COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 12 (2) (1992) 135–142

ON INTEGER POINTS IN POLYHEDRA: A LOWER BOUND

IMRE BÁRÁNY[1], ROGER HOWE and LÁSZLÓ LOVÁSZ

Received April 21, 1989
Revised March 12, 1991

Given a polyhedron $P \subset \mathbb{R}^n$ we write P_I for the convex hull of the integral points in P. It is known that P_I can have at most $O(\varphi^{n-1})$ vertices if P is a rational polyhedron with size φ. Here we give an example showing that P_I can have as many as $\Omega(\varphi^{n-1})$ vertices. The construction uses the Dirichlet unit theorem.

1. Results

Given a polyhedron $P \subset \mathbb{R}^n$ write P_I for the convex hull of integral points in P. P is a rational polyhedron if it is given by finitely many inequalities of the form $a^T x \leq \alpha$ where $a \in \mathbb{Q}^n$ and $\alpha \in \mathbb{Q}$. The size of this inequality is the number of bits necessary to encode it as a binary string (see Schrijver [7]). The size of a rational polyhedron $P \subset \mathbb{R}^n$ is the sum of the sizes of defining inequalities. Strengthening some earlier results of Shevchenko [8] and Hayes and Larman [3], Cook, Hartman, Kannan and McDiarmid [2] have proved recently that P_I can have at most $2m^n(12n^2\varphi)^{n-1}$ vertices where m is the number of defining inequalities. For some other results and comments see their paper [2]. For $n = 2$ and $n = 3$ there are examples in [6] and in [5] showing that P_I can have as many as $\Omega(\varphi^{n-1})$ vertices. Here we give such a construction for every $n \geq 2$.

Theorem 1. *For fixed $n \geq 2$ and for any $\varphi > 0$ there exists a rational simplex $P \subset \mathbb{R}^n$ of size at most φ such that the number of vertices of P_I is at least $c\varphi^{n-1}$ where c is a constant depending only on n.*

The proof will be based on the following construction. The automorphism group of the lattice $\mathbb{Z}^n$ consists of all integral matrices with determinant 1. We are going to construct a subgroup of this group which is isomorphic to $\mathbb{Z}^{n-1}$ in a non-trivial way. (A trivial subgroup of this form is the group of all matrices which differ from the identity matrix only in the first $n-1$ entries of the last column.) More exactly, we show the following.

AMS subject classification code (1991): 52 C 07, 11 H 06

[1] The results of the paper were obtained while this author was visiting the Cowles Foundation at Yale University

Theorem 2. *There exist n by n integral matrices $A_1, A_2, \ldots, A_{n-1}$ with determinant 1, with the following properties:*

(1) *Every A_k has the same set of eigenvectors $\{s_1, \ldots, s_n\}$.*
(2) *Let λ_{ki} be the eingenvalue of A_k belonging to s_i; then $\lambda_{ki} > 0$.*
(3) *The vectors $\Lambda_k \in \mathbb{R}^n$ $(k = 1, \ldots, n-1)$ are linearly independent over the reals, where the i-th component of Λ_k is $\Lambda_{ki} = \log \lambda_{ki}$.*

Clearly, condition (3) is equivalent to the following

(4) The vectors $\sum_{k=1}^{n-1} \alpha_k \Lambda_k$ where $a = (\alpha_1, \ldots, \alpha_{n-1})^T \in \mathbb{Z}^{n-1}$ form an $(n-1)$-dimensional lattice L in $\mathbb{R}^n$.

The lattice L is orthogonal to the vector $(1, \ldots, 1)^T \in \mathbb{R}^n$. This follows from $\det A = 1$. Another way to put (3) or (4) is to say that the matrices $A_1, \ldots, A_{n-1}$ multiplicatively generate a free commutative subgroup Γ of the automorphism group of $\mathbb{Z}^n$, isomorphic to an $(n-1)$-dimensional lattice.

