



UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA



Ivan Pavkov

**FAKTORIZACIJA POLINOMA DVE
PROMENLJIVE SA CELOBROJNIM
KOEFIČIJENTIMA POMOĆU
NEWTON-OVOG POLIGONA I
PRIMENA U DEKODIRANJU NEKIH
KLASA REED - SOLOMON KODOVA**
DOKTORSKA DISERTACIJA

Mentori:

Prof. dr Siniša Crvenković

Prof. dr Nebojša Ralević

Novi Sad, 2017.



КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, РБР:			
Идентификациони број, ИБР:			
Тип документације, ТД:	Монографска документација		
Тип записа, ТЗ:	Текстуални штампани материјал		
Врста рада, ВР:	Докторска дисертација		
Аутор, АУ:	Иван Павков		
Ментор, МН:	Проф. др Синиша Црвенковић, Проф. др Небојша Ралевић		
Наслов рада, НР:	Факторизација полинома две променљиве са целобројним коефицијентима помоћу Newton-овог полигона и примена у декодирању неких класа Reed – Solomon кодова		
Језик публикације, ЈП:	Српски		
Језик извода, ЈИ:	Српски, Енглески		
Земља публикавања, ЗП:	Република Србија		
Уже географско подручје, УГП:	Војводина		
Година, ГО:	2017		
Издавач, ИЗ:	Ауторски репринт		
Место и адреса, МА:	Нови Сад, Факултет техничких наука, Трг Доситеја Обрадовића 6		
Физички опис рада, ФО: (поглавља/страна/цитата/табела/слика/графика/прилога)	12/104/69/0/48/0/0		
Научна област, НО:	Примењена математика		
Научна дисциплина, НД:	Алгебра		
Предметна одредница/Кључне речи, ПО:	Полином две променљиве са целобројним коефицијентима, нетривијална факторизација, Newton-ов полигон, Reed – Solomon кодови, декодирање		
УДК			
Чува се, ЧУ:	Библиотека Факултета техничких наука, Трг Доситеја Обрадовића 6, Нови Сад		
Важна напомена, ВН:			
Извод, ИЗ:	Предмет истраживања докторске дисертације је факторизација полинома две променљиве са целобројним коефицијентима помоћу њима придружених Newton-ових полигона. Формализација потребног и довољног услова за постојање нетривијалне факторизације полинома две променљиве са целобројним коефицијентима омогућава конструкцију ефективног алгоритма за факторизацију. Коначно, добијени теоријски резултати су примењени на декодирање једне класе Reed – Solomon кодова, микса две кодне речи.		
Датум прихватања теме, ДП:	30.06.2016.		
Датум одбране, ДО:			
Чланови комисије, КО:	Председник:	др Илија Ковачевић, редовни професор у пензији	Потпис ментора
	Члан:	др Александар Липковски, редовни професор	
	Члан:	др Лидија Чомић, доцент	
	Члан, ментор:	др Синиша Црвенковић, редовни професор	
	Члан, ментор:	др Небојша Ралевић, редовни професор	



КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Accession number, ANO :			
Identification number, INO :			
Document type, DT :	Monographic publication		
Type of record, TR :	Textual printed material		
Contents code, CC :	PhD thesis		
Author, AU :	Ivan Pavkov		
Mentor, MN :	Professor Nebojša Ralević, PhD, Professor Siniša Crvenković, PhD		
Title, TI :	Factoring bivariate polynomials with integer coefficients via Newton polygon and its application in decoding of some classes of Reed – Solomon codes		
Language of text, LT :	Serbian		
Language of abstract, LA :	Serbian, English		
Country of publication, CP :	Republic of Serbia		
Locality of publication, LP :	Province of Vojvodina		
Publication year, PY :	2017		
Publisher, PB :	Author's reprint		
Publication place, PP :	Novi Sad, Faculty of Technical Sciences, Trg Dositeja Obradovića 6		
Physical description, PD : (chapters/pages/ref./tables/pictures/graphs/appendixes)	12/104/69/0/48/0/0		
Scientific field, SF :	Applied Mathematics		
Scientific discipline, SD :	Algebra		
Subject/Key words, S/KW :	Bivariate polynomial with integer coefficients, non – trivial factorization, Newton polygon, Reed – Solomon codes, decoding		
UC			
Holding data, HD :	Library of the Faculty of Technical Sciences, Trg Dositeja Obradovića 6, Novi Sad		
Note, N :			
Abstract, AB :	The research subject of the thesis is factorization of bivariate polynomials with integer coefficients via associated Newton polygons. Formalization of the necessary and sufficient condition for the existence of a non – trivial factorization of an arbitrary bivariate polynomial with integer coefficients obtains theoretical basis for construction of an effective factorization algorithm. Finally, these theoretical results are applied in decoding special class of Reed – Solomon codewords, mixture of two codewords.		
Accepted by the Scientific Board on, ASB :	30.06.2016.		
Defended on, DE :			
Defended Board, DB :	President:	Ilija Kovačević, PhD, full professor in retirement	
	Member:	Aleksandar Lipkovski, PhD, full professor	
	Member:	Lidija Čomić, PhD, assistant professor	Menthor's sign
	Member, Mentor:	Siniša Crvenković, PhD, full professor	
	Member, Mentor:	Nebojša Ralević, PhD, full professor	

Posebnu zahvalnost za podršku u radu i izdvojenom vremenu dugujem svojim mentorima, prof. dr Siniši Crvenkoviću i prof. dr Nebojši Raleviću. Zahvaljujem se i članovima komisije za ocenu i odbranu doktorske disertacije prof. dr Iliji Kovačeviću, prof. dr Aleksandru Lipkovskom i doc. dr Lidiji Čomić na korisnim sugestijama koje su bitno uticale na kvalitet ove disertacije.

Ivan Pavkov

Sažetak

Predmet istraživanja doktorske disertacije je faktorizacija polinoma dve promenljive sa celobrojnim koeficijentima na osnovu njima pridruženih Newton-ovih poligona. Formalizacija potrebnog i dovoljnog uslova za postojanje netrivialne faktorizacije polinoma dve promenljive sa celobrojnim koeficijentima na faktor-polinome sa celobrojnim koeficijentima omogućava konstrukciju efektivnog algoritma za faktorizaciju. Konačno, dobijeni teorijski rezultati omogućavaju primenu na dekodiranje jedne klase Reed - Solomon kodova, miksa dve kodne reči.

Disertacija je organizovana na sledeći način:

U prvom poglavlju obrazložena je potreba za istraživanjem koje je predmet ove disertacije sa ciljem potpunog definisanja veze između polinoma dve promenljive sa celobrojnim koeficijentima i njima pridruženih Newton-ovih poligona u smislu ispitivanja njihove svodljivosti.

U drugom poglavlju dat je pregled osnovnih pojmova neophodnih za dalji rad.

U trećem poglavlju izložene su osobine konveksnih skupova, a u četvrtom poglavlju osobine potpornih pravih i lica poligona u odnosu na potporne prave, što daje teorijsku osnovu za analizu rastavlјivosti Newton-ovih poligona u smislu Minkowskog.

U petom poglavlju opisan je razvoj ideje o ispitivanju nesvodljivosti polinoma dve promenljive preko njima pridruženih poligona nastale uopštavanjem nekih stavova o nesvodljivosti polinoma jedne promenljive. U okviru ovog poglavlja okarakterisane su neke unutrašnje tačke Newton-ovog poligona, što je predstavljalo osnov za kasnije istraživanje.

U šestom poglavlju predstavljen je princip ispitivanja apsolutne nesvodljivosti polinoma dve promenljive analizom njima pridruženih Newton-ovih poligona.

U sedmom poglavlju dat je potreban i dovoljan uslov za postojanje netrivialne faktorizacije polinoma dve promenljive sa celobrojnim koeficijentima pomoću Newton-ovih poligona, što predstavlja glavni originalni teorijski doprinos disertacije izložen u [6]. Na taj način se u potpunosti objašnjava veza polinoma dve promenljive sa celobrojnim koeficijentima i njima pridruženih Newton-ovih poligona u smislu njihove svodljivosti.

U osmom poglavlju dat je algoritam za faktorizaciju polinoma dve promenljive sa celobrojnim koeficijentima u faktor - polinome sa celobrojnim koeficijentima prezentovan u [47].

U devetom poglavlju dobijeni teorijski rezultati iz predhodnog poglavlja primenjeni su na dekodiranje nekih klasa Reed-Solomon kodova, miksa dve kodne reči, što je izloženo u [47].

U desetom poglavlju izložen je zaključak rada.

U jedanaestom poglavlju izloženi su budući pravci istraživanja zasnovani na rezultatima disertacije.

U dvanaestom poglavlju naveden je spisak korišćene literature.

Abstract

The research subject of the thesis is factorization of bivariate polynomials with integer coefficients via associated Newton polygons. Formalization of the necessary and sufficient condition for the existence of a non-trivial factorization of an arbitrary bivariate polynomial with integer coefficients into factor-polynomials with integer coefficients obtains theoretical basis for construction of an effective factorization algorithm. Finally, these theoretical results are applied in decoding special class of Reed - Solomon codewords, mixture of two codewords.

The dissertation is organized in the following way:

In the first chapter the explanation of the need for research that is the subject of the thesis is given, aiming to complete the connection between bivariate polynomials with integer coefficients and associated Newton polygons in the sense of their reducibility testing.

In the second chapter a brief review of some basic concepts necessary for further research is given.

In the third chapter some properties of convex sets are presented and in the fourth chapter some properties of supporting lines and faces of polygons are listed, that gives theoretical basis for studying decompositivity of Newton polygons in the sense of Minkowski.

In the fifth chapter development of an idea of irreducibility testing of bivariate polynomials via associated polygons is presented. Such approach originates at geometrical generalisation of some irreducibility criterions for univariate polynomials. Also, in this chapter some inner points of Newton polygon are characterized, that enabled further research.

In the sixth chapter a concept of absolute irreducibility testing via associated Newton polygons is presented.

In the seventh chapter a necessary and sufficient condition for the existence of a non-trivial factorization of the bivariate polynomial with integer coefficients is given, that is the main original theoretical contribution of the dissertation presented in [6]. In that way the relationship between bivariate polynomials with integer coefficients and associated Newton polygons in the sense of their reducibility testing is fully explained.

In the eighth chapter an algorithm for factorization of bivariate polynomials with integer coefficients into factor-polynomials with integer coefficients is given, that is presented in [47].

The ninth chapter deals with an application of obtained theoretical results on decoding some classes of Reed - Solomon based codes, mixture of two code-words, presented in [47].

In the tenth chapter the conclusion of the dissertation is given.

In the eleventh chapter are listed directions for further research based on the results of the dissertation.

In the twelfth chapter a list of cited references is given.

Sadržaj

1	Uvod	8
2	Pregled osnovnih pojmova	10
3	Neke osobine konveksnih skupova	15
4	Potporne prave i lica poligona	23
5	Veza polinoma i poligona - Newton-ov poligon polinoma	33
6	Nesvodljivost polinoma dve promenljive pomoću Newton-ovih poligona	51
7	Faktorizacija polinoma dve promenljive sa celobrojnim koeficijentima pomoću Newton-ovih poligona	61
8	Algoritam za faktorizaciju polinoma dve promenljive sa celobrojnim koeficijentima	87
9	Primena faktorizacije polinoma dve promenljive sa celobrojnim koeficijentima u dekodiranju nekih klasa Reed-Solomon kodova	91
10	Zaključak	97
11	Budući pravci istraživanja i dalji rad	98
12	Literatura	99

1 Uvod

Faktorisanje polinoma se smatra fundamentalnim problemom u algebr i teoriji brojeva. Algoritmi koji su pronađeni u poslednjih četrdesetak godina učinili su mogućim da se, uz pomoć računara, efikasno faktoriše polinom sa jednom, dve ili više promenljivih sa koeficijentima iz određenog polja (npr. konačnog polja ili polja racionalnih, realnih ili kompleksnih brojeva).

Za polinome sa 10 promenljivih i 1000 monoma, pri čemu je najveći stepen pojedinačne promenljive 10, preko 85% ovakvih polinoma može biti prepoznato kao nesvodljivo u deliću sekunde korišćenjem brzih testova nesvodljivosti. Međutim, ovakvi testovi ne prepoznaju sve nesvodljive polinome, tako da bi trebali biti korišćeni kao pretest pre korišćenja opštijih i sporijih algoritama.

Klase apsolutno nesvodljivih polinoma su od ogromnog značaja u brojnim oblastima, pre svega u algebarskoj geometriji [24], kombinatorici [63], permutacionim polinomima [35] i algebarskim geometrijskim kodovima [64].

Za geometrijsku analizu nesvodljivosti polinoma više promenljivih neophodno je uvesti pojam Newton-ovog politopa. Ako se eksponenti polinoma sa n promenljivih posmatraju kao tačke u n -dimenzionalnom vektorskom prostoru \mathbb{R}^n , konveksan omotač tog skupa tačaka naziva se Newton-ov politop pridružen datom polinomu. Shuhong Gao analizira apsolutnu nesvodljivost polinoma više promenljivih preko njima pridruženih Newton-ovih politopa u [14] i [15]. Sa druge strane, pored geometrijske analize apsolutne nesvodljivosti polinoma više promenljivih, Shuhong Gao je dao značajan doprinos na polju faktorizacije polinoma više promenljivih pomoću parcijalnih diferencijalnih jednačina u [13].

Nakon niza radova u kojima se preko Newton-ovog poligona analizira nesvodljivost polinoma jedne i dve promenljive, zavisnost između apsolutne nesvodljivosti polinoma više promenljivih i nerastavljivosti u smislu Minkowskog njima pridruženih politopa konačno je pokazao Shuhong Gao u [14] iz 2001. godine. Međutim, analiza svodljivosti polinoma više promenljivih na osnovu njima pridruženih Newton-ovih politopa ostala je otvoren problem. Problem istraživanja disertacije je analiza Newton-ovog poligona polinoma dve promenljive sa ciljem pronalazjenja eventualnih faktorizacija.

Za polinom nad proizvoljnim poljem kažemo da je apsolutno nesvodljiv ako ostaje nesvodljiv nad svakom algebarskom ekstenzijom tog polja. Na osnovu

pridruženog politopa moguće je doneti zaključak o eventualnoj apsolutnoj nesvodljivosti odgovarajućeg polinoma. Pored poznate veze između apsolutne nesvodljivosti polinoma više promenljive i nerastavljivosti njima pridruženih Newton-ovih politopa, u ovom radu se rešava obratan problem za polinome dve promenljive sa celobrojnim koeficijentima, tj. ispituje se njihova svodljivost preko njima pridruženog Newton-ovog poligona. Na taj način se povezanost polinoma dve promenljive sa njima pridruženim Newton-ovim poligonima, u smislu geometrijske analize svodljivosti polinoma, u potpunosti opisuje.

Kako je politop dimenzije dva koji odgovara polinomu sa dve promenljive poligon, istraživanja u tezi će biti usmerena na polinome sa dve promenljive zbog postojanja jednostavne geometrijske interpretacije.

2 Pregled osnovnih pojmova

U ovom delu rada biće dat pregled osnovnih pojmova. Definicije ograničenog, otvorenog, zatvorenog i kompaktnog skupa mogu se naći u [12] i [31]. S obzirom na to da je predmet istraživanja ove disertacije geometrijska analiza svodljivosti polinoma dve promenljive preko njima pridruženih Newton-ovih poligona, ove definicije se navode za slučaj \mathbb{R}^2 .

Definicija 2.1. Skup $A \subset \mathbb{R}^2$ je **ograničen** ako je skup

$$\{d(a, b) : a, b \in A\}$$

ograničen u \mathbb{R} , gde je d standardna metrika.

Definicija 2.2. Skup $A \subset \mathbb{R}$ je **ograničen** ako je ograničen i sa gornje i sa donje strane.

Definicija 2.3. Skup $A \subset \mathbb{R}^2$ je **otvoren** ako je okolina svake svoje tačke.

Definicija 2.4. Skup $A \subset \mathbb{R}^2$ je **zatvoren** ako je njegov komplement u odnosu na \mathbb{R}^2 otvoren skup.

Definicija 2.5. Skup $A \subset \mathbb{R}^2$ je **kompaktan** ako je zatvoren i ograničen. Prazan skup je kompaktan.

Osnovni algebarski pojmovi i tvrđenja neophodni za dalji rad dati su u [40], [5], [33] i [48].

Definicija 2.6. Neka je G neprazan skup i \cdot binarna operacija skupa G . Uređenu dvojku (G, \cdot) nazivamo **grupoid** ako za sve $x, y \in G$ važi da i $x \cdot y \in G$.

Definicija 2.7. Grupoid (G, \cdot) je **polugrupa** ako za sve $x, y, z \in G$ važi $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Definicija 2.8. Grupoid (G, \cdot) je **grupa** ako važi:

$$(1) (\forall x, y, z \in G) x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$(2) (\exists e \in G)(\forall x \in G) e \cdot x = x \cdot e = x$$

$$(3) (\forall x \in G)(\exists y \in G) y \cdot x = x \cdot y = e$$

Napomena 2.9. Element e iz (2) predhodne definicije naziva se **jedinica**

grupe. Za element y iz (3) predhodne definicije kažemo da je *inverzni element* elementa x .

Definicija 2.10. Ako je u grupi (G, \cdot) ispunjeno:

$$x \cdot y = y \cdot x$$

za sve $x, y \in G$, onda za grupu G kažemo da je *komutativna* ili *Abelova* grupa.

Teorema 2.11. Neka je (G, \cdot) grupa. Tada važi:

$$a \cdot b = a \cdot c \Rightarrow b = c,$$

$$b \cdot a = c \cdot a \Rightarrow b = c,$$

za sve $a, b, c \in G$.

Napomena 2.12. Predhodna teorema je poznata pod nazivom *zakon kancelacije u grupi*.

Definicija 2.13. Neprazan podskup H grupe G je *podgrupa* grupe G , ako je H grupa u odnosu na restrikciju operacije grupe G na skupu H .

Teorema 2.14. Presek proizvoljne neprazne familije podgrupa neke grupe je podgrupa te grupe.

Napomena 2.15. Neka je A neprazan podskup grupe G . Obeležimo sa S skup svih podgrupa grupe G koji sadrže skup A . Skup S je neprazan jer $G \in S$. Na osnovu **Teoreme 2.14.**, $\cap S$ je podgrupa grupe G . Obično ovu podgrupu označavamo sa $[A]$, tj. $[A] = \cap S$. Očigledno je da je $[A]$ najmanja podgrupa grupe G koja sadrži skup A .

Definicija 2.16. Neka je A neprazan podskup grupe G . Tada podgrupu $[A]$ nazivamo *podgrupa generisana skupom* A . Ako je $[A] = G$, onda skup A nazivamo *generatorni skup grupe* G , a elemente skupa A *generatorni elementi grupe* G .

Definicija 2.17. Grupa koja ima jednočlani generatorni skup naziva se *ciklična grupa*.

Definicija 2.18. Broj elemenata konačne grupe G naziva se *red grupe*. Za element $a \in G$, broj elemenata ciklične podgrupe $[\{a\}]$ grupe G nazivamo *red*

elementa a .

Definicija 2.19. Uređena trojka $(F, +, \cdot)$, gde je F neprazan skup, a $+$ i \cdot dve binarne operacije skupa F , je **prsten** ako važi:

(1) $(F, +)$ je komutativna grupa

(2) (F, \cdot) je polugrupa

(3) Za sve $x, y, z \in F$ važi:

$$x \cdot (y + z) = x \cdot y + x \cdot z,$$

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Definicija 2.20. Neka je $(F, +, \cdot)$ prsten.

(1) Prsten F je **prsten sa jedinicom**, ako F ima multiplikativnu jedinicu, tj. postoji element $e \in F$ takav da za sve $x \in F$ važi: $e \cdot x = x \cdot e = x$.

(2) Prsten F je **komutativan**, ako je multiplikativna operacija komutativna, tj. za sve $x, y \in F$ važi: $x \cdot y = y \cdot x$.

(3) Prsten F je **integralni domen** ako je komutativan prsten sa jedinicom i za sve $x, y \in F$ za koje važi: $x \cdot y = 0$ je $x = 0$ ili $y = 0$ (ne postoje delitelji nule).

(4) Prsten F je **polje** ako je $(F \setminus \{0\}, \cdot)$ komutativna grupa.

Definicija 2.21. Neka je $(F, +, \cdot)$ polje i e jedinica polja F . Ako postoji prirodan broj n takav da je $ne = 0$, onda najmanji takav broj p za koji je $pe = 0$ nazivamo **karakteristika** polja F . U tom slučaju kažemo da je polje **konačne karakteristike**. Ako ne postoji prirodan broj n takav da je $ne = 0$, onda kažemo da je polje F **karakteristike 0** ili **beskonačne karakteristike**.

Teorema 2.22. Ako je polje F konačne karakteristike, onda je karakteristika polja F prost broj.

Napomena 2.23. Polja konačne karakteristike se u čast francuskog matematičara Evariste Galois-a nazivaju i **poljima Galois-a**. Za konačno polje karakteristike p , često se u literaturi koristi oznaka $GF(p)$.

Definicija 2.24. Za element α polja konačne karakteristike $GF(p)$ kažemo da je **primitivni element polja** $GF(p)$ ako je α generatorni element multiplikativne grupe polja.

Teorema 2.25. Skup polinoma dve promenljive sa koeficijentima iz polja F , u oznaci $F[x, y]$, ima strukturu integralnog domena, odnosno komutativnog prstena sa jedinicom bez delitelja nule. Skup polinoma dve promenljive sa koeficijentima iz \mathbb{Z} , u oznaci $\mathbb{Z}[x, y]$, takođe ima strukturu integralnog domena.

Definicija 2.26. Za nenula polinom $f(x, y) \in \mathbb{Z}[x, y]$ kažemo da ima **netrivijalnu faktorizaciju** nad \mathbb{Z} ako postoje polinomi $g(x, y), h(x, y) \in \mathbb{Z}[x, y]$ takvi da oba imaju bar po dva monoma i da važi: $f(x, y) = g(x, y) \cdot h(x, y)$. Ako se neki od polinoma $g(x, y)$ i $h(x, y)$ sastoji samo od jednog monoma različitog od konstante, posmatrana faktorizacija je **trivijalna**. Ako polinom $f(x, y)$ nema ni netrivijalnu ni trivijalnu faktorizaciju nad \mathbb{Z} kažemo da je polinom $f(x, y)$ **nesvodljiv** nad \mathbb{Z} .

Napomena 2.27. Pojmovi netrivijalne faktorizacije, trivijalne faktorizacije i nesvodljivosti polinoma, koji su u **Definiciji 2.26.** uvedeni na prstenu celih brojeva \mathbb{Z} , mogu se definisati i za polinom nad proizvoljnim poljem.

Definicija 2.28. Neka je F proizvoljno polje. Kažemo da je $S, S \subset F$, **potpolje** polja F ako je S polje.

Definicija 2.29. Neka je S potpolje polja F , tada polje F nazivamo **ekstenzijom polja** S .

Definicija 2.30. Neka je F ekstenzija polja S . Element $a \in F$ naziva se **algebarski element** nad poljem S ako je $f(a) = 0$, za neki nenula polinom $f(x) \in S[x]$. U suprotnom, element $a \in F$ se naziva **transcendentni element**. Ekstenzija F je **algebarska ekstenzija** polja S ako je svaki element $a \in F$ algebarski element nad poljem S . U suprotnom ekstenzija F se naziva **transcendentnom ekstenzijom** polja S .

Definicija 2.31. Polinom nad poljem F je **apsolutno nesvodljiv** ako je nesvodljiv nad svakom algebarskom ekstenzijom polja F .

Primer 2.32. Polinom $f(x, y) = x^2 + y^2 \in \mathbb{Z}[x, y]$ je polinom nad poljem \mathbb{Q} i nesvodljiv je nad poljem \mathbb{Q} i nad njegovom algebarskom ekstenzijom, poljem \mathbb{R} .

Međutim, s obzirom na to da važi: $x^2 + y^2 = (x + iy)(x - iy)$, polinom $f(x, y)$ je svodljiv nad poljem \mathbb{C} koje je algebarska ekstenzija polja \mathbb{R} , pa nije apsolutno nesvodljiv.

Primer 2.33. Polinom $f(x, y) = x^2 + y^2 - 1 \in \mathbb{Z}[x, y]$ je apsolutno nesvodljiv.

Definicija 2.34. **Domen jedinstvene faktorizacije** je komutativan prsten sa jedinicom koji je integralni domen u kome svaki element različit od nule i jedinice može biti predstavljen kao proizvod nesvodljivih elemenata različitih od jedinice jedinstveno do na permutaciju činilaca.

Primer 2.35. Prsten celih brojeva \mathbb{Z} je domen jedinstvene faktorizacije.

3 Neke osobine konveksnih skupova

S obzirom na to da je oblast istraživanja disertacije faktorizacija polinoma dve promenljive sa celobrojnim koeficijentima preko Newton-ovih poligona, u ovom poglavlju dat je pregled nekih osobina konveksnih skupova neophodnih za dalji rad. Osobine konveksnih skupova mogu se naći u [68] i [1], a sve definicije i tvrđenja u ovoj disertaciji su navedene za slučaj \mathbb{R}^2 .

Obeležimo sa \mathbb{R}^2 dvodimenzionalni Euklidski prostor. Elemente tog prostora $v = (x, y)$ nazivamo vektorima ili tačkama. Sa $\|v\|$ obeležimo Euklidsku normu (dužinu) vektora v :

$$\|v\| = \sqrt{x^2 + y^2}.$$

U prostoru \mathbb{R}^2 vektorska jednačina prave kroz tačke a i b ima sledeći oblik:

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

Zatvorena duž $[a, b]$ usmerena od tačke a ka tački b se dobija kada $t \in [0, 1]$.

Formalne definicije zatvorene i otvorene usmerene duži u \mathbb{R}^2 glase:

Definicija 3.1. Neka su a i b proizvoljne tačke u \mathbb{R}^2 . **Zatvorena duž usmerena od tačke a ka tački b** u oznaci $[a, b]$ se definiše na sledeći način:

$$[a, b] = \{z \in \mathbb{R}^2 : z = (1 - t)a + tb, 0 \leq t \leq 1\}.$$

Definicija 3.2. Neka su a i b proizvoljne tačke u \mathbb{R}^2 . **Otvorena duž usmerena od tačke a ka tački b** u oznaci (a, b) se definiše na sledeći način:

$$(a, b) = \{z \in \mathbb{R}^2 : z = (1 - t)a + tb, 0 < t < 1\}.$$

Primedba 3.3. Poluotvorena usmerena duž $[a, b)$ koja sadrži tačku a , ali ne sadrži tačku b dobija se za parametar $t \in [0, 1)$. Poluotvorena usmerena duž $(a, b]$ se definiše potpuno analogno.

