ABSOLUTE IRREDUCIBILITY OF POLYNOMIALS VIA NEWTON POLYTOPES

SHUHONG GAO
DEPARTMENT OF MATHEMATICAL SCIENCES
CLEMSON UNIVERSITY
CLEMSON, SC 29634 USA
SGAO@MATH.CLEMSON.EDU

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 remaining absolutely irreducible when their coefficients are modified arbitrarily in the field, but keeping certain collection of them nonzero.

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, 25, 28, 38]. We examine the Newton polygon method and generalize it through Newton polytopes associated with multivariable polynomials. This leads us to a more general geometric criterion for absolute irreducibility of 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 [14], combinatorics [47], algebraic geometric codes [45], 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 even if their coefficients are modified arbitrarily but with certain collection 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 [22], Ore [30, 31, 32], Rella [35]) have generalized this criterion by using Newton polygons. Assume that $f_0f_n \neq 0$. One can

1991 *Mathematics Subject Classification.* Primary 12E05, 52B20; Secondary 13P05, 13B25, 12Y05.

Key words and phrases. Fields, multivariable polynomials, absolute irreducibility, Newton polytopes, Newton polygons, indecomposable polytopes, Eisenstein criterion, Minkowski sums.

construct a polygon in the Euclidean plane as follows. Suppose that the coefficient f_i is divisible by p^{a_i} but not any higher power, where $a_i \geq 0$ and a_i is undefined if $f_i = 0$. Plot the points $(0, a_0)$, $(1, a_1)$, $\ldots$, (n, a_n) in the Euclidean plane and form the 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, 20, 25]. 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 (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.*

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. The Eisenstein-Dumas criterion is also discovered by Wan [48].

In [36, Theorem 1B, p. 92], Schmidt describes another method for constructing absolutely irreducible polynomials which he attributes to Stepanov [43, 44]. 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 $(0, a_0)$, $(1, a_1)$, $\ldots$, (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 considering 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 Newton polytopes associated with polynomials is due to Ostrowski (1921) and is similarly defined for any multivariable polynomials. Ostrowski realizes that the factorization of polynomials implies

the decomposition of polytopes in the sense of Minkowski sum. In the 1970s, Ostrowski wrote two papers [33, 34] 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.

More precisely, we study the irreducibility of multivariable polynomials through the decomposability of their Newton polytopes. Our main contribution is in the construction of indecomposable polytopes and thus give many classes of absolutely irreducible polynomials over an arbitrary field. To get a glimpse of our results, we give two examples here; more general results can be found in Section 4.

Example 1. Let F be any field and

$$f = aX^n + bY^m + cX^uY^v + \sum c_{ij}X^iY^j \in F[X,Y]$$

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.

Example 2. 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). Then f is absolutely irreducible over F, provided $\gcd(\ell,m,n,u,v,w) = 1$.

Our paper is organized as follows. In the next section, we define the decomposability of polytopes with respect to Minkowski sums and discuss its relation with the factorization of polynomials. A general irreducibility criterion is established. Note our concept of decomposability of polytopes is incompatible with that in the literature, say in Grünbaun's book [13, Chapter 15]. In Section 3, we collect properties of Minkowski sums of polytopes, particularly on the decomposition of faces of polytopes. 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.

Related works. We should mention that Lipkovski [24] 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). To that extent, Lipkovski's method is local while our polytope method is somewhat 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. Wan [49] uses Newton polygon to study zeta functions and L functions. Recently, Gao and Shokrollahi [10] use Newton polygon method to compute roots of polynomials over function fields of curves. For a survey of Newton polygon method, see Mott [28].

There are several 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. Another method is presented by Janwa, McGuire and Wilson [15] using

Bezout's theorem on intersection multiplicity of curves. Noether's irreducibility forms [29] give yet another powerful method for proving irreducibility of polynomials. Noether's forms are carefully analysed by Schmidt [36] and greatly improved by Kaltofen [19] and Gao [9]. For efficient algorithms for testing irreducibility of multivariable polynomials, see von zur Gathen [11] and Kaltofen [17, 18].

We should also mention that Newton polytopes have been used extensively to study toric ideals and solutions of systems of (multivariable) polynomial equations; see Gel'fand et al [12], Khovanskiĭ [21], Sturmfels [46] and the references there.

