Computing unimodular matrices of power transformations

Alexander Bruno and Alijon Azimov

Abstract. An algorithm for solving the following problem is described. Let $m < n$ integer vectors in the n-dimensional real space be given. Their linear span forms a linear subspace L in $\mathbb{R}^n$. It is required to find a unimodular matrix such that the linear transformation defined by it takes the subspace L into a coordinate subspace. Computer programs implementing the proposed algorithms and the power transforms for which they are designed are described.

1. Introduction

Recall that a square matrix is said to be unimodular if all its elements are integers and its determinant equals ± 1. Its inverse is also unimodular.

We will write vectors as row vectors $A = (a_1, \dots, a_n)$,and $[a]$ is the integer part of the real number a.

Problem 1. Let m, $(m < n)$ integer vectors $A_1, \dots, A_m$ be given in the n-dimensional real space $\mathbb{R}^n$. Their linear span

$$L = \left\{ X = \sum_{j=1}^{m} \lambda_j A_j,\ \lambda_j \in \mathbb{R}, \quad j = 1, \dots, m \right\} \tag{1}$$

forms a linear subspace in $\mathbb{R}^n$. It is required to find a unimodular matrix α such that the transformation $X\alpha = Y$ takes L to the coordinate subspace

$$M = \{Y : y_{n-l+1} = \cdots = y_n = 0\},$$

where $l = \dim L$.

In this talk, we give an algorithm for solving this problem and provide its implementations in computer algebra systems [1]. If $n = 2$ and $m = 1$, then Problem 1 is solved by Eucledean algorithm or by continued fraction [2]. In Section 2, we describe the Euler algorithm [3], which generalizes the Euclidean algorithm (i.e., the continued fraction algorithm) to the n-dimensional integer vector. In Section 3 we describe a solution of Problem 1. In Section 4 we consider power transformations, for the calculation of the unimodular matrices of which, all these algorithms are developed.

2. Euler's algorithm and a generalization of continued fraction

Problem 2. Let an n-dimensional integer vector $A = (a_1, a_2, \dots, a_n)$ be given. Find an n-dimensional unimodular matrix α such that the vector $A\alpha = C = (c_1, \dots, c_n)$ contains only one nonzero component c_n.

Euler proposed the following algorithm for solving this problem [3]. Suppose for the time being that all components of vector A are nonzero. Using the permutation $A\alpha_0 = (\widetilde{a}_1, \widetilde{a}_2, \dots, \widetilde{a}_n)$ arrange its components in nondecreasing order $\widetilde{a}_j \le \widetilde{a}_{j+1}$, $j = 1, \dots, n-1$. Hereα_0 is the unimodular matrix of the permutation. Let $\widetilde{a}_k$ be the least number among $\widetilde{a}_j$ that is distinct from zero.

Let $b_j = [\widetilde{a}_j / \widetilde{a}_k]$, $j = 1, \dots, n$. Here $b_1 = \cdots = b_{k-1} = 0$, $b_k = 1$. Make the transformation

$$d_j = \widetilde{a}_j - b_j \widetilde{a}_k,\ 1 \le j \le n,\ j \ne k, d_k = \widetilde{\alpha}_k. \tag{2}$$

It is associated with the unimodular matrix α_1 the diagonal of which consists of ones, and the k-th row is

$$0, 0, \dots, 0, 1, -b_{k+1}, \dots, -b_n,\ \text{i.e. } \tilde{A}\alpha_1 = D = (d_1, \dots, d_n).$$

Now arrange the components of the vector D in non-decreasing order using the unimodular permutation matrix β_0 so that $D\beta_0 = \tilde{D} = \left(0, \dots, 0, \widetilde{d}_k, \dots, \widetilde{d}_n\right)$,where $\widetilde{d}_j \le \widetilde{d}_{j+1}$.

Let $\widetilde{d}_l$ be the least of $\widetilde{d}_j$, distinct from zero, and let $e_j = \left[\widetilde{d}_j / \widetilde{d}_l\right]$, $j = 1, \dots, l$. Make the transformation

$$f_j = \widetilde{d}_j - e_j \widetilde{d}_l, \quad 1 \le j \le n, \quad j \ne l, \quad f_l = \widetilde{d}_l,$$

and soon. At each step, the maximum of the components of the vector decreases and it is the n-th component. Therefore, in a finite number of steps we obtain a vector with the only (last) nonzero component. This component equals the GCD of all original components $a_1, \dots, a_n$. Each step involves a permutation matrix and a triangular matrix with the unit diagonal:

$$A\alpha_0\alpha_1\beta_0\beta_1\gamma_0\gamma_1 \dots \omega_0\omega_1 = A\alpha = C = (0, \dots, 0, c_n).$$

The matrix

$$\alpha = \alpha_0\alpha_1\beta_0\beta_1\gamma_0\gamma_1 \cdots \omega_0\omega_1 \tag{3}$$

is a solution of Problem 2.

