ISSN 1064-5624, Doklady Mathematics, 2016, Vol. 93, No. 3, pp. 243–247. © Pleiades Publishing, Ltd., 2016.
Original Russian Text © A.D. Bruno, 2016, published in Doklady Akademii Nauk, 2016, Vol. 468, No. 1, pp. 7–11.

Computation of the Best Diophantine Approximations and of Fundamental Units of Algebraic Fields

A. D. Bruno

Presented by Academician of the RAS B.N. Chetverushkin December 14, 2015

Received December 23, 2015

Abstract—A global generalization of continued fraction that yields the best Diophantine approximations of any dimension is considered. In the algebraic case, this generalization underlies a method for calculating the fundamental units of algebraic rings and the periods of best approximations, as well as the identification of the fundamental domain with respect to these periods. The units of an algebraic field are understood as the units of maximal order of this field.

DOI: 10.1134/S1064562416030017

Suppose that, in the real n-dimensional space $\mathbb{R}^n = \{X\}$, we are given m homogeneous real forms $f_i(X)$, $i = 1, 2, \ldots, m$, where $2 \le m \le n$. In many cases, the convex hull of the set of values $G(X) = (|f_1(X)|, \ldots, |f_m(X)|) \in \mathbb{R}^m$ for integer $X \in \mathbb{Z}^n$ is a convex polyhedral set. For $\|X\| <$ const, its boundary can be calculated using a standard software program. The points $X \in \mathbb{Z}^n$ for which the values $G(X)$ lie on this boundary are called boundary points. They are the best Diophantine approximations to the indicated forms. The computation of them yields a global generalization of continued fraction. For $n = 3$, unsuccessful attempts to generalize continued fractions have been made by numerous mathematicians.

Let $p(\xi)$ be an integer irreducible (in $\mathbb{Q}$) polynomial of degree n and λ be its root. The set of fundamental units of the ring $\mathbb{Z}[\lambda]$ can be calculated using the boundary points of a collection of linear and quadratic forms constructed with the help of the roots of the polynomial $p(\xi)$. The set of fundamental units of the field $\mathbb{Q}(\lambda)$ can be calculated in a similar manner. Thus far, these units have been calculated only for $n = 2$ (with the help of usual continued fractions) and for $n = 3$ (by applying the Voronoi algorithm).

The present approach generalizes the continued fraction and yields the best simultaneous approximations and the fundamental units of algebraic fields for any n.

1. Let α_0 and α_1 be positive integers. Their greatest common divisor can be found using the Euclidean algorithm of successive division with a remainder:

$$\alpha_0 = a_0\alpha_1 + \alpha_2, \quad \alpha_1 = a_1\alpha_2 + \alpha_3,$$
$$\alpha_2 = a_2\alpha_3 + \alpha_4, \ldots,$$

where the positive integers $a_0, a_1, a_2, \ldots$ are partial quotients. This algorithm decomposes the number $\alpha = \frac{\alpha_0}{\alpha_1}$ into a proper continued fraction [1], and it can be applied to any real number α. Lagrange [1, Section 10] proved that, for quadratic irrationalities α, the decomposition into a continued fraction is periodic (and conversely), i.e., starting at some index, the sequence of partial quotients a_0, a_1, a_2, a_3, ... consists of a repeated segment $a_k, a_{k+1}, \ldots, a_{k+t}$.

Summarizing, the decomposition of a number into a continued fraction is easy to do, gives the best rational approximations to the number, is finite for a rational number and periodic for quadratic irrationalities [1, Section 10], and has properties of almost all numbers [1, Chapter III] for cubic irrationalities [2].

Unsuccessful attempts to generalize continued fractions were made by Euler, Jacobi, Dirichlet, Hermite, Poincaré, Hurwitz, Klein, Minkowski, Brun, Arnold, and many others [3; 4; 5, Section 1.2]. Only the Voronoi stepwise algorithm [6] works, but it is rather complicated.

The following generalization of continued fraction was proposed in [5, 7, 8].

