Filomat 27:2 (2013), 215–226
DOI 10.2298/FIL1302215C

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Factoring bivariate polynomials with integer coefficients via Newton polygons

Siniša Crvenković[a], Ivan Pavkov[b]

[a]*University of Novi Sad, Faculty of Sciences and Mathematics, Department of Mathematics and Informatics, Trg Dositeja Obradovića 4, 21000 Novi Sad*
[b]*Higher School of Professional Business Studies, Vladimira Perića-Valtera 4, 21000 Novi Sad*

Abstract. It is known that the Newton polygon of a polynomial carries information on its irreducibility. In this paper we shall give another proof of the main theorem and characterize the inner points of the polygon. From that proof it will be obvious that the inner points of the Newton polygon play an important role in finding possible factorizations. We shall give a necessary and sufficient condition for the existence of the integer polynomial factorization in integer factor-polynomials.

Definition 0.1. *The convex hull of a set S (denoted by* $\mathrm{conv}(S)$*) is the smallest convex set that contains the set S.*

Definition 0.2. *For two arbitrary sets A and B, being subsets of $\mathbb{R}^2$, a 2-dimensional real Euclidean space, the set $A + B = \{a + b : a \in A, b \in B\}$ is called the Minkowski sum of sets A and B.*

Definition 0.3. *An arbitrary point from $\mathbb{R}^2$ is called an integer point if both of its coordinates are integers. An arbitrary polygon in $\mathbb{R}^2$ is called an integer polygon if all of its vertices are integer points.*

Definition 0.4. *We say that the integer polygon C is integrally decomposable if there exist integer polygons A and B that satisfy $C = A + B$, A and B containing at least two points. Polygons A and B are called polygon summands of the polygon C. Otherwise, polygon C is integrally indecomposable, i.e. there is no non-trivial decomposition of polygon C.*

Definition 0.5. *Consider an arbitrary polynomial in two variables with integer coefficients from $\mathbb{Z}[x, y]$, the ring of polynomials in two variables over $\mathbb{Z}$*

$$f(x, y) = \sum C_{e_1 e_2} x^{e_1} y^{e_2}.$$

Consider an exponent vector (e_1, e_2) as a point in $\mathbb{Z}^2$. The Newton polygon of the polynomial $f(x, y)$, denoted by P_f, is defined as the convex hull in $\mathbb{R}^2$ of all the points (e_1, e_2) with $C_{e_1 e_2} \in \mathbb{Z} \setminus \{0\}$.

Definition 0.6. *A polynomial over field F is called absolutely irreducible if it remains irreducible over every algebraic extension of F.*

2010 *Mathematics Subject Classification*. 12Y05)
Keywords. bivariate polynomials, non-trivial factorization, Newton polygon
Received: 10 May 2012; Accepted: 15 December 2012
Communicated by Miroslav Ćirić
[a]Supported by the Ministry of Education and Science, Serbia, grant 174018
Email addresses: sima@dmi.uns.ac.rs (Siniša Crvenković), pavkov.ivan@gmail.com (Ivan Pavkov)

Definition 0.7. *Let $f(x,y) \in \mathbb{Z}[x,y]$. The non-extended lattice of nodes of the polynomial $f(x,y)$ consists of all the points $(e_1,e_2)_i$, $i = 1,...,k$ corresponding to the terms with non-zero coefficients. If the Newton polygon of $f(x,y)$ contains, in its inner area, some integer points different from $(e_1,e_2)_i$, $i = 1,...,k$, these points, together with $(e_1,e_2)_i$, $i = 1,...,k$, form an extended lattice of nodes.*

The following theorem is well known.

Theorem 0.8. *Let F be an arbitrary field. Let $f(x,y), g(x,y), h(x,y) \in F[x,y]$ with $f(x,y) \neq 0$ and $f(x,y) = g(x,y)h(x,y)$. Then $P_f = P_g + P_h$.*

Proof: It is known that the Minkowski sum of two polygons is a polygon and any vertex of the resulting polygon is obtained as the sum of the vertices of the polygon summands. Let $(\alpha,\beta) \in P_f$ be an arbitrary vertex of the Newton polygon of polynomial $f(x,y)$. This implies that polynomial f contains monomial $x^\alpha y^\beta$ with non-zero coefficient. Due to the fact that $f(x,y) = g(x,y)h(x,y)$, we can conclude that polynomials $g(x,y)$ and $h(x,y)$ contain monomials $x^\gamma y^\delta$ and $x^{\alpha-\gamma}y^{\beta-\delta}$ in that order, both with non-zero coefficients. These monomials correspond to the points $(\gamma,\delta) \in P_g$ and $(\alpha-\gamma,\beta-\delta) \in P_h$. It is obvious that $(\gamma,\delta)+(\alpha-\gamma,\beta-\delta) \in P_g + P_h$. Namely, we obtain $(\gamma+\alpha-\gamma,\delta+\beta-\delta) \in P_g+P_h$, i.e. $(\alpha,\beta) \in P_g+P_h$. In other words, the inclusion $P_f \subseteq P_g+P_h$ holds. We will show that the reverse inclusion $P_g + P_h \subseteq P_f$ also holds. Since a Newton polygon is the convex hull of its vertices, it is sufficient to show that any vertex of a polygon $P_g + P_h$ lies in the polygon P_f. Let v be a vertex of the Newton polygon $P_g + P_h$. Since $v \in P_g + P_h$, we conclude that there exist points $v_g \in P_g$ and $v_h \in P_h$ such that $v = v_g + v_h$. The assumption that v is a vertex of the Newton polygon $P_g + P_h$ implies that such vectors v_g and v_h are unique. Assume the opposite, $v = v_g + v_h = v'_g + v'_h$, $v_g, v'_g \in P_g$, $v_h, v'_h \in P_h$, with $v_g \neq v'_g$ and $v_h \neq v'_h$.

