTICLE TYPE: Original scientific paper

Abstract

Introduction/purpose: A graph as a mathematical object occupies a special place in science. Graph theory is increasingly used in many spheres of business and scientific fields. This paper analyzes pentagonal cactus chains, a special type of graphs composed of pentagonal cycles in which two adjacent cycles have only one node in common. The aim of the research is to determine the dominant set and the dominance number on ortho and meta pentagonal cactus chains.

Methods: When the corresponding destinations are treated as graph nodes and the connections between them as branches in the graph, the complete structure of the graph is obtained, to which the laws of graph theory are applied. The vertices of the pentagon are treated as nodes of the graph and the sides as branches in the graph. By applying mathematical methods, the dominance was determined on one pentagon, then on two pentagons with a common node, and then on ortho and meta pentagonal cactus chains.

Results: The research has shown that the dominance number on the ortho chain O_h of the length h ≥ 2 is equal to the value of the expression $\left\lceil \frac{3h}{2} \right\rceil$ while on the meta chain M_h it is equal to the value of the expression h+1, which was proven in this paper.

Conclusion: The results show that the dominant sets and the dominance numbers on ortho and meta pentagonal cactus chains are determined and explicitly expressed by mathematical expressions. They also point to the possibility of their application in the fields of science as well as in the spheres of business in which these structures appear.

Keywords: graph, pentagonal cactus-chain, dominant set, dominance number.

Introduction

Mathematical apparatus and mathematical methods are used in almost all fields of science, both natural (Ghergu & Radulescu, 2011; Veličković et al, 2020) and social (Vladimirovich & Vasilyevich-Chernyaev, 2021). A graph as a mathematical object occupies a special place in science (Bakhshesh, 2022; Hajian & Rad, 2021; Hernández Mira et al, 2021). It is used in medicine, genetics, chemistry, etc. All structural formulas of covalently bound compounds are graphs. Chemical elements are represented by graphs where atoms are vertices and chemical bonds are lines in the graph (Balaban, 1985). A graphical representation of chemical structures provides a visual insight into molecular bonds and chemical properties of molecules. The QSPR study has shown that many of chemical properties of molecules are closely related to theoretical graphical invariants called molecular descriptors (Mihalić & Trinajstić, 1992). The theoretical graphical invariant is also the dominance number, which is the simplest variant of the k-dominance number that is used many times in mathematics (Zmazek & Žerovnik, 2003).

A graph is usually denoted by *G*, a set of its vertices (nodes) by *V(G)* and a set of its branches (lines) by *E(G).*

A set *D* that is a subset of the set *V(G)* is called a *k*-dominant set in the graph *G* if for each vertex outside the set *D* there is at least one vertex in the set *D* such that the distance between them is less than or equal to *k*. The number of elements of the smallest *k*-dominant set is called the *k*-dominance number and is denoted by γ_k. If *k* = 1, the 1-dominance number is called the dominance number and is denoted by γ and the 1-dominant set is called the dominant set.

A cactus graph is a connected graph in which no line (branch) is in more than one cycle. The study of cactus graphs began in the middle of the 20th century. In his work (Husimi, 1950) Husimi uses these graphs in studies of cluster integrals. Riddell (Riddell, 1951) uses them in the theory of condensation. They were later used in the theory of electrical and communication networks (Zmazek & Zerovnik, 2005) as well as in chemistry (Sharma et al, 1997; Gupta et al, 2001; Gupta et al, 2002).

It is known that many chemical compounds have a pentagonal shape in their configuration. Among them are cycloalkanes, which are very common compounds in the nature. The five-membered and six-membered cycloalkanes, cyclopentane (Figure 1) and cyclohexane, which contain 5 and 6 ring carbon atoms, respectively, are very stable and their structures appear in many biological molecules.

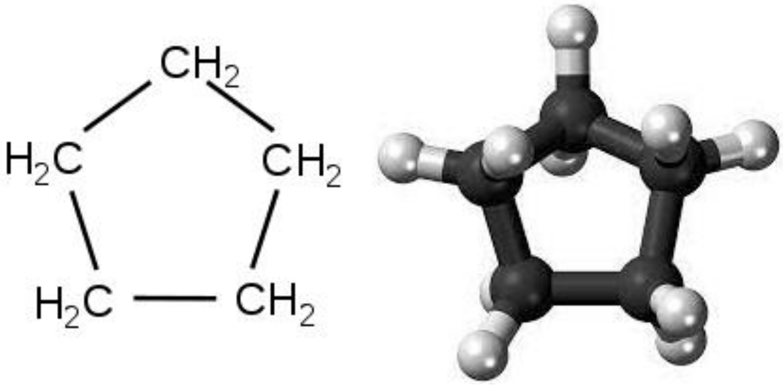


Figure 1– Cyclopentane
Рис. 1 – Циклопентан
Слика 1 – Циклопентан

Their ring structures are also included in the composition of steroids. A large number of steroids are synthesized in laboratories and used in the treatment of cancer, arthritis, various allergies and other diseases (Balaban & Zeljković, 2021). Pentagonal forms in combination with hexagonal forms are present in many compounds, among which are heterocyclic compounds: morphine, benzofuran, dibenzothiophene and others.

In this paper, we analyze the k-dominance of pentagonal cactus chains. Hexagonal cactus chains were investigated in papers (Farrell, 1987; Vukičević & Klobučar, 2007). Afterwards, the papers (Majstorovic et al, 2012; Klobučar & Klobučar, 2019) determined the dominance number on a uniform hexagonal cactus chain, the dominance number on an arbitrary hexagonal network, and the total and double total dominance number on a hexagonal network. The K-dominance on rhomboidal cactus chains (Carević et al, 2020) as well as on the icosahedral-hexagonal network (Carević, 2021) was also investigated.

Pentagonal cactus-chains

The pentagonal cactus-chain *G* is a graph consisting of a cycle with 5 vertices. A vertex that is common to two or three pentagons is called a cut-vertex. If each pentagon in the graph *G* has at most 2 cut-vertices and each cut-vertex is divided between exactly 2 pentagons, the graph *G* is called a pentagonal cactus-chain.

With G_h we will denote a pentagonal cactus-chain of the length h and G_h= $P^1P^2 \dots P^h$ where P^i are successive pentagons in the chain (Figure 2).

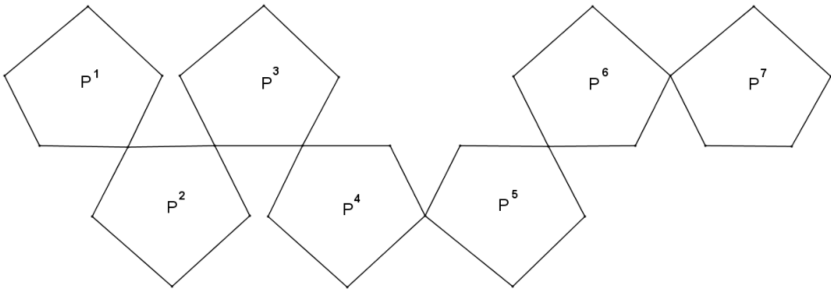


Figure 2 – Pentagonal cactus-chain of the length 7
Рис. 2 – Пятиугольная кактус-цепочка длиной 7
Слика 2 – Петоугаони кактус-ланац дужине 7

Denote by *x* and *y* the vertices in the graph *G* and by *d(x, y)* the distance between them, where the distance between two vertices is equal to the number of branches located from one vertex to another. Denote by p_i the minimum distance between the pentagons P^i and P^{i+2}:

p_i = *min*$\{d(x,y)\colon x\epsilon P^i \wedge y\epsilon P^{i+2}, i = 1,2,\dots,h-2\}$

Then p_i is the distance between the pentagons P^i and P^{i+2}.

With the exception of the first and last pentagons in the cactus chain, which have one cut-vertex, all other pentagons have two cut-vertices, and they are called inner pentagons.

In the pentagonal cactus chain G_h, we distinguish between ortho and meta inner pentagons. An inner pentagon is called an ortho pentagon if its cut-vertices are adjacent, and a meta pentagon if the distance between its cut-vertices is d = 2.

A pentagonal cactus chain is uniform if all its inner pentagons are of the same type. A chain G_h is called an ortho-chain, and is denoted by O_h if all its inner pentagons are ortho-pentagons (Figure 3).

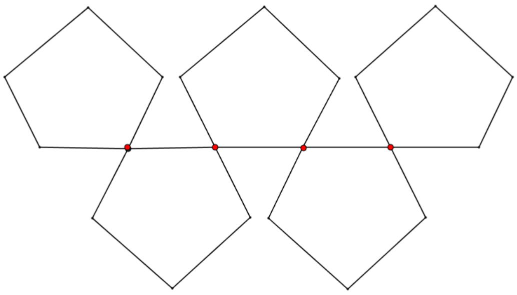


Figure 3 – Ortho cactus-chain O_5
Рис. 3 – Орто-кактус-цепочка O_5
Слика 3 – Орто кактус-ланац O_5

Analogously, a chain G_h is called a meta-chain, and is denoted by M_h if all its inner pentagons are meta-pentagons (Figure 4).

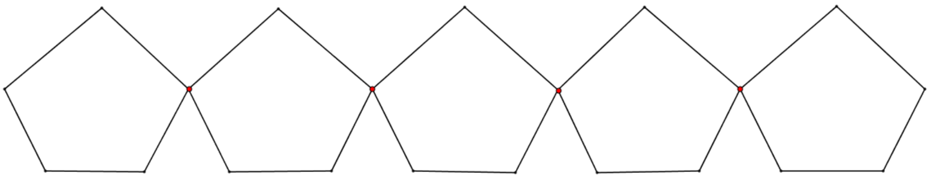


Figure 4 – Meta cactus-chain M_5
Рис. 4 – Мета кактус-цепочка M_5
Слика 4 – Мета кактус-ланац M_5

To determine the dominant set on the uniform pentagonal cactus chains O_h and M_h, it will be necessary to point out certain vertices in the cactus chain. That is why it is necessary to mark them. In the ortho pentagon P^i the cut-vertices are adjacent and we will denote them by V_i and V_{i+1}. The other vertices in P^i it will be denoted by x_1^i, x_2^iandx_3^i (Figure 5):

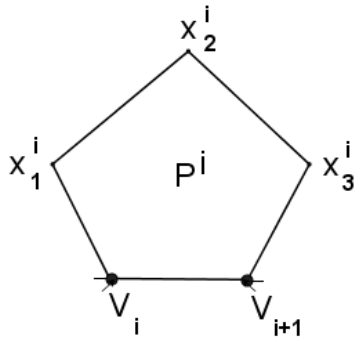


Figure 5 – Marking vertices in the ortho pentagon
Рис. 5 – Обозначение вершин в ортогональном пятиугольнике
Слика 5 – Означавање чворова у орто петоуглу

In the meta pentagon P^i the cut-vertices are at a distance d = 2 and we will denote them by V_{2i-1} and V_{2i+1}. With V_{2i}we will denote the vertex to which it applies *d(*V_{2i-1}*,* V_{2i}*)* = *d(*V_{2i}*,* V_{2i+1}*)* = 1. The other two nodes in the pentagon P^i will be denoted x_1^iandx_2^i (Figure 6):

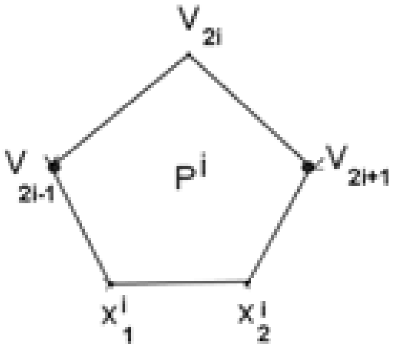


Figure 6 – Marking vertices in the meta pentagon
Рис. 6 – Обозначение вершин в мета-пятиугольнике
Слика 6 – Означавање чворова у мета петоуглу

Research results

In this section, we consider 1-dominance on ortho and meta pentagonal cactus chains. We will first consider the dominance of one pentagon and two adjacent pentagons in the ortho and meta chain of cacti.

Lemma 3.1. The dominance number for the pentagon is γ = 2.

Proof: Let us denote the vertices of the pentagon by x_1, x_2, x_3, x_4, x_5 (Figure 7):

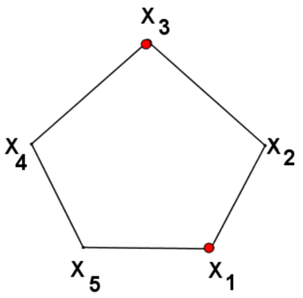


Figure 7 – Dominant set on a pentagon
Рис. 7 – Доминирующее множество на пятиугольнике
Слика 7 – Доминантни скуп на петоуглу

One pentagon vertex dominates two adjacent vertices. Let us take the vertex x_1. It dominates the vertices x_2 and x_5. As the pentagon has 5 vertices, domination over the other two vertices x_3 and x_4 is necessary. We conclude that one of the remaining two vertices must belong to the dominant set on the pentagon. Let it be the vertex x_3. Thus, the set *D* = $\{x_1,\ x_3\}$ is the dominant set for a given pentagon but it is not the only dominant set whose cardinality is equal to 2. They are also sets that contain any two non-adjacent pentagon vertices. Let us prove that any of the mentioned two-membered sets is the minimum dominant set on the pentagon. Assuming that there is a dominant set of less cardinality *D'*, it would have to contain only one vertex and one vertex cannot dominate the remaining 4 vertices of the pentagon. Thus, the minimum dominant set on a pentagon is a two-membered set, so the dominance number for the pentagon is γ = 2.

Lemma 3.2. The dominance number for two pentagons with one cut-vertex is γ = 3.

Proof: Let us denote the vertices of two pentagons by one common vertex with x_1, x_2, . . . , x_9 (Figure 8):

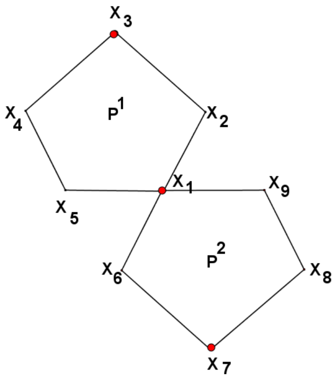


Figure 8 – Dominant set for two pentagons with a cut-vertex
Рис. 8 – Доминирующее множество для двух пятиугольников с пересекающейся вершиной
Слика 8 – Доминантни скуп за два петоугла са пресеченим чвором

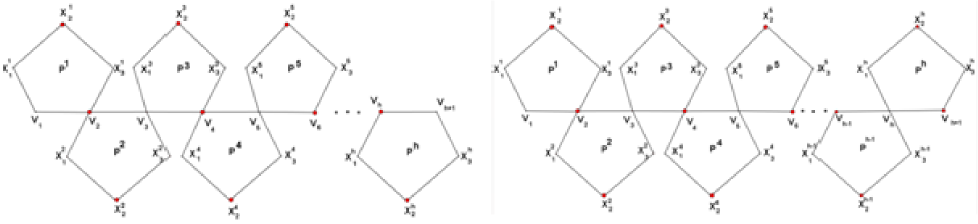
Let x_1 be the cut-vertex of the given pentagons P^1 and P^2.Based on Lemma 3.1. the pentagon P^1 excluding the vertex x_1 must have another dominant vertex that is not adjacent to the vertex x_1.Let it be the vertex x_3. Also by applying Lemma 3.1. the pentagon P^2 excluding the vertex x_1 must have another dominant vertex that is not adjacent to the vertex x_1. Let it be the vertex x_7. Thus the nodes x_1, x_3 and x_7 dominate over the nodes x_2, x_4, x_5, x_6, x_8 $\text{and} x_9$ so the dominant set for the pentagons P^1P^2 is the set D = $\{x_1$,x_3, $x_7\}$. Analogous to the consideration in Lemma 3.1. the set D is not the only three-membered set that is dominant on P^1P^2but there is no dominant set of less cardinality. Suppose that there is a dominant set D' whose cardinality is equal to 2. Let D' contain one vertex from each pentagon, for example D' = $\{x_1, x_3\}$.The vertices x_1 and x_3 would then dominate over the remaining 7 vertices in P^1P^2 and this is impossible.The vertex x_1 as a common vertex for both pentagons dominates over two neighboring vertices in both pentagons, so it dominates over 4 vertices in P^1P^2.The vertex x_3, or any other vertex not adjacent to the vertex x_1 dominates two adjacent vertices.So, the total sum of vertices covered by dominance is 4 + 2 = 6 and that is less than 7.Thus, 2 vertices cannot dominate the remaining 7 vertices in P^1P^2. We conclude that the minimum dominant set for P^1P^2 is a three-membered set and γ = 3.

Let us consider the dominance on pentagonal ortho and meta cactus chains of arbitrary length.

Theorem 3.1. *$\gamma(O_h)$ = $\left\lceil\frac{3h}{2}\right\rceil$ for each $h \geq 2 \wedge h \in N$.*

Proof: We observe a pentagonal ortho cactus-chain O_h = P^1P^2... P^h(Figure 9) and a set:

D_{O_h} = { x_2^i, *i = 1, h*} ∪ { V_{2i}, *i = 1,* $\left\lceil\frac{h}{2}\right\rceil$}



$9_A 9_B$

Figure 9 – Minimum dominant set for O_h
Рис. 9 – Минимально доминирующее множество для O_h
Слика 9 – Минимални доминантни скуп за O_h

Let us prove that D_{O_h} is the dominant set of minimum cardinality for a pentagonal ortho cactus-chain O_h= $P^1P^2 \ldots P^h$.

Let us divide the ortho-chain O_h into subchains $P^{2i-1}P^{2i}$, *i = 1, 2, ... ,* $\left\lfloor\frac{h}{2}\right\rfloor$ (Figure 10) and the last pentagon P^h if h is an odd number.

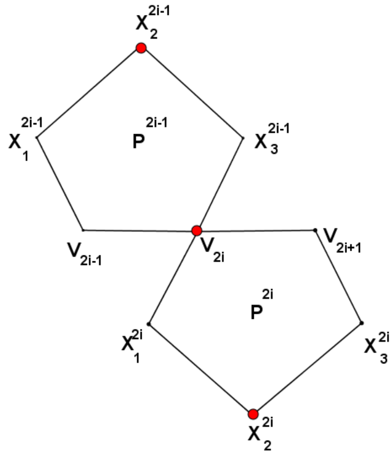


Figure 10 – Subchain of the ortho-chain O_h
Рис. 10 – Подцепочка орто-цепочки O_h
Слика 10 – Подланац орто ланца O_h

Based on Lemma 3.2. the set A_i= { $x_2^{2i-1}, x_2^{2i}, V_{2i}$} for *i = 1, 2, ... ,* $\left\lfloor \frac{h}{2} \right\rfloor$is the dominant set of minimum cardinality for the subchain $P^{2i-1}P^{2i}$. An ortho-chain of the length *h* for *h = 2k, k ϵ N* is composed of $\frac{h}{2}$ subchains $P^{2i-1}P^{2i}$, *i = 1, 2, ... ,* $\frac{h}{2}$ (Figure 9_{A}), so the set

D_1= $\bigcup_{i=1}^{k} A_i$, for *k =* $\frac{h}{2}$

is a dominant set for the ortho-chain O_h. Therefore, it is

$\gamma(O_h) \leq$ *card*(D_1) = $\frac{h}{2} \cdot 3 = \frac{3h}{2}$

where we have marked the cardinality of the set D_1 with *card*(D_1).

If *h* is an odd number (Figure 9_{B}), then the set

D_2= $\bigcup_{i=1}^{k} A_i \cup \{x_2^h,\ V_{h+1}\}$, for *k* = $\left\lfloor \frac{h}{2} \right\rfloor$

is a dominant set for the ortho-chain O_h and then is

$\gamma(\mathrm{O_h}) \leq$ *card*(D_2) = $\left\lfloor \frac{h}{2} \right\rfloor \cdot 3 + 2 = \left\lceil \frac{3h}{2} \right\rceil$.

Note that the set D_1 for *k* = $\frac{h}{2}$ if *h* an even number is equal to the following expression:

D_1= $\bigcup_{i=1}^{k} A_i = \bigcup_{i=1}^{k} \{ x_2^{2i-1}, x_2^{2i}, V_{2i} \}$ =

$= \{ x_2^1, x_2^2, V_2 \} \cup \{ x_2^3, x_2^4, V_4 \} \cup \ldots \cup \{ x_2^{h-1}, x_2^h, V_h \} =$

$= \{ x_2^i,\ i = 1, 2, \ldots, h \} \cup \{V_{2i}, i = 1, 2, \ldots, \frac{h}{2}\}$

Also for *k* = $\left\lfloor \frac{h}{2} \right\rfloor$ and *h* is an odd number, the set D_2 is equal to the following expression:

$$D_2 = \bigcup_{i=1}^{k} A_i \cup \{x_2^h,\ V_{h+1}\} =$$
$$= \bigcup_{i=1}^{k} \{ x_2^{2i-1}, x_2^{2i}, V_{2i}\} \cup \{x_2^h,\ V_{h+1}\} =$$
$$= \{ x_2^1, x_2^2, V_2\} \cup \{ x_2^3, x_2^4, V_4\} \cup \ldots \cup \{ x_2^{h-1}, x_2^h, V_h\} \cup \{x_2^h,\ V_{h+1}\} =$$
$$= \{ x_2^i,\ i = 1, 2, \ldots, h\} \cup \{V_{2i}, i = 1, 2, \ldots, \left\lceil \frac{h}{2} \right\rceil\}$$

In case h is an even number, $\frac{h}{2} = \left\lceil \frac{h}{2} \right\rceil$ then we conclude that it is $D_1 = D_2$.

So, the set D_{O_h} = { x_2^i, *i* = *1*, *h*} ∪ { V_{2i}, *i* = *1*, $\left\lceil \frac{h}{2} \right\rceil$} is the dominant set for the ortho-chain O_h when h is even or odd number.

Also, in the case where h is an even number, $\frac{3h}{2} = \left\lceil \frac{3h}{2} \right\rceil$. So, $\gamma(\mathrm{O_h}) \leq \left\lceil \frac{3h}{2} \right\rceil$when h is even or odd number. Prove that the set D_{O_h} is the dominant set of minimal cardinality. Each subchain $P^{2i-1}P^{2i}$ contains 3 dominant nodes based on Lemma 3.2. Based on this, we conclude that each dominant set on the chain O_h contains more than 3 or exactly 3 dominant nodes in each subchain $P^{2i-1}P^{2i}$and more than 2 or exactly 2 dominant nodes in the last pentagon if h is an odd number, based on Lemma 3.1. So, we conclude that it is $\gamma(\mathrm{O_h}) \geq \frac{h}{2} \cdot 3$ in case h is an even number, and $\gamma(\mathrm{O_h}) \geq \frac{h}{2} \cdot 3 + 2$ in case h is an odd number. When we combine both cases, we get that $\gamma(\mathrm{O_h}) \geq \left\lceil \frac{3h}{2} \right\rceil$.

It follows from $\gamma(O_h) \leq \left\lceil \frac{3h}{2} \right\rceil$ and $\gamma(O_h) \geq \left\lceil \frac{3h}{2} \right\rceil$ that it is $\gamma(O_h) = \left\lceil \frac{3h}{2} \right\rceil$.

Corollary 3.1.$D_{O_h} \subset D_{O_{h+1}}$ for each *h* ≥ *2* ∧ *h* ϵ *N*.

Theorem 3.2. $\gamma(M_h)$ = *h* + *1* for each *h* ≥ *2* ∧ *h* ϵ *N*.

Proof: We observe a pentagonal meta cactus-chain $M_h = P^1P^2$... P^h(Figure 11) and set:

D_{M_h} = { V_{2i-1}, *i* = *1*, *h* + *1*}

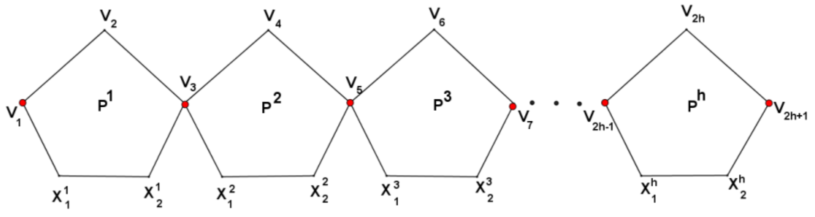


Figure 11 – Minimum dominant set for M_h
Рис. 11 – Минимально доминирующее множество для M_h
Слика 11 – Минималнидоминантни скуп за M_h

Let us prove that D_{M_h} is the dominant set of minimum cardinality for a pentagonal meta cactus-chain M_h= P^1P^2... P^h. Based on Lemma 3.1. each pentagon has a dominant set made up of two non-adjacent vertices. Thus, the set *{* V_{2i-1}, V_{2i+1}*}* is dominant for the pentagon P^i for each i = 1, h. By merging the dominant sets of all pentagons in the chain, we get a set that is dominant for the whole chain. But, each pentagon P^i has a common vertex with the pentagon P^{i+1} for each i = 1, h – 1. Common vertices should not be repeated in the dominant set. So, the set

D_{M_h} = $\bigcup_{i=1}^{h}\{ V_{2i-1}, V_{2i+1}\} \setminus \bigcup_{i=1}^{h-1}\{ V_{2i+1}\}$

is the dominant set for the meta-chain M_h.

Note that it is

$\bigcup_{i=1}^{h}\{ V_{2i-1}, V_{2i+1}\} \setminus \bigcup_{i=1}^{h-1}\{ V_{2i+1}\}$ =

$\big\{\{V_1, V_3\} \cup \{V_3, V_5\} \cup \{V_5, V_7\} \cup ... \cup \{V_{2h-1}, V_{2h+1}\}\big\} \setminus \{V_3, V_5, V_7, ..., V_{2h-1}\}$ =

$\{V_1, V_3, V_5, ..., V_{2h-1}, V_{2h+1}\}$ = *{* V_{2i-1}, *i = 1, h + 1}*

Thus, the set D_{M_h}= *{* V_{2i-1}, *i = 1, h + 1}* is the dominant set for the meta-chain M_h for each h**ϵ**N and h ≥2. Let us prove that D_{M_h} is the dominant set of minimal cardinality. Suppose that there is a set S of less cardinality that is dominant on the meta-chain M_h. The set S would then have one node less than the set D_{M_h}. Let it be a vertex V_{2i+1} for any i = 1, h. Then the pentagon P^i would have only one dominant node V_{2i-1}. Based on Lemma 3.1. that is not possible. We conclude that D_{M_h} is the minimum dominant set for M_h so it is $\gamma(M_h) = h + 1$.

Corollary 3.2.$D_{M_h} \subset D_{M_{h+1}}$ for each $h \geq 2 \wedge h \in N$.

Conclusion

In this paper, we have shown the arrangement of vertices in dominant sets on uniform ortho and meta pentagonal cactus chains that appear in molecule structures of numerous compounds. We also proved that the dominance number for a pentagonal ortho-chain of the length h is equal to the value of the expression $\left\lceil\frac{3h}{2}\right\rceil$ while for a pentagonal meta-chain it is equal to h + 1.

References

Bakhshesh, D. 2022. Isolate Roman domination in graphs. *Discrete Mathematics, Algorithms and Applications*, 14(3), art.number:2150131. Available at: https://doi.org/10.1142/S1793830921501317.

Balaban, A.T. 1985. Applications of graph theory in chemistry. *Journal of chemical information and computer sciences*, 25(3), pp.334-343. Available at: https://doi.org/10.1021/ci00047a033

Balaban, M. & Zeljković, S. 2021. *HEMIJA Teorija i eksperimenti.* Banja Luka, Republic of Srpska, Bosnia and Herzegovina: University of Banja Luka, Faculty of natural sciences and mathematics [online]. Available at: https://hemija.pmf.unibl.org/wp-content/uploads/2021/07/Balaban_Zeljkovic_Hemija_Teorija-i-eksperimenti.pdf (in Serbian) [Accessed: 20 February 2022]. ISBN: 978-99955-21-91-2.

Carević M.M. 2021. Dominating Number on Icosahedral-Hexagonal Network. *Mathematical Problems in Engineering,* art.ID:6663389. Available at: https://doi.org/10.1155/2021/6663389.

Carević, M.M., Petrović, M. & Denić, N. 2020. Dominating sets on the rhomboidal cactus chains and the icosahedral network. In: *19th International Symposium INFOTEH-Jahorina,* Jahorina, pp.152-157, March 18-20 [online]. Available at: https://infoteh.etf.ues.rs.ba/zbornik/2020/radovi/P-4/P-4-2.pdf [Accessed: 20 February 2022].

Farrell, E.J. 1987. Matchings in hexagonal cacti. *International Journal of Mathematics and Mathematical Sciences*, 10(art.ID:234184), pp.321-338. Available at: https://doi.org/10.1155/S0161171287000395.

Ghergu, M. & Radulescu, V. 2012. *Nonlinear PDEs: Mathematical Models in Biology, Chemistry and Population Genetics.* Berlin Heidelberg: Springer-Verlag. ISBN 13: 9783642226632.

Gupta, S., Singh, M. & Madan, A.K. 2001. Applications of graph theory: Relationship of molecular connectivity index and atomic molecular connectivity index with anti-HSV activity. *Journal of Molecular Structure: THEOCHEM*, 571(1-3), pp.147-152. Available at: https://doi.org/10.1016/S0166-1280(01)00560-7.

Gupta, S., Singh, M. & Madan, A.K. 2002. Application of Graph Theory: Relationship of Eccentric Connectivity Index and Wiener's Index with Anti-inflammatory Activity. *Journal of Mathematical Analysis and Applications*, 266(2), pp.259-268. Available at: https://doi.org/10.1006/jmaa.2000.7243.

Hajian, M. & Rad, N.J. 2021. Fair Total Domination Number in Cactus Graphs. *Discussiones Mathematicae Graph Theory*, 41, pp.647-664. Available at: https://doi.org/10.7151/DMGT.2225.

Hernández Mira, F.A., Parra Inza, E., Almira, J.M. S. & Vakhania, N. 2021. Properties of the Global Total k-Domination Number. *Mathematics*, 9(5), art.ID:480. Available at: https://doi.org/10.3390/math9050480.

Husimi, K. 1950. Note on Mayers' theory of cluster integrals. *The Journal of Chemical Physics*, 18(5), pp.682-684. Available at: https://doi.org/10.1063/1.1747725.

Klobučar,A. & Klobučar, A. 2019. Total and Double Total Domination Number on Hexagonal Grid. *Mathematics,* 7(11), art.number:1110. Available at: https://doi.org/10.3390/math7111110.

Majstorovic, S., Doslic, T. & Klobucar, A. 2012. *K*-Domination on hexagonal cactus chains. *Kragujevac Journal of Mathematics*, 36(2), pp.335-347 [online] Available at: https://imi.pmf.kg.ac.rs/kjm/pub/13569261514726_kjom3602-17.pdf [Accessed: 20 February 2022]

Mihalić, Z. & Trinajstić, N. 1992. A graph-theoretical approach to structure-property relationships. *Journal of Chemical Education,* 69(9), art.ID:701. Available at: https://doi.org/10.1021/ed069p701.

Riddell, R.J. 1951. *Contributions to the theory of condensation.* Ph.D. thesis. University of Michigan ProQuest Dissertations Publishing [online]. Available at: https://www.proquest.com/openview/4c69a76aaebdf43a91617e8dc2be8fe6/1?pq-origsite=gscholar&cbl=18750&diss=y [Accessed: 20 February 2022].

Sharma, V., Goswami, R. & Madan, A. K. 1997. Eccentric connectivity index: A novel highly discriminating topological descriptor for structure-property and structure-activity studies. *Journal of chemical information and computer sciences*, 37(2), pp.273-282. Available at: https://doi.org/10.1021/ci960049h.

Veličković, J., Arsić, N.B. & Stošić, L.T. 2020. The Efficiency of Galvanic Wastewater Treatment Facility ‘Frad‘ in Aleksinac. *Trendovi u poslovanju*, 8(2), pp.78-85. Available at: https://doi.org/10.5937/trendpos2002078V.

Vladimirovich, G.S. & Vasilyevich-Chernyaev, M. 2021. The experience of applying mathematical methods for analysis of the microgeneration sector in Russia. *International Review*, (1-2), pp.153-160. Available at: https://doi.org/10.5937/intrev2102156V.

Vukičević, D. & Klobučar, A. 2007. *K*-Dominating sets on linear benzenoids and on the infinite hexagonal grid. *Croatica Chemica Acta*, 80(2), pp.187-191 [online]. Available at: https://hrcak.srce.hr/12849 [Accessed: 20 February 2022].

Zmazek, B. & Zerovnik, J. 2005. Estimating the traffic on weighted cactus networks in linear time. In: *Ninth International Conference on Information Visualisation (IV'05),* London, UK, pp.536-541, July 6-7. Available at: https://doi.org/10.1109/IV.2005.48.

Zmazek, B. & Žerovnik, J. 2003. Computing the weighted Wiener and Szeged number on weighted cactus graphs in linear time. *Croatica Chemica Acta*, pp.137-143 [online]. Available at: https://hrcak.srce.hr/103089 [Accessed: 20 February 2022].

ДОМИНИРОВАНИЕ НА ПЯТИУГОЛЬНЫХ КАКТУС-ЦЕПЯХ

Мирослава Михайлов Царевич

Высшая школа экономики и предпринимательства,
г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 27.45.17 Теория графов,
61.13.21 Химические процессы
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Граф как математический объект занимает особое место в науке. Теория графов все чаще используется во многих видах деятельности и различных научных областях. В данной статье анализируются пятиугольные кактус-цепочки, как особый вид графов, состоящих из пятиугольных циклов, в которых два соседних цикла имеют только один общий узел. Цель исследования заключалась в определении доминирующего множества и доминируещего числа в орто- и мета-пятиугольных куктус-цепочках.

Методы: Когда соответствующие положения рассматриваются как узлы графа, а связи между ними − как ветви графа, получается полная структура графа, к которой применяются законы теории графов. Вершины пятиугольника рассматриваются как узлы графа, а стороны − как ветви графа. С помощью математических методов, было определено доминирование на одном пятиугольнике, затем на двух пятиугольниках с общим узлом, а затем на орто- и мета-пятиугольных кактус-цепочек.

Результаты: Исследование показало, что число доминирования на орто-цепи O_h с длиной h ≥ 2 равно значению выражения $\left\lceil\frac{3h}{2}\right\rceil$, в то время как на мета-цепи M_h оно равно значению выражения h+1, что и следовалось доказать в данной статье.

Выводы: Результаты исследования показали, что доминирующие множества и числа доминирования в орто- и мета-пятиугольных кактус-цепочках определяются и эксплицитно исчисляются математическими выражениями. Они также указывают на возможность их применения как в области науки, так и в сферах бизнеса, в которых присутствуют эти структуры.

Ключевые слова: граф, пятиугольная кактус-цепочка, доминирующее множество, число доминирования.

ДОМИНАЦИЈА НА ПЕТОУГАОНИМ КАКТУС-ЛАНЦИМА

Мирослава Михајлов Царевић

Висока школа за пословну економију и предузетништво,
Београд, Република Србија

ОБЛАСТ: материјали и хемијске технологије, математика
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Граф као математички објекат заузима посебно место у науци. Теорија графова налази све већу примену у многобројним *сферама пословања, као и научним областима. У овом раду анализирани су петоугаони кактус-ланци који представљају посебну врсту графа састављеног од петоугаоних циклуса у којима два суседна циклуса имају заједнички само један чвор. Циљ истраживања јесте одређивање доминантног скупа и доминацијског броја на орто и мета петоугаоним кактус-ланцима.*

Методе: Када се одговарајућа одредишта третирају као чворови графа, а везе међу њима као гране у графу, добија се потпуна структура графа на коју се примењују законитости теорије графова. Темена петоугла су третирана као чворови графа, а странице као гране у графу. Применом математичких метода одређена је доминација на једном петоуглу, затим на два петоугла са заједничким чвором, а након тога на орто и мета петоугаоним кактус-ланцима.

Резултати: Истраживања су показала да је доминацијски број на орто ланцу O_h *дужине h ≥2 једнак вредности израза* $\left\lceil\frac{3h}{2}\right\rceil$, *док је на мета ланцу* M_h *једнак вредности израза h + 1, што је доказано у раду.*

Закључак: Резултати показују да су доминантни скупови и доминацијски бројеви на орто и мета петоугаоним кактус-ланцима одређени и експлицитно исказани математичким изразима. Такође, упућују на могућност њихове примене у областима науке, као и у сферама пословања у којима се појављују ове структуре.

Кључне речи: граф, петоугаони кактус-ланац, доминантни скуп, доминацијски број.

Paper received on / Дата получения работы / Датум пријема чланка: 22.02.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.06.2022.
Paper accepted for publishingon / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24.06.2022.

NEW COMBINATORIAL PROOF OF THE MULTIPLE BINOMIAL COEFFICIENT IDENTITY

Vuk N. Stojiljković

University of Novi Sad, Faculty of Sciences,
Novi Sad, Republic of Serbia,
e-mail: vuk.stojiljkovic999@gmail.com,
ORCID iD: https://orcid.org/0000-0002-4244-4342

DOI: 10.5937/vojtehg70-37054;https://doi.org/10.5937/vojtehg70-37054

FIELD: Mathematics
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: In this paper a new combinatorial proof of an already existing multiple sum with multiple binomial coefficients is given. The derived identity is related to the Fibonacci numbers.

Methods: Combinatorial reasoning is used to obtain the results.

Results: The already known identity was obtained by using a new combinatorial reasoning.

Conclusions: The new combinatorial reasoning led to the solution of the already existing identity.

Key words: Fibonacci numbers, combinatorics.

Introduction

The Fibonacci numbers date as early as 200 BC in Indian mathematics, but they were named after the Italian mathematician Leonardo of Pisa, later known as Fibonacci. He published his masterpiece The Book of the Abacus in 1202 where he introduced a well-known problem of rabbits, the result of which was the Fibonacci numbers, known to many today. The Fibonacci numbers have been investigated by many and they occur in many areas. For more information about the Fibonacci numbers consult the following books (Flajolet & Sedgewick, 2009; Gessel, 1972; Grimaldi, 2012; Singh, 1985). The topic discussed in this paper is how to prove an already known multiple binomial coefficient sum, using different combinatorial reasoning than to the one already known. For the original proof see p.69 (Benjamin & Quinn, 2003).

Let us denote the notation which will be used throughout the paper. Writing

$$\sum_{\substack{\prod_{i=1}^{l} k_i=0 \\ l\geqslant 2}}^{n}$$

we mean that the number of sums depends on the parameter l, for example setting $l = 3$ we get

$$\sum_{\prod_{i=1}^{3} k_i=0}^{n} = \sum_{k_1=0}^{n}\sum_{k_2=0}^{n}\sum_{k_3=0}^{n}$$

Main results

We give our new combinatorial proof of the multi binomial identity.

THEOREM 1. *The following equality holds*

$$\sum_{\substack{\prod_{i=1}^{l+1} k_i=0 \\ l\geqslant 2}}^{n} \binom{n}{k_1}\binom{n-k_1}{k_2}...\binom{n-k_l}{k_{l+1}} = (F_{l+1})^n. \tag{1}$$

The F_l sequence is defined as follows

$$F_{l+1} = F_l + F_{l-1}, l \geq 2, F_1 = 2, F_2 = 3.$$

Where F_l is a Fibonacci Sequence but with different initial conditions and shifted by two index places.

Proof. We will prove our Theorem using combinatorial reasoning. Let n denote the number of white balls and k_i the number of colors we paint the balls with. The base case l=1 is trivial, we have n balls and we choose i of them to paint yellow $\binom{n}{i}$. On the right side we choose between two colors, yellow and white for each ball. Therefore the right side is 2^n. For simplicity let us consider the case $l = 2$. Therefore we have n balls and two colors. We pick k_1 white balls and paint them yellow which gives us $\binom{n}{k_1}$. Then we pick the balls that have not been painted yellow and paint them blue, which gives us $\binom{n-k_1}{k_2}$. The number of ways to paint the balls like this gives us the left-hand side. Alternatively, we can choose 3 colors for each ball to be painted with, white, yellow and blue, that is 3^n. Therefore, we get

$$\sum_{k_1=0}^{n}\binom{n}{k_1}\sum_{k_2=0}^{n}\binom{n-k_1}{k_2}=3^n$$

Let us now consider the case when $l = 3$, where we paint balls with three colors. We pick k_1 white balls to be painted yellow, which gives us $\binom{n}{k_1}$, then we paint those that have not been painted yellow to be painted blue $\binom{n-k_1}{k_2}$, now we choose balls which have not been painted blue to be painted red $\binom{n-k_2}{k_3}$. A ball that has been painted both yellow and red becomes an orange ball. The number of ways to paint the balls like this forms the left-hand side. On the other hand, each ball can be painted white, yellow, blue, red and orange. Therefore each ball has 5 ways to be painted, and we obtain the equality

$$\sum_{k_1=0}^{n}\binom{n}{k_1}\sum_{k_2=0}^{n}\binom{n-k_1}{k_2}\sum_{k_3=0}^{n}\binom{n-k_2}{k_3}=5^n.$$

Consider the case $l = 4$ with 4 colors. We choose k_1 white balls to be painted yellow $\binom{n}{k_1}$, and k_2 balls to be painted blue which have not been painted yellow $\binom{n-k_1}{k_2}$, k_3 balls to be painted red which have not been painted blue $\binom{n-k_2}{k_3}$, k_4 balls to be painted purple which have not been painted red $\binom{n-k_3}{k_4}$. By adding a new color, in this case purple, we paint all the balls which have not been painted with red, remember we painted a yellow one red to get an orange one and we have a red one itself, therefore we paint yellow blue and white, which is the number of colors we got in the $l = 2$ case. Therefore, by adding a new color, we have the relation $F_4 = F_3 + F_2 => F_4 = 5 + 3 => F_4 = 8$, which means that by adding a new color we have the old number of colors plus the painted ones which have not been painted with the previous color. This means we have 8 colors to choose from, which in combination with n balls gives us the following equality.

$$\sum_{k_1=0}^{n}\binom{n}{k_1}\sum_{k_2=0}^{n}\binom{n-k_1}{k_2}\sum_{k_3=0}^{n}\binom{n-k_2}{k_3}\sum_{k_4=0}^{n}\binom{n-k_3}{k_4}=8^n$$

Now observing the general case, let F_n denote the number of colors

$$\underline{F_1}\ \underline{F_2}\ldots\underline{F_{n-1}}\ \underline{F_n}\ \underline{F_{n+1}}$$

Adding a new color, we get F_{n+1}, which means we have F_n colors and we paint all the balls in F_n that have not been painted with the n-th color in F_n, which in turn gives us that the new color may paint all the balls which have not been painted with the n-th color. Therefore, we obtain a general formula

$$F_{n+1} = F_n + F_{n-1}.$$

The right-hand side is obtained by the fact that for each ball we can choose F_{n+1} colors, therefore we get $(F_{n+1})^n$.
The proof is done. □

In the following Corollary, we show the usage of the derived Theorem.

EXAMPLE 1. Setting $l = 6, n = 3$ in the previously derived Theorem, we get the following.

$$\sum_{\prod_{i=1}^{7} k_i=0}^{3} \binom{3}{k_1}\binom{3-k_1}{k_2}\binom{3-k_2}{k_3}\binom{3-k_3}{k_4}\binom{3-k_4}{k_5}\binom{3-k_5}{k_6}\binom{3-k_6}{k_7} = (34)^3$$

$$\sum_{\prod_{i=1}^{7} k_i=0}^{3} \binom{3}{k_1}\binom{3-k_1}{k_2}\binom{3-k_2}{k_3}\binom{3-k_3}{k_4}\binom{3-k_4}{k_5}\binom{3-k_5}{k_6}\binom{3-k_6}{k_7} = 39304$$

Conclusion

1. In this paper we have shown that the number of sums and the number of binomial coefficients is related to painting balls whose result is related to the Fibonacci numbers raised to the number of balls.

2. This paper motivates further research in a direction of painting various objects and the sums they can represent.

References

Benjamin, A.T. & Quinn, J.J. 2003. *Proofs that Really Count: The Art of Combinatorial Proof*. MAA -The Mathematical Association of America: The Dolciani Mathematical Expositions, 27. Available at: https://doi.org/10.5948/9781614442080.

Flajolet, P. & Sedgewick, R. 2009. *Analyitic Combinatorics*. Cambridge University Press [online]. Available at: http://algo.inria.fr/flajolet/Publications/book.pdf [Accessed: 18 March 2022]. ISBN: 978-0-521-89806-5.

Stojiljković, V., New combinatorial proof of the multiple binomial coefficient identity, pp.598–603

Gessel, I. 1972. Fibonacci is a Square. *The Fibonacci Quarterly*, 10(4), pp.417–419 [online]. Available at: https://www.fq.math.ca/Issues/10-4.pdf [Accessed: 18 March 2022].

Grimaldi, R.P. 2012. *Fibonacci and Catalan numbers: An introduction*. Hoboken, New Jersey: John Wiley and Sons, Inc. ISBN: 978-1-118-15976-7.

Singh, P. 1985. The So-called Fibonacci numbers in ancient and medieval India. *Historia Mathematica*, 12(3), pp.229-244. Available at: https://doi.org/10.1016/0315-0860(85)90021-7.

НОВОЕ КОМБИНАТОРНОЕ ДОКАЗАТЕЛЬСТВО ТОЖДЕСТВА С УЧАСТИЕМ КРАТНОГО БИНОМИАЛЬНОГО КОЭФФИЦИЕНТА

Вук Н. Стоилькович

Нови-Садский университет, факультет естественных наук,
г. Нови-Сад, Республика Сербия

РУБРИКА ГРНТИ: 27.23.25 Специальные функции,
27.25.15 Дескриптивная теория функций
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: В данной статье представлено новое комбинаторное доказательство уже существующей кратной суммы тождества биномиальных коэффициентов, связанной с числами Фибоначчи.

Методы: В статье использованы комбинаторные рассуждения.

Результаты: Уже известное тождество было получено с помощью нового комбинаторного рассуждения.

Выводы: Новое комбинаторное рассуждение привело к решению уже существующего тождества.

Ключевые слова: Числа Фибоначчи, комбинаторика.

НОВ КОМБИНАТОРНИ ДОКАЗ ИДЕНТИТЕТА СА ВИШЕСТРУКИМ БИНОМНИМ КОЕФИЦИЈЕНТИМА

Вук Н. Стојиљковић

Универзитет у Новом Саду, Природно-математички факултет, Нови Сад, Република Србија

ОБЛАСТ: математика
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак :

Увод/циљ: У овом раду представљен је нов комбинаторни доказ већ постојећег вишеструког збира, вишеструких биномних коефицијената идентитета који је у вези са Фибоначијевим бројевима

Методе: Како би се дошло до резултата користи се комбинаторно резоновање.

Резултати: Добија се већ познати идентитет коришћењем новог комбинаторног резоновања.

Закључак: Ново комбинаторно резоновање довело је до решења већ постојећег идентитета.

Кључне речи: Фибоначијеви бројеви, комбинаторика.

Paper received on / Дата получения работы / Датум пријема чланка: 19.03.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.06.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24.06.2022.

PROTOCOLS FOR SYMMETRIC SECRET KEY ESTABLISHMENT - MODERN APPROACH

Meiran Galis[a], *Tomislav* B. Unkašević[b],
Zoran Đ. Banjac[c], *Milan* M. Milosavljević[d]

[a] Institute VLATACOM, Belgrade, Republic of Serbia;
Scytale, Tel Aviv, State of Israel,
e-mail: meiran.galis@vlatacom.com,
ORCID iD: https://orcid.org/0000-0003-3017-9542

[b] Institute VLATACOM, Belgrade, Republic of Serbia,
e-mail: tomislav.unkasevic@vlatacom.com, **corresponding author**,
ORCID iD: https://orcid.org/0000-0002-6456-9250

[c] Institute VLATACOM, Belgrade, Republic of Serbia,
e-mail: zoran.banjac@vlatacom.com,
ORCID iD: https://orcid.org/0000-0001-8195-8576

[d] Singidunum University, Belgrade, Republic of Serbia,
e-mail: mmilosavljevic@singidunum.ac.rs,
ORCID iD: https://orcid.org/0000-0001-9630-804X

DOI: 10.5937/vojtehg70-36607;https://doi.org/10.5937/vojtehg70-36607

FIELD: Mathematics, Computer sciences, Telecommunications
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: The problem of efficient distribution of cryptographic keys in communication systems has existed since its first days and is especially emphasized by the emergence of mass communication systems. Defining and implementing efficient protocols for symmetric cryptographic keys establishment in such circumstances is of great importance in raising information security in cyberspace.

Methods: Using the methods of Information Theory and Secure Multiparty Computation, protocols for direct establishment of cryptographic keys between communication parties have been defined.

Results: The paper defines two new approaches to the problem of establishing cryptographic keys. The novelty in the protocol defined in the security model based on information theory is based on the source of common randomness, which in this case is the EEG signal of each subject participating in the communication system. Experimental results show that the amount of information leaking to the attacker is close to zero. A

ACKNOWLEDGMENT: The authors are grateful for the financial support from VLATACOM to project EEG and symmetric key establishment, project code: P-164

novelty in the second case, which provides security with keys at the level of computer security by applying Secure Multiparty Computation, is in the new application field, namely generation and distribution of symmetric cryptographic keys. It is characteristic of both approaches that within the framework of formal theories, it is possible to draw conclusions about their security characteristics in a formal way.

Conclusions: The paper describes two new approaches for establishing cryptographic keys in symmetric cryptographic systems with experimental results. The significance of the proposed solutions lies in the fact that they enable the establishment of secure communication between comunication parties from end to end, avoiding the influence of a trusted third party. In that way, the achieved communication level security significantly increases in relation to classical cryptographic systems.

Key words: symmetric cryptographic key, key establishment, source of randomness, advantage distillation, information reconciliation, privacy amplification, secure multiparty computation.

Introduction

The rapid development of communication and network technologies as well as technological advances in the design and implementation of microprocessor devices has led to information and communication connectivity of a large number of heterogeneous devices resulting in the creation of intelligent systems capable of monitoring and managing complex processes. Communication connectivity based on Internet infrastructure and protocols enables the establishment of complex management network systems, such as Wireless Sensor Networks (WSN) and the Internet of Things (IoT). This kind of progress brings the comfort of everyday life by advancing many technological and life processes through smart cities, autonomous vehicles, robotics and intelligent robot behavior (Mohamed, 2019; Atlam et al., 2018). In this way, a symbiotic community of people and machines is formed - Cyberspace. In this context, information security has a very important role in maintaining the integrity and privacy of data because their disruption in such an integrated world can cause serious damage, even to the level of general disaster (Ziegler, 2019; Mahmood, 2019; Banday, 2019). Therefore, in addition to security mechanisms built into Internet protocols, additional security mechanisms are used in devices and systems themselves to prevent external induction of their unwanted behavior. Almost all security mechanisms are realized by applying cryptographic methods based on cryptographic algorithms and their cryptographic keys. Accordingly, the basic precondition for the reliability of the created security mechanisms essentially depends on the quality of the designed cryptographic algorithms and the quality of the generated cryptographic keys. Each of these topics, the design of reliable cryptographic algorithms and the generation and management of cryptographic keys, represents an extensive research area. Techniques for efficient generation and management of cryptographic keys have been the subject of research throughout the history of cryptology, and the need to establish a high level of security in cyberspace has further emphasized this issue.

Managing cryptographic keys involves control over their life cycle. The life cycle of cryptographic keys assumes their generation, storage, implementation, activation, use, deactivation, revocation and destruction. In this process, the processes of generation and distribution cryptographic keys are of essential importance. The basic assumption of the quality of cryptographic solutions is that cryptographic keys are generated in a completely random way and that the parties intended to protect communications come into their possession in a way that prevents unauthorized parties from accessing their content. Until the beginning of the 1980s, classical cryptology was focused on a direct or centralized way of managing cryptographic keys:

- **Direct way of exchanging cryptographic keys** when protected communication actors exchange cryptographic keys in direct contact, Figure 1.

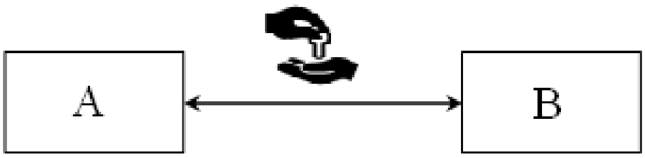


Figure 1 – Cryptographic key delivery by direct contact
Рис. 1 − Передача криптографических ключей путем прямого контакта
Слика 1 – Размена кључева у директном контакту

- **The Center for Distribution of Cryptographic Keys** can function in several different forms:
  - Predefined communication network and cryptographic keys when the communication network is defined in advance, who can com-

municate with whom, and each participant in communication is assigned a set of predefined cryptographic keys.

- Predefined communication network and assignment of cryptographic keys on request when a member of the communication system marked as A wants to protect his communication by a symmetric cryptographic algorithm with another member of the system marked as B. The initiator of the communication A addresses the Center for Generation and Distribution of Cryptographic Keys T, with the requirement for cryptographic key to communicate with B. The key assignment scenario is as follows:

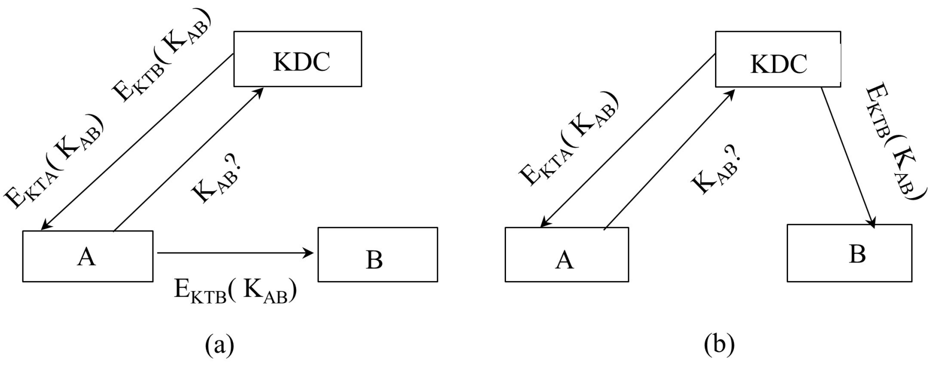


Figure 2 – Models of the cryptographic key delivery by the Key Distribution Center
Рис. 2 − Модели передачи криптографических ключей через Центр распределения криптографических ключей
Слика 2 – Модели уручења криптографских кључева преко Центра за дистрибуцију криптографских кључева

1. T generates a cryptographic key for the communication A and B denoted K_{AB}.
2. Then T form the ciphers $E_{K_{TA}}\left(K_{AB}\right)$ and $E_{K_{TB}}\left(K_{AB}\right)$.
3. The generated ciphers are delivered to the parties A and B, according to the agreed protocol, Figure 2

- **Predefined communication network and forwarding of cryptographic keys** when a member of the network, A, creates a cryptographic key K_{AB} and cipher $E_{K_{TA}}\left(K_{AB}\right)$ and forwards it to center T with a request to forward it to the user B. The Center T deciphers the received message, forms $E_{K_{TB}}\left(K_{AB}\right)$ and forwards it to B, Figure 3.