Suppose that, in the n-dimensional real space $\mathbb{R}^n$ with coordinates $X = (x_1, \ldots, x_n)$, we are given m homogeneous real forms (i.e., polynomials in variables) $f_1(X), \ldots, f_m(X)$, where $2 \le m \le n$. A nonzero integer point $X \in \mathbb{Z}^n \backslash 0 \subset \mathbb{R}^n$ is called a minimal point if there is no other nonzero integer point $Y \in \mathbb{Z}^n \backslash 0 \subset \mathbb{R}^n$, $Y \ne -X$, such that

$$|f_i(Y)| \le |f_i(X)|, \quad i = 1, 2, \ldots, m.$$

Keldysh Institute of Applied Mathematics, Russian Academy of Sciences, Miusskaya pl. 4, Moscow, 125047 Russia
e-mail: abruno@keldysh.ru

The minimal points are regarded as the best Diophantine approximations to the set of root spaces of m forms $f_i(X)$. There are other definitions of best Diophantine approximations associated with various norms [9, 10]. The consideration of minimal points goes back to Voronoi [6].

Problem 1. Find all minimal points.

Partial solution of Problem 1. The moduli $g_i(X) = |f_i(X)|$ of the forms $f_i(X)$, $i = 1, 2, \ldots, m$, define a mapping $G(X) = (g_1(X), \ldots, g_m(X))$ of $\mathbb{R}^n$ into the positive orthant $\mathbf{S} = \mathbb{R}^m_+$ of the m-dimensional space $\mathbb{R}^m$ with coordinates $S = (s_1, \ldots, s_m)$: $s_i = g_i(X) = |f_i(X)|$, $i = 1, 2, \ldots, m$. The integer lattice $\mathbb{Z}^n \subset \mathbb{R}^n$ is then mapped into a set $\mathbf{Z} \subset \mathbf{S}$. The closure of the convex hull $\mathbf{H}$ of the set $\mathbf{Z}\backslash 0$ is a convex set. All integer points $X \in \mathbb{Z}^n\backslash 0$ mapped onto the boundary $\partial\mathbf{H}$ of $\mathbf{H}$ are called boundary points. They are minimal ones. Possibly, there are minimal points X whose images $G(X)$ do not lie on $\partial\mathbf{H}$. However, we search for boundary points X that are a subset of the set of minimal points.

In what follows, we consider only the case when the convex set $\mathbf{H}$ is polyhedral, i.e., its boundary $\partial\mathbf{H}$ consists of vertices, edges, and faces of various dimensions, but does not contain continuous "curved" parts. In this case, the boundary $\partial\mathbf{H}$ can be calculated with the help of standard software intended for computing convex polyhedral hulls [11, 12]. This gives an algorithmic generalization of continued fraction to any dimension. For examples, see [5].

In particular, this makes it possible to compute the best simultaneous rational approximations $\frac{q_1}{q_0}, \ldots, \frac{q_m}{q_0}$ to real numbers $\beta_1, \ldots, \beta_m$, where $q_0, q_1, \ldots, q_m \in \mathbb{Z}$ and $f_i(q_0, q_i) = q_0\beta_i - q_i$ for $i = 1, 2, \ldots, m$. Here, $m = m$ and $n = m + 1$.

Conjecture. *If all $f_1, \ldots, f_m$ are linear and quadratic forms, then the boundary $\partial\mathbf{H}$ has no curved parts, i.e., is polyhedral.*

2. Let

$$p(\xi) = \xi^n + b_1\xi^{n-1} + \ldots + b_{n-1}\xi + b_n \qquad (1)$$

be an integer irreducible (in $\mathbb{Q}$) real polynomial with integer coefficients b_i. It is associated with the ring $\mathbb{Z}[\lambda]$ of numbers of the form

$$\xi(\lambda) = x_1 + x_2\lambda + \ldots + x_n\lambda^{n-1} \qquad (2)$$

with integer coefficients x_i, where λ is a root of polynomial (1). Each number (2) is associated with a square matrix $D(\xi) = (d_{ij})$:

$$\lambda^i\xi(\lambda) = \sum_{j=0}^{n-1} d_{ij}\lambda^j, \quad i = 0, 1, \ldots, n-1.$$