Let $v = (x,y)$ and $v_g = (a,b)$. As $v = v_g + v_h$, it is obvious that $v_h = (x-a, y-b)$. Let $v'_g = (c,d)$. Analogously we obtain $v'_h = (x-c, y-d)$. Consider the point $v_g + v'_h$. It is clear that $v_g + v'_h \in P_g + P_h$. We have the following

$$v_g + v'_h = (a,b) + (x-c, y-d) = (x+a-c, y+b-d) = (x+(a-c), y+(b-d)).$$

Further, consider the point $v'_g + v_h$. It is clear that $v'_g + v_h \in P_g + P_h$. We have the following

$$v'_g + v_h = (c,d) + (x-a, y-b) = (x-a+c, y-b+d) = (x-(a-c), y-(b-d)).$$

Let us look for a midpoint of the line segment whose endpoints are $v_g + v'_h$ and $v'_g + v_h$, $v_g + v'_h$, $v'_g + v_h \in P_g + P_h$.

$$\left(\frac{x+(a-c)+x-(a-c)}{2}, \frac{y+(b-d)+y-(b-d)}{2}\right) = (x,y).$$

In other words, the center of the line segment whose endpoints are $v_g + v'_h$ and $v'_g + v_h$, which both lie in the Newton polygon $P_g + P_h$, is the point (x,y). As a vertex of the Newton polygon is not on any line segment connecting any other two points of the polygon, we conclude that the point (x,y) is not the vertex of the polygon $P_g + P_h$, which is an obvious contradiction. Therefore, for an arbitrary vertex v of the Newton polygon $P_g + P_h$ there exist unique vectors $v_g \in P_g$ and $v_h \in P_h$ such that $v = v_g + v_h$.

As v is a vertex of the polygon $P_g + P_h$, we can conclude that v_g and v_h are also the vertices of the polygons P_g and P_h. Since v_g and v_h are unique, it is obvious that there exist unique terms of $g(x,y)$ and $h(x,y)$ such that v is a resulting exponent vector in $g(x,y)h(x,y)$. Therefore $v \in P_f$. We have shown that all vertices of polygon $P_g + P_h$ lie in the polygon P_f. Due to the fact that the Newton polygon is the convex hull of its vertices, we have $P_g + P_h \subseteq P_f$. □

Remark 0.9. From the proof of Theorem 0.8 it is obvious that the monomials of the polynomial $f(x,y)$ that are "obtained" in, at least, two different ways by multiplying factor-polynomials $g(x,y)$ and $h(x,y)$, certainly do not correspond to the vertices of the Newton polygon P_f.

Example 0.10. Consider a polynomial:

$$f(x,y) = x^2 + 2xy + y^2 \in \mathbb{Z}[x,y].$$

The factorization of polynomial $f(x, y)$ is given below

$$f(x, y) = (x + y)(x + y).$$

The monomial xy with coefficient 2 is "obtained" in two different ways by multiplying factor-polynomials

$$xy = (x)(y) = (y)(x).$$

Examine the Newton polygon of the polynomial $f(x, y)$ shown in Figure 1.

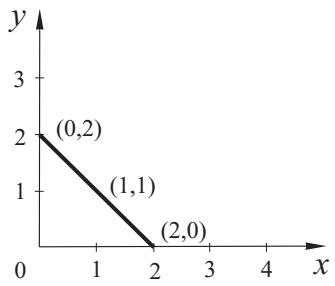

Figure 1

Clearly, $P_f = \text{conv}((1, 1), (0, 2), (2, 0))$ is a line segment with endpoints $(0, 2)$ and $(2, 0)$. Indeed, the monomial xy of the polynomial $f(x, y)$ that is "obtained" in two different ways by multiplying factor-polynomials corresponds to the point $(1, 1)$, which is not the vertex of the polygon P_f.