2. Polytope method

We assume that the reader is familiar with the basic properties of polytopes; see Ewald [6], Grünbaun [13], Webster [50] and Ziegler [52]. For the convenience of the reader, we review some basic concepts that will be needed in the sequel.

Let $\mathbb{R}$ be the set of real numbers and n a positive integer. 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,

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

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

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

When $S = \{a_1, \ldots, a_k\}$ is a finite set, denote $\text{conv}(S)$ by $\text{conv}(a_1, \ldots, a_k)$, which is called the convex hull of $a_1, \ldots, a_k$. The convex hull of finitely many points is called a polytope. A point of a polytope is called a vertex if it is not on the line segment of any other two points of the polytope. It is well known that a polytope is always the convex hull of its vertices.

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

For two sets A and B in $\mathbb{R}^n$, define $A + B = \{a + b : a \in A, b \in B\}$, which is called the Minkowski sum of A and B.

Lemma 2.1 (Ostrowski [33])**.** *Let $f, g, h \in F[X_1, X_2, \cdots, X_n]$ with $f = gh$. Then $P_f = P_g + P_h$.*

Proof. This result is well known in the literature. For the sake of completeness, we give a simple proof here. 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 a vertex 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 [13, Chapter 15]; see the comments at the end of the paper. Since we will not encounter any other type of decomposability in this paper, the word "integrally" will be freely omitted in the sequel.

Irreducibility criterion. *Let F be any field and $f \in F[X_1, X_2, \cdots, X_n]$ 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, if $f = 1 + Y + XY + X^2 + Y^2$ then P_f is decomposable (equal to the sum of the triangle $(0,0)$–$(1,0)$–$(0,1)$ with itself). Over a field F of characteristic different from two, it can be verified directly that f is absolutely irreducible. Over a field F of characteristic two, however, we have

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

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

It remains to show that indecomposable Newton polytopes exist, thus absolutely irreducible polynomials can be constructed via the irreducibility criterion above. This will be our main focus in Section 4. We conclude this section with some comments.

Remarks. 1. 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.

2. In [33], 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 [34], 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.

3. For the case of polynomials with three variables, the concept of Newton polytope also appears in Shanok's paper [39]. Shanok develops irreducibility criteria for polynomials by projecting a Newton polytope from $\mathbb{R}^3$ into planes.

4. As mentioned in the introduction, Lipkovski [24] 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.

3. Some properties of polytopes

To further discuss the decomposability of polytopes, we need more properties about Minkowski sums of polytopes, particularly on the decomposition of their faces. Minkowski sums of convex sets have been extensively studied in the literature, see for example Schneider [37].

Let P be a polytope in $\mathbb{R}^n$. A *face* of P is by definition the intersection of P with a supporting hyperplane to P. In another word, a face of P is the set of all the points in P that maximize some linear function. A vertex is a just face of dimension 0. A face of dimension 1 is a line segment, called an *edge* of P. A face of dimension one less than that of P is called *facet* of P.

The next result describes how faces decompose in a Minkowski sum of polytopes; for its proof, see Ewald [6, Theorem 1.5], Grünbaun [13, Theorem 1, p. 317], or Schneider [37, Theorem 1.7.5].

Lemma 3.1. *Let A and B be polytopes in $\mathbb{R}^n$ and $C = A + B$.*

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

(b) *Let C_1 be any 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 $C_1 = A_1 + B_1$.

Note that part (b) is the constructive version of part (a) and it says that the decomposition of all the faces are determined by the decomposition of vertices alone.

This is extremely useful in applications. Part (a) can be strengthened as follows. Let C_1 be any face of C. Suppose that A_1 and B_1 are any convex subsets of A and B, respectively, such that $C_1 = A_1 + B_1$. Then A_1 and B_1 must be faces of A and B, respectively. The proof is a little subtle and will be given elsewhere.

A polytope is associated naturally with a graph consisting of its vertices and edges.

Lemma 3.2 (Balinski [2])**.** *The graph of a polytope of dimension n is n-connected.*

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 $\lambda \geq 0$. The next result must be known in the literature, but we could not find a convenient reference, so a proof is included.

