ISSN 1684-8853 (print); ISSN 2541-8610 (online)

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНЫЙ ЖУРНАЛ

2(111)/2021

doi:10.31799/1684-8853-2021-2

ISSN 1684-8853 (print); ISSN 2541-8610 (online)

SCIENTIFIC JOURNAL

2(111)/2021

PEER REVIEWED JOURNAL

INFORMATSIONNO-UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

Contact information
The Editorial and Publishing Center, SUAI
67, B. Morskaia, 190000, St. Petersburg, Russia
Website: http://i-us.ru/en, e-mail: ius.spb@gmail.com
Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press, Broadcasting and Mass Media of the Russian Federation.
Registration Certificate JD № 77-12412 from April, 19, 2002.
Re-registration in the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) due to change of the founder: «Information and Control Systems», Ltd., JD № FS77-49181 from March, 30, 2012.

Submitted for publication 02.03.21. Passed for printing 23.04.21. Format 60×84$_{1/8}$.
Phototype SchoolBookC. Digital printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia

The journal is indexed in Scopus.
Free distribution.

doi:10.31799/1684-8853-2021-2 ISSN 1684-8853 (print); ISSN 2541-8610 (online)
НАУЧНЫЙ ЖУРНАЛ

2(111)/2021

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Учредитель
ООО «Информационно-управляющие системы»
Издатель
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-02, эл. адрес: ius.spb@gmail.com,
сайт: http://i-us.ru

Журнал входит в БД SCOPUS и в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук.

Сдано в набор 02.03.21. Подписано в печать 23.04.21. Формат 60×84 1/8.
Гарнитура SchoolBookC. Печать цифровая.
Усл. печ. л. 9,0. Уч.-изд. л. 12,4. Тираж 1000 экз (1-й завод 50 экз.). Заказ № 142.
Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.
Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

Распространяется бесплатно.

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.
Перерегистрирован в Роскомнадзоре.
Свидетельство о регистрации ПИ № ФС77-49181 от 30 марта 2012 г.

UDC 338.984
doi:10.31799/1684-8853-2021-2-2-12

Articles

Decomposition of abstract linear operators on Banach spaces

K. D. Tsilika[a], *PhD, Assistant Professor, orcid.org/0000-0002-9213-3120, ktsilika@uth.gr*
[a]*University of Thessaly, Hellenic Open University, 78, 28hs Octovriou St., 38333 Volos, Greece*

Introduction: *The majority of the known decomposition methods for solving boundary value problems (Adomian decomposition method, natural transform decomposition method, modified Adomian decomposition method, combined Laplace transform — Adomian decomposition method, and Domain decomposition method) use so-called Adomian polynomials or iterations to get approximate solutions. To our knowledge, a direct method for obtaining an exact analytical solution is not yet proposed.* ***Purpose:*** *Developing, in an arbitrary Banach space, a new universal decomposition method for the class of ordinary or partial integro-differential equations with non-local and initial boundary conditions in terms of the abstract operator equation* $B_1x = f$. ***Results:*** *A class of integro-differential equations in a Banach space with non-local and initial boundary conditions in terms of an abstract operator equation* $B_1x = \mathcal{A}x - \mathbf{S}_0\mathbf{F}(Ax) - \mathbf{G}_0\mathbf{\Phi}(Ax) = f$, $x = D(B_1)$*has been studied, where* $\mathcal{A}$, A *are linear abstract operators,* $\mathbf{S}_0$, $\mathbf{G}_0$ *are vectors and* $\mathbf{\Phi}$, $\mathbf{F}$ *the functional vectors. Usually,* $\mathcal{A}$, A *are linear ordinary or partial differential operators, and* $\mathbf{F}(Ax)$, $\mathbf{\Phi}(Ax)$ *are Fredholm integrals. The existence and uniqueness are proved under the assumption that the operator* B_1 *has a decomposition of the form* $B_1 = B_0B$ *with* B *and* B_0 *being different abstract linear operators of special forms. The proposed decomposition method is universal and essentially different from other decomposition methods in the relevant literature. This method can be applied to either ordinary integro-differential or partial integro-differential equations, providing a unique exact solution in closed analytical form in a Banach space. The stages of the method are illustrated by numerical examples corresponding to specific problems. Computer algebra system Mathematica is used to demonstrate the solution outcomes and to assess the effectiveness of the analysis.* ***Practical relevance:*** *The main advantage of the proposed solution method is that it can be integrated in the interface of any CAS software in an easy, programing-free way.*

Keywords *— correct operator, decomposition (factorization) of operators (equations), integro-differential equations, boundary value problems, exact solution.*

For citation: Tsilika K. D. Decomposition of abstract linear operators on Banach spaces. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 2–12. doi:10.31799/1684-8853-2021-2-2-12

Preliminaries and auxiliary results

Integro-differential equations are used in many problems from science and engineering. The integro-differential operators describing these problems are complicated and the exact solution of the corresponding boundary value problems is a difficult task. In some cases, the boundary value problem (BVP) can be transformed into a simpler one involving simpler operators and thus the solution can be found easier.

The decomposition (factorization) methods were used in many applications in gas dynamics, transport theory, electromagnetism, quantum physics, mechanics, hydrodynamics and cosmology [1–14]. In pure mathematics, decomposition (factorization) method continues to be a very successful tool for solving variational inequalities, linear and nonlinear ordinary and partial differential and Volterra — Fredholm integro-differential equations as well as systems of partial differential equations. This method is very important for solving fuzzy Volterra — Fredholm integral equations, integro-differential equations of fractional order and delay differential equations [15–32]. However, almost all the approaches of the literature listed above do not give exact solutions in their closed analytical forms and the corresponding problems are not formulated in terms of abstract operator equations. Thus, the decomposition methods proposed and employed in these problems are not universal.

Exact solutions in their analytical form for abstract operator equations in Hilbert and Banach spaces were obtained by quadratic and biquadratic decompositions of the integro-differential equations in [33–37]. The universal decomposition method for the abstract linear operator equation

$$B_1x = A^2x - \mathbf{S}\mathbf{F}(Ax) - \mathbf{G}\mathbf{F}(A^2x) = f,\ x \in D(B_1)$$

was given in [38] on a Hilbert space. We note that Banach spaces play a central role in functional analysis and it is important to study the exact solutions of correct BVPs in the context of Banach spaces. This work is a natural continuation of [38] to a Banach space and introduces the universal decomposition method for the similar linear abstract operator equation

$$B_1x = \mathcal{A}x - \mathbf{S}_0\mathbf{F}(Ax) - \mathbf{G}_0\mathbf{\Phi}(Ax) = f,\ x \in D(B_1), \quad (1)$$

where $\mathcal{A}$, A are linear abstract operators; $\mathbf{S}_0$, $\mathbf{G}_0$ are vectors and $\mathbf{\Phi}$, $\mathbf{F}$ — functional vectors. The decomposition method proposed here is different than the well-known decomposition methods (namely the Adomian decomposition method, the natural trans-

form decomposition method, modified Adomian decomposition method, the combined Laplace transform — Adomian decomposition method and domain decomposition method). In the relevant literature, the so-called Adomian polynomials or iterations were used to obtain numerical solutions (see [1–32]). The class of integro-differential equations with nonlocal boundary conditions described by an abstract operator equation is studied in [39], where all calculations are reproducible in any program of symbolic calculations and the computer codes in Mathematica are given.

In the sections that follow we use the following notations, definitions and statements.

We denote by X a complex Banach space and by X^* the adjoint space of X, i. e. the set of all complex-valued linear and bounded functionals f on X. We denote by $f(x)$ the value of f on x.

We write $D(A)$ and $R(A)$ for the domain and the range of the operator A, respectively. An operator $A: X \to X$ is called *correct* if $R(A) = X$ and the inverse A^{-1} exists and is continuous on X. If for an operator B_1 there are two operators B_0, B such that B_1 can be written as a product $B_1 = B_0B$, then we say that B_0B is a decomposition (factorization) of B_1 and write $B_1 = B_0B$. An operator B_1: $X \to X$ is called *quadratic* (*biquadratic*) if there exists an operator $B: X \to X$ such that $B_1 = B^2$, ($B_1 = B^4$) and the corresponding decomposition $B_1 = B^2$, ($B_1 = B^4$) is called *quadratic* (*biquadratic*). Recall that the problem $Ax = f$ is called *correct*, if the operator A is correct. If x, $g_i \in X$ and $\Phi_i \in X^*$, $i = 1, ..., m$ then we denote by $\mathbf{g} = (g_1, ..., g_m)$, $\mathbf{\Phi} = \mathrm{col}(\Phi_1, ..., \Phi_m)$ and $\mathbf{\Phi}(x) = \mathrm{col}(\Phi_1(x), ..., \Phi_m(x))$ and we write $\mathbf{g} \in X^m$, $\mathbf{\Phi} \in X^m$. We will denote by $\mathbf{\Phi}(\mathbf{g})$ the $m \times m$ matrix whose i, j-th entry $\Phi_i(g_j)$ is the value of functional Φ_i on element g_j. Note that $\mathbf{\Phi}(\mathbf{gC}) = \mathbf{\Phi}(\mathbf{g})\mathbf{C}$, where $\mathbf{C}$ is a $m \times k$ constant matrix. We will also denote by $\mathbf{0}_m$ and $\mathbf{I}_m$ the zero and identity $m \times m$ matrices.

Next, we state some useful outcomes. Specifically, Theorem 1 from [40] and Corollary 3.11 from [33].

Theorem 1. Let X, Y and Z be Banach spaces and $A_0: X \to Y$ be a correct operator with $D(A_0) \subset Z \subseteq X$. Further let the vector $\mathbf{G}_0 = \left(g_1^{(0)}, \ldots, g_m^{(0)}\right) \in Y^m$ and the column vector $\mathbf{\Phi} = \mathrm{col}(\phi_1, ..., \phi_m)$, where ϕ_1, ..., $\phi_m \in Z^*$ and their restrictions on $D(A_0)$ are linearly independent. Then:

(i) The operator $B_0: X \to X$ defined by

$$B_0x = A_0x - \mathbf{G}_0\mathbf{\Phi}(x) = f,\ D(B_0) = D(A_0),\ f \in X, \quad (2)$$

is correct if and only if

$$\det\mathbf{L}_0 = \det\left[\mathbf{I}_m - \mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right)\right] \neq 0. \quad (3)$$

(ii) If B_0 is correct, then for any $f \in Y$, the unique solution of (2) is given by

$$x = B_0^{-1}f = A_0^{-1}f + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}f\right). \quad (4)$$

Corollary 1. Let A be a correct operator on a Banach space X and the components of the vectors $\mathbf{G} = (g_1, ..., g_m)$, $\mathbf{F} = \mathrm{col}(F_1, ..., F_m)$ are arbitrary elements of X and X^*, respectively. Then the operator $B: X \to X$ defined by

$$Bx = Ax - \mathbf{GF}(Ax) = f,\ D(B) = D(A),\ f \in X \quad (5)$$

is correct if and only if

$$\det\mathbf{L} = \det[\mathbf{I}_m - \mathbf{F}(\mathbf{G})] \neq 0. \quad (6)$$

If B is correct, then the unique solution of (5) for every $f \in X$ is given by

$$X = B^{-1}f = A^{-1}f + A^{-1}\mathbf{GL}^{-1}\mathbf{F}(f). \quad (7)$$

Decomposition of abstract linear operators on a Banach space

In this section we investigate problem (1) where B_1 is not quadratic but it can be written as a product of two other correct operators B_0, B i. e. $B_1 = B_0B$. In this case the solvability condition and the solution formulation are essentially simpler than in the general case.

We will prove the following theorem using the technique that was first applied for the case of Hilbert space in Theorem 2.5 [38], where a given operator B_0 of the type $B_0x = A_0x - \mathbf{G}_0\mathbf{\Phi}(A_0x) = f$, $x \in D(B_0)$ and an operator A is densely defined. We use a different operator B_0 without the assumption of density of $D(A)$ on X.

Theorem 2. Let X and Z be Banach spaces, $Z \subseteq X$, the vectors $\mathbf{G} = (g_1, ..., g_m)$, $\mathbf{G}_0 = \left(g_1^{(0)}, \ldots, g_m^{(0)}\right)$, $\mathbf{S}_0 = \left(s_1^{(0)}, \ldots, s_m^{(0)}\right) \in X^m$, the components of the vectors $\mathbf{F} = \mathrm{col}(F_1, ..., F_m)$ and $\mathbf{\Phi} = \mathrm{col}(\Phi_1, ..., \Phi_m)$ belong to X^* and Z^*, respectively, and the operators $B_0, B, B_1: X \to X$ defined by

$$B_0x = A_0x - \mathbf{G}_0\mathbf{\Phi}(x) = f,\ D(B_0) = D(A_0) \subset Z; \quad (8)$$

$$Bx = Ax - \mathbf{GF}(Ax) = f,\ D(B) = D(A); \quad (9)$$

$$B_1x = A_0Ax - \mathbf{S}_0\mathbf{F}(Ax) - \mathbf{G}_0\mathbf{\Phi}(Ax) = f,$$
$$D(B_1) = D(A_0A), \quad (10)$$

where A_0 and A are linear correct operators on X; $\mathbf{G} \in D(A_0)^m$ and the restrictions of Φ_1, ..., Φ_m on $D(A_0)$ are linearly independent. Then the following statements are satisfied:

(i) If

$$\mathbf{S}_0 \in R(B_0)^m \text{ and } \mathbf{S}_0 = B_0\mathbf{G} = \\ = A_0\mathbf{G} - \mathbf{G}_0\mathbf{\Phi}(\mathbf{G}), \qquad (11)$$

then the operator B_1 can be decomposed in $B_1 = B_0B$.

(ii) If in addition the components of the vector $\mathbf{F} = \text{col}(F_1, ..., F_m)$ are linearly independent elements of X^* and since the operator B_1 can be decomposed in $B_1 = B_0B$, then (11) is fulfilled.

(iii) If the operator B_1 can be decomposed in $B_1 = B_0B$ then B_1 is correct if and only if the operators B_0, and B are correct which means that

$$\det\mathbf{L}_0 = \det\left[\mathbf{I}_m - \mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right)\right] \neq 0 \text{ and} \\ \det\mathbf{L} = \det[\mathbf{I}_m - \mathbf{F}(\mathbf{G})] \neq 0. \qquad (12)$$

(iv) If the operator B_1 has the decomposition in $B_1 = B_0B$ and is correct, then the unique solution of (10) is

$$x = B_1^{-1}f = A^{-1}A_0^{-1}f + A^{-1}\mathbf{G}\mathbf{L}^{-1}\mathbf{F}\left(A_0^{-1}f\right) + \\ + \left[A^{-1}A_0^{-1}\mathbf{G}_0 + A^{-1}\mathbf{G}\mathbf{L}^{-1}\mathbf{F}\left(A_0^{-1}\mathbf{G}_0\right)\right]\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}f\right). \qquad (13)$$

Proof: (i) Taking into account that $G \in D(A_0)^m$ and (8)–(10) we get

$$D(B_0B) = \{x \in D(B): Bx \in D(B_0)\} = \\ = \{x \in D(A): Ax - \mathbf{G}\mathbf{F}(Ax) \in D(A_0)\} = \\ = \{x \in D(A): Ax \in D(A_0)\} = D(A_0A) = D(B_1).$$

So $D(B_1) = D(B_0B)$. Let $y = \text{B}x$. Then for each $x \in D(A_0A)$ and taking into account (8) and (9) we have

$$B_0Bx = B_0y = A_0y - \mathbf{G}_0\mathbf{\Phi}(y) = \\ = A_0[Ax - \mathbf{G}\mathbf{F}(Ax)] - \mathbf{G}_0\mathbf{\Phi}(Ax - \mathbf{G}\mathbf{F}(Ax)) = \\ = A_0Ax - A_0\mathbf{G}\mathbf{F}(Ax) - \mathbf{G}_0\mathbf{\Phi}(Ax) + \mathbf{G}_0\mathbf{\Phi}(\mathbf{G})\mathbf{F}(Ax) = \\ = A_0Ax - \mathbf{G}_0\mathbf{\Phi}(Ax) - [A_0\mathbf{G} - \mathbf{G}_0\mathbf{\Phi}(\mathbf{G})]\mathbf{F}(Ax) = \\ = A_0Ax - B_0\mathbf{G}\mathbf{F}(Ax) - \mathbf{G}_0\mathbf{\Phi}(Ax), \qquad (14)$$

where the relation $B_0\mathbf{G} = A_0\mathbf{G} - \mathbf{G}_0\mathbf{\Phi}(\mathbf{G})$ results naturally from (8) by substituting $x = \mathbf{G}$.

By comparing (14) with (10), it is easy to verify that $B_1x = B_0Bx$ for each $x \in D(A_0A)$ if a vector $\mathbf{S}_0$ satisfies (11).

(ii) Let the operator B_1 can be decomposed in $B_1 = B_0B$. Then by comparing (14) with (10) we obtain

$$(B_0\mathbf{G} - \mathbf{S}_0)\mathbf{F}(Ax) = 0. \qquad (15)$$

Because of the correctness of operators A, A_0 and the linear independence of F_1, ..., F_m, there exists a system x_1, ..., $x_m \in D(A_0A)$ such that $\mathbf{F}(A_0x_0) = \mathbf{I}_m$ where $\mathbf{x}_0 = (x_1, ..., x_m)$. By substituting $x = \mathbf{x}_0$ into (15) we get $\mathbf{S}_0 = B_0\mathbf{G}$. Hence $\mathbf{S}_0 \in R(B_0)^m$ and $\mathbf{S}_0 = B_0\mathbf{G} = A_0\mathbf{G} - \mathbf{G}_0\mathbf{\Phi}(\mathbf{G})$.

(iii) Let the operator B_1 be defined by (10) where $\mathbf{S}_0 = B_0\mathbf{G}$. Then equation (10) can be equivalently represented as a matrix equation:

$$B_1x = A_0Ax - \left(B_0\mathbf{G}, \mathbf{G}_0\right)\begin{pmatrix}\mathbf{F}\left(A_0^{-1}A_0Ax\right)\\ \mathbf{\Phi}\left(A_0^{-1}A_0Ax\right)\end{pmatrix} = f, \qquad (16)$$

or

$$B_1 = \mathcal{A}x - \tilde{\mathbf{G}}\tilde{\mathbf{F}}(\mathcal{A}x) = f,\ D(B_1) = D(\mathcal{A}), \qquad (17)$$

where

$$\mathcal{A} = AA_0;\ \tilde{\mathbf{G}} = (B_0\mathbf{G}, \mathbf{G}_0);$$

$$\tilde{\mathbf{F}} = \text{col}\left(\hat{\mathbf{F}}, \hat{\mathbf{\Phi}}\right),\ \tilde{\mathbf{F}}(\mathcal{A}x) = \begin{pmatrix}\hat{\mathbf{F}}(\mathcal{A}x)\\ \hat{\mathbf{\Phi}}(\mathcal{A}x)\end{pmatrix},$$

then

$$\tilde{\mathbf{F}}(v) = \begin{pmatrix}\hat{\mathbf{F}}(v)\\ \hat{\mathbf{\Phi}}(v)\end{pmatrix} = \begin{pmatrix}\mathbf{F}\left(A_0^{-1}v\right)\\ \hat{\mathbf{\Phi}}\left(A_0^{-1}v\right)\end{pmatrix}.$$

Notice that the operator $\mathcal{A} = AA_0$ is correct, because of A and A_0 are correct operators, and the functional vector $\tilde{\mathbf{F}}$ is bounded, since the vectors $\hat{\mathbf{F}}, \hat{\mathbf{\Phi}}$ are bounded as a superposition of a bounded functional $\mathbf{F}, \mathbf{\Phi}$ respectively and a bounded operator A_0^{-1}. Then we apply Corollary 1. By this corollary the operator B_1 is correct if and only if

$$\det\mathbf{L}_1 = \det\left[\mathbf{I}_{2m} - \mathbf{F}\left(\tilde{\mathbf{G}}\right)\right] = \\ = \det\left[\begin{pmatrix}\mathbf{I}_m & 0_m\\ 0_m & \mathbf{I}_m\end{pmatrix} - \begin{pmatrix}\hat{\mathbf{F}}(B_0\mathbf{G}) & \hat{\mathbf{F}}(\mathbf{G}_0)\\ \hat{\mathbf{\Phi}}(B_0\mathbf{G}) & \hat{\mathbf{\Phi}}(\mathbf{G}_0)\end{pmatrix}\right] = \\ = \det\begin{pmatrix}\mathbf{I}_m - \mathbf{F}\left(\mathbf{G} - A_0^{-1}\mathbf{G}_0\mathbf{\Phi}(\mathbf{G})\right) & -\mathbf{F}\left(A_0^{-1}\mathbf{G}_0\right)\\ -\mathbf{\Phi}\left(\mathbf{G} - A_0^{-1}\mathbf{G}_0\mathbf{\Phi}(\mathbf{G})\right) & \mathbf{I}_m - \mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right)\end{pmatrix} = \\ = \det\begin{pmatrix}\mathbf{I}_m - \mathbf{F}(\mathbf{G}) + \mathbf{F}\left(A_0^{-1}\mathbf{G}_0\right)\mathbf{\Phi}(\mathbf{G}) & -\mathbf{F}\left(A_0^{-1}\mathbf{G}_0\right)\\ -\mathbf{\Phi}(\mathbf{G}) + \mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right)\mathbf{\Phi}(\mathbf{G}) & \mathbf{I}_m - \mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right)\end{pmatrix} \neq 0.$$

According to properties of determinants of matrices (Remark 1, [34]), taking $\mathbf{L}_1$ in the last formulation from above and adding $\mathbf{\Phi}(\mathbf{G})$ times the second

column of $\mathbf{L}_1$ to its first column, the determinant is unchanged. We then get

$$\det\mathbf{L}_1 = \det\begin{pmatrix} \mathbf{I}_m - \mathbf{F}(\mathbf{G}) & -\mathbf{F}\left(A_0^{-1}\mathbf{G}_0\right) \\ \mathbf{0}_m & \mathbf{I}_m - \mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right) \end{pmatrix} =$$

$$= \det\left[\mathbf{I}_m - \mathbf{F}(\mathbf{G})\right]\det\left[\mathbf{I}_m - \mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right)\right] =$$

$$= \det\mathbf{L}_0 \det\mathbf{L} \neq \mathbf{0}.$$

So we proved that the operator B_1 is correct if and only if (12) is fulfilled.

(iv) Let $x \in D(A_0A)$ and $B_0Bx = f$. Then by Theorem 1 (ii) since B_0, B are correct operators, we obtain

$$Bx = B_0^{-1}f = A_0^{-1}f + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}f\right),$$

$$x = B^{-1}\left(A_0^{-1}f + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}f\right)\right).$$

In the last equation we denote by $g = A_0^{-1}f + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}f\right)$. Following strictly Corollary 1 (ii), we get

$$x = B^{-1}g = A^{-1}g + A^{-1}\mathbf{G}\mathbf{L}^{-1}\mathbf{F}(g) =$$

$$= A^{-1}\left(A_0^{-1}f + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}f\right)\right) +$$

$$+ A^{-1}\mathbf{G}\mathbf{L}^{-1}\mathbf{F}\left(A_0^{-1}f + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}f\right)\right) =$$

$$= A^{-1}A_0^{-1}f + A^{-1}A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}f\right) +$$

$$+ A^{-1}\mathbf{G}\mathbf{L}^{-1}\left[\mathbf{F}\left(A_0^{-1}f\right) + \mathbf{F}\left(A_0^{-1}\mathbf{G}_0\right)\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}f\right)\right],$$

which implies (13). Thus, the theorem has been proved.

The next theorem is useful for applications.

Theorem 3. Let X and Z be Banach spaces, $Z \subseteq X$ the vectors $\mathbf{G}_0 = \left(g_1^{(0)}, \ldots, g_1^{(0)}\right)$, $\mathbf{S}_0 = \left(s_1^{(0)}, \ldots, s_1^{(0)}\right) \in X^m$, the components of the vectors $\mathbf{F} = \mathrm{col}(F_1, \ldots, F_m)$ and $\mathbf{\Phi} = \mathrm{col}(\Phi_1, \ldots, \Phi_m)$ belong to X^* and Z^*, respectively, the operators $\mathcal{A}, A, B_1: X \to X$ and the operator B_1 defined by

$$B_1x = \mathcal{A}x - \mathbf{S}_0\mathbf{F}(Ax) - \mathbf{G}_0\mathbf{\Phi}(Ax) = f,\ x \in D(B_1), \quad (18)$$

where A is a correct m-order differential operator and $\mathcal{A}$ is a n-order differential operator, $m < n$. Then the next statements are fulfilled:

(i) If there exist a bijective $n - m$ order differential operator $A_0: X \to X$ and the vector $\mathbf{G}$ such that

$$\mathcal{A} = A_0A,\ D(B_1) = D(A_0A),\ D(A_0) \subset Z; \quad (19)$$

$$\det\mathbf{L}_0 = \det\left[\mathbf{I}_m - \mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right)\right] \neq 0; \quad (20)$$

$$\mathbf{G} = A_0^{-1}\mathbf{S}_0 + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right), \quad (21)$$

and the restrictions of $\Phi_1, \ldots, \Phi_m$ are linearly independent on $D(A_0)$, then the operator B_1 is decomposed in $B_1 = B_0B$, where B_0, B are given by (8), (9), respectively, the operator B_0 is constructed by the triple of elements A_0, $\mathbf{\Phi}$, $\mathbf{G}_0$ from (18)–(20), and the operator B by the operator A and vector $\mathbf{F}$ from (18) and the vector $\mathbf{G}$ from (21).

(ii) If in addition to (i) A_0 is correct, then B_1 is correct if and only if

$$\det\mathbf{L} = \det[\mathbf{I}_m - \mathbf{F}(\mathbf{G})] =$$

$$= \det\left[\mathbf{I}_m - \mathbf{F}\left(A_0^{-1}\mathbf{S}_0\right) - \mathbf{F}\left(A_0^{-1}\mathbf{G}_0\right)\times\right.$$

$$\left.\times\,\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right)\right] \neq \mathbf{0}, \quad (22)$$

and the problem (18), (19) has the unique solution given by (13).

Proof: (i) If a bijective $n - m$ order differential operator A_0 and a vector $\mathbf{G}$ exist satisfying (19)–(21), then from (18) we get

$$B_1x = A_0Ax - \mathbf{S}_0\mathbf{F}(Ax) - \mathbf{G}_0\mathbf{\Phi}(Ax) = f,$$

$$x \in D(A_0A). \quad (23)$$

From (23) we take the operator A and vector $\mathbf{F}$, whereas from (21) we take a vector $\mathbf{G}$ and construct the operator B according to the formula (9). To determine the operator B_0 by the formula (8), we take from (23) the operator A_0 and the vectors $\mathbf{\Phi}$, $\mathbf{G}_0$. We proved in the previous theorem (i) that $D(B_0B) = D(A_0A) = D(B_1)$. Substituting (21) into (8) we obtain

$$B_0\mathbf{G} = B_0\left[A_0^{-1}\mathbf{S}_0 + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right)\right] =$$

$$= A_0\left[A_0^{-1}\mathbf{S}_0 + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right)\right] -$$

$$- \mathbf{G}_0\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0 + A_0^{-1}\mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right)\right) =$$

$$= \mathbf{S}_0 + \mathbf{G}_0\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right) - \mathbf{G}_0\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right) -$$

$$- \mathbf{G}_0\mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right)\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right) =$$

$$= \mathbf{S}_0 + \mathbf{G}_0\left[\mathbf{I}_m - \mathbf{\Phi}\left(A_0^{-1}\mathbf{G}_0\right)\right]\times$$

$$\times\,\mathbf{L}_0^{-1}\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right) - \mathbf{G}_0\mathbf{\Phi}\left(A_0^{-1}\mathbf{S}_0\right) = \mathbf{S}_0.$$

$\mathbf{S}_0 = B_0\mathbf{G}$ and from (23) for $\mathbf{S}_0 = B_0\mathbf{G}$ and every $x \in D(B_1)$ we get

$$B_1x = A_0Ax - B_0\mathbf{G}\mathbf{F}(Ax) - \mathbf{G}_0\mathbf{\Phi}(Ax) =$$

$$= B_0Ax - B_0\mathbf{G}\mathbf{F}(Ax) = B_0[Ax - \mathbf{G}\mathbf{F}(Ax)] = B_0Bx.$$

Thus we obtained the decomposition $B_1 = B_0B$.

(iii) If the statement (i) holds, then B_1 can be decomposed in $B_1 = B_0B$. By Theorem 3 (iii), B_1 is correct if and only if (12) holds or, taking into account (20) and (21), if and only if $\det\mathbf{L} = \det[\mathbf{I}_m - \mathbf{F(G)}] \neq 0$, or if and only if (22) is fulfilled. The last inequality immediately follows by substitution (21) into $\det\mathbf{L} = \det[\mathbf{I}_m - \mathbf{F(G)}]$. Since B_1 is correct and decomposed in $B_1 = B_0B$, by Theorem 2 (iv), we obtain the unique solution (13). So, the theorem is proved.

Remark. Usually as a Banach space X we have $C[a, b]$ or $L_p(a, b)$ and as a Banach space Z we have $C^k[a, b]$ or $W_p^k = (a, b)$, $k = 1, ..., n$.

Numerical examples

Let us examine several examples where our findings are applied and validated (the Mathematica notebook solving each example is available upon request).

Example 1. The operator B_1: $C[0, 1] \to C[0, 1]$ corresponding to the problem

$$x''(t) - t^2\int_0^1 t^3x'(t)\,dt - t\int_0^1 tx'(t)\,dt = 2t + 1,$$

$$x(0) + x(1) = 0,\ x'(0) - 2x'(1) = 0 \qquad (24)$$

is correct. The unique solution of problem (24) is given by the formula

$$x(t) = -\frac{31990t^4 - 158464t^3 - 451860t^2 + 2502304t - 961985}{903720}. \qquad (25)$$

Proof: If we compare equation (24) with equations (18), (19), it is natural to denote $\mathbf{\Phi} = \Phi_1 = \Phi$, $\mathbf{F} = F_1 = F$, $\mathbf{G}_0 = g_1^{(0)} = G_0$, $\mathbf{S}_0 = s_1^{(0)} = S_0$, $\mathbf{I}_m = 1$, and to take $X = C[0, 1]$,

$$B_1x(t) = x''(t) - t^2\int_0^1 t^3x'(t)\,dt - t\int_0^1 tx'(t)\,dt = 2t + 1; \qquad (26)$$

$$D(B_1) = \{x(t) \in C^2[0, 1] : x(0) + x(1) = 0,\ x'(0) - 2x'(1) = 0\}; \qquad (27)$$

$$\mathcal{A}x = A_0Ax = x''(t); \qquad (28)$$

$$Ax(t) = x'(t),\ D(A) = \{x(t) \in C^1[0, 1] : x(0) = -x(1)\}; \qquad (29)$$

$$\Phi(Ax) = \int_0^1 tx'(t)\,dt,\ \ F(Ax) = \int_0^1 t^3x'(t)\,dt, \qquad (30)$$

$G_0 = t$, $S_0 = t^2$. Let us denote $Ax(t) = x'(t) = y(t) = y$. Then from (28) and (27) we have $y \in D(A_0)$, $A_0Ax = (x'(t))' = y'(t) = A_0y(t)$, $y(0) - 2y(1) = 0$. So we proved that

$$A_0y = y'(t),\ D(A_0) = \{y(t) \in C^1[0, 1]: y(0) - 2y(1) = 0\}.$$

Now we check the condition $D(B_1) = D(A_0A)$. By definition

$$D(A_0A) = \{x(t) \in D(A): Ax(t) \in D(A_0)\} = \{x(t) \in C^1[0, 1]: x(0) = -x'(1),\ x'(t) \in C^1[0, 1],\ x'(0) - 2x'(1) = 0\} = \{x(t) \in C^2[0, 1]: x(0) + x(1) = 0,\ x'(0) - 2x'(1) = 0\} = D(B_1).$$

So $D(B_1) = D(A_0A)$. It is easy to verify that the operators A_0, A are correct on $C[0, 1]$ and for every $f(t) \in C[0, 1]$ the following equations hold true

$$A_0^{-1}f(t) = \int_0^t f(s)\,ds - 2\int_0^1 f(s)\,ds; \qquad (31)$$

$$A_0^{-1}f(t) = \int_0^t f(s)\,ds - \frac{1}{2}\int_0^1 f(s)\,ds. \qquad (32)$$

From (30) we have

$$\Phi(f) = \int_0^1 sf(s)\,ds,\ \ F(f) = \int_0^1 s^3f(s)\,ds. \qquad (33)$$

It is evident that Φ, $F \in C^*[0, 1]$. Consequently, we can take $Z = C[0, 1] = X$.

Using (33) and (21) we find

$$F(S_0) = \int_0^1 s^3s^2\,ds = \frac{1}{6},\ \ F(G_0) = \int_0^1 s^3s\,ds = \frac{1}{5},$$

$$A_0^{-1}G_0 = \int_0^t s\,ds - 2\int_0^1 s\,ds = \frac{t^2}{3} - 1,$$

$$\Phi\left(A_0^{-1}G_0\right) = \int_0^1 s\left(\frac{s^2}{2} - 1\right)ds = -\frac{3}{8},$$

$$A_0^{-1}S_0 = \int_0^t s^2\,ds - 2\int_0^1 s^2\,ds = \frac{t^3}{3} - \frac{2}{3},$$

$$\Phi\left(A_0^{-1}S_0\right) = \int_0^1 s\left(\frac{s^3}{2} - \frac{2}{3}\right)ds = -\frac{4}{15},$$

$$L_0 = I_m - \Phi\left(A_0^{-1}G_0\right) = \frac{11}{8},\ \ L_0^{-1} = \frac{8}{11},$$

$$G = A_0^{-1}S_0 + A_0^{-1}G_0L_0^{-1}\Phi\left(A_0^{-1}S_0\right) = \frac{t^3}{3} - \frac{2}{3} + \left(\frac{t^2}{2} - 1\right)\frac{8}{11}\left(-\frac{4}{15}\right) = \frac{1}{165}\left(55t^3 - 16t^2 - 78\right).$$

Taking into account (33) we obtain

$$F(G)=\frac{1}{165}\int_0^1 s^3\left(55s^3-16s^2-78\right)\mathrm{d}s=-\frac{601}{6930}.$$

Since $\det L=\det[1-F(G)]=\frac{7531}{6930}\neq 0$ then $L^{-1}=\frac{6930}{7531}$, and by Theorem 3 (ii), problem (26), (27) or (24) is correct. By (32) we calculate

$$A^{-1}G=\frac{330t^4-128t^3-1872t+835}{3960},$$

$$A^{-1}A_0^{-1}G_0=\frac{t^3}{6}-t+\frac{5}{12}$$

and for $f(t)=2t+1$ by (31)–(33) we obtain

$$A_0^{-1}f=-4+t+t^2,\ A^{-1}A_0^{-1}f=\frac{19}{12}-4t+\frac{t^2}{2}+\frac{t^3}{3},$$

$$F\left(A_0^{-1}f\right)=-\frac{19}{30},\ \Phi\left(A_0^{-1}f\right)=-\frac{17}{12}.$$

Substituting these values into (13) we obtain the unique solution of (26), (27) or (24), which is given by (25).

Example 2. The operator B_1: $C[0,\pi]\to C[0,\pi]$ corresponding to the problem

$$x'''(t)-\sin t\int_0^\pi t^2x''(t)\mathrm{d}t-$$
$$-\cos t\int_0^{\pi/2}(t+1)x''(t)\mathrm{d}t=\sin 2t, \qquad (34)$$
$$x(0)+x(\pi)=0,\ x'(0)+3x'(\pi)=0,\ x''(0)+x''(\pi)=0,$$

is correct. The unique solution of the problem (34) is given by the formula

$$x(t)=\frac{1}{48}\left[3\left(-2+\pi^2-6\pi t+4t^2+2\cos 2t\right)-\right.$$
$$-\frac{\pi\left(2\pi^2-3\right)\left(8\cos t+\pi(\pi-2t-4\sin t)\right)}{\pi^3-2}+$$
$$\left.+\frac{3(2+\pi)^2\left(\begin{array}{c}4\left(\pi^2-4\right)\cos t-(2\pi-1)\times\\ \times(\pi-2t-4\sin t)\end{array}\right)}{2\left(\pi^3-2\right)}\right]. \qquad (35)$$

Proof: If we compare (34) with equations (18), (19), it is natural to denote $\mathbf{\Phi}=\Phi_1=\Phi$, $\mathbf{F}=F_1=F$, $\mathbf{G}_0=g_1^{(0)}=G_0$, $\mathbf{S}_0=s_1^{(0)}=S_0$, $\mathbf{I}_m=1$, and to take $X=C[0,\pi]$,

$$B_1x(t)=x'''(t)-\sin t\int_0^\pi t^2x''(t)\mathrm{d}t-$$
$$-\cos t\int_0^{\pi/2}(t+1)x''(t)\mathrm{d}t=\sin 2t; \qquad (36)$$

$$D(B_1)=\{x(t)\in C^3[0,\pi]:\ x(0)+x(\pi)=0,$$
$$x'(0)+3x'(\pi)=0,\ x''(0)+x''(\pi)=0\}; \qquad (37)$$

$$\mathcal{A}x=A_0Ax=x'''(t); \qquad (38)$$

$$Ax(t)=x''(t);$$

$$D(A)=\{x(t)\in C^2[0,\pi]:\ x(0)=-x(\pi),$$
$$x'(0)+3x'(\pi)=0\}; \qquad (39)$$

$$\Phi(Ax)=\int_0^{\pi/2}(t+1)x''(t)\mathrm{d}t,$$

$$F(Ax)=\int_0^\pi t^2x''(t)\mathrm{d}t, \qquad (40)$$

$S_0=\sin t$, $G_0=\cos t$, $f=\sin 2t$. Denote $Ax(t)=x''(t)=y(t)=y$. Then from (37) and (38) we have $y\in D(A_0)$, $A_0Ax=(x''(t))'=y'(t)=A_0y(t)$, $y(0)+y(\pi)=0$. So we proved that

$$A_0y=y'(t),\ D(A_0)=$$
$$=\{y(t)\in C^1[0,\pi]:\ y(0)+y(\pi)=0\}. \qquad (41)$$

Now we check the condition $D(B_1)=D(A_0A)$. By definition

$$D(A_0A)=\{x(t)\in D(A):\ Ax(t)\in D(A_0)\}=$$
$$=\{x(t)\in C^2[0,\pi]:\ x(0)+x(\pi)=0,\ x'(0)+3x'(\pi)=0,$$
$$x''(t)\in C^1[0,\pi],\ x''(0)+x''(\pi)=0\}=$$
$$=\{x(t)\in C^3[0,\pi]:\ x(0)+x(\pi)=0,$$
$$x'(0)+3x'(\pi)=0,\ x''(0)+x''(\pi)=0\}=D(B_1).$$

So $D(B_1)=D(AA_0)$. It is easy to verify that the operators A, A_0 are correct on $C[0,\pi]$ and for every $f(t)\in C[0,\pi]$ from (39) and (41) follows that

$$A_0^{-1}f(t)=\int_0^t(t-s)f(s)\mathrm{d}s+$$
$$+\frac{1}{4}\int_0^\pi(2s-3t-\pi/2)f(s)\mathrm{d}s; \qquad (42)$$

$$A_0^{-1}f(t)=\int_0^t f(s)\mathrm{d}s-\frac{1}{2}\int_0^\pi f(s)\mathrm{d}s. \qquad (43)$$

From (40) we have

$$\Phi(f)=\int_0^{\pi/2}(s+1)f(s)\mathrm{d}s,\ F(f)=\int_0^\pi s^2f(s)\mathrm{d}s. \qquad (44)$$

It is evident that F, $\Phi\in C^*[0,\pi]$. Consequently we can take $Z=C[0,\pi]=X$. From (43), (44), (20), (21) we get

$$A_0^{-1}G_0=\int_0^t\cos s\mathrm{d}s-\frac{1}{2}\int_0^\pi\cos s\mathrm{d}s=\sin t,$$

$$\Phi\left(A_0^{-1}G_0\right)=\int_0^{\pi/2}(s+1)\sin s\,\mathrm{d}s=2,$$

$$A_0^{-1}S_0=-\cos t,$$

$$\Phi\left(A_0^{-1}S_0\right)=\int_0^{\pi/2}(s+1)(-\cos s)\,\mathrm{d}s=-\frac{\pi}{2},$$

$$\det L_0=\det\left[1-\Phi\left(A_0^{-1}G_0\right)\right]=1-2=-1\neq 0,\ L_0^{-1}=-1,$$

$$G=A_0^{-1}S_0+A_0^{-1}G_0L_0^{-1}\Phi\left(A_0^{-1}S_0\right)=\frac{\pi}{2}\sin t-\cos t,$$

$$F(G)=\int_0^{\pi}s^2\left(\frac{\pi}{2}\sin s-\cos s\right)\mathrm{d}s=\frac{\pi^3}{2},$$

then

$$\det L=\det\left[1-F(G)\right]=\frac{2-\pi^3}{2},\ L^{-1}=\frac{2}{2-\pi^3}.$$

Since $\det L\neq 0$, by Theorem 3 (ii), problem (36)–(39) or (34) is correct. Further by using (42) and taking into account that $A_0^{-1}G_0=\sin t$, we find

$$A^{-1}G=\cos t-\frac{\pi\sin t}{2}-\frac{\pi(2t-\pi)}{8},$$

$$A^{-1}A_0^{-1}G_0=\int_0^t(t-s)\sin s\,\mathrm{d}s+$$

$$+\frac{1}{4}\int_0^{\pi}\left(2s-3t-\frac{\pi}{2}\right)\sin s\,\mathrm{d}s=-\sin t-\frac{2t-\pi}{4}.$$

For $f(t)=\sin 2t$ by (42), (43) we calculate

$$A_0^{-1}f=\frac{1-\cos 2t}{2},\ \Phi\left(A_0^{-1}f\right)=(\pi+2)^2/16,$$

$$F\left(A_0^{-1}f\right)=\frac{\pi^3}{6}-\frac{\pi}{4},$$

$$A^{-1}A_0^{-1}f=\frac{1}{16}\left(4t^2-6\pi t+\pi^2-2+2\cos 2t\right).$$

Substituting these values into (13) we obtain the unique solution of (34), which is given by (35).

