Selçuk J. Appl. Math.
Vol. 7. No. 1. pp. 3-8, 2006

Selçuk Journal of Applied Mathematics

Integrally Indecomposable Polytopes

Fatih Koyuncu

Muğla University, Faculty of Arts and Sciences, Department of Mathematics 48000, Muğla, Turkey

e-mail: fatih@mu.edu.tr

Received: January 7, 2005

Summary. Gao gave a criterion for the integral indecomposability, with respect to the Minkowski sum, of polytopes lying inside a pyramid with an integrally indecomposable base. Here, we weakened this criterion to the polytopes lying inside the convex hull of two polytopes, one of which is integrally indecomposable, being in two parallel nonintersecting hyperplanes.

Key words: Polytopes, integral indecomposability, multivariate polynomials.

1. Introduction

Let $\mathbb{R}^n$ denote the n-dimensional Euclidean space and S be a subset of $\mathbb{R}^n$. The smallest convex set containing S, denoted by *conv(S)*, is called the *convex hull* of S. If $S = \{a_1, a_2, ..., a_n\}$ is a finite set then we shall denote $conv(S)$ by $conv(a_1, ..., a_n)$. It is straightforward to show that

$$conv(S) = \left\{ \sum_{i=1}^{k} \lambda_i x_i : x_i \in S, \lambda_i \geq 0, \sum_{i=1}^{k} \lambda_i = 1 \right\}.$$

The principle operation for convex sets in $\mathbb{R}^n$ is defined as follows.

Definition 1. For any two sets A and B in $\mathbb{R}^n$, the sum

$$A + B = \{a + b : \ a \in A, \ b \in B\}$$

is called *Minkowski sum*, or vector addition of A and B.

The convex hull of finitely many points in $\mathbb{R}^n$ is called a *polytope.*

A point in $\mathbb{R}^n$ is called *integral* if its coordinates are integers. A polytope in $\mathbb{R}^n$ is called *integral* if all of its vertices are integral. An integral polytope C is called *integrally decomposable* if there exist integral polytopes A and B such that $C = A + B$ where both A and B have at least two points. Otherwise, C is called *integrally indecomposable.*

Definition 2.. Let F be any field and consider any multivariate polynomial

$$f(x_1, x_2, ..., x_n) = \sum c_{e_1 e_2 ... e_n} x_1^{e_1} x_2^{e_2} ... x_n^{e_n} \in F[x_1, ..., x_n].$$

We can think an exponent vector $(e_1, e_2, ..., e_n)$ of f as a point in $\mathbb{R}^n$. The *Newton polytope* of f, denoted by P_f, is defined as the convex hull in $\mathbb{R}^n$ of all the points $(e_1, ..., e_n)$ with $c_{e_1 e_2 ... e_n} \neq 0$.

A polynomial over a field F is called *absolutely irreducible* if it remains irreducible over every algebraic extension of F.
Using Newton polytopes of multivariate polynomials, we can determine infinite families of absolutely irreducible polynomials over an arbitrary field F by the following result due to Ostrowski [5], *c.f.* [2].

Lemma 1. Let $f, g, h \in F[x_1, ..., x_n]$ with $f = gh$. Then $P_f = P_g + P_h$

As a direct result of Lemma 1, we have the following corollary which is an *irreducibility criterion* for multivariate polynomials over arbitrary fields.

Corollary. Let F be any field and f a nonzero polynomial in $F[x_1, ..., x_n]$ not divisible by any x_i. If the Newton polytope P_f of f is integrally indecomposable then f is absolutely irreducible over F.

When P_f is integrally decomposable, depending on the given field, f may be reducible or irreducible. For example, the polynomial $f = x^9 + y^9 + z^9$ has the Newton polytope

$$\begin{aligned} P_f &= conv((9,0,0),(0,9,0),(0,0,9)) \\ &= conv((6,0,0),(0,6,0),(0,0,6)) + conv((3,0,0),(0,3,0),(0,0,3)). \end{aligned}$$

But, while $f = x^9 + y^9 + z^9 = (x + y + z)^9$ over $\mathbb{F}_3$, it is irreducible over $\mathbb{F}_2, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}$, where $\mathbb{F}_m$ represents the finite field with m elements.