Lemma 3.3. *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 $t \geq 0$ 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 $a \neq \mathbf{v}$,

$$\alpha \cdot a < \alpha \cdot \mathbf{v}. \tag{3}$$

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

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

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

$$\alpha \cdot a_1 = \alpha \cdot \mathbf{v}. \tag{4}$$

For any $t \geq 0$,

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

belongs to C, as $a_1, b \in C$ and C is a convex cone with vertex $\mathbf{v}$. By (4), $\alpha \cdot (b + t(a_1 - \mathbf{v})) = \alpha \cdot b = \beta$. Hence $b + t(a_1 - \mathbf{v}) \in H$ and $b + t(a_1 - \mathbf{v}) \in C \cap H = Q$ for all $t \geq 0$, contradicting to the boundness of Q (note that $a_1 \neq \mathbf{v}$). Therefore (3) holds.

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

$$\{\mathbf{v} + \lambda(a - \mathbf{v}) : \lambda \geq 0\} \tag{5}$$

with the hyperplane

$$r + H = \{r + x \in \mathbb{R}^n : \alpha \cdot x = \beta\} = \{x \in \mathbb{R}^n : \alpha \cdot x = \alpha \cdot r + \beta\}. \tag{6}$$

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 (3), $\lambda \geq 0$ iff $\alpha \cdot r \leq \alpha \cdot \mathbf{v} - \beta$. In the latter case, $r + H$ intersects every ray (5) at a unique point determined by λ above.

For $r = 0$, since $\alpha \cdot \mathbf{v} - \beta > 0 = \alpha \cdot r$, each ray (5) intersects H, thus Q, at a unique point. Hence we may index all the rays (5) by $a \in Q$. Now suppose that

$\alpha \cdot r \leq \alpha \cdot \mathbf{v} - \beta$. Then for each $a \in Q$, the ray (5) 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 $t = \lambda_0$. □

4. Indecomposable polytopes and absolutely irreducible polynomials

We now proceed to construct 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 $\text{conv}(\mathbf{v}_1, \mathbf{v}_2)$ is simply denoted by $\mathbf{v}_1\mathbf{v}_2$. For an integral point or vector $\mathbf{v} = (a_1, \ldots, a_n)$, we write $\gcd(\mathbf{v})$ to mean $\gcd(a_1, \ldots, a_n)$, i.e. the greatest common divisor of the components in $\mathbf{v}$. Similarly, for several points $\mathbf{v}_1, \ldots, \mathbf{v}_k$, $\gcd(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ means the gcd of all the components in $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 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 $d - 1 + 2 = d + 1$.

Suppose $\mathbf{v}_2 = \mathbf{v}_0 + i/d(\mathbf{v}_1 - \mathbf{v}_0)$ 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. Let $C = \text{conv}(\mathbf{v}, Q)$ as depicted in Figure 1. 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 $\mathbf{vv}_1, \ldots, \mathbf{vv}_k$ are edges of C. By Lemma 3.1, there are unique vertices $\mathbf{a}_i \in A$ and $\mathbf{b}_i \in B$ such that

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

and

$$\mathbf{vv}_i = \mathbf{va}_i + 0\mathbf{b}_i, \quad 1 \le i \le k.$$

Since $0 \in 0\mathbf{b}_i$, the line segment $\mathbf{va}_i$ coincides with part of $\mathbf{vv}_i$ starting at $\mathbf{v}$; see Figure 1. Now take any two vertices, say $\mathbf{v}_1$ and $\mathbf{v}_2$ that are connected by an edge

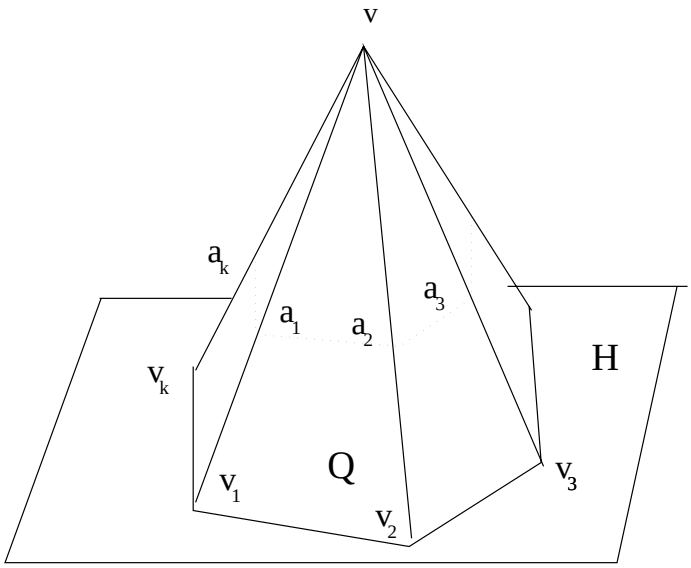

FIGURE 1. Indecomposable pyramid

in Q. Then $\mathbf{v}_1\mathbf{v}_2$ is also an edge of C. Again Lemma 3.1 (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