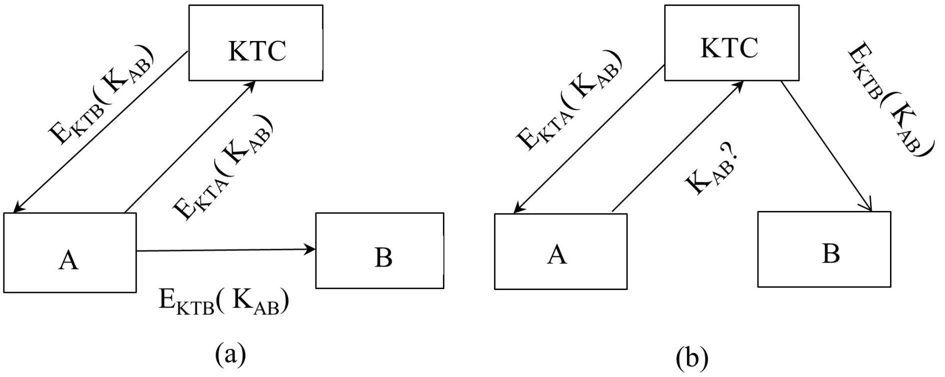


Figure 3 – Models of the Key translation center functioning
Рис. 3 − Модели функционирования Центра передачи криптографических ключей
Слика 3 – Модели уручења криптографских кључева преко Центра за пренос криптографских кључева

A more detailed overview and analysis of centralized systems for generating and distributing cryptographic keys can be found in (Menezes, 1997).

With the emergence and expansion of mass communication networks, and the need for information security, the centralized model of managing cryptographic proved to be inadequate. There are several reasons for this:

- Initial establishment of the system implies the distribution of cryptographic keys to users by the center for the generation and distribution of cryptographic keys in a secure manner (Trusted third party). In the initial phase when there are no secure data exchange channels, this is usually reduced to courier delivery of the subject keys, which in the case of mass networks, from the point of view of communication volume and number of participants, is uneconomical and inefficient.
- Achieving agreement on a single central entity for the generation and distribution of cryptographic keys is not realistic to expect according to required and necessary operational capacity as well as user needs, n^2 problem.
- A special issue is the realization of universal trust in the hypothetical center for the distribution and generation of cryptographic keys, which is, after all, the value attitude of each individual user. In today's world, which is divided over many issues, it is difficult to agree on a common high level of trust in one such entity and ways to control it.

- Attempts to the problem relaxation have led to the creation of complex hybrid models that have induced the creation of complex organizational structures resulting in demanding administration and maintenance procedures.

Searching for more efficient and comfortable solutions in the late 1970s, protocols for establishing cryptographic keys based on asymmetric cryptographic algorithms were discovered. The security of asymmetric cryptographic algorithms that are in mass use today is based on ignorance of efficient computer algorithms for factoring natural numbers, solving discrete logarithms and related problems. The theory of complexity of computer algorithms for this group of problems has no provable lower limits of complexity for algorithms that solve the mentioned problems, and accordingly their security cannot be absolute. Therefore, it is considered that this class of cryptographic protocols belongs to practically secure cryptographic algorithms, but there is no formal evidence for that. On the other hand, it has been shown that these problems are effectively solved in the quantum computer model of computation and therefore their security and usability is lost with the realization of quantum computers. In the early 1980s, ideas began to be developed to define protocols for which it would be possible to formally prove the level of security they provide to their users in relation to available computing resources, similar to Shannon's OTP encryption system. Researchers focused on the construction of protocols with the following properties:

– Elimination of the trusted third party from the process of creating and distributing cryptographic keys, which results in the possibility of establishing individual secure ”end to end” communication systems.

– For defined protocols, formal security models can be formed and theoretical conclusions can be drawn about the achieved level of security, while eliminating the need for the existence of the trusted third party.

In this context, two formal models of security of cryptographic solutions stand out:

1. Security model based on Information Theory
2. Security model based on Theory of computability and algorithm complexity

Information theoretically secure protocols for key establishment

In his seminal papers (Shannon, 1948a,b) Shannon defined the concept of cryptographic security using Information Theory and formulated the concept of absolutely secure cipher systems. Shannon's formulation did not need to take into account possible attacks and the power of a potential attacker for the simple reason that the security of cryptographic algorithms as defined by Shannon implied unlimited computing power of the attacker. In the case of cryptographic key protocols, the situation is somewhat more complex and the attacker's ability to access the messages exchanged by the protocol, the way in which it can affect protocol execution, and the ability to reconstruct the cryptographic key obtained by the protocol must be considered.

The first works on this topic appeared in the second half of the 1970s (Wyner, 1975; Maurer, 1993; Ahlswede & Csiszar, 1993) with the idea that, during the execution of the protocol illegitimate protocol observers who have access to exchanged messages cannot collect the necessary amount of information about the established cryptographic key with the aim of its restoration in an efficient manner. Over time, the importance of this type of protocol for establishing cryptographic keys has been recognized, and with the increase in security requirements in cyberspace, more and more attention has been paid to them.

The basic model of the environment in which protocols of this type are defined and analyzed is given in (Maurer, 1993). According to the symbols common in the literature, the environment in which the protocol takes place is defined in the following way. Alice and Bob are actors who want to achieve mutual protected communication using a symmetric cryptographic algorithm, and for that they need a common secret key. Eve is curious and interested in the information that Alice and Bob exchange and she knows the protocol according to which they exchange messages and the cryptographic algorithm they will use. The only way Eve can access Alice and Bob's information, provided the applied cryptographic algorithm is safe, is to somehow get their cryptographic key. It is assumed that Eve has an insight into all the messages that are exchanged during the protocol between Alice and Bob. Based on the information gathered, Eve tries to reconstruct the cryptographic key that Alice and Bob perform after the protocol is completed. The initial data, the strings of symbols, which are used in the execution of the protocol for establishing the cryptographic key Alice, Bob and Eve get in the following way. In a common source, a series of symbols is generated by some random process, denoted by $U^n = \{u_1, u_2, \ldots, u_n\}$, through independent binary symmetric channels of known characteristics are sent to Alice, Bob and Eve who register them as strings of symbols $X^n = \{x_1, x_2, \ldots, x_n\}$, $Y^n = \{y_1, y_2, \ldots, y_n\}$, $Z^n = \{z_1, z_2, \ldots, z_n\}$ respectively. The model is shown in Figure 4.

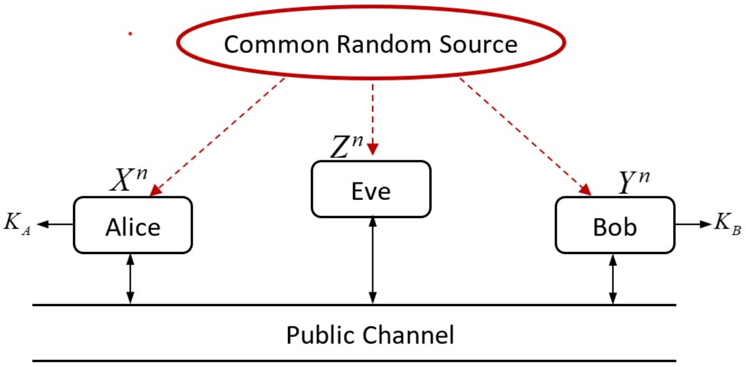


Figure 4 – Model of the execution environment for the Information theoretic based symmetric key establishment protocol
Рис. 4 – Изображение среды выполнения протокола установления криптографических ключей в рамках теоретико-информационной модели
Слика 4 – Графички приказ окружења извршавања протокола за установљавање криптографских кључева у информационо-теоретском моделу

The result of the protocol execution is to obtain a series of symbols K_A, K_B, with the objectives:

1. The probability that the resulting arrays are equal, $P(K_A = K_B)$, is close to unity. At the end of the protocol, a procedure, which does not violate the security of the process, can be performed to determine this equality, and the resulting symbol string is denoted by $K^{m(n)} = K_A = K_B$ where $m(n)$ is the length of the string symbols obtained after the protocol execution.
2. The protocol is safe from the point of view of the obtained key, $K^{m(n)}$, in the sense that Eve is not able to reconstruct the value of $K^{m(n)}$

which is expressed by

$$I\left(K^{m(n)}, Z^n\right) = 0. \tag{1}$$

This condition has proven to be quite limiting in practice and its somewhat weaker variant expressed with

$$\lim_{n\to\infty} I\left(K^{m(n)}, Z^n\right) = 0. \tag{2}$$

where n is the length of the initial string of symbols.

Condition (2) essentially means that Eve has the information about $K^{m(n)}$ but it is not enough to effectively approximate or reconstruct the key $K^{m(n)}$. In this way, the computing and algorithmic power that Eve has is abstracted, similar to the definition of the security of cryptographic algorithms in Shannon's book, (Shannon & Weaver, 1963).

General structure of the information theoretically secret key establishment protocols

According to the functional model shown in Figure 4, the protocol takes place in several steps. In the first step, a common source of randomness generates a series of random symbols $U^n = \{u_1, u_2, \ldots, u_n\}$ which by a discrete symmetric communication channels without the memory of known characteristics, P_{XYZ}, forwards to Alice, Bob and Eve who register them as strings of symbols X^n, Y^n, Z^n respectively. In the described communication channel $(P_{XYZ}$, X^n, Y^n, $Z^n)$ errors can occur during transmission, in the general case the sequences X^n, Y^n, Z^n are different from each other. In the next phase, Alice and Bob exchange messages via a public authenticated channel to detect parts of the initial set of symbols that are common to them. The way of communication is constructed so that the similarity of their symbol strings increases and the similarity of Eve's string of symbols with Alice's/Bob's string of symbols either does not change or decreases despite the known content of the exchanged messages. A measure appropriate to the situation is taken as a measure of similarity, most often Hamming's distance. This phase is called advantage distillation. After that, in the third phase of the protocol, Alice and Bob exchange messages through a publicly authenticated channel that allows them to extract identical parts in their symbol strings and thus arrive at a string of symbols that is common to both. Here, too, it is understood that Eve's knowledge of the obtained common set of symbols does not increase. This phase is called the phase of Information reconciliation. In the final part of the protocol, Alice and Bob construct a common symmetric key by applying a pre-agreed publicly known function to the derived common symbol string, and this step is called Privacy amplification.

Common randomness source sequence distribution

The primary requirement in the process of generating cryptographic keys is that the created cryptographic key has maximum entropy in relation to its length and that the entropy of the plain text messages is not greater than the entropy of the space of possible keys. Systems that meet this condition are known to be secure against an attacker with unlimited computing resources (processor speed, memory, power). This includes the attacker's approach to quantum computers. Probability theory and mathematical statistics have developed techniques by which realizations of random variables with different probability distribution functions under certain conditions can be transformed into realizations of random variables with uniform distribution. With this in mind, the idea of an information-theoretical approach in this context is to identify and extract equal parts with sufficiently high entropy from two mutually correlated signals. According to the nature of the randomness sources used in this phase, we distinguish two models:

1. Random processes that are not connected to the communication channel - source model, such as in (Galis et al., 2021).
2. Random processes related to the communication channel model are used as a source of randomness, such as in (Maurer, 1993).

Advantage distillation phase

In accordance with the model shown in Figure 4, we can consider that the binary symmetric channels through which Alice, Bob and Eve get their strings X^n, Y^n, Z^n are mutually independent and characterized by error probabilities p_A, p_B,and p_E respectively with $0 < p_A, p_B, p_E < \frac{1}{2}$. For practical applications, the relevant situation is when $0 < p_E < min\ \{p_A, p_B\}$. In this context, it can be considered that Alice sends her symbol string X^n through a binary symmetric channel to Bob who receives it as a string Y^n

with an error probability

$$\begin{aligned} & p_{AB} = P\left(x_i \neq y_i\right) = \\ & = P\left(x_i \neq y_i \,\middle|\, x_i = u_i\right) \cdot P\left(x_i = u_i\right) + P\left(x_i \neq y_i \,\middle|\, x_i \neq u_i\right) \cdot P\left(x_i \neq u_i\right) \\ & = P\left(y_i \neq u_i\right) \cdot P\left(x_i = u_i\right) + P\left(y_i = u_i\right) \cdot P\left(x_i \neq u_i\right) = \\ & = p_B \cdot (1 - p_A) + (1 - p_B) \cdot p_A \end{aligned} \tag{3}$$

The relationship between Alice's and Eve's set of symbols is observed in the same way, and the probability of error in that binary symmetric channel is given by

$$p_{AZ} = p_Z \cdot (1 - p_A) + (1 - p_Z) \cdot p_A \tag{4}$$

The aim of this part of the protocol for Alice and Bob is to exchange messages via a public authenticated channel and to select subsets of symbols from X^n, Y^n where the error will be less than (3) without revealing too much information to Eve and the error in her channel will not be less than (4). Below we will describe the most commonly used protocols of this type.

The repetition code advantage distillation protocol (RCAD) This protocol is described in (Maurer, 1993; Bloch & Barros, 2011; Tan et al., 2020). For the selected segment of the initial bit string of the length N, Alice randomly generates the bit r $\left(P\left(r=0\right) = P\left(r=1\right) = \frac{1}{2}\right)$ and the code word $R^N = \left(\overbrace{r, r, ...r}^{N}\right)$. Then she calculated

$$X^N + R^N = (r + x_1, r + x_2, \ldots, r + x_N)$$

and the resulting vector is sent to Bob. Upon receiving Alice's message, Bob calculates

$$Y^N + X^N + R^N = (y_1 + r + x_1, y_2 + r + x_2, \ldots, y_N + r + x_N)$$

If as a result Bob gets $\left(\overbrace{r, r, ...r}^{N}\right)$ where $r \in \{0, 1\}$ he assumes that his and Alice's sequences coincide. Bob in response to Alice sends the bit F

$$F = \begin{cases} 1 & \text{Bob gets } \left(\overbrace{r, r, ...r}^{N}\right) \\ 0 & \text{otherwise} \end{cases} .$$

If $F = 1$, that sequences are considered equal on both sides and participate in the construction of a new bit string, otherwise that bit sequence is omitted from the further process. The value of the parameter N is determined according to the situation and optimized so that the probability of matching is maximal and the level of information leakage to Eve is minimal. It can be shown that, on the accepted segments after the end of the RCAD protocol, the next statements are valid, (Bloch & Barros, 2011; Wang et al., 2015):

1. On the accepted segment of the length N between Alice and Bob the error probability is

$$p_{AB}^{RCAD} = \frac{(p_{AB})^N}{(p_{AB})^N + (1 - p_{AB})^N}$$

   and p_{AB} is the probability of error on the segment of the length N before starting the protocol execution.

2. Since $X^N + R^N$ is transmitted through a public channel, Eve can calculate $Z^N + X^N + R^N$ and then the error between Eve's and Alice's segment is expressed with

$$p_{AE}^{RCAD} = \frac{1}{(p_{AE})^N + (1 - p_{AE})^N} \cdot \sum_{w=\lceil \frac{N}{2} \rceil}^{N} \binom{N}{w} p_w$$

   where p_w is probability that vector of length N has Hamming weight w.

3. Data remaining efficiency, as a quotient between the length of the initial string and the length of the string obtained after the protocol execution, is given with the next equation (Wang et al., 2015)

$$\mu_{AB}^{RCAD}(p_{AB}) = \frac{(p_{AB})^N + (1 - p_{AB})^N}{N}.$$

The significance of this solution lies primarily in the fact that the possibility of implementing secure protocols for establishing cryptographic keys from the Information theory point of view elimination of trusted third parties has been demonstrated in a constructive way. The main drawback of this protocol lies in the fact that in the case when p_E is significantly less than p_A, p_B it is quite inefficient in terms of the length of the derived key. A more efficient variant of this protocol is described in (Maurer, 1993).

The bit pair iteration advantage distillation protocol (BPIAD) The BPIAD protocol is an iterative protocol that, starting from the initial bit strings X^n, Y^n in each iteration, generates a sequence for the next iteration. The result of the last iteration is processed in the next stages of the key establishment protocol. The following steps are performed in each iteration of the AD protocol, (Wang et al., 2015):

(1) In the $s-$th iteration Alice and Bob have strings of symbols of the length n_s bits and form blocks of two consecutive bits.

(2) Alice computes the parity bit for each block $\left\{X_{2i+1} \oplus X_{2i},\, i = 0, 1, \ldots, \left\lfloor \frac{n_s}{2} \right\rfloor\right\}$ and send them to Bob.

(3) Bob computes his parity bits $\left\{Y_{2i+1} \oplus Y_{2i},\, i = 0, 1, \ldots, \left\lfloor \frac{n_s}{2} \right\rfloor\right\}$ and compares them with Alice's parity bits. For every i for which is $X_{2i+1} \oplus X_{2i} \neq Y_{2i+1} \oplus Y_{2i}$ pairs X_{2i+1}, X_{2i} and Y_{2i+1}, Y_{2i} are removed from the further process. In the case that $X_{2i+1} \oplus X_{2i} = Y_{2i+1} \oplus Y_{2i}$ bit X_{2i+1} is included in Alice's string and bit Y_{2i+1} is included in Bob's string for the next iteration $s+1$.

It turns out that it is at the end of the $s-$th iteration, (Wang et al., 2015):

$$\begin{aligned} p_{AB_s}^{BPIAD} &= \frac{\left(p_{AB_0}\right)^{2^s}}{\left(p_{AB_0}\right)^{2^s} + \left(1 - p_{AB_0}\right)^{2^s}} \\ p_{AE_s}^{BPIAD} &= p_{AE_0}^{BPIAD} \\ \mu_{AB_s}^{RCAD}\left(p_{AB_0}\right) &= \frac{\left(p_{AB_0}\right)^2 + \left(1 - p_{AB_0}\right)^2}{2^s} \end{aligned} \tag{5}$$

The analysis of the described protocol and the results given in (5) concludes that the number of iterations depends on the size p_{AB_0} and that with its increase the required number of iterations increases so that the symbol strings obtained in this phase can be productively used in the following, $p_{AB_s}^{BPIAD} < p_{AE_s}^{BPIAD}$. Also, the protocol is extremely inefficient in terms of the ratio of the lengths of the initial and obtained bit strings, because according to the third equation in (5), the length of the obtained bit string decreases exponentially with the number of iterations.

The bit pair iteration advantage distillation/degeneration protocol (BPIADD) The fact that during the BPIAD protocol the probability of error in Eve's bit string remains constant during the execution of the protocol remains constant, the second equality in (5) indicates the possibility of increasing Eve's capacity to obtain more information about Alice's bit string during the next protocol phase. In order to reduce these possibilities and provide more favorable initial conditions for the next phase, Information reconciliation, the BPIADD protocol is defined as follows, (Wang et al., 2015):

(1) Alice computes $A_k = X_{2k-1} \oplus X_{2k}$ $k = 1, 2, \ldots$and sends A_k to Bob.

(2) Bob computes $B_k = Y_{2k-1} \oplus Y_{2k}$ $k = 1, 2, \ldots$and sends B_k to Alice.

(3) For every $k = 1, 2, \ldots$ the following procedure is performed:

- If $A_k \neq B_k$ then Alice deletes X_{2k-1}, X_{2k} from X and Bob deletes Y_{2k-1}, Y_{2k} from Y.
- If $A_k = B_k$ then Alice checks if $X_{2k} = 1$. If it is, then she deletes X_{2k-1} from X and if not, she deletes X_{2k} from X. Bob does the same in the case of the string Y.

It turns out that after the first iteration of this protocol, the following relations are valid (Wang et al., 2015):

$$\begin{aligned} p_{AB_1}^{BPIADD} &= \frac{1}{2} \cdot \frac{\left(p_{AB_0}\right)^2}{\left(p_{AB_0}\right)^2 + \left(1 - p_{AB_0}\right)^2} < p_{AB_0} \\ p_{AE_1}^{BPIADD} &= \frac{p_{AE_0}}{2} + p_{AE_0}\left(1 - p_{AE_0}\right) > p_{AE_0} \\ \mu_{AB_1}^{RCAD}\left(p_{AB_0}\right) &= \frac{\left(p_{AB_0}\right)^2 + \left(1 - p_{AB_0}\right)^2}{2} \end{aligned} \tag{6}$$

From the first and second expressions in (6) it is clear that the error in the Alice and Bob's sequence decreases monotonically and the error in the Alice and Eve's series increases monotonically. By applying the protocol in several iterations using (6) we get that in the $s-$th iteration in order, the following is valid:

$$\begin{aligned} p_{AB_s}^{BPIADD} &= \frac{1}{2} \cdot \frac{\left(p_{AB_{s-1}}\right)^2}{\left(p_{AB_{s-1}}\right)^2 + \left(1 - p_{AB_{s-1}}\right)^2} < p_{AB_{s-1}} \\ p_{AE_s}^{BPIADD} &= \frac{p_{AE_{s-1}}}{2} + p_{AE_{s-1}}\left(1 - p_{AE_{s-1}}\right) > p_{AE_{s-1}} \\ \mu_{AB_s}^{RCAD}\left(p_{AB_{s-1}}\right) &= \frac{\left(p_{AB_{s-1}}\right)^2 + \left(1 - p_{AB_{s-1}}\right)^2}{2} \end{aligned} \tag{7}$$

In this way, the difference between Eve's and Alice's string becomes large enough and the difference between Alice's and Bob's string becomes small enough that the process of information reconciliation and the amount of information that leaks to Eve during it does not have a significant impact on the derived cryptographic key.

Information reconciliation After completing the previous phase, advantage distillation, Alice and Bob have reached a situation where they have an advantage over Eve in terms of the amount of mutual information about their bit strings. In this phase of the protocol, Alice and Bob's goal is to use an authenticated public channel for communication to exchange information that will allow them to correct any differences in the current bit strings they formed during previous phases of the protocol. All messages exchanged through the public channel are also available to Eve. The more information Eve can extract from this communication imply the shorter length of the secret key at the end of the process.

The first such protocol is described in (Bennett et al., 1992). From the point of view of mass application and efficiency, several widely used solutions have crystallized:

- In practice, the CASCADE protocol defined in (Brassard & Salvail, 1992) is widely used today. The protocol is iterative in its nature and in the $i-$th iteration it takes place in the following way. According to a pre-agreed permutation, Alice and Bob permute $X^n Y^n$. The resulting bit strings are divided into blocks of length k_i bits. Alice calculates the parity bit for each of her blocks and sends them to Bob. Bob compares Alice's parity bits to his parity bits on matching positions. If there is a discrepancy between Alice and Bob's parity bit for some block they apply the binary search algorithm on that block and the exchange additional parity bits for some sub-blocks of the current block with the aim to detect an incorrect bit. Upon incorrect bit detection, Bob changes its value. Bob then analyzes the effect of the changed bit on the previous iterations and eventually detects and corrects previously masked errors. This procedure is repeated for each block of bits that does not agree with Alice's corresponding blocks. Since all blocks in this iteration are processed, the next iteration is taken with $k_{i+1} = 2 \cdot k_i$. The initial choice of the block length, k_1, is critical for the efficiency of the algorithm. Many papers have dealt with experimental and theoretical analyses of this problem in order to achieve an optimal performance (Bennett et al., 1988; Cachin & Maurer, 1997; Carleial & Hellman, 1977; Csiszar & Korner, 1978). Sugimoto and Yamazaki in their papers (Sugimoto & Yamazaki, 2000; Yamazaki & Sugimoto, 2000) defined certain modifications of this algorithm and showed that such a modified protocol has a performance close to the theoretical limits of efficiency. He also confirmed that four iterations are enough to reconcile the values of bit strings. On the other hand, the communication complexity of the protocol during the execution can be great, which results in a small length of the obtained string in order to minimize the amount of information that Eve has.

- The Winnow protocol is introduced in (Buttler et al., 2003) with the aim of reducing communication complexity by eliminating the use of a binary search algorithm for error detection and correction. The author's idea is to use Hamming's error detection and correction code to correct errors. Both sides, Alice and Bob, split their bit strings into blocks of equal length. Two corresponding blocks are denoted by M_a and M_b and their syndromes, S_a and S_b, are calculated using the generator matrix G and the check matrix H, $G \cdot H^T = 0$. Alice sends Bob S_a who calculates $S_d = S_a \oplus S_b$. If $S_d = 0$ then M_a and M_b are considered equal, otherwise Bob transforms M_b by changing the minimum number of positions and recalculating S_b for such a modified block to get $S_d = 0$. Analyses have shown that from the point of view of execution speed, achieved string length and security characteristics, the protocol has good performance with appropriate p_{AB}, (Elkouss et al., 2009; Buttler et al., 2003).
- The aforementioned protocols do not consider the situation when there are significant limitations in the communication environment in terms of loss of communication packets, limited time for protocol execution and limited communication and computational complexity, for example in satellite connections. Gallagher's Low Density Parity Check Codes (Gallager, 1962) were candidates for such environments as a promising solution. In this context, LDPC codes were first mentioned in (Elliott et al., 2005). The advantage of LDPC codes in these applications is that they provide low communication complexity, inherent and pronounced asymmetry in terms of computing resources of communication parties.

> Decoding LDPC codes requires more computing and memory resources than the Cascade and Winnow protocols but its significance is in communication resources and complexity reduction as it requires only one message to be exchanged. In resource-constrained networks, this feature provides a significant advantage in achieving large gains in execution time and security.

Other ideas in this context have emerged recently. One of them is the application of neural networks in the process of error correction during this phase of the protocol. (Niemiec, 2019).

More details on this topic with an exhaustive list of references can be found in (Bloch, 2016; Mehic et al., 2020; Gronberg, 2005)

Privacy amplification

This is the last phase in the process of the protocol which is carried out by Alice and Bob in order to obtain a cryptographic key that is information-theoretically secure in relation to Eve. At this point, Alice and Bob have a string of bits in common and know the estimate of the upper limit of the amount of information Eve has about that string. Nevertheless, Eve's information shows that Alice and Bob can extract from their strings a certain string of bits S_{AB} about which Eve knows nothing or

$$I\left(S_{AB}, S_E\right) = 0$$

where S_E is Eve's version of S_{AB} constructed based on the information Eve collected. Eve knows that $S_{AB} \neq S_E$ but does not know in which positions the sequences differ. Using the publicly known selected appropriate deterministic function f, Alice and Bob calculate the required cryptographic key as $k = f(S_{AB})$. Knowing the function f and S_E does not provide any knowledge to Eve about k because she does not know how the errors from S_E spread during the calculation of f and affect its result. Consequently, $f\left(S_E\right)$ does not give any information about k to Eve.

Precise formalizations and proofs are based on the notion of Rényi entropy and its derivatives, collision entropy and min-entropy.

Detailed references to protocols and formalizations can be found in (Bloch, 2016).

The common source of randomness choice

The previously described process of cryptographic keys establishment implies that Alice, Bob and Eve get their initial strings of symbols X^n, Y^n, Z^n from a common source of randomness as shown in Figure 4. This generally implies the participation of a trusted third party in the process itself. The level of communication security is increased when it is possible to eliminate the influence of the trusted third party and achieve protection of communication between Alice and Bob by controlling the generation of cryptographic keys and using proven cryptographic algorithms. One of the first examples of this communication protection type was the Quantum key exchange protocol (QKD) BB84, (Bennett & Brassard, 1984). An interesting and in some ways biometrical oriented approach is described in the works (Milosavljević et al., 2018) and (Galis et al., 2021). The authors used digitized recorded electroencephalogram (EEG) brain signals as a source of randomness for Alice and Bob during identical mental activities, looking at the image of the White Angel in (Milosavljević et al., 2018) and during the Wisconsin Card Sorting Test (WCST) in (Galis et al., 2021). Intuitively, Alice's and Bob's brain is stimulated by the same input stimulus but due to individual physiological differences it is registered as correlated but different and independent signals, for example in the case of an image the general image content is the same but color perceptions, physical dimensions and other characteristics may differ. So the digitalized form of Alice's EEG becomes X^n and the digitalized form of Bob's EEG becomes Y^n. In that situation, Eve has no information about X^n, Y^n and her only possibilities may be:

1. To be able to recognize in a set of registered EEG signals on the same stimulus, which does not contain Alice's and Bob's EEG, the one closest to them, measured by the Hamming's metric - Strong Eve
2. That the set of registered EEG signals includes both Alice's and Bob's EEG, but that Eve does not know the identity of the person from whom the EEG signals originate - Medium Eve
3. Eve has no information about Alice's and Bob's EEG signal, but she knows the process for obtaining it and the device for recording and digitizing it - weak Eve.

In (Galis et al., 2021), the authors used 76 of EEG signals from different individuals during WCST. For all registered samples, the previously described procedure of performing cryptographic keys in the information-theoretical model, advantage distillation, information reconciliation, private amplification was performed. A summary of the results is given in Table 1.

Table 1 – Experimental results of cryptographic keys establisment using EEG
Таблица 1 – Экспериментальные результаты создания криптографических ключей при использовании ЭЭГ
Табела 1 – Експериментални резултати успостављања криптографских кључева применом ЕЕГ-а

Type of Eve	Strong	Medium	Weak
Established key length	1301.55 ±502.16	1290.53 $\pm$ 496.85	1301.76 $\pm$ 502.44
Efficiency	4.79%	4.75%	4.79%
Hamming distance(A,E)	$0.4997\pm$ 0.0147	$0.5005\pm$ 0.0149	$0.4999\pm$ 0.0147
Successfully established pairs	100%	100%	100%

The table shows the results in relation to the assumed strength of Eve. The second row labeled Established key length shows the mean length value and the standard deviation of the established cryptographic keys lengths in the $(76 \cdot 75)/2$ implemented protocols. The third row shows the efficiency of the applied protocols expressed as the ratio of the length of the obtained cryptographic keys and the length of the initially used string. At first glance, it seems that the efficiency is small and unsatisfactory, but the length obtained, on average over a thousand bits, is many times higher than the currently accepted standards for cryptographic key lengths of secure symmetric cryptographic algorithms. The fourth row shows the Hamming distance between the keys obtained by Alice and Eve at the end of the process, normalized by the length of the key obtained, and the table shows that this value is practically 0.5, which is a characteristic value for independent and randomly generated arrays. In the end, the table shows that the procedure was successful in all cases in which it was carried out. In addition, it should be noted that the obtained sets of cryptographic keys were tested by the NIST package to check the randomness of the data and all requirements were met.

A full description of the basic idea, methodology, applied protocols and experimental results can be found in (Galis et al., 2021).

Computationally secure protocols for key establishment

With the expansion of information and communication systems, the distribution of cryptographic keys in a centralized way through a trusted third party has become a bottleneck in achieving security in the information and communication world. The first solutions that reduced and relatively eliminated this problem were defined in the second half of the 1970s with the discovery of asymmetric cryptographic algorithms, electronic signature and digital envelope techniques (Diffie & Hellman, 1976; Rivest et al., 1978; Menezes, 1997). However, such solutions assumes the existence of an infrastructure for generation and management of cryptographic keys for asymmetric cryptographic systems and digital certificates based on them (Public Key Infrastructure -PKI). This enables the introduction of digital identity in the digital world. This, in turn, means involving a trusted third party in the process of establishing cryptographic keys. Today's trend in the protection of messages in information and communication traffic is the creation of direct secure channels between the parties in communication and the development of techniques for establishing cryptographic keys directly between them in a secure way.

The first reflections on the protocol for secure decentralized computing of functions are presented in (Yao, 1982). The described approach considers the possibilities for defining a protocol by which n participants denoted by P_i and each has a private data x_i $i = 1, 2, \ldots, n$ for a given function f calculate the value $(y_1, y_2, \ldots, y_n) = f(x_1, x_2, \ldots, x_n)$ in such a way that:

1. After protocol execution, the generated value $(y_1, y_2, \ldots, y_n)$ is the exact value of the function f for the arguments $(x_1, x_2, \ldots, x_n)$ and each participant P_i received them as a result.
2. After protocol execution, each participant P_i knows only $(y_1, y_2, \ldots, y_n)$, x_i and nothing else.
3. Some participants in the protocol may behave maliciously in relation to the protocol in order to obtain information or influence the outcome of the protocol.

A graphical presentation of the Secure multiparty protocol is given in Figure 5.

Secure multiparty computing can be fully formally described thus createing a formal theory within which it is possible to infer conclusions about the security features of the created protocols in a logically based way.

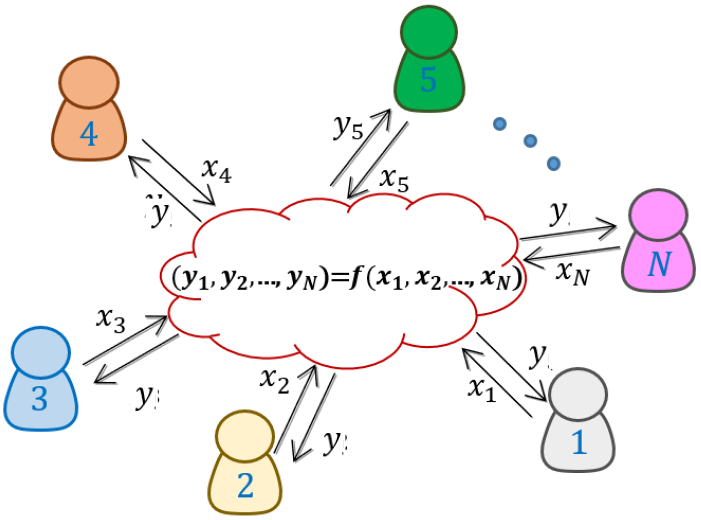


Figure 5 – Graphical presentation of the secure multiparty protocol
Рис. 5 – Графическое представление протокола безопасного многопартийного вычисления
Слика 5 – Графички приказ безбедног кооперативног рачунања

This formalization first defines the characteristics of network channels through which messages are exchanged during the execution of the protocol. Channels by their nature can be public, when the attacker has access to the content of messages but cannot change them, and private, when communication between each two participants is protected. As for the attacker, depending on the communication channel on which the protocol takes place, all messages can be available to him when the channel is public or only those received from malicious participants when the channel is private. According to the received messages, the attacker is passive when only by analysing the received messages he tries to reconstruct information inaccessible to him, or active when he can influence the malicious participants in the protocol available to him. In the case of an active attacker, his behavior does not have to be uniform, but he can adapt to the development of the situation during the execution of the protocol, and then he is called an adaptive active attacker. Some protocol participants under the influence of an attacker may behave in a way that affects the execution of the protocol and the types of such behavior can be described exactly. The protocol is considered safe if conditions listed on page 623 are met.

An interesting question is how to define security in a formal way. The idea is as follows.

By protocol history, we mean a collection of all non-private data used and constructed during protocol execution in an environment. The ideal environment is an abstract construction consisting of simulator S, a functional mechanism for executing protocol instructions that calculates f, and the attacker. All activities in an ideal environment are performed in the correct way, exactly as defined by the functionalities and protocol. The protocol to be executed is denoted by π, the attacker by $\mathcal{A}$, the protocol execution history by h and the security parameter by k. Since in an ideal environment, everything takes place in the right way, security threats and information leakage cannot be in it. Let us introduce the following two functions

$$R_{\pi,\mathcal{A}}(k,h) = \begin{cases} 1 & h \text{ belongs to real world} \\ 0 & \text{otherwise} \end{cases}$$

$$I_{\pi,\mathcal{A}}(k,h) = \begin{cases} 1 & h \text{ belongs to ideal world} \\ 0 & \text{otherwise} \end{cases}$$

Then we say that the protocol π safely calculates the function f in relation to the attacker $\mathcal{A}$ if there is a polynomial simulator S for which each execution with the security parameter k and each protocol history h next inequality is valid

$$\left|P\left(R_{\pi,\mathcal{A}}(k,h)=1\right) - P\left(I_{\pi,\mathcal{A}}(k,h)=1\right)\right| < \frac{1}{p(k)} \tag{8}$$

for a sufficiently large k, where $p(k)$ is an arbitrary positive polynomial. Inequality (8) essentially means that an attacker is unable to distinguish between protocol execution in an ideal and a real environment and, consequently, to gather additional information in addition to those already known. The exact formalization of this concept can be found in (Cramer et al., 2015; Hazay & Lindell, 2010).

The theory shows that in the case of public communication channels and the presence of an active attacker, each function f can be safely calculated in the previously stated sense, provided that the number of corrupt participants t is less than $\frac{n}{3}$. A detailed classification of the possibility of creating a protocol for secure multiparty computing depending on the type of attacker and communication model can be found in (Cramer et al., 2015).

This method is applicable in any situation when it is necessary to calculate a function based on the private information of individual entities so that the result is accurate and does not compromise the privacy of the entities private data participating in the calculation. The problem of generation and distribution cryptographic keys for bilateral or conference secure communication by its nature completely fits into the class of problems this area deals with. The model of decentralized generation and distribution of symmetric cryptographic keys for bilateral secure communication can be described as follows. The participants P_1 and P_2 who want to achieve secure bilateral communication agree on a symmetric cryptographic algorithm through a public communication channel and the function $f(x, y)$ which they will use to derive the desired cryptographic key. Then the participant P_1 chooses a random value x_1 and the participant P_2 a random value x_1, implementing the appropriate protocol for secure multiparty computing, and using it to compute $k = f(x_1, x_2)$ which they will use for the selected symmetric cryptographic algorithm for communication protection. The realization of the system for the automatic establishment of cryptographic keys for symmetric cryptographic algorithms begins with the selection of one of the existing universal protocols for bilateral secure multiparty computing, (Hazay & Lindell, 2010). The implementation of the selected protocol implies the existence of the following subsystems implemented:

- System for automated translation of the selected function f into an equivalent vector Boolean function in the algebraic normal form and then construction of its equivalent Boolean circuit.
- System for automated generation of Yao's garbled computing system based on the obtained Boolean circuit.
- System for the implementation of oblivious transfer protocols.

The realization of such a software package resulted in a system for the direct establishment of cryptographic keys of parties who want to establish secure communication without the mediation of a trusted third party. For the security characteristics of the protocol in the bilateral case, the restrictions related to the number of malicious participants in the protocol are not important for the simple reason of the number of participants, two. If at least one of the participants is malicious, the protocol will not be successfully completed and the key will not be established.

Similarly, this concept can be used to establish the protection of group communication, such as conference calls or complete video meetings.

Comparative analysis of proposed solutions

By applying the previously described methods, we are able to solve the problem of secure generation and distribution of cryptographic keys. The levels of security that the methods offer are different, but they provide a significant advantage over classical cryptology, the elimination of a trusted third party. The benefits of eliminating a trusted third party are manifold. In the first place, the absence of a trusted third party reduces the complexity of the system and thus reduces the number of potential possibilities for its compromise, and further simplifies its administration and maintenance. An additional quality from the security point of view lies in the fact that both systems can be described in a completely formal mathematical way and accordingly analyze the defined protocols and make formal claims about the achieved level of security.

In the Information theory model, it is possible to formally define protocols that can achieve levels of absolute security for generating cryptographic keys and that can be used even in Shannon's OTP system. In this model of performing cryptographic keys, an additional quality is the fact that the source of common randomness can be different environments, which increases the application area of such systems.

In the model of secure multiparty computing on public communication channels, protocols for establishing symmetric cryptographic keys that reach the level of computer security can be formally defined. This lower level of security is a consequence of the characteristics of communication channels and the level of security of cryptographic mechanisms applied in the implementation of the subsystem oblivious transfer.

Although the described systems offer important, technological and security improvements in the field of generation and distribution of cryptographic keys, their application in this context is still small. The main reason lies in the complexity of their implementation and demonstrated performance. Conceptually, these solutions have been proven, but great research efforts are being made to find opportunities to improve their performance and more efficient implementation in terms of computing resources (processing power, amount of memory).

Conclusion

One of the central problems of cryptology, from its inception to the present day, is the generation and distribution of cryptographic keys for symmetric cryptographic systems. The centralized system of generating and distributing cryptographic keys, characteristic of classical cryptology, has manifested its limitations with the expansion of information and communication systems and their network connection. The increased need for the application of cryptographic mechanisms in the protection of information systems has induced an increase in requirements. This paper presents two models by which the described problem can be solved in accordance with the security requirements of modern cryptology. Solutions based on the above proposals give users complete autonomy and end-to-end security protection. The applicability of solutions of this type allows

- Direct establishment of cryptographic keys between communication sites, people or machines, without the mediation of a trusted third party,
- Application of secure symmetric cryptographic algorithms in mass communication systems, IoT and WSN (Unkašević et al., 2019),
- Simplification of the complexity of security systems thus facilitating their administration, and
- By simplifying the complexity and administration of security systems, facilitation of their analysis, potential weaknesses detection and, overall, an in- crease of their security.

The described methods for the realization of direct establishment of cryptographic keys for symmetric cryptographic systems are in line with new trends in data protection in order to reduce the possibility of influence of entities that do not participate in communication directly. The applicability of these techniques in IoT and WSN significantly increases the possibilities of raising the level of security in cyberspace. This claim is supported primarily by the fact that the described methods support cryptographic algorithms with the highest degree of security.

References

Ahlswede, R. & Csiszar, I. 1993. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE Transactions on Information Theory*, 39(4), pp. 1121–1132. Available at: https://doi.org/10.1109/18.243431.

Atlam, H.F., Walters, R.J. & Wills, G.B. 2018. Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues. *International Journal of Intelligent Computing Research*, 9(3), pp. 928–938. Available at: https://doi.org/10.20533/ijicr.2042.4655.2018.0112.

Banday, M.T. (ed.) 2019. *Cryptographic Security Solutions for the Internet of Things*. IGI Global. Available at: https://doi.org/10.4018/978-1-5225-5742-5.

Bennett, C. & Brassard, G. 1984. Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*. Bangalore, India. December 9-12.

Bennett, C.H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. 1992. Experimental quantum cryptography. *Journal of Cryptology*, 5, pp. 3–28. Available at: https://doi.org/10.1007/bf00191318.

Bennett, C.H., Brassard, G. & Robert, J.M. 1988. Privacy Amplification by Public Discussion. *SIAM Journal on Computing*, 17(2), pp. 210–229. Available at: https://doi.org/10.1137/0217014.

Bloch, M. 2016. *Physical-Layer Security*. Cambridge University Press. ISBN 0521516501.

Bloch, M. & Barros, J. 2011. *Physical-Layer Security*. Cambridge University Press. Available at: https://doi.org/10.1017/cbo9780511977985.

Brassard, G. & Salvail, L. 1992. Secret-Key Reconciliation by Public Discussion. In: *Helleseth, T. (Eds.) Advances in Cryptology - EUROCRYPT '93*, vol. 765, pp.410–423. Springer Berlin Heidelberg. Available at: https://doi.org/10.1007/3-540-48285-7_35.

Buttler, W.T., Lamoreaux, S.K., Torgerson, J.R., Nickel, G.H., Donahue, C.H. & Peterson, C.G. 2003. Fast, efficient error reconciliation for quantum cryptography. *Physical Review A*, 67(5), p. 052303. Available at: https://doi.org/10.1103/physreva.67.052303.

Cachin, C. & Maurer, U. 1997. Unconditional security against memory-bounded adversaries. In: *Kaliski, B.S. (Eds.) Advances in Cryptology - CRYPTO '97*, vol. 1294, pp.292-306. Springer Berlin Heidelberg. Available at: https://doi.org/10.1007/bfb0052243.

Carleial, A. & Hellman, M. 1977. A note on Wyner's wiretap channel (Corresp.). *IEEE Transactions on Information Theory*, 23(3), pp. 387–390. Available at: https://doi.org/10.1109/tit.1977.1055721.

Cramer, R., Damgard, I.B. & Nielsen, J.B. 2015. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press. Available at: https://doi.org/10.1017/cbo9781107337756.

Csiszar, I. & Korner, J. 1978. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3), pp. 339–348. Available at: https://doi.org/10.1109/tit.1978.1055892.

Diffie, W. & Hellman, M. 1976. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), pp. 644–654. Available at: https://doi.org/10.1109/tit.1976.1055638.

Elkouss, D., Leverrier, A., Alleaume, R. & Boutros, J.J. 2009. Efficient reconciliation protocol for discrete-variable quantum key distribution. In: *IEEE International Symposium on Information Theory*. Seoul, South Korea, pp.1879-1883, June 28-July 3. Available at: https://doi.org/10.1109/isit.2009.5205475.

Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J. & Yeh, H. 2005. Current status of the DARPA quantum network (Invited Paper). In: *Donkor, E.J., Pirich, A.R. and Brandt, H.E. (Eds.) Proceedings Volume 5815, Quantum Information and Computation III, Defense and Security*. Orlando, Fl, March 28 - April 1. Available at: https://doi.org/10.1117/12.606489.

Galis, M., Milosavljević, M., Jevremović, A., Banjac, Z., Makarov, A. & Radomirović, J. 2021. Secret-Key Agreement by Asynchronous EEG over Authenticated Public Channels. *Entropy*, 23(10), p. 1327. Available at: https://doi.org/10.3390/e23101327.

Gallager, R. 1962. Low-density parity-check codes. *IEEE Transactions on Information Theory*, 8(1), pp. 21–28. Available at: https://doi.org/10.1109/tit.1962.1057683.

Gronberg, P. 2005. *Key reconciliation in quantum key distribution*. *Tech. rep.*, FOI-Swedish Defence Research Agency.

Hazay, C. & Lindell, Y. 2010. *Efficient Secure Two-Party Protocols*. Springer Berlin Heidelberg. Available at: https://doi.org/10.1007/978-3-642-14303-8.

Mahmood, Z. (ed.) 2019. *Security, Privacy and Trust in the IoT Environment*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-18075-1.

Maurer, U.M. 1993. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3), pp. 733–742. Available at: https://doi.org/10.1109/18.256484.

Mehic, M., Niemiec, M., Siljak, H. & Voznak, M. 2020. Error Reconciliation in Quantum Key Distribution Protocols. In: *Ulidowski, I., Lanese, I., Schultz, U., Ferreira, C. (Eds.) Reversible Computation: Extending Horizons of Computing. RC 2020. Lecture Notes in Computer Science*. 12070, pp. 222–236. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-47361-7_11.

Menezes, A.J. 1997. *Handbook of applied cryptography*. Boca Raton: CRC Press. ISBN 9780849385230.

Milosavljević, M., Adamović, S., Jevremovic, A. & Antonijevic, M. 2018. Secret key agreement by public discussion from EEG signals of participants. In: *5th International Conference IcEtran 2018*. Palić, Serbia, June 11-14.

Mohamed, K.S. 2019. *The Era of Internet of Things*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-18133-8.

Niemiec, M. 2019. Error correction in quantum cryptography based on artificial neural networks. *Quantum Information Processing*, 18(6, art.number:174). Available at: https://doi.org/10.1007/s11128-019-2296-4.

Rivest, R.L., Shamir, A. & Adleman, L. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), pp. 120–126. Available at: https://doi.org/10.1145/359340.359342.

Shannon, C.E. 1948a. A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27(3), pp. 379–423. Available at: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

Shannon, C.E. 1948b. A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27(4), pp. 623–656. Available at: https://doi.org/10.1002/j.1538-7305.1948.tb00917.x.

Shannon, C.E. & Weaver, W. 1963. *The Mathematical Theory of Communication*. University of Illinois Press. ISBN 0252725484.

Sugimoto, T. & Yamazaki, K. 2000. A study on secret key reconciliation protocol “Cascade”. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E83-A(10), pp. 1987–1991.

Tan, E.Y.Z., Lim, C.C.W. & Renner, R. 2020. Advantage Distillation for Device-Independent Quantum Key Distribution. *Physical Review Letters*, 124(2, art.number:020502). Available at: https://doi.org/10.1103/PhysRevLett.124.020502.

Unkašević, T., Banjac, Z. & Milosavljević, M. 2019. A Generic Model of the Pseudo-Random Generator Based on Permutations Suitable for Security Solutions in Computationally-Constrained Environments. *Sensors*, 19(23, art.number:5322). Available at: https://doi.org/10.3390/s19235322.

Wang, Q., Wang, X., Lv, Q., Ye, X., Luo, Y. & You, L. 2015. Analysis of the information theoretically secret key agreement by public discussion. *Security and Communication Networks*, 8(15), pp. 2507–2523. Available at: https://doi.org/10.1002/sec.1192.

Wyner, A.D. 1975. The Wire-Tap Channel. *The Bell System Technical Journal*, 54(8), pp. 1355–1387. Available at: https://doi.org/10.1002/j.1538-7305.1975.tb02040.x.

Yamazaki, K. & Sugimoto, T. 2000. On secret reconciliation protocol - modification of “Cascade”protocol. In: *International Symposium on Information Theory and Its applications*. Honolulu, Hawaii, pp.223–226, Nov. 5-8.

Yao, A.C. 1982. Protocols for secure computations. In: *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*. Chicago, IL, USA, pp.160-164, November 3-5. Available at: https://doi.org/10.1109/sfcs.1982.38.

Ziegler, S. (ed.) 2019. *Internet of Things Security and Data Protection*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-04984-3.

ПРОТОКОЛЫ УСТАНОВЛЕНИЯ СИММЕТРИЧНЫХ СЕКРЕТНЫХ КЛЮЧЕЙ – СОВРЕМЕННЫЙ ПОДХОД

Меиран Галис[а,в], *Томислав* Б. Ункашевич[а], **корреспондент**, *Зоран* Дж. Баняц[а], *Милан* М. Милосавлевич[б]

[а] Институт ВЛАТАКОМ, г. Белград, Республика Сербия

[б] Университет Сингидунум, г. Белград, Республика Сербия

[в] Scytale, Тель-Авив, Государство Израиль

РУБРИКА ГРНТИ:	27.47.17	Математическая теория информации
	28.21.19	Теория кодирования
	50.37.23	Защита от несанкционированного доступа. Физическая защита информации
	49.33.35	Надежность сетей связи и защита информации

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Проблема эффективного распределения криптографических ключей в системах связи появилась уже в первые дни их существования, но особенно она обострилась с появлением систем массовой связи. Определение и внедрение эффективных протоколов распределения криптографических ключей в таких условиях играет значительную роль в повышении информационной безопасности в киберпространстве.

Методы: С помощью методов теории информации и безопасных многосторонних вычислений были определены протоколы для прямого установления криптографических ключей между сторонами связи.

Результаты: В статье представлены два новых подхода к решению проблемы установления криптографических ключей. Новшество в протоколе, определенном в модели безопасности, согласно теории информации, основана на источнике общей случайности, которым в данном случае является сигнал ЭЭГ каждого отдельного субъекта, участвующего в системе связи. Экспериментальные результаты показывают, что объем информации, поступающей к противнику, близок к нулю. Новшество во втором случае, обеспечивающее безопасность ключам на уровне *компьютерной безопасности за счет применения безопасных многосторонних вычислений при наличии нескольких участников-злоумышленников, содержится в новом приложении одной вычислительной модели. Для обоих подходов характерно то, что в рамках формальных теорий можно формальным образом сделать выводы об их характеристиках безопасности.*

Выводы: В статье описываются два новых подхода к управлению криптографическими ключами в симметричных криптографических системах, подкрепленных экспериментальными результатами. Значимость предлагаемых решений заключается в том, что они позволяют установить надежную связь между заинтересованными сторонами, избегая влияния третьей доверенной стороны. Достигнутый таким образом уровень безопасности связи значительно повышается по сравнению с классическими криптографическими системами.

Ключевые слова: симметричный криптографический ключ, управление криптографическими ключами, источник случайности, преимущества дистилляции данных, согласование информации, усиление конфиденциальности, безопасные многосторонние вычисления.

ПРОТОКОЛИ ЗА УСТАНОВЉАВАЊЕ ТАЈНИХ СИМЕТРИЧНИХ КЉУЧЕВА - САВРЕМЕН ПРИСТУП

Меиран Галис[а,в], *Томислав* Б. Ункашевић[а], **аутор за преписку**, *Зоран* Ђ. Бањац[а], *Милан* М. Милосављевић[б]

[а] Институт ВЛАТАКОМ, Београд, Република Србија

[б] Универзитет Сингидунум, Београд, Република Србија

[в] Scytale, Тел Авив, Држава Израел

ОБЛАСТ: математика, рачунарство, телекомуникације
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Проблем ефикасне дистрибуције криптографских кључева у комуникационим системима постоји одавно, а са појавом масовних комуникационих система постао је изражен. Дефинисање и имплементација ефикасних протокола за установљавање симетричних криптографских *кључева у таквим околностима има велики значај у подизању информационе безбедности у сајбер простору.*

Методе: Применом метода теорије информација и безбедног кооперативног рачунања дефинисани су протоколи за директно установљавање криптографских кључева између комуникационих страна.

Резултати: У раду су дефинисана два нова приступа проблему установљавања криптографских кључева. Новина у протоколу дефинисаном у безбедносном моделу заснованом на теорији информација заснива се на извору заједничке случајности који је у овом случају ЕЕГ сигнал сваког субјекта учесника у комуникационом систему. Експериментални резултати показују да је количина информација која отиче ка противнику блиска нули. Новина у другом случају који кључевима обезбеђује сигурност на нивоу рачунарске сигурности применом безбедног кооперативног рачунања у присуству више злонамерних учесника садржана је у новој примени једног рачунарског модела. За оба приступа је карактеристично да је у оквиру формалних теорија могуће на формалан начин изводити закључке о њиховим безбед носним својствима.

Закључак: Представљена су два нова приступа за установљавање криптографских кључева у симетричним криптографским системима са експерименталним резултатима. Значај предложених решења лежи у чињеници да омогућавају установљавање поуздане комуникације између заинтересованих страна са краја на крај, избегавајући утицај треће стране од поверења. На тај начин се значајно повећава постигнути ниво сигурности њихове комуникације у односу на класичне криптографске системе.

Кључне речи: симетрични криптографски кључ, успостављање кључа, извор случајности, дестилација предности, усклађивање информација, појачавање приватности, безбедно кооперативно рачунање.

Paper received on / Дата получения работы / Датум пријема чланка: 23.02.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.06.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24.06.2022.

