

ABSOLUTE IRREDUCIBILITY OF BIVARIATE POLYNOMIALS VIA POLYTOPE METHOD

FATİH KOYUNCU

ABSTRACT. For any field F , a polynomial $f \in F[x_1, x_2, \dots, x_k]$ 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 results giving new integrally indecomposable classes of polygons. Consequently, we have some criteria giving many types of absolutely irreducible bivariate polynomials over arbitrary fields.

1. Introduction

The classes of absolutely irreducible polynomials are very important in many areas such as coding theory, combinatorics, permutation polynomials. There are some irreducibility criteria of polynomials like Eisenstein's criterion, Eisenstein-Dumas criterion. Another absolute irreducibility criterion for polynomials in literature is known as the Newton polygon method. Recently, the Newton polygon method has been generalized by Gao in [1, 2] as Newton polytope method for multivariate polynomials.

We give some definitions and recall some well-known facts in the rest of this section. Our new results are obtained in Section 2.

Let \mathbb{R}^n denote the n -dimensional Euclidean space and S be a subset of \mathbb{R}^n . The smallest convex set containing S , denoted by $\text{conv}(S)$, is called the *convex hull* of 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 [7, Proposition 2.2].

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

Received June 23, 2010; Revised January 18, 2011.

2010 *Mathematics Subject Classification.* 51E12, 52B12.

Key words and phrases. absolute irreducibility, bivariate polynomials, integral polygons, integral indecomposability, polytope method.

Definition 1.1. 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 .

If P , Q and R are polytopes in \mathbb{R}^n with $P = Q + R$, then Q and R are called *summands* of P .

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

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

We can think of an exponent vector (e_1, e_2, \dots, 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, \dots, e_n) with $c_{e_1 e_2 \dots e_n} \neq 0$.

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 [5].

Lemma 1.2. *Let $f, g, h \in F[x_1, \dots, x_n]$ with $f \neq 0$ and $f = gh$. Then $P_f = P_g + P_h$.*

Proof. See, for example, the proof of [1, Lemma 2.1]. □

As a direct result of Lemma 1.2, we have the following corollary which is an *irreducibility criterion* for multivariate polynomials over arbitrary fields.

Corollary 1.3. *Let F be any field and f a nonzero polynomial in $F[x_1, \dots, x_n]$ 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. See [1, page 5]. □

For a polynomial $f \in F[x_1, x_2, \dots, x_n]$, if P_f is integrally indecomposable, we say that f is *absolutely irreducible over F by the polytope method*. According to this method, a polynomial $f \in F[x_1, \dots, x_k]$ is absolutely irreducible over a field F if its Newton polytope is integrally indecomposable. In [1, 2, 3] many classes of integrally indecomposable polytopes were constructed and hence, many families of absolutely irreducible polynomials were found. A necessary and sufficient condition for integral indecomposability of triangles was found in [1]. For arbitrary n -gons, it seems difficult to give a necessary and sufficient condition for integral indecomposability.

In this paper we study integral decomposability of polygons in the Euclidean space \mathbb{R}^2 . We find new criteria for integrally indecomposable polygons different from the ones in [1, 2] and hence have new infinite families of absolutely irreducible bivariate polynomials over an arbitrary field F . In particular, we obtain a necessary and sufficient condition for integral indecomposability of arbitrary quadrangles.

Notation: For any element $v = (a_1, \dots, a_n)$ of \mathbb{Z}^n we shall write $\gcd(v)$ to mean $\gcd(a_1, \dots, a_n)$, i.e., the greatest common divisor of all the components of v . Similarly, for several vectors v_1, \dots, v_k in \mathbb{Z}^n , by writing $\gcd(v_1, \dots, v_k)$ we mean the greatest common divisor of all the components of the vectors v_1, \dots, v_k . For any points $v_1, v_2 \in \mathbb{Z}^n$, $[v_1, v_2]$ refers to the line segment from v_1 to v_2 , $\overrightarrow{v_1 v_2}$ stands for the vector from v_1 to v_2 and $\|v_1 v_2\|$ 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 .

2. Integrally indecomposable polygons

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 $v_0, v_1, \dots, v_{n-1}, v_n = v_0$ 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 $\{c_i e_i\}_{1 \leq i \leq n}$, 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 $\sum_{i=1}^n c_i e_i = (0, 0)$.