Theorem 0.11. *Let $f(x, y)$ be a non-zero bivariate polynomial over an arbitrary field F, non-divisible either by x or by y. If the Newton polygon of the polynomial is integrally indecomposable, then polynomial $f(x, y)$ is absolutely irreducible over F.*

Proof: Since polynomial $f(x, y)$ is non-divisible either by x or by y, it has no trivial decomposition. Assume the opposite, the polynomial $f(x, y)$ is not absolutely irreducible over field F, i.e. it does not remain irreducible over every algebraic extension of F. This implies that over some algebraic field extension of F, $f(x, y) = g(x, y)h(x, y)$ holds, with $g(x, y)$ and $h(x, y)$ having, at least, two non-zero terms. Due to the fact that $g(x, y)$ and $h(x, y)$ have, at least, two non-zero terms, their corresponding Newton polygons have, at least, two points. Since $f(x, y) = g(x, y)h(x, y)$, from the previous theorem we get $P_f = P_g + P_h$, with P_g and P_h having, at least, two points. This implies that polygon P_f has non-trivial decomposition, which is a contradiction. Therefore, the polynomial $f(x, y)$ is absolutely irreducible over F. □

Definition 0.12. *Let $f(x, y)$ be a polynomial in two variables over $\mathbb{Z}$. Let $P = \{A_1, A_2, ..., A_n\}$ be the lattice of nodes of the polynomial $f(x, y)$ possibly extended by some integer points that lie inside of the Newton polygon of the polynomial $f(x, y)$. Without loss of generality, we can assume that after the construction of the Newton polygon of the polynomial $f(x, y)$, $A_1, A_2, ..., A_k$, $k \geq 2$, become its vertices, and $A_{k+1}, ..., A_n$ do not. We say that the grouping of the set P, $G_1, ..., G_l$, $l \geq 2$, is a super-covering of P if:*

1. *Each group G_i, $i = 1, ..., l$, contains the same number of points not less than two,*
2. $\bigcup_{i=1}^{l} G_i = P$,
3. *Points $A_1, A_2, ..., A_k$ appear in one and only one of the sets $G_1, ..., G_l$,*
4. *Points $A_{k+1}, ..., A_n$ appear in at least one of the sets $G_1, ..., G_l$,*
5. *Convex polygons determined by $G_1, G_2, ..., G_l$ are congruent and $G_2, ..., G_l$ are obtained from G_1 by translation.*

Definition 0.13. *Let $f(x,y)$ be a bivariate polynomial with integer coefficients over $\mathbb{Z}$. Let $P = \{A_1, A_2, ..., A_n\}$ be the extended or non-extended lattice of nodes of the polynomial $f(x,y)$. Let $G_1 = \text{conv}(A_{i_{1,1}}, ..., A_{i_{1,k}})$, ..., $G_l = \text{conv}(A_{i_{l,1}}, ..., A_{i_{l,k}})$, $l \geq 2$, with $\{i_{1,1}, ..., i_{1,k}, ..., i_{l,1}, ..., i_{l,k}\} = \{1, ..., n\}$ be a super-covering of P by l congruent $k-$gons. Due to the fact that the composition of two translations is also a translation, we conclude that, for any of the G_p and G_q, $p \neq q$, $p, q \in \{1, ..., l\}$ there exists a translation $\tau_{p,q}$, such that $\tau_{p,q}(G_p) = G_q$. For each polygon, we list vertices in such a way that we firstly list the vertex with smallest $x-$coordinate. If such vertex is not unique, we choose the one having simultaneously smallest $y-$coordinate. Then we list the other vertices in counterclockwise order. It is clear that $\tau_{p,q}(A_{i_{p,w}}) = A_{i_{q,w}}$, for any of the p and q, $p \neq q$, $p, q \in \{1, ..., l\}$ and each $w = 1, ..., k$. Let us denote by $\text{coef}(A_i)$ the coefficient of the monomial of the polynomial $f(x,y)$ corresponding to the exponent vector A_i. Assume that polygons $G_1, G_2, ..., G_l$ have no common node. We say that the super-covering of P is suitable super-covering with respect to the coefficients of the polynomial $f(x,y)$ if*

$$\text{coef}(A_{i_{1,1}}) : \text{coef}(A_{i_{1,2}}) : ... : \text{coef}(A_{i_{1,k}}) = ... = \text{coef}(A_{i_{l,1}}) : \text{coef}(A_{i_{l,2}}) : ... : \text{coef}(A_{i_{l,k}}).$$

Assume that polygons $G_1, ..., G_l$ have common nodes. Each G_i, $i = 1, ..., l$, determines a polynomial $p_i(x,y)$ such that $f(x,y) = p_1(x,y) + ... + p_l(x,y)$, where polynomial summands $p_i(x,y)$, $i = 1, ..., l$, are ordered in the same way as the vertices. For each node A_c, that is common for s polygons, the coefficient of the monomial whose exponent vector is A_c is partitioned into s summands such that every summand belongs to one and only one $p_i(x,y)$, corresponding to the polygons having a common node A_c, in a way that the coefficients of $p_1(x,y)$,...,$p_l(x,y)$, $p_i(x,y) = c_{i,1}x^{\alpha_{i,1}}y^{\beta_{i,1}} + ... + c_{i,k}x^{\alpha_{i,k}}y^{\beta_{i,k}}$, are proportional, i.e.

$$c_{1,1} : c_{1,2} : ... : c_{1,k} = ... = c_{l,1} : c_{l,2} : ... : c_{l,k}.$$

If the above holds for every common node, we say that the super-covering is suitable.