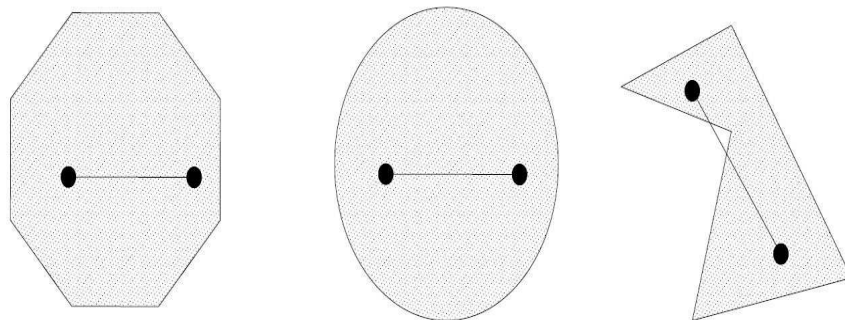
Definicija 3.4. Skup S , $S \subseteq \mathbb{R}^2$ je **konveksan** ako za bilo koje dve tačke a i b , $a, b \in S$ važi $[a, b] \subseteq S$.

Dakle, skup je konveksan ako za svake svoje dve tačke sadrži i celu duž koja ih spaja. Na primer, tačka, prava i kružnica zajedno sa svojim unutrašnjim tačkama su konveksni skupovi u \mathbb{R}^2 . Prazan skup i \mathbb{R}^2 su takođe konveksni. Primeri konveksnih i nekonveksnih skupova dati su na Slici 1.

konveksan skup

konveksan skup

nekonveksan skup



Slika 1

Teorema 3.5. Neka je $\{C_i\}_{i \in I}$ proizvoljna kolekcija konveksnih skupova u \mathbb{R}^2 . Tada je i skup $\bigcap_{i \in I} C_i$ konveksan.

Dokaz:

Neka $a, b \in \bigcap_{i \in I} C_i$. Po definiciji preseka skupova, to znači da $a, b \in C_i$, za sve $i \in I$. Kako su $C_i, i \in I$, konveksni skupovi, sledi da $[a, b] \subseteq C_i$, za sve $i \in I$, odnosno $[a, b] \subseteq \bigcap_{i \in I} C_i$. Dakle, $\bigcap_{i \in I} C_i$ je konveksan skup. \square

Definicija 3.6. **Konveksan omotač skupa** $S \subseteq \mathbb{R}^2$, u oznaci $\text{conv}(S)$, je najmanji konveksan skup koji sadrži skup S , tj. presek svih konveksnih skupova koji sadrže S :

$$\text{conv}(S) = \left\{ \bigcap_{S \subseteq K} K, K \subseteq \mathbb{R}^2, K \text{ je konveksan skup} \right\}.$$

Primedba 3.7. Kako je prazan skup konveksan, jasno je da važi $\text{conv}(\emptyset) = \emptyset$.

Primedba 3.8. Ako je skup S konačan, $S \subseteq \mathbb{R}^2$, tj. $S = \{a_1, \dots, a_k\}$, skup

$\text{conv}(S)$ obeležavamo sa $\text{conv}(a_1, \dots, a_k)$ i nazivamo ga **konveksni omotač tačkaka** a_1, \dots, a_k .

Definicija 3.9. Neka je $a_1, \dots, a_k \in \mathbb{R}^2$. Za tačku x kažemo da je **konveksna kombinacija tačkaka** a_1, \dots, a_k ako postoje realni brojevi $\lambda_1, \dots, \lambda_k$ takvi da važi:

$$x = \lambda_1 a_1 + \dots + \lambda_k a_k,$$

pri čemu je:

$$\lambda_1 \geq 0, \dots, \lambda_k \geq 0, \lambda_1 + \dots + \lambda_k = 1.$$

Sledećom teoremom ćemo pokazati da je konveksni omotač skupa S zapravo skup svih mogućih konveksnih kombinacija elemenata skupa S .

Teorema 3.10. Neka je S proizvoljan podskup \mathbb{R}^2 . Tada važi:

- (1) $\text{conv}(S) = \left\{ \sum_{i=1}^k \lambda_i a_i, \{a_1, \dots, a_k\} \subseteq S, \lambda_i \geq 0, i = 1, \dots, k, \sum_{i=1}^k \lambda_i = 1 \right\}$,
- (2) Skup S je konveksan ako i samo ako $S = \text{conv}(S)$
- (3) Ako je skup S konačan, tj. $S = \{a_1, \dots, a_m\} \subseteq \mathbb{R}^2$, tada je:

$$\text{conv}(S) = \left\{ \lambda_1 a_1 + \dots + \lambda_m a_m, \lambda_i \geq 0, i = 1, \dots, m, \sum_{i=1}^m \lambda_i = 1 \right\}.$$

Dokaz:

(1) Označimo desnu stranu jednakosti sa Δ . Pokažimo najpre da je skup Δ konveksan. Neka:

$$x = \sum_{i=1}^k \lambda_i x_i \in \Delta$$

i

$$y = \sum_{i=1}^m \eta_i y_i \in \Delta,$$

pri čemu:

$$x_1, \dots, x_k, y_1, \dots, y_m \in S, \lambda_1, \dots, \lambda_k, \eta_1, \dots, \eta_m \geq 0, \lambda_1 + \dots + \lambda_k = \eta_1 + \dots + \eta_m = 1.$$

Formirajmo konveksnu kombinaciju x i y :

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

pri čemu:

$$(1 - \lambda)\lambda_1, \dots, (1 - \lambda)\lambda_k, \lambda\eta_1, \dots, \lambda\eta_m \geq 0.$$

S obzirom na to da važi:

$$\begin{aligned} & (1 - \lambda)\lambda_1 + \dots + (1 - \lambda)\lambda_k + \lambda\eta_1 + \dots + \lambda\eta_m = \\ & = (1 - \lambda)(\lambda_1 + \dots + \lambda_k) + \lambda(\eta_1 + \dots + \eta_m) = (1 - \lambda) + \lambda = 1, \end{aligned}$$

sledi:

$$(1 - \lambda)x + \lambda y \in \Delta.$$

Kako je $\text{conv}(S)$ najmanji konveksan skup koji sadrži skup S , a Δ je konveksan skup koji sadrži skup S , važi: $\text{conv}(S) \subseteq \Delta$.

Indukcijom po k pokažimo da važi i obrnuta inkluzija $\Delta \subseteq \text{conv}(S)$.

Za $k = 1$, dobijamo: $1x_1 = x_1 \in S \subseteq \text{conv}(S)$.

Pretpostavimo da inkluzija važi za $k - 1$.

Posmatrajmo bilo koji konačan skup $\{x_1, \dots, x_k\} \subseteq S$ i parametre $\lambda_1, \dots, \lambda_k \geq 0$, $\lambda_1 + \dots + \lambda_k = 1$ i pokažimo da se tačka $\lambda_1 x_1 + \dots + \lambda_k x_k$ iz Δ nalazi u $\text{conv}(S)$.
Za $\lambda_k \neq 1$:

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

Ako je $\lambda_k = 1$ dobijamo da je $\lambda_1 x_1 + \dots + \lambda_k x_k = x_k$, a $x_k \in S \subseteq \text{conv}(S)$.

Pretpostavimo, dakle, da je $\lambda_k < 1$. Uvedimo oznaku:

$$z = \frac{\lambda_1}{1 - \lambda_k} x_1 + \dots + \frac{\lambda_{k-1}}{1 - \lambda_k} x_{k-1}.$$

S obzirom na to da je:

$$\frac{\lambda_1}{1 - \lambda_k} + \dots + \frac{\lambda_{k-1}}{1 - \lambda_k} = \frac{\lambda_1 + \dots + \lambda_{k-1}}{1 - \lambda_k} = \frac{1 - \lambda_k}{1 - \lambda_k} = 1,$$

na osnovu indukcijske pretpostavke sledi:

$$z \in \text{conv}(S).$$

Dalje dobijamo:

$$\lambda_1 x_1 + \dots + \lambda_k x_k = (1 - \lambda_k)z + \lambda_k x_k,$$

pri čemu $z \in \text{conv}(S)$, $x_k \in S \subseteq \text{conv}(S)$ i $(1 - \lambda_k) + \lambda_k = 1$.

Kako je $0 \leq \lambda_k < 1$, jasno je da važi i $0 < 1 - \lambda_k \leq 1$.

Oдавde, na osnovu indukcijske pretpostavke, sledi:

$$(1 - \lambda_k)z + \lambda_k x_k \in \text{conv}(S),$$

tj.

$$\lambda_1 x_1 + \dots + \lambda_k x_k \in \text{conv}(S).$$

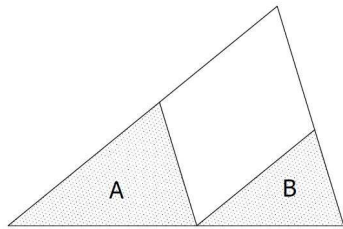
(2) Neka je S konveksan skup. Uvek važi $S \subseteq \text{conv}(S)$. Kako je $\text{conv}(S)$ najmanji konveksan skup koji sadrži skup S , a S konveksan skup koji sadrži skup S važi i $\text{conv}(S) \subseteq S$. Sledi $\text{conv}(S) = S$.

Neka važi $S = \text{conv}(S)$. Kako je $\text{conv}(S)$ konveksan skup, onda je to i S .

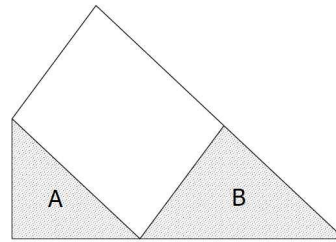
(3) Ovo tvrđenje je očigledna posledica (1). \square

Definicija 3.11. Neka su $A, B \subseteq \mathbb{R}^2$. Skup $A + B = \{a + b : a \in A, b \in B\}$ se naziva **suma Minkowskog** skupova A i B .

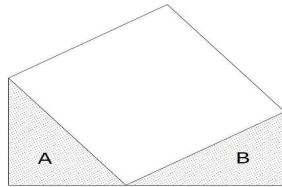
Suma Minkowskog dva trougla A i B u ravni je trougao, četvorougao, petougao ili šestougao, što je prikazano na Slikama 2.1-2.4. S obzirom na to da položaj rezultantnog poligona sume Minkowskog dva poligona zavisi od njihovog položaja u odnosu na koordinatni početak, na Slikama 2.1-2.4. su prikazani rezultantni poligoni u smislu sume Minkowskog do na translaciju.



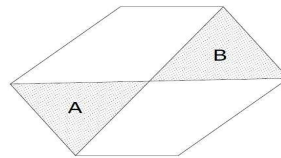
Slika 2.1



Slika 2.2

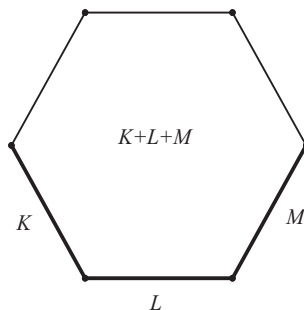


Slika 2.3



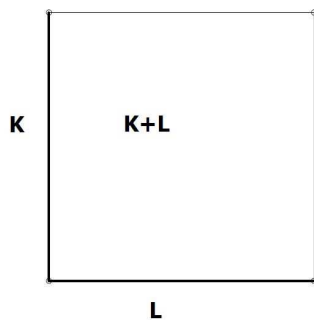
Slika 2.4

Svaki centralno simetričan dvodimenzionalni $2n$ -gon može se predstaviti kao suma n duži. Šestougao u ravni koji ima naspramne stranice paralelne može se predstaviti kao suma tri duži K , L i M (Slika 3), ali i kao suma dva trougla A i B , kao što je prikazano na Slici 2.4. Dakle, predstavljanje konveksnog i kompaktnog skupa kao konačne sume konveksnih i kompaktnih skupova, ako je moguće, nije jedinstveno.



Slika 3

Pravougaonik, centralno simetričan četvorougao u ravni, može se predstaviti kao suma dve duži, što je prikazano na Slici 4.



Slika 4

Teorema 3.12. Neka je τ označena proizvoljna translacija, a $+$ suma Minkowskog skupova. Tada za proizvoljne skupove A i B iz \mathbb{R}^2 važi:

$$(1) \tau(A) + B = \tau(A + B) = A + \tau(B)$$

(2) Ako su skupovi A i B oba konveksni, zatvoreni i konveksni ili kompaktni i konveksni skupovi u \mathbb{R}^2 , onda je i $A + B$ konveksan, zatvoren i konveksan ili kompaktna i konveksan skup.

Dokaz:

(1) Ako je translacija τ određena vektorom t , na osnovu asocijativnosti i komutativnosti sume Minkowskog važi:

$$(t + A) + B = t + (A + B) = A + (t + B),$$

a odavde direktno sledi tvrđenje teoreme.

(2) Pokažimo da ako su A i B konveksni skupovi u \mathbb{R}^2 , onda je to i skup $A+B$. Skup $A+B$ je konveksan ako za proizvoljne $a+b \in A+B$ i $a'+b' \in A+B$, pri čemu $a, a' \in A$ i $b, b' \in B$ i proizvoljno $\lambda, 0 \leq \lambda \leq 1$, važi da:

$$\lambda(a+b) + (1-\lambda)(a'+b') \in A+B.$$

Zaista,

$$\begin{aligned} \lambda(a+b) + (1-\lambda)(a'+b') &= \lambda a + \lambda b + (1-\lambda)a' + (1-\lambda)b' = \\ &= \lambda a + (1-\lambda)a' + \lambda b + (1-\lambda)b', \end{aligned}$$

Kako $a, a' \in A$, a skup A je konveksan pa sadrži svaku konveksnu kombinaciju svojih elemenata, važi:

$$\lambda a + (1-\lambda)a' \in A.$$

Potpuno analogno je:

$$\lambda b + (1-\lambda)b' \in B.$$

Dakle važi:

$$\lambda(a+b) + (1-\lambda)(a'+b') \in A+B,$$

što je i trebalo pokazati.

Ako su A i B zatvoreni i ograničeni skupovi u \mathbb{R}^2 , onda je to i skup $A+B$, jer je suma Minkowskog neprekidna operacija i preslikava parove ograničenih skupova na ograničen skup. \square

Primedba 3.13.

(1) Suma Minkowskog može se zapisati u formi: $A+B = \bigcup_{b \in B} (A+b)$.

(2) Ako $\lambda \in \mathbb{R}$ i $A \subseteq \mathbb{R}^2$, onda skup λA definišemo na sledeći način:

$$\lambda A = \{\lambda a : a \in A\}.$$

Ako su dati $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ i skupovi $A_1, \dots, A_k \subseteq \mathbb{R}^2$, onda $\lambda_1 A_1 + \dots + \lambda_k A_k$ nazivamo *linearnom kombinacijom skupova* A_1, \dots, A_k , pri čemu neki od koeficijenata $\lambda_1, \dots, \lambda_k$ mogu biti negativni. Primetimo, $(-1)A = -A$ nije suprotan element za A u smislu sume Minkowskog. Zaista, na Slici 2.4, ako je koordinatni početak u zajedničkom temenu trouglova A i B , jasno je da je $B = -A$, ali $A + B$ nije prazan skup, nego šestougao.

Teorema 3.14. Ako su A_1, \dots, A_k konveksni skupovi u \mathbb{R}^2 i $\lambda_1, \dots, \lambda_k$ realni brojevi, onda je i $\lambda_1 A_1 + \dots + \lambda_k A_k$ konveksan skup.

Dokaz:

Neka $x, y \in \lambda_1 A_1 + \dots + \lambda_k A_k$ i neka je λ proizvoljno $0 \leq \lambda \leq 1$ fiksirano, treba pokazati da:

$$\lambda x + (1 - \lambda)y \in \lambda_1 A_1 + \dots + \lambda_k A_k.$$

S obzirom na to da je $x \in \lambda_1 A_1 + \dots + \lambda_k A_k$, sledi da je $x = \lambda_1 x_1 + \dots + \lambda_k x_k$, za neke $x_1 \in A_1, \dots, x_k \in A_k$. Kako važi $y \in \lambda_1 A_1 + \dots + \lambda_k A_k$, sledi da je $y = \lambda_1 y_1 + \dots + \lambda_k y_k$, za neke $y_1 \in A_1, \dots, y_k \in A_k$.

Dobijamo:

$$\lambda x + (1 - \lambda)y = \lambda(\lambda_1 x_1 + \dots + \lambda_k x_k) + (1 - \lambda)(\lambda_1 y_1 + \dots + \lambda_k y_k),$$

odnosno:

$$\lambda x + (1 - \lambda)y = \lambda \lambda_1 x_1 + \dots + \lambda \lambda_k x_k + (1 - \lambda)\lambda_1 y_1 + \dots + (1 - \lambda)\lambda_k y_k.$$

Kako je množenje realnih brojeva komutativno, sledi:

$$\lambda x + (1 - \lambda)y = \lambda_1 \lambda x_1 + \dots + \lambda_k \lambda x_k + \lambda_1 (1 - \lambda)y_1 + \dots + \lambda_k (1 - \lambda)y_k.$$

Dalje dobijamo:

$$\lambda x + (1 - \lambda)y = \lambda_1 (\lambda x_1 + (1 - \lambda)y_1) + \dots + \lambda_k (\lambda x_k + (1 - \lambda)y_k).$$

Kako je A_1 konveksan i $x_1, y_1 \in A_1$, važi da i $\lambda x_1 + (1 - \lambda)y_1 \in A_1$.

Potpuno analogno zaključujemo da:

$$\lambda x_2 + (1 - \lambda)y_2 \in A_2, \dots, \lambda x_k + (1 - \lambda)y_k \in A_k.$$

Konačno dobijamo:

$$\lambda x + (1 - \lambda)y \in \lambda_1 A_1 + \dots + \lambda_k A_k,$$

što je i trebalo pokazati. \square

4 Potporne prave i lica poligona

Za geometrijsku analizu svodljivosti polinoma dve promenljive neophodno je uvesti pojam potporne prave i lica poligona, kao i navesti tvrđenja u vezi sa dekompozicijom lica poligona u smislu Minkowskog, što je pregledno izloženo u [29]. Inače, detaljnije o dekompoziciji politopa u smislu Minkowskog se može naći u [10], [19] i [52].

Neka je $P \subset \mathbb{R}^2$ konveksan i kompaktan skup. Kako je skalarni proizvod neprekidna funkcija, za proizvoljan nenula vektor $v = (v_1, v_2) \in \mathbb{R}^2$ važi:

$$\sup_{p \in P} (p \cdot v) = \max\{p \cdot v \mid p \in P\},$$

gde je:

$$p \cdot v = p_1 v_1 + p_2 v_2$$

skalarni proizvod vektora $p = (p_1, p_2)$ i $v = (v_1, v_2)$ u \mathbb{R}^2 .

Definicija 4.1. Neka je $P \subset \mathbb{R}^2$ neprazan, konveksan i kompaktan skup. Preslikavanje:

$$h_P : \mathbb{R}^2 \rightarrow \mathbb{R}, v \rightarrow \sup_{p \in P} (p \cdot v)$$

naziva se **potporna funkcija skupa** P .

Definicija 4.2. Neka $v \in \mathbb{R}^2$ i $s \in \mathbb{R}$. Skup tačaka:

$$H = \{x \in \mathbb{R}^2 : v \cdot x = s\}$$

je prava u \mathbb{R}^2 . **Zatvorene poluravni određene sa** H definisane su na sledeći način:

$$H^- = \{x \in \mathbb{R}^2 : v \cdot x \leq s\}, H^+ = \{x \in \mathbb{R}^2 : v \cdot x \geq s\}.$$

Definicija 4.3. Prava H_P naziva se **potporna prava** zatvorenog i konveksnog skupa P , $P \subset \mathbb{R}^2$ ako $P \subset H_P^-$ ili $P \subset H_P^+$ i $P \cap H_P \neq \emptyset$, tj. H_P sadrži rubnu tačku skupa P . Potporna prava H_P skupa P naziva se **netrivijalna potporna prava** ako skup P nije sadržan u H_P .

Skupovi H_P^- i H_P^+ nazivaju se **potpornim poluravninama** skupa P .

Napomena 4.4. Jedini konveksan poligon koji ima trivijalnu potpornu pravu je duž.

Teorema 4.5.

- (1) Ako je $P+a$ translacija konveksnog i kompaktnog skupa $P \subset \mathbb{R}^2$ za vektor $a \in \mathbb{R}^2$, onda je:

$$h_{P+a}(v) = h_P(v) + a \cdot v, \text{ za sve } v \in \mathbb{R}^2$$

- (2) Za svaki nenula vektor $v \in \mathbb{R}^2$, prava

$$H_P(v) = \{x \in \mathbb{R}^2 : x \cdot v = h_P(v)\},$$

je potporna prava konveksnog i kompaktnog skupa P .

- (3) Svaka potporna prava konveksnog i kompaktnog skupa P ima reprezentaciju u formi definisanoj u (2)

Dokaz:

- (1) Za svaki vektor $v \in \mathbb{R}^2$ važi:

$$\begin{aligned} h_{P+a}(v) &= \sup_{x \in P+a} (x \cdot v) = \sup_{x \in P} (x+a) \cdot v = \\ &= \sup_{x \in P} (x \cdot v + a \cdot v) = \sup_{x \in P} (x \cdot v) + a \cdot v = h_P(v) + a \cdot v \end{aligned}$$

- (2) Kako je funkcija skalarnog proizvoda neprekidna, neprekidna je i potporna funkcija konveksnog i kompaktnog skupa P , $h_P(v) = \sup_{x \in P} (x \cdot v)$.

Neprekidna funkcija $h_P(v)$ na kompaktnom skupu P dostiže maksimum, tj. postoji $x_0 \in P$ takav da važi:

$$h_P(v) = x_0 \cdot v = \max_{x \in P} (x \cdot v).$$

Dakle, za bilo koje $x \in P$ važi:

$$x \cdot v \leq x_0 \cdot v,$$

što znači:

$$P \subset H_P^-(v),$$

tj. $H_P(v)$ je potporna prava konveksnog i kompaktnog skupa P .

(3) Neka je $H_P(v) = \{x \in \mathbb{R}^2 : x \cdot v = x_0 \cdot v\}$ potporna prava konveksnog i kompaktnog skupa P u tački x_0 . Možemo izabrati nenula vektor $v \in \mathbb{R}^2$ za koji važi:

$$P \subset H_P^-(v).$$

Tada za taj vektor v važi:

$$x_0 \cdot v = \sup_{x \in P} x \cdot v = h_P(v).$$

Dakle, $H_P(v)$ potporna prava skupa P u tački x_0 može se zapisati i na sledeći način:

$$H_P(v) = \{x \in \mathbb{R}^2 : x \cdot v = h_P(v)\},$$

što je i trebalo pokazati. \square

Napomena 4.6. Pojmovi i tvrđenja izloženi u ovom poglavlju dati su za slučaj \mathbb{R}^2 , s obzirom na to da je predmet istraživanja disertacije faktorizacija polinoma dve promenljive preko Newton-ovih poligona. Naravno, tvrđenja važe i za slučaj \mathbb{R}^n .

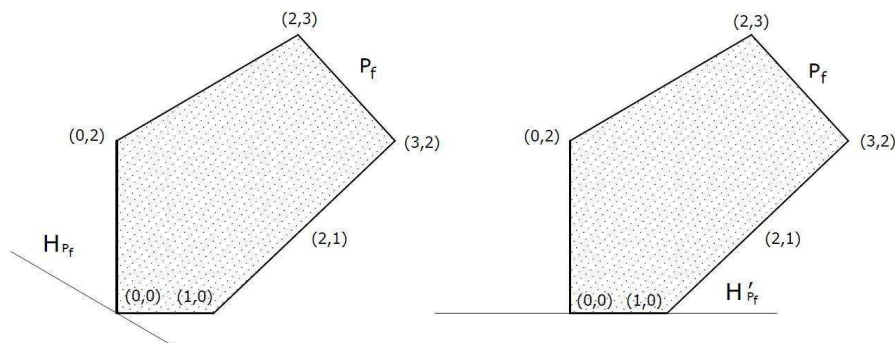
Definicija 4.7. Neka je P konveksan poligon i H_P njegova potporna prava. Presek poligona P i prave H_P se naziva **lice poligona** P u odnosu na potpornu pravu H_P .

Napomena 4.8. Kako svaka potporna prava poligona P_f ima neprazan presek sa tim poligonom i poligon je sadržan u jednoj od dve zatvorene poluravnii određene tom pravom, jasno je da lice Newton-ovog poligona polinoma $f(x, y)$, u odnosu na neku potpornu pravu, može biti teme ili ivica poligona P_f .

Primer 4.9. Posmatrajmo polinom:

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

Na Slici 5 su prikazane dve potporne prave Newton-ovog poligona polinoma f , u oznaci P_f . U prvom slučaju lice poligona u odnosu na potpornu pravu H_{P_f} je teme $(0, 0)$, a u drugom slučaju lice poligona u odnosu na potpornu pravu H'_{P_f} je ivica poligona P_f koja spaja temena $(0, 0)$ i $(1, 0)$.



Slika 5

Sledeća teorema daje najvažnije osobine dekompozicije poligona.

Teorema 4.10. Neka su $h_K(v)$ i $h_L(v)$ potporne funkcije konveksnih i kompaktnih skupova $K, L \subset \mathbb{R}^2$ u odnosu na proizvoljan vektor $v \in \mathbb{R}^2$, $v = (u, w)$, gde su $u, w > 0$. Tada važi:

- (1) $h_K(v) + h_L(v)$ je potporna funkcija kompaktnog i konveksnog skupa $K + L$, tj.

$$h_{K+L}(v) = h_K(v) + h_L(v).$$

- (2) $H_{K+L}(v) = H_K(v) + H_L(v)$,

- (3) Ako je F lice skupa $K + L$, onda postoje jedinstvena lica F_K i F_L skupova K i L takva da važi:

$$F = F_K + F_L.$$

Svako teme $K + L$ je suma temena K i L .

- (4) Ako su K i L konveksni poligoni, onda je to i $K + L$.

