ABSOLUTE IRREDUCIBILITY OF POLYNOMIALS VIA NEWTON POLYTOPES

SHUHONG GAO

Abstract. A multivariable polynomial is associated with a polytope, called its Newton polytope. A polynomial is absolutely irreducible if its Newton polytope is indecomposable in the sense of Minkowski sum of polytopes. Two general constructions of indecomposable polytopes are given, and they give many simple irreducibility criteria including the well-known Eisenstein's criterion. Polynomials from these criteria are over any field and have the property of being absolutely irreducible when one modifies their coefficients arbitrarily in the field, keeping only some of them nonzero. Some results on Minkowski sums of convex sets and polyhedra are also presented.

1. Introduction

It is well-known that Eisenstein's criterion gives a simple condition for a polynomial to be irreducible. Over the years this criterion has witnessed many variations and generalizations using Newton polygons, prime ideals and valuations; see for examples [3, 19, 22, 32]. We examine the Newton polygon method and generalize it through Newton polytopes associated with multivariable polynomials. Since the Newton polygon of a polynomial is only a small fraction of its Newton polytope, our method is much more powerful. Absolute irreducibility of polynomials is crucial in many applications including but not limited to finite geometry [11], combinatorics [40], algebraic geometric codes [39], permutation polynomials [23] and function field sieve [1]. We present many infinite families of absolutely irreducible polynomials over an arbitrary field. These polynomials remain absolutely irreducible when their coefficients are modified arbitrarily with only some of them nonzero.

As in many standard algebra textbooks, Eisenstein's criterion [5] is described as follows.

Eisenstein's criterion. *Let R be a unique factorization domain and $f = f_0 + f_1X + \cdots + f_nX^n \in R[X]$. If there is a prime $p \in R$ such that all the coefficients except f_n of f are divisible by p, but f_0 is not divisible by p^2, then f is irreducible in $R[X]$.*

Several people (Dumas [4], Kurschak [17], Ore [24, 25, 26], Rella [29]) have generalized this criterion by using Newton polygons. Assume that $f_0f_n \neq 0$. One can construct a polygon in the plane $\mathbb{R}^2$ where $\mathbb{R}$ is the set of real numbers. Suppose that the coefficient f_i is exactly divisible by p^{a_i} where $a_i \geq 0$ and a_i is undefined if $f_i = 0$. Plot the points $(0, a_0)$, $(1, a_1)$, ... , (n, a_n) in the plane $\mathbb{R}^2$ and form the

Date: September 11, 1998.

1991 *Mathematics Subject Classification.* Primary 12E05, 11Y11; Secondary 13P05, 13B25, 12Y05,

Key words and phrases. Fields, absolute irreducibility, Newton polytopes, Newton polygons, indecomposable polytopes, Eisenstein criterion, convex sets, polyhedra.

lower convex hull of these points. This results in a sequence of line segments starting at the y-axis and ending at the x-axis, called the Newton polygon of f (with respect to the prime p). Dumas [4] determines the degrees of all the possible nontrivial factors of f in terms of the widths of the line segments on the Newton polygon of f. Consequently a simple criterion for the irreducibility of f is established.

Eisenstein-Dumas criterion. *Let R be a unique factorization domain and $f = f_0 + f_1X + \cdots + f_nX^n \in R[X]$ with $f_0f_n \neq 0$. Assume that f is primitive, i.e., $f_0, \ldots, f_n$ have no nontrivial common factor in R. If the Newton polygon of f with respect to some prime $p \in R$ consists of the only line segment from $(0, m)$ to $(n, 0)$ and if $\gcd(n, m) = 1$ then f is irreducible in $R[X]$.*

The condition on the Newton polygon means that $a_i \geq (n-i)m/n$ for $0 \leq i \leq n$ where p^{a_i} exactly divides f_i. When $m = a_0 = 1$, this condition is the same as in Eisenstein's criterion. Hence Eisenstein-Dumas criterion generalizes that of Eisenstein.

Eisenstein-Dumas criterion were originally proved for integer coefficients. Later it was generalized to local fields or any field with valuations [3, 16, 19]. We are interested in the case when R is a polynomial ring over a field. Let F be a field and $R = F[Y]$ where Y is a new variable. Then Y is a prime in R and Eisenstein-Dumas criterion can be applied in $R[X] \cong F[X, Y]$. We restate the criterion as follows.

Eisenstein-Dumas criterion (a special case). *Let F be any field and $f = f_0(Y) + f_1(Y)X + \cdots + f_n(Y)X^n \in F[X, Y]$. Assume that $f_0(Y) \neq 0$ and $f_n(Y)$ is a nonzero constant in F. If the Newton polygon of f has only one line segment from $(0, m)$ to $(n, 0)$ and $\gcd(n, m) = 1$, then f is (absolutely) irreducible over F.*

A polynomial over a field F is called absolutely irreducible if it remains irreducible over every algebraic extension of F. The same proof for the irreducibility of f under the Eisenstein-Dumas condition also shows that f is absolutely irreducible. In [31, Theorem 1B, p. 92], Schmidt describes another method for constructing absolutely irreducible polynomials which he attributes to Stepanov [37, 38]. This method can also be interpreted as a polygon method. Let $f = f_0(Y) + f_1(Y)X + \cdots + f_n(Y)X^n \in F[X, Y]$. The *upper Newton polygon* of f with respect to Y is defined to be the upper convex hull of the points $(0, a_0)$, $(1, a_1)$, ... , (n, a_n) where a_i is the degree of $f_i(Y)$ in Y and a_i is not defined if $f_i(Y) = 0$.

Stepanov-Schmidt criterion. *Let F be a field and $f \in F[X, Y]$ with degree n in X. If the upper Newton polygon of f with respect to Y has only one line segment from $(0, m)$ to $(n, 0)$ and $\gcd(n, m) = 1$, then f is absolutely irreducible over F.*

Note that the Eisenstein-Dumas and Stepanov-Schmidt criteria read exactly the same except that they exploit "different parts" of the polynomials. This leads us to consider the convex hull of the exponent vectors (i, j) of all the nonzero terms cX^iY^j of a polynomial f and call the resulted convex set *the Newton polytope* of f. Its boundary gives us a "whole" polygon that contains both the lower and upper polygons used above. This concept of polytopes associated with polynomials is due to Ostrowski (1921). Ostrowski realizes that the factorization of polyomials implies the decomposition of polytopes in the sense of Minkowski sum. In the 1970s, Ostrowski wrote two papers [27, 28] dealing with term ordering and irreducibility of multivariable polynomials. His irreducibility criteria are, however, based mainly on algebraic techniques (such as algebraic independence) and Puiseux developments. We show that Newton polytopes carry a lot of information about the irreducibility of polynomials. Indeed, the Eisenstein-Dumas and Stepanov-Schmidt criteria are just very special cases of our reults.

Our paper is organized as follows. In the next section, we describe the polytope method for irreducibility of multivariable polynomials. In Section 3, we discuss properties of convex sets and polytopes with respect to Minkowski sum. We prove a cancellation law on Minkowski sum of convex sets and, in Theorem 3.3, we show that the faces of polytopes in a Minkowski sum decompose uniquely. In Section 4, we give two general constructions of indecomposable polytopes and thus give many simple and explicit criteria for absolute irreducibility of multivariable polynomials. Many infinite families of absolutely irreducible polynomials are described. Our paper should be accessable to senior undergraduate students in mathematics.

Related works. We should mention that Lipkovski [18] associates a polynomial with a polyhedron (unbounded), called its Newton polyhedron, which is a direct analogue of Newton polygon in higher dimension. Indecomposability of its Newton polyhedron implies the analytic irreducibility of a polynomial at the origin (i.e., irreducibility in the formal power series ring). So the polyhedron method is local, while the polytope method is global. Lipkovski discusses indecomposability of polyhedra and gives several constructions of indecomposable polyhedra. Filaseta [7] uses Newton polygon method to decide irreducibility of Bessel polynomials. Recently, Gao and Shokrollahi [9] use Newton polygon method to compute roots of polynomials over function fields of curves. For a survey of Newton polygon method, see Mott [22]. There are two other methods in the literature for proving absolute irreducibility. One is using singularity analysis: if a polynomial defines a smooth hypersurface then it is absolutely irreducible. This method is often used in algebraic geometry. The other method is presented by Janwa, McGuire and Wilson [12] using Bezout's theorem on intersection multiplicity of curves. Also, Kaltofen [14, 15] presents polynomial time algorithms for testing irreducibility of multivariable polynomials.