From Theorem 0.11 it follows that integral indecomposability of the corresponding Newton polygon of a polynomial, that is completely determined by its vertices, implies irreducibility of a polynomial. Moreover, any polynomial having the same non-zero terms is also absolutely irreducible over that field. It remains irreducible if we add monomials whose exponent vectors lie in the inner area of the polygon. On the other hand, the Newton polygon of a polynomial does not carry the entire information on the existence of the polynomial factorization. In what follows we are going to see that, when factoring a polynomial, it is important to consider the vertices that determine Newton polygon, as well as the points disregarded for vertices of the Newton polygon and integer points captured by the polygon.

Remark 0.14. Note that it is sufficient to discuss possible factorization of polynomials non-divisible either by x or by y, and therefore, having no trivial factorization. For example, multiplying by x and y means, in the sense of Newton polygon, translation for vectors $(1,0)$ and $(0,1)$. Since we are not interested in the trivial factorizations, in the following we examine polynomials non-divisible either by x or by y. So, if we intend to examine possible non-trivial factorization of a polynomial divisible by x, y or both of them, firstly we extract a trivial factor x^α, y^β or $x^\alpha y^\beta$ and discuss possible factorizations of the non-trivial factor-polynomial.

Let us formulate a necessary and sufficient condition for the existence of the non-trivial integer factorization of the bivariate polynomial with integer coefficients.

Theorem 0.15. *Let $f(x,y)$ be a non-zero bivariate polynomial over $\mathbb{Z}$. Polynomial $f(x,y)$ has non-trivial integer factorization if and only if its lattice of nodes, possibly extended by some integer points captured by the Newton polygon of the polynomial $f(x,y)$, has suitable super-covering with respect to the coefficients of $f(x,y)$.*

Proof: ($\Rightarrow$) Assume that $f(x,y)$ has non-trivial integer factorization, i.e. there exist integer polynomials $g(x,y)$ and $h(x,y)$ both having, at least, two monomials with non-zero terms such that $f(x,y) = g(x,y)h(x,y)$. Let $h(x,y) = c_1x^{\alpha_1}y^{\beta_1} + ... + c_kx^{\alpha_k}y^{\beta_k}$, with $c_i \neq 0$, for at least, two i, $i = 1, ..., k$. Let $c_p \neq 0$ and $c_q \neq 0$. It is clear that either $(\alpha_p, \beta_p) \neq (0,0)$ or $(\alpha_q, \beta_q) \neq (0,0)$. So, let us rewrite polynomial $h(x,y)$ in the following form

$$h(x,y) = c_px^{\alpha_p}y^{\beta_p} + c_qx^{\alpha_q}y^{\beta_q} + \sum_{i \in I} c_ix^{\alpha_i}y^{\beta_i},$$

where $I \subset \{1, ..., k\} \setminus \{p, q\}$, is a collection of all indices different from p and q, such that for each $i \in I$, $c_i \neq 0$. Clearly, if the polynomial $h(x, y)$ has no other non-zero terms except $c_p x^{\alpha_p} y^{\beta_p}$ and $c_q x^{\alpha_q} y^{\beta_q}$, the set I is empty. We can rewrite the polynomial f(x,y) in the following way

$$f(x, y) = g(x, y)\Big(c_p x^{\alpha_p} y^{\beta_p} + c_q x^{\alpha_q} y^{\beta_q} + \sum_{i \in I} c_i x^{\alpha_i} y^{\beta_i}\Big).$$

Further, we obtain

$$f(x, y) = g(x, y)c_p x^{\alpha_p} y^{\beta_p} + g(x, y)c_q x^{\alpha_q} y^{\beta_q} + g(x, y) \sum_{i \in I} c_i x^{\alpha_i} y^{\beta_i}.$$

Let us denote the Newton polygons of polynomials $g(x, y)$ and $f(x, y)$ by P_g and P_f. Due to the fact that the multiplication of the polynomial $g(x, y)$ by monomials $c_p x^{\alpha_p} y^{\beta_p}$, $c_q x^{\alpha_q} y^{\beta_q}$, and eventually others, corresponds to the translation of the polygon P_g for vectors (α_p, β_p), (α_q, β_q), and others, it is clear that the Newton polygon of $f(x, y)$ is the convex hull of polygon P_g translated by vectors (α_p, β_p), (α_q, β_q) and others. In other words, the lattice of nodes is covered by congruent polygons P_g. So, the super-covering of the lattice of nodes is obtained. From the representation above of the polynomial $f(x, y)$ it is obvious that, if monomials obtained in more than one way exist, they are split into the polynomial summands $g(x, y)c_p x^{\alpha_p} y^{\beta_p}$, $g(x, y)c_q x^{\alpha_q} y^{\beta_q}$, and eventually others, in the way that appropriate coefficients of these polynomial summands are proportional as $c_p : c_q : ...$, so it follows that such a covering is suitable super-covering.