Example 3. Let $\Omega=\{(t,\ s)\in R\colon 0\le t,\ s\le 1$. The operator $B_1\colon C(\Omega)\to C(\Omega)$ corresponding to the problem

$$x''_{ts}(t,s)-t^3s\int_0^1\int_0^1 s^2x'_t(t,s)\,\mathrm{d}t\,\mathrm{d}s-$$

$$-ts^2\int_0^1\int_0^1 tx'_t(t,s)\,\mathrm{d}t\,\mathrm{d}s=5t^2+s,$$

$$x'_t,\ x''_{ts}\in C(\Omega),\ \ x(0,s)=s^2\int_0^1\int_0^1 x(t,s)\,\mathrm{d}t\,\mathrm{d}s,$$

$$x'_t(t,0)=t\int_0^1\int_0^1 sx'_t(t,s)\,\mathrm{d}t\,\mathrm{d}s, \qquad (45)$$

is correct. The unique solution of problem (45) is given by the formula

$$x(t,s)=\frac{85148684t^2+31416680s^3t^2+}{172657440}+$$

$$+\frac{287762400st^3}{172657440}+$$

$$+\frac{s^2\left(123613741+86328720t+15746840t^4\right)}{172657440}. \qquad (46)$$

Proof: If we compare (45) with (18), (19), it is natural to denote

$\mathbf{\Phi}=\Phi_1=\Phi$, $\mathbf{F}=F_1=F$, $\mathbf{G}_0=g_1^{(0)}=G_0$, $\mathbf{S}_0=s_1^{(0)}=S_0$, $\mathbf{I}_m=1$, and to take $X=C(\Omega)$,

$$B_1x(t)=x''_{ts}(t,s)-t^3s\int_0^1\int_0^1 s^2x'_t(t,s)\,\mathrm{d}t\,\mathrm{d}s-$$

$$-ts^2\int_0^1\int_0^1 tx'_t(t,s)\,\mathrm{d}t\,\mathrm{d}s=5t^2+s; \qquad (47)$$

$$D(B_1)=\{x(t,\ s)\in C(\Omega),\ x'_t,$$

$$x''_{ts}\in C(\Omega),\ x(0,\ s)=s^2\int_0^1\int_0^1 x(t,s)\,\mathrm{d}t\,\mathrm{d}s;$$

$$x'_t(t,0)=t\int_0^1\int_0^1 sx'_t(t,s)\,\mathrm{d}t\,\mathrm{d}s\}; \qquad (48)$$

$$A_0Ax=x''_{ts}(t,s); \qquad (49)$$

$$Ax(t,s)=x'_t(t,s); \qquad (50)$$

$$D(A)=\{x(t,s)\in C(\Omega)\colon x'_t(t,s)\in C(\Omega),$$

$$x(0,s)=s^2\int_0^1\int_0^1 x(t,s)\,\mathrm{d}t\,\mathrm{d}s,$$

$$F(Ax)=\int_0^1\int_0^1 s^2x'_t(t,s)\,\mathrm{d}t\,\mathrm{d}s,$$

$$\Phi(Ax)=\int_0^1\int_0^1 tx'_t(t,s)\,\mathrm{d}t\,\mathrm{d}s, \qquad (51)$$

$S_0=t^3s$, $G_0=ts^2$, $f=5t^2+s$. We denote $Ax(t,s)=x'_t(t,s)=y(t,s)=y$. Then from (48), (49) we have

$$y\in D(A_0),$$

$$A_0Ax=\left(x'_t(t,s)\right)'_s=y'_s(t,s)=A_0y(t,s),$$

$$y(t,0)=t\int_0^1\int_0^1 sy(t,s)\,\mathrm{d}t\,\mathrm{d}s.$$

So we proved that

$$A_0y=y'_s(t,s),$$

$$D(A_0)=\{y(t,s)\in C(\Omega)\colon y'_s\in C(\Omega),\ y(t,0)=$$

$$=t\int_0^1\int_0^1 sy(t,s)\,\mathrm{d}t\,\mathrm{d}s\}.$$

Now we check the condition $D(B_1)=D(AA_0)$. By definition

$$D(A_0A)=\{x(t,s)\in D(A): Ax(t,s)\in D(A_0)\}=$$
$$=\{x(t,s)\in C(\Omega): x'_t\in C(\Omega),\ x(0,s)=$$
$$=s^2\int_0^1\int_0^1 x(t,s)\,dt\,ds,\ x''_{ts}(t,s)\in C(\Omega),$$
$$x'_t(t,0)=t\int_0^1\int_0^1 sx'_t(t,s)\,dt\,ds\}=$$
$$=\{x(t,s)\in C(\Omega): x'_t,\ x''_{ts}\in C(\Omega),$$
$$x(0,s)=s^2\int_0^1\int_0^1 x(t,s)\,dt\,ds\},$$

$$x'_t(t,0)=t\int_0^1\int_0^1 sx'_t(t,s)\,dt\,ds\}=D(B_1).$$

So $D(B_1)=D(A_0A)$. It is easy to verify that the operators A, A_0 are correct on $C(\Omega)$ and for every $f(t, s)\in C(\Omega)$ the following hold true

$$A_0^{-1}f(t,s)=\int_0^s f(t,s_1)\,ds_1+$$
$$+\frac{4t}{3}\int_0^1\int_0^1 s\int_0^s f(t,s_1)\,ds_1\,dt\,ds; \qquad (52)$$

$$A_0^{-1}f(t,s)=\int_0^t f(t_1,s)\,dt_1+$$
$$+\frac{3s^2}{2}\int_0^1\int_0^1\int_0^t f(t_1,s)\,dt_1\,dt\,ds. \qquad (53)$$

From (51) for every $f(t, s)\in C(\Omega)$ we get

$$F(f)=\int_0^1\int_0^1 s^2 f(t,s)\,dt\,ds,$$
$$\Phi(f)=\int_0^1\int_0^1 tf(t,s)\,dt\,ds. \qquad (54)$$

It is evident that $F, \Phi\in C^*(\Omega)$. Consequently we can take $Z=C(\Omega)=X$.

Further by using (52), (54), (20), (21) for $S_0=t^3s$, $G_0=ts^2$ we get

$$A_0^{-1}S_0=\int_0^s t^3s_1\,ds_1+$$
$$+\frac{4t}{3}\int_0^1\int_0^1 s\int_0^s t^3s_1\,ds_1\,dt\,ds=\frac{t}{24}+\frac{s^2t^3}{2},$$
$$A_0^{-1}G_0=\int_0^s ts_1^2\,ds_1+$$
$$+\frac{4t}{3}\int_0^1\int_0^1 s\int_0^s ts_1^2\,ds_1\,dt\,ds=\frac{2t}{45}+\frac{s^3t}{3},$$
$$F\left(A_0^{-1}G_0\right)=\int_0^1\int_0^1 s^2\left(\frac{2t}{45}+\frac{s^3t}{3}\right)dt\,ds=\frac{19}{540},$$
$$\Phi\left(A_0^{-1}G_0\right)=\int_0^1\int_0^1 t\left(\frac{2t}{45}+\frac{s^3t}{3}\right)dt\,ds=\frac{23}{540},$$
$$\det L_0=\det\left[1-\Phi\left(A_0^{-1}G_0\right)\right]=\frac{517}{540},\ L_0^{-1}=\frac{540}{517},$$

$$G=A_0^{-1}S_0+A_0^{-1}G_0L_0^{-1}\Phi\left(A_0^{-1}S_0\right)=$$
$$=\frac{t\left(907+340s^3+10340s^2t^2\right)}{20680},$$
$$F(G)=\frac{1393}{41360},\ \det L=\det\left[1-F(G)\right]=\frac{39967}{41360},$$
$$L^{-1}=\frac{41360}{39967}.$$

Since $\det L\neq 0$ then, by Theorem 3 (ii), problem (47), (48) or (45) is correct.

By (53) we calculate

$$A^{-1}G=\frac{907t^2+340s^3t^2+s^2\left(1013+5170t^4\right)}{41360},$$
$$A^{-1}A_0^{-1}G=\frac{120s^3t^2+23s^2+16t^2}{720}$$

and for $f(t, s)=5t^2+s$ by (52)–(54) we obtain

$$A_0^{-1}f=\frac{s^2}{2}+\frac{49t}{54}+5st^2,$$
$$A^{-1}A_0^{-1}f=s^2\left(\frac{t}{2}+\frac{287}{432}\right)+\frac{5st^3}{3}+\frac{49t^2}{108},$$
$$F\left(A_0^{-1}f\right)=\frac{541}{810},\ \Phi\left(A_0^{-1}f\right)=\frac{655}{648}.$$

Substituting these terms into (13) we obtain the unique solution of (45), which is given by (46).

Conclusion

The main research result of this paper is the existence and uniqueness of the operator equation $B_1u=f$ in the space setting of Banach spaces, given that $B_1=B_0B$. The necessary and sufficient conditions for the correctness of the operator B_1 are intermediate, secondary results. The solution procedure follows the universal decomposition method and provides a unique exact solution in closed form. This method can be also applied in more complex problems, as of the type $B_1u=f$, where $B_1=B_0B^2$ or $B_1=B_0^2B$ and for B_0, B given by (8), (9), respectively.

The entire approach is given in an algorithmic procedure that is reproducible in any program of symbolic calculations.

References

1. Adomian G. A review of the decomposition method in applied mathematics. *Journal of Mathematical Analysis and Applications*, 1988, vol. 135(2), pp. 501–

544. doi:https://doi.org/10.1016/0022-247X(88)90170-9
2. Geiser J. *Decomposition methods for differential equations: theory and applications*. CRC Press, Taylor and Francis Group, Boca Raton, 2009. 304 p.
3. Dong S.-H. *Factorization method in quantum mechanics*. Part of the Fundamental Theories of Physics book series (FTPH, vol. 150). Springer, Dordrecht, 2007. 297 p.
4. Van der Mee C. V. M. *Semigroup and factorization methods in transport theory*. Mathematisch Centrum, Amsterdam, 1981. 167 p.
5. Nyashin Y., Lokhov V., Ziegler F. Decomposition method in linear elastic problems with eigenstrain. *Journal of Applied Mathematics and Mechanics (ZAMM)*, 2005, vol. 85, pp. 557–570. doi: https://doi.org/10.1002/zamm.200510202
6. Kelesoglu O. The solution of fourth order boundary value problem arising out of the beam-column theory using Adomian Decomposition Method. *Mathematical Problems in Engineering*, vol. 2014, Article ID 649471, 6 p. doi:https://doi.org/10.1155/2014/649471
7. Fahmy E. S. Travelling wave solutions for some time-delayed equations through factorizations. *Chaos Solitons & Fractals*, 2008, vol. 38(4), pp. 1209–1216. doi:10.1016/j.chaos.2007.02.007
8. Ferapontov E. V., Veselov A. P. Integrable Schrödinger operators with magnetic fields: factorization method on curved surfaces. *Journal of Mathematical Physics*, 2001, vol. 42 (2), pp. 590–607. doi:10.1063/1.1334903
9. Amirkhanov I. V., Konnova S. V., Zhidkov E. P. The factorization method and particular solutions of the relativistic Schrodinger equation of *n*th order (*n*= 4,6). *Computer Physics Communications*, 2000, vol. 126(1-2), pp. 12–15. doi:10.1016/S0010-4655(99)00421-X
10. Caruntu D. I. Factorization of self-adjoint ordinary differential equations. *Applied Mathematics and Computation*, 2013, vol. 219, pp. 7622–7631. doi: 10.1016/j.amc.2013.01.049
11. Soh C. W. Isospectral Euler — Bernoulli beams via factorization and the Lie method. *International Journal of Non-Linear Mechanics*, 2009, vol. 44(4), pp. 396–403. doi:10.1016/j.ijnonlinmec.2009.01.004
12. Caruntu D. I. Relied studies on factorization of the differential operator in the case of bending vibration of a class of beams with variable cross-section. *Revue Roumaine des Sciences Techniques — Série de Mécanique Appliqu e*, 1996, no. 41(5-6), pp. 389–397.
13. Lokshin A. A. Interaction of non-linear waves and the factorization method. *Journal of Applied Mathematics and Mechanics*, 1995, vol. 59(2), pp. 325–331. doi: 10.1016/0021-8928(95)00038-Q
14. Barkovsky L. M., Furs A. N. Factorization of integro-differential equations of the acoustics of dispersive viscoelastic anisotropic media and the tensor integral operators of wake packet velocities. *Acoustical Physics*, 2002, vol. 48(2), pp. 128–132. doi:10.1134/1.1460945
15. Araghi M., Behzadi S. Solving nonlinear Volterra — Fredholm integro-differential equations using the modified Adomian decomposition method. *Computational Methods in Applied Mathematics*, 2009, vol. 9(4), pp. 321–331. doi:https://doi.org/10.2478/cmam-2009-0020
16. Adomian G. A review of the decomposition method and some recent results for nonlinear equations. *Mathematical and Computer Modelling*, 1990, vol. 13(7), pp. 17–43. doi:https://doi.org/10.1016/0895-7177(90)90125-7
17. Babolian E., Biazar J., Vahidi A. R. The decomposition method applied to systems of Fredholm integral equations of the second kind. *Applied Mathematics and Computation*, 2004, vol. 148(2), pp. 443–452. doi:10.1016/S0096-3003(02)00859-7
18. Badriev I. B., Zadvornov O. A. A decomposition method for variational inequalities of the second kind with strongly inverse-monotone operators. *Differential Equations*, 2003, vol. 39, pp. 936–944. doi:https://doi.org/10.1023/B:DIEQ.0000009189.91279.93
19. Baskonus H. M., Bulut H., Pandir Y. The natural transform decomposition method for linear and nonlinear partial differential equations. *Mathematics in Engineering, Science and Aerospace*, 2014, vol. 5(1), pp. 111–126.
20. Berkovich L. M. Factorization and transformations of linear and nonlinear ordinary differential equations. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 2003, vol. 502(2-3), pp. 646–648. doi:10.1016/S0168-9002(03)00531-X
21. Davari A., Khanian M. Solution of system of Fredholm integro-differential equations by Adomian decomposition method. *Australian Journal of Basic and Applied Sciences*, 2011, vol. 5(12), pp. 2356–2361.
22. Evans D. J., Raslan K. R. The Adomain decomposition method for solving delay differential equation. *International Journal of Computer Mathematics*, 2005, vol. 82(1), pp. 49–54. doi:10.1080/00207160412331286815
23. El-Sayed S., Kaya D., Zarea S. The decomposition method applied to solve high-order linear Volterra — Fredholm integro-differential equations. *International Journal of Nonlinear Sciences and Numerical Simulation*, 2004, vol. 5(2), pp. 105–112. doi:https://doi.org/10.1515/IJNSNS.2004.5.2.105
24. Hamoud A. A., Ghadle K. P. The reliable modified of Laplace Adomian decomposition method to solve nonlinear interval Volterra — Fredholm integral equations. *The Korean Journal of Mathematics*, 2017, vol. 25(3), pp. 323–334. doi:https://doi.org/10.11568/kjm.2017.25.3.323
25. Hamoud A. A., Ghadle K. P. Modified Adomian decomposition method for solving fuzzy Volterra — Fredholm integral equations. *The Journal of the Indi-*

an Mathematical Society, 2018, vol. 85(1-2), pp. 52–69. doi:https://doi.org/10.18311/jims/2018/16260
26. Hamoud A., Ghadle K. The combined modified Laplace with Adomian decomposition method for solving the nonlinear Volterra — Fredholm integrodifferential equations. *Journal of the Korean Society for Industrial and Applied Mathematics*, 2017, vol. 21(1), pp. 17–28. doi:10.12941/jksiam.2017.21.017
27. Kamachkin A. M., Shamberov V. N. The decomposition method of research into the nonlinear dynamical systems' space of parameters. *Applied Mathematical Sciences*, 2015, vol. 9(81), pp. 4009–4018. doi:10.12988/ams.2015.54355
28. Mittal R., Nigam R. Solution of fractional integro-differential equations by Adomian decomposition method. *International Journal of Applied Mathematics and Mechanics*, 2008, vol. 4(2), pp. 87–94.
29. Rawashdeh M. S., Maitama S. Solving coupled system of nonlinear PDEs using the natural decomposition method. *International Journal of Pure and Applied Mathematics*, 2014, vol. 92(5), pp. 757–776. doi:10.12732/ijpam.v92i5.10
30. Tsarev S. P. Factoring linear partial differential operators and the Darboux method for integrating nonlinear partial differential equations. *Theoretical and Mathematical Physics*, 2000, vol. 122(1), pp. 144–160. doi:https://doi.org/10.4213/tmf561
31. Wazwaz A. M. The combined Laplace transform-Adomian decomposition method for handling nonlinear Volterra integro-differential equations. *Applied Mathematics and Computation*, 2010, vol. 216(4), pp. 1304–1309. doi:https://doi.org/10.1016/j.amc.2010.02.023
32. Yang C., Hou J. Numerical solution of integro-differential equations of fractional order by Laplace decomposition method. *WSEAS Transactions on Mathematics*, 2013, vol. 12(12), pp. 1173–1183.
33. Parasidis I. N., Tsekrekos P. C. Some quadratic correct extensions of minimal operators in Banach space. *Operators and Matrices*, 2010, vol. 4(2), pp. 225–243. doi:dx.doi.org/10.7153/oam-04-11
34. Parasidis I. N. Extension and decomposition method for differential and integro-differential equations. *Eurasian Mathematical Journal*, 2019, vol. 10(3), pp. 48-67. doi:https://doi.org/10.32523/2077-9879-2019-10-3-48-67
35. Parasidis I. N., Providas E., Zaoutsos S. *On the solution of boundary value problems for ordinary differential equations of order n and 2n with general boundary conditions*. In: Daras N., Rassias T. (eds). *Computational mathematics and variational analysis. Springer optimization and its applications*, Springer, Cham, 2020. Vol. 159. Pp. 299–314. doi:https://doi.org/10.1007/978-3-030-44625-3_17
36. Providas E., Parasidis I. N. On the solution of some higher-order integro-differential equations of special form. *Vestnik of Samara University*, *Natural Science Series*, 2020, vol. 26(1), pp. 14–22. doi:10.18287/2541-7525-2020-26-1-14-22
37. Vassiliev N. N., Parasidis I. N., Providas E. Exact solution method for Fredholm integro-differential equations with multipoint and integral boundary conditions. Part 2. Decomposition-extension method for squared operators. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 2, pp. 2–9. doi:https://doi.org/10.31799/1684-8853-2019-2-2-9
38. Parasidis I. N., Providas E., Tsekrekos P. C. Factorization of linear operators and some eigenvalue problems of special operators. *Vestnik of Bashkir University*, 2012, vol. 17(2), pp. 830–839 (In Russian).
39. Tsilika K. D. A *n* exact solution method for Fredholm integro-differential equations. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 4, pp. 2–8. doi:10.31799/1684-8853-2019-4-2-8
40. Parasidis I. N., Providas E. *Extension operator method for the exact solution of integro-differential equations*. In: Pardalos P., Rassias T. (eds). *Contributions in Mathematics and Engineering*. Springer, 2016. Pp. 473–496. doi:10.1007/978-3-319-31317-7_23

УДК 338.984
doi:10.31799/1684-8853-2021-2-2-12

Разложение абстрактных линейных операторов на банаховых пространствах

К. Д. Тсилика[a], PhD, доцент, orcid.org/0000-0002-9213-3120, ktsilika@uth.gr
[a]Университет Фессалии, 38221, Волос, Греция

Введение: большинство известных методов декомпозиции для решения краевых задач (метод декомпозиции Адомяна, естественное преобразование метода декомпозиции, модифицированный метод декомпозиции Адомяна, комбинированный метод преобразования Лапласа — декомпозиции Адомяна и метод декомпозиции области) используют так называемые полиномы Адомяна или итерации для получения приближенных решений. Насколько нам известно, прямой метод получения точного аналитического решения пока не предложен. **Цель:** разработать в произвольном банаховом пространстве новый универсальный метод разложения для класса обыкновенных интегро-дифференциальных уравнений или интегро-дифференциальных уравнений в частных производных с нелокальными и начальными граничными условиями в терминах абстрактного операторного уравнения $B_1x = f$. **Результаты:** исследован класс интегро-дифференциальных уравнений в банаховом пространстве с нелокальными и начальными граничными условиями в терминах абстрактного операторного уравнения $B_1x = \mathcal{A}x - \mathbf{S}_0\mathbf{F}(\mathcal{A}x) - \mathbf{G}_0\mathbf{\Phi}(\mathcal{A}x) = f$, $x \in D(B_1)$,

где $\mathcal{A}, A$ — линейные абстрактные операторы; $\mathbf{S}_0$, $\mathbf{G}_0$ — векторы, а $\mathbf{\Phi}$, $\mathbf{F}$ — функциональные векторы. Обычно $\mathcal{A}, A$ — это линейные обыкновенные дифференциальные операторы или дифференциальные операторы в частных производных, а $\mathbf{F}(Ax)$, $\mathbf{\Phi}(Ax)$ — интегралы Фредгольма. Основным результатом нашего исследования является теорема существования и единственности уравнения $B_1x = f$ при условии, что оператор B_1 имеет разложение вида $B_1 = B_0B$, где B и B_0 — различные абстрактные линейные операторы специального вида. Предлагаемый метод разложения универсален и существенно отличается от других методов разложения в соответствующей литературе. Этот метод может быть применен как к обыкновенным интегро-дифференциальным уравнениям, так и к интегро-дифференциальным уравнениям в частных производных, и дает единственное точное решение в замкнутой аналитической форме в банаховом пространстве. Этапы метода решения иллюстрируются численными примерами, соответствующими конкретным задачам. Система компьютерной алгебры Mathematica используется для демонстрации результатов решения и оценки эффективности анализа. **Практическая значимость:** основным преимуществом настоящего метода решения является легкость его интеграции в интерфейс любого программного обеспечения CAS.

Ключевые слова — корректный оператор, разложение (факторизация, декомпозиция) операторов (уравнений), интегро-дифференциальные уравнения, краевые задачи, точное решение.

Для цитирования: Tsilika K. D. Decomposition of abstract linear operators on Banach spaces. *Информационно-управляющие системы*, 2021, № 2, с. 2–12. doi:10.31799/1684-8853-2021-2-2-12

For citation: Tsilika K. D. Decomposition of abstract linear operators on Banach spaces. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 2–12. doi:10.31799/1684-8853-2021-2-2-12

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, что снижает рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12-ти языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org

UDC 519.633.6, 519.642.2
doi:10.31799/1684-8853-2021-2-13-19

Articles

The implementation of the boundary element method to the Helmholtz equation of acoustics

S. A. Sivak[a], *Post-Graduate Student, orcid.org/0000-0003-4740-2210, siwakserg@yandex.ru*
M. E. Royak[a], *Dr. Sc., Tech., Professor, orcid.org/0000-0001-8304-7784*
I. M. Stupakov[a], *PhD, Tech., Associate Professor, orcid.org/0000-0003-1094-3961*
E. S. Voznuk[a], *Post-Graduate Student , orcid.org/0000-0001-7362-6002*
A. S. Aleksashin[a], *Master Student, orcid.org/0000-0003-1871-5517*
[a]*Novosibirsk State Technical University, 20, K. Marksa St., 630073, Novosibirsk, Russian Federation*

Introduction: *To solve the Helmholtz equation is important for the branches of engineering that require the simulation of wave phenomenon. Numerical methods allow effectiveness' enhancing of the related computations.* ***Methods:*** *To find a numerical solution of the Helmholtz equation one may apply the boundary element method. Only the surface mesh constructed for the boundary of the three-dimensional domain of interest must be supplied to make the computations possible. This method's trait makes it possible to conduct numerical experiments in the regions which are external in relation to some Euclidian three-dimensional subdomain bounded in the three-dimensional space. The later also provides the opportunity of not using additional geometric techniques to consider the infinitely distant boundary. However, it's only possible to use the boundary element methods either for the homogeneous domains or for the domains composed out of adjacent homogeneous subdomains.* ***Results:*** *The implementation of the boundary element method was committed in the program complex named Quasar. The discrepancy between the analytic solution approximation and the numerical results computed through the boundary element method for internal and external boundary value problems was analyzed. The results computed via the finite element method for the model boundary value problems are also provided for the purpose of the comparative analysis done between these two approaches.* ***Practical relevance:*** *The method gives an opportunity to solve the Helmholtz equation in an unbounded region which is a significant advantage over the numerical methods requiring the volume discretization of computational domains in general and over the finite element method in particular.* ***Discussion:*** *It is planned to make a coupling of the two methods for the purpose of providing the opportunity to conduct the computations in the complex regions with unbounded homogeneous subdomain and subdomains with substantial inhomogeneity inside.*

Keywords *— boundary element method, finite element method, the Helmholtz equation, acoustics.*

For citation: Sivak S. A., Royak M. E., Stupakov I. M., Voznuk E. S., Aleksashin A. S. The implementation of the boundary element method to the Helmholtz equation of acoustics. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 13–19. doi:10.31799/1684-8853-2021-2-13-19

Introduction

One of the most vastly used instruments applied to solve differential equations is the boundary element method (BEM) because it's possible to use BEM for the computations in regions with infinitely distant boundaries in order to find a solution to the so-called external boundary problem. This is particularly important for the problems of wave propagation.

The method has been in use for a long time. Its first mentions may be found in [1–5]. These papers consider the collocation version of BEM. In present days, the versions of BEM based on Galerkin's form are much more preferred. Probably, the first papers describing these versions are [6–9].

There're two versions of BEM: direct and indirect. The direct method is based on the so-called reciprocity relation, which may be seen while analyzing problems based on the concept of fundamental solution of differential equation. For example, the classic work describing BEM in the mentioned context is [10]. The indirect approach of BEM applied to the problem of acoustics is described, for instance, in [11]. In our work, the direct version of BEM is under consideration.

The classic disadvantage of the original versions of BEM is the necessity to work with dense matrices of SLAE produced by the method. Hence there are many different techniques helping to minimize the asymptotic complexity of BEM while working with such matrices. The techniques are the method of T-spline curves [12], the wavelet approach [13–16], the adaptive cross-approximation [10, 17–19] and the fast multipole method [20–24].

It is also worth mentioning that BEM is only capable of handling the cases of the domains that can be decomposed into subdomains with homogeneous media. However, it's possible to get rid of this problem by coupling BEM with FEM (finite element method) so that significantly inhomogeneous domains are handled by the FEM part and the remaining domains are taken care of by BEM. Such coupling is done in [25–29].

The Helmholtz equation of acoustics

The wave equation in a homogeneous medium Ω is of the form:

$$\Delta u(\mathbf{x},\, t)=\frac{\partial^2 u(\mathbf{x},\, t)}{v^2\partial t^2}+F(\mathbf{x},\, t),\ \mathbf{x}\in\Omega. \qquad (1)$$

The parameters of (1) in terms of acoustics can be seen as follows: u — velocity potential; $\mathbf{x}$ — point-vector in space; t — time; v — speed of sound in the medium; F — intensity-function of volume sources of sound; Ω — the homogeneous domain where the problem (1) is to be solved [30].

For the boundary Γ of the domain Ω let the following be true:

$$\Gamma=\Gamma_1\cup\Gamma_2,\ \Gamma_1\cap\Gamma_2=\varnothing.$$

The boundary conditions on Γ_1 and Γ_2 are written as follows:

$$u(\mathbf{x},\, t)\big|_{\mathbf{x}\in\Gamma_1}=F_D(\mathbf{x},\, t); \qquad (2)$$

$$\frac{\partial u(\mathbf{x},\, t)}{\partial\mathbf{n}}\bigg|_{\mathbf{x}\in\Gamma_2}=F_N(\mathbf{x},\, t), \qquad (3)$$

where $\mathbf{n}$ is a normal vector defined on Γ and external with respect to Ω.

Suppose for the functions in (1)–(3) the following representation is justified:

$$F(\mathbf{x},\, t)=F(\mathbf{x})e^{i\omega t}; \qquad (4)$$

$$F_D(\mathbf{x},\, t)=F_D(\mathbf{x})e^{i\omega t}; \qquad (5)$$

$$F_N(\mathbf{x},\, t)=F_N(\mathbf{x})e^{i\omega t}, \qquad (6)$$

where i designates the imaginary unit; ω is the angular frequency.

As a corollary of (4)–(6):

$$u(\mathbf{x},\, t)=u(\mathbf{x})e^{i\omega t}. \qquad (7)$$

Substituting (7) into (1) one derives the Helmholtz equation:

$$\Delta u(\mathbf{x})+k^2u(\mathbf{x})=F(\mathbf{x}),\ k=\frac{\omega}{v}. \qquad (8)$$

The boundary conditions then may be represented accordingly:

$$u(\mathbf{x})\big|_{\mathbf{x}\in\Gamma_1}=F_D(\mathbf{x}); \qquad (9)$$

$$\frac{\partial u(\mathbf{x})}{\partial\mathbf{n}}\bigg|_{\mathbf{x}\in\Gamma_2}=F_N(\mathbf{x}). \qquad (10)$$

For what follows next, suppose that $F=0$, so there's no volume sources of sound waves in Ω.

The boundary element method

The method exploits the boundary representation of the unknown function u (8) implementing the concept of the so-called trace operators. Let us define the trace operators for the domain Ω: the Dirichlet trace γ_0^Ω and the Neumann trace γ_1^Ω:

$$\left(\gamma_0^\Omega u\right)(\mathbf{x})=\lim_{\mathbf{r}\in\Omega,\mathbf{r}\to\mathbf{x}}u(\mathbf{r}),\ \mathbf{x}\in\Gamma; \qquad (11)$$

$$\left(\gamma_1^\Omega u\right)(\mathbf{x})=\lim_{\mathbf{r}\in\Omega,\mathbf{r}\to\mathbf{x}}\mathbf{n}(\mathbf{x})\cdot\nabla u(\mathbf{r}),\ \mathbf{x}\in\Gamma, \qquad (12)$$

where $\mathbf{n}$ is the unit normal vector specified for the point $\mathbf{x}$ on Γ and it's directed to the outside of Ω.

The resulting function of the Dirichlet trace operator applied to the function u is called the Dirichlet data and is designated as $\gamma_0^\Omega u$, whereas $\gamma_1^\Omega u$ stands for the Neumann data respectively.

"The solution u to the equation (8) inside Ω can be expressed by using Green's theorem and the trace operators defined in (11)–(12) [10]"

$$u(\mathbf{y})=\int_{\mathbf{x}\in\Gamma}G_k(\mathbf{y},\,\mathbf{x})\gamma_1^\Omega u(\mathbf{x})\mathrm{d}s_{\mathbf{x}}-\int_{\mathbf{x}\in\Gamma}\gamma_{1,\mathbf{x}}^\Omega G_k(\mathbf{y},\,\mathbf{x})\gamma_0^\Omega u(\mathbf{x})\mathrm{d}s_{\mathbf{x}}, \qquad (13)$$

where G_k is the fundamental solution of the Helmholtz equation:

$$G_k(\mathbf{y},\,\mathbf{x})=\frac{e^{ik\|\mathbf{x}-\mathbf{y}\|}}{4\pi\|\mathbf{x}-\mathbf{y}\|}, \qquad (14)$$

and $\|\cdot\|$ is the Euclidian norm in the three-dimensional space.

By applying the two trace operators (11), (12) to the equation (13), one can formulate a system of integral equations with the unknowns: $\gamma_0^\Omega u$ и $\gamma_1^\Omega u$. To formally define the mentioned system, the half-integer Sobolev spaces are introduced:

$$H^{1/2}(\Gamma)=\left\{g\,|\,g=\gamma_0^\Omega f,\ f\in H^1(\Omega)\right\};$$

$$H^{-1/2}(\Gamma)=\left\{g\,|\,g=\gamma_1^\Omega f,\ f\in H^1(\Omega)\right\},$$

where $H^1(\Omega)$ is the Sobolev space of differentiable functions defined on Ω. For the details related to the half-integer Sobolev spaces see [27]. Let us introduce as well the linear boundary integral operators V_k, K_k, K_k^{add} and D_k following [10]. The single layer operator V_k is defined as follows:

$$(V_kf)(\mathbf{y})=\int_\Gamma G_k(\mathbf{y},\,\mathbf{x})f(\mathbf{x})\mathrm{d}\Gamma_{\mathbf{x}},$$

$$V_k:H^{-1/2}(\Gamma)\to H^{1/2}(\Gamma), \qquad (15)$$

the adjoint double layer operator $(K'_k f)$:

$$(K'_k f)(\mathbf{y}) = \int_\Gamma \gamma_{1,\mathbf{y}}^\Omega G_k(\mathbf{y}, \mathbf{x}) f(\mathbf{x}) \mathrm{d}\Gamma_\mathbf{x},$$
$$K'_k : H^{-1/2}(\Gamma) \to H^{-1/2}(\Gamma), \quad (16)$$

the double layer operator K_k:

$$(K_k f)(\mathbf{y}) = \int_{\mathbf{x}\in\Gamma} \gamma_{1,\mathbf{x}}^\Omega G_k(\mathbf{y}, \mathbf{x}) f(\mathbf{x}) \mathrm{d}s_\mathbf{x},$$
$$K_k : H^{1/2}(\Gamma) \to H^{1/2}(\Gamma), \quad (17)$$

and the hypersingular operator D_k:

$$(D_k f)(\mathbf{y}) = \gamma_{1,\mathbf{y}} \int_{\mathbf{x}\in\Gamma} \gamma_{1,\mathbf{x}}^\Omega G_k(\mathbf{y}, \mathbf{x}) f(\mathbf{x}) \mathrm{d}s_\mathbf{x},$$
$$D_k : H^{1/2}(\Gamma) \to H^{-1/2}(\Gamma). \quad (18)$$

Here's also the definition of the duality pairing between the half-integer Sobolev spaces $H^{1/2}$ and $H^{-1/2}$:

$$\langle u, w\rangle = \int_{\mathbf{x}\in\Gamma} u(\mathbf{x})\overline{w}(\mathbf{x}) \mathrm{d}s_\mathbf{x}, \; u \in H^{1/2}, \; w \in H^{-1/2}. \quad (19)$$

Using relations (15)–(18), the Galerkin representation of integral equation can be obtained in the following form [10]:

$$\langle V_k \gamma_1^\Omega u, w\rangle = \left\langle \left(\frac{1}{2} I + K_k\right) \gamma_0^\Omega u, w \right\rangle, \; \forall w \in H^{-1/2}(\Gamma); \quad (20)$$

$$\langle D_k \gamma_0^\Omega u, v\rangle = \left\langle \left(\frac{1}{2} I - K'_k\right) \gamma_1^\Omega u, v \right\rangle, \; \forall v \in H^{1/2}(\Gamma). \quad (21)$$

If there's only the Dirichlet data function defined on Γ then through the substitution of the known data into (20) one derives the variational problem with the Neumann data as the only unknown. The variational problem (21) allows determining the Dirichlet data when the Neumann data is predefined. The later problem is solvable and has a unique solution only when the number $-k^2$ is not an eigenvalue of the Laplace operator [28]. When the two conditions are mixed on the border of Ω then a variational problem has to be solved. This problem can be formulated in terms of the Steklov — Poincare operator [10]:

$$\langle S_k \gamma_0^\Omega u, v\rangle = \langle \gamma_1^\Omega u, v\rangle, \quad (22)$$

where S_k is defined as follows:

$$S_k = D_k + \left(\frac{1}{2} I + K'_k\right) V_k^{-1} \left(\frac{1}{2} I + K_k\right), \quad (23)$$

and the test function v is from the space of functions, that are equal to zero on Γ_1.

The discretization of (20) and (21) is possible via projecting the unknown data to the finite dimensional subspaces $U_h(\Gamma_h) \subset H^{1/2}(\Gamma_h)$ и $W_h(\Gamma_h) \subset H^{-1/2}(\Gamma_h)$, where Γ_h may stand for a surface mesh which geometry approximates Γ, h is a discretization parameter.

Let the dimension of $U_h(\Gamma_h)$ be equal to N and the dimension $W_h(\Gamma_h)$ be equal to M respectively. Let also g_p, $p = 1, N$ be the basis functions in $U_h(\Gamma_h)$, w_q, $q = 1, M$ — the basis functions in $W_h(\Gamma_h)$. In order to construct the corresponding discreate system, one can approximate the Dirichlet and Neumann data using the linear combinations of the vectors belonging to the corresponding finite-dimensional subspaces:

$$\gamma_0^\Omega u(\mathbf{x}) \approx \sum_{p=1}^N \alpha_p g_p(\mathbf{x}), \; g_p \in U_h(\Gamma); \quad (24)$$

$$\gamma_1^\Omega u(\mathbf{x}) \approx \sum_{q=1}^M \beta_q w_q(\mathbf{x}), \; w_q \in W_h(\Gamma). \quad (25)$$

Substituting (24), (25) into (20), (21) one derives a SLAE:

$$\begin{pmatrix} \mathbf{V} & -\mathbf{K} \\ \mathbf{K}^\mathrm{T} & \mathbf{D} \end{pmatrix} \begin{pmatrix} \boldsymbol{\beta} \\ \boldsymbol{\alpha} \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \boldsymbol{\Phi} \end{pmatrix}, \quad (26)$$

where $\boldsymbol{\alpha}$ is a vector of coefficients α_p in decomposition (24); $\boldsymbol{\beta}$ — vector of coefficients β_q in (25). SLAE blocks in (26) can be expressed as follows:

$$\mathbf{V}_{i,j} = \langle V_k w_i, w_j\rangle, \; i, j = 1, M; \quad (27)$$

$$\mathbf{D}_{i,j} = \langle D_k g_i, g_j\rangle, \; i, j = 1, N; \quad (28)$$

$$\mathbf{K}_{i,j} = \left\langle \left(\frac{1}{2} I + K_k\right) g_i, w_j \right\rangle, \; i = 1, N, \; j = 1, M; \quad (29)$$

$$\boldsymbol{\Phi}_i = \langle F_N, g_i\rangle, \; i = 1, N. \quad (30)$$

The indirect integration of the function G_k stands in the formulae (27)–(29) because of the definitions (15)–(18). This is why the computation of (27)–(29) is not trivial. The traditional methods of numerical integration are inapplicable to the problem of computing the correct values because the fundamental solution $G_k(\mathbf{x}, \mathbf{y})$ is not continuous when the arguments $\mathbf{x}$ and $\mathbf{y}$ are equal. Different solutions to this problem are suggested in [29–35].

FEM and BEM comparison conducted via model problems

As a part of the computer program implementation of BEM, a mesh composed out of triangular

elements was exploited to approximate the boundary of the computational domains specified for the model problems. The basis functions g_q of $W_h(\Gamma_h)$ used to approximate the Neumann data were chosen to be piecewise constant functions equal to one only on their corresponding local supports that are triangles of the mesh Γ_h. The basis functions w_p of $U_h(\Gamma_h)$ are piecewise linear functions. See more about the basis functions in [10]. For the finite element method program implementation, the quadratic basis was chosen. See more about quadratic basis implementation for the Helmholtz equation solved via FEM in [36].

To test the efficiency of the computation strategies, let us consider the model problems described below.

The first model problem geometry looks like this: in a closed domain of a cube with 20 m length of its edges, a ball of radius equal to 1.5 m and a central point coincident with the center of the cube is situated. The wave number k in (8) is equal to 2 m^{-1}, which corresponds to the case of the sound speed equal to 400 m/s and the frequency equal to 127.32 Hz. The boundary conditions for all the boundary parts can be expressed as follows:

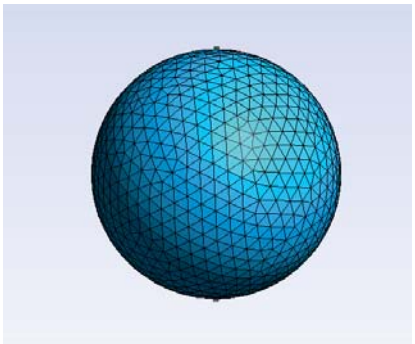
$$u(\mathbf{x})\big|_{\mathbf{x}\in\Gamma} = \cos(kx), \qquad (31)$$

where x is a coordinate of $\mathbf{x}$ along OX axis. Every axis of the Cartesian coordinate system is parallel to one of the edges of the cube. It's clear that with conditions (31) the corresponding analytic solution of (8) takes a form

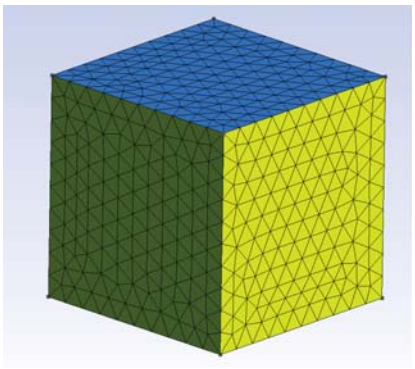
$$u(\mathbf{x}) = \cos(kx) \qquad (32)$$

everywhere in the computation domain.

The surface mesh (Fig. 1) used for BEM computations consists of 3284 elements. The number of nodes is equal to 1646. The volume mesh (Fig. 2) used for the FEM computations is composed out of 17133 elements. The corresponding number of nodes is 26007.



■ ***Fig. 1.*** An example of the surface mesh of the sphere used for the BEM computations



■ ***Fig. 2.*** An example of the cube mesh used for the FEM computations

Figure 3 illustrates the curves of relative discrepancies of the solutions resulted from the implementation of numerical approaches in relation with the analytic solution. The values are given at the points situated along the OX axis. The value of relative discrepancy is equal to:

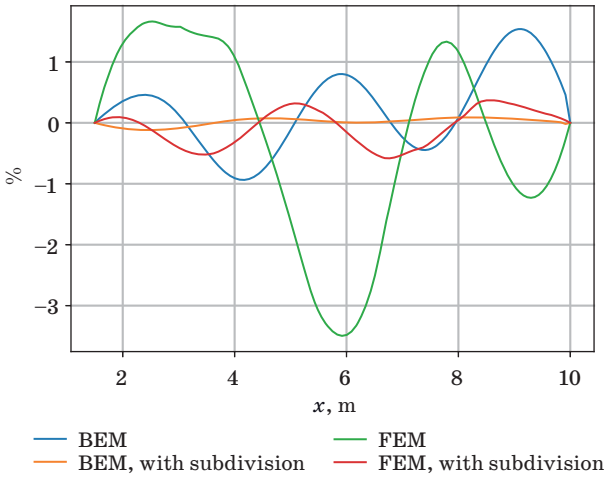
$$\frac{u(\mathbf{x}) - u^*(\mathbf{x})}{\max\left|u^*\right|}.$$

As one can see, the solution resulted from BEM turns out to be more accurate than the one obtained with FEM.

Let's solve the problem for which the analytic solution is known. An incident wave in a medium is represented as follows:

$$\Psi_{inc} = e^{i(-\mathbf{k}\cdot\mathbf{x})},$$

where i is an imaginary one; $\mathbf{k}$ is the direction of the incident wave; $\mathbf{x}$ — radius vector characterizing



■ ***Fig. 3.*** The numerical errors' curves produced for the plane wave solution compared with the numerical methods' results working with the original mesh and its subdivision

the position in space. The spheric boundary of the ball is the source of the scattered wave Ψ_{sc}. The sum of Ψ_{sc} and Ψ_{inc} is denoted as Ψ. Let the Dirichlet condition be imposed on the sphere:

$$\Psi\big|_{\Gamma_s} = \Psi_{inc} + \Psi_{sc}\big|_{\Gamma_s} = 0,$$

or

$$\Psi_{sc}\big|_{\Gamma_s} = -\Psi_{inc}\big|_{\Gamma_s} = 0, \qquad (33)$$

where Γ_s is the spheric boundary of the ball.

The scattered wave should then take a form [37]:

$$\Psi_{sc}(\mathbf{x}) = \sum_{m=0}^{\infty} (2m+1) i^{-m} P_m\left(\cos(\theta)\right) \times$$
$$\times \left(j_m\left(k\|\mathbf{x}\|\right) - \frac{j_m(ka)}{h_m(ka)} h_m\left(k\|\mathbf{x}\|\right) \right) - \Psi_{inc}(\mathbf{x}), \qquad (34)$$

where P_m — the Legendre polynomial of order m; θ is the angle between $\mathbf{x}$ and $\mathbf{k}$; j_m — the spherical Bessel function of order m; k — the modulus of $\mathbf{k}$ or its length; a — the sphere radius; h_m — the spherical Hankel function of order m.

To compare (34) with the numerical solution of the Helmholtz equation, one has to take as an approximation of $\Psi_{sc}(\mathbf{x})$ a sum composed out of a finite number of terms in (34):

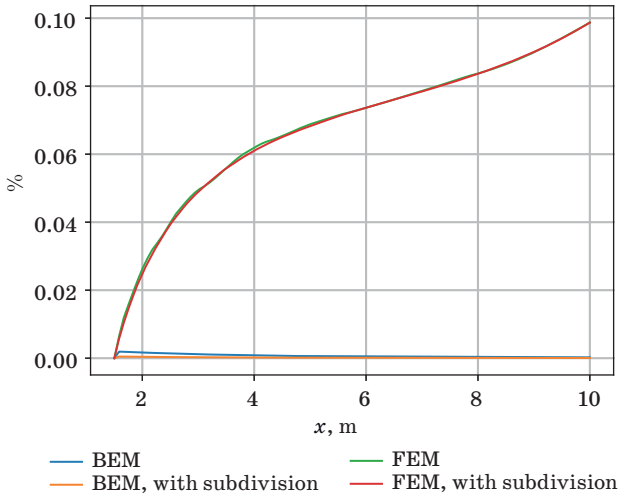
$$\Psi_K(\mathbf{x}) = \sum_{m=0}^{K} (2m+1) i^{-m} P_m\left(\cos(\theta)\right) \times$$
$$\times \left(j_m(kr) - \frac{j_m(ka)}{h_m(ka)} h_m(kr) \right) - e^{-\mathbf{x}\cdot\mathbf{k}}. \qquad (35)$$

To make such comparison possible, the value of K was chosen to be equal to 20, which provides six digits of the approximation accuracy.