2. Polytope method

We consider polynomials with n variables $X_1, X_2, \cdots, X_n$. Let F be any field and $R = F[X_1, X_2, \cdots, X_n]$. Let $f = \sum f_{i_1 i_2 \cdots i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \in R$. An exponent vector $(i_1, i_2, \cdots, i_n)$ of f can be considered as a point in $\mathbb{R}^n$ where $\mathbb{R}$ is the set of real numbers. The *Newton polytope* of f is defined to be the convex hull in $\mathbb{R}^n$ of all the points $(i_1, i_2, \cdots, i_n)$ with $f_{i_1 i_2 \cdots i_n} \neq 0$, denoted by P_f. For example, let

$$\begin{aligned}
f_1 &= X + Y + XY, \\
f_2 &= 1 + Y + XY + X^2 + Y^2, \\
f_3 &= X + Y + 2XY + Y^2 + X^3 + 2X^2Y + 3XY^2 + Y^3 + X^3Y + X^2Y^2 + XY^3.
\end{aligned}$$

Their Newton polytopes are drawn in Figure 1. Note that the coefficients 2 and 3 of f_3 may be zero in a field of characteristic 2 or 3. But the corresponding exponent vectors are not extreme points of P_{f_3}. So the Newton polytope of f_3 is the same no matter which field it is considered over. When f_1, f_2, f_3 are considered as polynomials in X with coefficients in $F[Y]$, their Newton polygons with respect to Y are: for f_1 the line segment from $(0,1)$ to $(1,0)$, for f_2 the two line segments from $(0,2)$ to $(0,0)$ then to $(2,0)$, and for f_3 the three line segments from $(0,3)$ to $(0,1)$ then to $(1,0)$ and $(3,0)$. The Newton polygon of a polynomial is only a fraction of the boundary of its Newton polytope.

For two sets A and B in $\mathbb{R}^n$, their sum is defined to be $A + B = \{a + b : a \in A, b \in B\}$, which is called the Minkowski sum of A and B. Observe that $f_1 f_2 = f_3$

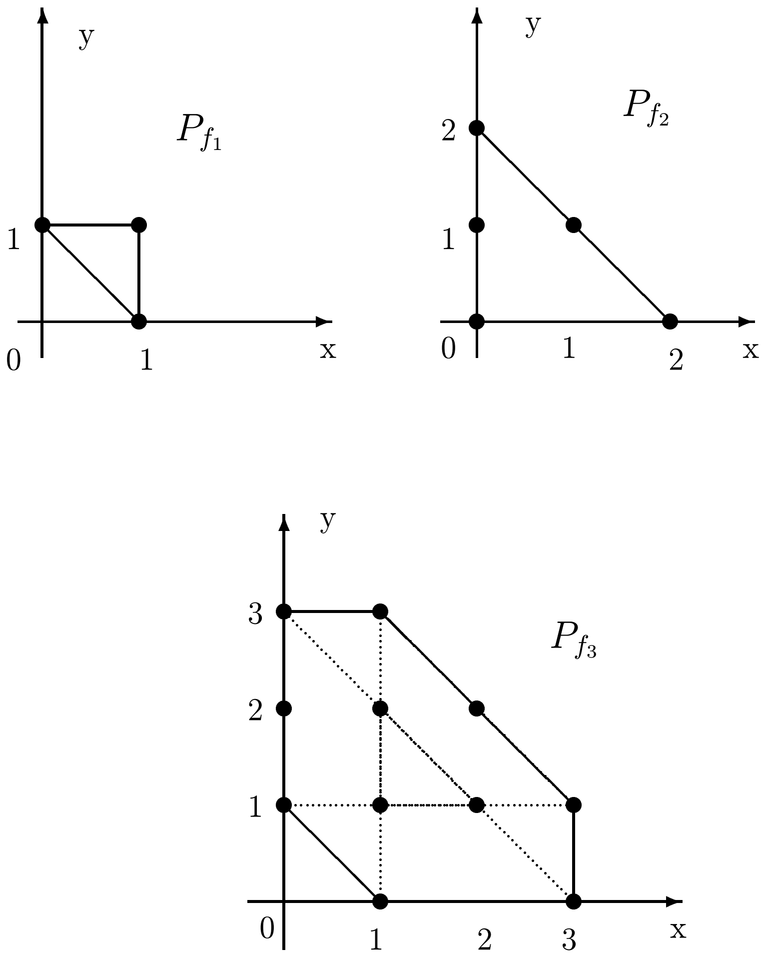

FIGURE 1. Newton polytopes of f_1, f_2, f_3

and $P_{f_1} + P_{f_2} = P_{f_3}$ (as indicated by the larger triangles in P_{f_3}). In general, Ostrowski [27, Theorem VI, p. 226] proves that this phenomenon holds for any polynomials. For the sake of completeness, we include a simple proof.

Lemma 2.1. *Let $f, g, h \in F[X_1, X_2, \cdots, X_n]$ with $f = gh$. Then $P_f = P_g + P_h$.*

Proof. By multiplication of polynomials , it is obvious that $P_f \subseteq P_g + P_h$. To prove the other inclusion, let $\mathbf{v}$ be any vertex of $P_g + P_h$. We show that there are unique points $\mathbf{v}_1 \in P_g$ and $\mathbf{v}_2 \in P_h$ such that $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$. Since $\mathbf{v} \in P_g + P_h$, the existence is no problem. Suppose that there is another pair $\mathbf{v}_1' \in P_g$ and $\mathbf{v}_2' \in P_h$ such that

$$\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}_1' + \mathbf{v}_2'. \tag{1}$$

Then

$$\mathbf{v} = \frac{1}{2}(\mathbf{v}_1 + \mathbf{v}_2') + \frac{1}{2}(\mathbf{v}_1' + \mathbf{v}_2).$$

Since $\mathbf{v}_1 + \mathbf{v}_2', \mathbf{v}_1' + \mathbf{v}_2 \in P_g + P_h$ and $\mathbf{v}$ is an extreme point of $P_g + P_h$, one must have

$$\mathbf{v}_1 + \mathbf{v}_2' = \mathbf{v}_1' + \mathbf{v}_2. \tag{2}$$

Subtracting (2) from (1) yields

$$\mathbf{v}_2 - \mathbf{v}_2' = \mathbf{v}_2' - \mathbf{v}_2, \text{ i.e., } 2(\mathbf{v}_2 - \mathbf{v}_2') = 0.$$

Hence $\mathbf{v}_2 = \mathbf{v}_2'$ and $\mathbf{v}_1 = \mathbf{v}_1'$.

Since $\mathbf{v}$ is a vertex of $P_g + P_h$, $\mathbf{v}_1$ and $\mathbf{v}_2$ must be vertices of P_g and P_h, respectively. There is a unique term in the expansion of $g \cdot h$ that has $\mathbf{v}$ as its exponent vector. Hence $\mathbf{v} \in P_f$. This proves that all the vertices of $P_g + P_h$ are in P_f. Consequently, $P_f \supseteq P_g + P_h$ as a polytope is the convex hull of its vertices. □

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. Certainly Newton polytopes of polynomials 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, we say that C is *integrally indecomposable.* Note that our concept of indecomposability is different from that in Grünbaun's book [10, Chapter 15]; see the comments at the end of the paper.

Irreducibility criterion. *Let F be any field and $f \in F[X_1, X_2, \cdots, X_n]$ be a nonzero polynomial not divisible by any X_i. If the Newton polytope of f is integrally indecomposable then f is absolutely irreducible over F.*

Proof. First note that f has no factor with only one term. Suppose that f factors nontrivially over some algebraic extension of F, say $f = gh$ where both g and h have at least two nonzero terms. Then the Newton polytopes of g and h have at least two points. By Lemma 2.1, $P_f = P_g + P_h$, contradicting to our assumption that P_f is integrally indecomposable. □

When P_f is decomposable, f can be either reducible or irreducible. For example, P_{f_2} is decomposable (equal to the sum of the triangle $(0,0)$–$(1,0)$–$(0,1)$ with itself). It can be verified directly that f_2 is absolutely irreducible over F when its characteristic is not two. Over a field F of characteristic two, we have

$$f_2 = (1 + X + \omega Y)(1 + X + \omega^2 Y)$$

where ω is an element of order 3 (so f_2 is irreducible over F if $\omega \notin F$).

Remarks. 1. In [27], Ostrowski uses the term "baric polyhedron" in place of the "Newton polytope" of a polynomial. Lemma 2.1 is proved for more general polynomials called algebraic polynomials where the exponents of variables may be rational numbers. Ostrowski mentions that he gave a talk at a German Mathematical Society meeting in 1921 about baric polyhedron and its applications to the irreducibility problem. In his sequel paper [28], Ostrowski discusses irreducibility of polynomials in details. It is surprising, however, that the concept of decomposability of polytopes does not arise there. Ostrowski develops irreducibility criteria using mainly algebraic tools (such as algebraic independence and conjugates) and the Puiseux developments.

2. For the case of polynomials with three variables, the concept of Newton polytope also appears in Shanok's paper [33]. Shanok develops irreducibility criteria for polynomials by projecting a Newton polytope from $\mathbb{R}^3$ into planes.

3. As mentioned in the introduction, Lipkovski [18] develops an analogue of the Newton polygon method in higher dimension for formal power series. Lipkovski associates a power series f of n variables with a Newton polyhedron $P_f + \mathbb{R}_0^n$ where P_f is defined similarly as for polynomials and $\mathbb{R}_0$ is the set of nonnegative real numbers. A Newton polyhedron is unbounded and, when $n = 2$, its finite edges form the Newton polygon. Lipkovski defines the decomposability of Newton polyhedra and gives several constructions of indecomposable Newton polyhedra. For a polynomial of two variables, the only indecomposable Newton polyhedron is that corresponding to the Newton polygon as described in Eisenstein-Dumas criteria. We will see, however, that there are many indecomposable polytopes in dimension two or higher.
4. One can change the coefficients of a polynomial f arbitrarily and its Newton polytope will remain the same provided the coefficients of all the terms of f that correspond to vertices are nonzero. If the Newton polytope of f is indecomposable then f will remain absolutely irreducible when its coefficients are modified arbitrarily but with those of vertices nonzero. This gives great freedom in choosing suitable polynomials in applications. For all the examples in the sequel, we often give polynomials with coefficients fixed at 1, but one may change the coefficients to any nonzero elements in the ground field.