Dokaz:

- (1) Kako su konveksni poligoni K, L kompaktni skupovi, na osnovu **Teoreme 3.12.**, (2), $K + L$ je konveksan i kompaktan skup. Uzmimo, sada, proizvoljan vektor $v \in \mathbb{R}^2$, $v = (u, w)$, gde su $u, w > 0$. Za taj vektor v važi:

$$h_{K+L}(v) = \sup_{x \in K, y \in L} (x + y) \cdot v = \sup_{x \in K, y \in L} (x \cdot v + y \cdot v) =$$

$$= \sup_{x \in K} x \cdot v + \sup_{y \in L} y \cdot v = h_K(v) + h_L(v)$$

(2) Pokažimo najpre: $H_{K+L}(v) \subseteq H_K(v) + H_L(v)$. Neka je:

$$(x, y) \in H_{K+L}(v) = \{(a, b) \in \mathbb{R}^2 \mid (a, b) \cdot (u, w) = h_{K+L}(v)\}, v = (u, w).$$

Na osnovu (1) dobijamo:

$$(x, y) \cdot (u, w) = h_{K+L}(v) = h_K(v) + h_L(v) \quad (2.1.)$$

Jasno:

$$h_K(v) = \sup_{(a,b) \in K} [(a, b) \cdot (u, w)]$$

i

$$h_L(v) = \sup_{(c,d) \in L} [(c, d) \cdot (u, w)].$$

Pošto su K i L kompaktni skupovi, supremum se na njima dostiže, tj. postoje tačke $(a_0, b_0) \in K$ i $(c_0, d_0) \in L$ takve da važi:

$$h_K(v) = \sup_{(a,b) \in K} [(a, b) \cdot (u, w)] = (a_0, b_0) \cdot (u, w) \quad (2.2.)$$

$$h_L(v) = \sup_{(c,d) \in L} [(c, d) \cdot (u, w)] = (c_0, d_0) \cdot (u, w) \quad (2.3.)$$

Uvrštavanjem (2.2.) i (2.3.) u (2.1.) dobijamo:

$$(x, y) \cdot (u, w) = (a_0, b_0) \cdot (u, w) + (c_0, d_0) \cdot (u, w),$$

odnosno:

$$(x, y) \cdot (u, w) = (a_0 + c_0, b_0 + d_0) \cdot (u, w).$$

Oдавde sledi:

$$(x, y) \cdot (u, w) - (a_0 + c_0, b_0 + d_0) \cdot (u, w) = 0,$$

odnosno:

$$[(x, y) - (a_0 + c_0, b_0 + d_0)] \cdot (u, w) = 0,$$

pa je:

$$[x - (a_0 + c_0), y - (b_0 + d_0)] \cdot (u, w) = 0.$$

S obzirom na to da je $u, w > 0$ važi:

$$(x - (a_0 + c_0), y - (b_0 + d_0)) = (0, 0),$$

tj.

$$x = a_0 + c_0 \text{ i } y = b_0 + d_0.$$

Dakle:

$$(x, y) = (a_0 + c_0, b_0 + d_0) = (a_0, b_0) + (c_0, d_0).$$

Kako $(a_0, b_0) \in H_K(v)$ i $(c_0, d_0) \in H_L(v)$, važi:

$$(x, y) \in H_K(v) + H_L(v).$$

Pokažimo i obratnu inkluziju $H_K(v) + H_L(v) \subseteq H_{K+L}(v)$. Neka

$$(x, y) \in H_K(v) + H_L(v).$$

Tada postoje $(x_K, y_K) \in H_K$ i $(x_L, y_L) \in H_L$ takvi da važi:

$$x = x_K + x_L \text{ i } y = y_K + y_L.$$

S obzirom na to da $(x_K, y_K) \in H_K$ važi:

$$\sup_{(a,b) \in K} [(a, b) \cdot (u, w)] = (x_K, y_K) \cdot (u, w) = h_K(v).$$

S obzirom na to da $(x_L, y_L) \in H_L$ važi:

$$\sup_{(c,d) \in L} [(c, d) \cdot (u, w)] = (x_L, y_L) \cdot (u, w) = h_L(v).$$

Sabiranjem poslednje dve jednakosti dobijamo:

$$(x_K, y_K) \cdot (u, w) + (x_L, y_L) \cdot (u, w) = h_K(v) + h_L(v),$$

odnosno:

$$(x_K + x_L, y_K + y_L) \cdot (u, w) = h_K(v) + h_L(v).$$

Na osnovu (1) sledi:

$$(x_K + x_L, y_K + y_L) \cdot (u, w) = h_{K+L}(v).$$

Oдавде sledi da je:

$$(x_K + x_L, y_K + y_L) \in H_{K+L}(v),$$

tj.

$$(x, y) \in H_{K+L}(v).$$

(3) Na osnovu **Teoreme 4.5.**, (2), za kompaktnan i konveksan skup $K + L$ i nenula vektor v sa ciljnom tačkom izvan skupa $K + L$, prava $H_{K+L}(v) = \{x \in \mathbb{R}^2 : x \cdot v = h_{K+L}(v)\}$ je potporna prava skupa $K + L$. Onda je $F = (K + L) \cap H_{K+L}(v)$ lice skupa $K + L$ u odnosu na potpornu pravu $H_{K+L}(v)$. Potpuno analogno, za kompaktne i konveksne skupove K i L i vektor v biramo njihove potporne prave $H_K(v) = \{x \in \mathbb{R}^2 : x \cdot v = h_K(v)\}$ i $H_L(v) = \{x \in \mathbb{R}^2 : x \cdot v = h_L(v)\}$. Neka su lica skupova K i L u odnosu na date potporne prave: $F_K = K \cap H_K(v)$ i $F_L = L \cap H_L(v)$. Očigledno je da su prave $H_{K+L}(v)$, $H_K(v)$ i $H_L(v)$ paralelne i važi: $H_{K+L}(v) = H_K(v) + H_L(v)$. Možemo pretpostaviti da važi $H_K(v) = H_L(v)$, do na translaciju skupa L . Dalje dobijamo:

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

Jedinstvenost F_K i F_L sledi iz (1).

(4) Za konveksne poligone K i L , na osnovu **Teoreme 3.12.**, (2), sledi da je $K + L$ kompaktnan i konveksan skup. Uočimo dva proizvoljna temena v_K i v_L poligona K i L . Odaberimo vektor v tako da lica poligona K i L u odnosu na potporne prave $H_K(v)$ i $H_L(v)$ budu v_K i v_L . Tada važi: $v_K + v_L \in H_K(v) + H_L(v)$. Na osnovu (2) sledi: $v_K + v_L \in H_{K+L}(v)$. Drugim rečima, suma Minkowskog dva temena je svakako tačka ruba skupa $K + L$. Pokazaćemo da je $K + L$ poligon koji nastaje kao konveksan omotač svih tačaka oblika $v_K + v_L$, gde su v_K i v_L temena poligona K i L . S obzirom na konveksnost skupa $K + L$ dovoljno je pokazati da, osim tačaka

oblika $v_K + v_L$, ne postoji nijedna tačka skupa $K + L$ čije je lice u odnosu na neku potpornu pravu samo ta tačka. Naime, ako bi postojala tačka F , onda bi prema (3) ove teoreme postojala jedinstvena lica poligona K i L , F_K i F_L takva da je: $F = F_K + F_L$. Kako je F tačka, očigledno je da i F_K i F_L moraju biti tačke, tj. temena poligona K i L , odnosno F je oblika $F = v_K + v_L$, što je kontradikcija. \square

Sledeća teorema je važna posledica **Teoreme 4.10.**

Teorema 4.11. Ako za konveksne poligone $A, B, C \subset \mathbb{R}^2$ važi: $A + C = B + C$, tada je: $A = B$.

Dokaz:

Neka je v nenula vektor sa ciljnom tačkom izvan skupa $A + C$. Dalje, za taj vektor v definišimo:

$$h_{A+C}(v) = \sup_{p \in A+C} (p \cdot v),$$

potpornu funkciju poligona $A + C$ u odnosu na dati vektor v . Tada je prava:

$$H_{A+C}(v) = \{x \in \mathbb{R}^2 : x \cdot v = h_{A+C}(v)\}$$

potporna prava skupa $A + C$. Neka je $F_{A+C} = (A + C) \cap H_{A+C}(v)$ lice poligona $A + C$ u odnosu na pravu $H_{A+C}(v)$. Bez umanjenja opštosti, pretpostavimo da je lice poligona $A + C$ u odnosu na pravu teme poligona $A + C$. Naime, ako je za izabrani vektor v lice poligona $A + C$ duž, odaberimo drugi vektor v' sa ciljnom tačkom izvan skupa $A + C$ tako da za taj vektor odgovarajuće lice poligona bude teme.

Na osnovu **Teoreme 4.10.**, (3) za teme F_{A+C} poligona $A + C$ postoje jedinstvena temena poligona A i C , F_A i F_C , čija je suma F_{A+C} :

$$F_{A+C} = F_A + F_C.$$

Potpuno analogno, za teme F_{A+C} poligona $B + C$ postoje jedinstvena temena poligona B i C , F_B i F'_C , čija je suma F_{A+C} :

$$F_{A+C} = F_B + F'_C.$$

Kako se svako teme poligona $A + C$ može predstaviti na jedinstven način kao

suma Minkowskog jednog temena poligona A i jednog temena poligona C , zaključujemo da važi:

$$F_A = F_B \text{ i } F_C = F_{C'}.$$

S obzirom da je izbor vektora v bio slučajan, pravac potporne prave smo slobodno birali, zaključujemo da poligoni A i B imaju ista temena. Kako je svaki poligon konveksan omotač svojih temena ([69]), sledi $A = B$. \square

Napomena 4.12. U daljem tekstu ćemo skup konveksnih poligona u \mathbb{R}^2 obeležavati sa $K(\mathbb{R}^2)$. Na osnovu **Teoreme 4.10.**, (4) i **Teoreme 4.11.** zaključujemo da je $(K(\mathbb{R}^2), +)$ komutativna polugrupa sa zakonom kancelacije.

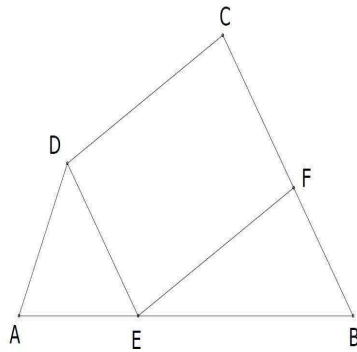
Napomena 4.13. Primitimo da obrat **Teoreme 4.10.**, (3) ne važi. Dakle, ako su F_Q i F_P lica konveksnih i kompaktnih skupova Q i P , tada $F_Q + F_P$ nije obavezno lice $Q + P$. Posmatrajmo četvorougao $\text{conv}(A, B, C, D)$ prikazan na Slici 6 koji se može predstaviti kao suma Minkowskog dva trougla, $\triangle AED$ i $\triangle EBF$. Dakle važi:

$$\text{conv}(A, B, C, D) = \text{conv}(A, E, D) + \text{conv}(E, B, F).$$

Međutim:

$$\text{conv}(E, D) + \text{conv}(E, F) = \text{conv}(E, F, C, D).$$

Dakle, duži $\text{conv}(E, D)$ i $\text{conv}(E, F)$ su lica $\triangle AED$ i $\triangle EBF$, ali njihova suma paralelogram $\text{conv}(E, F, C, D)$ nije lice $\text{conv}(A, B, C, D)$.



Slika 6

Napomena 4.14. Neka su U , V i W konveksni poligoni u \mathbb{R}^2 takvi da važi: $W = U + V$. Na osnovu **Teoreme 4.10.**, (3), svaka ivica poligona W može se predstaviti jedinstveno kao suma Minkovskog jedne ivice poligona U i jedne ivice poligona V , pri čemu jedna od njih može biti tačka. Obratno, svaka ivica poligona U i V je poligon sabirak tačno jedne ivice poligona W .

5 Veza polinoma i poligona - Newton-ov poligon polinoma

Ideja o ispitivanju nesvodljivosti polinoma jedne i dve promenljive preko njima pridruženih Newton-ovih poligona nastala je uopštavanjem nekih stavova o nesvodljivosti polinoma jedne promenljive. Gotthold Eisenstein 1850. godine u [9] formuliše jednostavan dovoljan uslov nesvodljivosti polinoma jedne promenljive sa celobrojnim koeficijentima. Ovaj stav prvi je formulisao Theodor Schönemann 1846. godine u [53], tako da se je u literaturi poznat kao Schönemann - Eisenstein-ova teorema.

Teorema 5.1. Polinom $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n$, pri čemu $a_i \in \mathbb{Z}$, za sve $i = 0, \dots, n$ i $a_n \neq 0$ je nesvodljiv nad \mathbb{Q} ako postoji prost broj p takav da deli sve koeficijente a_0, \dots, a_{n-1} , pri čemu vodeći koeficijent a_n nije deljiv sa p i slobodan član a_0 nije deljiv sa p^2 .

Napomena 5.2. Predhodnom teoremom je dat dovoljan, ali ne i potreban uslov nesvodljivosti polinoma jedne promenljive sa celobrojnim koeficijentima. Zaista, polinom $f(x) = x^2 + 1$ je nesvodljiv nad \mathbb{Q} , ali ne zadovoljava uslove **Teoreme 5.1.**

Eisenstein-ov stav je uopštio Dumas 1906. godine u [7].

Teorema 5.3. Neka je $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n$, pri čemu $a_i \in \mathbb{Z}$, za sve $i = 0, \dots, n$ i $a_n \neq 0$. Ako postoji prost broj p takav da p^{S_i} deli a_i ($S_i = \infty$ ako $a_i = 0$), $0 \leq i \leq n$, pri čemu $S_0 = 0$, $\frac{S_i}{i} > \frac{S_n}{n}$, za sve $0 \leq i \leq n-1$ i $NZD(S_n, n) = 1$, onda je polinom $f(x)$ nesvodljiv nad \mathbb{Q} .

Primedba 5.4. Primitimo da je **Teorema 5.1.** specijalan slučaj **Teoreme 5.3.** za $S_n = 1$.

Eisenstein-ov kriterijum su takođe generalizovali i J. Kurschak [32], O. Ore [41], [42],[43] i T. Rella [50]. Dumas je formulisao tvrđenje kojim se omogućava grafička analiza svodljivosti polinoma jedne promenljive, što predstavlja koren izučavanja veze između svodljivosti polinoma i osobina njima pridruženih poligona. Da bismo formulisali ovaj stav neophodno je, najpre, da uvedemo definicije nekih pojmova.

Neka je $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n$, pri čemu $a_i \in \mathbb{Z}$, za sve $i = 0, \dots, n$ i $a_0a_n \neq 0$ i neka je p prost broj. Neka je za $0 \leq i \leq n$, α_i najviši stepen kojim p deli a_i , tj. $a_i = p^{\alpha_i}a'_i$, pri čemu p ne deli a'_i .

Definicija 5.5. Polinomu $f(x)$ pridružujemo skup tačaka celobrojne rešetke:

$$T_i = (i, \alpha_i), \quad 0 \leq i \leq n.$$

Newton-ov poligon polinoma $f(x)$ u odnosu na p je konveksni omotač ovog skupa tačaka.

Definicija 5.6. Neka je $T_i = (i, \alpha_i)$, $0 \leq i \leq n$. Neka je $P_0 = T_0$ i neka je $P_1 = P_{i_1}$, pri čemu je $i_1 > 0$ maksimalni indeks takav da se sve preostale tačke T_k nalaze u istoj poluravni u odnosu na pravu određenu tačkama P_0 i P_1 , i to iznad ove prave. Neka je, zatim, $i_2 > i_1$ maksimalni indeks tako da isto to važi za pravu određenu tačkama P_1 i P_2 , gde je $P_2 = T_{i_2}$. Postupak se ponavlja sve dok ne dođemo do tačke $P_s = T_n$. Na ovaj način konstruisana poligonalna linija $P_0P_1 \dots P_s$ naziva se **donja grana Newton-ovog poligona polinoma** $f(x)$ u odnosu na prost broj p . Poligonalna linija $P_0P_1 \dots P_s$ se naziva još i **donji konveksni omotač** tačaka $T_i = (i, \alpha_i)$, $0 \leq i \leq n$, u odnosu na prost broj p .

Primedba 5.7. Potpuno istim postupkom kao u **Definiciji 5.6.**, sa razlikom što se pri konstrukciji pravih traži maksimalni indeks takav da se sve preostale tačke nalaze u poluravni ispod posmatranih pravih dobija se **gornja grana Newton-ovog poligona polinoma** $f(x)$ u odnosu na prost broj p . Na taj način dobijena poligonalna linija $P_0P_1 \dots P_s$ se naziva još i **gornji konveksni omotač** tačaka $T_i = (i, \alpha_i)$, $0 \leq i \leq n$, u odnosu na prost broj p .

Primedba 5.8. Posmatrajmo duži P_iP_{i+1} , $0 \leq i \leq s-1$, stranice donje grane Newton-ovog poligona polinoma $f(x)$. Koefficienti pravaca pravih koje redom sadrže ove duži formiraju strogo rastući niz.

Definicija 5.9. Neka je $P_0P_1 \dots P_s$ donja grana Newton-ovog poligona polinoma $f(x)$ u odnosu na prost broj p . Ako neke od duži P_iP_{i+1} , $0 \leq i \leq s-1$, u svojoj unutrašnjosti sadrže celobrojne tačke različite od T_0, \dots, T_n , te tačke ćemo takođe smatrati temenima poligonalne linije. Na taj način dobijena poligonalna linija $Q_0Q_1 \dots Q_{s+t}$ naziva se **Newton-ov dijagram polinoma** $f(x)$ u odnosu na prost broj p . Vektori $\overrightarrow{Q_iQ_{i+1}}$, $0 \leq i \leq s+t-1$ nazivaju se **p -komadi** polinoma $f(x)$. **Sistem p -komada** polinoma $f(x)$ je multiskup nje-

govih p -komada, pri čemu se svaki vektor uzima sa višestrukošću s kojom se pojavljuje u Newton-ovom dijagramu.

Primedba 5.10. Posmatrajmo vektore $\overrightarrow{Q_i Q_{i+1}}$, $0 \leq i \leq s + t - 1$, sistema p -komada polinoma $f(x)$. Koeficijenti pravaca pravih koje sadrže ove vektore redom formiraju neopadajući niz.

Sada ćemo formulisati Dumas-ovu lemu [7].

Teorema 5.11. Neka je p prost broj i $f(x), g(x), h(x) \in \mathbb{Z}[x]$. Ako je $f(x) = g(x)h(x)$, tada je sistem p -komada polinoma $f(x)$ jednak uniji sistema p -komada za $g(x)$ i $h(x)$.

Dokaz:

Neka su:

$$f(x) = \sum_{i=0}^n p^{\alpha_i} a'_i x^i, \quad g(x) = \sum_{i=0}^m p^{\beta_i} b'_i x^i \quad \text{i} \quad h(x) = \sum_{i=0}^{n-m} p^{\gamma_i} c'_i x^i,$$

pri čemu brojevi a'_i, b'_i i c'_i nisu deljivi sa p . Posmatrajmo jednu stranicu $P_t P_{t+1}$ Newton-ovog dijagrama u odnosu na p (ovo ćemo podrazumevati i izostavljati u daljem), koja može da se sastoji iz više p -komada.

Neka je:

$$P_t = (i_-, \alpha_-) \quad \text{i} \quad P_{t+1} = (i_+, \alpha_+).$$

Tada je nagib posmatrane stranice:

$$k = \frac{\alpha_+ - \alpha_-}{i_+ - i_-}.$$

Jednačina prave određena tačkama P_t i P_{t+1} je:

$$y - \alpha_- = \frac{\alpha_+ - \alpha_-}{i_+ - i_-} (x - i_-) \tag{1}$$

ili:

$$y - \alpha_+ = \frac{\alpha_+ - \alpha_-}{i_+ - i_-} (x - i_+). \tag{2}$$

Množenjem (1) sa $(i_+ - i_-)$ dobijamo:

$$(i_+ - i_-)(y - \alpha_-) = (\alpha_+ - \alpha_-)(x - i_-).$$

Dalje sledi:

$$(i_+ - i_-)y - (i_+ - i_-)\alpha_- = (\alpha_+ - \alpha_-)x - (\alpha_+ - \alpha_-)i_-,$$

odnosno:

$$(i_+ - i_-)y - (\alpha_+ - \alpha_-)x = (i_+ - i_-)\alpha_- - (\alpha_+ - \alpha_-)i_-,$$

Potpuno analogno, iz (2) dobijamo:

$$(i_+ - i_-)y - (\alpha_+ - \alpha_-)x = (i_+ - i_-)\alpha_+ - (\alpha_+ - \alpha_-)i_+.$$

Kombinacijom dve poslednje jednakosti dobijamo:

$$(i_+ - i_-)y - (\alpha_+ - \alpha_-)x = (i_+ - i_-)\alpha_- - (\alpha_+ - \alpha_-)i_- = (i_+ - i_-)\alpha_+ - (\alpha_+ - \alpha_-)i_+.$$

Na osnovu konstrukcije Newton-ovog dijagrama, nijedna od tačaka $T_i = (i, \alpha_i)$, $0 \leq i \leq n$ ne leži ispod ove prave, tj. za sve i , $0 \leq i \leq n$ važi nejednakost:

$$(i_+ - i_-)\alpha_i - (\alpha_+ - \alpha_-)i \geq (i_+ - i_-)\alpha_- - (\alpha_+ - \alpha_-)i_- = (i_+ - i_-)\alpha_+ - (\alpha_+ - \alpha_-)i_+,$$

pri čemu je nejednakost stroga kad je $i < i_-$ ili $i > i_+$.

Broj $(i_+ - i_-)\alpha_i - (\alpha_+ - \alpha_-)i$ nazivamo težina monoma $p^{\alpha_i} a'_i x^i$.

Brojevi i_- i i_+ su jednoznačno određeni kao najmanji i najveći stepeni monoma polinoma $f(x)$ sa minimalnom težinom.

Za polinom $g(x)$ posmatrajmo broj:

$$G = \min\{(i_+ - i_-)\beta_j - (\alpha_+ - \alpha_-)j \mid 0 \leq j \leq m\}$$

i definišemo j_- i j_+ redom kao najmanji i najveći indeks za koji je:

$$G = (i_+ - i_-)\beta_{j_-} - (\alpha_+ - \alpha_-)j_- = (i_+ - i_-)\beta_{j_+} - (\alpha_+ - \alpha_-)j_+.$$

Na potpuno analogan način se za polinom $h(x)$ uočava veličina:

$$H = \min\{(i_+ - i_-)\gamma_k - (\alpha_+ - \alpha_-)k \mid 0 \leq k \leq n - m\}$$

i definišemo k_- i k_+ redom kao najmanji i najveći indeks za koji je:

$$H = (i_+ - i_-)\gamma_{k_-} - (\alpha_+ - \alpha_-)k_- = (i_+ - i_-)\gamma_{k_+} - (\alpha_+ - \alpha_-)k_+.$$

Kako je $f(x) = g(x) \cdot h(x)$ dobijamo:

$$p^{\alpha_{j_-+k_-}} a'_{j_-+k_-} x^{j_-+k_-} = \sum_{j+k=j_-+k_-} (p^{\beta_j} b'_j x^j) (p^{\gamma_k} c'_k x^k).$$

Takođe, očigledno je da je težina proizvoda dva monoma jednaka zbiru njihovih težina. Zbog toga je težina sabirka u gornjoj sumi koji se dobija za $j = j_-$ i $k = k_-$ jednaka $G + H$. Težina ostalih sabiraka je strogo veća od $G + H$, pošto je za njih $j < j_-$ ili $k < k_-$.

S obzirom na to da je $(i_+ - i_-) > 0$, težina monoma za $j + k = \text{const}$ monotono raste sa rastom zbira $\beta_j + \gamma_k$. Prema tome, u slučaju $j + k = j_- + k_-$ ova suma je strogo minimalna za $j = j_-$ i $k = k_-$, pa sledi da je najveći stepen kojim p deli koeficijent u $f(x)$ uz $x^{j_-+k_-}$ jednak $\beta_{j_-} + \gamma_{k_-}$. Drugim rečima, $\alpha_{j_-+k_-} = \beta_{j_-} + \gamma_{k_-}$.

Dalje, po izboru G i H , težina monoma $p^{\alpha_i} a'_i x^i$ je strogo veća od $G + H$ za $i < j_- + k_-$, a ne manja od $G + H$ za $i \geq j_- + k_-$. Sledi da je $i_- = j_- + k_-$. Analogno se dokazuje da je $i_+ = j_+ + k_+$, pa dobijamo:

$$i_+ - i_- = (j_+ - j_-) + (k_+ - k_-).$$

Očigledno, bar jedna od razlika u zagradi je različita od nule.

Ako su obe gornje razlike $(j_+ - j_-)$ i $(k_+ - k_-)$ različite od nule, tada je duž određena tačkama (j_-, β_{j_-}) i (j_+, β_{j_+}) stranica u Newton-ovom dijagramu polinoma $g(x)$ koja pripada pravoj $(i_+ - i_-)y - (\alpha_+ - \alpha_-)x = G$.

Potpuno analogno, duž određena tačkama (k_-, γ_{k_-}) i (k_+, γ_{k_+}) je stranica u Newton-ovom dijagramu $h(x)$ koja pripada pravoj $(i_+ - i_-)y - (\alpha_+ - \alpha_-)x = H$.

Koeficijenti nagiba ovih stranica su u oba slučaja jednaki:

$$k = \frac{\alpha_+ - \alpha_-}{i_+ - i_-}.$$

Odavde je jasno da je zbir dužina stranica Newton-ovog dijagrama za $g(x)$ i $h(x)$ sa nagibom k jednak dužini stranice Newton-ovog dijagrama za $f(x)$ sa odgovarajućim nagibom.

Ako je jedan od brojeva $(j_+ - j_-)$ i $(k_+ - k_-)$ jednak nuli, to znači da jedan od polinoma $g(x)$, $h(x)$ ima u svom Newton-ovom dijagramu stranicu nagiba k podudarnu stranici istog nagiba za $f(x)$, dok drugi polinom nema takvu stranicu.

Kako je izbor stranice $P_t P_{t+1}$ Newton-ovog dijagrama (tj. koeficijenta pravca k) bio proizvoljan, sledi da za proizvoljan pravac zbir dužina p -komada za $g(x)$

i $h(x)$ jednak zbiru dužina p -komada za $f(x)$, čime je teorema pokazana. \square

Na sledećem primeru ćemo dati grafički prikaz sistema p -komada, gde ćemo istaći bitne elemente koji se javljaju u dokazu Dumas-ove leme.

Primer 5.12. Posmatrajmo polinome $g(x)$, $h(x)$ i $f(x)$:

$$g(x) = 2 - 12x + 4x^2 - 8x^3 + x^4,$$

$$h(x) = 2 - 2x - 11x^2 + 2x^3 = (1 + 2x)(2 - 6x + x^2)$$

i

$$f(x) = g(x) \cdot h(x) \text{ u odnosu na } p = 2.$$

Formirajmo sistem 2-komada polinoma $g(x)$ i $h(x)$:

$$g(x) = 2 - 12x + 4x^2 - 8x^3 + x^4$$

$$A_0 = 2 \quad \Rightarrow \quad T_0 = (0, 1)$$

$$A_1 = -12 = 2^2 \cdot (-3) \quad \Rightarrow \quad T_1 = (1, 2)$$

$$A_2 = 4 = 2^2 \quad \Rightarrow \quad T_2 = (2, 2)$$

$$A_3 = -8 = 2^3 \cdot (-1) \quad \Rightarrow \quad T_3 = (3, 3)$$

$$A_4 = 1 \quad \Rightarrow \quad T_4 = (4, 0).$$

$$h(x) = 2 - 2x - 11x^2 + 2x^3$$

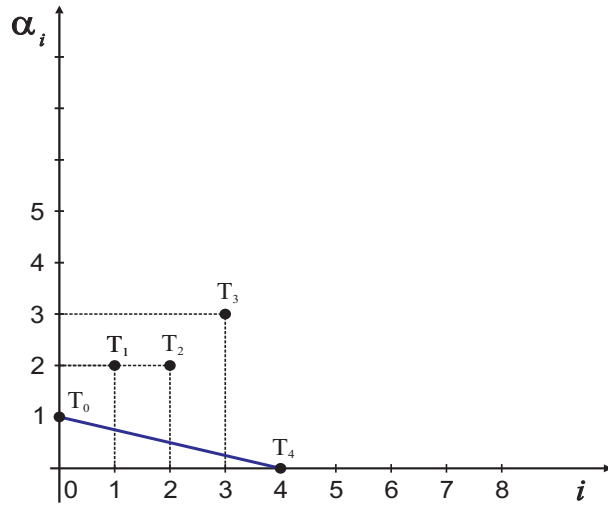
$$A_0 = 2 \quad \Rightarrow \quad T_0 = (0, 1)$$

$$A_1 = -2 = 2 \cdot (-1) \quad \Rightarrow \quad T_1 = (1, 1)$$

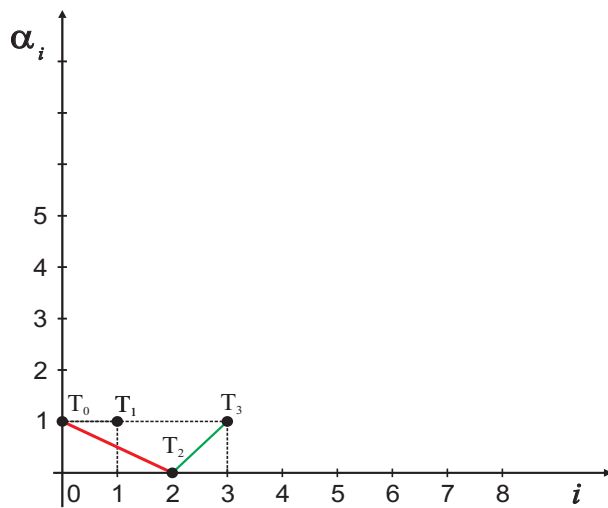
$$A_2 = -11 \quad \Rightarrow \quad T_2 = (2, 0)$$

$$A_3 = 2 \quad \Rightarrow \quad T_3 = (3, 1)$$

Sistemi 2-komada polinoma $g(x)$ i $h(x)$ prikazani su na Slici 7 i Slici 8.