($\Leftarrow$) Assume that the lattice of nodes of $f(x, y)$, possibly extended by some integer points captured by the Newton polygon of the polynomial $f(x, y)$, has suitable super-covering with respect to the coefficients of $f(x, y)$. Further, we assume that this covering is reached by l congruent polygons $G_1, G_2, ..., G_l$. We group monomials of the polynomial $f(x, y)$ in the way determined by polygons $G_1, G_2, ..., G_l$, $l \geq 2$. We split monomials into polynomial summands that correspond to the nodes that are common for, at least, two polygons in order to obtain proportionality of the coefficients of the polynomial summands. This is possible to achieve because of the fact that super-covering is suitable with respect to the coefficients of $f(x, y)$. It is obvious that such splitting of the monomials into polynomial summands defines a non-trivial integer factorization of the polynomial $f(x, y)$. □

Remark 0.16. Under the same conditions as in the previous theorem, the same holds if we consider the polynomial with rational coefficients.

Example 0.17. Consider a polynomial $f(x, y)$ over $\mathbb{Z}$,

$$f(x, y) = x^2 + 2xy + y^2 \in \mathbb{Z}[x, y].$$

The lattice of nodes of $f(x, y)$, shown in Figure 2, contains the vertices of the polygon $(0, 2)$ and $(2, 0)$, but also the point $(1, 1)$ that is disregarded for the vertex because of its collinearity with two consecutive vertices.

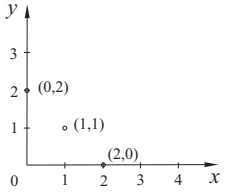

Figure 2

The only way to achieve super-covering on this lattice is to cover it with two congruent line segments $\text{conv}((2, 0), (1, 1))$ and $\text{conv}((1, 1), (0, 2))$ having a common node $(1, 1)$. This super-covering is suitable if the coefficient of the monomial corresponding to the comon node $(1, 1)$, i.e. xy, can be split in such a way as to obtain proportionality of the appropriate coefficients of polynomial summands induced by the super-covering. We use brackets to announce the grouping of the monomials

$$f(x, y) = (x^2 + axy) + ((2 - a)xy + y^2).$$

Line segment conv((1, 1), (0, 2)) is obtained from the line segment conv((2, 0), (1, 1)) by the translation for the vector (−1, 1). If we denote such translation by τ, it follows that $\tau((2,0)) = (1,1)$ and $\tau((1,1)) = (0,2)$. In the first brackets, the order of the monomials is such that firstly we list the monomial corresponding to the exponent vector (2, 0) and secondly the monomial corresponding to the exponent vector (1, 1). In the second brackets, firstly we list the monomial corresponding to the exponent vector $\tau((2,0))$ and secondly the monomial corresponding to the exponent vector $\tau((1,1))$. The super-covering is suitable if $1 : a = (2-a) : 1$, i.e. $a = 1$. We have

$$f(x,y) = x(x+y) + y(x+y) = (x+y)(x+y).$$

Example 0.18. Consider a polynomial $f(x, y)$ over $\mathbb{Z}$

$$p(x,y) = y^2 - x^2 \in \mathbb{Z}[x,y].$$

The exponent vectors corresponding to non-zero terms of the polynomial $p(x, y)$ are (0, 2) and (2, 0) and the Newton polygon of the polynomial $p(x, y)$ is a line segment with endpoints (0, 2) and (2, 0) as in the previous example. It is not possible to reach a factorization of this polynomial if we only consider the vertices of its Newton polygon. Nevertheless, this line segment contains an integer point (1, 1) that corresponds to the monomial xy with coefficient 0. Consider the extended lattice of nodes that consists of vertices (0, 2) and (2, 0) together with the point (1, 1). We reach the super-covering of the lattice in the same way as in the previous example. So let us rewrite polynomial $p(x, y)$ in the following way

$$p(x,y) = y^2 + 0xy - x^2.$$

This super-covering is suitable if we can choose an appropriate way to represent zero in order to obtain proportionality of the appropriate coefficients of polynomial summands

$$p(x,y) = y^2 + (-a+a)xy - x^2 = (y^2 - axy) + (axy - x^2), \quad a \in \mathbb{Z}.$$

As 1:(- a) = a:(-1), i.e. $a^2 = 1$, we conclude that suitable super-covering is reached for $a = 1$ and $a = -1$. Choosing $a = 1$, we get

$$p(x,y) = (y^2 - xy) + (xy - x^2) = y(y-x) + x(y-x) = (y+x)(y-x).$$

Remark 0.19. Choosing $a = -1$ leads to the same factorization of the polynomial

$$p(x,y) = (y^2 + xy) + (-xy - x^2) = y(y+x) - x(y+x) = (y-x)(y+x).$$

Example 0.20. Consider a polynomial $p(x, y)$ over $\mathbb{Z}$

$$p(x,y) = y^2 - 2x^2 = y^2 + 0xy - 2x^2 \in \mathbb{Z}[x,y].$$

As in Example 0.17 and Example 0.18, the extended lattice of nodes consists of points (0, 2), (2, 0) and (1, 1) and we cover it in the same way. This super-covering is suitable if the monomial $0xy$ can be split in such a way as to obtain proportionality of the appropriate coefficients, i.e.

