A GEOMETRIC APPROACH
TO
ABSOLUTE IRREDUCIBILITY OF POLYNOMIALS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

FATİH KOYUNCU

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE
OF
DOCTOR OF PHILOSOPHY
IN
THE DEPARTMENT OF MATHEMATICS

APRIL 2004

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Canan Özgen
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Şafak Alpay
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Doç. Dr. Ferruh Özbudak
Supervisor

Examining Committee Members

Prof. Dr. Ersan Akyıldız

Prof. Dr. Mehpare Bilhan

Prof. Dr. Mahmut Kuzucuoğlu

Prof. Dr. Sinan Sertöz

Doç. Dr. Ferruh Özbudak

TABLE OF CONTENTS

ABSTRACT v

ÖZ vi

ACKNOWLEDGEMENTS viii

CHAPTER

1. INTRODUCTION 1

2. PRELIMINARIES 6

2.1 Some Properties of Convex Sets 6

2.2 Supporting Hyperplanes and Faces of Polytopes 12

3. INTEGRALLY INDECOMPOSABLE POLYGONS 17

3.1 Line Segments 19

3.2 Triangles 22

3.3 Quadrangles 23

3.4 Pentagons 35

4. INTEGRALLY INDECOMPOSABLE POLYTOPES IN $\mathbb{R}^n$ 45

4.1 Relation Between Integral and Homothetic Indecomposability of Polytopes 46

4.2 A New Observation Giving New Integrally Indecomposable Polytopes in $\mathbb{R}^n$ 57

5. ON ABSOLUTE IRREDUCIBILITY OF SOME POLYNOMIALS OVER LARGE CHARACTERISTICS 67

5.1 Introduction 67

5.2 Main Observation And Result 68

6. PROBABILITY OF THE POLYNOMIALS TO BE IRREDUCIBLE BY THE POLYTOPE METHOD 73

BIBLIOGRAPHY 76

ABSTRACT

A GEOMETRIC APPROACH TO ABSOLUTE IRREDUCIBILITY OF POLYNOMIALS

Koyuncu, Fatih
Ph.D., Department of Mathematics
Supervisor: Doç. Dr. Ferruh Özbudak

April 2004, 78 pages.

This thesis is a contribution to determine the absolute irreducibility of polynomials via their Newton polytopes.

For any field F, a polynomial $f \in F[x_1, x_2, ..., x_k]$ can be associated with a polytope, called its Newton polytope. If the polynomial f has integrally indecomposable Newton polytope, in the sense of Minkowski sum, then it is absolutely irreducible over F, i.e. irreducible over every algebraic extension of F. We present some new results giving integrally indecomposable classes of polytopes. Consequently, we have some new criteria giving infinitely many types of absolutely irreducible polynomials over arbitrary fields.

Keywords: Polynomials, absolute irreducibility, polytopes, integral indecomposability.

ÖZ

POLİNOMLARIN İNDİRGENEMEZLİĞİNE GEOMETRİK BİR YAKLAŞIM

Koyuncu, Fatih
Yüksek Lisans, Matematik Bölümü
Tez Yöneticisi: Doç. Dr. Ferruh Özbudak

Nisan 2004, 78 sayfa.

Bu tez, polinomların Newton çokzirvelilerine göre indirgenemezliğini belirlemeye bir katkıdır.

Herhangi bir F cismi için, $F[x_1, x_2, ..., x_k]$ halkasından alınan bir f polinomu bir Newton çokzirvelisine eşlenebilir. Bu f polinomu, Minkowski toplamına göre ayrılamayan bir Newton çokzirvelisine sahipse, F üzerinde mutlak olarak indirgenemez, yani F'nin her cebirsel uzantısında indirgenemez. Biz burada, integral olarak ayrılamayan çokzirveliler sınıfları veren bazı yeni sonuçlar vermekteyiz. Sonuç olarak, rastgele bir cisim uzerinde sonsuz sayıda indirgenemeyen polinom tipleri veren yeni kriterlere sahip oluyoruz.

Anahtar Sözcükler: Polinomlar, mutlak indirgenemezlik, çokzirveliler, integral ayrılmazlık.

To My Lovable Daughters Beyzanur and Tuğba

ACKNOWLEDGEMENTS

I would like to express sincere appreciation to my supervisor, Doç. Dr. Ferruh Özbudak for his motivation, helpful discussions, encouragement, patience and constant guidance during this work.

Also, I would like to express my deep gratitude to Prof. Dr. Mehpare Bilhan for her guidance, continuous support, attentive insight throughout the research and education at Middle East Technical University.

Finally, I am glad to express my appreciation to my lovely wife Sacide for her continuous helps.

Chapter 1

INTRODUCTION

We know that the classes of absolutely irreducible polynomials are very vital in many areas such as finite geometry [H], algebraic geometric codes [St], combinatorics [Sz], permutation polynomials [LN] and function field sieve [A]. There are some irreducibility criteria of polynomials like Eisenstein's criterion, Eisenstein-Dumas criterion. Moreover, we also have absolute irreducibility criteria of polynomials in the literature as Newton polygon method. Recently, Newton polygon method has been strengthened by Gao in [G1, G2] as Newton polytope method for multivariate polynomials. In this study, we shall give some new integrally indecomposable Newton polytopes which are not included in [G1, G2].

Let $\mathbb{R}^n$ denote the n-dimensional real Euclidean space and S be a subset of $\mathbb{R}^n$. The smallest convex set containing S, denoted by *conv(S)*, is called the *convex hull* of S. Note that

$$conv(S) = \left\{ \sum_{i=1}^{k} \lambda_i x_i : \{x_1, ..., x_k\} \subseteq S, \lambda_i \geq 0, \sum_{i=1}^{k} \lambda_i = 1 \right\}.$$

The *affine hull* aff(S) of S is defined as

$$\text{aff}(S)=\left\{\sum_{i=1}^{k}\lambda_i x_i : \{x_1,...,x_k\}\subseteq S, \sum_{i=1}^{k}\lambda_i=1\right\}.$$

For any point $x\in S$, x is said to be in the *relative interior* of S, denoted as $x\in \text{relint}(S)$, if x lies in the interior of S relative to aff(S), i.e. there exists an open ball B in aff(S) such that $x\in B\subset S$.

The convex hull of finitely many points in $\mathbb{R}^n$ is called a ***polytope***. A point of a polytope is called a *vertex* if it is not on the line segment joining any other two different points of the polytope. It is known that a polytope is always the convex hull of its vertices, for example see [Z, Proposition 2.2].

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

Definition 1.0.1 For any two sets A and B in $\mathbb{R}^n$, the sum

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

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

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

Let F be any field and consider any polynomial

$$f(x_1,x_2,...,x_n)=\sum c_{e_1e_2...e_n}x_1^{e_1}x_2^{e_2}...x_n^{e_n}\in F[x_1,...,x_n].$$

We can think an exponent vector $(e_1,e_2,...,e_n)$ of f as a point in $\mathbb{R}^n$. The ***Newton polytope*** of f, denoted by P_f, is defined as the convex hull in $\mathbb{R}^n$ of all the points $(e_1,...,e_n)$ with $c_{e_1e_2...e_n}\neq 0$.

Recall that a polynomial over a field F is called ***absolutely irreducible*** if it remains irreducible over every algebraic extension of F.

By using Newton polytopes of multivariate polynomials, we can determine infinite families of absolutely irreducible polynomials over an arbitrary field F by using the following result due to Ostrowski [O1].

Lemma 1.0.2 *Let $f, g, h \in F[x_1, ..., x_n]$ with $f = gh$. Then $P_f = P_g + P_h$.*

Proof: See, for example, the proof of [G1, Lemma 2.1]. □

As a direct result of Lemma 1.0.2, we have the following corollary which is an *irreducibility criterion* for multivariate polynomials over arbitrary fields.

Corollary 1.0.3 *Let F be any field and f a nonzero polynomial in $F[x_1, ..., x_n]$ not divisible by any x_i. If the Newton polytope P_f of f is integrally indecomposable then f is absolutely irreducible over F.*

Proof: Since f is not divisible by any x_i, it has no factor having only one term. Let f be reducible over some algebraic extension of F. This means that we have $f = gh$ 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 1.0.2, we have $P_f = P_g + P_h$, which is a contradiction. □

When P_f is integrally decomposable, depending on the given field, f may be reducible or irreducible. For example, $f = x^9 + y^9 + z^9$ has Newton polytope $P_f = conv((9,0,0)(0,9,0)(0,0,9)) = conv((6,0,0)(0,6,0)(0,0,6)) + conv((3,0,0)(0,3,0)(0,0,3))$. But, while $f = x^9 + y^9 + z^9 = (x + y + z)^9$ over $\mathbb{F}_3$, it is irreducible over $\mathbb{F}_2, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}$, where $\mathbb{F}_m$ represents the finite field with m elements. Also, the polynomial $g = x^6 + y^6 + 1$ has the decomposable Newton polytope $P_g = conv((0,0)(6,0)(0,6)) = conv((0,0),(3,0),(0,3)) +$

$conv((0,0),(3,0),(0,3))$ whereas $g = (x^3 + y^3 + 1)^2$ over $\mathbb{F}_2$, $g = (x^2 + y^2 + 1)^3$ over $\mathbb{F}_3$ and g is irreducible over $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{11}$, $\mathbb{F}_{13}$, $\mathbb{F}_{41}$, $\mathbb{F}_{103}$.

Our aim in this thesis is mainly to find integrally indecomposable integral polytopes in $\mathbb{R}^n$ and then, being associated to these polytopes, to determine infinite families of absolutely irreducible polynomials over any field F.

In Chapter 3, we study integral indecomposability of polygons on the real Euclidean space $\mathbb{R}^2$. We find new infinite families of absolutely irreducible bivariate polynomials over $F[x, y]$ for an arbitrary field F. We also find, in particular, a necessary and sufficient condition for integral indecomposability of arbitrary quadrangles.

In Chapter 4, we study integral indecomposability of polytopes. Using results on homothetic indecomposability, we find new infinite classes of integrally indecomposable polytopes in $\mathbb{R}^n$. More importantly, we also modify some interesting methods for constructing homothetically indecomposable polytopes so that we find new methods for constructing integrally indecomposable polytopes. Therefore, we find further new infinite classes of integrally indecomposable polytopes in $\mathbb{R}^n$. We also give different explanations of some of the main results in [G1] and [G2]. Throughout the thesis, we provide many examples illustrating our results.

In Chapter 5, we work on a conjecture of McGuire and Wilson given in [MW]. We provide solutions to some special cases of this conjecture over large characteristics.

Finally, in Chapter 6, we introduce a way of determining the probability of a polynomial to be irreducible by the polytope method in a family of polynomials over arbitrary fields.

Notation: For any integral element $v = (a_1, ..., a_n)$ of $\mathbb{R}^n$ we shall write $gcd(v)$ to mean $gcd(a_1, ..., a_n)$, i.e. the greatest common divisor of all the components of v. Similarly, for several vectors $v_1, ..., v_k$ in $\mathbb{R}^n$, by writing $gcd(v_1, ..., v_k)$ we mean the greatest common divisor of all the components of the vectors $v_1, ..., v_k$. For any points $v_1, v_2 \in \mathbb{R}^n$, $[v_1, v_2]$ refers to line segment from v_1 to v_2, $\overrightarrow{v_1v_2}$ stands for the vector from v_1 to v_2 and $\parallel v_1v_2 \parallel$ shows the Euclidean length of the line segment $[v_1, v_2]$. Naturally, for example $(v_1, v_2]$ stands for all the points on the closed line segment $[v_1, v_2]$ except for the point v_1. We note that $gcd(v_1, v_2) = gcd(v_1, v_2 - sv_1)$ for any integer s.

All mentioned regions in $\mathbb{R}^n$ in this thesis are assumed to be convex and compact.

Chapter 2

PRELIMINARIES

In this chapter, after briefly recalling some important properties of convex sets in $\mathbb{R}^n$, we shall explain how integral polytopes decomposes in terms of their faces. We need these possessions later to prove some significant characteristics of homothetically or integrally indecomposable polytopes.

2.1 SOME PROPERTIES OF CONVEX SETS

Let $\mathbb{R}^n$ denote the n-dimensional Euclidean space. The elements $x = (x_1, ..., x_n)$ of $\mathbb{R}^n$ are called *vectors* or *points*. We shall write

$$\|x\| = (x_1^2 + ... + x_n^2)^{1/2}$$

for the *Euclidean norm* or *length* of a vector x.

In $\mathbb{R}^n$, a vector equation of a line through the points a and b is given by

$$x = a + t(b - a) = (1 - t)a + tb, \qquad -\infty < t < \infty.$$

The closed directed line segment $[a, b]$ with direction from initial point a to terminal point b corresponds to values of $t \in [0, 1]$.

Now, we can give the following formal definition.

Definition 2.1.1 *Let x and y be arbitrary points in $\mathbb{R}^n$. The closed line segment from x to y is denoted by $[x, y]$ and is defined by*

$$[x, y] = \{a \in \mathbb{R}^n : a = (1 - \lambda)x + \lambda y, \quad 0 \leq \lambda \leq 1\},$$

or equivalently,

$$[x, y] = \{a \in \mathbb{R}^n : a = \alpha x + \beta y, \alpha \geq 0, \beta \geq 0, \alpha + \beta = 1\}.$$

The open line segment from x to y is denoted by (x, y) and is defined by

$$(x, y) = \{a \in \mathbb{R}^n : a = (1 - \lambda)x + \lambda y, \quad 0 < \lambda < 1\},$$

or equivalently,

$$(x, y) = \{a \in \mathbb{R}^n : a = \alpha x + \beta y, \alpha > 0, \beta > 0, \alpha + \beta = 1\}.$$

The half-open line segment $[x, y)$, including x but not y, is obtained by restricting λ to the half-open interval $0 \leq \lambda < 1$, or equivalently by restricting α and β to satisfy $\alpha > 0, \beta \geq 0, \alpha + \beta = 1$. Similarly, the half-open line segment $(x, y]$, which includes x but not y, is obtained for the values of λ on the half-open interval $0 < \lambda \leq 1$, or equivalently for the values of α, β satisfying $\alpha \geq 0, \beta > 0, \alpha + \beta = 1$.

A set $S \subseteq \mathbb{R}^n$ is said to be *convex*, if the line segment $[x, y]$ from x to y is contained in S for all $x, y \in S$. For example, a point, a line, an ellipse together with its interior points in $\mathbb{R}^2$, a sphere or an ellipsoid in $\mathbb{R}^3$ are convex regions. The empty set $\emptyset$ and the whole space $\mathbb{R}^n$ are also convex.

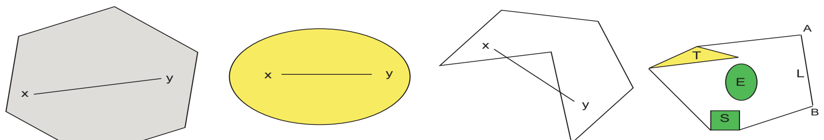
Proposition 2.1.2 *Let $\{C_i\}_{i \in I}$ be an arbitrary collection of convex sets in $\mathbb{R}^n$. Then, the set $\bigcap_{i \in I} C_i$ is convex.*

Proof: Let $x, y \in \bigcap_{i \in I} C_i$. Then, the line segment $[x, y]$ from x to y is contained in all sets $C_i, i \in I$ since they are convex. So, $[x, y]$ is also contained in $\bigcap_{i \in I} C_i$. □

For any set $S \subseteq \mathbb{R}^n$, the smallest convex set containing S, denoted by $conv(S)$ and called the *convex hull* of S, is the intersection of all convex sets that contain S, that is

$$conv(S) = \bigcap_{S \subseteq K_i, K_i \ convex} K_i.$$

When $S = \{a_1, ..., a_k\}$ is finite, we denote conv(S) by $conv(a_1, ..., a_k)$ and call it the convex hull of $a_1, ..., a_k$. Since the empty set is convex, $conv(\emptyset) = \emptyset$.



Convex Region Convex Region Nonconvex Region Conv(T USUE UL)
i s a convex 6-gon

Figure 0.1

Let $x, x_1, ..., x_k \in \mathbb{R}^n$. We say that x is a *convex combination* of $x_1, ..., x_k$ if there exist real numbers $\lambda_1, ..., \lambda_k$ such that

$$x = \lambda_1 x_1 + ... + \lambda_k x_k, \quad \lambda_1 + ... + \lambda_k = 1, \quad \lambda_1 \geq 0, ..., \lambda_k \geq 0.$$

As we see in Theorem 2.1.3, for any set $S \subseteq \mathbb{R}^n$, $conv(S)$ is equal to the set of all convex combinations of elements of S.

Theorem 2.1.3 *Let S be a subset of $\mathbb{R}^n$. Then,*

(1)

$$conv(S) = \left\{ \sum_{i=1}^{k} \lambda_i x_i : \{x_1, ..., x_k\} \subseteq S, \lambda_i \geq 0, \sum_{i=1}^{k} \lambda_i = 1 \right\}.$$

(2) S is convex if and only if $S = conv(S)$.

(3) if $S = \{a_1, ..., a_m\} \subseteq \mathbb{R}^n$ is finite,

$$conv(S) = \left\{ \lambda_1 x_1 + ... + \lambda_m x_m : \lambda_i \geq 0, \sum_{i=1}^{m} \lambda_i = 1 \right\}.$$

Proof: (1) Let us call the right-hand side of this equation as R. Firstly, we shall prove that R is convex. Let $x = \sum_{i=1}^{k} \lambda_i x_i$, $y = \sum_{i=1}^{m} \mu_i y_i \in R$ where $x_1, ..., x_k, y_1, ..., y_m \in S$ and $\lambda_1, ..., \lambda_k, \mu_1, ..., \mu_m \geq 0$ are real numbers with $\lambda_1 + ... + \lambda_k = \mu_1 + ... + \mu_m = 1$. Then, for any real number $0 \leq \lambda \leq 1$, we have

$$(1-\lambda)x + \lambda y = (1-\lambda) \sum_{i=1}^{k} \lambda_i x_i + \lambda \sum_{i=1}^{m} \mu_i y_i \in R$$

since

$$(1-\lambda)\lambda_1, ..., (1-\lambda)\lambda_k, \lambda\mu_1, ..., \lambda\mu_m \geq 0$$

and

$$(1-\lambda)(\lambda_1 + ... + \lambda_k) + \lambda(\mu_1 + ...\mu_m) = (1-\lambda) + \lambda = 1.$$

Now, by the definition of $conv(S)$, it is enough to prove the inclusion "$\supseteq$" of the given equality. Let K be a convex set such that $S \subseteq K$. We shall show that $R \subseteq K$. To see this, we shall use induction on k. For $k = 1$, $1x_1 \in S \subseteq K$ for all $x_1 \in S$. Let us assume the result for $k-1$. Then, for any finite set $\{x_1, ..., x_k\} \subseteq S$ and parameters $\lambda_1, ..., \lambda_k \geq 0$ with $\lambda_1 + ... + \lambda_k = 1$, the point $\lambda_1 x_1 + ... + \lambda_k x_k$ lies in K if $\lambda_k = 1$. And, for $\lambda_k < 1$,

$$\lambda_1 x_1 + ... + \lambda_k x_k = (1-\lambda_k) \left(\frac{\lambda_1}{1-\lambda_k} x_1 + ... + \frac{\lambda_{k-1}}{1-\lambda_k} x_{k-1} \right) + \lambda_k x_k \in K$$

since K is convex and the point $\frac{\lambda_1}{1-\lambda_k} x_1 + ... + \frac{\lambda_{k-1}}{1-\lambda_k} x_{k-1} \in K$ by the induction hypothesis while $\frac{\lambda_1}{1-\lambda_k} + ... + \frac{\lambda_{k-1}}{1-\lambda_k} = \frac{1-\lambda_k}{1-\lambda_k} = 1$ as $\lambda_1 + ... + \lambda_k = 1$.