$$\frac{\gcd(\mathbf{a}_1 - \mathbf{v})}{\gcd(\mathbf{v}_1 - \mathbf{v})} = \frac{\gcd(\mathbf{a}_2 - \mathbf{v})}{\gcd(\mathbf{v}_2 - \mathbf{v})}. \tag{7}$$

By Lemma 3.2, the graph of a polytope is connected. Since the equation (7) holds for any two adjacent vertices, we see that

$$\frac{|\mathbf{a}_i - \mathbf{v}|}{|\mathbf{v}_i - \mathbf{v}|} = \frac{\gcd(\mathbf{a}_i - \mathbf{v})}{\gcd(\mathbf{v}_i - \mathbf{v})} = t, \quad 1 \le i \le k, \tag{8}$$

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

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

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

we see that d must be 1. Hence $m = 0$ or 1, and so $t = 0$ or 1. If $t = 0$ then (8) implies that $\mathbf{a}_i = \mathbf{v}$ for $1 \le i \le k$; so $A = \{\mathbf{v}\}$. If $t = 1$ then (8) 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 $\gcd(\mathbf{v} - \mathbf{v}_1, \mathbf{v} - \mathbf{v}_2, \dots, \mathbf{v} - \mathbf{v}_k) = d > 1$. 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

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

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

For example, Let f be the polynomial $1 + X^n + Y^m + X^n Y^m + X^i Y^j Z^k \in F[X, Y, Z]$ 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.

The following corollaries specialize to the simple cases when Q is an integral point, a line segment or a triangle.

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 (Ostrowski [34, Theorem IX])**.** *A two-term polynomial*

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

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

For examples, $X^n + Y^m$ is absolutely irreducible over F iff $\gcd(n, m) = 1$; similarly, $Y^i + X^j Z^k$ 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 $f = aX^n + bY^m + cX^u Y^v + \sum c_{ij} X^i Y^j \in F[X, Y]$ 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.*

Corollary 4.10. *Let $f = g(X) + h(X_1, \ldots, X_n)$ where $g \in F[X]$ of degree r and $h \in F[X_1, \ldots, X_n]$ of total degree m. If $\gcd(r,m) = 1$ then f is absolutely irreducible over F.*

Proof. By a translation of the variable X, we may assume that the constant of f is nonzero. So the Newton polytope of f is a pyramid with the Newton polytope of h as its base. Since h has total 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_h. Since g has degree r, X^r has a nonzero coefficient in f and its exponent vector $(r,0,\ldots,0) = \mathbf{v}$ is a vertex of the pyramid outside its base. Since $\gcd(m,r) = 1$ and $k_1 + \cdots + k_n = m$, we have

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

By the above corollary, P_f is indecomposable and so f is absolutely irreducible over F. □

Theorem 4.11. *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 2. 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 3.1, 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 that $A = A_1 = \{0\}$. This is geometrically "clear" from Figure 2, as any shift $r + Q$, $r \neq 0$, of Q can not be contained in the cone $\text{conv}(\mathbf{v}, Q)$, not to mention in C. We prove it algebraically.