$$p(x,y) = y^2 - axy + axy - 2x^2 = (y^2 - axy) + (axy - 2x^2), \quad a \in \mathbb{Z},$$

with $1 : (-a) = a : (-2)$, i.e. $a^2 = 2$. There is no a, $a \in \mathbb{Z}$, such that $a^2 = 2$. Therefore, the polynomial $f(x, y)$ has no integer factorization. Since $a = \sqrt{2} \in \mathbb{R}$, $p(x, y)$ has factorization over the field of real numbers

$$p(x,y) = (y - \sqrt{2}x)(y + \sqrt{2}x).$$

Example 0.21. Consider a polynomial $r(x, y)$ over $\mathbb{Z}$

$$r(x,y) = y^2 - 4x^2 = y^2 + 0xy - 4x^2 \in \mathbb{Z}[x,y]$$

with the same lattice of nodes as in the previous examples and we cover it in the same way. This supercovering is suitable if the polynomial can be written in the following form

$$r(x,y) = y^2 + 0xy - 4x^2 = (y^2 - axy) + (axy - 4x^2), \quad a \in \mathbb{Z}$$

with $1 : (-a) = a : (-4)$, i.e. $a = 2$ or $a = -2$. Choosing $a = 2$, we get

$$r(x,y) = (y^2 - 2xy) + (2xy - 4x^2) = y(y - 2x) + 2x(y - 2x) = (y + 2x)(y - 2x).$$

Remark 0.22. We have stated earlier that, if we want to factor a bivariate polynomial, it is important to consider the vertices that determine the Newton polygon as well as the points disregarded as vertices of the Newton polygon, because of their collinearity with two consecutive vertices or their position inside the constructed polygon. In other words, all the points corresponding to any of the exponent vectors are important for finding the possible factorizations of a polynomial. In the previous examples we have shown that integer points, that do not correspond to exponent vectors but lie inside the Newton polygon of a polynomial, may also be important for its factorization.

Remark 0.23. It would be wrong to conclude that if all the points that correspond to exponent vectors of a polynomial are vertices of its Newton polygon and the polygon has no other integer points in its inner area, the polynomial is irreducible. In other words, the inner points of the Newton polygon play an important role in finding possible factorizations, but their absence does not necessary imply irreducibility of the polynomial. This will be illustrated by the following example.

Example 0.24. Consider a polynomial $f(x,y)$ over $\mathbb{Z}$

$$f(x,y) = xy + x + y + 1 \in \mathbb{Z}[x,y].$$

The terms of the polynomial $f(x,y)$ with non-zero coefficients correspond to the following exponent vectors: $(1,1), (1,0), (0,1)$ i $(0,0)$. The Newton polygon of $f(x,y)$ is a square with integer vertices shown in Figure 3 having no other integer points in its inner area.

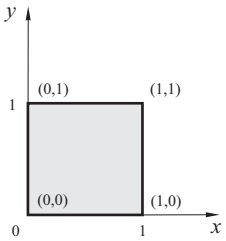

Figure 3

P_f can be integrally decomposed in a way as shown in Figure 4, i.e.

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

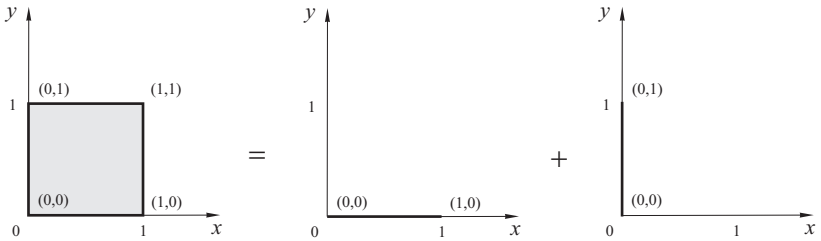

Figure 4

Since the Newton polygon of the polynomial $f(x, y)$ is integrally decomposable, the polynomial $f(x, y)$ can be either reducible or irreducible. We cover the lattice with two congruent line segments and factor $f(x, y)$ in the following way

$$f(x, y) = (x + 1)(y + 1).$$

Note that the Newton polygon of $f(x, y)$ does not capture any integer point except its vertices. However, $f(x, y)$ has integer factorization. Due to the absence of the inner integer points, it is understandable that there is no monomial obtained in more than one way from the factor-polynomials of $f(x, y)$.

Example 0.25. Consider a polynomial $f(x, y)$ over $\mathbb{Z}$

$$f(x, y) = x^2y^2 + x^2 + y^2 + 1 \in \mathbb{Z}[x, y].$$

The terms of the polynomial $f(x, y)$ with non-zero coefficients correspond to the following exponent vectors: $(2, 2), (2, 0), (0, 2)$ and $(0, 0)$. The Newton polygon of the polynomial $f(x, y)$ is a square with integer vertices shown in the Figure 5.

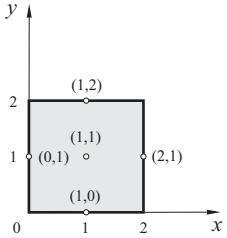

Figure 5

The polynomial $f(x, y)$ has following integer factorization

$$f(x, y) = (x^2 + 1)(y^2 + 1).$$

Remark 0.26. Note that the Newton polygon of the polynomial $f(x, y)$ contains the following integer points in its inner area: $(0, 1), (1, 0), (1, 2), (2, 1)$ and $(1, 1)$. These points are not of interest for polynomial factorization because super-covering can be reached on the non-extended lattice of nodes.