In [2], [3] and [4], infinitely many integrally indecomposable polytopes in $\mathbb{R}^n$ are presented and then, being associated to these polytopes, infinite families of absolutely irreducible polynomials are determined over any field F.

We need some new terminologies. For details, see [1].

Definition 3. For $\alpha \in \mathbb{R}, \beta \in \mathbb{R}^n$ the set

$$H = \{x \in \mathbb{R}^n : \beta \cdot x = \alpha\}$$

is called a *hyperplane*, where

$$\beta \cdot x = \beta_1 v_1 + ... + \beta_n v_n$$

is the dot product of the vectors $\beta = (\beta_1, ..., \beta_n)$, $v = (v_1, ..., v_n)$. In a natural manner, the closed halfspaces formed by H are defined as

$$H^- = \{x \in \mathbb{R}^n : \beta \cdot x \leq \alpha\}, \quad H^+ = \{x \in \mathbb{R}^n : \beta \cdot x \geq \alpha\}.$$

A hyperplane H_K is called a *supporting hyperplane* of a closed convex set $K \subset \mathbb{R}^n$ if $K \subset H_K^+$ or $K \subset H_K^-$ and $K \cap H_K \neq \emptyset$, i.e. H_K contains a boundary point of K. A supporting hyperplane H_K of K is called nontrivial if K is not contained in H_K. The halfspace H_K^- (or H_K^+) is called a supporting halfspace of K, possibly we may have $K \subset H_K$.
Let $C \subset \mathbb{R}^n$ be a compact convex set. Then for any nonzero vector $v \in \mathbb{R}^n$, the real number $s = sup_{x \in C}(x \cdot v)$ is defined as $max\{x \cdot v : x \in C\}$, where

$$x \cdot v = x_1 v_1 + ... + x_n v_n$$

is the dot product of the vectors $x = (x_1, ..., x_n)$ and $v = (v_1, ..., v_n)$.

Let $K \subset \mathbb{R}^n$ be a nonempty convex compact set. The map

$$h_K : \mathbb{R}^n \to \mathbb{R}, \qquad u \to sup_{x \in K}(x \cdot u)$$

is called the support function of K.
Let $K \subset \mathbb{R}^n$ be a nonempty convex compact set. For every fixed nonzero vector $u \in \mathbb{R}^n$, the hyperplane having normal vector u is defined as

$$H_K(u) = \{x \in \mathbb{R}^n : x \cdot u = h_K(u)\}.$$

Note that $H_K(u)$ is a supporting hyperplane of K.

It is known that every supporting hyperplane of K has a representation of this form. See [1].

Let P be a polytope. The intersection of P with a supporting hyperplane H_P is called a *face* of P. A vertex of P is a face of dimension zero. An *edge* of P is a face of dimension 1, which is a line segment. A face F of P is called a *facet* if dim (F)= dim (P) -1. If u is any nonzero vector in $\mathbb{R}^n$, $F_P(u) = H_P(u) \cap P$ shows the face of P in the direction of u, that is the intersection of P with its supporting hyperplane $H_P(u)$ having outer normal vector u. And, it is known that $F_P(u) = F_Q(u) + F_R(u)$ if $P = Q + R$ for some polytopes Q and R.

If P is a polytope and v is a point in $\mathbb{R}^n$ then, the translation of P by v is the set

$$P + v = \{a + v : a \in P\}$$

The following theorem explains the most important properties about the decomposition of polytopes. Especially, it shows how faces of a polytope decompose in a Minkowski sum of polytopes.