(2) and (3) are obvious consequences of (1). $\Box$

The sum of two convex sets in $\mathbb{R}^n$ is defined as follows.

Definition 2.1.4 *For any two sets A, B in $\mathbb{R}^n$, the vector sum*

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

is called Minkowski sum of A and B.

We shall shortly recall some important properties of the Minkowski sum, mainly following the book [E].

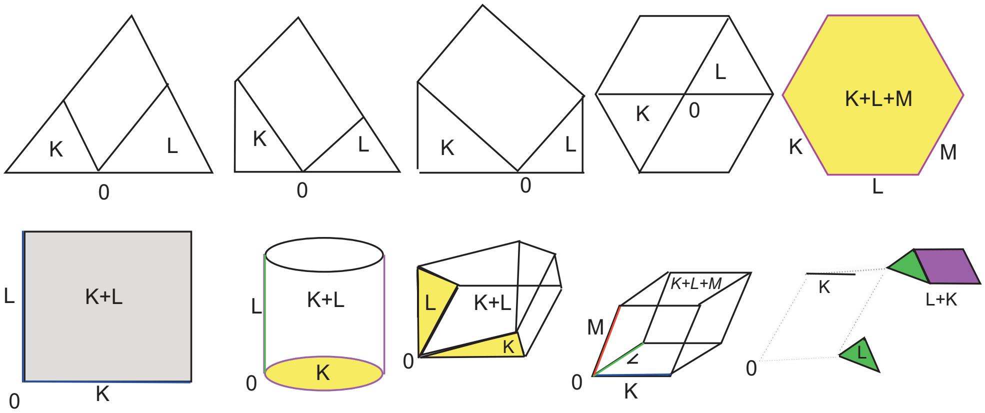


Figure 0.2

The sum of two triangles K, L in a plane is either a triangle, a quadrangle, a pentagon or a hexagon; and Minkowski addition may increase the dimension. Every centrally symmetric 2-dimensional 2n-gon can be written as a sum of n line segments. A regular hexagon in the plane can be written as the sum of two triangles and also as the sum of three line segments, see Figure 0.2. Thus, a representation of a convex compact set as a finite sum of indecomposable convex compact sets, if possible, is not unique.

Lemma 2.1.5 *(a) If τ denotes a translation then for any sets K, L in $\mathbb{R}^n$,*

$$\tau(K) + L = \tau(K + L) = K + \tau(L).$$

(b) If K, L are both convex, closed convex or compact convex sets in $\mathbb{R}^n$ then $K + L$ is convex, closed convex, or a compact convex set respectively.

Proof: (a) If τ is given by a translation vector t then the assertion follows from

$$(t + K) + L = t + (K + L) = K + (t + L).$$

(b) Let $a, a' \in K$ and $b, b' \in L$. Then for $0 \leq \lambda \leq 1$,

$$\lambda(a + b) + (1 - \lambda)(a' + b') = \lambda a + (1 - \lambda)a' + \lambda b + (1 - \lambda)b' \in K + L,$$

if K and L are convex. While K and L are closed and bounded, so is $K + L$ since addition is a continuous operation and maps pairs of bounded sets onto a bounded set. □

Remark 2.1.6 (1) We can rewrite the definition of Minkowski sum in the form

$$A + B = \bigcup_{b \in B} (A + b).$$

If $K \cap L \neq \emptyset$ then it can easily be shown that

$$K + L = K \cup \left(\bigcup_{p \in \partial K} (p + L) \right),$$

where ∂K is the boundary of K.

(2) If $\lambda \in \mathbb{R}$ and $K \subset \mathbb{R}^n$ is a set then the set $\lambda K = \{\lambda x : x \in K\}$ is called a multiple of K. If $\lambda_1, ..., \lambda_r \in \mathbb{R}$ and $K_1, ..., K_r$ are sets in $\mathbb{R}^n$, we call $\lambda_1 K_1 + ... + \lambda_r K_r$ a linear combination of $K_1, ..., K_r$. Here, λ may be negative. However, $(-1)K = -K$ is not the negative of K with respect to Minkowski addition. For the fourth case in Figure 0.2, $L = -K$, but $K + L = K + (-K)$ is a hexagon. For $m \in \mathbb{Z}^+$, and convex set K in $\mathbb{R}^n$, $mK = \underbrace{K + ... + K}_{m \ \ times}$.

(3) If $K_1, ...K_r$ are convex sets in $\mathbb{R}^n$ and $\lambda_1, ..., \lambda_r$ any real numbers, then $\lambda_1 K_1 + ... + \lambda_r K_r$ is convex. This can be proved by considering the convexity and using induction on r.

2.2 SUPPORTING HYPERPLANES AND FACES OF POLYTOPES

Let $C \subset \mathbb{R}^n$ be a compact convex set. Then for any nonzero vector $v \in \mathbb{R}^n$, we define the real number $sup_{x \in C} x \cdot v$ as the maximum of the set $\{x \cdot v : x \in C\}$ where

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

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

Definition 2.2.1 *(1) Let $K \subset \mathbb{R}^n$ be a nonempty convex compact set. The map*

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

is called the support function of K.
(2) For $\alpha \in \mathbb{R}, \beta \in \mathbb{R}^n$ the set

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

is a hyperplane. In a natural manner, the closed halfspaces formed by H are defined as

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

See Figure 0.3, (a).
(3) A hyperplane H_K is called a supporting hyperplane of a closed convex set $K \subset \mathbb{R}^n$ if $K \subset H_K^+$ or $K \subset H_K^-$ and $K \cap H_K \neq \emptyset$, i.e. H_K contains a

boundary point of K. A supporting hyperplane H_K to K is called nontrivial if K is not contained in H_K. We call H_K^- or H_K^+ a supporting halfspace of K, possibly $K \subset H_K$.

Example 2.2.2 *Let $n = 1, K = [-3, 2]$. Then we see that*

$$h_K(u) = \begin{cases} 2u & \textit{if } u \geq 0, \\ -3u & \textit{if } u \leq 0. \end{cases}$$

See Figure 0.3, (b).

Lemma 2.2.3 *(a) If $K + a$ is a translate of the compact convex set $K \subset \mathbb{R}^n$ then,*

$$h_{K+a} = h_K(u) + a \cdot u \quad \textit{for all } u \in \mathbb{R}^n.$$

(b) For every fixed nonzero vector $u \in \mathbb{R}^n$, the hyperplane

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

is a supporting hyperplane of K. See Figure 0.3, (c).

(c) Every supporting hyperplane of K has a representation of the form $(\star)$.

Proof: (a) We have $h_{K+a}(u) = sup_{x \in K+a}(x + a) \cdot u = sup_{x \in K}(x \cdot u + a \cdot u) = sup_{x \in K} x \cdot u + a \cdot u = h_K(u) + a \cdot u, \quad \forall u \in \mathbb{R}^n$.

(b) We see that continuity of the dot product function $f(x) = x \cdot u$ implies the continuity of the support function $h_K(u) = sup_{x \in K} x \cdot u$. Since K is compact, we must have some $x_0 \in K$ such that

$$h_K(u) = x_0 \cdot u.$$

Therefore, for any $a \in K$, we have $a \cdot u \leq x_0 \cdot u$, which means that $K \subset H_K^-(u)$ i.e. $H_K(u)$ is a supporting hyperplane of K.

(c) Let $H_K = \{x \in \mathbb{R}^n : x \cdot u = x_0 \cdot u\}$ be a supporting hyperplane of K at x_0. We can choose a nonzero vector $u \in \mathbb{R}^n$ satisfying $K \subset H_K^-$. Then, we have $h_K(u) = sup_{x \in K} x \cdot u = x_0 \cdot u$, which proves this case. See Figure 0.3, (c). $\square$

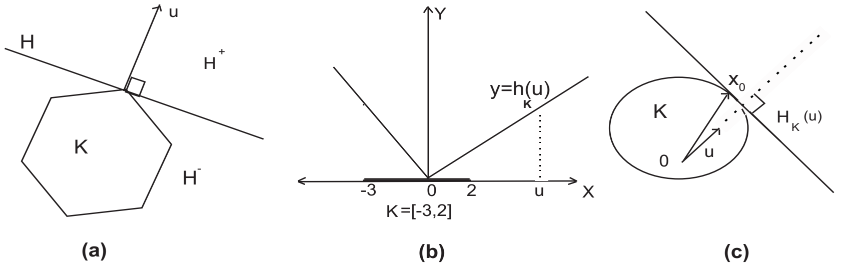


Figure 0.3

Let P be a polytope. The intersection of P with a supporting hyperplane H_P is called a *face* of P. A vertex is a face of dimension zero. An *edge* of P is a face of dimension 1, which is a line segment. A face F of P is called a *facet* if dim (F)= dim (P) -1.

The following theorem explains the most important properties about the decomposition of polytopes. As we see, Minkowski sum keeps the additivity of the support function.

Theorem 2.2.4 *(a) If h_K, h_L are the support functions of the convex sets K, L in $\mathbb{R}^n$ respectively, then, $h_K + h_L$ is the support function of $K + L$, i.e.*

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

(b) $H_{K+L} = H_K + H_L$.

(c) If F is a face of $K + L$, then there exist unique faces F_K, F_L of K, L respectively such that

$$F = F_K + F_L.$$

In particular, each vertex of $K+L$ is the sum of vertices of K, L respectively.

(d) If K, L are polytopes then so is $K+L$.

(e) If A is a polytope in $\mathbb{R}^n$ with $A = B + C$ then so are B and C (which are called summands of A).

Proof: (a) $h_{K+L}(u) = sup_{x \in K, y \in L}(x+y) \cdot u = sup_{x \in K} x \cdot u + sup_{y \in L} y \cdot u = h_K(u) + h_L(u)$ for any $u \in \mathbb{R}^n \setminus \{0\}$.

(b) This is an immediate consequence of (a), or Lemma 2.2.3.

(c) For any compact convex set C and a vector u pointing away from C, according to Lemma 2.2.3, let $H_C(u)$ be a supporting hyperplane of C. Then $F = (K+L) \cap H_{K+L}(u)$. We set $F_K = K \cap H_K(u)$, $F_L = L \cap H_L(u)$. Then $H_K(u), H_L(u), H_{K+L}(u)$ are parallel hyperplanes, and $H_{K+L}(u) = H_K(u) + H_L(u)$. Up to a translation of L, we may assume $H_K(u) = H_L(u)$. Then, we obtain

$$\begin{aligned} F = (K+L) \cap H_{K+L}(u) &= (K+L) \cap (H_K(u) + H_L(u)) \\ &= (K \cap H_K(u)) + (L \cap H_L(u)) = F_K + F_L. \end{aligned}$$

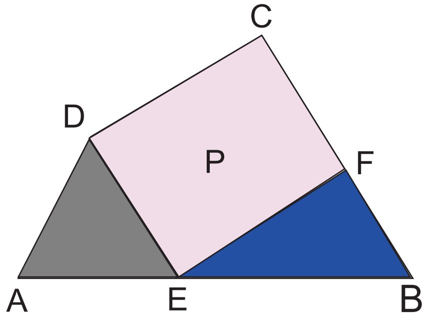
Uniqueness of F_K and F_L follows from (a).

(d) This case is a consequence of (c) since the sum of two vertices is a vertex and each vertex of $K+L$ is obtained in this way.

(e) Every summand of a polytope is also a polytope. Because, every polytope is formed by the fact that its supporting function is piecewise linear. □

An important consequence of Theorem 2.2.4,(a) is that if we have $A+C = B+C$ for compact convex sets $A, B, C \subset \mathbb{R}^n$ then $A = B$. Therefore, $(\mathbb{R}^n, +)$ is a commutative semigroup with cancellation law.

We also note that converse of Theorem 2.2.4,(c) is not true. That is, if F_1 and F_2 are faces of K and L respectively then $F_1 + F_2$ is not necessarily a face of $K+L$. To see this, consider a quadrangle which can be written as a sum of two triangles. In Figure 0.4, the quadrangle $Q = conv(A, B, C, D)$ is equal to sum of two triangles. But, as we see in this figure the parallelogram $P = conv(E, F, C, D)$, which is not a face of Q, is equal to sum of two line segments $[E, D]$ and $[E, F]$.



Q=conv(A,B,C,D)=conv(A,E,D)+conv(E,B,F)

P=conv(E,F,C,D)=conv(E,D)+conv(E,F)

Figure 0.4

A polytope of dimension two is called a *polygon*. A polygon has the only proper faces as its vertices and edges. We can give the following result, which is given in [G2], of the above theorem for polygons.

Corollary 2.2.5 *Let A, B and C be convex polygons in $\mathbb{R}^n$ with $C = A + B$. Then every edge of C can be decomposed uniquely as the sum of an edge of A and an edge of B, possibly one of them may be a point. Conversely, any edge of A or B is a summand of precisely one edge of C.*

Chapter 3

INTEGRALLY INDECOMPOSABLE POLYGONS

In this chapter, we shall determine some integrally indecomposable polygons. Then we shall give examples of absolutely irreducible polynomials associated to these polygons over arbitrary fields.

Recall that a polytope of dimension two is called a *polygon*.

For a convex polygon P in the Euclidean plane $\mathbb{R}^2$, we may construct a finite sequence of vectors associated with its edges as follows. Let $v_0, v_1, ..., v_{n-1}$, $v_n = v_0$ be the vertices of the polygon ordered in counterclockwise direction. We may represent the edges of P by the vectors $E_i = v_i - v_{i-1} = (a_i, b_i)$ for $1 \leq i \leq n$, where $a_i, b_i \in \mathbb{Z}$ and the indices are taken modulo n. We call each E_i an *edge vector.* A vector $v = (x, y) \in \mathbb{Z}^2$ is called a *primitive vector* if $gcd(x, y) = 1$. Letting $c_i = gcd(a_i, b_i)$ and defining $e_i = (a_i/c_i, b_i/c_i)$, we have $E_i = c_i e_i$ where e_i is a primitive vector for $1 \leq i \leq n$. Each edge E_i contains exactly $c_i + 1$ integral points including its end points. The sequence of vectors

$\{c_ie_i\}_{1\leq i\leq n}$, called the *edge sequence* or *polygonal sequence,* uniquely indicates the polygon up to translation determined by v_0. Since we can insert an arbitrary number of zero vectors to any edge sequence, we may assume that the edge sequence of a summand of a polygon P has the same number of terms as the edge sequence of P. While the boundary of a polygon is a closed path, we have $\sum_{i=1}^{n} c_ie_i = (0,0)$.

Lemma 3.0.6 *Let P be an integral polygon having the edge sequence $\{c_ie_i\}_{1\leq i\leq n}$ where $e_i \in \mathbb{Z}^2$ are primitive vectors. Then, an integral polytope Q is a summand of P if and only if it has the edge sequence of the form $\{d_ie_i\}_{1\leq i\leq n}$, $0 \leq d_i \leq c_i$, where $\sum_{i=1}^{n} d_ie_i = (0,0)$.*

Proof: See, e.g., the proof of [G2, Lemma 13] or [L, Lemma 2.11]. □

Remark 3.0.7 According to Lemma 3.0.6, any integral polygon having two parallel edges, say $e_i = -e_j$, is integrally decomposable since $e_i + e_j = 0$. Therefore, from now on we assume that the mentioned polygons in Section 3 are integral and they have no parallel edges. And, we call an integral summand of a polygon as *trivial summand* if it is a line segment or an integral point.

By Lemma 3.0.6, we also observe that any integral n-gon, $n \geq 3$, having no parallel edges may only have integral summands having i edges with $i \in \{3, 4, ..., n-1, n\}$. For example, any integral pentagon without parallel edges may have only triangular, quadrangular or pentagonal integral summands. Moreover, we observe that any edge of a summand S of a polygon P may occur only a summand of a unique edge of P.

In this chapter, we get some new integral indecomposability criteria for the polygons on the 2-dimensional real Euclidean space $\mathbb{R}^2$. Our results on integral indecomposability about n-gons, for $n \geq 4$, and especially for quadrangles are important. However, for the sake of completeness, we begin from line segments.

We begin with the simplest case on the plane. We shall give direct proofs to determine the integrally indecomposable line segments and triangles.

3.1 LINE SEGMENTS

For any two distinct points a_1 and a_2 in $\mathbb{R}^n$, the line segment $[a_1, a_2]$ from a_1 to a_2 is the set of all points of the form

$$a = a_1 + \lambda(a_2 - a_1), \qquad 0 \leq \lambda \leq 1.$$

We should note that for distinct points $v_1, v_2, a_1, a_2, b_1, b_2$ in $\mathbb{R}^n$ such that $v_1 = a_1 + b_1$ and $v_2 = a_2 + b_2$ we have $[v_1, v_2] \subseteq [a_1, a_2] + [b_1, b_2]$. And, if $[v_1, v_2] = [a_1, a_2] + [b_1, b_2]$, then three line segments $[v_1, v_2]$, $[a_1, a_2]$ and $[b_1, b_2]$ are parallel since

$$[v_1, v_2] = \bigcup_{b \in [b_1, b_2]} ([a_1, a_2] + b) = \bigcup_{a \in [a_1, a_2]} (a + [b_1, b_2]).$$

One can find the number of integral points on any line segment by using the following proposition. Note that [G1, Lemma 4.1] has a similar statement, and here we give a different proof.

Proposition 3.1.1 *Let a_1 and a_2 be two distinct integral points in $\mathbb{R}^n$. Then the number of integral points on the line segment $[a_1, a_2]$, together with a_1 and a_2, is equal to $gcd(a_2 - a_1) + 1$. Moreover, if a_3 is any integral point on the open line segment (a_1, a_2), such that $a_3 = \alpha a_1 + \beta a_2$ with $\alpha > 0$, $\beta > 0$ and $\alpha + \beta = 1$ then*

$$\frac{gcd(a_3 - a_1)}{gcd(a_3 - a_2)} = \frac{\| a_3 - a_1 \|}{\| a_3 - a_2 \|} = \frac{\beta}{\alpha}.$$

Proof: Let a_3 be a point on the open line segment (a_1, a_2). Then $a_3 = \alpha a_1 + \beta a_2$ where $\alpha > 0$, $\beta > 0$ and $\alpha + \beta = 1$. So, we have

$$a_3 - a_1 = (1-\beta)a_1 + \beta a_2 - a_1 = \beta(a_2 - a_1)$$

and

$$a_3 - a_2 = \alpha a_1 + (1-\alpha)a_2 - a_2 = \alpha(a_1 - a_2)$$

with $0 < \alpha, \beta < 1$. Consequently, we have

$$\frac{\parallel a_3 - a_1 \parallel}{\parallel a_3 - a_2 \parallel} = \frac{\beta}{\alpha}.$$

As we see, the last equality is true for any point $a_3 \in (a_1, a_2)$, which may not be integral.

From the equality $a_3 - a_1 = \beta(a_2 - a_1)$, we see that a_3 is integral if and only if $\beta(a_2 - a_1)$ is integral. Let a_3 be integral. Since the vector $a_2 - a_1$ has integer components and $a_3 \neq a_1, a_2$, β must be a rational number of the form

$$\beta = m/n \quad \text{for some} \quad 0 < m < n \quad \text{with} \quad gcd(m, n) = 1.$$

We see that $\beta(a_2 - a_1)$ is integral if and only if n divides $d = gcd(a_2 - a_1)$. Therefore, to have a_3 integral, we must have

$$\beta = m/d \quad \text{with} \quad 0 < m < d.$$

As it is seen, we have $d-1$ choices for m. Consequently, the number of integral points on $[a_1, a_2]$ is $(d-1) + 2 = d + 1$.