As a matter of fact, Theorem 2 can be deduced from the Dirichlet unit theorem (see, e.g. [1]). We will explain how this can be done. For the sake of the reader who is not familiar with algebraic number theory a separate and selfcontained proof of Theorem 2 will be given in the third section.

2. Proof of Theorem 1

We use Theorem 2. Set $S = \operatorname{cone}\{s_1, \ldots, s_n\}$ and consider the convex hull H of $\mathbb{Z}^n \cap \operatorname{int} S$. Note that S and $\mathbb{Z}^n$ are invariant under Γ, and therefore so is H. The set H is not a polyhedron but its intersection with any supporting hyperplane $u^T x = \gamma$ with $u^T s_i > 0$ $(i = 1, \ldots, n)$ is a polytope, and if we take u "generic" then this intersection is a single vertex $v = (v_1, \ldots, v_n)^T$. Define the set

$$V = \{Av : A \in \Gamma\} = \{A_1^{\alpha_1} \ldots A_{n-1}^{\alpha_{n-1}} v \in \mathbb{R}^n : a = (\alpha_1, \ldots, \alpha_{n-1})^T \in \mathbb{Z}^{n-1}\}.$$

Clearly $V \subset \mathbb{Z}^n \cap \operatorname{int} S$.

Claim. *Each point of V is an extreme point of H.*

Proof. The hyperplane $(A^{-1}u)^T x = \gamma$ supports H and has the unique point Av in common with it. ∎

Consider now $\varphi \in \mathbb{R}$, large enough, and the sets

$$B(\varphi) = \{w = \omega_1 s_1 + \ldots + \omega_n s_n : 0 \le \omega_i \le 2^\varphi \quad i = 1, \ldots, n\}$$

and

$$H(\varphi) = B(\varphi)_I = \operatorname{conv}(B(\varphi) \cap \mathbb{Z}^n).$$

Then $H(\varphi)$ is a polytope and every point in $V \cap B(\varphi)$ is a vertex of it. The cardinality of $V \cap B(\varphi)$ is the same as the number of points $a \in \mathbb{Z}^{n-1}$ with

$$\sum_{k=1}^{n-1} \alpha_k \log \lambda_{ki} + \log v_i \le \varphi, \qquad i = 1, \ldots, n.$$

In view of (4), this number is essentially the same as the $(n-1)$-dimensional volume of the set defined by the inequalities

$$\sum_{k=1}^{n-1} x_k \log \lambda_{ki} + \log v_i \le \varphi, \qquad i = 1, \dots, n.$$

As this set is a simplex, its volume is $\text{const} \cdot \varphi^{n-1}$ with the constant depending only on $A_1, \dots, A_{n-1}$. Thus the number of vertices of $H(\varphi)$ is at least $\text{const} \cdot \varphi^{n-1}$.

Now we are going to replace $B(\varphi)$ with a polytope Q of small size, such that $Q_I = H(\varphi)$ (and so Q_I has $\text{const} \cdot \varphi^{n-1}$ vertices). The point $x = \xi_1 s_1 + \dots + \xi_n s_n \in \mathbb{R}^n$ has components $x_1, \dots, x_n$ in the standard basis of $\mathbb{R}^n$. Let $v_i \in \mathbb{Z}^n \cap B(\varphi)$ be the point with minimal i-th component in the basis $s_1, \dots, s_n$ $(i = 1, \dots, n)$, and let m_i be the i-th component of v_i. Then the inequality $\xi_i \ge m_i$ is implied by n inequalities that define facets of $H(\varphi)$. These inequalities have the form

$$0 \ge \det \begin{pmatrix} 1 & \dots & 1 & 1 \\ w_1 & \dots & w_n & x \end{pmatrix} = b_0 + b_1 x_1 + \dots + b_n x_n \tag{5}$$