The determinant $\det D(\xi)$ is called the norm of number (2) and is denoted by $N(\xi)$. Numbers (2) having the norm $N(\xi) = \pm 1$ are called units [13, Chapter II]. There exists a set of units $\varepsilon_1, \ldots, \varepsilon_r$ such that any unit $\varepsilon \in \mathbb{Z}[\lambda]$ can be uniquely represented in the form

$$\varepsilon = \pm\varepsilon_1^{a_1}\ldots\varepsilon_r^{a_r}, \qquad (3)$$

where a_i are integers. These units $\varepsilon_1, \ldots, \varepsilon_r$ are called fundamental.

Problem 2. For a fixed polynomial (1), find the set of fundamental units of the ring $\mathbb{Z}[\lambda]$.

Solution of Problem 2. Suppose that the irreducible (in $\mathbb{Q}$) polynomial (1) has l real roots $\lambda_1, \ldots, \lambda_l$ and k pairs of complex conjugate roots $\lambda_{l+1}, \ldots, \lambda_{l+k}$, $\bar{\lambda}_{l+1}, \ldots, \bar{\lambda}_{l+k}$, where $l + 2k = n$. Here, $l \geq 0$ and $k \geq 0$. Consider $m = k + l$ forms

$$f_i(X) = \langle L_i, X\rangle, \quad i = 1, 2, \ldots, l,$$

$$f_{l+j}(X) = \langle K_{l+j}, X\rangle\langle \bar{K}_{l+j}, X\rangle, \quad j = 1, 2, \ldots, k,$$

where

$$L_i = (1, \lambda_i, \lambda_i^2, \ldots, \lambda_i^{n-1}),$$

$$\langle L_i, X\rangle = x_1 + x_2\lambda_i + \ldots + x_n\lambda_i^{n-1},$$

$$K_{l+j} = (1, \lambda_{l+j}, \lambda_{l+j}^2, \ldots, \lambda_{l+j}^{n-1}),$$

$$\bar{K}_{l+j} = (1, \bar{\lambda}_{l+j}, \bar{\lambda}_{l+j}^2, \ldots, \bar{\lambda}_{l+j}^{n-1}).$$

By the Dirichlet theorem [13, Chapter II, Section 4, item 3], for polynomial (1), the number of fundamental units is $r = k + l - 1$. In what follows, we assume that $m = k + l \geq 2$ because, if $k + l \leq 1$, then $r \leq 0$ and, by the Dirichlet theorem, there are no fundamental units.

Theorem 1 [13, Chapter II, Section 1, item 2]. *For numbers* (2) *with* $X = (x_1, \ldots, x_n)$,

$$N(\xi) = f(X) \overset{\text{def}}{=} f_1(X)\ldots f_m(X).$$

Therefore, for all units of form (2),

$$f(X) = \pm 1 \text{ and } g(X) \overset{\text{def}}{=} |f(X)| = 1. \qquad (4)$$

Let $\tilde{\mathbb{Z}}^n$ be the set of points $X \in \mathbb{Z}^n$ with property (4). For this set (i.e., for $X \in \tilde{\mathbb{Z}}^n$) consider constructions of Section 1, namely, the set $\tilde{\mathbf{Z}}$ of values

$$G(X) = (g_1(X), \ldots, g_m(X)) \subset \mathbf{S} = \mathbb{R}^m_+,$$

where $g_i(X) = |f_i(X)|$ for $i = 1, 2, \ldots, m$; the convex hull $\tilde{\mathbf{H}}$ of the set $\tilde{\mathbf{Z}}$; and its boundary $\partial\tilde{\mathbf{H}}$. The boundary $\partial\tilde{\mathbf{H}}$ is of dimension $m - 1 = r$; has no curved parts; and consists of vertices, edges, and faces.

Theorem 2. *All faces of the boundary $\partial\tilde{\mathbf{H}}$ are simplices, and $G_0 = (1, 1, \ldots, 1)$ is its vertex.*

Let Δ be some $(m - 1)$-dimensional face of $\partial\tilde{\mathbf{H}}$ containing the vertex $G_0 = (1, 1, \ldots, 1)$, and let $R_1, \ldots, R_{m-1}$ be its edges containing G_0.