Lemma 2.1. *Let P be an integral polygon having edge sequence $\{c_i e_i\}_{1 \leq i \leq n}$ 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 an edge sequence of the form $\{d_i e_i\}_{1 \leq i \leq n}$, $0 \leq d_i \leq c_i$, where $\sum_{i=1}^n d_i e_i = (0, 0)$.*

Proof. See, e.g., the proof of [2, Lemma 13] or [4, Lemma 2.11]. □

Remark 2.2. According to Lemma 2.1, 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 are integral and they

have no parallel edges. We call an integral summand of a polygon a *trivial summand* if it is a line segment or an integral point.

By the decomposition property of polytopes, we know that if P, Q and R are convex polygons in \mathbb{R}^n with $P = Q + R$, then every edge of P can be written uniquely as the sum of an edge of Q and an edge of R , perhaps one of them being a point. Conversely, any edge of Q or R is a summand of precisely one edge of P . See [2, Lemma 5] and [2, Corollary 6] for detail.

In this study, we get some new integral indecomposability criteria for the polygons in \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 shall give direct proofs to determine the integrally indecomposable line segments and triangles.

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

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

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 [1, Lemma 4.1] has a similar statement, and here we give a different proof.

Proposition 2.3. *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

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

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

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

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. \square

Corollary 2.4. *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 $\|b_1 b_2\|, \|c_1 c_2\| > 0$. 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. \square

Example 2.5 ([6, Theorem IX]). A two-term polynomial

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

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

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.

Triangles

In order to decompose an integral triangle $\text{conv}(v_1, v_2, v_3)$ 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

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

Let $T = \text{conv}(v_1, v_2, v_3)$ be an integral triangle in \mathbb{R}^n . We can form edge vectors of T as $E_1 = c_1 e_1 = v_2 - v_1$, $E_2 = c_2 e_2 = v_3 - v_2$ and $E_3 = c_3 e_3 = v_1 - v_3$ 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 2.2, all convex integral summands of T must be triangular and any convex integral summand S of T must have edges of the form $E'_1 = d_1 e_1$, $E'_2 = d_2 e_2$, $E'_3 = d_3 e_3$, 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

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

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 $T' = \text{conv}(0, v_2 - v_1, v_3 - v_1)$ is integral. Hence, $T = v_1 + d \cdot (\frac{1}{d}T')$.

As a result, we have proved the following proposition.

Proposition 2.6. *A triangle $\text{conv}(v_1, v_2, v_3)$ in \mathbb{R}^n is integrally indecomposable if and only if*

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

By Proposition 2.6, we see that a triangle in \mathbb{R}^n with integral vertices v_1, v_2, v_3 is integrally indecomposable if

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

For example, the polynomial

$$f = a_1 x^{13} + a_2 y^9 + a_3 x^2 y + a_4 x^4 y^4 + a_5 x^5 y^3 + a_6 x^6 y^2 + a_7 x^3 y^4 + \sum c_{ij} x^i y^j$$

having Newton polytope $P_f = \text{conv}((13, 0)(0, 9)(2, 1))$ is absolutely irreducible over any field F since P_f is an integrally indecomposable triangle as $\text{gcd}(13, 9) = 1$.

Quadrangles

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

By Remark 2.2, 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 , we call the common edges of Q and T a *base edge* of Q . So, any quadrangle Q has exactly two base edges. Observe that base edges of Q are adjacent. Therefore, in this subsection we refer to an arbitrary quadrangle $Q = \text{conv}(A, B, C, D)$ lying inside the triangles $T_1 = \text{conv}(A, B, v_1)$ and $T_2 = \text{conv}(B, C, v_2)$ for some points $v_1, v_2 \in \mathbb{R}^2$. See Figure 1.