Example 0.27. Consider the following bivariate polynomials over $\mathbb{Z}$

$$f(x, y) = xy^4 + x^2y^3 + 3xy^2 + y^3 + x^2y + x + y \in \mathbb{Z}[x, y],$$
$$g(x, y) = xy^4 + x^2y^3 + 2xy^2 + y^3 + x^2y + x + y \in \mathbb{Z}[x, y],$$
$$h(x, y) = xy^4 + x^2y^3 + 5xy^2 + y^3 + x^2y + x + y \in \mathbb{Z}[x, y].$$

Since these polynomials have the same non-zero terms, their non-extended lattices of nodes are the same and Newton polygons are also the same, i.e. $P_f = P_g = P_h$. Let $A = (1, 0)$, $B = (0, 1)$, $C = (1, 2)$, $D = (0, 3)$, $E = (1, 4)$, $F = (2, 1)$ and $G = (2, 3)$. The polygon P_f is shown in Figure 6.

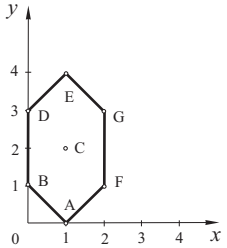

Figure 6

The only point from the non-extended lattice of nodes that is not a vertex of the Newton polygon is C and, if the polynomial is reducible, the monomial that corresponds to the point $C = (1, 2)$, that is $3xy^2$, would be obtained from the factor-polynomials in more than one way. Since its coefficient in $f(x, y)$ is 3 and all the other coefficients are 1, intuitively it is clear that, in order to obtain suitable super-covering with respect to coefficients of the polynomial $f(x, y)$, we have to cover the non-extended lattice of nodes by three congruent figures, such that each node belongs to one and only one figure, except node C which should be common to all of these figures. Such covering by three congruent triangles $\triangle ABC$, $\triangle CDE$ and $\triangle FCG$ is shown in Figure 7.

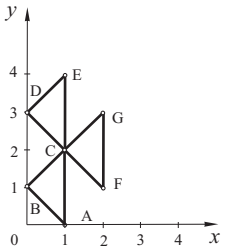

Figure 7

In order to obtain factorization of the polynomial, we group monomials in such a way that the vertices of each triangle are collected in the same brackets. Nevertheless, xy^2 appears in each of these three groups. This is appropriate because it is $xy^2 + xy^2 + xy^2 = 3xy^2$. We have

$$f(x, y) = (x + y + xy^2) + (xy^2 + y^3 + xy^4) + (x^2y + xy^2 + x^2y^3).$$

As triangles $\triangle CDE$ and $\triangle FCG$ are obtained from the triangle $\triangle ABC$ by translation for vectors $(0, 2)$ and $(1, 1)$, we extract from the second brackets y^2 and from the third xy

$$f(x, y) = (x + y + xy^2) + y^2(x + y + xy^2) + xy(x + y + xy^2) = (1 + y^2 + xy)(x + y + xy^2).$$

Since the Newton polygons of the factor-polynomials $1 + y^2 + xy$ and $x + y + xy^2$ have no super-covering, we conclude that these polynomials have no integer factorization. It is easy to prove that another possible suitable super-covering of this lattice of nodes with respect to coefficients of the polynomial $f(x, y)$ shown in Figure 8 leads to the same factorization.

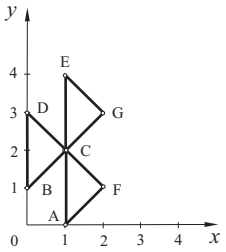

Figure 8

Nevertheless, super-coverings of the lattice of nodes shown in Figure 7 and Figure 8 are not suitable with respect to the coefficients of $g(x, y)$. Due to the fact that the coefficient of the monomial xy^2 is 2, suitable covering of the lattice is the covering by two congruent figures such that each node belongs to one and only one figure, except the node $(1, 2)$, which is common to these two figures. Such covering is given in Figure 9.

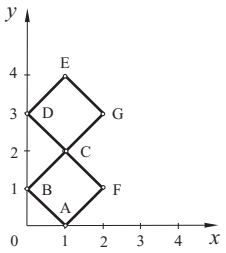

Figure 9

Analogously, we obtain integer factorization induced by this covering

$$g(x,y) = xy^4 + x^2y^3 + 2xy^2 + y^3 + x^2y + x + y = (x + y + xy^2 + x^2y) + (xy^2 + y^3 + xy^4 + x^2y^3)$$

$$g(x,y) = (x + y + xy^2 + x^2y) + y^2(x + y + xy^2 + x^2y) = (1 + y^2)(x + y + xy^2 + x^2y).$$

It is easy to prove that the polynomial $1 + y^2$ has no integer factorization.

Further, we factor polynomial $x + y + xy^2 + x^2y$ with the lattice of nodes shown in Figure 10.

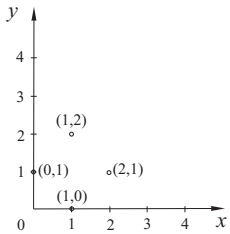

Figure 10

We cover the lattice by two congruent line segments, as shown in Figure 11.