We have

$$a_3 - a_1 = \beta(a_2 - a_1) = \frac{m}{d} dv'$$

and

$$a_3 - a_2 = \alpha(a_1 - a_2) = \frac{d-m}{d}(-dv')$$

for some primitive vector v', i.e. gcd of all the components of v' is 1. Since v' is primitive, we must have $gcd(a_3 - a_1) = m$ and $gcd(a_3 - a_2) = d - m$. As a result, we have

$$\frac{gcd(a_3 - a_1)}{gcd(a_3 - a_2)} = \frac{m}{d - m} = \frac{\beta}{\alpha},$$

which completes the proof. □

Corollary 3.1.2 *A line segment from an integral point a_1 to another integral point a_2 in $\mathbb{R}^n$ is integrally indecomposable if and only if $gcd(a_2 - a_1) = 1$.*

Proof: If $gcd(a_2 - a_1) = d > 1$ then the line segment $[a_1, a_2]$ has an integral point $c \neq a_1, a_2$ on it. So, we have

$$[a_1, a_2] = [a_1, c] + [0, a_2 - c].$$

Conversely, suppose that $gcd(a_2 - a_1) = 1$, but $[a_1, a_2] = [b_1, b_2] + [c_1, c_2]$ for some integral line segments on the plane with $\parallel b_1 b_2 \parallel, \parallel c_1 c_2 \parallel > 0$. From the remark in the first paragraph of this subsection, the line segments $[a_1, a_2]$, $[b_1, b_2]$ and $[c_1, c_2]$ are parallel. This is a contradiction since the line segment $[a_1, a_2]$ is primitive. □

Example 3.1.3 [O2, Theorem IX] A two-term polynomial

$$ax_1^{i_1} \cdots x_k^{i_k} + bx_{k+1}^{i_{k+1}} \cdots x_n^{i_n} \in F[x_1, ..., x_n], \quad a, b \in F \setminus \{0\},$$

is absolutely irreducible over F if and only if $gcd(i_1, ..., i_n) = 1$.

For example, $f = x^n + y^m$ is absolutely irreducible over any field F if and only if $gcd(n, m) = 1$. Similarly, the polynomial $g = x^i y^j + z^k$ is absolutely irreducible over F if and only if $gcd(i, j, k) = 1$. Of course, these polynomials remain absolutely irreducible when we add any new terms whose exponent vectors lie in the Newton polytopes of them.

3.2 TRIANGLES

In order to decompose an integral triangle $conv(v_1, v_2, v_3)$ in $\mathbb{R}^n$, we must have $gcd(v_1 - v_2, v_1 - v_3) = d > 1$, which implies that we also have

$$gcd(v_1 - v_2, v_1 - v_3) = gcd(v_2 - v_1, v_2 - v_3) = gcd(v_3 - v_1, v_3 - v_2) = d.$$

For example, we have

$$conv((1,2),(7,4),(5,8)) = conv((1,2),(4,3)(3,5)) + conv((0,0)(3,1)(2,3)).$$

Let $T = conv(v_1, v_2, v_3)$ be an integral triangle in $\mathbb{R}^n$. We can form edge vectors of T as $E_1 = c_1e_1 = v_2 - v_1$, $E_2 = c_2e_2 = v_3 - v_2$ and $E_3 = c_3e_3 = v_1 - v_3$ where $c_1 = gcd(v_2 - v_1)$, $c_2 = gcd(v_3 - v_2)$, $c_3 = gcd(v_1 - v_3)$ are positive integers and e_1, e_2, e_3 are primitive edge vectors of T. Since T has no parallel edges, by Remark 3.0.7, all convex integral summands of T must be triangular and any convex integral summand S of T must have edges of the form $E'_1 = d_1e_1$, $E'_2 = d_2e_2$, $E'_3 = d_3e_3)$ where d_i are integers with $0 \leq d_i \leq c_i$ for $i = 1, 2, 3$ and $E'_1 + E'_2 + E'_3 = 0$. Therefore, any integral summand S of T must be a triangle having edges as pieces of edges of T and similar to itself. Hence, we have

$$\frac{\parallel E'_1 \parallel}{\parallel E_1 \parallel} = \frac{\parallel E'_2 \parallel}{\parallel E_2 \parallel} = \frac{\parallel E'_3 \parallel}{\parallel E_3 \parallel} = \frac{d_1}{c_1} = \frac{d_2}{c_2} = \frac{d_3}{c_3} = k = \frac{m}{n}$$

where $0 \leq k \leq 1$ is a rational number with $gcd(m, n) = 1$ and $0 \leq m \leq n$. Since d_i for $i = 1, 2, 3$ are integers, we see that n must divide c_j for $j = 1, 2, 3$.

Assume that $gcd(v_1 - v_2, v_1 - v_3) = 1$. Since we have $gcd(v_1 - v_2, v_1 - v_3) = gcd(gcd(v_1 - v_2), gcd(v_1 - v_3)) = gcd(c_1, c_3) = 1$, we see that $n = 1$. So, $m = 0$ or $m = 1$. Consequently, $S = \{0\}$ or $S = T$.

Assume that $gcd(v_1 - v_2, v_1 - v_3) = gcd(c_1, c_3) = d > 1$. Then, the polytope $T' = conv(0, v_2 - v_1, v_3 - v_1)$ is integral. Hence, $T = v_1 + d \cdot (\frac{1}{d}T')$.

As a result, we have proved the following proposition.

Proposition 3.2.1 *A triangle $conv(v_1, v_2, v_3)$ in $\mathbb{R}^n$ is integrally indecomposable if and only if*

$$gcd(v_1 - v_2, v_1 - v_3) = 1.$$

By Proposition 3.2.1, we see that a triangle in $\mathbb{R}^n$ with integral vertices v_1, v_2, v_3 is integrally indecomposable if

$$gcd(v_i - v_j) = 1 \quad \text{for some} \quad i, j \in \{1, 2, 3\}.$$

For example, the polynomial

$$f = a_1x^{13} + a_2y^9 + a_3x^2y + a_4x^4y^4 + a_5x^5y^3 + a_6x^6y^2 + a_7x^3y^4 + \sum c_{ij}x^iy^j,$$

with $a_1, ..., a_7 \in F \setminus \{0\}$ and $(i, j) \in P_f = conv((13, 0)(0, 9)(2, 1))$, is absolutely irreducible over any field F since P_f is an integrally indecomposable triangle as $gcd(13, 9) = 1$.

3.3 QUADRANGLES

In this subsection, we give a necessary and sufficient condition on the integral decomposability of integral quadrangles.

By Remark 3.0.7, any integral quadrangle Q having two parallel edges is integrally decomposable. First, we observe that any quadrangle Q without parallel edges must lie inside exactly two kinds of triangles having precisely one common edge with Q. For a quadrangle Q lying in a triangle T as in Figure 1, we call the common edges of Q and T a *base edge* of Q. So, any quadrangle Q has exactly two base edges. We also observe that base edges of Q are adjacent. Therefore, in this subsection we refer to an arbitrary quadrangle $Q = conv(A, B, C, D)$ lying inside the triangles $T_1 = conv(A, B, v_1)$ and

$T_2 = conv(B, C, v_2)$ for some points $v_1, v_2 \in \mathbb{R}^2$. See Figure 1.

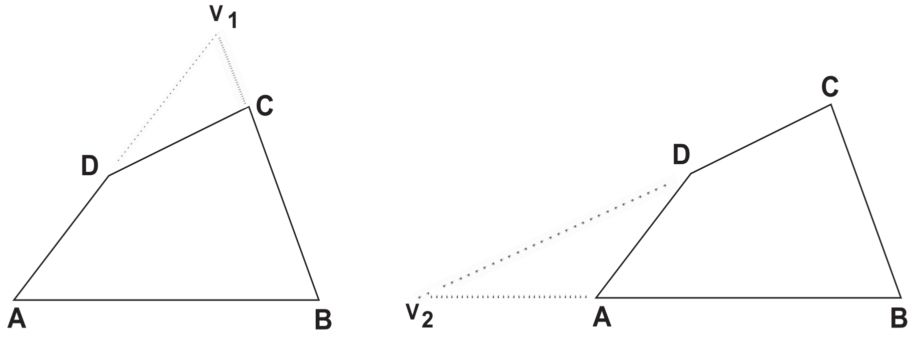


Figure 1

We fix how to indicate the corners of a quadrangle Q. In the counterclockwise direction, if Q lies inside the triangles $T_1 = conv(A, B, v_1)$ and $T_2 = conv(B, C, v_2)$ with $[A, B]$ and $[B, C]$ being the base edges of Q, then we indicate the vertices of Q as $Q = conv(A, B, C, D)$. Therefore, $[A, B]$ is the first and $[B, C]$ is the second base edge of Q in the counterclockwise direction. Moreover, without loss of generality we assume that our quadrangle is shaped as in Figure 2, (i). See Figure 2 to observe how we indicate the vertices of an arbitrary quadrangle with respect to its base edges.

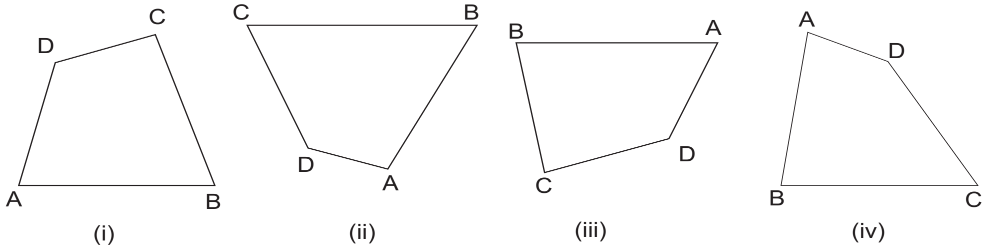
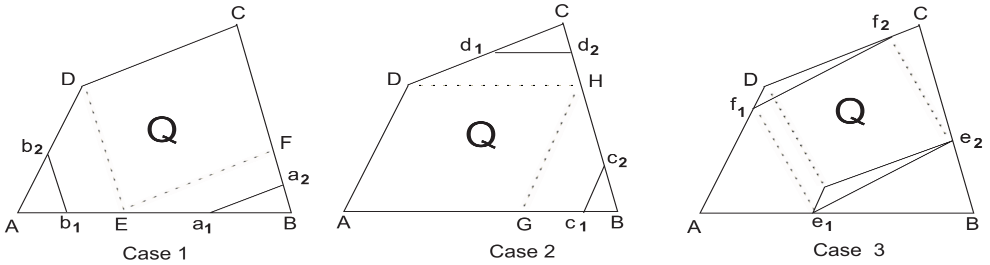


Figure 2



Case 1

Case 2

Case 3

Decomposition methods of integral quadrangles

Figure 3

First we form the parallelograms $CDEF$ and $AGHD$ on Q as shown in Figure 3, Case 1 and Case 2 respectively. Note that the points E, F, G and H are not necessarily integral. By Lemma 3.0.6, any nontrivial summand of Q may only be a triangle or a quadrangle. We list all possible conditions which can give a nontrivial integral triangular or quadrangular summand of Q :

(C1) There exist integral points $a_1 \in (B, E]$ and $a_2 \in (B, F]$ such that $[a_1, a_2]$ is parallel to $[D, C]$. See Figure 3, Case 1.

(C2) There exist integral points $b_1 \in (A, E]$ and $b_2 \in (A, D]$ such that $[b_1, b_2]$ is parallel to $[B, C]$. See Figure 3, Case 1.

(C3) There exist integral points $c_1 \in (B, G]$ and $c_2 \in (B, H]$ such that $[c_1, c_2]$ is parallel to $[A, D]$. See Figure 3, Case 2.

(C4) There exist integral points $d_1 \in (C, D]$ and $d_2 \in (C, H]$ such that $[d_1, d_2]$ is parallel to $[A, B]$. See Figure 3, Case 2.

(C5) There exist integral points $e_1 \in (A, B)$, $e_2 \in (B, C)$, $f_1 \in (D, A)$ and $f_2 \in (C, D)$ such that $[e_1, e_2]$ is parallel to $[f_1, f_2]$ and $\|e_1 e_2\| = \|f_1 f_2\|$. See Figure 3, Case 3.

The conditions (C1), (C2), (C3) and (C4) above corresponds to possible nontrivial integral triangular summands and the condition (C5) corresponds to possible nontrivial integral quadrangular summand of Q. We observe that $(C1) \Longleftrightarrow (C4)$ and $(C2) \Longleftrightarrow (C3)$.

Now, we give our theorem on quadrangles.

Theorem 3.3.1 *The quadrangle $Q = conv(A, B, C, D)$ in Figure 3 is integrally indecomposable if and only if the conditions (C1), (C2) and (C5) do not hold.*

Proof: Let $E_1 = B - A$, $E_2 = C - B$, $E_3 = D - C$ and $E_4 = A - D$ be the edge vectors of Q. Assume first that a nontrivial integral summand of Q is triangular. Then either condition (C1) or condition (C2) holds. Indeed by Lemma 3.0.6, any edge of a nontrivial integral triangular summand of Q must be a summand of only one of the edges E_1, E_2, E_3 or E_4. From Figure 3, it is clear that the edges of a triangular summand can only be formed by the edge groups

(a) $\{E_1, E_2, E_3\}$,

(b) $\{E_1, E_2, E_4\}$,

(c) $\{E_2, E_3, E_4\}$,

(d) $\{E_3, E_4, E_1\}$.

The cases (a) and (b) are covered by conditions (C1) and (C2) respectively. It is also clear from Figure 3 that the cases (c) and (d) cannot give a triangular summand because of the directions of the corresponding edges of Q.

Next we assume that a nontrivial integral summand S of Q is quadrangular such that $Q = S + T$, where T is a nontrivial quadrangular summand. Then the condition (C5) holds. More precisely, by Lemma 3.0.6, a nontrivial integral quadrangular summand S must be formed by the edges which are summand of the edges of Q. Let us assume that S has the edge vectors F_1, F_2, F_3 and F_4 which are nontrivial summands of the edges E_1, E_2, E_3 and E_4 respectively. Let $e_1 = B - F_1$, $e_2 = B + F_2$, $f_1 = D + F_4$ and $f_2 = D - F_3$ be the integral points on the edges of Q. Then

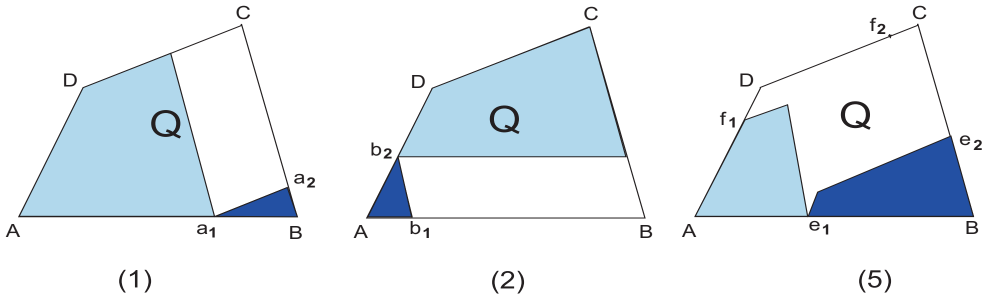
$$\overrightarrow{e_1e_2} = \overrightarrow{e_1B} + \overrightarrow{Be_2} = (B - (B - F_1)) + ((B + F_2) - B) = F_1 + F_2,$$

and

$$\overrightarrow{f_1f_2} = \overrightarrow{f_1D} + \overrightarrow{Df_2} = (D - (D + F_4)) + ((D - F_3) - D) = -(F_3 + F_4).$$

Since S has a closed boundary, we have $F_1 + F_2 + F_3 + F_4 = 0$ and hence $\overrightarrow{e_1e_2} = \overrightarrow{f_1f_2}$. In particular, $[e_1, e_2]$ is parallel to $[f_1, f_2]$ and $\|e_1e_2\| = \|f_1f_2\|$.

Conversely, we show in Figure 4 how we can decompose Q if either of the conditions (C1), (C2) or (C5) is satisfied. □



Decomposition methods for integral quadrangles

Figure 4

By [G1, Corollary 4.12], it is implied that the integral quadrangle Q is integrally indecomposable if $gcd(A-B)=1$ or $gcd(B-C)=1$. This is just a very special case of Theorem 3.3.1.

Note that, in order to apply Theorem 3.3.1 for decomposing Q whenever it is possible, obeying the rules of decomposition of polygons and considering the lengths of the edges $[C,D]$ and $[A,D]$, it is not necessary to find the points E, F, G and H on Q. That is, for example one can easily find the points a_1 and a_2 in Figure 3 using the slope of the line segment $[C,D]$ and the fact that $a_1 \in [A,B]$, $a_2 \in [B,C]$. Alternatively, we can first constitute the primitive edge vectors $v_1 = (p_1, p_2)$, $v_2 = (q_1, q_2)$ for the directed line segments $[B,A]$ and $[B,C]$ respectively. Then we can find the smallest positive integers m, n such that $((u_1,u_2)+mv_1)-((u_1,u_2)+nv_2) = mv_1 - nv_2$ has the same slope as the edge $[C,D]$, where (u_1,u_2) is the position vector for the vertex B. Here, of course, we must take care of the length of $[a_1,a_2]$, i.e. $\|a_1a_2\|$ must be less than or equal to $\|CD\|$.

For instance, consider the quadrangle $Q = conv(A,B,C,D)$ where $A = (0,3)$, $B=(6,0)$, $C=(14,4)$, $D=(6,4)$. By using the same terminology above, we have $v_1 = (-2,1)$ and $v_2 = (2,1)$. And, the vector $m(-2,1)-n(2,1)$ has slope zero if $m=n$. So, taking $m=n=1$ we get the points $a_1 = (6,0)+1\cdot(-2,1) = (4,1)$ and $a_2 = (6,0)+1\cdot(2,1) = (8,1)$ on the line segments (B,A) and (B,C) respectively. In this case, we have

$$Q = conv((0,2),(4,0),(6,3),(10,3)) + conv((0,1),(2,0),(4,1)).$$

If we take $m=n=2$, then we can decompose Q as

$$Q = conv((0,1),(2,0),(6,2)) + conv((0,2),(4,0),(8,2)).$$

As a consequence of Theorem 3.3.1, using the same terminology of the theorem, we obtain the following result.

Corollary 3.3.2 *The quadrangle $Q = conv(A, B, C, D)$ is integrally indecomposable if one of the following cases holds:*

(a) *E_3 is primitive and the line segment $(A, E]$ does not contain an integral point.*

(b) *E_3 is primitive, the point E is not integral and the line segment (D, A) does not contain an integral point.*

(c) *E_4 is primitive and the line segment $[E, B)$ does not contain an integral point.*

(d) *E_4 is primitive and the line segment $(B, F]$ does not contain an integral point.*

(e) *E_3 and E_4 are primitive and the point E (or F) is not integral.*

(f) *E_1 or E_2 is primitive.*

Proof: Consider case (a). As E_3 is primitive, if S is a nontrivial integral quadrangular summand of Q with $Q = S + T$ then T must be nontrivial integral triangular summand of Q. Hence, either condition (C1) or condition (C2) holds. However, while E_3 is primitive and E is not an integral point, condition (C1) does not hold. Moreover, as $(A, E]$ does not contain an integral point, condition (C2) does not hold either. This completes the proof of case (a). We prove the other cases similarly. □

Remark 3.3.3 Theorem 3.3.1 gives a necessary and sufficient condition for integral indecomposability of quadrangles. Note that only the case (f) in Corollary 3.3.2 is covered by [G1, Corollary 4.12] as a result about quadrangles.

Now, we consider some special cases of Theorem 3.3.1 and find new integrally indecomposable quadrangles. Note that the corresponding absolutely irreducible polynomials of the given quadrangles in Proposition 3.3.4, Proposition 3.3.5 and Proposition 3.3.6 were, in general, not covered in [G1, G2].

