EURASIAN MATHEMATICAL JOURNAL
volume 16 , number 2, 2025

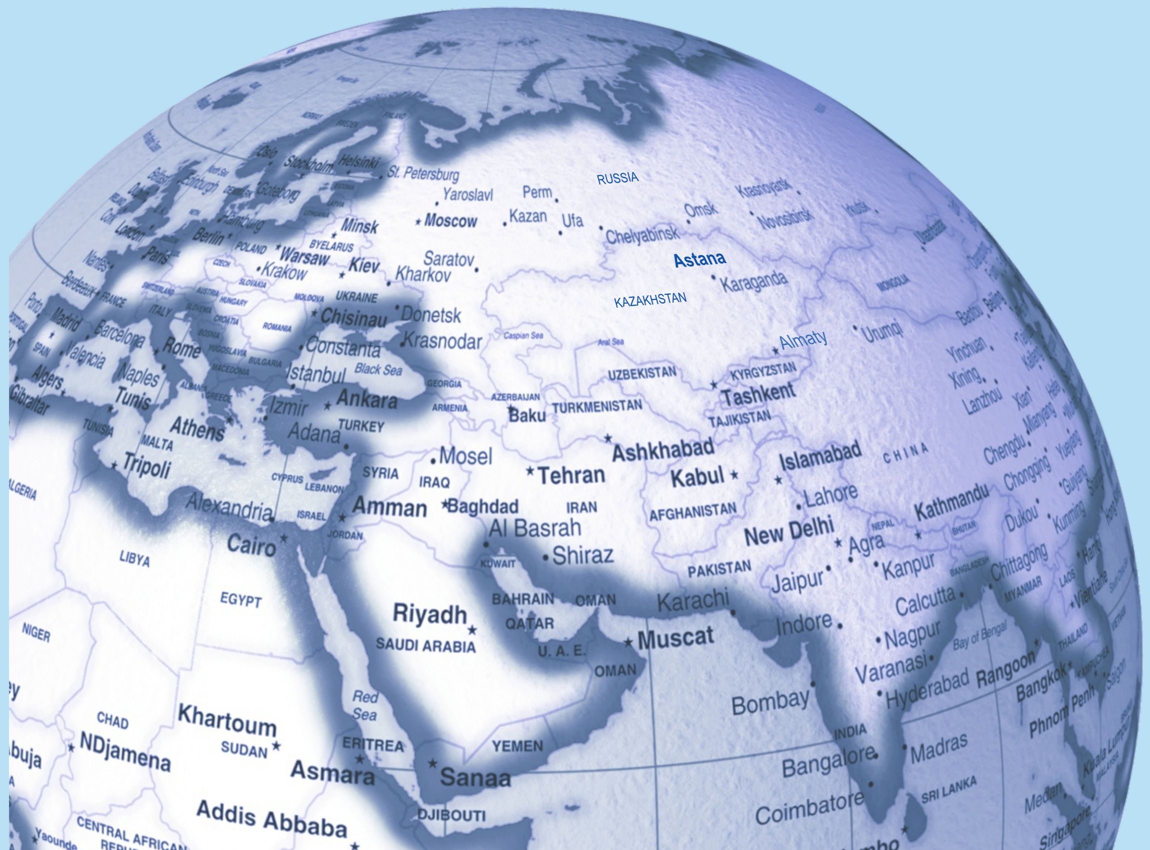
CONTENTS

Events

EURASIAN NATIONAL UNIVERSITY

ISSN (Print): 2077-9879
ISSN (Online): 2617-2658

EURASIAN MATHEMATICAL JOURNAL



ISSN 2077-9879

VOLUME 16, NUMBER 2 2025

ISSN (Print): 2077-9879
ISSN (Online): 2617-2658

Eurasian Mathematical Journal

2025, Volume 16, Number 2

Founded in 2010 by
the L.N. Gumilyov Eurasian National University
in cooperation with
the M.V. Lomonosov Moscow State University
the Peoples' Friendship University of Russia (RUDN University)
the University of Padua

Starting with 2018 co-funded
by the L.N. Gumilyov Eurasian National University
and
the Peoples' Friendship University of Russia (RUDN University)

Supported by the ISAAC
(International Society for Analysis, its Applications and Computation)
and
by the Kazakhstan Mathematical Society

Published by

the L.N. Gumilyov Eurasian National University
Astana, Kazakhstan

EURASIAN MATHEMATICAL JOURNAL

Aims and Scope

The Eurasian Mathematical Journal (EMJ) publishes carefully selected original research papers in all areas of mathematics written by mathematicians, principally from Europe and Asia. However papers by mathematicians from other continents are also welcome.