APPLICATION OF FINITE SAMPLING POINTS IN PROBABILITY BASED MULTI – OBJECTIVE OPTIMIZATION BY MEANS OF THE UNIFORM EXPERIMENTAL DESIGN

Maosheng Zheng[a], *Haipeng* Teng[b], *Yi* Wang[c], *Jie* Yu[d]

[a] Northwest University, School of Chemical Engineering,
Xi'an, People's Republic of China,
e-mail: mszhengok@aliyun.com, **corresponding author**,
ORCID iD: https://orcid.org/0000-0003-3361-4060

[b] Northwest University, School of Chemical Engineering,
Xi'an, People's Republic of China,
e-mail: tenghp@nwu.edu.cn,
ORCID iD: https://orcid.org/0000-0003-2987-7415

[c] Northwest University, School of Chemical Engineering,
Xi'an, People's Republic of China,
e-mail: wangyi11@nwu.edu.cn,
ORCID iD: https://orcid.org/0000-0001-6711-0026

[d] Northwest University, School of Life Science,
Xi'an, People's Republic of China,
e-mail: yujie@nwu.edu.cn,
ORCID iD: https://orcid.org/0000-0001-6606-5462

DOI: 10.5937/vojtehg70-37087; https://doi.org/10.5937/vojtehg70-37087

FIELD: Mathematics, Materials
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: An approximation for assessing a definite integral is continuously an attractive topic owing to its practical needs in scientific and engineering areas. An efficient approach for preliminarily calculating a definite integral with a small number of sampling points was newly developed to get an approximate value for a numerical integral with a complicated integrand. In the present paper, an efficient approach with a small number of sampling points is combined to the novel probability–based multi–objective optimization (PMOO) by means of uniform experimental design so as to simplify the complicated definite integral in the PMOO preliminarily.

Methods: The distribution of sampling points within its single peak domain is deterministic and uniform, which follows the rules of the uniform design method and good lattice points; the total preferable probability is the unique and deterministic index in the PMOO.

Results: The applications of the efficient approach with finite sampling points in solving typical problems of PMOO indicate its rationality and convenience in the operation.

Conclusion: The efficient approach with finite sampling points for assessing a definite integral is successfully combined with PMOO by means of the uniform design method and good lattice points.

Key words: preferable probability, multi–objective optimization, finite sampling points, simplifying evaluation, uniform design method.

Introduction

Recently, an efficient approach for assessing a definite integral with a small number of sampling points has been proposed based on the uniform experimental design method and the good lattice point from the viewpoint of practical application (Yu et al, 2022) preliminarily. It indicated that the efficient evaluation of a definite integral for a periodical function in its single peak domain can be obtained by using 11 sampling points in one dimension, 17 sampling points in two dimensions, and 19 sampling points in three dimensions with a small relative error preliminarily. The fundamental of the finite sampling points (FSPs) for assessing a definite integral was the rules of uniform and deterministic distribution of the FSPs according to the good lattice point (Hua & Wang, 1981; Fang, 1980; Fang, et al, 1994, 2018; Ripley, 1981; Wang & Fang, 2010), or the so-called "quasi – Monte Carlo method" (QMC).

The so–called "curse of dimensionality" problem was broken in the publication of the calculating results of Paskov & Traub (1995) by using Halton sequences and Sobol sequences for accounting a ten – tranche CMO (Collateralized Mortgage Obligation) in high dimensions, reaching even 360 dimensions. Their findings were that QMC methods performed very well as compared to simple MC methods, as well as to antithetic MC methods (Tezuka, 1998, 2002; Paskov & Traub, 1995; Paskov, 1996; Sloan & Wozniakowski, 1998). Afterwards, a lot of similar phenomena were found in different evaluations for pricing problems by using different types of low–discrepancy sequences (Tezuka, 1998). All these consequences provide a powerful support to using the QMC with finite sampling points to conduct a definite integral numerically.

In the present paper, the newly developed efficient approach for assessing a definite integral with a small number of sampling points is combined to the novel probability – based multi – objective optimization (PMOO) so as to simplify the complicated definite integral in PMOO. The novel PMOO aims to overcome the shortcomings of personal and subjective factors in the previous multi – object optimizations, so a novel concept of preferable probability and the corresponding assessment are developed (Zheng, 2022; Zheng et al, 2021, 2022). The preferable probability is used to reflect the preferablity degree of the candidate in the optimization, all performance utility indicators of candidates are divided into beneficial or unbeneficial types according to their features in the selection, and each performance utility indicator contributes to one partial preferable probability quantitatively. The total preferable probability is the product of all partial preferable probabilities in the viewpoint of probability theory, which is the overall consideration of various response variables simultaneously so as to reach a compromised optimization. The total preferable probability is the unique deterministic index in the optimal process comparatively. Appropriate achievements have been obtained.

Essence of the uniform experimental design method

The uniform experimental design method (UED) was proposed by Fang & Wang (1994, 2018) and the essence of the UED contains:

A) **Uniformity**. The sampling points for an experiment are evenly distributed in the input variable (parameter) space, so the term "space filling design" is widely used in the literature. The UED arranges the test design (test point, sampling points in space) through a uniform design table, which is deterministic without any randomness.

B) **Overall Mean Model**. The UED is to hope that the test point can give the minimum deviation of the total mean value of the output (response) variable from the actual total mean value.

C) **Robust**. The UED design can be applied to a variety of situations and is robust to model changes.

D) **Following basic procedures are involved in the UED**:

1) Total Mean Model

It assumes that there exists a deterministic relationship between the input independent variables x_1, x_2, x_3, ..., x_s and the response y by

$$y = f(x_1, x_2, x_3,...x_r),\ X = \{x_1, x_2, x_3, \ldots, x_r\} \in C^r. \qquad (1)$$

Furthermore, it supposes that the experiment domain is the unit cube $C^r = [0, 1]^r$, the total mean value the response y on C^r is,

$$E(y) = \int_{C^r} f(x_1, x_2, x_3,...x_r)\cdot dx_1 \cdot dx_1 \cdot dx_3 \cdots dx_r\ , \qquad (2)$$

If m sampling points p_1, p_2, p_3, …, p_m are taken on C^r, then the mean value of y on these m sampling points is

$$\overline{y(D_m)} = \frac{1}{m}\sum_{j=1}^{m} f(p_j)\,. \tag{3}$$

In Eq.(3), $D_m = \{p_1, p_2, p_3, \ldots, p_m\}$ represents a design of these m sampling points.

Fang & Wang (1994, 2018) proved that if the sampling points p_1, p_2, p_3, …, p_m are uniformly distributed on the domain C^r, the deviation $\overline{E(y)} - \overline{y(D_m)}$ of the sampling point set on C^r and D_m is the smallest approximately.

2) Uniform Design Table

Fang & Wang (1994, 2018) and Wang & Fang (2010) developed a Uniform Design Table for the proper utilization of the UED which can be employed by anyone to arrange their sampling points. However, the preliminarily necessary number of sampling points was not clarified by Fang in their UED. Here in this paper, the number of sampling points suggested in the article of Yu et al (2022) is adopted for our utilization.

3) Regression

Regression is the next procedure to complete the optimum.

For our purpose, the total preferable probability and the approximate expression for the response $y' = f'(x_1, x_2, x_3, ..., x_r)$ can be obtained through data fitting, which is close to the true model (Fang & Wang, 1994, 2018).

The application of uniform design is becoming more and more extensive these years, including a successful application of the uniform experimental design in the Chinese Missile Design and Ford Motor Company of the USA, and the number of successful cases is increasing.

Combination of finite sampling points with the probability–based multi–objective optimization by means of the uniform experimental design

The above statements indicate the remarkable features of the UED, i.e., the uniform distribution of experiment / sampling points within the test domain and the small number of tests, fully representative of each point, and an easy to perform regression analysis. So here the Finite Sampling Points method is combined with the novel probability–based multi–objective optimization by means of the uniform experimental design and the good lattice point (GLP) to simplify the complicated data processing preliminarily in the following section.

In order to demonstrate the combination of finite sampling points with the probability–based multi–objective optimization, some typical examples are given in the following sections in detail.

1) Multi–objective optimization of tower crane boom tie rods

Qu et al (2004) conducted the multi – objective optimization of tower crane boom tie rods by the fuzzy optimization model.

Through a careful analysis, they set the minimum mass *W*(*X*) of the boom tie rod and the minimum angular displacement *θ*(*X*) of the boom as the multiple objectives, and obtained the following model,

$$W(X) = 208.323x_1 + 433.868x_2, \tag{4}$$

$$\theta(X) = \frac{2.0288 \times 10^{-4}}{9.8621x_1 + 5.3471x_2}. \tag{5}$$

The constraint conditions are,

$$0.003379 < x_1 < 0.005805, \tag{6}$$

$$0.003379 < x_2 < 0.005468. \tag{7}$$

According to the optimal requirements of *W*(*X*) and *θ*(*X*), both *W*(*X*) and *θ*(*X*) are unbeneficial indexes (Qu et al, 2004) which have “the smaller the better” features in the optimization.

Thus, according to the probability–based multi–objective optimization (Zheng, 2022; Zheng et al, 2021, 2022), the partial preferable probabilities of *W*(*X*) and *θ*(*X*) are expressed as

$$P_W = \beta_W \cdot [W_{max} + W_{min} - W(X)], \tag{8}$$

$$P_\theta = \beta_\theta \cdot [\theta_{max} + \theta_{min} - \theta(X)], \tag{9}$$

In Eqs. (8) and (9), β_W, $W_{\min}$, and $W_{\max}$ express the normalization factor, the minimum and maximum values of the index *W*(*X*), respectively; β_θ, $\theta_{\min}$, and $\theta_{\max}$ indicate the normalization factor, the minimum and maximum values of the index *θ*(*X*), individually.

Simultaneously,

$$\beta_W = \frac{1}{\int_{x_{1l},x_{2u}}^{x_{1u},x_{2u}} [W_{\max} + W_{\min} - W(X)] dx_1 \cdot dx_2} \tag{10}$$

$$\beta_\theta = \frac{1}{\int_{x_{1l},x_{2u}}^{x_{1u},x_{2u}} [\theta_{\max} + \theta_{\min} - \theta(X)] \cdot dx_1 \cdot dx_2} \tag{11}$$

In Eqs. (8) and (9), x_{1L}, x_{1U}, x_{2L} and x_{2U} express the lower limit and the upper limit of x_1 and x_2 in their domain, respectively.

According to the common procedure, the subsequent thing is to substitute Eqs. (4) and (5) into Eqs. (8) through (11) with the constraints of Eqs. (6) and (7) to conduct the evaluations. It can be seen that the assessments are tediously long and complicated due to the sophisticated integration. However, if we use the finite sampling points algorithm proposed by Yu et al (2022), the approximate assessments of the definite integral in Eqs. (10) and (11) can be simplified with the finite numbers of discrete sampling points.

According to Yu et al (2022), 17 discrete sampling points are suggested for the two independent variables x_1 and x_2 preliminarily. So the Uniform Design Table of $U^*_{17}(17^5)$ is taken to conduct the approximate assessment. The designed results for the 17 discrete sampling points are shown in Table 1 together with the calculated consequences of $W(X)$ and $\theta(X)$, in which x_{10} and x_{20} indicate the original positions from the Uniform Design Table $U^*_{17}(17^5)$ for the [1, 17] × [1, 17] domain.

Table 2 shows the evaluation results of this problem.

Table 1 – Designed results $U^*_{17}(17^5)$ together with the calculated consequences of W(X) and θ(X)
Таблица 1 – Полученные результаты $U^*_{17}(17^5)$ вместе с рассчитанными последствиями W(X) и θ(X)
Табела 1 – Пројектовани резултати $U^*_{17}(17^5)$ заједно са израчунатим последицама W(X) и θ(X)

No.	x_{10}	x_{20}	x_1 / m^2	x_2 / m^2	W / T	θ/°
1	1	7	0.003450	0.004178	2.5314	0.0036
2	2	14	0.003593	0.005038	2.9343	0.0033
3	3	3	0.003736	0.003686	2.3776	0.0036
4	4	10	0.003879	0.004546	2.7805	0.0032
5	5	17	0.004021	0.005407	3.1834	0.0030
6	6	6	0.004164	0.004055	2.6267	0.0032
7	7	13	0.004307	0.004915	3.0296	0.0030
8	8	2	0.004449	0.003563	2.4729	0.0032
9	9	9	0.004592	0.004424	2.8758	0.0029
10	10	16	0.004735	0.005284	3.2788	0.0027
11	11	5	0.004877	0.003932	2.7220	0.0029

No.	x_{10}	x_{20}	x_1 / m^2	x_2 / m^2	W / T	θ/°
12	12	12	0.005020	0.004792	3.1250	0.0027
13	13	1	0.005163	0.003440	2.5682	0.0029
14	14	8	0.005306	0.004301	2.9712	0.0027
15	15	15	0.005448	0.005161	3.3741	0.0025
16	16	4	0.005591	0.003809	2.8174	0.0027
17	17	11	0.005734	0.004669	3.2203	0.0025

Table 2 – Evaluation results of this problem
Таблица 2 – Результаты оценки данной проблемы
Табела 2 – Резултати процене овог проблема

	Partial preferable probability		Total	
No.	$P_{W(x)}$	$P_{\theta(x)}$	P_t×10^3	Rank
1	0.0659	0.0471	3.1006	16
2	0.0576	0.0536	3.0905	17
3	0.0690	0.0473	3.2642	13
4	0.0608	0.0538	3.2703	12
5	0.0525	0.0592	3.1091	15
6	0.0639	0.0540	3.4512	8
7	0.0557	0.0593	3.3037	11
8	0.0671	0.0542	3.6333	5
9	0.0588	0.0595	3.4993	7
10	0.0506	0.0639	3.2346	14
11	0.0620	0.0596	3.6957	3
12	0.0537	0.0641	3.4426	9
13	0.0651	0.0598	3.8930	1
14	0.0569	0.0642	3.6514	4
15	0.0486	0.0680	3.3052	10
16	0.0600	0.0643	3.8609	2
17	0.0518	0.0681	3.5246	6

Table 2 shows that the preliminarily assessed result of the total preferable probability of sampling point *No. 13* exhibits the maximum in the first glance, so the optimal configuration could be around sampling point *No. 13*.

As to sampling point *No. 13*, the optimal mass $W_{\text{optim.}}$ of the boom tie rod and the optimal angular displacement $\theta_{\text{optim.}}$ of the boom are *2.5682* *tons* and *0.0029°* at x_1 = *0.0052* m^2 and x_2 = *0.0034* m^2, which are better than those of Qu's (2004) results of *2.8580 tons*, and *0.0026°* at x_1 = *0.0058* m^2 and x_2 = *0.0038* m^2, comprehensively.

Moreover, regression can be applied for further optimization. The regressed result of the total probability P_t with respect to x_1 and x_2 is

$$P_t \times 10^3 = 8.2971 - 249.4110x_1 - 304.5570x_2 - 0.0978\times 10^{-1}x_1^{-1} - 0.0083\times 10^{-1}x_2^{-1}, \qquad (12)$$

$$R^2 = 0.9362. \qquad (13)$$

The regressed result of the W with respect to x_1 and x_2 is

$$W = 2.89\times 10^{-15} + 208.3230x_1 + 433.8680x_2, \qquad (14)$$

$$R^2 = 1. \qquad (15)$$

The regressed result of the total probability θ with respect to x_1 and x_2 is

$$\theta = 0.0035 - 0.1459x_1 - 0.2412x_2 - 5.7700\times 10^{-6}x_1^{-1} - 1.4000\times 10^{-7}x_2^{-1}, \qquad (16)$$

$$R^2 = 0.9941. \qquad (17)$$

The optimal result of the regressed formula of Eq. (12) being maximum is $P_t^* \times 10^3 = 3.8890$ at $x_1 = 0.0058$ m^2 and $x_2 = 0.0034$ m^2; the corresponding values for optimal W and θ are, $W^* = 2.6754$ *tons*, $\theta^* = 0.0028°$, which are much better than those of Qu's results as well.

2) Multi–objective optimization with a single input variable

It is certain that multi–objective optimization with a single input variable is a very simple problem and direct assessment can be conducted.

The simple example is that the optimal solution of the *min* $f_1(x) = x^2$ together with *min* $f_2(x) = (x - 2)^2$ simultaneously within the range of $x \in [-5, 7]$, which was discussed by Huang & Chen (2009) with tediously long and complex evolutionary computations of Pareto optimization.

Here, by using the probability–based multi–objective optimization, the problem can be reanalyzed and the partial preferable probability for $f_1(x)$ and $f_2(x)$ can be expressed as,

$$P_{f1} = (49 - x^2)/432, \quad P_{f2} = [49 - (x - 2)^2]/432. \qquad (14)$$

Thus, the total preferable probability $P_t = P_{f1} \cdot P_{f2}$ takes its maximum value at x = 1 distinctly; therefore, the simultaneous minimum values of $f_1(x)$ and $f_2(x)$ are compromisingly equaled to *1*. Obviously, the assessing process is much simpler than that of complex evolutionary computations of Pareto optimization (Huang & Chen, 2009).

Furthermore, if the sampling point method is used, 11 sampling points can be employed for the assessment preliminarily (Yu, et al, 2022). The uniformly distributed sampling points are shown in Table 3 in their domain *x* ∈ [*-5, 7*] together with the value of P_t and their ranking.

Table 3 – The positions of the distribution of the sampling points in the integral domain [-5, 7] together with the value of Pt and their ranking
Таблица 3 – Положения распределения точек выборки в интегральной области [-5, 7] вместе со значением Pt и их ранжированием
Табела 3 – Позиције дистрибуције тачака узорковања у домену интеграла [-5, 7] *заједно са вредношћу* Pt *и њихово рангирање*

No	Location of point	$P_t \times 10^2$	Rank
1	-4.45455	0.114658	6
2	-3.36364	0.408543	5
3	-2.27273	0.722118	4
4	-1.18182	0.991634	3
5	-0.09091	1.171558	2
6	1.00000	1.234568	1
7	2.09091	1.171558	2
8	3.18182	0.991634	3
9	4.27273	0.722118	4
10	5.36364	0.408543	5
11	6.45455	0.114658	6

Again, the maximum value for P_t is located at $x = 1$ exactly.

Discussion

1) On the number of the discrete sampling points in the evaluation

In the literature of Yu et al (2022), it is suggested roughly but not proven mathematically that 17 and 19 sampling points are proper preliminarily for evaluating a complicated integral.

Here, we would stress the following. In accordance wih Hua and Wang (1081) and Fang and Wang (1994), as to the GLP, the discrepancy of the low–discrepancy point set is $O(p^{-1}(\log p)^{s-1})$ for the s – dimension with the prime number p, so if we take 11 GLPs for a 1 – dimensional problem, the value of O(1/11) ≈ 0.0909, i.e., less than 10%; analogically, for a 2 – dimensional problem, if we adopt to use 17 GLPs, the value of O(p^{-1}(logp)$^{s-1}$) is approximately O(17^{-1}(log17)^{1}) ≈ 0.0724, which is near to the situation of 1 – dimensional problem; while for a 3 – dimensional problem, if we take 19 GLPs, the approximate result of O(p^{-1}(logp)^{s}) is O(19^{-1}(log19)^{2}) ≈ 0.0861, which is close to the situation of a 1 – dimensional problem as well. However, if we accept 23, 29, 31 or even 41 GLPs for 3-d, the consequences for O(p^{-1}(logp)$^{s-1}$) are 0.0806, 0.0737, 0.0717, or 0.0634, respectively, which are nearly the same as that of 19 GLPs basically.

The successful results of assessing complicated definite integrations realize the applicability of the approximation from the point of view of engineering practice. Perhaps the abstruse physical detail is related to the spatial correlation of spatial sampling points, which was pointed by Ripley (1981) and worth to be further explored by mathematicians.

2) On the combination of the finite sampling points in probability-based multi–objective optimization by means of the Uniform Experimental Design

The newly developed efficient approach for preliminarily assessing a definite integral with a small number of sampling points can be combined with the novel probability–based multi–objective optimization (PMOO), provided the discrete specimen points are uniformly and deterministically distributed within the domain according to the rules of the GLP and the UED. The optimal results in the present paper for typical examples indicate the advantages of this treatment. However, further applications and mathematical intensions of the appropriate algorithm for assessing numerical integration developed newly are needed to be deeply explored in future.

Besides, in order to improve the precision of approximate maximum by using discrete sampling point method, sequential algorithm for optimization can be combined with the probability – based multi – objective optimization in its discreterization (Zheng et al, 2022).

Conclusion

From the above discussion, the efficient approach for preliminarily calculating a definite integral with a small number of sampling points is successfully combined with the novel probability–based multi–objective optimization (PMOO) so as to simplify the complicated calculation of a definite integral in PMOO. The Uniform Experimental Design method and the good lattice point are involved in the combination, thus significantly simplifying complicated data processing by approximation.

References

Fang, K. 1980. Uniform design — Application of Number Theory Method in Experimental Design. *Acta Mathematicae Applicatea Sinica,* 3(4), pp.363-272..

Fang, K-T., Liu, M-Q., Qin, H. & Zhou, Y-D. 2018. *Theory and Application of Uniform Experimental Designs*. Beijing: Science Press & Singapore: Springer Nature. Available at: https://doi.org/10.1007/978-981-13-2041-5.

Fang, K-T. & Wang, Y. 1994. *Number-theoretic Methods in Statistics*. London, UK: Chapman & Hall. ISBN: 0-412-46520-5.

Hua, L-K. & Wang, Y. 1981. *Applications of Number Theory to Numerical Analysis*. Berlin & New York: Springer-Verlag & Beijing: Science Press. ISBN: 9783540103820.

Huang, B. & Chen, D. 2009. Effective Pareto Optimal Set of Multi-objective Optimization Problems. *Computer & Digital Engineering, 37*(2), pp.28-34 [online]. Available at: https://caod.oriprobe.com/articles/17362139/Effective_Pareto_Optimal_Set_of_Multi_Objective_Op.htm [Accessed: 20 March 2022].

Paskov, S.H. 1996. New methodologies for valuing derivatives. In: Pliska, S. & Dempster, M. & (Eds.) *Mathematics of Derivative Securities*, pp.545-582. Cambridge: Isaac Newton Institute & Cambridge University Press. Available at: https://doi.org/10.7916/D8TB1FRJ.

Paskov, S.H. & Traub, J.F. 1995. Faster valuation of financial derivatives. Journal of Portfolio Management 22(1), pp.113-120. Available at: https://doi.org/10.3905/jpm.1995.409541.

Qu, X., Lu, N., & Meng, X. 2004. Multi-objective Fuzzy Optimization of Tower Crane Boom Tie Rods. *Journal of Mechanical Transmission,* 28(3), pp.38-40 [online]. Available at: https://caod.oriprobe.com/articles/7413876/Fuzzy_Optimization_of_Arm_Link_Rod_in_Tower_Crane.htm [Accessed: 20 March 2022].

Ripley, B.D. 1981. *Spatial Statistics.* Hoboken, NJ: John Wiley & Sons. ISBN: 0-47169116-X.

Sloan, I.H. & Wozniakowski, H. 1998. When Are Quasi-Monte Carlo Algorithms Efficient for High Dimensional Integrals?. *Journal of Complexity*, 14(1), pp.1-33. Available at: https://doi.org/10.1006/jcom.1997.0463.

Tezuka, S. 1998. Financial applications of Monte Carlo and Quasi-Monte Carlo methods. In: Hellekalek, P. & Larcher, G. (Eds.) *Random and Quasi-Random Point Sets. Lecture Notes in Statistics,* 138*,* pp.303-332. New York: Springer. Available at: https://doi.org/10.1007/978-1-4612-1702-2_7.

Tezuka, S. 2002. Quasi-Monte Carlo - Discrepancy between theory and practice. In: Fang, K.T., Niederreiter, H. & Hickernell, F.J. (Eds.) *Monte Carlo and Quasi-Monte Carlo Methods 2000*, pp.124-140. Heidelberg: Springer-Verlag. Available at: https://doi.org/10.1007/978-3-642-56046-0_8.

Wang, Y. & Fang, K. 2010. On number-theoretic method in statistics simulation. *Science in China Series A: Mathematics,* 53, pp.179-186. Available at: https://doi.org/10.1007/s11425-009-0126-3.

Yu, J., Zheng, M., Wang, Y. & Teng, H. 2022. An efficient approach for calculating a definite integral with about a dozen of sampling points. *Vojnotehnički glasnik/Military Technical Courier*, 70(2), pp. 340-356. Available at: https://doi.org/10.5937/vojtehg70-36029.

Zheng, M. 2022. Application of probability-based multi–objective optimization in material engineering. *Vojnotehnički glasnik/Military Technical Courier*, 70(1), pp.1-12. Available at: https://doi.org/10.5937/vojtehg70-35366.

Zheng, M., Teng, H., Yu, J., Cui, Y. & Wang, Y. 2022. *Probability-Based Multi-objective Optimization for Material Selection*. Singapore: Springer. ISBN: 978-981-19-3350-9.

Zheng, M., Wang, Y. & Teng, H. 2021. A New "Intersection" Method for Multi-objective Optimization in Material Selection. *Tehnički glasnik,* 15(4), pp.562-568. Available at: https://doi.org/10.31803/tg-20210901142449.

ПРИМЕНЕНИЕ КОНЕЧНЫХ ТОЧЕК ВЫБОРКИ В МНОГОЦЕЛЕВОЙ ОПТИМИЗАЦИИ, ОСНОВАННОЙ НА ВЕРОЯТНОСТИ С ПОМОЩЬЮ ЕДИНОЙ ЭКСПЕРИМЕНТАЛЬНОЙ РАЗРАБОТКИ

Маошенг Чжэн[а], **корреспондент**, *Хайпэн* Тен[а], *Йи* Вон[а], *Джи* Йю[б]

Северо-западный политехнический университет,
г. Сиань, Народная Республика Китай

[а] факультет химической инженерии

[б] факультет естественных наук

РУБРИКА ГРНТИ: 27.47.00 Математическая кибернетика,
27.47.19 Исследование операций,
81.09.00 Материаловедение,
45.09.00 Электротехнические материалы

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Аппроксимация для оценки определенного интеграла не перестает привлекать внимание ученых, ввиду своего практического применения в различных областях инженерных наук. Недавно был разработан эффективный подход к вычислению определенного интеграла с небольшим числом точек выборки для получения приблизительного значения численного интеграла со сложным подынтегральным выражением. В данной работе в целях упрощения сложного определенного интеграла в МООВ был применен эффективный подход с небольшим числом точек выборки, объединенный с новой многоцелевой оптимизацией, основанной на вероятности (МООВ) с помощью единой экспериментальной разработки.

Методы: Распределение точек выборки в пределах области с одним пиком является детерминированным и равномерным, что *соответствует правилам метода единой разработки и точек идеальной решетки; общая предпочтительная вероятность является уникальным и детерминированным индексом в МООВ.*

Результаты: Применение эффективного подхода с конечными точками выборки при решении типовых проблем в МООВ указывает на его рациональность и удобство в эксплуатации.

Выводы: Эффективный подход с конечными точками выборки для оценки определенного интеграла успешно комбинируется с МООВ с помощью метода единой разработки и точек идеальной решетки.

Ключевые слова: предпочтительная вероятность, многоцелевая оптимизация, конечные точки выборки, упрощение оценки, единый метод разработки.

ПРИМЕНА КОНАЧНИХ ТАЧАКА УЗОРКОВАЊА У ВИШЕКРИТЕРИЈУМСКОЈ ОПТИМИЗАЦИЈИ ЗАСНОВАНОЈ НА ВЕРОВАТНОЋИ ПОМОЋУ УНИФОРМНОГ ЕКСПЕРИМЕНТАЛНОГ ДИЗАЈНА

Маошенг Џенг[а], **аутор за преписку**, *Хаипенг* Тенг[а], *Ји* Ванг[а], *Ђе* Ју[б]

Универзитет Северозапад, Сијан, Народна Република Кина

[а] Факултет хемијског инжењерства

[б] Факултет природних наука

ОБЛАСТ: математика, материјали
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Апроксимација процене коначног интеграла не престаје да буде привлачна тема захваљујући својој практичној примени у научним и инжењерским областима. Недовно је развијен ефикасан приступ израчунавању одређеног интеграла с малим бројем тачака узорковања како би се добила приближна вредност за нумерички интеграл са компликованим интеграндом. У овом раду ефикасан приступ с малим бројем тачака узорковања комбинован је са новом вишекритеријумском оптимизацијом заснованом на вероватноћи (ПМОО) помоћу униформног експерименталног дизајна с циљем да се поједностави компликовани одређени интеграл у ПМОО.

Методе: Дистрибуција тачака узорковања унутар подручја издвојеног врха детерминистичка је и униформна, што следи из правила метода униформног дизајна и тачака добре решетке.

Укупна пожељна вероватноћа је јединствени и детерминистички индекс у ПМОО.

Резултати: Примене ефикасног приступа с коначним тачкама узорковања за решавање типичних проблема у ПМОО указују на његову рационалност и погодност при операцијама.

Закључак: Ефикасан приступ с коначним тачкама узорковања за оцену одређеног интеграла успешно се комбинује са ПМОО помоћу метода униформног дизајна и тачака добре решетке.

Кључне речи: пожељна вероватноћа, вишекритеријумска оптимизација, коначне тачке узорковања, поједностављивање евалуације, метод униформног дизајна.

Paper received on / Дата получения работы / Датум пријема чланка: 22.03.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22. 06. 2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24. 06. 2022.

KINETIC SIMULATION OF VACUUM PLASMA EXPANSION BEYOND THE “PLASMA APPROXIMATION”

Vasily Y. Kozhevnikov[a], *Andrey* V. Kozyrev[b], *Aleksandr* O. Kokovin[c], *Natalia* S. Semeniuk[d]

Institute of High Current Electronics, Laboratory of Theoretical Physics, Tomsk, Russian Federation

[a] e-mail: Vasily.Y.Kozhevnikov@ieee.org, **corresponding author**, ORCID iD: https://orcid.org/0000-0001-7499-0578

[b] e-mail: kozyrev@to.hcei.tsc.ru, ORCID iD: https://orcid.org/0000-0002-7078-7991

[c] e-mail: kokovin.alexandr@mail.ru, ORCID iD: https://orcid.org/0000-0003-2068-7674

[d] e-mail: viliiskoeozero@yandex.ru, ORCID iD: https://orcid.org/0000-0002-5972-2839

DOI: 10.5937/vojtehg70-37337; https://doi.org/ 10.5937/vojtehg70-37337

FIELD: Plasma physics
ARTICLE TYPE: Original scientific paper

Summary:

Introduction/purpose: One of the key approaches to solving an entire class of modern plasma physics problems is the so-called "plasma approximation". The most general definition of the "plasma approximation" is a theoretical approach to the electric field calculation of a system of charges under the electric quasi-neutrality condition. The purpose of this paper is to compare the results of the numerical simulation of the kinetic processes of the quasi-neutral plasma bunch expansion to the analytical solution of a similar kinetic model but in the "plasma approximation".

Methods: The given results are obtained by the methods of deterministic modeling based on the numerical solution of the system of Vlasov-Poisson equations.

ACKNOWLEDGMENT:
This paper is dedicated to the blessed memory of our good friend, permanent Chair of the TELFOR Telecommunications Forum Steering Committee Prof. Dr. Đorđe Paunović (1938-2021). During his long and rich career, he was a professor, head, mentor, colleague, friend, and, in every sense, much more than that.
The work was carried out within the framework of the state assignment of the Ministry of Science and Higher Education of the Russian Federation on the topics FWRM-2021-0007, FWRM-2021-0014.

Results: The provided comparison of the analytical expressions for the solution of kinetic equations in the "plasma approximation" and the numerical solutions of the Vlasov-Poisson equations system convincingly show the limitations of the "plasma approximation" in some important cases of the considered problem of plasma formation decay.

Conclusion: The theoretical results of this work are of great importance for understanding the shortcomings of the "plasma approximation", which can manifest themselves in practical applications of computational plasma physics.

Key words: physical kinetics, vacuum plasma, plasma expansion.

Introduction

The “plasma approximation” is known to be applicable to a low-frequency and steady-state phenomenon, popular among plasma scientists in various fields (Chen, 1984). Sometimes more appropriable term is used here “the plasma condition” (Nishikawa & Wakatani, 1990), i.e. the number of electrons in a Debye sphere is large enough to effect charge shielding. But utilizing it leads to inconsistencies in the equation of motion and prevents a proper, field-theoretic treatment of a condensed matter in the plasma state. This circumstance takes place due to the fact that if plasma reaches a quasi-neutral state $n_e \approx n_i$, its space charge is approximately equal to zero $\rho \approx 0$. According to Poisson equation, this leads to $\boldsymbol{E} = 0$. But the “plasma approximation” states that $\boldsymbol{E} \neq 0$ and the electric field can be found elsewise (Chen, 1984). Such a separation of the initially consistent solution of plasma and field equations in the most cases leads to an ambiguous multivalued interpretation of the electric field definition. That seems to be the main methodological drawback of the "plasma approximation".

As only formal definitions equate with formal mathematics, so the “quasineutral” term correlates to “the plasma condition” $n_e \approx n_i$. It refers to the profound tendency of plasma electrons to change their positions as a response to the electrostatic potential of ions to exponentially attenuate the Coulomb field, and is often taken as the definition of the “plasma approximation.” We know that the the traditional term “neutral” already embraces the implications of quasineutrality, as no discrete medium remains neutral on characteristic scales sufficiently smaller to resolve isolated charges. In quasineutral media, the microscopic field fluctuates strongly, but on the particle scale it averages out as the differential volume element grows. The author of the monograph (Chen, 1984) claims that “the plasma approximation is almost the same as the condition of quasineutrality discussed earlier but has a more exact meaning … is a mathematical shortcut that one can use even for wave motions… it is usually possible to assume $n_e = n_i$ and $div\, \boldsymbol{E} \neq 0$ at the same time".

The physical kinetics of plasma provides a different point of view on a "quasineutrality" concept given from more fundamental positions. Indeed, if we consider simple two component plasma that consists of least of electrons and single-charged ions, then the ensemble of each type of particles in terms of physical kinetics is characterized by its distribution function, here f_e and f_i, respectively. Hence the number density of each particle type is a special case of the distribution function zero-moment

$$n_{e,i} = \int f_{e,i}\left(\boldsymbol{r}, \boldsymbol{p}, t\right) d^3\boldsymbol{p} \tag{1}$$

where ($\boldsymbol{r}$, $\boldsymbol{p}$) – phase-space coordinates, t – time variable.

Such zero-moments, like e.g. (1), of the particle distribution function, do not characterize the microscopic state of the ensemble of particles. They just represent particular macroscopic characteristics of certain plasma components. That is why the approximation of $n_e \approx n_i$ is the equality in a "weak form", i.e. the identity $f_e = f_i$ does not follow from the quasi-neutrality condition. Frequently, depending on a particular physical problem based, one has to introduce extra conditions for two or more additional (higher) moments of the distribution function in order to satisfy the "plasma approximation". If we assume that the "plasma approximation" is a convenient computational approach to a number of physical problems, then one has to determine the limits of its use.

This paper is aimed to clarify the details of the two-component vacuum plasma bunch expansion into free space by numerically solving the system of Poisson-Vlasov equations. Its main purpose is to show the features of this process without using the "plasma approximation". For simplicity, but without loss of generality, we solve the problem of plasma expansion in a one-dimensional Cartesian spatial configuration. The calculation results are compared with the exact self-similar solutions of the Vlasov equations with the "plasma approximation" (Dorozhkina & Semenov, 1998) pointing out possible shortcomings of the "plasma approximation".

Vacuum plasma expansion

General terms

Let us consider a one-dimensional planar plasma bunch, consisting only of electrons and singly charged ions, located around the point x_0, on the x-axis. The bunch has a localization region of the order of x_c (spatial distribution half-width). We assume that both ions and electrons inside the bunch have Maxwellian velocity distributions with slightly different temperatures T_e for electrons and T_i for ions. Assuming that the intial plasma is quasi-neutral, the particle distribution functions can be written in the following form

$$f_{e,i}^{0}(x,p)=\frac{N_0}{Sx_c\sqrt{8\pi^2 m_{e,i}kT_{e,i}}}\exp\left(-\frac{p^2}{2m_{e,i}kT_{e,i}}\right)\times \\ \times\exp\left(-\frac{x^2}{x_c^2}\right) \tag{2}$$

where N_0 – full number of particles in the bunch, m_e and m_i – electron and ion rest mass, respectively, (x, p) – one-dimensional phase-space coordinates, S – bunch transversal cross section, x_c – characteristic spatial scale of a plasma bunch, and $T_{e,i}$ – initial ion and electron temperatures, respectively. If the initial electron distribution is assumed to be a non-Maxwellian, then it evolves to a Maxwellian one due to electron-electron elastic collisions. The Maxwellian distribution conserves, since collisions no longer have any influence on the electron distribution function, because the relevant term for elastic collisions is zero for a Maxwellian distribution. As the effects of collisions of the other kind are much more negligible with regard to electron-electrons, so the restriction to the Maxwellian initial distribution form is justified enough.

The electron and ion distribution function comply with the collisionless Boltzmann (Vlasov) equations without a magnetic field (Vlasov, 1968)

$$\begin{gathered}\frac{\partial f_e}{\partial t}+\frac{p}{m_e}\frac{\partial f_e}{\partial x}-qE\frac{\partial f_e}{\partial p}=0,\\ \frac{\partial f_i}{\partial t}+\frac{p}{m_i}\frac{\partial f_i}{\partial x}+qE\frac{\partial f_i}{\partial p}=0,\end{gathered} \tag{3}$$

where E - the electric field vector component along the x-axis, q – the electron charge.

During the expansion process, the assumption of a collisionless plasma is valid if the electron-electron collision time $\tau_{ee} >> \tau_{*} = L/C_s$, where L is the characteristic size and $C_s = (qT_e/m)^{1/2}$ is the ion sound velocity. As

$\tau_{ee} = T_e^{3/2}/(5 \cdot 10^{-6} n_e \Lambda)$, where Coulomb log is $\Lambda \approx 10$ and A is the atomic number, we can estimate the condition for a number density $n_e << n_* = T_e^2/(5 \cdot 10^{-12} A^{1/2} \Lambda L)$. For an antimony plasma ($A = 51$) at characteristic lengths of $L = 1$ cm and $T_e = 5$ eV, the value of $n_* \sim 7 \cdot 10^{10}$ cm^{-3} (Baitin & Kuzanyan, 1998).

In most cases where the domination of space-charge effects is significant and global plasma quasi-neutrality condition is not met, the system of equations (3) is complemented by the Poisson's equation in order to account the electric field in a self-consistent way

$$\frac{\partial^2 \varphi}{\partial x^2} = -\frac{q}{\varepsilon_0}\left(n_i - n_e\right), \quad E = -\frac{\partial \varphi}{\partial x}, \tag{4}$$

where φ - electrostatic (electric) potential, ε_0 – vacuum dielectric permittivity, n_e and n_i are electron and ion number densities, respectively, that have to be found from (1).

"Plasma approximation"

Regarding the problem of interest, the first paper where the "plasma approximation" and the associated theoretical approach have been introduced is Gurevich's paper (Gurevich et al, 1966). The case of a half-infinite plasma with a sharp boundary has been considered by using the Boltzmann electron distribution in order to find the electric field under the quasi-neutrality assumption

$$n_e\left(x,t\right) = n_0 \exp\left(-\frac{q\varphi\left(x,t\right)}{kT_e}\right), \tag{5}$$

where n_0 – is the constant characteristic number density of ions. This assumption is not appropriate, since the electrostatic potential is non-stationary and the electron distribution function is different from a Boltzmann for a collisionless plasma. So, the total electron energy changes in time and the electron thermal energy becomes a source of the ion component acceleration in the expanding plasma. In a bounded collisionless plasma, the electrons are trapped and oscillate in a potential well, which is formed in order to satisfy a quasi-neutrality condition. Since the parameters of the potential well change during plasma expansion, so the variation of the electron energy becomes significant.

A more complicated approach to the implementation of the "plasma approximation" is based directly on the physical kinetics principles (Dorozhkina & Semenov, 1998). From the plasma quasi-neutrality condition $n_e \approx n_i$, the left and right parts of equations in (3) are multiplied by p and then integrated by the moment variable over the phase space. Considering the number densities definition and the boundary conditions for the distribution functions at $|p| \to \infty$, the following equations can be obtained

$$\begin{aligned} &\frac{\partial}{\partial t}\int pf_e dp + \frac{1}{m_e}\frac{\partial}{\partial x}\int p^2 f_e dp + qEn_e = 0, \\ &\frac{\partial}{\partial t}\int pf_i dp + \frac{1}{m_i}\frac{\partial}{\partial x}\int p^2 f_i dp - qEn_i = 0. \end{aligned} \tag{6}$$

In order to obtain the electric field strength from expression (6), the authors of the approach (Dorozhkina & Semenov, 1998) impose an additional approximation, namely, they assume that the plasma bunch is “currentless“, so

$$q\int pf_e dp - q\int pf_i dp \approx 0, \tag{7}$$

in this case by subtracting the second equation from the first one in (6), the following expression for the electric field is obtained

$$E = \frac{\frac{1}{m_e}\frac{\partial}{\partial x}\int p^2 f_e dp - \frac{1}{m_i}\frac{\partial}{\partial x}\int p^2 f_i dp}{2qn_e}. \tag{8}$$

We can now compare (8) to the electric field obtained from Gurevich's formula (5)

$$E = -\frac{kT_e}{q}\frac{\partial}{\partial x}\ln n_e\,. \tag{9}$$

As it could be estimated, the given formulas (8) and (9) represent significantly different electric field values for the same plasma parameters. Namely, formula (9) gives a stronger electric field, which is an order of magnitude higher than the similar value obtained by formula (8). These arguments demonstrate the inconsistency of the "plasma approximation" concept. The whole point is the ambiguity of the definition of the electric field, and there are other approaches to obtaining the electric field in “plasma approximation“ leading to different electric field estimations which are all different (Baitin & Kuzanyan, 1998).

The presented discussion highlights the main disadvantages of the so-called "plasma approximation". First, the variety of the electric field representations in the "plasma approximation" is determined by different theoretical approaches (liquid, kinetic or particle-in-cell) in use, obviously depriving the unambiguity of such approaches. Secondly, the calculation of the electric field requires some additional approximations that come far beyond the basic "quasi-neutrality" condition which is find to be insuffucient. In the scientific literature, the use of such approximations is given without sufficient justification (Dorozhkina & Semenov, 1998). Finally, there is no unambiguous way to identify physical situations where the electric field in the "plasma approximation" smoothly transforms into the field determined from the Poisson’s equation or Maxwell's system of equations in the transition regions.

Numerical simulation

The obvious difficulties in choosing the correct formulation of the "plasma approximation" lead to the fact that the most accurate plasma dynamics has to be explained in terms of the complete Vlasov-Poisson system solution (3)-(4) where the electric field is determined in a self-consistent way. Here we choose a one-dimensional formulation of the problem in the Cartesian coordinates. Its advantages are obvious: the obtained solution results can be directly compared to the analytical formulas in the "plasma approximation" from (Dorozhkina & Semenov, 1998).

The direct numerical integration of (4) by using the trapezoidal or Simpson methods leads to significant inaccuracies associated with the accumulation of errors. To accurately determine the electric field and potential in this work, we used the advanced fourth order method (Knorr et al, 1980). As the computational phase space is restricted to the finite spatial interval $x \in [x_{\min}, x_{\max}]$, so we apply $\boldsymbol{E} = 0$ boundary conditions at the both sides of it.

In this paper, the system of partial differential equations (3) was solved numerically on a rectangular uniform phase-space grid (x, p) having 5000 per 2001 grid points for electrons and ions. The Vlasov equations have been solved by using the high-order Cheng-Knorr semi-Lagrangian method similar to that previously used (Zubarev et al, 2020, Kozhevnikov et al, 2021). The numerical solution algorithm was implemented in Mathworks MATLAB exploiting the embedded high-performance CPU capabilities. The results of numerical calculations have been validated by the computational grid and the computational time step value refining.

As an example, here we consider a two-component metallic plasma consisting of electrons and single-charged antimony ions Sb^+. This plasma components are typical for vacuum discharge in diodes with antimony cathodes (Anders, 1997). For this plasma composition, a number of numerical calculation series have been carried out. The simulations were processed for a wide range of total number of particles $N_0 = 10^7 - 10^{13}$. In each calculation, it was assumed that the plasma bunch had a characteristic scale of $x_c = 100$ μm, while the plasma was assumed to be nonequilibrium, i.e. $T_e = 1$ eV, $T_i = 5$ eV that corresponds to real cathode plasma emission (Bugaev et al, 1975). For computational purposes, we restrict the spatial boundaries of the computational phase space to $x_{min} = - 2$ cm, $x_{max} = 2$ cm. It is sufficient to simulate the ionized state behavior far enough from the computational borders. The obtained results were compared with the analytical solutions of the Vlasov equations with an electric field in the "plasma approximation" (8) (Dorozhkina & Semenov, 1998).

Figure 1 shows the comparisons of the number densities distributions of electrons and ions at a time point of $t = 500$ ns for the cases of plasma expansion consisting of different initial number of particles. A quasi-neutral plasma distribution profile is shown with a black line in accordance with the analytical solution in the “plasma approximation” (Dorozhkina & Semenov, 1998). The results of the numerical calculations (without the “plasma approximation”) - the number densities distribution profiles - are given for both electrons and ions to show the difference in their spatial distributions.

The first two plots in Figure 1 correspond to the decay of ionized states with a small number of particles - $N_0 = 10^7$ and $N_0 = 10^9$. Such initial distributions of charged particles cannot be called “plasma” due to the fact that the Debye length (Chen, 1984) is much larger than the characteristic scale of the bunch, i.e. $\lambda_D >> x_c$. In the first case, the Debye length is much greater than x_c, in the second case it has the same order of magnitude. In both cases, the numerical calculation shows a violation of the initially given quasi-neutrality conditions and a significant deviation from the "plasma approximation" profiles.

For a denser plasma ($N_0 = 10^{11}$), a different situation is observed. This case corresponds to true plasma decay $\lambda_D << x_c$. The electron and ions number density distribution profiles in the Vlasov-Poisson model are close to the quasi-neutral profile obtained from the "plasma approximation". For the specified time point ($t = 500$ ns), quasi-neutrality is not significantly disturbed over the entire length of the plasma bunch. This situation is most fully described by the "plasma approximation": the plasma bunch expands with thermal velocities without significant loss of the initial quasi-neutrality. At the very beginning of the process, the more mobile and thermalized electronic component of the plasma is displaced with regard to the electrically neutral state, which leads to the appearance of a weak electric field close to the field in the "plasma approximation" in this case. Thus, plasma tends to remain quasi-neutral: if the ions move, then the electrons will follow them, and the electric field is adjusting to maintain the neutrality in accordance with the displacement of electrons and ions.

Finally, the most important case considered here represents the decay of a dense plasma bunch. The corresponding result of these calculations is given at the fourth plot in Figure 1. For a plasma bunch with the total number of particles equal to $N_0 = 10^{13}$, other regularities are observed. First of all, one can find a similarly to the previous case $N_0 = 10^{11}$. For $N_0 = 10^{13}$ the plasma bunch expands in time while preserving quasi-neutrality. But resulting from the calculations without the "plasma approximation", plasma decays faster. The profiles of a quasi-neutral plasma in the “plasma approximation“ and that one obtained as a numerical solution of the Vlasov-Poisson equations (without the "plasma approximation") noticeably differ. In comparison with the decay of the ionized state (in $N_0 = 10^9$), where the quasi-neutrality is noticeably violated, the decay of the dense plasma is more intense with regard to the reference calculation (black line in Figure 1).

Since the bunch quasi-neutrality is not violated (for $N_0 = 10^{13}$), it can be assumed that in this case other factors affect the plasma decay process, which are not taken into account by the "plasma approximation" (Dorozhkina & Semenov, 1998). As we have already mentioned previously, the kinetic formulation of the "plasma approximation" requires an additional "currentless" approximation (7). The "currentless" approximation is introduced independently of the quasi-neutrality approximation. It leads to a linearization of kinetic equations (3), so that the plasma number densities (black lines in Figure 1) for different number of particles have the same characteristic width and differ only by the scale factor of the curve magnitude. In reality, the system of Vlasov-Poisson equations is essentially non-linear and its solutions for various parameters do not scale. The calculations show that condition (7) is violated for a dense plasma. It leads to faster plasma expansion due to the nonlinearly increasing influence of electron and ion currents without affecting the total bunch quasi-neutrality.

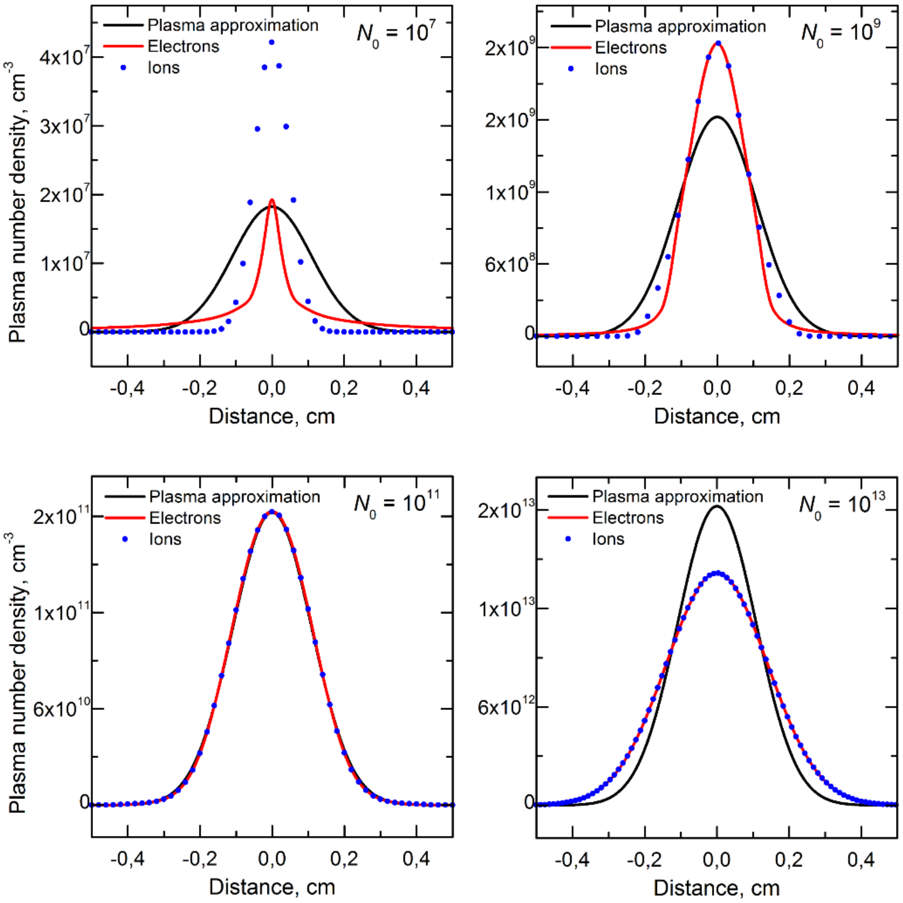


Figure 1 – Comparative plasma number density distributions obtained from numerical calculations without the "plasma approximation" (red line and blue points) and from exact analytical formulas in the "plasma approximation" (black line)

Рисунок 1 – Сравнительные распределения концентрации компонентов плазмы, полученные из численных расчётов без "плазменного приближения" (цветные кривые) и по точным аналитическим формулам в "плазменном приближении" (черная линия)

Слика 1 – Упоредне расподеле концентрације компоненти плазме добијене из нумеричких прорачуна без „плазма апроксимације”(обојене криве) и из тачних аналитичких формула у „плазма апроксимацији” (црна линија)

Conclusions

The results presented in this paper represent a counterexample convincingly showing the groundlessness of the "plasma approximation" for solving particular non-stationary plasma physics problems. The existing contradictions in the use of the "plasma approximation" can be formulated as the following theoretical statements:

- In all of the existing "plasma approximation" formulations, the electric field at $t = 0$ is nonzero, while the initial plasma is quasi-neutral, so the electric field initially is $\boldsymbol{E} = 0$;
- Accurate numerical simulation (without the "plasma approximation”) shows that for some cases of the quasi-neutral plasma bunch decay a local violation of plasma electrical neutrality appears. This leads to the electric field redistribution and affects further plasma dynamics, while in the "plasma approximation" plasma quasi-neutrality is preserved every time;
- Finally, the known "plasma approximations" are ambiguous. They require additional physical approximations depending on the theoretical approach in use. Such approximations in some cases make the “plasma approximation” less accurate.

Following the comparisons given in this paper, it can be argued that the "plasma approximation" can be used to study plasma decay without an external electric field only for a restricted range of dense plasma parameters. In other cases, the initial quasi-neutrality conditions do not guarantee the preservation of electrical neutrality during the whole ionized state decay process making the use of the “plasma approximation” unacceptable.

References

Anders, A. 1997. Ion charge state distributions of vacuum arc plasmas: The origin of species. *Physical Review E*, 55(1), pp.969-981. Available at: https://doi.org/10.1103/physreve.55.969.

Baitin, A.V. & Kuzanyan, K.M. 1998. A self-similar solution for expansion into a vacuum of a collisionless plasma bunch. *Journal of Plasma Physics*, 59(1), pp.83-90. Available at: https://doi.org/10.1017/s0022377897005916.

Bugaev, S.P., Litvinov, E.A., Mesyats, G.A. & Proskurovskiĭ, D.I. 1975. Explosive emission of electrons. *Soviet Physics Uspekhi*, 18(1), pp.51-61. Available at: https://doi.org/10.1070/pu1975v018n01abeh004693.

Chen, F.F. 1984. *Introduction to Plasma Physics and Controlled Fusion*. New York, NY: Springer. Available at: https://doi.org/10.1007/978-1-4757-5595-4.

Dorozhkina, D.S. & Semenov, V.E. 1998. Exact Solution of Vlasov Equations for Quasineutral Expansion of Plasma Bunch into Vacuum. *Physical Review Letters*, 81(13), pp.2691-2694. Available at: https://doi.org/10.1103/physrevlett.81.2691.

Gurevich, A.V., Pariiskaya, L.V. & Pitaevskii, L.P. 1966. Self-similar motion of rarefied plasma. *Soviet Phisics JETP*, 22(2), pp.449-454 [online]. Available at: http://jetp.ras.ru/cgi-bin/dn/e_022_02_0449.pdf [Accessed: 5 April 2022].

Kozhevnikov, V., Kozyrev, A., Kokovin, A. & Semeniuk, N. 2021. The Electrodynamic Mechanism of Collisionless Multicomponent Plasma Expansion in Vacuum Discharges: From Estimates to Kinetic Theory. *Energies*, 14(22), art.ID:7608. Available at: https://doi.org/10.3390/en14227608.

Knorr, G., Joyce, G. & Marcus, A. 1980. Fourth-order Poisson solver for the simulation of bounded plasmas. *Journal of Computational Physics*, 38(2), pp.227-236. Available at: https://doi.org/10.1016/0021-9991(80)90054-6.