3. Results on convex sets and polyhedra

To further discuss the decomposability of polytopes, we need more properties about Minkowski sums. For convenience of the reader, we review some basic concepts and results that will be needed in the next section; see [6, 10, 41, 43]. Some results we prove here are interesting in their own right.

As in the previous section, $\mathbb{R}$ denotes the field of real numbers. A subset $S \subseteq \mathbb{R}^n$ is called convex if, for any two points $a, b \in S$, the line segment from a to b is also contained in S, that is,

$$a + \lambda(b - a) = (1 - \lambda)a + \lambda b \in S, \quad \forall 0 \leq \lambda \leq 1.$$

For any subset $S \subseteq \mathbb{R}^n$, $\mathrm{conv}(S)$ denotes the smallest convex set in $\mathbb{R}^n$ that contains S. It is straightforward to check that

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

When $S = \{a_1, \ldots, a_k\}$ is a finite set, denote $\mathrm{conv}(S)$ by $\mathrm{conv}(a_1, \ldots, a_k)$, which is called the convex hull of $a_1, \ldots, a_k$. Also, $\mathrm{aff}(S)$ denotes the smallest affine space in $\mathbb{R}^n$ that contains S, i.e.,

$$\mathrm{aff}(S) = \left\{ \sum_{i=1}^{t} \lambda_i a_i : a_i \in S, \sum_{i=1}^{t} \lambda_i = 1 \right\}.$$

For a convex set S, the dimension of S is defined to be that of $\mathrm{aff}(S)$ as an affine space in $\mathbb{R}^n$, denoted by $\dim S$.

A point $a \in \mathbb{R}^n$ is called a boundary point of S if each open ball ($\{x \in \mathbb{R}^n : |a - x| < \epsilon\}$) of a contains both points of S and $\mathbb{R}^n \setminus S$, while $a \in \mathbb{R}^n$ is called a relative boundary point of S if each open ball of a contains both points of S and $\mathrm{aff}(S) \setminus S$. Let H be a hyperplane $\{x \in \mathbb{R}^n : \alpha \cdot x = \beta\}$ where $\alpha \in \mathbb{R}^n$, $\beta \in \mathbb{R}$ and

$\alpha \cdot x$ denotes the inner product of vectors. The closed halfspaces of H are defined as

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

A hyperplane H is called a supporting hyperplane to S if S is contained in one of its closed halfspaces and H contains a boundary point of S. A supporting hyperplane H to S is called nontrivial if S is not contained in H. The next result is from Webster [41, Theorem 2.4.12, p. 71].

Lemma 3.1. *Suppose that S is a convex set in $\mathbb{R}^n$. Then, for any relative boundary point a of S, there is a nontrivial supporting hyperplane to S that passes a (i.e. $a \in H$).*

We are ready to prove a cancellation law on Minkowski sum of convex sets.

Lemma 3.2. *Let A, B, C be nonempty subsets of $\mathbb{R}^n$ with A, B convex and C compact. Then $A + C = B + C$ implies $A = B$.*

Proof. Suppose that the lemma does not hold. Choose nonempty subsets A, B of $\mathbb{R}^n$ satisfying (a), (b) and (c) below:

(a) A and B are convex and $\dim A \geq \dim B$;
(b) There exists a nonempty compact set $C \in \mathbb{R}^n$ such that

$$A + C = B + C, \text{ but } A \neq B;$$

(c) $\dim B$ is the smallest among all such pairs A, B verifying (a) and (b).

Since $dim A \geq \dim B$, there is a point $a_0 \in A$ with $a_0 \notin B$. (This is certainly true if $\dim A > \dim B$. When $dim A = \dim B$, we can exchange A and B if necessary.)

Let $d = d(a_0, B)$ be the distance from a_0 to B. Suppose that $d > 0$. Then there is a hyperplane that strongly separates a_0 from B. That is, there are $\alpha \in \mathbb{R}^n$ and $\beta \in \mathbb{R}$ such that

$$\alpha \cdot a_0 = \beta \tag{3}$$

and, for all $b \in B$,

$$\alpha \cdot b < \beta. \tag{4}$$

Since C is compact, there is $c_0 \in C$ such that

$$\alpha \cdot c \leq \alpha \cdot c_0, \quad \forall c \in C. \tag{5}$$

For any $e \in A + C$, there are $b \in B$ and $c \in C$ such that $e = b + c$, and by (4) and (5),

$$\alpha \cdot e = \alpha \cdot b + \alpha \cdot c < \beta + \alpha \cdot b_0. \tag{6}$$

But $a_0 + c_0 \in A + C$ and $\alpha \cdot (a_0 + c_0) = \beta + \alpha \cdot c_0$, contradicting to (6).

Therefore d must be 0. If $\dim B = 0$, i.e., $B = \{b\}$ for some $b \in \mathbb{R}^n$ then $d = d(a_0, B) = |a_0 - b|$, and so $d = 0$ implies that $a_0 = b \in B$, contradicting again. So we assume henceforth that $\dim B \geq 1$. Since $a_0 \notin B$ and $d(a_0, B) = 0$, a_0 must be a relative boundary point of B. By Lemma 3.1, there is a nontrivial supporting hyperplane $H = \{x \in \mathbb{R}^n : \alpha \cdot x = \beta\}$ to B that passes through a_0. That is, (3) holds, there exists $b \in B$ such that (4) holds, and

$$\alpha \cdot b \leq \beta, \quad \forall b \in B. \tag{7}$$

The argument above for the case $d > 0$ shows that (4) can not be satisfied by all $b \in B$. Hence

$$B_1 = B \cap H = \{b \in B : \alpha \cdot b = \beta\}$$

is nonempty. Since B contains a point outside of H, $\dim B_1 < \dim B$. Define

$$A_1 = A \cap H \supseteq \{a_0\}$$

and

$$C_1 = C \cap H_1 \supseteq \{c_0\}$$

where $H_1 = \{x \in \mathbb{R}^n : \alpha \cdot x = \alpha \cdot c_0\}$. As H and H_1 are both convex and closed, A_1 is convex and C_1 is compact. We show that

$$A_1 + C_1 = B_1 + C_1. \tag{8}$$

In fact, for any $a \in A_1$ and $c \in C_1$, there are $b \in B$ and $c_1 \in C$ such that $a + c = b + c_1$. Then

$$\alpha \cdot b + \alpha \cdot c_1 = \alpha \cdot (b + c_1) = \alpha \cdot (a + c) = \alpha \cdot a + \alpha \cdot c = \beta + \alpha \cdot c_0.$$

By (5) and (7), we see that $\alpha \cdot b = \beta$ and $\alpha \cdot c_1 = \alpha \cdot c_0$. Hence $b \in B_1$ and $c_1 \in C_1$. So $a + c \in B_1 + C_1$ and $A_1 + C_1 \subseteq B_1 + C_1$. Similarly, the other inclusion holds. Therefore (8) holds.

Now since $\dim B_1 < \dim B$ and by the minimality of the dimension of B in (c), (8) implies that $A_1 = B_1$. Therefore $a_0 \in B_1 \subseteq B$, contradicting to the fact that $a_0 \notin B$. This means that there are no A, B satisfying (a) and (b), and the lemma is proved. ☐

Remarks. It is interesting to mention the following result of Rådström [30] (see also Webster [41, Corollary 2.1.9, p. 52]):

> *Let A, B, C be nonempty subsets of $\mathbb{R}^n$ with A, B closed and convex and with C bounded. Then $A + C = B + C$ implies $A = B$.*

That is, the cancellation law holds if A, B are "nice" and C bounded. Our lemma 3.2 complements Rådström's result when C is "nice." Note that lemma 3.2 does not hold when C is unbounded or not closed. Examples are (in $\mathbb{R}$): $A = [0,1]$, $B = (0,1)$ and $C = (0,1)$ with $A + C = B + C = (0,2)$; or $A = [0,1]$, $B = \{0\}$ and $C = [0,\infty)$ with $A + C = B + C = [0,\infty)$.

A polyhedron is a subset of $\mathbb{R}^n$ that is the intersection of closed halfspaces of finitely many hyperplanes. Since closed halfspaces are convex, a polyhedron is always convex and closed in our paper. If a polyhedron is bounded, it is called a polytope. So a polytope is compact. It is well-known that a subset of $\mathbb{R}^n$ is a polytope iff it is the convex hull of finitely many points. Let P be a polyhedron in $\mathbb{R}^n$. For any hyperplane H with $P \subseteq H^-$ (or $P \subseteq H^+$), the intersection $P \cap H$ is called a face of P. A face can be the empty set or P itself; any other face of P is called a proper face. Obviously, a face is also a polyhedron and a compact face is a polytope. A face of dimension 0 has only one point, called a vertex of P. A polytope is always the convex hull of its vertices; this property will be used freely below. A face of dimension 1 is a line segment, called an edge of P. A face of dimension $\dim P - 1$ is called a facet of P. The next result describes how faces decompose in a Minkowski sum of polyhedra.