From time to time the EMJ publishes survey papers.

The EMJ publishes 4 issues in a year.

The language of the paper must be English only.

The contents of the EMJ are indexed in Scopus, Web of Science (ESCI), Mathematical Reviews, MathSciNet, Zentralblatt Math (ZMATH), Referativnyi Zhurnal – Matematika, Math-Net.Ru.

The EMJ is included in the list of journals recommended by the Committee for Control of Education and Science (Ministry of Education and Science of the Republic of Kazakhstan) and in the list of journals recommended by the Higher Attestation Commission (Ministry of Education and Science of the Russian Federation).

Information for the Authors

Submission. Manuscripts should be written in LaTeX and should be submitted electronically in DVI, PostScript or PDF format to the EMJ Editorial Office through the provided web interface (www.enu.kz).

When the paper is accepted, the authors will be asked to send the tex-file of the paper to the Editorial Office.

The author who submitted an article for publication will be considered as a corresponding author. Authors may nominate a member of the Editorial Board whom they consider appropriate for the article. However, assignment to that particular editor is not guaranteed.

Copyright. When the paper is accepted, the copyright is automatically transferred to the EMJ. Manuscripts are accepted for review on the understanding that the same work has not been already published (except in the form of an abstract), that it is not under consideration for publication elsewhere, and that it has been approved by all authors.

Title page. The title page should start with the title of the paper and authors' names (no degrees). It should contain the Keywords (no more than 10), the Subject Classification (AMS Mathematics Subject Classification (2010) with primary (and secondary) subject classification codes), and the Abstract (no more than 150 words with minimal use of mathematical symbols).

Figures. Figures should be prepared in a digital form which is suitable for direct reproduction.

References. Bibliographical references should be listed alphabetically at the end of the article. The authors should consult the Mathematical Reviews for the standard abbreviations of journals' names.

Authors' data. The authors' affiliations, addresses and e-mail addresses should be placed after the References.

Proofs. The authors will receive proofs only once. The late return of proofs may result in the paper being published in a later issue.

Offprints. The authors will receive offprints in electronic form.

Publication Ethics and Publication Malpractice

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the EMJ implies that the work described has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The EMJ follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/NewCode.pdf). To verify originality, your article may be checked by the originality detection service CrossCheck http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the EMJ.

The Editorial Board of the EMJ will monitor and safeguard publishing ethics.

The procedure of reviewing a manuscript, established by the Editorial Board of the Eurasian Mathematical Journal

1. **Reviewing procedure**

1.1. All research papers received by the Eurasian Mathematical Journal (EMJ) are subject to mandatory reviewing.

1.2. The Managing Editor of the journal determines whether a paper fits to the scope of the EMJ and satisfies the rules of writing papers for the EMJ, and directs it for a preliminary review to one of the Editors-in-chief who checks the scientific content of the manuscript and assigns a specialist for reviewing the manuscript.

1.3. Reviewers of manuscripts are selected from highly qualified scientists and specialists of the L.N. Gumilyov Eurasian National University (doctors of sciences, professors), other universities of the Republic of Kazakhstan and foreign countries. An author of a paper cannot be its reviewer.

1.4. Duration of reviewing in each case is determined by the Managing Editor aiming at creating conditions for the most rapid publication of the paper.

1.5. Reviewing is confidential. Information about a reviewer is anonymous to the authors and is available only for the Editorial Board and the Control Committee in the Field of Education and Science of the Ministry of Education and Science of the Republic of Kazakhstan (CCFES). The author has the right to read the text of the review.

1.6. If required, the review is sent to the author by e-mail.

1.7. A positive review is not a sufficient basis for publication of the paper.

1.8. If a reviewer overall approves the paper, but has observations, the review is confidentially sent to the author. A revised version of the paper in which the comments of the reviewer are taken into account is sent to the same reviewer for additional reviewing.

1.9. In the case of a negative review the text of the review is confidentially sent to the author.

1.10. If the author sends a well reasoned response to the comments of the reviewer, the paper should be considered by a commission, consisting of three members of the Editorial Board.