Nishikawa, K. & Wakatani, M. 1990. Basic Properties of Plasma. In: *Plasma Physics*, 8, pp.6-13. Springer, Berlin, Heidelberg: Springer Series on Atoms+Plasmas. Available at: https://doi.org/10.1007/978-3-662-02658-8_2.

Vlasov, A.A. 1968. The vibrational properties of an electron gas. *Soviet Physics Uspekhi*, 10(6), pp.721-733. Available at: https://doi.org/10.1070/pu1968v010n06abeh003709.

Zubarev, N.M., Kozhevnikov, V.Y., Kozyrev, A.V., Mesyats G.A., Semeniuk, N.S., Sharypov, K.A., Shunailov, S.A. & Yalandin, M.I. 2020. Mechanism and dynamics of picosecond radial breakdown of a gas-filled coaxial line. *Plasma Sources Science and Technology*, 29(12), art.ID:125008. Available at: https://doi.org/10.1088/1361-6595/abc414.

КИНЕТИЧЕСКОЕ МОДЕЛИРОВАНИЕ РАСШИРЕНИЯ ВАКУУМНОЙ ПЛАЗМЫ ЗА ПРЕДЕЛАМИ “ПЛАЗМЕННОГО ПРИБЛИЖЕНИЯ”

Василий Ю. Кожевников, **корреспондент**, *Андрей* В. Козырев,
Александр О. Коковин, *Наталия* С. Семенюк

Институт сильноточной электроники, Лаборатория теоретической физики,
г. Томск, Российская Федерация

РУБРИКА ГРНТИ: 29.27.03 Общие свойства плазмы
29.27.47 Численные методы в физике плазмы
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Одним из ключевых подходов к решению целого класса задач современной физики плазмы является так называемое "плазменное приближение". Наиболее общее определение "плазменного приближения" - это теоретический подход к вычислению электрического поля системы зарядов в *условиях их электрической квазинейтральности. Целью данной работы является сравнение результатов численного моделирования кинетических процессов распада сгустка квазинейтральной плазмы с аналитическим самоподобным решением аналогичной кинетической модели, полученным в условиях "плазменного приближения".*

Методы: Приведенные результаты получения детерминистического моделирования, основанные на вычисленном обнаружении системы обнаружения Власова-Пуассона.

Результаты: Сравнение аналитических выражений решения кинетических уравнений в "плазменном приближении" и численных решений системы уравнений Власова-Пуассона убедительно показывают ограниченность использования "плазменного приближения" в ряде случаев рассматриваемой задачи о распаде плазменного образования.

Выводы: Теоретические результаты данной работы имеют большое значение для понимания недостатков "плазменного приближения", которые могут проявляться в практических приложениях вычислительной физики плазмы.

Ключевые слова: физическая кинетика, вакуумная плазма, разлет плазмы.

КИНЕТИЧКА СИМУЛАЦИЈА ЕКСПАНЗИЈЕ ВАКУУМСКЕ ПЛАЗМЕ ИЗВАН ГРАНИЦА „ПЛАЗМА АПРОКСИМАЦИЈЕ”

Василиј Ј. Кожевников, **аутор за преписку**, *Андреј* В. Козирев, *Александар* О. Коковин, *Наталија* С. Семенјук

Институт за високострујну електронику, Лабораторија за теоријску физику, Томск, Руска Федерација

ОБЛАСТ: физика (општа својства плазме)
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Један од кључних приступа решавању читаве класе проблема модерне физике плазме јесте такозвана апроксимација плазме. Најопштије се дефинише као теоријски приступ израчунавању електричног поља наелектрисаних честица под условом електричне квази-неутралности. Циљ овог рада јесте да упореди резултате нумеричке симулације кинетичких процеса ширења квазинеутралне згуснуте плазме са аналитичким решењем сличног кинетичког модела али у апроксимацији плазме.

Методе: Резултати су добијени методама детерминистичког моделовања заснованим на нумеричком решењу Власов-Поасоновог система једначина.

Резултати: Представљено поређење аналитичких израза за решавање кинетичких једначина у апроксимацији плазме, као и нумеричка решења Власов-Поасоновог система једначина, убедљиво показују ограничења апроксимације плазме у неким важним случајевима разматраног проблема распадања формација плазме.

Закључци: Теоријски резултати овог рада од великог су значаја за разумевање недостатака апроксимације плазме до којих може доћи приликом практичне примене компјутерске физике плазме.

Кључне речи: физичка кинетика, вакуум плазма, експанзија плазме.

Paper received on / Дата получения работы / Датум пријема чланка: 08.04.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.06.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24.06.2022.

ANALYSIS OF REPEATER JAMMING OF A SLOW FREQUENCY HOPPING RADIO

Nenad M. Stojanović[a], *Branislav* M. Todorović[b],
Vladimir B. Ristić[c]

[a] University of Defence in Belgrade, Military Academy, Department of Telecommunications and Informatics, Belgrade, Republic of Serbia,
e-mail: nivzvk@hotmail.com, **corresponding author,**
ORCID iD: https://orcid.org/0000-0001-9328-5348

[b] RT-RK Institute for Computer Based Systems,
Novi Sad, Republic of Serbia,
e-mail: branislav.todorovic@rt-rk.com,
ORCID iD: https://orcid.org/0000-0003-1932-8332

[c] University of Defence in Belgrade, Military Academy, Department of Telecommunications and Informatics, Belgrade, Republic of Serbia,
e-mail: vladarist@gmail.com,
ORCID iD: https://orcid.org/0000-0003-0422-9737

DOI: 10.5937/vojtehg70-37535; https://doi.org/10.5937/vojtehg70-37535

FIELD: Telecommunications
ARTICLE TYPE: Original scientific paper

Summary:

Introduction/purpose: The article presents a model of a slow frequency hopping radio in the case of repeater jamming. The aim is to analyze the effectiveness of repeater jamming to a military tactical slow frequency hopping radio.

Methods: It is assumed that the repeater jammer will be successful in detecting signals with slow frequency hopping at each hop and that it will perform successful partial jamming of the intercepted communication. Under partial jamming, it is considered that a certain part of the transmission time of each hop will be jammed. A theoretical analysis of the impact of a repeater jammer on a frequency hopping radio was performed based on the definition of the total probability of error. Various parameters that affect the segment of hop duration under jamming were considered.

Results: The obtained results show that high effective jamming is achieved even when a short segment of hop duration is jammed. We discuss the conditions for the repeater jammer to detect the signal during each hop and

ACKNOWLEDGMENT:
This research has been a part of Project No. VA-TT/3/20-22 supported by the Ministry of Defence, Republic of Serbia.

emit the jamming signal with the required strength. It has been shown that increasing the frequency hopping rate can significantly reduce the effectiveness of the repeater jammer.

Conclusion: Repeater jammers are highly effective against slow frequency hopping radio communication systems.

Key words: spread spectrum, frequency hopping, repeater jamming, error probability.

Introduction

Frequency hopping (FH) radios are designed to avoid narrowband interference or jamming (Scholtz, 1982). That is achieved by frequent changes of the operating frequency in a wide range of the spectrum. The performance of military tactical radio communications is often evaluated by the low probability of intercept and the anty-jamming characteristics (Lee et al, 2006). Frequency hopping belongs to the spread spectrum technology which has a lot of advantages, including but not limited to: anti-jamming, anti-eavesdroping and secrecy (Zhang et al, 2012). Due to these advantages, frequency hopping is a very important part of military communication systems, but also widely used in commercial telecommunication systems.

Frequency hopping is divided into fast and slow. Fast frequency hopping is a technique in which a hop duration is shorter than a bit duration, i.e. one bit is transmitted over several hops. Slow frequency hopping is a technique in which a hop duration is longer than a bit duration, i.e. several bits are transmitted within one hop. Slow frequency hopping is much often used, primarily due to simpler implementation (Torrieri, 1981).

Jammers are malicious radio devices used by attackers to cause intentional interference in radio communications. Jammers are used to completely or at least partially prevent the target from efficient use of the electromagnetic spectrum. Efficient use of the electromagnetic spectrum represents a successful radio communication between two radio devices. Jamming is performed by generating a signal with high strength which is received by the receiver of the jammed device. When a useful signal arrives at the receiver along with a jamming signal, it is not possible to extract useful information.

One of jammers classifications is on continuous wave (CW), pulse and repeater (Todorović, 1994). Based on their bandwidth, jammers can be classified as: wideband, partial-band and narrowband (Lee et al, 2006). Also, some other classifications of jamming techniques focus on noise jamming, tone jamming, sweep jamming and repeater jamming (Zhang et al, 2020). There are many other classifications of jamming techniques (Grover et al, 2014).

In military applications, the ability of the frequency hopping radio to avoid interference is limited by a repeater jammer (also known as a follower jammer). A repeater jammer is a device that intercepts a radio signal, processes it, and then transmits a jamming signal at the same operating frequency. When the transmitter changes the operating frequency, the repeater jammer scans the observed bandwidth and searches for a new frequency to jam again. In the optimal case, the jammer has the transmitter's hopping rate and the sequence of frequencies. To be effective against a frequency hopping system, the jamming energy must reach the target receiver before it hops to the next operating frequency. Thus, the hopping rate is the critical factor in protecting a radio system against a repeater jammer (Torrieri, 2015).

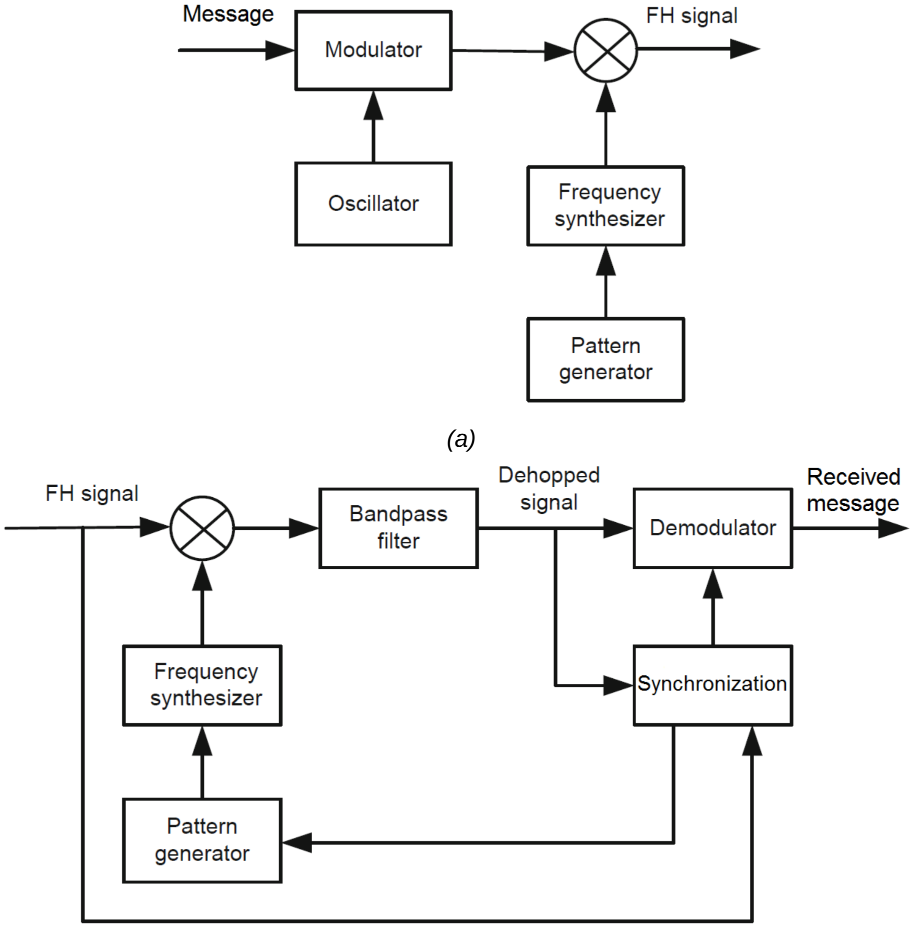
In this article, the effectiveness of a repeater jammer in the case of a radio system with slow frequency hopping is considered. The aim is to determine how the segment of hop duration under jamming affects the performance of the frequency hopping radio.

The second section of the article presents a model of a frequency hopping radio. Section three will present a model of repeater jamming in the case of slow frequency hopping. In Section four, numerical results and their analysis are given, while in the last section the most important conclusions are made.

Model of a frequency hopping radio

Frequency hopping is based on operating frequency change in a wide range. During communication, the transmitter and the receiver change their operating frequency in hops, according to a pre-agreed rate and order, which should remain secret for everyone except them. (Todorović, 2021).

A block diagram of the transmitter and the receiver of a frequency hopping radio is given in Figure 1 (Torrieri, 2015). Figure 1 (a) shows a transmitter block diagram. The frequency hopping radio transmitter consists of a modulator, where some of the conventional digital modulations are applied. The modulated signal is further sent to the mixer where it is mixed with the carrier generated in the frequency synthesizer. The rule by which frequency hopping is performed is generated by the pattern generator. The pattern generator actually generates a pseudonoise sequence that defines which next frequency the frequency synthesizer should be set to.



(a)

(b)

Figure 1 – General block diagram of a frequency hopping radio: (a) transmitter, (b) receiver
Рис. 1 – Общая блок-схема радиоустройства со скачкообразной перестройкой частоты: (а) передатчик (б) приемник
Слика 1 – Општа блок-шема радио-уређаја са фреквенцијским скакањем: (а) предајник, (б) пријемник

The general block diagram of the receiver is shown in Figure 1 (b). The pattern generator in the receiver is identical and has to be synchronized with the pattern generator in the transmitter. This ensures that the operating signal frequencies of the transmitter and the receiver change simultaneously. The signal from the output of the mixer is filtered, thus returning to the frequency band of the applied conventional modulation. By demodulating such a signal, an output signal from the receiver is obtained.

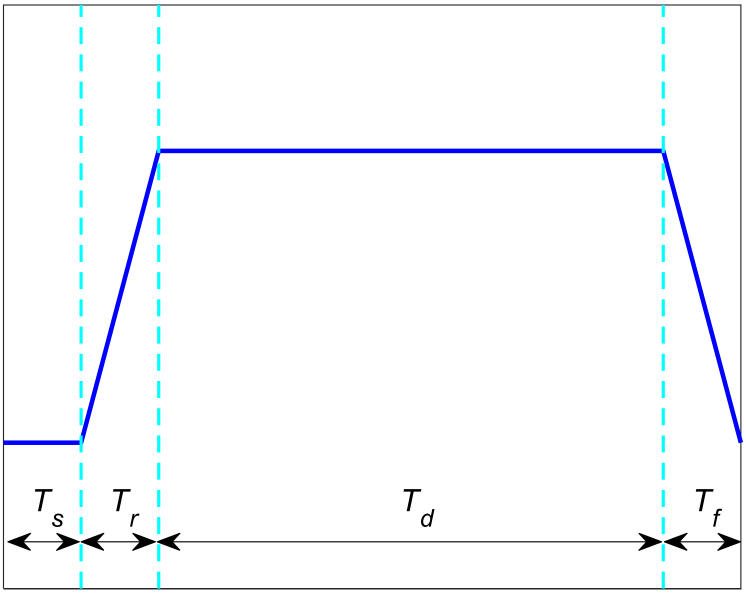


Figure 2 – Structure of a frequency hop
Рис. 2 – Структура скачка частоты
Слика 2 – Структура једног фреквенцијског скока

The time duration of one hop is called the hop interval and denoted by T_h (Torrieri, 2015). The structure of the hop interval is presented in Figure 2. The hop duration can be represented as a single pulse consisting of several segments. The most important segment, which also lasts the longest, is called the dwell time and it is marked with T_d. The rest of the time is the rise time, T_r, in order to reach the appropriate level before emission, and the fall time, T_f, in order to level drop after emission. The first segment is the silent time, T_s, which is used to set up the frequency synthesizer. It is short when hops are within the same subband, and much longer when two neighbouring hops are in different subbands.

Jamming scenario

Repeater jamming is effective against slow frequency hopping signals. A repeater jammer consists of two parts: a radio signal scanner and a radio signal generator. At first, the jammer performs spectrum scan and detection of received signals (signal intercept) and, based on that information reacts by generating a jamming signal the strength of which has enough power to completely degrade the useful signal on the receiver side (Lichtman & Reed, 2016). The jamming signal must reach the receiver before the jammed communication system moves to the next operating frequency. The repeater jammer has to quickly successively set the frequency synthesizer to different operating frequencies within a wide frequency range (Lee et al, 2006; Hansson et al, 2015).

The FSK (Frequency Shift Keying) modulation technique is the most common in frequency hopping devices. It has been shown that the FSK modulation has additional advantage as the most robust modulation, especially in military applications (Blanchard, 1982). We assume that the repeater jammer cover the entire FSK channel. After detection, the jammer begins to transmit a jamming signal and after a certain time completely jams the useful signal. The error probability would then be defined as follows:

$$P_e = P\left(\overline{J}\right) \cdot P\left(e/\overline{J}\right) + P\left(J\right) \cdot P\left(e/J\right), \qquad (1)$$

where are:

- $P(\overline{J})$ – the probability that there is no jamming in a certain period of hop duration,
- $P(e/\overline{J})$ – the error probability when there is no jamming,
- $P(J)$ – the probability that there is jamming in a certain period of hop duration, and
- $P(e/J)$ – the error probability when there is jamming of the useful signal.

As it is assumed that communication between two radio devices will be certainly jammed in each hop, the key parameter becomes the segment of the dwell time that will be jammed.

Figure 3 shows the geometric arrangement of a transmitter (T_x), a receiver (R_x) and a jammer (Torrieri, 1989). The distances between the elements are indicated. The distance between the transmitter and the receiver is denoted by d_1, the distance between the transmitter and the jammer with d_2, and the distance between the jammer and the receiver with d_3. The directions of signal propagation are represented by arrows. In order to meet the condition for the repeater jammer to be effective in jamming, the following inequation must be met:

$$\frac{d_2}{c}+T_{SJ}+T_{PJ}+T_{RJ}+\frac{d_3}{c}\leq\frac{d_1}{c}+T_d\ , \qquad (2)$$

where the remaining undefined elements of the expression are:

- c – speed of propagation of electromagnetic waves through free space which is $3\cdot10^8$ m/s,
- T_{SJ} – time required to scan the frequency band used for signal transmission by the repeater jammer,
- T_{PJ} – time required for the jammer to set the frequency synthesizer to the appropriate operating frequency,
- T_{RJ} – time required for the jammer to reach 90% of the maximum emission strength (rise time), and
- T_d – pulse duration of the useful signal during one hop (dwell time).

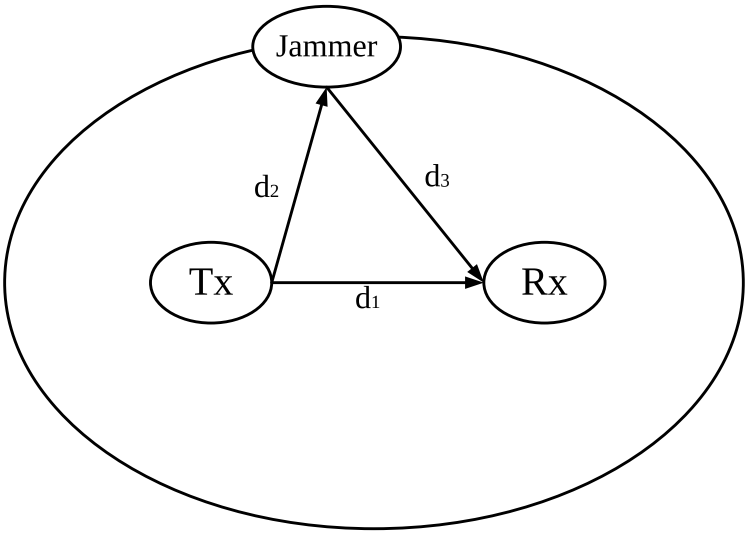
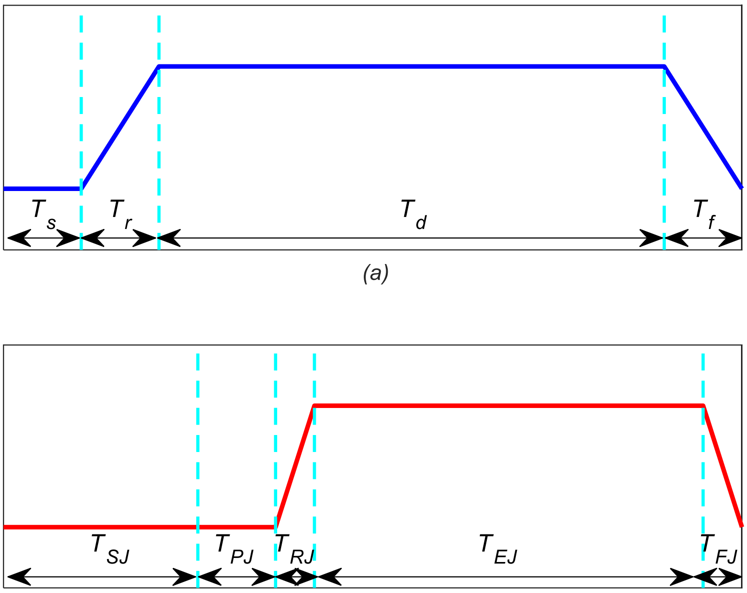


Figure 3 – Position geometry of the jammer, the transmitter and the receiver
Рис. 3 – Геометрия положения генератора помех, передатчика и приемника
Слика 3 – Геометрија позиција ометача, предајника и пријемника

If expression (2) were to be written as follows:

$$d_2+d_3\leq d_1+\left(T_d-T_{SJ}-T_{PJ}-T_{RJ}\right)\cdot c\ , \qquad (3)$$

and if it were assumed that the right side of the inequality is constant, then it would be an expression for an ellipse, where the transmitter and the receiver would be in the foci of the ellipse, and the jammer on the ellipse itself (Torrieri, 1989). If the jammer was outside the ellipse, the jamming would not be effective. Effective jamming could be achieved in cases when the jammer is on the ellipse or inside of the ellipse (Torrieri, 1989).



(a)

(b)

Figure 4 – Structure of a frequency hop: (a) transmitter, (b) repeater jammer
Рис. 4 – Структура скачка частоты:
(а) передатчика (б) передатчика ответных помех
Слика 4 – Структура једног фреквенцијског скока код:
(а) предајника, (б) репетитивног ометача

Figure 4 shows the segments in hop durations for the transmitter and the jammer. Figure 4 (a) is identical to Figure 2, and it is used for comparative representation. In Figure 4 (b), time segments at the repeater jammer's hop are shown.

The repeater jammer is scanning the spectrum until it detects a communication signal. After detection, during processing, the jammer is setting up a frequency synthesizer on the appropriate operating frequency. The adequate radiated signal strength of the jammer is achieved during the rise time. The effective jamming period is in the segment marked with T_{EJ} (time during which the jammer emits and jams).

The jammer emitted time can be obtained using the following expression:

$$T_{EJ} = T_h - T_{SJ} - T_{PJ} - T_{RJ} - T_{FJ} . \tag{4}$$

After the strength of the communication signal decreases for 3 dB of its maximum, the repeater jammer also decreases its strength in the T_{FJ} interval (fall time). The rise time and the fall time of the repeater jammer are shorter than the rise time and the fall time at the frequency hopping transmitter.

Numerical results

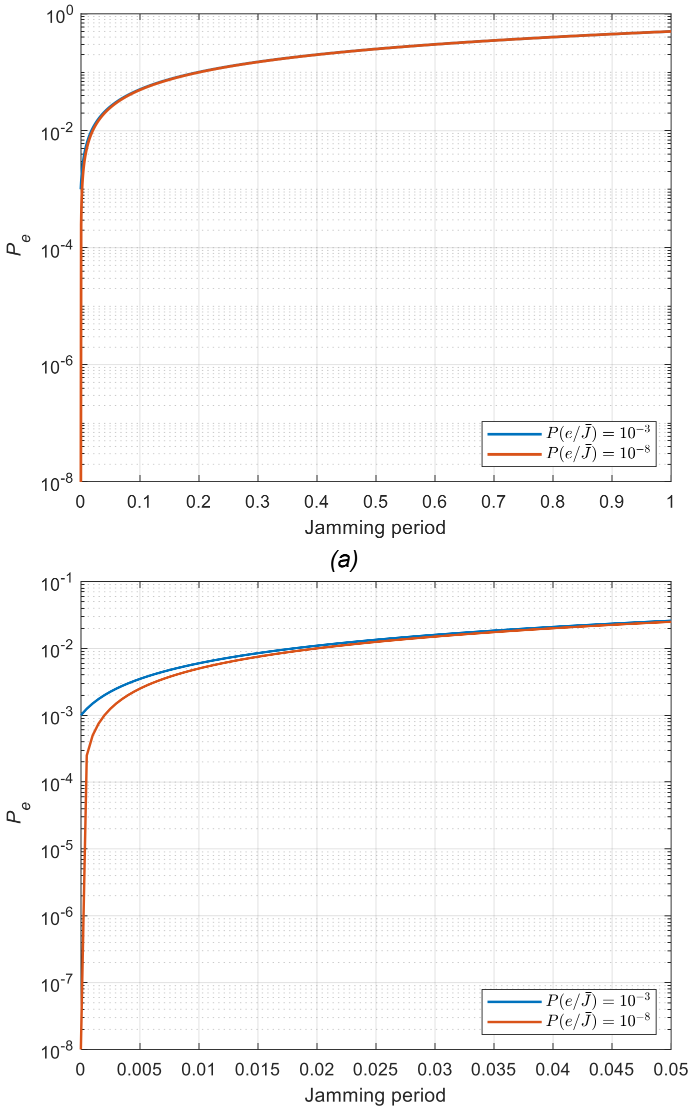
The analysis of the proposed slow frequency hopping radio and the jammer can be performed based on expression (1). It is assumed in the case of no jamming, the error probability depends only on the noise and multipath fading that can occur in the channel during signal transmission. In this case, the error probability is small enough and communication will be realized successfully. In accordance with the above, two values of $P(e/\overline{J})$ were considered: $P(e/\overline{J}) = 10^{-3}$ and $P(e/\overline{J}) = 10^{-8}$. Commercial radios require a high quality of service (QoS), so it is necessary that the error probability have very low values. In military radios, functionality has to be provided in hostile environment, so higher values of error probability can be acceptable.

If there is jamming during transmission, one can assume that a signal will be completely degraded. Accordingly, the value of $P(e/J) = 0.5$.

The remaining two parameters from expression (1) are complementary, i.e.:

$$P\left(\overline{J}\right) + P\left(J\right) = 1 . \tag{5}$$

Figure 5 shows the error probability versus the jamming period. Figure 5 (a) shows the entire jamming period for the two cases: $P(e/\overline{J}) = 10^{-3}$ and $P(e/\overline{J}) = 10^{-8}$. It can be noticed that two curves almost coincide. This was actually expected because the values of error probability when there is no jamming slightly contribute to the overall error probability. For a more detailed view, Figure 5 (b) shows only 5% of the jamming period. From this Figure, one can see that these two curves are different for only 2% of the jamming period.



(a)

(б)

Figure 5 – Error probability versus jamming period during a hop: (a) overall diagram, (b) first 5% of the overall diagram

Рис. 5 – Вероятность ошибки в зависимости от периода помех во время перехода: (а) общая диаграмма (б) первые 5% общей диаграммы

Слика 5 – Вероватноћа грешке у односу на период ометања током трајања хопа: (а) комплетан дијаграм, (б) првих 5% временског дела дијаграма

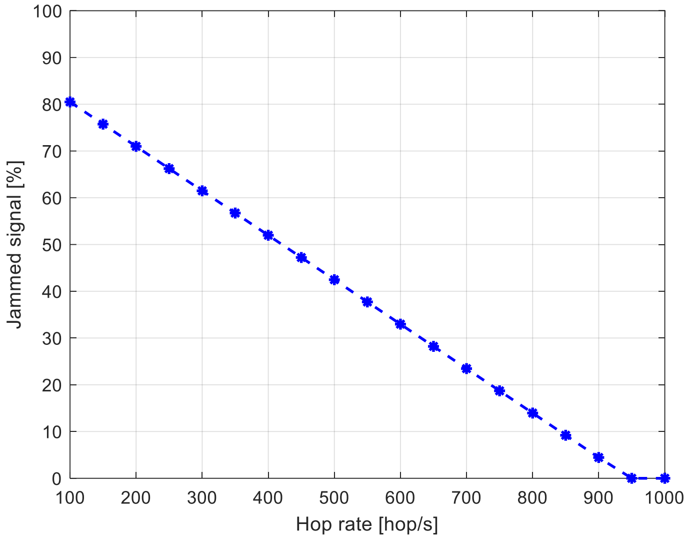


Figure 6 – Jammed signal in percent against the hop rate of the frequency hopping radio
Рис. 6 – Заглушенный сигнал в процентах по отношению к частоте скачков радиосвязи со скачкообразной перестройкой частоты
Слика 6 – Проценат ометаног сигнала у односу на брзину скакања радија са фреквенцијским скакањем

In order to calculate numerical results based on the proposed model, we used realistic data for the repeater jammer: d_1 = 30 km, d_2 = 20 km and d_3 = 25 km. The repeater jammer scanning time, the repeater jammer processing time, and the repeater jammer rise time are T_{SJ} = 150 µs, T_{PJ} = 800 µs and T_{RJ} = 500 ns, respectively. It is assumed that the FH radio dwell time is 90% of the hop duration and that the silent time is $T_s \approx 0$ s.

The percentage of the jammed signal versus the hop rate is presented in Figure 6. The hop rate varies in a wide range from 100 hops/s to 1000 hops/s. This figure shows a linear decrease in the percentage of jammed signals with the increase of the number of hops per second. It can be seen that the jammer is effective up to a frequency hopping rate of 900 hops/s, at least in a small percentage for higher frequency hopping rates. For frequency hopping rates higher than 900 hops/s, the repeater jammer becomes inefficient.

From Figure 6, it can be seen that over 80% of the hop duration is jammed when the hop rate is 100 hops/s. For higher frequency hopping rates, the percentage of jammed signals is lower. For example, for 900 hops/s, the jammed signal drops to around 4.5%.

Figure 7 once again shows the error probability versus the signal jamming period during a hop. Here, additionally indicated are two values of the error probability for the jamming period which corresponds to the frequency hopping rate of 300 hops/s and 700 hops/s. For 300 hops/s, about 61% of the dwell time is jammed, which causes a high error probability of about $3{\cdot}10^{-1}$. For 700 hops/s, about 23% of the dwell time is jammed, which also causes a high error probability of about 10^{-1}. With the increasing frequency hopping rate, from 300 hops/s to 700 hops/s, the error probability is decreasing for 20%, but still has high values, even for robust military radios.

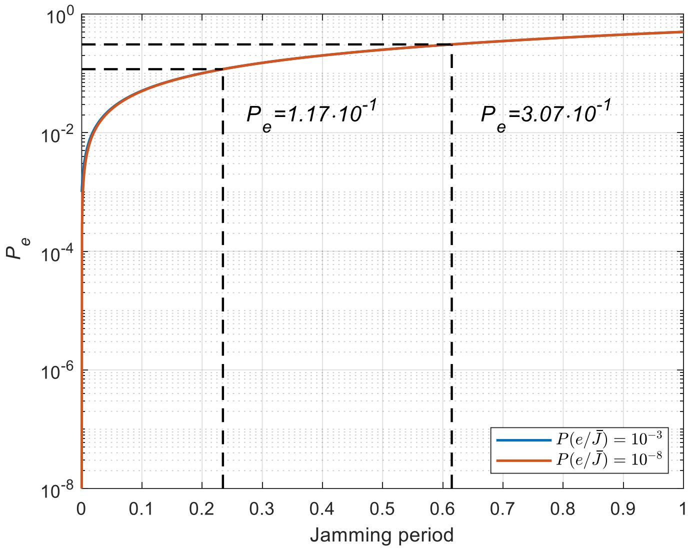


Figure 7 – Error probability versus the period of jamming during a hop with the specified characteristic values

Рис. 7 – Вероятность ошибки в зависимости от периода помех во время перехода с заданными значениями характеристик

Слика 7 – Вероватноћа грешке у односу на период ометања током трајања хопа са назначеним карактеристичним вредностима

Conclusion

Although frequency hopping signal transmission technology was created primarily to avoid jamming signals, it can still be effectively jammed using a repeater jammer. Slow frequency hopping is particularly susceptible to jamming with a repeater jammer. Slow frequency hopping transmits more bits during one hop and the time spent on one operating frequency is longer, so the repeater jamming is facilitated by jamming a certain part of the hop duration.

The considered model of the jamming of the slow frequency hopping radio simply shows the dependence of the error probability on the jammed period of hop duration using the total probability equation. It has been found that the error probability increases significantly after a very short period of hop jamming. It is assumed that the repeater jammer will be successful in detecting and jamming each hop.

The success rate of the hop duration jamming was analyzed depending on the frequency hopping rate. It is shown that the increase of the frequency hopping rate can significantly degrade the efficiency of the repeater jammer.

References

Blanchard, J.E. 1982. A slow frequency hopping technique that is robust to repeat jamming. In: *MILCOM 1982 - IEEE Military Communications Conference - Progress in Spread Spectrum Communications*, Boston, MA, USA, pp.14.1-1-14.1-9, October 17-19. Available at: https://doi.org/10.1109/MILCOM.1982.4805913.

Grover, K., Lim, A. & Yang, Q. 2014. Jamming and anti-jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing*, 17(4), pp.197-215. Available at: https://doi.org/10.1504/IJAHUC.2014.066419.

Hansson, A., Nilssen, J. & Wiklundth, K. 2015. Performance analysis of frequency-hopping ad hoc networks with random dwell-time under follower jamming. In: *MILCOM 2015 - 2015 IEEE Military Communications Conference*, Tampa, FL, USA, pp.848-853, October 26-28. Available at: https://doi.org/10.1109/MILCOM.2015.7357551.

Lee, C., Jeong, U., Ryoo, Y.J. & Lee, K. 2006. Performance of follower noise jammers considering practical tracking parameters. In: *IEEE Vehicular Technology Conferenc*e, Montreal, QC, Canada, pp.1-5, September 25-28. Available at: https://doi.org/10.1109/VTCF.2006.376.

Lichtman, M. & Reed, J.H. 2016. Analysis of reactive jamming against satellite communications. *International Journal of Satellite Communications and Networking*, 34(2), pp.195-210. Available at: https://doi.org/10.1002/sat.1111.

Scholtz, R. 1982. The origins of spread-spectrum communications. *IEEE Transactions on Communications*, 30(5), pp.822-854. Available at: https://doi.org/10.1109/TCOM.1982.1095547.

Todorović, B. 1994. Analiza uticaja ometačkih signala na radio-sisteme za prenos u proširenom spektru metodom direktne sekvence. *Vojnotehnički glasnik/Military Technical Courier*, 42(5), pp.370-374 (In Serbian). Available at: https://doi.org/10.5937/VojTehG9405370T.

Todorović, B. 2021. *Osnove telekomunikacija*. Belgrade: Akademska Misao/Academic Mind (in Serbian). ISBN: 978-86-7466-864-1.

Torrieri, D. 1981. *Principles of military communications systems*. Dedham, MA, USA: Artech House, Inc. ISBN: 9780890061022.

Torrieri, D. 1989. Fundamental limitations on repeater jamming of frequency-hopping communications. *IEEE Journal on Selected Areas in Communications*, 7(4), pp.569-575. Available at: https://doi.org/10.1109/49.17721.

Torrieri, D. 2015. *Principles of Spread-Spectrum Communication Systems*. Springer Cham. Available at: https://doi.org/10.1007/978-3-319-70569-9.

Zhang, Y., Sun, Z., Lu J. & An, J. 2012. Simulation and Performance Analysis of FH Spread Spectrum Communication System under Repeater Jamming. *Applied Mechanics and Materials (AMM),* 195, pp.744-747. Available at: https://doi.org/10.4028/www.scientific.net/AMM.195-196.744.

Zhang, X., Quan, H., Cui P. & Sun, H. 2020. Simulation and analysis of frequency hopping communication jamming. *Journal of Physics: Conference Series*, 1550(5), art.ID:052025. Available at: https://doi.org/10.1088/1742-6596/1550/5/052025.

АНАЛИЗ РЕТРАНСЛИРОВАННЫХ ПОМЕХ РАДИОСВЯЗИ С ПЛАВНОЙ ПЕРЕСТРОЙКОЙ ЧАСТОТЫ

Ненад М. Стояновичᵃ, **корреспондент**, *Бранислав* М. Тодоровичᵇ, *Владимир* Б. Ристичᵃ

[а] Университет обороны в г. Белград, Военная академия, кафедра телекоммуникаций и информатики, г. Белград, Республика Сербия

[б] Институт компьютерных систем РТ-РК, г. Нови-Сад, Республика Сербия

РУБРИКА ГРНТИ: 47.47.00 Радиопередающие и радиоприемные устройства
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: В данной статье представлена модель радиоприемника с плавной перестройкой частоты в случае ретранслированных помех. Цель статьи заключается в проведении анализа эффективности подавления ретранслированных помех в военной тактической радиостанции с плавной скачкообразной перестройкой частоты.

Методы: Предполагается, что устройство подавления ретранслированных помех сможет успешно обнаружить сигналы с плавной перестройкой частоты при каждом переходе и что оно будет успешно выполнять частичное подавление перехваченного сообщения. При частичном подавлении помех считается, что определенная часть времени передачи каждого *перехода будет подавлена. На основе определения общей вероятности ошибки был проведен теоретический анализ воздействия ретранслированных помех на радиосвязь со скачками частоты. Были рассмотрены различные параметры, влияющие на продолжительность скачков при помехах.*

Результаты: Полученные результаты показывают, что высокая эффективность глушения достигается даже при помехах с короткой длительностью скачка. В статье проанализированы условия, при которых устройство подавления ретранслированных помех должно обнаруживать сигнал во время каждого скачка и производить сигнал подавления с требуемой силой. В статье доказано, что увеличение скорости скачкообразной перестройки частоты может значительно снизить эффективность ретранслированных помех.

Выводы: Ретранслированные помехи оказывают сильное воздействие на систему радиосвязи с плавными скачками частоты.

Ключевые слова: расширение спектра, скачкообразная перестройка частоты, глушение ретранслятора, вероятность ошибки.

АНАЛИЗА РЕПЕТИТИВНОГ ОМЕТАЊА РАДИЈА СА СПОРИМ ФРЕКВЕНЦИЈСКИМ СКАКАЊЕМ

Ненад М. Стојановић[а], **аутор за преписку**, *Бранислав* М. Тодоровић[б], *Владимир* Б. Ристић[а]

[а] Универзитет одбране у Београду, Војна академија, Катедра телекомуникација и информатике, Београд, Република Србија

[б] РТ-РК Институт за рачунарске системе, Нови Сад, Република Србија

ОБЛАСТ: телекомуникације
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: У раду је представљен модел радија са спорим фреквенцијским скакањем у случају када је ометан репетитивним ометачем. Анализирано је ометање војног тактичког радио-уређаја са фреквенцијским скакањем репетитивним ометачем.

Методе: Претпостављено је да ће репетитивни ометач бити ефикасан приликом детекције сигнала са спорим фреквенцијским скакањем код сваког скока и да ће успешно извршити делимично ометање пресретнуте комуникације. Под делимичним ометањем се подразумева да ће одређени временски део трансмисије сваког хопа бити ометан. Спроведена је теоријска анализа утицаја *репетитивног ометача на радио са фреквенцијским скакањем на основу дефиниције тоталне вероватноће грешке. Разматрани су и различити параметри који утичу на дужину периода хопа који ће успешно бити ометан.*

Резултати: Добијени резултати показују да се ефикасно ометање постиже ако се омета мали део трајања једног скока. У разматраним условима репетитивни ометач детектује сигнал током сваког хопа и емитује ометајући сигнал потребном снагом. Показано је да се са повећањем брзине фреквенцијског скакања може знатно смањити утицај репетитивног ометача.

Закључак: Репетитивни ометачи су веома ефикасни у ометању комуникационих радио-система са спорим фреквенцијским скакањем.

Кључне речи: проширени спектар, фреквенцијско скакање, репетитивно ометање, вероватноћа грешке.

Paper received on / Дата получения работы / Датум пријема чланка: 21.04.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.06.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24.06.2022.

DESIGN AND IMPLEMENTATION OF A SMART STERILIZING DEVICE TO SOLVE THE DOORKNOB CONTAMINATION PROBLEM

Ihab Abdulrahman Satam[a], *Mohammed* U. Zaenal[b]

[a] Northern Technical University, Electronics Techniques Department,
Mosul, Nineveh, Republic of Iraq;
Obuda University, Doctoral School of Safety and Security Sciences,
Budapest, Hungary,
e-mail: Ihab.satam@uni-obuda.hu, **corresponding author**,
ORCID iD: https://orcid.org/0000-0002-9749-0944

[b] Al-Qalam University College, Computer Technical
Engineering Department, Kirkuk, Republic of Iraq,
e-mail: mohammedomid.eng@alqalam.edu.iq,
ORCID iD: https://orcid.org/0000-0002-8532-9643

DOI: 10.5937/vojtehg70-37492; https://doi.org/10.5937/vojtehg70-37492

FIELD: IT, Electrical engineering
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction: In 2020, the World Health Organization announced that Corona virus (Covid-19) is a global pandemic. Since then, social distancing and sterilization have become essential as precaution measures to decrease the infection. The risk of Covid virus spread led people, industries as well as governments to implement several approaches to control the transmission rate of the virus. During their daily life activities such as work, shopping, eating, etc. people touch a lot of surfaces and also open a large number of doors. This is considered to be one of the fastest ways to spread viruses because many people touch door handles which are generally rarely cleaned.

Method: In this paper, the implementation of a cost-effective smart device has been presented. The device sprays ethanol onto a doorknob from an ethanol sterilizer after any person touches the knob. The sensor detects a hand touching the knob, after that a signal is sent to the Arduino for processing, and then after a 4.5-sec delay, the Arduino sends a signal to the water pump to pump ethanol alcohols through the nozzle directly to the knob.

Results: The device shows precise and accurate results regarding the number of uses and the temperature of the surrounding ambient.

Conclusion: The system is applicable in offices and public buildings. Due to its functionality, it can be of great assistance in decreasing the contamination of doorknobs.

Keywords: smart sterilizer, arduino, actuators, doorknob, water pump.

ACKNOWLEDGMENT:
This work is dedicated to the University of Al-Qalam for Its aid in funding this work.

Introduction

Doorknobs are considered to be the most common places for viruses and infectious bacteria. They are the hotspot of viruses and bacteria since they are the main means for opening doors (Abdelmoktader & El Far, 2019; Chin et al, 2021; Narayana et al, 2021; Umamaheswari, 2020; Woodstock & Karlicek, 2020). Regular doors (non-automatic doors), especially office doors, are opened during the day at least hundreds of times, when each hand touching them contains a number of viruses or germs, which leads to an increase in infections among people. The idea of a smart sterilizing device was realized in order to protect people from germ infections arising from touching contaminated surfaces. The Arduino is an open-source electronic prototyping platform on the basis of flexible, easy-to-use hardware and software. The Arduino controller used in this work has 14 digital input/output pins (6 out of which can be used as PWM outputs), and 6 analog inputs. A low voltage switching relay used to integrate the pump with the Arduino shows the switching functionality (Rossetto et al, 2021; Katkar, 2021; Gheorghe & Stoica, 2021; De Felici et al, 2021; Pranata, 2021).

The PIR sensor is used to detect the radiation emitted from a user-touched door handle and then to send a signal to the Arduino which makes a decision based on the software program uploaded to it (Zemmouri et al, 2017; Youssef et al, 2020; Saravanamoorthi et al, 2017). There are few studies regarding sterilizing devices. Seongkeun Kwak et al (Kwak et al, 2013) used a smart device to control and monitor a pipeline-type UV sterilizer. The device proved to be more convenient and economical than a regular controller. Eddy et al proposed a design and implementation of a smart contactless hand sanitizer-dispensing system (Eddy et al, 2019). Mohammed et al suggested an intelligent system for door sterilization; despite the fact that the idea was only theoretical, it was good and could be executed (Alenzi & Abdudayem, 2017).

Theoretical backgrounds of the solution of modern control engineering design problems are thoroughly discussed and outlined in (Szabolcsi, 2019). In (Szabolcsi, 2020), Szabolcsi introduced several theoretical and practical approaches related to computer-aided design and analysis of modern control systems using MATLAB.

This paper solves the doorknob contamination problem with a cost-effective smart device controlled by an Arduino controller that can squirt ethanol from an ethanol sterilizer towards the doorknob after it is touched by a human hand.

Research method

The system operation principles depend on the detection of the hand motion over the doorknob. Figure (1) shows the existing system of a smart sterilizing system for doorknobs, while Figure 2 shows the system sketch design in Fritzing software. Fritzing software is open-source software used to design and simulate electronic circuits before they are actually built in. The system contains the controller, the Arduino in this particular case. After the doorknob is touched, the sensor detects the motion over the knob, sends a signal to the controller, and then the controller, based on the information coming from the sensor, commands the water pump (the actuator) to pump ethanol from the sterilizer onto the doorknob to clean it and sanitize it from germs.

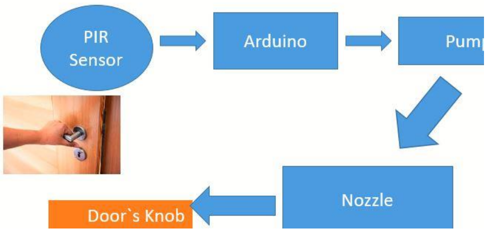


Figure 1 – Existing system of a smart sterilizer
Рис. 1 – Существующая система умного стерилизатора
Слика 1 – Постојећи систем паметног стерилизатора

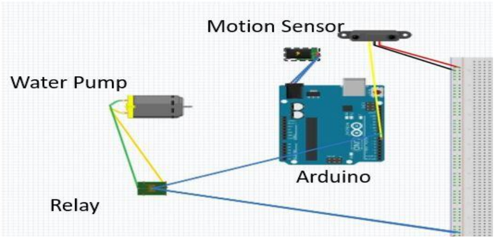


Figure 2 – System hardware sketch
Рис. 2 – Эскиз системы аппаратного обеспечения
Слика 2 – Скица хардверског система

System design

A. Arduino:

The Arduino can be described as the brain of the system. It is open-source hardware; it consists of sets of analog and digital pins that can be interfaced with various expansion boards, sensors, and actuators (Satam et al, 2021). The Arduino controller is widely used in different applications because of several reasons such as its price, its speed, the easiness of its use, etc. The controller board is shown in Figure 3.

Figure 3 – Arduino
Рис. 3 – Arduino
Слика 3 – Ардуино

B.   PIR sensor:

A Passive Infrared Sensor - PIR (as shown in Figure 4) is an electronic device that detects infrared light radiated from objects. It differs from an active IR sensor which consists of both emitter and detector, the emitter radiating infrared light and the receiver detecting the reflected radiation coming from the object. On the other hand, the PIR sensor consists of a detector only. When an object approaches the sensor, the detector detects the radiation coming from the object itself. The PIR does not radiate energy for detection purposes, it only detects the radiations coming or being reflected from objects (Simeon et al, 2018; Jindal et al, 2019). The sensor used in this research is Hc-SR501.

The sensor measures 1.2 * 0.9 inches. The front side is covered by a white Fresnel lens, the purpose of it being to increase the performance of the lens as well as to protect it. The other side is the PCB circuitry and other components required for processing information received from the sensor.

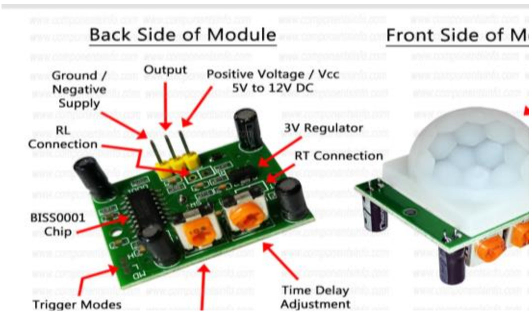


Figure 4 – PIR sensor
Рис. 4 – Датчик PIR
Слика 4 – ПИР сензор

C. Water gear pump:

A water gear pump can be defined as a positive displacement-rotating pump that moves fluids with the assistance of inbuilt gears. It consists of two gears which can create a vacuum force to boost the liquid within the gear. The pump also has other parts such as a shaft, a rotor, and a casing. The water gear pump working principle is easy to explain. The pump uses the gear rotating actions to move the liquid. The liquid seal will extend by the pump case to generate suction at the pump inlet. The drawn liquid can be included in the rotating gear cavities and moved to the ejection. There are two types of gear pumps: external and internal ones. They are widely used. The external gear pump consists of two gears: an interlocking one and an identical one. The interlocking gear is held up with separate shafts.

The internal gear pump has two gears different in size. The rotor is a larger gear (Ivanov & Ivanova, 2020; Du et al, 2019).

The water pump in this system pumps 100 ml of ethanol. The authors did some calculations regarding the time the pump should be ON as well as the position for the pump inside the device i.e. "the distance between the pump and the nozzle spray". The pump model used in this research is CH370-6A. Table 1 shows the pump specifications.

Table 1 – Water pump specifications
Таблица 1 – Технические характеристики водяного насоса
Табела 1 – Спецификације водене пумпе

Model	CH370-6A
Rated voltage	6 DCV
Rated current	380mA
Inflation time	10 s
Pump flow rate	2 L/M
Pressure	50mmHg
Life test	30000

Table 1 shows that the pump flow rate is 2 liters per minute. However, for the system, the amount flow rate needed is 1 ml of alcohol. In order for this to be achieved, the ON time for the pump should be taken into account. A simple proportion math ratio is done as follows.

$$\frac{Pump\ flow\ rate}{60\ sec.} = \frac{1\ ml}{x} \qquad (1)$$

$\frac{2}{60} = \frac{0.001}{x}$, from that x= 30 ms which means the pump should be ON for 0.03 seconds in order to pump 1 ml of ethanol.

The next step is to determine the distance between the pump and the nozzle inside the device.

$Q = \frac{Volume}{TIme}$ (2)

$Volume\ (V) = Q.t$

$V = 0.001 * 0.003$

$V = 3 * 10^{-5}\ liter$

$V = Area * distance$ (3)

$Distance\ (d) = \frac{Volume}{Area}$

The diameter of the pump hole is 10 mm

$Area = \pi * r^2$ (4)

$A = 8\ mm^2$

$d = 0.37\ m = 37\ cm$

From the above, the distance between the pump and the nozzle is 37 cm.

D. Relay:

An electromagnetic switch is used to turn the circuit on and off using a low-power signal (Figure 5). The relay came in two modes, Normally Open and Normally Closed. Normally open (NO) means that, when the relay is not energized, the contact is open. The same principle applies for the Normally Closed (NC) mode: NC means the contact is closed when the relay is not energized. (Tin et al, 2021; Alabed et al, 2021)

Figure 5 – Relay
Рис. 5 – Реле
Слика 5 – Релеј

E. Liquid Crystal Display (LCD):

One of the flat panel displays uses liquid crystals in its operation. Liquid crystals do not directly emit light. Instead, they use a backlight or a reflector to create images. The LCD combines two states, solid and liquid, as shown in Figure 6. The characters can easily be shown on the LCD screen. (Kobayashi et al, 2021)

Figure 6 – LCD
Рис. 6 – ЖК-дисплей
Слика 6 – ЛЦД

F. Spray nozzle

A spray nozzle is a device that disperses liquids into a spray. The three uses for the nozzle are: liquid distribution, widening the liquid surface area, and producing impact force on a solid surface.

G. Power source

A 9-volt battery is used to power the Arduino controller and the other parts of the system.

Experimental work

The functioning principles of the device depend on combining the parts described in the previous section. The device represents a new idea to prevent infections provoked by contamination with germs, or in this case viruses. The functioning of the electronic circuit of the system is explained in a few steps given below:

1 - The parts (PIR sensor, Water pump, LCD) are connected to the Arduino.

2 - When an object approaches the PIR sensor, the sensor will detect the radiation emitted from the object. Then the sensor sends a signal to the controller.

3 - The Arduino will receive the signal, process it, and then send a signal to the LCD and the water pump.

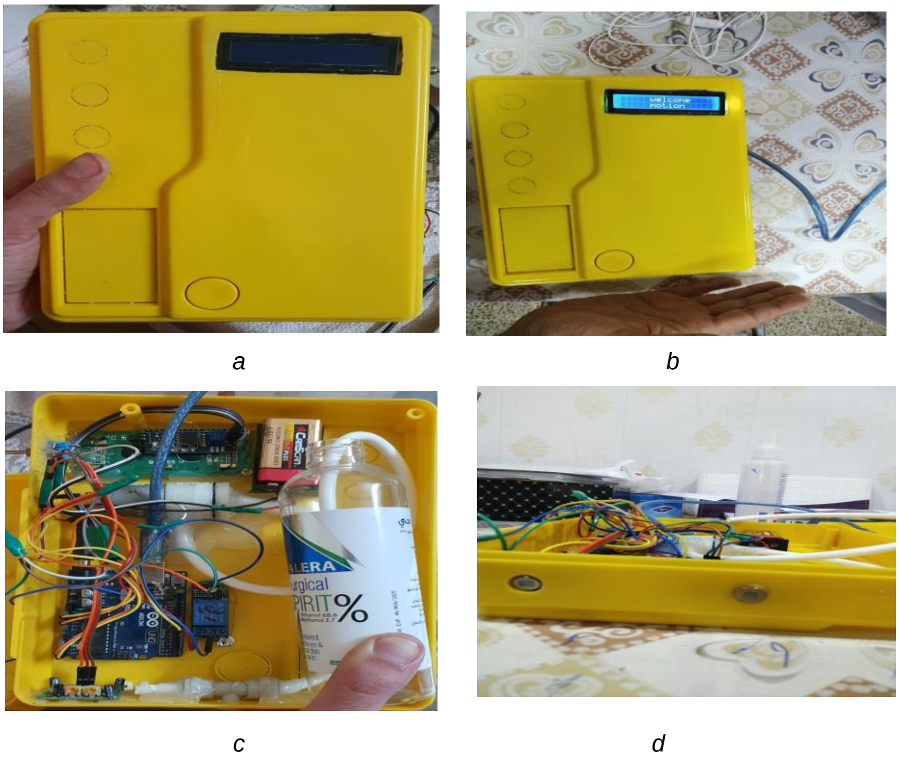
4 - After receiving the signal, the LCD will change the default message that appears on its screen from “No motion“ to “Motion“.