If the indecomposable regions that we shall describe have one primitive edge, e_j say, lie in a triangle having one edge as e_j then of course they are integrally indecomposable by [G1, Corollary 4.12]. But, the others give new integrally indecomposable polygons on the real plane $\mathbb{R}^2$.

The following three propositions are computational consequences of Lemma 3.0.6. Hence, we do not give their proofs in detail. Note that in these propositions, the conditions for indecomposability of quadrangles in the corresponding cases are reduced drastically compared to applying Lemma 3.0.6 directly.

Proposition 3.3.4 *Let m, n, k be positive integers and Q an integral quadrangle having the edge sequence $\{me_1, ne_2, ke_3, e_4\}$. Then Q is integrally indecomposable if and only if*

$$c_1e_1 + c_2e_2 + c_3e_3 \neq 0, \quad 1 \leq c_1 \leq m, \quad 1 \leq c_2 \leq n, \quad 1 \leq c_3 \leq k,$$

and

$$d_1e_1+d_2e_2+d_3e_3+e_4 \neq 0, \quad 0 \leq d_1 \leq m-1, \quad 0 \leq d_2 \leq n-1, \quad 0 \leq d_3 \leq k-1.$$

As an example of Proposition 3.3.4, any integral quadrangle Q with the edge sequence $\{3e_1, 2e_2, 2e_3, e_4\}$ is integrally indecomposable if and only if $e_1 + e_2 + e_4 \neq 0$, $e_1 + e_3 + e_4 \neq 0$, $e_1 + e_2 + 2e_3 \neq 0$, $e_1 + 2e_2 + e_3 \neq 0$. Since Q is convex, the last three conditions are already satisfied. Hence, Q is integrally indecomposable if and only if $e_1 + e_2 + e_4 \neq 0$.

For example, the quadrangle $Q = conv((6,0),(14,4),(4,20),(0,3))$ having the edge sequence $\{3(2,-1), 4(2,1), 2(-5,8), (-4,-13)\}$ is integrally indecomposable. Actually, Q is integrally indecomposable since it lies in a triangle $conv((0,3),(4,20),v)$ for some point in $v \in \mathbb{R}^2$. So, it is better to find another example for which [G1, Corollary 4.12] does not work. We consider the quadrangle

$$Q' = conv((6,0),(14,4),(2,6),(0,3))$$

with the edge sequence $\{3(2,-1), 4(2,1), 2(-6,1), (-2,-3)\}$. Q' is integrally indecomposable since $(2,-1)+(2,1)+(-2,-3) \neq 0$. Consequently, every polynomial

$$f = a_1x^6 + a_2y^3 + a_3x^{14}y^4 + a_4x^2y^6 + \sum c_{ij}x^iy^j,$$

with $(i,j) \in Q'$ and $a_i \neq 0$, is absolutely irreducible over any field F.

Proposition 3.3.5 *Let m, n be positive integers and Q an integral quadrangle having the edge sequence $\{me_1, ne_2, e_3, e_4\}$. Consider the integral pairs (i,j) satisfying $1 \leq i \leq m-1$, $1 \leq j \leq n-1$ (if n divides m and d divides n, omit the pairs (md/n, d)). Then Q is integrally indecomposable if and only if $ie_1 + je_2 + e_3 \neq 0$ with (i,j) as described.*

For example, by Proposition 3.3.5, we easily see that a convex integral quadrangle Q with the edge sequence $\{3e_1, 2e_2, e_3, e_4\}$ is integrally indecomposable if and only if $2e_1 + e_2 + e_3 \neq 0$, equivalently $e_1 + e_2 + e_4 \neq 0$. Also, a convex integral quadrangle having the edge sequence $\{4e_1, 2e_2, e_3, e_4\}$ is integrally indecomposable if and only if $3e_1 + e_2 + e_3 \neq 0$.

Proposition 3.3.6 *Let m be a positive integer and Q an integral quadrangle having the edge sequence $\{me_1, me_2, e_3, e_4\}$. Consider the integral pairs (i,j)*

satisfying $1 \leq i, j \leq m-1$ *except for the pairs* (i,i). *Then,* Q *is integrally indecomposable if and only if* $ie_1 + je_2 + e_3 \neq 0$ *with* (i,j) *as described.*

Proof: Only if part is clear from Lemma 3.0.6.

Conversely, any integral summand of Q must be of the form $c_1e_1 + c_2e_2 + c_3e_3 + c_4e_4 = 0$ where $3 \leq \sum_{i=1}^{4} c_i \leq 2m+1$, $0 \leq c_1, c_2 \leq 3$ and $0 \leq c_3, c_4 \leq 1$. Since Q has no parallel edges, we have only two cases for the value of the pair (c_3, c_4) as $(1,0)$ or $(0,1)$. So, we have two cases to examine:

$$(1) \quad ie_1 + je_2 + e_3 = 0 \quad \text{with} \quad 1 \leq i \leq m-1, \quad 1 \leq j \leq m-1, \quad i \neq j,$$

$$(2) \quad ie_1 + je_2 + e_4 = 0 \quad \text{with} \quad 1 \leq i \leq m-1, \quad 1 \leq j \leq m-1, \quad i \neq j.$$

By using the fact that $me_1 + me_2 + e_3 + e_4 = 0$, we observe that while counting case (1), we also count the case (2). So, it is enough to study the case (1). Consequently, we see that we are examining all possible summands of Q. We can omit the cases with $i = j$. Because, if $ie_1 + ie_2 + e_3 = 0$ then $mie_1 + mie_2 + me_3 = i(me_1 + me_2) + me_3 = i(-e_3 - e_4) + me_3 = (m-i)e_3 + -ie_4 = 0$ which is a contradiction since Q has no parallel edges. As a result, if all possible summands in case (1) are not zero then Q is integrally indecomposable. □

As an application of Proposition 3.3.6, we easily get the result of Proposition 3.3.5 for $m = n = 3$. Because, the quadrangle Q with edge sequence

$$\{3e_1, 3e_2, e_3, e_4\}$$

is integrally indecomposable if and only if
$e_1 + 2e_2 + e_3 \neq 0$ and $2e_1 + e_2 + e_3 \neq 0$. As Q is convex, it is integrally indecomposable if and only if $2e_1 + e_2 + e_3 \neq 0$.

As a second example of Proposition 3.3.6, an integral quadrangle Q with edge sequence

$$\{4e_1, 4e_2, e_3, e_4\}$$

is integrally indecomposable if and only if $e_1 + 2e_2 + e_3 \neq 0$, $e_1 + 3e_2 + e_3 \neq 0$, $2e_1 + e_2 + e_3 \neq 0$, $2e_1 + 3e_2 + e_3 \neq 0$, $3e_1 + e_2 + e_3 \neq 0$, $3e_1 + 2e_2 + e_3 \neq 0$. By eliminating the cases already satisfied due to convexity of Q, we see that Q is integrally indecomposable if and only if $2e_1 + e_2 + e_3 \neq 0$, $3e_1 + e_2 + e_3 \neq 0$, $3e_1 + 2e_2 + e_3 \neq 0$.

For example, the quadrangle $Q = conv((0, 4), (8, 0), (12, 8), (3, 9))$ has the edge sequence $\{4(2, -1), 4(1, 2), (-9, 1), (-3, -5)\}$ which satisfies three conditions at the end of the preceding paragraph. Hence, it is integrally indecomposable.

Now, we give some further numerical examples of Proposition 3.3.4, Proposition 3.3.5 and Proposition 3.3.6.

Example 3.3.7

(1) Any integral quadrangle Q having the edge sequence

$$\{2e_1, 2e_2, e_3, e_4\}$$

is integrally indecomposable.

Let us consider the quadrangle

$$Q = conv((0, 8), (10, 0), (8, 18), (3, 15)).$$

Since Q has the edge sequence $\{2(5, -4), 2(-1, 9), (-5, -3), (-3, -7)\}$, it is integrally indecomposable.

For example, the polynomial

$$f = a_1x^{10} + a_2y^8 + a_3x^8y^{18} + a_4x^3y^{15} + \sum c_{ij}x^iy^j,$$

with $(i,j) \in Q$ and $a_i \neq 0$, is absolutely irreducible over any field F.

(2) Any integral quadrangle Q with the edge sequence

$$\{3e_1, 2e_2, e_3, e_4\}$$

is integrally indecomposable if and only if $e_1 + e_2 + e_4 \neq 0$.

For example, let us consider the quadrangle

$Q = conv((0,9),(15,0),(17,20),(7,19))$ which has the edge sequence $\{3e_1, 2e_2, e_3, e_4\}$ with $e_1 = (5,-3)$, $e_2 = (1,10)$, $e_3 = (-10,-1)$ and $e_4 = (-7,-10)$. We see that $e_1 + e_2 + e_4 \neq 0$. So, Q is integrally indecomposable. Consequently, e.g. the polynomial

$$f = b_1x^{15} + b_2y^9 + b_3x^{17}y^{20} + b_4x^7y^{19} + \sum c_{ij}x^iy^j,$$

with $b_i \neq 0$ and $(i,j) \in Q$, is absolutely irreducible over any field F.

(3) Let Q be an integral quadrangle having the edge sequence

$$\{3e_1, 3e_2, e_3, e_4\}.$$

Then, Q is integrally indecomposable if and only if $e_1 + 2e_2 + e_4 \neq 0$.

As an example of this case, consider the quadrangle

$$Q = conv((0,3),(9,0),(12,15),(4,8))$$

which has the edge sequence $\{3(3,-1), 3(1,5), (-8,-7), (-4,-5)\}$ with $e_1 = (3,-1)$, $e_2 = (1,5)$, $e_3 = (-8,-7)$, $e_4 = (-4,-5)$ satisfying $e_1 + 2e_2 + e_4 \neq 0$. Therefore, Q is integrally indecomposable. For example, the polynomial

$$f = a_1x^9 + a_2y^3 + a_3x^{12}y^{15} + a_4x^4y^8 + \sum c_{ij}x^iy^j,$$

where $(i,j) \in Q$ and $a_i \neq 0$, is absolutely irreducible over any field F.

Remark 3.3.8 Let m, n be positive relatively prime integers. Then, considering the sum of the edge vectors, we see that there are no quadrangles with the edge sequences $\{me_1, ne_2, ne_3, me_4\}$ and $\{me_1, ne_2, ne_3, ne_4\}$. For example, there is no quadrangle having the edge sequence $\{2e_1, 2e_2, 2e_3, e_4\}$.

3.4 PENTAGONS

We can examine pentagons in three different cases as in Figure 5.

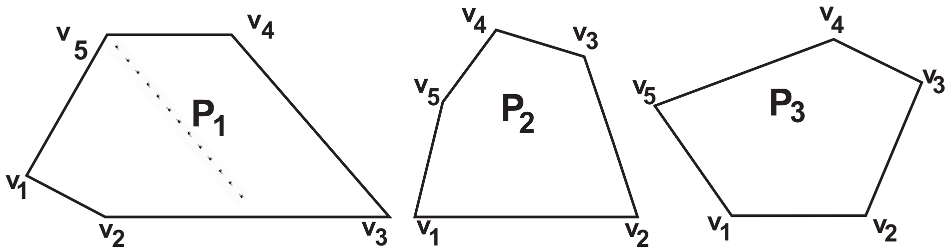


Figure 5

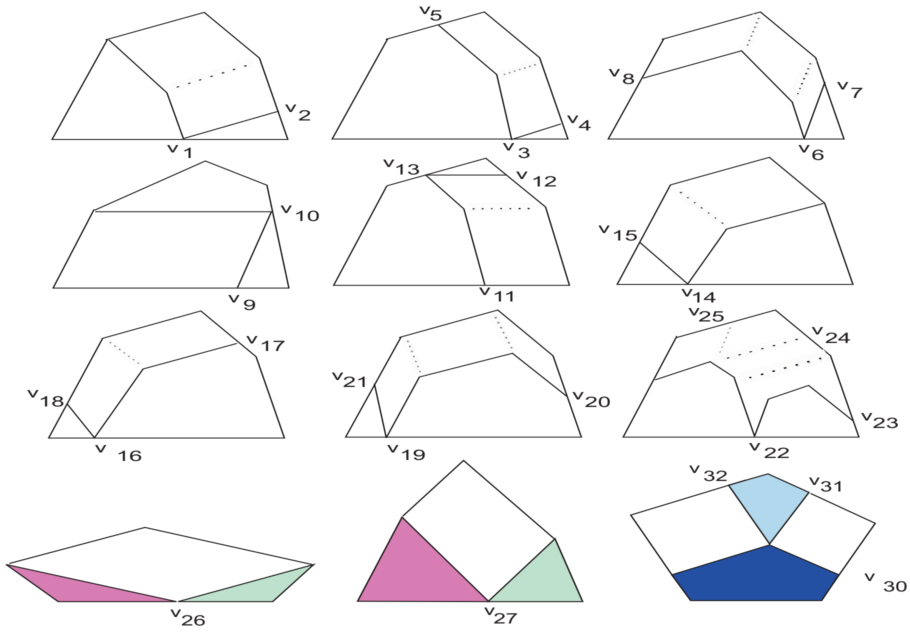
Let P_1 be an integral pentagon with two parallel edges as in Figure 5, (i). Note that

$$P_1 = conv(v_1, v_2, v_3 - (v_4 - v_5), v_5) + conv(0, v_4 - v_5).$$

Hence, P_1 is integrally decomposable. This also follows from Remark 3.0.7.

Let P_2 be an integral pentagon without parallel edges and having two adjacent interior angles whose sum is strictly less than 2π as in Figure 5, (ii). P_2 lies in a triangle T with base $[v_1, v_2]$. Integral indecomposability of P_2 is given in [G1, Corollary 4.12] when $gcd(v_1 - v_2) = 1$. Note that this also follows directly from the facts that any integral summand S of P_2 must have a closed boundary and the edges of S must be pieces of edges of P_2. If $gcd(v_1 - v_2) \neq 1$,

P_2 may be integrally indecomposable or not. By Lemma 3.0.6, if P_2 is integrally decomposable, then it may have only triangular, quadrangular or pentagonal nontrivial integral summands. In Figure 6, we give some examples of integrally decomposable pentagons of type P_2 with $gcd(v_1 - v_2) \neq 1$ provided that the indicated points v_i are integral.



Some decomposition methods for integral pentagons

Figure 6

Later in this subsection, we also give some examples of integrally indecomposable pentagons of type P_2 with $gcd(v_1 - v_2) \neq 1$.

Let P_3 be an integral pentagon which is not of type P_1 or P_2. Then the sum of any two adjacent interior angles of P_3 is strictly greater than 2π , see Figure 5, (iii). In Figure 6, we give two examples of integrally decomposable pentagons of type P_3 in case the indicated points v_i are integral.

The next two propositions give some criteria for integral indecomposability of pentagons of type P_2 or P_3.

Proposition 3.4.1 *The following integral polygons on the plane are integrally indecomposable:*

(1) *Any pentagon P which has the edge sequence $\{e_1, e_2, e_3, e_4, e_5\}$,*

(2) *Any pentagon P with the edge sequence $\{me_1, e_2, e_3, e_4, e_5\}$ satisfying $ce_1 + e_2 + e_4 \neq 0$ for any integer $1 \leq c \leq m-1$,*

(3) *Any pentagon P having the edge sequence $\{2e_1, 2e_2, e_3, e_4, e_5\}$ which satisfies*
$e_1 + e_2 + e_4 \neq 0,\ e_1 + e_3 + e_4 \neq 0,\ e_1 + e_3 + e_5 \neq 0,\ e_2 + e_3 + e_5 \neq 0,$
$e_2 + e_4 + e_5 \neq 0,$

(4) *Any 6-gon with the edge sequence $\{e_1, e_2, e_3, e_4, e_5, e_6\}$ such that $e_i + e_j + e_k \neq 0$ for $i, j, k \in \{1, 2, 3, 4, 5, 6\}$, more precisely, for*
$e_1 + e_2 + e_4 \neq 0,\ e_1 + e_2 + e_5 \neq 0,\ e_1 + e_3 + e_4 \neq 0,\ e_1 + e_3 + e_5 \neq 0,$
$e_1 + e_3 + e_6 \neq 0,\ e_1 + e_4 + e_5 \neq 0,\ e_1 + e_4 + e_6 \neq 0,$

(5) *Any 7-gon having the edge sequence $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ with $e_i + e_j + e_k \neq 0$ for $i, j, k \in \{1, 2, 3, 4, 5, 6, 7\}$,*

(6) *Any 8-gon having the edge sequence $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$ such that $e_i + e_j + e_k \neq 0$ and $e_i + e_j + e_k + e_s \neq 0$ for $i, j, k, s \in \{1, 2, 3, 4, 5, 6, 7, 8\}$,*

(7) *Any 9-gon having the edge sequence $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9\}$ such that $e_i + e_j + e_k \neq 0$ and $e_i + e_j + e_k + e_s \neq 0$ for i, j, k, s changing in the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$,*

(8) Any 10-gon having the edge sequence $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}\}$ *such that* $e_i + e_j + e_k \neq 0$, $e_i + e_j + e_k + e_s \neq 0$ *and* $e_i + e_j + e_k + e_s + e_t \neq 0$ *for* $i, j, k, s, t \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$,

(9) Any 11-gon having the edge sequence $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}\}$ *such that* $e_i + e_j + e_k \neq 0$, $e_i + e_j + e_k + e_s \neq 0$ *and* $e_i + e_j + e_k + e_s + e_t \neq 0$ *for* $i, j, k, s, t \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$,

(10) Any n-gon, $n \geq 3$*, having the edge sequence* $\{e_1, e_2, ..., e_n\}$ *such that* $e_i + e_j + e_k \neq 0$, $e_i + e_j + e_k + e_s \neq 0$,......, $e_i + e_j + e_k + e_s + ... + e_t \neq 0$ *i.e. we consider the sum of 3,4,5,...,n/2 edges if n is even and sum of 3,4,5,...,(n-1)/2 edges if n is odd for* $i, j, k, s, ..., t \in \{1, 2, 3, ..., n\}$.

Proof: We use Lemma 3.0.6.

(1) The edge sequence $\{e_1, e_2, e_3, e_4, e_5\}$ of P cannot have a subsequence whose sum of terms is zero while we have $e_1 + e_2 + e_3 + e_4 + e_5 = 0$.

(2),(3) We can easily see these effects by considering the sum of interior angles of any nontrivial summands of these pentagons.

(4) Proof has the same idea. We only need to observe that it is enough to consider only sum of $\binom{6}{3} \cdot \frac{1}{2} = 10$ triple edge vectors. Moreover, since the sum of three consecutive edges of an n-gon, for $n \geq 4$, cannot be zero we can omit to check the cases $e_1 + e_2 + e_3 \neq 0$, $e_1 + e_2 + e_6 \neq 0$ and $e_1 + e_5 + e_6 \neq 0$.