where $w_i \in H(\varphi)$. As the Euclidean distance of w_i from the origin is at most $n2^{\varphi}$, its components in the standard basis are at most $n2^{\varphi}$ in absolute value. So b_i is equal to the value of an integral n by n determinant all of whose entries are at most $n2^{\varphi}$ in absolute value. Then the size of the inequality (5) is at most $\text{const} \cdot \varphi$ where the constant depends only on $A_1, \dots, A_{n-1}$. The number of such inequalities is n for each v_i and so it is n^2 altogether. Similarly, we can replace the inequalities $\xi_i \le 2^{\varphi}$ by n^2 inequalities with size $O(\varphi)$ such that the resulting $2n^2$ inequalities define a polytope Q contained in $B(\varphi)$ but containing $H(\varphi)$. So $Q_I = H(\varphi)$ as claimed.

Finally, we cut Q into simplices $P^1, \dots, P^N$ whose vertices are all vertices of Q. The number N of such simplices will clearly be bounded by a constant (depending only on n). Now every vertex of Q_I is a vertex of one of the $(P^j)_I$, so at least one of them has $\text{const} \cdot \varphi^{n-1}$ vertices. Since the size of each P^j is bounded by $\text{const} \cdot \varphi$, this proves the theorem. ∎

Remark. A similar argument shows that the number of k-dimensional faces ($k = 0, 1, \dots, n-1$) of P_I is at least $\text{const} \cdot \varphi^{n-1}$. It would be interesting to extend the results of [2] by showing that P_I has at most $O(\varphi^{n-1})$ k-dimensional faces for any polytope P of size φ.

3. Proof of Theorem 2

To avoid some trivial complications, we assume that $n > 2$. Define the polynomial

$$p(\lambda) = (\lambda - 2)(\lambda - 4) \dots (\lambda - 2n) + 1 = \lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_0.$$

Clearly, $a_{n-1}, \dots a_0$ are integers. Computing p at $\lambda = 1, 3, \dots, 2n+1$ we see that p has n real roots $\lambda_1 < \lambda_2 < \dots < \lambda_n$. The root λ_i is close to $2i$, more precisely:

$$|\lambda_i - 2i| < 1 \text{ and so } |\lambda_i - 2j| > 1 \text{ when } i \ne j. \tag{6}$$

Define the n by n integral matrix A as

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ -a_0 & -a_1 & \dots & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

Then, as it is well-known and actually easy to check

$$\det(A - \lambda I) = (-1)^n p(\lambda).$$

Hence A has n (real) eigenvectors $s_1, \dots s_n$ with $As_i = \lambda_i s_i$. Define now

$$A_k = A - 2kI, \qquad k = 1, 2, \dots, n.$$

Then $A_k s_i = (A - 2kI)s_i = (\lambda_i - 2k)s_i$ and so A_k has the same set of eigenvectors as A with eigenvalues $\lambda_{ki} = \lambda_i - 2k$. Then $\det(A_k) = (-1)^n p(2k) = (-1)^n$ and $A_1 \dots A_n = -I$, because $A_1 \dots A_n s_i = \prod_{k=1}^{n} \lambda_{ik} s_i = \prod_{k=1}^{n} (\lambda_i - 2k)s_i = -s_i$. Next, we prove that the vectors Λ'_k are linearly independent, where $\Lambda'_{kj} = \log|\lambda_j - 2k|$. Then the requirements of the theorem will be satisfied by the matrices $A_1^2, A_2^2, \dots, A_{n-1}^2$. So assume

$$\sum_{k=1}^{n-1} \alpha_k \Lambda'_k = 0$$

for some real numbers $\alpha_1, \dots, \alpha_{n-1}$. Defining $\alpha_n = 0$ we have

$$\sum_{k=1}^{n} \alpha_k \Lambda'_k = 0.$$

Set $|\alpha_j| = \max\{|\alpha_k| : k = 1, \dots, n\}$. If $j = n$ then we are done. So $j \neq n$ and consider the j-th component of the above equation:

$$\sum_{k=1}^{n} \alpha_k \log|\lambda_j - 2k| = 0.$$

Then, using (6),

$$\begin{aligned} \Big|\alpha_j \log|\lambda_j - 2j|\Big| &= \Big|\sum_{k \neq j} \alpha_k \log|\lambda_i - 2k|\Big| \leq \sum_{k \neq j} |\alpha_k| \Big|\log|\lambda_j - 2k|\Big| \\ &= \sum_{k \neq j} |\alpha_k| \log|\lambda_j - 2k| \leq |\alpha_j| \sum_{k \neq j} \log|\lambda_j - 2k| \\ &= |\alpha_j| \Big|\log|\lambda_j - 2j|\Big| \end{aligned}$$

because $A_1 \dots A_n = -I$ implies $\sum_{k=1}^{n} \log|\lambda_i - 2k| = 0$. But then equality holds throughout and so $|\alpha_j| = |\alpha_n| = 0$. ∎

4. Remarks on the construction

We make some remarks on the structure of lattice points in the cone S spanned by the eigenvectors of a group Γ with the properties in Theorem 2.

For $x=\xi_1 s_1+\ldots+\xi_n s_n$ define

$$\operatorname{prod}(x)=\prod_{i=1}^{n}\xi_i.$$

Then for all $x\in S$ and $A\in\Gamma$, $\operatorname{prod}(Ax)=\operatorname{prod}(x)$. Indeed,

$$\operatorname{prod}(A_k x)=\prod_{i=1}^{n}\lambda_{ki}x_i=\operatorname{prod}(x)\prod_{i=1}^{n}\lambda_{ki}\operatorname{prod}(x)\det(A_k)=\operatorname{prod}(x)$$

and hence the assertion follows by an easy induction. Moreover, it is easy to see that the function $f(x)=\log\operatorname{prod}(x)$ is strictly concave on $\operatorname{int}S$. Hence the set $\{x\in S:\operatorname{prod}(x)\geq\operatorname{prod}(v)\}$ is convex and each point of V lies on its boundary.

The function prod assumes only a set of discrete values on the set $\mathbb{Z}^n\cap\operatorname{int}S$. This follows immediately if one uses the Dirichlet unit theorem: prod is proportional to the norm of the appropriate algebraic integer and the norm takes integral values only (see section 5, and also [1], [4]). Another way to see this is to fix any $A\in\Gamma$ with eigenvalues $\lambda_1,\ldots,\lambda_n$. Let M be the Vandermonde matrix with $M_{ij}=\lambda_i^{j-1}$. Then we have the identity

$$\operatorname{prod}(v)(\det[s_1,\ldots,s_n])(\det M)=\det[v,Av,\ldots,A^{n-1}v].$$

Since the right hand side is an integer, $\operatorname{prod}(v)$ is a fixed constant multiple of an integer.

Let us choose $v\in\mathbb{Z}^n\cap\operatorname{int}S$ so that $\operatorname{prod}(v)$ is minimum. Then we have three rather similar sets: $V=\{Av:A\in\Gamma\}$, V', the set of all lattice points in S with $\operatorname{prod}(w)=\operatorname{prod}(v)$, and V'', the set of all vertices of $\operatorname{conv}(\operatorname{int}(S)\cap\mathbb{Z}^n)$. Clearly $V\subseteq V'\subseteq V''$, and all three sets are invariant under the group Γ.

The sets $K=\operatorname{conv}V$, $K'=\operatorname{conv}V'$ and $H=\operatorname{conv}V''$ are not polyhedra because they are the convex hulls of infinitely many points. However, "locally" they are polytopes. More generally, let U be a discrete set in $\operatorname{int}(S)$ invariant under Γ and u, a vertex of $\operatorname{conv}U$. Let Q be the minimal cone having apex u and containing U. We define a face of $\operatorname{conv}U$ as the intersection of $\operatorname{conv}U$ with a hyperplane H such that one halfspace with boundary H contains U.