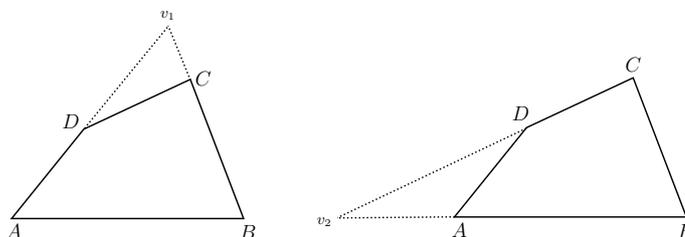


FIGURE 1

We fix how to indicate the corners of a quadrangle Q . In the counterclockwise direction, if Q lies inside the triangles $T_1 = \text{conv}(A, B, v_1)$ and $T_2 = \text{conv}(B, C, v_2)$ with $[A, B]$ and $[B, C]$ being the base edges of Q , then we indicate the vertices of Q as $Q = \text{conv}(A, B, C, D)$. 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 in \mathbb{R}^2 with respect to its base edges.

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 2.1, 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.

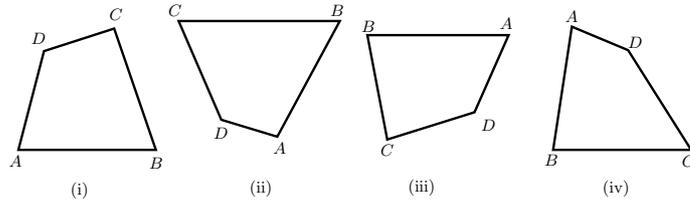
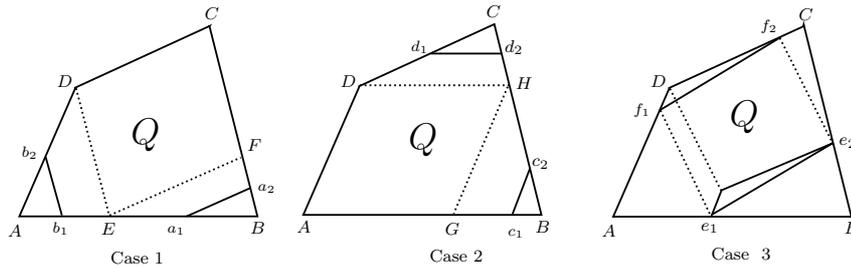


FIGURE 2



Decomposition methods of integral quadrangles

FIGURE 3

- (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 non-trivial integral triangular summands and the condition (C5) corresponds to possible nontrivial integral quadrangular summands of Q . We observe that $(C1) \iff (C4)$ and $(C2) \iff (C3)$.

Now, we give our theorem on quadrangles.

Theorem 2.7. *The quadrangle $Q = \text{conv}(A, B, C, D)$ in Figure 3 is integrally indecomposable if and only if neither (C1), (C2) nor (C5) holds.*

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 2.1, 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 2.1, 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

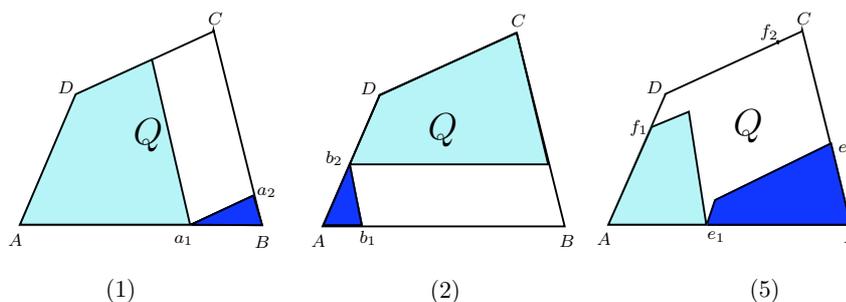
$$\overrightarrow{e_1 e_2} = \overrightarrow{e_1 B} + \overrightarrow{B e_2} = (B - (B - F_1)) + ((B + F_2) - B) = F_1 + F_2,$$

and

$$\overrightarrow{f_1 f_2} = \overrightarrow{f_1 D} + \overrightarrow{D f_2} = (D - (D + F_4)) + ((D - F_3) - D) = -(F_3 + F_4).$$

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

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

As a consequence of Theorem 2.7, using the same terminology of the theorem, we obtain the following result.

Corollary 2.8. *The quadrangle $Q = \text{conv}(A, B, C, D)$ is integrally indecomposable if any of the following cases occurs:*

- (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. (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). The other cases are proved similarly. \square

Remark 2.9. Theorem 2.7 gives a necessary and sufficient condition for integral indecomposability of quadrangles. Note that the case (f) in Corollary 2.8 is also covered by [1, Corollary 4.12]. The cases (a-e) do not directly follow from [1, 2].