Slika 7



Slika 8

Formirajmo sada sistem 2-komada polinoma $f(x)$:

$$f(x) = g(x) \cdot h(x) = (2 - 12x + 4x^2 - 8x^3 + x^4)(2 - 2x - 11x^2 + 2x^3)$$

$$f(x) = 4 - 28x + 10x^2 + 112x^3 - 50x^4 + 94x^5 - 27x^6 + 2x^7$$

$$A_0 = 4 = 2^2 \quad \Rightarrow \quad T_0 = (0, 2)$$

$$A_1 = -28 = 2^2 \cdot (-7) \quad \Rightarrow \quad T_1 = (1, 2)$$

$$A_2 = 10 = 2 \cdot 5 \quad \Rightarrow \quad T_2 = (2, 1)$$

$$A_3 = 112 = 2^4 \cdot 7 \quad \Rightarrow \quad T_3 = (3, 4)$$

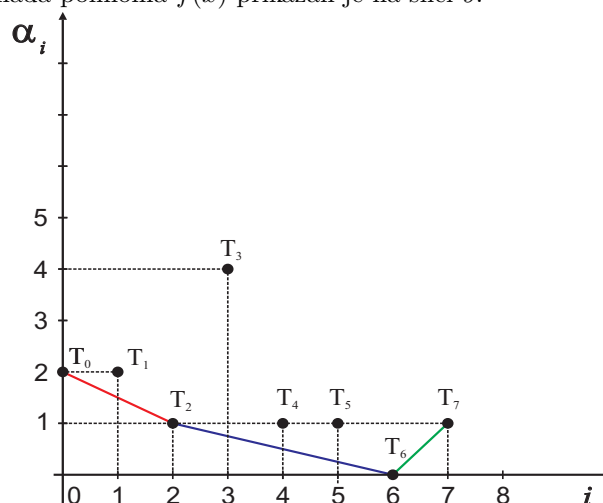
$$A_4 = -50 = 2 \cdot (-25) \quad \Rightarrow \quad T_4 = (4, 1)$$

$$A_5 = 94 = 2 \cdot 47 \quad \Rightarrow \quad T_5 = (5, 1)$$

$$A_6 = -27 \quad \Rightarrow \quad T_6 = (6, 0)$$

$$A_7 = 2 \quad \Rightarrow \quad T_7 = (7, 1).$$

Sistem 2-komada polinoma $f(x)$ prikazan je na slici 9.



Slika 9

Kao što se može uočiti sa Slika 7, 8 i 9, sistem 2-komada polinoma $f(x)$ jednak je uniji sistema 2-komada za $g(x)$ i $h(x)$, što i tvrdi Dumas-ova lema. Redosled 2-komada je takav da su prvo, polazeći od $i = 0$, raspoređeni oni sa "većim padom"ka onima sa "manjim padom". U suprotnom bi uslov konveksnosti omotača bio narušen.

Teorema 5.13. Neka je p prost broj. Ako Newton-ov dijagram polinoma $f(x) \in \mathbb{Z}[x]$ u odnosu na p ima stranicu sa sledeće dve osobine:

- (1) dužina njene projekcije na x -osu je k ,
 (2) ne sadrži celobrojne tačke u svojoj unutrašnjosti, tj. sastoji se iz samo jednog p -komada,
 tada $f(x)$ sadrži nesvodljiv faktor (nad \mathbb{Z}) stepena bar k .

Specijalno, ako se Newton-ov dijagram sastoji iz jedne duži koja ne sadrži unutrašnje celobrojne tačke, tada je $f(x)$ nesvodljiv nad \mathbb{Z} .

Dokaz:

S obzirom da stranica Newton-ovog dijagrama polinoma $f(x)$ u odnosu na p iz uslova teoreme ne sadrži celobrojne tačke u svojoj unutrašnjosti, pri konstrukciji sistema p -komada ta stranica će činiti jedan p -komad čija je dužina projekcije na x -osu k .

Pretpostavimo suprotno, da su nesvodljivi faktori polinoma $f(x)$ stepena manjeg ili jednakog $k - 1$. Odavde sledi da se sistem p -komada polinoma $f(x)$ sastoji iz vektora čija je projekcija na x -osu manja ili jednaka $k - 1$, što je očigledna kontradikcija. \square

Primer 5.14. Uočimo 2-komad na Slici 9 obojen plavom bojom, čija je dužina projekcije na x -osu je 4. Na osnovu **Teoreme 5.13.**, 2-komad plave boje garantuje postojanje nesvodljivog faktora (nad \mathbb{Z}) polinoma $f(x)$ stepena bar 4. S obzirom da se sistem 2-komada polinoma $g(x)$, prikazan na Slici 7, sastoji samo iz ovog 2-komada, polinom $g(x)$ je nesvodljiv nad \mathbb{Z} .

Primer 5.15. Dat je polinom

$$f(x) = -5 + 25x - 35x^2 + 15x^3 - 10x^4 + 2x^5.$$

Formirajmo donju granu Newton-ovog poligona za $f(x)$ u odnosu na $p = 5$.

$$A_0 = -5 = 5 \cdot (-1) \quad \Rightarrow \quad T_0 = (0, 1)$$

$$A_1 = 25 = 5^2 \quad \Rightarrow \quad T_1 = (1, 2)$$

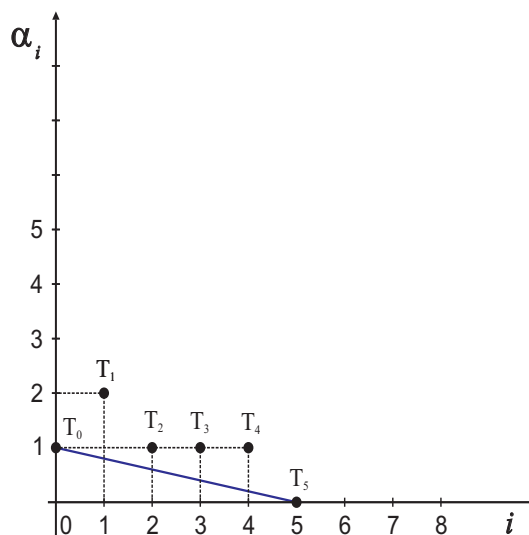
$$A_2 = -35 = 5 \cdot (-7) \quad \Rightarrow \quad T_2 = (2, 1)$$

$$A_3 = 15 = 5 \cdot 3 \quad \Rightarrow \quad T_3 = (3, 1)$$

$$A_4 = -10 = 5 \cdot (-2) \quad \Rightarrow \quad T_4 = (4, 1)$$

$$A_5 = 2 \quad \Rightarrow \quad T_5 = (5, 0)$$

Na Slici 10 je prikazana donja grana Newton-ovog poligona za $f(x)$ u odnosu na $p = 5$.



Slika 10

S obzirom na to da se donja grana Newton-ovog poligona za $f(x)$ u odnosu na $p = 5$ sastoji od samo jedne duži koja u svojoj unutrašnjosti ne sadrži celobrojne tačke, sistem 5-komada polinoma $f(x)$ se sastoji samo od jednog vektora, pa na osnovu **Teoreme 5.13.** sledi da je polinom $f(x)$ nesvodljiv nad \mathbb{Z} .

Nesvodljivost polinoma $f(x)$ se dobija i na osnovu **Teoreme 5.1.** za $p = 5$. Zaista, 5 deli $-5, 25, -35, 15, -10$, pri čemu 5 ne deli 2 i 5^2 ne deli -5 , pa su ispunjeni uslovi **Teoreme 5.1.** odakle sledi da je $f(x)$ nesvodljiv \mathbb{Q} .

Sledeći jednostavan stav o nesvodljivosti poznat je u literaturi kao Eisenstein-Dumas kriterijum, videti [14].

Teorema 5.16. Neka je R domen jedinstvene faktorizacije i neka je $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n \in R[x]$, pri čemu je $a_0a_n \neq 0$. Pretpostavimo da a_0, \dots, a_n nemaju netrivialni zajednički faktor u R . Ako se Newton-ov dijagram polinoma $f(x)$ u odnosu na neki prost broj $p \in R$ sastoji iz samo jedne duži čija su temena $(0, m)$ i $(n, 0)$, pri čemu je $NZD(m, n) = 1$, tada je $f(x)$ nesvodljiv u $R[x]$.

Dokaz:

Kako je $NZD(m, n) = 1$, duž čija su temena $(0, m)$ i $(n, 0)$ ne sadrži celobrojne tačke u svojoj unutrašnjosti. Dakle, Newton-ov dijagram polinoma $f(x)$ se sastoji iz jedne duži koja ne sadrži unutrašnje celobrojne tačke, pa je na osnovu **Teoreme 5.13.** polinom $f(x)$ nesvodljiv. \square

Definicija 5.17. Neka $f(x, y) = f_0(y) + f_1(y)x + \dots + f_{n-1}(y)x^{n-1} + f_n(y)x^n \in F[x, y]$, gde je F polje. **Donja grana Newton-ovog poligona** polinoma $f(x, y)$ u odnosu na y je donji konveksni omotač tačaka $(0, a_0), \dots, (n, a_n)$, gde je a_i stepen $f_i(y)$ po y za $i = 1, \dots, n$.

Primedba 5.18. U slučaju kada je $f_i(y) = 0$ tada a_i nije definisano.

Posmatrajmo slučaj kad je R prsten polinoma nad nekim poljem. Neka je F polje i neka je $R = F[y]$, gde je y nova promenljiva. Tada je y prost u R i Eisenstein-Dumas kriterijum se može primeniti u $R[x] \simeq F[x, y]$. Dakle, sledeća teorema je specijalan slučaj Eisenstein-Dumas kriterijuma, videti [14].

Teorema 5.19. Neka je F polje i neka je:

$$f(x, y) = f_0(y) + f_1(y)x + \dots + f_{n-1}(y)x^{n-1} + f_n(y)x^n \in F[x, y],$$

pri čemu $f_0(y), f_1(y), \dots, f_{n-1}(y), f_n(y) \in F[y]$. Pretpostavimo da je $f_0(y) \neq 0$ i $f_n(y)$ je nenula konstanta u F . Ako se donja grana Newton-ovog poligona polinoma $f(x, y)$ u odnosu na y sastoji iz samo jedne duži čija su temena $(0, m)$ i $(n, 0)$, pri čemu je $NZD(m, n) = 1$, tada je $f(x, y)$ apsolutno nesvodljiv nad poljem F .

Definicija 5.20. Neka $f(x, y) = f_0(y) + f_1(y)x + \dots + f_{n-1}(y)x^{n-1} + f_n(y)x^n \in F[x, y]$, gde je F polje. **Gornja grana Newton-ovog poligona** polinoma $f(x, y)$ u odnosu na y je gornji konveksni omotač tačaka $(0, a_0), \dots, (n, a_n)$, gde je a_i stepen $f_i(y)$ po y za $i = 1, \dots, n$.

Schmidt [51], oslanjajući se na rad Stepanova [59], [60], formuliše geometrijski metod za proveru apsolutne nesvodljivosti jedne klase polinoma sa dve promenljive. Teorema je poznata u literaturi kao teorema Stepanov-Schmidt-a.

Teorema 5.21. Neka je F polje i neka je:

$$f(x, y) = f_0(y) + f_1(y)x + \dots + f_{n-1}(y)x^{n-1} + f_n(y)x^n \in F[x, y].$$

Ako se gornja grana Newton-ovog poligona polinoma $f(x, y)$ u odnosu na y sastoji iz jedne duži čija su temena $(0, m)$ i $(n, 0)$, pri čemu je $NZD(m, n) = 1$, tada je $f(x, y)$ apsolutno nesvodljiv nad poljem F .

Primedba 5.22. U [14] Shuhong Gao konstatuje da teoreme Eisenstein-Dumas i Stepanov-Schmidt donose, zapravo, isti kriterijum nesvodljivosti polinoma sa dve promenljive, s tim što prva uzima u obzir donju, a druga gornju granu Newton-ovog poligona pridruženog polinomu $f(x, y)$ u odnosu na y . Odavde je intuitivno jasno da, pri analizi nesvodljivosti polinoma sa dve promenljive, treba uzeti u obzir ceo Newton-ov poligon, tj. i donju i gornju granu Newton-ovog poligona. Ovaj pristup rezultiraće formulacijom opštijih stavova o nesvodljivosti polinoma sa dve promenljive, tako da će Eisenstein-Dumas i Stepanov-Schmidt kriterijum biti specijalni slučajevi tih rezultata. Ova geometrijska uopštenja Eisenstein-ovog stava omogućila su ispitivanje nesvodljivosti polinoma dve promenljive pomoću Newton-ovih poligona. Međutim, geometrijsku analizu nesvodljivosti polinoma tri i više promenljivih omogućio je rad Ostrowskog [44], [45].

Formalno, Newton-ov politop polinoma sa više promenljivih se uvodi u [14]. S obzirom na to da je predmet istraživanja ove disertacije faktorizacija polinoma dve promenljive, a da je politop u dvodimenzionalnom Euklidovom prostoru koji odgovara polinomu sa dve promenljive ustvari poligon, navedimo definiciju Newton-ovog politopa iz [14] za polinom dve promenljive.

Definicija 5.23. Neka je F polje. Posmatrajmo proizvoljan polinom iz $F[x, y]$ -prstena polinoma sa dve promenljive nad tim poljem:

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

Posmatrajmo vektore eksponenata (e_1, e_2) onih monoma gornjeg polinoma sa nenula koeficijentima ($C_{e_1 e_2} \neq 0$) kao tačke u \mathbb{R}^2 . Svakom vektoru (e_1, e_2) pridružimo tačku Dekartove koordinatne ravni sa koordinatama (e_1, e_2) . Konveksni omotač ovog skupa tačaka naziva se **Newton-ov poligon polinoma** f , u oznaci P_f .

Algoritam za konstrukciju konveksnog omotača konačnog skupa tačaka u \mathbb{R}^n

je dat u [16], dok je algoritam za konstrukciju konveksnog omotača konačnog skupa tačaka u ravni dat u [17].

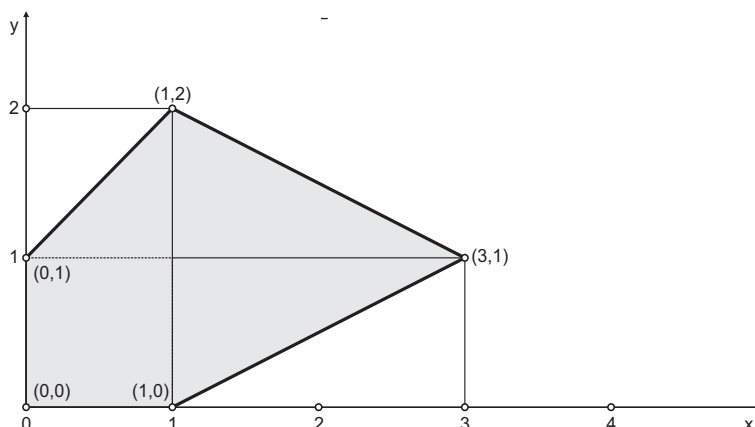
Napomena 5.24. Newton-ov poligon polinoma $f(x, y)$ efektivno konstruišemo na sledeći način: najpre u Dekartovoj koordinatnoj ravni ucrtamo sve tačke $(e_1, e_2)_i$, koje odgovaraju monomima polinoma sa nenula koeficijentima, $i = 1, \dots, k$ (pod pretpostavkom da polinom f ima k monoma sa nenula koeficijentima). Jasno je da sve tačke $(e_1, e_2)_i$, imaju obe celobrojne, nenegativne koordinate, pa se nalaze u prvom kvadrantu Dekartove koordinatne ravni zajedno sa nenegativnim delovima x i y ose. Za prvo teme poligona odaberimo onu tačku $(e_1, e_2)_i$, $i = 1, \dots, k$ sa najmanjom x koordinatom. Ako postoji više od jedne takve tačke, za polaznu tačku biramo tačku sa najmanjom x koordinatom koja pritom ima i najmanju y koordinatu, odnosno koja je bliža koordinatnom početku. Neka je za polaznu tačku odabrana tačka $(e_1, e_2)_p$, $1 \leq p \leq k$. Za drugo teme prve duži biramo jednu od preostalih tačaka $(e_1, e_2)_i$, $i = 1, \dots, k$, $i \neq p$, obeležimo je sa $(e_1, e_2)_c$ takvu da se sve ostale tačke $(e_1, e_2)_i$, $i = 1, \dots, k$, $i \neq p$, $i \neq c$ nalaze u istoj zatvorenoj poluravni u odnosu na pravu određenu tačkama $(e_1, e_2)_p$ i $(e_1, e_2)_c$. Pretpostavimo da postoji više od jedne takve tačke. Neka su to recimo tačke $(e_1, e_2)_{c'}$ i $(e_1, e_2)_{c''}$. Jasno je da su tada tačke $(e_1, e_2)_p$, $(e_1, e_2)_{c'}$ i $(e_1, e_2)_{c''}$ kolinearne, pa važi jedan od rasporeda: $(e_1, e_2)_p - (e_1, e_2)_{c'} - (e_1, e_2)_{c''}$ ili $(e_1, e_2)_p - (e_1, e_2)_{c''} - (e_1, e_2)_{c'}$. Bez umanjenja opštosti, pretpostavimo da važi raspored: $(e_1, e_2)_p - (e_1, e_2)_{c'} - (e_1, e_2)_{c''}$. Tada za sledeće teme Newton-ovog poligona polinoma f biramo tačku $(e_1, e_2)_{c'}$. Za sledeće teme poligona biramo jednu od tačaka različitu od $(e_1, e_2)_p$, $(e_1, e_2)_{c'}$ i $(e_1, e_2)_{c''}$, takvu da su sve tačke u istoj zatvorenoj poluravni u odnosu na pravu određenu izabranom tačkom i tačkom $(e_1, e_2)_{c''}$. Potpuno analogno, postupak nastavljamo izborom za sledeće teme poligona tačke koja do tada nije izabrana za teme, niti je odbačena zbog kolinearnosti sa dva uzastopno izabrana temena. Postupak se prekida kada se više nijedna tačka ne može izabrati za teme. Newton-ov poligon polinoma f je poligon čija su temena redom tačke izabrane opisanim algoritmom.

Primer 5.25. Posmatrajmo polinom:

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

Monomima polinoma $f(x, y)$ sa nenula koeficijentima odgovaraju redom sledeći

vektori eksponenata: $(3,1)$, $(1,2)$, $(1,0)$, $(0,1)$ i $(0,0)$. Newton-ov poligon polinoma $f(x, y)$ je konveksni omotač ovog skupa tačaka prikazan na Slici 11.



Slika 11

Za dalji rad neophodno je da uvedemo neke pojmove.

Definicija 5.26. Za tačku iz \mathbb{R}^2 kažemo da je **celobrojna** ako su obe njene koordinate celi brojevi. Za poligon kažemo da je **celobrojni poligon** ako su sva njegova temena celobrojne tačke.

Definicija 5.27. Za celobrojni poligon C kažemo da **ima netrivialnu dekompoziciju u smislu sume Minkowskog**, odnosno da je **integralno rastavljiv** ako postoje celobrojni poligoni A i B takvi da važi $C = A + B$, pri čemu i A i B sadrže bar dve tačke. Poligoni A i B se nazivaju **poligoni sabirci** od C . U suprotnom, kažemo da celobrojni poligon C **nema netrivialnu dekompoziciju** odnosno da je **integralno nerastavljiv**.

Pored integralne nerastavljivosti, postoji i koncept homotetične nerastavljivosti [19]. Homotetična nerastavljivost je detaljnije izložena u [25], [38], [39], [56], [57] i [58]. Ne postoji direktna veza između integralne i homotetične nerastavljivosti. Poligon može zadovoljavati i integralnu i homotetičnu nerastavljivost, samo jednu ili nijednu od njih.

Sledeća teorema, koju je dokazao Ostrowski 1921. godine u [44], uspostavlja vezu između faktorizacije polinoma i rastavljivosti u smislu sume Minkowskog njemu pridruženog poligona.

Teorema 5.28. Neka su $f, g, h \in F[x, y]$ i neka je $f = gh$. Tada važi $P_f = P_g + P_h$.

Dokaz:

Neka je $(\alpha, \beta) \in P_f$ proizvoljno teme Newton-ovog poligona polinoma f . Po definiciji Newton-ovog poligona, to znači da polinom f sadrži monom $x^\alpha y^\beta$ sa nenula koeficijentom. Kako je $f = gh$, zaključujemo da polinomi g i h sadrže redom monome $x^\gamma y^\delta$ i $x^{\alpha-\gamma} y^{\beta-\delta}$ sa nenula koeficijentima. Ovim monomima odgovaraju tačke $(\gamma, \delta) \in P_g$ i $(\alpha - \gamma, \beta - \delta) \in P_h$. Jasno je da važi: $(\gamma, \delta) + (\alpha - \gamma, \beta - \delta) \in P_g + P_h$, odakle dobijamo $(\gamma + \alpha - \gamma, \delta + \beta - \delta) \in P_g + P_h$, tj. $(\alpha, \beta) \in P_g + P_h$. Kako za proizvoljno $(\alpha, \beta) \in P_f$, važi $(\alpha, \beta) \in P_g + P_h$, pa je $P_f \subseteq P_g + P_h$.

Pokazaćemo da važi i obratna inkluzija: $P_g + P_h \subseteq P_f$. Na osnovu **Teoreme 4.10.**, (4), sledi da je $P_g + P_h$ poligon. Kako je poligon konveksni omotač svojih temena ([69]), dovoljno je pokazati da se svako teme poligona $P_g + P_h$ nalazi u poligonu P_f . Neka je v teme Newton-ovog poligona $P_g + P_h$. Kako $v \in P_g + P_h$, zaključujemo da postoje tačke $v_g \in P_g$ i $v_h \in P_h$ takve da je $v = v_g + v_h$.

Jedinstvenost ćemo dokazati direktno, bez korišćenja **Teoreme 4.10.**, (3). Iz pretpostavke da je v teme Newton-ovog poligona $P_g + P_h$ sledi jedinstvenost vektora v_g i v_h . Pretpostavimo suprotno, $v = v_g + v_h = v'_g + v'_h$, gde $v_g, v'_g \in P_g, v_h, v'_h \in P_h$, pri čemu važi $v_g \neq v'_g$ i $v_h \neq v'_h$. Neka je $v = (x, y)$ i $v_g = (a, b)$. Kako je $v = v_g + v_h$, očigledno je $v_h = (x - a, y - b)$. Ako je $v'_g = (c, d)$, potpuno analogno zaključujemo da je $v'_h = (x - c, y - d)$.

Posmatrajmo, sada, tačku $v_g + v'_h$. Jasno je da $v_g + v'_h \in P_g + P_h$ i važi:

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

Posmatrajmo, zatim, tačku $v'_g + v_h$. Jasno je da $v'_g + v_h \in P_g + P_h$ i važi:

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

Potražimo sredinu duži čije su krajnje tačke $v_g + v'_h$ i $v'_g + v_h$ Newton-ovog poligona $P_g + P_h$:

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

Dakle, sredina duži čije su krajnje tačke $v_g + v'_h$ i $v'_g + v_h$ Newton-ovog poligona $P_g + P_h$ je tačka (x, y) . Kako je teme poligona tačka koja se ne nalazi ni na jednoj duži koja spaja bilo koje druge dve tačke poligona, sledi da tačka (x, y) nije teme poligona $P_g + P_h$, što je očigledna kontradikcija. Dakle, za teme v Newton-ovog poligona $P_g + P_h$ postoje jedinstveni vektori $v_g \in P_g$ i $v_h \in P_h$ takvi da je $v = v_g + v_h$.

S obzirom na to da su v_g i v_h jedinstveni, jasno je da postoji jedinstven monom u izrazu $g \cdot h$ koji ima v za svoj vektor eksponenta. Odavde sledi $v \in P_f$. Na ovaj način smo pokazali da su sva temena poligona $P_g + P_h$ u poligonu P_f , a kako je Newton-ov poligon konveksni omotač svojih temena ([69]), važi: $P_g + P_h \subseteq P_f$. \square

Napomena 5.29. Dokaz **Teoreme 5.28.** koji je prezentovan u [46], imajući u vidu osobine celobrojne rešetke u prvom kvadrantu, omogućio je karakterizaciju nekih unutrašnjih tačaka Newton-ovog poligona i predstavlja polaznu osnovu u smislu analize Newton-ovih poligona sa ciljem pronalazjenja faktorizacija polinoma dve promenljive. Naime, možemo primetiti da monomima polinoma f koji se nastaju na bar dva različita načina množenjem monoma faktor-polinoma g i h sigurno ne odgovaraju temena Newton-ovog poligona P_f . Posmatrajmo, recimo, polinom:

$$f(x, y) = 2x^2y^2 + xy^3 + x^3y \in F[x, y].$$

Polinom $f(x, y)$ se može faktorisati na sledeći način:

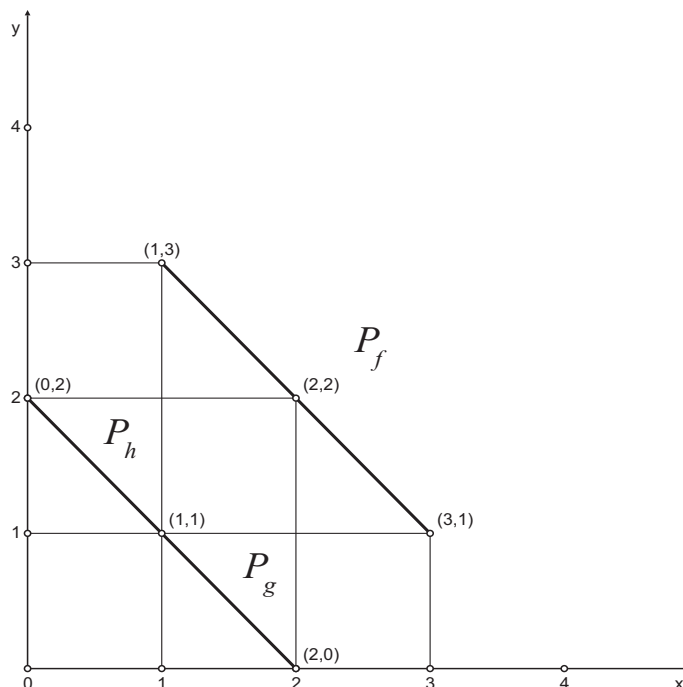
$$f(x, y) = 2x^2y^2 + xy^3 + x^3y = (x^2 + xy)(y^2 + xy) = gh.$$

Monom x^2y^2 polinoma f sa koeficijentom 2 se dobija iz faktor-polinoma na dva različita načina:

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

Posmatrajmo, sada, Newton-ove poligone polinoma f i njegovih faktor-polinoma g i h .