Claim. *Q is a polyhedral cone. Moreover, each face of $\operatorname{conv}U$ is bounded (and hence a polytope).*

Proof. We show first that U contains points arbitrarily close to the ray $\{ts_j:t>0\}$ for every $j=1,\ldots,n$. For notational convenience we do so only when $j=1$. Since

$$A_1^{\alpha_1}\ldots A_{n-1}^{\alpha_{n-1}}u=\prod_{k=1}^{n-1}\lambda_{k1}^{\alpha_k}u_1s_1+\ldots+\prod_{k=1}^{n-1}\lambda_{kn}^{\alpha_k}u_ns_n,$$

we have to prove the existence of $(\alpha_1,\ldots,\alpha_{n-1})^T\in\mathbb{Z}^{n-1}$ with

$$\prod_{k=1}^{n-1} \lambda_{ki}^{\alpha_k} u_i < \varepsilon, \qquad (i = 2, \dots, n)$$

for any fixed $\varepsilon > 0$. But this is the same as

$$\sum_{k=1}^{n-1} \alpha_k \Lambda_{ki} + \log \nu_i < \log \varepsilon, \qquad (i = 2, \dots, n).$$

The existence of such a vector $a \in \mathbb{Z}^{n-1}$ is guaranteed by condition (4) and the fact that L is orthogonal to the vector of all ones.

Define now $\varepsilon = \frac{1}{2} \min\{u_1, \dots, u_n\} > 0$. Let $w_j \in U$ be any point closer than ε to the ray $\{ts_j : t > 0\}$. Define the cone C with apex u as

$$C = u + \operatorname{cone}\{w_1 - u, \dots, w_n - u\}.$$

Clearly $C \subset Q$. It is easy to see that the set $S \setminus C$ is bounded. Then the discreteness of U implies that $S \subset C$ contains finitely many points from U, $v_1, \dots, v_m$, say. Then

$$Q = u + \operatorname{cone}\{w_1 - u, \dots, w_n - u, v_1 - u, \dots, v_m - u\}$$

and so Q is a polyhedral cone. It also follows that every face containing u must be the convex hull of points in $U \cap (S \setminus C)$, and so it is a polytope. ∎

Using the above construction one can find highly regular triangulations of $\mathbb{R}^{n-1}$ that are perhaps new and interesting. Consider $K = \operatorname{conv} V$, and assume each facet of it is a simplex. This gives rise to a simplical complex $\mathcal{K}$ with (infinite) vertex set where vertices $w_1, \dots, w_d$ form a simplex if their convex hull is a face of $\operatorname{conv} U$. $\mathcal{K}$ is $(n-1)$-dimensional and can be represented as a triangulation T of $\mathbb{R}^{n-1}$ with vertex set $\mathbb{Z}^{n-1}$ in the following way. For $a = (\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{Z}^n$, let $v^a = A_1^{\alpha_1} \dots A_{n-1}^{\alpha_{n-1}} v$. The points $a_1, \dots, a_d \in \mathbb{Z}^{n-1}$ form a simplex if the convex hull of the points $v^{a_1}, \dots, v^{a_{n-1}}$ is a face of K. The triangulation T is invariant under translations from $\mathbb{Z}^{n-1}$. The geometric properties of T could be deduced from those of the cone$Q$. When one uses the Dirichlet unit theorem for the construction, the triangulation comes from an irreducible polynomial. So most probably, there are many different triangulations of this type. We do not go into the study of such triangulations in this paper.