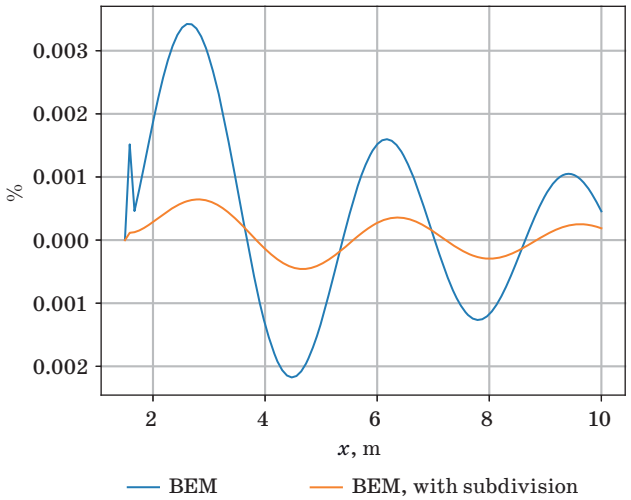
Let the value of k be equal to 0.1 m^{-1}. To be able to solve this problem, FEM requires the area of significant volume to be set up. In our framework, it's a cube with the edge length equal to 20 m. That's why the FEM geometry of the computation domain is left unchanged in comparison with the previous problem description. The cube boundary also requires the Dirichlet condition to be homogeneous. The BEM variation of this problems is solved in the open region.

Figure 4 illustrates that the numerical discrepancy grows for FEM when the point argument approaches the border of the computation domain that is far away from the sphere. The set of points used for the comparison (see Figs. 3 and 4) is the same.

Figure 5 demonstrates the curves of relative discrepancy only for the case of BEM computations.



■ ***Fig. 4.*** The scattered wave numerical error curves



■ ***Fig. 5.*** The comparison for the scattered wave with the wave number equal to 2 m^{-1}

FEM requires a significant number of volume elements in case of the border distant from the sphere when $k = 2$ m^{-1}. That's why we were unable to obtain adequate FEM results.

Conclusion

The program implementation of the BEM allowing the Helmholtz equation to be solved in bounded and unbounded regions has been developed. The validity of this approach has been tested for internal and external Dirichlet problems. The comparison with analytics demonstrates effectiveness of BEM relatively to FEM because the latter requires a fine mesh to be used in the computation domains of significant volume.

References

1. Chen L. H., Schweikert D. G. Sound radiation from an arbitrary body. *The Journal of the Acoustical society of America*, 1963, no. 10, pp. 1626–1632. doi:10.1121/1.1918770
2. Banaugh R. P., Goldsmith W. Diffraction of steady acoustic waves by surfaces of arbitrary shape. *The Journal of the Acoustical Society of America*, 1963, no. 10, pp. 1590–1601. doi:10.1121/1.1918764
3. Chertock G. Sound radiation from vibrating surfaces. *The Journal of the Acoustical Society of America*, 1964, no. 7, pp. 1305–1313. doi:10.1121/1.2142487
4. Greenspan D., Werner P. A numerical method for the exterior Dirichlet problem for the reduced wave equation. *Archive for Rational Mechanics and Analysis*, 1966, no. 4, pp. 288–316. doi:10.1007/BF00281165
5. Copley L. G. Integral equation method for radiation from vibrating bodies. *The Journal of the Acoustical Society of America*, 1967, no. 4A, pp. 807–816. doi:10.1121/1.1910410
6. Hsiao G. C., Wendland W. L. Super-approximation for boundary integral methods. *Proc. of the 4th IMACS Conf. on Computer Mem. for Part. Diff. Equ.*, 1981, pp. 200–205.
7. Wendland W. L. *On asymptotic error estimates for combined BEM and FEM*. In: Stein E., Wendland W. (Eds.) *Finite element and boundary element techniques from mathematical and engineering point of view*. Springer-Verlag, New York, 1988. Pp. 273–333. doi:10.1002/zamm.19900701019
8. Demkowicz L., Karafiat A., Oden J. T. Solution of elastic scattering problems in linear acoustics using hp boundary element method. *Computer Methods in Applied Mechanics and Engineering*, 1992, no. 1–3, pp. 251–282. doi:10.1016/0045-7825(92)90025-F
9. Geng P., Oden J. T., Demkowicz L. Numerical solution and a posteriori error estimation of exterior acoustics problems by a boundary element method at high wave numbers. *The Journal of the Acoustical Society of America*, 1996, no. 1, pp. 335–345. doi:10.1121/1.415883
10. Rjasa now S., Steinbach O. *The fast solution of boundary integral equations*. Springer Science & Business Media, 2007. 291 p.
11. Coox L., Atak O., Vandepitte D., Desmet W. An isogeometric indirect boundary element method for solving acoustic problems in open-boundary domains. *Computer Methods in Applied Mechanics and Engineering*, 2017, pp. 186–208. doi:10.1016/j.cma.2016.05.039
12. Simpson R. N., Scott M. A., Taus M., Thomas D. C., Lian H. Acoustic isogeometric boundary element analysis. *Computer Methods in Applied Mechanics and Engineering*, 2014, pp. 265–290. doi:10.1016/j.cma.2013.10.026
13. Harbrecht H., Schneiderd R. Biorthogonal wavelet bases for the boundary element method. *Mathematische Nachrichten*, 2004, vol. 261, no. 1, pp. 167–188. doi:10.1002/mana.200310171
14. Wang G. A hybrid wavelet expansion and boundary element analysis of electromagnetic scattering from conducting objects. *IEEE Transactions on Antennas and Propagation*, 1995, vol. 43, no. 2, pp. 170–178. doi:10.1109/8.366379
15. Koro K., Abe K. Non-orthogonal spline wavelets for boundary element analysis. *Engineering Analysis with Boundary Elements*, 2001, vol. 25, no. 3, pp. 149–164. doi:10.1016/S0955-7997(01)00036-4
16. Harbrecht H., Utzinger M. On adaptive wavelet boundary element methods. *Journal of Computational Mathematics*, 2018, vol. 36, no. 1, pp. 90–109. doi:10.4208/jcm.1610-m2016-0496
17. Kurz S., Rain O., Rjasanow S. The adaptive cross-approximation technique for the 3D boundary-element method. *IEEE Transactions on Magnetics*, 2002, no. 2, pp. 421–424. doi:10.1109/20.996112
18. Brancati A., Aliabadi M. H., Benedetti I. Hierarchical adaptive cross approximation GMRES technique for solution of acoustic problems using the boundary element method. *Computer Modeling in Engineering and Sciences (CMES)*, 2009, vol. 38, no. 2, pp. 149–172. doi:10.1109/20.996112
19. Smajic J., Andjelic Z., Bebendorf M. Fast BEM for eddy-current problems using H-matrices and adaptive cross approximation. *IEEE Transactions on Magnetics*, 2007, vol. 43, no. 4, pp. 1269–1272. doi:10.1109/TMAG.2006.890971
20. Coifman R., Rokhlin V., Wandzura S. The fast multipole method for electromagnetic scattering calculations. *Proceedings of IEEE Antennas and Propagation Society International Symposium*, 1993, pp. 48–51. doi:10.1109/APS.1993.385405
21. Shen L., Liu Y. J. An adaptive fast multipole boundary element method for three-dimensional acoustic wave problems based on the Burton–Miller formulation. *Computational Mechanics*, 2007, no. 3, pp. 461–472. doi:10.1007/s00466-006-0121-2
22. Gumerov N. A., Duraiswami R. *Fast multipole methods for the Helmholtz equation in three dimensions*. Elsevier, 2005. 551 p.
23. Gumerov N. A., Duraiswami R. *Fast, exact, and stable computation of multipole translation and rotation coefficients for the 3-d Helmholtz equation*. 2001, Available at: https://drum.lib.umd.edu/bitstream/handle/1903/1141/CS-TR-4264.pdf?sequence = 1 (accessed 8 August 2020).
24. Sivak S. A., Stupakov I. M., Kondratieva N. S. A combined vector method of finite and boundary elements for simulating electromagnetic filed propagation considering an eddy current model. *Science Bulletin of the Novosibirsk State Technical University*, 2018, no. 4(73), pp. 79–90 (In Russian). doi:10.17212/1814-1196-2018-4-79-90
25. Stupakov I. M., Royak M. E., Bubley P. A. Using fast multipole method for magnetic field calculation in complex system of current coils. *2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE)*, 2018, pp. 307–310. doi:10.1109/APEIE.2018.8545530

26. Stupakov I., Royak M., Kondratyeva N. Coupled finite and boundary element method for solving magnetic hysteresis problems. *Transactions on Engineering Sciences*, 2019, pp. 125–135. doi:10.2495/be420111
27. Adams R. A., Fournier J. J. F. *Sobolev spaces*. Academic Press, New York, 2003. 317 p.
28. Stolper M. Computing and compression of the boundary element matrices for the Helmholtz equation. *Journal of Numerical Mathematics*, 2004, no. 1, pp. 55–75. doi:10.1515/1569395041172935
29. Keller P. A method for indefinite integration of oscillatory and singular functions. *Numerical Algorithms*, 2007, no. 3, pp. 219–251. doi:10.1007/s11075-007-9134-y
30. Assari P., Adibi H., Dehghan M. The numerical solution of weakly singular integral equations based on the meshless product integration (MPI) method with error analysis. *Applied Numerical Mathematics*, 2014, pp. 76–93. doi:10.1016/j.apnum.2014.02.013
31. Nair N. V., Pray A. J., Villa-Giron J., Shanker B., Wilton D. R. A singularity cancellation technique for weakly singular integrals on higher order surface descriptions. *IEEE Transactions on Antennas and Propagation*, 2013, no. 4, pp. 2347–2352. doi:10.1109/TAP.2013.2238880
32. Cancela A. C. *Transformation methods for the integration of singular and near-singular functions in XFEM*. Doctoral Dissertation, Tesis Doctoral, Universidad Nacional de Educaci n a Distancia (UNED) Faculty of Science Department of Statistics, Operations Research and Numerical Analysis, 2017. Available at: http://62.204.194.43/fez/eserv/tesisuned:Ciencias-Acano/CANO_CANCELA_Alfredo_Tesis.pdf (accessed 5 January 2021).
33. Vasconcelos A. C. A., Cavalcante I., Labaki J. On the accuracy of adaptive quadratures in the numerical integration of singular Green's functions for layered media. *Proceedings of the Iberian Latin American Congress on Computational Methods in Engineering*, 2017. doi:10.20906/cps/cilamce2017-0063
34. Järvenp S., Taskinen M., Yl-Oijala P. Singularity extraction technique for integral equation methods with higher order basis functions on plane triangles and tetrahedra. *International Journal for Numerical Methods in Engineering*, 2003, no. 8, pp. 1149–1165. doi:10.1002/nme.810
35. Huang S., Liu Y. J. A new fast direct solver for the boundary element method. *Computational Mechanics*, 2017, no. 3, pp. 379–392. doi:10.1007/s00466-017-1407-2
36. Solovejchik J. G., Rojak M. E., Persova M. G. *Metod konechnyh jelementov dlja reshenija skaljarnyh i vektornyh zadach* [The finite element method for solving the scalar and vector problems]. Novosibirsk, NSTU Publ., 2007. 896 p. (In Russian).
37. Lependin L. F. *Akustika* [Acoustics]. Moscow, Vysshaja shkola Publ., 1978. 448 p. (In Russian).

УДК 519.633.6, 519.642.2
doi:10.31799/1684-8853-2021-2-13-19

Использование метода граничных элементов при решении уравнения Гельмгольца для задачи акустики

С. А. Сивак[a], аспирант, orcid.org/0000-0003-4740-2210, siwakserg@yandex.ru
М. Э. Рояк[a], доктор техн. наук, профессор, orcid.org/0000-0001-8304-7784
И. М. Ступаков[a], канд. техн. наук, доцент, orcid.org/0000-0003-1094-3961
Е. С. Вознюк[a], аспирант, orcid.org/0000-0001-7362-6002
А. С. Алексашин[a], магистрант, orcid.org/0000-0003-1871-5517
[a]Новосибирский государственный технический университет, К. Маркса пр., 20, Новосибирск, 630073, РФ

Введение: решение уравнения Гельмгольца представляет практическую значимость для отраслей, в которых требуется моделирование волновых процессов. Использование численных методов позволяет повысить эффективность проводимых расчетов. **Методы:** для численного решения уравнения Гельмгольца можно использовать метод граничных элементов. Для его применения необходимо построить только поверхностную сетку границы трехмерной области, в которой решается задача. Данная особенность позволяет производить расчеты в том числе и во внешней области по отношению к некоторой ограниченной замкнутой подобласти трехмерного евклидова пространства, что также дает возможность обходиться без дополнительных геометрических построений, необходимых для учета бесконечно удаленной границы. Однако расчет методом граничных элементов возможно проводить только для однородной области либо для множества смежных однородных областей. **Результаты:** разработана реализация метода граничных элементов для решения уравнения Гельмгольца применительно к задаче акустики в рамках программного комплекса Quasar. Проанализировано отклонение результатов, полученных методом граничных элементов для внутренней и внешней краевых задач, от приближенной аналитики. Приводятся также результаты, полученные при решении модельных задач методом конечных элементов, для сравнения двух различных подходов. **Практическая значимость:** данный метод позволяет решать уравнение Гельмгольца в неограниченной области, что является большим преимуществом по сравнению с численными методами, требующими объемной дискретизации расчетной области, и, в частности, с методом конечных элементов. **Обсуждение:** в дальнейшем планируется осуществить комбинирование методов граничных и конечных элементов для расчетов в неограниченной подобласти с постоянными параметрами среды и в расчетных подобластях, чья среда является существенно неоднородной.

Ключевые слова — метод граничных элементов, метод конечных элементов, уравнение Гельмгольца, акустика.

Для цитирования: Sivak S. A., Royak M. E., Stupakov I. M., Voznuk E. S., Aleksashin A. S. The implementation of the boundary element method to the Helmholtz equation of acoustics. *Информационно-управляющие системы*, 2021, № 2, с. 13–19. doi:10.31799/1684-8853-2021-2-13-19

For citation: Sivak S. A., Royak M. E., Stupakov I. M., Voznuk E. S., Aleksashin A. S. The implementation of the boundary element method to the Helmholtz equation of acoustics. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 13–19. doi:10.31799/1684-8853-2021-2-13-19

UDC 004.93
doi:10.31799/1684-8853-2021-2-20-32

Articles

Second-order total generalized variation based model for restoring images with mixed Poisson — Gaussian noise

Pham Cong Thang[a], *PhD, Lecturer, orcid.org/0000-0002-6428-102X, pcthang@dut.udn.vn*
Tran Thi Thu Thao[b], *M. Sc., Lecturer, orcid.org/0000-0001-7705-2405*
Nguyen Thanh Cong[a], *M. Sc., Specialist, orcid.org/0000-0002-8060-0238*
Vo Duc Hoang[a], *PhD, Lecturer, orcid.org/0000-0002-6974-9023*
[a]*The University of Danang — University of Science and Technology, 54 Nguyen Luong Bang Street, Danang 550000, Vietnam*
[b]*The University of Danang — University of Economics, 71 Ngu Hanh Son Street, Danang 550000, Vietnam*

Introduction: *A common problem in image restoration is image denoising. Among many noise models, the mixed Poisson — Gaussian model has recently aroused considerable interest.* ***Purpose:*** *Development of a model for denoising images corrupted by mixed Poisson — Gaussian noise, along with an algorithm for solving the resulting minimization problem.* ***Results:*** *We proposed a new total variation model for restoring an image with mixed Poisson — Gaussian noise, based on second-order total generalized variation. In order to solve this problem, an efficient alternating minimization algorithm is used. To illustrate its comparison with related methods, experimental results are presented, demonstrating the high efficiency of the proposed approach.* ***Practical relevance:*** *The proposed model allows you to remove mixed Poisson — Gaussian noise in digital images, preserving the edges. The presented numerical results demonstrate the competitive features of the proposed model.*

Keywords *— image denoising, total variation, minimization, mixed Poisson — Gausian noise.*

For citation: Pham C. T., Tran T. T. T., Nguyen T. C., Vo D. H. Second-order total generalized variation based model for restoring images with mixed Poisson — Gaussian noise. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 20–32. doi:10.31799/1684-8853-2021-2-20-32

Introduction

Image denoising is an important task in digital image processing. During the formation procedure, the image is usually degraded by noise. The denoising problem is to recover u from an observed image f with the size of $M \times N$. In literature, many types of noise generated by different devices and processes have been considered, e. g., Gaussian [1], Poisson [2], as well as mixed noise, e. g., mixed Poisson — Gaussian [3]. In practical, the Poisson — Gaussian model can accurately describe the noise present in a number of imaging applications such as astronomy, medicine, biology, etc... [4, 5]. The Poisson component accounts for the signal-dependent uncertainty inherent to the photon counting process, and the additive white Gaussian noise component accounts for the other signal-independent noise sources, such as thermal noise [6].

As is well known, several approaches have been developed for recovering images corrupted by the mixed Poisson — Gaussian noise. Among them, one of popular approaches is perhaps total variation (TV) model for mixed Poisson — Gaussian noise removal (TVPG) [7, 8] using the TV norm as regularization term, formulated as follows:

$$u^* = \arg\min_u \left(\int_\Omega |\nabla u| \, \mathrm{d}x + \frac{\lambda}{2} \int_\Omega (u - f)^2 \, \mathrm{d}x + \beta \int_\Omega (u - f \log u) \, \mathrm{d}x \right), \quad (1)$$

where f is the observed image; $\Omega \subset \mathbb{R}^2$ be bounded open set and u must be positive almost everywhere over Ω; λ, β are positive regularization parameters.

In literature, we can find many efficient algorithms for solving the TV regularized mixed Poison — Gaussian denoising model (1), such as a primal-dual algorithm [9], an augmented Lagrangian method [10–12], the split Bregman method [13, 14], etc.

As is well known, the TV regularizer framework preserves edges well but has the transformation of smooth regions into piecewise constant regions. To avoid this problem, many regularization techniques for the denoising problem have been introduced, including non-local total variation [15], TV combined with higher-order term [16], Euler's elastic model [17], a mean curvature model [18, 19]. Reccently, a well-known method is the total generalized variation (TGV) introduced as penalty functional for image restoration [20, 21]. TGV includes higher-order derivatives of u. Image reconstructed by TGV regularization usually includes sharp edges and

piecewise polynomial intensities [22]. With simplicity and prominence, the second-order TGV with weight α $\left(TGV_{\alpha}^{2}\right)$ based models have been widely researched recently, and achieved great successes in image processing [23–25]. Applied for image denoising, the resulting model is given by:

$$u^{*}=\arg\min_{u}\left(TGV_{\alpha}^{2}(u)+\frac{\lambda_1}{2}\int_{\Omega}(u-f)^{2}\,\mathrm{d}x\right). \tag{2}$$

The model (2) was proposed in [23] for denoising image corrupted by Gaussian noise. Therefore, in case of mixed Poisson — Gaussian noise, the model itself cannot provide necessary accuracy for further data interpretation and analysis.

Inspired by the advantages of TGV_{α}^{2} regularization, we propose an second-order TGV regularized model for the mixed Poisson — Gaussian noise removal problem as follows:

In this paper, we employ the the second-order TGV instead of the standard TV norm in the model (1) and propose the following optimization problem:

$$u^{*}=\arg\min_{u}\left(TGV_{\alpha}^{2}(u)+\frac{\lambda_1}{2}\int_{\Omega}(u-f)^{2}\,\mathrm{d}x+\lambda_2\int_{\Omega}(u-f\log u)\mathrm{d}x\right), \tag{3}$$

where λ_1 and λ_2 are positive parameter.

Our main contributions in this paper are following. We introduce a new total variation model for restoring image with mixed Poisson — Gaussian on the basis of the TGV_{α}^{2}. The second important advantage is to extend an efficient alternating minimization method for solving the proposed model. Furthermore, we provide experimental results to demonstrate the high efficiency of our algorithm for considered problem, in comparison with related methods.

Proposed method

The denoising model

In this paper, we consider the following optimization problem (3):

$$u^{*}=\arg\min_{u}\left(TGV_{\alpha}^{2}(u)+\frac{\lambda_1}{2}\int_{\Omega}(u-f)^{2}\,\mathrm{d}x+\lambda_2\int_{\Omega}(u-f\log u)\mathrm{d}x\right).$$

Referring [20, 24], we shortly review the concept of the second-order TGV. The definnitions can be found in Appendix.

Following the Refs. [7, 23–26], we have theorem (Theorem 1) for the considered model.

Theorem 1. The optimization problem (3) has a solution.

Proof: The proof will be given in the Appendix for completeness.

According to [20, 23–25], the discrete TGV_{α}^{2} regularization of u can be formulated as

$$TGV_{\alpha}^{2}(u)=\min_{w}\alpha_1\left\|\nabla u-w\right\|_1+\alpha_2\left\|\varepsilon(w)\right\|_1,$$

where $w=(w_1, w_2)^{\mathrm{T}}$; $\varepsilon(w)=(1/2)\left(\nabla w+\nabla w^{\mathrm{T}}\right)$.

The operators $\varepsilon(w)$ and ∇u can be expressed as follows:

$$\nabla u=\begin{bmatrix}\nabla_1 & u\\ \nabla_2 & u\end{bmatrix} \text{ and } \varepsilon(w)=\begin{bmatrix}\nabla_1 w_1 & \frac{1}{2}(\nabla_2 w_1+\nabla_1 w_2)\\ \frac{1}{2}(\nabla_2 w_1+\nabla_1 w_2) & \nabla_2 w_2\end{bmatrix},$$

where $\nabla=(\nabla_1;\nabla_2)$, ∇_1 and ∇_2 are derivative operators in the horizontal and vertical directions, respectively.

According to the version of TGV_{α}^{2}, the discrete version of the minimization problem (3) is given by

$$u^{*} = \arg\min_{u,\, w}\left(\alpha_1 \|\nabla u - w\|_1 + \alpha_2 \|\varepsilon(w)\|_1 + \frac{\lambda}{2}\|u - f\|_2^2 + \beta\langle 1, u - f\log u\rangle\right). \tag{4}$$

Computational method

In this section, we derive the numerical method for problem (4) in detail. By the classical augmented Lagrangian multiplier method [16, 17, 19–21], we introduce three new variables (d, g, z) and rewrite the equation (4) in the constrained optimization problem as follows:

$$\min_{u,\, d, g, z}\left(\alpha_1 \|d\|_1 + \alpha_2 \|g\|_1 + \frac{\lambda}{2}\|z - f\|_2^2 + \beta\langle 1, z - f\log z\rangle\right), \tag{5}$$

$$\text{s.t. } d = \nabla u - w,\ g = \varepsilon(w),\ z = u$$

with

$$d = \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} \text{ and } g = \begin{bmatrix} g_1 & g_3 \\ g_3 & g_2 \end{bmatrix}.$$

The augmented Lagrangian functional for the constrained optimization problem (5) is defined as

$$\mathcal{L}(u,\, w, d,\, g,\, z, \theta_1,\, \mu_2,\, \xi_3) = \left(\alpha_1 \|d\|_1 + \alpha_2 \|g\|_1 + \frac{\lambda}{2}\|z - f\|_2^2 + \beta\langle 1, z - f\log z\rangle - \langle \theta, d - \nabla u + w\rangle + \right.$$

$$\left. + \frac{\eta_1}{2}\|d - \nabla u + w\|_2^2 - \langle \xi, g - \varepsilon(w)\rangle + \frac{\eta_2}{2}\|g - \varepsilon(w)\|_2^2 - \langle \mu, z - u\rangle + \frac{\eta_3}{2}\|z - u\|_2^2\right), \tag{6}$$

where η_1, η_2, η_3 — positive parameters; θ, ξ, μ — with Lagrangian multipliers.

The discrete gradient ∇z and the second-order derivatives $\nabla^2 u$ of an image u for the pixel location (i, j) in $u(i = 1...M;\ j = 1...N)$ are defined like:

$$\nabla_1 u_{i,j} = u_{i+1,j} - u_{i,j},\ \nabla_2 u_{i,j} = u_{i+1,j} - u_{i,j},$$

$$\nabla_1 u_{i,j} = (\nabla_x u_{i,j},\ \nabla_y u_{i,j}),\ \left|\nabla u_{i,j}\right| = \sqrt{\left(\nabla_1 u_{i,j}\right)^2 + \left(\nabla_2 u_{i,j}\right)^2}.$$

The minimization method to solve the problem (6) can be expressed as follows:

$$\begin{cases} u^{(k+1)} = \arg\min\limits_{u}\left(-\left\langle \theta^{(k)}, d^{(k)} - \nabla u + w^{(k)}\right\rangle + \frac{\eta_1}{2}\left\|d^{(k)} - \nabla u + w^{(k)}\right\|_2^2 - \right. \\ \left. - \left\langle \mu^{(k)}, z^{(k)} - u\right\rangle + \frac{\eta_3}{2}\left\|z^{(k)} - u\right\|_2^2\right); \\ w^{(k+1)} = \arg\min\limits_{w}\left(-\left\langle \theta, d^{(k)} - \nabla u^{(k+1)} + w\right\rangle + \frac{\eta_1}{2}\left\|d^{(k)} - \nabla u^{(k+1)} + w\right\|_2^2 - \right. \\ \left. - \left\langle \xi, g^{(k)} - \varepsilon(w)\right\rangle + \frac{\eta_2}{2}\left\|g - \varepsilon(w)\right\|_2^2\right); \\ d^{(k+1)} = \arg\min\limits_{d}\left(\alpha_1 \|d\|_1 - \left\langle \theta, d - \nabla u^{(k+1)} + w^{(k+1)}\right\rangle + \frac{\eta_1}{2}\left\|d - \nabla u^{(k+1)} + w^{(k+1)}\right\|_2^2\right); \\ g^{(k+1)} = \arg\min\limits_{g}\left(\alpha_2 \|g\|_1 - \left\langle \xi^{(k)}, g - \varepsilon\left(w^{(k+1)}\right)\right\rangle + \frac{\eta_2}{2}\left\|g - \varepsilon\left(w^{(k+1)}\right)\right\|_2^2\right); \\ z^{(k+1)} = \arg\min\limits_{z}\left(\frac{\lambda}{2}\|z - f\|_2^2 + \beta\langle 1, z - f\log z\rangle - \left\langle \mu^{(k)}, z - u^{(k+1)}\right\rangle + \frac{\eta_3}{2}\left\|z - u^{(k+1)}\right\|_2^2\right) \end{cases} \tag{7}$$

with update for $\theta_1^{(k+1)}$, $\xi_2^{(k+1)}$, $\mu_3^{(k+1)}$:

$$\begin{cases} \theta^{(k+1)} = \theta^{(k)} + \eta_1\left(\nabla u^{(k+1)} - d^{(k+1)} - w^{(k+1)}\right); \\ \xi^{(k+1)} = \xi^{(k)} + \eta_2\left(\varepsilon\left(w^{(k+1)}\right) - g^{(k+1)}\right); \\ \mu^{(k+1)} = \mu^{(k)} + \eta_3\left(u^{(k+1)} - z^{(k+1)}\right). \end{cases} \tag{8}$$

The *u* subproblem in (7) is given by:

$$u^{(k+1)} = \arg\min_u\left(-\left\langle\theta^{(k)}, d^{(k)} - \nabla u + w^{(k)}\right\rangle + \frac{\eta_1}{2}\left\|d^{(k)} - \nabla u + w^{(k)}\right\|_2^2 - \left\langle\mu^{(k)}, z^{(k)} - u\right\rangle + \right.$$
$$\left. + \frac{\eta_3}{2}\left\|z^{(k)} - u\right\|_2^2\right) = \frac{\eta_1}{2}\left\|d^{(k)} - \nabla u + w^{(k)} - \frac{\theta^{(k)}}{\eta_1}\right\|_2^2 + \frac{\eta_3}{2}\left\|z^{(k)} - u - \frac{\mu^{(k)}}{\eta_3}\right\|_2^2.$$

Thus, we get

$$\eta_1\nabla^{\mathrm{T}}\left(\nabla u + \frac{\theta^{(k)}}{\eta_1} - d^{(k)} - w^{(k)}\right) + \eta_3\left(u + \frac{\mu^{(k)}}{\eta_3} - z^{(k)}\right) = 0. \tag{9}$$

We can rewrite the equation (9) as follows:

$$\left(\eta_1\nabla^{\mathrm{T}}\nabla + \eta_3\right)u^{(k+1)} = \eta_1\nabla^{\mathrm{T}}\left(d^{(k)} + w^{(k)} - \frac{\theta^{(k)}}{\eta_1}\right) + \eta_3\left(z^{(k)} - \frac{\mu^{(k)}}{\eta_3}\right). \tag{10}$$

It is obvious that system (10) is linear and symmetric positive definite, therefore $z^{(k+1)}$ can be efficiently solved by fast Fourier transform [18], under the periodic boundary conditions:

$$u^{(k+1)} = F^{-1}\left(\frac{F\left(\eta_1\nabla^{\mathrm{T}}\left(d^{(k)} + w^{(k)} - \frac{\theta^{(k)}}{\eta_1}\right) + \eta_3\left(z^{(k)} - \frac{\mu^{(k)}}{\eta_3}\right)\right)}{\eta_1 F\left(\nabla^{\mathrm{T}}\nabla\right) + \eta_3}\right), \tag{11}$$

where F and F^{-1} are the forward and inverse Fourier transform operators.

The *w* problem is

$$w^{(k+1)} = \arg\min_w\left(-\left\langle\theta^{(k)}, d^{(k)} - \nabla u^{(k+1)} + w\right\rangle + \right.$$
$$\left. + \frac{\eta_1}{2}\left\|d^{(k)} - \nabla u^{(k+1)} + w\right\|_2^2 - \left\langle\xi^{(k)}, g^{(k)} - \varepsilon(w)\right\rangle + \frac{\eta_2}{2}\left\|g - \varepsilon(w)\right\|_2^2\right) =$$
$$= \frac{\eta_1}{2}\left\|w + d^{(k)} - \nabla u^{(k+1)} - \frac{\theta^{(k)}}{\eta_1}\right\|_2^2 + \frac{\eta_2}{2}\left\|\varepsilon(w) - g^{(k)} + \frac{\xi^{(k)}}{\eta_2}\right\|_2^2.$$

Therefore, we get:

$$\begin{cases} \eta_1\left(d_1^{(k)}-\nabla_1 u^{(k+1)}+w_1-\dfrac{\theta_1^{(k)}}{\eta_1}\right)+\eta_2\nabla_1^{\mathrm{T}}\left(\nabla_1 w_1-g_1+\dfrac{\xi_1^{(k)}}{\eta_2}\right)+ \\ +\eta_2\nabla_2^{\mathrm{T}}\left(\dfrac{1}{2}\left(\nabla_2 w_1+\nabla_1 w_2\right)-g_3+\dfrac{\xi_3^{(k)}}{\eta_2}\right)=0; \\ \eta_1\left(d_2^{(k)}-\nabla_2 u^{(k+1)}+w_2-\dfrac{\theta_2^{(k)}}{\eta_1}\right)+\eta_2\nabla_1^{\mathrm{T}}\left(\dfrac{1}{2}\left(\nabla_2 w_1+\nabla_1 w_2\right)-g_3+\dfrac{\xi_3^{(k)}}{\eta_2}\right)+ \\ +\eta_2\nabla_2^{\mathrm{T}}\left(\nabla_2 w_2-g_2+\dfrac{\xi_2^{(k)}}{\eta_2}\right)=0. \end{cases} \tag{12}$$

We have:

$$\begin{cases} \left(\eta_1 I+\eta_2\nabla_1^{\mathrm{T}}\nabla_1+\dfrac{\eta_2}{2}\nabla_2^{\mathrm{T}}\nabla_2\right)w_1+\dfrac{\eta_2}{2}\nabla_2^{\mathrm{T}}\nabla_1 w_2=\eta_1\left(\nabla_1 u^{(k+1)}-d_1^{(k)}+\dfrac{\theta_1^{(k)}}{\eta_1}\right)+ \\ +\eta_2\nabla_1^{\mathrm{T}}\left(g_1-\dfrac{\xi_1^{(k)}}{\eta_1}\right)+\eta_2\nabla_2^{\mathrm{T}}\left(g_3-\dfrac{\xi_3^{(k)}}{\eta_1}\right); \\ \dfrac{\eta_2}{2}\nabla_1^{\mathrm{T}}\nabla_2 w_1+\left(\eta_1 I+\dfrac{\eta_2}{2}\nabla_1^{\mathrm{T}}\nabla_1+\eta_2\nabla_2^{\mathrm{T}}\nabla_2\right)w_2=\eta_1\left(\nabla_2 u^{(k+1)}-d_2^{(k)}+\dfrac{\theta_2^{(k)}}{\eta_1}\right)+ \\ +\eta_2\nabla_1^{\mathrm{T}}\left(g_3-\dfrac{\xi_3^{(k)}}{\eta_2}\right)+\eta_2\nabla_2^{\mathrm{T}}\left(g_2-\dfrac{\xi_2^{(k)}}{\eta_2}\right). \end{cases} \tag{13}$$

From (13), we have a system of linear equations in two unknowns $w_1^{(k+1)}$, $w_2^{(k+1)}$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} w_1^{(k+1)} \\ w_2^{(k+1)} \end{bmatrix}=\begin{bmatrix} s \\ t \end{bmatrix} \tag{14}$$

with

$$a=\left(\eta_1 I+\eta_2\nabla_1^{\mathrm{T}}\nabla_1+\frac{\eta_2}{2}\nabla_2^{\mathrm{T}}\nabla_2\right);\ b=\frac{\eta_2}{2}\nabla_2^{\mathrm{T}}\nabla_1;\ c=\frac{\eta_2}{2}\nabla_1^{\mathrm{T}}\nabla_2;$$

$$d=\left(\eta_1 I+\frac{\eta_2}{2}\nabla_1^{\mathrm{T}}\nabla_1+\eta_2\nabla_2^{\mathrm{T}}\nabla_2\right);$$

$$s=\eta_1\left(\nabla_1 u^{(k+1)}-d_1^{(k)}+\frac{\theta_1^{(k)}}{\eta_1}\right)+\eta_2\nabla_1^{\mathrm{T}}\left(g_1-\frac{\xi_1^{(k)}}{\eta_1}\right)+\eta_2\nabla_2^{\mathrm{T}}\left(g_3-\frac{\xi_3^{(k)}}{\eta_1}\right),$$

$$t=\eta_1\left(\nabla_2 u^{(k+1)}-d_2^{(k)}+\frac{\theta_2^{(k)}}{\eta_1}\right)+\eta_2\nabla_1^{\mathrm{T}}\left(g_3-\frac{\xi_3^{(k)}}{\eta_2}\right)+\eta_2\nabla_2^{\mathrm{T}}\left(g_2-\frac{\xi_2^{(k)}}{\eta_2}\right).$$

Similar to the u subproblem, we can solve problems (14) with fast Fourier transform, under the periodic boundary conditions:

$$w_1^{(k+1)}=F^{-1}\left(\frac{F(sd-bt)}{F(ad-cb)}\right);\ w_2^{(k+1)}=F^{-1}\left(\frac{F(at-cs)}{F(ad-cb)}\right). \tag{15}$$

The *d* subproblem is given by:

$$d^{(k+1)} = \arg\min_{d}\left(\alpha_1 \|d\|_1 - \left\langle \theta,\, d - \nabla u^{(k+1)} + w^{(k+1)} \right\rangle + \frac{\eta_1}{2}\left\| d - \nabla u^{(k+1)} + w^{(k+1)} \right\|_2^2 \right) =$$

$$= \arg\min_{d}\left(\alpha_1 \|d\|_1 + \frac{\eta_1}{2}\left\| d - \nabla u^{(k+1)} + w^{(k+1)} - \frac{\theta^{(k)}}{\eta_1} \right\|_2^2 \right).$$

The solution of the *d* subproblem can readily be obtained by applying the soft thresholding operator [27]:

$$d^{(k+1)} = \frac{\nabla u^{(k+1)} - w^{(k+1)} + \dfrac{\theta^{(k)}}{\eta_1}}{\left| \nabla u^{(k+1)} - w^{(k+1)} + \dfrac{\theta^{(k)}}{\eta_1} \right|} \cdot \max\left(\left| \nabla u^{(k+1)} - w^{(k+1)} + \frac{\theta^{(k)}}{\eta_1} \right| - \frac{\alpha_1}{\eta_1}, 0 \right). \tag{16}$$

The *g* subproblem is given by:

$$g^{(k+1)} = \arg\min_{g}\left(\alpha_2 \|g\|_1 - \left\langle \xi^{(k)},\, g - \varepsilon\left(w^{(k+1)} \right) \right\rangle + \frac{\eta_2}{2}\left\| g - \varepsilon\left(w^{(k+1)} \right) \right\|_2^2 \right) =$$

$$= \arg\min_{g}\left(\alpha_2 \|g\|_1 + \frac{\eta_2}{2}\left\| g - \varepsilon\left(w^{(k+1)} \right) - \frac{\xi^{(k)}}{\eta_2} \right\|_2^2 \right).$$

The solution of the *g* subproblem can be obtained by applying the soft thresholding operator too:

$$g^{(k+1)} = \frac{\varepsilon\left(w^{(k+1)} \right) + \dfrac{\xi^{(k)}}{\eta_2}}{\left| \varepsilon\left(w^{(k+1)} \right) + \dfrac{\xi^{(k)}}{\eta_2} \right|} \cdot \max\left(\left| \varepsilon\left(w^{(k+1)} \right) + \frac{\xi^{(k)}}{\eta_2} \right| - \frac{\alpha_2}{\eta_2}, 0 \right). \tag{17}$$

The *z* subproblem is given by:

$$z^{(k+1)} = \arg\min_{z}\left(\frac{\lambda}{2}\|z - f\|^2 + \beta\langle 1,\, z - f\log z\rangle - \left\langle \rho_3^{(k)},\, z - u^{(k+1)} \right\rangle + \frac{\eta_3}{2}\left\| z - u^{(k+1)} \right\|_2^2 \right) =$$

$$= \arg\min_{z}\left(\frac{\lambda}{2}\|z - f\|_2^2 + \beta\langle 1,\, z - f\log z\rangle + \frac{\eta_3}{2}\left\| z - u^{(k+1)} - \frac{\rho_3^{(k)}}{\eta_3} \right\|_2^2 \right).$$

Therefore, we get

$$\lambda(z - f) + \beta\left(1 - \frac{f}{z} \right) + \eta_3\left(z - u^{(k+1)} \right) - \rho_3^{(k)} = 0.$$

This equation can be rewritten as follows:

$$(\lambda + \eta_3) z^2 - z\left(\eta_3 u^{(k+1)} + \rho_3^{(k)} - \beta + \lambda f \right) - \beta f = 0.$$

The solution of $z^{(k+1)}$ is the positive solution given by:

$$z^{(k+1)} = \frac{\left(\eta_3 u^{(k+1)} + \rho_3^{(k)} - \beta + \lambda f\right) + \sqrt{\left(\eta_3 u^{(k+1)} + \rho_3^{(k)} - \beta + \lambda f\right)^2 + 4(\eta_3 + \lambda)\beta f}}{2(\eta_3 + \lambda)}. \quad (18)$$

The complete method is summarized in Algorithm 1. We need a stopping criterion for the iteration: we end the loop if the maximum number of allowed outer iterations N has been carried out (to guarantee an upper bound on running time) or the following condition is satisfied for some prescribed tolerance σ:

$$\frac{\left\|u^{(k)} - u^{(k-1)}\right\|_2}{\left\|u^{(k)}\right\|_2} < \varsigma, \quad (19)$$

where σ is a small positive parameter.

Algorithm 1: Alternating minimization method for solving the model (5).

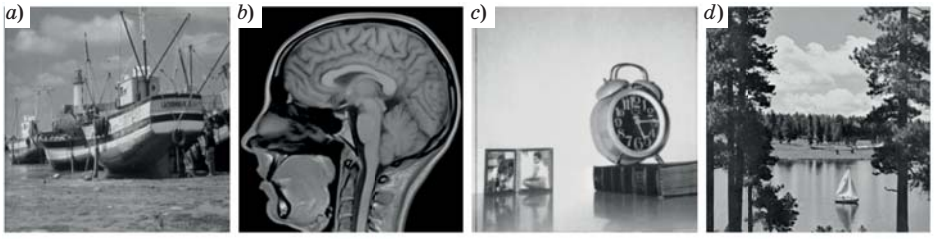
1. **Initialize:** $z^{(0)} = u^{(0)} = f$; $d^{(0)} = g^{(0)} = 0$; $w^{(0)} = 0$; $k = 0$.
2. **While** Stopping condition is not satisfied **do:**
3. Compute $u^{(k+1)}$ according to (11).
4. Compute $w^{(k+1)}$ according to (15).
4. Compute $d^{(k+1)}$ according to (16).
5. Compute $g^{(k+1)}$ according to (17).
6. Compute $z^{(k+1)}$ according to (18).
7. Update $\theta_1^{(k+1)}$, $\mu_2^{(k+1)}$, $\xi_3^{(k+1)}$ by (8).
10. $k = k + 1$.
11. **Endwhile.**
12. **Return** u.

Numerical experiments

In this section, we present some numerical results to illustrate the performance of the proposed model for MPGN removal. In order to prove the superiority of the proposed model, we compare our results with closely related approaches [8, 23]: the TVPG model (1) and TGV model (2). For compared models, the optimization problem are implemented by the state-of-the-art alternating minimization algorithm. The original test images are shown in Fig. 1, *a*–*d*.

All experiments were carried out in Windows 10 and Matlab running on a desktop equipped with an Intel Corei3, 2.1 GHz and 12 GB of RAM. To assess quality of the restoration results, we use peak signal-to-noise ratio (PSNR) defined as follows:

$$PSNR = 10\log_{10}\left(\frac{255^2 \cdot MN}{\left\|u^* - u\right\|_2^2}\right),$$



■ ***Fig. 1.*** Test images: *a* — Boat; *b* — Head; *c* — Clok; *d* — Lake

where u, u^* are the original image, the reconstructed or noisy image accordingly; M and N are the number of image pixels in rows and columns.

We also use other popular measure called SSIM (structural similarity index measure). The SSIM measure compares local patterns of pixel intensities normalized for luminance and contrast, and allows us to get more consistent with human visual characteristics [28]:

$$SSIM\left(u, u^*\right) = \frac{\left(2\mu_u\mu_{u^*} + c_1\right)\left(2\sigma_{u,u^*} + c_2\right)}{\left(\mu_u^2 + \mu_{u^*}^2 + c_1\right)\left(\sigma_u^2 + \sigma_{u^*}^2 + c_2\right)^*},$$

where μ_u, μ_{u^*} are the means of u, u^* respectively; σ_u, σ_{u^*} — their standard deviations; σ_{u,u^*} — the covariance of two images u and u^*; $c_1 = (K_1L)^2$; $c_2 = (K_2L)^2$, L is the dynamic range of the pixel values (255 for 8-bit grayscale images), and $K_1 \ll 1$, $K_2 \ll 1$ are small constants.