Theorem 3.3. *Let A and B be polyhedra in $\mathbb{R}^n$ and $C = A + B$.*

(a) *Each face of C is a Minkowski sum of faces of A and B.*

(b) *Each compact face of C is a unique Minkowski sum of convex subsets of A and B.*

(c) *Let C_1 be any compact face of C and $c_1, c_2, \ldots, c_k$ all of its vertices. Suppose that $c_i = a_i + b_i$ where $a_i \in A$ and $b_i \in B$ for $1 \le i \le k$. Let*

$$A_1 = conv(a_1, a_2, \ldots, a_k), \quad B_1 = conv(b_1, b_2, \ldots, b_k).$$

Then A_1 and B_1 are faces of A and B, respectively, and $C_1 = A_1 + B_1$.

Proof. (a). This part is well-known in the literature; see [6, Theorem 1.5, p. 105] and [10, Theorem 1, p. 317]. We prove (a) in such a fashion that (b) and (c) follows easily. Let C_1 be any face of C. Define

$$\begin{aligned} F_1 &= \{a \in A : \text{there exists } b \in B \text{ such that } a + b \in C_1\}, \\ F_2 &= \{b \in B : \text{there exists } a \in A \text{ such that } a + b \in C_1\}. \end{aligned}$$

We claim that F_1 and F_2 are faces of A and B, respectively, and $C_1 = F_1 + F_2$. Let $H = \{x \in \mathbb{R}^n : \alpha \cdot x = \beta\}$ be any supporting hyperplane of C such that $C_1 = C \cap H$ and $C_1 \subseteq H^+$, i.e.,

$$\alpha \cdot x \ge \beta, \quad \forall x \in C. \tag{9}$$

Let c_0 be an arbitrary point of $C_1 (\subseteq H)$. Then $c_0 = a_0 + b_0$ for some $a_0 \in A$ and $b_0 \in B$, and

$$\beta = \alpha \cdot c_0 = \alpha \cdot a_0 + \alpha \cdot b_0.$$

For any $a \in A$, since $a + b_0 \in C$, (9) implies that $\alpha \cdot (a + b_0) \ge \beta = \alpha \cdot a_0 + \alpha \cdot b_0$. Thus

$$\alpha \cdot a \ge \alpha \cdot a_0, \quad \forall a \in A. \tag{10}$$

This means that

$$A \subseteq \{x \in \mathbb{R}^n : \alpha \cdot x \ge \alpha \cdot a_0\}. \tag{11}$$

Similarly,

$$B \subseteq \{x \in \mathbb{R}^n : \alpha \cdot x \ge \alpha \cdot b_0\}. \tag{12}$$

For any $a \in F_1$, there exists $b \in B$ such that $a + b \in C_1$, so the same argument leading to (10) shows that $\alpha \cdot a_0 \ge \alpha \cdot a$. Hence

$$\alpha \cdot a = \alpha \cdot a_0, \quad \forall a \in F_1. \tag{13}$$

Similarly,

$$\alpha \cdot b = \alpha \cdot b_0, \quad \forall b \in F_2. \tag{14}$$

The equations (13) and (14) imply that, for any $a \in F_1$ and $b \in F_2$, $\alpha \cdot (a + b) = \alpha \cdot a_0 + \alpha \cdot b_0 = \beta$. Thus $a + b \in H \cap C = C_1$ and $F_1 + F_2 \subseteq C_1$. Obviously $C_1 \subseteq F_1 + F_2$. Therefore $C_1 = F_1 + F_2$.

To show that F_1 and F_2 are faces, define two hyperplanes

$$\begin{aligned} H_1 &= \{x \in \mathbb{R}^n : \alpha \cdot x = \alpha \cdot a_0\}, \\ H_2 &= \{x \in \mathbb{R}^n : \alpha \cdot x = \alpha \cdot b_0\}. \end{aligned}$$

Then (13) and (14) imply that

$$F_1 \subseteq A \cap H_1 \text{ and } F_2 \subseteq B \cap H_2.$$

For any $a \in A \cap H_1$, since $\alpha \cdot (a + b_0) = \alpha \cdot a + \alpha \cdot b_0 = \alpha \cdot a_0 + \alpha \cdot b_0 = \beta$, we have $a + b_0 \in H$ and thus in $H \cap C = C_1$. By the definition of F_1, $a \in F_1$. This proves that $A \cap H_1 \subseteq F_1$. Consequently, $F_1 = A \cap H_1$. By (11), H_1 is a supporting hyperplane of A so F_1 is a face of A. Similarly $F_2 = B \cap H_2$ and thus a face of B, as H_2 is a supporting hyperplane of B by (12).

(b). Let C_1 be any compact face of C and F_1, F_2 as defined as above. Then $C_1 = F_1 + F_2$, and F_1 and F_2 are faces of A and B, respectively. Since C_1 is bounded, F_1 and F_2 are also bounded. So F_1 and F_2 compact, as faces are closed. For the uniqueness, let F_1' and F_2' be any convex subsets of A and B, respectively, such that $C_1 = F_1' + F_2'$. By our definition of F_1 and F_2, we have

$$F_1' \subseteq F_1, \quad F_2' \subseteq F_2.$$

Note that

$$C_1 = F_1' + F_2' \subseteq F_1' + F_2 \subseteq F_1 + F_2 = C_1.$$

We have $F_1' + F_2 = F_1 + F_2 = C_1$. By Lemma 3.2, $F_1' = F_1$. Similarly, $F_2' = F_2$.

(c). Certainly, $C_1 = \mathrm{conv}(c_1, \dots, c_k) \subseteq A_1 + B_1$. By the definition of F_1 and F_2, $a_i \in F_1$ and $b_i \in F_2$ for $1 \le i \le k$. Hence $A_1 \subseteq F_1$ and $B_1 \subseteq F_2$. It follows that $A_1 + B_1 \subseteq F_1 + F_2 \subseteq C_1$. Therefore $C_1 = A_1 + B_1$. By the uniqueness of (a), we have $A_1 = F_1$ and $B_1 = F_2$. So A_1 and B_1 are faces of A and B, respectively. □

A convex cone with a vertex $\mathbf{v}$ is defined to be a convex set S in $\mathbb{R}^n$ such that $\mathbf{v}$ is an extreme point of S and, for any $a \in S$, $\mathbf{v} + \lambda(a - \mathbf{v}) \in S$ for all real numbers $\lambda \ge 0$.

Lemma 3.4. *Let C be a convex cone with vertex $\mathbf{v}$ and H a hyperplane in $\mathbb{R}^n$ with $\mathbf{v} \notin H$. Suppose that $Q = C \cap H$ is nonempty and bounded. Then, for any $r \in \mathbb{R}^n$, either $C \cap (r + H)$ is empty or there exists a real number $t \ge 0$ such that*

$$C \cap (r + H) = \mathbf{v} + t(Q - \mathbf{v}) = \{\mathbf{v} + t(a - \mathbf{v}) : a \in Q\}.$$

Proof. Choose $\alpha \in \mathbb{R}^n$ and $\beta \in \mathbb{R}$ such that

$$H = \{x \in \mathbb{R}^n : \alpha \cdot x = \beta\} \text{ and } \alpha \cdot \mathbf{v} > \beta.$$

We show that for every point $a \in C$ with $a \neq \mathbf{v}$,

$$\alpha \cdot a < \alpha \cdot \mathbf{v}. \tag{15}$$

Suppose on the contrary that $\alpha \cdot a \ge \alpha \cdot \mathbf{v}$ for some $a \in C$. Let $b \in Q = C \cap H$ be any fixed point. Then

$$\alpha \cdot b = \beta < \alpha \cdot \mathbf{v} \le \alpha \cdot a.$$

Let $a_1 = \lambda_1 a + (1 - \lambda_1) b$ where $\lambda_1 = (\alpha \cdot \mathbf{v} - \beta)/(\alpha \cdot a - \beta) > 0$. Since $\lambda_1 \le 1$ and C is convex, $a_1 \in C$ and

$$\alpha \cdot a_1 = \alpha \cdot \mathbf{v}. \tag{16}$$

For any $t \ge 0$,

$$b + t(a_1 - \mathbf{v}) = \mathbf{v} + (t+1)\left(\left(\frac{t}{t+1} a_1 + \frac{1}{t+1} b\right) - \mathbf{v}\right)$$

belongs to C, as $a_1, b \in C$ and C is a convex cone with vertex $\mathbf{v}$. By (16), $\alpha \cdot (b + t(a_1 - \mathbf{v})) = \alpha \cdot b = \beta$. Hence $b + t(a_1 - \mathbf{v}) \in H$ and $b + t(a_1 - \mathbf{v}) \in C \cap H = Q$ for all $t \ge 0$, contradicting to the boundness of Q (note that $a_1 \neq \mathbf{v}$). Therefore (15) holds.