Jasno, $P_f = \text{conv}((2, 2), (1, 3), (3, 1))$ je duž sa krajnjim tačkama u $(1, 3)$ i $(3, 1)$, $P_g = \text{conv}((2, 0), (1, 1))$ je duž sa krajnjim tačkama u $(2, 0)$ i $(1, 1)$ i $P_h = \text{conv}((0, 2), (1, 1))$ je duž sa krajnjim tačkama u $(0, 2)$ i $(1, 1)$. Poligoni P_f , P_g i P_h prikazani su na Slici 12.



Slika 12

Zaista, monomu x^2y^2 polinoma f koji se dobija na dva različita načina iz faktor-polinoma g i h odgovara tačka $(2, 2)$ koja nije teme poligona P_f .

Rad Ostrowskog je omogućio sledeći fundamentalni rezultat koji je formulisao Shuhong Gao 2001. godine u [14].

Teorema 5.30. Neka je F proizvoljno polje i f nenula polinom iz $F[x, y]$ koji nije deljiv ni sa x ni sa y . Ako je Newton-ov poligon polinoma f integralno nerastavljiv u smislu sume Minkowskog, onda je polinom f apsolutno nesvodljiv nad poljem F .

Dokaz:

Kako polinom f nije deljiv ni sa x ni sa y , f nema trivijalnu faktorizaciju. Pretpostavimo suprotno, polinom f nije apsolutno nesvodljiv nad poljem F , tj. ne ostaje nesvodljiv nad svakom algebarskom ekstenzijom polja F . To znači da nad nekom algebarskom ekstenzijom polja F važi $f = gh$, pri čemu g i h imaju bar dva nenula terma. Međutim, kako i g i h imaju bar po dva nenula terma njihovi pridruženi Newton-ovi poligoni imaju najmanje dve tačke. Kako je $f = gh$, na

osnovu **Teoreme 5.28.** sledi da važi $P_f = P_g + P_h$, pri čemu P_g i P_h imaju najmanje dve tačke. Dakle, ovo je netrivialna dekompozicija Newton-ovog poligona P_f , što je u kontradikciji sa pretpostavkom teoreme da je P_f integralno nerastavljiv. Zaključujemo da je polinom f apsolutno nesvodljiv nad poljem F .
□

Napomena 5.31. Na potpuno analogan način kao u **Definiciji 5.23.**, polinomu sa n promenljivih pridružujemo Newton-ov politop u \mathbb{R}^n , a **Teorema 5.28.** i **Teorema 5.30.** važe i u ovom slučaju. S obzirom na to da je tema ove disertacije svodljivost polinoma dve promenljive, ove teoreme su formulisane i dokazane za $n = 2$.

Napomena 5.32. Na osnovu **Teoreme 5.30.** zaokružuje se veza između nesvodljivosti polinoma dve promenljive i nerastavljivosti u smislu Minkowskog njima pridruženih Newton-ovih poligona. Naime, determinisanjem integralno nerastavljivih poligona biće, zapravo, određene čitave klase apsolutno nesvodljivih polinoma, što će biti prezentovano u narednom poglavlju.

6 Nesvodljivost polinoma dve promenljive pomoću Newton-ovih poligona

Na osnovu *Teoreme 5.30.*, problem pronalaženja apsolutno nesvodljivih polinoma dve promenljive nad proizvoljnim poljem se svodi na problem konstrukcije integralno nerastavljivih poligona. S obzirom na to, u ovom poglavlju bavićemo se pronalaženjem integralno nerastavljivih poligona i daćemo primere apsolutno nesvodljivih polinoma nad proizvoljnim poljem pridruženih ovim poligonima.

Definicija 6.1. Vektor $v = (x, y) \in \mathbb{Z}^2$ se naziva *primitivni vektor* ako je $NZD(x, y) = 1$.

Napomena 6.2. Ako je $c_i = NZD(a_i, b_i)$, onda su vektori $e_i = \left(\frac{a_i}{c_i}, \frac{b_i}{c_i}\right)$, $1 \leq i \leq n$ primitivni vektori.

Definicija 6.3. Neka je dat konveksan poligon P sa celobrojnim temenima u Euklidskoj ravni \mathbb{R}^2 i neka su $v_0, v_1, \dots, v_{n-1}, v_n = v_0$ redom temena poligona P u smeru suprotnom od smera kretanja kazaljke na satu. Ivice poligona su mogu predstaviti vektorima $E_i = v_i - v_{i-1} = (a_i, b_i)$, $1 \leq i \leq n$, pri čemu $a_i, b_i \in \mathbb{Z}$. Niz vektora E_i , $1 \leq i \leq n$, se naziva *poligonalni niz vektora (ivični niz vektora)* poligona P .

Napomena 6.4. Primitimo da važi $E_i = c_i e_i$, $1 \leq i \leq n$.

Napomena 6.5. Neka je $c_i = NZD(a_i, b_i)$, $1 \leq i \leq n$ i neka su $e_i = \left(\frac{a_i}{c_i}, \frac{b_i}{c_i}\right)$, $1 \leq i \leq n$. Poligonalni niz vektora poligona P se može zapisati u obliku $\{c_i e_i\}_{1 \leq i \leq n}$.

Napomena 6.6. Poligonalni niz vektora jedinstveno određuje poligon do na translaciju. Kako je rub poligona zatvorena putanja, važi: $\sum_{i=1}^n c_i e_i = (0, 0)$.

Sledeća teorema je dokazana u [15].

Teorema 6.7. Neka je P poligon sa celobrojnim temenima čiji je poligonalni niz vektora $\{c_i e_i\}_{1 \leq i \leq n}$, pri čemu su $e_i \in \mathbb{Z}^2$ primitivni vektori. Tada je poligon sa celobrojnim temenima Q poligon sabirak poligona P ako i samo ako je poli-

gonalni niz vektora poligona Q oblika $\{d_i e_i\}_{1 \leq i \leq n}$, pri čemu važi $0 \leq d_i \leq c_i$ i $\sum_{i=1}^n d_i e_i = (0, 0)$.

Dokaz:

(\Rightarrow) Neka je $\{d_i e_i\}_{1 \leq i \leq n}$ ivični niz vektora poligona Q . Iz **Napomene 4.14.** sledi da je svaka ivica poligona Q poligon-sabirak neke ivice $c_i e_i$ poligona P , gde je e_i primitivni vektor. Toj ivici poligona Q odgovara ivični vektor oblika $d_i e_i$, pri čemu važi $0 \leq d_i \leq c_i$. Kako je omotač poligona zatvorena putanja ivičnih vektora važi:

$$\sum_{i=1}^n d_i e_i = (0, 0).$$

(\Leftarrow) Proizvoljan niz vektora $\{d_i e_i\}_{1 \leq i \leq n}$ za koji važi $0 \leq d_i \leq c_i$, pri čemu je $\sum_{i=1}^n d_i e_i = (0, 0)$, definiše zatvorenu putanju. Kako je $\{c_i e_i\}_{1 \leq i \leq n}$ poligonalni niz vektora poligona P , $\{d_i e_i\}_{1 \leq i \leq n}$ definiše omotač konveksnog poligona koji je poligon sabirak poligona P i koji daje poligon P u zbiru Minkowskog sa poligonom čiji je ivični niz $\{(c_i - d_i) e_i\}_{1 \leq i \leq n}$. \square

Napomena 6.8. Za svaki poligon sa celobrojnim temenima koji ima dve paralelne ivice kojima odgovaraju primitivni vektori e_i i e_j važi: $e_i = -e_j$, odnosno $e_i + e_j = 0$. Odavde iz **Teoreme 6.7.** sledi da je ovaj poligon integralno rastavljiv u smislu sume Minkowskog. Zbog toga će, za sve poligone koji će biti razmatrani u ovom poglavlju, standardna pretpostavka biti da su im sva temena celobrojna i da nemaju paralelnih ivica.

Napomena 6.9. U daljem tekstu pod pojmom integralne nerastavljivosti poligona podrazumevaćemo da posmatrani poligon nema netrivialnu dekompoziciju u smislu sume Minkowskog.

Napomena 6.10. Iz **Teoreme 6.7.** je očigledno da bilo koji n -tougao sa celobrojnim temenima, $n \geq 3$, koji nema paralelnih ivica može jedino imati celobrojne poligone sabirke sa i ivica, pri čemu $i \in \{3, 4, \dots, n-1, n\}$.

U [29] su dokazani kriterijumi nerastavljivosti u smislu Minkowskog za poligone sa celobrojnim temenima u dvodimenzionalnoj Euklidskoj ravni \mathbb{R}^2 . Iz razloga kompletnosti, analizu počinjemo dužima.

Definicija 6.11. Za bilo koje dve tačke a_1 i a_2 iz \mathbb{R}^2 **duž** $[a_1, a_2]$ koja spaja

tačke a_1 i a_2 je skup svih tačaka oblika:

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

Napomena 6.12. Neka su $v_1, v_2, a_1, a_2, b_1, b_2$ tačke iz \mathbb{R}^2 za koje važi: $v_1 = a_1 + b_1$ i $v_2 = a_2 + b_2$. Tada je: $[v_1, v_2] \subseteq [a_1, a_2] + [b_1, b_2]$.

Ako važi: $[v_1, v_2] = [a_1, a_2] + [b_1, b_2]$, onda su duži $[v_1, v_2]$, $[a_1, a_2]$ i $[b_1, b_2]$ paralelne jer:

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

Očigledno važi: $(0, 0) = (0, 0) + (0, 0)$ i $(1, 1) = (0, 1) + (1, 0)$, pa važi i:

$$\text{conv}((0, 0), (1, 1)) \subseteq \text{conv}((0, 0), (0, 1)) + \text{conv}((0, 0), (1, 0))$$

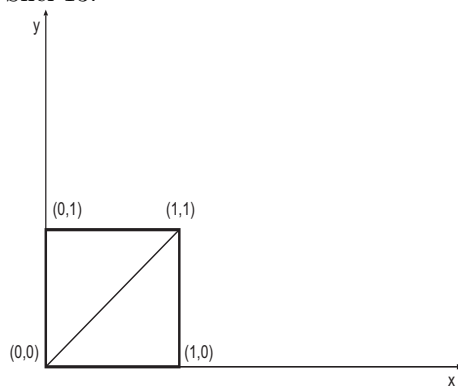
tj.

$$\text{conv}((0, 0), (1, 1)) \subseteq \text{conv}((0, 0), (0, 1), (1, 1), (1, 0)),$$

jer je $\text{conv}((0, 0), (1, 1))$ dijagonala kvadrata $\text{conv}((0, 0), (0, 1), (1, 1), (1, 0))$. S obzirom na to da duži $\text{conv}((0, 0), (1, 1))$, $\text{conv}((0, 0), (0, 1))$ i $\text{conv}((0, 0), (1, 0))$ nisu paralelne, ne važi:

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

što je prikazano na Slici 13.



Slika 13

Napomena 6.13. Sa $NZD(a)$ ćemo obeležavati $NZD(a_x, a_y)$, pri čemu je $a = (a_x, a_y)$ proizvoljna tačka iz \mathbb{R}^2 sa celobrojnim koordinatama. Slično, sa

$NZD(a, b)$ ćemo označavati $NZD(NZD(a), NZD(b))$, gde su a, b proizvoljne tačke iz \mathbb{R}^2 sa celobrojnim koordinatama.

Sledeća teorema nam daje mogućnost da odredimo broj tačaka sa celobrojnim koordinatama na proizvoljnoj duži.

Teorema 6.14. Neka su a_1 i a_2 dve različite tačke sa celobrojnim koordinatama iz \mathbb{R}^2 . Tada na duži $[a_1, a_2]$ ima tačno $NZD(a_2 - a_1) + 1$ tačka sa celobrojnim koordinatama, računajući a_1 i a_2 . Štaviše, ako je a_3 proizvoljna tačka sa celobrojnim koordinatama na otvorenoj duži (a_1, a_2) , tj. $a_3 = \alpha a_1 + \beta a_2$, za neke $\alpha > 0$ i $\beta > 0$ takve da je $\alpha + \beta = 1$, tada važi:

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

Dokaz:

Neka je a_3 tačka na otvorenoj duži (a_1, a_2) . Tada je $a_3 = \alpha a_1 + \beta a_2$, za neke $\alpha > 0$ i $\beta > 0$ takve da je $\alpha + \beta = 1$.

Tada važi:

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

kao i:

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

Odavde sledi:

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

Jasno je da prethodna jednakost važi za bilo koju tačku na otvorenoj duži (a_1, a_2) , bez obzira da li su njene koordinate celobrojne.

Iz jednakosti $a_3 - a_1 = \beta(a_2 - a_1)$ očigledno je da je a_3 tačka sa celobrojnim koordinatama ako i samo ako je $\beta(a_2 - a_1)$ tačka sa celobrojnim koordinatama. Neka je a_3 tačka sa celobrojnim koordinatama. Kako je $a_2 - a_1$ tačka sa celobrojnim koordinatama i $a_3 \neq a_1$, sledi da je β racionalan broj oblika:

$$\beta = \frac{m}{n}, \text{ za neke } 0 < m < n, \text{ takve da je } NZD(m, n) = 1.$$

Jasno je da je $\beta(a_2 - a_1)$ tačka sa celobrojnim koordinatama ako i samo ako n deli $d = NZD(a_2 - a_1)$. Dakle, da bi a_3 bila tačka sa celobrojnim koordinatama, potrebno je da važi:

$$\beta = \frac{g}{d}, \text{ gde je } g = \frac{md}{n},$$

pa važi: $0 < g < d$.

Oдавde sledi da g biramo na $d - 1$ način, pa zaključujemo da na zatvorenoj duži $[a_1, a_2]$ ima $(d - 1) + 2 = d + 1$ tačka sa celobrojnim koordinatama.

Dalje dobijamo:

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

za neki primitivni vektor v' .

Slično dobijamo:

$$\begin{aligned} a_3 - a_2 &= \alpha(a_1 - a_2) = (1 - \beta)(a_1 - a_2) = \\ &= \left(1 - \frac{g}{d}\right)(a_1 - a_2) = \frac{d - g}{d}(a_1 - a_2) = \frac{d - g}{d}(-dv'). \end{aligned}$$

Kako je v' primitivni vektor, sledi da je:

$$NZD(a_3 - a_1) = g \text{ i } NZD(a_3 - a_2) = d - g.$$

Oдавde dobijamo:

$$\frac{NZD(a_3 - a_1)}{NZD(a_3 - a_2)} = \frac{g}{d - g} = \frac{\frac{g}{d}}{\frac{d - g}{d}} = \frac{\frac{g}{d}}{1 - \frac{g}{d}} = \frac{\beta}{1 - \beta} = \frac{\beta}{\alpha},$$

čime je dokaz završen. \square

Teorema 6.15. Neka su a_1 i a_2 dve različite tačke sa celobrojnim koordinatama iz \mathbb{R}^2 . Duž $[a_1, a_2]$ je integralno nerastavljiva u smislu sume Minkowskog ako i samo ako je $NZD(a_2 - a_1) = 1$.

Dokaz:

(\Rightarrow) Neka je duž $[a_1, a_2]$ integralno nerastavljiva u smislu Minkowskog. Pokažimo da je $NZD(a_2 - a_1) = 1$. Pretpostavimo suprotno: $NZD(a_2 - a_1) = d > 1$.

Tada na duži $[a_1, a_2]$ ima tačno $d + 1$ tačka sa celobrojnim koordinatama, računajući a_1 i a_2 . Kako je $d > 1$, sledi da je $d + 1 > 2$, odnosno $d + 1 \geq 3$.

Dakle, na duži $[a_1, a_2]$ ima bar 3 tačke sa celobrojnim koordinatama, računajući a_1 i a_2 . Odavde je jasno da se na otvorenoj duži (a_1, a_2) nalazi bar jedna tačka c sa celobrojnim koordinatama. Tada za nju važi:

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

odnosno duž $[a_1, a_2]$ je integralno rastavljiva u smislu Minkowskog, što je kontradikcija. Dakle, važi $NZD(a_2 - a_1) = 1$.

(\Leftarrow) Neka je $NZD(a_2 - a_1) = 1$. Pokažimo da je duž $[a_1, a_2]$ integralno nerastavljiva u smislu sume Minkowskog. Pretpostavimo suprotno: $[a_1, a_2] = [b_1, b_2] + [c_1, c_2]$, za neke duži $[b_1, b_2]$, $[c_1, c_2]$ sa celobrojnim koordinatama za koje važi $\|(b_1, b_2)\| > 0$ i $\|(c_1, c_2)\| > 0$. Odavde sledi da su duži $[a_1, a_2]$, $[b_1, b_2]$ i $[c_1, c_2]$ paralelne. Ovo je očigledna kontradikcija s obzirom na to da je duž $[a_1, a_2]$ primitivna. Dakle, duž $[a_1, a_2]$ je integralno nerastavljiva u smislu sume Minkowskog. \square

Primer 6.16. Polinom $f(x, y) = x^m + y^n$ je apsolutno nesvodljiv nad proizvoljnim poljem ako i samo ako je $NZD(m, n) = 1$.

Teorema 6.17. Trougao $\text{conv}(v_1, v_2, v_3)$ u \mathbb{R}^2 sa celobrojnim temenima v_1, v_2, v_3 je integralno nerastavljiv u smislu sume Minkowskog ako i samo ako je:

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

Dokaz:

(\Leftarrow) Neka je $T = \text{conv}(v_1, v_2, v_3)$ trougao sa celobrojnim temenima u \mathbb{R}^2 . Formirajmo ivične vektore trougla T na sledeći način:

$$E_1 = v_2 - v_1 = c_1 e_1, \quad E_2 = v_3 - v_2 = c_2 e_2 \quad \text{i} \quad E_3 = v_1 - v_3 = c_3 e_3,$$

pri čemu su:

$$c_1 = NZD(v_2 - v_1), \quad c_2 = NZD(v_3 - v_2) \quad \text{i} \quad c_3 = NZD(v_1 - v_3)$$

pozitivni, celi brojevi, a e_1, e_2 i e_3 su primitivni ivični vektori trougla T . Kako T nema paralelnih ivica, na osnovu **Napomene 6.10.** zaključujemo da svaki konveksan poligon S sa celobrojnim temenima koji je poligon sabirak trougla T mora biti trougao i njegov ivični niz vektora je oblika:

$$E'_1 = d_1 e_1, \quad E'_2 = d_2 e_2 \quad \text{i} \quad E'_3 = d_3 e_3,$$

gde su $0 \leq d_i \leq c_i$, za $i = 1, 2, 3$, pri čemu važi:

$$E'_1 + E'_2 + E'_3 = (0, 0).$$

Stoga, svaki poligon sabirak trougla T mora biti trougao koji je sličan trouglu T . Drugim rečima, važi:

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

gde je $\frac{m}{n}$ racionalan broj, $0 \leq m \leq n$ i $NZD(m, n) = 1$.

Kako su d_i , $i = 1, 2, 3$ celi brojevi, jasno je da n deli c_j , $j = 1, 2, 3$.

S obzirom na to da je $NZD(v_1 - v_2, v_1 - v_3) = 1$, važi:

$$NZD(NZD(v_1 - v_2), NZD(v_1 - v_3)) = NZD(c_1, c_3) = 1,$$

tj. c_1 i c_3 su uzajamno prosti. Kako n deli i c_1 i c_3 , zaključujemo da je $n = 1$. Iz relacije $0 \leq m \leq n$ sledi da je $m = 0$ ili $m = 1$. Odavde dobijamo $S = (0, 0)$ ili $S = T$. Dakle, trougao T nema netrivialnu dekompoziciju, pa je integralno nerastavljiv u smislu sume Minkowskog.

(\Rightarrow) Neka je trougao T integralno nerastavljiv. Treba pokazati da je:

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

Pretpostavimo suprotno, $NZD(v_1 - v_2, v_1 - v_3) = NZD(c_1, c_3) = d > 1$. Tada je $S = conv(0, v_2 - v_1, v_3 - v_1)$ trougao sa celobrojnim temenima i očigledno važi: $T = v_1 + d \left(\frac{1}{d}S\right)$. Dakle, sledi da trougao T ima netrivialnu dekompoziciju u smislu sume Minkowskog, što je kontradikcija. Dakle, važi $NZD(v_1 - v_2, v_1 - v_3) = 1$. \square

Napomena 6.18. Na osnovu dokaza **Teoreme 6.17.** jasno je da je trougao u \mathbb{R}^2 sa celobrojnim temenima v_1, v_2, v_3 integralno nerastavljiv u smislu sume Minkowskog ako važi:

$$NZD(v_i - v_j, v_i - v_k) = 1, \text{ za neke } i, j, k, \{i, j, k\} = \{1, 2, 3\}.$$

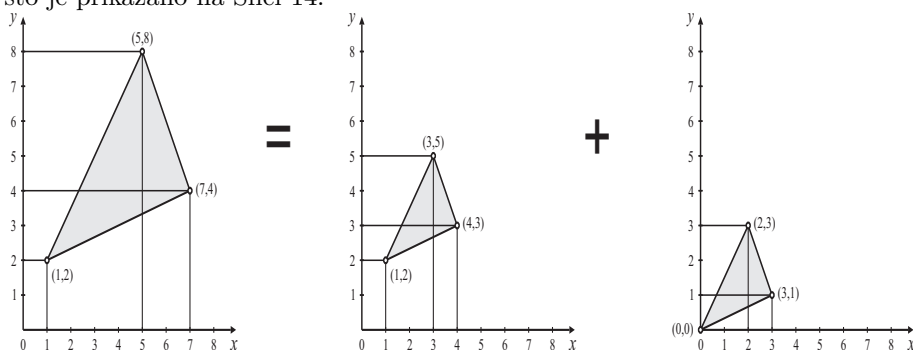
Primer 6.19. Posmatrajmo trougao $conv((1, 2), (7, 4), (5, 8))$. Kako je:

$$NZD((7, 4) - (1, 2), (7, 4) - (5, 8)) = NZD((6, 2), (2, -4)) = 2 > 1$$

sledi da je trougao $\text{conv}((1, 2), (7, 4), (5, 8))$ rastavljiv u smislu sume Minkowskog i njegova dekompozicija je:

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

što je prikazano na Slici 14.



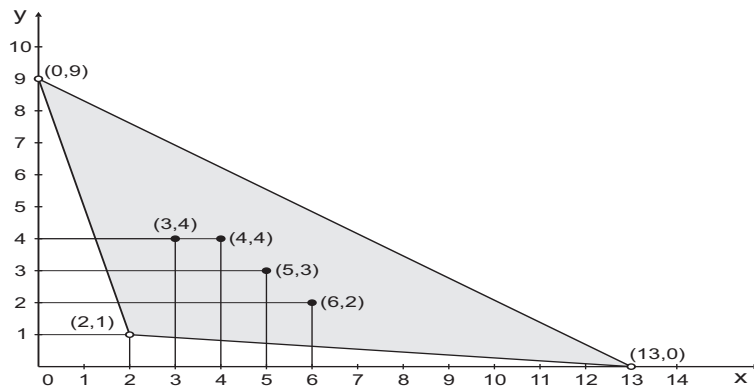
Slika 14

Primer 6.20. Posmatrajmo polinom:

$$f(x, y) = a_1x^{13} + a_2y^9 + a_3x^2y + a_4x^4y^4 + a_5x^5y^3 + a_6x^6y^2 + a_7x^3y^4,$$

pri čemu je $a_1, \dots, a_7 \in F \setminus \{0\}$, gde je F proizvoljno polje.

Monomima polinoma $f(x, y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponenata: $(13, 0)$, $(0, 9)$, $(2, 1)$, $(4, 4)$, $(5, 3)$, $(6, 2)$ i $(3, 4)$. Newton-ov poligon polinoma $f(x, y)$ je trougao $P_f = \text{conv}((13, 0), (0, 9), (2, 1))$ prikazan na Slici 15.



Slika 15

Kako je:

$$\begin{aligned} NZD((13, 0) - (0, 9), (13, 0) - (2, 1)) &= NZD((13, -9), (11, -1)) = \\ &= NZD(NZD(13, -9), NZD(11, -1)) = NZD(1, 1) = 1, \end{aligned}$$

sledi da je trougao $P_f = \text{conv}((13, 0), (0, 9), (2, 1))$ integralno nerastavljiv u smislu sume Minkowskog, pa je polinom $f(x, y)$ apsolutno nesvodljiv nad poljem F .

Polinom $f(x, y)$ "ostaje" apsolutno nesvodljiv nad poljem F ako mu se dodaju monomi čiji vektori eksponenata leže u Newton-ovom poligonu polinoma $f(x, y)$.

S obzirom da njihovi vektori eksponenata leže u P_f , možemo dodati monome x^7y^2, x^5y^4 itd. sa proizvoljnim koeficijentima iz polja F .

Drugim rečima, svaki polinom oblika:

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

gde $a_1, \dots, a_7, c_{ij} \in F \setminus \{0\}$ i $(i, j) \in P_f$, je apsolutno nesvodljiv nad F .

Napomena 6.21. Na sličan način u [29] formulisani su stavovi o integralnoj nerastavljivosti za četvorouglove i petouglove sa celobrojnim temenima i, na taj način, pronalaze se familije njima pridruženih apsolutno nesvodljivih polinoma sa dve promenljive nad proizvoljnim poljem. Naravno, analiza se za četvorouglove i petouglove značajno komplikuje, ali princip je potpuno analogan kao u slučaju kad se razmatraju stavovi o apsolutnoj nesvodljivosti polinoma dve promenljive zasnovani na integralnoj nerastavljivosti duži i trouglova prezentovani u ovom poglavlju, pa ih iz tog razloga nećemo navoditi. Zadatak ove disertacije je, u izvesnoj meri, rešavanje obratnog problema u odnosu na [29] - formulisanje potrebnog i dovoljnog uslova pod kojim bi polinom dve promenljive sa celobrojnim koeficijentima imao netrivialnu faktorizaciju na faktor - polinome sa celobrojnim koeficijentima.