5 - The system waits for 4.5 seconds and then the water pump operates: it sucks the ethanol alcohol from the bottle attached to it and sends it to the nozzle. In accordance with the program software, the water pump is on for 30ms.

6 - The nozzle will spray the liquid onto the doorknob.

7 - An LCD message appears with the text of “No motion “

The Electronic circuit and the complete device are shown in Figure 7 (A to D).



a

b

c

d

Figure 7 – Complete system
Рис. 7 – Комплексная система
Слика 7 – Комплетан систем

Results and discussions

The device proves to be reliable in use and accurate in spraying the sterilizing material (ethanol) in a moment of use. However, we conducted several case studies with the device to prove that.

A. Case study Number 1 (Number of uses)

To measure the effectiveness of the device, we should calculate the number of uses the device can endure. With a simple software code, the PIR sensor also worked as a counter to count the number of people who touched the doorknob. The counter reached up to 589 trials and the device still performed properly as shown in Figure 8. This case depends on the delay time for the PUMP "which in this case was 4.5 sec". Unlike

(Vyawhare et al, 2020), we were to indicate the number of users of the device.

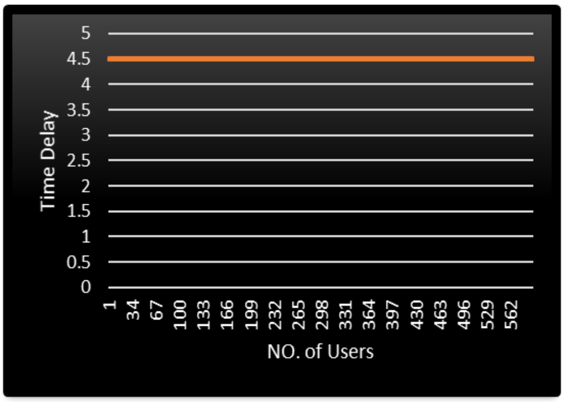


Figure 8 – Case study 1
Рис. 8 – Изучение конкретного случая 1
Слика 8 – Студија случаја 1

B. Case study Number 2 (Temperature)

In previous research studies, as in (Alenzi & Abdudayem, 2017; Vyawhare et al, 2020), temperature increase or decrease was not taken into account. In this work, we include temperature difference as a factor that can affect the performance of the device. At standard room temperature (25℃ or 68 F), the device works very precisely, which means the water pump will be ON for 30 ms. We raised the temperature for around 5 degrees and the device still worked properly with a slight difference - hence the ON mode for the water pump is 45 ms. When we decreased the temperature of the device for 5 degrees, the ON mode lasted for 35 ms, as shown in Figure 9.

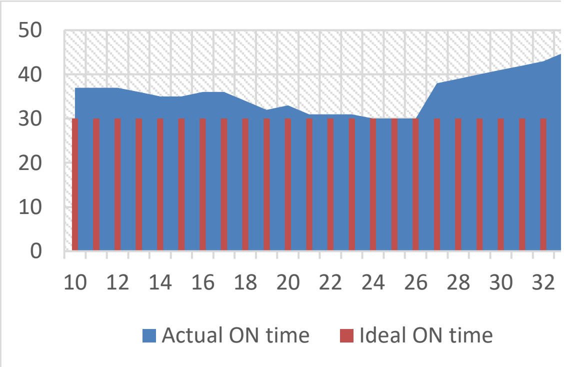


Figure 9 – Temperature effect on the device performance
Рис. 9 – Влияние температуры на производительность устройства
Слика 9 – Утицај температуре на функционисање уређаја

C. Case study Number 3 (Overlap)

This is an important case study. When the “Motion“ message appears, it means that after 4.5 seconds the water pump will be ON. However, since someone might hold the doorknob for 4.5 seconds, this is called an overlap, and to overcome this problem we added another PIR sensor to the system. The new sensor is located at a point of the door outside the door to detect the next person trying to open the door. In this case, there will be no delay for the water pump and it will start spraying alcohol immediately. Research studies as in (Vyawhare et al, 2020) recommended not using the device during the sanitation, but in this work we found a better solution to that problem. Figure 10 shows a flow chart of the case study 3 process.

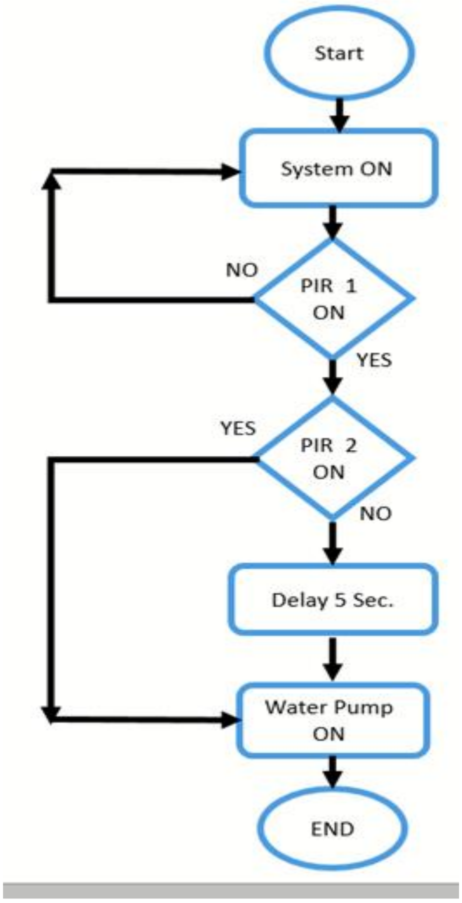
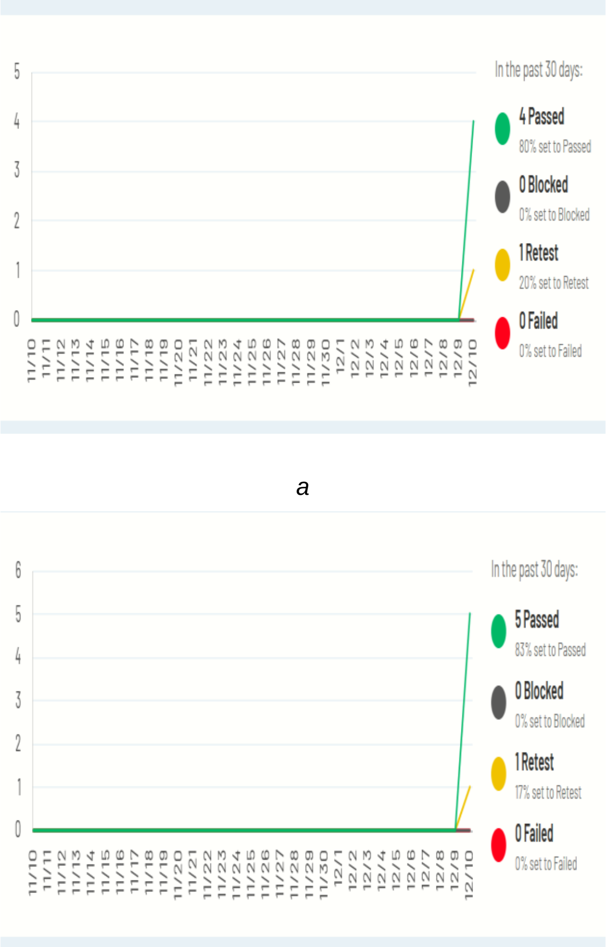


Figure 10 – Flow chart of case study 3 (Overlap)
Рис. 10 – Блок-схема исследования конкретного случая 3 (перекрытие)
Слика 10 – Дијаграм тока студије случаја 3

Figures 11(a) and 11(b) show the system performance with the overlap before and after adding an extra PIR sensor. Figure 11(a) represents the system without an additional PIR sensor. The result of the system performance appeared to be a retest for the system which means that the system with a new person touching the doorknob added extra delay time to the old one, which means that alcohol was not sprayed by the water pump. After the addition of the PIR sensor Number 2 to the system, the performance status changed to “passed“ (Figure 11(b). Accordingly, the new condition for the system worked accurately.



a

b

Figure 11 – System performance
Рис. 11 – Производительность системы
Слика 11 – Функционисање система

Conclusion

This work deals with a problem of doorknobs contaminated due to their everyday use. After a thorough study of the problem, the authors came up with an idea to sterilize the knob and prevent potential infections or diseases. The work in this paper is new and, more importantly, cost-effective with a high accuracy. The major problem encountered at first was the overlapping as mentioned in case study 3 in the Results and Discussions Section but an effective solution was found. The device is accurate, reliable, and useful for both private and public premises and all kinds of doors with knobs. The controller used to operate the device, the Arduino, is simple, easy to program, low in cost and with a very good response speed, providing precise results. For future work, fuzzy logic can be used in order to determine the amount of ethanol needed to be sprayed, which will enable the water pump to be located at any part of the device. A camera can be installed instead of a PIR sensor to solve the overlapping problem.

References

Abdelmoktader, A. & El Far, A.T. 2019. Nosocomial Infections Caused by ESBL. *Vaccines & Vaccination Open Access (VVOA)*, 4(1), art.ID: 000128 [online]. Available at: https://medwinpublishers.com/VVOA/VVOA16000128.pdf [Accessed: 15 April 2022].

Alabed, S., Maaz, I. & Al-Rabayah, M. 2021. Two-phase bidirectional dual-relay selection strategy for wireless relay networks. *Computers, Materials & Continua*, 69(1), pp.539-553. Available at: https://doi.org/10.32604/cmc.2021.018061.

Alenzi, M.M. & Abdudayem, A. 2017. Intelligent System For The Sterilization Of Doors. *International Journal of Scientific & Technology Research*, 6(5), pp.5-7 [online]. Available at: https://www.ijstr.org/final-print/may2017/Intelligent-System-For-The-Sterilization-Of-Doors.pdf [Accessed: 15 April 2022].

Chin, Y.H., Chin, H.H., Yap, Y.L. & Lau, B.K. 2021. Hypothalamic-pituitary fungal infection causing panhypopituitarism. *Medical Journal of Malaysia*, 76(4), pp.606-609 [online]. Available at: http://www.e-mjm.org/2021/v76n4/panhypopituitarism.pdf [Accessed: 15 April 2022].

De Felici, M., Klinger, F.G., Campolo, F., Balistreri, C.R., Barchi, M. & Dolci, S. 2021. To Be or Not to Be a Germ Cell: The Extragonadal Germ Cell Tumor Paradigm. *International Journal of Molecular Sciences*, 22(11), art.number: 5982. Available at: https://doi.org/10.3390/ijms22115982.

Du, T., Chu, N., Cao, L., Miao, T. & Wu, D. 2019. Study on Acoustic Performance of a Water Muffler for Gear Pump. *International Journal of Acoustics and Vibration*, 24(1), pp.34-43. Available at: https://doi.org/10.20855/ijav.2019.24.11143.

Eddy, Y., Mohammed, M.N., Arif Sameh, A., Al-Zubaidi, S. & Al-Sanjary, O.I. & Sairah, A.K. 2020. 2019 Novel Coronavirus Disease (Covid-19): Design and Development of Disinfectant Fogging System Using IoT Based Drone

Technology. *Revista Argentina Clínica Psicológica*, 29(5), pp.221-227 [online]. Available at: https://www.proquest.com/docview/2457332989?pq-origsite=gscholar&fromopenview=true [Accessed: 15 April 2022].

Gheorghe, A.C. & Stoica, C.I. 2021. Wireless Weather Station Using Arduino Mega And Arduino Nano. T*he Scientific Bulletin of Electrical Engineering Faculty*, 21(1), pp.35-38. Available at: https://doi.org/10.2478/sbeef-2021-0008.

Ivanov, V.V. & Ivanova, S.V. 2020. Flow rate of gear pumps with cycloid meshing. In: *Materials of the II International Maritime Scientific Conference of the Ship Power Plants and Technical Operation Department of Odessa National Maritime University*, pp.57-62, April 2020 [online]. Available at: http://dspace.pdpu.edu.ua/handle/123456789/10099 [Accessed: 15 April 2022].

Jindal, K., Kaushik, M. & Tripathi, A. 2019. Classroom monitoring and energy conservation system by employing PIR sensor. *International Journal of Recent Technology and Engineering (IJRTE)*, 8(2S11), pp.2098-2100. Available at: https://doi.org/10.35940/ijrte.B1208.0982S1119.

Katkar, R.B. 2021. COVID-19 Infection Causing Atypical Thyroiditis. *Journal of the Endocrine Society*, 5(Issue Supplement_1), pp.925-926. Available at: https://doi.org/10.1210/jendso/bvab048.1891.

Kobayashi, S., Miyama, T., Akiyama, H., Ikemura, A. & Kitamura, M. 2021. Generation of Geometric Extra Phase and Accompanying Temporal Effects in Asymmetric Optically Compensated IPS-LCDs and FFS-LCDs. *Symmetry*, 13(7), art.ID: 1143. Available at: https://doi.org/10.3390/sym13071143.

Kwak, S., Ryu, J., Chong, K. & Park, J. 2013. Smart device interface for intelligent control of pipeline type UV Sterilizer. In: *2013 IEEE RO-MAN*, Gyeongju, Korea (South), pp.352-353, August 26-29. Available at: https://doi.org/10.1109/ROMAN.2013.6628492.

Narayana, S., Prasad, R.V., Rao, V.S., Prabhakar, T.V., Kowshik, S.S. & Iyer, M.S. 2021. PIR sensors: characterization and novel localization technique. In: *IPSN '15: Proceedings of the 14th International Conference on Information Processing in Sensor Networks*, Seattle, Washington, pp.142-153, April 13-16. Available at: https://doi.org/10.1145/2737095.2742561.

Pranata, A. 2021. Automatic Scroll Saw System Dengan Teknik Kendali Kecepatan Pulse Width Modulation (PWM) Berbasis Arduino UNO. *Jurnal Teknologi Sistem Informasi Dan Sistem Komputer TGD*, 4(1), pp.69-77. Available at: https://doi.org/10.53513/jsk.v4i1.2602.

Rossetto, A.L., Amarante, L.F., Rossetto, A.L. & Junior, V.H. 2021. Injuries and infection caused by capybara bites in a human. *Revista da Sociedade Brasileira de Medicina Tropical*, 54(e0043-2021), pp.1-2. Available at: https://doi.org/10.1590/0037-8682-0043-2021.

Saravanamoorthi, R., Rathinavel, P., Sandhya, E. & Manu, K.M. 2017. Arduino based PWM voltage control of boost converter. I*nternational Journal of Engineering Research & Technology (IJERT)*, 6(3), pp.348-350. Available at: https://doi.org/10.17577/ijertv6is030350.

Satam, I.A., Shahab, S.N., Kamel, H.A. & Al-hamadani, M.N.A. 2021. Execution of a smart street lighting system for energy saving enhancement Execution of a smart street lighting system for energy saving enhancement.

Bulletin of Electrical Engineering and Informatics, 10(4), pp.1884-1892. Available at: https://doi.org/10.11591/eei.v10i4.2924.

Simeon, M., Elizabeth, A., Wara, S.T., Adoghe, A. & Hope, O. 2018. Efficient Energy Management System Using Pir Sensor. In: *2018 IEEE PES/IAS PowerAfrica*, Cape Town, South Africa, pp.601-606, June 28-29. Available at: https://doi.org/10.1109/PowerAfrica.2018.8521059.

Szabolcsi, R. 2019. *Modern Control Engineering*. Budapest: Óbuda University. ISBN: 978-963-449-18-80.

Szabolcsi, R. 2020. *Solution of Control Enginnering Problems Using MATLAB*. Budapest: Óbuda University. ISBN: 978-963-449-18-73.

Tin, P.T., Phan, V-D., Nguyen, P.X. & Nguyen, T-L., Thien Chau, D-S. & Nguyen, T.N. 2021. Outage Analysis in SWIPT-Based Decode-and-Forward Relay Networks with Partial Relay Selection. *Modelling and Simulation in Engineering*, 2021(art.ID: 9944565), pp.1-7. Available at: https://doi.org/10.1155/2021/9944565.

Umamaheswari, S. 2020. Pir sensor based security system. *Annals of Robotics and Automation*, 4(1), pp.22-24. Available at: https://doi.org/10.17352/ara.000006.

Vyawhare, R., Gagpalliwar, P. & Shirke, A. 2020. Automatic Door Knob/Handle Sanitization Using UV-C Light. *International Research Journal of Engineering and Technology (IRJET)*, 7(7), pp.2778-2781 [online]. Available at: https://www.irjet.net/archives/V7/i7/IRJET-V7I7489.pdf [Accessed: 15 April 2022].

Woodstock, T-K. & Karlicek, R.F. 2020. RGB Color Sensors for Occupant Detection: An Alternative to PIR Sensors. *IEEE Sensors Journal*, 20(20), pp.12364-12373. Available at: https://doi.org/10.1109/JSEN.2020.3000170.

Youssef, M., Boubahri, C., Aloui, F. & Fetni, S. 2020. Simulation and Design of A Single Phase Inverter with Digital PWM Issued by An Arduino Board. *International Journal of Engineering Research & Technology (IJERT)*, 9(8), art.ID: IJERTV9IS080237. Available at: https://doi.org/10.17577/ijertv9is080237.

Zemmouri, A., Elgouri, R., Alareqi, M., Dahou, H., Benbrahim, M. & Hlou, L. 2017. A comparison analysis of PWM circuit with arduino and FPGA. *ARPN Journal of Engineering and Applied Sciences*, 12(16), pp.4679-4683 [online]. Available at: http://www.arpnjournals.org/jeas/research_papers/rp_2017/jeas_0817_6261.pdf. [Accessed: 15 April 2022].

РАЗРАБОТКА И ИСПОЛЬЗОВАНИЕ УМНОГО СТЕРИЛИЗУЮЩЕГО УСТРОЙСТВА ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ ЗАГРЯЗНЕНИЯ ДВЕРНЫХ РУЧЕК

Ихаб Абдулрахман Сатам[а], **корреспондент**, *Мохаммед* У. Заеналь[б]

[а] Северный технический университет, кафедра электронной техники,
г. Мосул, Ниневия, Республика Ирак;
Обудский университет, Докторская школа безопасности,
г. Будапешт, Венгрия

[б] Университетский колледж Аль-Калам, департамент
вычислительной техники, г. Киркук, Республика Ирак

РУБРИКА ГРНТИ: 45.31.31 Электрические аппараты низкого напряжения
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: В 2020 году Всемирная организация здравоохранения объявила мировую пандемию коронавируса (Covid-19). С тех пор социальное дистанцирование и стерилизация стали необходимыми мерами предосторожности для уменьшения распространения инфекции. Риск распространения коронавируса побудил людей, промышленные предприятия, а также правительства внедрить несколько способов контроля над скоростью распространения вируса. Во время своей повседневной деятельности на работе, в магазинах, при приготовлении пищи и пр. люди прикасаются к большому количеству предметов, а также открывают большое количество дверей. А именно это и считается одним из самых быстрых способов распространения вирусов, поскольку многие люди трогают дверные ручки, которые в основном не так часто дезинфицируются.

Методы: В данной статье представлено применение выгодного умного устройства, которое распыляет спирт на дверную ручку после каждого контакта. Датчик обнаруживает прикосновение руки к ручке, после чего посылает сигнал в Arduino для обработки, а Arduino после 4,5 секунд посылает сигнал водяному насосу, который через сопло направляет струю прямо на ручку.

Результаты: Устройство показывает верные и точные результаты, учитывая количество контактов и температуру окружающей среды.

Выводы: Система хорошо подходит для применения в офисах и общественных зданиях. Благодаря своей функциональности она превосходно помогает уменьшить загрязнение дверных ручек.

Ключевые слова: умный стерилизатор, Arduino, приводы, дверная ручка, водяной насос.

ДИЗАЈН И ПРИМЕНА ПАМЕТНОГ УРЕЂАЈА ЗА СТЕРИЛИЗАЦИЈУ У РЕШАВАЊУ ПРОБЛЕМА КОНТАМИНАЦИЈЕ КВАКА НА ВРАТИМА

Ихаб Абдулрахман Сатам[а], **аутор за преписку**, Мохамед У. Заенал[б]

[а] Северни технички универзитет, Одсек за електронске технике,
Мосул, Нинива, Република Ирак;
Универзитет Обуда, Школа докторских безбедносних студија,
Будимпешта, Мађарска

[б] Универзитетски колеџ Ал-Калам, Рачунарско-технички одсек,
Киркук, Република Ирак

ОБЛАСТ: рачунарске науке, електротехника
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Светска здравствена организација је 2020. године прогласила пандемију вируса корона (ковид 19). Од тада је држање социјалне дистанце и стерилизација од суштинске важности јер представља превентиву за смањивање инфекције. Ризик од ширења ковид вируса навео је појединце, индустрије и владе да примене различите начине како би се брзина трансмисије вируса држала под контролом. Током свакодневних активности, попут обављања посла, куповине или припреме хране, људи додирују велики број површина, а нарочито кваке на вратима, што се сматра једним од најбржих начина ширења вируса.

Методе: У раду је предложена примена исплативог паметног уређаја којим се квака на вратима прска етанолом после сваког коришћења. Након што сензор детектује додир по кваци, сигнал се шаље Ардуину на обраду, а након 4,5 секунди он га прослеђује воденој пумпи која кроз млазницу усмерава млаз етанола директно на кваку.

Резултати: Узимајући у обзир број употреба и температуру околине уређај показује прецизне и тачне резултате.

Закључак: Систем је примењив у пословним и јавним зградама. Захваљујући својој функционалности може бити од велике помоћи при смањивању контаминације квака на вратима.

Кључне речи: паметни стерилизатор, Ардуино, актуатори, квака на вратима, водена пумпа.

Paper received on / Дата получения работы / Датум пријема чланка: 19.04.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.06.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24.06.2022.

COMPARISON OF THE CONTINUOUS MODEL AND THE FINITE ELEMENT MODEL OF THE GANTRY CRANE CARRYING STRUCTURE FOR MODAL ANALYSIS

Rade R. Vasiljević
Faculty of Maritime Academic Studies, Belgrade, Republic of Serbia,
e-mail: r.r.vasiljevic@gmail.com,
ORCID iD: https://orcid.org/0000-0003-0458-8545

DOI: 10.5937/vojtehg70-36051; https://doi.org/10.5937/vojtehg70-36051

FIELD: Mechanical engineering, Transportation devices, Mechanics
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: To study the adequacy of applying numerical methods in the modal analysis of complex carrying structures of cranes.

Methods: Comparative application of the analytical method and the numerical method - FEM.

Results: Some comparative values of the modal parameters were obtained both analytically and numerically for the derived solution of a gantry crane carrying structure.

Conclusion: It is shown that the numerical method can give a reliable general quality estimate of the structural behaviour of a complex carrying structure from the aspect of modal analysis.

Key words: Carrying structure, modal analysis, analytical method, FEM, frequencies.

Introduction

The problem of structural dynamics is of great importance in constructions and design engineering. Modal analysis of conceptual designs of carrying structures of hoisting machinery is the first and most essential element of dynamic analysis for the estimation of their dynamic stability. The process of determining eigenvalues in complex systems with a large number of degrees of freedom is the most expensive phase in dynamic analysis (Ćorić et al, 1998). The first motive for making this paper is the development of a model of a gantry crane with one pair of rigid legs and the second pair of hinge-elastic legs for modal analysis. Modal analysis and continuation of the analysis of dynamic behaviour should enable the design of a light and reliable structure. The second motive of this paper is to present a modern approach to problems in the dynamics of structures. According to the authors, this type of the gantry crane structure has not been researched so far.

In older research works, the determination of natural frequencies of complex carrying structures was based on the use of approximate expressions and methods (Filippov, 1970). Analytic determination of natural frequencies was limited to simple carrying structures (e.g. simple beam and cantilever). In a complex elastic system, solving the frequency equation was difficult because it contains trigonometric and hyperbolic functions. Today, mathematical software packages (e.g. Mathematica, MATLAB, and the others) enable easy solving of the frequency equation of the oscillation of complex elastic systems. recise determination of natural frequencies is fundamental from the aspect of optimizing carrying structures. The method with distributed masses has been treated in numerous literature books, e.g. (Karanovsky & Lebed, 2001; Krodkiewski, 2008).

However, the use of analytical methods in complex carrying structures is still limited. In this case, for determining the natural frequencies of a carrying structure, some of the numerical methods are used. The main advantage of numerical methods is that very complex structures can be viewed as reduced models whose analysis from the aspect of engineering accuracy is sufficient to evaluate the behaviour of complex structures. Today, the method with consistent masses is very common. For more details on the finite element method (FEM), see (Bathe, 2016; Zienkiewicz et al, 2005; Zaimović-Uzunović & Lemeš, 2002).

Analytical and numerical methods for structural dynamics are considered in a number of papers. In the first selected paper (Alexandropoulo et al, 1986), for a simple elastic system (a simple frame with two elements), the effect on the bending eigenfrequencies of the longitudinal motion, alone or in combination with other parameters, is thoroughly discussed. In the paper (Oguamanam et al, 2001), the dynamics of a 3D model of an overhead crane system is considered. The transverse and longitudinal vibrations of a frame structure caused by a moving trolley and a hoisted object using a moving finite element are treated by (Wu, 2008). The paper (Lazarević & Lazarević, 2018), deals with the research into the dynamic characteristics (natural frequencies and movements) of hydraulic excavators. A comparative approach of analytical and numerical solutions for a jib crane system was explored in (Umar et al, 2019). The paper (Vasiljević, 2019) focused on comparative modal analysis of the portals of a type “H” and “X” portal cranes. In a recent paper, (Milana et al, 2021) investigates the moving load problem for the lifting boom of a ship unloader.

Description of the problem

In this paper, the object of the research is a double girder gantry crane with one side cantilever. Depending on the main girder support method, gantry cranes can be executed in two ways, as follows:

- with both pairs of rigid legs, and
- with one pair of rigid legs and the second pair of hinge-elastic legs.

Gantry cranes with both rigid legs are simpler from the aspect of the complexity of the carrying structure. So, in papers from the field of dynamic analysis of gantry cranes, subject studies were only gantry cranes with rigid connections of both pairs of legs with the main girders. For this reason, the author of this paper has opted for a modal analysis of the carrying structure of gantry cranes with one rigid connection and one flexible (hinged) connection of the legs with the main girders (Figure 1). For more details on gantry cranes, see (Ostrić & Tošić, 2005).

The carrying structure of a gantry crane (Figure 1) consists of two main box girders which are on ends connected to crossbars. The main girders rely on the boxed legs, one of which is rigid and the other hinge-elastic. The flexible (hinged) connection is located at the cantilever of the main girder. The rigid leg receives influences from the trolley braking, while both legs receive the influence from the crane braking.

This type of the carrying structure of the gantry crane is shown in Figure 2. For the defined type of the gantry crane carrying structure, modal analysis will be conducted in the following sections. In this paper, the modal analysis considering the gantry crane was conducted analytically and numerically. In the first step, the continuous model is presented, i.e. the analytical approach for modal analysis. In the second step, the finite element models are presented, i.e. the numerical approach for modal analysis.

To obtain all eigenvalues and eigenvectors, it is necessary to perform a large number of numerical operations. In order to reduce the scope of dynamic calculation, only the adequate eigenvectors are selected. The mode shape with a frequency close to the frequency of load of most influence on the dynamic response of the system is defined as dynamic load and assumed to be the dominant mode shape.

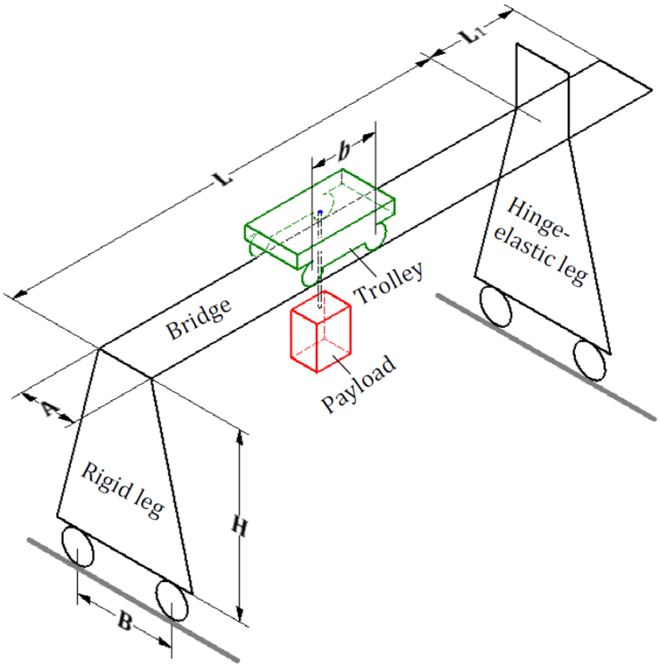


Figure 1 – Sketch of a gantry crane system
Рис. 1 – Эскиз системы козлового крана
Слика 1 – Скица система рамне дизалице

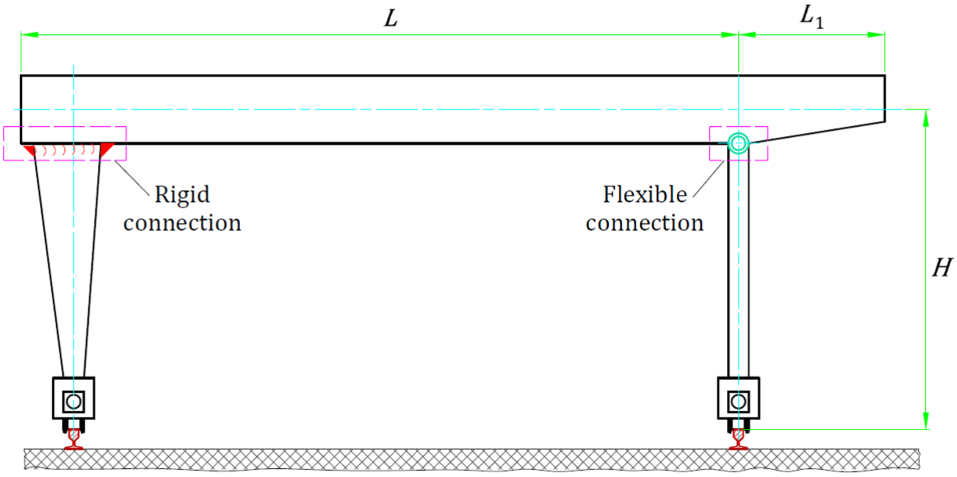


Figure 2 – Type of the carrying structure of the gantry crane
Рис. 2 – Тип несущей конструкции козлового крана
Слика 2 – Тип носеће конструкције рамне дизалице

Continuous model

The continuous model of the gantry crane carrying structure was adopted (Figure 3). The continuous model is a model with uniformly distributed masses. This model is a plane frame with the following assumptions (idealization):

- the material of the elements is homogeneous and isotropic,
- the main structural elements are uniform beams,
- the elements are significant by the transverse oscillation in the Bernoulli-Euler beam theory,
- the transverse displacements of the center of the section are normal to the longitudinal axis and small in relation to the length of the element, and
- the cross-sections of the elements remain plane and normal to the elastic line.

The axial and shear deformations and the influences of rotation inertia can be ignored due to the known structural behaviour of gantry cranes.

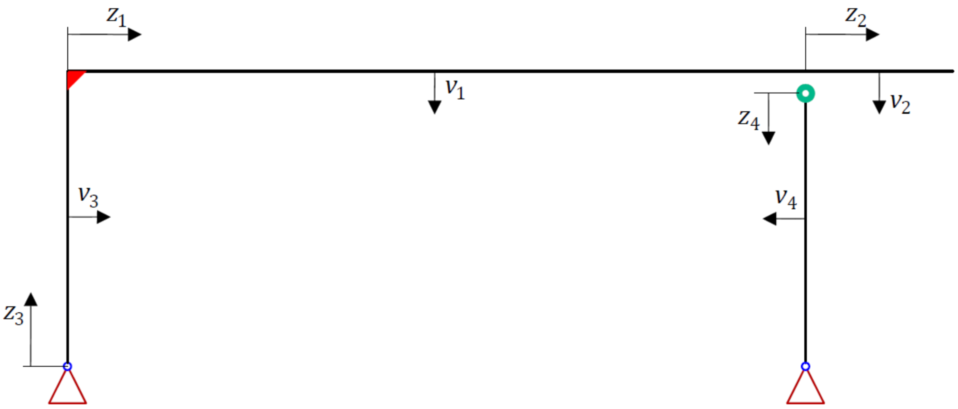


Figure 3 – Continuous model
Рис. 3 – Непрерывная модель
Слика 3 – Континуални модел

Partial differential equations of free undamped transverse oscillations of the frame elements read:

$$\frac{\partial^2 v_i(z,t)}{\partial t^2}+c^2\frac{\partial^4 v_i(z,t)}{\partial z^4}=0, \quad i=1,2,3,4. \tag{1}$$

The notations in Eq. (1) are as follows:

- $v_i(z,t)$ – transversal displacements of the element i,
- z – spatial coordinate,
- t – time, and
- c – speed of wave propagation.

The speed of wave propagation c is equal:

$$c^2 = \frac{EI_i}{\rho A_i}, \tag{2}$$

where:

- E – elastic modulus,
- ρ – material mass density,
- A_i – area of the cross-section of the element i, and
- I_i – moment of inertia of the cross-section of the element i.

Let us look at the solution of differential equation (1) in the form:

$$v_i\left(z,t\right) = Z_i\left(z\right)T\left(t\right). \tag{3}$$

The notations in Eq. (3) are two functions:

- $Z_i(z)$ – mode shapes of the element i, and
- $T(t)$ – time function.

The transversal displacements for each element of the frame read:

$$\begin{aligned} v_1 &= v_1\left(z,t\right) = Z_1\left(z\right)T\left(t\right), \quad 0 \le z \le L, \\ v_2 &= v_2\left(z,t\right) = Z_2\left(z\right)T\left(t\right), \quad 0 \le z \le L_1, \\ v_3 &= v_3\left(z,t\right) = Z_3\left(z\right)T\left(t\right), \quad 0 \le z \le H, \\ v_4 &= v_4\left(z,t\right) = Z_4\left(z\right)T\left(t\right), \quad 0 \le z \le H. \end{aligned} \tag{4}$$

The functions of the mode shapes and the function of time are equal:

$$\begin{aligned} Z_i\left(z\right) &= C_{1i}\mathrm{ch}(k_i z) + C_{2i}\mathrm{sh}(k_i z) + \\ &\quad + C_{3i}\cos(k_i z) + C_{4i}\sin(k_i z), \\ T\left(t\right) &= B_1\cos(\omega t) + B_2\sin(\omega t). \end{aligned} \tag{5}$$

Due to the complexity of the elastic system, the functions $Z_i(z)$ will be presented by Krylov functions:

$$\begin{aligned} Z_i\left(z\right) &= C_{1i}S(k_i z) + C_{2i}T(k_i z) + \\ &\quad + C_{3i}U(k_i z) + C_{4i}V(k_i z). \end{aligned} \tag{6}$$

The circular frequency ω in the time function in Eq. (5) is equal to:

$$\omega = ck_i^2 = k_i^2\sqrt{\frac{EI_i}{\rho A_i}}. \tag{7}$$

The frequency of the oscillation *f* is calculated by the expression:

$$f = \frac{\omega}{2\pi} = \frac{k_i^2}{2\pi}\sqrt{\frac{EI_1}{\rho A_1}}. \tag{8}$$

Boundary conditions

As the structure consists of four beam elements, it is necessary to define sixteen boundary conditions. The boundary conditions can be (Karanovsky, 2004):

- geometric boundary conditions (deflections and inclinations), and
- load boundary conditions (transverse forces and bending moments).

On the support of the rigid leg (element 3) there are two boundary conditions:

$$Z_3(0) = 0, \tag{9.1}$$

$$-EI_3Z_3'(0) = 0. \tag{9.2}$$

At the location of the rigid connection between the main girder and the rigid leg (elements 1 and 3), there are three boundary conditions:

$$Z_3(0) = 0, \tag{9.3}$$

$$-EI_3Z_3''(0) = 0, \tag{9.4}$$

$$-EI_1Z_1''(0) = -EI_3Z_3''(0). \tag{9.5}$$

At the location of the rigid connection between the main girder and the cantilever (elements 1 and 2), there are four boundary conditions:

$$Z_2(0) = 0, \tag{9.6}$$

$$Z_1(L) = 0, \tag{9.7}$$

$$Z_1'(L) = Z_2'(0), \tag{9.8}$$

$$-EI_1Z_1''(L)=-EI_2Z_2''(0). \qquad (9.9)$$

At the end of the cantilever (element 2), there are two boundary conditions:

$$-EI_2Z_2''(L_1)=0, \qquad (9.10)$$

$$-EI_2Z_2'''(L_1)=0. \qquad (9.11)$$

At the location of the flexibly connection between the main girder and the hinge leg (elements 1 and 4), the following boundary condition is valid:

$$-EI_4Z_4''(0)=0. \qquad (9.12)$$

On the support of the hinge leg (element 4), there are two boundary conditions:

$$Z_4(H)=0, \qquad (9.13)$$

$$-EI_4Z_4''(H)=0. \qquad (9.14)$$

The boundary condition on the basis of equality displacements of the end of rigid leg and the end of hinge-elastic leg reads:

$$Z_3(H)=Z_4(0). \qquad (9.15)$$

Finally, the dynamic boundary condition on the basis of the Law on motion of the centre of mass of the main girder (element 1) and the action of the transverse forces at the places of its connection with the rigid leg and the hinge leg (elements 3 and 4) reads:

$$-\rho(A_1L+A_2L_1)\ddot{v}_4(0,t)=EI_3v_3'''(H,t)+EI_4v_4'''(0,t). \qquad (9.16i)$$

This condition, after replacing v_3 and v_4 for Eq. (4) and Eq. (6) in Eq. (9.16i), obtains the following form:

$$\rho(A_1L+A_2L_1)Z_4(0)\omega^2=EI_3Z_3'''(H)+EI_4Z_4'''(0). \qquad (9.16)$$

Frequency equation

From Eq. (7), the characteristic values k_i defined by k_1:

$$k_i = k_1 \sqrt[4]{\frac{A_i I_1}{A_1 I_i}} = k_1 \xi_i, i = 1, 2, 3, 4. \tag{10}$$

From the defined boundary conditions (Eqs. (9.1-9.16)), a homogeneous system of linear equations is formed, from which the frequency equation follows:

$$\det(F) = 0. \tag{11}$$

The notice *F* in Eq. (11) is defined by Eq. (12) and Eqs. (13.1) to (13.11). The frequency equation is very complex because the combinations of trigonometric and hyperbolic functions depend on a number of parameters, so that its solution in the algebraic form cannot be found.

$$\left[F\right]_{11\times 11} = \left[F_1\ F_2\ F_3\ F_4\ F_5\ F_6\ F_7\ F_8\ F_9\ F_{10}\ F_{11}\right]. \tag{12}$$

The vectors F_i in Eq. (12) read:

$$F_1 = \left\{-1 0\ T\left(k_1 L\right) S\left(k_1 L\right) V\left(k_1 L\right) 0\,0\,0\,0\,0\,0\right\}^T, \tag{13.1}$$

$$F_2 = \left\{0 - l_1\, U\left(k_1 L\right) T\left(k_1 L\right) S\left(k_1 L\right) 0\,0\,0\,0\,0\,0\right\}^T, \tag{13.2}$$

$$F_3 = \left\{0\,0\, V\left(k_1 L\right) U\left(k_1 L\right) T\left(k_1 L\right) 0\,0\,0\,0\,0\,0\right\}^T, \tag{13.3}$$

$$F_4 = \left\{0\,0\,0 - \xi_2\ 0\, V\left(k_1 L\right) U\left(k_1 L\right) 0\,0\,0\,0\right\}^T, \tag{13.4}$$

$$F_5 = \left\{0\,0\,0\,0 - \frac{I_2}{I_1} \xi_2^2\ S\left(k_1 L\right) V\left(k_1 L\right) 0\,0\,0\,0\right\}^T, \tag{13.5}$$

$$F_6 = \left\{0\,0\,0\,0\,0\, T\left(k_1 L\right) S\left(k_1 L\right) 0\,0\,0\,0\right\}^T, \tag{13.6}$$

$$\begin{gathered} F_7 = \left\{\xi_3 S\left(k_1 \xi_3 H\right) I_3 \xi_3^2 V\left(k_1 \xi_3 H\right) 0\,0\,0\,0\,0\,0\,0 \right. \\ \left. T\left(k_1 \xi_3 H\right) I_3 \xi_3^2 U\left(k_1 \xi_3 H\right)\right\}^T, \end{gathered} \tag{13.7}$$

$$F_8 = \left\{ \xi_3 U\left(k_1\xi_3 H\right) I_3 \xi_3^2 T\left(k_1\xi_3 H\right) 0\,0\,0\,0\,0\,0\,0 \; V\left(k_1\xi_3 H\right) I_3 \xi_3^2 S\left(k_1\xi_3 H\right) \right\}^T , \tag{13.8}$$

$$F_9 = \left\{ 0\,0\,0\,0\,0\,0\,0\, S\left(k_1\xi_4 H\right) U\left(k_1\xi_4 H\right) \; -1\, k_1 \frac{I_1}{A_1}\left(A_1 L + A_2 L_1\right) \right\}^T , \tag{13.9}$$

$$F_{10} = \left\{ 0\,0\,0\,0\,0\,0\,0\, T\left(k_1\xi_4 H\right) V\left(k_1\xi_4 H\right) 0\,0 \right\}^T , \tag{13.10}$$

$$F_{11} = \left\{ 0\,0\,0\,0\,0\,0\,0\, V\left(k_1\xi_4 H\right) T\left(k_1\xi_4 H\right) 0\,0 \right\}^T . \tag{13.11}$$

Finite element models

For the gantry crane carrying structure, the finite element models were adopted:

- Case I: model with 7 finite elements (Figure 4), and
- Case II: model with 14 finite elements (Figure 5).

The finite element model is a model with consistent masses. The models are plane frames divided into beam finite elements (plane-frame element).

This element was adopted based on the following assumptions:

- the axial deformations of the elements are in accordance with Hooke's law, and
- the transverse deformations of the elements are in accordance with the Bernoulli-Euler theory.

The adopted finite element is a combination of a plane element of the bar type and the element of the carrier type. All elements of the plane frame are made of steel. The basic characteristics (mechanical and static) of the element *i* are:

- ρ_i – mass density of the material,
- E – elastic modulus,
- A_i – area of the cross-section, and
- I_i – moment of inertia of the cross-section.

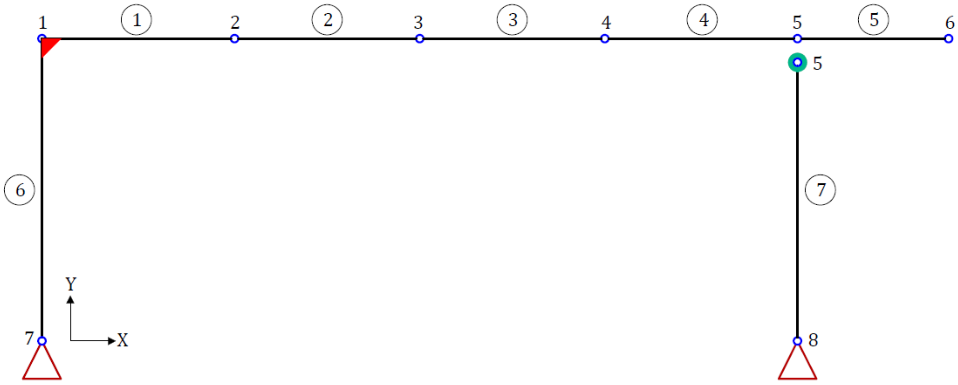


Figure 4 – Finite element model – 7 FE
Рис. 4 – Конечно-элементная модель – 7 КЭ
Слика 4 – Коначноелементни модел – 7 КЕ

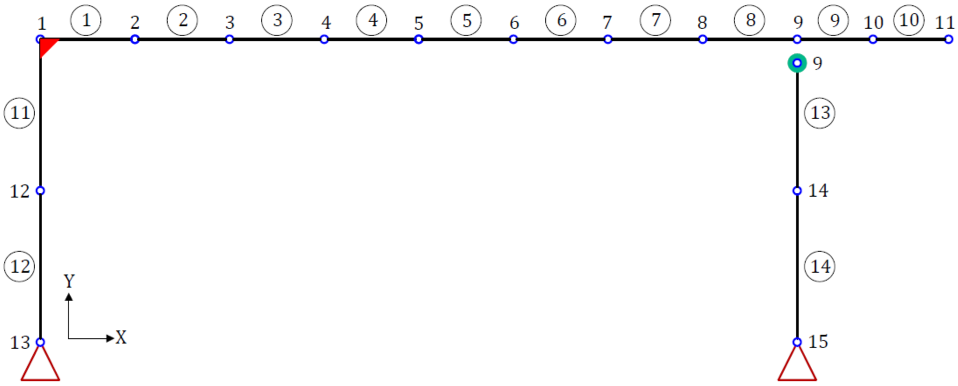


Figure 5 – Finite element model – 14 FE
Рис. 5 – Конечно-элементная модель – 14 КЭ
Слика 5 – Коначноелементни модел – 14 КЕ

The numerical method consists of determining the inertial load along the element during the movement of the girder, and then replacing the inertial load with the equivalent nodal load.

The formed reduced models are coarse models based on the methodology of the reduction of the number of degrees of freedom of the node, so the box-section is replaced by a beam element.

The carrying structure is modelled with two types of beam finite elements:

- finite element *ik* - type (Figure 6a), and
- finite element *ig* - type (Figure 6b).

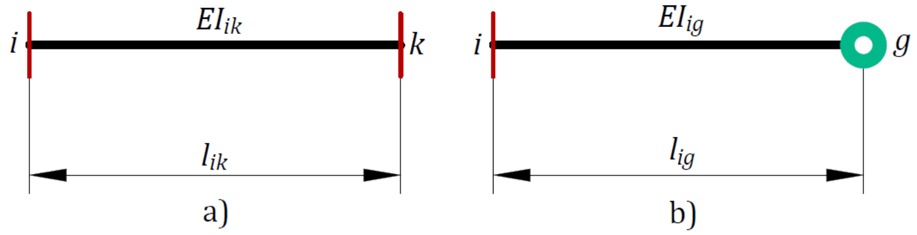


Figure 6 – Types of finite elements
Рис. 6 – Типы конечных элементов
Слика 6 – Типови коначних елемената

The beam element type *ik* is a planar frame element with 3DOF in each node. The beam element type *ig* is a planar frame element with 3DOF in the first node and 2DOF in the second node.

In case I, the girder of the carrying structure is divided into 5 finite elements, while both legs were modelled as one finite element.

In case II, the girder of the carrying structure is divided into 10 finite elements, while both legs were modelled as 2 finite elements.

The formed finite element models of the structure are relatively simple, but they enable sufficiently accurate static and dynamic analyses. In research, this is a common measure of discretization. Furthermore, increase in the number of finite elements relate to an increase in the number of programming operations. Also, the time required to obtain the dynamic parameters in the software package increases.

For the restrained element on both sides of the constant cross-section, the vector of the interpolation functions reads:

$$N_{ik}^{T}=\begin{bmatrix} 1-\xi & 0 \\ 0 & 1-\xi^{2}+2\xi^{3} \\ 0 & l\left(\xi-2\xi^{2}+\xi^{3}\right) \\ \xi & 0 \\ 0 & \xi^{2}+2\xi^{3} \\ 0 & l\left(2\xi^{2}+\xi^{3}\right) \end{bmatrix},\quad \xi=\frac{x}{l}. \qquad (14)$$

For the element that is on the one side restrained and on the other side with a hinge connection, with a constant cross section, the vector of the interpolation functions reads:

$$N_{ig}^{T} = \begin{bmatrix} 1-\xi & 0 \\ 0 & 1-\frac{3}{2}(\xi)^{2}+\frac{1}{2}(\xi)^{3} \\ 0 & x-\frac{3}{2}l(\xi)^{2}+\frac{1}{2}l(\xi)^{3} \\ \xi & 0 \\ 0 & \frac{3}{2}(\xi)^{2}-\frac{1}{2}(\xi)^{3} \end{bmatrix},\ \xi=\frac{x}{l}. \qquad (15)$$

The corresponding matrix of masses and stiffness of the line element *i* are defined on the basis of the interpolation functions (Eq. (14) or Eq. (15)) and their first and second derivatives and they read:

$$M_{i} = \int_{V} \rho N^{T} N dV, \qquad (16)$$

$$K_{i}^{a} = \int_{V} E N^{'T} N^{'} dV; \quad K_{i}^{t} = \int_{V} E N^{''T} N^{''} dV. \qquad (17)$$

The transformation matrix element of the type *ik* is:

$$T_{ik} = \begin{bmatrix} \cos\theta & -\sin\theta & 0 & 0 & 0 & 0 \\ \sin\theta & \cos\theta & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cos\theta & \sin\theta & 0 \\ 0 & 0 & 0 & -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad (18)$$

while the transformation matrix element of the type *ig* is:

$$T_{ig}=\begin{bmatrix}\cos\theta & -\sin\theta & 0 & 0 & 0\\ \sin\theta & \cos\theta & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & \cos\theta & \sin\theta\\ 0 & 0 & 0 & -\sin\theta & \cos\theta\end{bmatrix} \quad (19)$$

The symbol *θ* in Eq. (18) and Eq. (19) takes the following values:

- Case I: *θ*=0° for *i*=1…5; *θ*=270° for *i*=6; *θ*=90° for *i*=7.
- Case II: *θ*=0° for *i*=1…10; *θ*=270° for *i*=11,12; *θ*=90° for *i*=13,14.

The mass matrix in the global coordinate system is equal to:

$$M_i^G = T_i^T M_i T \quad (20)$$

The stiffness matrix in the global coordinate system is equal to:

$$K_i^G = T_i^T K_i T \quad (21)$$

- Case I:

$$M = \sum_i^7 M_i, \quad (20.I)$$

$$K = \sum_i^7 K_i \quad (21.I)$$

- Case II:

$$M = \sum_i^{14} M_i, \quad (20.II)$$

$$K = \sum_i^{14} K_i \quad (21.II)$$

Similarly to the system mass matrix, the system stiffness matrix is also decomposed into submatrices. The submatrix of the system mass matrix by the unknown M_{nn} is obtained by decomposing the matrix in Eq. (20.I) or in Eq. (20.II), while the submatrix of the system stiffness matrix per the unknown K_{nn} is obtained by decomposing the matrix in Eq. (21.I) or the matrix in Eq. (21.II).

The circular frequencies of the carrying structure are obtained by solving the algebraic equations:

$$\det\left(K_{nn} - \omega^2 M_{nn}\right) = 0 \tag{22}$$

Equation (22) is complex.

Numerical example

On the theoretical basis given in the previous sections, a numerical example was given for the derived solution for a gantry crane (Mašinska industrija Niš – Fabrika dizalica, 1981).

Starting data

Table 1 gives the general information about the gantry crane.

Table 1 – General information about the gantry crane
Таблица 1 – Общие сведения о козловом кране
Табела 1 – Опште информације за рамну дизалицу

Technical characteristics	Value
Payload, *Q*	10 [t]
Span of the main girder, *L*	20 [m]
Span of the cantilever, L_1	4 [m]
Height of legs, *H*	8 [m]

The material of the carrying structure is steel S235J2G3. The main mechanical characteristics of the carrying structure are equal: E=2.1×10^{11} N⁄m^2; ρ=7850 kg⁄m^3.

Figure 7 shows the cross-sections of the main girder, the rigid leg and the hinge-elastic leg.

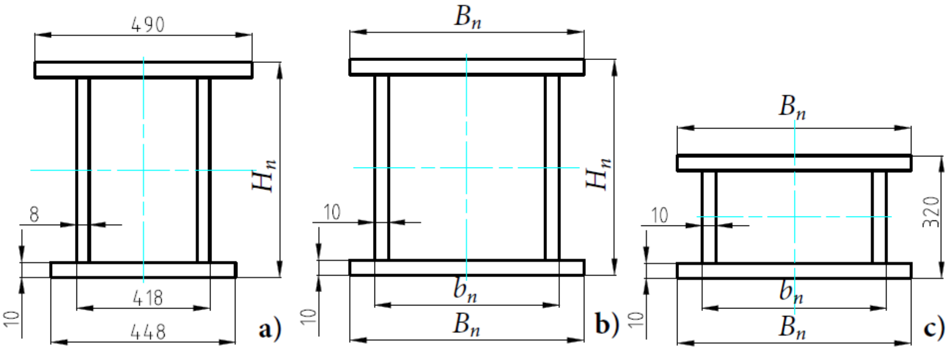


Figure 7 – The cross sections: a) main girder, b) rigid leg, c) hinge-elastic leg
Рис. 7 – Поперечные сечения: а) главной балки, б) жесткой опоры, в) шарнирно-подвижной опоры
Слика 7 – Попречни пресеци: а) главни носач, б) крута нога, в) зглобно-еластична нога

Results of the continuous model

Table 2 presents the data for the continuous model of the carrying structure of the gantry crane.

Table 2 – Characteristics of the continuous model
Таблица 2 – Характеристики непрерывной модели
Табела 2 – Карактеристике континуалног модела

Element (*i*)	l_i [m]	H_n [mm]	B_n [mm]	b_n [mm]
1	Z_1	1000	-	-
2	Z_2	851	-	-
3	Z_3	570	587.5	557.5
4	Z_4	-	603.5	573.5

Frequency equation (12) is solved using Mathematica software (Wolfram Research, Nd). In the first step, the characteristic values of k_1 of the frequency equation are graphically determined (Figure 8).

In the second step, the characteristic values of k_1 are localized first and then their exact values are determined using the command *FindRoot*. The first four values are k_1={0.0808, 0.16794, 0.23261, 0.2955}. Based on the characteristic values of k_1, according to Eq. (7), the first four own circular frequencies of the model of the gantry crane carrying structure are determined (Table 3).