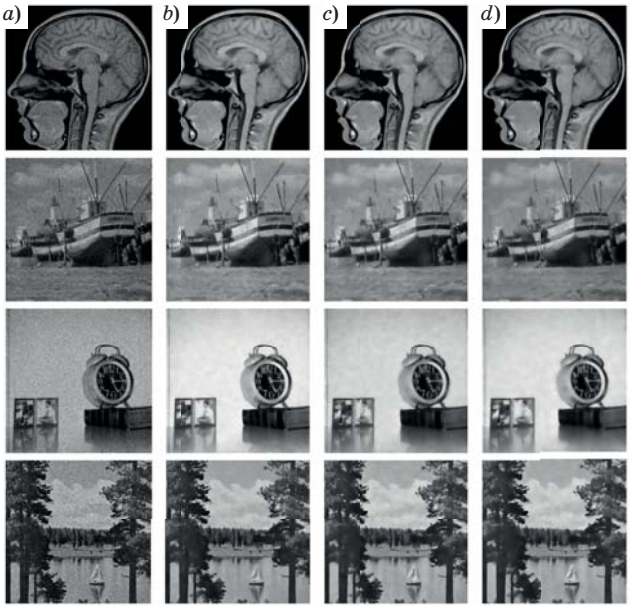
For our experiments, we set tolerance in (19): $\sigma = 0.0001$ and $N = 200$. The observed images in our experiments are simulated as follows. To test different noise levels, the noisy images are generated by Poisson noise with some fixed peak $I_{\max}$, and by Gaussian noise with standard deviation σ_g. Empirically, all of the compared methods perform image denoising with their optimal parameters. All images are processed with the equivalent parameters $\lambda = 0.4$, $\beta = 0.6$, which gave the best restoration results. For our models, we set $\eta_1 = 5$, $\eta_2 = 5$ and $\eta_3 = 1$.

In Figures 2, *a*–*d* and 3, *a*–*d* we exhibit the results of compared methods for noise levels $I_{\max} = 120$, $\sigma_g = 5$ and $I_{\max} = 60$, $\sigma_g = 5$.

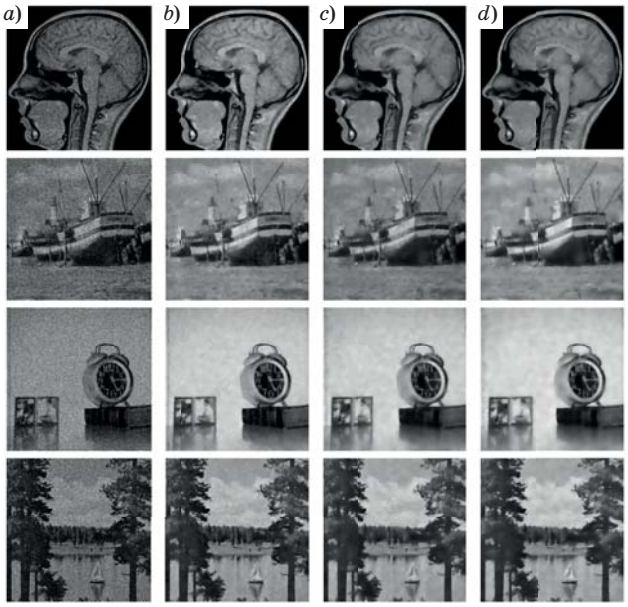
For a better visual comparison, we show some details of the restored images in Fig. 4 for noise levels $I_{\max} = 120$, $\sigma_g = 5$, and in Fig. 5 for $I_{\max} = 60$, $\sigma_g = 5$. In these Figures, we include details of the noisy and original images. It can be seen that our method gives even better visual improvement than the other two methods. For the comparison of the performance quantitatively, the measures of PSNR and SSIM values are reported in Tables 1 and 2. In each of the Tables, we include the PSNR and SSIM values for noisy images and recovered images, and the average results over test images for each method are shown. The better restored results are highlighted in bold.

In Figures 6, *a*–*d* and 7, *a*–*d*, we also show the results details of compared methods for noise levels $I_{\max} = 120$, $\sigma_g = 10$ and $I_{\max} = 60$, $\sigma_g = 10$, respectively. We report the PSNR and SSIM values for noisy images and recovered images in Tables 3 and 4. The average results over test images also appear in last row of each table. The better restored results are highlighted in bold.

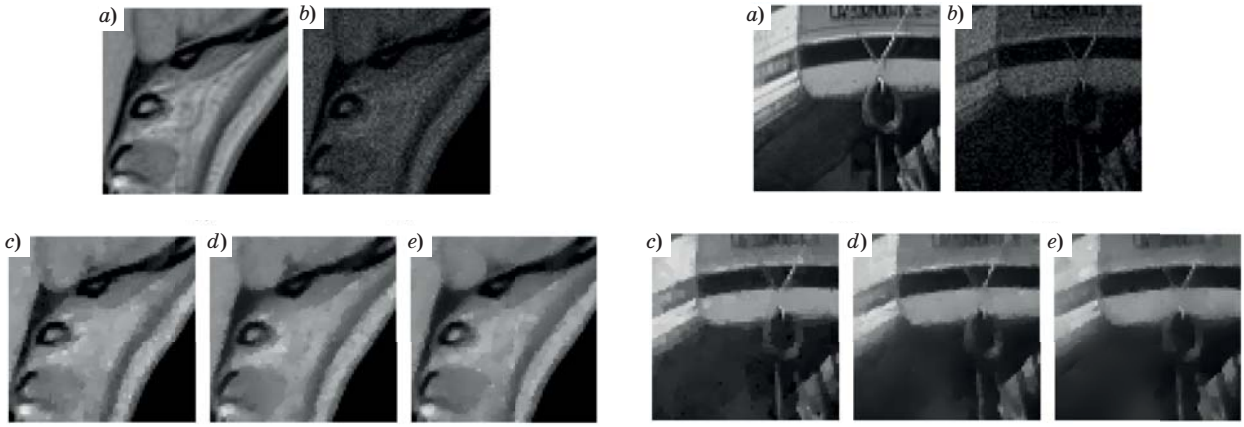
From Figures, we can see that the images recovered by our proposed model are better quality than those of the compared approaches. Beside, the measurable comparisons reported in Tables 1–4, the our proposed approach gets higher PSNR, SSIM values than those of the TVPG and TGV approaches. It indicates the competitive performance of the proposed method for denoising image corrupted by MPGN.



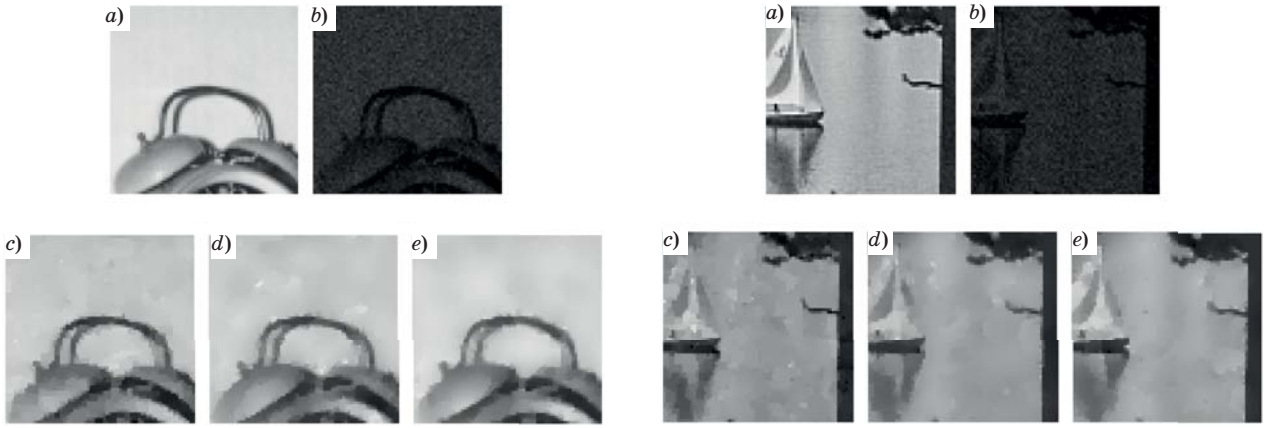
■ ***Fig. 2.*** Recovered results for the test images with noise level $I_{\max} = 120$, $\sigma_g = 0.5$: *a* — Noisy; *b* — TVPG; *c* — TGV; *d* — Ours



■ ***Fig. 3.*** Recovered results for the test images with noise level $I_{\max} = 60$, $\sigma_g = 0.5$: *a* — Noisy; *b* — TVPG; *c* — TGV; *d* — Ours



■ ***Fig. 4.*** The zoom-in part of the recovered images in first row and in second row of Fig. 2: *a* — details of original images; *b* — details of noisy images; *c* — details of restored images by TVPG; *d* — details of restored images by TGV; *e* — details of restored images by our approach



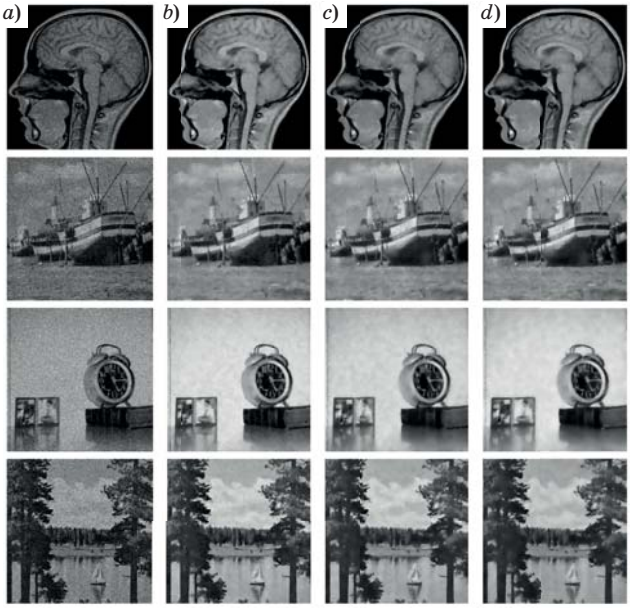
■ ***Fig. 5.*** The zoom-in part of the recovered images in third row and in second row of Fig. 3: *a* — details of original images; *b* — details of noisy images; *c* — details of restored images by TVPG; *d* — details of restored images by TGV; *e* — details of restored images by our approach

■ ***Table 1.*** PSNR and SSIM values for noisy images and restored images with noise level $I_{\max} = 120$, $\sigma_g = 5$

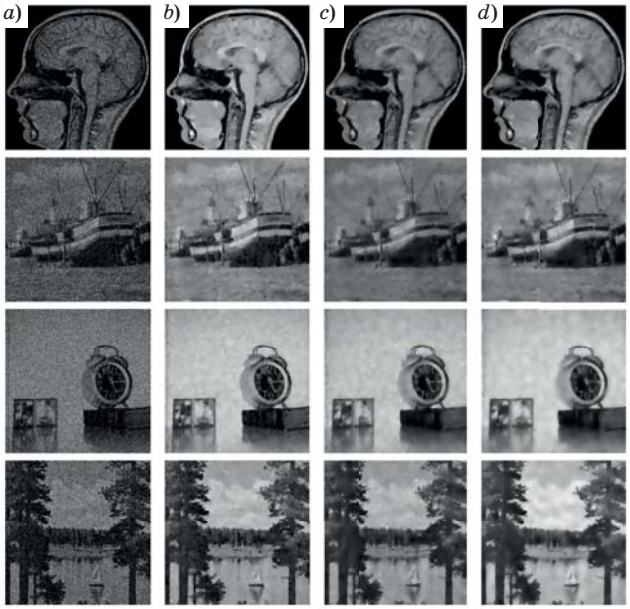
Image	PSNR				SSIM			
	Noisy	TGV	TVPG	Ours	Noisy	TGV	TVPG	Ours
Board	20.5670	26.9777	27.1435	**27.5823**	0.5482	0.7688	0.7749	**0.7812**
Clock	15.3632	24.2404	25.9160	**26.4658**	0.36742	0.8856	0.8884	**0.8956**
Lake	18.6823	24.7286	24.7002	**25.7141**	0.61996	0.7649	0.7779	**0.7864**
Head	20.7322	26.9048	27.9500	**28.8874**	0.60745	0.8624	0.8657	**0.8739**
Average	18.8362	25.7129	26.4274	**27.1624**	0.5358	0.8204	0.8267	**0.8343**

■ ***Table 2.*** PSNR and SSIM values for noisy images and restored images with noise level $I_{\max} = 60$, $\sigma_g = 5$

Image	PSNR				SSIM			
	Noisy	TGV	TVPG	Ours	Noisy	TGV	TVPG	Ours
Board	18.6799	24.0460	24.7064	**25.1713**	0.3871	0.6701	0.6818	**0.6931**
Clock	13.0537	24.3635	24.4234	**25.5345**	0.2600	0.8409	0.8423	**0.8587**
Lake	16.339	22.0954	22.4670	**22.8379**	0.4735	0.6762	0.6877	**0.6920**
Head	16.7107	25.2752	25.6161	**26.4411**	0.5736	0.7724	0.7923	**0.8087**
Average	16.1958	23.9450	24.3032	**24.9962**	0.4235	0.7399	0.7510	**0.7631**



■ ***Fig. 6.*** Recovered results for the test images with noise level $I_{\max} = 120$, $\sigma_g = 10$: *a* — Noisy; *b* — TVPG; *c* — TGV; *d* — Ours



■ ***Fig. 7.*** Recovered results for the test images with noise level $I_{\max} = 60$, $\sigma_g = 10$: *a* — Noisy; *b* — TVPG; *c* — TGV; *d* — Ours

■ ***Table 3.*** PSNR and SSIM values for noisy images and restored images with noise level $I_{\max} = 120$, $\sigma_g = 10$

Image	PSNR				SSIM			
	Noisy	TGV	TVPG	Ours	Noisy	TGV	TVPG	Ours
Board	19.7547	24.7675	25.9887	**26.1733**	0.4376	0.7255	0.7218	**0.7316**
Clock	14.5413	22.4326	24.6121	**25.9687**	0.2980	0.8571	0.8421	**0.8749**
Lake	17.805	23.3247	23.7328	**24.2787**	0.5191	0.7249	0.7270	**0.7396**
Head	16.031	26.3812	26.5097	**27.0119**	0.6075	0.8154	0.8292	**0.8358**
Average	17.0330	24.2265	25.2108	**25.8582**	0.4655	0.78073	0.7800	**0.7955**

■ ***Table 4.*** PSNR and SSIM values for noisy images and restored images with noise level $I_{\max} = 60$, $\sigma_g = 10$

Image	PSNR				SSIM			
	Noisy	TGV	TVPG	Ours	Noisy	TGV	TVPG	Ours
Board	17.5737	23.3837	23.5885	**23.8189**	0.2566	0.6060	0.6054	**0.6215**
Clock	12.2833	24.3595	24.2930	**24.4320**	0.1793	0.7965	0.7726	**0.8150**
Lake	14.6131	20.8641	20.8629	**21.5523**	0.3230	0.6018	0.6097	**0.6207**
Head	14.1531	23.4717	24.2758	**24.6904**	0.4588	0.7304	0.7386	**0.7496**
Average	14.6558	23.0198	23.2551	**23.6234**	0.3044	0.6837	0.6816	**0.7017**

Conclusions

In this paper, we have investigated a second-order TGV_{α}^{2} based model for denoising image corrupted by MPGN. Computationally, an alternating minimization algorithm is employed for solving the proposed optimization problem. Finally, compared with several existing state-of-the-art approaches, the experiments demonstrate competitive performance of the proposed method.

Financial support

This work was supported by The University of Danang, University of Science and Technology, code number of Project T2020-02-33.

Appendix

Definition 1 [20, 23–25]. *Let* $\Omega \subset \mathbb{R}^2$ *be a bound domain,* $k > 1$ *and* $\alpha = (\alpha_0, \alpha_1) > 0$.

Then the total generalized variation of order k with weight α *for* $u \in L^1(\Omega)$ *is defined as the value of the functional:*

$$TGV_\alpha^2(u) = \sup\left\{\int_\Omega u \operatorname{div}^2 \vartheta \mathrm{d}x \,\middle|\, \vartheta \in C_C^2\left(\Omega, \mathbb{S}^{d\times d}\right), \|\vartheta\|_\infty \le \alpha_0, \|\operatorname{div}\vartheta\|_\infty \le \alpha_1\right\},$$

where d denotes the dimension of images, $C_C^2\left(\Omega, \mathbb{S}^{d\times d}\right)$ *is the space of compactly supported symmetric* $d \times d$ *matrix fields,* $\mathbb{S}^{d\times d}$ *is the set of all symmetric* $d \times d$ *matrices,*

$$\left(\operatorname{div}\vartheta\right)_i = \sum_{j=1}^d \frac{\partial \vartheta_{ij}}{\partial x_j}, \quad \left(\operatorname{div}^2 \vartheta\right)_i = \sum_{i=1,j=1}^d \frac{\partial^2 \vartheta_{ij}}{\partial x_i \partial x_j}.$$

The infinite norms of θ *and* $\operatorname{div}\theta$ *are given by*

$$\|\vartheta\|_\infty = \sup_{x\in\Omega}\left(\sum_{i=1,j=1}^d \left|\vartheta_{ij}\right|^2\right)^{\frac{1}{2}};$$

$$\|\operatorname{div}\vartheta\|_\infty = \sup_{x\in\Omega}\left(\sum_{j=1}^d \left|\left(\operatorname{div}\vartheta\right)_j(x)\right|^2\right)^{\frac{1}{2}}.$$

Definition 2 [20, 23–25]. *The space of functions of bounded generalized variation (BGV) is defined as follows:*

$$BGV^2(\Omega) = \left\{u \in L^1(\Omega) \,\middle|\, TGV_\alpha^2(u) < \infty\right\},$$

$$\|u\|_{BGV^2} = \|u\|_1 + TGV_\alpha^2(u).$$

$BGV^2(\Omega)$ *is a Banach space independent of the weight vector* α, TGV_α^2 *is a seminorm and a convex function in* $BGV^2(\Omega)$. *Subsequently, we denote the spaces* $U = C_C^2(\Omega, \mathbb{R})$, $V = C_C^2\left(\Omega, \mathbb{R}^2\right)$ *and* $G = C_C^2\left(\Omega, \mathbb{S}^{2\times 2}\right)$.

Proof for Theorem 1.

Let $u^{(k)}$ be a bounded minimizing sequence. By the compactness property in the space of bound variation $BV(\Omega)$, there exists $u^* \in BV(\Omega)$, such that $u^{(k)}$ converges weakly to $u^* \in BV(\Omega)$ and $u^{(k)}$ converges strongly to u^* in $L^1(\Omega)$. According to [7, 23–26], we know that the functions $TGV_\alpha^2(u)$ and data fidelity term are all lower semi-continuous, proper and convex; and according to Fatou's lemma [29], we have

$$E(u) \ge E(u^*).$$

Thus, u^* is a minimizer of the optimization problem (4).

References

1. Pham Cong Thang, Andrei V. Kopylov. Tree-serial parametric dynamic programming with flexible prior model for image denoising. *Computer Optics*, 2018, vol. 42(5), pp. 838–845.
2. Le T., Chartrand R., Asaki T. J. A variational approach to reconstructing images corrupted by Poisson noise. *Journal of Mathematical Imaging and Vision*, 2007, vol. 27, pp. 257–263.
3. Li J., Shen Z., Yin R., Zhang X. A reweighted method for image restoration with Poisson and mixed Poisson–Gaussian noise. *Inverse Problems & Imaging*, 2015, vol. 9 (3), pp. 875–894.
4. Chouzenoux E., Jezierska A., Pesquet J. C., Talbot H. A convex approach for image restoration with exact Poisson-Gaussian likelihood. *SIAM Journal on Imaging Sciences*, 2015, vol. 8(4), pp. 2662–2682.
5. Benvenuto F., Camera A. L., Theys C., Ferrari A., Lanteri H., Bertero M. The study of an iterative method for the reconstruction of images corrupted by Poisson and Gaussian noise. *Inverse Problems*, 2008, vol. 24(3), pp. 35016.
6. Lanza A., Morigi S., Sgallari F., Wen Y. W. Image restoration with Poisson–Gaussian mixed noise. *Computer Methods in Biomechanics and Biomedical Engineering: Imaging and Visualization*, 2014, vol. 2(1), pp. 12–24.
7. Calatroni L., De Los Reyes J., and Schronlieb C. Infimal convolution of data discrepancies for mixed noise removal. *SIAM Journal on Imaging Sciences*, 2017, vol. 10(3), pp. 1196–1233.
8. Pham C. T., Gamard G., Kopylov A., Tran T. T. T. An algorithm for image restoration with mixed noise using total variation regularization. *Turkish Journal of Electrical Engineering and Computer Sciences*, 2018, vol. 26(6), pp. 2831–2845.
9. Chambolle A. An algorithm for total variation minimization and applications. *Journal of Mathematical Imaging and Vision*, 2004, vol. 20, pp. 89–97.
10. He C., Hu C., Zhang W., Shi B. A fast adaptive parameter estimation for total variation image restoration. *IEEE Transactions on Image Processing*, 2014, vol. 23(12), pp. 4954–4967.
11. Huang Y. M., Ng M. K., Wen Y. W. A fast total variation minimization method for image restoration.

Multiscale Modeling and Simulation, 2008, vol. 7(2), pp. 774–795.
12. Wang Y., Yang J., Yin W., Zhang Y. A New alternating minimization algorithm for total variation image reconstruction. *SIAM Journal on Imaging Sciences*, 2008, vol. 1 (3), pp. 248–272.
13. Goldstein T., Osher S. The split Bregman method for L1-regularized problems. *SIAM Journal on Imaging Sciences*, 2009, vol. 2(2), pp. 89–97.
14. Chen H., Wang C., Song Y., and Li Z. Split bregmanized anisotropic total variationmodel for image deblurring. *Journal of Visual Communication and Image Representation*, 2015, vol. 31, pp. 282–293.
15. Kayyar S. H., Jidesh P. Non-local total variation regularization approach for image restoration under a Poisson degradation. *Journal of Modern Optics*, 2018, vol. 65, pp. 2231–2242.
16. Lysaker M., Lundervold A., Tai X.-C. Noise removal using fourth order partial differential equation with applications to medical magnetic resonance images in space and time. *IEEE Transactions on Image Processing*, 2003, vol. 12 , pp. 1579–1590.
17. Zhang J., Chen R., Deng C., and Wang S. Fast linearized augmented Lagrangian method for Euler's elastica model. *Numerical Mathematics: Theory, Methods and Applications*, 2017, vol. 10, pp. 98–115.
18. Zhu W., Tai X. C., Chan T. *A fast algorithm for a mean curvature based image denoising model using augmented Lagrangian method*. In: *Efficient Algorithms for Global Optimization Methods in Computer Vision. Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg, 2014. Vol. 8293. Pp. 104–118.
19. Myllykoski M., Glowinski R., Karkkainen T., Rossi T. A new augmented Lagrangian approach for -mean curvature image denoising. *SIAM Journal on Imaging Sciences*, 2015, vol. 8(1), pp. 95–125.
20. Bredies K., Kunisch K., Pock T. Total generalized variation. *SIAM Journal on Imaging Sciences*, 2010, vol. 3(3), pp. 492–526.
21. Bredies L. K, Dong Y., Hintermller M. Spatially dependent regularization parameter selection in total generalized variation models for image restoration. *International Journal of Computer Mathematics*, 2013, vol. 90(1), pp. 109–123.
22. He C., Hu C., Yang X., He H., Zhang Qi. An adaptive total generalized variation model with augmented Lagrangian method for image denoising. *Mathematical Problems in Engineering*, 2014, vol. 2014, Article ID 157893, 11 p.
23. Knoll F., Bredies K., Pock T., Stollberger R. Second order total generalized variation (TGV) for MRI. *Magnetic Resonance in Medicine*, 2011, vol. 65(2), pp. 480–491.
24. Guo W., Qin J., Yin W. A new detail-preserving regularity scheme. *SIAM Journal on Imaging Sciences*, 2014, vol. 7(2), pp. 1309–1334.
25. Liu X. Augmented Lagrangian method for total generalized variation based Poissonian image restoration. *Computers & Mathematics with Applications*, 2016, vol. 71(8), pp. 1694–1705.
26. Pham C. T., Tran T. T. T., Gamard G. An efficient total variation minimization method for image restoration. *Informatica*, 2020, vol. 31(3), pp. 539–560.
27. Micchelli C. A., Shen L., Xu Y. Proximity algorithms for image models: denoising. *Inverse Problem*, 2011, vol. 27(4), 045009.
28. Wang Z., Bovik A. C., Sheikh H. R., Simoncelli E. P. Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*, 2004, vol. 13, pp. 600–612.
29. Feinberg E. A., Kasyanov P. O., Zadoianchuk N. V. Fatou's lemma for weakly converging probabilities. *Theory of Probability & its Applications*, 2014, vol. 58(4), pp. 683–689.

УДК 004.93
doi:10.31799/1684-8853-2021-2-20-32

Модель на основе полной обобщенной вариации второго порядка для восстановления изображений со смешанным пуассоновско-гауссовским шумом

Фам Конг Тханг[а], PhD, преподаватель, orcid.org/0000-0002-6428-102X, pcthang@dut.udn.vn
Чан Тхи Тху Тхао[б], магистр, преподаватель, orcid.org/0000-0001-7705-2405
Нгуен Тхань Конг[а], магистр, специалист, orcid.org/0000-0002-8060-0238
Во Дык Хоанг[а], PhD, преподаватель, orcid.org/0000-0002-6974-9023
[а]Университет науки и техники, Нгуэн Лунг Банг, 54, Дананг, 550000, Вьетнам
[б]Университет экономики, Нгу Ханх Сон, 71, Дананг, 550000, Вьетнам

Введение: восстановление изображений играет важную роль в обработке цифровых изображений. Распространенной проблемой восстановления изображений является шумоподавление. В области шумоподавления изображений существует множество моделей шума, одной из них можно назвать модель смешанного пуассоновско-гауссовского шума, которая с недавнего времени вызывает большой интерес. **Цель:** разработка модели шумоподавления изображений, искаженных смешанным пуассоновско-гауссовским шумом, и алгоритма для решения результирующей задачи минимизации. **Результаты:** предложена новая модель полной вариации для восстановления изображения со смешанным пуассоновско-гауссовским шумом на основе полной обобщенной

вариации второго порядка. Для решения рассматриваемой задачи оптимизации применяется эффективный алгоритм чередующейся минимизации. В качестве иллюстрации, в сравнение с родственными методами, представлены экспериментальные результаты, свидетельствующие о высокой эффективности предлагаемого подхода. **Практическая значимость:** разработанная модель позволяет удалить смешанный пуассоновско-гауссовский шум на цифровых изображениях с сохранением границ. Приведенные численные результаты демонстрируют конкурентоспособные характеристики предложенной модели для шумоподавления изображений, искаженных смешанным пуассоновско-гауссовским шумом.

Ключевые слова — шумоподавление изображения, полная вариация, минимизация, смешанный пуассоновско-гауссовский шум.

Для цитирования: Pham C. T., Tran T. T. T., Nguyen T. C., Vo D. H. Second-order total generalized variation based model for restoring images with mixed Poisson — Gaussian noise. *Информационно-управляющие системы*, 2021, № 2, с. 20–32. doi:10.31799/1684-8853-2021-2-20-32

For citation: Pham C. T., Tran T. T. T., Nguyen T. C., Vo D. H. Second-order total generalized variation based model for restoring images with mixed Poisson — Gaussian noise. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 20–32. doi:10.31799/1684-8853-2021-2-20-32

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.

UDC 004.431.4
doi:10.31799/1684-8853-2021-2-33-42

Articles

A method for decompilation of AMD GCN kernels to OpenCL

K. I. Mihajlenko[a,b], *Master Student, Junior Programmer, orcid.org/0000-0002-6168-2653, Kristina.Mihajlenko@gmail.com*
M. A. Lukin[a,b], *PhD, Tech., CTO, orcid.org/0000-0002-1088-3324, lukinma@gmail.com*
A. S. Stankevich[a], *PhD, Tech., Associate Professor, orcid.org/0000-0002-3532-8941, stankev@itmo.ru*
[a]*ITMO University, 49, Kronverkskii Pr., 197101, Saint-Petersburg, Russian Federation*
[b]*Sudo Ltd., 20, Nahimov St., 199226, Saint-Petersburg, Russian Federation*

Introduction: *Decompilers are useful tools for software analysis and support in the absence of source code. They are available for many hardware architectures and programming languages. However, none of the existing decompilers support modern AMD GPU architectures such as AMD GCN and RDNA.* ***Purpose:*** *We aim at developing the first assembly decompiler tool for a modern AMD GPU architecture that generates code in the OpenCL language, which is widely used for programming GPGPUs.* ***Results:*** *We developed the algorithms for the following operations: preprocessing assembly code, searching data accesses, extracting system values, decompiling arithmetic operations and recovering data types. We also developed templates for decompilation of branching operations.* ***Practical relevance:*** *We implemented the presented algorithms in Python as a tool called OpenCLDecompiler, which supports a large subset of AMD GCN instructions. This tool automatically converts disassembled GPGPU code into the equivalent OpenCL code, which reduces the effort required to analyze assembly code.*

Keywords *— decompiler, disassembler, OpenCL, AMD GCN, GPGPU, control flow graph, reverse engineering.*

For citation: Mihajlenko K. I., Lukin M. A., Stankevich A. S. A method for decompilation of AMD GCN kernels to OpenCL. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 33–42. doi:10.31799/1684-8853-2021-2-33-42

Introduction

OpenCL [1] is a widespread standard for high performance computing. It is supported by all of the modern graphics processing unit (GPU) and central processing unit (CPU) vendors in contrast to vendor locked Compute Unified Device Architecture (CUDA) [2]. In particular, both Nvidia and AMD GPU support OpenCL. There are great general-purpose computing on graphics processing units (GPGPU) development tools in the Nvidia ecosystem, but AMD development tools have fallen behind the Nvidia ecosystem. Sometimes developers need to analyze assembly code for implementing better optimizations or reverse engineering. Nevertheless, there is no public decompilation tool for AMD GPU assembly. Decompiler also allows supporting programs without source code and checking for undocumented functions and backdoors. [3, 4]

OpenCL is designed to unleash the power of massively parallel processors. The OpenCL platform consist of a *host* (typically a CPU) and a set of *compute devices* (or, simply, *devices*). In this paper, devices are AMD GPUs. To avoid confusion, we denote by *program* the code executed on the host and by *kernel*, the code executed on the device. Each compute device consists of a set of *compute units*. Each compute unit consists of a set of *processing elements*.

Massive parallelism means a large number of launched processes. The process index space could be one-, two-, or three-dimensional. The set of launched process indices is called *NDRange* [5]. NDRange is divided by equal-sized *work-groups* (Fig. 1). NDRange size must be divisible by work-group size on each dimension. Otherwise NDRange size is automatically increased on each dimension to fulfill this requirement. The single process is called *work-item*. Each work-item has a unique identifier (ID) in NDRange index space (*global id*) and a unique ID in its work-group (*local id*). Each work-group also has a unique ID (*work-group ID*).

OpenCL defines four types of memory:

— global memory — a memory accessible to read and write to host and all work-items in the NDRange space;

— constant memory — a region of host-allocated global memory that is not changed during kernel execution;

— local memory — a memory accessible to work-items in a single work-group;

— private memory — a memory accessible to a single work-item.

The AMD GCN architecture

The AMD GCN architecture [6] is related to OpenCL platform model. A GPU device consists of several compute units. Each compute unit has four *single instruction, multiple data* (*SIMD*) *Vector Units* for computing and one *SIMD Scalar Unit* for flow control. Each SIMD Unit has 16 *processing elements*. One processing element contains one arithmetic logic unit (ALU) and can execute a single OpenCL work-item. Thus, one

■ ***Fig. 1***. OpenCL execution model on the example of two-dimensional NDRange

compute unit contains 64 ALU. Compute units work independently.

GCN devices have two-level data cache hierarchy. Each compute unit has L1 data cache and an entire GPU device has L2 data cache. Also they have 32 KiB instruction cache. If kernel does not fit in instruction cache, it has significant performance decrease. This fact encourages GPGPU developers to decompose a compute task between small kernels.

AMD GCN devices have an equivalent to each type of OpenCL memory. Global and constant memories from OpenCL are represented by *video random access memory* (VRAM). The equivalent of OpenCL local memory is *Local Data Share* (LDS). Data access in LDS is orders of magnitude faster than that of a VRAM. Private memory is stored in registers. Data access in registers is orders of magnitude faster than LDS. If there are not enough registers, a region in VRAM is allocated for private memory. These additional "registers" are named *scratch registers*. Usually scratch registers are in data cache and decrease performance by not really much. Registers are 32-bit but they can be combined into pairs for 64-bit instructions. Registers are the most expensive and valuable memory resource. Each work item can have at most 256 vector registers (VGPR) and 104 scalar registers (SGPR). Moreover, a compute unit has only 2048 registers for 64 ALU.

The lowest group of work-items that flow control can affect is named *wavefront*. This means that all the work-items in a single wavefront have the same program counter. All the work-items in a wavefront execute all branching paths (with the exception of a case when all the work-items choose the same conditional jump). Irrelevant branch paths are executed without any effect. Each SIMD Vector Unit can run from one to ten wavefronts depending on the used VGPRs, SGPRs and LDS.

AMD GCN has two different application binary interfaces (ABI) [7]. The first one comes with Windows Adrenaline or Linux AMDGPU-Pro driver. The second one comes with Linux-only ROCm driver. In this paper the first one is considered. ABI defines data and kernel parameters' location in memory. Some parameters are stored in registers, others are in VRAM. More detailed location of parameters will be considered in the next sections.

Statement of the problem

The purpose of this work is to create a decompiler for GCN assembly. It takes a disassembled file as input and translates it into its equivalent in OpenCL. Since there are no OpenCL decompilers for AMD GPUs, the following state-of-the-art theoretical [8–18] and instrumental [19, 20] solutions for C and C++ were considered as a basis:

— Ida Pro (Hex-Rays plugin): Intel x86 / x64, ARM;

— GHIDRA: Intel x86, ARM, AVR, MIPS, PIC, PowerPC;

— RetDec: Intel x86 / x64, ARM, MIPS, PIC32, PowerPC;

— Hopper: Intel x86 / x64, ARM, PowerPC;

— Snowman: Intel x86, AMD64, ARM.

As a result of research to achieve this goal, the following tasks were formulated:

1) extraction of the body of the program and data of the CPU module;

2) search for memory accesses;

3) search for control structures;

4) data type recovery.

The result of solving these tasks is a translation assembly code to an OpenCL code. Out method consists of the following steps:

1. Separation of program body, configuration part and kernel name.

2. Initialization of registers and kernel parameters using application binary interface.

3. Assembly instructions processing: control flow graph construction and determination of stored in registers data types.

4. Transformation control flow graph into region graph and its further processing (determination of flow-control instructions).

5. OpenCL code generation using processed region graph.

The body extraction

Extracting the body of the program is a small, but quite important task, serving as a preparatory stage for further decompilation. In addition, here we parse config section with work group size, number of index range dimensions, and other kernel properties. An example of the structure of the program body is shown in Listing 1.

Listing 1. An example of the structure of the program body

```
.kernel [kernel name]
    .config
        dims xyz
        .cws 8, 8, 2
                [other kernel configuration]
    .text
                [program body]
                s_endpgm <- end of program
```

This config means 3D index range with work-group size $8 \times 8 \times 2$ (128 threads in total).

The algorithm of body extraction is presented in listing 2.

Listing 2. The algorithm of body extraction

```
parse_status = “start”
instruction_set = []
config_set = []
program_name = “”
for current_row in bode_of_file:
  if current_row contains “.kernel”
     if parse_status == “instruction”:
       parse_status = “kernel”
       process_data(program_name, config_set,
instruction_set)
       instruction_set = []
       config_set = []
      program_name = current_row.split()[1] // take the
second word.
  if current_row == “.config”:
       parse_status = “config
  elif current_row == “.text”:
       parse_status = “instruction”
  elif current_row == “instruction”:
       instruction_set += current_row
  elif current_row == “config”:
       config_set += current_row
  else:
       continue
process_data(program_name, config_set, instruction_set)
```

The program body consists of a sequence of assembly instructions. Most of GCN assembly instruction names consist of three parts delimited by symbol “_”. In this paper they are called prefix, root and suffix.

Prefix means one of the following instruction types:

— Scalar instructions. Operands are mostly SGPRs. These instructions are used to control flow instructions, VRAM access, thread synchronization, atomic operations and others. The prefix is “s”.

— Vector instructions. Operands are mostly VGPRs. These instructions are used for computing. The prefix is “v”.

— Data share operations. Instructions for manipulating with LDS. The prefix is “ds”.

— FLAT instructions. Operands are mostly pairs of VGPRs that hold 64-bit address. These instructions are used to access to VRAM, LDS and scratch buffer. The prefix is “flat”.

Suffix (if present) means data type and size. Supported data types are indicated by the following suffixes:

i — signed integer;

u — unsigned integer;

f — floating-point;

b — binary (for bitwise operations).

The data type size can be 8, 16, 24, 32 and 64. Some instructions contain double suffix. For example, V_MUL_HI instruction family (V_MUL_HI_I32_I24, V_MUL_HI_U32_U24).

The rest of command name defines the operation. Some operations do not have direct equivalents in OpenCL. Such operations are decompiled to several OpenCL instructions. Otherwise, some assembly instructions are grouped and decompiled into a single OpenCL instruction.

AMD GCN devices do not have a call stack. Consequently, all the function calls are inlined into a kernel. Therefore, assembly code does not have any information about functions. We can only guess that there was a function if we discovered identical code fragments (ignore register renaming). But such an analysis is not considered in this paper.

Search for memory accesses

Assembly instructions processing starts from searching for memory accesses. The basic data structure used in the following algorithms is called *Register*. It holds the information about a single register and contains the following fields: *version*, *type*, *integrity*. *Integrity* can hold one of these values: {*entire*, *high_part*, *low_part*}. *Entire* means the register holds the whole 32 (or less) bit variable. Other values mean the register holds a part of 64 bit variable.

AMD ABI documentation contains description for OpenCL work-item built-in functions.

At this stage, the following functions are supported:

```
get_global_id(uint dimindx);
get_global_offset(uint dimindx);
get_local_id(uint dimindx);
get_global_size(uint dimindx);
get_local_size(uint dimindx);
get_group_id(uint dimindx);
get_num_groups(uint dimindx);
get_work_dim().
```

The result of these functions is stored to specific addresses. Therefore, if such an address is loaded into a register, then further access to that register means a call to this function.

The get_global_id(dim) function returns a global thread identifier that is unique in the entire task space. dim can take possible values of 0, 1 or 2. Since the thread numbering can be shifted in kernels, in order to get a thread index starting from zero, there is the following idiom:

```
uint idx0 = get_global_id(0) –
get_global_offset(0);
```

This thread index is often used to refer to an array. We parse this index and get_global_id in the following steps:

In *the first step*, we detect get_global_offset(uint dimindx). The value of this function is stored in global memory by address s[4:5]. So instruction s_load_dwordx2 s[2:3] s[4:5] 0x0 means get_global_offset(0) stored in register pair s2, s3.

The second step is determining the local ID: get_local_id(0). Local ID is stored in register v0 before the program starts executing, and in case of 2D or 3D index range get_local_id(1) and get_local_id(2) are stored in v1 and v2, respectively. Therefore the field *type* of these registers data is filled before the instruction processing (it corresponds to get_local_id(uint dimindx)).

The third step is identifying the work-group ID: get_group_id(uint dimindx) . The result of calling this function is also compile-time constant and stored before the program execution. If "useargs" is used by the kernel in the configuration, get_group_id(0) is stored in register s6, and (in case of 2D and 3D index range) get_group_id(1) and get_group_id(2), are stored in s7 and s8, respectively. This instruction is processed like the previous one. The registers fields *type* are filled with corresponding values before the instruction processing.

The fourth step is discovering the work-group size. In OpenCL this value can be retrieved using get_local_size function. It is impossible to determine the call to this function from the assembly code. This is because the value of this function call is replaced by numeric constant. Therefore, we have no semantic information about this number in the assembly code. However, we have obtained work-group size in the previous section.

The last step is multiplying the work-group ID by the work-group size, and then the local thread ID.

Function get_global_id(uint dimindx)is deconstructed in similar way but with the addition of the offset value.

The result of a function that returns the size of the workspace in a given dimension, get_global_size(uint dimindx), is stored in global memory by address s[4:5]+ 0xc, 0x10 or 0x14 depending on the dimension. Processing of this instruction is same with get_global_offset: data type inference is done using instruction s_load_dword with offsets (0xc, 0x10, 0x14).

Next, consider a function that returns the number of work-groups that will run the kernel for a given dimension, get_num_groups(uint dimindx). The value is obtained by dividing the size of the workspace by the size of the work-group for a given dimension.

The last function to consider is get_work_dim(). It returns the number of dimensions used. The value is obtained when dword is loaded from the registers storing a pointer to kernel settings — s[4:5], with an offset of 0x20010. Processing of this instruction is the same with get_global_offset и get_global_size.

The result of matching with the presented templates is a restoration of work-item built-in functions.

Also, calls to array elements and simple arithmetic operations were supported.

Search for control structures

The decompiler was implemented using an algorithm based on structural analysis [21]. At first step, we construct the control flow graph [22]. After that, we transform it to region graph. Initially, each instruction represents one region.

The analysis process in based on depth-first search. Each node is checked whether it is a header of one of known templates. If the template is determined, all the nodes corresponding to this template are merged into a single node. This process is iterated until the single node remains.

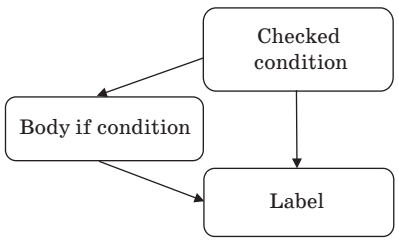
Our decompiler supports the if construction. The template presented for it in Fig. 2, corresponds to the one described in theoretical solutions, and does not require any additional transformations for detection and decompilation.

The region graph processing algorithm is illustrated by the example shown in Fig. 3. The algorithm consists of the following steps:

1. Regions ##1–3 are not beginning of any known templates. Region #4 in conjunction with regions #5 and #6 constitute an *if template*. However, region #6 is connected with another regions. So, we merge only regions #4 and #5 into a new region #7.

2. Regions #1 and #2 are not beginning of any known templates. Regions #3 and #7 constitute a *linear region*. Merge them into a new region #8.

3. Region #1 is not beginning of any known templates. Regions #2, #8 and #6 constitute an *if template*. Region #6 is connected with another region (region #1), so merge only regions #2 and #8 into a new region #9.



■ ***Fig. 2.*** Template for if statement

4. Regions #1, #9 and #6 constitute an *if template*. Merge them into a new region #10.

5. There is a single region now. So, we extracted all flow-control information from the region graph and can now generate OpenCL code.

The main difference with CPU *if-else template* is the presence of a 64-bit mask, which is responsible for the execution of threads. This is because 64 threads have the same instruction pointer. AMD compiler generates *if-else* construction in several forms. We demote the most frequent form as the *first form*. The *first form* is shown in Fig. 4, *a*. For more convenient processing, this template was reduced to the form shown in Fig. 4, b (*standard form*).