Theorem 3. *Let G_i be another vertex of the edge R_i other than G_0, $i = 1, 2, \ldots, m - 1$. Numbers* (2) *for which*

$G(X) = G_i$, $i = 1, 2, ..., m - 1$, *form the set of fundamental units of the ring* $\mathbb{Z}[\lambda]$.

Therefore, to compute the fundamental units, on some bounded set $\|X\| <$ const, $X \in \tilde{\mathbb{Z}}^n$, we need to calculate a piece of $\partial\tilde{\mathbf{H}}$ containing the $(m - 1)$-dimensional face Δ.

For a unit ε, its norm is $N(\varepsilon) = \pm 1$. Sometimes, for even n, only units with a positive norm are required. To find the basis set of such (quasi-fundamental) units, following the procedure described, we have to leave only those points $X \in \tilde{\mathbb{Z}}^n$ for which $f(X) = +1$ and use them as described above to obtain a multiplicative basis. For odd n, every unit ε is associated with a unit ε' with $N(\varepsilon') = 1$: this is either ε or $-\varepsilon$, i.e., X in (2) is replaced by $-X$.

Each number (2) is associated with the matrix

$$T(\xi) = x_1 E + x_2 B + \ldots + x_n B^{n-1},$$

where E is the identity matrix and B is a matrix accompanying polynomial (1):

$$B = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ -b_n & -b_{n-1} & -b_{n-2} & \ldots & -b_2 & -b_1 \end{pmatrix}.$$

If number (2) is a unit, then the matrix $T(\xi)$ is unimodular and the linear transformation $\tilde{X} = T(\xi)X$ in $\mathbb{R}^n$ induces the automorphism

$$\tilde{s}_i = g_i(X)s_i, \quad i = 1, 2, \ldots, m, \tag{5}$$

of the set $\tilde{\mathbf{H}}$ into $\mathbf{S} = \mathbb{R}^m_+$. Therefore, each unit ε is associated with the period $T(\varepsilon)$ of the generalized continued fraction. The number of independent periods is $m - 1$. This is a generalization of the Lagrange theorem [1, Section 10], which was proved for $n = l = 2$ and $k = 0$, i.e., $m = k + l = 2$.

3. Now consider the quotient field $\mathbb{Q}(\lambda)$ of the ring $\mathbb{Z}[\lambda]$. In this field, the coefficients x_i in numbers (2) can be rational numbers. According to [13, Chapter II], there is a fundamental basis $\omega_1, ..., \omega_n$ of numbers (2) over which the field $\mathbb{Q}(\lambda)$ is a module; i.e., all numbers $\alpha \in \mathbb{Q}(\lambda)$ have the form

$$\alpha = y_1\omega_1 + y_2\omega_2 + \ldots + y_n\omega_n, \quad y_i \in \mathbb{Z}. \tag{6}$$

For the computation of a fundamental basis, see [13, Chapter II, Section 2]. Specifically, units (2) of this field can have rational coefficients x_i. There is a set of units $\varepsilon_1, ..., \varepsilon_r \in \mathbb{Q}(\lambda)$ such that all units of the field have the form of (3). These units are called fundamental. All constructions and theorems from Section 2 are valid for them. Only the matrix of the period $T(\varepsilon)$ can have rational elements, but $\det T(\varepsilon) = N(\varepsilon) = \pm 1$. Therefore, the fundamental units of the field can be found by calculating $f(X)$ on the lattice of numbers (6) written in the form of (2) with rational x_i. The rest of the computations is the same as for the ring $\mathbb{Z}[\lambda]$.For even n, a multiplicative basis of units with a positive norm forms a set of quasi-fundamental units.