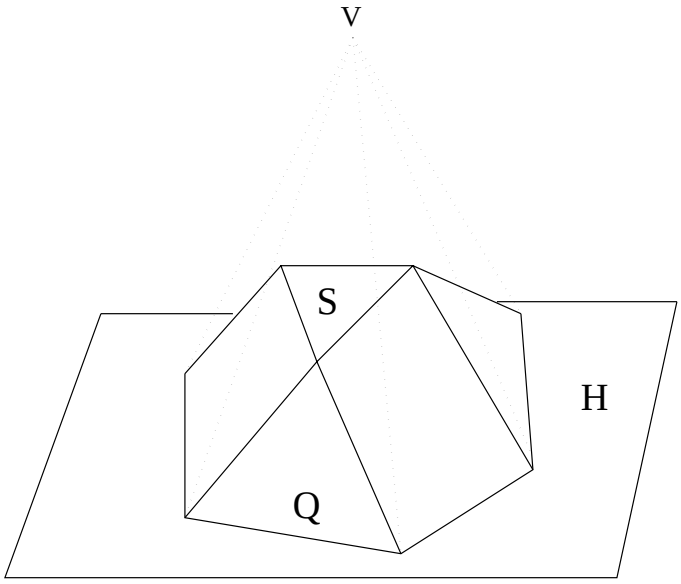

FIGURE 2. $C = \text{conv}(S, Q)$

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

$$r + Q \subseteq C \cap (r + H). \tag{9}$$

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

$$C_1 \supseteq \text{conv}(\mathbf{v}, Q) \supseteq C \text{ and } C_1 \cap H = Q. \tag{10}$$

By (9),

$$r + Q \subseteq C_1 \cap (r + H), \tag{11}$$

so the latter is nonempty. By Lemma 3.3, there exists a number $t \geq 0$ such that

$$(r + H) \cap C_1 = \mathbf{v} + t(Q - \mathbf{v}). \tag{12}$$

We show that $t \leq 1$. Take any $a \in Q$. Then $r + a \in C_1 \cap (r + H)$. By (12), there exists $b \in Q$ such that $r + a = \mathbf{v} + t(b - \mathbf{v})$. Also, since $r + a \in C \subseteq \text{conv}(\mathbf{v}, Q)$, 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

$$t(b - \mathbf{v}) = t_1(b_1 - \mathbf{v}). \tag{13}$$

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 (13) 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 (11) and (12) imply that $r + Q \subseteq \mathbf{v} + t(Q - \mathbf{v})$, i.e.,

$$Q \subseteq tQ + a \tag{14}$$

where $a = (1 - t)\mathbf{v} - r \in \mathbb{R}^n$. For any integer $k > 0$, applying (14) k times yields

$$Q \subseteq t^k Q + (t^{k-1} + \cdots + t + 1)a. \tag{15}$$

If $0 \le t < 1$ then (15) 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 (14) is the same as

$$r + Q \subseteq Q. \tag{16}$$

For any integer $k > 0$, applying (16) 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. □

For an example with $n = 3$, Figure 3 (d) shows a polytope contained in the tetrahedron with vertices $(0,0,0), (n,0,0), (0,m,0)$ and $(0,0,u)$ for some number u. It is indecomposable if $\gcd(n,m) = 1$. For the polynomial $f = 1 + X^n + Y^m + X^u Z^v + Y^i Z^j + Z^w$, its Newton polytope is of type (d) if $u < n$ and $i < m$. Hence f is absolutely irreducible for any choice of v, w and j, provided $u < n$ and $i < m$.

The next corollary deals with the case $n = 2$.

Corollary 4.12. *Let $f = aX^m + by^n + \sum c_{ij} X^i Y^j \in F[X,Y]$ with a, b nonzero and (i,j) different from $(m,0), (0,n)$. Suppose that the Newton polytope of f is contained in the triangle with vertices $(m,0), (0,n)$ and (u,v) for some point $(u,v) \in \mathbb{R}^2$. If $\gcd(m,n) = 1$ then f is absolutely irreducible over F.*

This corollary includes Eisenstein-Dumas and Stepanov-Schmidt criteria as special cases, as shown in Figure 3 (a)–(c). 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 in X 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. 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 $f = X^2 + y^3 + aX^3Y + bX^4y^6 + cX^{11}Y^{10}$ has a Newton polytope of type (c), so is absolutely irreducible over F for any values of a, b, c. For another 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.

We should emphasize that Theorems 4.2 and 4.11 can be used to build many types of indecomposable polytopes in higher dimensions iteratively from lower dimensions. Thus one can obtain many types of absolutely irreducible polynomials over any given field.