In this paper we also consider another two frequent forms. We denote them as the *second form* and the *third form*. The *second form* is shown in Fig. 5, *a*. The *third form* is shown in Fig. 5, *b*. The reduction the second form of *if-else template* to the *standard form* (see Fig. 4, *b*) consists of two steps:

1. Transformation to the *first form* of *if-else template*.

2. Reduction to *standard form*.

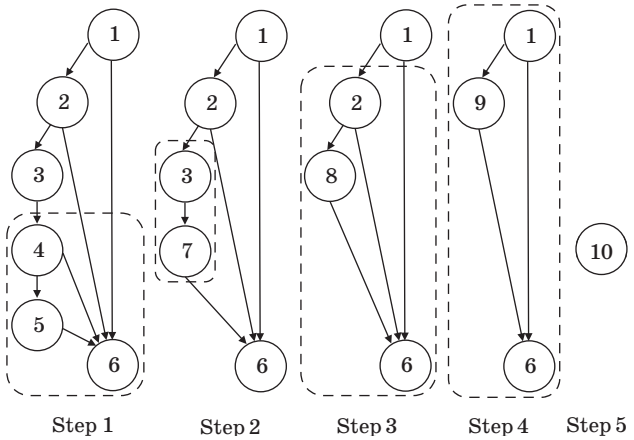
The second form of if-else template looks like the if template. But the main difference is the second change exec mask and else condition body before restoration of exec mask. The main difference between the first form and the second form is a quantity of "goto" labels.

The transformation of the *second form* to the *first form* is made by fake insertion of the second label after the else condition body and condition jump to the second label before it. The transformation of the *third form* is made similarly.

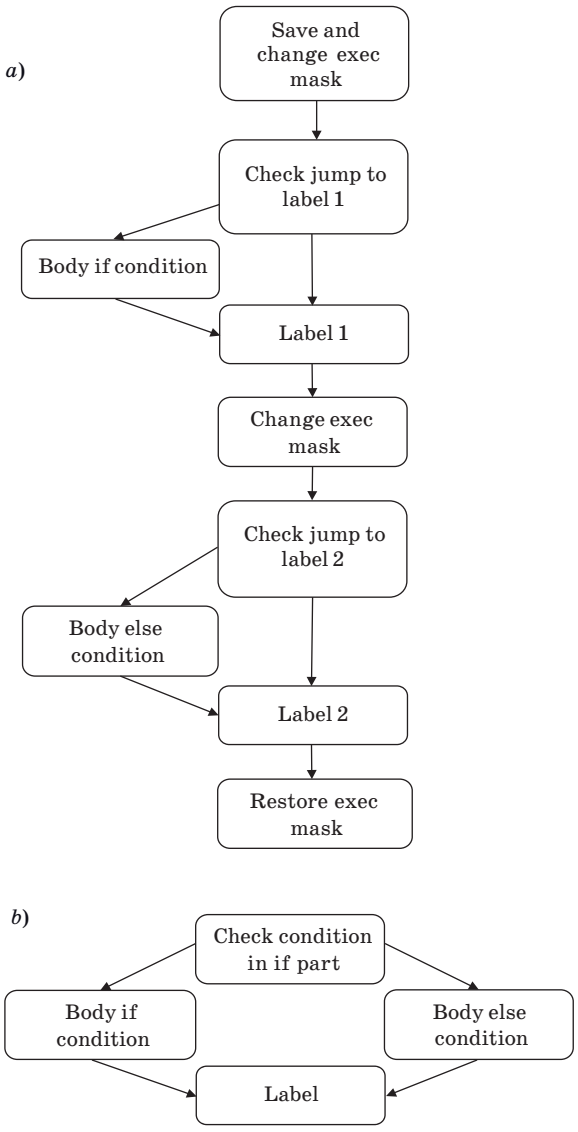
The processing of nested structures is the following. Firstly, the most nested structures are detected using control instruction templates. Detected structures are combined in the region graph. After that, the most nested of the remaining structures can be detected. The processing is continued until the root structure is combined in the region graph.

When processing branches, it was taken into account that at a vertex that has several ancestors, the values of registers can be determined ambiguously. And if in the future some of these registers were used, then variables were created for them. In the implementation, this was done by assigning versions to registers and working with them [23, 24].

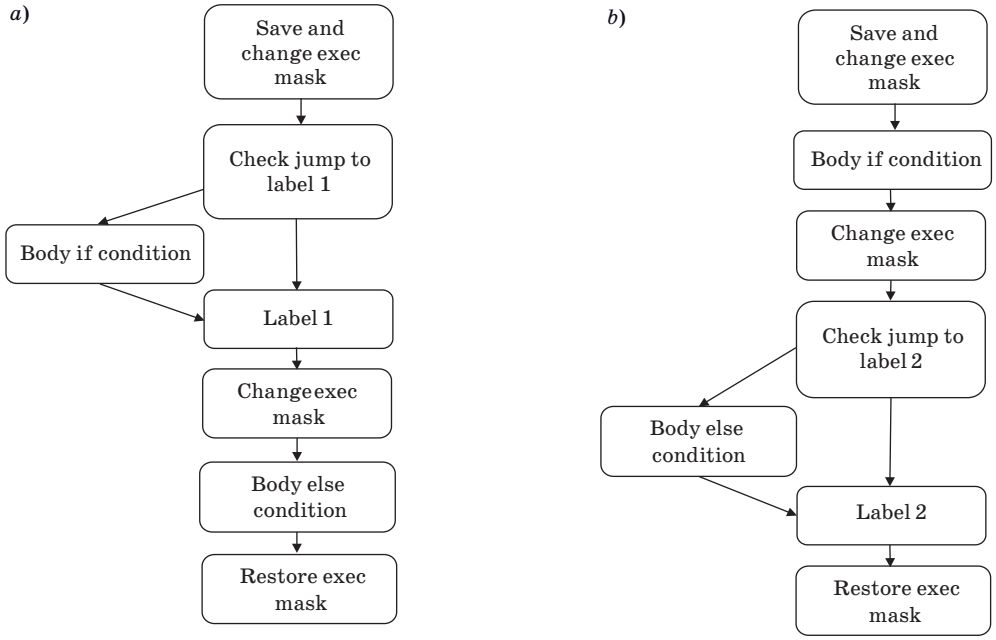
The last considered in this paper control structure is the ternary operator. It is represented in the assembly code of one instruction and does not require overlapping templates.



■ ***Fig. 3.*** Example of region graph handling



■ ***Fig. 4.*** Templates for if-else conditions part 1: *a* — with two labels; *b* — standard form



■ ***Fig. 5***. Templates for if-else conditions part 2: *a* — with label in the if part; *b* — with label in the else part

Data type recovery

Two ways of data type recovery were implemented: from the .config section of kernel and using assembly instructions. The .config section contains data types for kernel arguments. For example, the .config section of kernel with signature void copy(__global int *data, int x) is shown in Listing 2. As can be seen from Listing 2, data type for kernel arguments can be restored unambiguously.

Listing 3. Kernel arguments

```
.kernel copy
  .config
    .dims x
    .cws 64, 1, 1
    .sgprsnum 13
    .vgprsnum 3
    .floatmode 0xc0
    .pgmrsrc1 0x00ac0040
    .pgmrsrc2 0x0000008c
    .dx10clamp
    .ieeemode
    .useargs
    .priority 0
    .arg_.global_offset_0, “size_t”, long
    .arg_.global_offset_1, “size_t”, long
    .arg_.global_offset_2, “size_t”, long
    .arg _.printf_buffer, “size_t”, void*, global, , rdonly
  .arg_.vqueue_pointer,”size_t”, long
  .arg_.aqlwrap_pointer,”size_t”, long
    .arg data, “int*”, int*, global,
    .arg x, “int”, int
```

Data type determination using assembly instructions is based on instruction suffixes. For example, instruction

```
s_add_u32 s0, s4, s0
```

means sum of two unsigned 32-bit integers.

Practical implementation

As a practical implementation of this research, the OpenCL Decompiler tool was developed. At this moment, it supports only a reduced set of AMD GCN ISA.

The OpenCL Decompiler was implemented in Python 3. It requires an assembly file compatible with CLRX Disassembler [25] output or CodeXL assembly listing as input data.

The output of the OpenCL Decompiler is a valid OpenCL file. All decompiled kernels can be compiled and executed on AMD GPUs. The exception is case when the decompiler gets an unsupported instruction. In this case decompiler lefts unsupported assembly code as is in inline assembly (inline assembly is not supported by AMDGPU-Pro driver and cannot be compiled).

The source code is available at https://github.com/sudo-team-company/OpenCLDecompiler.

The repository has about 931 synthetic tests and real free open-source kernels. Decompiler passes all the tests in the repository, which confirms correctness described functionality.

The examples of the real kernels are mask_kernel and weighted_sum_kernel (https://github.com/ganyc717/Darknet-On-OpenCL/blob/master/darknet_cl/cl_kernels/blas_kernels_1.cl). The result of their decompilation is in folder real_tests (https://github.com/sudo-team-company/OpenCLDecompiler/tree/master/tests/real_kernels).

These tests confirm the compliance of the theoretical considerations and practical results.

Conclusion

In this paper, a decompiling method for AMD GPU assembly was described. It has an implementation called *OpenCLDecompiler* and was introduced into Sudo Ltd. The *OpenCLDecompiler* tool was demonstrated on real open-source projects. All of this reveals the practical applicability of described method.

The described method is based on standard techniques for CPU decompilers but some techniques required significant modification for massive parallel architecture.

Decompiler works with any valid assembly code. However, restoration of some complicated loop constructions and some instructions is not implemented. In this case all supported assembly instructions are decompiled into a pseudo-code in accordance with their documentation. Unsupported instructions are remained unchanged. This approach does not provide full-fledged OpenCL code but significantly facilitate further manual code analysis.

It is further planned to extend the set of supported instructions and support the new RDNA architecture [26] and processing of more complicated flow control instructions.

Financial support

This work was supported by Sudo Ltd, project No cr-776, and National Center for Cognitive Research of ITMO University.

References

1. *OpenCL Overview — The Khronos Group Inc.* Available at: https://www.khronos.org/opencl (accessed 25 January 2020).
2. Jedel' G. E. *Parallel'nye vychislenija na graficheskih processorah Nvidia CUDA*. In: *Sbornik izbrannyh statej nauchnoj sessii TUSUR* [Parallel computing on GPU Nvidia Cuda. In: Collection of selected articles of the TUSUR scientific session]. Tomsk, Tomskij gosudarstvennyj universitet sistem upravlenija i radiojelektroniki, 2020, no. 1-1, pp. 41–43 (In Russian).
3. Kondakov E. V. Parallel computing on GPUs. *Materialy XL nauchno-prakticheskoj konferencii "Nauka XXI veka: problemy, poiski, reshenija"* [Materials of the XL Scientific-Practical Conference "Science of the 21st Century: Problems, Search, Solutions"]. Miass, 2016, pp. 34–39 (In Russian).
4. Pryadko S. A., Troshin A. Y., Kozlov V. D., Ivanov A. E. Parallel programming technologies on computer complexes. *Radio industry*, 2020, vol. 30, no. 3, pp. 28–33 (In Russian). doi:10.21778/2413-9599-2019-30-3-28-33
5. *The OpenCL Specification. Version: 1.2.* Available at: https://www.khronos.org/registry/OpenCL/specs/opencl-1.2.pdf (accessed 26 January 2020).
6. Yifan Sun, Trinayan Baruah, Saiful A. Mojumder, Shi Dong, Xiang Gong, Shane Treadway, Yuhui Bao, Spencer Hance, Carter McCardwell, Vincent Zhao, Harrison Barclay, Amir Kavyan Ziabari, Zhongliang Chen, Rafael Ubal, José L. Abellán, John Kim, Ajay Joshi, and David Kaeli. MGPUSim: Enabling Multi-GPU performance modeling and optimization. *The 46th Annual International Symposium on Computer Architecture (ISCA '19)*, June 22–26, 2019, Phoenix, AZ, USA. ACM, New York, NY, USA, 2019, 13 p. https://doi.org/10.1145/3307650.3322230
7. *ROCm — AMDGPU Compute Application Binary Interface.* Available at: https://github.com/ROCm-Developer-Tools/ROCm-ComputeABI-Doc/blob/master/AMDGPU-ABI.md (accessed 12 April 2020).
8. Mikhailov A. A., Khmelnov A. E. Control flow graph visualization. *BSU Bulletin. Mathematics, Informatics*, 2018, no. 2, pp. 50–62 (In Russian). doi:10.18101/2304-5728-2018-2-50-62/issn2304-5728
9. Klimenko V. Y., Saradzhishvili S. E. Optimization of loop search in flowgraphs. *Veles*, 2019, no. 10–1 (76), pp. 63–66 (In Russian).
10. Menshikov M. A. Effective translation of directed acyclic graphs to intermediate representation. *Processy upravlenija i ustojchivost'*, 2020, no. 1, pp. 271–275 (In Russian).
11. Jumaganov A. S. A combined method of similar code sequences search in executable files. *V mezhdunarodnaja konferencija i molodjozhnaja shkola «Informacionnye tehnologii i nanotehnologii»* [The V International Conference and Youth School "Information Technology and Nanotechnology"]. Samara, 2019, pp. 639–646 (In Russian).
12. Treshhev I. A, Serikov V. A. A practical approach to the implementation of the decompilation of machine code. *Sbornik materialov IV Vserossijskoj nauch-*

no-prakticheskoj konferencii (s mezhdunarodnym uchastiem) "Informacionnye tehnologii v jekonomike i upravlenii" [Collection of Materials of the IV All-Russian Scientific-Practical Conference (with international participation) "Information Technologies in Economy and Management"]. Mahachkala, 2020, pp. 168–173 (In Russian).
13. Izrailov K. E. Applying of genetic algorithms to decompile machine code. *Zashhita informacii*, Insajd, Saint-Petersburg, 2020, no. 3(93), pp. 24–30 (In Russian).
14. Andreev A. A., Datsun N. N. Optimization analisys of fore language translation stages. *Materialy Vserossijskoj nauchno-prakticheskoj konferencii molodyh uchenyh s mezhdunarodnym uchastiem "Matematika i mezhdisciplinarnye issledovanija"* [Materials of the All-Russian Scientific and Practical Conference of Young Scientists with International Participation "Mathematics and Interdisciplinary Research"]. Perm', 2020, pp. 11–15 (In Russian).
15. Katz D. S., Ruchti J., and Schulte E. Using recurrent neural networks for decompilation. *IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 2018, pp. 346–356. doi: 10.1109/SANER.2018.8330222
16. Andrea Gussoni, Alessandro Di Federico, Pietro Fezzardi, and Giovanni Agosta. A comb for decompiled C code. *15th ACM Asia Conference on Computer and Communications Security (ASIA CCS'20)*, October 5–9, 2020, Taipei, Taiwan, ACM, New York, NY, USA, 15 p. https: //doi.org/10.1145/3320269.3384766
17. Gusenko M. The use of regular expressions for decompiling static data. *Software Systems and Computational Methods*, 2017, no. 2, pp. 1–13. doi:10.7256/2454-0714.2017.2.22608
18. Liu Z., and S. Wang. How far we have come: Testing decompilation correctness of C decompilers. *Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2020)*, Association for Computing Machinery, New York, NY, USA, pp. 475–487. doi:10.1145/3395363.3397370
19. Ayoshin I. T. Reverse engineering of software by IDA Pro. *Aktual'nye problemy aviacii i kosmonavtiki*, 2018, vol. 3, no. 4 (14), pp. 808–809 (In Russian).
20. Vorob'ev A. M., Bocvin A. S., Nagibin D. V. Functional analysis of Ghidra — a framework for reverse engineering. *Metody i tehnicheskie sredstva obespechenija bezopasnosti informacii*, 2019, no. 28, pp. 86–88 (In Russian).
21. Derevenec E. O., Troshina E. N. Structural analysis in a decompilation problem. *Prikladnaya informatika*, 2009, no. 4(22), pp. 87–99 (In Russian).
22. Blank Ya. A., Savkin M. K. Control flow graph. *Materialy regional'noj nauchno-tehnicheskoj konferencii "Naukoemkie tehnologii v priboro- i mashinostroenii i razvitie innovacionnoj dejatel'nosti v vuze"* [Materials of the Regional Scientific and Technical Conference "Science-Intensive Technologies in Instrument and Mechanical Engineering and the Development of Innovative Activities in the University"]. Kaluga, 2016, pp. 75–78 (In Russian).
23. Masud A. N., and Ciccozzi F. More precise construction of static single assignment programs using reaching definitions. *Journal of Systems and Software*, 2020, vol. 166. doi:10.1016/j.jss.2020.110590
24. Masud A. N., and Ciccozzi F. Towards Constructing the SSA form using Reaching Definitions Over Dominance Frontiers. *19th International Working Conference on Source Code Analysis and Manipulation (SCAM)*, 2019, pp. 23–33. doi: 10.1109/SCAM.2019.00012
25. *CLRadeonExtender*. Available at: http://clrx.nativeboinc.org (accessed 11 April 2020).
26. Secrets of the new RDNA graphics architecture revealed. *Otkrytye sistemy. SUBD*, 2019, no. 3, p. 5 (In Russian).

УДК 004.431.4
doi:10.31799/1684-8853-2021-2-33-42

Метод декомпиляции AMD GCN ядер в OpenCL

К. И. Михайленко[а,б], магистрант, младший программист, orcid.org/0000-0002-6168-2653, Kristina.Mihajlenko@gmail.com
М. А. Лукин[а,б], канд. техн. наук, технический директор, orcid.org/0000-0002-1088-3324, lukinma@gmail.com
А. С. Станкевич[а], канд. техн. наук, доцент, orcid.org/0000-0002-3532-8941, stankev@itmo.ru
[а]Национальный исследовательский университет ИТМО, Кронверкский пр., 49, Санкт-Петербург, 197101, РФ
[б]ООО «Судо», Нахимова ул., 20, Санкт-Петербург, 199226, РФ

Введение: декомпиляторы являются удобным инструментом для анализа и поддержки программ при отсутствии исходного кода. Существуют декомпиляторы для многих архитектур и языков программирования, но для графических процессоров семейств AMD GCN и RDNA такого инструмента в настоящее время нет. **Цель:** разработать декомпилятор ассемблерного кода AMD GPU в язык программирования OpenCL, широко используемый для программирования на устройствах класса GPGPU. **Результаты:** определены алгоритмы первичной обработки ассемблерного кода: выделение названия программы, параметров и тела программы; поиска обращений к данным и к элементам массивов; извлечения системных значений; поиска и декомпиляции некоторых арифметических операций. Также выработан метод восстановления типов и для работы с локальной памятью. Разработаны шаблоны для определения управляющих конструкций. **Практическая значимость:** предложенные алгоритмы и метод реализованы

на языке Python в виде инструмента OpenCLDecompiler, поддерживающего достаточно большое подмножество команд архитектуры AMD GCN. Разработанный инструмент производит декомпиляцию ассемблерного кода, полученного в результате дизассемблирования исполняемого файла, в код на языке OpenCL, что позволяет сократить трудозатраты на анализ ассемблерного кода.

Ключевые слова — декомпилятор, дизассемблер, OpenCL, AMD GCN, GPGPU, граф потока управления, обратная разработка.

Для цитирования: Mihajlenko K. I., Lukin M. A., Stankevich A. S. A method for decompilation of AMD GCN kernels to OpenCL. *Информационно-управляющие системы*, 2021, № 2, с. 33–42. doi:10.31799/1684-8853-2021-2-33-42

For citation: Mihajlenko K. I., Lukin M. A., Stankevich A. S. A method for decompilation of AMD GCN kernels to OpenCL. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 33–42. doi:10.31799/1684-8853-2021-2-33-42

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Текст рукописи должен быть оригинальным, а цитирование и самоцитирование корректно оформлено.

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, ORCID и электронный адрес одного из авторов. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы. Предоставляйте подрисуночные подписи и названия таблиц на русском и английском языках.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени.

Формулы набирайте в Word, не используя формульный редактор (Mathtype или Equation), при необходимости можно использовать формульный редактор; для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other…, используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; в формулах не отделяйте пробелами знаки: + = –.

Для набора формул в Word никогда не используйте Конструктор (на верхней панели: «Работа с формулами» — «Конструктор»), так как этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Иллюстрации предоставляются отдельными исходными файлами, поддающимися редактированию:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio (*.vsd, *.vsdx); Coreldraw (*.cdr); Excel (*.xls); Word (*.docx); Adobe Illustrator (*.ai); AutoCad (*.dxf); Matlab (*.ps, *.pdf или экспорт в формат *.ai);

— если редактор, в котором Вы изготавливаете рисунок, не позволяет сохранить в векторном формате, используйте функцию экспорта (только по отношению к исходному рисунку), например, в формат *.ai, *.esp, *.wmf, *.emf, *.svg;

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей и названий таблиц на русском и английском языках обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40×55 мм;

— экспертное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц, doi;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц, doi;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules): Литература и References.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Руководство для авторов».

Контакты

Куда: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Тел.: (812) 494-70-02
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru

UDC 003.26
doi:10.31799/1684-8853-2021-2-43-51

Articles

A post-quantum digital signature scheme on groups with four-dimensional cyclicity

D. N. Moldovyan[a], *PhD, Tech., Research Fellow, orcid.org/0000-0001-5039-7198*
N. A. Moldovyan[a], *Dr. Sc., Tech., Professor, Chief Researcher, orcid.org/0000-0002-4483-5048, nmold@mail.ru*
[a]*Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation*

Introduction: *Development of practical post-quantum signature schemes is a current challenge in the applied cryptography. Recently, several different forms of the hidden discrete logarithm problem were proposed as primitive of signature schemes resistant to quantum attacks.* ***Purpose:*** *Development of a new form of the hidden discrete logarithm problem set in finite commutative groups possessing multi-dimensional cyclicity, and a method for designing post-quantum signature schemes.* ***Results:*** *A new form of the hidden discrete logarithm problem is introduced as the base primitive of practical post-quantum digital signature algorithms. Two new four-dimensional finite commutative associative algebras have been proposed as algebraic support for the introduced computationally complex problem. A method for designing signature schemes on the base of the latter problem is developed. The method consists in using a doubled public key and two similar equations for the verification of the same signature. To generate a pair of public keys, two secret minimum generator systems* $<\boldsymbol{G}, \boldsymbol{Q}>$ *and* $<\boldsymbol{H}, \boldsymbol{V}>$ *of two different finite groups* $\Gamma_{<\boldsymbol{G}, \boldsymbol{Q}>}$ *and* $\Gamma_{<\boldsymbol{H}, \boldsymbol{V}>}$ *possessing two-dimensional cyclicity are selected at random. The first public key* ($\boldsymbol{Y}$, $\boldsymbol{Z}$, $\boldsymbol{U}$) *is computed as follows:* $\boldsymbol{Y} = \boldsymbol{G}^{y_1}\boldsymbol{Q}^{y_2\alpha}$, $\boldsymbol{Z} = \boldsymbol{G}^{z_1}\boldsymbol{Q}^{z_2\beta}$, $\boldsymbol{U} = \boldsymbol{G}^{u_1}\boldsymbol{Q}^{u_2\gamma}$, *where the set of integers* (y_1, y_2, α, z_1, z_2, β, u_1, u_2, γ) *is a private key. The second public key* ($\boldsymbol{Y}'$, $\boldsymbol{Z}'$, $\boldsymbol{U}'$) *is computed as follows:* $\boldsymbol{Y}' = \boldsymbol{H}^{y_1}\boldsymbol{V}^{y_2\alpha}$, $\boldsymbol{Z}' = \boldsymbol{H}^{z_1}\boldsymbol{V}^{z_2\beta}$, $\boldsymbol{U}' = \boldsymbol{H}^{u_1}\boldsymbol{V}^{u_2\gamma}$. *Using the same parameters to calculate the corresponding elements belonging to different public keys makes it possible to calculate a single signature which satisfies two similar verification equations specified in different finite commutative associative algebras.* ***Practical relevance:*** *Due to a smaller size of the public key, private key and signature, as well as approximately equal performance as compared to the known analogues, the proposed digital signature scheme can be used in the development of post-quantum signature algorithms.*

Keywords *— post-quantum cryptoschemes, computer security, digital signature, discrete logarithm problem, finite commutative groups, associative algebras, multi-dimensional cyclicity.*

For citation: Moldovyan D. N., Moldovyan N. A. A post-quantum digital signature scheme on groups with four-dimensional cyclicity. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 43–51. doi:10.31799/1684-8853-2021-2-43-51

Introduction

Currently the most widely used public-key cryptoschemes exploit the computational complexity of the factoring problem (FP) [1, 2] and the discrete logarithm problem (DLP) [3, 4]. However, the expected breakthrough in quantum computing technology in the near future makes it extremely urgent to develop cryptosystems that are resistant to attacks using quantum computers. Post-quantum public-key cryptosystems should be based on computationally difficult problems other than FP and DLP, since efficient polynomial algorithms for solving FP and DLP on a quantum computer are known [5–7].

In the current field of development of public-key post-quantum cryptoschemes, considerable attention of the cryptographers is paid to the development of cryptoschemes on algebras [8, 9], on boolean functions [10, 11], and on linear codes [12, 13].

One of attractive post-quantum primitives is the hidden discrete logarithm problem (HDLP) defined usually in non-commutative finite associative algebras (FAAs). Different forms of the HDLP were proposed to develop signature schemes on non-commutative FAAs [9, 14, 15]. For the first time, a signature scheme on a commutative FAA was proposed in [16]. The interest in the HDLP problem is related to the fact that the HDLP-based signature schemes have relatively small sizes of the public key and signature. This area of research is quite new, and for a deeper and more complete understanding of the possibilities for the development of practical post-quantum HDLP-based, it is of significant interest to search for new forms, especially for the case of using commutative FAAs as a carrier of the HDLP.

In this paper, we propose a new form of setting the HDLP in commutative FAAs characterized in that the multiplicative group of the algebras possesses four-dimentional cyclicity in terms of the paper [17]: a finite commutative group whose minimum generator system includes μ ($\mu \geq 2$) elements that have the same order is called group with μ-dimensional cyclicity. The method of setting the proposed form of the HDLP is fundamentally different from the method introduced earlier in the paper [16] for development of the HDLP-based signature on a commutative algebra.

Two commutative FAAs used as algebraic support

A finite m-dimensional vector space over the finite ground field $GF(p)$, in which a vector multiplication operation is defined additionally to the scalar multiplication and addition operations, is called m-dimensional algebra, if the vector multiplication is distributive at the left and at the right relatively the addition. A vector $\mathbf{A}$ is presented as an ordered set of its coordinates: $\mathbf{A} = (a_0, a_1, ..., a_{m-1})$ or as a sum of its components: $\mathbf{A} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + ... + a_{m-1}\mathbf{e}_{m-1}$, where $\mathbf{e}_i$ ($i = 0, 1, ..., m - 1$) are formal basis vectors. Defining additionally the operation of vector multiplication ($\circ$) possessing the property of the two-sided distributivity relatively the addition operation, one gets the finite m-dimensional algebra.

Usually, the multiplication of two vectors $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ and $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is defined by the following formula: $\mathbf{A} \circ \mathbf{B} = \sum_{j=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \mathbf{e}_i \circ \mathbf{e}_j$, where the coordinates a_i and b_i are multiplied as elements of the field $GF(p)$ and every the product of two formal basis vectors is to be replaced by an one-component vector indicated in a cell at the intersection of the i-th row and j-th column of so called basis vector multiplication table, for example, see Table 1 [16]. Each of these tables defines a four-dimensional commutative FAA, multiplicative group of which has order Ω that can be computed as number of invertible vectors. Consider, for example, the algebra defined by Table 1.

The unit element of this commutative FAA is the vector $\mathbf{E} = (0, 0, 1, 0)$. If for some vector $\mathbf{A}$ the vector equation

$$\mathbf{AX} = \mathbf{E} \qquad (1)$$

has a unique solution, then the vector $\mathbf{A}$ is called invertible. For a fixed invertible vector $\mathbf{A}$ the vector equation $\mathbf{AX} = \mathbf{E}$ has a unique solution denoted as $\mathbf{A}^{-1}$ (called inverses of $\mathbf{A}$). Evidently, $\mathbf{AA}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{E}$. An invertibility condition can be derived from equation (1) that can be reduced to the following system of four linear equations, where the unknowns are coordinates of the vector $\mathbf{X} = (x_0, x_1, x_2, x_3)$:

$$\begin{cases} a_2x_0 + a_3x_1 + a_0x_2 + a_1x_3 = 1 \\ \lambda a_3x_0 + a_2x_1 + a_1x_2 + \lambda a_0x_3 = 0 \\ \lambda a_0x_0 + a_1x_1 + a_2x_2 + \lambda a_3x_3 = 0 \\ a_1x_0 + a_0x_1 + a_3x_2 + a_2x_3 = 0 \end{cases}. \qquad (2)$$

The main determinant of the system (2) is

$$\Delta = \begin{vmatrix} a_2 & a_3 & a_0 & a_1 \\ \lambda a_3 & a_2 & a_1 & \lambda a_0 \\ \lambda a_0 & a_1 & a_2 & \lambda a_3 \\ a_1 & a_0 & a_3 & a_2 \end{vmatrix} = a_2 \begin{vmatrix} a_2 & a_1 & \lambda a_0 \\ a_1 & a_2 & \lambda a_3 \\ a_0 & a_3 & a_2 \end{vmatrix} -$$

$$- a_3 \begin{vmatrix} \lambda a_3 & a_1 & \lambda a_0 \\ \lambda a_0 & a_2 & \lambda a_3 \\ a_1 & a_3 & a_2 \end{vmatrix} + a_0 \begin{vmatrix} \lambda a_3 & a_2 & \lambda a_0 \\ \lambda a_0 & a_1 & \lambda a_3 \\ a_1 & a_0 & a_2 \end{vmatrix} -$$

$$- a_1 \begin{vmatrix} \lambda a_3 & a_2 & a_1 \\ \lambda a_0 & a_1 & a_2 \\ a_1 & a_0 & a_3 \end{vmatrix} = a_2\left(a_2\left(a_2^2 - \lambda a_3^2\right) - a_1\left(a_1a_2 - \lambda a_0a_3\right) + \lambda a_0\left(a_1a_3 - a_0a_2\right)\right) -$$

$$- a_3\left(\lambda a_3\left(a_2^2 - \lambda a_3^2\right) - a_1\left(\lambda a_0a_2 - \lambda a_1a_3\right) + \lambda a_0\left(\lambda a_0a_3 - a_1a_2\right)\right) + a_0\left(\lambda a_3\left(a_1a_2 - \lambda a_0a_3\right) - a_2\left(\lambda a_0a_2 - \lambda a_1a_3\right) + \lambda a_0\left(\lambda a_0^2 - a_1^2\right)\right) -$$

$$- a_1\left(\lambda a_3\left(a_1a_3 - a_0a_2\right) - a_2\left(\lambda a_0a_3 - a_1a_2\right) + a_1\left(\lambda a_0^2 - a_1^2\right)\right) = \ldots = \lambda^2\left(a_0^2 + a_3^2\right)^2 - 4\lambda a_0^2a_3^2 +$$

$$+ \left(a_1^2 + a_2^2\right)^2 - 4\lambda a_0^2a_3^2 - 2\lambda\left(a_0^2 + a_3^2\right)\left(a_1^2 + a_2^2\right) + 8\lambda a_0a_1a_2a_3 = \ldots = \left(\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2\right)^2 - 4\left(\lambda a_0a_3 - a_1a_2\right)^2.$$

The case $\Delta \neq 0$ defines the following invertibility condition:

$$\left(\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2\right)^2 - 4\left(\lambda a_0a_3 - a_1a_2\right)^2 \neq 0. \qquad (3)$$

The case $\Delta = 0$ defines the following non-invertibility condition:

$$\left(\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2\right)^2 = 4\left(\lambda a_0a_3 - a_1a_2\right)^2. \qquad (4)$$

Proposition 1. Suppose the structural constant λ is a quadratic non-residue in $GF(p)$. Then the number of different non-invertible vectors in the

■ ***Table 1***. Setting the multiplication operation in the first used FAA multiplicative group of which possesses multi-dimensional cyclicity ($\lambda \neq 0$)

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$

four-dimensional FAA set by Table 1 is equal to $\eta = 2p^2 - 1$.

Proof: The non-invertibility condition (4) sets the following two cases:

i) $\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 = 2\lambda a_0 a_3 - 2a_1 a_2 \Rightarrow$

$\Rightarrow \lambda(a_0 - a_3)^2 = (a_1 - a_2)^2;$

ii) $\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 = -2\lambda a_0 a_3 + 2a_1 a_2 \Rightarrow$

$\Rightarrow \lambda(a_0 + a_3)^2 = (a_1 + a_2)^2.$

If the structural constant λ is a quadratic non-residue modulo p, then for the first case the equality holds true only if $(a_0 - a_3)^2 = (a_1 - a_2)^2 = 0$. This gives p different sets of coordinates a_0 and a_1 and p different sets of coordinates a_2 and a_3, including the zero vector (0, 0, 0, 0). Totally, in the first case we have $p^2 - 1$ non-inverible vectors. In the second case the equality holds true only if $(a_0 + a_3)^2 = (a_1 + a_2)^2 = 0$. This defines other p^2 sets of coordinates a_0, a_1, a_2, and a_3, including (0, 0, 0, 0). Therefore we have $\eta = 2p^2 - 1$. Proposition 1 is proven.

Proposition 2. Suppose the structural constant λ is a quadratic non-residue in $GF(p)$. Then the order of the multiplicative group of the FAA set by the Table 1 is equal to $\Omega = (p^2 - 1)^2$.

Proof: Among p^4 different vectors of the algebra you have $\eta = 2p^2 - 1$ non-invertible ones, therefore $\Omega = p^4 - \eta = (p^2 - 1)^2$. Proposition 2 is proven.

Proposition 3. Suppose the structural constant λ is a quadratic residue in $GF(p)$. Then the number of non-invertible vectors in the four-dimensional FFA set by Table 1 is equal to $\eta = 4p^3 - 6p^2 + 4p^2 - 1$.

Proof: Since the structural constant λ is a quadratic residue, formula (4) defines the following two cases:

i) $\left(a_0\sqrt{\lambda} - a_3\sqrt{\lambda}\right)^2 = (a_1 - a_2)^2 \Rightarrow a_0\sqrt{\lambda} - a_3\sqrt{\lambda} =$

$= \pm(a_1 - a_2);$

ii) $\left(a_0\sqrt{\lambda} + a_3\sqrt{\lambda}\right)^2 = (a_1 + a_2)^2 \Rightarrow a_0\sqrt{\lambda} + a_3\sqrt{\lambda} =$

$= \pm(a_1 + a_2).$

Sets of coordinates (a_0, a_1, a_2, a_3) satisfying one of four conditions defined by the said two cases represent non-invertible vectors. The following Table 2 shows the number of vectors coordinates of which satisfy a condition indicated in the left column.

Totally, we have

$$\eta = p^2 + p^2 + 2p(p-1)^2 + 2p(p-1)^2 = 4p^3 - 6p^2 + 4p - 1.$$

Proposition 3 is proven.

■ ***Table 2***. Number of non-invertible vectors relating to different subsets for the case when λ is a quadratic residue

Condition	# of different combinations of coordinates (a_0, a_1, a_2, a_3) satisfying the condition at the left
$a_0\sqrt{\lambda} - a_3\sqrt{\lambda} = a_1 - a_2 = 0$	p^2 including (0, 0, 0, 0)
$a_0\sqrt{\lambda} + a_3\sqrt{\lambda} = a_1 + a_2 = 0$	p^2 including (0, 0, 0, 0)
$a_0\sqrt{\lambda} - a_3\sqrt{\lambda} = \pm(a_1 - a_2) \neq 0$	$2p(p-1)^2$
$a_0\sqrt{\lambda} + a_3\sqrt{\lambda} = \pm(a_1 + a_2) \neq 0$	$2p(p-1)^2$

Proposition 4. Suppose the structural constant λ is a quadratic residue in $GF(p)$. Then the order of the multiplicative group of the FAA set by the Table 1 is equal to $\Omega = (p-1)^4$.

Proof: Among p^4 different vectors of the algebra you have $\eta = 4p^3 - 6p^2 + 4p^2 - 1$ non-invertible ones, therefore $\Omega = p^4 - \eta = p^4 - (4p^3 - 6p^2 + 4p^2 - 1) = (p-1)^4$. Proposition 4 is proven.

Thus, if the structural constant λ is equal to a quadratic residue modulo p, then the multiplicative group of the considered algebra has order $(p-1)^4$ and possesses four-dimensional cyclicity [16]. If the structural constant λ is equal to a quadratic non-residue modulo p, then the multiplicative group of the considered algebra has order $(p^2 - 1)^2$ and possesses two-dimensional cyclicity [16].

In the developed signature scheme, it is assumed that the first commutative FAA is set by Table 1, where λ is equal to a quadratic residue, and the characteristic of the field $GF(p)$ is a prime having the following structure $p = 2q + 1$ with 256-bit prime q. In this case the integer q divides $p - 1$ and one can generate a minimum generator system $<\mathbf{G}, \mathbf{Q}>$, where $\mathbf{G}$ and $\mathbf{Q}$ are vectors of the order q, which sets a two-dimensional cyclicity subgroup of order q^2.

We also use another commutative FAA possessing the properties similar to that of the algebra set by Table 1. The second used commutative FAA is set by basis vector multiplication table represented as Table 3, where λ is equal to a quadratic residue, and includes the unit vector $\mathbf{E} = (0, 0, 0, 1)$. Consideration of the number of invertible vectors in the second commutative FAA shows that for the latter the Propositions 1 to 4 are also true. Thus, we have two different commutative FAAs multiplicative group each of which possesses four-dimensional cyclicity. The latter group contains a large num-

■ ***Table 3.*** Setting the second used FAA ($\lambda \neq 0$)

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_3$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$\lambda\mathbf{e}_3$	$\mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$

ber of two-dimensional cyclicity subgroups of the order q^2.

Example 1. In the case of the first FAA with $p = 2q + 1 = 307771779467$ (prime $q = 153885889733$) and $\lambda = 3$ (quadratic residue) one can select the following minimum generator system $<\mathbf{G}, \mathbf{Q}, \mathbf{H}, \mathbf{V}>$ setting a primary group $\Gamma_{<\mathbf{G},\mathbf{Q},\mathbf{H},\mathbf{V}>}$ of the order $\Omega_{<\mathbf{G},\mathbf{Q},\mathbf{H},\mathbf{V}>} = q^4 = 560783464662101934272226806080639851841841521$:

$$\mathbf{G} = (0, 0, 3, 0); \mathbf{Q} = (0, 2, 5, 0); \mathbf{H} = (2, 7, 3, 0);$$

$$\mathbf{V} = (13, 12, 10, 17).$$

For $\lambda = 2$ (quadratic non-residue) one can select the following minimum generator system $<\mathbf{G}, \mathbf{Q}>$ setting a primary group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ of the order $\Omega_{<\mathbf{G},\mathbf{Q}>} = q^2 = 947234682362836828040 89$:

$$\mathbf{G} = (0, 0, 3, 0) \text{ and } \mathbf{Q} = (0, 1, 2, 0).$$

Example 2. In the case of the second FAA with $p = 2q + 1 = 273413518347119$ (prime $q = 136706759173559$) and $\lambda = 2$ (quadratic residue) one can select the following minimum generator system $<\mathbf{G}, \mathbf{Q}, \mathbf{H}, \mathbf{V}>$ setting a primary group $\Gamma_{<\mathbf{G},\mathbf{Q},\mathbf{H},\mathbf{V}>}$ of the order $\Omega_{<\mathbf{G},\mathbf{Q},\mathbf{H},\mathbf{V}>} = q^4 = 34926892817234073926007473842204106865502885395378264336 1$:

$$\mathbf{G} = (0, 0, 0, 2); \mathbf{Q} = (0, 0, 1, 2); \mathbf{H} = (0, 1, 4, 7);$$

$$\mathbf{V} = (1, 3, 7, 10).$$

For $\lambda = 13$ (quadratic non-residue) one can select the following minimum generator system $<\mathbf{G}, \mathbf{Q}>$ setting a primary group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ of the order $\Omega_{<\mathbf{G},\mathbf{Q}>} = q^2 = 18688738003737457800684726481$:

$$\mathbf{G} = (0, 189, 0, 222) \text{ and } \mathbf{Q} = (0, 0, 0, 2).$$

Consider a method for generating a minimun generator system of a two-dimensional cyclicity subgroup of order q^2. The following procedure outputs a random vector of the order q:

1. Generate a random vector $\mathbf{R}$ and compute the vector $\mathbf{Q} = \mathbf{R}^2$.

2. If $\mathbf{Q} \neq \mathbf{E}$, then output $\mathbf{Q}$. Else go to step 1.

The next probabilistic procedure outputs the minimum generator system:

1. Generate a uniformly random vector $\mathbf{G}$ of prime order q.

2. Generate a uniformly random vector $\mathbf{Q}$ of order q.

The multiplicative group of the algebra contains $q^4 - 1$ vectors of order q. The cyclic group generated by the vector $\mathbf{G}$ includes $q - 1$ vectors of order q, therefore, probability that the vector $\mathbf{Q}$ is an element of the cyclic group generated by the vector $\mathbf{G}$ is equal approximately to q^{-3}. In another case the pair of vectors $<\mathbf{G}, \mathbf{Q}>$ represents a minimum generator system of a primary subgroup of order q^2 that is contained in the multiplicative group of the algebra. For the case of 256-bit prime q the probability q^{-3} that the latter procedure fails is negligible.

A new HDLP-based signature scheme

In the developed signature scheme a 256-bit collision-resistant hash function f_H is assumed to be used. Computation of the public key is proposed as the following procedure.

Public-key generation algorithm.

1. Generate at random a minimum generator system $<\mathbf{G}, \mathbf{Q}>$ of the group of order q^2, which is contained in the first commutative FAA.

2. Generate at random integers $y_1 < q$, $y_2 < q$, and $\alpha < p$, where α is a primitive element in $GF(p)$. Then calculate the vector $\mathbf{Y} = \mathbf{G}^{y_1}\mathbf{Q}^{y_2}\alpha$.

3. Generate at random integers $z_1 < q$, $z_2 < q$, and $\beta < p$, where β is a primitive element in $GF(p)$. Then calculate the vector $\mathbf{Z} = \mathbf{G}^{z_1}\mathbf{Q}^{z_2}\beta$.

4. Generate at random integers $\gamma < p$, $u_1 < q$, and $u_2 < q$, such that non-equality $z_1u_2 \neq z_2u_1$ holds true and γ is a primitive element in $GF(p)$. Then calculate the vector $\mathbf{U} = \mathbf{G}^{u_1}\mathbf{Q}^{u_2}\gamma$.

5. Generate at random a minimum generator system $<\mathbf{H}, \mathbf{V}>$ of the group of order q^2, which is contained in the second commutative FAA.

6. Calculate the vectors $\mathbf{Y}' = \mathbf{H}^{y_1}\mathbf{V}^{y_2}\alpha$, $\mathbf{Z}' = \mathbf{H}^{z_1}\mathbf{V}^{z_2}\beta$, and $\mathbf{U}' = \mathbf{H}^{u_1}\mathbf{V}^{u_2}\gamma$.

7. Output the public key in the form of two triples of vectors: $(\mathbf{Y}, \mathbf{Z}, \mathbf{U})$ and $(\mathbf{Y}', \mathbf{Z}', \mathbf{U}')$.

In the developed signature scheme, we use the idea of doubling the signature verification equation connected with doubling the public key. Therefore, the triple $(\mathbf{Y}, \mathbf{Z}, \mathbf{U})$ will be called in this paper the first public key. Respectively, the triple $(\mathbf{Y}', \mathbf{Z}', \mathbf{U}')$ will be called the second public key. Each of the public keys has been calculated with using the same private key representing nine 256-bit integers (y_1, y_2, α, z_1, z_2, β, u_1, u_2, γ) and the same formulas. The first (second) public key is computed in the first (second) commutative FAAs. The size of each

of public keys is equal to 384 bytes, and the size of doubled public key equals to 768 bytes.