For any $r \in \mathbb{R}^n$ and any $a \in C$ with $a \neq \mathbf{v}$, consider the intersection of the ray

$$\{\mathbf{v} + \lambda(a - \mathbf{v}) : \lambda \ge 0\} \tag{17}$$

with the hyperplane

$$r + H = \{r + x \in \mathbb{R}^n : \alpha \cdot x = \beta\} = \{x \in \mathbb{R}^n : \alpha \cdot x = \alpha \cdot r + \beta\}. \qquad (18)$$

Note that $\alpha\cdot(\mathbf{v}+\lambda(a-\mathbf{v})) = \alpha\cdot r+\beta$ implies that $\lambda = (\alpha\cdot\mathbf{v}-\beta-\alpha\cdot r)/(\alpha\cdot\mathbf{v}-\alpha\cdot a)$. Since $\alpha\cdot\mathbf{v}-\alpha\cdot a > 0$ by (15), $\lambda \geq 0$ iff $\alpha\cdot r \leq \alpha\cdot\mathbf{v}-\beta$. In the latter case, $r+H$ intersects every ray (17), $a \in C$, at a unique point determined by λ above.

For $r = 0$, since $\alpha\cdot\mathbf{v}-\beta > 0 = \alpha\cdot r$, each ray (17) intersects H, thus Q, at a unique point. Hence we may index all the rays in (17) by $a \in Q$. Now suppose that $\alpha\cdot r \leq \alpha\cdot\mathbf{v}-\beta$. Then for each $a \in Q$, the ray (17) intersects $r+H$ at the point $b = \mathbf{v}+\lambda_0(a-\mathbf{v})$ where

$$\lambda_0 = \frac{\alpha\cdot\mathbf{v}-\beta-\alpha\cdot r}{\alpha\cdot\mathbf{v}-\beta}.$$

Therefore the lemma holds with $t = \lambda_0$. □

Finally, a polytope is associated naturally with a graph consisting of its vertices and edges. The next result is due to Balinski [2].

Lemma 3.5. *The graph of a polytope of dimension n is n-connected.*

4. Indecomposable polytopes and absolutely irreducible polynomials

The question is to find or construct integrally indecomposable polytopes in $\mathbb{R}^n$. Each type of indecomposable polytopes gives us a family of absolutely irreducible polynomials. When a polytope has only one point we say that it is trivial. We examine several types of simple nontrivial polytopes such as line segments, triangles, tetrahedrons, pyramids, etc. We show how to construct indecomposable polytopes from a given polytope.

We need more terminology. A line segment $\mathrm{conv}(\mathbf{v}_1,\mathbf{v}_2)$ is simply denoted by $\mathbf{v}_1\mathbf{v}_2$. For an integral point or vector $\mathbf{v} = (a_1,\dots,a_n)$, we write $\gcd(\mathbf{v})$ to mean $\gcd(a_1,\dots,a_n)$, i.e. the greatest common divisor of the components in $\mathbf{v}$. Similarly, for several points $\mathbf{v}_1,\dots,\mathbf{v}_k$, $\gcd(\mathbf{v}_1,\dots,\mathbf{v}_k)$ means the gcd of all the components in $\mathbf{v}_1,\dots,\mathbf{v}_k$ together. For example, if $\mathbf{v}_1 = (n,0)$, $\mathbf{v}_2 = (0,m)$ and $\mathbf{v}_3 = (u,u)$, then $\gcd(\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3) = \gcd(n,0,0,m,u,u) = \gcd(n,m,u)$. For any two integral vectors $\mathbf{v}_1$ and $\mathbf{v}_2$, we have $\gcd(\mathbf{v}_1,\mathbf{v}_2) = \gcd(\mathbf{v}_1,\mathbf{v}_2-t\mathbf{v}_1)$ for any integer t.

Lemma 4.1. *Let $\mathbf{v}_0$ and $\mathbf{v}_1$ be two distinct integral points in $\mathbb{R}^n$. Then the number of integral points on the line segment $\mathbf{v}_0\mathbf{v}_1$, including $\mathbf{v}_0$ and $\mathbf{v}_1$, is equal to $\gcd(\mathbf{v}_0-\mathbf{v}_1)+1$. Furtherly, if $\mathbf{v}_2$ is any integral point on $\mathbf{v}_0\mathbf{v}_1$, then*

$$\frac{|\mathbf{v}_2-\mathbf{v}_0|}{|\mathbf{v}_1-\mathbf{v}_0|} = \frac{\gcd(\mathbf{v}_2-\mathbf{v}_0)}{\gcd(\mathbf{v}_1-\mathbf{v}_0)}$$

where $|\mathbf{v}|$ denotes the Euclidean length of a vector $\mathbf{v}$.

Proof. All the points on the line segment $\mathbf{v}_0\mathbf{v}_1$ are of the form

$$\mathbf{v} = \mathbf{v}_0 + t(\mathbf{v}_1-\mathbf{v}_0), \quad 0 \leq t \leq 1.$$

Since $\mathbf{v}_0$ is integral, $\mathbf{v}$ is integral iff $t(\mathbf{v}_1-\mathbf{v}_0)$ is integral. But the components of $\mathbf{v}_1-\mathbf{v}_0$ are all integers, so t must be rational. Let

$$t = \frac{i}{k}, \quad \text{for some } 0 < i < k \text{ with } \gcd(k,i) = 1.$$

Then $t(\mathbf{v}_1-\mathbf{v}_0)$ is integral iff $k|\gcd(\mathbf{v}_1-\mathbf{v}_0)$. Hence if $\mathbf{v}$ is an integral point different from $\mathbf{v}_0$ and $\mathbf{v}_1$, then t must be of the form

$$t=\frac{i}{d},\quad 0<i<d$$

where $d=\gcd(\mathbf{v}_1-\mathbf{v}_0)\geq 1$. The number of choices for i is $d-1$. So the total number of integral points $\mathbf{v}$ on $\mathbf{v}_0\mathbf{v}_1$ is $d-1+2=d+1$.

Now suppose that $\mathbf{v}_2=\mathbf{v}_0+i/d(\mathbf{v}_1-\mathbf{v}_0)$ is any integral point on $\mathbf{v}_0\mathbf{v}_1$ with $0\leq i\leq d$ where $d=\gcd(\mathbf{v}_1-\mathbf{v}_0)$. Note that $(\mathbf{v}_1-\mathbf{v}_0)/d$ is integral and $\gcd((\mathbf{v}_1-\mathbf{v}_0)/d)=1$. Hence $\gcd(\mathbf{v}_2-\mathbf{v}_0)=\gcd(i\cdot(\mathbf{v}_1-\mathbf{v}_0)/d)=i$. Also

$$|\mathbf{v}_2-\mathbf{v}_0|=i|(\mathbf{v}_1-\mathbf{v}_0)/d|,\quad |\mathbf{v}_1-\mathbf{v}_0|=d|(\mathbf{v}_1-\mathbf{v}_0)/d|.$$

Therefore the equation in the lemma holds. □

Theorem 4.2. *Let Q be any integral polytope in $\mathbb{R}^n$ contained in a hyperplane H and $\mathbf{v}\in\mathbb{R}^n$ an integral point lying outside of H. Suppose that $\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_k$ are all the vertices of Q. Then the polytope conv$(\mathbf{v},Q)$ is integrally indecomposable iff*

$$\gcd(\mathbf{v}-\mathbf{v}_1,\mathbf{v}-\mathbf{v}_2,\ldots,\mathbf{v}-\mathbf{v}_k)=1.$$

Proof. Suppose that $C=A+B$ for some integral polytopes A and B in $\mathbb{R}^n$. By appropriately shifting A and B, we may assume that $\mathbf{v}\in A$ and $0\in B$. Note that $\mathbf{v},\mathbf{v}_1,\ldots,\mathbf{v}_k$ are all the vertices of C, and $\mathbf{v}\mathbf{v}_1,\ldots,\mathbf{v}\mathbf{v}_k$ are edges of C. By Lemma 3.3, there are unique vertices $\mathbf{a}_i\in A$ and $\mathbf{b}_i\in B$ such that

$$\mathbf{v}_i=\mathbf{a}_i+\mathbf{b}_i,\quad 1\leq i\leq k,$$

and

$$\mathbf{v}\mathbf{v}_i=\mathbf{v}\mathbf{a}_i+0\mathbf{b}_i,\quad 1\leq i\leq k.$$

Since $0\in 0\mathbf{b}_i$, the line segment $\mathbf{v}\mathbf{a}_i$ coincides with part of $\mathbf{v}\mathbf{v}_i$ starting at $\mathbf{v}$; see Figure 2. Now take any two vertices, say $\mathbf{v}_1$ and $\mathbf{v}_2$ that are connected by an edge in Q. Then $\mathbf{v}_1\mathbf{v}_2$ is also an edge of C. Again Lemma 3.3 (b) implies that

$$\mathbf{v}_1\mathbf{v}_2=\mathbf{a}_1\mathbf{a}_2+\mathbf{b}_1\mathbf{b}_2.$$

So the line segment $\mathbf{a}_1\mathbf{a}_2$ (possibly a point) is parallel to the edge $\mathbf{v}_1\mathbf{v}_2$. This means that the triangle conv$(\mathbf{v},\mathbf{a}_1,\mathbf{a}_2)$ is similar to the larger triangle conv$(\mathbf{v},\mathbf{v}_1,\mathbf{v}_2)$. Hence

$$\frac{|\mathbf{a}_1-\mathbf{v}|}{|\mathbf{v}_1-\mathbf{v}|}=\frac{|\mathbf{a}_2-\mathbf{v}|}{|\mathbf{v}_2-\mathbf{v}|}$$

where $|\mathbf{v}|$ means the Euclidean length of a vector $\mathbf{v}$ in $\mathbb{R}^n$. By Lemma 4.1, we have

$$\frac{\gcd(\mathbf{a}_1-\mathbf{v})}{\gcd(\mathbf{v}_1-\mathbf{v})}=\frac{\gcd(\mathbf{a}_2-\mathbf{v})}{\gcd(\mathbf{v}_2-\mathbf{v})}. \tag{19}$$

By Lemma 3.5, the graph of a polytope is connected. Since the equation (19) holds for any two adjacent vertices, we see that

$$\frac{|\mathbf{a}_i-\mathbf{v}|}{|\mathbf{v}_i-\mathbf{v}|}=\frac{\gcd(\mathbf{a}_i-\mathbf{v})}{\gcd(\mathbf{v}_i-\mathbf{v})}=t,\quad 1\leq i\leq k, \tag{20}$$

where t is a constant $0\leq t\leq 1$. This common value t must be a rational number, say m/d where $d\geq 1$, $d\geq m\geq 0$ and $\gcd(m,d)=1$. Then d divides $\gcd(\mathbf{v}_i-\mathbf{v})$ for $1\leq i\leq k$.