Theorem 1. *(a)* If h_K and h_L are the support functions of the convex sets K and L in $\mathbb{R}^n$ respectively, then, $h_K + h_L$ is the support function of $K + L$, i.e.

$$h_{K+L} = h_K + h_L.$$

(b) $H_{K+L} = H_K + H_L$.
(c) If F is a face of $K + L$, then there exist unique faces F_K, F_L of K, L respectively such that

$$F = F_K + F_L.$$

In particular, each vertex of $K + L$ is the sum of unique vertices of K, L respectively.
(d) If K and L are polytopes, then so is $K + L$.
(e) If A is a polytope in $\mathbb{R}^n$ with $A = B + C$, then so are B and C (which are called *summands* of A).

Proof: See, e.g., the proof of [1].

A New Criterion for Integral Indecomposability

In [2], Gao gave the following result.

Theorem 2. Let Q be an integrally indecomposable polytope in $\mathbb{R}^n$ which is contained in a hyperplane H and having at least two points. Let $v \in \mathbb{R}^n$ be an arbitrary point which is not contained in H. If S is any set of integral points in the pyramid $conv(v, Q)$, then the polytope $P = conv(Q, S)$ is integrally indecomposable.

Our new criterion is given as follows.

Theorem 3. Let $v \in \mathbb{R}^n$, H_1 and $H_2 = H_1 + v$ be nonintersecting parallel hyperplanes in $\mathbb{R}^n$, and let Q_1 be an integrally indecomposable polytope lying inside H_1 and having at least two points. Consider the polytope $Q_2 \subset Q_1 + v \subset H_2$. Assume that at least one of the vertices of Q_2 does not lie on the boundary of the polytope Q_1+v. If S is any set of integral points in the polytope $conv(Q_1, Q_2)$ then the polytope $P = conv(Q_1, S)$ is integrally indecomposable.

Proof. Let $P = conv(Q_1, S)$ be the polytope as described in Figure 1. Observe that, since $Q_1 = P \cap H_1$, Q_1 is a face of P. If $P = K + L$ for some integral polytopes K and L then, by Theorem 1, K and L have unique faces K_1 and L_1

respectively, such that $Q_1 = K_1 + L_1$. While Q_1 is integrally indecomposable, K_1 or L_1 must consist of only one point, say $K_1 = \{a\}$ for some point $a \in \mathbb{R}^n$, and hence $L_1 = Q_1 + (-a)$. Shifting K and L suitably, i.e. writing

$$P = (K + (-a)) + (L + a),$$

we may suppose that $K_1 = \{0\}$ and $L_1 = Q_1$. Our aim is to show that K must contain only one point, i.e. $K = K_1 = \{0\}$. But, this is geometrically obvious from Figure 1, since for $0 \neq u \in \mathbb{R}^n$, any shifting $u + Q_1$ cannot lie in the polytope $conv(Q_1, Q_2)$.

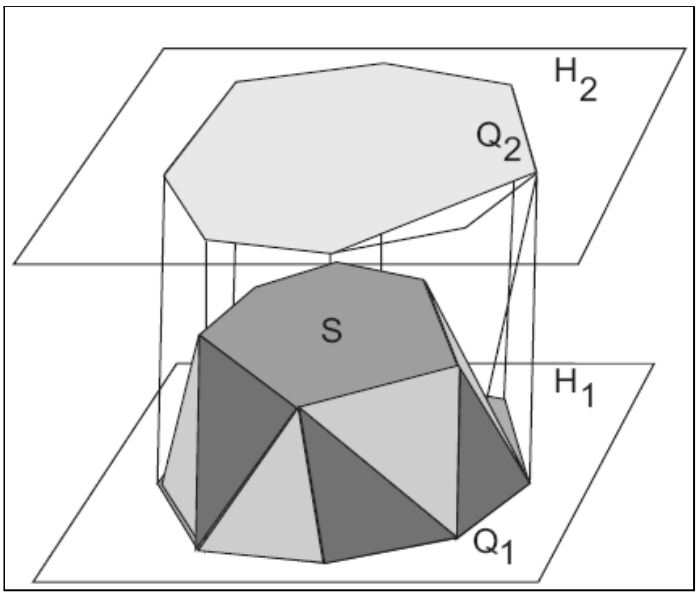

Figure 1.