The vectors **G**, **Q**, **H**, and **V** are secret, but the developed signature scheme offers the possibility to choose one of two signature generation procedures. In the first one, only four exponentiation operations are executed in FAAs, however, the vectors **G**, **Q**, **H**, and **V** must be stored by the owner of the public key (the person who generated the public key) as additional elements of his private key. In this case the size of private key is equal to 704 bytes.

In the second version of the signature generation procedures, six exponentiation operations are to be performed in FAAs, but the vectors **G**, **Q**, **H**, and **V** are not needed and the set of nine integers (y_1, y_2, α, z_1, z_2, β, u_1, u_2, γ) represent the full private key having the size equal to 192 bytes.

Usually, finding the integer x satisfying the exponential equation $Y' = G'^x$, where Y' and G' are known group elements, which is set in a finite cyclic group is called discrete logarithm problem. If one of the elements Y' and G' or both of them is not directly given, then we have a number of problems we call HDLPs. Different forms of the HDLP are considered in [9, 15]. The HDLP form exploited in the present paper is defined as follows:

Given a triple of vectors (**Y**, **Z**, **U**) contained in the first FAA and a triple of vectors (**Y**′, **Z**′, **U**′) contained in the second FAA. Find the set of integer powers (y_1, y_2, z_1, z_2, u_1, u_2) and the set of scalars (α, β, γ) such that equations $\mathbf{Y} = \mathbf{G}^{y_1}\mathbf{Q}^{y_2}\alpha$, $\mathbf{Z} = \mathbf{G}^{z_1}\mathbf{Q}^{z_2}\beta$, $\mathbf{U} = \mathbf{G}^{u_1}\mathbf{Q}^{u_2}\gamma$ (in the first FAA), $\mathbf{Y}' = \mathbf{H}^{y_1}\mathbf{V}^{y_2}\alpha$, $\mathbf{Z}' = \mathbf{H}^{z_1}\mathbf{V}^{z_2}\beta$, and $\mathbf{U}' = \mathbf{H}^{u_1}\mathbf{V}^{u_2}\gamma$ (in the second FAA) hold true for i) some secret vectors **G** and **Q** generating two different cyclic groups of prime order q in the first FAA; ii) some secret vectors **H** and **V** generating two different cyclic groups of prime order q in the second FAA.

One can easily show that, due to using random vectors **G** and **Q** (**H** and **V**) and scalar multiplications, the vectors **Y**, **Z**, and **U** (**Y**′, **Z**′ and **U**′) compose a basis of a three-dimensional cyclicity group in the first (second) FAA. Therefore the vector **Y** (**Y**′) cannot be represented as a product of some powers of the vectors **Z** and **U** (**Z**′ and **U**′) and a periodic function set on the base of the known parameters has periods defined by the order of the public key elements, i. e., by the prime q. The latter means that the Shor quantum algorithm [5] is not applicable to find one of the values y_1, y_2, z_1, z_2, u_1, and u_2.

The said computationally complex problem underlying the developed signature scheme is a new one and currently the authors have no proposal for solving it (except exhaustive search). However, the importance of finding effective solutions allows us to hope that this article will stimulate independent researchers to address this issue. At the moment, the authors expect that choosing a 256-bit prime number q will provide a 128-bit level of security for the proposed signature algorithm.

The first signature generation algorithm.

1. Generate three uniformly random integers $k < q$, $t < q$, and $\rho < p$.

2. Calculate the vector $\mathbf{R} = \mathbf{G}^k\mathbf{Q}^t\rho$.

3. Calculate the vector $\mathbf{R}' = \mathbf{H}^k\mathbf{V}^t\rho$.

4. Compute the first signature element e that is a hash-function value calculated from the document M to be signed, to which the vectors **R** and **R**′ are concatenated: $e = f_H(M, \mathbf{R}, \mathbf{R}')$.

5. Interpreting the hash value as a 256-bit binary number e, calculate the second s and third d signature elements, which represent the solution of the following system of two linear equations:

$$\begin{cases} z_1 s + u_1 d = k - e y_1 \bmod q \\ z_2 s + u_2 d = t - e y_2 \bmod q \end{cases}. \qquad (5)$$

It is easy to get the following formulas for computation of the second and third signature elements:

$$s = \frac{u_2(k - e y_1) - u_1(t - e y_2)}{z_1 u_2 - z_2 u_1} \bmod q; \qquad (6)$$

$$d = \frac{z_1(t - e y_2) - z_2(k - e y_1)}{z_1 u_2 - z_2 u_1} \bmod q. \qquad (7)$$

6. Compute the fourth signature element $\sigma = \rho\alpha^{-e}\beta^{-s}\gamma^{-d}$.

The output signature is four 256-bit numbers (e, s, d, σ) with total size equal to 128 bytes.

The second signature generation algorithm.

1. Generate four uniformly random integers $a < q$, $b < q$, $c < q$, and $\rho < p$.

2. Calculate the vector $\mathbf{R} = \mathbf{Y}^a\mathbf{Z}^b\mathbf{U}^c\rho$.

3. Calculate the vector $\mathbf{R}' = \mathbf{Y}'^a\mathbf{Z}'^b\mathbf{U}'^c\rho$.

4. Compute the first signature element e that is a hash-function value calculated from the document M to be signed, to which the vectors **R** and **R**′ are concatenated: $e = f_H(M, \mathbf{R}, \mathbf{R}')$.

5. Interpreting the hash value as a 256-bit binary number e, calculate the second s and third d signature elements, which represent the solution of the system (5) and can be computed by formulas (6) and (7), substituting the following values of the randomization integers k and t:

$$k = a y_1 + b z_1 + c u_1 \bmod q \text{ and}$$

$$t = a y_2 + b z_2 + c u_2 \bmod q.$$

6. Compute the fourth signature element $\sigma = \rho\alpha^{a-e}\beta^{b-s}\gamma^{c-d}$.

The main contribution to the computational complexity of the signature generation procedure is introduced by the exponentiation operations.

The exponentiation in each of the four-dimensional FAAs takes about 6144 multiplications in $GF(p)$. One exponentiation in $GF(p)$ takes on the average about 384 multiplications. One can roughly estimate the execution time of the first and second signature generation procedures as 25728 and 38016 multiplications in $GF(p)$, correspondingly.

The signature verification algorithm.

1. Calculate the vector $\mathbf{R}^* = \mathbf{Y}^e\mathbf{Z}^s\mathbf{U}^d\sigma$.

2. Calculate the vector $\mathbf{R}'^* = \mathbf{Y}'^e\mathbf{Z}'^s\mathbf{U}'^d\sigma$.

3. Compute the hash-function value from the document M to which the vectors $\mathbf{R}^*$ and $\mathbf{R}'^*$are concatenated: $e^* = f_H(M, \mathbf{R}^*, \mathbf{R}'^*)$.

4. If $e^* = e$, then the signature is accepted as a genuine one, otherwise the signature is rejected as a false one.

One can roughly estimate the computational complexity (execution time) of the signature verification procedure as six exponentiations in the used four-dimensional algebras or as 37248 multiplications in $GF(p)$.

Signature scheme correctness proof.

To prove correctness of the introduced signature scheme, consider a signature (e, s, d, σ) computed in full correspondence with the first signature generation procedure when using the correct signer's private key. When, submitting the signature (e, s, d, σ) to the input of the verification procedure, we have the following proof of the correctness of the proposed signature scheme with the first signature generation algorithm [take into account formulas in the system (5)]:

$$\mathbf{R}^* = \mathbf{Y}^e\mathbf{Z}^s\mathbf{U}^d\sigma =$$
$$= \mathbf{G}^{ey_1}\mathbf{Q}^{ey_2}\alpha^e\mathbf{G}^{sz_1}\mathbf{Q}^{sz_2}\beta^s\mathbf{G}^{du_1}\mathbf{Q}^{du_2}\gamma^d\sigma =$$
$$= \mathbf{G}^{ey_1+sz_1+du_1}\mathbf{Q}^{ey_2+sz_2+du_2}\alpha^e\beta^s\gamma^d\sigma =$$
$$= \mathbf{G}^{ey_1+(k-ey_1)}\mathbf{Q}^{ey_2+(t-ey_2)}\alpha^e\beta^s\gamma^d\rho\alpha^{-e}\beta^{-s}\gamma^{-d} =$$
$$= \mathbf{G}^k\mathbf{Q}^t\rho = \mathbf{R};$$
$$\mathbf{R}'^* = \mathbf{Y}'^e\mathbf{Z}'^s\mathbf{U}'^d\sigma =$$
$$= \mathbf{H}^{ey_1}\mathbf{V}^{ey_2}\alpha^e\mathbf{H}^{sz_1}\mathbf{V}^{sz_2}\beta^s\mathbf{H}^{du_1}\mathbf{V}^{du_2}\gamma^d\sigma =$$
$$= \mathbf{H}^{ey_1+sz_1+du_1}\mathbf{V}^{ey_2+sz_2+du_2}\alpha^e\beta^s\gamma^d\sigma =$$
$$= \mathbf{H}^{ey_1+(k-ey_1)}\mathbf{V}^{ey_2+(t-ey_2)}\alpha^e\beta^s\gamma^d\rho\alpha^{-e}\beta^{-s}\gamma^{-d} =$$
$$= \mathbf{H}^k\mathbf{V}^t\rho = \mathbf{R}';$$
$$\{\mathbf{R}'^* = \mathbf{R}'; \mathbf{R}^* = \mathbf{R}\} \Rightarrow e^* = e.$$

The final equality means the input signature passes the verification procedure as a genuine signature, i. e., the signature scheme performs correctly. The correctness proof of the signature scheme with the second signature generation algorithm is similar to the presented one.

Discussion

The fact that the same signature satisfies two similar, but different, verification equations is ensured by the same pairs of powers (y_1, y_2), (z_1, z_2), and (u_1, u_2) and the same multipliers α, β, and γ, which are used to compute the corresponding elements of the first $(\mathbf{Y}, \mathbf{Z}, \mathbf{U})$ and second $(\mathbf{Y}', \mathbf{Z}', \mathbf{U}')$ public keys. The public keys are computed after selection random minimum generator systems $<\mathbf{G}, \mathbf{Q}>$ (in the first FAA) and $<\mathbf{H}, \mathbf{V}>$ (in the second FAA) which are secret. Every of the element of the first (second) public key is calculated as an element of the two-dimensional cyclicity group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ ($\Gamma_{<\mathbf{H},\mathbf{V}>}$), which is multiplied by a random scalar. After scalar multiplication we get with a high probability a vector outside the group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ ($\Gamma_{<\mathbf{H},\mathbf{V}>}$). Thus, the elements of the first (second) public key are not elements of the group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ ($\Gamma_{<\mathbf{H},\mathbf{V}>}$).

Suppose a vector $\mathbf{W}$ is an element of the group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$. The problem of finding the powers w_1 and w_2 such that $\mathbf{W} = \mathbf{G}^{w1}\mathbf{Q}^{w2}$ is called discrete logarithm problem in a two-dimensional cyclicity group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$. In this paper we assume that a potential signature forger can efficiently solve this problem, i. e., if a minimum generator system is given, then a forger can efficiently express any group element as product of some powers of two generators.

Consider an arbitrary minimum generator system $<\mathbf{G}_i, \mathbf{Q}_i>$ of the primary group of order q^2 in the first algebra. The forger can generate random integers α_i, β_i, γ_i and efficiently compute the values $(y_{i1}, y_{i2}, z_{i1}, z_{i2}, u_{i1}, u_{i2})$ such that $\mathbf{Y}\alpha_i^{-1} = \mathbf{G}_i^{y_{i1}}\mathbf{Q}_i^{y_{i2}}$, $\mathbf{Z}\beta_i^{-1} = \mathbf{G}_i^{z_{i1}}\mathbf{Q}_i^{z_{i2}}$, and $\mathbf{U}\gamma_i^{-1} = \mathbf{G}_i^{u_{i1}}\mathbf{Q}_i^{u_{i2}}$. Then, using the formulas (6) and (7), he can compute a signature satisfying the first verification equation. However, this signature will satisfy the second verification equation only if the primary group of order q^2 of the second algebra contains a minimum generator system $<\mathbf{H}_i, \mathbf{V}_i>$ such that $\mathbf{Y}'\alpha_i^{-1} = \mathbf{H}_i^{y_{i1}}\mathbf{V}_i^{y_{i2}}$, $\mathbf{Z}'\beta_i^{-1} = \mathbf{H}_i^{z_{i1}}\mathbf{V}^{z_{i2}}$, and $\mathbf{U}'\gamma_i^{-1} = \mathbf{H}_i^{u_{i1}}\mathbf{V}_i^{u_{i2}}$. However, in fact, the fixed four values $(y_{i1}, y_{i2}, z_{i1}, z_{i2})$ define one minimum generator system $<\mathbf{H}_i, \mathbf{V}_i>$ (that can be supposedly computed) such that $\mathbf{Y}'\alpha_i^{-1} = \mathbf{H}_i^{y_{i1}}\mathbf{V}_i^{y_{i2}}$ and $\mathbf{Z}'\beta_i^{-1} = \mathbf{H}_i^{z_{i1}}\mathbf{V}_i^{z_{i2}}$. For the fixed values of the vectors $\mathbf{H}_i$ and $\mathbf{V}_i$ one will get $\mathbf{U}'\gamma_i^{-1} = \mathbf{H}_i^{u'_{i1}}\mathbf{V}_i^{u'_{i2}}$, where the values u'_{i1} and u'_{i2} are random. Since the first and second commutative FAAs are independent, the equalities $u'_{i1} = u_{i1}$ and $u'_{i2} = u_{i2}$ of two pairs of 256-bit numbers can take place only at random with probability about 2^{-512}.

Therefore, we expect that the signature forger is unable to find efficiently the required alternative pair of vectors $<\mathbf{G}_i, \mathbf{Q}_i>$ or to guess the secret elements $<\mathbf{G}, \mathbf{Q}>$. A quantum computer will not provide much help to the forger, since the discrete logarithm problem that arises is hidden (the "bases" of logarithms, i. e., $<\mathbf{G}, \mathbf{Q}>$ and $<\mathbf{H}, \mathbf{V}>$ are unknown).

In fact, breaking the proposed signature scheme is to find two minimum generator systems of two different two-dimensional cyclicity groups (contained in two different FAAs) which are consistent with each other. These two minimum generator systems are connected by the mechanism of doubling the verification equation, i. e., by a single digital signature, which must satisfy the verification equation given in two different independent commutative FAAs.

One can note, that the method [18, 19] of the reductionist security proof that was applied to the Schnorr signature algorithm [20] can be also applied to the proposed signature scheme. Indeed, an assumption that a signature forger is able to calculate a signature equally well for six different hash functions leads to potential possibility to compute the private key (y_1, y_2, α, z_1, z_2, β, u_1, u_2, γ).

Indeed, like in [19], suppose a potential signature forger can compute signatures for different hash functions, when the values of the randomization parameters are k, t, and ρ are fixed. For four different hash functions he computes the signatures (e_1, s_1, d_1, σ_1), (e_2, s_2, d_2, σ_2), (e_3, s_3, d_3, σ_3), and (e_4, s_4, d_4, σ_4). Then the signature forger composes the following system of eight linear equations with eight unknowns y_1, y_2, z_1, z_2, u_1, u_2, k, and t [see (5)]:

$$\begin{cases} z_1 s_1 + u_1 d_1 = k - e_1 y_1 \bmod q \\ z_2 s_1 + u_2 d_1 = t - e_1 y_2 \bmod q \\ z_1 s_2 + u_1 d_2 = k - e_2 y_1 \bmod q \\ z_2 s_2 + u_2 d_2 = t - e_2 y_2 \bmod q \\ z_1 s_3 + u_1 d_3 = k - e_3 y_1 \bmod q \\ z_2 s_3 + u_2 d_3 = t - e_3 y_2 \bmod q \\ z_1 s_4 + u_1 d_4 = k - e_4 y_1 \bmod q \\ z_2 s_4 + u_2 d_4 = t - e_4 y_2 \bmod q \end{cases}.$$

Note, the probability that the main determinant of his system of equations equals to zero is negligibly small (q^{-1}). Solving the latter system one can get the values of y_1, y_2, z_1, z_2, u_1, and u_2. It easy to show that, using the formulas $\sigma_i = \rho\alpha^{-e_i}\beta^{-s_i}\gamma^{-d_i}$ for $i = 1, 2, 3, 4$ (see step 6 in the first signature generation algorithm) and finding roots from different ratio values σ_i/σ_j in $GF(p)$, one can calculate the values of scalars α, β, and γ. Thus, taking into account that operations of finding roots in $GF(p)$, where $p = 2q + 1$, have polynomial computational complexity, one can conclude that a polynomial algorithm for forging a signature is reducible to a polynomial algorithm of solving the HDLP underlying the introduced signature scheme.

The above provides a general idea for constructing a signature scheme and a general justification for its resistance to attacks using conventional and quantum computers. Detailed consideration of the security issue and obtaining detailed estimates is a separate independent task for the new study.

■ ***Table 4***. Comparison with some known post-quantum signature schemes

Signature scheme	Signature size, byte	Public key size, byte	Rate of signature generation, arb. un.	Rate of signature verification, arb. un.
Falcon	1280	1793	50	25
Crystals-Dilithium	2701	1472	15	2
Rainbow	64	150 000	–	–
[15]	192	768	50	80
[16]	192	512	40	80
Proposed	128	768	70	80

It is important that the proposed fundamentally new method for setting the HDLP can be implemented in numerous different ways. The most obvious is the use of different pairs of finite associative algebras. In particular, pairs of algebras of different orders, different types and structures can be used. In particular, is interesting to consider the following versions:

i) one algebra is commutative and the other one is non-commutative;

ii) one algebra is defined over a ground finite field $GF(p)$, and the other one is defined over a finite extension of the binary field $GF(2^s)$.

The introduced design method opens up quite wide possibilities for implementing various design variants of digital signature schemes. The introduced signature scheme suites well for software implementation, since it uses only additions, multiplications, exponentiations and inversions (mod p and mod q).

Currently, the NIST competition [21] for the development of post-quantum public-key cryptosystems has entered the final stage [22]. The finalists in the category of post-quantum signatures were Falcon [23] and Crystals-Dilithium [24], and Rainbow [25]. It is interesting to compare the proposed signature scheme with the finalists and with other HDLP-based signatures. A rough comparison is presented in Table 4.

Conclusion

A new design method and a practical HDLP-based post-quantum signature scheme have been introduced. The proposed method is quite simple to understand and has fundamental differences from

other known methods of designing post-quantum digital signature schemes. This reduces the complexity of the further stage of a detailed study of the security of the developed signature scheme. Another important advantage of the proposed method is that it opens up the possibility of developing a new class of practical post-quantum cryptosystems. The latter is of particular importance in the light of the widely conducted researches on the development of post-quantum digital signature standards.

References

1. Rivest R. L., Shamir A., Adleman L. M. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 1978, vol. 21, pp. 120–126.
2. Chiou S. Y. Novel digital signature schemes based on factoring and discrete logarithms. *International Journal of Security and its Applications*, 2016, vol. 10, no. 3, pp. 295–310.
3. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 1985, vol. IT-31, no. 4, pp. 469–472.
4. Schnorr C. P. Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174.
5. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.
6. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 1996, vol. 68, pp. 733–752.
7. Smolin J. A., Smith G., Vargo A. Oversimplifying quantum factoring. *Nature*, 2013, vol. 499, no. 7457, pp. 163–165.
8. Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A. Cryptographic algorithms on groups and algebras. *Journal of Mathematical Sciences*, 2017, vol. 223, no. 5, pp. 629–641.
9. Moldovyan N. A., Moldovyan A. A. Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem. *Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software*, 2019, vol. 12, no. 1, pp. 66–81. doi:10.14529/mmp190106
10. Agibalov G. P., Pankratova I. A. Asymmetric cryptosystems on Boolean functions. *Prikl. Diskr. Mat.*, 2018, no. 40, pp. 23–33. doi:10.17223/20710410/40/3
11. Agibalov G. P. ElGamal cryptosystems on Boolean functions. *Prikl. Diskr. Mat*, 2018, no. 42, pp. 57–65. DOI:10.17223/20710410/42/4
12. Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme. *Designs, Codes and Cryptography*, 2017, vol. 82, no. 1–2, pp. 469–493.
13. Kosolapov Y. V., Turchenko O. Y. On the construction of a semantically secure modification of the McEliece cryptosystem. *Prikl. Diskr. Mat.*, 2019, no. 45, pp. 33–43. doi:10.17223/20710410/45/4
14. Moldovyan N. A., Moldovyan A. A. New forms of defining the hidden discrete logarithm problem. *SPIIRAS Proceedings*, 2019, vol. 18, no. 2, pp. 504–529. doi:10.15622/sp.18.2.504-529
15. Moldovyan N. A., Moldovyan A. A. Candidate for practical post-quantum signature scheme. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2020, vol. 16, iss. 4, pp. 455–461. doi:10.21638/11701/spbu10.2020.410
16. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A novel method for development of post-quantum digital signature schemes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 21–29. doi:10.31799/1684-8853-2020-6-21-29
17. Moldovyan N. A. Fast signatures based on non-cyclic finite groups. *Quasigroups and Related Systems*, 2010, vol. 18, no. 1, pp. 83–94.
18. Pointcheval D., Stern J. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 2000, vol. 13, pp. 361–396.
19. Koblitz N., Menezes A. J. Another look at "Provable Security". *Journal of Cryptology*, 2007, vol. 20, pp. 3–38.
20. Schnorr C. P. Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174.
21. *Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms*. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed 27 January 2021).
22. *Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed 27 January 2021).
23. *Fast-Fourier Lattice-Based Compact Signatures over NTRU*. Available at: https://falcon-sign.info/ (accessed 27 January 2021).
24. Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D. *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*. https://eprint.iacr.org/2017/633.pdf. Available at: https://pq-crystals.org/dilithium/index.shtml (accessed 27 January 2021).
25. Ding J., Schmidt D. *Rainbow, a New Multivariable Polynomial Signature Scheme*. In: Ioannidis J., Keromytis A., Yung M. (eds). *Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg, 2005. Vol. 3531. Pp. 164–175.

УДК 003.26
doi:10.31799/1684-8853-2021-2-43-51

Постквантовая схема цифровой подписи на группе с четырехмерной цикличностью

Д. Н. Молдовян[a], канд. техн. наук, научный сотрудник, orcid.org/0000-0001-5039-7198
Н. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0002-4483-5048, nmold@mail.ru
[a]Санкт-Петербургский институт информатики и автоматизации РАН, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ

Введение: разработка практичных постквантовых схем подписи является одним из вызовов прикладной криптографии. Несколько различных форм скрытой задачи дискретного логарифмирования были предложены недавно в качестве примитива схем подписи, стойких к квантовым атакам. **Цель:** разработка новой формы скрытой задачи дискретного логарифмирования, заданной в коммутативной группе, обладающей многомерной цикличностью, и метода построения постквантовых схем подписи. **Результаты:** предложена новая форма скрытой задачи дискретного логарифмирования в качестве базового примитива для практичных постквантовых алгоритмов цифровой подписи. Представлены две новые четырехмерные конечные коммутативные ассоциативные алгебры в качестве алгебраического носителя предложенной новой вычислительно трудной задачи. Разработан метод построения схем подписи на основе последней. Суть метода состоит в использовании удвоенного открытого ключа и двух одинаковых уравнений для проверки подлинности одной и той же подписи. Для генерации пары открытых ключей выбираются случайным образом два базиса $<\mathbf{G}, \mathbf{Q}>$ и $<\mathbf{H}, \mathbf{V}>$ двух различных конечных групп $\Gamma_{<\mathbf{G}, \mathbf{Q}>}$ и $\Gamma_{<\mathbf{H}, \mathbf{V}>}$, обладающих двумерной цикличностью. Первый открытый ключ $(\mathbf{Y}, \mathbf{Z}, \mathbf{U})$ вычисляется следующим образом: $\mathbf{Y} = \mathbf{G}^{y_1}\mathbf{Q}^{y_2}\alpha$, $\mathbf{Z} = \mathbf{G}^{z_1}\mathbf{Q}^{z_2}\beta$, $\mathbf{U} = \mathbf{G}^{u_1}\mathbf{Q}^{u_2}\gamma$, где набор целых чисел $(y_1, y_2, \alpha, z_1, z_2, \beta, u_1, u_2, \gamma)$ является секретным ключом. Второй открытый ключ $(\mathbf{Y}', \mathbf{Z}', \mathbf{U}')$ вычисляется следующим образом: $\mathbf{Y}' = \mathbf{H}^{y_1}\mathbf{V}^{y_2}\alpha$, $\mathbf{Z}' = \mathbf{H}^{z_1}\mathbf{V}^{z_2}\beta$, $\mathbf{U}' = \mathbf{H}^{u_1}\mathbf{V}^{u_2}\gamma$. Использование одинаковых параметров для вычисления соответствующих друг другу элементов, принадлежащих разным открытым ключам, обеспечивает возможность вычисления единой подписи, удовлетворяющей двум сходным проверочным уравнениям, заданным в различных конечных коммутативных ассоциативных алгебрах. **Практическая значимость:** предложенная схема цифровой подписи представляет практический интерес для разработки постквантовых алгоритмов подписи, обладающих сравнительно малыми размерами подписи, открытого и секретного ключей.

Ключевые слова — постквантовые криптосхемы, компьютерная безопасность, электронная цифровая подпись, задача дискретного логарифмирования, конечные коммутативные группы, ассоциативные алгебры, многомерная цикличность.

Для цитирования: Moldovyan D. N., Moldovyan N. A. A post-quantum digital signature scheme on groups with four-dimensional cyclicity. *Информационно-управляющие системы*, 2021, № 2, с. 43–51. doi:10.31799/1684-8853-2021-2-43-51
For citation: Moldovyan D. N., Moldovyan N. A. A post-quantum digital signature scheme on groups with four-dimensional cyclicity. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 43–51. doi:10.31799/1684-8853-2021-2-43-51

UDC 621.396
doi:10.31799/1684-8853-2021-2-52-59

Articles

On multiplexing data streams using trellis-coded modulation in centralized wireless networks

N. A. Yankovskii[a], *Student, orcid.org/0000-0001-5783-8304*
I. A. Pastushok[a], *PhD, Tech., Associate Professor, orcid.org/0000-0002-3296-562X, igpastushok@gmail.com*
[a]*Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation*

Introduction: *The proliferation of services and applications requiring ultra-low latency and high reliability of data transmission in communication networks leads to creating new approaches and architectures in order to ensure the simultaneous transmission of Enhanced Mobile Broadband (eMBB) and Ultra-Reliable and Low Latency Communication (URLLC) traffic. Providing efficient eMBB and URLLC multiplexing schemes with preset key performance indicators for each stream is the most challenging problem in wireless network development.* ***Purpose:*** *To provide a simultaneous transmission of eMBB and URLLC streams without reducing the user experience of eMBB services by developing a multiplexing scheme and the coherent architecture of physical (PHY) and media access control (MAC) layers in the downlink channel.* ***Results:*** *An eMBB and URLLC multiplexing scheme has been proposed, along with a coherent architecture for PHY and MAC layers, ensuring the given wireless network key performance indicators. The proposed solution performance has been estimated by simulation. The multiplexing scheme outperforms the baseline solution in Bit Error Rate and Frame Error Rate metrics. The coherent PHY and MAC layers architecture provides transmission with an arrival rate of 400 messages per millisecond and 99% message delivery probability in one millisecond.* ***Practical relevance:*** *The obtained results allow communication system developers to deploy centralized wireless networks at industrial objects.*

Keywords *— URLLC, eMBB, multiplexing, radio resource management, centralized wireless networks, trellis-coded modulation, LDPC.*

For citation: Yankovskii N. A., Pastushok I. A. On multiplexing data streams using trellis-coded modulation in centralized wireless networks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 52–59. doi:10.31799/1684-8853-2021-2-52-59

Introduction

In just a few decades, wireless technology has undergone rapid growth from its original concept to ubiquitous penetration, which has changed our daily lives and thinking. Wireless connection has become an essential link between people and information networks. The growing density of user devices triggered an increasing demand for higher capacity and network reliability. The constant increase in traffic leads to congestion of base stations and a decrease in service level quality.

An attractive solution to this problem is the multiplexing of data streams in the downlink. A substantial amount of in-depth research has been dedicated to this topic.

In [1], authors consider various models for the Enhanced Mobile Broadband (eMBB) rate loss associated with Ultra-Reliable and Low Latency Communication (URLLC) superposition/puncturing, for which we characterize the associated feasible throughput regions and online joint scheduling algorithms. The first model considered by the authors is the linear model. When the rate loss to eMBB is directly proportional to the fraction of superposed/punctured mini-slot. The second model considered was the convex model, where the rate loss can be modeled through a convex function. And the last model considered was the threshold model where eMBB traffic is unaffected by puncturing until a threshold. Beyond this threshold, it suffers complete throughput loss.

There are also several papers describing a specific scheme for the coexistence of multiple data streams. So, in [2], the authors introduced an approach for coexisting URLLC [3] and eMBB [4] traffic in the same radio resource for enabling 5G wireless systems. They have expressed the coexisting dilemma as a maximizing problem of the minimum expected achieved rate value of eMBB user equipment (UEs) meanwhile attending the URLLC traffic.

Also, they presented a heuristic algorithm for the efficient scheduling of resource blocks among eMBB UEs. In [5], the authors considered approaches to data multiplexing based on machine learning. In their work, they proposed an optimization-aided deep reinforcement learning-based algorithm, which proposed to distribute the incoming URLLC traffic among eMBB users intelligently. In [6], the authors consider the optimization problem of maximizing the transmission rate of eMBB traffic, subject to URLLC requirements. To study the impact of puncturing eMBB resources to accommodate URLLC transmission, the authors in [7] investigated the problem of joint planning of eMBB and

URLLC data transmission according to linear, convex, and threshold velocity stall models by eMBB associated with the drilling of the eMBB resource. In [8], a risk-sensitive approach was introduced to mitigate the risk of puncturing into eMBB resources. A resource allocation planner was proposed in [9], where the formulated problem considered the overhead associated with URLLC load segmentation while maximizing speed utility. In [10], a null space-based spatial perforation scheduler for joint URLLC / eMBB traffic has been proposed. The authors in [11] formulated a URLLC traffic allocation problem by adopting an overlay or perforation scheme. In practice, when the URLLC service is started in the middle of the eMBB transport block, part of the eMBB symbols are replaced and/or overlapped with the symbols in the URLLC packet. As a result, the reception quality of eMBB services can be significantly reduced.

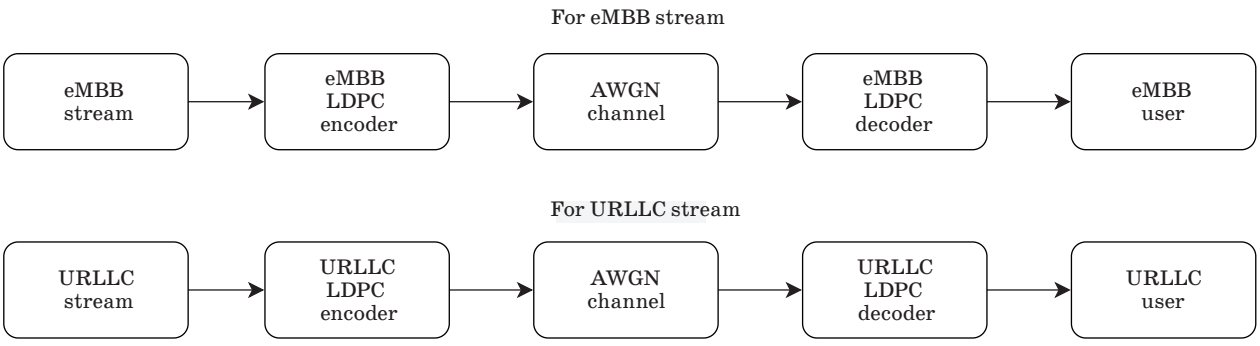
In [12], the authors also study the orthogonal and non-orthogonal slicing of radio resources for eMBB and URLLC using a maximum matching diversity (MMD) algorithm to locate frequency channels of eMBB users. In [13], the authors adopted a time/frequency resource block approach to address the problem of maximizing the sum rate subject to latency and cutoff isolation constraints while ensuring the reliability requirements using adaptive modulation coding. In [14], the authors studied a multi-cell scenario with a single-cell base stations for an Ultra-Narrow Band and Low Power Wide Area Network. Article [15] analyzes the use of non-orthogonal multiple accesses (NOMA) for different URLLC devices. To achieve this, the authors propose a NOMA sharing approach, successive interference cancellation, and frequency diversity as a solution to increase the number of URLLC de-vices that can be connected to the same base station. In [16], a new class of NOMA has been proposed, namely bits similarity NOMA. It has been shown that without a perfect successive interference cancellation, bit similarity NOMA can achieve better efficiency between users than traditional NOMA techniques.

Another approach to multiplexing URLLC and eMBB traffic is Trellis- and Network-coded modulation (TC-NCM) [17]. Based the Ungerboeck's scheme [18] and the general type of coset coding advocated by Goldsmith in [19] and Chapter 8 of [20], the authors propose adaptive TC-NCM structure, where the transmitter adapts the coding rate and modulation mode according to the channel estimates fed back via feedback channels. The main disadvantage of this method is the lack of encoding of the URLLC stream, which negatively affects the reliability and transmission rate of URLLC messages. This work's main task is to propose a Trellis-Coded Modulation (TCM) scheme for multiplexing streams and define the loss function for it. The remainder of this paper is organized as follows. We commence by describing the system model along with a system of assumptions. We then conceive our generic structure of the multiplexing scheme, where the motivation, the transmitter design, and the data flow are detailed. Finally, we present some modeling results and conclusions.

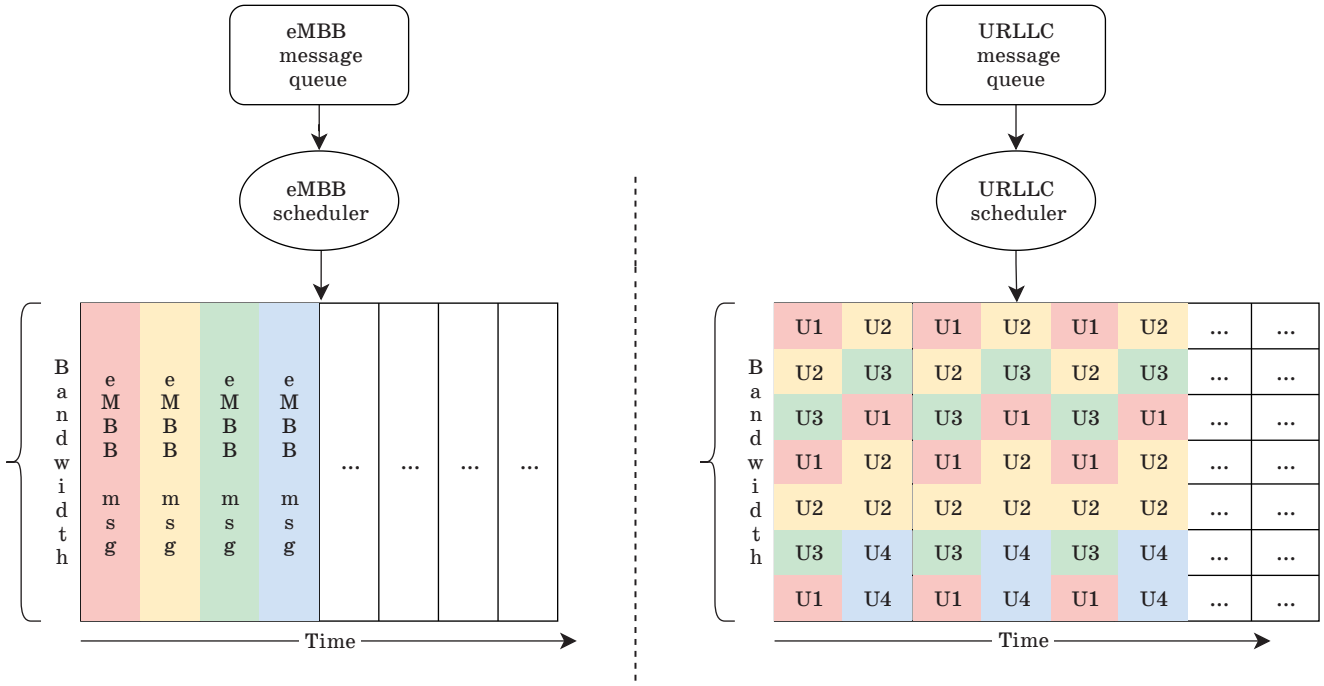
Baseline system model

In this article, we discuss the development of the model proposed in [21] generalized to the physical layer of wireless centralized systems. As before, the baseline scenario will be the case when only 1 data stream is transmitted. However, in contrast to the previous work [21], we will consider the Viterbi decoder's quantized output — the general scheme for basic scenarios presented in Fig. 1.

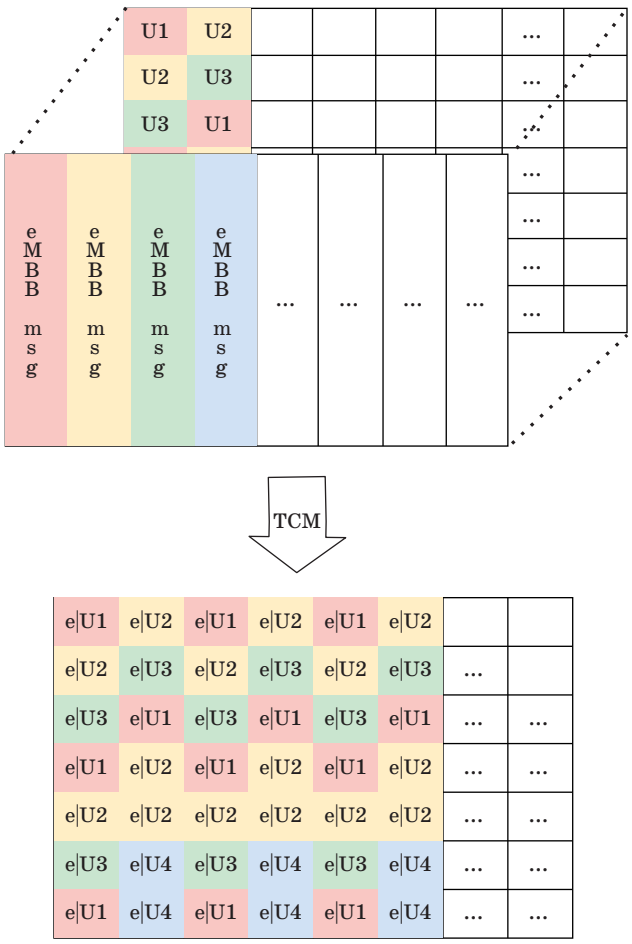
In the case of a multiplexing scenario, the network contains a base station, as well as users receiving eMBB and URLLC traffic from the base station, respectively. As in the previous article, the simultaneous transmission is considered data for different recipients from one sender. Each data stream has its own scheduler. The scheduler for eMBB traffic uses time division multiplexing (TDM/TDMA), and the scheduler for URLLC uses (OFDM/OFDMA) (Fig. 2).



■ *Fig. 1.* Baseline scenario



■ ***Fig. 2.*** Resource scheduling for different data streams



■ ***Fig. 3.*** Scheduling resources after using multiplexing

After the allocation of the radio resource by the schedulers, a multiplexing scheme is used, after which the information bits of different streams are located in the combined resource block for further transmission over the channel (Fig. 3).

Assumptions

Having outlined the transmission model, next we list all of our operating assumptions used throughout this paper.

1. Channel state information is always available on the sender. Assume that the feedback path does not introduce any errors, which can be approximately satisfied, provided that sufficiently powerful error correction and detection codes are used on the feedback path.

2. We are considering a channel with additive white Gaussian noise.

3. We consider the downlink in TDMA mode for eMBB data stream and OFDMA for URLLC data stream.

4. We know on the receiving side of the URLLC traffic transmission position for the user.

5. EMBB users are not aware of the existence of URLLC traffic and do not decode it.

Multiplexing algorithm

It is known that the Ungerboeck scheme [18] combines encoding and modulation by expanding

the Euclidean distance between codewords and absorbs parity bits without bandwidth expansion by doubling the number of points in the constellation due to increasing the number of bits / symbols by one. This design jointly optimizes both channel encoding and modulation, hence again, resulting in significant encoding gains without any bandwidth expansion. Based on these ideas, our adaptive stream multiplexing scheme was developed.

Generic multiplexing scheme

At some point in time, an eMBB message and several URLLC messages appear on this station. Then the algorithm for multiplexing and transmitting messages is as follows (Fig. 4):

1. A checksum is added to all messages.

2. Messages are fed to the LDPC encoding unit. For eMBB traffic the code rate is 8/9, and for URLLC traffic it is 1/2. This choice is due to the fact that URLLC messages are shorter and more demanding on the reliability of transmission.

3. After LDPC encoding, the messages are combined into one using an interleaver.

4. The general message is fed to the input of the TCM, which selects the modulation dimension required to transmit ($l + r$) symbols, where l — message length; r — redundancy of the applied convolutional code.

5. Then the message is transmitted over the communication channel and enters the input of the decoder, which is a soft output Viterbi algorithm.

6. The message is quantized according to the following rule: the most significant $\log_2(Q)$ bits of the Log-Likelihood Ratio are stored, where Q is the number of quantization levels.

7. The codewords of each stream passes the deinterleaver and LDPC decoder.

8. The checksum is checked, and a decision is made on the correctness of the received message.

Key performance indicators of the system

To assess the quality of the proposed multiplexing algorithm, it is necessary to introduce indicators of efficiency. This article discusses the following key performance parameters:

1) frame error rate (FER) for URLLC and eMBB streams;

2) bit error rate (BER) for eMBB stream;

3) channel capacity for URLLC stream;

4) complexity of separating eMBB and URLLC streams.

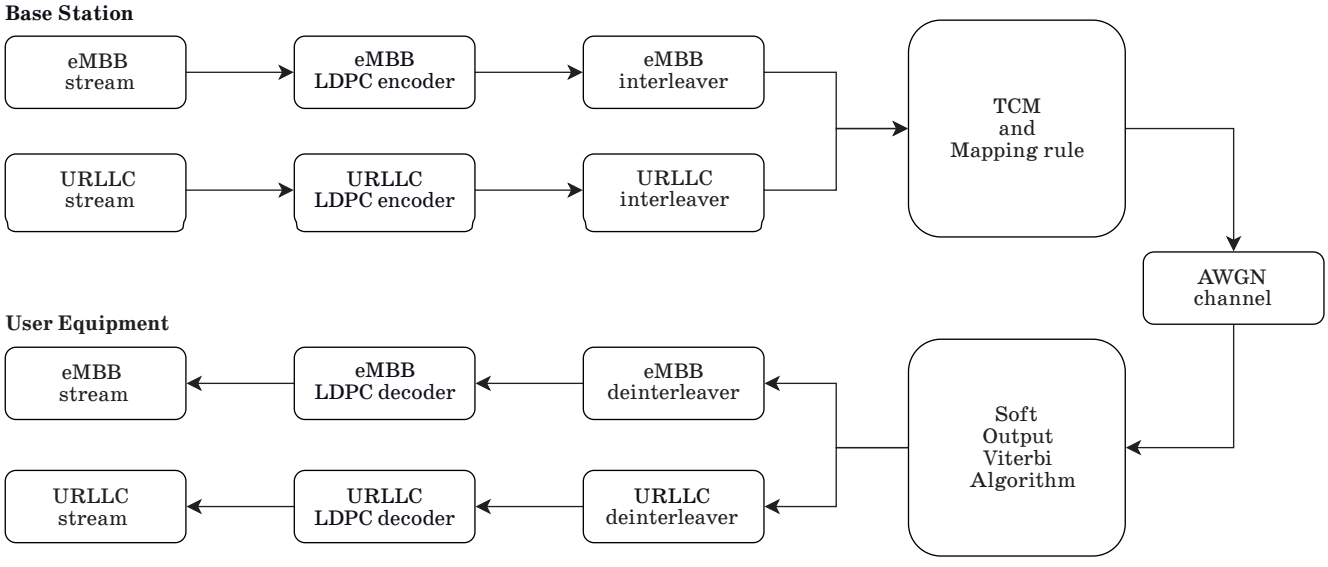
To evaluate the first two performance criteria, we introduce the following notation A_{ber} and B_{ber} — functions for the considered scenarios that return the SNR (signal-to-noise ratio) value to achieve the required BER value. A_{fer} and B_{fer} — return SNR value to achieve the required FER respectively. Thus, we consider that system B is not inferior to system A if:

$$B_{ber}(10^{-7}) <= A_{fer}(10^{-7});$$
$$B_{fer}(10^{-4}) <= A_{fer}(10^{-4});$$

frequency bands of A and B are the same.