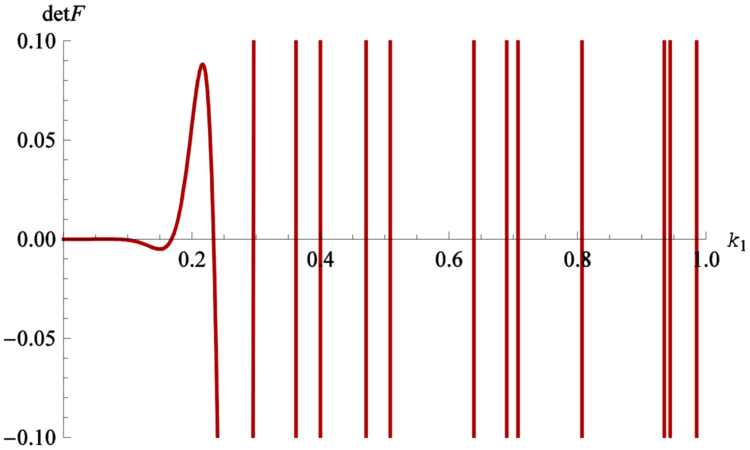


Figure 8 – Dependence of detF on k_1
Рис. 8 – Зависимость detF от k_1
Слика 8 – Зависност detF од k_1

Table 3 – Frequencies of the continuous model
Таблица 3 – Частоты непрерывной модели
Табела 3 – Фреквенције континуалног модела

Mode No	Circular frequency [rad/s]	Frequency [Hz]	Period [s]
1st	12.710	2.023	0.4943
2nd	54.882	8.735	0.1145
3rd	106.146	16.894	0.0592
4th	169.999	27.056	0.0367

Results of the finite element model

■ Case I

Table 4 presents the data for the FE model with 7 finite elements of the gantry crane carrying structure.

Table 4 – Characteristics of the model with 7 finite elements
Таблица 4 – Характеристики модели с 7 конечными элементами
Табела 4 – Карактеристике модела са 7 коначних елемената

Element (*i*)	l_i [m]	H_n [mm]	B_n [mm]	b_n [mm]
1…4	5	1000	-	-
5	4	851	-	-
6	8	570	587.5	557.5
7	8	-	603.5	573.5

Due to its complexity, equation (22) for case I is solved through the programming code “RV.ModAn-FEM7×7” written in a Mathematica software package (Wolfram Research, Nd).

Table 5 shows the values of the first four frequency oscillating carrying structures of the gantry crane (model I - with 7 finite elements).

Table 5 – Frequencies of the model with 7 finite elements
Таблица 5 – Частоты моделей с 7 конечными элементами
Табела 5 – Фреквенције модела са 7 коначних елемената

Mode No	Circular frequency [rad/s]	Frequency [Hz]	Period [s]
1st	11.818	1.881	0.5317
2nd	54.682	8.703	0.1149
3rd	140.334	22.335	0.0448
4th	170.249	27.096	0.0369

■ Case II

Table 6 presents the data for the FE model with 14 finite elements of the gantry crane carrying structure.

Table 6 – Characteristics of the model with 14 finite elements
Таблица 6 – Характеристики модели с 14 конечными элементами
Табела 6 – Карактеристике модела са 14 коначних елемената

Element (*i*)	l_i [m]	H_n [mm]	B_n [mm]	b_n [mm]
1...8	2.5	1000	-	-
9…10	2	851	-	-
11…12	4	570	587.5	557.5
13…14	4	-	603.5	573.5

Analogically, equation (22) for case II, due to the complexity, is solved through the programming code “RV.ModAn-FEM14×14” written in Mathematica software.

Table 7 shows the values of the first four frequency oscillating carrying structures of the gantry crane (model II - with 14 finite elements).

Table 7 – Frequencies of the model with 14 finite elements
Таблица 7 – Частоты моделей с 14 конечными элементами
Табела 7 – Фреквенције модела са 14 коначних елемената

Mode No	Circular frequency [rad/s]	Frequency [Hz]	Period [s]
1st	12.525	1.993	0.5016
2nd	56.226	8.949	0.1117
3rd	109.350	17.404	0.0575
4th	168.327	26.790	0.0373

Mode shapes

Figures 9 and 10 present the shapes of the first two eigenmodes of the oscillation of the carrying structure of the considered type of the gantry crane.

There are two main mode shapes of the considered structure which are of the greatest significance for the analysis of the structure dynamic behaviour. The first mode shape is called the basic form of oscillation.

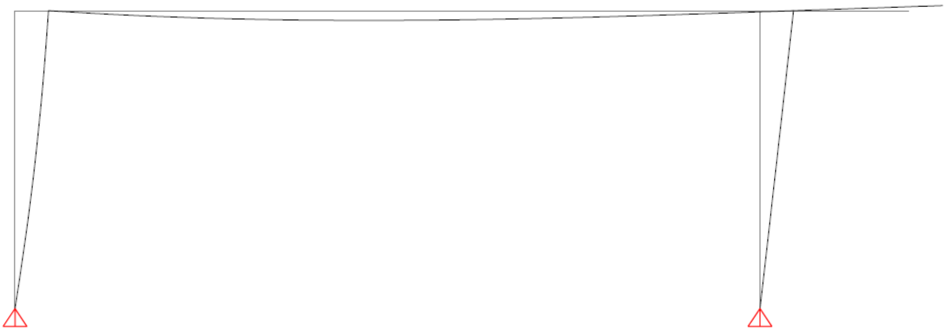


Figure 9 – 1st mode shape of the crane carrying structure
Рис. 9 – 1 форма колебаний несущей конструкции крана
Слика 9 – Први облик осциловања носеће конструкције дизалице

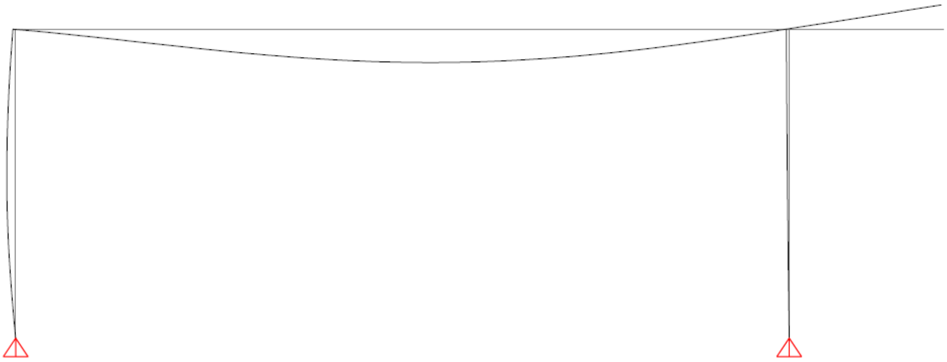


Figure 10 – 2nd mode shape of the carrying structure
Рис. 10 – 2 форма колебаний несущей конструкции крана
Слика 10 – Други облик осциловања носеће конструкције дизалице

Analysis of the results

The analysis of the results shows that the results for the natural frequencies of the numerical method correspond well with the results of the analytical method. For a greater accuracy in numerical methods, it is necessary to apply a greater number of finite elements.

From the aspect of modal analysis, the worst dynamic behaviour of the construction is reflected in the first mode of oscillation. Also, based on the same aspect, a good dynamic behaviour requests high first frequency. The first lowest (basic) vibration frequency of the gantry crane carrying structure is within the limits of 0.5-3.5 Hz, so the condition for small mass, or its slimness, is fulfilled. In accordance with these conclusions, the carrying structure of the considered gantry crane has the necessary dynamic stability.

The diagram in Figure 11 shows the influence of the number of finite elements of the carrying structure of the gantry crane on the accuracy results of the numerical method. This influence is particularly expressed in the third mode. Of particular importance is the accuracy of the first mode of oscillation.

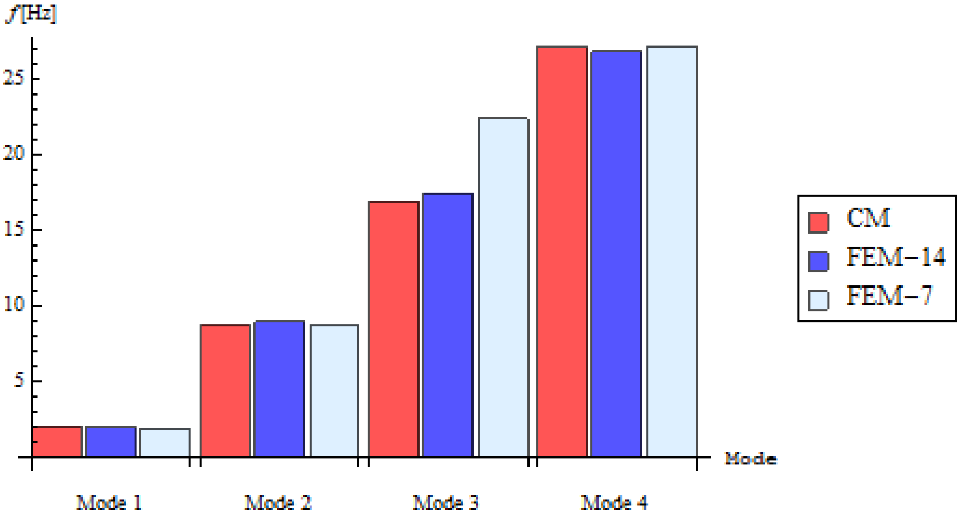


Figure 11 – Influence of the number of finite elements on the accuracy results
Рис. 11 – Влияние количества конечных элементов на точность результатов
Слика 11 – Утицај броја коначних елемената на тачност резултата

Based on the results in the previous section, Table 8 shows the comparative results for the first four natural frequencies of the mathematical model. The disparity between the analytical method (AM) and the FEM method is calculated according to the expression:

$$D = \frac{AM - FEM}{AM} 100\ \%$$

Table 8 – Comparative values of the frequencies for the two models
Таблица 8 – Сравнительные значения частот по двум моделям
Табела 8 – Упоредне вредности фреквенција за два модела

Frequency [Hz]	Continuous model	Finite element model – 14 FE	Disparity [%]
f_1	2.023	1.993	1,48
f_2	8.735	8.949	-2,45
f_3	16.894	17.404	-3,02
f_4	27.056	26.790	0,98

Comparing the values of the natural frequencies obtained by the analytical method with those obtained by the numerical method leads to the conclusion that the maximum relative error for the first two modes is 1.48% and 2.45%. The results for the first and fourth frequencies match best.

Conclusion

The conclusions of the comparison of the continuous model and the finite element model of the carrying structure of a double girder gantry crane with one cantilever for modal analysis are:

- Analytical approach is recommended for structures where it is possible to find solutions of dynamic parameters in the analytical form;
- It is shown that the priority of the numerical approach is reflected in its possibility to view very complex structures as reduced models whose analysis results in an estimate that is precise enough from the aspect of engineering accuracy;
- In the numerical method, it has been shown with high accuracy that the results are obtained by dividing a discretized model into a high number of finite elements;
- It is shown that it is possible to detect the causes of undesirable behaviour of a structure with the numerical method;
- It is shown that the numerical method can provide a reliable general estimate of the quality of structural behaviour from the aspect of modal analysis;
- It was determined that the values of the modal parameters obtained by the analytical method and the numerical method (FEM) coincide well from the aspect of engineering accuracy;
- For the first mode, a relative error of natural frequencies obtained by the FEM (method with consistent masses) in relation to the exact value (method with distributed masses) amounts to 1.48%;
- The study in this paper can be useful in selecting methods for researching dynamic behaviours of carrying structures.

References

Alexandropoulo, A., Michaltsos, G. & Kounadis, A. 1986. The effect of longitudinal motion and other parameters on the bending eigenfrequencies of a simple frame. *Journal of Sound and Vibration*, 106(1), pp.153-159. Available at: https://doi.org/10.1016/S0022-460X(86)80179-1.

Bathe, K-J. 2016. *Finite Element Procedures.* New Jersey: Prentice-Hall. ISBN: 978-0-9790049-0-2.

Ćorić, B., Ranković, S. & Salatić, R. 1998. *Dinamika konstrukcija.* Belgrade: University of Belgrade (in Serbian). ISBN: 8681019732 9788681019733.

Filippov, A.P. 1970. *Vibration of deformable systems.* Moscow: Mashinostroenie (in Russian).

Karanovsky, I.A. & Lebed, O.I. 2004. *Formulas for Structural Dynamics: Tables, Graphs and Solutions, 1st Edition.* New York: McGraw-Hill.

Krodkiewski, J.M. 2008. *Mechanical vibration.* Melbourne: University of Melbourne. ISBN: 0-7325-1536-X.

Lazarević, Ž. & Lazarević, B. 2018. Determining the dynamic characteristics of hydraulic excavators. *Vojnotehnički glasnik/Military Technical Courier*, 66(1), pp.41-62. Available at: https://doi.org/10.5937/vojtehg66-14400.

-Mašinska industrija Niš - Fabrika dizalica. 1981. *Projekat portalne dizalice nosivosti 10 t i raspona 20+4 m - PD-083.* Niš, Serbia: Mašinska industrija Niš - Fabrika dizalica (in Serbian).

Milana, G., Banisoleiman, K. & Gonzalez, A. 2021. An investigation into the moving load problem for the lifting boom of a ship unloader. *Engineering Structures*, 234(art.number:111899), pp.1-20. Available at: https://doi.org/10.1016/j.engstruct.2021.111899.

Oguamanam, D.C.D., Hansen, J.S. & Heppler, G.R. 2001. Dynamics of a three-dimensional overhead crane system. *Journal of Sound and Vibration*, 242(3), pp.411-426. Available at: https://doi.org/10.1006/jsvi.2000.3375.

Ostrić, D. & Tošić, S. 2005. *Dizalice.* Belgrade: University of Belgrade, Faculty of Mechanical Engineering (in Serbian). ISBN: 978-86-7083-520-7.

Umar, S.U., Hamisu, M.T., Jamil, M.M. & Sa'ad, A. 2019. Dynamic responses of structures to moving bodies using combined finite element and analytical methods. *Journal of Mechanical Design and Vibration*, 7(1), pp.33-42. Available at: https://doi.org/10.12691/jmdv-7-1-5.

Vasiljević, R. 2019. Comparative Modal Analysis of the Portals of a Type “H” and “X” Portal Cranes. *IMK–14 Research & Development in Heavy Machinery*, 25(1), pp.13-20. Available at: https://doi.org/10.5937/IMK1901013V.

-Wolfram Research. Nd(a). *FindRoot, Wolfram Language function,* [online] Available at: https://reference.wolfram.com/language/ref/FindRoot.html. [Accessed: 6 june 2021].

-Wolfram Research. Nd(b) *ProceduralProgramming,* [online] Available at: https://reference.wolfram.com/language/guide/ProceduralProgramming.html. [Accessed: 18 October 2021].

Wu, J.J. 2008. Transverse and longitudinal vibrations of a frame structure due to a moving trolley and the hoisted object using moving finite element. *International Journal of Mechanical Sciences*, 50(4), pp.613-625. Available at: https://doi.org/10.1016/j.ijmecsci.2008.02.001.

Zaimović-Uzunović, N. & Lemeš, S. 2002. *Metod konačnih elemenata.* Zenica, Bosnia and Herzegovina: Dom štampe (in Serbian). ISBN: 9958-42-079-1.

Zienkiewicz, O.C., Taylor, R.L. & Zhu, J.Z. 2005. *The Finite Element Method: Its Basis and Fundamentals, Sixth Edition.* Oxford, UK: Elsevier Butterworth-Heinemann. ISBN-13: 978-0-7506-6320-5.

СРАВНЕНИЕ НЕПРЕРЫВНОЙ МОДЕЛИ И КОНЕЧНО-ЭЛЕМЕНТНОЙ МОДЕЛИ НЕСУЩЕЙ КОНСТРУКЦИИ КОЗЛОВОГО КРАНА ДЛЯ ПРОВЕДЕНИЯ МОДАЛЬНОГО АНАЛИЗА

Раде Р. Васильевич

Факультет академических исследований судоходства,
г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 55.03.14 Проектирование, конструирование и расчет машин и механизмов,
55.51.31 Краны и крановое оборудование,
30.03.19 Математические методы механики
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Цель данной статьи заключалась в изучении соответствующего применения численных методов при модальном анализе сложных несущих конструкций кранов.

Методы: В статье применен метод сравнительного анализа и численный метод − МКЭ.

Результаты: С помощью аналитического и численного методов были получены сравнительные значения модальных параметров для примененного решения несущей конструкции козлового крана.

Выводы: Было показано, что численный метод может обеспечить надежную глобальную оценку качества поведения сложной несущей конструкции с точки зрения модального анализа.

Ключевые слова: несущая конструкция, модальный анализ, аналитический метод, МКЭ, частоты.

ПОРЕЂЕЊЕ КОНТИНУАЛНОГ МОДЕЛА И КОНАЧНОЕЛЕМЕНТНОГ МОДЕЛА НОСЕЋЕ КОНСТРУКЦИЈЕ РАМНЕ ДИЗАЛИЦЕ ЗА МОДАЛНУ АНАЛИЗУ

Раде Р. Васиљевић

Висока бродарска школа академских студија, Београд, Република Србија

ОБЛАСТ: машинство, транспортни уређаји, механика
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Циљ рада јесте истраживање адекватности примене нумеричких метода код модалне анализе сложених носећих конструкција дизалица.

Методе: Спроведена је упоредна примена аналитичке и нумеричке методе – МКЕ.

Резултати: Помоћу аналитичког и нумеричког метода добијене су упоредне вредности модалних параметара за изведено решење носеће конструкције рамне дизалице.

Закључак: Показано је да се нумеричком методом може добити поуздана глобална оцена квалитета понашања сложене носеће конструкције са аспекта модалне анализе.

Кључне речи: носећа конструкција, модална анализа, аналитичка метода, МКЕ, фреквенције.

Paper received on / Дата получения работы / Датум пријема чланка: 31.01.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.06.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24.06.2022.

VOJNOTEHNIČKI GLASNIK / MILITARY TECHNICAL COURIER, 2022, Vol. 70, Issue 3

ПРЕГЛЕДНИ РАДОВИ
ОБЗОРНЫЕ СТАТЬИ
REVIEW PAPERS

REGULARIZATION IN QUANTUM FIELD THEORIES

Nicola Fabiano

University of Belgrade, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, Belgrade, Republic of Serbia,
e-mail: nicola.fabiano@gmail.com,
ORCID iD: https://orcid.org/0000-0003-1645-2071

DOI: 10.5937/vojtehg70-34284;https://doi.org/10.5937/vojtehg70-34284

FIELD: Mathematics
ARTICLE TYPE: Review paper

Abstract:

Introduction/purpose: The principal techniques of regularization schemes and their validity for gauge field theories are discussed.

Methods: Schemes of dimensional regularization, Pauli–Villars and lattice regularization are discussed.

Results: The Coleman–Mandula theorem shows which gauge theories are renormalizable.

Conclusion: Some gauge field theories are renormalizable, the Standard Model in particular.

Key words: regularization, renormalization, Gauge Field Theory, Coleman–Mandula Theorem.

Regularization schemes

Up to now, we have encountered quantum electrodynamics and other theories such as the scalar potential ϕ^4 and the Standard Model (Fabiano, 2021a,b). In QED, we have seen in some detail how to get rid of infinities coming from loop integrations and obtain meaningful results for physical quantities with renormalization. For this purpose, we have used dimensional regularization, but there are other regularization schemes with different properties.

Dimensional regularization

This is the scheme we have already used in (Fabiano, 2021a,b), perhaps the most versatile one (Bollini & Giambiagi, 1972; 't Hooft & Veltman, 1972). First, a Wick rotation (Wick, 1954) is performed to an Euclidean space. Then the action is extended to an arbitrary dimension D that becomes a complex number. In these regions, all Feynman diagrams are finite. All integrals are analytically continued for $D \to 4$, and the resulting simple poles due to Gamma functions are to be reabsorbed into the physical parameters. This scheme, beyond its simplicity, has the great advantage of preserving all symmetries of the theory that do not depend on dimensionality such as gauge symmetry, Poincaré symmetry etc., as well as the Ward–Takahashi identities (Ward, 1950; Takahashi, 1957). A remark on the notation. We have already encountered the minimal subtraction scheme MS ('t Hooft, 1973; Weinberg, 1973), where the counterterms computed with dimensional regularization have no finite part. There is another widely used scheme, the *modified minimal subtraction scheme*, or the $\overline{\text{MS}}$ (Bardeen et al, 1978), where the finite part is a constant by means of the substitution

$$\frac{1}{D-4} \to \frac{1}{D-4} + \frac{\gamma}{2} - \frac{1}{2}\log 4\pi \ , \tag{1}$$

where, as usual, $\gamma \approx 0.57721$ is the Euler–Mascheroni constant.

Pauli–Villars regularization

In this procedure of 1949 (Pauli & Villars, 1949) the propagator is modified as:

$$\frac{1}{p^2-m^2} \to \frac{1}{p^2-m^2} - \frac{1}{p^2-M^2} = \frac{m^2-M^2}{p^4} + \frac{m^2-M^2}{p^6} + \mathcal{O}\left(\frac{1}{p^8}\right) \ , \tag{2}$$

where the fictitious mass is chosen $M \gg m$. The propagator behaviour for large momenta $\sim 1/p^4$ is usually enough to render finite all Feynman graphs. Eventually, the $M^2 \to +\infty$ limit is taken to decouple the unphysical particle. This technique has the advantage of preserving local gauge invariance in QED, as well as Ward identities.

Lattice regularization

Another popular scheme is the lattice regularization, where the theory is defined on a four–dimensional Euclidean lattice with the finite spacing

a (Wilson, 1975; Kadanoff, 1966). This spacing serves as a cutoff $\Lambda = 1/a$ for the Feynman integrals, rendering the results finite. This approach is mostly used for QCD, and results are extrapolated to the continuum limit for $a \to 0$ comparing different lattice spacings. Almost invariably, this method is used to simulate QCD on computers using Monte Carlo methods. The symmetry on the lattice is of course lost as Lorentz invariance is broken. There is also the problem of fermion doubling, with the appearance of more particles for each original fermion. This approach is also very computationally intensive with large memory bandwidth requirements.

Overview of renormalization

The divergences are given by graphs with loops. To determine the degree of divergence of any graph we need to know the dimensions of various fields, coupling constants and the behaviour of propagators at large momenta. As the action is given by

$$S = \int \mathrm{d}^D x \; \mathcal{L}(\phi, \partial\phi) \tag{3}$$

and has the dimensions of $\hbar$, that is zero dimensions in our units, $[S] = 0$, then the Lagrangian has the dimensions in length units (for energy units just reverse the sign)

$$[\mathcal{L}] = -D \; . \tag{4}$$

From the free action for a generic bosonic field ϕ and for a $1/2$ spin fermion ψ, we readily obtain

$$[\phi] = -\frac{D-2}{2} \tag{5}$$

and

$$[\psi] = -\frac{D-1}{2} \; . \tag{6}$$

The dimensions of the coupling constants are then easily computed, for instance in the Higgs potential with $g\phi^4/4!$ interaction, $[g] = D - 4$, so in 4 dimension g is dimensionless. We will now calculate the *superficial degree of divergence* D of a Feynman diagram. Any diagram with loops could be represented by

$$\int \mathrm{d}^D p \; f(p) = \int \mathrm{d}p \; F(p) \; , \tag{7}$$

(f is made out of different propagators in general) and the behaviour of F when all internal momenta go to infinity gives the superficial degree of convergence D

$$F(p) \sim p^{D-1} \text{ for } p \to +\infty \ . \tag{8}$$

When $D > 0$, the diagram diverges like a power

$$\int^{\Lambda} \mathrm{d}p \, p^{D-1} \sim \Lambda^{D} \ , \tag{9}$$

while if $D = 0$ implies a logarithmic divergence, $\log \Lambda$, and the integrals with $D < 0$ are convergent.

The asymptotic behaviour for large momenta of various propagators are well known: for bosonic scalar fields ϕ and vector fields A_μ it is $1/p^2$, while for electron (lepton) fields ψ is $1/p$. In general, the asymptotic behaviour for a propagator $\Delta_f(p)$ of a field f is given by

$$\Delta_f(p) \sim p^{-2+2s_f} \ , \tag{10}$$

and it can be shown that for a massive field f that transforms under Lorentz group as (A, B) one has $s_f = A + B$, so loosely speaking s_f is the "spin" of field. For massless bosonic fields, $s_f = 0$. The photon (spin=1) propagator and also the graviton field $g_{\mu\nu}$ (with spin=2) behave like $1/p^2$.

By power counting, one could calculate the superficial degree of convergence D. Each fermion propagator contributes to p^{-1}, each boson propagator gives a p^{-2} term, each loop from integration contributes with a p^4 term, and each vertex with n derivatives contributes at most with a p^n term. We will see the superficial degree of divergence for QED graphs in some detail. Define

$$\begin{aligned}
L &= \text{number of loops,} \\
V &= \text{number of vertices,} \\
E_\psi &= \text{number of external electron legs,} \\
I_\psi &= \text{number of internal electron legs,} \\
E_A &= \text{number of external photon legs,} \, and \\
I_A &= \text{number of internal photon legs} \ ,
\end{aligned} \tag{11}$$

then the superficial degree of divergence is:

$$D = 4L - 2I_A - I_\psi \ . \tag{12}$$

We want to rewrite this relation as a function of external legs only, no matter how many internal legs or loops the graph may have.

Consider electrons. Each vertex connects to one end of an internal electron leg. For external legs, only one end connects onto a vertex, thus:

$$V = I_\psi + \frac{1}{2}E_\psi \text{ implies } I_\psi = V - \frac{1}{2}E_\psi \ . \tag{13}$$

For photons, each vertex connects to one end of an internal photon line, unless it is external, that is

$$V = 2I_A + E_A \text{ implies } I_A = \frac{1}{2}(V - E_A) \ . \tag{14}$$

We know that the total number of independent momenta is equal to L, which in turn equals the total number of internal lines in the graph minus the number of vertices, because of moment conservation at each vertex, plus one, as we have overall momentum conservation as well. So:

$$L = I_\psi + I_A - V + 1 \ . \tag{15}$$

By substituting for I_ψ, I_A, L the expressions found in eqs. (13)–(15) into eq. (12), we obtain

$$D = 4 - \frac{3}{2}E_\psi - E_A \ . \tag{16}$$

What is renormalizable?

The procedure of renormalization we have met in QED is not substantially different from any other theory. When calculating Feynman diagrams one encounters diagrams with momenta integration inside loops. These integrals diverge, and have to be regularized in some manner, that is, their divergencies should be isolated. Then these infinities are reabsorbed by a set of bare physical parameters, such as coupling constants and masses. These parameters have divergencies that cancel out the ultraviolet infinities coming from loops in Feynman diagrams. Eventually, we are left with the physical (or “renormalized” or “dressed”) parameters, that are the actual parameters one could measure in an experiment.

Since there is only a finite number of such parameters in a Lagrangian, one can make only a finite number of such redefinitions. In other words, it is possible to renormalize only a theory with a finite number of fundamentally divergent diagrams that are the building blocks of all divergent diagrams of the theory. For instance, QED is such a theory, and we have encountered those kinds of diagrams in (Fabiano, 2021a,b).

Of course, all this procedure has to be built on solid grounds, requiring a sound mathematical proof that this can be actually done. It is usually done by an induction argument, that is, if one proves that the nth order of a theory is finite, and the $n + 1$th order is finite in terms of the nth order, then the theory is renormalizable. The induction proof uses Weinberg's theorem, which essentially states that a Feynman graph converges if the superficial degree of the divergence D of the graph and all its subgraphs is negative.

We will now find out whether a particular theory is renormalizable. Consider its Lagrangian and compute the dimensions of the coupling g starting from eqs. (4)–(6). Let d be the length dimension of g, that is

$$[g] = d \ , \tag{17}$$

and from the scaling of the Lagrangian parameters we have met in (Fabiano, 2021b), eq. (16) in particular, for which $e = e_0\mu^{-(4-D)/2}\ldots$, we could deduce the scaling

$$g \sim g_0 L^{-d} \ \text{ or } \ g \sim g_0 E^d \ , \tag{18}$$

L being a length scale, E an energy scale, and g_0 the bare coupling constant. Suppose now that $d > 0$, then we see that with decreasing distance, or increasing energy, the coupling constant g increases indefinitely:

$$g = +\infty \text{ for } \ L \to 0, \text{ or } \ E \to +\infty \ . \tag{19}$$

As the coupling constant increases, perturbation theory will fail; therefore, it will not be renormalizable.

So, we have obtained the important result: if the length dimension of the coupling constant is positive, then the theory is *non renormalizable*. On the other hand, if d is negative, $g \to 0$ for increasing energy, then perturbation theory is applicable. In this case, the theory is called *super renormalizable*. If the coupling constant is adimensional, then the theory is *renormalizable*.

Non renormalizable theories

Non renormalizable theories have coupling constants with negative energy dimensions: for instance, any theory with the interaction $g\phi^n$ with $n > 4$ in four dimensions. Such theories have infinite divergent Feynman diagrams of infinite different kinds. The proliferation of different types of divergencies cannot be controlled by redefinition of a finite number of physical parameters.

Some examples of such theories are:

Any nonpolinomial action: an action that has an infinite number of terms like $\sum_{n=3}^{+\infty} g_n c_n \phi^n$. Independently of the dimension there will be an (infinite) number of dimensionful coupling constants with negative energy dimensions.

Fermi's interaction: the four fermion interactions proposed by Fermi in 1934 (Fermi, 1934a,b) much before the electroweak theory, $G_F(\overline{\psi}\psi)^2$. As it is well known, $G_F \sim 1/m_W^2$, so the coupling has the energy dimension of -2.

Massive vector boson with a non Abelian gauge group: a vector field with mass M has a propagator such as

$$\frac{g_{\mu\nu} - p_\mu p_\nu / M^2}{p^2 - M^2 + i\epsilon}$$

that goes like a constant $-1/M^2$ at infinity. No integral of a loop diagram could converge with such behaviour.

Gravitation: Newtonian potential is $G m_1 m_2 / r$. So G has negative energy dimensions.

Theories with anomalies: symmetries of the original classical Lagrangian could be broken by quantum effects and are called *anomalies*. They in turn spoil Ward–Takahashi identities, essential for proving that a theory could be renormalizable.

Renormalizable theories

These theories are of course the most important ones. They have only a finite numbers of necessary counterterms, and their coupling constant is adimensional. Some examples follow.

ϕ^4 in four dimensions: a scalar field with such interaction, like the Higgs potential, has a dimensionless coupling constant g for $D = 4$. From hints by the ϵ–expansion method, this theory is also probably free in four dimensions.

QED: we already discussed quantum electrodynamics in (Fabiano, 2021a,b), and explicitly wrote the counterterms. Historically, it was the first theory to be proven renormalizable.

Standard Model: the SM of particles with a gauge group $SU_{col}(3) \times SU_L(2) \times U_Y(1)$ broken to $SU_{col}(3) \times U_{em}(1)$ has three adimensional coupling constants (Glashow, 1959; Salam & Ward, 1959; Weinberg, 1967). Notice, however, that electroweak model alone, $SU_L(2) \times U_Y(1)$, is not renormalizable. The further presence of quarks is needed in order to cancel all anomalies and render the SM anomaly free.

Yukawa theory: it is also part of the SM. It describes a coupling between fermions and scalars given by

$$g\phi\overline{\psi}\psi$$

the coupling constant g is, as usual, dimensionless (Yukawa, 1935).

Spontaneously broken non Abelian gauge theories: although we have seen that a massive vector boson is non renormalizable, spontaneously broken massless non Abelian gauge symmetries are actually renormalizable. These are spontaneously broken Yang–Mills theories. The proof was given by 't Hooft and Veltman in 1972 ('t Hooft & Veltman, 1972), and only after that the usage of gauge theories was fully justified. It is important to notice that unbroken Yang–Mills theories are renormalizable only in four dimensions.

Two dimensional fermion theory: for $D = 2$, a term $\left(\overline{\psi}\psi\right)^2$ of Fermi's theory is renormalizable there.

Super renormalizable theories

They converge very rapidly, only a finite number of graphs is divergent. Actually, the degree of divergence decreases when the number of loops increases.

ϕ^3: in three dimensions, this bosonic theory is super renormalizable. However, this theory is ill–defined because the potential is unbounded from below, so the vacuum is unstable.

ϕ^4: in three dimensions, this theory is super renormalizable as its coupling is such that $[g] = D - 4$, negative for $D < 4$.

Two dimensional boson theory: for $D=2$, that is, only time and a space coordinate, there is a sort of magic. Any theory of bosonic field is super renormalizable, because the field itself is dimensionless, and $[g]=-2$.

Two dimensional theory: combining the results previously obtained, in two dimensions a theory

$$P(\phi)\overline{\psi}\psi$$

where P is an arbitrary polynomial is super renormalizable.

Why gauge theory?

We have followed the full path starting from the Lagrangian to a measurable physical quantity. On our walk, we have encountered infinite quantities and rigorous results that allow us to get rid of them. All the time we have dealt with gauge theories that combine Poincaré group invariance (that is the Lorentz plus translation group) and some internal symmetry groups, the gauge group, for instance $U(1)$ for QED or $SU(3)$ for QCD.

A question naturally arises whether it is possible to have theories with different kinds of symmetries than those previously described, which are able to give physically meaningful results?

This question has been answered by the Coleman–Mandula *no–go theorem* of 1967 (Coleman & Mandula, 1967) and, to a certain extent, the short answer is "no".

We recall that the Lorentz group preserves the distance with Minkowski metric $s^2 = x_\mu g^{\mu\nu} x_\nu$. It has $L_{\mu\nu}$ generators of rotations, boosts and inversions that obey the $SO(3,1)$ Lie algebra

$$[L_{\mu\nu}, L_{\rho\sigma}] = i g_{\mu\sigma} L_{\nu\rho} + i g_{\nu\rho} L_{\mu\sigma} - i g_{\mu\rho} L_{\nu\sigma} - i g_{\nu\sigma} L_{\mu\rho} \; . \tag{20}$$

Remember that the Lie algebra is defined by its generators T^a with commuting properties

$$[T^a, T^b] = i f^{abc} T^c \; , \tag{21}$$

where f^{abc} is the structure constant. The Lie algebra is obtained from the Lie group by taking the logarithm of group elements G.

The generators $L_{\mu\nu}$ together with the generators of translations P^μ form the Poincaré algebra. While the translations commute among them

$$[P^\mu, P^\nu] = 0 \ , \tag{22}$$

they do not commute with the Lorentz generator, because the latter has two indices opposed to only one:

$$[L^{\mu\nu}, P^\rho] = ig^{\mu\rho}P^\nu - ig^{\mu\nu}P^\rho \ . \tag{23}$$

Wigner (Wigner, 1939) gave all possible classifications for real particles from the Poincaré group, where states are labelled by the invariant mass $P^2 = m^2$, the spin s and the helicity h.

1. $P^2 = m^2 > 0$ and the spin s is discrete, then the state is $|m, s\rangle$, $s = 0, 1/2, 1, 3/2, \ldots$.
2. $P^2 = m^2 = 0$, and the state is determined by its helicity, $|h\rangle$, where $h = \pm s$, $s = 0, 1/2, 1, 3/2, \ldots$.
3. $P^2 = m^2 = 0$, and the spin is continuous, so h is continuous. These states do not seem to be realized in nature.

Coleman–Mandula theorem

It states that, given some reasonable physical assumptions we will discuss later, the only possible Lie algebra of symmetry generators consist of the generators of the Poincaré group and of some other symmetry generators of the gauge group that commute between them. Let $\mathcal{P}$ be the Poincaré group, P its algebra, and $\mathcal{G}$ the symmetry group, G its algebra. Then the only possible algebra CM of allowed symmetry group $\mathcal{CM}$ is given by the direct product of those two, that is

$$CM = P \otimes G \ . \tag{24}$$

In plain language, it means these two groups never mix, the Lorentz indices do not affect the group indices and vice versa. For instance, in QED, an $U(1)$ rotation will not affect electron energy, likewise a Lorentz boost is unable to flip electron charge.

The assumptions of this theorem are very reasonable. Consider the scattering matrix S, and its symmetry group $\mathcal{CM}$ with the following assumptions

- **Mass gap:** for any given mass $m > 0$ there is only a finite number of particles with mass less than m. No continuous spectrum is allowed.
- **Scattering:** it occurs at almost all energies except maybe for some discrete set of energies.
- **Analyticity:** the S matrix for two body scattering is an analytic function of angle, energy and momentum, except maybe for some discrete set of energies.
- **"Ugly technical assumption":** stating that the matrix elements of the group generators are distributions in momentum space.

Under these assumptions, the only allowed algebra for the symmetry group $\mathcal{CM}$ of the S matrix is given by eq. (24).

There is actually a possible way out of this theorem. If one considers a symmetry that exchanges bosons with fermions, so called *supersymmetry*, then it is possible to extend this particular symmetry to the allowed symmetries of the S matrix without breaking the Coleman–Mandula theorem, which is known as the Haag-Łopuszański-Sohnius theorem (Haag et al, 1975).

It must be stressed, however, that up to this date supersymmetric particles are yet to be discovered.

References

Bardeen, W.A., Buras, A.J., Duke, D.W. & Muta, T. 1978. Deep-inelastic scattering beyond the leading order in asymptotically free gauge theories. *Physical Review D*, 18(11), pp.3998-4017. Available at: https://doi.org/10.1103/PhysRevD.18.3998.

Bollini, C.C. & Giambiagi, J.J. 1972. Dimensional renorinalization : The number of dimensions as a regularizing parameter. *Il Nuovo Cimento B (1971-1996)*, 12(1), pp.20–26. Available at: https://doi.org/10.1007/BF02895558.

Coleman, S. & Mandula, J. 1967. All Possible Symmetries of the S Matrix. P*hysical Review*, 159(5), pp.1251-1256. Available at: https://doi.org/10.1103/PhysRev.159.1251.

Fabiano, N. 2021a. Quantum electrodynamics divergencies. *Vojnotehnički glasnik/Military Technical Courier*, 69(3), pp.656-675. Available at: https://doi.org/10.5937/vojtehg69-30366.

Fabiano, N. 2021b. Corrections to propagators of quantum electrodynamics. *Vojnotehnički glasnik/Military Technical Courier*, 69(4), pp.930-940. Available at: https://doi.org/10.5937/vojtehg69-30604.

Fermi, E. 1934a. Tentativo di una teoria dei raggi β. *Il Nuovo Cimento (1924-1942)*, 11, art.number:1 (in Italian). Available at: https://doi.org/10.1007/BF02959820.

Fermi, E. 1934b. Versuch einer Theorie der β-Strahlen. I. *Zeitschrift für Physik*, 88(3-4), pp.161-177 (in German). Available at: https://doi.org/10.1007/BF01351864.

Glashow, S. 1959. The renormalizability of vector meson interactions. *Nuclear Physics*, 10(February–May), pp.107-117. Available at: https://doi.org/10.1016/0029-5582(59)90196-8.

Haag, R.J., Łopuszański, J.T. & Sohnius M. 1975. All possible generators of supersymmetries of the *S*-matrix. *Nuclear Physics B*, 88(2), pp.257-274. Available at: https://doi.org/10.1016/0550-3213(75)90279-5.

't Hooft, G. 1973. Dimensional regularization and the renormalization group. *Nuclear Physics B*, 61, pp.455-468. Available at: https://doi.org/10.1016/0550-3213(73)90376-3.

't 'Hooft, G. & Veltman, M. 1972. Regularization and renormalization of gauge fields. *Nuclear Physics B*, 44(1), pp.189–213. Available at: https://doi.org/10.1016/0550-3213(72)90279-9.

Kadanoff, L.P. 1966. Scaling laws for Ising models near T_c. *Physics Physique Fizika*, 2(6), pp.263-272. Available at: https://doi.org/10.1103/PhysicsPhysiqueFizika.2.263.

Pauli, W. & Villars F. 1949. On the Invariant Regularization in Relativistic Quantum Theory. *Reviews of Modern Physics*, 21(3), pp.434-444. Available at: https://doi.org/10.1103/RevModPhys.21.434.

Salam, A. & Ward, J.C. 1959. Weak and electromagnetic interactions. *Il Nuovo Cimento (1955-1965)*, 11(4), pp.568-577. Available at: https://doi.org/10.1007/BF02726525.

Takahashi, Y. 1957. On the generalized ward identity. *Il Nuovo Cimento (1955-1965)*, 6(2), pp.371–375. Available at: https://doi.org/10.1007/BF02832514.

Ward, J.C. 1950. An Identity in Quantum Electrodynamics. *Physical Review*, 78(2), p.182. Available at: https://doi.org/10.1103/PhysRev.78.182.

Wick, G.C. 1954. Properties of Bethe-Salpeter Wave Functions. *Physical Review*, 96(4), pp.1124–1134. Available at: https://doi.org/10.1103/PhysRev.96.1124.

Weinberg, S. 1967. A Model of Leptons. *Physical Review Letters*, 19(21), pp.1264-1266. Available at: https://doi.org/10.1103/PhysRevLett.19.1264.

Weinberg, S. 1973. New Approach to the Renormalization Group. *Physical Review D*, 8(10), pp.3497-3509. Available at: https://doi.org/10.1103/PhysRevD.8.3497.

Wigner, E. 1939. On unitary representations of the inhomogeneous Lorentz group. *Annals of Mathematics*, 40(1), pp.149–204. Available at: https://doi.org/10.2307/1968551.

Wilson, K.G. 1975. The renormalization group: Critical phenomena and the Kondo problem. *Reviews of Modern Physics*, 47(4), pp.773–840. Available at: https://doi.org/10.1103/revmodphys.47.773.

Yukawa, H. 1935. On the interaction of elementary particles. *Proceedings of the Physico-Mathematical Society of Japan. 3rd Series*, 17, pp.48-75. Available at: https://doi.org/10.11429/ppmsj1919.17.0_48.

РЕГУЛЯРИЗАЦИЯ В КВАНТОВЫХ ТЕОРИЯХ ПОЛЯ

Никола Фабиано

Белградский университет, Институт ядерных исследований
«Винча» - Национальный институт Республики Сербия,
г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 29.05.03 Математические методы теоретической физики,
29.05.23 Релятивистская квантовая теория. Квантовая теория поля
29.05.33 Электромагнитное взаимодействие
ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: В данной статье рассматриваются основные методы схем регуляризации и их применимость в калибровочных теориях полей.

Методы: В статье применены схемы размерной регуляризации, Паули - Вилларса и регуляризации решетки. обсуждаются регуляризация.

Результаты: Теорема Коулмана-Мандулы показывает какие калибровочные теории подлежат ренормализации.

Выводы: В ходе исследования выявлено, что некоторые теории калибровочного поля перенормируемы, в частности − стандартная модель.

Ключевые слова: регуляризация, перенормировка, теория калибровочного поля, теорема Колемана - Мандулы.

РЕГУЛАРИЗАЦИЈА У ТЕОРИЈАМА КВАНТНОГ ПОЉА

Никола Фабиано

Универзитет у Београду, Институт за нуклеарне науке „Винча“ - Национални институт Републике Србије, Београд, Република Србија

ОБЛАСТ: математика
ВРСТА ЧЛАНКА: прегледни рад

Сажетак:

Увод/циљ: Разматрају се основне технике шема регуларизације као и њихова ваљаност за теорије калибрационих поља.

Методе: Примењују се шеме димензионалне регуларизације, Паули-Виларсова регуларизација као и регуларизације решетке.

Резултати: Колеман-Мандула теорема показује које калибрационе теорије се могу ренормализовати.

Закључак: Неке теорије калибрационог поља се могу ренормализовати, специфично стандардни модел.

Кључне речи: регуларизација, ренормализација, теорија калибрационог поља, Колеман–Мандула теорема.

Paper received on / Дата получения работы / Датум пријема чланка: 05. 10. 2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 23. 06. 2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24. 06. 2022.

MALICIOUS CODE IN THE CLOUD

Dragan Z. Damjanović

Independent researcher, Zrenjanin, Republic of Serbia,
e-mail: damjanovic1971@gmail.com,
ORCID iD: https://orcid.org/0000-0001-8169-4507

DOI: 10.5937/vojtehg70-37168; https://doi.org/10.5937/vojtehg70-37168

FIELD: IT
ARTICLE TYPE: Review paper

Abstract:

Introduction/purpose: The paper analyzes the impact of malicious codes in the cloud. Malicious code is an unauthorized piece of code that violates the integrity of an application and infrastructure to cause certain effects, such as security breaches, spread of infections, and data infiltration from the computer with the help of malicious software - this is a simple form of data theft which can lead to disastrous consequences in all segments of society, especially when it comes to national security. To overcome this challenge, it is necessary to detect holes in the safety of cloud environments and repair them before the attackers use these vulnerabilities to bypass the integrated cloud infrastructure.

Methods: Structural analysis, functional analysis, comparative analysis, synthesis.

Results: There are many factors for collecting, comparing, and delivering intelligence data on cloud threats. Cloud applications are increasingly being targeted because their use to store and share data with mobile application hosting has been increased exponentially, enabling industrial automation and business information monitoring and procurement. In addition, billions of devices on the Internet use the cloud infrastructure as a background for processing and transmitting large data sets. Malicious code is easily distributed due to the ease of sharing documents and files via the cloud.

Conclusion: As cloud technologies are taking a central place in the world of digital transformation, the threat to the cloud environment is expected to grow exponentially. This means that organizations need to ensure that the cyber security position of the cloud infrastructure they possess is robust and mature enough to combat all relevant security threats in order to minimize business risks. Understanding the nature of practical security controls and how they are assessed enables organizations to build a practical approach to security and privacy in the cloud.

Keywords: malicious code, cloud, malware, intelligence.

Introduction

Malicious code (malver) is an unauthorized piece of code that violates the integrity of an application and infrastructure to cause certain effects, such as security breaches, the spread of infection, and data infiltration (it can lead to disastrous consequences in all segments of society, especially when it comes to national security). Attackers can use the cloud infrastructure to set up malicious code that performs malicious operations and unauthorized activities, such as spreading malware, filtering out sensitive information, and launching additional attacks. This malicious code can take many forms including scripts, add-ons, executables, binaries, and applets (any small application that performs a specific task within a larger program). (Sood, 2021)

Malicious code can (Hutchins et al, 2011):

- spread infections to a large number of Internet users,
- filter out sensitive and critical data from compromised systems,
- use additional online systems to spread infections within the network,
- install advanced malware, such as remote administration toolkits (RAT) and ransomware (Some types of rensomers can block a computer by creating a blackmail message that the user cannot remove without paying a ransom. Other types can encrypt files. In that case, the user whose computer is infected is asked to ransom in exchange for decrypting the data recorded on the disk),
- reconnoiter and collect information about the target environment,
- use endangered infrastructure for additional abuses, such as launching miners,
- arm compromised systems to act as launching platforms for targeted and widely based attacks, and
- violate the integrity of cloud-based cloud web sessions.

A complex code can combine many of these functions in collaboration for infection distribution and data filtering (Sood & Zeadally, 2016).

Malicious code distribution: Download attack model

It is important to understand the most prominent model for distributing malware and attacks on the Internet. Attackers typically opt for a download attack (Sood & Zeadally, 2016) that involves creating a socially-crafted “fishing” email to encourage a user to visit an attacker-controlled URL that distributes malware.

An attacker embeds a link in an email with a tempting (or even ominous) message to trick users into clicking on the link. Let us understand this model by dissecting its steps:

Step 1: An attacker sends an official email containing a built-in link to a malware download site. This is called a social engineering technique because it relies on the interests or emotions of users and tricks them into clicking on an embedded link.

Step 2: The user opens the link in the email and is redirected while the browser downloads the contents of the file hosted on the cloud infrastructure (applications, storage services or instances).

Step 3: The browser automatically downloads the malicious file located on the cloud infrastructure to the end user's system. Depending on the type of attack, an attacker can either force the browser directly to download a malicious executable file or download a maliciously created file that exploits a vulnerability in the browser to install the payload into the system. After a successful operation of the system, a dropper is installed in the system. (Droper is an intermediate file that installs the final malicious load on the system.)

Step 4: A droper loads malicious code into the user's system, which can (in some cases) bypass system security checks to perform unauthorized operations. Upon completion of these steps, a successful download attack was successfully achieved. The cloud infrastructure here acts as a launching platform for the distribution of infections (Sood & Zeadally, 2016).

Similarly, an attacker may host phishing sites (phishing or network identity theft is an attempt to steal Internet user data through a forged website) on the cloud infrastructure to steal credentials from the end user system (Sood, 2021).

Hosting a malicious code in cloud storage services

This allows us to understand the true picture of cloud infrastructure abuse, especially that of storage services.

Misuse of inherent storage service functionality

Attackers abuse cloud storage service functionality to host malicious codes and spread infections on the Internet. Attackers take advantage of cloud storage functionality either through free accounts or by using compromised accounts to host malicious code. Cloud storage services allow users to host files and share links with a specific set of users or more, that is, anyone who has a link to a file can download the file.

In addition, certain cloud services allow us to download files directly when the link is opened in a browser without any notification from the browser. Both of these features allow attackers to host a malicious code, make it public, and share a connection with large sections of Internet users. When the user downloads the connection, the file is automatically downloaded to the system. The first case study is a witty DNS malware. This shows how attackers can abuse the functionality of cloud storage service providers to host and distribute a malicious code.

The install.sh file is a bash shell file that, when executed, runs the specified commands. Looking at the contents of the install.sh file, we notice the URL for the cloud storage provider.

URL points to /brut.zip?dl=1. Due to its inherent functionality, the cloud service provider supports binary verification using dl as a parameter. If the dl value is set to 0, the browser downloads the file only after displaying a notification. If the dl value is set to 1, the browser automatically downloads it. This indicates that the attacker may force users to download the gross. zip without any user intervention (Sood, 2021).

Hosting scareware for social engineering

Scareware is another social engineering technique that allows an attacker to trick (or manipulate) users into believing they have to perform certain actions such as downloading files, providing specific information, opening additional links, or buying malicious software. This can either spread infections or extract sensitive information from the target user.

Attackers use intimidating software in conjunction with social engineering tricks to force users to perform actions by playing on their fears, such as sending computer virus notifications, indicating they will be subject to a tax audit or even pretend to be a bank infringer. Users must now re-authenticate or verify their account information. Modern attackers who carry out online scams largely use this intimidating code.

This example of scareware illustrates user fraud by causing fear of virus infection in the end user's system. This is potentially a phone scam, because the intimidating software asks the end user to call the specified number in order to get support and solve the virus problem in the end user's system. In reality, the real goal is to deceive the user. An important point is the distribution of this scareware through the cloud storage service (Sood, 2021).

Man-in-the-Browser (MitB)

Another client-side attack is Man-in-the-Browser (MitB), which attackers use to steal the credentials of cloud management accounts by installing malicious code on the end user's system. There are two variants of MitB malware. One involves installing malicious code on the system as an executable file, the other installs it in a browser as a browser add-on or extension.

Both variants of MitB are capable of bypassing browser functionality to perform unauthorized operations. These two models of attacks undermine the integrity of the browser by implementing hooks into the components of the browser and initiating a process to control the execution of the task, which ultimately leads to the theft of sensitive information.

Hooking (Sood & Enbody, 2011) is an inherent technique for controlling the execution behavior of running processes by intercepting the flow of communication, which changes the known behavior of the operating system. In this MitB model, the attacker has already installed malicious code into a system that has the ability to monitor communication that takes place from a browser.

Let us say a user opens a cloud management account from a browser. As malicious code is found in the system, it filters that traffic and implements hooks to redirect requests that the browser sends to the domain controlled by the attacker.

If you give credentials, the malicious code steals the credentials through a hook and leaves the original request to a legitimate server.

The response was received from the server and the communication was successful. This attack occurs on the end user's system before the request actually passes through the network. The manipulation is going smoothly and no one knows that the credentials for the cloud management accounts have already been stolen. This model reflects the MitB attack, as malicious code is capable of modifying or stealing browser communication.

There are, of course, other variations of the MitB attack.

Grabbing form (Sood et al, 2011): Malicious code searches for an HTML form that an application displays in a browser to request credentials. For example, it may display a web page to sign up for a cloud management account. When a user provides their credentials, malicious code makes a copy of the complete HTML form data, which is mostly an HTTP POST request, and transmits it to the domain managed by the attacker. As a result, letters of credit were stolen.

Inserting Content: Malicious code can easily insert unauthorized HTML content on the client's side and lead the user to believe that the content is legitimate. Let us say a user logs into a cloud management account through a browser. Malicious code can insert HTML content to trick the user into believing that the content is coming from a cloud server, but in fact, malicious code on the system injects unauthorized content into the HTTP response before it is displayed.

In addition to the above techniques, MitB malware can perform potentially catastrophic operations in active web sessions with the cloud management console.

We will show a few of them:

Stopping Elastic Cloud Compute (EC2) cloud instances,

Change inbound and outbound filtering rules to change communication settings,

Inserting malicious code into S3 bins and making it publicly available to spread malware,

Initiation of workloads for illegal crypto mining operations of bitcoin,

Data filtering via data backups and recordings,

Gaining access to private S3 baskets,

Deleting other user accounts,

Hosting phishing websites on cloud instances,

Hosting illegal services and advertising accordingly using newly created unauthorized instances, and

Synchronizing malicious files via cloud agents with storage services from compromised systems.

It is clear how significant MitB attacks are and have the inherent ability to abuse the integrity of the operating system and installed packages (Sood, 2021).

Cloud CLI exfiltration of stored credentials

Cloud administrators and engineers use Command Line Interface (CLI) tools to execute commands directly in the cloud infrastructure. This design gives them an easy way to perform operations. However, for CLI tools to work, they store credentials in a client-side figurative file. The local configuration is unencrypted and the credentials are stored in plain text on the end user's machine. If an attacker successfully installs malware, then it is easy to filter out all saved credentials for cloud management accounts. Installed malware can easily transfer credentials from a hidden .avs directory. Even in this attack mode, the malicious actor does not directly attack the cloud infrastructure. Instead, they first compromise the end-user system and then use stolen credentials to misuse the cloud infrastructure. In addition, they can also use the AVS CLI package to execute commands on behalf of users on the AVS account. As mentioned earlier, a malicious actor can perform countless operations to affect the environment in the cloud (Sood, 2021).

Synchronization token exfiltration via human cloud attack (MitC)

Man-in-the-Cloud (MitC) (Dulce & Shulman, 2015) synchronization token filtering (MitC) is another variant of the MitB attack, but in this scenario, malicious code installed on the end-user system has a built-in synchronization token targeting module used by various agents installed on end-user systems to synchronize cloud files. As mentioned earlier, malicious code running in a compromised system can be very powerful in interacting with system software and running processes.

Numerous users install cloud vendor software agents to synchronize files present in dedicated directories with cloud storage. This allows the user to store the files in the appropriate directory, and the agent will automatically sync the files. For this, agents need a synchronization token to verify authentication and authorization for the cloud storage service before the data synchronization operation begins. To facilitate the synchronization process, the token is stored on the local machine so that the user does not have to enter a password every time the synchronization operation starts. This improves the ability of users to work seamlessly with the cloud and allows files to be synchronized in an automated way. If malicious code steals this token, then any device can sync and access files available in the cloud storage for cloud user accounts. Attackers use the MitC technique to filter out tokens and use tokens from various devices to gain access to files or synchronize malicious files to trigger chain infections. In some cases, malicious code can modify tokens to avoid detection as a result of missing tokens and trigger alerts. All in all, the MitC technique is an advanced approach that abuses the file synchronization mechanism using cloud agents that run the system.