The remaining cases are generalizations of the previous idea and have same method of proving. We should note that the sum of terms of any edge sequence of upper or lower edges of a polygon cannot be zero. Therefore, beside the sum of three consecutive edges it is also not necessary to check the addition of those kinds of edge sequences for the polygons in these cases. See Figure 7 for the meaning of upper and lower edges of a polygon. □

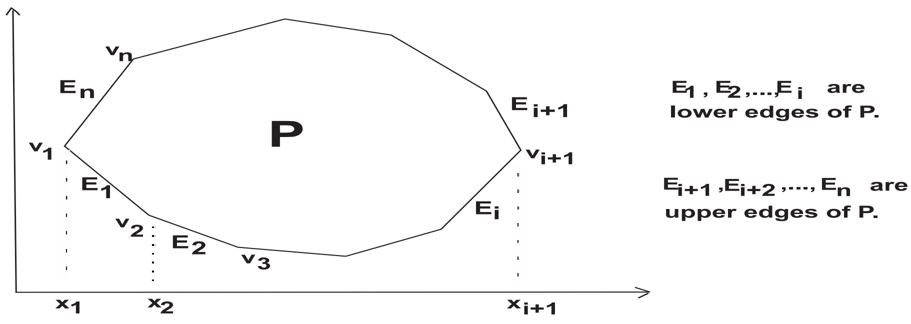

v_n
E_n
P
E_{i+1}
v_1
v_{i+1}
E_1
E_i
v_2
E_2
v_3
x_1
x_2
x_{i+1}
E_1 , E_2 ,...,E_i are lower edges of P.
E_{i+1} ,E_{i+2} ,..., E_n are upper edges of P.

Figure 7

Proposition 3.4.2 *Let P be an integral polygon in $\mathbb{R}^2$ having the edge sequence $\{(a_i, b_i)\}_{1 \leq i \leq n}$. And let k be an integer such that $gcd(k, n) = 1$. If either of the following two cases holds, then P is integrally indecomposable.*
Case (1) $a_i \equiv k(mod \quad n)$ for $1 \leq i \leq n$.
Case (2) $b_i \equiv k(mod \quad n)$ for $1 \leq i \leq n$.

Proof: Let S be a proper nonempty subset of the set $\{1, 2, ..., n\}$ with cardinality $|S| = s$. Then we have $\sum_{j \in S} a_j \equiv ks \not\equiv 0$ (mod n) or $\sum_{j \in S} b_j \equiv ks \not\equiv 0$ (mod n) since $s \lneqq n$. Consequently, the edge sequence $\{(a_i, b_i)\}_{1 \leq i \leq n}$ cannot have a proper subsequence whose sum of terms is zero since $\sum_{j \in S} a_j \neq 0$ or $\sum_{j \in S} b_j \neq 0$. □

We illustrate Proposition 3.4.1 and Proposition 3.4.2 with some examples.

Example 3.4.3

(1) Let us first consider the pentagon

$$P = conv((0,2),(1,0),(3,1),(2,5),(1,6)).$$

Since P has the edge sequence $\{(1,-2),(2,1),(-1,4),(-1,1),(-1,-4)\}$, it is integrally indecomposable. So, the polynomial

$$f = a_1x + a_2y^2 + a_3x^3y + a_4x^2y^5 + a_5xy^6 + \sum c_{ij}x^iy^j,$$

with $a_i \neq 0$ and $(i,j) \in P$, is absolutely irreducible over any field F.

(2) Let m, n be positive integers such that $gcd(m,n) = 1$. Then any bivariate polynomial $f \in F[x,y]$ having Newton polytope

$$P_f = conv((m,0),(0,n),(m+1,n+1),(m,n+m+1),(0,n+1))$$

is absolutely irreducible over any field F by Proposition 3.4.1, (1) since P_f is a pentagon having all edges primitive. For example, taking $m = 3$ and $n = 2$, the polynomial

$$f = a_1x^3 + a_2y^2 + a_3x^4y^3 + a_4x^3y^6 + a_5y^3 + \sum c_{ij}x^iy^j,$$

with $a_i \neq 0$ and $(i,j) \in P_f$, is absolutely irreducible over any field F.

(3) As an example of Proposition 3.4.1, (2), consider the pentagon

$$P = conv((0,4),(8,0),(15,5),(10,18),(1,16))$$

which has no parallel edges and does not lie in a triangle. It has the edge sequence $\{2(4,-2),(7,5),(-5,13),(-9,-2),(-1,-12)\}$ and is integrally indecomposable since $(4,-2)+(7,5)+(-9,-2)\neq 0$. Consequently, any polynomial

$$f=a_1x^8+a_2y^4+a_3x^{15}y^5+a_4x^{10}y^{18}+a_5xy^{16}+\sum c_{ij}x^iy^j,$$

with $a_i\neq 0$ and $(i,j)\in P$, is absolutely irreducible over any field F.

(4) As another example of Proposition 3.4.1, (2), the pentagon

$$P=conv((m,0),(0,n),(m+1,n+1),(m,n+m+1),(0,n+m))$$

is integrally indecomposable if m and n are relatively prime positive integers. Because, P has the edge sequence

$$\{m(0,-1),(m,-n),(1,n+1),(-1,m),(-m,-1)\}$$

with $i(0,-1)+(m,-n)+(-1,m)=(m-1,m-n-i)\neq(0,0)$ for any integer $1\leq i\leq m-1$.

(5) As a consequence of Proposition 3.4.1, (3), the polynomial

$$f=b_1x^6+b_2y^4+b_3x^{14}y^2+b_4x^{18}y^{11}+b_5x^9y^{12}+\sum c_{ij}x^iy^j,$$

where $b_i\neq 0$ and $(i,j)\in P_f$, is absolutely irreducible over any field F. Because, its Newton polytope is the integrally indecomposable pentagon

$$P_f=conv((0,4),(6,0),(14,2),(18,11),(9,12))$$

with the edge sequence $\{2(3,-2),2(4,1),(4,9),(-9,1),(-9,-8)\}$ which satisfies the conditions of Proposition 3.4.1, (3).

(6) Consider the 6-gon

$$P=conv((7,0),(8,0)(15,2),(16,7),(11,8),(0,3))$$

which has the edge sequence

$$\{(7,-3),(1,0),(7,2),(1,5),(-5,1),(-11,-5)\}$$

for which $7,1,-11,-5 \equiv 1 \pmod 6$. So, P is integrally indecomposable by Proposition 3.4.2. Alternatively, since the edge sequence of P satisfies the conditions of Proposition 3.4.1, (4), it is integrally indecomposable.

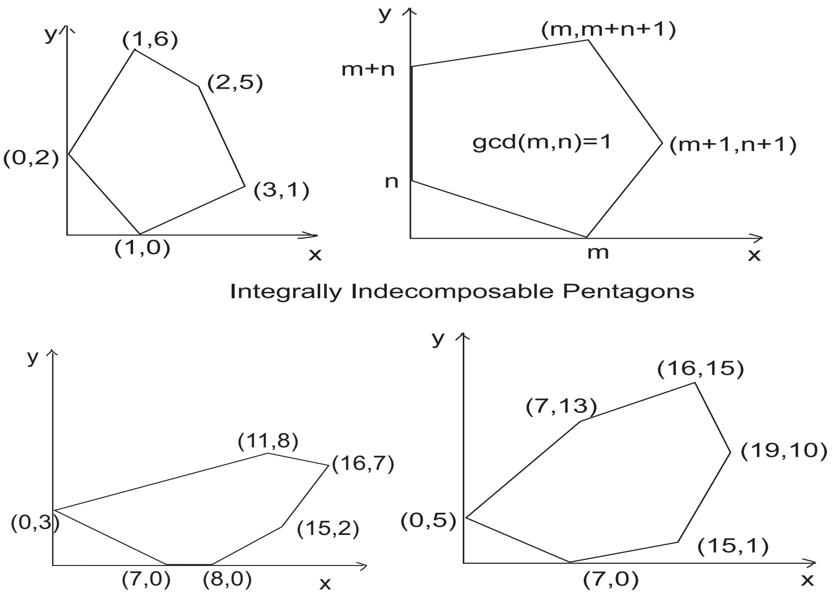
(7) Now, we give an example for which only item (4) Proposition 3.4.1 works. Let us consider the 6-gon

$$C = conv((7,0),(15,1),(19,10),(16,15),(7,13),(0,5))$$

having the edge sequence

$$\{(7,-5),(8,1),(4,9),(-3,5),(-8,-1),(-8,-9)\}.$$

We see that C is integrally indecomposable since its edge sequence satisfies the conditions of Proposition 3.4.1, (4).



Integrally Indecomposable Pentagons

Integrally Indecomposable Hexagons

Figure 8

The polygons presented in Example 3.4.3 have no parallel edges and do not lie inside a triangle having a common edge with the polygon. Figure 8 shows four of these polygons.

These examples are not covered by the methods presented in [G1]. Note that the methods of [G1] for indecomposability of polygons assume that P_f lies inside a triangle having a common edge with P_f, and this is not the case in our examples of Example 3.4.3.

Remark 3.4.4 While giving above criteria for integral indecomposability, we are actually having classification of decomposable quadrangles, pentagons. For example, if Q is an integrally decomposable quadrangle with the edge sequence $\{4e_1, 4e_2, e_3, e_4\}$ then its integral summands are included in one and only one of the following three different types:

(1): $2e_1 + e_2 + e_3 = 0$,

(2): $3e_1 + e_2 + e_3 = 0$,

(3): $3e_1 + 2e_2 + e_3 = 0$.

Moreover, Q may have only one unique decomposition up to translation of summands in all these cases.

Let us give an integrally decomposable quadrangle of type (1). In order to have this example, we take the primitive edge vectors as $e_1 = (2, -1)$, $e_2 = (3, 1)$. Using $2e_1 + e_2 + e_3 = 0$, we have $e_3 = (-7, 1)$. Since we must have $2e_1 + 3e_2 + e_4 = 0$, we get $e_4 = (-13, -1)$. We see that the quadrangle

$$Q = conv((8, 0), (20, 4), (13, 5), (0, 4))$$

with the edge sequence

$$\{4(2, -1), 4(3, 1), (-7, 1), (-13, -1)\}$$

has unique integral decomposition (up to translation of summands) as

$$Q = conv((4,0),(13,3),(0,2)) + conv((4,0),(7,1),(0,2)).$$

Note that the polynomial $f = 3x^8 + 3y^4 + x^{20}y^4 + x^{13}y^5 + x^8y + x^{13}y^3$, which has the integrally decomposable Newton polytope $P_f = Q$, is absolutely irreducible over the complex numbers $\mathbb{C}$ and irreducible over the field $\mathbb{F}_{2^{21}}$, and reducible over $\mathbb{F}_3$.

We can generalize Proposition 3.4.2 for any n-dimensional polytope P in $\mathbb{R}^n$. First, we choose a fixed vertex v_0, and consider any connected edge sequence $S = \{c_ie_i\}_{1\leq i\leq m}$, i.e. $e_i \cap e_{i+1} \neq \emptyset$, starting and ending at v_0. Since we mention about a closed path, we must have $\sum_{i=1}^{m} c_ie_i = (0,,...,0)$. If Q is a summand of P containing the vertex v_0 then the corresponding edge sequence of Q to the edge sequence S of P must be of the form $\{d_ie_i\}_{1\leq i\leq m}$ where $0 \leq d_i \leq c_i$. and $\sum_{i=1}^{n} d_ie_i = (0,...,0)$.

Corollary 3.4.5 *Let P be an n-dimensional integral polytope having all edges primitive with vertices v_0, v_1, ..., v_k in $\mathbb{R}^n$. Let us consider all edge sequences, starting and ending at v_0, $S_j = \{(a_{1i}, a_{2i}, ..., a_{ni})\}_{1\leq i\leq m_j}$, $1 \leq j \leq r$. And let k be relatively prime integer with m_j. If we have at least one of the following cases for all edge sequences S_j then P is integrally indecomposable.*

Case (1) $a_{1i} \equiv k \pmod{m_j}$ for $1 \leq i \leq m_j$.

Case (2) $a_{2i} \equiv k \pmod{m_j}$ for $1 \leq i \leq m_j$.

$\vdots$

Case (m) $a_{mi} \equiv k \pmod{m_j}$ for $1 \leq i \leq m_j$.

Chapter 4

INTEGRALLY INDECOMPOSABLE POLYTOPES IN $\mathbb{R}^n$

Beside the integral indecomposability, there is another concept, *homothetic indecomposability* for polytopes, see the book [Gr, Chapter 15]. Let P and Q be polytopes in $\mathbb{R}^n$, not necessarily integral. Q is said to be homothetic to P if there exists a real number $r \geq 0$ and a vector $v \in \mathbb{R}^n$ such that

$$Q = rP + v = \{ra + v : a \in P\}.$$

A polytope Q is said to be homothetically indecomposable if $Q = A + B$ for some polytopes A and B then either A or B is homothetic to Q, e.g. if A is homothetic to Q then

$$Q = A + B = (rQ + v) + (1 - r)Q + (-v)$$

for some $0 \leq r \leq 1$ and $v \in \mathbb{R}^n$. Otherwise, Q is called homothetically decomposable.

4.1 RELATION BETWEEN INTEGRAL AND HOMOTHETIC INDECOMPOSABILITY OF POLYTOPES

Homothetically indecomposable polytopes have been widely studied in the literature, for example in [K, Mc, Me, Sh, Sm1, Sm2]. There is no direct comparison between integral and homothetic indecomposability of polytopes. A polytope may satisfy only one of them or both or none.

For example, the only homothetically indecomposable polytopes in the plane are line segments and triangles. Any summand of a line segment must be parallel to it and have smaller length than itself. Also, the edges of a summand of triangle T must be parallel to the edges of T and have smaller length than them.

As we have seen in Chapter 3, only some triangles or line segments, and many polygons having more than three edges are integrally indecomposable. An integral square is both integrally and homothetically decomposable. There is a result in [G2] giving a relation between these two different concepts of decomposability of polytopes.

Proposition 4.1.1 *Let P be an integral polytope in $\mathbb{R}^n$ with vertices $v_1, ..., v_m$. If P is homothetically indecomposable and*

$$gcd(v_1 - v_2, ..., v_1 - v_m) = 1$$

then P is integrally indecomposable.

Proof: See the proof of [G2, Proposition 12]. □

From Proposition 4.1.1 we get the following simple and useful lemma.

Lemma 4.1.2 *Let Q be a homothetically indecomposable integral polytope with vertices v_1,... ,v_m. Then, Q is integrally indecomposable if and only if*

$$gcd(v_1 - v_2, ..., v_1 - v_m) = 1.$$

Proof: Let $gcd(v_1 - v_2, ..., v_1 - v_m) = d > 1$. Then, the polytope $P = conv(0, v_2 - v_1, ..., v_m - v_1)$ is integral. Therefore, $Q = v_1 + d \cdot (\frac{1}{d}P)$.

Converse follows from Proposition 4.1.1. □

By Lemma 4.1.2, we can get many integrally indecomposable polytopes using the homothetically indecomposable polytopes constructed in [K, Mc, Me, Sh, Sm1, Sm2]. The following three theorems are combinations (and specializations to integral polytopes) of theorems about homothetic indecomposability given in these references and Lemma 4.1.2.

Let P be a polytope. A sequence $F_0, F_1, ..., F_m$ of faces of P is called a *strong chain* if $dim(F_i \cap F_{i+1}) \geq 1$ for $i = 0, ..., m-1$. Such a chain is said to join two vertices u and v of P if, say $u \in F_0$, and $v \in F_m$. See [Mc].

Theorem 4.1.3 *Let $P = conv(v_1, v_2, ..., v_k)$ be a polytope in $\mathbb{R}^n$ such that any two of whose vertices can be joined by a strong chain of homothetically indecomposable faces. Then P is homothetically indecomposable.*

In particular, if P is also integral then it is integrally indecomposable if and only if $gcd(v_1 - v_2, ..., v_1 - v_k) = 1$.

Proof: For the first part, see the proof of [Sh, Statement 12]. The second part follows from Lemma 4.1.2. □

Now, we give some applications of Theorem 4.1.3,

Example 4.1.4 Let $k \geq 3$ be an integer and $C = conv(v_1, ..., v_k)$ be an integral polytope on an $(n-1)$-dimensional hyperplane H in $\mathbb{R}^n$. Let $a, b, u, v, w \in$

$H^+ \setminus H$ and $a', b', u', v', w' \in H^- \setminus H$ be distinct integral points in the corresponding half spaces. Let us form the triangles $A = conv(v, u, w) \subset H^+$ and $B = conv(v', u', w') \subset H^-$. Assume that the projections of A and B on H are in relint(C), relint($[a, a']$)$\cap$ relint(C) $= \{p\}$ is a single point, and relint($[b, b']$)$\cap$ relint(C) $= \emptyset$. Assume also that affine hull of any edge of A is skew with affine hull of any edge of C (nonintersecting and nonparallel) and affine hull of any edge of B is skew with affine hull of any edge of C. Then, the following seven polytopes are homothetically indecomposable by the first part of Theorem 4.1.3 since any two vertices of them can be joined by a strong chain of triangular faces. Moreover, since C, A and B are integral, by the second part of Theorem 4.1.3 we have the following:

(1) The pyramid $P = conv(C, v)$ is integrally indecomposable if and only if

$$gcd(v - v_1, ..., v - v_k) = 1.$$

(2) The bipyramid $Q = conv(C, a, a')$ is integrally indecomposable if and only if

$$gcd(a - v_1, ..., a - v_k, a - a') = 1.$$

See Figure 9,(i).

(3) Let $D = conv(C, b, b')$. As relint($[b, b']$)$\cap$ relint(C) $= \emptyset$, some of the vertices $v_1, ..., v_k$ of C are no longer a vertex of D (see Figure 9, ii). However, it is clear by convexity that the vertices of D are b, b' and a subset of $\{v_1, ..., v_k\}$. By relabelling the vertices of C if necessary, let the vertices of D be $\{b, b', v_1, ..., v_r, v_s, ..., v_k\}$ where $1 \leq r < s \leq k$. We call such a polytope D *degenerate bipyramid*. D is integrally indecomposable

if and only if

$$gcd(b - v_1, ..., b - v_r, b - v_s, ..., b - v_k, b - b') = 1.$$

(4) $R = conv(C, u, v, u')$ is integrally indecomposable if and only if

$$gcd(u - v_1, ..., u - v_k, u - v, u - u') = 1.$$

(5) $T = conv(C, u, v, w, u')$ is integrally indecomposable if and only if

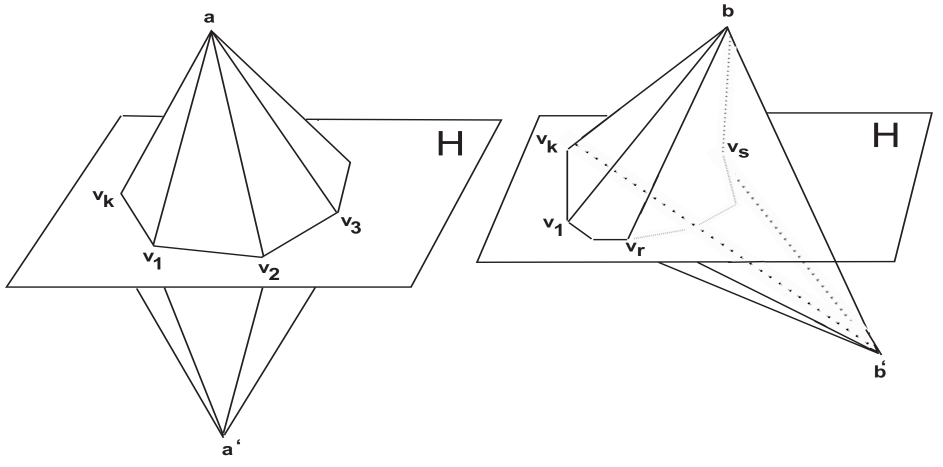
$$gcd(u - v_1, ..., u - v_k, u - v, u - w, u - u') = 1.$$

(6) $S = conv(C, u, v, w, u', v')$ is integrally indecomposable if and only if

$$gcd(u - v_1, ..., u - v_k, u - v, u - w, u - u', u - v') = 1.$$

(7) $K = conv(C, u, v, w, u', v', w')$ is integrally indecomposable if and only if

$$gcd(u - v_1, ..., u - v_k, u - v, u - w, u - u', u - v', u - w') = 1.$$



(i)

Indecomposable bipyramid

(ii)

An indecomposable degenerate bipyramid

Figure 9

Remark 4.1.5 Note that Example 4.1.4, (1) is precisely [G1, Theorem 4.2]. The other items of Example 4.1.4 are not covered in [G1] and [G2].