The channel capacity here means the ability to transmit all URLLC messages in one time slot. The following algorithm was used to calculate the channel capacity for the URLLC stream:

1. A set of messages is generated according to the Poisson distribution.



■ ***Fig. 4.*** General scheme of the multiplexing algorithm

2. The generated messages occupy slots in the current time slot.

3. Messages that did not get free resource blocks or were incompletely allocated are discarded and replenished the message buffer that was refused transmission.

4. Based on the number of discarded messages and the total number, the probability is calculated that the message will not be transmitted in 1 time slot.

Stream splitting algorithm consists of two parts: Soft-Output Viterbi Algorithm (SOVA) and deinterleaver. The time complexity of the Viterbi algorithm can be expressed as $O(NS^2)$, where N is a length of message in bits, and S is a number of states in a hidden Markov model.

The complexity of deinterleaving is equal to the size of the message, so the overall complexity of streaming can be considered equal to the complexity of decoding using the Viterbi algorithm.

System parameters

The 5G-NR standard implies the use of a different number of templates with different network parameters (Table 1).

■ ***Table 1***. 5G-NR numerology

Parameter	Numerology values				
	0	1	2	3	4
Subcarrier width, kHz	15	30	60	120	240
Num of slot in subframe	1	2	4	8	16
Slot duration, ms	1	0.5	0.25	0.125	0.0625

Each template allows you to adaptively configure the physical layers of the system. Such templates are called numerology, and, in this paper, we use the numerology parameters under number 3 (see Table 1). The structure of the frame is presented in Fig. 5. This article considers the mm-Wave scenario with 50 MHz cell and numerology 3. All-time divided by subframes 1ms duration each. By numerology 3, each subframe is divided into eight slots, 0.125 ms each. Thus, we can calculate the number of available OFDM symbols for multiplexing in each slot and subframe.

LDPC codes in the 5G-NR standard also have many different parameters. The parameters used in our system are shown in Table 2.

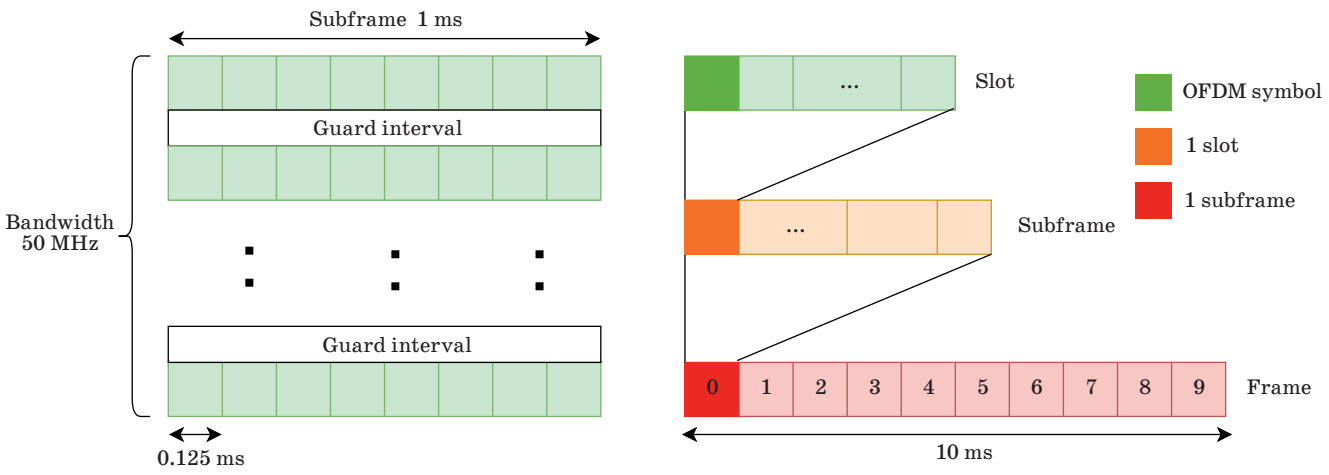
The main parameter of TCM is the use of convolutional polynomial coding. In our work, we use the polynomial presented by William G. Chambers [10] (Fig. 6), since it provides the maximal possible free

■ ***Table 2***. *LDPC parameters*

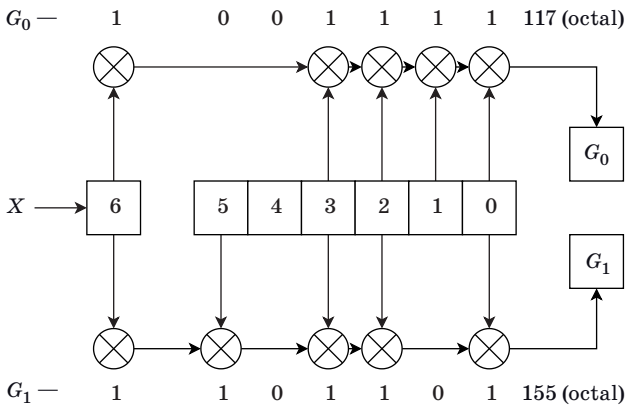
Stream	Code rate	Reduncity level	nlayers
eMBB	8/9	0	3
URLLC	1/2	0	3

■ ***Table 3***. *TCM parameters*

Octets	Memory	d_f	Code rate	Modulation	Mapping rule
117 155	6	10	1/2	QAM-16	Gray mapping



■ ***Fig. 5***. 5G-NR Numerology 3 frame structure



■ ***Fig. 6.*** Convolutional code

distance (d_f) and so the maximal asymptotic coding gain. The parameters of the selected polynomial are shown in Table 3.

Simulation results

Using the parameters described above, the FER versus SNR plots were obtained using simulation for both data streams (Fig. 7, *a* and *b*).

It can be seen from the figures above that due to the complication of the decoding procedure when multiplexing streams, the FER values for all quantization levels exceed the FER values for the baseline scenario.

Let us consider the efficiency of the multiplexing algorithm in terms of BER for the eMBB stream. Fig. 8 shows a plot of BER versus SNR for different quantization levels.

■ ***Table 4.*** *Coding gain*

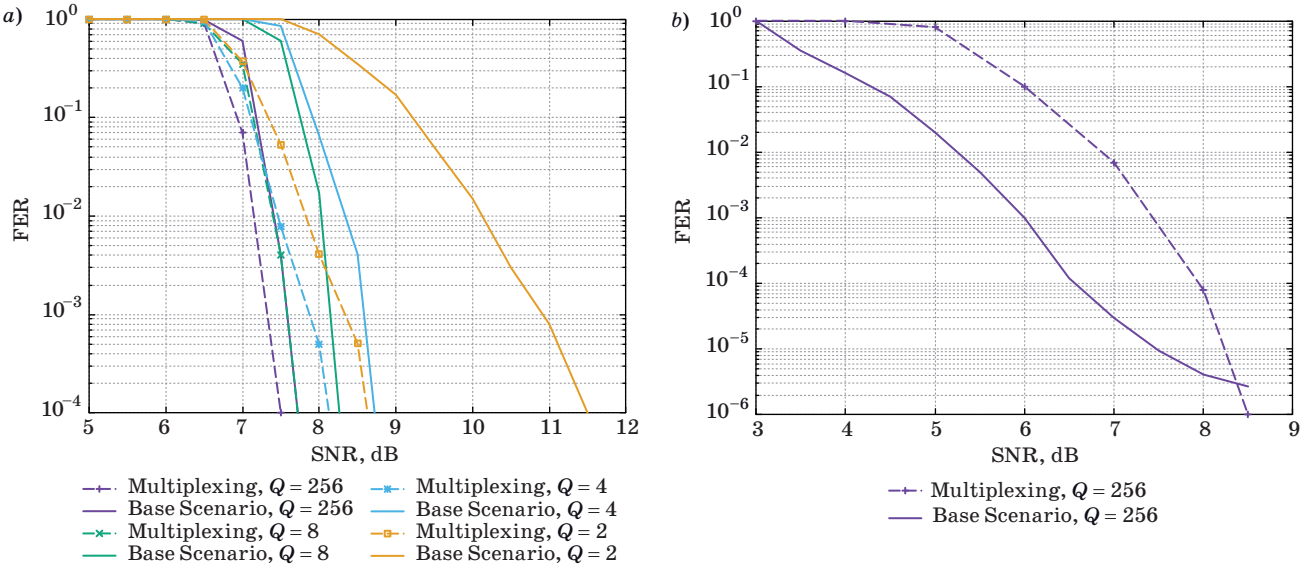
Stream	$Q = 2$	$Q = 4$	$Q = 16$	$Q = 256$
eMBB, FER = 10^{-2}	2.5	0.8	0.7	0.3
eMBB, FER = 10^{-4}	2.6	0.5	0.5	0.3
URLLC, FER = 10^{-5}	–	–	–	–0.5
URLLC, FER = 10^{-6}	–	–	–	0.5

Table 4 shows the gain in dB when using multiplexing for different quantization levels.

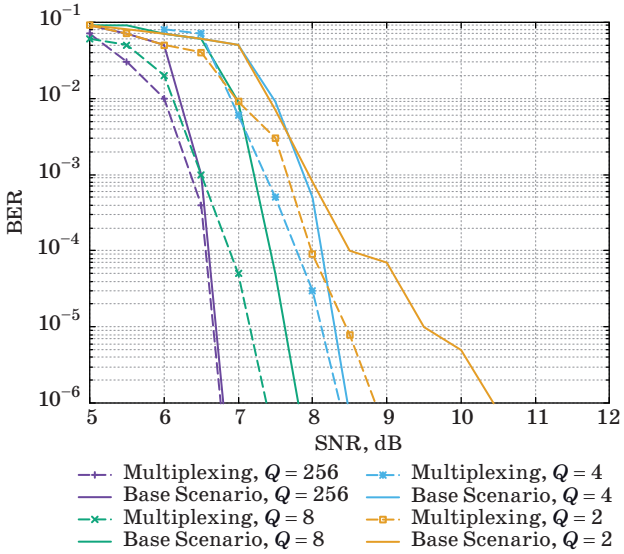
URLLC stream capacity

Since the URLLC stream must fulfill the requirements of immediate transmission, we will assume that if the message was not transmitted per 1ms subframe, then it loses its relevance for the end user. Fig. 9 shows the probability of non-transfer URLLC messages with a length of 100 bits per 1 ms subframe for the considered multiplexing scenario (see simulation details in [21]). We can conclude that the probability of sending a URLLC message in one mini-slot more than 99% for an incoming rate of up to 400 messages per slot.

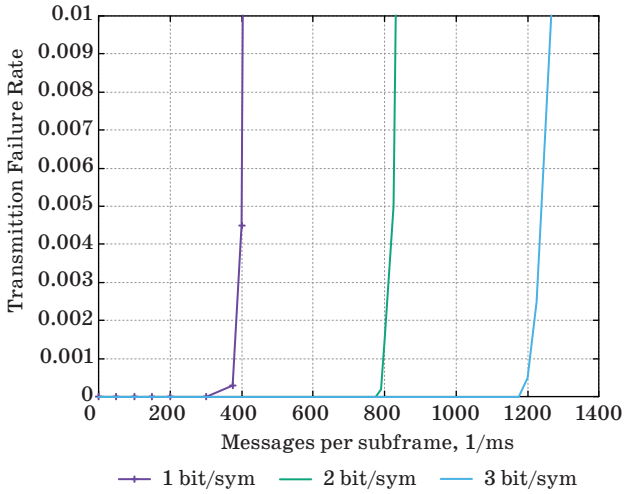
Thus, the proposed downlink multiplexing scheme using TCM allows to obtain a lower error probability in the channel for eMBB traffic, as well as to preserve the key parameters of the efficiency applied to URLLC traffic. The proposed scheme



■ ***Fig. 7.*** FER versus SNR for eMBB (*a*) and URLLC (*b*) stream



■ ***Fig. 8***. BER versus SNR for eMBB stream, Q is a number of quantization levels



■ ***Fig. 9***. Denial of service rate

can be classified as a threshold model by [1], and all known results can be applied to ours.

Conclusion

This article proposed an algorithm for multiplexing data streams in the downlink communication of centralized wireless networks. This algorithm fits the threshold model proposed by Veciana G. Then, a general scheme based on TCM was considered and applied to 5G-NR Numerology 3 networks. Our simulation results show that the proposed algorithm achieves better BER and FER performance for the eMBB stream compared to the baseline scenario without multiplexing. We also presented graphs of the channel throughput for the URLLC stream, from which it can be seen that this scheme allows providing the probability of sending a URLLC message in one mini-slot more than 99% for an incoming rate of up to 400 messages per slot. For promising future research, an attractive direction is the study of achievable improvement in constellation formation, improving system performance.

Financial support

This work was supported by grant MK-1326.2021.1.6 “Research of algorithms for access to radio channel resources for systems of the industrial Internet of things”.

References

1. Anand A., Veciana G., and Shakkottai S. Joint scheduling of URLLC and eMBB traffic in 5G wireless networks. *IEEE/ACM Transactions on Networking*, 2020, vol. 28, pp. 477–490.
2. Bairagi K., Munir M. S., Alsenwi M., Tran N. H., Alshamrani S. S., Masud M., Han Z., and Hong C. S. *Coexistence mechanism between eMBB and uRLLC in 5G wireless networks*. 2020. Available at: https://arxiv.org/pdf/2003.04551.pdf (accessed 20 November 2020).
3. ITU-R M.2083-0. IMT Vision — framework and overall objectives of the future development of IMT for 2020 and beyond. ITU-R, 2015. 21 p.
4. 3GPP TS 22.261 16.4.0. Service requirements for next generation new services and markets. 3GPP, 2017. 55 p.
5. Alsenwi M., Tran N. H., Bennis M., Pandey S. R., Bairagi A. K., and Hong C. S. *Intelligent resource slicing for eMBB and URLLC coexistence in 5G and beyond: A deep reinforcement learning based approach*. Available at: https://arxiv.org/pdf/2003.07651.pdf (accessed 14 December 2020).
6. Alsenwi M., Hong C. S. *Resource scheduling of URLLC/eMBB traffics in 5G new radio: A punctured scheduling approach*. Avaliable at: http://networking.khu.ac.kr/xe/Gallery/entry/document_srl/141/page/layouts/net/publications/data/KCC2018/14.Madyan.pdf (accessed 14 December 2020). doi:10.1109/INFOCOM.2018.8486430.
7. Anand A., Veciana G., and Shakkottai S. Joint scheduling of URLLC and eMBB traffic in 5G wireless networks. *IEEE INFOCOM 2018 — IEEE Conference on Computer Communications*, April 2018, pp. 1970–1978.
8. Alsenwi M., Tran N. H., Bennis M., Kumar Bairagi A., and Hong C. S. eMBB-URLLC resource slicing: A risk-sensitive approach. *IEEE Commun. Lett.*, 2019, vol. 23, no. 4, pp. 740–743.

9. Karimi A., Pedersen K. I., Mahmood N. H., Pocovi G., and Mogensen P. Efficient low complexity packet scheduling algorithm for mixed URLLC and eMBB traffic in 5G. *IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, April 2019, pp. 1–6.
10. Khalifa N. B., Angilella V., Assaad M., and Debbah M. Low-complexity channel allocation scheme for URLLC traffic. *IEEE Trans. on Commun.*, 2020. doi:10.1109/TCOMM.2020.3022008
11. Manzoor A., Kazmi S. M. A., Pandey S. R., and Hong C. S. Contract-based scheduling of URLLC packets in incumbent EMBB traffic. *IEEE Access*, 2020, vol. 8, pp. 167516–167526. doi:10.1109/ACCESS.2020.3023128
12. Santos E. J., Souza R. D., Rebelatto J. L., and Alves H. Network slicing for URLLC and eMBB with max-matching diversity channel allocation. *IEEE Commun. Lett.*, 2020, vol. 24, no. 3, pp. 658–661.
13. Korrai P. K., Lagunas E., Sharma S. K., Chatzinotas S., and Ottersten B. Slicing based resource allocation for multiplexing of eMBB and URLLC services in 5G wireless networks. *IEEE CAMAD*, Sep. 2019, pp. 1–5.
14. Mo Y., Goursaud C., and Gorce J. Uplink multiple base stations diversity for UNB based IoT networks. *IEEE Conference on Antenna Measurements Applications (CAMA)*, 2018, pp. 1–4.
15. Kassab R., Simeone O., Popovski P. and Islam T. Non-orthogonal multiplexing of ultra-reliable and broadband services in fog-radio architectures. *IEEE Access*, 2019, vol. 7, pp. 13035–13049. doi: 10.1109/ACCESS.2019.2893128
16. Chraiti M., Ghrayeb A., and Assi C., A NOMA scheme exploiting partial similarity among users bit sequences. *IEEE Trans. on Commun.*, 2018, vol. 66, no. 10, pp. 4923–4935.
17. Yang Y., Chen W., Li O., Ke K., and Hanzo L. Trellis- and network-coded modulation for decode-and-forward two-way relaying over time-varying channels. *IEEE Trans. Veh. Technol.*, 2017, vol. 66, no. 6, pp. 4845– 4858. doi:10.1109/TVT.2016.2615656
18. Ungerboeck G. Channel coding with multilevel/phase signals. *IEEE Trans. Inf. Theory.*, 1982, vol. 28, no. 1, pp. 55–67. doi:10.1109/TIT.1982.1056454
19. Goldsmith J., Chua S. G. Adaptive coded modulation for fading channels. *IEEE Trans. Commun.*, 1998, vol. 46, no. 5, pp. 595–602. doi: 10.1109/ICC.1997.595036
20. Goldsmith J. *Wireless communications*. Cambridge, UK, Cambridge Univ. Press, 2005. 644 p. doi:10.1017/CBO9780511841224
21. Pastushok I. A., Boikov N. A., and Yankovskii N. A. Bit stream multiplexing in 5G networks. *Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, Saint-Petersburg, Russia, 2020, pp. 1–4. doi:10.1109/WECONF48837.2020.9131511

УДК 621.396
doi:10.31799/1684-8853-2021-2-52-59

О мультиплексировании потоков данных с использованием решетчатого кодирования в централизованных беспроводных сетях

Н. А. Янковский[a], студент, orcid.org/0000-0001-5783-8304
И. А. Пастушок[a], канд. техн. наук, доцент, orcid.org/0000-0002-3296-562X, igpastushok@gmail.com
[a]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ

Введение: распространение сервисов и приложений, требующих сверхнизкой задержки и высокой надежности передачи данных в сетях связи, приводит к необходимости создания новых подходов и архитектур для обеспечения одновременной передачи разнородного трафика улучшенной широкополосной связи (eMBB) и сверхнадежной связи с низкими задержками (URLLC). Одной из самых актуальных задач в области разработки стандартов беспроводной связи является обеспечение мультиплексирования потоков eMBB и URLLC с требуемыми показателями производительности передачи каждого потока. **Цель:** обеспечить одновременную передачу потоков eMBB и URLLC без потерь пользовательского опыта сервисов eMBB путем создания метода мультиплексирования потоков данных на основе решетчатого кодирования и модуляции сигнала, а также соответствующую настоящему методу архитектуру физического и канального уровней беспроводных централизованных сетей связи. **Результат:** предложены метод мультиплексирования потоков данных eMBB и URLLC в нисходящем канале связи, а также согласованная с ним архитектура физического и канального уровней сетей, позволяющие обеспечить заданные требования функционирования беспроводной сети. Оценка эффективности представленного решения путем имитационного моделирования дает возможность сделать следующие утверждения. Разработанный метод мультиплексирования обеспечивает лучшие значения вероятностей ошибки на бит и на кодовое слово в сравнении с опорным сценарием на физическом уровне. Предложенная архитектура канального уровня позволяет обеспечить передачу потока URLLC с интенсивностью 400 сообщений в миллисекунду с вероятностью доставки сообщения, равной 99% , в течение одной миллисекунды. **Практическая значимость:** полученные результаты помогут разработчикам систем связи планировать развертывания беспроводных централизованных сетей в промышленности.

Ключевые слова — URLLC, eMBB, мультиплексирование, планирование, беспроводные централизованные сети, решетчатое кодирование и модуляция, LDPC.

Для цитирования: Yankovskii N. A., Pastushok I. A. On multiplexing data streams using trellis-coded modulation in centralized wireless networks. *Информационно-управляющие системы*, 2021, № 2, с. 52–59. doi:10.31799/1684-8853-2021-2-52-59
For citation: Yankovskii N. A., Pastushok I. A. On multiplexing data streams using trellis-coded modulation in centralized wireless networks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 52–59. doi:10.31799/1684-8853-2021-2-52-59

UDC 004.94
doi:10.31799/1684-8853-2021-2-60-71

Articles

Development and application of problem-oriented digital twins for magnetic observatories and variation stations

A. V. Vorobev[a,b], *PhD, Tech., Associate Professor, orcid.org/0000-0002-9680-5609, geomagnet@list.ru*
V. A. Pilipenko[b,c], *Dr. Sc., Phys.-Math., Principal Researcher, orcid.org/0000-0003-3056-7465*
G. R. Vorobeva[a], *PhD, Tech., Associate Professor, orcid.org/0000-0001-7878-9724*
O. I. Khristodulo[a], *Dr. Sc., Tech., Associate Professor, orcid.org/0000-0002-3987-6582*
[a]*Ufa State Aviation Technical University, 12, K. Marx St., 450008, Ufa, Russian Federation*
[b]*Geophysical Center of the RAS, 3, Molodezhnaya St., 119296, Moscow, Russian Federation*
[c]*Institute of Physics of the Earth of the RAS, 10, b. 1, B. Gruzinskaya St., 123995, Moscow, Russian Federation*

Introduction: *Magnetic stations are one of the main tools for observing the geomagnetic field. However, gaps and anomalies in time series of geomagnetic data, which often exceed 30% of the number of recorded values, negatively affect the effectiveness of the implemented approach and complicate the application of mathematical tools which require that the information signal is continuous. Besides, the missing values add extra uncertainty in computer simulation of dynamic spatial distribution of geomagnetic variations and related parameters.* ***Purpose:*** *To develop a methodology for improving the efficiency of technical means for observing the geomagnetic field.* ***Method:*** *Creation of problem-oriented digital twins of magnetic stations, and their integration into the collection and preprocessing of geomagnetic data, in order to simulate the functioning of their physical prototypes with a certain accuracy.* ***Results:*** *Using Kilpisjärvi magnetic station (Finland) as an example, it is shown that the use of digital twins, whose information environment is made up of geomagnetic data from adjacent stations, can provide the opportunity for reconstruction (retrospective forecast) of geomagnetic variation parameters with a mean square error in the auroral zone of up to 11.5 nT. The integration of problem-oriented digital twins of magnetic stations into the processes of collecting and registering geomagnetic data can provide automatic identification and replacement of missing and abnormal values, increasing, due to the redundancy effect, the fault tolerance of the magnetic station as a data source object. For example, the digital twin of Kilpisjärvi station recovers 99.55% of annual information, and 86.73% of it has an error not exceeding 12 nT.* ***Discussion:*** *Due to the spatial anisotropy of geomagnetic field parameters, the error at the digital twin output will be different in each specific case, depending on the geographic location of the magnetic station, as well as on the number of the surrounding magnetic stations and the distance to them. However, this problem can be minimized by integrating geomagnetic data from satellites into the information environment of the digital twin.* ***Practical relevance:*** *The proposed methodology provides the opportunity for automated diagnostics of time series of geomagnetic data for outliers and anomalies, as well as restoration of missing values and identification of small-scale disturbances.*

Keywords *— digital twins, time series reconstruction, statistical analysis, geomagnetic data, magnetic stations.*

For citation: Vorobev A. V., Pilipenko V. A., Vorobeva G. R., Khristodulo O. I. Development and application of problem-oriented digital twins for magnetic observatories and variation stations. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 60–71. doi:10.31799/1684-8853-2021-2-60-71

Introduction

Today, magnetic observatories and variation stations are among the main instruments for observing the geomagnetic field (GMF) and its variations. There are more than 300 ground magnetic stations that record the parameters of the GMF in real time mode. Usually, these magnetic stations are integrated into networks, which for the data consumers are represented as the specialized web-services that provide access to geomagnetic data and have the functionality necessary for their search, preview and download. By the end of 2020, more than 20 such networks of magnetic stations are known, the largest of which are INTERMAGNET, IMAGE, CARISMA, MACCS, MAGDAS, etc.

Outliers, gaps in time series, noise and other anomalies are widespread and still not having a final solution to the problem on the way of processing the received geophysical information. Even for magnetic observatories of the INTERMAGNET network [1, 2], which maintains the highest quality standard, the lengths of the missing fragments occupy a fairly wide range and vary both in time and from station to station. For example, in 2015 the quantity of missing values for station AlmaAta was 36% of the annual operating time, for station Dalat it was more than 12%, for station Sodankyla it was 0.4%, etc. [3].

Multiple anomalies in time series (occurring as a result of measurement errors, registration or noisy information signal), in addition to negatively affecting the efficiency of the implemented

approach to monitoring GMF, also complicate the use of software elements that require compliance with the condition of information signal continuity (calculation of the derivative, Fourier transform, wavelet transform, etc.). In addition, the missing values complicate the problems of computer modeling of the dynamics of the spatial distribution of GMF variations [4, 5] and associated high-level experimental information (indices of geomagnetic activity, perturbation maps, magnetic keograms, etc.) [6].

Until recently, the reconstruction of the GMF observations results was provided by using a linear interpolation or a cubic spline, which is generally acceptable to recover the single gaps, but absolutely unsuitable for imputing long-term fragments. Today more complex approaches to the reconstruction of this type of time series are known. They are based mainly on analytical processing of data in the vicinity of missing fragments, analysis of periodic and seasonal components, as well as the study of Fourier and wavelet spectra of the information signal [7–11]. Usually all of them can be used to reconstruct the missing fragments, which size does not exceed several tens of minutes. The methods provide a methodological error within 15%, require significant computing power, direct human participation and, as a result, are not applicable to large amounts of data. Thus, the existing practice of collecting and registering geomagnetic data using ground magnetic stations is connected with a number of difficulties and limitations, which largely impede the effective conduct of geophysical/heliogeophysical research.

A promising approach to solving the problem can be the creation and integration the problem-oriented digital twins (DT) of magnetic stations into the process of collecting geomagnetic data. The DT allow with a certain accuracy (at the data consumer level) to simulate the work of their physical prototypes [12, 13]. The implementation and development of the proposed concept can significantly increase the efficiency of the operation of separate magnetic stations, as well as reduce the labor intensity of preliminary processing of geomagnetic data.

Analysis of gaps in time series of geomagnetic data and assessment of reliability indicators of ground magnetic stations

An experimental set is provided by the minute data of the IMAGE magnetometer network (https://space.fmi.fi/image/) [14] for 2015, that is the period corresponding to the maximum activity of the 24th solar cycle (January 2009–May 2020).

Table 1 describes the results of assessing the completeness of the time series of 36 stations, where the appearance of a missing value is regarded as a failure of a technical object, i. e., its transition to an inoperative state (State Standard 27.002-2015). Hence, the total idle time TF of the station, corresponding to the number of missing values in the time series, is determined as follows:

$$T_F = T - T_W, \quad (1)$$

where T is an operating time; T_W is a number of informative values (total uptime) for a time period T.

The average time to recover the operating state (equivalent to the mathematical expectation of the missing fragment size) and the average time to failure of the system (equivalent to the average size of the fragment without gaps) can be determined from next expressions:

$$\langle T2R \rangle = \frac{1}{N_F} \sum_{i=1}^{N_F} T2R_i = \frac{T_F}{N_F}; \quad (2)$$

$$\langle T2F \rangle = \frac{1}{N_W + k} \sum_{i=1}^{N_W + k} T2F_i = \frac{T_W}{N_W + k}, \quad (3)$$

where $T2R_i$ and $T2F_i$ are the time until the i-th system recovery after a failure and the time before the i-th system failure, respectively; N_F and N_W are the number of system failures and the number of failover recoveries, respectively; $k = 1$ or $k = 0$, if at the moment of observation beginning the system was in a working or inoperative state, respectively.

The analysis of gaps in the IMAGE network time series demonstrated that in 50% of magnetic stations the expected value of the missing fragment size exceeds 58.5 min. The averaged (over all stations) non-operational time is 1066 min/year. The expected value of the number of failures with recovery for all stations exceeds 45 per year. At the same time, 50% of stations experience more than 17 failures per year. In extreme cases, the total volume of missing fragments of one station can exceed 11.2% (more than 41 days) of the total size of the annual sample, while the average recovery time can reach 10 days or more.

The results indicate that the application of well-known approaches to the reconstruction of time series (linear interpolation, interpolation by cubic splines, as well as the methods described in [7–11]) for most fragments of the missing values of the sources considered here (mainly due to the size missing fragment) is ineffective. In addition, if we are talking about large amounts of information (the results of observing the parameters of the GMF

■ ***Table 1***. Assessment of reliability indicators of magnetic stations of the IMAGE network

IAGA code	Coordinates, degr.				T_W		T_F		N_F	<T2R>, min	<T2F>, min
	GEO		CGM								
	LAT	LON	LAT	LON	min	%	min	%			
NAL	78.92	11.95	76.57	109.96	509551	96.947	16049	3.053	20	802.45	25477.55
LYR	78.20	15.82	75.64	111.03	506314	96.331	19286	3.669	11	1753.27	46028.55
HOR	77.00	15.60	74.52	108.72	466554	88.766	59046	11.234	4	14761.5	116638.5
HOP	76.51	25.01	73.53	114.59	492524	93.707	33076	6.293	49	675.02	10051.51
BJN	74.50	19.20	71.89	107.71	525523	99.985	77	0.015	7	11	75074.71
NOR	71.09	25.79	68.19	109.28	519087	98.761	6513	1.239	144	45.23	3604.77
SOR	70.54	22.22	67.80	106.04	523740	99.646	1860	0.354	43	43.26	12180.0
KEV	69.76	27.01	66.82	109.22	525569	99.994	31	0.006	11	2.82	47779.0
TRO	69.66	18.94	67.07	102.77	524713	99.831	887	0.169	15	59.13	34980.87
MAS	69.46	23.70	66.65	106.36	524144	99.723	1456	0.277	73	19.95	7180.05
AND	69.30	16.03	66.86	100.22	525284	99.94	316	0.06	6	52.67	87547.33
KIL	69.06	20.77	66.37	103.75	523732	99.645	1868	0.355	33	56.61	15870.67
IVA	68.56	27.29	65.60	108.61	486940	92.645	38660	7.355	6	6443.33	81156.67
ABK	68.35	18.82	65.74	101.70	525600	100	0	0	0	–	–
MUO	68.02	23.53	65.19	105.23	492390	93.682	33210	6.318	359	92.51	1371.56
KIR	67.84	20.42	65.14	102.62	525577	99.996	23	0.004	13	1.77	40429.0
SOD	67.37	26.63	64.41	107.33	524905	99.868	695	0.132	12	57.92	43742.08
PEL	66.90	24.08	64.03	104.97	491992	93.606	33608	6.394	8	4201.0	61499.0
JCK	66.40	16.98	63.82	98.94	516366	98.243	9234	1.757	36	256.5	14343.5
DON	66.11	12.50	63.75	95.19	511710	97.357	13890	2.643	19	731.05	26932.11
RAN	65.90	26.41	62.92	106.30	519118	98.767	6482	1.233	130	49.86	3993.22
RVK	64.94	10.98	62.61	93.27	513440	97.686	12160	2.314	61	199.34	8417.05
LYC	64.61	18.75	61.87	99.33	525600	100	0	0	0	–	–
OUJ	64.52	27.23	61.47	106.27	525304	99.944	296	0.056	11	26.91	47754.91
MEK	62.77	30.97	59.57	108.66	511795	97.373	13805	2.627	23	600.22	22251.96
HAN	62.25	26.60	59.12	104.72	520619	99.052	4981	0.948	381	13.07	1366.45
DOB	62.07	9.11	59.64	90.19	524128	99.72	1472	0.28	19	77.47	27585.68
SOL	61.08	4.84	58.82	86.25	512471	97.502	13129	2.498	31	423.52	16531.32
NUR	60.50	24.65	57.32	102.35	525540	99.989	60	0.011	2	30.0	262770.0
UPS	59.90	17.35	56.88	95.95	525600	100	0	0	0	–	–
KAR	59.21	5.24	56.70	85.69	524637	99.817	963	0.183	41	23.49	12796.02
TAR	58.26	26.46	54.88	103.11	525137	99.912	463	0.088	12	38.58	43761.42
BRZ	56.17	24.86	52.66	100.97	523584	99.616	2016	0.384	3	672.0	174528.0
SUW	54.01	23.18	50.21	98.95	487904	92.828	37696	7.172	20	1884.8	24395.2
WNG	53.74	9.07	50.15	86.75	525577	99.996	23	0.004	19	1.21	27661.95
NGK	52.07	12.68	48.03	89.28	525600	100	0	0	0	–	–

Note: GEO is a geographic coordinate system; CGM (Corrected GeoMagnetic) is a geomagnetic coordinate system; the magnetic stations of the auroral cluster are highlighted in gray.

for one year or more), then the application of methods, in the algorithms of which the participation of a person is provided, also becomes very complicated.

Synthesis, modification and validation of digital twin models

The physical prototype of DT is considered as a magnetometric module that registers the northern component (*X*-component) of the GMF vector at the Kilpisjärvi (KIL) station. The research here is considered with spatial clustering of the entire set of magnetic stations in order to identify the reference data sources for subsequent modeling of the parameter.

Assessment of the spatial homogeneity of geographic objects based on the Moran's index for geographic proximity according to the metric [15] revealed between a number of stations located in the range of 66–71° N (see Table 1), the presence of a positive spatial autocorrelation, which indicates that these stations belong to the same spatial cluster with KIL (hereinafter referred to as the "auroral cluster").

A comparative analysis of the correlations of the northern (*X*) component of the geomagnetic disturbance vector of the KIL station with similar parameters of other stations of the auroral cluster (Table 2), as well as a number of additional studies [16, 17] confirmed the validity of the assumption and indicate the possibility of using these data as predicates (features) for modeling the parameter X_{KIL}.

Estimation of the coefficient of determination ($R^2 = 0.999$) demonstrated that for the problem being solved, the approach based on the method of multiple linear regression is the best. Linear regression equation that allows to restore the value of the desired parameter $f(x, \beta)$ from the known values $x_1, \ldots, x_k$ has the form:

$$f(x, \beta) = \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_k x_k = \sum_{j=1}^{k} \beta_j x_j = \mathbf{x}^{\mathrm{T}} \beta, \quad (4)$$

where $\mathbf{x}^{\mathrm{T}} = (x_1, x_2, \ldots, x_k)$ is a vector of regressors; $\hat{\boldsymbol{\beta}} = (\beta_1, \beta_2, \ldots, \beta_k)^{\mathrm{T}}$ is a vector column of coefficients; k is a number of model features.

Taking into account the data in Table 2, it is possible to define the expression (4) as follows:

$$\begin{aligned} X^*_{\text{KIL}} = \alpha + \beta_1 X_{\text{NOR}} + \beta_2 X_{\text{NOR}} + \beta_3 X_{\text{NOR}} + \\ + \beta_4 X_{\text{NOR}} + \beta_5 X_{\text{MAS}} + \beta_6 X_{\text{AND}} + \beta_7 X_{\text{IVA}} + \\ + \beta_8 X_{\text{ABK}} + \beta_9 X_{\text{MUO}} + \beta_{10} X_{\text{KIR}} + \\ + \beta_{11} X_{\text{SOD}} + \beta_{12} X_{\text{PEL}} + \beta_{13} X_{\text{JCK}} + \beta_{14} X_{\text{DON}}, \quad (5) \end{aligned}$$

where $\alpha = 418$ nT is an ordinate offset; β_1, β_2, ..., β_{14} are the coefficients calculated by the least squares method: $\beta_1 = -0.0511992$; $\beta_2 = -0.0791793$; $\beta_3 = 0.011932$; $\beta_4 = 0.5858979$; $\beta_5 = -0.2199333$; $\beta_6 = -0.203925$; $\beta_7 = 0.1138129$; $\beta_8 = 0.6873423$; $\beta_9 = 0.0020214$; $\beta_{10} = -0.2845333$; $\beta_{11} = 0.0170759$; $\beta_{12} = 0.0152406$; $\beta_{13} = 0.0037965$; $\beta_{14} = -0.0263773$.

Mean squared error (MSE) of model (5), which is calculated using the cross-validation procedure, was 11.5 nT. This MSE corresponds to 0.51% of the range of X_{KIL} parameter values for 2015. Pearson's correlation coefficient ($r = 0.999$) and the results of Student's *t*-test (statistical criterion ≈ 0, *p*-value ≈ 1) indicate that the original (X_{KIL}) and synthesized (X^*_{KIL}) data are statistically indistinguishable and belong to the same sample. However, the probability of failure-free operation of model (5) is limited by the probability of failure of at least one of the stations included in the auroral cluster (see Table 1) and, according to the available data, is 77.4%.

■ ***Table 2***. Correlations between X_{KIL} and a similar parameter of other stations

Magnetic stations included in the auroral cluster				Magnetic stations not included in the auroral cluster					
Code	*r*	Code	*r*	Code	*r*	Code	*r*	Code	*r*
NOR	0.872	ABK	0.986	NAL	−0.164	LYC	0.642	UPS	0.218
SOR	0.933	MUO	0.957	LYR	−0.129	OUJ	0.617	KAR	0.142
KEV	0.978	KIR	0.958	HOR	0.015	MEK	0.432	TAR	0.176
TRO	0.985	SOD	0.909	HOP	0.015	HAN	0.384	BRZ	0.098
MAS	0.99	PEL	0.875	BJN	0.427	DOB	0.363	SUW	−0.045
AND	0.987	JCK	0.845	RAN	0.053	SOL	0.262	WNG	−0.017
IVA	0.975	DON	0.820	RVK	0.694	NUR	0.274	NGK	−0.044

It is possible to increase the reliability of the DT by modifying the model (5), for example, by using the LASSO method [18, 19]. The method is concerned with identifying the constraints of norm of a vector of coefficients of the model, which will lead to zero of some of its coefficients, i. e., in fact, the exclusion of one or more stations from expression (5). Also, an important positive effect arising from the use of the LASSO method is an increase in the stability and interpretability of the model, since, as a result, the features that have the greatest influence on the response vector are selected. In other word, at a zero value of the regularization parameter λ, the LASSO regression is reduced to the least squares (LS) method, and with its increase, the formed model becomes more and more "laconic" until it degenerates into the so-called null model, which gives the same output for all possible inputs [20]. This can be seen from the expression

$$\hat{\beta}_{\text{LASSO}} = \arg\min_{\beta}\left(\sum_{i=1}^{n}\left(y_i - \sum_{j=1}^{k}\beta_j x_{ij}\right)^2 + \lambda|\beta|\right), \quad (6)$$

where y is an expected model response.

At $\lambda = 1$, it is possible to reduce expression (5) to 3 terms (β_3, β_9, $\beta_{12} = 0$), thereby increasing the probability of the model triggering to 86.3%, while practically without losing accuracy (MSE ~ 12 nT) and maintaining the correlation parameters and the statistical homogeneity of the original and synthesized samples at the model level (5). It is even more significant to increase the probability of the model triggering, possibly excluding the maximum number of terms from expression (5), while controlling the constancy of the correlation parameter and the Student's t-test results, as well as keeping the MSE in some acceptable range, for example, MSE ≤ 30 nT.

However, according to previous experience, the implementation of this operation by simply increasing the parameter λ is ineffective and leads to a significant increase in the simulation error with a relatively small decrease in the number of its terms. In other words, further application of machine optimization methods (including ridge regression and Elastic Net [21]) is impractical, and the subsequent minimization of the number of features should be done manually, for example, by pairwise comparative analysis of the statistics of available predicates. For this purpose, we exclude the baseline from the time series of each station, normalize the histogram and on the basis of by Kolmogorov — Smirnov criteria select for the obtained samples $|\Delta X|$ the function that best approximates the distribution of its values. The function, in turn, in addition to the homogeneity of general samples, may indicate the homogeneity of the physical mechanisms responsible for the appearance of disturbances at the points of their observation [16]:

$$\left|\Delta X_{ij}\right| = \left|X_{ij} - \text{Me}\left(X_j\right)\right|, \quad (7)$$

where X_{ij} is the i-th value for j-th day of X-component at the station; Me(X_j) is a sample median X for j-th day; i and j correspond to the ordinal numbers of a minute in a day (from 1 to 1440) and a day in a year (from 1 to 365), respectively.

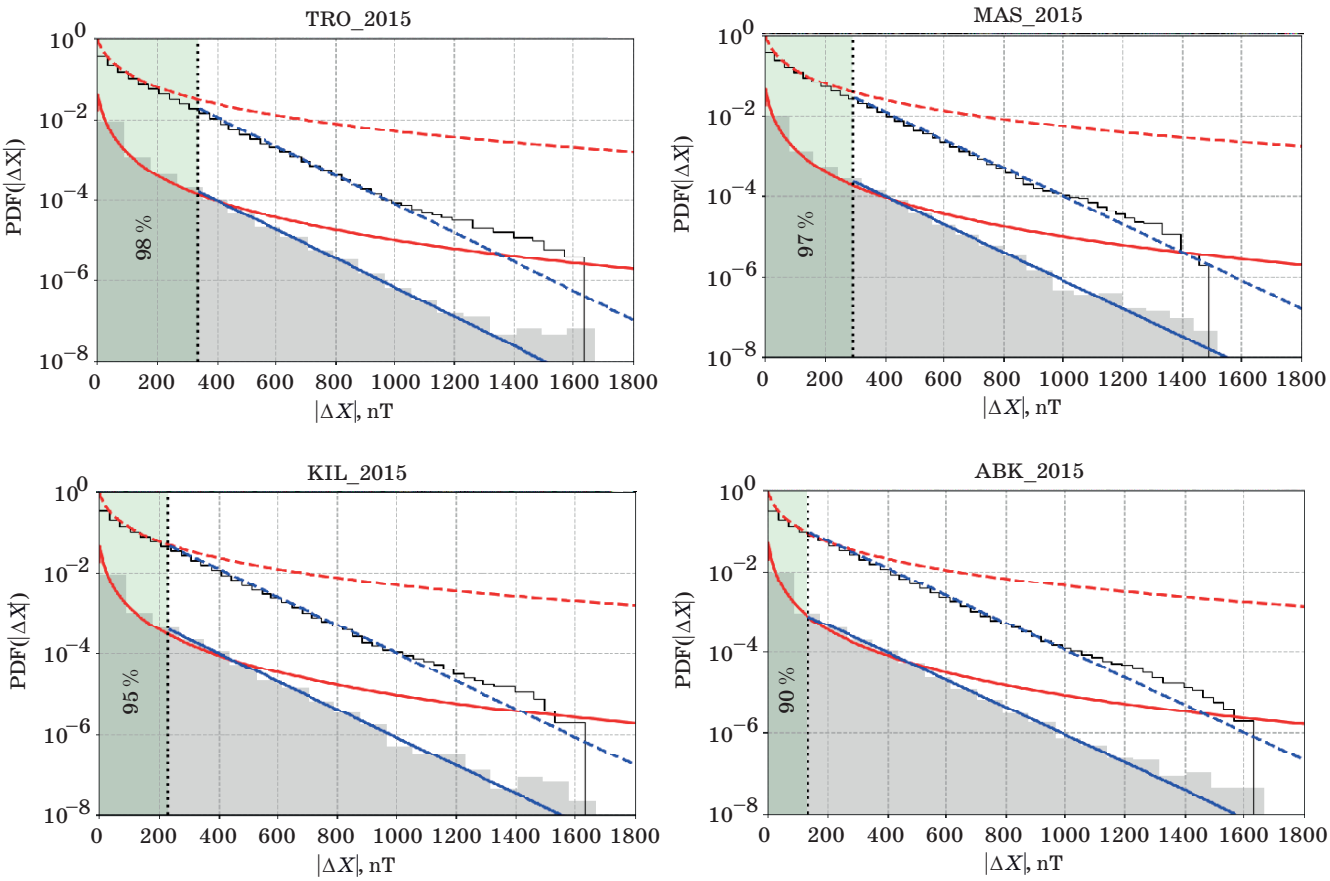
Analysis of the disturbed (i. e., in this case, excluding the daily variations of the GMF) X-components of the GMF at the KIL station ($|\Delta X|_{\text{KIL}}$) absolute values distribution demonstrated that most of the sample values are distributed according to the lognormal law (Fig. 1). However, starting from the 95th percentile, an exponential tail is observed, indicating that the variance of the studied value is determined mainly by rare intense (rather than frequent small) deviations, apparently in this case due to substorm activity. Further research demonstrated that the samples statistically closest to $|\Delta X|_{\text{KIL}}$ are $|\Delta X|_{\text{TRO}}$, $|\Delta X|_{\text{MAS}}$ and $|\Delta X|_{\text{ABK}}$, which are the absolute values of the disturbed components of the GMF X-component at stations Tromsø (TRO), Masi (MAS) and Abisko (ABK). In this case, almost the only difference is the sample percentile corresponding to the beginning of the exponential tail, which is apparently determined by the latitudinal location of a particular station (see Fig. 1, Table 1).