The following three propositions are computational consequences of Lemma 2.1. 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 2.1 directly.

Proposition 2.10. *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 2.10, any integral quadrangle Q with the edge sequence $\{3e_1, 2e_2, 2e_3, e_4\}$ is integrally indecomposable if and only if $e_1 + e_2 + e_4 \neq 0$, $e_1 + e_3 + e_4 \neq 0$, $e_1 + e_2 + 2e_3 \neq 0$, $e_1 + 2e_2 + e_3 \neq 0$, $2e_1 + e_2 + e_3 + e_4 \neq 0$. Actually, since we consider quadrangles shaped as in Figure 1 and form the edge sequence of an arbitrary quadrangle with respect to this assumption, by making

vector addition of these related edge vectors, we can easily see that all of these conditions are already satisfied. Hence, Q is integrally indecomposable.

For example, the quadrangle $Q = \text{conv}((6, 0), (14, 4), (4, 20), (0, 3))$ having the edge sequence $\{3(2, -1), 4(2, 1), 2(-5, 8), (-4, -17)\}$ is integrally indecomposable. In fact, Q is integrally indecomposable since it lies in a triangle $\text{conv}((0, 3), (4, 20), v)$ for some point in $v \in \mathbb{R}^2$. So, it is better to find another example for which Corollary 2.8 does not work. We consider the quadrangle

$$Q' = \text{conv}((6, 0), (14, 4), (2, 6), (0, 3))$$

with the edge sequence $\{3(2, -1), 4(2, 1), 2(-6, 1), (-2, -3)\}$. By making vector addition of all edge vectors indicated in Proposition 2.10, we see that Q' is integrally indecomposable. Consequently, every polynomial

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

having Newton polytope $P_f = Q'$ is absolutely irreducible over any field F .

Proposition 2.11. *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 2.11, 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 2.12. *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 2.1.

Conversely, any nontrivial integral summand of Q has an edge sequence $\{c_i e_i\}$ such that $c_1 e_1 + c_2 e_2 + c_3 e_3 + c_4 e_4 = 0$ where $0 \leq c_1, c_2 \leq m - 1$ and $0 \leq c_3, c_4 \leq 1$. Since Q has no parallel edges, we have only two possibilities $(1, 0)$ and $(0, 1)$ for the value of (c_3, c_4) . So, we have two cases to examine:

- (1) $ie_1 + je_2 + e_3 = 0$ with $1 \leq i \leq m - 1$, $1 \leq j \leq m - 1$,
- (2) $ie_1 + je_2 + e_4 = 0$ with $1 \leq i \leq m - 1$, $1 \leq j \leq m - 1$.

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. \square

As an application of Proposition 2.12, we easily get the result of Proposition 2.11 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 $2e_1 + e_2 + e_3 \neq 0$. Since we assume that arbitrary quadrangles are shaped as in Figure 1 and form the edge sequence with respect to this assumption, we see that all of these conditions are already satisfied. Therefore, Q is integrally indecomposable.

As a second example of Proposition 2.12, 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 shape 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 $Q = \text{conv}((0, 4), (8, 0), (12, 8), (3, 9))$ has the edge sequence $\{4(2, -1), 4(1, 2), (-9, 1), (-3, -5)\}$ which satisfies the three conditions at the end of the preceding paragraph. Hence, it is integrally indecomposable.

Now, we give some further numerical examples of Proposition 2.10, Proposition 2.11 and Proposition 2.12.

Example 2.13. (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

$$Q = \text{conv}((0, 8), (10, 0), (8, 18), (3, 15)).$$

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

For example, the polynomial

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

having Newton polytope $P_f = Q$ 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

$$Q = \text{conv}((0, 9), (15, 0), (17, 20), (7, 19))$$

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

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

having Newton polytope $P_f = Q$ 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

$$Q = \text{conv}((0, 3), (9, 0), (12, 15), (4, 8))$$

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

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

having Newton polytope $P_f = Q$ is absolutely irreducible over any field F .