Finally, we briefly discuss the relationship of our decomposability to that of Grünbaun [13, 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

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

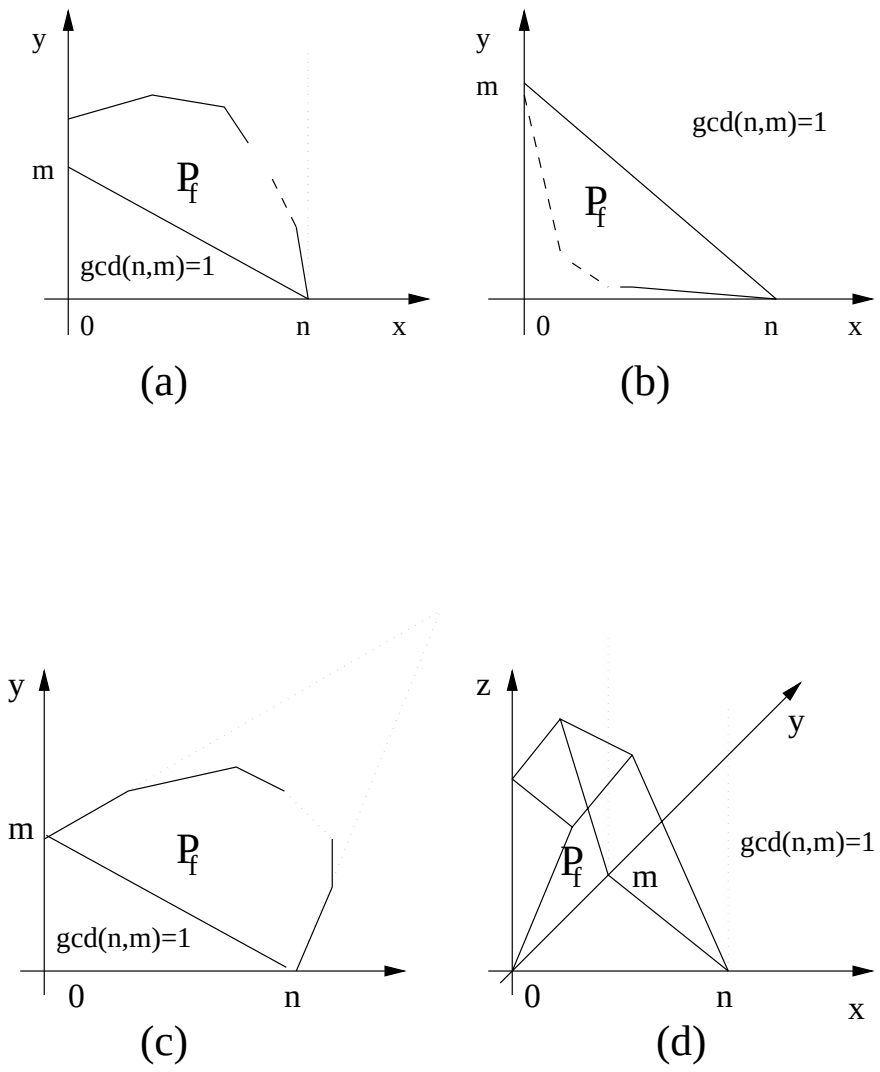

FIGURE 3. Indecomposable polytopes

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, 16, 26, 27, 40, 41, 42].

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 3 shows many integrally indecomposable polygons!

Acknowledgement. The author would like to thank Joel Brawley, Erich Kaltofen, Jenny Key, Hendrik Lenstra, Jr., and Daqing Wan for their useful comments of an earlier version of the paper and for bringing some of the references to his attention. Thanks is also due to Joe Mott for sending a copy of his paper to the author. A preliminary version of the paper was presented at an Oberwolfach Workshop on Designs and Codes, March 15–21, 1998, Germany, and at a Dagstuhl-Seminar on Algorithms and Number Theory, October 26 – 30, 1998, Germany.