In addition, analysis of correlation between the regional IL-index (the intensity of the western auroral electrojet, i. e., the horizontal current flowing in the auroral region of the ionosphere) and the X-component of the four stations identified (see Fig. 1) revealed the proportionality of these correlations (in each case, the Pearson correlation coefficient is ~0.7), which again indicates that the stations under consideration are equally affected by the same external factors. Thus, datasets including data of TRO, MAS and ABK stations, are best suited for modeling the desired parameter. In this case, obviously, the minimum set of data sources can only consist of these stations. Taking this into account, expression (5) can be reduced to the following:

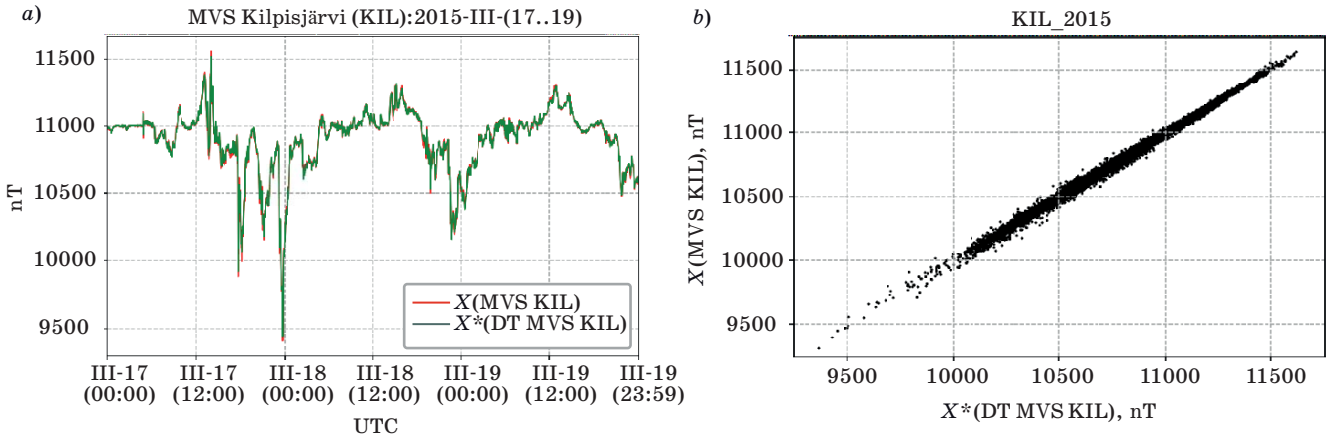
$$X^*_{\text{KIL}} = \alpha + \beta_4 X_{\text{NOR}} + \beta_5 X_{\text{MAS}} + \beta_8 X_{\text{ABK}}, \quad (8)$$

where $\alpha = 248.719$ nT; $\beta_4 = 0.2914795$; $\beta_5 = 0.286204$; $\beta_8 = 0.4405047$.

Figure 2, *a* represents the magnetograms of the initial time series and time series reconstructed on the basis of the regression model (8), which includes one of the most powerful magnetic storms over the past few years of observations. The dispersion of the simulation results can be estimated from the



■ ***Fig. 1.*** Statistics of the disturbed geomagnetic variations: red and blue solid (dashed) lines correspond to the probability density functions (survival) of the lognormal and exponential distribution laws, respectively; black solid line — empirical survival function; PDF — probability density function



■ ***Fig. 2.*** Verification of the digital twin of the station KIL: *a* — magnetograms of the initial time series; *b* — magnetograms of the time series reconstructed on the basis of the regression model

scattering diagram is demonstrated in Fig. 2, *b*. The probability of triggering a DT based on model (8) is 99.5%, and MSE < 30 nT (Table 3).

It should be noted that methods based on geospatial interpolation may be a possible alternative, and in some situations the only approach to creating a DT. For example, according to the Inverse Distance Weighting (IDW) method [22], the interpolated value of the parameter at a given geographical point is determined by the weighted average sum of deterministic values in its vicinity. In the case of Shepard's modification [22], the level of influence of the deterministic point on the desired value is set by the exponent p and with distance from the top of

■ ***Table 3.*** KIL station digital twin model validation parameters

Model	MSE, nT	MSE, %	r	Student's t-test		T_W, min	T_F, min	P_W, %
				Statistic	p-value			
Expr. (5), LS	11.5	0.51	0.999	~0	~1	406936	118664	77.423
Expr. (5), LASSO	12.0	0.54	0.999	~0	~1	453819	71781	86.343
Expr. (8), LASSO	28.9	1.25	0.999	~0	~1	523257	2343	99.554
Expr. (9), IDW ($p = 3$)	114.1	4.94	0.995	~0	~1	406936	118664	77.423

Note: P_W is the expected probability of the model being triggered.

the polygon, including the reference data sources, its influence on the interpolated value weakens. For the case under consideration, the ratio of the IDW method is as follows:

$$X^*_{\text{KIL}} = \sum_{i=1}^{m} \frac{1}{d_i^p} X_i \Big/ \sum_{i=1}^{m} \frac{1}{d_i^p}, \qquad (9)$$

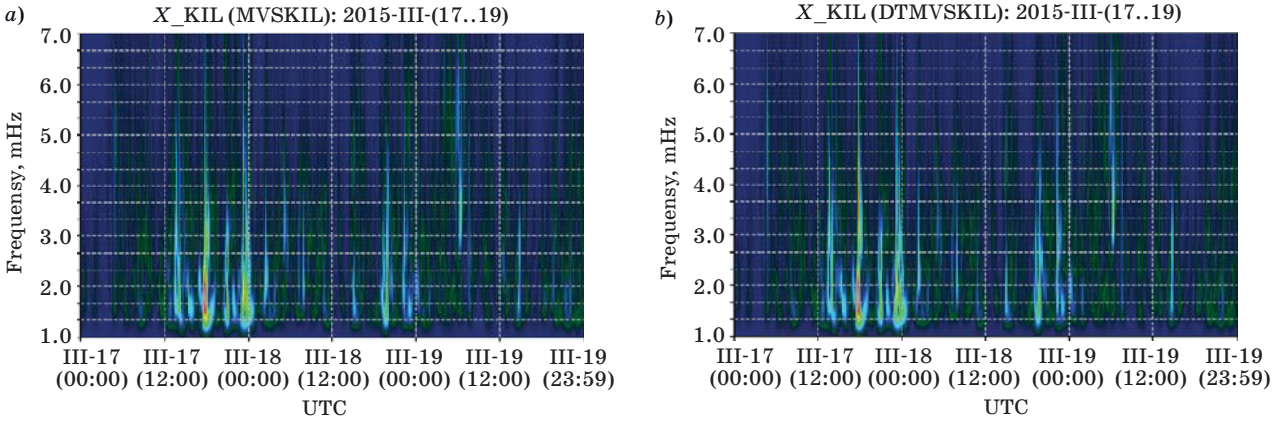
where m is a number of stations in the auroral cluster; d is a distance between the KIL station and the i-th station of the auroral cluster; p is a weight coefficient; X_i is a value of X-component of i-th station.

The disadvantage of the IDW method for interpolating geomagnetic disturbances is the assumption that the disturbance field is isotropic in it. However, here it should be taken into account that latitudinal and longitudinal scales of most geomagnetic disturbances differ significantly. Research results have shown that in relation to the problem under consideration, the MSE of the DT model built on the basis of the IDW method monotonically increases with decreasing p, which indicates that the sought parameter is determined mainly by the data of the stations closest to the modeled object. As a result, the modeling error by means of expression (9) will be slightly higher than the MSE of the regression models (see Table 3). However, despite this, the geospatial interpolation method can be useful in the absence of a response vector, i. e., in the situation when there is no physical prototype of the station.

Digital twin verification in frequency domain

Although variations in the GMF in the range of periods of 2–12 min significantly inferior in intensity to global geomagnetic disturbances — magnetic storms and substorms — they are still extremely important.

Disturbances in this frequency range (Pi3 / Ps6 pulsations, Pc5 waves, the beginnings of substorms) lead to the most powerful bursts of geoinduced currents in power lines. Therefore, an important aspect in the functioning of the DT is the identification and storage of information about these disturbances. Let us select by means of the Butterworth high-pass filter in the X_{KIL} and X^*_{KIL}



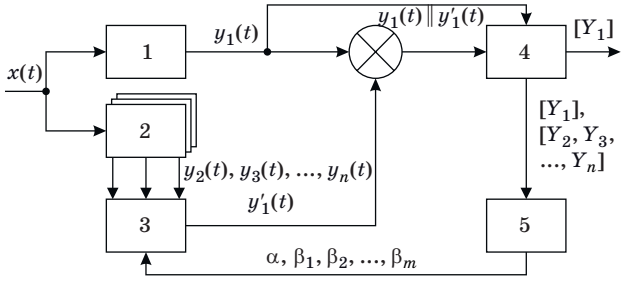
■ ***Fig. 3.*** Verification of the digital twin of the magnetic station KIL in the frequency range of 1–7 mHz: wavelet scalogram of original (*a*) and recovered (*b*) time series

Thus, from Fig. 3, *a* and *b* as well as from a number of similar tests for other fragments of the time series, it follows that in the region of ultra-low frequencies (with periods of 2–12 min), insignificant (within the limits of the error stated in Table 3) deviations of the amplitude are observed, while the spatial localization of frequency packets remains practically unchanged.

Integration of the digital twin into the process of collecting geomagnetic data

Figure 4 schematically demonstrates the model of integration of the DT of magnetic station into the processes of collecting and registering geomagnetic data. So, according to the proposed scheme, the disturbing effect $x(t)$ extends to the physical prototype of the magnetic station (1) and a number of reference data sources (2), involved in the base of the DT models (3).

Depending on the number m of stations available at the time t_i, a model that provides the minimum error is selected, by means of which the DT of the magnetic station (1) generates the corresponding value $y'_1(t_i)$. Further, the data corresponding to the state of the GMF at the i-th moment of time, from the output of the DT and its physical prototype, are sent to the comparison device, which, by comparing these values, makes a decision on registration as a measurement result or data from a magnetic station, for example, based on the fulfillment of the condition (10), or its DT (in cases of its failure), while the value of the magnetic station is also saved, however, it is marked as anomalous. If there is no output signal from the magnetic station, then the DC value is recorded as the measurement result. The verified values stored in the geomagnetic database (4) are structured in the form of response vectors and regressors and are used to update and adjust the vectors of coefficients of the DT models (5).



■ ***Fig. 4.*** Model of digital twin integration into the processes of collection and registration of geomagnetic data: *1* — magnetic station; *2* — reference magnetic stations; *3* — digital twin of the magnetic station; *4* — data base; *5* — machine learning system

$$\left|x_i - x_i^*\right| < 3\sigma \quad \text{or}$$

$$\left|x_i - x_i^*\right| < 3\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(\left(x_i - x_i^*\right) - \bar{x}\right)^2}, \qquad (10)$$

where σ is a standard deviation; x_i^* and x_i are the values of the digital twin and its physical prototype, respectively, at the i-th moment of time t.

Figure 5 on the example of the KIL station demonstrates an algorithm that explains the diagram shown in Fig. 4.

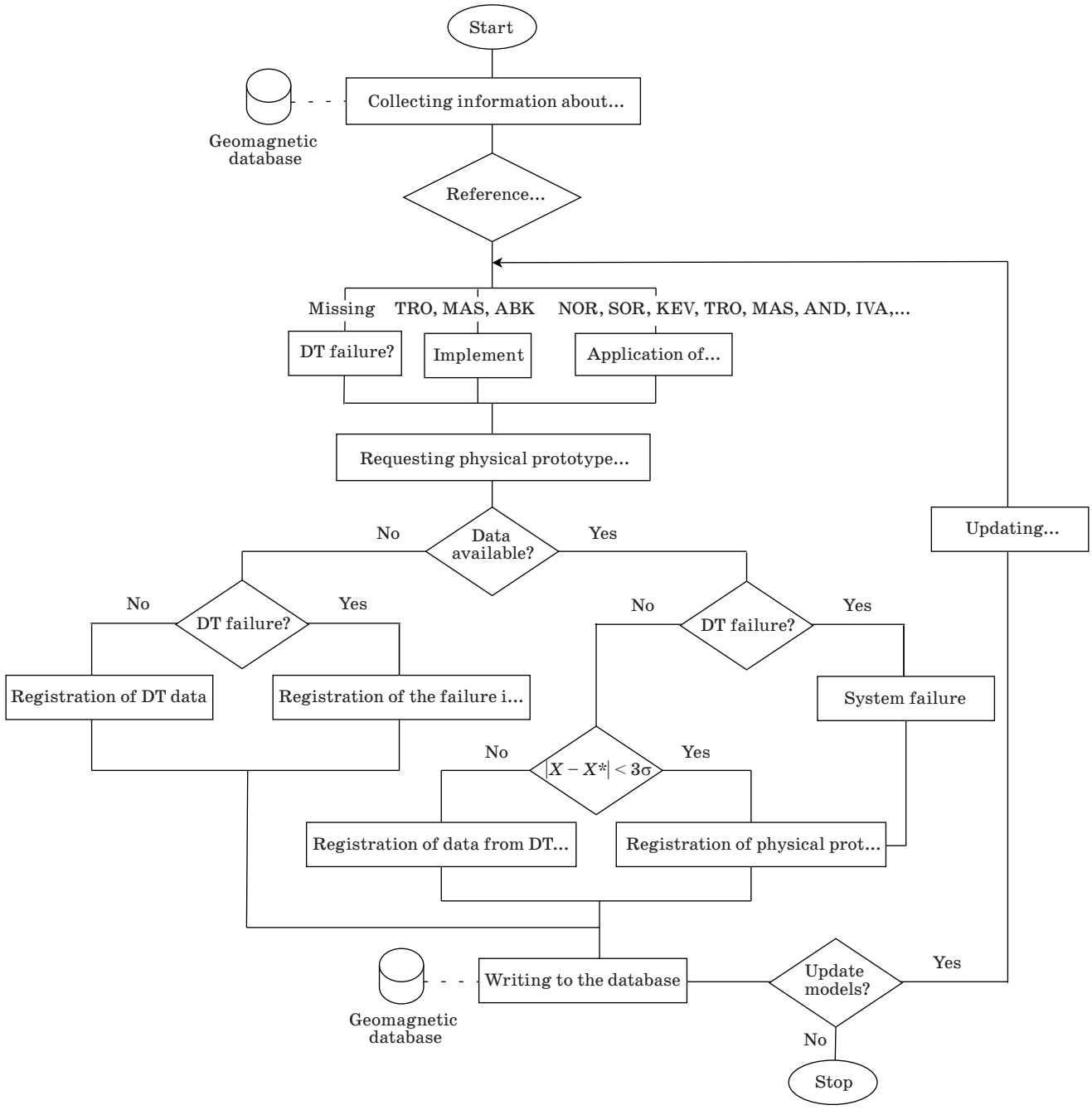
Thus, the application of the proposed scheme and algorithm in the case of the KIL station makes it possible to recover 99.55% of the data for 2015, while the MSE of 86.73% of the recovered values does not exceed 12 nT. As follows from the algorithm (see Fig. 5), the state of failure of the entire local system for collecting and registering geomagnetic data occurs with the simultaneous absence of a signal at the output of the magnetic station and its DT. For the KIL station, the calculated value of the probability of such an event occurring is less than 0.0016%, which corresponds to eight missing values per year, which, in turn, can be restored using linear interpolation methods.

Discussion of the results and prospects for their application

As has been shown, the introduction of magnetic station DT into the processes of collecting and registering geomagnetic data due to the redundancy effect can (at the data consumer level) significantly increase the reliability and fault tolerance of individual magnetometers, as well as reduce the labor intensity of preprocessing of geomagnetic data, for example, such as search and identification of outliers in time series.

However, when implementing the approach, it is necessary to take into account the limitations of its effective application, which are determined, first of all, by the spatial anisotropy of the GMF parameters. Thus, the MSE of the DT for each specific case (magnetic station) will differ, depending on the geographic location of this physical prototype, as well as the number and distance of the surrounding magnetic stations. At the same time, the general methodology for selecting reference stations, synthesis and optimization of regression models will practically not change.

A perspective in the development of virtual magnetic stations is the integration of GMF satellite observation data (for example, SWARM, CHAMP missions, etc.) into the information environment of the DT. It can be assumed that the implementation of the approach, in addition to the aggregation of ad-



■ ***Fig. 5.*** Algorithm of the process of geomagnetic data collecting and registering with the implementation of the digital twin on the example of the KIL magnetic station

ditional data required for the calibration (settings of models) of the DT of magnetic stations, can also weaken a number of methodological limitations of the effective use of the DTs, associated, for example, with the absence of nearby magnetic stations.

Speaking about the prospects of using the DT of magnetic stations, the following tasks should mainly be highlighted:

— reconstruction of geomagnetic data time series;

— automated search and identification of outliers in geomagnetic data time series;

— collection of geomagnetic data in conditions where the use of physical magnetic stations is unacceptable or ineffective, for example, in the immediate vicinity of objects that have a strong noisy effect on magnetic sensors and primary measuring transducers (trunk pipelines, power lines, railway and oil and gas infrastructure facilities, etc.).

— information support of the processes of directional drilling of deep wells in the Arctic zone of the Russian Federation [23, 24].

Also, it should be noted here that DTs have the potential to be used in problems of machine search and identification of localized GMF disturbances, for example, such as MPE (magnetic perturbation events), which are isolated bursts of field intensity with a duration of 5–15 min at night [25] and can be responsible for intense bursts of geoinduced currents in power lines [26]. The horizontal scale of such disturbances is ~200–300 km, and they are recorded, as a rule, at 1–2 stations of the network. Thus, DTs are able to automate this process by isolating disturbances that sharply differ from the model values.

Conclusion

In this paper (using the KIL magnetic station as an example), it is shown that the DTs of magnetic stations built on the basis of LASSO regression are capable of providing retrospective forecast and restoration of the *X*-component of the GMF vector in the auroral zone with a mean square error from 11.5 (in 77.4% of cases) to 29 nT (in 99.6% of cases) depending on the number of reference stations used.

Comparative analysis of wavelet spectrograms of data from the magnetic station DT and its physical prototype in the frequency range with periods of 2–12 min (Pi3 / Ps6 pulsations, Pc5 waves, the onset of substorms) showed that in the amplitude region of the information signal there may be minor differences commensurate with modeling error, however, the spatial localization of frequency packets remains practically unchanged.

In the absence of a physical prototype of the magnetic station (the response vector of the training sample), the implementation of the DT is possible on the basis of spatial interpolation methods, but here one should expect a slightly larger (compared to the regression approach) modeling error.

The main factors limiting the effectiveness of the proposed approach are the specifics of the geographic location of a particular physical prototype, as well as the number and distance of nearby magnetic stations. It is possible to minimize the influence of these factors by expanding the information environment of the DT, for example, by aggregating data from satellite observations of the GMF.

Financial support

This work was supported by a grant from the Russian Science Foundation No. 21-77-30010, and also partially supported by grants from the Russian Foundation for Basic Research No. 20-07-00011-a and the Expert Center “Project Office for the Development of the Arctic” (Agreement No. 217-G dated January 13, 2021).

Acknowledgements

We thank the institutes who maintain the IMAGE Magnetometer Array: Tromsø Geophysical Observatory of UiT the Arctic University of Norway (Norway), Finnish Meteorological Institute (Finland), Institute of Geophysics Polish Academy of Sciences (Poland), GFZ German Research Centre for Geosciences (Germany), Geological Survey of Sweden (Sweden), Swedish Institute of Space Physics (Sweden), Sodankylä Geophysical Observatory of the University of Oulu (Finland), and Polar Geophysical Institute (Russia).

References

1. Love J. An international network of magnetic observatories. *EOS, Transactions, American Geophysical Union*, 2013, vol. 94, no. 42, pp. 373–384.
2. Khomutov S. Yu. International project INTERMAGNET and magnetic observatories of Russia: cooperation and progress. *E3S Web of Conferences*, 2018, no. 62, pp. 02008. doi:10.1051/e3sconf/2018620
3. Vorobev A. V., Vorobeva G. R. Approach to assessment of the relative informational efficiency of INTERMAGNET magnetic observatories. *Geomagnetism and Aeronomy*, 2018, vol. 58, no. 5, pp. 648–652 (In Russian). doi:10.1134/S0016793218050158
4. Vorobev A. V., Pilipenko V. A., Enikeev T. A., Vorobeva G. R. Geoinformation system for analyzing the dynamics of extreme geomagnetic disturbances from observations of ground stations. *Computer Optics*, 2020, vol. 44, no. 5, pp. 782–790 (In Russian). doi:10.18287/2412-6179-CO-707
5. Reich K., Roussanova E. Visualising geomagnetic data by means of corresponding observations. *Int J Geomath*, 2013, no. 4, pp. 1–25. doi:10.1007/s13137-012-0043-4
6. Gvishiani A. D., Lukianova R. Yu., Soloviev A. A. *Geomagnetizm: ot yadra Zemli do Solnca* [Geomagnetism: from the core of the Earth to the Sun]. Moscow, Rossijskaya akademiya nauk Publ., 2019. 186 p. (In Russian).
7. Gvishiani A. D., Agayan S. M., Bogoutdinov Sh. R., Kagan A. I. Gravitational smoothing of time series. *Trudy Instituta matematiki i mekhaniki UrO RAN*, 2011, vol. 17, no. 2, pp. 62–70 (In Russian).
8. Mandrikova O. V., Soloviev I. S. Wavelet technology for processing and analyzing geomagnetic data. *Ci-*

frovaya obrabotka signalov, 2012, no. 2, pp. 24–28 (In Russian).
9. Mandrikova O. V., Solovyev I. S., Khomutov S. Y., Geppener V. V., Klionskiy D. M., Bogachev M. I. Multiscale variation model and activity level estimation algorithm of the Earth's magnetic field based on wavelet packets. *Ann. Geophys.*, 2018, no. 36, pp. 1207–1225. doi:10.5194/angeo-36-1207-2018
10. Kondrashov D., Shprits Y., Ghil M. Gap filling of solar wind data by singular spectrum analysis. *Geophys. Res. Lett.*, 2010, vol. 37, L15101, doi:10.1029/2010GL044138
11. Vorobev A. V., Vorobeva G. R. Inductive method of geomagnetic data time series recovering. *SPIIRAS Proceedings*, 2018, no. 2, pp. 104–133 (In Russian). doi:10.15622/sp.57.5
12. Parmar R., Leiponen A., Llewellyn D. W. T. Building an organizational digital twin. *Business Horizons*, 2020, vol. 63, no. 6, pp. 725–736. doi:10.1016/j.bushor.2020.08.001
13. Zongyan W. *Digital Twin Technology*. In: *Industry 4.0 — Impact on Intelligent Logistics and Manufacturing*. IntechOpen. Pp. 95–114. doi:10.5772/intechopen.80974
14. Tanskanen E. I. A comprehensive high-throughput analysis of substorms observed by IMAGE magnetometer network: Years 1993–2003 examined. *J. Geophys. Res.*, 2009, no. 114, p. A05204. doi:10.1029/2008JA013682
15. Demyanov V. V., Savelyeva E. A. *Geostatistika. Teoriya i praktika* [Geostatistics. Theory and practice]. Moscow, Nauka Publ., 2010. 327 p. (In Russian).
16. Vorobev A., Vorobeva G. *Properties and type of latitudinal dependence of statistical distribution of geomagnetic field variations*. In: *Kocharyan G., Lyakhov A. (eds). Trigger Effects in Geosystems. Springer Proceedings in Earth and Environmental Sciences*. Springer, Cham., 2019. Pp. 187–196. https://doi.org/10.1007/978-3-030-31970-0_22
17. Vorobev A. V., Vorobeva G. R. Correlation analysis of geomagnetic data synchronously recorded by the INTERMAGNET magnetic laboratories. *Geomagnetism and Aeronomy*, 2018, vol. 58, no. 2, pp. 187–193 (In Russian). doi:10.1134/S0016793218020196
18. She Yiyuan. Sparse regression with exact clustering. *Electron. J. Statist.*, 2010, vol. 4, pp. 1055–1096. doi:10.1214/10-EJS578
19. Hoerl R. W. Ridge regression: a historical context. *Technometrics*, 2020, vol. 62, no. 4, pp. 420–425. doi:10.1080/00401706.2020.1742207
20. Tokmakova A. A., Strijov V. V. Estimation of linear model hyperparameters for noise or correlated feature selection problem. *Informatics and Applications*, 2012, vol. 6, no. 4, pp. 66–75 (In Russian).
21. Zou H., Hastie T. Regularization and variable selection via the elastic net. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 2005, no. 67, pp. 301–320. doi:10.1111/j.1467-9868.2005.00503.x
22. Isaaks E. H., Mohan R. *An Introduction to Applied Geostatistics*. Oxford, Oxford University Press, 1989. 592 p.
23. Gvishiani A. D., Lukianova R. Yu. Study of the geomagnetic field and problems of accuracy of directional drilling in the Arctic region. *Izvestiya vysshikh uchebnykh zavedenii. Gornyi zhurnal*, 2015, no. 10, pp. 94–99 (In Russian). doi:10.17580/gzh.2015.10.17
24. Gvishiani A. D., Lukianova R. Yu. Estimating the influence of geomagnetic disturbances on the trajectory of the directional drilling of deep wells in the Arctic region. *Izvestiya. Physics of the Solid Earth*, 2018, no. 4, pp. 19–30 (In Russian). doi:10.1134/S0002333718040051
25. Engebretson M. J., Steinmetz E. S., Posch J. L., et al. Nighttime magnetic perturbation events observed in Arctic Canada: 2. Multiple-instrument observations. *Journal of Geophysical Research: Space Physics*, 2019, no. 124, pp. 7459–7476. https://doi.org/10.1029/2019JA026797
26. Datcu M., Le Moigne J., Loekken S., Soille P., Xia G.-S. Special issue on big data from space. *IEEE Transactions on Big Data*, 2020, vol. 6, no. 3, pp. 427–429. doi:10.1109/TBDATA.2020.3015536

УДК 004.94
doi:10.31799/1684-8853-2021-2-60-71

Методология создания и перспективы применения проблемно-ориентированных цифровых двойников магнитных обсерваторий и вариационных станций

А. В. Воробьев[а,б], канд. техн. наук, доцент, orcid.org/0000-0002-9680-5609, geomagnet@list.ru
В. А. Пилипенко[б,в], доктор физ.-мат. наук, главный научный сотрудник, orcid.org/0000-0003-3056-7465
Г. Р. Воробьева[а], канд. техн. наук, доцент, orcid.org/0000-0001-7878-9724
О. И. Христодуло[а], доктор техн. наук, доцент, orcid.org/0000-0002-3987-6582
[а]Уфимский государственный авиационный технический университет, К. Маркса ул., 12, Уфа, 450008, РФ
[б]Геофизический центр РАН, Молодежная ул., 3, Москва, 119296, РФ
[в]Институт физики Земли им. О. Ю. Шмидта РАН, Б. Грузинская ул., 10, стр. 1, Москва, 123995, РФ

Введение: магнитные станции являются одним из основных инструментов наблюдения геомагнитного поля, однако пропуски и аномалии во временных рядах геомагнитных данных, нередко превышающие 30 % от числа зарегистрированных значений, негативно отражаются на эффективности реализуемого подхода и затрудняют применение элементов математического обеспечения, требующих соблюдения условия непрерывности информационного сигнала. Кроме этого, отсутствующие значения вносят дополнительную неопределенность в задачах компьютерного моделирования динамики пространственного распределения параметров геомагнитных вариаций. **Цель:** разработать методологию повышения эффективности технических средств наблюдения геомагнитного поля. **Метод:** создание и интеграция в процессы сбора и предварительной обработки геомагнитных данных проблемно-ориентированных цифровых двойников магнитных станций, позволяющих с известной точностью имитировать функционирование их физических прототипов. **Результаты:** на примере магнитной станции Kilpisjärvi (Финляндия) показано, что использование цифровых двойников, информационную среду которых составляют геомагнитные данные окрестных станций, позволяет провести восстановление (ретроспективный прогноз) параметров геомагнитных вариаций со среднеквадратической ошибкой в авроральной зоне до 11,5 нТл. Интеграция проблемно-ориентированных цифровых двойников магнитных станций в процессы сбора и регистрации геомагнитных данных способна обеспечить автоматическую идентификацию и замещение отсутствующих и аномальных значений, повышая за счет эффекта резервирования отказоустойчивость магнитной станции как объекта-источника данных. Так, например, цифровой двойник станции Kilpisjärvi реализует восстановление 99,55 % годовой информации, из них 86,73 % с ошибкой, не превышающей 12 нТл. **Обсуждение:** по причине пространственной анизотропии параметров геомагнитного поля ошибка на выходе цифрового двойника для каждого конкретного случая будет отличаться в зависимости от географического местоположения магнитной станции, а также числа и удаленности окрестных магнитных станций. Однако данную проблему возможно минимизировать, интегрируя в информационную среду цифрового двойника геомагнитные данные спутниковых наблюдений. **Практическая значимость:** применение предложенной методологии делает возможными автоматизированную диагностику временных рядов геомагнитных данных на предмет выбросов и аномалий, а также восстановление отсутствующих значений и идентификацию мелкомасштабных возмущений.

Ключевые слова — цифровые двойники, восстановление временных рядов, статистический анализ, геомагнитные данные, магнитные станции.

Для цитирования: Vorobev A. V., Pilipenko V. A., Vorobeva G. R., Khristodulo O. I. Development and application of problem-oriented digital twins for magnetic observatories and variation stations. *Информационно-управляющие системы*, 2021, № 2, с. 60–71. doi:10.31799/1684-8853-2021-2-60-71

For citation: Vorobev A. V., Pilipenko V. A., Vorobeva G. R., Khristodulo O. I. Development and application of problem-oriented digital twins for magnetic observatories and variation stations. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 60–71. doi:10.31799/1684-8853-2021-2-60-71

X Всероссийская с международным участием научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем» — МЭС-2021

Март–ноябрь 2021 г.

Конференция МЭС является крупнейшей конференцией в области САПР микроэлектроники на территории России и стран СНГ.

Формат проведения
Онлайн

Организаторы
Институт проблем проектирования в микроэлектронике РАН (ИППМ РАН)
Корпорация развития Зеленограда (КПР)

Соорганизатор
Московское научно-техническое общество радиотехники, электроники и связи (МНТОРЭС) им. А. С. Попова

Учредители
Российская академия наук
Министерство науки и высшего образования Российской Федерации
Российский фонд фундаментальных исследований
Правительство г. Москвы
Префектура Зеленоградского АО г. Москвы
Южный федеральный университет

Направления работы
Теоретические аспекты проектирования микро- и наноэлектронных систем (МЭС)
Методы и средства автоматизации проектирования микро- и наноэлектронных схем и систем МЭС (САПР СБИС)
Опыт разработки цифровых, аналоговых, цифро-аналоговых, радиотехнических функциональных блоков СБИС
Особенности проектирования СБИС для нанометровых технологий
Системы на кристалле перспективной РЭА

Рабочие языки
Русский и английский

Оргвзнос
Участие в конференции МЭС-2021 бесплатное.

Публикация трудов
Принятые доклады будут опубликованы на web-сайте конференции, а также в четырех выпусках трудов конференции, которые будут издаваться по мере поступления, рецензирования и редакционной подготовки.
Сборник трудов конференции МЭС включен в Перечень ВАК российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней доктора и кандидата наук.
Как и в 2020 году, будут проведены конкурсы на лучшие доклады с призами для победителей.

Контрольные сроки
Прием докладов — с 01 марта по 01 августа 2021 г.

Дополнительная информация и справки
124365 Москва, Зеленоград, Советская ул., д. 3, Институт проблем проектирования в микроэлектронике РАН
Представитель Оргкомитета Ходош Лев Соломонович
Эл. адрес: khod@ippm.ru
Сайт: http://www.mes-conference.ru

АЛЕКСАШИН Александр Сергеевич

Магистрант факультета прикладной математики и информатики Новосибирского государственного технического университета.
В 2019 году окончил бакалавриат Новосибирского государственного технического университета по специальности «Прикладная математика и информатика».
Область научных интересов — метод граничных элементов, метод конечных элементов.
Эл. адрес:
aleksashin.a.s@yandex.ru

ВОЗНЮК Екатерина Сергеевна

Аспирант кафедры прикладной математики, младший научный сотрудник научно-исследовательской лаборатории моделирования и обработки данных наукоемких технологий Новосибирского государственного технического университета.
В 2017 году окончила Новосибирский государственный технический университет по специальности «Прикладная математика и информатика».
Область научных интересов — метод конечных элементов.
Эл. адрес: elfy@ami.nstu.ru

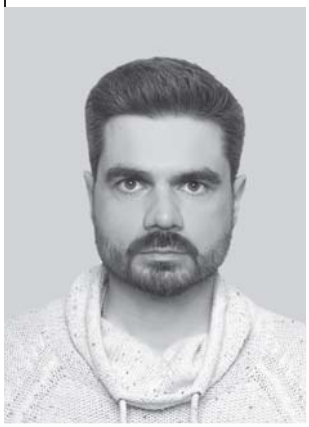
ВОРОБЬЕВА Гульнара Равилевна

Доцент кафедры вычислительной математики и кибернетики Уфимского государственного авиационного технического университета.
В 2005 году окончила Уфимский государственный авиационный технический университет по специальности «Автоматизированные системы обработки информации и управления».
В 2008 году защитила диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций и двух патентов на изобретения.
Область научных интересов — веб-технологии, веб-программирование, программная инженерия.
Эл. адрес:
gulnara.vorobeva@gmail.com

ВО Дык Хоанг

Преподаватель факультета информационных технологий Данангского университета науки и технологий, Данангский университет, Дананг, Вьетнам.
В 2006 году окончил Данангский университет науки и технологий по специальности «Информационные технологии».
В 2019 году защитил диссертацию на соискание ученой степени кандидата технических наук в Данангском университете.
Является автором десяти научных публикаций.
Область научных интересов — обработка изображений.
Эл. адрес:
hoangvd.it@dut.udn.vn

ВОРОБЬЕВ Андрей Владимирович



Доцент кафедры геоинформационных систем Уфимского государственного авиационного технического университета.
В 2006 году окончил магистратуру Уфимского государственного авиационного технического университета по специальности «Электроника и микроэлектроника».
В 2009 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций и четырех патентов на изобретения.
Область научных интересов — обработка и анализ пространственных данных, методы машинного обучения, геоинформационные системы и технологии.
Эл. адрес: geomagnet@list.ru

ЛУКИН Михаил Андреевич

Архитектор-разработчик ООО «Судо», доцент практики кафедры компьютерных технологий Университета ИТМО, Санкт-Петербург.
В 2009 году окончил Санкт-Петербургский государственный университет информационных технологий, механики и оптики по специальности «Прикладная математика и информатика».
В 2014 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 13 научных публикаций.
Область научных интересов — верификация программного обеспечения, статические анализаторы кода.
Эл. адрес:
lukinma@gmail.com

МИХАЙЛЕНКО Кристина Игоревна

Магистрант кафедры компьютерных технологий Университета ИТМО, Санкт-Петербург.
В 2020 году окончила бакалавриат Университета ИТМО по специальности «Прикладная математика и информатика».
Область научных интересов — методы декомпиляции, статический анализ.
Эл. адрес: Kristina.Mihajlenko@gmail.com

МОЛДОВЯН Николай Андреевич

Профессор, заведующий научно-исследовательским отделом проблем информационной безопасности Санкт-Петербургского института информатики и автоматизации РАН, заслуженный изобретатель РФ.
В 1975 году окончил Кишиневский политехнический институт по специальности «Полупроводниковые приборы».
В 2001 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 250 научных публикаций и 60 патентов на изобретения.
Область научных интересов — информационная безопасность, криптография, электронная цифровая подпись, блочные шифры.
Эл. адрес: nmold@mail.ru

ПАСТУШОК Игорь Анатольевич

Доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2014 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Комплексная защита объектов информатизации».
В 2018 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 24 научных публикаций.
Область научных интересов — математическая оптимизация, беспроводные сети, алгоритмы распределения ресурсов, теория вероятности, имитационное моделирование.
Эл. адрес: i.pastushok@vu.spb.ru

МОЛДОВЯН Дмитрий Николаевич

Научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского института информатики и автоматизации РАН.
В 2009 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Компьютерная безопасность».
В 2012 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 79 научных публикаций и шести патентов на изобретения.
Область научных интересов — информационная безопасность, защита информации, криптосистемы с открытым ключом, постквантовая криптография, конечные некоммутативные алгебры.
Эл. адрес: mdn.spectr@mail.ru

НГУЕН Тхань Конг

Эксперт департамента науки, технологий и международного сотрудничества Данангского университета науки и технологий, Данангский университет, Дананг, Вьетнам.
В 2013 году окончил магистратуру Университета Юань Цзе, Тайвань, по специальности «Машиностроение».
Область научных интересов — обработка изображений.
Эл. адрес: nthcongbk@dut.udn.vn

ПИЛИПЕНКО Вячеслав Анатольевич

Главный научный сотрудник Геофизического центра РАН, заведующий лабораторией физики околоземного пространства Института физики Земли РАН, Москва.
В 1973 году окончил Московский государственный университет им. М. В. Ломоносова по специальности «Физик».
В 2000 году защитил диссертацию на соискание ученой степени доктора физико-математических наук.
Является автором более 300 научных публикаций.
Область научных интересов — космическая физика, геомагнитные вариации, космическая погода, солнечно-земная физика.
Эл. адрес: pilipenko_va@mail.ru

РОЯК
Михаил
Эммануилович

Профессор кафедры прикладной математики, директор Института дистанционного обучения Новосибирского государственного технического университета.
В 1989 году окончил Новосибирский электротехнический институт по специальности «Инженер-математик».
В 2008 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 100 научных публикаций.
Область научных интересов — математическое моделирование электромагнитных процессов.
Эл. адрес: royak@corp.nstu.ru

СИВАК
Сергей
Андреевич

Аспирант кафедры прикладной математики и информатики, младший научный сотрудник научно-образовательного центра «Моделирование наукоемких технологий» Новосибирского государственного технического университета.
В 2013 году окончил магистратуру Новосибирского государственного технического университета по специальности «Прикладная математика и информатика».
Является автором четырех научных публикаций.
Область научных интересов — метод конечных элементов, метод граничных элементов.
Эл. адрес: siwakserg@yandex.ru

СТАНКЕВИЧ
Андрей
Сергеевич

Доцент факультета информационных технологий и программирования Университета ИТМО, Санкт-Петербург.
В 2004 году окончил Санкт-Петербургский государственный университет информационных технологий, механики и оптики по специальности «Прикладная математика и информатика».
В 2011 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 13 научных публикаций.
Область научных интересов — формальные языки, теория сложности, алгоритмы и структуры данных.
Эл. адрес: stankev@itmo.ru

СТУПАКОВ
Илья
Михайлович

Доцент кафедры прикладной математики Новосибирского государственного технического университета.
В 2009 году окончил магистратуру Новосибирского государственного технического университета по специальности «Прикладная математика и информатика».
В 2016 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 30 научных публикаций.
Область научных интересов — метод конечных элементов, метод граничных элементов, математическое моделирование электромагнитных полей.
Эл. адрес: istupakov@gmail.com

ТСИЛИКА
Кириаки
Димитрос

Ассистент кафедры экономики Университета Фессалии, преподаватель Школы социальных наук Греческого открытого университета, Волос, Греция.
В 1995 году окончила математический факультет Университета Аристотеля в Салониках, Греция.
В 1999 году защитила диссертацию на соискание ученой степени (PhD) по прикладной математике.
Является автором 68 научных публикаций.
Область научных интересов — вычислительная математика, символические вычисления, системы компьютерной алгебры, теория и методы оптимизации, невыпуклый негладкий анализ, хеми-вариационные неравенства, визуализация данных, теория графов, экономические сети и др.
Эл. адрес: ktsilika@teilar.gr

ФАМ
Конг Тханг

Преподаватель факультета информационных технологий Данангского университета науки и технологий, Дананг, Вьетнам.
В 2013 году окончил Тульский государственный университет по специальности «Вычислительные машины, комплексы, системы и сети».
В 2016 году защитил диссертацию на соискание ученой степени кандидата технических наук в Тульском государственном университете.
Является автором 20 научных публикаций.
Область научных интересов — обработка изображений, машинное обучение, наука о данных.
Эл. адрес: pcthang@dut.udn.vn

ХРИСТОДУЛО
Ольга
Игоревна

Заведующая кафедрой геоинформационных систем Уфимского государственного авиационного технического университета.
В 1991 году окончила Уфимский государственный авиационный технический университет по специальности «Автоматизация и механизация процессов обработки и выдачи информации».
В 2012 году защитила диссертацию на соискание ученой степени доктора технических наук.
Является автором более 100 научных публикаций.
Область научных интересов — обработка и хранение пространственных данных.
Эл. адрес: o-hristodulo@mail.ru

ЯНКОВСКИЙ
Никита
Андреевич

Магистрант кафедры информационной безопасности Санкт-Петербургского государственного университета аэрокосмического приборостроения.
Является автором четырех научных публикаций.
Область научных интересов — математическая оптимизация, беспроводные сети, алгоритмы распределения ресурсов, теория вероятностей, имитационное моделирование.
Эл. адрес: yannik98@yandex.ru

ЧАН
Тхи Тху Тхао

Преподаватель факультета статистики и информатики Экономического университета, Данангский университет, Дананг, Вьетнам.
В 2018 году окончила магистратуру Тульского государственного университета по специальности «Прикладная математика и информатика».
Является автором десяти научных публикаций.
Область научных интересов — обработка изображений, машинное обучение.
Эл. адрес: thaotran@due.udn.vn