1.11. The final decision on publication of the paper is made by the Editorial Board and is recorded in the minutes of the meeting of the Editorial Board.

1.12. After the paper is accepted for publication by the Editorial Board the Managing Editor informs the author about this and about the date of publication.

1.13. Originals reviews are stored in the Editorial Office for three years from the date of publication and are provided on request of the CCFES.

1.14. No fee for reviewing papers will be charged.

2. **Requirements for the content of a review**

2.1. In the title of a review there should be indicated the author(s) and the title of a paper.

2.2. A review should include a qualified analysis of the material of a paper, objective assessment and reasoned recommendations.

2.3. A review should cover the following topics:

- compliance of the paper with the scope of the EMJ;

- compliance of the title of the paper to its content;

- compliance of the paper to the rules of writing papers for the EMJ (abstract, key words and phrases, bibliography etc.);

- a general description and assessment of the content of the paper (subject, focus, actuality of the topic, importance and actuality of the obtained results, possible applications);

- content of the paper (the originality of the material, survey of previously published studies on the topic of the paper, erroneous statements (if any), controversial issues (if any), and so on);

- exposition of the paper (clarity, conciseness, completeness of proofs, completeness of bibliographic references, typographical quality of the text);

- possibility of reducing the volume of the paper, without harming the content and understanding of the presented scientific results;

- description of positive aspects of the paper, as well as of drawbacks, recommendations for corrections and complements to the text.

2.4. The final part of the review should contain an overall opinion of a reviewer on the paper and a clear recommendation on whether the paper can be published in the Eurasian Mathematical Journal, should be sent back to the author for revision or cannot be published.

Web-page

The web-page of the EMJ is www.emj.enu.kz. One can enter the web-page by typing Eurasian Mathematical Journal in any search engine (Google, Yandex, etc.). The archive of the web-page contains all papers published in the EMJ (free access).

Subscription

Subscription index of the EMJ 76090 via KAZPOST.

E-mail

eurasianmj@yandex.kz

The Eurasian Mathematical Journal (EMJ)
The Astana Editorial Office
The L.N. Gumilyov Eurasian National University
Building no. 3
Room 306a
Tel.: +7-7172-709500 extension 33312
13 Kazhymukan St
010008 Astana, Republic of Kazakhstan

The Moscow Editorial Office
The Patrice Lumumba Peoples' Friendship University of Russia
(RUDN University)
Room 473
3 Ordzonikidze St
117198 Moscow, Russian Federation

EURASIAN MATHEMATICAL JOURNAL
ISSN 2077-9879
Volume 16, Number 2 (2025), 23 – 29

NOTES ON THE GENERALIZED GAUSS REDUCTION ALGORITHM

Y. Baissalov, R. Nauryzbayev

Communicated by J.A. Tussupov

Key words: lattice, well-ordered basis, reduced basis, generalized Gaussian algorithm.

AMS Mathematics Subject Classification: 68W40.

Abstract. The hypothetical possibility of building a quantum computer in the near future has forced a revision of the foundations of modern cryptography. The fact is that many difficult algorithmic problems, such as the discrete logarithm, factoring a (large) natural number into prime factors, etc., on the complexity of which many cryptographic protocols are based these days, have turned out to be relatively easy to solve using quantum algorithms.

Intensive research is currently underway to find problems that are difficult even for a quantum computer and have potential applications for cryptographic protocols. Our article contains notes related to the so-called generalized Gauss algorithm, which calculates the reduced basis of a two-dimensional lattice [8], [2]. Note that researchers are increasingly putting forward difficult algorithmic problems from lattice theory as candidates for the foundation of post-quantum cryptography. The majority of algorithmic problems related to lattice reduction become NP-hard as the lattice dimension increases [3], [1]. Fundamental problems such as the Shortest Vector Problem (SVP), the Closest Vector Problem (CVP), and Bounded Distance Decoding (BDD) are conjectured to remain hard even for quantum algorithms [4], [6]. Although the generalized Gauss reduction algorithm applies to two-dimensional lattices, where exact analysis is feasible (dimensions 3 and 4 are studied in [7], [5]), understanding such low-dimensional reductions provides important insights into the structure and complexity of lattice-based cryptographic constructions.