Pentagons

We do not give a necessary condition and only give some new sufficient conditions for integral indecomposability of pentagons. We can examine pentagons in three different cases as in Figure 5:

- (i) Pentagons having two parallel edges.
- (ii) Pentagons lying inside a triangle having a common edge with the pentagon. In this case, if the common edge of the pentagon and the triangle is primitive then the pentagon is integrally indecomposable by [1].
- (iii) Pentagons which do not lie inside a triangle having a common edge with the pentagon.

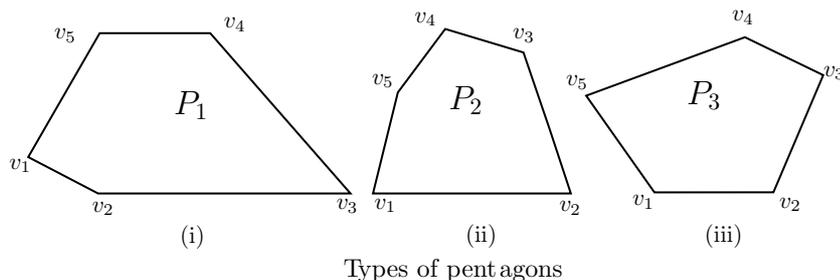
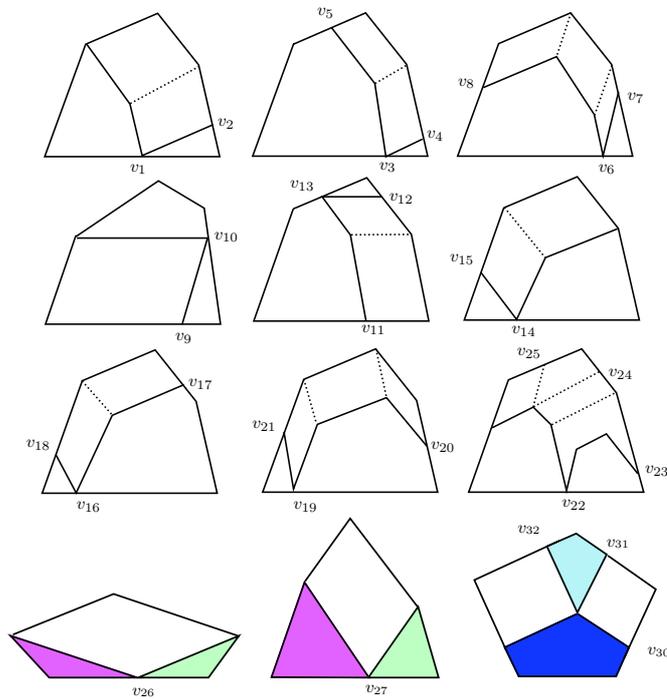


FIGURE 5



Some decomposition methods for integral pentagons

FIGURE 6

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

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

Hence, P_1 is integrally decomposable. This also follows from Remark 2.2.

Let P_2 be an integral pentagon without parallel edges and having two adjacent interior angles whose sum is strictly less than π 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 [1, Corollary 4.12] when $\text{gcd}(v_1 - v_2) = 1$. 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 $\text{gcd}(v_1 - v_2) \neq 1$, P_2 may be integrally indecomposable or not. By Lemma 2.1, 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 $\text{gcd}(v_1 - v_2) \neq 1$ provided that the indicated points v_i are integral.

Later, we shall 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 π , 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.

Some general results

Now, we give some results for general n -gons. In particular, we also give some new criteria for integral decomposability of pentagons of the types P_2 and P_3 .

Proposition 2.14. *Any n -gon P , $n \geq 5$, is integrally indecomposable if it has edge sequence $\{e_1, e_2, \dots, e_n\}$ such that the sum of any three edges of any k edges of P is nonzero, whenever $k \leq 3 \leq (n - 2)$.*

Proof. This is a result of Lemma 2.1. □

Note that in Proposition 2.14, it is enough to consider the sum of at most $n/2$ edges if n is even and sum of at most $(n - 1)/2$ edges if n is odd. For example, the following integral polygons on the plane are integrally indecomposable:

- (1) Any pentagon P which has edge sequence $\{e_1, e_2, e_3, e_4, e_5\}$. Here, since we assume that P has no parallel edges, we observe that the condition $e_1 + e_2 + e_3 \neq 0$ is already satisfied.
- (2) Any pentagon P with 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 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 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 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 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 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 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 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 $i, j, k, s, t \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

The following result uses a different observation from the previous ones.