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, "Factoring multivariable polynomials," in preparation.
[10] S. Gao and M. A. Shokrollahi, "Computing roots of polynomials over function fields of curves," preprint, 1998.
[11] J. von zur Gathen, "Irreducibility of multivariate polynomials," *J. Comput. System Sci.* **31** (1985), no. 2, 225–264.
[12] I. Gel'fand, M. Kapranov and A. Zelevinsky, *Discriminants, Resultants and Multi-Dimensional Determinants*, Birkhäuser, Boston, 1994.
[13] B. Grünbaum, *Convex Polytopes*, London, New York, Sydney, Interscience Publ., 1967.
[14] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.
[15] 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.
[16] M. Kallay, "Indecomposable polytopes," *Israel J. Math.* **41** (1982), no. 3, 235–243.
[17] E. Kaltofen, "Fast parallel absolute irreducibility testing," *J. Symbolic Comput.* **1** (1985), no. 1, 57–67.
[18] E. Kaltofen, "Deterministic irreducibility testing of polynomials over large finite fields," *J. Symbolic Comput.* **4** (1987), no. 1, 77–82.
[19] E. Kaltofen, "Effective Noether irreducibility forms and applications," Symposium on the Theory of Computing (New Orleans, LA, 1991). *J. Comput. System Sci.* **50** (1995), no. 2, 274–295.
[20] S. K. Khanduja and J. Saha, "On a generalization of Eisenstein's irreducibility criterion," *Mathematika* **44** (1997), no. 1, 37–41.
[21] A. G. Khovanskiĭ, *Fewnomials*, Translations of Mathematical Monographs, vol. 88, American Mathematical Society, 1991.
[22] J. Kurschak, "Irreduzible Formen," *Journal für die Reine und Angew. Math.* **152** (1923), 180–191.
[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] A. Lipkovski, "Newton polyhedra and irreducibility," *Math. Z.* **199** (1988), 119–127.
[25] S. MacLane, "The Schönemann-Eisenstein irreducibility criteria in terms of prime ideals," *Trans. Amer. Math Soc.* **43** (1938), 226–239.

[26] P. McMullen, "Indecomposable convex polytopes," *Israel J. Math.* **58** (1987), no. 3, 321–323.
[27] W. Meyer, "Indecomposable polytopes," *Trans. Amer. Math. Soc.* **190** (1974), 77–86.
[28] 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.
[29] E. Noether, "Ein algebraisches Kriterium für absolute Irreduzibilität," *Math. Ann.* **85** (1922), 26–33.
[30] O. Ore, "Zur Theorie der Irreduzibilitätskriterien," *Math. Zeit.* **18** (1923), 278–288.
[31] O. Ore, "Zur Theorie der Eisensteinschen Gleichungen," *Math. Zeit.* **20** (1924), 267–279.
[32] O. Ore, "Zur Theorie der Algebraisschen Körper," *Acta. Math.* **44** (1924), 219–314.
[33] A. M. Ostrowski, "On multiplication and factorization of polynomials, I. Lexicographic ordering and extreme aggregates of terms," *Aequationes Math.* **13** (1975), 201–228.
[34] A. M. Ostrowski, "On multiplication and factorization of polynomials, II. Irreducibility discussion," *Aequationes Math.* **14** (1976), 1–32.
[35] T. Rella, "Ordnungsbestimmungen in Integritätsbereichen und Newtonsche Polygone," *Journal für die Reine und Angew. Math.* **158** (1927), 33–48.
[36] W. M. Schmidt, *Equations over Finite Fields: an Elementary Approach*, Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin-New York, 1976.
[37] R. Schneider, *Convex bodies: the Brunn-Minkowski theory*, Encyclopedia of Mathematics and its Applications, 44. Cambridge University Press, Cambridge, 1993.
[38] T. Schönemann, "Von denjenigen moduln, welche potenzen von primzahlen sind," *Journal für die Reine und Angew. Math.* **32** (1846), 93–105.
[39] C. Shanok, "Convex polyhedra and criteria for irreducibility," *Duke Mathematical Journal* **2** (1936), 103–111.
[40] G. C. Shephard, "Decomposable convex polyhedra," *Mathematika* **10** (1963), 89–95.
[41] Z. Smilansky, "An indecomposable polytope all of whose facets are decomposable," *Mathematika* **33** (1986), no. 2, 192–196.
[42] Z. Smilansky, "Decomposability of polytopes and polyhedra," *Geometriae Dedicata* **24** (1987), no. 1, 29–49.
[43] S. A. Stepanov, "Congruences with two unknowns" (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 683–711.
[44] 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.
[45] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.
[46] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series, vol. 8. American Mathematical Society, 1996.
[47] *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.
[48] D. Wan, "Minimal polynomials and distinctness of Kloosterman sums," *Finite Fields and Their Applications* **1** (1995), no. 2, 189–203.
[49] D. Wan, "Newton polygons of zeta functions and L functions," *Ann. of Math. (2)* **137** (1993), no. 2, 249–293.
[50] R. Webster, *Convexity*, Oxford University Press, Oxford, 1994.
[51] K. S. Williams "Eisenstein's criteria for absolute irreducibility over a finite field," *Canad. Math. Bull.* **9** (1966), 575–580.
[52] G. M. Ziegler, *Lectures on Polytopes*, GTM 152, Springer-Verlag, 1995.