DOI: https://doi.org/10.32523/2077-9879-2025-16-2-23-29

1 Preliminaries

All necessary information on the basics of lattice theory can be found in [8]. For those who are familiar with the group theory, a *lattice* is a finitely generated subgroup of the additive group of the Euclidean space $\mathbb{R}^n$. In this note we will limit ourselves to considering the 2-generated lattice $L \in \mathbb{R}^n$. Any pair of vectors generating L is called a *basis* of the lattice.

The Euclidean space metric $\mathbb{R}^n$, obtained by the standard dot product, induces a metric on L. Let us clarify the notation associated with this metric: for vectors $a, b \in L$, let us denote by (a, b) their dot product, by $\|a\|$ the length of vector a, and by $[a]$ the square of this length, that is, $[a] = (a, a) = \|a\|^2$.

Definition 1. Vectors $a, b \in L$ will be called an *ordered basis* and denoted by $\langle a, b\rangle$ if the following conditions are satisfied:
(1) $\|a\| \leq \|b\|$;
(2) $\|a - b\| \leq \|a + b\|$.

Note that for any lattice basis it is easy to obtain an ordered basis: if the vectors $a, b \in L$ form a basis, then first we arrange them in increasing length, and if we already have $\|a\| \leq \|b\|$, and $\|a-b\| \leq \|a+b\|$ is not satisfied, then we change b to $-b$. Therefore, in what follows only ordered bases of the lattice L are considered.

Definition 2. (1) If $\|a\| \leq \|a-b\| < \|b\|$, then the ordered basis $\langle a, b\rangle$ is called *well-ordered.*
(2) An ordered basis $\langle a, b\rangle$ is called *reduced* if $\|b\| \leq \|a-b\|$.

In Sections 2 and 3 we present results that are valid for any normed lattices, that is, for lattices with a norm which their norm is obtained by restricting a certain norm on the space $\mathbb{R}^n$.

Definition 3. A function $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_+$, where $\mathbb{R}_+$ is the set of all non-negative real numbers, is called a *norm* if it satisfies the following conditions for any vectors $x, y \in \mathbb{R}^n$ and for any real number $\alpha \in \mathbb{R}$:
(1) $\|x\| = 0$ if and only if x is the zero vector;
(2) $\|x+y\| \leq \|x\| + \|y\|$ (*the triangle inequality*);
(3) $\|\alpha x\| = |\alpha| \cdot \|x\|$.

We will call a norm *strict* if the equality in condition (2) is satisfied only when at least one of the vectors x, y is the zero vector or the vectors x, y are collinear and co-directional.

The following corollary of the triangle inequality is often useful.

Corollary 1.1. *For any $x, y \in \mathbb{R}^n$ we have $\big|\|x\| - \|y\|\big| \leq \|x-y\|$.*

Definition 4. (1) $\lambda_1 = \min\{\|a\| : 0 \neq a \in L\}$
(2) $\lambda_2 = \min\{\|b\| : \langle a, b\rangle$ is an ordered basis for some $a \in L\}$.

The numbers λ_1, λ_2 are always defined, since the lattice L is a discrete group: any ball of finite radius centered at the zero vector contains only a finite number of lattice elements [8].

The following theorem, the proof of which can be found in [8, Theorem 16] (see also [2, Theorem 4]), explains why a reduced basis is sometimes called a *minimal basis.*

Theorem 1.1. *An ordered basis $\langle a, b\rangle$ is reduced if and only if $\|a\| = \lambda_1$ and $\|b\| = \lambda_2$.*

The following useful lemma was also proven in [8, Lemma 17].

Lemma 1.1. *Consider three vectors on a line: x, $x+y$ and $x+\alpha y$, where $\alpha \in (1, \infty)$. For any norm $\|\cdot\|$ from the inequality $\|x\| \leq \|x+y\|$ it follows that $\|x+y\| \leq \|x+\alpha y\|$, and from the inequality $\|x\| < \|x+y\|$ it follows that $\|x+y\| < \|x+\alpha y\|$.*

Note that using Lemma 1.1 one can prove that if a basis $\langle a, b\rangle$ is well-ordered, then $\|a\| \leq \|a-b\| < \|b\| < \|a+b\|$ (see [2]).