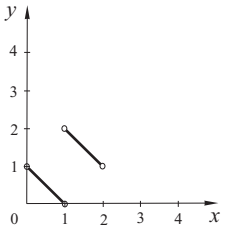

Figure 11

This covering implies grouping of the monomials in the following way

$$x + y + xy^2 + x^2y = (x + y) + (x^2y + xy^2).$$

Since $1 : 1 = 1 : 1$, the proportionality of the coefficients of the polynomial summands is obtained. So, we conclude that this covering is suitable super-covering of the lattice of nodes of the polynomial $x+y+xy^2+x^2y$. Further, we obtain

$$(x + y) + (x^2y + xy^2) = (x + y) + xy(x + y) = (1 + xy)(x + y).$$

So, the polynomial $g(x, y)$ has integer factorization, that is

$$g(x,y) = (1 + y^2)(1 + xy)(x + y).$$

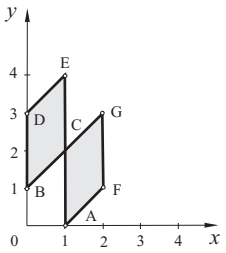

Figure 12

Another suitable covering of the lattice of nodes with respect to the coefficients of the polynomial $g(x, y)$ is shown in Figure 12 and it leads to the same integer factorization of $g(x, y)$.

Finally, consider the polynomial $h(x, y)$ and super-covering of its lattice of nodes shown in Figure 7. We group monomials in the way induced by this covering.

$$h(x, y) = (x + y + axy^2) + (bxy^2 + y^3 + xy^4) + (x^2y + cxy^2 + x^2y^3) \in \mathbb{Z}[x, y], \quad a + b + c = 5.$$

This covering is not suitable with respect to the coefficients of the polynomial $h(x, y)$ since:

$$1 : 1 : a = b : 1 : 1 = 1 : c : 1,$$

implies:

$$a = b = c = 1,$$

i.e.,

$$a + b + c = 3.$$

Completely analogously, for each super-covering reached on its lattice of nodes, it can be shown that it is not suitable with respect to the coefficients of $h(x, y)$, so we conclude that $h(x, y)$ has no non-trivial integer factorization.

Example 0.28. Consider following polynomial over $\mathbb{Z}$

$$h(x, y) = 9xy^4 + 6x^2y^3 + 10xy^2 + 6y^3 + 2x^2y + x + 2y \in \mathbb{Z}[x, y].$$

Since this polynomial has the same non-zero terms as the polynomials $f(x, y)$ and $g(x, y)$ in the previous example, the lattice of nodes is the same too. Super-covering of the lattice shown in the Figure 7 is suitable super-covering with respect to the coefficients of the polynomial $h(x, y)$ if it can be written in the form of the sum of three polynomials determined by triangles $\triangle ABC$, $\triangle CDE$ and $\triangle FCG$, while monomial $10xy^2$ is split in order to satisfy the proportionality of appropriate coefficients if possible

$$h(x, y) = (x + 2y + 3xy^2) + (3xy^2 + 6y^3 + 9xy^4) + (2x^2y + 4xy^2 + 6x^2y^3).$$

As $1 : 2 : 3 = 3 : 6 : 9 = 2 : 4 : 6$, the proportionality is satisfied. Further, we get

$$h(x, y) = (x + 2y + 3xy^2) + 3y^2(x + 2y + 3xy^2) + 2xy(x + 2y + 3xy^2),$$

i.e.,

$$h(x, y) = (1 + 3y^2 + 2xy)(x + 2y + 3xy^2).$$

It is easy to prove that both of the Newton polygons of the factor-polynomials of $h(x, y)$ have no super-covering.

References

[1] F. Abu Salem, S. Gao, A. G. B. Lauder, Factoring polynomials via polytopes: extended version, Report PRG-RR-04-07, Oxford University Computing Laboratory, (2004)
[2] S. Gao, Absolute irreducibility of polynomials via Newton polytopes, Journal of Algebra 237, No.2 (2001) 501-520.
[3] S. Gao, A.G.B. Lauder, Decomposition of polytopes and polynomials, Discrete and Computational Geometry 26 (2001) 89-104.
[4] S. Gao, A.G.B. Lauder, Fast absolute irreducibility testing via Newton polytopes, preprint (2003)
[5] F. Koyuncu, A geometric approach to absolute irreducibility of polynomials, doctoral thesis, The Middle East Technical University - The Department of Mathematics (2004)
[6] F. Koyuncu, An application of the polytope method, JFS, Vol 28 (2005) 13-19.
[7] A. Lipkovski, Newton polyhedra and irreducibility, Math. Z. 199 (1988) 119-127.
[8] A. M. Ostrowski, On multiplication and factorization of polynomials, I. Lexicographic ordering and extreme aggregates of terms, Aequationes Math. 13 (1975) 201-228.
[9] A. M. Ostrowski, On multiplication and factorization of polynomials, II. Irreducibility discussion, Aequationes Math. 14 (1976) 1-32.
[10] I. Pavkov, Irreducibility of polynomials in two variables, master thesis, University of Novi Sad, Faculty of Sciences and Mathematics, Department of Mathematics and Informatics, Novi Sad (2010), (in Serbian)