We observe that, by combining [G1, Theorem 4.11] and Example 4.1.4, (1), any integral pyramid P in $\mathbb{R}^n$ is integrally indecomposable if one of its faces is integrally indecomposable.

Corollary 4.1.6 *If all 2-dimensional faces of a polytope $P = conv(v_1, v_2, ..., v_k)$ in $\mathbb{R}^n$ are triangles, then it is homothetically indecomposable.*

In particular, if P is also integral then it is integrally indecomposable if and only if $gcd(v_1 - v_2, ..., v_1 - v_k) = 1$.

Proof: See the proof of [Gr, (3) on page 321] or [Sh, Statement 13]. The second part follows from Lemma 4.1.2. □

We illustrate some of the polytopes presented in Example 4.1.4 with numerical examples. Note that the presented polytopes in Example 4.1.7 and Example 4.1.8 do not lie inside a pyramid. Hence, [G1, Theorem 4.2 and Theorem 4.11] do not work in order to decide the integral indecomposability of these polytopes.

Example 4.1.7 Let F be any field and $f_1, f_2, f_3 \in F[x, y, z]$ be polynomials as

$f_1 = x^3y^2 + yz^4 + x^4z + xyz^9 + x^2yz,$

$f_2 = y^2z^5 + xz^6 + x^3yz^3 + x^4y^2z + x^4y^3 + x^2y^5 + xy^6 + y^7 + xy^2z^{12} + x^3y^2z,$

$f_3 = x^8z^2 + x^{10} + x^2y^7z + y^4z^6 + yz^9 + x^5y^3z^{10} + x^3y^2.$

Then the corresponding polytopes P_{f_i} for $i = 1, 2, 3$ are of type bipyramid and these polynomials are absolutely irreducible over F by Example 4.1.4, (2). For example, $P_{f_1} = conv(C, a, a')$ with

$$C = conv((3, 2, 0), (0, 1, 4), (4, 0, 1)) \subset H$$

and $a = (1,1,9) \in H^+$, $a' = (2,1,1) \in H^-$, where H is the hyperplane $x+y+z=5$ in $\mathbb{R}^3$. Moreover, $gcd(a-(3,2,0)) = gcd(-2,-1,9) = 1$.

Let us consider the polynomial

$f_4 = x^5z^{10} + x^{13}y^2z^{10} + x^{15}y^7z^{10} + x^{16}y^{12}z^{10} + x^{14}y^{16}z^{10} + x^{10}y^{19}z^{10} +$

$x^5y^{17}z^{10} + x^2y^{13}z^{10} + y^6z^{10} + x^{32}y^{15}z^{20} + x^{27}y^{12} \in F[x,y,z]$.

Then $P_{f_4} = conv(C, b, b')$ with

$C = conv((5,0,10),(13,2,10),(15,7,10),(16,12,10),(14,16,10),(10,19,10),$

$(5,17,10),(2,13,10),(0,6,10)) \subset H$

and $b = (32,15,20) \in H^+$, $b' = (27,12,0) \in H^-$, where H is the hyperplane $z = 10$ in $\mathbb{R}^3$. Moreover, the set of vertices of P_{f_4} is

$$\{b, b', (5,0,10),(13,2,10),(10,19,10),(5,17,10),(2,13,10),(0,6,10)\}.$$

Hence, P_{f_4} is a degenerate bipyramid and as $gcd(b-b') = gcd(5,3,20) = 1$, f is absolutely irreducible over F by Example 4.1.4, (3).

The polynomial

$g = x^5y^{20} + x^6z^6 + y^6z^8 + x^2yz^9 + x^{14}y^2 + x^4y^7z^8 + x^8y^{11}z^6 + xy^6z^2 \in F[x,y,z]$

has the Newton polytope $P_g = conv(C, u, v, u')$ of type Example 4.1.4, (4), see Figure 10, with $C = conv((5,20,0),(0,6,8),(2,1,9),(14,2,0)) \subset H$ and $u = (4,7,8), v = (8,11,6) \in H^+$, $u' = (1,6,2) \in H^-$, where H is the hyperplane $2x+y+3z = 30$ in $\mathbb{R}^3$. Since $gcd(u-(0,6,8)) = gcd(13,-6,0) =$, g is absolutely irreducible over F.

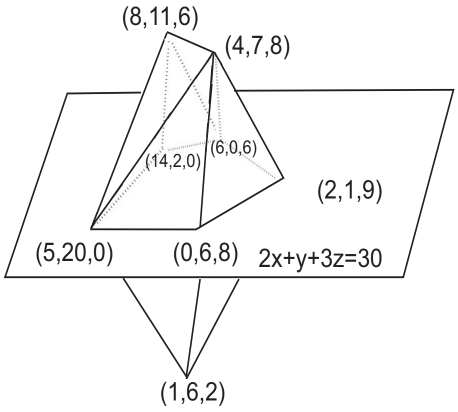
The following polynomial

$h = x^7z^{21} + x^{10}y^{18} + y^{12}z^{16} + x^3y^9z^{48} + x^7y^8z^{45} + x^4y^{13}z^{43} + x^5y^6z^9 \in F[x,y,z]$

has $P_h = conv(C, u, v, w, u')$ with

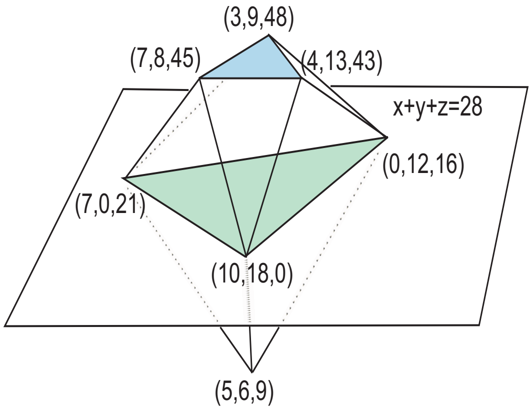
$$C = conv((7,0,21),(10,18,0),(0,12,16)) \subset H$$

and $u = (7,8,45), v = (4,13,43), w = (3,9,48) \in H^+$, $u' = (5,6,9) \in H^-$, where H is the hyperplane $x+y+z = 28$ in $\mathbb{R}^3$ (See Figure 11). In addition, since P_h is a polytope of type Example 4.1.4, (5) and $gcd(v - u') = gcd(-1, 7, 34) = 1$, h is absolutely irreducible over F.



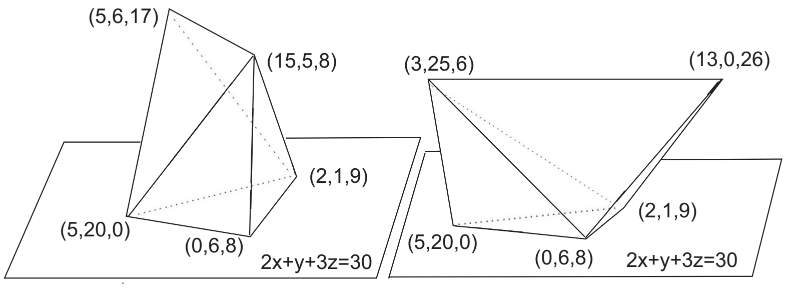
The Newton polytope of g.

Figure 10



The Newton Polytope of h.

Figure 11



The Newton polytope of k

The Newton polytope of m

Figure 12

Example 4.1.8 Let F be any field and $k, m \in F[x, y, z]$ be polynomials as
$k = c_1x^5y^{20} + c_2y^6z^8 + c_3x^2yz^9 + c_4x^5y^6z^{17} + c_6x^{15}y^5z^8$
$m = d_1x^5y^{20} + d_2y^6z^8 + d_3x^2yz^9 + d_4x^3y^{25}z^6 + d_6x^{13}z^{26}$
with $c_i, d_i \in F \setminus \{0\}$. Then the polytopes P_k and P_m are integrally indecom-

posable by Corollary 4.1.6. For example, $P_k = conv(C, u, v)$ is the polytope with

$$C = conv((5, 20, 0), (0, 6, 8), (2, 1, 9)) \subset H$$

and $u = (5, 6, 17), v = (15, 5, 8) \in H^+$, where H is the hyperplane $2x+y+3z = 30$ in $\mathbb{R}^3$. Moreover, since P_k is a tent T over a triangle and has triangular faces and $gcd((0, 6, 8) - u) = gcd(-5, 0, -9) = 1$, g is absolutely irreducible over F. Figure 12 shows the Newton polytopes of k and m.

Remark 4.1.9 All of the presented polynomials in Example 4.1.7 and Example 4.1.8 still will be absolutely irreducible over F if the coefficients of them are changed with any nonzero elements $c_i \in F \setminus \{0\}$, and if they are added any number of terms whose exponent vectors lie inside their Newton polytopes. For any polynomial f over F, the number of such integral exponents inside P_f is always finite and bounded from above by a number depending on f. Moreover, in some cases, depending on the configuration of P_f, we can even add as many terms as we like to the given polynomial. For example, consider the polynomial
$f = c_1x^7y^7z^{20} + c_2x^4y^6 + c_3x^5y^5z^{11} + c_4x^5y^4z^{10} + c_5x^6z^7 + c_6y^3z^4 + c_7x^2z^3 + c_8x^5y^3z^9 + c_9x^5y^2z^8 + c_{10}x^5yz^7 + c_{11}x^5z^6 + c_{12}x^4y^5z^{10} + c_{13}x^4y^6z^{11} + c_{14}x^4y^7z^{12} + c_{15}x^4y^8z^{13} + c_{16}x^4y^9z^{14} + c_{17}x^4y^{10}z^{15} + c_{18}x^3y^2z^6 + c_{19}x^{20}y^{25}z^{46} + c_{20}x^{99}yz^{101} + c_{21}xy^2z^4 + c_{22}x^7yz^9 + c_{23}x^5y^9z^{14} + c_{24}x^7y^8z^{16} + c_{25}x^4y^{10}z^{15} + c_{26}x^{41}y^{42}z^{84}$
with nonzero coefficients c_i over the field F. Newton polytope of f is the bipyramid $P_f = conv(C, a, a')$ with $C \subset H$ and $a = (7, 7, 20) \in H^+$, $a' = (4, 6, 0) \in H^-$, where H is the hyperplane $-x - y + z = 1$ in $\mathbb{R}^3$. Moreover, since relint $(C) \cap$ relint $([a, a']) = (97/16, 107/16, 55/4)$ is a single point and $gcd(a - a') = gcd(3, 1, 20) = 1$, P_f is integrally indecomposable by Example 4.1.4 (2). Hence, if f is added any new terms whose exponent vectors lying on

the hyperplane $-x-y+z=1$, then it is still absolutely irreducible over F since its Newton polytope is always an integrally indecomposable bipyramid.

Using Statement 14 in [Sh] we obtain the following.

Corollary 4.1.10 *Let $P_1 = conv(v_1, v_2, ..., v_m), P_2 = conv(u_1, u_2, ..., u_k)$ be two disjoint $(n-1)$-dimensional polytopes, $n \geq 3$, lying in parallel hyperplanes H_1, H_2 respectively, such that affine hull of any edge of one is skew with affine hull of any edge of the other. Then the polytope $P = conv(P_1 \cup P_2)$ is homothetically indecomposable.*

In particular, if P is also integral then it is integrally indecomposable if and only if $gcd(v_1 - v_2, ..., v_1 - v_m, v_1 - u_1, ...v_1 - u_k) = 1$.

Proof: Since all the lateral faces of P are triangular, we can apply Theorem 4.1.3. $\square$

Example 4.1.11 We give an example for Corollary 4.1.10 for $n = 3$. Let P_1 and P_2 be polygons with no parallel edges lying in different parallel planes. Then $P = conv(P_1 \cup P_2)$ is an antiprism having all the 2-dimensional faces as triangular except for P_1 and P_2. Since we can find a strong chain of triangular faces connecting any two of vertices of P, P is homothetically indecomposable by Theorem 4.1.3. For $n > 3$, see [Sh].

Remark 4.1.12 Note that if the hyperplanes H_1 and H_2 are not parallel in $\mathbb{R}^n$ for $n \geq 3$, they divide $\mathbb{R}^n$ into four different regions. If the polytope P, mentioned in Corollary 4.1.10, lies in only one of these regions, we can still apply Corollary 4.1.10. See Figure 13.

Moreover, in Corollary 4.1.10, beside the vertices of integral polytopes $P_1 = conv(v_1, v_2, ..., v_m)$ and $P_2 = conv(u_1, u_2, ..., u_k)$ we can adjoin integral points $v_{m+1} \notin H_1$ and $u_{k+1} \notin H_2$ as shown in Figure 14. And then the obtained integral polytope $Q = conv(P_1, P_2, v_{m+1}, u_{k+1})$ is homothetically indecomposable. So, the methods of Corollary 4.1.10 also work for the polytope Q instead of P. The polytope Q is shown in Figure 14.

Remark 4.1.13 Let $P = conv(P_1 \cup P_2)$ be an integral polytope in $\mathbb{R}^n$, where P_1 and P_2 are disjoint homothetically indecomposable facets lying on parallel hyperplanes H_1 and H_2 respectively. Then, in [Sm1, Result 3] it is stated that P is homothetically decomposable if and only if P_1 and P_2 are homothetic. Consequently, P is homothetically indecomposable if and only if P_1 is not homothetic to P_2. For example, for $n = 3$, if P_1 and P_2 are not homothetic homothetically indecomposable polytopes lying on two disjoint parallel planes then the polytope $P = conv(P_1 \cup P_2) = conv(v_1, v_2, ..., v_m)$ is integrally indecomposable if and only if

$$gcd(v_1 - v_2, v_1 - v_3, ..., v_1 - v_m) = 1.$$

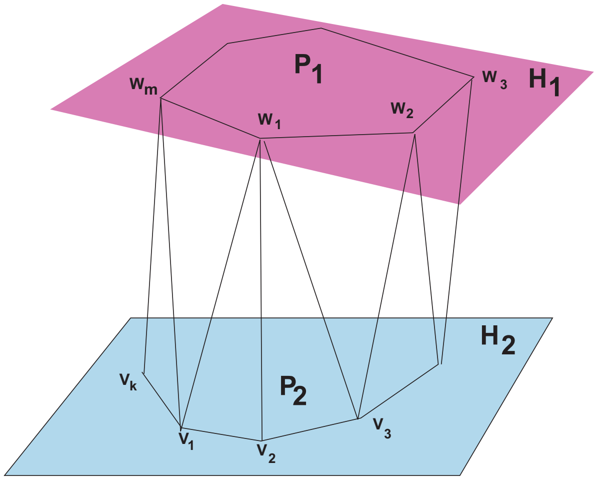


Figure 13

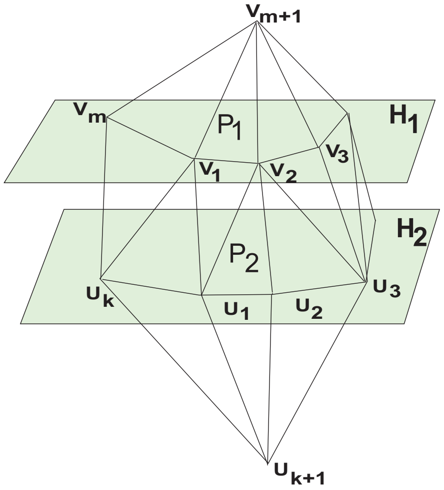


Figure 14

A family $\mathfrak{F}$ of faces of a polytope P is called *strongly connected* if for each $F, G \in \mathfrak{F}$, there exists a strong chain $F = F_1, F_2, ..., F_m = G$ with each $F_i \in \mathfrak{F}$. A subset $\mathfrak{F}$ of faces *touches* a face F of P if $(\bigcup_{F_i \in \mathfrak{F}} F_i) \cap F \neq \emptyset$. Recall that a facet of P is a face F of dimension $dim(F) = dim(P) - 1$. See [Mc].

In Theorem 4.1.14 and Theorem 4.1.15, the results about homothetic indecomposability, are due to Mcmullen [Mc].

Theorem 4.1.14 *If P is a polytope having a strongly connected family of homothetically indecomposable faces that touches each of its facets then it is homothetically indecomposable.*

In addition, if P is also an integral polytope with vertices $v_1, v_2, ..., v_n$ then, it is integrally indecomposable if and only if $gcd(v_1 - v_2, v_1 - v_3, ..., v_1 - v_n) = 1$.

Proof: See the proof of [Mc, Theorem 2]. □

By using Theorem 4.1.14, the following theorem is obtained.

Theorem 4.1.15 *Let A, B be polytopes such that $C = conv(A \cup B)$ and $dim(C) = dim(A) + dim(B) + 1$. Then C is homothetically indecomposable.*

Moreover, if C is also an integral polytope having the vertices $v_1, v_2, ..., v_n$ then, it is integrally indecomposable if and only if

$$gcd(v_1 - v_2, v_1 - v_3, ..., v_1 - v_n) = 1.$$

Proof: See the proof of [Mc, Theorem 3]. □

Example 4.1.16 Let $P = conv(v_1, v_2, ..., v_k)$ be an $(m-1)$-dimensional integral polytope lying in a hyperplane H in $\mathbb{R}^n$. Take any integral point $v \notin H$. Then the pyramid C=conv(P,v) is homothetically indecomposable by Theorem 4.1.15 since

$$m = dim(C) = dim(P) + dim(\{v\}) + 1 = (m-1) + 0 + 1.$$

In particular, our pyramid C is integrally indecomposable if and only if

$$gcd(v - v_1, v - v_2, ..., v - v_k).$$

Consequently, e.g., for two distinct integral points v_1 and v in $\mathbb{R}^n$, the line segment $\ell = [v_1, v]$ is integrally indecomposable if and only if $gcd(v - v_1) = 1$ since

$$dim(\ell) = 1 = 0 + 0 + 1 = dim(\{v_1\}) + dim(\{v\}) + 1.$$

Moreover, if v_1, v_2 and v are three distinct nonlinear integral points in $\mathbb{R}^n$ then the triangle $T = conv(v_1, v_2, v)$ is integrally indecomposable if and only if $gcd(v - v_1, v - v_2) = 1$ since

$$dim(T) = 2 = 1 + 0 + 1 = dim([v_1, v_2]) + dim(\{v\}) + 1.$$

Let $\ell_1 = [v_1, v_2]$ and $\ell_2 = [v_3, v_4]$ be the skew line segments formed by the distinct integral points v_1, v_2, v_3, v_4 in $\mathbb{R}^n$ not lying in the same plane. Then, by Theorem 4.1.15, the polytope $conv(v_1, v_2, v_3, v_4)$ is integrally indecomposable if and only if $gcd(v_1 - v_2, v_1 - v_3, v_1 - v_4) = 1$. Because, we have

$$dim(conv(\ell_1 \cup \ell_2)) = 3 = 1 + 1 + 1 = dim(\ell_1) + dim(\ell_2) + 1.$$

Remark 4.1.17 In Example 4.1.16, we have given another proofs of [G1, Theorem 4.2], [G1, Corollary 4.3], [G1, Corollary 4.5] and [G1, Corollary 4.7]. As we see, Gao's results are examples of Theorem 4.1.15.

4.2 A NEW OBSERVATION GIVING NEW INTEGRALLY INDECOMPOSABLE POLYTOPES IN $\mathbb{R}^n$

We observe that in the previous theorems in Section 4.1, we can consider strong chain of integrally indecomposable faces instead of strong chain of homothetically indecomposable faces. Then, we get new theorems giving many new integrally indecomposable polytopes in $\mathbb{R}^n$. Note that the proofs of the following three theorems are obtained by modifications of the proofs of the corresponding results from [Sh, Mc].