Proposition 2.15. *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) $a_i \equiv k \pmod{n}$ for $1 \leq i \leq n$.
- Case (2) $b_i \equiv k \pmod{n}$ for $1 \leq i \leq n$.

Proof. Let S be a proper nonempty subset of the set $\{1, 2, \dots, n\}$ with cardinality $|S| = s$. Then we have $\sum_{j \in S} a_j \equiv ks \not\equiv 0 \pmod{n}$ or $\sum_{j \in S} b_j \equiv ks \not\equiv 0 \pmod{n}$ since $s \not\equiv n$. 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 $\sum_{j \in S} b_j \neq 0$. □

Example 2.16. (1) Let m, n be positive integers such that $\gcd(m, n) = 1$. Then any bivariate polynomial $f \in F[x, y]$ having Newton polytope

$$P_f = \text{conv}((m, 0), (0, n), (m + 1, n + 1), (m, n + m + 1), (0, n + 1))$$

is absolutely irreducible over any field F by Proposition 2.14 since P_f is a pentagon having all edges primitive. For example, taking $m = 3$ and $n = 2$, the polynomial

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

having $P_f = \text{conv}((3, 0), (0, 2), (4, 3), (3, 6), (0, 3))$ is absolutely irreducible over any field F .

- (2) As another example of Proposition 2.14, the pentagon

$$P = \text{conv}((m, 0), (0, n), (m + 1, n + 1), (m, n + m + 1), (0, n + m))$$

is integrally indecomposable if m and n are relatively prime positive integers. Because, P has 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 $1 \leq i \leq m - 1$. See Figure 7.

- (3) Consider the 6-gon

$$P = \text{conv}((7, 0), (8, 0)(15, 2), (16, 7), (11, 8), (0, 3))$$

which has 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 2.15.

The polygons given in Example 2.16 have no parallel edges and do not lie inside a triangle having a common edge with the polygon so that the result of [1, Corollary 4.12] cannot be applied.

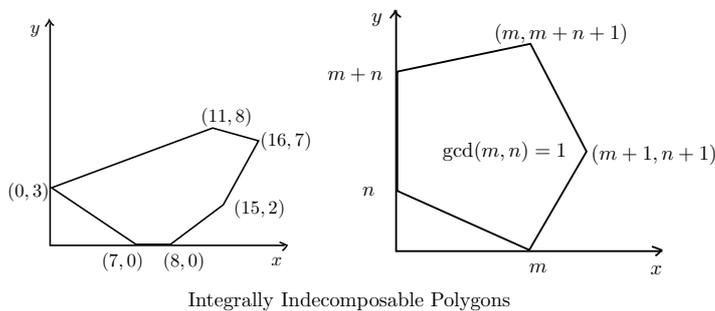


FIGURE 7

Acknowledgments. We thank the referee for a careful reading of the manuscript and making helpful comments, which led to progressions in presentation.

References

- [1] S. Gao, *Absolute irreducibility of polynomials via Newton polytopes*, J. Algebra **237** (2001), no. 2, 501–520.
- [2] S. Gao and A. G. B. Lauder, *Decomposition of Polytopes and Polynomials*, Discrete Comput. Geom. **26** (2001), no. 1, 89–104.
- [3] F. Koyuncu and F. Özbudak, *Integral and homothetic indecomposability with applications to irreducibility of polynomials*, Turkish J. Math. **33** (2009), no. 3, 283–294.
- [4] A. Lipkovski, *Newton polyhedra and irreducibility*, Math. Z. **199** (1998), no. 2, 119–127.
- [5] A. M. Ostrowski, *On multiplication and factorization of polynomials I, Lexicographic orderings and extreme aggregates of terms*, Aequationes Math. **13** (1975), no. 3, 201–228.
- [6] ———, *On multiplication and factorization of polynomials II, Irreducibility discussion*, Aequationes Math. **14** (1976), no. 1-2, 1–31.
- [7] G. M. Ziegler, *Lectures on Polytopes*, GTM 152, Springer-Verlag, 1995.

DEPARTMENT OF MATHEMATICS
 MUĞLA UNIVERSITY
 48170, MUĞLA, TURKEY
 E-mail address: fatih@mu.edu.tr