Example1. Let m and n be relatively prime positive integers, and $c \geq 0$ and $d \geq n + 1$ be arbitrary integers. Then, the quadrangle

$$Q = conv((m, 0), (m + 1, d + c), (0, d), (0, n))$$

is integrally indecomposable by Theorem 2, or Theorem 3. Consequently, by Theorem 3, the integral polytopes

$$A = conv((m, 0, 0), (m + 1, d + c, 0), (0, d, 0), (0, n, 0), (m, 0, r), (0, d, r), (0, n, r)),$$

$$B = conv((m, 0, 0), (m{+}1, d{+}c, 0), (0, d, 0), (0, n, 0), (m, 0, r), (m{+}1, d{+}c, r), (0, d, r)),$$

$$C = conv((m, 0, 0), (m{+}1, d{+}c, 0), (0, d, 0), (0, n, 0), (m, 0, r), (m{+}1, d{+}c, r), (0, n, r))$$

are integrally indecomposable, where r is any positive integer, see Figure 2.

For example, taking $m = 10$, $n = 21$, $d = 30$, $c = 5$ and $r = 70$, we see that the integral polytope

$$P = conv((10,0,0),(11,35,0),(0,30,0),(0,21,0),(10,0,70),(0,30,70),(0,21,70))$$

is integrally indecomposable.
As a result, the multivariate polynomial

$$f = a_1x^{10}+a_2x^{11}y^{35}+a_3y^{30}+a_4y^{21}+a_5x^{10}z^{70}+a_6y^{30}z^{70}+a_7y^{21}z^{70}+\sum c_{ijk}x^iy^jz^k,$$

with $(i,j,k) \in P$ and $a_i \in F \setminus \{0\}$, is absolutely irreducible over any field F by Corollary 1.

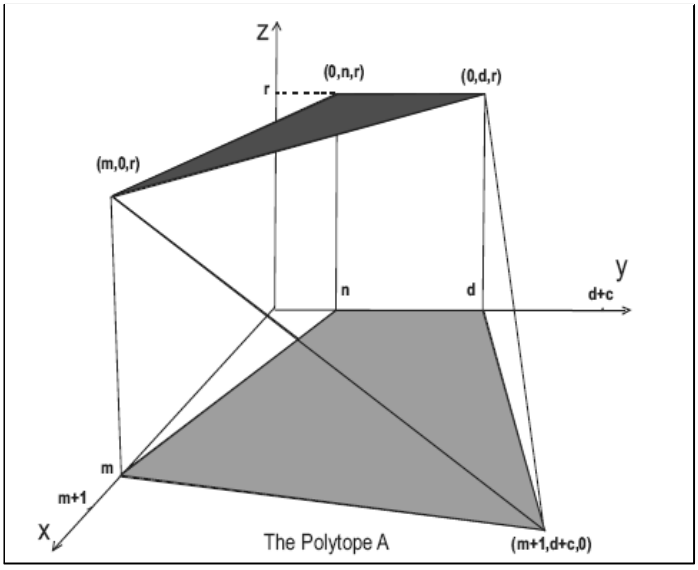

Figure 2.

References

1. Ewald G. (1996): *Combinatorial Convexity and Algebraic Geometry*, GTM 168, Springer.

2. Gao S. (2001): *Absolute irreducibility of polynomials via Newton polytopes*, Journal of Algebra 237, No.2 501-520.

3. Gao S. (2001): *Decomposition of Polytopes and Polynomials*, Discrete and Computational Geometry 26 , No. 1, 89-104.

4. Koyuncu F., Özbudak F. : *A Geometric Approach to Absolute Irreducibility of Polynomials*, submitted.

5. Ostrowski A. M. (1975): *On multiplication and factorization of polynomials*, I. Lexicographic orderings and extreme aggregates of terms, Aequationes Math. 13, 201-228.