Theorem 4.2.1 *Let P be an integral polytope in $\mathbb{R}^n$ such that any two of whose vertices can be joined by a strong chain of integrally indecomposable faces. Then P is integrally indecomposable.*

Proof: Let us assume that $P = Q + R$ for some integral polytopes such that $P = conv(p_1, p_2, ..., p_m)$ and $Q = conv(q_1, q_2, ..., q_m)$, where in order to have the same number of vertices we allow the repetition of vertices of Q.. We shall show that Q is a translation of P, i.e. $Q = P + v$ for some vector $v \in \mathbb{R}^n$.

Let p_i be any vertex of P and $F = conv(p_i, p_{i+1}, ..., p_k) = P \cap H_P(u)$ be an integrally indecomposable face of P containing p_i, where $H_P(u)$ is a supporting hyperplane of P having normal vector $u \in \mathbb{R}^n$. Then, the corresponding face $G = conv(q_i, q_{i+1}, ..., q_k) = F \cap H_P(u)$ of Q, i.e. $F = G + H$ for some face H of R, must be of the form $G = F + v$ for some vector $v \in \mathbb{R}^n$. Therefore, any edge $[q_j, q_{j+1}]$ of Q must be of the form $[q_j, q_{j+1}] = [p_j, p_{j+1}] + v$. Hence, $q_j = p_j + v$ and $q_{j+1} = p_{j+1} + v$. Since any two vertices e, e' of P can be joined by a strong chain of integrally indecomposable faces $F_1, ..., F_s$, where $e \in F_1, ..., e' \in F_s$ and $F_i \cap F_{i+1}$ is a line segment, we conclude that $q_i = p_i + v$ for all $i, = 1, ..., m$. So, $Q = P + v$. Consequently, P is integrally indecomposable. □

Example 4.2.2 As a result of Theorem 4.2.1, we give six new integrally indecomposable polytopes in $\mathbb{R}^n$. Of course, we can have infinitely many examples of this kind by taking extra suitable hyperplanes in the following items. We consider our polytopes as seen in the respective figures. That is, in Figures 15,16, 18, 19,20, we assume that projection of C_1 on C_2 lies in relint(C_2).

(1) Consider Figure 15. Let $n \geq 3$ be an integer. Let $C_1 = conv(v_1, v_2, v_3, ..., v_n)$, $C_2 = conv(u_1, u_2, u_3, ..., u_{2n})$ and $C_3 = conv(w_1, w_2, w_3, ..., w_n)$ be integral polytopes lying on different nonparallel hyperplanes as shown in Figure 15. Consider the integral polytope $C = conv(C_1, C_2, C_3)$. Assume that the lateral white faces of C are integrally indecomposable quadrangles $conv(v_1, v_2, u_2, u_3)$, $conv(v_2, v_3, u_4, u_5), ...,$ $conv(v_n, v_1, u_{2n}, u_1)$. Then, C is integrally indecomposable if C_1 or C_2 is integrally indecomposable.

(2) Consider Figure 16. Let $n \geq 4$ be an even integer. We take the integral polytopes $C_1 = conv(v_1, v_2, v_3, ..., v_n)$, $C_2 = conv(u_1, u_2, u_3, ..., u_n)$ and $C_3 = conv(w_1, w_2, w_3, ..., w_n)$ lying on different nonparallel hyperplanes as shown in Figure 16. Consider the integral polytope $C = conv(C_1, C_2, C_3)$. Assume that the lateral faces $conv(v_1, v_2, u_1, u_2)$, $conv(v_3, v_4, u_3, u_4), ..., conv(v_{n-1}, v_n, u_{n-1}, u_n)$ are integrally indecomposable quadrangles. Then, C is integrally indecomposable if C_1 or C_2 is integrally indecomposable.

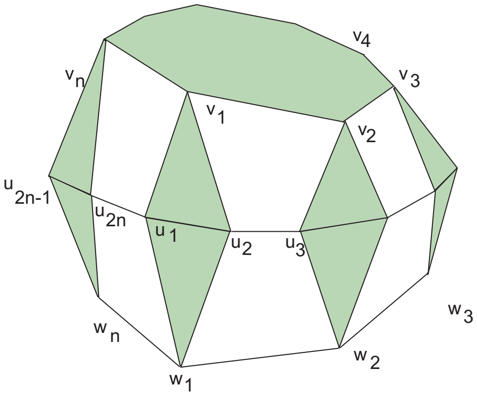


Figure 15

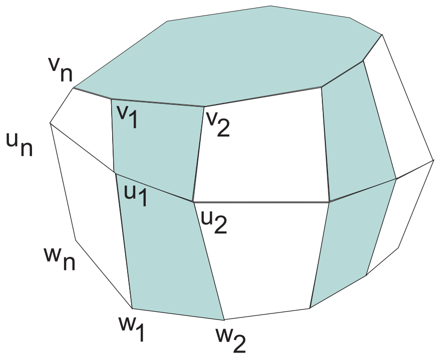


Figure 16

(3) Consider Figure 17. Let $n \geq 4$ be an integer and H_1, H_2 be parallel-nonintersecting hyperplanes in $\mathbb{R}^n$. Let $C_1 = conv(v_1, v_2, v_3, ..., v_n) \subset H_1$ and $C_2 = conv(u_1, u_2, u_3, ..., u_n) \subset H_2$ be integral polytopes such that

(i) $[v_1, v_2]$ is not parallel to $[u_1, u_2]$, $[v_3, v_4]$ is not parallel to $[u_3, u_4], ...,$ ($[v_n, v_1]$ is not parallel to $[u_n, u_1]$ if n is a positive odd integer),

(ii) $[v_2, v_3]$ is not parallel to $[u_2, u_3]$, $[v_4, v_5]$ is not parallel to $[u_4, u_5], ...,$ ($[v_n, v_1]$ is not parallel to $[u_n, u_1]$ if n is a positive even integer).

Figure 17 corresponds to the case n is an even positive integer. Assume that the triangular lateral faces of the polytope $C = conv(C_1, C_2)$ are integrally indecomposable. If C_1 or C_2 is integrally indecomposable then so is C. Note that, as in Remark 4.1.12, for nonparallel hyperplanes H_1 and H_2 in $\mathbb{R}^n$, a similar result holds.

(4) Consider Figure 18. Let $n \geq 4$ be an integer. Let
$C_1 = conv(v_1, v_2, v_3, ..., v_n)$, $C_2 = conv(u_1, u_2, u_3, ..., u_n)$, and
$C_3 = conv(w_1, w_2, w_3, ..., w_n)$ be integral polytopes lying on different parallel hyperplanes as shown in Figure 18. Consider the integral polytope $C = conv(C_1, C_2, C_3)$. Assume that

(i) $[v_1, v_2]$ is not parallel to $[u_1, u_2]$, $[v_3, v_4]$ is not parallel to $[u_3, u_4], ...,$ ($[v_{n-1}, v_n]$ is not parallel to $[u_{n-1}, u_n]$ if n is a positive even integer),

(ii) $[u_1, u_2]$ is not parallel to $[w_1, w_2]$, $[u_3, u_4]$ is not parallel to $[w_3, w_4], ...,$ ($[u_n, u_1]$ is not parallel to $[w_n, w_1]$ if n is a positive odd integer).

Also suppose that the lateral triangular faces of C are integrally indecomposable. Then, C is integrally indecomposable if C_1 or C_2 is integrally indecomposable.

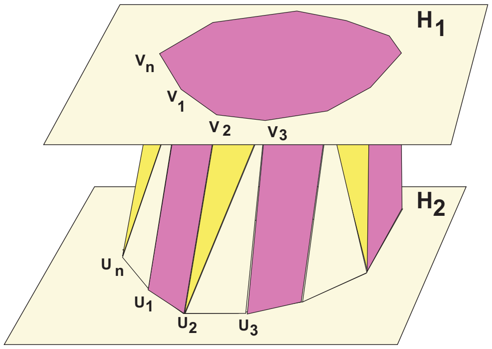


Figure 17

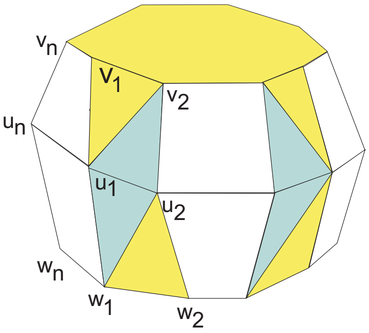


Figure 18

(5) Consider the polytope P in Figure 19. P is in the type of the polytope of Example 4.2.2, (4). Therefore, the same result holds in this case also. Furthermore, in this case P lies inside a pyramid. Therefore, if the integral polytope

$$C_3 = conv(w_1, w_2, ..., w_n)$$

is integrally indecomposable then P is integrally indecomposable by [G1, Theorem 4.11].

(6) Consider Figure 20. In order to have another example of integrally indecomposable polytope Q, we take an extra integral point v_0 and form the integral polytope $Q = conv(C, v_0)$ where $C = conv(C_1, C_2, C_3)$ is the polytope considered in Example 4.2.2, (4). Suppose that the lateral colored triangular faces of Q are integrally indecomposable. If the polytope

$$C_3 = conv(w_1, w_2, ..., w_n)$$

is integrally indecomposable then so is Q. Note that Q may not lie inside a pyramid.

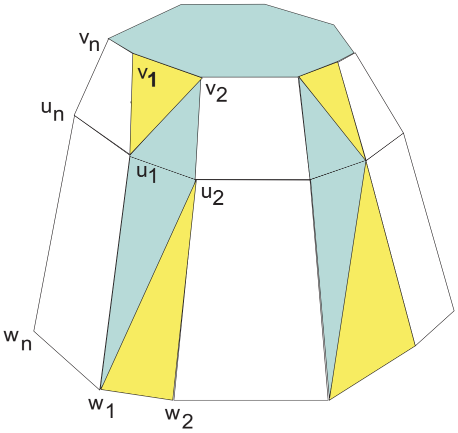


Figure 19

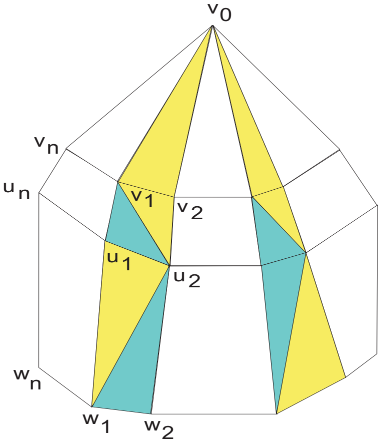


Figure 20

Note that in Example 4.2.2, (1), (2), (3), (4), (5) it is impossible to find a strong chain of homothetically indecomposable faces joining any two distinct vertices of the related polytopes and hence, Theorem 4.1.3 is not applicable. Theorem 4.1.3 may not be applicable also for the polytope Q in Example 4.2.2, (6). We shall later give some numerical examples in Example 4.2.5.

Corollary 4.2.3 *If all 2-dimensional faces of a polytope P in $\mathbb{R}^n$ are integrally indecomposable, then so is P.*

Proof: Let $Q = conv(q_1, ..., q_m)$ be a summand of $P = conv(p_1, ..., p_m)$, where to have the same number of vertices we allow the repetition of vertices of Q. Consider any 2-dimensional face $F_P(u) = conv(p_i, p_{i+1}, ..., p_{j-1}, p_j) = P \cap H_P(u)$ of P, which is formed by the intersection of P with a supporting hyperplane $H_P(u)$ of P having normal vector $u \in \mathbb{R}^n$. Then, since $F_P(u)$ is integrally indecomposable, the face $F_Q(u) = conv(q_i, q_{i+1}, ..., q_{j-1}, q_j) = Q \cap H_P(u)$ of Q must be of the form $F_Q(u) = F_P(u) + v$ for some nonzero vector $v \in \mathbb{R}^n$. Thus, any edge $[q_r, q_{r+1}]$ of Q must be of the form $[q_r, q_{r+1}] = [p_r, p_{r+1}] + v$.

Hence, $q_r = p_r + v$ and $q_{r+1} = p_{r+1} + v$. Since any two edges E, E' of P can be joined by a strong chain of integrally indecomposable faces $F_0, ..., F_s$, where $E \subset F_0, ..., E' \subset F_s$ and $F_i \cap F_{i+1}$ is a line segment, we deduce that $q_i = p_i + v$ for all $i, = 1, ..., m$. So, $Q = P + v$. Consequently, P is integrally indecomposable. $\square$

Theorem 4.2.4 *If P is an integral polytope having a strongly connected family of integrally indecomposable faces that touches each of its facets then it is integrally indecomposable.*

Proof: We can consider an n-dimensional polytope P in $\mathbb{R}^n$, which has a strongly connected family $\mathfrak{F}$ of integrally indecomposable faces touching every facet of P. We can express P as

$$P = \{x \in \mathbb{R}^n : x \cdot u_i \leq h_P(u_i), \quad i = 1, ..., m\}$$

where $u_1, ..., u_m$ are the outer normal vectors to the facets of P having supporting functions $h_P(u_i) = sup_{x \in P}(x \cdot u_i)$ and the supporting hyperplanes $H_P(u_i) = \{x \in \mathbb{R}^n : x \cdot u_i = h_P(u_i)\}$.

Let us suppose that $P = Q + R$ for some integral polytopes Q, R in $\mathbb{R}^n$. Now, consider any strong chain $F_0, F_1, ..., F_k \in \mathfrak{F}$ of integrally indecomposable faces of P. Let G_j be the face of Q corresponding to F_j, i.e. $F_j = G_j + H_j$ for some face H_j of R. Since G_j is a summand of the integrally indecomposable face F_j, there exists a vector $t_j \in \mathbb{R}^n$ such that $G_j = F_j + t_j$. Since $dim(F_{j-1} \cap F_j) \geq 1$ for each j, we see that $t_{j-1} = t_j$. Therefore, for any strongly connected family $\mathfrak{F}$ of integrally indecomposable faces of P, we have a vector $t \in \mathbb{R}^n$ such that, if G is the face of Q corresponding to $F \in \mathfrak{F}$ then $G = F + t$.

By the hypothesis of our theorem, the family $\mathfrak{F}$ touches every facet of P. If $F_i = F_P(u_i)$ is such a facet then it has a vertex a lying in some face $F_P(v) \in \mathfrak{F}$.

The corresponding vertex b of Q lies in $F_Q(v)$. Hence, we have $b = a + t$. By considering the support function h_Q of Q, we have $h_Q(u_i) = b \cdot u_i = (a+t) \cdot u_i = a \cdot u_i + t \cdot u_i = h_P(u_i) + t \cdot u_i = h_{P+t}(u_i)$ for $i = 1, ..., m$. As a result, $Q = P + t$, showing that P is integrally indecomposable. $\square$

Example 4.2.5 (i) Numeric example for Theorem 4.1.3:
Let us consider the polytopes
$C_1 = conv((0, 10, 0), (15, 0, 0), (30, 0, 0), (35, 10, 0), (35, 28, 0),$
$(32, 40, 0), (16, 40, 0), (0, 26, 0)),$
$C_2 = conv((5, 12, 10), (14, 3, 10), (27, 3, 10), (33, 9, 10), (33, 24, 10),$
$(28, 3, 10), (16, 33, 10), (5, 26, 10)),$
$C_3 = conv((12, 14, 20), (17, 7, 20), (25, 7, 20), (30, 10, 20), (30, 20, 20),$
$26, 23, 20), (18, 23, 20), (12, 22, 20))$
lying in the planes $z = 0$, $z = 10$ and $z = 20$ respectively. Then, the polytope $C = conv(C_1, C_2, C_3, (21, 15, 30))$, which is of type of the polytope in Example 4.2.2, (6), is integrally indecomposable by Theorem 4.1.3 since C has a strong chain of triangular faces joining any two of its vertices and $gcd((21, 15, 30) - (12, 14, 20)) = gcd(9, 1, 10) = 1$.

(ii) Numeric example for item (5) of Example 4.2.2:
Now, take the polytopes
$P_1 = conv((0, 10, 0), (15, 0, 0), (30, 12, 0), (12, 36, 0)),$
$P_2 = conv((5, 14, a), (14, 6, a), (24, 14, a), (11, 12, a)),$
$P_3 = conv((8, 14, b), (15, 10, b), (20, 14, b), (11, 18, b))$
located in the planes $z = 0$, $z = a$ and $z = b$ respectively with a, b positive integers such that $b \geq a$. P_3 is an integrally indecomposable quadrangle since its all edges are primitive. We see that the polytope $P = conv(P_1, P_2, P_3)$ is integrally indecomposable by Theorem 4.2.1 (also by Theorem 4.2.4) since it

has a strongly connected family $\mathcal{F}$ of integrally indecomposable faces which connects any two vertices of P (which touches each facet of P.) Actually, this strongly connected family of faces is
$\mathcal{F} = \{conv((8, 14, b), (15, 10, b), (20, 14, b), (11, 18, b)),$
$conv((0, 10, 0), (15, 0, 0), (14, 6, a)), conv((0, 10, 0), (14, 6, a), (5, 14, a))$
$conv((5, 14, a), (14, 6, a), (15, 10, b), conv((5, 14, a), (15, 10, b), (8, 14, b)),$
$conv((30, 12, 0), (12, 36, 0), (24, 14, a)), conv((12, 36, 0), (11, 22, a), (24, 14, a)),$
$conv((24, 14, a), (11, 22, a), (20, 14, b), conv((11, 22, a), (20, 14, b), (11, 18, b))\}.$

(iii) Numeric example for item (4) of Example 4.2.2:
Consider the polytopes
$Q_1 = conv((5, 14, c), (14, 6, c), (24, 14, c), (11, 12, c)),$
$Q_2 = conv((0, 10, d), (15, 0, d), (30, 12, d), (12, 36, d)),$
$Q_3 = conv((8, 14, e), (15, 10, e), (20, 14, e), (11, 18, e))$
placed in the planes $z = c$, $z = d$ and $z = e$ respectively with c, d, e positive integers such that $e > d > c$. Q_3 is an integrally indecomposable quadrangle since its all edges are primitive. We see that the polytope $Q = conv(Q_1, Q_2, Q_3)$ is integrally indecomposable by Theorem 4.2.1 (also by Theorem 4.2.4) since it has a strongly connected family $\mathcal{F}$ of integrally indecomposable faces which connects any two vertices of Q (which touches each facet of Q.) The suitable strongly connected family of integrally indecomposable faces is
$\mathcal{F} = \{conv((8, 14, e), (15, 10, e), (20, 14, e), (11, 18, e)),$
$conv((0, 10, d), (15, 0, d), (14, 6, c)), conv((0, 10, d), (14, 6, c), (5, 14, c))$
$conv((5, 14, c), (14, 6, c), (15, 10, e), conv((5, 14, c), (15, 10, e), (8, 14, e)),$
$conv((30, 12, d), (12, 36, d), (24, 14, c)), conv((12, 36, d), (11, 22, c), (24, 14, c)),$
$conv((24, 14, c), (11, 22, c), (20, 14, e), conv((11, 22, c), (20, 14, e), (11, 18, e))\}.$

The following theorem is a consequence of Theorem 4.2.4.