2 About the function $l(\tau) = \|b - \tau a\|$

In this section, we study the properties of the function $l(\tau) = \|b - \tau a\|$, $\tau \in \mathbb{R}$, where a, b are vectors of some real space with the norm $\|\cdot\|$. If a is the zero vector, then $l(\tau) \equiv \|b\|$ is a constant function, and if b is the zero vector, then $l(\tau) = \|a\| \cdot |\tau|$ is the absolute value function multiplied by the constant $\|a\|$. A similar function will be obtained if the vectors a, b are linearly dependent: for example, if $b = \gamma a$, then $l(\tau) = \|a\| \cdot |\tau - \gamma|$. Therefore, the case is interesting when the vectors a, b are linearly independent.

Theorem 2.1. *Let a, b be linearly independent vectors of some real space with the norm $\|\cdot\|$. Then the function $l(\tau) = \|b - \tau a\|, \tau \in \mathbb{R}$, has the following properties:*
(1) l is continuous on the entire real line;
(2) l is not bounded from above: $\lim_{\tau \to -\infty} l(\tau) = +\infty$ and $\lim_{\tau \to +\infty} l(\tau) = +\infty$;
(3) there exists $\mu_0 \overset{def}{=} \min\{l(\tau) : \tau \in \mathbb{R}\} > 0$ and there exists a closed interval of minimality $[\tau_0, \tau_1] \overset{def}{=} \{\tau \in \mathbb{R} : l(\tau) = \mu_0\}$;
(4) on the interval $(-\infty, \tau_0)$ the function l strictly decreases, and on the interval $(\tau_1, +\infty)$ it strictly increases.

Proof. (1) Let us prove the continuity of the function l at an arbitrary point $\tau_0 \in \mathbb{R}$. By Corollary 1.1 we have

$$|l(\tau + \tau_0) - l(\tau_0)| = |\|b - (\tau + \tau_0)a\| - \|b - \tau_0 a\|| \leq \|\tau a\| = \|a\| \cdot |\tau|.$$

Therefore, $|l(\tau + \tau_0) - l(\tau_0)| < \varepsilon$ holds for $|\tau| < \delta = \frac{\varepsilon}{\|a\|}$.

(2) Using Corollary 1.1 again and property (3) of the norm, we obtain

$$l(\tau) = \|b - \tau a\| \geq \|a\| \cdot |\tau| - \|b\|,$$

which obviously implies $\lim_{\tau \to -\infty} l(\tau) = +\infty$ and $\lim_{\tau \to +\infty} l(\tau) = +\infty$.

(3) Let us choose numbers $\alpha_0 < 0 < \beta_0 \in \mathbb{R}$ so that $l(\tau) > l(0) = \|b\|$ for any real number τ lying outside the interval $[\alpha_0, \beta_0]$: this is possible according to (2). According to Weierstrass's theorem, the function l reaches its minimum at a point τ_0 of the interval $[\alpha_0, \beta_0]$, which we denote by $\mu_0 = l(\tau_0)$. Obviously, this μ_0 will be the minimum of the function over the entire $\mathbb{R}$.

Let us call $\tau \in \mathbb{R}$ a *point of monotonicity* (of the function l), if $l(\tau) > \mu_0$. Let $\gamma < \tau_0$ be a point of monotonicity. Then note that each $\delta < \gamma$ is a point of monotonicity, since $l(\delta) > l(\gamma) > \mu_0$ holds (apply Lemma 1.1 for the vectors $x = b - \tau_0 a$ and $y = (\tau_0 - \gamma)a$). So, the interval $(-\infty, \gamma]$ consists entirely of monotonicity points. In addition, due to the continuity of the function l, some neighborhood of the point γ will consist entirely of monotonicity points. This means that each monotonicity point $\gamma < \tau_0$ is contained in a certain interval of the form $(-\infty, \alpha)$, consisting entirely of monotonicity points. Since the union of intervals of this type again gives an open interval of the same type, we conclude that the monotonicity points located to the left of τ_0 form an interval of this type, which we will denote without loss of generality by $(-\infty, \tau_0)$. Similar reasoning shows that monotonicity points located to the right of τ_0 form an interval $(\tau_1, +\infty)$ for some $\tau_1 \geq \tau_0$.