Suppose that $\gcd(\mathbf{v}-\mathbf{v}_1,\mathbf{v}-\mathbf{v}_2,\ldots,\mathbf{v}-\mathbf{v}_k)=1$. Since

$$\gcd(\mathbf{v}-\mathbf{v}_1,\mathbf{v}-\mathbf{v}_2,\ldots,\mathbf{v}-\mathbf{v}_k)=\gcd(\gcd(\mathbf{v}_1-\mathbf{v}),\gcd(\mathbf{v}_2-\mathbf{v}),\ldots,\gcd(\mathbf{v}_k-\mathbf{v})),$$

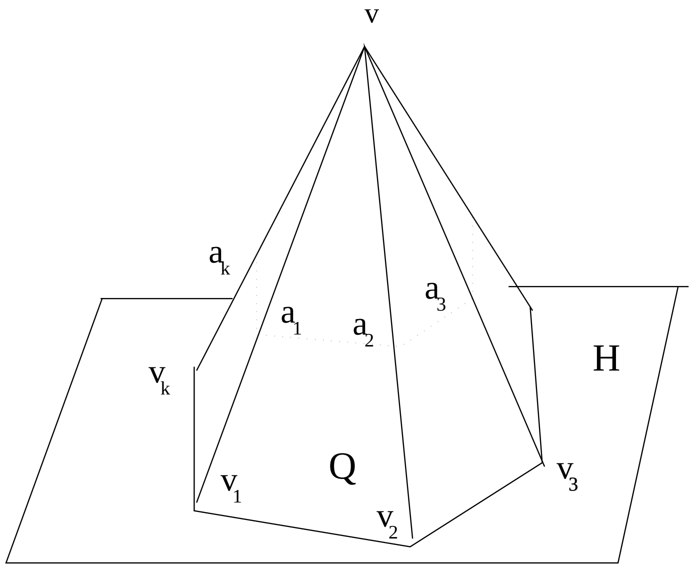

FIGURE 2. Indecomposable pyramid

we see that d must be 1. Hence $m = 0$ or 1, and so $t = 0$ or 1. If $t = 0$ then (20) implies that $\mathbf{a}_i = \mathbf{v}$ for $1 \le i \le k$; so $A = \{\mathbf{v}\}$. If $t = 1$ then (20) implies that $\mathbf{a}_i = \mathbf{v}_i$ for $1 \le i \le k$; so $A = C$ and $B = \{0\}$. Therefore C is indecomposable.

Suppose that $\gcd(\mathbf{v} - \mathbf{v}_1, \mathbf{v} - \mathbf{v}_2, \ldots, \mathbf{v} - \mathbf{v}_k) = d > 1$. Let $\mathbf{u}_i = \frac{1}{d}(\mathbf{v}_i - \mathbf{v})$ for $1 \le i \le k$. Then $\mathbf{u}_i$'s are integral points in $\mathbb{R}^n$. Define

$$A = \operatorname{conv}(\mathbf{v}, \mathbf{v}_1 - \mathbf{u}_1, \mathbf{v}_2 - \mathbf{u}_2, \ldots, \mathbf{v}_k - \mathbf{u}_k), \quad B = \operatorname{conv}(0, \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k).$$

Then it is straightforward to check that $A + B = C$. Since $d > 1$, $\mathbf{u}_i \neq 0$ and $\mathbf{v}_i - \mathbf{u}_i \neq \mathbf{v}$ for $1 \le i \le k$. So both A and B have at least two points, and thus C is decomposable. $\square$

For example, Let f be the polynomial $1 + X^n + Y^m + X^nY^m + X^iY^jZ^k \in F[X, Y, Z]$ where $n, m, k > 0$ and $i, j \ge 0$. Then the Newton polytope of f is the pyramid with vertices $(0, 0, 0)$, $(n, 0, 0)$, $(n, m, 0)$, $(0, m, 0)$ and (i, j, k). If $\gcd(n, m, i, j, k) = 1$ then the pyramid is indecomposable and thus f is absolutely irreducible over F. Of course, f remains absolutely irreducible if it is added any number of terms whose exponent vectors lie inside the pyramid.

When Q is an integral point, a line segment or a triangle, we have the following corollaries.

Corollary 4.3. *Let $\mathbf{v}_0$ and $\mathbf{v}_1$ be two distinct integral points in $\mathbb{R}^n$. Then the line segment $\mathbf{v}_0\mathbf{v}_1$ is integrally indecomposable iff* $\gcd(\mathbf{v}_0 - \mathbf{v}_1) = 1$.

Corollary 4.4. *A two-term polynomial*

$$aX_1^{i_1} \cdots X_k^{i_k} + bX_{k+1}^{i_{k+1}} \cdots X_n^{i_n} \in F[X_1, \ldots, X_n], \quad a, b \in F \setminus \{0\}$$

is absolutely irreducible over F iff $\gcd(i_1, \ldots, i_n) = 1$.

For examples, $X^n + Y^m$ is absolutely irreducible over F iff $\gcd(n, m) = 1$; similarly, $Y^i + X^jZ^k$ is absolutely irreducible over F iff $\gcd(i, j, k) = 1$.

Corollary 4.5. *Let $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2$ be three integral points in $\mathbb{R}^n$ not all on one line. Then the triangle conv$(\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2)$ is integrally indecomposable iff*

$$\gcd(\mathbf{v}_0 - \mathbf{v}_1, \mathbf{v}_0 - \mathbf{v}_2) = 1.$$

Corollary 4.6. *Let $f = aX^n + bY^m + cX^uY^v + \sum c_{ij}X^iY^j \in F[X,Y]$ with a, b, c nonzero. Suppose that the Newton polytope of f is the triangle with vertices $(n,0)$, $(0,m)$ and (u,v). If $\gcd(m,n,u,v) = 1$ then f is absolutely irreducible over F.*

The Newton polytope of the polynomial f in the corollary is the triangle with vertices $(n,0)$, $(0,m)$ and (u,v) provided that $un + mv \neq mn$ and if $c_{ij} \neq 0$ then

$$d(mi + nj - mn) \geq 0, \quad -d(vi + (n-u)j - vn) \geq 0, \quad d((v-m)i - uj + um) \geq 0,$$

where $d = mu + nv - mn$.

Corollary 4.7. *Let $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ be four integral points in $\mathbb{R}^n$, not all contained in one plane. Then the tetrahedron conv$(\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is integrally indecomposable iff*

$$\gcd(\mathbf{v}_0 - \mathbf{v}_1, \mathbf{v}_0 - \mathbf{v}_2, \mathbf{v}_0 - \mathbf{v}_3) = 1.$$

Corollary 4.8. *Suppose that the Newton polytope of*

$$f = a_1X^\ell + a_2Y^m + a_3Z^n + a_4X^uY^vZ^w + \sum c_{ijk}X^iY^jZ^k \in F[X,Y,Z]$$

is the tetrahedron with vertices $(\ell,0,0), (0,m,0), (0,0,n)$ and (u,v,w). If

$$\gcd(\ell, m, n, u, v, w) = 1$$

then f is absolutely irreducible over F.

Corollary 4.9. *Let Q be any integral polytope in $\mathbb{R}^n$ contained in a hyperplane H and $\mathbf{v} \in \mathbb{R}^n$ an integral point lying outside of H. If Q has one edge $\mathbf{v}_1\mathbf{v}_2$ such that $\gcd(\mathbf{v}_1 - \mathbf{v}_2) = 1$ or a vertex $\mathbf{v}_1$ such that $\gcd(\mathbf{v} - \mathbf{v}_1) = 1$ then the polytope conv$(\mathbf{v}, Q)$ is integrally indecomposable.*

For example, let $f_1 \in \mathbb{F}[X_1, \ldots, X_n]$ be any polynomial of degree m and $f = aX^r + f_1 \in F[X, X_1, \ldots, X_n]$. If $\gcd(m, r) = 1$ then f is absolutely irreducible over F. The reason is simple. The Newton polytope of f is a pyramid with the Newton polytope of f_1 as its base. Since f_1 has degree m, it has a term $cX_1^{k_1} \cdots X_n^{k_n}$ of degree m such that its exponent vector $(0, k_1, \ldots, k_n) = \mathbf{v}_1$ is a vertex of P_{f_1}. The exponent vector of aX^r is $(r, 0, \ldots, 0) = \mathbf{v}$. Since $\gcd(m, r) = 1$ and $k_1 + \cdots + k_n = m$, there is at least one k_i such that $\gcd(m, k_i) = 1$. It follows that

$$\gcd(\mathbf{v} - \mathbf{v}_1) = \gcd(r, k_1, \ldots, k_n) = 1.$$

Hence P_f is indecomposable and f is absolutely irreducible over F.