Theorem 4.2.6 *Let A and B be polytopes such that $C = conv(A \cup B)$ with $dim(C) = dim(A)+dim(B)+1$. Moreover, suppose also that a_i, a_{i+1}, a are vertices of A, such that a_i and a_{i+1} are adjacent, and b is a vertex of B satisfying $gcd(b-a_i, b-a_{i+1}) = 1$ or $gcd(b-a) = 1$. Then C is integrally indecomposable.*

Proof: Every facet of $C = conv(A \cup B)$ contains either A or B. Therefore, if a_i, a_{i+1}, a are vertices of A, a_i and a_{i+1} are being adjacent, and b is a vertex of B with $gcd(b-a_i, b-a_{i+1}) = 1$ or $gcd(b-a) = 1$ then the face $T = conv(a_i, a_{i+1}, b)$, which is an integrally indecomposable triangle, or the face $L = conv(a, b)$, which is an integrally indecomposable line segment, meets every facet of C. Therefore, by Theorem 4.2.4, taking $\mathcal{F} = \{T\}$ or $\mathcal{F} = \{L\}$, C is integrally indecomposable. $\square$

Remark 4.2.7 There are several criteria in the literature about the homothetic decomposability of polytopes. But, since we are trying to find the families of absolutely irreducible polynomials directly, our aim is to find integrally indecomposable polytopes. Therefore, we do not go into details of such interesting facts. For example, the following results are due to Smilansky [Sm2]:

(1) If a 3-dimensional polytope P has more vertices than facets, then P is homothetically decomposable.

(2) If a 3-dimensional polytope P has no more than three triangular facets, then P is homothetically decomposable.

(3) If all the facets of a 3-dimensional polytope P are homothetically decomposable, then so is P. $\square$

Chapter 5

ON ABSOLUTE IRREDUCIBILITY OF SOME POLYNOMIALS OVER LARGE CHARACTERISTICS

In this chapter, motivated by a conjecture of McGuire and Wilson given in [MW], we show absolute irreducibility of some classes of homogeneous polynomials for sufficiently large characteristics.

5.1 INTRODUCTION

First we recall the conjecture of McGuire and Wilson.

Conjecture: Let t be a positive odd integer satisfying

$t \equiv 1 \pmod 4$,

$t \neq 2^i + 1$ for any integer i, i.e. $t \notin \{1, 3, 5, 9, 17, ...\}$,

$t \neq 2^{2i} - 2^i + 1$ for any integer i, i.e. $t \notin \{1, 3, 13, ...\}$.

Then the homogeneous polynomial

$$g(x,y,z) = \frac{x^t + y^t + z^t + (x+y+z)^t}{(x+y)(x+z)(y+z)}$$

is absolutely irreducible over the finite field $\mathbb{F}_2$, i.e. irreducible over every algebraic extension of $\mathbb{F}_2$.

In Section 5.2, first we have constructed three kinds of polynomial classes. Then, by making a suitable combination of the methods presented in [R2], [GR] and [G1], we have shown that these three classes of polynomials are absolutely irreducible over the finite fields $\mathbb{F}_p$ for the prime numbers $p > C_i$ for some certain constant numbers C_i.

5.2 MAIN OBSERVATION AND RESULT

Instead of considering the polynomial $g(x,y,z)$, we think of the polynomials

$$g_1(x,y,z) = \frac{x^t - y^t - z^t + (x-y-z)^t}{(x-y)(x-z)} \quad \text{for any even positive integer } t \geq 4,$$

$$g_2(x,y,z) = \frac{x^t - y^t - z^t + (-x+y+z)^t}{(x-y)(x-z)} \quad \text{for any even positive integer } t \geq 4,$$

$$g_3(x,y,z) = \frac{x^t - y^t - z^t + (-x+y+z)^t}{(x-y)(x-z)(y+z)} \quad \text{for any odd positive integer } t \geq 5$$

over the finite field $\mathbb{F}_p$ with large characteristic p.

Remark 5.2.1 For a polynomial

$$f(x,y) = \sum_{i,j} a_{ij} x^i y^j \in \mathbb{Z}[x,y],$$

we write $deg_x(f)$ for its degree in x, $deg_y(f)$ for its degree in y, $deg(f)$ for its total degree and $H(f)$ for its height (which is defined as $max_{i,j}\{\mid a_{ij} \mid\}$).

In order to give our result, we shall use the following lemma.

Lemma 5.2.2 *Let* $f(x_1, x_2, ..., x_n) \in \mathbb{Z}[x_1, x_2, ..., x_n]$ *be a homogeneous polynomial over* $\mathbb{Q}$. *Then* $f(x_1, x_2, ..., x_n)$ *is absolutely irreducible if and only if* $f(x_1, x_2, ..., x_{n-1}, 1)$ *is absolutely irreducible.*

Proof: If $f(x_1, x_2, ..., x_n)$ is reducible, $f(x_1, x_2, ..., x_{n-1}, 1)$ is also reducible. Converse follows from the equality

$$f(x_1, x_2, ..., x_n) = f(\frac{x_1}{x_n}, \frac{x_2}{x_n}, ..., \frac{x_{n-1}}{x_n}, 1)x_n^{deg(f)}$$

while $f(x_1, x_2, ..., x_n)$ is homogeneous. □

Remark 5.2.3 We observe that the polynomials $g_k(x, y, x)$ have polygonal Newton polytopes. Actually, Newton polytope of the polynomials $g_1(x, y, z)$ and $g_2(x, y, z)$ is the triangle $conv((t-2, 0, 0), (0, t-2, 0), (0, 0, t-2))$ lying in the plane $x+y+z = t-2$ for each values of t. And, $g_3(x, y, z)$ has also polygonal Newton polytope, which is the triangle $conv((t-3, 0, 0), (0, t-3, 0), (0, 0, t-3))$, lying in the plane $x + y + z = t - 3$.

Now, we construct the polynomials

$$f_k(x, y) = g_k(x, y, 1), \qquad k = 1, 2, 3.$$

As a result of Remark 5.2.3, $f_1(x, y)$ and $f_2(x, y)$ have Newton polytopes

$$conv((0, 0), (t-2, 0), (0, t-2)$$

which is an integrally decomposable triangle. And, $f_3(x, y)$ has the Newton polytope

$$conv((0, 0), (t-3, 0), (0, t-3)$$

which is also an integrally decomposable triangle.

Let us assume that $deg_x(f_k) = m_k$, $deg_y(f_k) = n_k$ and $H(f_m) = H_m$.

We form the Ruppert bounds, achieved in [R2], B_{f_k} as

$$B_{f_k} = [m_k(n_k+1)n_k^2 + (m_k+1)(n_k-1)m_k^2]^{m_kn_k+(n_k-1)/2} \cdot H_k^{2m_kn_k+n_k-1}.$$

Then, we also form the Gao-Rodrigues bounds for each polynomial, attained in [GR],

$$C_{f_k} = (\sqrt{m_k^2+n_k^2} \cdot \parallel f_k \parallel_2)^{2t_k-3}$$

where t_k is the number of integral points in the Newton polytope P_{f_k} of f_k, and $\parallel f_k \parallel_2 = \sqrt{\sum_{i,j} a_{kij}^2}$ is the Euclidean norm of f_k.

Now, we can give our result.

Corollary 5.2.4 *Let $f_k(x,y) = g_k(x,y,1) \in \mathbb{Z}[x,y]$, $k = 1,2,3$ be absolutely irreducible over $\mathbb{Q}$. Then $f_k(x,y)$ are also absolutely irreducible over $\mathbb{F}_p$, by [R2] and [GR], for the prime numbers p such that*

$$p > B_{f_k} \quad or \quad p > C_{f_k},$$

Consequently, the polynomials $g_k(x,y,z)$ are absolutely irreducible over the finite fields $\mathbb{F}_p$ by Lemma 5.2.2.

Example 5.2.5 *(1)* Consider the polynomial

$$g_3(x,y,z) = \frac{x^5-y^5-z^5+(-x+y+z)^5}{(x-y)(x-z)(y+z)} = 5(x^2+y^2+z^2-xy-xz+yz).$$

Then $g_3(x,y,z)$ is reducible over $\mathbb{Z}$ if and only if the polynomial

$$q(x,y,z) = x^2+y^2+z^2-xy-xz+yz$$

reducible over $\mathbb{Z}$. So, we can work on the polynomial $q(x, y, z)$ instead of $g_3(x, y, z)$.

We have $deg_x(q(x, y, 1)) = deg_y(q(x, y, 1)) = 2$, $H(q(x, y, 1)) = 1$. Moreover, Newton polytope of $q(x, y, 1)$ is the triangle $conv((2, 0), (0, 2), (0, 0))$ which contains six integral points. So, we have $t_3 = 6$ for the Gao-Rodrigues bound. Furthermore, $q(x, y, 1) = x^2 + y^2 + 1 - xy - x + y$ is absolutely irreducible over $\mathbb{Q}$.

Consequently, $g_3(x, y, z)$ is absolutely irreducible over $\mathbb{F}_p$ if p is a prime number such that

$$p > 36^4 6 = 10077696 \qquad \text{or} \qquad p > (4\sqrt{3})^9 = 36777784$$

(2) Consider the polynomial

$$f(x, y, z) = \frac{x^7 - y^7 - z^7 + (-x + y + z)^7}{(x - y)(x - z)(y + z)}$$

$$= 7x^4 - 14x^3y - 14x^3z + 21y^2x^2 + 35x^2zy + 21x^2z^2 - 14xy^3 - 35xy^2z$$
$$- 35xyz^2 - 14xz^3 + 7y^4 + 14y^3z + 21y^2z^2 + 14yz^3 + 7z^4.$$
$$= 7(x^4 - 2x^3y - 2x^3z + 3y^2x^2 + 5x^2zy + 3x^2z^2 - 2xy^3 - 5xy^2z$$
$$- 5xyz^2 - 2xz^3 + y^4 + 2y^3z + 3y^2z^2 + 2yz^3 + z^4) = 7g(x, y, z).$$

We have $deg_x(g(x, y, 1)) = deg_y(g(x, y, 1)) = 4$ and $H(g(x, y, 1)) = 5$. Also, Newton polytope of $g(x, y, 1)$ is the polygon $conv((4, 0), (0, 4), (0, 0))$ which contains 15 integral points. Moreover, $g(x, y, 1)$ is absolutely irreducible over $\mathbb{Q}$.

As a result, by Corollary 5.2.4, $f(x, y, z)$ is absolutely irreducible over $\mathbb{F}_p$ if p is a prime number such that

$$p > 3,607784792 \cdot 10^{72} \qquad \text{or} \qquad p > 6,493603934 \cdot 10^{48}.$$

Note that $f(x, y, z)$ is irreducible over $\mathbb{F}_{11}$ and $\mathbb{F}_{17}$ and reducible over $\mathbb{F}_{13}$. Actually, we have
$f(x, y, z)(mod \quad 13) \equiv 7(x^2 + 5xy + 2x + 3y^2 + 6xz + 11x + 11yz + 9z^2)$
$(x^2 + 6xy + 6x + 9y^2 + 5xz + 7x + 11yz + 3z^2)$.

Remark 5.2.6 Note that the polytope method presented in [G1] does not work about the absolute irreducibility of the polynomials $g_k(x, y, z)$, for $k = 1, 2, 3$. Because, these three polynomials have integrally decomposable Newton polytopes, which are integrally decomposable triangles in $\mathbb{R}^3$.

Remark 5.2.7 Actually, we had considered to take the homogeneous polynomials

$$f_k(x, y) = g_k(x, y, 1) + px^{deg(g_k+1)}y^{deg(g_k+1)} \qquad k = 1, 2, 3$$

for a suitable prime number p. These polynomials have integrally indecomposable Newton polytopes which are quadrangles in the plane $\mathbb{R}^2$. Hence, they are absolutely irreducible over the field of rational numbers $\mathbb{Q}$. Thus,

$$f_k(x, y) \ \ (mod \ \ p) = g_k(x, y, 1)$$

would be absolutely irreducible over the finite field $\mathbb{F}_p$. Consequently, by Lemma 5.2.2, $g_k(x, y, z)$ would be absolutely irreducible over $\mathbb{F}_p$.

But, this idea did not work since the prime numbers , achieved by Ruppert and Gao, depend on the height of the polynomials. As a result, if we can find a suitable large prime number p which does not depend on the height of the polynomials, then we will be able to solve the related conjecture over large characteristics completely.

Chapter 6

PROBABILITY OF THE POLYNOMIALS TO BE IRREDUCIBLE BY THE POLYTOPE METHOD

In this chapter, being motivated by the method, which is about to determine the probability of the polynomials to be irreducible by Eisenstein's criterion in a family of polynomials in $\mathbb{Z}[x]$, presented in the paper [D], we shall introduce how to determine the probability showing the ratio of irreducible polynomials by the polytope method in some families of polynomials over arbitrary fields. In order to find this ratio, we shall work with the exponents of terms of polynomials in this family.

First, we start with the simplest forms of polynomials having Newton polytopes as line segments. Then we examine some polynomials with two variables. Of course, we can give infinitely many examples in any number of variables.

Given any family of polynomials $S = \{f_i(x_1, ..x_n) \in F[x_1, ..., x_n] \mid i \in I\}$ over any field F, we use the notation

$$P(A, I, P) = \frac{\mid K \mid}{\mid L \mid}$$

to mean the chance that a random polynomial $f(x_1, ..., x_n) \in F[x_1, ..., x_n]$ in S is absolutely irreducible by the polytope method, where K is the set of all exponents of polynomials which are absolutely irreducible by the polytope method and L is the set of all possible exponents which form the Newton polytopes of all polynomials in S.

Beside the Euler-phi function ϕ, we also need to define the following set.

Definition 6.0.8 *Let M and N be positive integers with $M \leq N$. Then for any positive integer i, we define the set*

$$S_{M-N}(i) = \{x \in \mathbb{Z} \mid \quad M \leq x \leq N, \quad gcd(x, i) = 1\}.$$

Throughout this chapter, F^* stands for the set of all nonzero elements for a field F.

Example 6.0.9 Let $\{ax^N + by^m \mid 1 \leq m \leq N\}$ be a set of family of polynomials over an arbitrary field F with $a, b \in F^*$ and $N \geq 1$ a given integer. Then, we have

$$P(A, I, P) = \frac{\phi(N)}{N}.$$

Example 6.0.10 Consider the following set of family of polynomials

$$\{ax^n + by^m + \sum c_{ij}x^iy^j \mid a, b \in F^*, c_{ij} \in F, mi + nj = mn\}$$

where N and M are given positive integers such that $1 \leq n \leq N$, $1 \leq m \leq M$ with $N \leq M$. Then

$$P(A, I, P) = \frac{\sum_{i=1}^{N} \phi(i) + \sum_{i=2}^{N} \phi(i)}{NM} = \frac{2\sum_{i=1}^{N} \phi(i) - 1}{NM}$$

$$= \frac{\sum_{i=1}^{N} \mid S_{1-N}(i) \mid}{NM} \quad if \quad N = M,$$

and

$$P(A, I, P) = \frac{2\sum_{i=1}^{N} \phi(i) + \sum_{i=N+1}^{M} \mid S_{1-N}(i) \mid -1}{NM}$$
$$= \frac{\sum_{i=1}^{N} \mid S_{1-M}(i) \mid}{NM} \quad if \quad N < M.$$

Example 6.0.11 Consider the set of polynomials

$$\{ax^n + by^m + cx^u y^v + \sum c_{ij}x^i y^j \mid a, b, c \in F^*, c_{ij} \in F, 1 \leq n \leq N, 1 \leq m \leq M\}$$

where N,M,A,B,C,D are given positive integers satisfying

$$A \leq u \leq B, \quad C \leq v \leq D \quad \text{and} \quad Mu + Nv > MN.$$

Without loss of generality, assume that $N \leq M < C \leq A \leq B \leq D$. By the polytope method, a polynomial $f = a_1x^{e_1} + b_1y^{e_2} + c_1x^{e_3}y^{e_4} + \sum c_{ij}x^i y^j$ in this set is absolutely irreducible over F if $gcd(e_1, e_2, e_3, e_4) = 1$. Hence, we have $P(A, I, P) = \Big[r + \sum_{i=1}^{N} \Big(\mid S_{1-M}(i) \mid + \mid S_{A-B}(i) \mid + \mid S_{C-D}(i) \mid \Big) + \sum_{i=1}^{M} \Big(\mid S_{A-B}(i) \mid + \mid S_{C-D}(i) \mid \Big) + \sum_{i=A}^{B} \mid S_{C-D}(i) \mid \Big] / \Big[NM(B-A+1)(D-C+1)\Big]$ where r is the cardinality of the set of triple and quad relatively prime exponents in the related intervals.

Bibliography

[A] Adleman L. M. *The function field sieve*, Algorithmic Number Theory (Ithaca, NY, 1994), 108-121, Lecture Notes in Comput. Sci., 877, Springer, Berlin, 1994.

[D] Dubickas A. *Polynomials Irreducible by Eisenstein's Criterion*, AAECC **14** (2003), 127-132.

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

[G1] Gao S. *Absolute irreducibility of polynomials via Newton polytopes*, Journal of Algebra **237** (2001), No.2 501-520.

[G2] Gao S. *Decomposition of Polytopes and Polynomials*, Discrete and Computational Geometry **26** (2001), no. 1, 89-104.

[GR] Gao S. and Rodrigues V. M. *Irreducibility of polynomials modulo p via Newton polytopes*, Journal of Number Theory, **101** (2003), 32-47.

[Gr] Grümbaum B. *Convex Polytopes*, London, New York, Sydney, Interscience Publications, 1967.

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

[K] Kallay M. *Indecomposable Polytopes*, Israel Journal of Mathematics, **41** (1982), no. 3, 235-243.

[LN] Lidl R. and Niederreiter H. *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison-Wesley Publ. Co. 1983.

[L] Lipkovski A. *Newton Polyhedra and Irreducibility*, Math. Z., **199** (1998), no. 2, 119-127.

[MW] McGuire G. and Wilson R.M. *Double-Error-Correcting Cyclic Codes and Absolutely Irreducible Polynomials over GF(2)*, Journal of Algebra, **178** (1995), 665-676.

[Mc] Mcmullen P. *Indecomposable Convex Polytopes*, Israel Journal of Mathematics, **58** (1987), no. 3, 321-323.

[Me] Meyer W. *Indecomposable Polytopes*, Trans. Amer. Math. Soc, **190** (1974), 77-86.

[O1] Ostrowski A.M. *On multiplication and factorization of polynomials I*, Lexicographic orderings and extreme aggregates of terms, Aequationes Math. **13** (1975), 201-228.

[O2] Ostrowski A. M. *On multiplication and factorization of polynomials II*, Irreducibility discussion, Aequationes Math. **14** (1976), 1-32.

[R1] Ruppert W. M. *Reducibility of Cubic Polynomials mod p*, Journal of Number Theory, **57** (1996), 198-206.

[R2] Ruppert W. M. *Reducibility of Polynomials $f(x, y)$ Modulo p*, Journal of Number Theory, **77** (1999), 62-70.

[Sc] Schneider R. *Convex Bodies: The Brunn-Minkowski Theory*, Encyclopedia of Mathematics and its Applications, **44**, Cambridge University Press, Cambridge, 1993.

[Sh] Shephard G. C. *Decomposable Convex Polyhedra*, Mathematika, **10** (1963), 89-95.

[Si] Silverman R. *Decomposition of Plane Convex Sets, Part 1*, Pacific Journal of Mathematics, **47** (1973), no. 2, 521-530.

[Sm1] Smilansky Z. *An Indecomposable Polytope All of Whose Facets Are Decomposable*, Mathematika, **33** (1986), no. 2, 192-196.

[Sm2] Smilansky Z. *Decomposability of Polytopes and Polyhedra*, Geometriae Dedicata, **24** (1987), no. 1, 29-49.

[St] Stichtenoth H. *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993. of Mathematics, **41** (1982), no. 3, 235-243.

[Sz] Szönyi T. *Some Applications of Algebraic Curves in Finite Geometry and Combinatorics*, Surveys in Combinatorics, 1997 (R. A. Railey, Ed.), London Mathematical Society Lecture Notes Series 241, Cambridge University Press, 1997.

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