(4) In the last paragraph of the proof of point (3), in fact, it was proven that $l(\delta) > l(\gamma)$ holds for $\delta < \gamma < \tau_0$, that is, that the function l strictly decreases on the interval $(-\infty, \tau_0)$. Similarly, using Lemma 1.1 we prove the second statement of this point, namely, that the function l is strictly increasing on the interval $(\tau_1, +\infty)$. □

Example. The norm defined for $\mathbb{R}^2$ as follows is not strict: for $(\alpha, \beta) \in \mathbb{R}^2$ we set

$$\|(\alpha, \beta)\| \overset{def}{=} \max\{|\alpha|, |\beta|\}.$$

With $a = (0, 1), b = (1, 0)$ for the function $l(\tau) = \|b - \tau a\|$ we have $\mu_0 \overset{def}{=} \min\{l(\tau) : \tau \in \mathbb{R}\} = 1$, and the interval of minimality is $[-1, 1]$. □

Note that it may well be $\tau_0 = \tau_1$, that is, the interval $[\tau_0, \tau_1]$ can consist of only one point. This situation occurs if the norm $\|\cdot\|$ on the subspace generated by the vectors a, b is strict. Indeed, if

$\tau_0 \neq \tau_1$ and the norm $\|\cdot\|$ is strict, then the vectors $b - \tau_0 a$, $b - \tau_1 a$ are not collinear, therefore the sum of their lengths is strictly greater than the length of their sum:

$$2\mu_0 = \|b - \tau_0 a\| + \|b - \tau_1 a\| > \|2b - (\tau_0 + \tau_1)a\| = 2\left\|b - \frac{\tau_0 + \tau_1}{2}a\right\|.$$

We obtain $l(\frac{\tau_0+\tau_1}{2}) = \|\frac{\tau_0+\tau_1}{2}a + b\| < \mu_0$, which contradicts the minimality of the value μ_0.

In particular, we have $\tau_0 = \tau_1$, when the norm $\|\cdot\|$ is generated by the dot product in $\mathbb{R}^n$. In addition, in this case the value of τ_0 is explicitly calculated. Indeed, we have

$$l(\tau)^2 = [b - \tau a] = (b - \tau a, b - \tau a) = [a]\tau^2 - 2(a,b)\tau + [b],$$

and this quadratic function reaches a minimum at point $\tau_0 = \frac{(a,b)}{(a,a)} = \frac{(a,b)}{[a]}$.

In the next section we use an oracle that solves the following problem.

Problem. For a given ordered basis $\langle a, b\rangle$, find an integer $\mu = \mu(a,b)$ such that $\|b - \mu a\| = \min\{\|b - na\| : n \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of integers.

By Theorem 2.1 for the function $l(\tau) = \|b - \tau a\|$ it follows that the problem is correct, that is, it always has a solution. In general, if the interval $[\tau_0, \tau_1]$ contains an integer, then any integer from it will be a solution, if not, then $\mu = \lfloor \tau_0 \rfloor$ or $\mu = \lceil \tau_1 \rceil$, where $\lfloor x \rfloor$ ($\lceil x \rceil$) is the largest (smallest) integer from the interval $(-\infty, x]$ ($[x, +\infty)$. Thus, this problem can be solved effectively if we can efficiently calculate an approximate value of some number from $[\tau_0, \tau_1]$. This is the case when, for example, the norm $\|\cdot\|$ is defined by the scalar product in $\mathbb{R}^n$, in this case $\tau_0 = \tau_1 = \frac{(a,b)}{(a,a)} = \frac{(a,b)}{[a]}$.

As noted in [8], if we know a not very large interval of real numbers containing $[\tau_0, \tau_1]$, then the above problem can be effectively solved using the binary search algorithm. It is also proved there that $\mu(a,b) \in [1, 2\|b\|/\|a\|)$ provided $\|b\| > \|b - a\|$.

3 On the generalized Gauss reduction algorithm

In this section we will give some notes about the generalized Gaussian reduction algorithm, which allows to find a minimal lattice basis from an initial ordered basis. This algorithm is described in sufficient detail in [8] and [2].

First, we will describe the introductory part of the algorithm, during which we obtain from a given ordered basis, in the worst case, some well-ordered basis, and in the best case, a solution to our problem, i.e. we find some reduced basis.

Let us assume that an ordered basis $\langle a, b\rangle$ is given. Recall that by the definition of an ordered basis we have $\|a\| \leq \|b\|$ and $\|a - b\| \leq \|a + b\|$. Let us consider possible cases:

(1)$\|b\| \leq \|a - b\|$.

In this case, the basis $\langle a, b\rangle$ is reduced and our problem is solved.

(2) $\|a - b\| < \|a\|$.