U [15] dat je algoritam kojim se testira apsolutna nesvodljivost polinoma dve promenljive analizom nerastavljivosti njima pridruženih Newton-ovih poligona u smislu Minkowskog. Naime, ako je pridružen Newton-ov poligon nerastavljiv u smislu Minkowskog, onda je odgovarajući polinom apsolutno nesvodljiv.

Sa druge strane, u slučaju da je Newton-ov poligon rastavljiv u smislu Minkowskog, algoritam ne daje zaključak o nesvodljivosti odgovarajućeg polinoma. Dakle, s obzirom na to da uzima u obzir samo Newton-ov poligon polinoma, ali ne i njegove koeficijente, ovaj algoritam se ne može koristiti kao test apsolutne nesvodljivosti za polinome sa rastavljivim Newton-ovim poligonom, jer je tada potrebno analizirati i koeficijente polinoma. Međutim, s obzirom na to da je algoritam dat u [15] izuzetno brz u poređenju sa nekim drugim algoritmima kojim se može testirati nesvodljivost proizvoljnog polinoma dve promenljive, ovaj algoritam bi se mogao koristiti kao pretest pre primene nekog od sporijih i zahtevnijih algoritama [8], [67], [18], [27] i [34].

Geometrijski pristup nesvodljivosti polinoma predmet je izučavanja brojnih radova. Filaseta [11] analizira nesvodljivost Bessel-ovih polinoma pomoću Newton-ovih poligona. Lipkovski [36] pridružuje polinomu neograničeni Newton-ov polihedron i formuliše nekoliko kriterijuma za konstrukciju nerastavljivih Newton-ovih polihedrona. Shanok [54] formuliše stavove o nesvodljivosti polinoma tri promenljive pomoću Newton-ovih politopa u \mathbb{R}^3 njihovom projekcijom na ravan.

7 Faktorizacija polinoma dve promenljive sa celobrojnim koeficijentima pomoću Newton-ovih poligona

Vežu između integralno nerastavljivih politopa i apsolutno nesvodljivih polinoma više promenljivih je u potpunosti opisao Shuhong Gao 2001. godine u [14]. Naime, ukoliko je politop pridružen polinomu integralno nerastavljiv u smislu sume Minkowskog, onda je odgovarajući polinom apsolutno nesvodljiv. Međutim, rešavanje obrnutog problema ostalo je otvoren problem - pod kojim uslovima integralno rastavljivi politop odgovara svodljivom polinomu. Potrebu istraživanja u pravcu geometrijske analize faktorizacije polinoma konstatuje Erich Kaltofen 1992. godine u preglednom radu [26] i Sturmfels 1996. godine u [61]. Ovaj problem parcijalno rešava Fatih Koyuncu 2005. godine u [30], gde diskutuje svodljivost polinoma dve i tri promenljive kojima odgovara rastavljivi politop u zavisnosti od karakteristike polja.

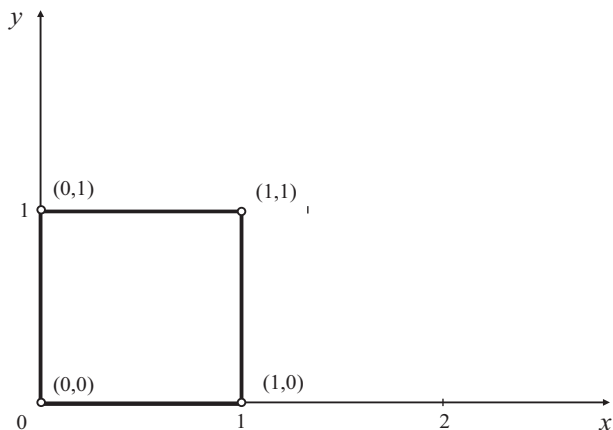
Napomena 7.1. Posmatrajmo polinom f nad poljem F . Ako je Newton-ov poligon polinoma f integralno rastavljivi u smislu sume Minkowskog, u zavisnosti od datog polja, f može biti svodljiv ili nesvodljiv.

S obzirom na **Teoremu 5.28.**, ako polinom f ima faktorizaciju, tada njemu pridruženi Newton-ov poligon ima dekompoziciju u smislu sume Minkowskog. Dakle, neka je Newton-ov poligon polinoma $f(P_f)$ integralno rastavljivi. Pretpostavimo da P_f ima m mogućih dekompozicija u smislu sume Minkowskog, tj. da važi: $P_f = A_i + B_i$, $A_i, B_i \subseteq \mathbb{R}^2$, $i = 1, \dots, m$, za neke integralne poligone A_i i B_i . Na osnovu **Teoreme 5.28.**, ako polinom f ima faktorizaciju $f = g_i h_i$, tada su Newton-ovi poligoni polinoma g_i i h_i upravo A_i i B_i za neko $i = 1, \dots, m$.

Primer 7.2. Posmatrajmo polinom:

$$f(x, y) = xy + x + y + 1 \in F[x, y], \text{ za proizvoljno polje } F.$$

Monomima polinoma $f(x, y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponentata: $(1, 1)$, $(1, 0)$, $(0, 1)$ i $(0, 0)$. Newton-ov poligon polinoma $f(x, y)$ je kvadrat sa celobrojnim temenima prikazan na Slici 16.

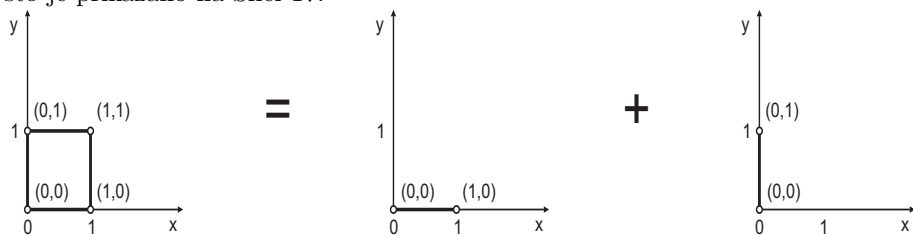


Slika 16

Jasno je da P_f može biti integralno rastavljen u smislu sume Minkowskog samo na jedan način:

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

što je prikazano na Slici 17.



Slika 17

Polinom $f(x, y)$ može se faktorirati na sledeći način:

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

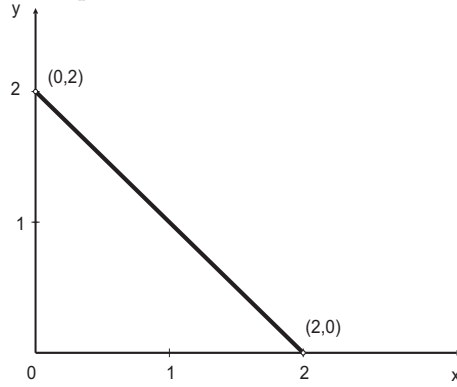
Očigledno je da su $\text{conv}((0, 0), (1, 0))$ i $\text{conv}((0, 0), (0, 1))$ Newton-ovi poligoni faktor - polinoma od $f(x, y)$.

Primer 7.3. Posmatrajmo polinom:

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

i razmortimo njegovu svodljivost u zavisnosti od karakteristike polja.

Monomima polinoma $f(x, y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponenata: $(2, 0)$ i $(0, 2)$. Newton-ov poligon polinoma $f(x, y)$ je duž sa celobrojnim temenima prikazana na Slici 18.

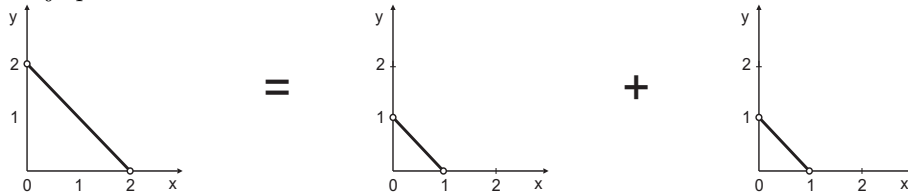


Slika 18

Očigledno je da P_f može biti integralno rastavljen u smislu sume Minkowskog samo na jedan način:

$$P_f = \text{conv}((2, 0), (0, 2)) = \text{conv}((1, 0), (0, 1)) + \text{conv}((1, 0), (0, 1)),$$

što je prikazano na Slici 19.



Slika 19

Koristeći komutativnost množenja u polju i s obzirom da nad poljem karakteristike 2 važi $xy + xy = 0$, dobijamo:

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

Drugim rečima, nad poljem karakteristike 2 važi:

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

Oдавде zaključujemo da se polinom $f(x, y) = x^2 + y^2$ nad poljem karakteristike 2 može faktorisati na sledeći način:

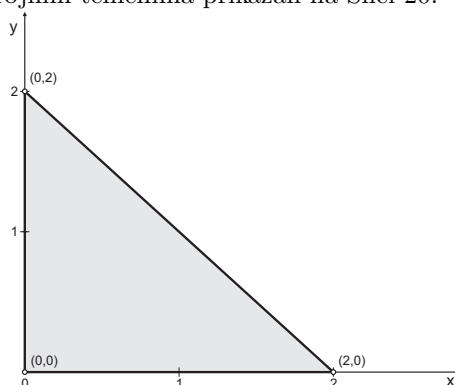
$$f(x, y) = (x + y)(x + y).$$

Primer 7.4. Posmatrajmo polinom:

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

i razmortimo njegovu svodljivost u zavisnosti od karakteristike polja.

Monomima polinoma $f(x, y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponenata: $(2, 0)$, $(0, 2)$ i $(0, 0)$. Newton-ov poligon polinoma $f(x, y)$ je trougao sa celobrojnim temenima prikazan na Slici 20.

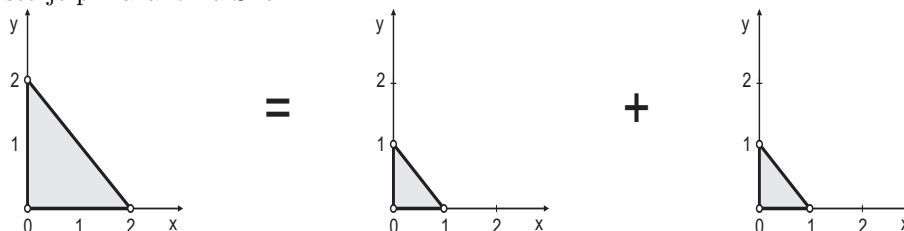


Slika 20

Očigledno je da $P_f = \text{conv}((2, 0), (0, 2), (0, 0))$ može biti integralno rastavljen u smislu sume Minkowskog samo na jedan način:

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

što je prikazano na Slici 21.



Slika 21

Očigledno važi:

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

Koristeći komutativnost množenja u polju dobijamo:

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

Kako nad poljem karakteristike 2 važi: $xy + xy = 0$, $x + x = 0$, $y + y = 0$, koristeći osobinu asocijativnosti sabiranja u polju iz prethodnog izraza dobijamo:

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

Drugim rečima, nad poljem karakteristike 2 važi:

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

Odavde zaključujemo da se polinom $f(x, y) = x^2 + y^2 + 1$ nad poljem karakteristike 2 može faktorisati na sledeći način:

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

Napomena 7.5. Kao što je prikazano u **Primeru 7.2.**, **Primeru 7.3.** i **Primeru 7.4.**, **Teorema 5.28.** se može koristiti da se pronađu moguće faktorizacije polinoma sa dve promenljive malog stepena. S obzirom na to da je rastavlјivost pridruženog Newton-ovog poligona, u smislu sume Minkowskog, potreban uslov za postojanje faktorizacije polinoma sa dve promenljive, za polinome kojima odgovara rastavlјiv Newton-ov poligon se diskutuje svodljivost u odnosu na karakteristiku polja. Jasno je da se u slučaju polinoma sa velikim stepenom analiza komplikuje. Međutim, **Teorema 5.28.** može bar pružiti informaciju o obliku faktora polinoma sa dve promenljive visokog stepena.

Na osnovu **Teoreme 5.30.** sledi da Newton-ov poligon koji odgovara proizvolјnom polinomu dve promenljive sa celobrojnim koeficijentima daje potpunu informaciju o njegovoj eventualnoj apsolutnoj nesvodljivosti, pa je intuitivno očekivano da nosi i deo informacije o njegovoj eventualnoj svodljivosti. Naime, ostalo je otvoreno pitanje pod kojim uslovima rastavlјiv Newton-ov poligon odgovara svodljivom polinomu. Drugim rečima, nameće se potreba karakterizacije svodljivih polinoma dve promenljive sa celobrojnim koeficijentima u smislu formulacije potrebnog i dovoljnog uslova za egzistenciju netrivialne faktorizacije u faktor - polinome sa celobrojnim koeficijentima pomoću Newton-ovog poligona pridruženog datom polinomu. Na taj način bi se, pored poznate veze između apsolutne nesvodljivosti polinoma dve promenljive i nerastavlјivosti njima pridruženih Newton-ovih poligona, ustanovila i povezanost svodljivosti polinoma

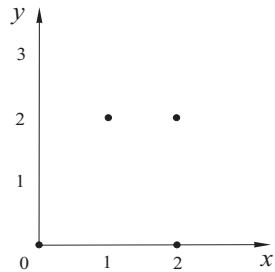
dve promenljive sa Newton-ovim poligonima, pa bi se povezanost polinoma dve promenljive i njima pridruženih Newton-ovih poligona, u smislu svodljivosti polinoma, u potpunosti opisala.

Definicija 7.6. Neka je $f(x, y) \in \mathbb{Z}[x, y]$. **Neproširena mreža čvorova** polinoma $f(x, y)$ se sastoji od svih tačaka $(e_1, e_2)_i, i = 1, \dots, k$ koje odgovaraju vektorima eksponenata monoma polinoma $f(x, y)$ sa nenula koeficijentima. Ako Newton-ov poligon polinoma $f(x, y)$ sadrži, u svojoj unutrašnjosti i na rubu, neke celobrojne tačke različite od $(e_1, e_2)_i, i = 1, \dots, k$, te tačke, zajedno sa tačkama $(e_1, e_2)_i, i = 1, \dots, k$, formiraju **proširenu mrežu čvorova** polinoma $f(x, y)$.

Primer 7.7. Posmatrajmo polinom $f(x, y) \in \mathbb{Z}[x, y]$:

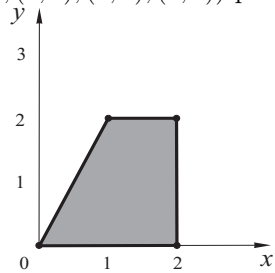
$$f(x, y) = 3x^2y^2 + 2xy^2 + x^2 + 1.$$

Nenula monomima polinoma $f(x, y)$ odgovaraju tačke $(2, 2), (1, 2), (2, 0)$ i $(0, 0)$. Ove tačke formiraju neproširenu mrežu čvorova polinoma $f(x, y)$ koja je prikazana na Slici 22.



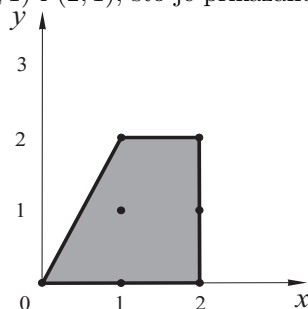
Slika 22

Newton-ov poligon polinoma $f(x, y)$ je konveksni omotač tačaka $(2, 2), (1, 2), (2, 0)$ i $(0, 0)$, tj. $\text{conv}((2, 2), (1, 2), (2, 0), (0, 0))$ prikazan na Slici 23.



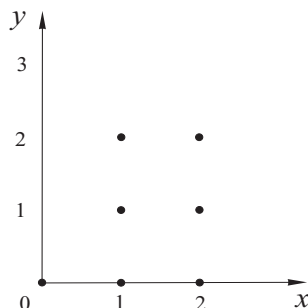
Slika 23

Newton-ov poligon polinoma $f(x, y)$ sadrži u svojoj unutrašnjosti i na rubu celobrojne tačke $(1, 0)$, $(1, 1)$ i $(2, 1)$, što je prikazano na Slici 24.



Slika 24

Tačke neproširene mreže čvorova polinoma $f(x, y)$ zajedno sa tačkama $(1, 0)$, $(1, 1)$ i $(2, 1)$ formiraju proširenu mrežu čvorova polinoma $f(x, y)$ koja je prikazana na Slici 25.



Slika 25

Definicija 7.8. Neka $f(x, y) \in \mathbb{Z}[x, y]$ i neka je $P = \{A_1, A_2, \dots, A_n\}$ mreža čvorova polinoma $f(x, y)$ eventualno proširena sa nekim celobrojnim tačkama iz unutrašnjosti ili sa ruba Newton-ovog poligona polinoma $f(x, y)$. Bez gubitka opštosti možemo pretpostaviti da, nakon konstrukcije Newton-ovog poligona polinoma $f(x, y)$ tačke A_1, A_2, \dots, A_k , $k \geq 2$, postaju temena poligona, a A_{k+1}, \dots, A_n ne postaju. Kažemo da je grupisanje čvorova skupa P , G_1, \dots, G_l , $l \geq 2$, **prekrivanje** P ako:

1. Svaka grupa G_i , $i = 1, \dots, l$, sadrži isti broj tačaka ne manji od dva,
2. $\bigcup_{i=1}^l G_i = P$,

3. Tačke A_1, A_2, \dots, A_k se pojavljuju u tačno jednom od skupova G_1, \dots, G_l ,
4. Tačke A_{k+1}, \dots, A_n se pojavljuju u najmanje jednom od skupova G_1, \dots, G_l ,
5. Konveksni poligoni određeni sa G_1, G_2, \dots, G_l su podudarni i G_2, \dots, G_l se dobijaju iz G_1 translacijom.

Definicija 7.9. Neka $f(x, y) \in \mathbb{Z}[x, y]$ i neka je $P = \{A_1, A_2, \dots, A_n\}$ mreža čvorova polinoma $f(x, y)$ eventualno proširena sa nekim celobrojnim tačkama iz unutrašnjosti ili sa ruba Newton-ovog poligona polinoma $f(x, y)$. Neka je:

$$G_1 = \text{conv}(A_{i_{1,1}}, \dots, A_{i_{1,k}}), \dots, G_l = \text{conv}(A_{i_{l,1}}, \dots, A_{i_{l,k}}), l \geq 2,$$

pri čemu je $\{i_{1,1}, \dots, i_{1,k}, \dots, i_{l,1}, \dots, i_{l,k}\} = \{1, \dots, n\}$ prepoкрivanje P sa l podudarnih k -gona. S obzirom na to da je kompozicija dve translacije takođe translacija, za svako G_p i G_q , $p \neq q$, $p, q \in \{1, \dots, l\}$ postoji translacija $\tau_{p,q}$, takva da $\tau_{p,q}(G_p) = G_q$. Za svaki poligon redosled temena je takav da je najpre navedeno teme koje ima najmanju x -koordinatu. Ako takvo teme nije jedinstveno, najpre navodimo ono teme sa najmanjom y -koordinatom. Zatim navodimo ostala temena u smeru suprotnom od smera kazaljke na satu. Jasno je da važi: $\tau_{p,q}(A_{i_{p,w}}) = A_{i_{q,w}}$, za svako p i q , $p \neq q$, $p, q \in \{1, \dots, l\}$ i svako $w = 1, \dots, k$. Obeležimo sa $\text{coef}(A_i)$ koeficijent polinoma $f(x, y)$ koji odgovara eksponent vektoru A_i . Pretpostavimo da poligoni G_1, G_2, \dots, G_l nemaju zajedničkih čvorova. Kažemo da je prepoкрivanje P **odgovarajuće prepoкрivanje** u odnosu na koeficijente polinoma $f(x, y)$ ako:

$$\begin{aligned} \text{coef}(A_{i_{1,1}}) : \text{coef}(A_{i_{1,2}}) : \dots : \text{coef}(A_{i_{1,k}}) &= \dots = \\ &= \text{coef}(A_{i_{l,1}}) : \text{coef}(A_{i_{l,2}}) : \dots : \text{coef}(A_{i_{l,k}}). \end{aligned}$$

Pretpostavimo da poligoni G_1, \dots, G_l imaju zajedničkih čvorova. Svaki G_i , $i = 1, \dots, l$, određuje polinom $p_i(x, y)$ takav da $f(x, y) = p_1(x, y) + \dots + p_l(x, y)$, pri čemu su polinomi sabirci $p_i(x, y)$, $i = 1, \dots, l$, uređeni na isti način kao temena. Za svako teme A_c , koje je zajedničko za s poligona, koeficijent monoma čiji je eksponent vektor A_c je prikazan kao suma s celih brojeva na način da svaki od njih pripada tačno jednom polinomu $p_i(x, y)$, tako da su koeficijenti polinoma $p_1(x, y), \dots, p_l(x, y)$, $p_i(x, y) = c_{i,1}x^{\alpha_{i,1}}y^{\beta_{i,1}} + \dots + c_{i,k}x^{\alpha_{i,k}}y^{\beta_{i,k}}$ proporcionalni, tj.:

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

Ako ovo važi za svaki zajednički čvor, kažemo da je prepokrivanje P **odgovarajuće prepokrivanje** u odnosu na koeficijente polinoma $f(x, y)$.

Napomena 7.10. Ako su neke od tačaka A_{k+1}, \dots, A_n unutrašnje tačke poligona G_1 te tačke se translacijama preslikavaju na odgovarajuće unutrašnje tačke poligona G_2, \dots, G_l . Predhodna definicija je, iz razloga jednostavnosti zapisa, data za slučaj bez unutrašnjih tačaka. Naravno, proporcije važe i u slučaju da su neke od tačaka A_{k+1}, \dots, A_n unutrašnje tačke poligona G_1 . Iz **Teoreme 5.30.** očigledno je da iz integralne nerastavljivosti odgovarajućeg Newton-ovog poligona, koji je u potpunosti određen svojim temenima, sledi apsolutna nesvodljivost polinoma nad tim poljem. Štaviše, svaki polinom koji ima iste nenula terme je takođe apsolutno nesvodljiv nad tim poljem. Svaki takav polinom ostaje nesvodljiv ukoliko mu se dodaju monomi čiji vektori eksponenata leže u unutrašnjosti ili na rubu Newton-ovog poligona. Sa druge strane, Newton-ov poligon polinoma ne nosi kompletnu informaciju o eventualnom postojanju faktorizacije polinoma. U delu koji sledi biće pokazano da, pri faktorizaciji polinoma, važno je uzeti u obzir temena Newton-ovog poligona, ali i tačke koje nisu postale temena Newton-ovog poligona, kao i celobrojne tačke koje se nalaze u unutrašnjosti ili na rubu Newton-ovog poligona.

Napomena 7.11. S obzirom na to da su predmet istraživanja ovog rada netrivialne faktorizacije, u radu se analiziraju polinomi koji nisu deljivi ni sa x ni sa y . Dakle, ukoliko treba diskutovati postojanje netrivialne faktorizacije polinoma koji je deljiv sa x , y ili i sa x , i sa y , najpre treba predstaviti polinom kao proizvod trivijalnog faktora x^α , y^β ili $x^\alpha y^\beta$, a zatim diskutovati eventualne faktorizacije netrivialnog faktor-polinoma.

Potreban i dovoljan uslov za postojanje netrivialne faktorizacije polinoma dve promenljive sa celobrojnim koeficijentima, koji predstavlja centralni originalni rezultat disertacije dat je u [6].

Teorema 7.12. Neka je $f(x, y)$ nenula polinom, $f(x, y) \in \mathbb{Z}[x, y]$. Polinom $f(x, y)$ ima netrivialnu faktorizaciju u faktor-polinome sa celobrojnim koeficijentima ako i samo ako mreža čvorova koja odgovara polinomu $f(x, y)$, eventualno proširena nekim celobrojnim tačkama koje leže u unutrašnjosti ili na rubu Newton-ovog poligona polinoma $f(x, y)$, ima odgovarajuće prepokrivanje u odnosu na koeficijente polinoma $f(x, y)$.

Dokaz:

(\Rightarrow) Pretpostavimo da polinom $f(x, y)$ ima netrivialnu faktorizaciju, odnosno da postoje polinomi sa celobrojnim koeficijentima $g(x, y)$ i $h(x, y)$ koji oba imaju bar dva monoma i za koje važi: $f(x, y) = g(x, y) \cdot h(x, y)$. Neka je $h(x, y) = c_1 x^{\alpha_1} y^{\beta_1} + \dots + c_k x^{\alpha_k} y^{\beta_k}$, pri čemu je $c_i \neq 0$, bar za dva i , $i = 1, \dots, k$. Neka je $c_p \neq 0$ i $c_q \neq 0$. Očigledno je da $(\alpha_p, \beta_p) \neq (0, 0)$ ili $(\alpha_q, \beta_q) \neq (0, 0)$. Dakle, polinom $h(x, y)$ se može zapisati u sledećem obliku:

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

pri čemu je $I \subset \{1, \dots, k\} \setminus \{p, q\}$, skup svih indeksa različitih od p i q , takvih da je za $i \in I$, $c_i \neq 0$. Jasno, ako polinom $h(x, y)$ nema drugih nenula monoma osim $c_p x^{\alpha_p} y^{\beta_p}$ i $c_q x^{\alpha_q} y^{\beta_q}$, skup I je prazan. Polinom $f(x, y)$ se može zapisati u sledećem obliku:

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

Odnosno:

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

Obeležimo Newton-ove poligone polinoma $g(x, y)$ i $f(x, y)$ sa P_g i P_f . S obzirom na to da množenje polinoma $g(x, y)$ monomima $c_p x^{\alpha_p} y^{\beta_p}$, $c_q x^{\alpha_q} y^{\beta_q}$ itd. odgovara translaciji poligona P_g za vektore (α_p, β_p) , (α_q, β_q) itd., jasno je da je Newton-ov poligon polinoma $f(x, y)$ konveksni omotač poligona P_g transliranog za vektore (α_p, β_p) , (α_q, β_q) itd. Naravno, ukoliko P_g sadrži unutrašnje čvorove koji odgovaraju nenula monomima polinoma $g(x, y)$, oni se translacijama preslikavaju u odgovarajuće čvorove ostalih poligona. Drugim rečima, mreža čvorova je pokrivena podudarnim poligonima P_g , odnosno postignuto je pre pokrivanje mreže čvorova polinoma $f(x, y)$. Iz predhodnog zapisa polinoma $f(x, y)$ očigledno je da, ako postoje monomi koji se dobijaju množenjem faktor-polinoma na više nego jedan način, oni su podeljeni na polinome sabirke $g(x, y) c_p x^{\alpha_p} y^{\beta_p}$, $g(x, y) c_q x^{\alpha_q} y^{\beta_q}$, i eventualno još neke na način da se odgovarajući koeficijenti polinoma sabiraka odnose kao $c_p : c_q : \dots$. Dakle, sledi da je posmatrano pre pokrivanje odgovarajuće u odnosu na koeficijente polinoma $f(x, y)$.