Theorem 4.10. *Let Q be an indecomposable integral polytope in $\mathbb{R}^n$ that is contained in a hyperplane H and has at least two points, and let $\mathbf{v} \in \mathbb{R}^n$ be a point (not necessarily integral) lying outside of H. Let S be any set of integral points in the polytope conv$(\mathbf{v}, Q)$. Then the polytope conv(S, Q) is integrally indecomposable.*

Proof. Let $C = \text{conv}(S, Q)$ as depicted in Figure 3. Note that $Q = C \cap H$, so Q is a face of C. If $C = A + B$ for some integral polytopes A and B then, by Lemma 3.3, A and B have unique faces A_1 and B_1, respectively, such that $Q = A_1 + B_1$. Since Q is indecomposable, A_1 or B_1 must have only one point, say A_1. By appropriately shifting A and B, we may assume that $A_1 = \{0\}$ and $B_1 = Q$. We want to show

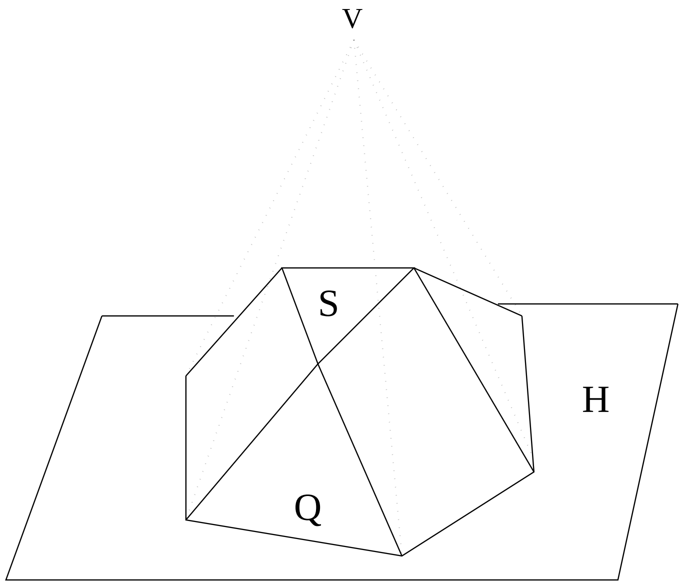

FIGURE 3. $C = \operatorname{conv}(S, Q)$

that $A = A_1 = \{0\}$. This is geometrically "clear" from Figure 3, as any shift $r+Q$, $r \neq 0$, of Q can not be contained in the cone $\operatorname{conv}(\mathbf{v}, Q)$, not to mention in C.

Fix any $r \in A$. Then $r + Q \subseteq r + B \subseteq C$. Since $Q \subseteq H$, we have

$$r + Q \subseteq C \cap (r + H). \tag{21}$$

Let C_1 be the cone generated by $\mathbf{v}$ as its vertex and all points in Q. Then

$$C_1 \supseteq \operatorname{conv}(\mathbf{v}, Q) \supseteq C \text{ and } C_1 \cap H = Q. \tag{22}$$

By (21),

$$r + Q \subseteq C_1 \cap (r + H), \tag{23}$$

so nonempty. By Lemma 3.4, there exists a number $t \geq 0$ such that

$$(r + H) \cap C_1 = \mathbf{v} + t(Q - \mathbf{v}). \tag{24}$$

We show that $t \leq 1$. Take any $a \in Q$. Then $r + a \in C_1 \cap (r + H)$. By (24), there exists $b \in Q$ such that $r + a = \mathbf{v} + t(b - \mathbf{v})$. Also, since $r + a \in C \subseteq \operatorname{conv}(\mathbf{v}, Q)$, there is $b_1 \in Q$ such that $r + a = \mathbf{v} + t_1(b_1 - \mathbf{v})$ for some $0 \leq t_1 \leq 1$. Hence

$$t(b - \mathbf{v}) = t_1(b_1 - \mathbf{v}). \tag{25}$$

Assume that H is defined by $\alpha \in \mathbb{R}^n$ and $\beta \in \mathbb{R}$, i.e., $H = \{x \in \mathbb{R}^n : \alpha \cdot x = \beta\}$. Since $b, b_1 \in Q \subseteq H$, we have $\alpha \cdot b = \alpha \cdot b_1$. The equation (25) implies that $t(\beta - \alpha \cdot \mathbf{v}) = t_1(\beta - \alpha \cdot \mathbf{v})$. Since $\mathbf{v} \notin H$, $\alpha \cdot \mathbf{v} \neq \beta$. Therefore $t = t_1$ and so $0 \leq t \leq 1$.

Now the equations (23) and (24) imply that $r + Q \subseteq \mathbf{v} + t(Q - \mathbf{v})$, i.e.,

$$Q \subseteq tQ + a \tag{26}$$

where $a = (1-t)\mathbf{v} - r \in \mathbb{R}^n$. For any integer $k > 0$, applying (26) k times yields

$$Q \subseteq t^k Q + (t^{k-1} + \cdots + t + 1)a. \tag{27}$$

If $0 \le t < 1$ then (27) can be written as

$$Q \subseteq t^k Q + \frac{t^k - 1}{t - 1} a.$$

Since Q is bounded, when $k \to \infty$, we have

$$Q \subseteq \{0\} + \frac{-1}{t-1} a = \left\{ \frac{-1}{t-1} a \right\},$$

contradicting to the assumption that Q has at least two points. Therefore $t = 1$. Then (26) is the same as

$$r + Q \subseteq Q. \tag{28}$$

For any integer $k > 0$, applying (28) k times yields $kr + Q \subseteq Q$. This is impossible if $r \neq 0$, as Q is bounded. Therefore $r = 0$ and so $A = \{0\}$. The theorem is proved. □

Corollary 4.11. *Let $f \in F[X_1, \dots, X_n]$. If the Newton polytope of f has one indecomposable edge and is contained in a triangle which has the indecomposable edge as one of its sides then f is absolutely irreducible over F.*

This corollary includes Eisenstein-Dumas and Stepanov-Schmidt criteria as special cases. In Figure 4 (a)–(c), we give examples of Corollary 4.11 when $n = 2$. Any polynomial whose Newton polytope is one of them must be absolutely irreducible. The case (a) corresponds to the Eisenstein-Dumas criterion. In this case, P_f has only one point on the dotted vertical line (which means that f has degree n and the coefficient of X^n is a constant in F), so P_f is contained in a triangle with two vertices on the y-axis. The case (b) corresponds to the Stepanov-Schmidt criterion. For example, for any polynomial $g \in F[X]$ of odd degree, the bivariate polynomial $Y^2 + g$ is absolutely irreducible over F, as its Newton polytope is of type (b). In the case (c), the dotted triangle can be at any position, so (a) is a special case of it. For an example, the polynomial $f = X^n + Y^m + X^{n+u}Y^v + X^iY^{m+j}$ has a Newton polytope of type (c) whenever

$$\gcd(n, m) = 1, \quad \frac{j}{i} < \frac{v}{u},$$

where $i, u \ge 1$ and $j, v \ge 0$. So f is absolutely irreducible under the above restriction. The case (d) is a solid contained in the tetrahedron with vertices $(0,0,0), (n,0,0), (0,m,0)$ and $(0,0,z)$ for some number z. For an example, if $\gcd(n,m) = 1$ then the polynomial $1 + X^n + Y^m + X^uZ^v + Y^iZ^j + Z^w$ has Newton polytope of type (d) and so is absolutely irreducible for any choice of v, w and j, provided $u < n$ and $i < m$.

One can construct many types of indecomposable polytopes of any dimension by combining Theorems 4.2 and 4.10, and thus give many types of absolutely irreducible polynomials of many variables over any given field.