If $\|a\| = \|b\|$, then $\langle a - b, a\rangle$ is a reduced basis and our problem is solved again:

$$\|a - b\| < \|a\| = \|-b\| = \|(a - b) - a\|$$

$$= 2\|a\| - \|b\| \leq \|2a - b\| = \|(a - b) + a\|.$$

If $\|a\| < \|b\|$, then $\langle b - a, b\rangle$ is a well-ordered basis:

$$\|b - a\| = \|a - b\| < \|a\| = \|-a\| = \|(b - a) - b\|$$

$$< \|b\| < 2\|b\| - \|a\| \leq \|2b - a\| = \|(b - a) + b\|.$$

(3) $\|a\| \le \|a-b\| < \|b\|$.
In this case, the basis $\langle a, b\rangle$ is well-ordered. □

We would like to evaluate the complexity of the generalized Gaussian algorithm, so we must consider worst-case scenarios in all stages of the algorithm. We assume that having received an ordered basis at the input, after the introductory part of the algorithm described above, we obtain a well-ordered basis at the output. The time spent on the introductory part will be short, since the main operations in it are to compare the lengths of some specific vectors.

We move on to describe the next, main stage of the algorithm, which consists of cyclically repeating the same procedure. Let us assume that before the start of this stage we have a well-ordered basis $\langle a, b\rangle$. A cyclically repeated procedure updates this basis as follows. First, using the oracle described in section 2, we find $\mu = \mu(a, b)$ and consider the basis consisting of the vectors a and $b - \mu a$. We correct the second vector of this basis, multiplying it by $\varepsilon \in \{-1, +1\}$ so that the sum of vectors a and $\varepsilon(b - \mu a)$ has a norm no less than the norm of their difference. Further,

(1) if $\|a\| \le \|b-\mu a\|$, then $\langle a, \varepsilon(b-\mu a)\rangle$ is a reduced basis and the algorithm terminates,

(2) if $\|b - \mu a\| < \|a\|$, then according to the analysis from the introductory part of the algorithm, the ordered basis $\langle \varepsilon(b-\mu a), a\rangle$ will be either reduced or well-ordered, since case (2) from the introductory part of the algorithm for the basis $\langle \varepsilon(b-\mu a), a\rangle$ is impossible.

So, the procedure, having obtained a well-ordered basis $\langle a, b\rangle$ at the input, produces a new well-ordered basis $\langle \varepsilon(b-\mu a), a\rangle$ at the output (in an unsuccessful scenario). Since each time the procedure is executed, the length of one of the vectors of the well-ordered basis decreases, after a certain finite number of steps the procedure, due to the discreteness of the lattice, will produce the reduced basis and the algorithm completes its work.

Finally, let us move on to estimating the number of repetitions of the procedure of the main stage of the algorithm. Let k be the number of repetitions and $\langle a, b\rangle = \langle a_k,\ a_{k+1}\rangle$ be a well-ordered basis at the beginning of the stage. Let us represent the results of cyclic procedures as a sequence of ordered bases

$$\langle a_k,\ a_{k+1}\rangle\,,\ \langle a_{k-1},\ a_k\rangle\,, \dots, \langle a_1,\ a_2^0\rangle\,,$$

where $\langle a_1,\ a_2^0\rangle$ is a reduced basis. Then the following lemma, proven in [8], is true.

Lemma 3.1. *For $i \ge 3$, the inequality $2\|a_i\| < \|a_{i+1}\|$ holds.*

The notation a_2^0 is introduced due to the following circumstances. There are two possibilities for completing the algorithm by obtaining the reduced basis $\langle a_1,\ a_2^0\rangle$ from the well-ordered basis $\langle a_2,\ a_3\rangle$. It may well be $a_1 = \varepsilon(a_3 - \mu a_2)$, $a_2^0 = a_2$, if case (2) occurred during the last update of the basis by the main stage procedure. But there could also be case (1), then $a_1 = a_2$, $a_2^0 = \varepsilon(a_3 - \mu a_2)$.