4. The $(m - 1)$-dimensional boundary $\partial\mathbf{H}$ of the polyhedral set $\mathbf{H}$ is injectively projected onto the positive coordinate orthant $\mathbf{S}^{m-1}_+$ of the orthant $\mathbf{S}_+ = \mathbf{R}^m_+$: $(s_1, ..., s_{m-1}, s_m) \leftrightarrow (s_1, ..., s_{m-1})$. The logarithmic substitution $h_i = \ln s_i$, $i = 1, 2, ..., s_{m-1}$, $H = (h_1, ..., h_{m-1})$, where ln means log, injectively maps $\mathbf{S}^{m-1}_+$ to $\mathbb{R}^{m-1}$. Moreover, automorphism (5) becomes

$$\tilde{h}_i = \ln g_i(X) + h_i, \quad i = 1, 2, \ldots, m-1, \tag{7}$$

i.e., is a parallel translation. The units of a field or ring form a multiplicative Abelian group. Therefore, their logarithms form an additive Abelian group. In $\mathbb{R}^{m-1}$, there exists a fundamental domain $\mathcal{F}$ with respect to translations (7) of this group. Let the m-dimensional vectors G_i ($i = 1, 2, ..., m - 1$) corresponding to the fundamental units in Theorem 3 have the form $G_i = (g_{1i}, ..., g_{mi})$. Define

$$\Gamma_i = (\ln g_{1i}, \ldots, \ln g_{m-1,i}), \quad i = 1, 2, \ldots, m-1. \tag{8}$$

Theorem 4. *In* $\mathbb{R}^{m-1}$ *the fundamental domain with respect to translations* (7), (8) *is an* $(m - 1)$*-dimensional "cube"*

$$\begin{gathered} \mathcal{F} = \{H = \mu_1\Gamma_1 + \ldots + \mu_{m-1}\Gamma_{m-1}\}, \\ 0 \le \mu_i \le 1, \quad i = 1, 2, \ldots, m-1. \end{gathered} \tag{9}$$

In computing the boundary of the convex hull of a set of points, difficulties increase as the number of points grows. To reduce these difficulties, the computations can be divided into the following six steps.

Step 1. In the field $\mathbb{Q}(\lambda)$, find all units X from the domain $\|X\| <$ const by calculating the values $g(X)$ at these X.

Step 2. On the set of units $\tilde{X}$, calculate the boundary $\partial\tilde{\mathbf{H}}$ of their convex hull $\tilde{\mathbf{H}}$.

Step 3. By Theorem 3, from $\partial\tilde{\mathbf{H}}$, extract a set of fundamental units represented in $\mathbf{S}_+$ by the vertices $G_1, ..., G_{m-1}$.

Step 4. By Theorem 4, find fundamental domain (9).

Step 5. Calculate the convex hull of $G(X)$ with $\xi(X) \in \mathbb{Q}(\lambda)$ only for those X at which $H(X)$ belong to fundamental domain (9) and its close neighborhood.

Step 6. Use this part of $\partial\mathbf{H}$ to recover the whole boundary $\partial\mathbf{H}$ with the help of the periods G_i, $i = 1, 2, ..., n - 1$, corresponding to the fundamental units, or translations (7).

Example. Let $p(\xi) = \xi^3 - 7\xi - 2$ and all of its roots are real: $\lambda_1 \approx -2.489288$, $\lambda_2 \approx -0.289168$, and $\lambda_3 \approx 2.778457$. Here, $n = m = l = 3$, $k = 0$, and $r = m - 1 = 2$. The fundamental basis of the field is given by 1, λ, and $\frac{\lambda + \lambda^2}{2}$.