Finally, we briefly discuss the relationship of our decomposability to that of Grünbaun [10, Chapter 15]. Let P, Q be polytopes in $\mathbb{R}^n$ (not necessarily integral). Q is said to be *homothetic* to P if there is a real number $t > 0$ and a vector $a \in \mathbb{R}^n$ such that

$$Q = tP + a = \{tb + a : b \in P\}.$$

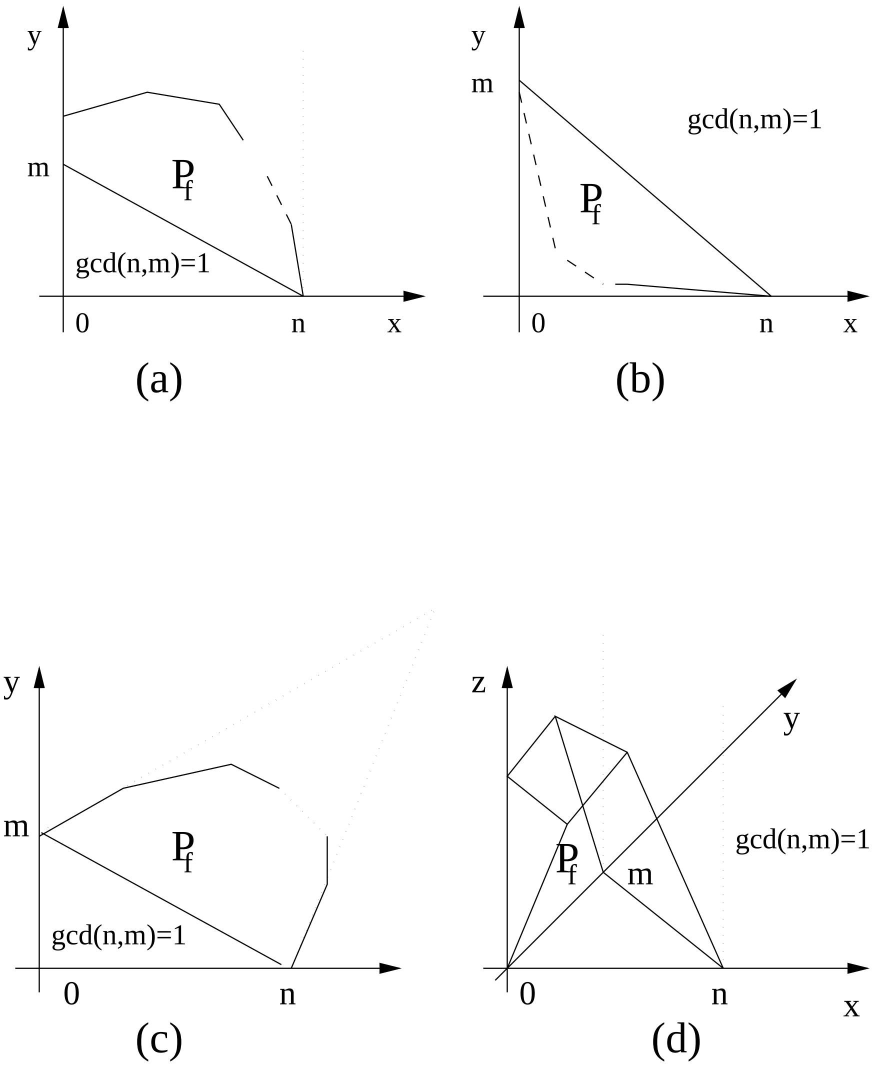

Figure 4. Indecomposable polytopes

A polytope Q is called *homothetically indecomposable* if $Q = P_1 + P_2$ for any polytopes P_1 and P_2 then either P_1 or P_2 is homothetic to Q. Otherwise, Q is called *homothetically decomposable.* Indecomposable polytopes in this sense have been extensively studied in the literature [8, 13, 20, 21, 34, 35, 36].

Homothetic decomposability is not comparable with integral decomposability. On the one hand, a triangle is always homothetically indecomposable, but an integral triangle is integrally indecomposable iff the condition in Corollary 4.5 is satisfied. On the other hand, any polygon with more than 3 edges in the plane is homothetically decomposable, while Figure 4 shows many integrally indecomposable polygons!

References

[1] , L.M. Adleman, "The function field sieve," in *Algorithmic number theory* (Ithaca, NY, 1994), 108–121, Lecture Notes in Comput. Sci., 877, Springer, Berlin, 1994.

[2] M. Balinski, "On the graph structure of convex polyhedra in n-space," *Pacific J. Math.* **11** (1961), 431–434.

[3] J. W. S. Cassels, *Local Fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, London, 1986.

[4] G. Dumas, "Sur queques cas d'irreductibilite des polynomes à coefficients rationnels," *Journal de Math. Pures et Appliqués*, **2** (1906), no. 2, 191–258.

[5] G. Eisenstein, "Über die Irreduzibilität und einige andere Eigenschaften der Gleichungen," *Journal für die Reine und Angew. Math.* **39** (1850), 160–179.

[6] G. Ewald, *Combinatorial Convexity and Algebraic Geometry*, GTM 168, Springer 1996.

[7] M. Filaseta, "The irreducibility of all but finitely many Bessel polynomials," *Acta Math.* **174** (1995), no. 2, 383–397.

[8] D. Gale, "Irreducible convex sets," *Proc. Intern. Congr. Math.*, Amsterdam 1954, vol. 2, 217–218.

[9] S. Gao and M. A. Shokrollahi, "Computing roots of polynomials over function fields of curves," preprint, 1998.

[10] B. Grünbaum, *Convex Polytopes*, London, New York, Sydney, Interscience Publ., 1967.

[11] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.

[12] H. Janwa, G. McGuire and R. M. Wilson, "Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2)," *J. Algebra* **178** (1995), no. 2, 665–676.

[13] M. Kallay, "Indecomposable polytopes," *Israel J. Math.* **41** (1982), no. 3, 235–243.

[14] E. Kaltofen, "Fast parallel absolute irreducibility testing," *J. Symbolic Comput.* **1** (1985), no. 1, 57–67.

[15] E. Kaltofen, "Deterministic irreducibility testing of polynomials over large finite fields," *J. Symbolic Comput.* **4** (1987), no. 1, 77–82.

[16] S. K. Khanduja and J. Saha, "On a generalization of Eisenstein's irreducibility criterion," *Mathematika* **44** (1997), no. 1, 37–41.

[17] J. Kurschak, "Irreduzible Formen," *Journal für die Reine und Angew. Math.* **152** (1923), 180–191.

[18] A. Lipkovski, "Newton polyhedra and irreducibility," *Math. Z.* **199** (1988), 119–127.

[19] S. MacLane, "The Schönemann-Eisenstein irreducibility criteria in terms of prime ideals," *Trans. Amer. Math Soc.* **43** (1938), 226–239.

[20] P. McMullen, "Indecomposable convex polytopes," *Israel J. Math.* **58** (1987), no. 3, 321–323.

[21] W. Meyer, "Indecomposable polytopes," *Trans. Amer. Math. Soc.* **190** (1974), 77–86.

[22] J. Mott, "Eisenstein-type irreducibility criteria," in *Zero-dimensional commutative rings* (Knoxville, TN, 1994), 307–329, Lecture Notes in Pure and Appl. Math., 171, Dekker, New York, 1995.

[23] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Math. and Its Appl., Vol. 20, Addison-Wesley Publ. Co., Reading, Mass., 1983, xx + 755 pp.

[24] O. Ore, "Zur Theorie der Irreduzibilitätskriterien," *Math. Zeit.* **18** (1923), 278–288.

[25] O. Ore, "Zur Theorie der Eisensteinschen Gleichungen," *Math. Zeit.* **20** (1924), 267–279.

[26] O. Ore, "Zur Theorie der Algebraisschen Körper," *Acta. Math.* **44** (1924), 219–314.

[27] A. M. Ostrowski, "On multiplication and factorization of polynomials, I. Lexicographic ordering and extreme aggregates of terms," *Aequationes Math.* **13** (1975), 201–228.

[28] A. M. Ostrowski, "On multiplication and factorization of polynomials, II. Irreducibility discussion," *Aequationes Math.* **14** (1976), 1–32.

[29] T. Rella, "Ordnungsbestimmungen in Integritätsbereichen und Newtonsche Polygone," *Journal für die Reine und Angew. Math.* **158** (1927), 33–48.

[30] H. Rådström, "An embedding theorem for spaces of convex sets," *Proc. Amer. Math. Soc.* **3** (1952), 165–169.

[31] W. M. Schmidt, *Equations over Finite Fields: an Elementary Approach*, Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin-New York, 1976.

[32] T. Schönemann, "Von denjenigen moduln, welche potenzen von primzahlen sind," *Journal für die Reine und Angew. Math.* **32** (1846), 93–105.

[33] C. Shanok, "Convex polyhedra and criteria for irreducibility," *Duke Mathematical Journal* **2** (1936), 103–111.

[34] G. C. Shephard, "Decomposable convex polyhedra," *Mathematika* **10** (1963), 89–95.

[35] Z. Smilansky, "An indecomposable polytope all of whose facets are decomposable," *Mathematika* **33** (1986), no. 2, 192–196.

[36] Z. Smilansky, "Decomposability of polytopes and polyhedra," *Geometriae Dedicata* **24** (1987), no. 1, 29–49.

[37] S. A. Stepanov, "Congruences with two unknowns" (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 683–711.

[38] S. A. Stepanov, "Rational points of algebraic curves over finite fields" (Russian), *Current problems of analytic number theory* (Proc. Summer School, Minsk, 1972) (Russian), pp. 223–243, 272. Izdat. "Nauka i Tehnika", Minsk, 1974.

[39] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[40] *T. Szönyi*, "Some applications of algebraic curves in finite geometry and combinatorics," in *Surveys in Combinatorics, 1997* (R. A. Railey, Ed.), London Mathematical Society Lecture Notes Series 241, Cambridge University Press, 1997.

[41] R. Webster *Convexity*, Oxford University Press, Oxford, 1994.

[42] K. S. Williams "Eisenstein's criteria for absolute irreducibility over a finite field," *Canad. Math. Bull.* **9** (1966), 575–580.

[43] G. M. Ziegler, *Lectures on Polytopes*, GTM 152, Springer-Verlag, 1995.

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634 USA
E-mail address: sgao@math.clemson.edu