If not all components a_j of the original vector A have the same sign, then we first arrange them in non-decreasing order of their moduli $|\widetilde{a}_j| \le |\widetilde{a}_{j+1}|$ and set $b_j = [|\widetilde{a}_j| \,/\, |\widetilde{a}_k|] \operatorname{sign} \widetilde{a}_j \operatorname{sign} \widetilde{a_k}$.

Let the given vector A be perpendicular to a linear variety. Then, after the transformation using the matrix α, we obtain the vector in which all first $n-1$ components are zero. Therefore, the last component of all vectors of the original variety will be zero after this transformation.

Euler's algorithm generalizes the continued fraction algorithm only for integer vectors. Such a generalization for arbitrary real vectors was sought by all major mathematicians of the 19th century, but without success. Such a generalization of the continued fraction algorithm for the n-dimensional vector was proposed in [4]. It gives a sequence of best approximations, and it is periodic if all the components of the original vector are roots of a polynomial of degree n with integer coefficients.

3. Solution to Problem 1

Let integer vectors

$$\begin{aligned} A_1 &= (a_{11}, a_{12}, \dots, a_{1n})\,, \\ A_2 &= (a_{21}, a_{22}, \dots, a_{2n})\,, \\ &\dots \\ A_m &= (a_{m1}, a_{m2}, \dots, a_{mn}) \end{aligned} \tag{4}$$

$(m < n)$ and a linear space (1) be given.

First, we check if there are identical vectors among them. If there are any, we discard duplicates and leave only one of them. Now, we are sure that all vectors (4) are different. Apply Euler's algorithm to the vector A, i.e., calculate the matrix α such that $A_1\alpha_0 = C_1 = c_n E_n$, where c_n is an integer and E_k is the k-th unit vector.

Let $A_j\alpha_0 = C_j = (c_{j1}, \dots, c_{jn})$, $j = 2, \dots, m$. Set $A_j^1 = (c_{j1}, \dots, c_{jn-1})$, $j = 2, \dots, m$. Apply Euler's algorithm to the $(n-1)$-dimensional vector A_2^1 to obtain $A_2^1\alpha_1 = C_2^1 = (0, 0, \dots, c_{n-1}^1)$, where α_1 is an $(n-1)$-dimensional square matrix. Let

$$A_j^1\alpha_1 = C_j^1 = (c_{j1}^1, \dots, c_{jn-1}^1), \quad j = 3, \dots, m.$$

Apply Euler's algorithm to the $(n-2)$-dimensional vector C_3^1, and so on. Finally, we obtain the sequence of matrices $\alpha_0, \alpha_1, \dots, \alpha_{m-1}$ of decreasing size $n, n-1, \dots, n-m+1$. Form the block matrices

$$\beta_j = \begin{pmatrix} \alpha_j & 0 \\ 0 & I_{j+1} \end{pmatrix}, \quad j = 0, \dots, n-m,$$

of size n, where I_{j+1} are the identity matrices of size $j+1$. Set $\gamma = \beta_0\beta_1 \cdots \beta_{m-1}$. Then

$$A_j\gamma = (0, 0, \dots, 0, w_{j,n-j+1}, \dots, w_{j,n}) = W_j, \quad j = 1, \dots, m.$$

The matrix γ is a solution to Problem 1.

4. Power transformations

Let the polynomial

$$f(X) = \sum f_Q X^Q, Q \in \mathbf{S}, \tag{5}$$

where $X = (x_1, \ldots, x_n) \in \mathbb{R}^n$ or $\mathbb{C}^n$, $Q = (q_1, \ldots, q_n) \in \mathbb{Z}^n, Q \geq 0, f_Q$ are constant coefficients from $\mathbb{R}$ or $\mathbb{C}$, $\mathbf{S} = \mathbf{S}(f)$ is the support of f, be given. Let $\mathcal{F}$ be the algebraic variety $f(X) = 0$ and the point $X = X^0 \in \mathcal{F}$.