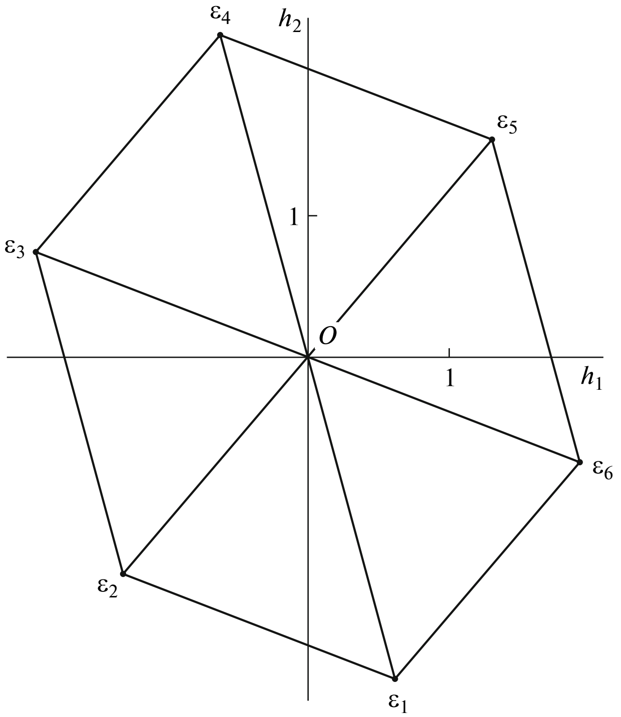

Fig. 1. Logarithmic projections of the vertices, edges, and faces of the polyhedron $\partial\tilde{\mathbf{H}}$. The projections of units close to zero are shown. The projections of the edges are rectified.

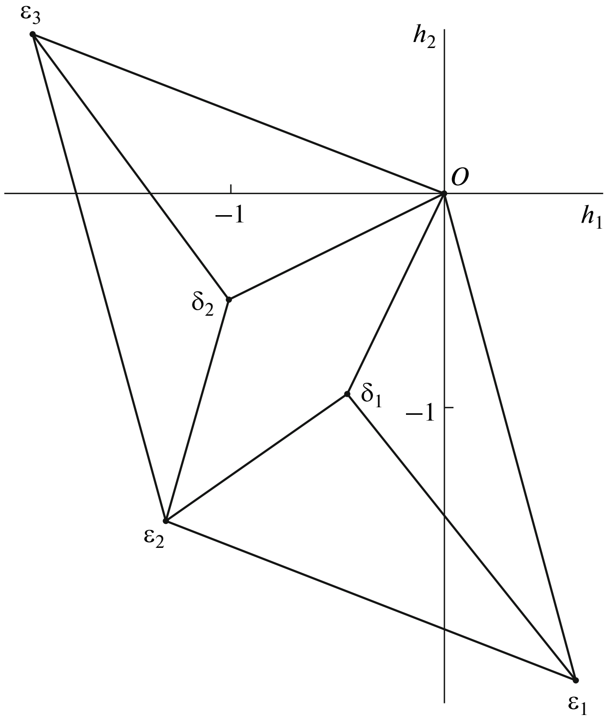

Fig. 2. Logarithmic projection of the polyhedron $\partial\mathbf{H}$ onto the fundamental domain.

Step 1. Calculating the values $g(Y)$ at the points $\xi = y_1 + y_2\lambda + \frac{y_3(\lambda+\lambda^2)}{2}$ with integer y_i, we find the units $\varepsilon_i = (y_1, y_2, y_3)$: $\varepsilon_1 = (0, 0, 1)$, $\varepsilon_2 = (1, 2, 2)$, $\varepsilon_3 = (-2, 0, 1)$, $\varepsilon_4 = (-10, -2, 3)$, $\varepsilon_5 = (5, 2, -2)$, and $\varepsilon_6 = (0, 2, -1)$.

Step 2. Computing the convex hull of the corresponding points G_0 and $G_i = G(Y)$, we obtain its six two-dimensional faces. Their logarithmic projections onto the plane (h_1, h_2) are shown in Fig. 1. Here, the logarithmic projections of the edges are depicted by direct segments, although they are curvilinear. Note that $\varepsilon_{i+3} = \varepsilon_i^{-1}$, $i = 1, 2, 3$.

Step 3. Any pair ε_i and $\varepsilon_j \neq \varepsilon_i^{\pm 1}$ $(i, j = 1, 2, ..., 6)$ forms a set of fundamental units.

Step 4. For the pair ε_1, ε_3, the fundamental domain $\mathcal{F}$ is the quadrilateral with vertices 0, ε_1, ε_2, and ε_3.