Infecting virtual machines and containers

Attackers can choose different ways to infect VMs and containers to inject malicious code or misuse it to perform unauthorized cloud operations. Numerous attack models that we talked about earlier can contribute to the infection process, but there are some additional ways that attackers can go after targeting VMs and containers.

Exploiting vulnerabilities in network services

Launching misconfigured and unsecured containers and orchestration frameworks attracts threat actors, who then attack and use them for evil purposes. Docker containers (Cimpanu, 2020) and Kubernetes orchestration are often targeted by attackers via automated malicious code to steal information or launch other malicious useful content, depending on the design of the vulnerable component.

Inserting code into container images

Endangering the integrity of container images (Remillano, 2020) is another technique that attackers use to distribute malicious code. A number of developers use images and it is possible to insert malicious code into an image and distribute it. When developers retrieve and deploy a container image in a cloud environment, malicious code is activated and unauthorized operations are performed, such as scanning vulnerable dockers on the Internet or installing crypto miners.

Unsecured API endpoints

Unauthorized and insecure API endpoints in containers are the most prominent vectors for compromising containers and installing malicious code. Threat actors scan exposed API endpoints for container-based services and execute code to perform unwarranted operations. One such example is the malicious code Doki (Fishbein & Kajiloti, 2020) which scans unsecured Docker images and compromises them for evil activities on the Internet.

Secretly executing malicious code in VMs

VMs run as background processes without any visible element to end users. This means that there is no graphical user interface (GUI) for the VM and the user has no way to interact with the VM using the GUI. As most VMs share resources, such as disks and resources with the host OS, it is possible to misuse this design with specially crafted malicious code. One such example is Ragnar (Arghire, 2020) locker ransomware, which attackers distribute using a VM without performing ransomware operations by encrypting files on the host over a guest VM over shared resources.

Applying software without patches

One of the biggest security concerns is placing unpatched and outdated software in containers and VMs. Running code infiltrated with security vulnerabilities makes the cloud infrastructure vulnerable to exploitation - for example, running an insecure OS in VMs, placing vulnerable database software in containers, and so on.

This makes it much easier for attackers to exploit the inherent software and plant malicious code to perform illegal operations from the cloud infrastructure. In one case, unpatched Linux server software (Poston, 2020) was used by attackers to install persistent backdoor or malicious code to gain access to Linux servers.

Embedding malicious code through vulnerable applications

Deploying vulnerable applications to containers and VMs is one of the prominent vectors used by attackers to distribute malicious code. Applications that allow injection attacks, such as multi-site scripting (KSSS), structured query language (SKL), non-SKL (NoSKL), OS commands, Extensible Markup Language (KSML), and Simple Object Access Protocol SOAP), allow attackers to enter unverified useful data that is executed dynamically. After the successful execution of useful data, the code provided by the attacker is executed in the context of the application and unauthorized operations are performed. A recent study (Millman, 2020) highlighted an exponential increase in attacks on web applications where the CDN security provider blocked billions of web layer attacks.

Threat intelligence

Threat intelligence is defined as evidence-based knowledge that includes detailed system artifacts, events, compromise indicators (IoC), attack mechanisms, and potential risks for gaining detailed visibility of system status to proactively detect and prevent threats, including incidents. In general, evidence-based knowledge can be gathered only if there is sufficient insight into systems, networks, and overall infrastructure - including end-user behavior.

Cloud threat reporting

There are many factors for collecting, comparing, and committing cloud threat intelligence. A number of factors are:

Cloud applications are increasingly being targeted by threat actors because

• the use of cloud applications to store and share files with mobile application hosting, enabling industrial automation, monitoring and collecting business information, has increased exponentially,

• multiple cloud environments is seamlessly integrated for large-scale data transfer for sharing and productivity purposes, and

• billions of devices on the Internet use the cloud infrastructure as a backdrop to process and transmit large data sets.

Malicious code is easily distributed due to the ease of sharing documents and files via the cloud.

Malicious code is used to filter sensitive data from cloud instances.

Cloud infrastructure is often used for unauthorized operations such as cryptocurrency mining.

Detecting and preventing security breaches reduces business risks and potential damage to the brand.

Understanding the behavior of users who communicate with the cloud is used for fingerprints of suspicious and anomalous behaviors.

Violations of privacy and compliance may occur due to insecure application of controls.

The effectiveness of security controls is assessed in order to create defense against threats.

Based on these scenarios, it is vital to gain and import visibility into cloud infrastructure using organized threat alert operations (Sood, 2021).

Classification of threat intelligence

It is important to understand what we mean by the classification of "threat intelligence". In general, threat reporting includes contextual information from multiple resources needed to bring about information about the threats in particular environment, and then take appropriate action or precautionary measures accordingly. These actions are specific to detecting and preventing malware, as well as manual, targeted attack frames. Within the environment, it is possible to obtain and manage contextual data (granular event-related details) from multiple resources to generate threat intelligence.

These resources are:

In-house platforms - internal platforms for handling large-scale contextual data to build threat intelligence, Enterprise platforms - platforms managed by third party organizations that provide contextual data, which can then be used directly in the internal platform, and

Platforms open source - community researchers use it to manage and provide contextual data in open source format, which can then be used directly in the internal platform to make informed decisions (Sood, 2021).

Basic threat intelligence classification model

Once contextual data has been received, different types of threat intelligence can be generated:

Strategic intelligence

- threat Intelligence to help make strategic and informed decisions by conducting high-level analysis and building risk profiles,

Operational intelligence

- threat intelligence related to the mode of operation of attacks (broad-based, targeted) and threat actors (attackers) associated with those attacks,

Tactical intelligence

- threat intelligence that reveals details of advanced and covert techniques, tactics and procedures adopted by threat actors to launch various attacks,

Technical intelligence

- threat intelligence covering technical aspects of threats, such as detection indicators that detect the functionality of malware in the system and the network level to build technical intelligence that can be incorporated into automated detection and prevention products (Sood, 2021).

Threat intelligence frameworks

In this section, we consider cyber threat intelligence frameworks that use a modular approach to implementing the various phases and building blocks of a mature threat intelligence platform.

Basic information for different cyber threat frameworks: DNI cyber threat framework. The US government has introduced a cyber threat framework (ODNI, 2021) to provide a consolidated approach to the classification and categorization of various cyber threats. This DNI framework is designed to provide a common language for describing the number of cyber threats and related suspicious activities. It also allows policy makers and researchers to communicate about threat events in a structured way so that appropriate action can be taken.

The framework emphasizes the rival life cycle, which consists of four phases: preparation, engagement, presence and consequences. In addition to these phases, the framework also explicitly relies on objectives, actions and indicators to detect threats and conflicting activities.

MITER ATT & CK Framework MITER Corporation provides the ATT & CK Framework (MITER, 2021) to highlight techniques, tactics and procedures adopted by opponents to launch either targeted or broad-based attacks, depending on the conditions. This box provides information that can be used to categorize various attacks and threats to be detected in particular environment as part of a threat notification platform. In essence, the latest version of ATT & CK illustrates the comprehensive paths of attack from reconnaissance to the persistence and exfiltration of various attacking entities.

This framework can be used in many ways, such as building threat intelligence logic, cyber risk analytics, enemy detection / prevention techniques, technology stack application, and automated attack assessment. The MITER framework for conducting cyber threat modeling (Bodeau, McCollum, Fox, 2018) can also be used to detect potential threats against cloud infrastructure in a proactive way. The framework enables the dissection of infrastructure and the implementation of threat modeling by supporting a variety of threat-focused approaches, systems and assets.

It supports attack characterization using a cyber defense framework in which risks can be categorized into devices, people, data, network, and applications. In addition, the risk associated with cloud infrastructure and how vulnerable the cloud environment is to threats and attacks can be calculated. Overall, this framework allows the application of threat information to detect unknown infections by adopting a single standard. Overall, both the DNI and MITER frameworks provide an efficient way to use different types of cloud threat information to design threat intelligence frameworks. These frames can be used directly or adapted to specific requirements.

Conceptual view of the threat notification platform

The threat notification platform is designed to enter raw data from multiple resources and process it to create intelligence that can be used to detect and prevent threats.

Consider different components:

Data collection

This component is designed to enter large sets of raw data in the form of records, events, devices and CIDR lists from a wide range of hosts working in the infrastructure, including different types of networks and end-user devices. The goal is to collect data on a continuous basis and maintain it for processing. Data includes objects such as IP addresses, URLs, domains, file hashes, customer information, and complete billing for users and services. All types of records are entered, such as debugging and application execution, cloud service execution, access and communication protocols.

Data operations

When data is collected, it is passed to the next component for operations. The intention is to create a structural data format after performing normalization and duplicate removal operations to build a generic data format, remove duplicate records, and clear data entries with missing information. Once the data is normalized and cleaned, it is transformed into a structural format before validation and analytical operations are performed on it.

Certified Intelligence

This component handles validated threat intelligence from multiple sources, such as enterprise security tools deployed in the environment, enterprise classification feeds, malware family information, and open source threat sources to link to data operations and analysis machine. This is validated threat information that is used in conjunction with data from various organizational resources to build contextual threat intelligence.

Correlation and data analysis

Once the data structure is in place, it is time to perform data correlation and analysis using a variety of data science techniques, including machine learning and artificial intelligence, to link large amounts of data to detect anomalies and threats located in the organization of infrastructure. The goal is to detect threats that are in the system by analyzing raw data and using threat intelligence to reveal the time frame of the threat.

Contextual intelligence threats

Contextual Intelligence Threats (CTI) emphasizes threats that are found in systems in significant detail with the intention of showing business risks to the organization. CTI can provide very specific insights into the various assets used in infrastructure, including end users, and assess how prone these entities are to malware infections or are already infected with malicious code. This component also provides the ability to search for contextual intelligence for any particular entity (end user, system, and device). CTI can also be used for other purposes, such as performing risk mapping and proposing safety remedies. It may be particularly useful to specify areas of unacceptably high risk and exposure.

Understanding compromise and attack indicators

The Compromise Indicator (IoC) highlights data or metadata that reflects potential system compromise or the presence of threat actors in the environment, especially in this context, the cloud infrastructure. The IoC can help assemble the automated response needed to detect a threat in the environment so that appropriate prevention steps can be taken. Threat intelligence and security solutions import the IoC database to instruct tools to scan network data and endpoints from different systems in the infrastructure to detect network and endpoint threats, respectively. Another term used in the same context is Attack Indicators (IoA), which provides information regarding a potential attack that is ongoing or has previously been performed on cloud infrastructure. The primary difference between the IoC and the IoA is that the IoC indicates that a compromise has been reached, while the IoA reflects that the threat actor launched the attack, but there is no confirmation of a compromise. In order to obtain a detailed context on the security stance, an alert triggered by scans, assessments, and other security software must be linked using IoC and IoA to make specific calls about potential threats to the system and determine how they arose (Sood, 2021).

Understanding malware protection

It is crucial to apply inherent security protection in a proactive way to defend against malicious code and thus significantly reduce the impact and risk on the organization.

Proactive security mechanisms help prevent the spread of malicious code by detecting infections and stopping problems in early stages of infection. This helps to significantly reduce business risk, and thus reduce the occurrence of security breaches. The term "protection" here includes both "detection" and "prevention". This means that "malware protection" includes security mechanisms and strategies for the implementation of "malware detection" and "malware prevention" controls (Sood, 2021).

Malware detection

Controls that can be applied to detect malware in the cloud.

All cloud computing instances (hosts) should have a Host Intrusion Detection System (HIDS) installed that is able to do the following:

• Apply File Integrity Monitoring (FIM) to assess changes that occur in system files and maintain the state of the modified file. The goal is to check for file integrity violations on critical cloud servers.

• Detect anomalies using log analysis to build a risk attitude so that potential security risks can be analyzed. Detecting anomalies also helps identify potential attacks targeting cloud instances, such as brute force and cracking accounts. This technique is also called log-based intrusion detection (LID).

• Process and file level analysis to detect malicious code, such as rootkits running on the system. HIDS enables the detection of suspicious and hidden processes in critical cloud servers in order to detect possible infections.

All critical servers must have antivirus mechanisms installed to scan for malicious code (viruses, trojans, ransomware and rootkits) running on the system. Antivirus programs are updated at regular intervals with advanced signatures and heuristics to stay up to date to detect malicious code in the system. The antivirus engine has a built-in ability to scan documents, executables, mail and archive files to detect malicious code.

Scan files stored in cloud storage to detect potentially malicious code. By default, storage baskets do not have the built-in ability to check the nature of files. Either a third-party security solution or a cloud vendor-specific security service must be implemented to scan files in the storage bin for malware.

Implement an improved scanning process to dissect the contents of files uploaded to cloud services to detect the presence of malicious code. This content verification check must be enabled for each file upload feature in cloud applications.

Implement scanning of the content of specially embedded links and attachments for emails associated with cloud accounts, such as O365, to detect phishing attacks, such as

• embedded URLs that point to malicious domains for download attacks and

• attachments that contain malicious files resulting in malware installation.

Check the integrity and security of third-party applications integrated with cloud accounts for enhanced functionality to ensure that malicious files are not served through these third-party services.

Always scan network traffic for intrusion detection by dissecting network traffic and related protocols to detect command and control (C&C) communication, data exfiltration, and sensitive data leakage. In addition, scan the network traffic for malicious code that served as part of the download attack and the spread of the infection.

Mandatory implementation of a system for detecting suspicious behavior of end systems in relation to critical cloud services displayed on the Internet. For example, for attempts to retrieve accounts that target SSH and RDP services, the end customer sends multiple brute force requests and account breaches to gain access. The same system of behavior should detect a wide range of attacks and malicious code.

Perform periodic Azure authentication checks from Active Directory Federation Services (ADFS) to ensure that all authentication traffic flows properly through the ADFS instance and that no “golden SAML” cards have been created to bypass normal authentication (Vijayan, 2020).

Malware prevention

If any malicious files detected during the scanning process are implemented at the operating system level, ensure that the quarantine file takes place in an automated manner to avoid any interference. This helps filter out malicious files on the fly and restrict access to, share or transfer malicious files.

While uploading files to the cloud environment, i.e. application or storage services, if the file is found to be malicious in nature, it should be discarded, never stored in storage bins. This helps prevent malicious files from spreading after storage.

During the email scanning process, if malicious files are detected as part of an attachment or malicious URL, apply automated quarantine to filter emails that contain malicious content.

During the network scanning process, if intrusions are detected, make sure that the intrusion prevention system restricts malicious code and communication to prevent malicious code from reaching the end user's system via the cloud.

If the system detects a data leak during the on-line scan process in which the contents of the file are scanned to see if any sensitive data is present in the file, make sure the system restricts file sharing with other users and filter accordingly. A file containing sensitive data can be transferred as part of a data exfiltration process using malicious code.

Since systems detect suspicious communication using behavioral tracking, such as retrieval attempts, be sure to blacklist the end customer by limiting the IP address to prevent retrieval attacks. Make sure that all software running in the cloud has no vulnerabilities. If vulnerable packages or network services are found to be active, make sure patches are applied to remove vulnerabilities or poor configuration in the cloud environment. Make sure that there is a strong strategy for backing up and recovering the implementation in case of a ransomware attack. This helps administrators recover damaged data from backups at some point. In general, the detection and prevention of malware depend on each other to protect against malicious code in the cloud. This is because in order to prevent malicious code infections, they must first be detected. This means that gaining insight into the work of malicious code is the most important task. Once an understanding of the malicious code and how it affects the cloud infrastructure is gained, preventative solutions can be applied to completely disrupt the life cycle of the malicious code. Thus, a complete malware protection framework can be applied to prevent malicious use of cloud infrastructure (Sood, 2021).

Techniques, tactics, and procedures

Threat intelligence plays a significant role in building proactive and reactive security approaches in the fight against malicious code in the cloud. They also allow risk analysis to be performed to determine the level of risk associated with critical hosts, applications, and services deployed in the cloud. Threat intelligence also helps identify techniques, tactics, and procedures (TTPs) used by threat actors and malicious code. Using threat intelligence, mechanisms can be put in place to assess the effectiveness of security controls in the environment and to verify that the security stance is robust enough. Overall, it is an important condition to have an internal threat alert platform to implement rigorous cloud infrastructure security procedures and processes. Applied intelligence on threats helps to prevent the abuse and exploitation of the cloud environment (Sood, 2021).

Conclusion

The attackers are targeting the cloud infrastructure to carry out cybercrime and vile Internet operations. The attackers use the cloud infrastructure for various attacks, such as distributing malicious code, launching crypto mining operations, running DDoS, filtering sensitive information and more. As cloud technologies take center stage in the world of digital transformation, threats to cloud environments are expected to grow exponentially. This means that organizations need to ensure that the cybersecurity position of the cloud infrastructure they possess is robust and mature enough to combat all relevant security threats so that business risks are minimized. To overcome this challenge, it is necessary to detect security holes in cloud environments and fix them before attackers take advantage of these shortcomings to circumvent the integrity of the cloud infrastructure. Understanding the nature of practical security controls and how to evaluate them enables organizations to build a practical approach to security and privacy in the cloud. There are no shortcuts to cloud security because it is an ongoing process which requires constant improvement how technology evolves.

References

Arghire, I. 2020. Ragnar Locker Ransomware Uses Virtual Machines for Evasion. *Security Week*, May 22 [online]. Available at: https://www.securityweek.com/ragnar-locker-ransomware-uses-virtual-machines-evasion [Accessed: 20 March 2022].

Cimpanu, C. 2020. Docker malware is now common, so devs need to take Docker security seriously. *ZDnet (Zero Day Blog),* November 30 [online]. Available at: https://www.zdnet.com/article/docker-malware-is-now-common-so-devs-need-to-take-docker-security-seriously/ [Accessed: 20 March 2022].

Dulce, S. & Shulman, A. 2015. Man in the Cloud Attacks. *Slideshare*, August 05 [online]. Available at: https://www.slideshare.net/Imperva/maninthecloudattacksfinal?from_action=save [Accessed: 20 March 2022].

Fishbein, N. & Kajiloti, M. 2020. Watch Your Containers: Doki Infecting Docker Servers in the Cloud. *Intezer*, July 28 [online]. Available at: https://www.intezer.com/blog/cloud-security/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/ [Accessed: 20 March 2022].

Hutchins, E.M., Cloppert, M.J. & Amin, R.M. 2011. Amin Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In: *ICIW 2011: 6th International Conferenceon i-Warfare and Security*, Washington, DC, pp.113-126, March 17-18 [online]. Available at: https://www.proceedings.com/16654.html [Accessed: 20 March 2022]. ISBN: 9781622766758.

Millman, R. 2020. Web app attacks are up 800% compared to 2019. *IT Pro*, November 23 [online]. Available at: https://www.itpro.com/security/357872/web-app-attacks-increase-2020 [Accessed: 20 March 2022].

Poston, H. 2020. Linux vulnerabilities: How unpatched servers lead to persistent backdoors. *Infosec*, September 23 [online]. Available at: https://resources.infosecinstitute.com/topic/linux-vulnerabilities-how-unpatched-servers-lead-to-persistent-backdoors/ [Accessed: 20 March 2022].

Remillano, A. 2020. Malicious Docker Hub Container Images Used for Cryptocurrency Mining. *Trend Micro*, August 19 [online]. Available at: https://www.trendmicro.com/vinfo/fr/security/news/virtualization-and-cloud/malicious-docker-hub-container-images-cryptocurrency-mining [Accessed: 20 March 2022].

Sood, A.K. 2021. *Empirical Cloud Security: Practical Intelligence to Evaluate Risks and Attacks*. Herndon, VA: Mercury Learning and Information. ISBN: 978-1683926856.

Sood, A.K. & Enbody, R.J. 2011. A browser malware taxonomy. *Virus Bulletin*, June 06 [online]. Available at: https://www.virusbulletin.com/virusbulletin/2011/06/browser-malware-taxonomy/ [Accessed: 20 March 2022].

Sood, A.K., Enbody, R.J. & Bansal, R. 2011. The art of stealing banking information – form grabbing on fire. *Virus Bulletin*, November 01 [online]. Available at: https://www.virusbulletin.com/virusbulletin/2011/11/art-stealing-banking-information-form-grabbing-fire [Accessed: 20 March 2022].

Sood, A.K. & Zeadally, S. 2016. Drive-By Download Attacks: A Comparative Study. *IT Professional*, 18(5), pp.18-25. Available at: https://doi.org/10.1109/MITP.2016.85.

Vijayan, J. 2020. SolarWinds Campaign Focuses Attention on ‘Golden SAML’ Attack Vector. *DARKReading*, December 22 [online]. Available at: https://www.darkreading.com/attacks-breaches/solarwinds-campaign-focuses-attention-on-golden-saml-attack-vector [Accessed: 20 March 2022].

ВРЕДОНОСНЫЙ КОД В ОБЛАЧНОМ ХРАНИЛИЩЕ

Драган З. Дамьянович
независимый исследователь, г. Зренянин, Республика Сербия

РУБРИКА ГРНТИ: 20.23.25 Информационные системы с базами знаний,
81.93.29 Информационная безопасность. Защита информации
ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: В данной статье анализируется влияние вредоносных кодов в облачном хранилище. Вредоносный код − это несанкционированный фрагмент кода, который нарушает целостность приложения и сетевой инфраструктуры, вызывая определенные последствия, такие как: нарушение безопасности, распространение инфекций и проникновение в компьютерные данные с помощью вредоносного программного обеспечения. Иными словами, речь идет о простой краже данных, которая может привести к неизгладимым последствиям во всех сферах общества, угрожая тем самым национальной безопасности. Для того чтобы преодолеть эту проблему, необходимо обнаружить дыры в безопасности облачных сред и устранить их до того, как злоумышленники воспользуются ими для обхода интеграции облачной инфраструктуры.

Методы: В статье использовались: структурно-функциональный анализ, сравнительный анализ и метод синтеза.

Результаты: Существует множество факторов для сбора, сравнения и предоставления разведывательной информации об облачных угрозах. Облачные приложения часто становятся мишенью, поскольку их использование для хранения и обмена данными с хостингом мобильных приложений растет в геометрической прогрессии, что позволяет осуществлять промышленную автоматизацию, мониторинг и сбор деловой информации. Кроме того, миллиарды устройств в интернете используют облачную инфраструктуру в качестве фона для обработки и передачи больших массивов данных. Вредоносный код легко распространяется из-за простоты обмена документами и файлами через облако.

Выводы: Поскольку облачные технологии занимают центральное место в мире цифровой трансформации, предполагается, что угроза облачной среде будет экспонциально расти. Это означает, что для того чтобы минимизировать бизнес-риски организациям необходимо обеспечить сверхнадежную систему кибербезопасности облачной инфраструктуры, которая сможет противостоять всем угрозам безопасности. Понимание характера практических средств контроля безопасности и способов их оценки поможет организациям выработать практический подход к обеспечению безопасности и конфиденциальности в облаке.

Ключевые слова: вредоносный код, облако, вредоносное ПО, интеллект.

ЗЛОНАМЕРНИ КОД У ОБЛАКУ

Драган З. Дамјановић
независни истраживач, Зрењанин, Република Србија

ОБЛАСТ: информационе технологије
ВРСТА ЧЛАНКА: прегледни рад

Сажетак:

Увод/циљ: У раду је извршена анализа утицаја злонамерних кодова у облаку. Злонамерни код (малвер) неовлашћени је део кода који нарушава интегритет апликације и инфраструктуре како би изазвао одређене ефекте, као што су нарушавање безбедности, ширење инфекције и инфилтрација података са рачунара уз помоћ злонамерног софтвера (ради се о једноставнијој крађи података, која може довести до погубних последица у свим сегментима друштва, посебно када је у питању национална безбедност). Како би се овај изазов превазишао, неопходно је открити безбедносне рупе у окружењима у облаку и поправити их пре него што нападачи искористе ове недостатке и заобиђу интегритет инфраструктуре облака.

Методе: Структурна анализа, функционална анализа, компаративна анализа, синтеза.

Резултати: Постоји много метода за прикупљање, поређење и достављање обавештајних података о претњама у облаку. Клоуд апликације су све чешће на мети актера претњи, јер се употреба апликација у облаку за складиштење и дељење датотека са хостингом мобилних апликација, које омогућавају индустријску аутоматизацију, праћење и прикупљање пословних информација, експоненцијално повећала. Поред тога, милијарде уређаја на интернету користе инфраструктуру облака као позадину за обраду и пренос великих скупова података. Злонамерни код се лако дистрибуира због лакоће дељења докумената и датотека преко облака.

Закључак: Како технологије облака заузимају централно место у свету дигиталне трансформације, очекује се да ће претње окружењима у облаку експоненцијално расти. То значи да организације треба да обезбеде да сајбер безбедносна позиција инфраструктуре облака коју поседују буде довољно робустна и зрела за борбу против свих релевантних безбедносних претњи како би се минимизирали пословни ризици. Разумевање природе практичних безбедносних контрола и начина на који се оне процењују омогућавају организацијама да изграде практичан приступ безбедности и приватности у облаку.

Кључне речи: злонамерни код, облак, малвер, интелигенција.

Paper received on / Дата получения работы / Датум пријема чланка: 25.03.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.06.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24.06.2022.

САВРЕМЕНО НАОРУЖАЊЕ И ВОЈНА ОПРЕМА
СОВРЕМЕННОЕ ВООРУЖЕНИЕ И ВОЕННОЕ ОБОРУДОВАНИЕ
MODERN WEAPONS AND MILITARY EQUIPMENT

Конвенционалне подморнице остају дуже под водом[1]

Подморничке снаге имају све већу потребу за дејствовањем у приобалним водама у дужем интервалу.

Захваљујући својим способностима да остану невидљиве током боравка испод воде, дизел-електричне подморнице постају врло ефикасне платформе за забрану и одвраћање пловидбом морским површинама.

Међутим, за разлику од нуклеарних подморница, дизел-електричне подморнице не могу неограничено остати под водом због ограничења енергетског складиштења. Дизел-електричне подморнице на површини користе своје дизел-генераторе за стварање електричне енергије, али се они гасе приликом зароњавања, па се електрична енергија за погон и друге оперативне системе, као и за системе одржавања, обезбеђује из акумулатора.

Подморница шведске морнарице класе Gotland користи погон независан од ваздуха Stirling, снаге 75 kW, који јој омогућује да се две недеље креће под водом брзином до 4 чвора

Дизел-мотори не раде док је подморница под водом, јер им је потребан кисеоник за сагоревање горива, а поред тога емитују штетне гасове. Када се акумулатори истроше, дизел-електрична подморница мора да изрони потпуно или на дубину перископа како би могла употребити шноркел који би усисавао свеж ваздух помоћу кога би прорадили дизел-мотори и генератори, чиме би почео процес пуњења акумулатора.

[1] Janes Navy International January February 2021

Израњање подморнице на површину или на дубину перископа је опасно, јер може бити лакше откривена и нападнута. Чак и при малим брзинама, подморница која користи оловне акумулаторе мора да израони на дубину перископа сваких три до пет дана ради пуњења акумулатора. Ту би дошао до изражаја погон независан од ваздуха, који користи хемијске или електричне процесе ради генерисања струје.

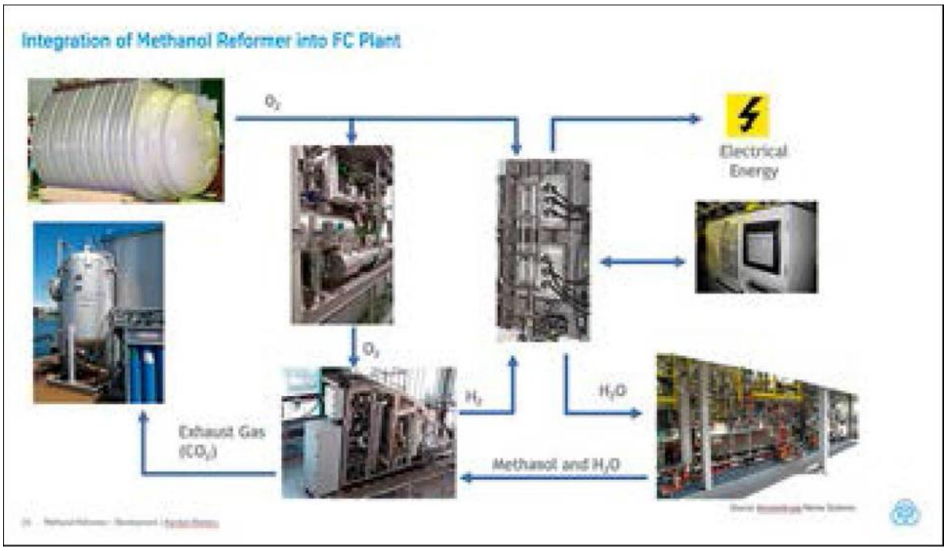
Системи независни од ваздуха укључују дизел-моторе затвореног циклуса, горивне ћелије као и погоне *Stirling*. Сви ови системи захтевају кисеоник и гориво. Кисеоник се складишти криогено у резервоарима као течност под ниским-средњим притиском и употребљава се за производњу струје у горивним ћелијама и конверторском систему за производњу водоника. Овај процес може генерисати довољно струје која би дизел-електричној подморници омогућио останак под водом и до три недеље.

Алтернативни приступи

Циклични систем независан од ваздуха под називом *Stirling* развила је шведска компанија *Kockums* (сада у власништву компаније *Saab*) и први пут је уграђен у подморнице шведске ратне морнарице крајем осамдесетих година. *Stirling* је топлотни погон који користи стандардно дизел-гориво са малим процентом сумпора и ускладиштеног кисеоника. Извор топлоте долази од константног горења, али без експлозија карактеристичних за обичан дизел-мотор. На тај начин погон је врло тих и без вибрација. Енергија се користи за грејање радне течности, у овом случају инертног гаса, који се шири и скупља када је охлађен што покреће цилиндре који покрећу мотор.

Мотор је повезан са перманентним магнетским генератором који се налази у простору који је звучно изолован, а који генерише струју и пуни акумулаторе. Једини издувни гас је угљен-диоксид који се раствара у расхладној течности пре него што буде избачен са подморнице. Овакав поступак обезбеђује да се не појаве мехури који би могли открити положај подморнице. Део поступка сагоревања који ствара топлотну енергију је спољни у односу на део погона независног од ваздуха који конвертује топлотну енергију у механичку. То значи да постоји могућност бољег управљања издувним производима и проблемима акустике. Подморница класе *Gotland* користи два система независна од ваздуха типа *Stirling,* снаге од по 75 kW. Овакав погон омогућава подморници да остане под водом две недеље развијајући брзину до 4 чвора.

Алтернатива систему независном од ваздуха је водонична горивна ћелија, технологија коју је почела да развија компанија *Siemens* у сарадњи са немачким бродоградилиштем *Howaldtswerke Deutsche Werft (HDW)* које сада припада компанији *Thyssen Krupp Marine Systems (TKMS).* Водоничне горивне ћелије користе водоник и кисеоник у процесу електролизе за генерисање струје. Компанија *Siemens* употребљава полимерску електролитску мембрану или мембрану за размену протона за своју горивну ћелију типа *SINAVY PEM.* У оваквом систему модули горивних ћелија смештени су заједно са системом погона независног од ваздуха и заједно генеришу струју за акумулаторе и електрични мотор.



Integration of Methanol Reformer into FC Plant

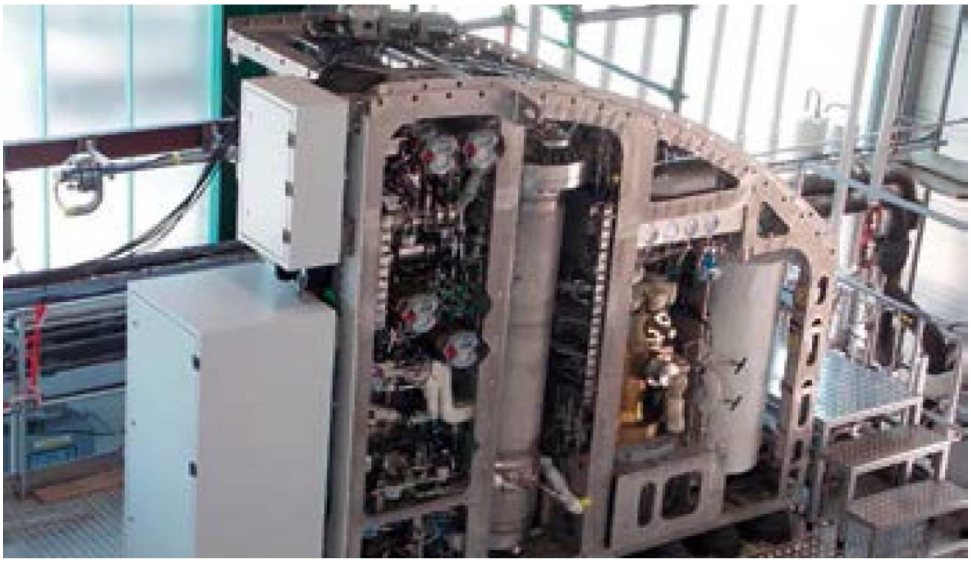
Дијаграм система TKMS/SENER MRFC који интегрише конвертер метанола у систем горивних ћелија у метал-хидридне цилиндре. Употреба овог система, као извора водоника који снабдева горивну ћелију, значи да подморница не мора ускладиштити водоник.

Предност горивне ћелије јесте да она као нуспроизвод ствара воду и топлоту, што је лако уклонити за разлику од штетних гасова од сагоревања горива. Међутим, изазов за горивне ћелије се састоји од потребе складиштења велике количине водоника. Складиштење запаљивих гасова као што је водоник под високим притиском, нарочито у затвореном простору подморнице, може бити опасно иако примена металних хидрида донекле помаже у овој ситуацији. Ипак, иако су развијене безбедносне процедуре за складиштење водоника под нижим притиском и ван трупа, и даље постоји забринутост да је тај поступак врло скуп и да компликује допуњавање горивом.

Решење за складиштење водоника је у употреби реагенсног горива које би стварало водоник у самој подморници. Компанија *SENER,* у сарадњи са компанијом *TKMS,* настоји да реши безбедносне проблеме горивних ћелија погона независног од ваздуха. Проблем је у томе што је погон независан од ваздуха ограничен складишним простором, јер подморница може носити само одређени број цилиндара са водоником.

Ова компанија развија горивну ћелију са метанолом као реагенсом, где погон независан од ваздуха добија водоник тако што га извлачи из метанола.

Компанија наводи да је складиштење метанола у течном стању много безбедније него складиштење водоника, а да је процес екстраховања водоника из метанола већ доказан у комерцијалној сфери. Такође, тврди се да је овај процес ефикаснији и да се као нуспроизвод јавља само мала количина угљен-диоксида.



Систем екстраховања водника из метанола

Горивна ћелија са метанолом као реагенсом ради кроз парно реформатовање метанола. Кисеоник се доводи у реформатор под високим притиском у облику гаса на околној температури. То смањује потрошњу енергије током процеса конверзије. У овом процесу се течни кисеоник ниског притиска у резервоару доводи у помоћни контејнер где делимично испарава, а притисак повећава све док не достигне високе вредности и испари помоћу воде, а затим гас одлази у реформатор.

Ради континуиране испоруке кисеоника употребљава се други помоћни контејнер за спровођење истог процеса када је први контејнер испражњен и депресуризован за поновни почетак процеса у коме се снабдева реформатор.

Горионик који ради на кисеоник обезбеђује топлотну енергију која загрева вишак воде из горивне ћелије у пару. Реформатор одваја водоник, угљен-диоксид, угљен-моноксид и воду, који затим одлазе у модул за пречишћавање. То екстрахује чисти водоник за употребу у горивним ћелијама, а угљен-диоксид се раствара у морској води ради одлагања.

Главни технолошки изазов јесте спровођење процеса у тихим условима, без компромитовања подморнице. Због тога је потребно да се гас у потпуности раствори тако да се појаве мехури ваздуха у води. Дакле, систем избацује гас у морску воду у облику мехурића чиме се завршава процес растварања.

Количина ускладиштеног метанола зависи од оперативних захтева погона независног од ваздуха. Ради смањења просторног захтева ускладиштени метанол се налази у неколико структурних резервоара. Празни резервоари метанола користе се за складиштење воде коју производи погон независан од ваздуха, тако да је тежина равномерно компензована.

Реформатирање помоћу дизел-горива

Претходни погон независан од ваздуха француске компаније *Naval Group* носи назив *Module d'Energie Sous-Marin Autonome (MESMA)*; ради се о парној турбини затвореног циклуса која сагорева етанол и ускладиштени кисеоник. Процес производи топлоту која покреће парни генератор, турбину и алтернатор који генерише струју. Међутим, овај систем користи велику количину кисеоника у процесу што га чини мање ефикасним, иако обезбеђује високу излазну снагу од 200 kW, која омогућава две недеље подводних операција брзином од 4 чвора.

Компанија *Naval Group* сада ради на новој водоничној горивној ћелији друге генерације *Fuel Cell 2nd Generation (FC2G) AIP system* која је приказана 2018. године на изложби поморског наоружања у Паризу. Компанија је изнела решење складиштења водоника за реформатор дизела. Навела је да претходне генерације погона независних од ваздуха карактерише висока потрошња кисеоника и/или врло мала густина горива. Оба захтевају велике количине ускладиштеног реагенса, ограничавајући укупну количину енергије која се може обезбедити. Овај погон независан од ваздуха карактеришу смањена потрошња кисеоника са великом густином горива, што омогућава значајно унапређење у густини енергије.

Према компанији *Naval Group,* смештање хидридних цилиндара ван подморнице представља ризични изазов у смислу подморничке архитектуре и баланса тежине, а уз то је неефикасно. Наиме, од 160 тона хидрида који се транспортују као део погона независног од ваздуха, само 1% чини водоник који се може употребити у горивној ћелији, што је неефикасно и скупо. Ту су и импликације логистичке подршке пуњења подморница горивом ултрачистим водоником и кисеоником које захтевају посебне објекте за третман гаса, камионе који су кондиционирани у складу са строгим прописима за транспорт водоника, као и квалификације и процедуре за одржавање чистоће водоника и обезбеђивање интегритета подморнице и њене посаде. Према компанији, то је сложен и скуп логистички ланац, који, штавише, није доступан ни у једној луци.

Анализа коју је спровела компанија *Naval Group* показала је да у поређењу са другим изворима водоника, као што је метанол, дизел- гориво има вишу тачку паљења, што смањује ризик од пожара. Такође, најмање је токсичан када је изложен, а посаде су обучене за руковање њиме. Процес његовог утовара и истовара је једноставан, доступан је широм света, а што се тиче перформанси има бољи енергетски одзив и густину водоника.

Тестирање новог погона независног од ваздуха FC2G који користи дизел-гориво као извор водоника за горивне ћелије

Сматрало се да је метанол превелики ризик: у случају цурења његова висока токсичност за људе и кратко време реакције угрозили би период у којем би подморница могла да остане под водом. Компанија *Naval Group* је саопштила да је метанол веома запаљив на температури од 12°Ц навише, што је прекорачење у свим условима рада подморнице. Дизел је пожељнији с обзиром на то да је једино гориво које није запаљиво, односно улази у запаљиво стање на температури већој од 55°Ц. .

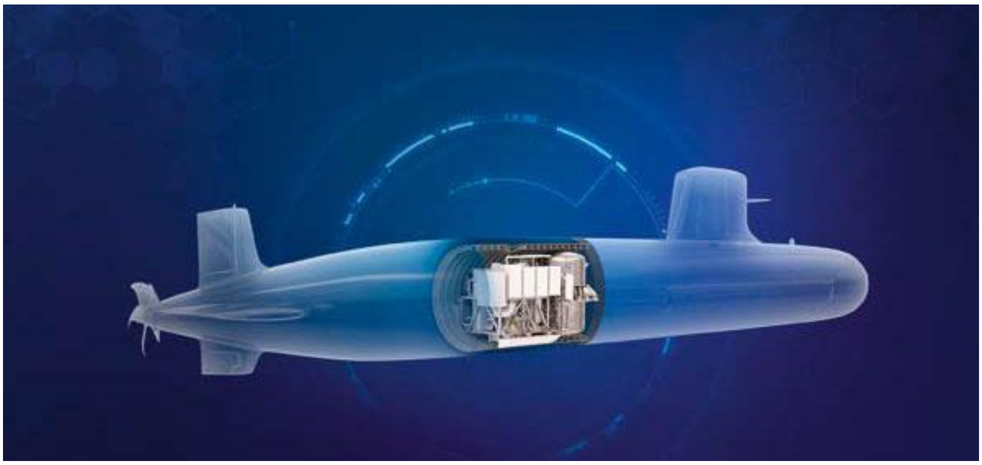
За производњу водоника у систем *FC2G* гориво се сагорева да би се обезбедио извор топлоте ради добијања температуре потребне за обраду течности (што треба да се одржава кроз процес каталитичког реформисања). Компанија *Naval Group* је навела да оксидирано дизел-гориво даје више топлоте као извор енергије од метанола за око 130% и да то чини ефикасније. Такође, има већу густину водоника, садржи 20% више водоника по литру у поређењу са метанолом.

Главне компоненте система *FC2G* укључују реформатор, који се напаја дизел-горивом, кисеоником и паром (која се рециклира), претварајући ову мешавину у синтетички гас богат водоником. „Промена реактора” покреће реакцију „померања воде-гаса” која претвара угљен-моноксид у угљен-диоксид, заједно са конверзијом воде у водоник. То повећава садржај водоника у синтетичком гасу на максимум који је доступан и елиминише већину угљен-моноксида, повећавајући принос водоника.

Гас затим пролази кроз мембране за пречишћавање израђене од специјалних металних легура које пропуштају само водоник, чиме се одваја од синтетичког гаса који се задржава унутар цеви. То осигурава чистоћу водоника који се користи у *PEM* горивим ћелијама за производњу електричне енергије. Кисеоник за горивну ћелију долази из истих модула за складиштење развијених за *MESMA* систем који такође обезбеђује кисеоник за контролу атмосфере подморнице, али је уместо тога помешан са азотом како би се олакшала његова употреба у *PEM* горивној ћелији.

Све компоненте су интегрисане на посебном делу са еластичним монтажама и висећим постољима како би се избегао било какав утицај на акустични потпис.

Дизајн реактора за реформисање и катализатора модификован је тако да мешавина реагенса и температура реакције избегавају стварање чађи, што је део изазова у развоју водоничних горивних ћелија да се пронађе прави баланс између перформанси и издржљивости.

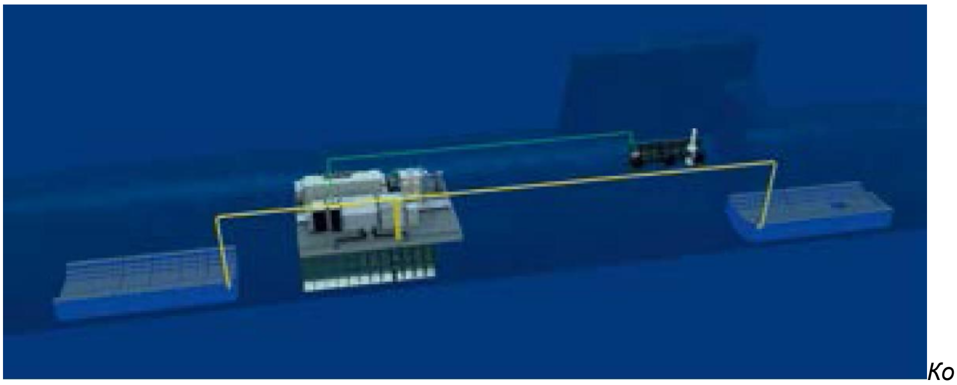


Нови систем FC2G независан од ваздуха који се види као модул у оквиру дизајна подморнице Scorpene, компаније Naval Group. Очекује се да ће компанија понудити ову могућност будућим корисницима својих подморница класе Scorpene како се потражња за погоном независним од ваздуха повећава.

Управљање термичком интеграцијом и смањење потрошње кисеоника су, такође, суштински елементи система. Компанија *Naval Group* наводи да се термичком интеграцијом управља враћањем калорија преко измењивача топлоте , што оптимизује ефикасност и минимизира потрошњу кисеоника. Штавише, дизајн хемијског реактора постављен је да повећа ефикасност кисеоника до максимума, као и да омогући одговарајућу издржљивост. То је посебно важно, јер ће одлучујући фактор у оперативној издржљивости бити потрошња кисеоника, па је цео процес у функцији оптимизације.

За систем *FC2G* емисије угљен-диоксида избацују се из подморница на исти начин као и код система *MESMA* и у нуклеарним подморницама. Компанија *Naval Group* је саопштила да постоје две оперативне предности: прво, систем ради под високим притиском, што му омогућава да се користи у читавом опсегу оперативних дубина подморнице без потребе за додатним актуатором затвореним на издувном систему, друго, третман пре пражњења спречава да он утиче на акустични и инфрацрвени потпис подморнице, постижући његово растварање неколико метара од подморнице.

Систем *FC2G* је развијен од индустријских горивних ћелија да би имао користи од побољшања доступних на комерцијалном тржишту, али је затим прилагођен да задовољи потребе морнарице. Развој је био фокусиран на збијање горивних ћелија, узимајући у обзир типичне потребе подморнице за простором, као и разматрања везана за одржавање, односно олакшавање укрцавања, искрцавања и приступа посади. Још један кључни аспект прилагођавања подморском окружењу је строга контрола емисије водоника на броду. Горивне ћелије су дизајниране тако да им није потребно складиште водоника за рад, заједно са дубоким смањењем протока прочишћавања. То омогућава већу контролу квалитета атмосфере и бољу безбедност када систем независан од ваздуха није у употреби.



Ко

Компјутерска слика најбољег погона независног од ваздуха уграђеног у нове подморнице S-80P шпанске морнарице. Компанија Navantia се одлучила за реформаторски систем етанола као метод за производњу водоника за своју горивну ћелију.

Систему *FC2G* потребно је шест сати да се покрене, што укључује загревање свих компоненти, посебно реформатора, како би се постигла максимална ефикасност. Систем се укључује непосредно пре достизања тачке зарањања, тако да је спреман за употребу када то захтева командант подморнице.

Компанија не верује да ће бити потребни додатни чланови посаде подморнице за управљање системом *FC2G,* јер ће то бити још један систем за рад подморнице који ће спроводити исти оператер који врши контролу погона и надгледа систем независан од ваздуха из контролне собе.

Компанија *Naval Group* је потврдила да је систем *FC2G* прошао више од 7.000 сати тестирања на копну како би се оптимизирала ефикасност сваке компоненте и потврдили периоди одржавања. Тестови су обављени са репрезентативним профилом мисије подморнице који је узимао у обзир максимални високи притисак који је подморница издржала и био је повезан са подморничким батеријама и контролисан од једног оператера преко система за управљање интегрисаном платформом.

Током „патролне демонстрације” 2019. године, систем *FC2G* био је квалификован за издржљивост од 18 дана, али са ефикасним процесом који се односи на кисеоник и резервоаре за складиштење може да постигне и до три недеље. Подводна издржљивост, у ствари, зависи од равнотеже између перформанси и тежине платформе коју желе купци, са запремином складиштења течног кисеоника као параметром. Могуће је премашити тронедељну издржљивост, али за сада за ту алтернативу нема интересовања купаца. Компанија *Naval Group* наставља рад на побољшању ефикасности процеса реформисања за већу оперативну доступност, укључујући оптимизацију термичке интеграције са мањом потрошњом кисеоника и већом производњом водоника уз напредак у материјалима за смањење величине и тежине и лакоћу одржавања.

Алтернативе погону независном од ваздуха

Од појаве технологија за погон независан од ваздуха за подморнице и њихове доступности на међународном тржишту, читав низ земаља је набавио нове подморнице и избегавао ову опцију. Иако из доступних информација није могуће прецизно утврдити који су разлози за такву одлуку, може се говорити о неколико општих трендова. Државе као што су Бангладеш, Индонезија, Мијанмар и Вијетнам изабрали су подморнице које немају погон независан од ваздуха због приступачности. Алжир тренутно не размишља о таквом погону због трошкова у својој флоти. У међувремену, одлука Бразила је вероватно узела у обзир планове да његове подморнице на нуклеарни погон преузму дугорочне дужности, док Русија, због постојећег развијеног дизајна нуклеарних и обичних дизел-електричних подморница, за сада не разматра ове опције.

Јапан је више од деценије опремао своје подморнице системом независним од ваздуха *Kockums Stirling AIP,* али је недавно одлучио да прекине ову праксу и примени технологију литијум-јонских батерија. Ове батерије имају значајне предности у односу на класичне акумулаторе и могу за неке оператере постати алтернативно решење за испуњавање њихових потреба за перформансама у будућности.

Кључни фактори перформанси укључују степен нечујности, брзину напредовања и оперативну флексибилност. Погон независан од ваздуха је веома ефикасан, омогућавајући неколико недеља рада под водом, у поређењу са неколико дана за конвенционалну подморницу. Литијум-јонске батерије, у зависности од хемије, имају густину енергије која је више него двоструко већа од оловне батерије за одређену запремину и стога такође имају велики потенцијал.

Још једна предност литијум-јонских батерија јесте да се могу пунити брже од оловних батерија и до било ког степена. Оне не само да смањују време изложености близу површине током употребе шноркела већ и смањују ограничења која су инхерентна при пуњењу класичне оловне батерије у фазама.

Литијум-јонске батерије такође нуде неке предности подводне брзине. Пуна снага батерије је доступна у свим стањима напуњености, дајући више опција убрзавања за подморницу које се јављају чешће када се комбинују са поменутим карактеристикама пуњења. Типичне инсталације погона независног од ваздуха имају тенденцију да обезбеде издржљивост и домет при малим брзинама, али се и даље ослањају на инсталиране батерије за већу брзину напредовања.

Још једна предност коју нова технологија батерија може да пружи у поређењу са оловним јесте смањена сложеност система подршке за батерије. Ради се о смањењу захтева за циркулацијом киселине, хлађењем, вентилацијом и испирањем, јер се ризици од корозивних течности и експлозивних гасова могу избећи дизајном затворених литијум-јонских ћелија које се не одржавају.

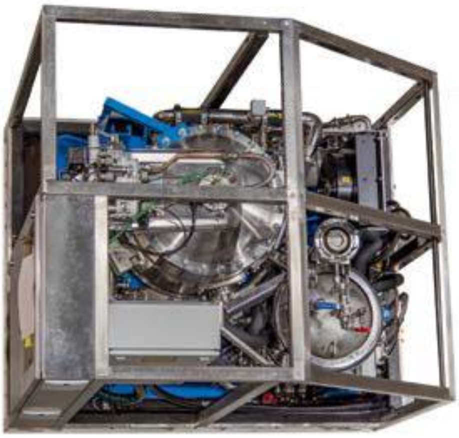
У зависности од оперативних захтева, нека литијум-јонска подешавања могу донети побољшања у односу на традиционалне системе оловних батерија и могу се упоредити са сложеношћу, захтевима за простором за реагенсе и машине, трошковима набавке током целог века одржавања и лакоћом допуњавања горива разних система погона независним од ваздуха. Међутим, литијум-јонска технологија се и даље суочава са неким изазовима, међу којима је и постизање потребних нивоа безбедности за употребу у подморницама у односу на поузданост доказаних оловних батерија које се користе више од једног века.

Комбинација нових батерија и погона независним од ваздуха у међувремену обећава да ће још више затворити јаз између подморница на конвенционални погон и подморница на нуклеарни погон, пре свега у контексту веће цене.

Одржива решења

Шпанско бродоградилиште Navantia такође је развило сопствени систем горивних ћелија под називом *Bio-Ethanol Stealth Technologies (BEST),* који користи реформатор етанола за производњу водоника. *Navantia* је развила систем у партнерству са шпанском морнарицом и компанијама *Collins Aerospace, Abengoa,* и *Bionet*. Компанија *Collins* је испоручила *PEM* горивну ћелију, која је посебно дизајнирана за војне операције. Компанија *Abengoa* је развила минијатурни био-етанолни реформатор, а компанија *Bionet* систем за одлагање угљен-диоксида. *BEST* такође укључује систем за подешавање снаге и контролни систем. Главне компоненте могу се заменити кроз логистички отвор од 800 мм у подморници. Према компанији *Navantia* погон обезбеђује 300 kW снаге и њиме се управља преко система за управљање интегрисаном платформом.

Процес реформисања етанола је сличан оном који се користи за дизел-гориво и реформисање метанола у системима *MRFC* и *FC2G.* Процес се састоји од две фазе каталитичке реакције, почевши од реформисања горива, која разлаже угљоводоник у водоник и друге нуспроизводе као што су угљен-диоксид, метан или угљен-моноксид. Након тога следи пречишћавање тока реформатора, што повећава производњу водоника и смањује угљен-моноксид. Компанија *Navantia* навела је да је главна разлика система компанија *Naval Group* или *SENER* у томе што су *BEST* горивне ћелије дизајниране тако да раде директно на реформатираном гасу, док друге захтевају реформисање под високим притиском и мембране како би се добио чисти водоник, што овај систем чини једноставнијим и поузданијим.



Систем Stirling, који је у употреби од 80-их година, ажурира се како би се осигурало да остане конкурентан новим системима заснованим на горивним ћелијама.

Према компанији *Navantia,* ћелије су израђене од порозних биполарних плоча за пасивно управљање водом и равномерно, континуирано мембранско влажење без потребе за овлаживањем или системима за уклањање течне воде. Овај напредни дизајн не само да чини горивну ћелију једноставнијом на нивоу система већ, такође, обезбеђује двоструки радни век у поређењу са тржишним стандардом који ради на реформатираном гасу и чистом кисеонику (не ваздуху). Тиме се избегава потреба за системима за пречишћавање водоника, као што је мембрана, или симулацијом ваздуха, што је додатно поједностављење система.

Развој је завршен у фебруару 2020. године. Компанија *Navantia* је заговарала употребу биоетанола због његове доступности, лакоће руковања, његове безбедности, као и због високог нивоа ефикасности уз минималне конверзије.

Компанија је саопштила да постоје ограничења у коришћењу других горива. Дизел-гориво потребно за реформатирање захтева посебне процесе и опрему за уклањање сумпора пре укрцавања. Наиме, реформатирање за производњу водоника са алкохолом трајније је и робустније у поређењу са другим угљоводоничним горивима. Метанол је такође алкохол, али је веома токсичан и канцероген, што представља додатни безбедносни изазов за дизајн платформе.