If X^0 is a simple point, i.e., if at least one derivative $\partial f/\partial x_j$ is nonzero at X^0 then the implicit function theorem implies that the variety $\mathcal{F}$ in the neighborhood of X^0 is described by the equation

$$\Delta x_j = \varphi(\Delta x_1, \ldots, \Delta x_{j-1}, \Delta x_{j+1}, \ldots, \Delta x_n), \tag{6}$$

where $\Delta x_k = x_k - x_k^0$ and φ is a convergent series of its arguments.

If X^0 is not a simple point, then, according to [5, 6] we can seek the branches of the variety $\mathcal{F}$, passing through X^0 in the form of parametric expansions

$$\Delta x_j = \varphi_j(\xi_1, \ldots, \xi_{n-1}), i = 1, \ldots, n, \tag{7}$$

where ξ_k are small parameters and φ_j — are converging power series. To this end the convex hull Γ of the support $\mathbf{S}$ in the space is constructed. Then, Γ is the polyhedron the boundary $\partial\Gamma$ of which consists of (generalized) faces $\Gamma_j^{(d)}$ of dimension d, $0 \leq d < n$. Here j is the face index. Since all vertices $\Gamma_j^{(0)}$ of Γ are integer, each face $\Gamma_j^{(d)}$ has $n-d$ integer linearly independent normals $N_{j1}^{(d)}, \ldots, N_{jn-d}^{(d)} \in \mathbb{R}_*^n$ i.e., normals belonging to the space $\mathbb{R}_*^n$, which is dual of the space $\mathbb{R}^n$.

In addition, each face $\Gamma_j^{(d)}$ is associated with the boundary set

$$D_j^{(d)} = \left\{ Q \in \mathbf{S} \cap \Gamma_j^{(d)} \right\},$$

and the truncated sum is

$$\hat{f}_j^{(d)}(X) = \sum f_Q X^Q \text{ over } Q \in D_j^{(d)}. \tag{8}$$

Theorem 1 **(**[5, Corollary in Chapter II, § 3]**,** [6, Theorem 3.1]**).** *For the face* $\Gamma_j^{(d)}$ *there exists a power transformation*

$$\ln Y = \ln X \cdot \alpha,$$

where $\ln Y = (\ln y_1, \ldots, \ln y_n)$ *and* $\ln X = (\ln x_1, \ldots, \ln x_n)$ *with a unimodular matrix* α*, that takes the truncated sum* (8) *to a polynomial* g *of* d *variables, i.e.,*

$$\hat{f}_j^{(d)}(X) = Y^T g(y_1, \ldots, y_d), \tag{9}$$

where $T = (t_1, \ldots, t_n) \in \mathbb{Z}^n$.

However in [5, 6], it was not pointed out how the unimodular matrix α can be calculated. This is done in the current paper. In [7, Part I, Ch. I, Section 1.9] it was made for $n = 2$. In [1, 8] we describe software of these algorithms. It will be considered in our talk.

References

[1] *Bruno, A.D., Azimov, A.A.* Computing unimodular matrices of power transformations // Programming and Computer Software, 2023, Vol. 49, No. 1, pp. 32–41. DOI: 10.1134/S0361768823010036

[2] *Khinchin, A. Ya.* Continued Fractions, Moscow: Fizmatgiz, 1961 (in Russian); Mineola, NY: Dover, 1997.

[3] *Euler L.* De relatione inter ternas pluresve quantitates instituenda // 1785, All Works 591.

[4] *Bruno, A.D.* Computation of the fundamental units of number rings using a generalized continued fraction, Program. Comput. Software, 2019, vol. 45, no. 2, pp. 37–50. DOI: 10.1134/S036176881902004X.

[5] *Bruno, A.D.* Power Geometry in Algebraic and Differential Equations, Moscow: Nauka, 1998 (in Russian); Amsterdam: Elsevier, 2000.

[6] *Bruno, A.D., Batkhin, A.B.* Resolution of an algebraic singularity by power geometry algorithms, Program. Comput. Software, 2012, vol. 38, no. 2, pp. 57–72.

[7] *Bruno, A.D.* Local Methods in Nonlinear Differential Equations, Berlin: Springer, 1989.

[8] *Bruno, A.D., Azimov, A.A.* Computation of Unimodular Matrices // Preprints of KIAM, Moscow, No 46, 2022 (in Russian). DOI: https://doi.org/10.20948/prepr-2022-46

Alexander Bruno
Singular Problems Department
Keldysh Institute of Applied Mathematics of RAS
Moscow, Russia
e-mail: abruno@keldysh.ru

Alijon Azimov
Algebra and Geometry Department
Samarkand State University after Sh. Rashidov
Samarkand, Uzbekistan
e-mail: Azimov_Alijon_Akhmadovich@mail.ru