Note that in any case we have $\|a_2^0\| = \lambda_2 < \|a_3\|$. Therefore, we get

$$\frac{\|b\|}{\lambda_2} = \frac{\|a_{k+1}\|}{\lambda_2} > \frac{2^{k-2}\|a_3\|}{\lambda_2} > 2^{k-2},$$

which implies the estimate $k < 2 + \log_2\left(\frac{\|b\|}{\lambda_2}\right)$. □

Finally, the last remark concerns the minimality intervals of the functions $l(\tau) = \|b - \tau a\|$, $\tau \in \mathbb{R}$, for well-ordered bases $\langle a, b\rangle$. It is clear that long minimality intervals can significantly reduce the running time of the Gaussian reduction algorithm. Without going into complex computational analysis, we will limit ourselves to just one simple example confirming this fact.

Lemma 3.2. *If the minimality interval of the function $l(\tau) = \|b - \tau a\|$, $\tau \in \mathbb{R}$, for the basis $\langle a, b\rangle$ contains an integer n_0, then $\|b - n_0 a\| = \lambda_1$ or $\|a\| = \lambda_1$.*

Proof. So, assume that $\|b - n_0 a\| = \mu_0 \stackrel{def}{=} \min\{l(\tau) : \tau \in \mathbb{R}\}$. On the other hand, for some $\alpha, \beta \in \mathbb{Z}$ we have $\|\alpha a + \beta b\| = \lambda_1$. If $\beta = 0$, then obviously $|\alpha| = 1$ and $\|a\| = \lambda_1$. Therefore, let us assume that $\beta \neq 0$. Then, $\lambda_1 = |\beta| \cdot \|\frac{\alpha}{\beta} a + b\| = |\beta| \cdot l(-\frac{\alpha}{\beta}) \geq |\beta| \cdot \mu_0 = |\beta| \cdot \|b - n_0 a\|$, which implies $|\beta| = 1$ and $\|b - n_0 a\| = \lambda_1$. □

Thus, if during the execution of the procedure of the main stage of the algorithm, a well-ordered basis $\langle a, b \rangle$ is given as input, satisfying the condition of Lemma 3.2, then at the output we obtain an ordered basis $\langle c, d \rangle$ with $\|c\| = \lambda_1$, and, if $\langle c, d \rangle$ is not a reduced basis, then at the next step the result of the procedure falling into case (1) will be a reduced basis. Therefore, the number k of repetitions of the procedure will not exceed 2.

Acknowledgments

The research of the first author is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19677451).

References

[1] M. Ajtai, *The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract)*, Proceedings of the thirtieth annual ACM symposium on Theory of computing, (1998), 10-19. https://doi.org/10.1145/276698.276705

[2] M. Kaib, C.P. Schnorr, *The generalized gauss reduction algorithm*, Journal of Algorithms, 21 (1996), 565-578. https://doi.org/10.1006/jagm.1996.0059

[3] D. Micciancio, *The hardness of the shortest vector problem*, SIAM Journal on Computing, 30(6), (2001), 2008-2035. https://doi.org/10.1137/S0097539700373039

[4] D. Micciancio, S. Goldwasser, *Complexity of lattice problems: a cryptographic perspective*, Springer (2002). https://doi.org/10.1007/978-1-4615-0897-7

[5] P.Q. Nguyen, D. Stehlé, *Low-dimensional lattice basis reduction revisited*, ACM Transactions on Algorithms 5 (2004), no. 4, 1 - 48. https://doi.org/10.1145/1597036.1597050

[6] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, Journal of the ACM, 56(6), (2009), 1-40. https://doi.org/10.1145/1568318.15683

[7] I. Semaev, *A 3-dimensional lattice reduction algorithm*, In: Silverman, J.H. (eds) Cryptography and Lattices. CaLC 2001. Lecture Notes in Computer Science, vol. 2146, 181-193, Springer, Berlin, Heidelberg (2001). https://doi.org/10.1007/3-540-44670-2_13

[8] A.V. Shokurov, N.N. Kuzyurin, S.A. Fomin, *Lattices, algorithms and modern cryptography, electronic textbook.* January 12, 2023 (in Russian). Access mode: `https://discopal-lab.0x1.tv/share/raw/daa0d349f9f28831eb97affb2ff02ff0ab5314f3/lectures-cs/books/cryptography/book-lattice-cryptography.pdf` (date of access 01/05/2025).

Yerzhan Baissalov, Ruslan Nauryzbayev
Department of Mechanics and Mathematics
L.N. Gumilyov Eurasian National University
13 Kazhymukan St, Office 115
010008 Astana, Republic of Kazakhstan
E-mails: baisalov_yer@enu.kz, nauryzbayev_rzh@enu.kz

Received: 19.07.2024