Коришћење биогорива (биоетанола уместо синтетичког етанола) има додатне предности које се односе на логистику, доступност у било којој земљи са развијеном пољопривредном индустријом, и вођење бриге о одрживости животне средине. Систем *BEST* је дизајниран да омогући подморници да остане под водом до три недеље, а планирано је да буде инсталиран у нове подморнице шпанске морнарице *Isaac Peral (S-80 Plus)*, почевши са трећом подморницом из класе *Cosme Garcia (S 83).* Прве две подморнице се већ увелико граде, тако да ће добити систем *BEST* током свог првог већег ремонта.

Међутим, увођење система горивних ћелија заснованих на реформатору не значи да је складиштење метал-хидрида прошлост. У септембру 2019. на Конференцији о подморницама у Килу, у Немачкој, компанија *TKMS* је лансирала сопствени нови погон независан од ваздуха *FC4G,* назвавши га системом четврте генерације. У саопштењу за штампу компанија је навела да овај систем побољшава доступност, редундантност и невидљивост на основу „модуларног система састављеног од редундантних компоненти" који наставља да користи металне хидридне цилиндре за складиштење водоника. Ускладиштени водоник се и даље користи у подморницама и, упркос тврдњама о супротном.

Stirling еволуира

Компаније *Saab Kockums* и *FMV* и даље верују у развој Стирлинговог погона независног од ваздуха. Потреба горивне ћелије за водоником, било да се складишти у резервоарима или је производи реформатор, озбиљно ограничава систем.

Подморнице које складиште водоник у резервоарима имају неколико стотина тона цеви у којима се налази водоник. За пуњење ових резервоара потребно је неколико контејнера у поморској бази и 10 до 12 великих приколица са водоником, а сам процес пуњења траје отприлике 36 сати.

Претпоставља се да је то предуго за подморницу у луци у ратном сценарију. Подморница са погоном независним од ваздуха *Stirling* може много брже напунити све залихе – дизел, оружје, храну итд. Допуна се, такође, може извршити на мору са било ког брода за снабдевање. Ћелије се и даље морају послати назад добављачу на одржавање. Ако систем горивних ћелија добије водоник из реформатора, вишак се изненада драматично смањује. Још не постоји оперативна подморница са реформатором, али ако икада буде постојала вероватно ће бити само један реформатор на броду, док систем *Stirling* има велики број појединачних мотора, нуди доста редундантности и погодан је за одржавање на мору.

Компанија *FMV* је проценила да би, када се ради о трошковима, упоредиви систем горивних ћелија на подморници морао бити бар десет пута већи у поређењу са системом *Stirling*, са истим односом који се односи на допуну горива и кисеоника. Систем *Stirling* је веома робустан и исплатив. То је систем који ради у ратном сценарију, јер је логистика врло једноставна у поређењу са системом горивних ћелија.

Систем *Stirling* је достигао своју пету итерацију. Најновија верзија, позната као *Double Stirling Module (DSM),* комбинује два *Stirling* мотора од 75 kW (генеришући комбиновану снагу од 150 KW) у простору који је претходно заузимао један модул. То је постигнуто побољшањем интеграције свих компоненти система како би се минимизирао физички отисак на броду. Постоје неке компоненте са веома високом доступношћу које би могле да се деле између два или више мотора без ризика од укупне редундантности и доступности, што ће резултирати компактнијим системом са више инсталиране енергије по јединици запремине.

Енергетска ефикасност је од суштинског значаја како би се обезбедило максимално коришћење расположиве електричне енергије. Компанија *Saab Kockums* развија начине да искористи отпадну топлоту из мотора *Stirling* за загревање унутрашњости чамца или регенерацију јединица за апсорпцију угљен-диоксида.

Друга област која се разматра јесте коришћење паре за производњу хладне воде у систему за апсорпцију. На тај начин могли би сезаменити бучни компресори веома тихим пумпама и истовремено уштедети електрична енергија.

У току су истраживачки програми који испитују различита горива са већом густином енергије од дизела како би се искористила способност мотора *Stirling* да користи било који извор топлоте. За сада су резултати веома обећавајући, а у року од неколико година очекује се да се издржљивост још више повећа.

Драган М. Вучковић (*Dragan* M. Vučković),
e-mail: draganvuckovic64@gmail.com,
ORCID iD: https://orcid.org/0000-0003-1620-5601

ПОЗИВ И УПУТСТВО АУТОРИМА

ПРИГЛАШЕНИЕ И ИНСТРУКЦИЯ ДЛЯ АВТОРОВ РАБОТ

CALL FOR PAPERS AND INSTRUCTIONS FOR AUTHORS

ПОЗИВ И УПУТСТВО АУТОРИМА О НАЧИНУ ПРИПРЕМЕ ЧЛАНКА

Упутство ауторима о начину припреме чланка за објављивање у Војнотехничком гласнику урађено је на основу Правилника о категоризацији и рангирању научних часописа Министарства просвете, науке и технолошког развоја Републике Србије ("Службени гласник РС", број 159/20). Примена овог Правилника првенствено служи унапређењу квалитета домаћих часописа и њиховог потпунијег укључивања у међународни систем размене научних информација.

Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier (втг.мо.упр.срб, www.vtg.mod.gov.rs, ISSN 0042-8469 – штампано издање, e-ISSN 2217-4753 – online, UDC 623+355/359, DOI: 10.5937/VojnotehnickiGlasnik; https://doi.org/10.5937/VojnotehnickiGlasnik), јесте рецензирани међународни научни часопис.

Власници часописа су Министарство одбране Републике Србије и Војска Србије. Издавач и финансијер часописа је Универзитет одбране у Београду (Војна академија).

Програмска оријентација часописа заснива се на годишњој категоризацији часописа, коју врши надлежно државно министарство у одређеним областима, као и на његовом индексирању у међународним индексним базама.

Часопис обухвата научне, односно стручне области у оквиру образовно-научног поља **природно-математичких наука**, као и у оквиру образовно-научног поља **техничко-технолошких наука**, а нарочито области **одбрамбених наука и технологија**. Објављује теоријска и практична достигнућа која доприносе усавршавању свих припадника српске, регионалне и међународне академске заједнице, а посебно припадника војски и министарстава одбране. Публикује радове са уравнотеженим извештавањем о аналитичким, експерименталним и примењеним истраживањима, као и нумеричким симулацијама, обухватајући различите дисциплине. Објављени материјали су високог квалитета и релевантности, написани на начин који их чини доступним широкој читалачкој публици. Сви радови који извештавају о оригиналним теоријским и/или практично оријентисаним истраживањима или проширеним верзијама већ објављених радова са конференција су добродошли. Радови за објављивање одабиру се двоструко слепим поступком рецензије како би се осигурала оригиналност, релевантност и читљивост. Притом циљ није само да се квалитет објављених радова одржи високим већ и да се обезбеди правовремени, темељни и уравнотежени поступак рецензије.

Уређивачка политика Војнотехничког гласника заснива се на препорукама Одбора за етичност у издаваштву (COPE Core Practices), као и на најбољим прихваћеним праксама у научном издаваштву. Војнотехнички гласник је члан COPE (Committee on Publication Ethics) од 2. маја 2018. године.

Министарство просвете, науке и технолошког развоја Републике Србије утврдило је дана 23. 12. 2021. године категоризацију Војнотехничког гласника, за 2021. годину:

– на листи часописа за рачунарске науке:
категорија истакнути национални часопис **(М52)**,

– на листи часописа за електронику, телекомуникације и информационе технологије:
категорија истакнути национални часопис **(М52)**,
– на листи часописа за машинство:
категорија врхунски часопис националног значаја **(М51)**,
– на листи часописа за материјале и хемијске технологије:
категорија врхунски часопис националног значаја **(М51)**.

Усвојене листе домаћих часописа за 2021. годину могу се видети на сајту Војнотехничког гласника, страница *Категоризација часописа*.

Детаљније информације могу се пронаћи и на сајту Министарства просвете, науке и технолошког развоја Републике Србије.

Подаци о категоризацији могу се пратити и на сајту КОБСОН-а (Конзорцијум библиотека Србије за обједињену набавку).

Категоризација часописа извршена је према Правилнику о категоризацији и рангирању научних часописа Министарства просвете, науке и технолошког развоја Републике Србије ("Службени гласник РС", број 159/20).

Часопис се прати у контексту Српског цитатног индекса – СЦИндекс (база података домаћих научних часописа) и Руског индекса научног цитирања (РИНЦ). Подвргнут је сталном вредновању (мониторингу) у зависности од утицајности (импакта) у самим базама и, посредно, у међународним (Clarivate Analytics) цитатним индексима. Детаљи о индексирању могу се видети на сајту Војнотехничког гласника, страница *Индексирање часописа*.

Војнотехнички гласник омогућава и примењује Creative Commons (CC BY) одредбе о ауторским правима. Детаљи о ауторским правима могу се видети на сајту часописа, страница *Ауторска права и политика самоархивирања*.

Радови се предају путем онлајн система за електронско уређивање АСИСТЕНТ, који је развио Центар за евалуацију у образовању и науци (ЦЕОН).

Приступ и регистрација за сервис врше се на сајту www.vtg.mod.gov.rs, преко странице *АСИСТЕНТ* или *СЦИНДЕКС*, односно директно на линку aseestant.ceon.rs/index.php/vtg.

Детаљно упутство о регистрацији и пријави за сервис налази се на сајту www.vtg.mod.gov.rs, страница *Упутство за АСИСТЕНТ*.

Потребно је да се сви аутори који подносе рукопис за објављивање у Војнотехничком гласнику региструју у регистар ORCID (Open Researcher and Contributor ID), према упутству на страници сајта *Регистрација за добијање ORCID идентификационе шифре*.

Војнотехнички гласник објављује чланке на енглеском језику (arial, величина слова 11 pt, проред Single).

Поступак припреме, писања и уређивања чланка треба да буде у сагласности са *Изјавом о етичком поступању* (http://www.vtg.mod.gov.rs/izjava-o-etickom-postupanju.html).

Чланак треба да садржи сажетак са кључним речима, увод (мотивацију за рад), разраду (адекватан преглед репрезентативности рада у његовој области, јасну изјаву о новини у представљеном истраживању, одговарајућу теоријску позадину, један или више примера за демонстрирање и дискусију о представљеним идејама), закључак и литературу (без нумерације наслова и поднаслова). Обим чланка треба да буде до једног ауторског табака (16 страница формата А4 са проредом Single), а највише 24 странице.

Чланак треба да буде написан на обрасцу за писање чланка, који се у електронској форми може преузети са сајта на страници *Образац за писање чланка*.

Наслов

Наслов треба да одражава тему чланка. У интересу је часописа и аутора да се користе речи прикладне за индексирање и претраживање. Ако таквих речи нема у наслову, пожељно је да се придода и поднаслов.

Текући наслов

Текући наслов се исписује са стране сваке странице чланка ради лакше идентификације, посебно копија чланака у електронском облику. Садржи презиме и иницијал имена аутора (ако аутора има више, преостали се означавају са „et al.“ или „и др.“), наслове рада и часописа и колацију (година, волумен, свеска, почетна и завршна страница). Наслови часописа и чланка могу се дати у скраћеном облику.

Име аутора

Наводи се пуно име и презиме (свих) аутора. Веома је пожељно да се наведу и средња слова аутора. Имена и презимена домаћих аутора увек се исписују у оригиналном облику (са српским дијакритичким знаковима), независно од језика на којем је написан рад.

Назив установе аутора (афилијација)

Наводи се пун (званични) назив и седиште установе у којој је аутор запослен, а евентуално и назив установе у којој је аутор обавио истраживање. У сложеним организацијама наводи се укупна хијерархија (нпр. Универзитет одбране у Београду, Војна академија, Катедра природно-математичких наука). Бар једна организација у хијерархији мора бити правно лице. Ако аутора има више, а неки потичу из исте установе, мора се, посебним ознакама или на други начин, назначити из које од наведених установа потиче сваки од наведених аутора. Афилијација се исписује непосредно након имена аутора. Функција и звање аутора се не наводе.

Контакт подаци

Адреса или е-адреса свих аутора даје се поред имена и презимена аутора.

Категорија (тип) чланка

Категоризација чланака обавеза је уредништва и од посебне је важности. Категорију чланка могу предлагати рецензенти и чланови уредништва, односно уредници рубрика, али одговорност за категоризацију сноси искључиво главни уредник.

Чланци у *Војнотехничком гласнику* класификују се на научне и стручне чланке.

Научни чланак је:

– оригиналан научни рад (рад у којем се износе претходно необјављени резултати сопствених истраживања научним методом);

– прегледни рад (рад који садржи оригиналан, детаљан и критички приказ истраживачког проблема или подручја у којем је аутор остварио одређени допринос, видљив на основу аутоцитата);

– кратко или претходно саопштење (оригинални научни рад пуног формата, али мањег обима или прелиминарног карактера);

– научна критика, односно полемика (расправа на одређену научну тему, заснована искључиво на научној аргументацији) и осврти.

Изузетно, у неким областима, научни рад у часопису може имати облик монографске студије, као и критичког издања научне грађе (историјско-архивске, лексикографске, библиографске, прегледа података и сл.), дотад непознате или недовољно приступачне за научна истраживања.

Радови класификовани као научни морају имати бар две позитивне рецензије.

Ако се у часопису објављују и прилози ваннаучног карактера, научни чланци треба да буду груписани и јасно издвојени у првом делу свеске.

Стручни чланак је:

– стручни рад (прилог у којем се нуде искуства корисна за унапређење професионалне праксе, али која нису нужно заснована на научном методу);

– информативни прилог (уводник, коментар и сл.);

– приказ (књиге, рачунарског програма, случаја, научног догађаја, и сл).

Пожељно је да обим кратких саопштења буде 4 до 7 страница, научних чланака и студија случаја 10 до 14 страница, док прегледни радови могу бити и дужи. Број страница није строго ограничен и, уз одговарајуће образложење, пријављени чланци такође могу бити дужи или краћи.

Ако су радови који су претходно објављени на конференцији проширени, уредници ће проверити да ли је додато довољно новог материјала који испуњава стандарде часописа и квалификује поднесак за поступак рецензије. Додати материјал не сме бити претходно објављен. Нови резултати нису нужно потребни, али су пожељни. Међутим, поднесак треба да садржи проширене кључне идеје, примере, разраде, итд., који су претходно били садржани у поднеску са конференције.

Језик рада

Језик рада треба да буде енглески.

Текст мора бити језички и стилски дотеран, систематизован, без скраћеница (осим стандардних). Све физичке величине морају бити изражене у Међународном систему мерних јединица – SI. Редослед образаца (формула) означава се редним бројевима, са десне стране у округлим заградама.

Сажетак

Сажетак јесте кратак информативан приказ садржаја чланка који читаоцу омогућава да брзо и тачно оцени његову релевантност. У интересу је уредништава и аутора да сажетак садржи термине који се често користе за индексирање и претрагу чланака. Саставни делови сажетка су увод/циљ истраживања, методи, резултати и закључак. Сажетак треба да има од 100 до 250 речи и треба да се налази између заглавља (наслов, имена аутора и др.) и кључних речи, након којих следи текст чланка.

Кључне речи

Кључне речи су термини или фразе које адекватно представљају садржај чланка за потребе индексирања и претраживања. Треба их додељивати ослањајући се на неки међународни извор (попис, речник или тезаурус) који је најшире прихваћен или унутар дате научне области. За нпр. науку уопште, то је листа кључних речи Web of Science. Број кључних речи не може бити већи од 10, а у интересу је уредништва и аутора да учесталост њихове употребе буде што већа. У чланку се пишу непосредно након сажетка.

Систем АСИСТЕНТ у ту сврху користи специјалну алатку KWASS: аутоматско екстраховање кључних речи из дисциплинарних тезауруса/речника по избору и рутине за њихов одабир, тј. прихватање односно одбацивање од стране аутора и/или уредника.

Датум прихватања чланка

Датум када је уредништво примило чланак, датум када је уредништво коначно прихватило чланак за објављивање, као и датуми када су у међувремену достављене евентуалне исправке рукописа наводе се хронолошким редоследом, на сталном месту, по правилу на крају чланка.

Захвалница

Назив и број пројекта, односно назив програма у оквиру којег је чланак настао, као и назив институције која је финансирала пројекат или програм, наводи се у посебној напомени на сталном месту, по правилу при дну прве стране чланка.

Претходне верзије рада

Ако је чланак у претходној верзији био изложен на скупу у виду усменог саопштења (под истим или сличним насловом), податак о томе треба да буде наведен у посебној напомени, по правилу при дну прве стране чланка. Рад који је већ објављен у неком часопису не може се објавити у Војнотехничком гласнику (прештампати), ни под сличним насловом и измењеном облику.

Табеларни и графички прикази

Пожељно је да наслови свих приказа, а по могућству и текстуални садржај, буду дати двојезично, на језику рада и на енглеском језику.

Табеле се пишу на исти начин као и текст, а означавају се редним бројевима са горње стране. Фотографије и цртежи треба да буду јасни, прегледни и погодни за репродукцију. Цртеже треба радити у програму word или corel. Фотографије и цртеже треба поставити на жељено место у тексту.

За слике и графиконе не сме се користити снимак са екрана рачунара програма за прикупљање података. У самом тексту чланка препоручује се употреба слика и графикона непосредно из програма за анализу података (као што су Excel, Matlab, Origin, SigmaPlot и други).

Навођење (цитирање) у тексту

Начин позивања на изворе у оквиру чланка мора бити једнообразан.

Војнотехнички гласник за референцирање (цитирање и навођење литературе) примењује Харвардски систем референци, односно Харвардски приручник за стил (Harvard Referencing System, Harvard Style Manual). У самом тексту, у обичним заградама, на месту на којем се врши позивање, односно цитирање литературе набројане на крају чланка, обавезно у обичној загради написати презиме цитираног аутора, годину издања публикације из које цитирате и, евентуално, број страница. Нпр. (Petrović, 2012, pp.10–12).

Детаљно упутство о начину цитирања, са примерима, дато је на страници сајта *Упутство за Харвардски приручник за стил*. Потребно је да се позивање на литературу у тексту уради у складу са поменутим упутством.

Систем АСИСТЕНТ у сврху контроле навођења (цитирања) у тексту користи специјалну алатку CiteMatcher: откривање изостављених цитата у тексту рада и у попису референци.

Напомене (фусноте)

Напомене се дају при дну стране на којој се налази текст на који се односе. Могу садржати мање важне детаље, допунска објашњења, назнаке о коришћеним изворима (на пример, научној грађи, приручницима), али не могу бити замена за цитирану литературу.

Листа референци (литература)

Цитирана литература обухвата, по правилу, библиографске изворе (чланке, монографије и сл.) и даје се искључиво у засебном одељку чланка, у виду листе референци. Референце се не преводе на језик рада и набрајају се у посебном одељку на крају чланка.

Војнотехнички гласник, као начин исписа литературе, примењује Харвардски систем референци, односно Харвардски приручник за стил (Harvard Referencing System, Harvard Style Manual).

Литература се обавезно пише на латиничном писму и набраја по абецедном редоследу, наводећи најпре презимена аутора, без нумерације.

Детаљно упутство о начину пописа референци, са примерима, дато је на страници сајта *Упутство за Харвардски приручник за стил*. Потребно је да се попис литературе на крају чланка уради у складу са поменутим упутством.

Нестандардно, непотпуно или недоследно навођење литературе у системима вредновања часописа сматра се довољним разлогом за оспоравање научног статуса часописа.

Систем АСИСТЕНТ у сврху контроле правилног исписа листе референци користи специјалну алатку RefFormatter: контрола обликовања референци у складу са Харвардским приручником за стил.

Изјава о ауторству

Поред чланка доставља се *Изјава о ауторству* у којој аутори наводе свој појединачни допринос у изради чланка. Такође, у тој изјави потврђују да су чланак урадили у складу са *Позивом и упутством ауторима* и *Изјавом о етичком поступању часописа*.

Сви радови подлежу стручној рецензији.

Списак рецензената Војнотехничког гласника може се видети на страници сајта *Списак рецензената*. Процес рецензирања објашњен је на страници сајта *Рецензентски поступак*.

Уредништво

Адреса редакције:
Војнотехнички гласник
Вељка Лукића Курјака 33
11042 Београд
e-mail: vojnotehnicki.glasnik@mod.gov.rs.
тел: војни 40-260 (011/3603-260), 066/8700-123

ПРИГЛАШЕНИЕ И ИНСТРУКЦИЯ ДЛЯ АВТОРОВ О ПОРЯДКЕ ПОДГОТОВКИ СТАТЬИ

Инструкция для авторов о порядке подготовки статьи к опубликованию в журнале «Военно-технический вестник» разработана согласно Регламенту о категоризации и ранжировании научных журналов Министерства образования, науки и технологического развития Республики Сербия («Службени гласник РС», № 159/20). Применение этого Регламента способствует повышению качества отечественных журналов и их более полному вовлечению в международную систему обмена научной информацией.

Военно-технический вестник (**Vojnotehnički glasnik / Military Technical Courier**), втг.мо.упр.срб, www.vtg.mod.gov.rs/index-ru.html, ISSN 0042-8469 – печатное издание, e-ISSN 2217-4753 – online, UDK 623+355/359, DOI: 10.5937/VojnotehnickiGlasnik; https://doi.org/10.5937/VojnotehnickiGlasnik, является рецензируемым международным научным журналом.

Собственники журнала: Министерство обороны и Вооруженые силы Республики Србия.

Издатель журнала: Университет обороны в г. Белград (Военная академия).

Программная ориентация журнала основана на ежегодной категоризации журнала, которая производится соответствующим отраслевым министерством, в зависимости от области исследований, а также на его индексировании в международных наукометрических базах данных.

Журнал охватывает научные и профессиональные сферы в рамках учебно-научной области **естественно-математических наук**, а также в рамках учебно-научной области **технико-технологических наук**, особенно в области **оборонных наук и технологии**. В журнале публикуются теоретические и практические достижения, которые способствуют повышению квалификации представителей сербского, регионального и международного академического сообщества, особенно служащих Министерств Обороны и Вооружённых сил. В журнале публикуются статьи со соответствующими обзорами об аналитических, экспериментальных и прикладных исследованиях, а также о численном моделировании, охватывая различные дисциплины. Публикуемые материалы отличаются высоким качеством и актуальностью. Они написаны научным, но понятным и доступным для широкого круга читателей языком. Приветствуются все статьи, сообщающие об оригинальных теоретических и/или практических исследованиях и/или расширенные версии ранее опубликованных статей, представленных на конференциях. Статьи для публикации отбираются путем двойного слепого рецензирования, которое гарантирует оригинальность, актуальность и удобочитаемость. Цель состоит не только в поддержании высокого качества публикуемых статей, но и в обеспечении своевременного, тщательного и соответствующего процесса рецензирования.

Редакционная политика журнала «Военно-технический вестник» основана на рекомендациях Комитета по этике научных публикаций (COPE Core Practices), а также на лучшей практике в научно-издательской деятельности. «Военно-технический вестник» является членом COPE со 2 мая 2018 года.

Министерством образования, науки и технологического развития Республики Сербия утверждена 23 декабря 2021 г. категоризация журнала «Военно-технический вестник» за 2021 год:

– Область компьютерные науки:

высококачественный национальный журнал **(M52)**,

- **Область электроники, телекоммуникаций и информационных технологий:**
  высококачественный национальный журнал **(M52)**,
- **Область машиностроения:**
  ведущий журнал государственного значения **(M51)**,
- **Область материалов и химической технологии:**
  ведущий журнал государственного значения **(M51)**.

С информацией относительно категоризации за 2021 год можно ознакомиться на странице сайта «Военно-технического вестника» *Категоризация Вестника*.

Более подробную информацию можно найти на сайте Министерства образования, науки и технологического развития Республики Сербия.

С информацией о категоризации можно ознакомиться и на сайте КОБСОН (Консорциум библиотек Республики Сербия по вопросам объединения закупок).

Категоризация Вестника проведена согласно Регламенту о категоризации и ранжировании научных журналов Министерства образования, науки и технологического развития Республики Сербия («Службени гласник РС», № 159/20)

Журнал соответствует стандартам Сербского индекса научного цитирования (СЦИндекс/SCIndeks) – наукометрической базы данных научных журналов Республики Сербия, а также Российского индекса научного цитирования (РИНЦ). Журнал постоянно подвергается мониторингу и оценивается количественными наукометрическими показателями, отражающими его научную ценность, в т.ч. опосредованно в международных индексах цитирования (Clarivate Analytics).

С информацией об индексировании можно ознакомиться на странице сайта журнала *Индексирование Вестника*.

«Военно-технический вестник» обеспечивает читателям возможность открытого доступа, в соответствии с положениями об авторских правах, утверждёнными Creative Commons (CC BY). С инструкцией об авторских правах можно ознакомиться на странице *Авторские права и политика самоархивирования*, перейдя по ссылке http://www.vtg.mod.gov.rs/index-ru.html.

Рукописи статей направляются в редакцию журнала с использованием online системы ASSISTANT, запущенной Центром поддержи развития образования и науки (ЦПРОН).

Регистрация в системе и оформление прав доступа выполняется по адресу http://www.vtg.mod.gov.rs/index-ru.html, через страницу *ASSISTANT* или *СЦИНДЕКС* (aseestant.ceon.rs/index.php/vtg).

С инструкцией по регистрации и правам доступа можно ознакомиться по адресу http://www.vtg.mod.gov.rs/index-ru.html, на странице *Инструкция по ASSISTANT*.

Все авторы, предоставляющие свои рукописи для публикации в редакцию журнала «Военно-технический вестник» должны пройти предварительную регистрацию в реестре ORCID (Open Researcher and Contributor ID). Эта процедура осуществляется в соответствии с инструкцией, размещенной на странице сайта *Регистрация в реестре ORCID для присвоения идентификационного кода*.

«Военно-технический вестник» публикует статьи на английском языке (Arial, шрифт 11 pt, пробел Single).

Процесс подготовки, написания и редактирования статьи должен осуществляться в соответствии с принципами *Этического кодекса* (http://www.vtg.mod.gov.rs/etichyeskiy-kodyeks.html).

Статья должна содержать резюме с ключевыми словами, введение (цель исследования), основную часть (соответствующий обзор представительного исследования в данной области, четкое изложение научной новизны в представленном исследовании, соответствующую теоретическую основу, один или несколько примеров для демонстрирования и обсуждения представленных тезисов), заключение и список литературы (без нумерации заголовков и подзаголовков). Объем статьи не должен превышать один авторский лист (16 страниц формата А4 с одинарным интервалом, максимум до 24 страниц, включая ссылки и приложения).

Статья должна быть набрана на компьютере с использованием специально подготовленного редакцией макета, который можно скачать на странице сайта *Правила и образец составления статьи*.

Заголовок

Заголовок должен отражать тему статьи. В интересах журнала и автора необходимо использовать слова и словосочетания, удобные для индексации и поиска. Если такие слова не содержатся в заголовке, то желательно их добавить в подзаголовок.

Текущий заголовок

Текущий заголовок пишется в титуле каждой страницы статьи с целью упрощения процесса идентификации, в первую очередь копий статьей в электронном виде. Заголовок содержит в себе фамилию и инициал имени автора (в случае если авторов несколько, остальные обозначаются с «et al.» или «и др.»), название работы и журнала (год, том, выпуск, начальная и заключительная страница). Заголовок статьи и название журнала могут быть приведены в сокращенном виде.

ФИО автора

Приводятся полная фамилия и полное имя (всех) авторов. Желательно, чтобы были указаны инициалы отчеств авторов. Фамилия и имя авторов из Республики Сербия всегда пишутся в оригинальном виде (с сербскими диакритическими знаками), независимо от языка, на котором написана работа.

Наименование учреждения автора (аффилиация)

Приводится полное (официальное) наименование и местонахождение учреждения, в котором работает автор, а также наименование учреждения, в котором автор провёл исследование. В случае организаций со сложной структурой приводится их иерархическая соподчинённость (напр. Военная академия, кафедра военных электронных систем, г. Белград). По крайней мере, одна из организаций в иерархии должна иметь статус юридического лица. В случае если указано несколько авторов, и если некоторые из них работают в одном учреждении, нужно отдельными обозначениями или каким-либо другим способом указать в каком из приведённых учреждений работает каждый из авторов. Аффилиация пишется непосредственно после ФИО автора. Должность и специальность по диплому не указываются.

Контактные данные

Электронный адрес автора указываются рядом с его именем на первой страницы статьи.

Категория (тип) статьи

Категоризация статьей является обязанностью редакции и имеет особое значение. Категорию статьи могут предлагать рецензенты и члены редакции, т.е. редакторы рубрик, но ответственность за категоризацию несет исключительно главный редактор. Статьи в журнале распределяются по следующим категориям:

Научные статьи:

– оригинальная научная статья (работа, в которой приводятся ранее неопубликованные результаты собственных исследований, полученных научным методом);

– обзорная статья (работа, содержащая оригинальный, детальный и критический обзор исследуемой проблемы или области, в который автор внёс определённый вклад, видимый на основе автоцитат);

– краткое сообщение (оригинальная научная работа полного формата, но меньшего объёма или имеющая предварительный характер);

– научная критическая статья (дискуссия-полемика на определённую научную тему, основанная исключительно на научной аргументации) и научный комментарий.

Однако, в некоторых областях знаний научная работа в журнале может иметь форму монографического исследования, а также критического обсуждения научного материала (историко-архивного, лексикографического, библиографического, обзора данных и т.п.) – до сих пор неизвестного или недостаточно доступного для научных исследований. Работы, классифицированные в качестве научных, должны иметь, по меньшей мере, две положительные рецензии.

В случае если в журнале объявляются и приложения, не имеющие научный характер, научные статьи должны быть сгруппированы и четко выделены в первой части номера.

Профессиональные статьи:

– профессиональная работа (приложения, в которых предлагаются опыты, полезные для совершенствования профессиональной практики, но которые не должны в обязательном порядке быть обоснованы на научном методе);

– информативное приложение (передовая статья, комментарий и т.п.);

– обзор (книги, компьютерной программы, случая, научного события и т.п.).

Объем кратких сообщений составляет 4-7 страниц, исследовательские статьи и тематические исследования с проблемно-ситуационным анализом − 10-14 страниц, однако объем обзорных статей может быть больше. Ограничения по количеству страниц не являются строгими, следовательно при соответствующем обосновании предоставленные работы могут быть длиннее или короче. В случае подачи расширенных версий ранее опубликованных докладов, представленных на конференции, редакция проверит было ли добавлено достаточно новых материалов для того, чтобы статья соответствовала стандартам журнала и условиям рецензирования. Добавленный материал должен быть новым, неопубликованным ранее. Новые результаты приветствуются, но не являются обязательным условием; однако ключевые тезисы, примеры, разработки и пр. должны быть более подробно представлены в статье по сравнению с первичным докладом на конфереции.

Язык работы

Статья должна быть написана на английском языке.

Текст должен быть в лингвистическом и стилистическом смысле упорядочен, систематизирован, без сокращений (за исключением стандартных). Все физические величины должны соответствовать Международной системе единиц измерения – СИ. Очередность формул обозначается порядковыми номерами, проставляемыми с правой стороны в круглых скобках.

Резюме

Резюме является кратким информативным обзором содержания статьи, обеспечивающим читателю быстроту и точность оценки её релевантности. В интересах редакции и авторов, чтобы резюме содержало термины, часто используемые для индексирования и поиска статьей. Составными частями резюме являются введение/цель исследования, методы, результаты и выводы. В резюме должно быть от 100 до 250 слов, и оно должно находится между титулами (заголовок, ФИО авторов и др.) и ключевыми словами, за которыми следует текст статьи.

Ключевые слова

Ключевыми словами являются термины или фразы, адекватно представляющие содержание статьи, необходимые для индексирования и поиска. Ключевые слова необходимо выбирать, опираясь при этом на какой-либо международный источник (регистр, словарь, тезаурус), наиболее используемый внутри данной научной области. Число ключевых слов не может превышать 10. В интересах редакции и авторов, чтобы частота их встречи в статье была как можно большей. В статье они пишутся непосредственно после резюме.

Программа ASSISTANT предоставляет возможность использования сервиса KWASS, автоматически фиксирующего ключевые слова из источников/словарей по выбору автора/редактора.

Дата получения статьи

Дата, когда редакция получила статью; дата, когда редакция окончательно приняла статью к публикации; а также дата, когда были предоставлены необходимые исправления рукописи, приводятся в хронологическом порядке, как правило, в конце статьи.

Выражение благодарности

Наименование и номер проекта, т.е. название программы благодаря которой статья возникла, совместно с наименованием учреждения, которое финансировало проект или программу, приводятся в отдельном примечании, как правило, внизу первой страницы статьи.

Предыдущие версии работы

В случае если статья в предыдущей версии была изложена устно (под одинаковым или похожим названием, например, в виде доклада на научной конференции), сведения об этом должны быть указаны в отдельном примечании, как правило, внизу первой страницы статьи. Работа, которая уже была опубликована в каком-либо из журналов, не может быть напечатана в «Военно-техническом вестнике» ни под похожим названием, ни в изменённом виде.

Нумерация и название таблиц и графиков

Желательно, чтобы нумерация и название таблиц и графиков были исполнены на двух языках (на языке оригинала и на английском). Таблицы подписываются таким же способом как и текст и обозначаются порядковым номером с верхней стороны. Фотографии и рисунки должны быть понятны, наглядны и удобны для репродукции. Рисунки необходимо делать в программах Word или Corel. Фотографии и рисунки надо поставить на желаемое место в тексте. Для создания изображений и графиков использование функции снимка с экрана (скриншота) не допускается. В самом тексте статьи рекомендуется применение изображений и графиков, обработанных такими компьютерными программами, как: Excel, Matlab, Origin, SigmaPlot и др.

Ссылки (цитирование) в тексте

Оформление ссылок на источники в рамках статьи должно быть однообразным. «Военно-технический вестник» для оформления ссылок, цитат и списка использованной литературы применяет Гарвардскую систему (Harvard Referencing System, Harvard Style Manual). В тексте в скобках приводится фамилия цитируемого автора (или фамилия первого автора, если авторов несколько), год издания и по необходимости номер страницы. Например: (Petrović, 2010, pp.10-20). Рекомендации о способе цитирования размещены на странице сайта *Инструкция по использованию Гарвардского стиля*. При оформлении ссылок, цитат и списка использованной литературы необходимо придерживаться установленных норм. Программа ASSISTANT предоставляет при цитировании возможность использования сервиса CiteMatcher, фиксирующего пропущенные цитаты в работе и в списке литературы.

Примечания (сноски)

Примечания (сноски) к тексту указываются внизу страницы, к которой они относятся. Примечания могут содержать менее важные детали, дополнительные объяснения, указания об использованных источниках (напр. научном материале, справочниках), но не могут быть заменой процедуры цитирования литературы.

Литература (референции)

Цитированной литературой охватываются, как правило, такие библиографические источники как статьи, монографии и т.п. Вся используемая литература в виде референций размещается в отдельном разделе статьи.

Названия литературных источников не переводятся на язык работы.

«Военно-технический вестник» для оформления списка использованной литературы применяет Гарвардскую систему (Harvard Style Manual). В списке литературы источники указываются в алфавитном порядке фамилий авторов или редакторов. Рекомендации о способе цитирования размещены на странице сайта *Инструкция по использованию Гарвардского стиля*. При оформлении списка использованной литературы необходимо придерживаться установленных норм.

При оформлении списка литературы программа ASSISTANT предоставляет возможность использования сервиса RefFormatter, осуществляющего контроль оформления списка литературы в соответствии со стандартами Гарвардского стиля.

Нестандартное, неполное и непоследовательное приведение литературы в системах оценки журнала считается достаточной причиной для оспаривания научного статуса журнала.

Авторское заявление

Авторское заявление предоставляется вместе со статьей, в нем авторы заявляют о своем личном вкладе в написание статьи. В заявлении авторы подтверждают, что статья написана в соответствии с *Приглашением и инструкциями для авторов*, а также с *Кодексом профессиональной этики журнала*.

Все рукописи статей подлежат профессиональному рецензированию.

Список рецензентов журнала «Военно-технический вестник» размещён на странице сайта *Список рецензентов*. Процесс рецензирования описан в разделе *Правила рецензирования*.

Редакция

Почтовый адрес редакции:

«Војнотехнички гласник»
ул. Велька Лукича Куряка 33
11042 Белград, Республика Сербия
e-mail: vojnotehnicki.glasnik@mod.gov.rs.
тел: +381 11 3603 260, +381 66 8700 123

CALL FOR PAPERS AND ARTICLE FORMATTING INSTRUCTIONS

The instructions to authors about the article preparation for publication in the Military Technical Courier are based on the Regulations on categorization and ranking of scientific journals of the Ministry of Education, Science and Technological Development of the Republic of Serbia (Official Gazette of the Republic of Serbia, No 159/20). This Regulations aims at improving the quality of national journals and raising the level of their compliance with the international system of scientific information exchange.

The Military Technical Courier / Vojnotehnički glasnik (www.vtg.mod.gov.rs/index-e.html, втг.мо.упр.срб, ISSN 0042-8469 – print issue, e-ISSN 2217-4753 – online, UDC 623+355/359, DOI: 10.5937/VojnotehnickiGlasnik; https://doi.org/10.5937/VojnotehnickiGlasnik), is an international peer-reviewed scientific journal.

The owners of the journal are the Ministry of Defence of the Republic of Serbia and the Serbian Armed Forces. The publisher and financier of the Military Technical Courier is the University of Defence in Belgrade (Military Academy).

The program of the journal is based on the annual classification of journals performed by a relevant Ministry as well as on its indexing in international indexing databases.

The journal covers scientific and professional fields within the educational-scientific field of **Natural-Mathematical Sciences**, as well as within the educational-scientific field of **Technical-Technological Sciences**, and especially the field of **defense sciences and technologies**. It publishes theoretical and practical achievements leading to professional development of all members of Serbian, regional and international academic communities as well as members of the military and ministries of defence in particular. It publishes papers with balanced coverage of analytical, experimental, and applied research as well as numerical simulations from various disciplines. The material published is of high quality and relevance, written in a manner that makes it accessible to a wider readership. The journal welcomes papers reporting original theoretical and/or practice-oriented research as well as extended versions of already published conference papers. Manuscripts for publication are selected through a double-blind peer-review process to validate their originality, relevance, and readability. This being so, the objective is not only to keep the quality of published papers high but also to provide a timely, thorough, and balanced review process.

The editorial policy of the Military Technical Courier is based on the COPE Core Practices and the journal articles are consistent with accepted best practices in their subject areas. As of 2 May 2018, the Military Technical Courier is a member of COPE (Committee on Publication Ethics).

The Ministry of Education, Science and Technological Development of the Republic of Serbia classified the Military Technical Courier for the year 2021, on December 23, 2021

– **on the list of periodicals for computer sciences,**
category: quality national journal **(M52)**,

– **on the list of periodicals for electronics, telecommunications and IT,**
category: quality national journal **(M52)**,

– **on the list of periodicals for mechanical engineering,**
category: reputed national journal **(M51)**,

– **on the list of periodicals for materials and chemical technology,**
category: reputed national journal **(M51)**.

The approved lists of national periodicals for the year 2021 can be viewed on the website of the Military Technical Courier, page *Journal categorization*.

More detailed information can be found on the website of the Ministry of Education, Science and Technological Development of the Republic of Serbia.

The information on the categorization can be also found on the website of KOBSON (Consortium of Libraries of Serbia for Unified Acquisition).

The periodical is categorized in compliance with the Regulations on categorization and ranking of scientific journals of the Ministry of Education, Science and Technological Development of the Republic of Serbia (Official Gazette of the Republic of Serbia, No 159/20). More detailed information can be found on the website of the Ministry of Education, Science and Technological Development.

The journal is in the Serbian Citation Index – SCIndex (data base of national scientific journals), in the Russian Index of Science Citation/Российский индекс научного цитирования (RINC/РИНЦ) and is constantly monitored depending on the impact within the bases themselves and indirectly in the international (e.g. Clarivate Analytics) citation indexes. More detailed information can be viewed on the website of the Military Technical Courier, page *Journal indexing*.

Military Technical Courier enables open access and applies the Creative Commons Attribution (CC BY) licence provisions on copyright. The copyright details can be found on the *Copyright notice and Self-archiving policy* page of the journal's website.

Manuscripts are submitted online, through the electronic editing system ASSISTANT, developed by the Center for Evaluation in Education and Science – CEON.

The access and the registration are through the Military Technical Courier site http://www.vtg.mod.gov.rs/index-e.html, on the page *ASSISTANT* or the page *SCINDEKS* or directly through the link (aseestant.ceon.rs/index.php/vtg).

The detailed instructions about the registration for the service are on the website http://www.vtg.mod.gov.rs/index-e.html, on the page *Instructions for ASSISTANT*.

All authors submitting a manuscript for publishing in the Military Technical Courier should register for an ORCID ID following the instructions on the web page *Registration for an ORCID identifier*.

The Military Technical Courier publishes articles in English, using Arial and a font size of 11pt with Single Spacing.

The procedures of article preparation, writing and editing should be in accordance with the *Publication ethics statement* (http://www.vtg.mod.gov.rs/publication-ethics-statement.html).

The article should contain an abstract with keywords, introduction (motivation for the work), body (adequate overview of the representative work in the field, a clear statement of the novelty in the presented research, suitable theoretical background, one or more examples to demonstrate and discuss the presented ideas), conclusion, and references (without heading and subheading enumeration). The article length should not normally exceed 16 pages of the A4 paper format with single spacing, up to a maximum of 24 pages with references and supplementary material included.

The article should be formatted following the instructions in the Article Form which can be downloaded from website page *Article form*.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable for indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle.

Letterhead title

The letterhead title is given at a top of each page for easier identification of article copies in an electronic form in particular. It contains the author's surname and first name initial (for multiple authors add "et al"), article title, journal title and collation (year, volume, issue, first and last page). The journal and article titles can be given in a shortened form.

Author's name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form (with diacritic signs if in Serbian).

Author's affiliation

The full official name and seat of the author's affiliation is given, possibly with the name of the institution where the research was carried out. For organizations with complex structures, give the whole hierarchy (for example, University of Defence in Belgrade, Military Academy, Department for Military Electronic Systems). At least one organization in the hierarchy must be a legal entity. When some of multiple authors have the same affiliation, it must be clearly stated, by special signs or in other way, which department exactly they are affiliated with. The affiliation follows the author's name. The function and title are not given.

Contact details

The postal addresses or the e-mail addresses of the authors are given in the first page.

Type of articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification.

Journal articles are classified as follows:
Scientific articles:

– Original scientific papers (giving the previously unpublished results of the author's own research based on scientific methods);

– Review papers (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution demonstrated by self-citation);

– Short communications or Preliminary communications (original scientific full papers but shorter or of a preliminary character);

– Scientific commentaries or discussions (discussions on a particular scientific topic, based exclusively on scientific argumentation) and opinion pieces.

Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Papers classified as scientific must have at least two positive reviews.

If the journal contains non-scientific contributions as well, the section with scientific papers should be clearly denoted in the first part of the Journal.

Professional articles:

– Professional papers (contributions offering experience useful for improvement of professional practice but not necessarily based on scientific methods);

– Informative contributions (editorial, commentary, etc.);

– Reviews (of a book, software, case study, scientific event, etc.)

Short communications are usually 4-7 pages long, research articles and case studies 10-14 pages, while reviews can be longer. Page number limits are not strict and, with appropriate reasoning, submitted manuscripts can also be longer or shorter. If extended versions of previously published conference papers are submitted, Editors will check if sufficient new material has been added to meet the journal standards and to qualify such manuscripts for the review process. The added material must not have been previously published. New results are desired but not necessarily required; however, submissions should contain expansions of key ideas, examples, elaborations, etc. of conference papers.

Language

The language of the article should be in English.

The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and summary

An abstract is a concise informative presentation of the article content for fast and accurate evaluation of its relevance. It contains the terms often used for indexing and article search. A 100- to 250-word abstract has the following parts: introduction/purpose of the research, methods, results and conclusion.

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is, the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

For this purpose, the ASSISTANT system uses a special tool KWASS for the automatic extraction of key words from disciplinary thesauruses/dictionaries by choice and the routine for their selection, i.e. acceptance or rejection by author and/or editor.

Article acceptance date

The date of the reception of the article, the dates of submitted corrections in the manuscript (optional) and the date when the Editorial Board accepted the article for publication are all given in a chronological order at the end of the article.

Acknowledgements

The name and the number of the project or programme within which the article was realised is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programme.

Article preliminary version

If an article preliminary version has appeared previously at a meeting in a form of an oral presentation (under the same or similar title), this should be stated in a separate note at the bottom of the first page. An article published previously cannot be published in the *Military Technical Courier* even under a similar title or in a changed form.

Tables and illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by Arabic numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

For figures and graphs, proper data plot is recommended i.e. using a data analysis program such as Excel, Matlab, Origin, SigmaPlot, etc. It is not recommended to use a screen capture of a data acquisition program as a figure or a graph.

Citation in the text

Citation in the text must be uniform. The Military Technical Courier applies the Harvard Referencing System given in the Harvard Style Manual. When citing sources within your paper, i.e. for in-text references of the works listed at the end of the paper, place the year of publication of the work in parentheses and optionally the number of the page(s) after the author’s name, e.g. (Petrovic, 2012, pp.10-12). A detailed guide on citing, with examples, can be found on Military Technical Courier website on the page *Instructions for Harvard Style Manual*. In-text citations should follow its guidelines.

For checking in-text citations, the ASSISTANT system uses a special tool CiteMatcher to find out quotes left out within papers and in reference lists.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

Reference list (Literature)

The cited literature encompasses bibliographic sources such as articles and monographs and is given in a separate section in a form of a reference list.

References are not translated to the language of the article.

In compiling the reference list and bibliography, the Military Technical Courier applies the Harvard System – Harvard Style Manual. All bibliography items should be listed alphabetically by author’s name, without numeration. A detailed guide for listing references, with examples, can be found on Military Technical Courier website on the page *Instructions for Harvard Style Manual*. Reference lists at the end of papers should follow its guidelines.

In journal evaluation systems, non-standard, insufficient or inconsequent citation is considered to be a sufficient cause for denying the scientific status to a journal.

Authorship Statement

The Authorship statement, submitted together with the paper, states authors’ individual contributions to the creation of the paper. In this statement, the authors also confirm that they followed the guidelines given in *the Call for papers* and the *Publication ethics and malpractice statement of the journal*.

All articles are peer reviewed.

The list of referees of the Military Technical Courier can be viewed at website page *List of referees*. The article review process is described on the *Peer Review Process* page of the website.

Editorial Team

Address of the Editorial Office:
Vojnotehnički glasnik / Military Technical Courier
Veljka Lukića Kurjaka 33
11042 Belgrade, Republic of Serbia
e-mail: vojnotehnicki.glasnik@mod.gov.rs.
tel.: +381 11 3603 260, +381 66 8700 123

Ликовно-графички уредник
Марија Марић, e-mail: marija.maric@mod.gov.rs

Лектор
Добрила Милетић, e-mail: miletic.dobrila@gmail.com

Превод на енглески
Јасна Вишњић, e-mail: jasnavisnjic@yahoo.com

Превод на руски
Др *Карина* Авагјан, e-mail: karinka2576@mail.ru

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

623+355/359

ВОЈНОТЕХНИЧКИ гласник : научни часопис Министарства одбране
и Војске Србије = Военно-технический вестник : научный журнал
Министерства обороны и Вооружённых сил Республики Сербия =
Military Technical Courier : scientific Journal of the Ministry of Defence and the Serbian
Armed Forces / главни и одговорни уредник Драган Памучар. -
Год. 1, бр. 1 (1. јан. 1953)- . - Београд : Универзитет одбране у Београду,
Војна академија, 1953- (Београд : Војна штампарија). - 23 cm

Тромесечно. - Текст на срп., рус. и енгл. језику. - Друго издање
на другом медијуму: Vojnotehnički glasnik (Online) = ISSN 2217-4753
ISSN 0042-8469 = Војнотехнички гласник
COBISS.SR-ID 4423938

Цена: 600,00 динара

Тираж: 100 примерака

На основу мишљења Министарства за науку, технологију и развој Републике Србије, број 413-00-1201/2001-01 од 12. 9. 2001. године,
часопис „Војнотехнички гласник“ је публикација од посебног интереса за науку.

УДК: Народна библиотека Србије, Београд

Адреса редакције: Војнотехнички гласник,
Вељка Лукића Курјака 33, 11042 Београд

http://www.vtg.mod.gov.rs
http://aseestant.ceon.rs/index.php/vtg/issue/current
http://scindeks.nb.rs/journaldetails.aspx?issn=0042-8469
http://elibrary.ru/title_about.asp?id=53280
https://doaj.org/toc/2217-4753

Војнотехнички гласник је лиценциран код EBSCO Publishing-a.
Комплетан текст *Војнотехничког гласника* доступан је у базама података EBSCO Publishing-a.

e-mail: vojnotehnicki.glasnik@mod.gov.rs

Претплата на штампано издање: e-mail: vojnotehnicki.glasnik@mod.gov.rs; тел. 066/87-00-123.

Часопис излази тромесечно.

Први штампани број *Војнотехничког гласника* објављен је 1. 1. 1953. године.

Прво електронско издање *Војнотехничког гласника* на Интернету објављено је 1. 1. 2011. године.

Штампа: Војна штампарија – Београд, Ресавска 40б, e-mail: vojna.stamparija@mod.gov.rs

Художественный редактор
Мария Марич, e-mail: marija.maric@mod.gov.rs

Корректор
Добрила Милетич, e-mail: miletic.dobrila@gmail.com

Перевод на английский язык
Ясна Вишнич, e-mail: jasnavisnjic@yahoo.com

Перевод на русский язык
Д.филол.н. *Карина* Кареновна Авагян, e-mail: karinka2576@mail.ru

CIP – Каталогизация в публикации
Национальная библиотека Сербии, г. Белград

623+355/359

ВОЈНОТЕХНИЧКИ гласник : научни часопис Министарства одбране
и Војске Србије = Военно-технический вестник : научный журнал
Министерства обороны и Вооружённых сил Республики Сербия =
Military Technical Courier : scientific Journal of the Ministry of Defence and the Serbian
Armed Forces / главни и одговорни уредник Драган Памучар. -
Год. 1, бр. 1 (1. јан. 1953)- . - Београд : Универзитет одбране у Београду,
Војна академија, 1953- (Београд : Војна штампарија). - 23 cm

Тромесечно. - Текст на срп., рус. и енгл. језику. - Друго издање
на другом медијуму: Vojnotehnički glasnik (Online) = ISSN 2217-4753
ISSN 0042-8469 = Војнотехнички гласник
COBISS.SR-ID 4423938

Цена: 600,00 динаров

Тираж: 100 экземпляров

На основании решения Министерства науки и технологий Республики Сербия,
№ 413-00-1201/2001-01 от 12. 9. 2001 года, журнал «Военно-технический вестник»
объявлен изданием, имеющим особое значение для науки.

УДК: Национальная библиотека Сербии, г. Белград

Адрес редакции: Војнотехнички гласник,
Ул. Велька Лукича Куряка 33, 11042 Белград, Республика Сербия

http://www.vtg.mod.gov.rs
http://aseestant.ceon.rs/index.php/vtg/issue/current
http://scindeks.nb.rs/journaldetails.aspx?issn=0042-8469
http://elibrary.ru/title_about.asp?id=53280
https://doaj.org/toc/2217-4753

«Военно-технический вестник» включен в систему EBSCO. Полный текст журнала
«Военно-технический вестник» можно найти в базах данных EBSCO Publishing.

e-mail: vojnotehnicki.glasnik@mod.gov.rs

Подписка на печатную версию журнала: e-mail: vojnotehnicki.glasnik@mod.gov.rs;
тел. +381 66 87 00 123.

Журнал выпускается ежеквартально.

Первый номер журнала «Военно-технический вестник» выпущен 1.1.1953 года.

Первая электронная версия журнала размещена на интернет странице 1.1.2011 года.

Типография: Војна штампарија – Белград, Ресавска 40б, e-mail: vojna.stamparija@mod.gov.rs

Graphic design editor
Marija Marić, e-mail: marija.maric@mod.gov.rs

Proofreader
Dobrila Miletić, e-mail: miletic.dobrila@gmail.com

English translation and polishing
Jasna Višnjić, e-mail: jasnavisnjic@yahoo.com

Russian translation and polishing
Dr. *Karina* Avagyan, e-mail: karinka2576@mail.ru

CIP – Catalogisation in the publication
National Library of Serbia, Belgrade

623+355/359

ВОЈНОТЕХНИЧКИ гласник : научни часопис Министарства одбране
и Војске Србије = Военно-технический вестник : научный журнал
Министерства обороны и Вооружённых сил Республики Сербия =
Military Technical Courier : scientific Journal of the Ministry of Defence and the Serbian
Armed Forces / главни и одговорни уредник Драган Памучар. -
Год. 1, бр. 1 (1. јан. 1953)- . - Београд : Универзитет одбране у Београду,
Војна академија, 1953- (Београд : Војна штампарија). - 23 cm

Тромесечно. - Текст на срп., рус. и енгл. језику. - Друго издање
на другом медијуму: Vojnotehnički glasnik (Online) = ISSN 2217-4753
ISSN 0042-8469 = Војнотехнички гласник
COBISS.SR-ID 4423938

Price: 600.00 RSD

Printed in 100 copies

According to the Opinion of the Ministry of Science and Technological Development No 413-00-1201/2001-01 of 12th September 2001, the *Military Technical Courier* is a publication of special interest for science.

UDC: National Library of Serbia, Belgrade

Address: Vojnotehnički glasnik/Military Technical Courier,
Veljka Lukića Kurjaka 33, 11042 Belgrade, Republic of Serbia

http://www.vtg.mod.gov.rs/index-e.html

http://aseestant.ceon.rs/index.php/vtg/issue/current

http://scindeks.nb.rs/journaldetails.aspx?issn=0042-8469

http://elibrary.ru/title_about.asp?id=53280

https://doaj.org/toc/2217-4753

Military Technical Courier has entered into an electronic licensing relationship with EBSCO Publishing. The full text of *Military Technical Courier* can be found on EBSCO Publishing's databases.

e-mail: vojnotehnicki.glasnik@mod.gov.rs

Subscription to print edition: e-mail: vojnotehnicki.glasnik@mod.gov.rs; Tel. +381 66 87 00 123.

The journal is published quarterly.

The first printed issue of the *Military Technical Courier* appeared on 1st January 1953.
The first electronic edition of the *Military Technical Courier* on the Internet appeared on 1st January 2011.

Printed by Vojna štamparija – Belgrade, Resavska 40b, e-mail: vojna.stamparija@mod.gov.rs

7
ОД 1953.
ВТГ
ГОДИНА

7
OD 1953.
VTG
GODINA

7
С 1953 г.
ВТВ
ЛЕТ

7
SINCE 1953
MTC
YEARS