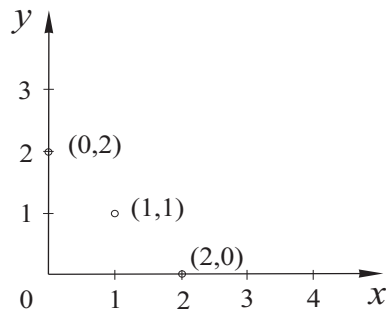
(\Leftarrow) Pretpostavimo da mreža čvorova polinoma $f(x, y)$, eventualno proširena nekim celobrojnim tačkama iz unutrašnjosti ili sa ruba Newton-ovog poligona polinoma $f(x, y)$, ima odgovarajuće prepoкрivanje u odnosu na koeficijente polinoma $f(x, y)$. Neka je ovo prepoкрivanje ostvareno pomoću l podudarnih poligona G_1, G_2, \dots, G_l . Grupišimo monome polinoma $f(x, y)$ na način određen poligonima G_1, G_2, \dots, G_l , $l \geq 2$. Ako postoje monomi polinoma koji odgovaraju čvorovima koji su zajednički za dva ili više poligona, podelimo ih na polinome sabirke na način da se postigne proporcionalnost odgovarajućih koeficijenata polinoma sabiraka, što je moguće s obzirom na to da je prepoкрivanje poligonima G_1, G_2, \dots, G_l odgovarajuće u odnosu na koeficijente polinoma $f(x, y)$. Kako su poligoni G_1, G_2, \dots, G_l podudarni i G_2, \dots, G_l se dobijaju translacijom poligona G_1 za vektore $(\alpha_2, \beta_2), \dots, (\alpha_l, \beta_l)$, polinomi sabirci koji odgovaraju poligonima G_2, \dots, G_l imaju trivijalnu faktorizaciju, pri čemu je jedan faktor $x^{\alpha_2} y^{\beta_2}, \dots, x^{\alpha_l} y^{\beta_l}$, a drugi faktor je polinom sabirak koji odgovara poligonu G_1 ili polinom koji ima koeficijente proporcionalne polinomu koji odgovara poligonu G_1 . Odavde sledi da polinom $f(x, y)$ ima netrivialnu faktorizaciju. \square

Napomena 7.13. Predhodna teorema važi i ako posmatramo polinom sa racionalnim koeficijentima.

Primer 7.14. Posmatrajmo polinom

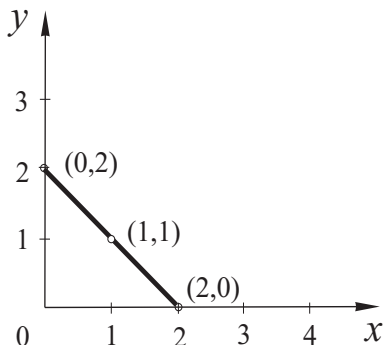
$$f(x, y) = x^2 + 2xy + y^2 \in \mathbb{Z}[x, y].$$

Mreža čvorova polinoma $f(x, y)$, prikazana na Slici 26, sadrži tačke $(0, 2)$, $(2, 0)$, i $(1, 1)$.



Slika 26

Jedino prepoкрivanje mreže čvorova je sa dve podudarne duži $\text{conv}((2, 0), (1, 1))$ i $\text{conv}((1, 1), (0, 2))$ koje imaju zajednički čvor $(1, 1)$, prikazano na Slici 27.



Slika 27

Ovo prekrivanje je odgovarajuće ako se monom koji odgovara zajedničkom čvoru $(1, 1)$, tj. monom $2xy$, može podeliti na polinome sabirke na način da se postigne proporcionalnost odgovarajućih koeficijenata. Zgrade se koriste da bi se označio način grupisanja monoma polinoma:

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

Duž $conv((1, 1), (0, 2))$ se dobija translacijom duži $conv((2, 0), (1, 1))$ za vektor $(-1, 1)$. Ako obeležimo tu translaciju sa τ , očigledno je da važi: $\tau((2, 0)) = (1, 1)$ i $\tau((1, 1)) = (0, 2)$. U prvoj zagradi redosled monoma je takav da je prvo naveden monom koji odgovara eksponent vektoru $(2, 0)$, a zatim monom koji odgovara eksponent vektoru $(1, 1)$. U drugoj zagradi redosled monoma je takav da je prvo naveden monom koji odgovara eksponent vektoru $\tau((2, 0))$, a zatim monom koji odgovara eksponent vektoru $\tau((1, 1))$. Ovo prekrivanje je odgovarajuće ako $1 : a = (2 - a) : 1$, tj. $a = 1$. Polinom $f(x, y)$ se može faktorisati na sledeći način:

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

Primer 7.15. Posmatrajmo polinom:

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

Nenula monomima polinoma $f(x, y)$ odgovaraju vektori eksponenata $(0, 2)$ i $(2, 0)$, pa je Newton-ov poligon polinoma $f(x, y)$ duž $conv((0, 2), (2, 0))$, kao u **Primeru 7.14.** S obzirom na to da nije moguće dostići prekrivanje na

neproširenoj mreži čvorova, posmatrajmo mrežu čvorova $(0, 2)$ i $(2, 0)$ proširenu tačkom $(1, 1)$ kojoj odgovara monom xy sa koeficijentom 0.

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

Grupišimo monome polinoma $f(x, y)$ u skladu sa prepokrivanjem ove mreže čvorova iz **Primer 7.14.**

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

Kako $1 : (-a) = a : (-1)$, tj. $a^2 = 1$, odgovarajuće prepokrivanje mreže čvorova se postiže za: $a = 1$ i $a = -1$. Za $a = 1$, dobijamo

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

Napomena 7.16. Za $a = -1$ se dobija ista faktorizacija polinoma $f(x, y)$:

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

Primer 7.17. Posmatrajmo polinom

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

Proširena mreža čvorova sastoji se iz tačaka $(0, 2)$, $(2, 0)$ i $(1, 1)$. Grupišimo monome $f(x, y)$ u skladu sa prepokrivanjem ove mreže čvorova iz **Primer 7.14.**

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

pri čemu $1 : (-a) = a : (-2)$, tj. $a^2 = 2$, odnosno $a = \sqrt{2}$ i $a = -\sqrt{2}$. Dakle, polinom $f(x, y)$ nema celobrojnu faktorizaciju, ali ima faktorizaciju nad poljem realnih brojeva:

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

Primer 7.18. Posmatrajmo polinom

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

Proširena mreža čvorova sastoji se iz tačaka $(0, 2)$, $(2, 0)$ i $(1, 1)$. Grupišimo monome $f(x, y)$ u skladu sa pre pokrivanjem ove mreže čvorova iz **Primera 7.14.**

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

pri čemu $1 : (-a) = a : (-4)$, tj. $a = 2$ i $a = -2$. Za $a = 2$, dobijamo

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

Primer 7.19. Posmatrajmo polinome $f(x, y), g(x, y), h(x, y) \in \mathbb{Z}[x, y]$:

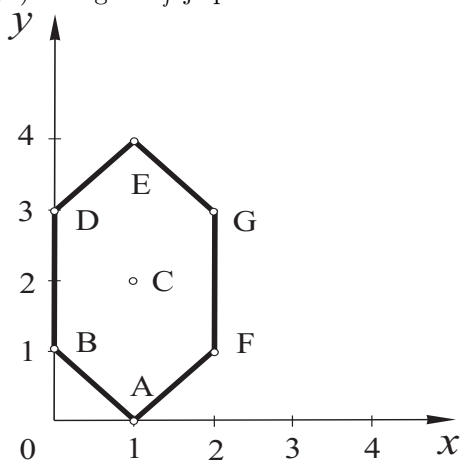
$$f(x, y) = xy^4 + x^2y^3 + 3xy^2 + y^3 + x^2y + x + y,$$

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

i

$$h(x, y) = xy^4 + x^2y^3 + 5xy^2 + y^3 + x^2y + x + y.$$

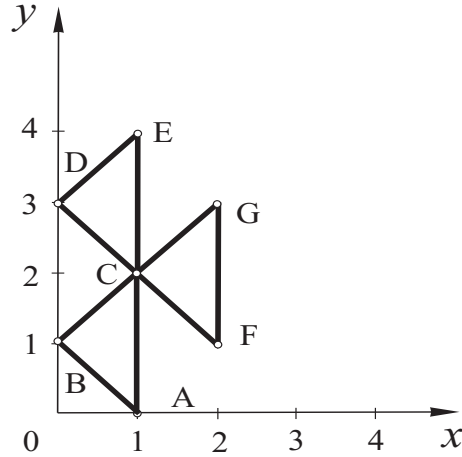
S obzirom na to da polinomi $f(x, y), g(x, y)$ i $h(x, y)$ imaju iste nenula monome, njihova mreža čvorova je ista, pa samim tim imaju isti Newton-ov poligon, tj. $P_f = P_g = P_h$. Neka $A = (1, 0)$, $B = (0, 1)$, $C = (1, 2)$, $D = (0, 3)$, $E = (1, 4)$, $F = (2, 1)$ i $G = (2, 3)$. Poligon P_f je prikazan na Slici 28.



Slika 28

S obzirom na to da jedino tačka C nije teme Newton-ovog poligona polinoma $f(x, y)$, pre pokrivanjem mreže čvorova jedino tačka C može biti zajednička za

više poligona. Posmatrajmo prekrivanje mreže čvorova sa tri podudarna trougla $\triangle ABC$, $\triangle CDE$ i $\triangle FCG$, prikazano na Slici 29.



Slika 29

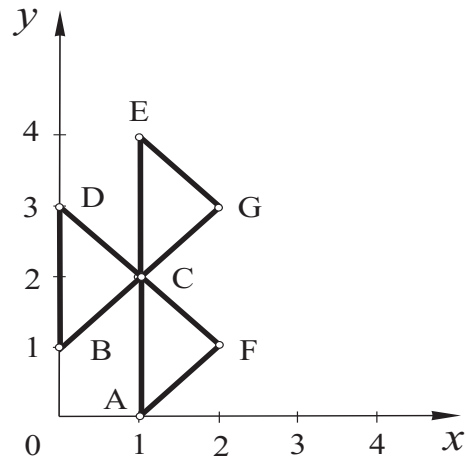
Polinom $f(x, y)$ predstavimo kao zbir tri polinoma sabirka indukovana prekrivanjem prikazanim na Slici 29, pri čemu je monom $3xy^2$ koji odgovara čvoru $C = (1, 2)$, koji je zajednički za sva tri trougla, predstavljen na sledeći način $3xy^2 = xy^2 + xy^2 + xy^2$. Dalje je:

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

Očigledno je da su koeficijenti polinoma sabiraka proporcionalni, pa je prekrivanje prikazano na Slici 29 odgovarajuće u odnosu na koeficijente polinoma $f(x, y)$. Kako se trouglovi $\triangle CDE$ i $\triangle FCG$ dobijaju translacijom trougla $\triangle ABC$ za vektore $(0, 2)$ i $(1, 1)$, drugi i treći polinom sabirak imaju trivijalne faktore y^2 i xy .

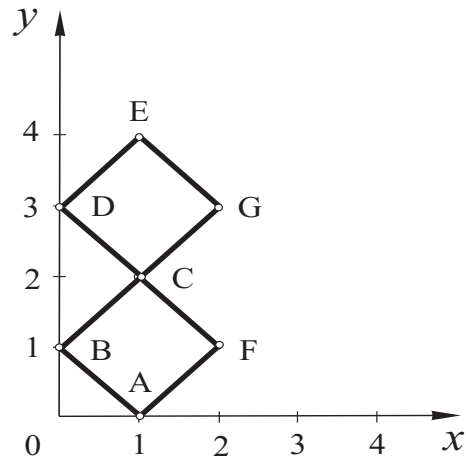
$$f(x, y) = (x + y + xy^2) + y^2(x + y + xy^2) + xy(x + y + xy^2) = (1 + y^2 + xy)(x + y + xy^2).$$

Lako je pokazati da faktor polinomi $1 + y^2 + xy$ i $x + y + xy^2$ nemaju netrivialnu celobrojnu faktorizaciju. Drugo odgovarajuće prekrivanje u odnosu na koeficijente polinoma $f(x, y)$ prikazano na Slici 30 rezultira istom faktorizacijom polinoma $f(x, y)$.



Slika 30

Međutim, prekrivanja mreže čvorova prikazana na Slici 29 i Slici 30 nisu odgovarajuća u odnosu na koeficijente polinoma $g(x, y)$. Posmatrajmo prepoкрivanje prikazano na Slici 31.



Slika 31

Polinom $g(x, y)$ predstavimo kao zbir dva polinoma sabirka indukovana prepoкрivanjem prikazanim na Slici 31, pri čemu je monom $2xy^2$ koji odgovara čvoru $C = (1, 2)$, koji je zajednički za oba trougla, predstavljen na sledeći način $2xy^2 = xy^2 + xy^2$. Dalje je:

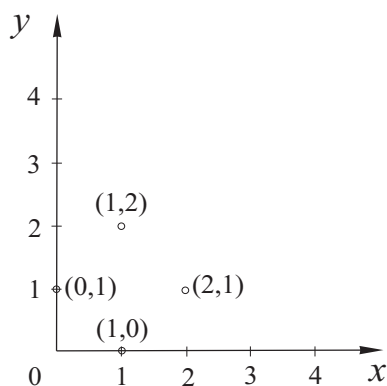
$$g(x, y) = xy^4 + x^2y^3 + 2xy^2 + y^3 + x^2y + x + y =$$

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

Očigledno je da su koeficijenti polinoma sabiraka proporcionalni, pa je prepo-
krivanje prikazano na Slici 31 odgovarajuće u odnosu na koeficijente $g(x, y)$.
Dobijamo:

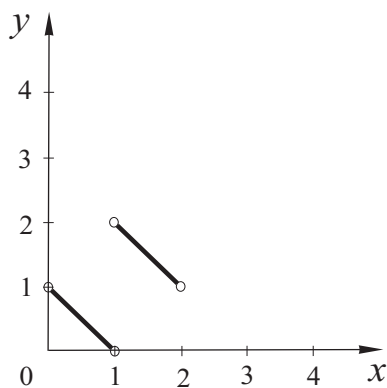
$$g(x, y) = (x + y + xy^2 + x^2y) + y^2(x + y + xy^2 + x^2y) = (1 + y^2)(x + y + xy^2 + x^2y).$$

Očigledno je da faktor - polinom $1 + y^2$ nema netrivialnu celobrojnu faktoriza-
ciju. Dalje, faktorišimo faktor - polinom $x + y + xy^2 + x^2y$ sa mrežom čvorova
prikazanom na Slici 32.



Slika 32

Mreža čvorova polinoma $x + y + xy^2 + x^2y$ može se prepokriti sa dve podudarne
duži, što je prikazano na Slici 33.



Slika 33

Ovo prepostrivanje indukuje grupisanje monoma na sledeći naćin:

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

S obzirom na to da važi: $1 : 1 = 1 : 1$, odgovarajući koeficijenti polinoma sabiraka su proporcionalni, pa je prepostrivanje mreže ćvorova polinoma $x + y + xy^2 + x^2y$ prikazano na Slici 33 odgovarajuće u odnosu na koeficijente polinoma $x + y + xy^2 + x^2y$. Dalje dobijamo:

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

Dakle, faktorizacija polinoma $g(x, y)$ na nesvodljive faktore sa celobrojnim koeficijentima je:

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

Konaćno, posmatrajmo polinom $h(x, y)$ i prepostrivanje mreže ćvorova prikazano na Slici 29. Grupišimo monome polinoma $h(x, y)$ na naćin indukovan ovim prepostrivanjem:

$$h(x, y) = (x + y + axy^2) + (bxy^2 + y^3 + xy^4) + (x^2y + cxy^2 + x^2y^3), \quad a + b + c = 5.$$

Ovo prepostrivanje nije odgovarajuće u odnosu na koeficijente polinoma $h(x, y)$ jer:

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

odnosno:

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

tj.,

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

Potpuno analogno može se pokazati da sva ostala prepostrivanja koja se mogu postići na mreži ćvorova polinoma $h(x, y)$ nisu odgovarajuća u odnosu na koeficijente ovog polinoma, tako da polinom $h(x, y)$ nema netrivialnu celobrojnu faktorizaciju.

Primer 7.20. Posmatrajmo polinom:

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

Kako polinom $f(x, y)$ ima iste nenula monome kao polinomi iz predhodnog primera, njegova mreža ćvorova je ista kao u predhodnom primeru. Grupišimo

monome polinoma $f(x, y)$ u skladu sa prepokrivanjem mreže čvorova prikazanim na Slici 29, pri čemu je monom $10xy^2$ koji odgovara čvoru $C = (1, 2)$, koji je zajednički za sva tri trougla, predstavljen na sledeći način $10xy^2 = 3xy^2 + 3xy^2 + 4xy^2$. Dobijamo:

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

Kako važi: $1 : 2 : 3 = 3 : 6 : 9 = 2 : 4 : 6$, odgovarajući koeficijenti polinoma sabiraka su proporcionalni, pa je ovo prepokrivanje odgovarajuće u odnosu na koeficijente polinoma $f(x, y)$. Dalje je:

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

odnosno,

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

Lako je pokazati da faktor - polinomi polinoma $f(x, y)$ nemaju netrivialnu celobrojnu faktorizaciju.

Primer 7.21. Posmatrajmo polinome $f(x, y), g(x, y), h(x, y) \in \mathbb{Z}[x, y]$:

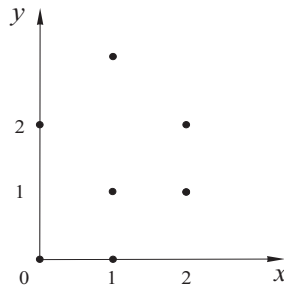
$$f(x, y) = 3xy^3 + 2x^2y^2 + 2x^2y + 3xy + 3y^2 + 2x + 1,$$

$$g(x, y) = 3xy^3 + 2x^2y^2 + 2x^2y + 7xy + 3y^2 + 2x + 1,$$

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

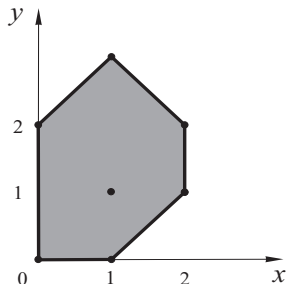
Posmatrajmo neka prepokrivanja mreže čvorova datih polinoma i za odgovarajuća prepokrivanja nađimo faktorizacije posmatranih polinoma.

S obzirom na to da polinomi $f(x, y)$ i $g(x, y)$ imaju iste nenula monome, koji odgovaraju tačkama $(1, 3), (2, 2), (2, 1), (1, 1), (0, 2), (1, 0)$ i $(0, 0)$, ovi polinomi imaju istu mrežu čvorova koja je prikazana na Slici 34.



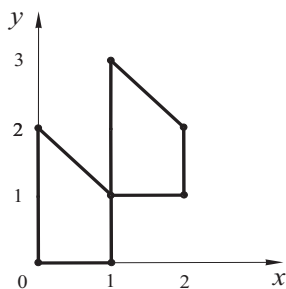
Slika 34

Konveksni omotač mreže čvorova polinoma $f(x, y)$ i $g(x, y)$ je prikazan na Slici 35.



Slika 35

Jedno prepokrivanje mreže čvorova polinoma $f(x, y)$ i $g(x, y)$ je prikazano na Slici 36.



Slika 36

Grupišimo monome polinoma $f(x, y)$ na način indukovani prepokrivanjem prikazanim na Slici 36. Koeficijent monoma koji odgovara čvoru $(1, 1)$, koji je zajednički za dva poligona, podeljen je na poligone sabirke da bi se postigla proporcionalnost odgovarajućih koeficijenata:

$$f(x, y) = (3xy^3 + 2x^2y^2 + 2x^2y + cxy) + (3y^2 + (3 - c)xy + 2x + 1),$$

$$3 : 2 : 2 : c = 3 : (3 - c) : 2 : 1, \text{ tj. } c = 1.$$

Dakle, posmatrano prepokrivanje je odgovarajuće u odnosu na koeficijente polinoma $f(x, y)$. Dalje sledi:

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

tj.

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

odnosno:

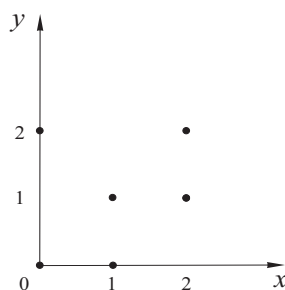
$$f(x, y) = (xy + 1)(3y^2 + 2xy + 2x + 1).$$

Međutim, ovo prekrivanje nije odgovarajuće u odnosu na koeficijente polinoma $g(x, y)$ jer ne postoji ceo broj c za koji važi:

$$3 : 2 : 2 : c = 3 : (7 - c) : 2 : 1.$$

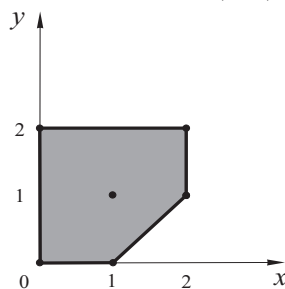
Nenula monomi polinoma $h(x, y)$ odgovaraju tačkama $(2, 2)$, $(2, 1)$, $(1, 1)$, $(0, 2)$, $(1, 0)$ i $(0, 0)$.

Mreža čvorova polinoma $h(x, y)$ je prikazana na Slici 37.



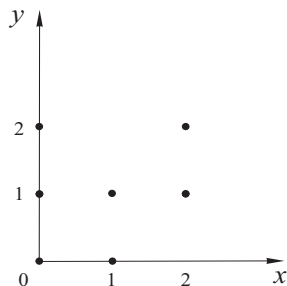
Slika 37

Konveksni omotač mreže čvorova polinoma $h(x, y)$ je prikazan na Slici 38.



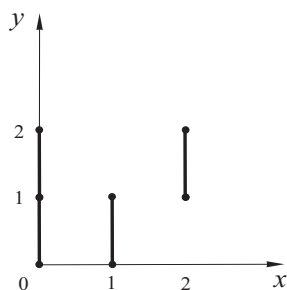
Slika 38

Prekrivanje se ne može postići na neproširenoj mreži čvorova, tako da treba posmatrati mrežu čvorova proširenu celobrojnim tačkama iz unutrašnjosti ili sa ruba Newton-ovog poligona polinoma $h(x, y)$. Posmatrajmo, najpre, mrežu čvorova polinoma $h(x, y)$ proširenu tačkom $(0, 1)$, koja je prikazana na Slici 39.



Slika 39

Prepokrivanje mreže čvorova polinoma $h(x, y)$ proširene tačkom $(0, 1)$ je prikazano na Slici 40.

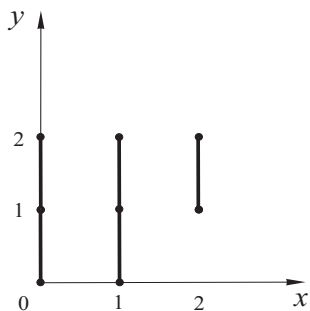


Slika 40

S obzirom na to ne postoji ceo broj c takav da važi proporcija:

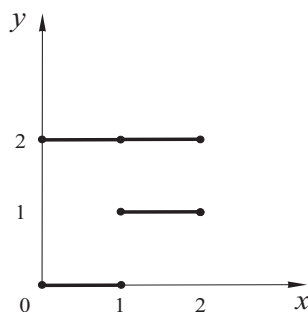
$$3 : c = (0 - c) : 1 = 3 : 2 = 2 : 2,$$

ovo prepokrivanje nije odgovarajuće u odnosu na koeficijente polinoma $h(x, y)$. Prepokrivanje mreže čvorova proširene tačkama $(0, 1)$ i $(1, 2)$, prikazano na Slici 41, takođe nije odgovarajuće u odnosu na koeficijente polinoma $h(x, y)$.



Slika 41

Isto važi i za prepoкрivanje mreže čvorova proširene tačkom $(1, 2)$, koje je prikazano na Slici 42.



Slika 42

Lako se pokazuje da nijedno drugo prepoкрivanje mreže čvorova nije odgovarajuće u odnosu na koeficijente polinoma $h(x, y)$.

Sledi da polinom $h(x, y)$ nema netrivialnu celobrojnu faktorizaciju.

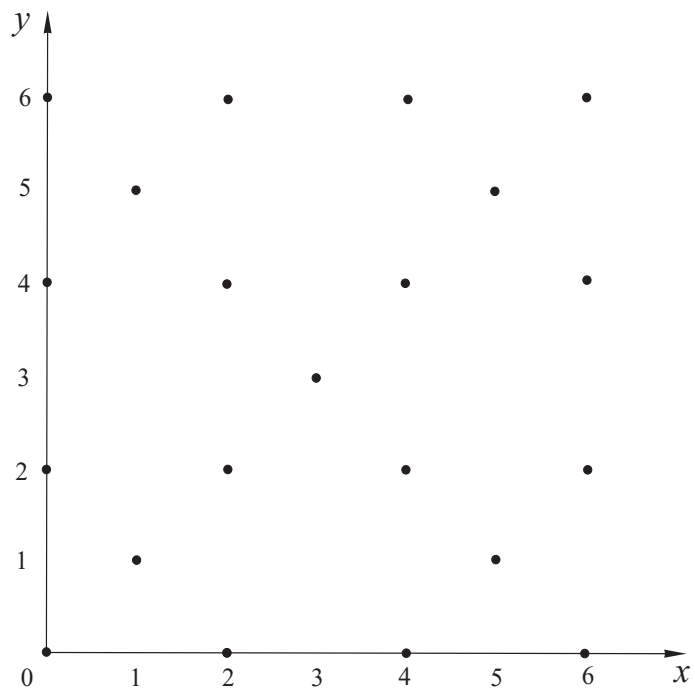
Napomena 7.22. U predhodnim primerima prepoкрivanja mreže čvorova su bila ostvarena podudarnim poligonima bez unutrašnjih čvorova. U narednom primeru jedino prepoкрivanje koje je odgovarajuće u odnosu na koeficijente polinoma je prepoкрivanje podudarnim poligonima sa unutrašnjim čvorom.

Primer 7.23. Posmatrajmo polinom $f(x, y) \in \mathbb{Z}[x, y]$:

$$f(x, y) = x^6y^6 + x^4y^6 + 2x^4y^4 + x^6y^4 + x^5y^5 + x^2y^6 + y^6 + y^4 + 2x^2y^4 + xy^5 + 2x^2y^2 + 2x^4y^2 + x^3y^3 + y^2 + 1 + x^2 + xy + x^6y^2 + x^4 + x^6 + x^5y.$$

Nenula monomi polinoma $f(x, y)$ odgovaraju tačkama $(6, 6)$, $(4, 6)$, $(4, 4)$, $(6, 4)$, $(5, 5)$, $(2, 6)$, $(0, 6)$, $(0, 4)$, $(2, 4)$, $(1, 5)$, $(2, 2)$, $(4, 2)$, $(3, 3)$, $(0, 2)$, $(0, 0)$, $(2, 0)$, $(1, 1)$, $(6, 2)$, $(4, 0)$, $(6, 0)$ i $(5, 1)$.

Mreža čvorova polinoma $f(x, y)$ je prikazana na Slici 43.