5. Relation to totally real number fields

The above construction is a particularly transparent case of a general phenomenon of algebraic number theory. Precisely, given $A_1, \dots, A_{n-1}$ as in Theorem 2, let $\mathcal{A}_{\mathbb{Q}}$ be the set of all linear combinations, with rational coefficients, of the products of the A_k's. Let $\mathcal{A}_{\mathbb{R}}$ be defined similarly, but allow real coefficients. And let $\mathcal{I}$ be what you get when you restrict yourself to integer coefficients. Then $\mathcal{A}_{\mathbb{R}}$ will be an n-dimensional vector space and will be an algebra, i.e., closed under multiplication. Also $\mathcal{I}$ will be a lattice in $\mathcal{A}_{\mathbb{R}}$, and will also be closed under multiplication. Each matrix A_k will be a unit of $\mathcal{I}$, in the sense that A_k^{-1} will also be in $\mathcal{I}$. This is so because, since A_k is integral with determinant 1, it satisfies an equation

$$A^n + c_1 A^{n-1} + \dots + c_{n-1} A + I = 0$$

where the c_i are integers. Hence

$$A_k^{-1} = -(c_{n-1}I + c_{n-2}A_k + \ldots + c_1 A_k^{n-2} + A_k^{n-1})$$

and the right hand side is obviously in $\mathcal{I}$.

The entity $\mathcal{A}_{\mathbb{Q}}$ is a vector space of dimension n over $\mathbb{Q}$, and is closed under multiplication. In fact, $\mathcal{A}_{\mathbb{Q}}$ is a field: every element in it is invertible. It is a type of field known as *totally real number field*. Precisely, a totally real number field is a field generated by the rational numbers $\mathbb{Q}$ together with an element x which satisfies an equation

$$p(x) = x^n + c_1 x^{n-1} + \ldots + c_1 x + c_n = 0$$

with all c_i's in $\mathbb{Q}$. The polynomial p should be irreducible over $\mathbb{Q}$, but should have n distinct real roots.

Given a totally real number field F, there is a distinguished spanning lattice I_F in F, called the *ring of integers of* F. It consists of all elements of F which satisfy polynomials with coefficients in $\mathbb{Z}$ and main coefficient 1. It is closed under multiplication. Let U be the group of *units* of I_F, i.e. elements A of I_F such that A^{-1} is also in I_F. Then the Dirichlet unit theorem [1], [4] guarantees that U contains $n-1$ elements A_k as required by Theorem 2. Other objects of the discussion can also be interpreted as appurtenances of a totally real number field.

Acknowledgement. The authors thank Herb Scarf, Bill Cook, Ravi Kannan and David Shallcross for fruitful discussions, the Cowles Foundation for hospitality, and the referee for suggesting substantial improvements in the presentation.

References

[1] Z. I. BOREVICH, and I. R. SAFAREVICH: *Number theory,* Academic Press, New York and London, 1966.

[2] W. COOK, M. HARTMANN, R. KANNAN, and C. MCDIARMID: On integer points in polyhedra, *Combinatorica* **12** (1992), 27–37.

[3] A. C. HAYES, and D. G. LARMAN: The vertices of the knapsack polytope, *Discrete Applied Math.* **6** (1983), 135–138.

[4] S. LANG: *Algebraic number theory,* Graduate Texts in Mathematics 110, Springer Verlag, New York etc., 1986.

[5] D. MORGAN: Personal communication, 1989.

[6] D. S. RUBIN: On the unlimited number of faces in integer hulls of linear programs with a single constraint, *Operations Research* **18** (1970), 940–946.

[7] A. SCHRIJVER: *Theory of linear and integer programming,* Wiley, Chichester, 1987.

[8] V. N. SHEVCHENKO: On the number of extreme points in integer programming, *Kibernetika* **2** (1981), 133–134.

Imre Bárány

Mathematical Institute,
Pf. 127, 1364 Budapest,
Hungary
h2923bar@ella.hu

Roger Howe

Department of Mathematics,
Yale University,
New Haven, CT 06520,
U. S. A.

László Lovász

Department of Computer Science,
Eötvös University,
1088 Budapest, Múzeum krt. 6–8.
Hungary
h599lov@ella.hu

and

Princeton University,
Princeton, NJ 08544,
U. S. A.