Step 5. The logarithmic projection of the boundary of the convex hull of values $G(Y)$ over $Y \in \mathbb{Z}^3$ with $H(Y) \in \mathcal{F}$ is shown in Fig. 2. Here, there are two new vertices: $\delta_1 = (0, 1, 1)$ and $\delta_2 = (1, 1, 1)$. At them, $g(Y) = 2$. There is a quadrilateral face with vertices 0, δ_1, ε_2, and δ_2.

Step 6. Translating the fundamental domain of Fig. 2 through integer linear combinations of logarithms of known units, we obtain the projection of the entire polyhedron $\partial\mathbf{H}$ onto the plane (h_1, h_2), which is shown in Fig. 3. This example was taken from Voronoi [6, Section 59, Example], where two pairs of fundamental units ε_2, ε_3 and ε_2, ε_4 were found, but there were

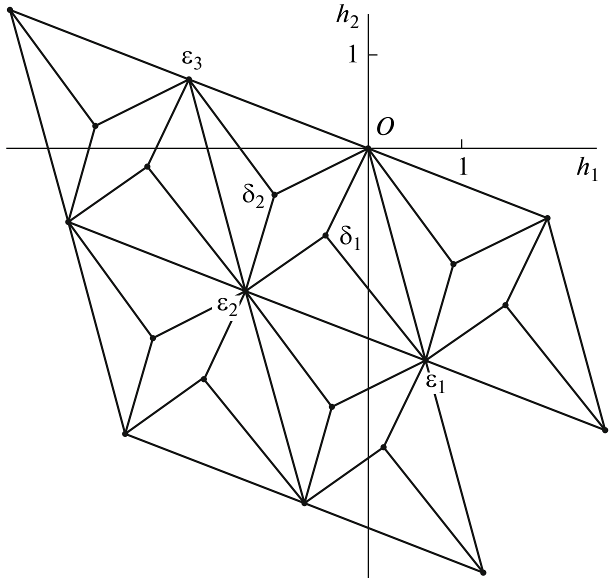

Fig. 3. Logarithmic projection of the polyhedron $\partial\mathbf{H}$ onto a part of the plane h_1, h_2.

no analogues of our plots. Actually, the boundary $\partial\mathbf{H}$ in this example is calculated as the convex hull of $G(Y)$ over $Y \in \mathbb{Z}^3$, because the dimension of the problem ($n = 3$) is rather low. Nevertheless, the partition into steps is shown, which can be useful for high dimensions n and m.

Remark. Here, we assume that each root of polynomial (1) is not a unit.

REFERENCES

1. A. Ya. Khinchin, *Continued Fractions* (Fizmatgiz, Moscow, 1961; Noordhoff, Groningen, 1963).
2. A. D. Bruno, USSR Comput. Math. Math. Phys. **4** (2), 1–15 (1964).
3. A. D. Bruno, Funct. Approx. **43** (1), 55–104 (2010).
4. A. D. Bruno, “On geometric methods in works by V.I. Arnold and V.V. Kozlov,” Preprint arXiv No. 1401.6320.
5. A. D. Bruno, Chebyshev. Sb. (Tula) **16** (2), 35–65 (2015).
6. G. F. Voronoi, *On Generalization of the Algorithm of Continued Fraction* (Warsaw Univ., 1896).
7. A. D. Bruno, Dokl. Math. **82** (1), 587–589 (2010).
8. A. D. Bruno, Chebyshev. Sb. (Tula) **11** (1), 68–83 (2010).
9. F. Schweiger, *Multidimensional Continued Fractions (*Oxford Univ. Press, New York, 2000).
10. A. J. Brentjes, *Multidimensional Continued Fraction Algorithms*, Mathematical Center Tracts 145 (Math. Centrum, Amsterdam, 1981).
11. K. Fukuda, in *Proceedings of ISSAC'08 21st International Symposium on Symbolic and Algebraic Computations* (ACM, New York, 2008), pp. 333–334.
12. C. B. Barber, D. P. Dobkin, and H. T. Huhdanpaa, ACM Trans. Math. Software **22** (4), 469–483 (1996); http://www.qhull.org.
13. Z. I. Borevich and I. R. Shafarevich, *Number Theory* (Academic, New York, 1966; Nauka, Moscow, 1972).

Translated by I. Ruzanova