Slika 43

Posmatrajmo prekrivanje mreže čvorova kvadratom sa unutrašnjim čvorom:

$$\text{conv}\{(0, 0), (2, 0), (2, 2), (0, 2), (1, 1)\}$$

i njegovim translatorskim slikama:

$$\text{conv}\{(4, 0), (6, 0), (6, 2), (4, 2), (5, 1)\},$$

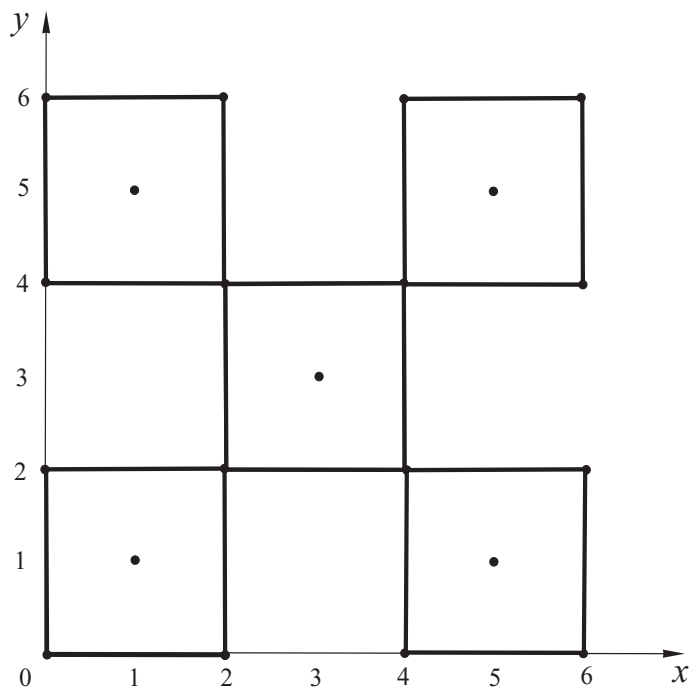
$$\text{conv}\{(2, 2), (4, 2), (4, 4), (2, 4), (3, 3)\},$$

$$\text{conv}\{(0, 4), (2, 4), (2, 6), (0, 6), (1, 5)\}$$

i

$$\text{conv}\{(4, 4), (6, 4), (6, 6), (4, 6), (5, 5)\},$$

prikazano na Slici 44.



Slika 44

Grupišimo monome polinoma $f(x, y)$ na način indukovano prekrivanjem prikazanim na Slici 44.

$$\begin{aligned}
 f(x, y) = & (1 + x^2 + cx^2y^2 + y^2 + xy) + (x^4 + x^6 + x^6y^2 + dx^4y^2 + x^5y) + \\
 & + ((2-c)x^2y^2 + (2-d)x^4y^2 + ex^4y^4 + fx^2y^4 + x^3y^3) + \\
 & (y^4 + (2-f)x^2y^4 + x^2y^6 + y^6 + xy^5) + ((2-e)x^4y^4 + x^6y^4 + x^6y^6 + x^4y^6 + x^5y^5).
 \end{aligned}$$

S obzirom na to da proporcija:

$$\begin{aligned}
 1 : 1 : c : 1 : 1 &= 1 : 1 : 1 : d : 1 = (2-c) : (2-d) : e : f : 1 = \\
 &= 1 : (2-f) : 1 : 1 : 1 = (2-e) : 1 : 1 : 1 : 1,
 \end{aligned}$$

važi za $c = d = e = f = 1$, ovo prekrivanje je odgovarajuće u odnosu na koeficijente polinoma $f(x, y)$.

Dalje sledi:

$$f(x, y) = (1 + x^2 + x^2y^2 + y^2 + xy) + (x^4 + x^6 + x^6y^2 + x^4y^2 + x^5y) +$$

$$+(x^2y^2 + x^4y^2 + x^4y^4 + x^2y^4 + x^3y^3) + (y^4 + x^2y^4 + x^2y^6 + y^6 + xy^5) + \\ +(x^4y^4 + x^6y^4 + x^6y^6 + x^4y^6 + x^5y^5).$$

Odnosno:

$$f(x, y) = (1 + x^2 + x^2y^2 + y^2 + xy) + x^4(1 + x^2 + x^2y^2 + y^2 + xy) + \\ x^2y^2(1 + x^2 + x^2y^2 + y^2 + xy) + y^4(1 + x^2 + x^2y^2 + y^2 + xy) \\ + x^4y^4(1 + x^2 + x^2y^2 + y^2 + xy),$$

tj.

$$f(x, y) = (1 + x^4 + x^2y^2 + y^4 + x^4y^4)(1 + x^2 + x^2y^2 + y^2 + xy).$$

Napomena 7.24. U predhodnom poglavlju determinisane su klase apsolutno nesvodljivih polinoma dve promenljive nad proizvoljnim poljem pronalaženjem integralno nerastavljivih poligona u smislu sume Minkowskog. U ovom poglavlju je diskutovan obratan problem, pod kojim uslovima polinom dve promenljive, kome odgovara integralno rastavljiv poligon u smislu sume Minkowskog, ima netrivialnu faktorizaciju. Na osnovu **Teoreme 7.12.**, za postojanje netrivialne faktorizacije polinoma dve promenljive potrebna je proporcionalnost odgovarajućih koeficijenata, pa se zbog toga posmatraju polinomi dve promenljive sa celobrojnim koeficijentima, pri čemu se rezultati mogu primeniti i na polinome sa racionalnim koeficijentima.

8 Algoritam za faktorizaciju polinoma dve promenljive sa celobrojnim koeficijentima

S obzirom na to da **Teorema 7.12.** daje potreban i dovoljan uslov za postojanje netrivialne faktorizacije polinoma dve promenljive sa celobrojnim koeficijentima u faktor - polinome sa celobrojnim koeficijentima, na taj način se stvara teorijska osnova za konstrukciju efektivnog algoritma za faktorizaciju, koji je prezentovan u [47].

U ovom delu predstavimo algoritam koji pronalazi odgovarajuće prepokrivanje mreže čvorova, eventualno proširene nekim celobrojnim tačkama iz unutrašnjosti ili sa ruba Newton-ovog poligona datog polinoma dve promenljive f . Algoritam iterativno pokušava da postigne prepokrivanje skupa A tačkama skupa B koji sadrži j tačaka, $j \geq 2$, za rastuće j i na taj način određuje skupove G_i .

```

1. read( $A$ );
/* $A = \{A_i[x[i], y[i], a[i]] : i = 1, \dots, n\}$ , pri čemu su  $x[i]$  i  $y[i]$  koordinate tačaka
iz mreže čvorova i  $a[i]$  je koeficijent odgovarajućeg monoma.*/
2. sort( $A$ );
/*Tačke  $A_i \in A$  su sortirane u leksikografskom poretku, najpre u odnosu na
 $x[i]$ , a zatim u odnosu na  $y[i]$ .*/
3. convexhull( $A, ExtA$ );
/* $ExtA = \{ExtA_j[xx[j], yy[j], aa[j]]\}$ , su tačke proširene mreže čvorova poli-
noma  $f$ . Za svako  $A_j \in AA = ExtA \setminus A$ ,  $x[j]$  i  $y[j]$  su koordinate te tačke i
 $a[j] = 0$ .*/
4. sort( $ExtA$ );
5. sort( $AA$ );
6. for( $cover := 0, m := 2; cover = 0, m < n; m := m + 1$ );
6.1 form( $B$ );
/* $B = \{B_j[bx[j], by[j], ba[j]] : j = 1, \dots, m\}$ ,  $B_1 \equiv A_1$ ,  $B_j$ ,  $2 \leq j \leq m$  su
tačke mreže čvorova  $A$  u leksikografskom poretku;  $ba[j] := aa[j], \dots, 2, 1$  ako  $B_j$ 
nije teme Newton-ovog poligona polinoma  $f$ , a  $ba[j] := aa[j]$  ako  $B_j$  jeste teme
Newton-ovog poligona polinoma  $f$ */
6.2. covering( $A, B$ );
/* $C = \{B_1\}$  (tačke iz  $C$  definišu  $G_i$ );  $D = A \setminus B$ ;
```

repeat

Naći u leksikografskom poretku najmanju tačku X iz D i translirati B za vektor $\overrightarrow{B_j X}$, $j = 1, 2, \dots, m$. Ako τB_j je jednako A i odgovarajući koeficijenti a i ba su proporcionalni, onda τB_1 dodati C i koeficijenti tačaka A_{jj} iz τB su promenjeni: $a[jj] := a[jj] - ba[j]$, ako $a[jj] = 0$, onda $D = D \setminus \{A_{jj}\}$

Ako za neko B_j , X nije prepokriveno, tada promeniti B_j . Ako X nije prepokriveno ni za jedno j , tada otići na korak 6.1 i promeniti koeficijente $ba[j]$.

sve dok $D = \emptyset$. */

7. Ako $D = \emptyset$, onda $cover := 1$ i otići na korak 8, inače $cover := 0$.

8. write($cover, B, C$).

/*ako $cover = 0$ izlazna poruka je da ne postoji prepočrivanje mreže čvorova, ako $cover = 1$ izlaz je skup tačaka B kojim prepočrivamo inicijalni skup i koji indukuje jedan faktor polinoma, a skup tačaka C definiše drugi faktor itd*/

Sledeća teorema dokazana je u [47].

Teorema 8.1. Neka $f(x, y) \in \mathbb{Z}[x, y]$ i neka je $P = \{A_1, A_2, \dots, A_n\}$ mreža čvorova polinoma $f(x, y)$ eventualno proširena nekim celobrojnim tačkama iz unutrašnjosti ili sa ruba Newton-ovog poligona polinoma $f(x, y)$. Neka je:

$$G_1 = conv(A_{i_{1,1}}, \dots, A_{i_{1,k}}), \dots, G_l = conv(A_{i_{l,1}}, \dots, A_{i_{l,k}}), l \geq 2,$$

$\{i_{1,1}, \dots, i_{1,k}, \dots, i_{l,1}, \dots, i_{l,k}\} = \{1, \dots, n\}$, odgovarajuće prepočrivanje mreže čvorova P u odnosu na koeficijente polinoma $f(x, y)$ sa l podudarnih k -gona. Dalje, neka je $G_2 = \tau_2(G_1), \dots, G_l = \tau_l(G_1)$. Tada je:

$$conv(A_{i_{1,1}}, \tau_2(A_{i_{1,1}}), \dots, \tau_l(A_{i_{1,1}})), \dots, conv(A_{i_{1,k}}, \tau_2(A_{i_{1,k}}), \dots, \tau_l(A_{i_{1,k}}))$$

takođe odgovarajuće prepočrivanje mreže čvorova P u odnosu na koeficijente polinoma $f(x, y)$ sa k podudarnih l -gona.

Dokaz:

Neka je $G_1 = conv(A_{i_{1,1}}, \dots, A_{i_{1,k}}), \dots, G_l = conv(A_{i_{l,1}}, \dots, A_{i_{l,k}}), l \geq 2$, odgovarajuće prepočrivanje mreže čvorova P u odnosu na koeficijente polinoma $f(x, y)$ sa l podudarnih k -gona. Uvedimo oznake: $c_{i_j,k} = coef(A_{i_j,k})$. Tada važi:

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

Jasno, ako postoji čvor zajednički za dva ili više poligona, koeficijent njemu odgovarajućeg monoma je podeljen na način da je proporcionalnost koeficijenata

zadovoljena. Očigledno je da je:

$$\text{conv}(A_{i_1,1}, \tau_2(A_{i_1,1}), \dots, \tau_l(A_{i_1,1})), \dots, \text{conv}(A_{i_1,k}, \tau_2(A_{i_1,k}), \dots, \tau_l(A_{i_1,k}))$$

prepokrivanje mreže čvorova P .

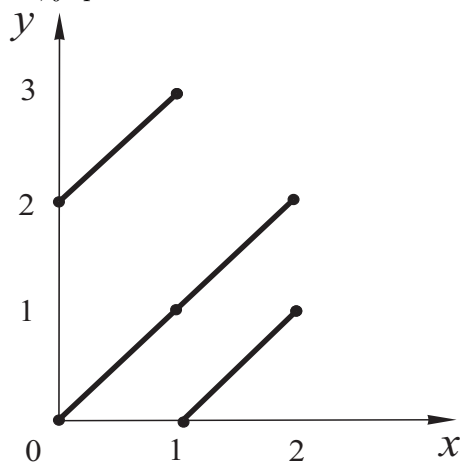
S obzirom na to da proporcija:

$$c_{i_1,1} : c_{i_2,1} : \dots : c_{i_l,1} = \dots = c_{i_1,k} : c_{i_2,k} : \dots : c_{i_l,k},$$

takođe važi, ovo prepokrivanje mreže čvorova P je odgovarajuće u odnosu na koeficijente polinoma $f(x, y)$. \square

Napomena 8.2. Iz predhodne teoreme sledi da svako odgovarajuće prepokrivanje mreže čvorova P u odnosu na koeficijente polinoma $f(x, y)$ sa l podudarnih k -gona jedinstveno određuje drugo odgovarajuće prepokrivanje mreže čvorova P sa k podudarnih l -gona, koje se naziva **dualno odgovarajuće prepokrivanje mreže čvorova P** .

Primer 8.3. Dualno odgovarajuće prepokrivanje mreže čvorova prepokrivanju prikazanom na Slici 36, je prikazano na Slici 45.



Slika 45

Napomena 8.4. Dualno prepokrivanje nekom prepokrivanju indukuje istu faktorizaciju posmatranog polinoma.

Napomena 8.5. Prezentovani algoritam, koji počinje sa podudarnim dužima, podudarnim trouglovima itd., pod uslovom da odgovarajuće prepokrivanje mreže

čvorova polinoma $f(x, y)$ sa l podudarnih k -gona postoji, pri čemu je $k \leq l$, najpre će dostići to prekrivanje i izvršiti faktORIZACIJU polinoma.

9 Primena faktorizacije polinoma dve promenljive sa celobrojnim koeficijentima u dekodiranju nekih klasa Reed-Solomon kodova

Teorija kodiranja je matematička disciplina koja se bavi analizom podataka koji se prenose kroz kanale sa šumom i ispravljanjem eventualnih grešaka koje nastaju pri prenosu. Osnove teorije kodiranja mogu se naći u [2], [3],[55],[66], [64] i [65].

Kodovi za korekciju grešaka (error-correcting codes) omogućavaju pouzdan prenos podataka preko komunikacionog kanala sa šumom (noisy communication channel). Ideja je da se poruka prenese u duži, redundantni niz, koji se naziva kodna reč (codeword), a zatim da se prenese kodna reč komunikacionim kanalom sa šumom. Redundansa se unosi da bi omogućila da se nakon prijema dekodira kodna reč, čak i u slučaju da je kodna reč u izvesnoj meri oštećena. Osnovni pojmovi vezani za kodove za korekciju grešaka dati su u [23].

Reed-Solomon kodovi su primer kodova za korekciju grešaka, kod kojih se redundantna informacija dodaje podacima tako da oni mogu pouzdano dekodirati i pored grešaka pri skladištenju ili vraćanju podataka. Reed-Solomon kodovi su korišćeni u nekoliko NASA i ESA misija planetarnih istraživanja. Reed-Solomon kodovi, koje su u [49] definisali I. S. Reed i G. Solomon 1960. godine, su predmet istraživanja brojnih naučnih radova, između ostalih [4], [21], [22], [28], [37] i [62].

Definicija 9.1. Neka je n prost broj i neka je $GF(n)$ konačno polje karakteristike n . Neka je $(m_0, m_1, m_2, \dots, m_{k-1})$, $m_0, m_1, m_2, \dots, m_{k-1} \in GF(n)$, k -torka elemenata iz $GF(n)$. Neka je $p(x) = m_0 + m_1x + m_2x^2 + \dots + m_{k-1}x^{k-1}$. Neka je α primitivni element polja $GF(n)$. **Reed-Solomon kodna reč** c je:

$$c = (c_0, c_1, c_2, \dots, c_{n-1}) = (p(0), p(\alpha), p(\alpha^2), \dots, p(\alpha^{n-1})).$$

Uzimanjem svih k -torki $(m_0, m_1, m_2, \dots, m_{k-1})$ se dobija kompletan skup kodnih reči iz $GF(n)$.

Napomena 9.2. S obzirom na to da ima n^k različitih k -torki elemenata iz

$GF(n)$, Reed-Solomon kod ima n^k kodnih reči.

Definicija 9.3. Kod je *linearan* ako je suma dve kodne reči takođe kodna reč.

Napomena 9.4. Kako je suma dva polinoma stepena $(k-1)$ polinom stepena najviše $(k-1)$, Reed-Solomon kodovi su linearni.

Napomena 9.5. Lako se dokazuje da skup svih Reed-Solomon kodnih reči čini vektorski prostor dimenzije k nad poljem $GF(n)$. Reed-Solomon kodovi, kao i svi drugi linearni kodovi, označavaju kao (n, k) kodovi.

U [20] Venkatesan Guruswami definiše miks dve kodne reči.

Definicija 9.6. Neka je n prost broj i neka je $GF(n)$ konačno polje karakteristike n . Neka su $(m_0, m_1, m_2, \dots, m_{k-1})$, $m_0, m_1, m_2, \dots, m_{k-1} \in GF(n)$ i $(d_0, d_1, d_2, \dots, d_{k-1})$, $d_0, d_1, d_2, \dots, d_{k-1} \in GF(n)$ dve k -torke elemenata iz $GF(n)$. Dalje, neka su polinomi $p_1(x)$ i $p_2(x)$ nad $GF(n)$ dati na sledeći način: $p_1(x) = m_0 + m_1x + m_2x^2 + \dots + m_{k-1}x^{k-1}$ i $p_2(x) = d_0 + d_1x + d_2x^2 + \dots + d_{k-1}x^{k-1}$. Neka su c_1 i c_2 Reed-Solomon kodne reči koje odgovaraju polinomima p_1 i p_2 . **Miks kodnih reči** c_1 i c_2 odgovara polinomu dve promenljive: $q(x, y) = y^2 - s(x)y + p(x)$, pri čemu je $s(x) = p_1(x) + p_2(x)$ i $p(x) = p_1(x) \cdot p_2(x)$.

Napomena 9.7. Očigledno je da polinom $q(x, y)$ ima jedinstvenu faktorizaciju u formi $q(x, y) = (y - p_1(x))(y - p_2(x))$. Stoga, polinomi $p_1(x)$ i $p_2(x)$ mogu se odrediti direktno faktorizacijom polinoma $q(x, y)$, što je prikazano u narednom primeru.

U ovom delu rada će biti prikazan algoritam prezentovan u [47] koji, za datu primljenu kodnu reč, koja predstavlja miks dve kodne reči, rekonstruiše polazne kodne reči direktno faktorizacijom odgovarajućeg polinoma dve promenljive.

Primer 9.8. Neka su $(1, 0, 3, 1, 2)$ i $(2, 2, 0, 3, 1)$ dve 5-torke elemenata iz polja \mathbb{Z}_5 i neka su $p_1(x) = 1 + 3x^2 + x^3 + 2x^4$ i $p_2(x) = 2 + 2x + 3x^3 + x^4$ odgovarajući polinomi. Neka su c_1 i c_2 kodne reči koje odgovaraju polinomima $p_1(x)$ and $p_2(x)$. Miks kodnih reči c_1 i c_2 odgovara polinomu dve promenljive:

$$q(x, y) = y^2 - ((1 + 3x^2 + x^3 + 2x^4) + (2 + 2x + 3x^3 + x^4))y \\ + (1 + 3x^2 + x^3 + 2x^4)(2 + 2x + 3x^3 + x^4),$$

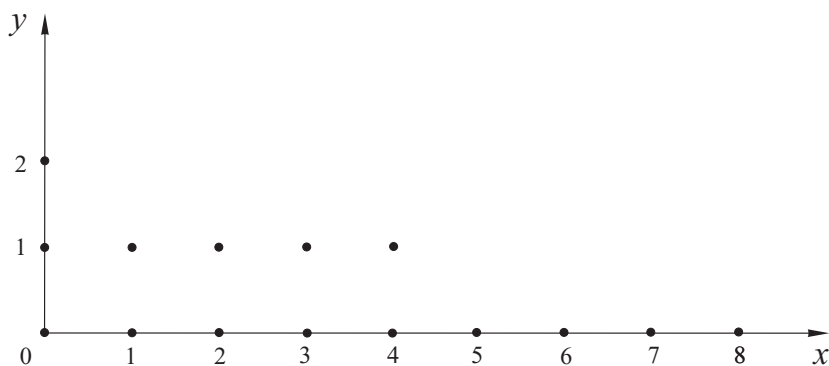
tj.

$$q(x, y) = y^2 - 3y - 2xy - 3x^2y - 4x^3y - 3x^4y \\ + 2 + 2x + 6x^2 + 11x^3 + 7x^4 + 13x^5 + 6x^6 + 7x^7 + 2x^8.$$

Kako su koeficijenti polinoma $q(x, y)$ iz polja \mathbb{Z}_5 , $q(x, y)$ ima formu:

$$q(x, y) = y^2 - 3y - 2xy - 3x^2y - 4x^3y - 3x^4y + 2 + 2x + x^2 + \\ + x^3 + 2x^4 + 3x^5 + x^6 + 2x^7 + 2x^8.$$

Nenula monomi polinoma $q(x, y)$ odgovaraju tačkama $(0, 2)$, $(0, 1)$, $(1, 1)$, $(2, 1)$, $(3, 1)$, $(4, 1)$, $(0, 0)$, $(1, 0)$, $(2, 0)$, $(3, 0)$, $(4, 0)$, $(5, 0)$, $(6, 0)$, $(7, 0)$ i $(8, 0)$. Mreža čvorova polinoma $q(x, y)$ je prikazana na Slici 46.



Slika 46

Prepokrivanje mreže čvorova sa:

$$\text{conv}\{(0, 1), (0, 0), (1, 0), (2, 0), (3, 0), (4, 0)\},$$

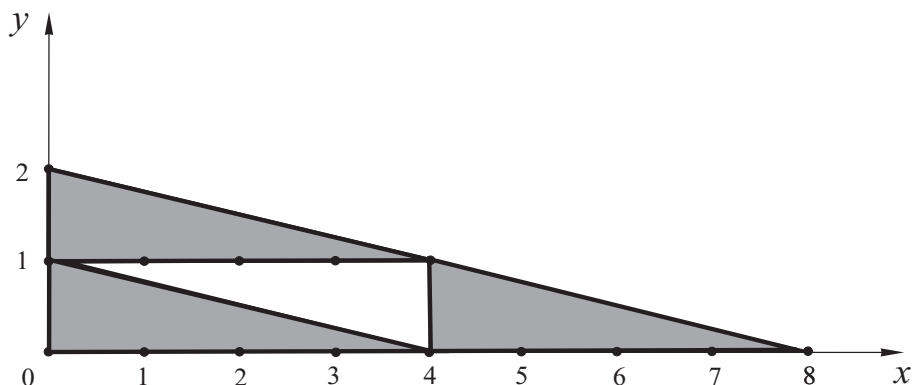
i njegovim translatorskim slikama:

$$\text{conv}\{(0, 2), (0, 1), (1, 1), (2, 1), (3, 1), (4, 1)\},$$

i

$$\text{conv}\{(4, 1), (4, 0), (5, 0), (6, 0), (7, 0), (8, 0)\}$$

je prikazano na Slici 47.



Slika 47

Čvorovi $(1, 0)$, $(2, 0)$, $(3, 0)$, $(1, 1)$, $(2, 1)$, $(3, 1)$, $(5, 0)$, $(6, 0)$ i $(7, 0)$ pripadaju samo jednom od poligona, pri čemu se čvorovi $(1, 0)$, $(2, 0)$, $(3, 0)$ preslikavaju translacijama redom na $(1, 1)$, $(2, 1)$, $(3, 1)$ i $(5, 0)$, $(6, 0)$, $(7, 0)$. S obzirom na to da proporcija:

$$2 : 1 : 1 = (-2) : (-3) : (-4) = 3 : 1 : 2,$$

ne važi, ovo pre pokrivanje mreže čvorova nije odgovarajuće u odnosu na koeficijente polinoma $q(x, y)$.

Posmatrajmo pre pokrivanje mreže čvorova sa:

$$\text{conv}\{(0, 1), (0, 0), (1, 0), (3, 0), (4, 0)\}$$

(prikazan na Slici 48) i njegovim translatorskim slikama:

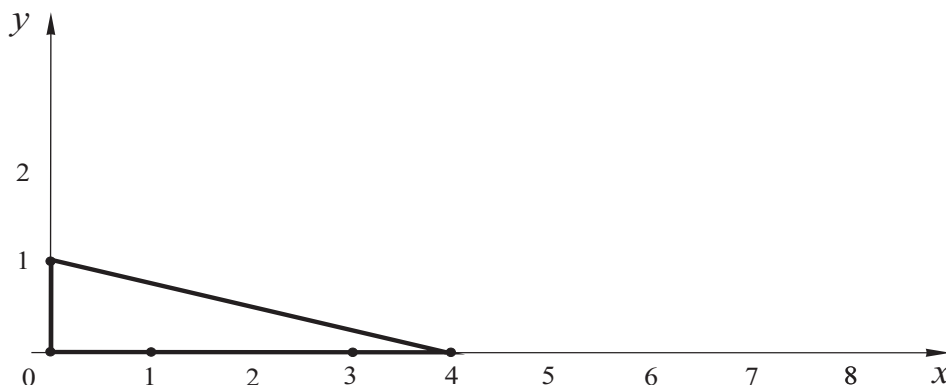
$$\text{conv}\{(0, 2), (0, 1), (1, 1), (3, 1), (4, 1)\},$$

$$\text{conv}\{(2, 1), (2, 0), (3, 0), (5, 0), (6, 0)\},$$

$$\text{conv}\{(3, 1), (3, 0), (4, 0), (6, 0), (7, 0)\}$$

i

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



Slika 48

Grupišimo monome polinoma $q(x, y)$ na način indukovano ovim prekrivanjem:

$$\begin{aligned} q(x, y) = & (ay + 2 + 2x + bx^3 + dx^4) + (y^2 + (-3 - a)y - 2xy + fx^3y + gx^4y) + \\ & + (-3x^2y + x^2 + cx^3 + hx^5 + vx^6) + \\ & + ((-4 - f)x^3y + (1 - b - c)x^3 + ex^4 + (1 - v)x^6 + wx^7) + \\ & + ((-3 - g)x^4y + (2 - d - e)x^4 + (3 - h)x^5 + (2 - w)x^7 + 2x^8). \end{aligned}$$

S obzirom na to da su koeficijenti polinoma $q(x, y)$ iz \mathbb{Z}_5 , svi koeficijenti trebaju biti posmatrani po modulu 5 da bi se dobila proporcionalnost. Izaberimo:

$$\begin{aligned} q(x, y) = & (ay + 2 + 2x + bx^3 + dx^4) + (y^2 + (-3 - a)y - 2xy + fx^3y + gx^4y) + \\ & + (-3x^2y + 6x^2 + cx^3 + hx^5 + vx^6) + ((-4 - f)x^3y + (11 - b - c)x^3 + ex^4 + (6 - v)x^6 + wx^7) + \\ & + ((-3 - g)x^4y + (7 - d - e)x^4 + (13 - h)x^5 + (7 - w)x^7 + 2x^8). \end{aligned}$$

Proporcionalnost odgovarajućih koeficijenata se zadovoljena za: $a = -1$, $c = 6$, $b = 3$, $d = 1$, $f = -3$, $g = -1$, $h = 9$, $v = 3$, $e = 2$ i $w = 1$.

Dalje je:

$$\begin{aligned} q(x, y) = & (-y + 2 + 2x + 3x^3 + x^4) + (y^2 - 2y - 2xy - 3x^3y - x^4y) + \\ & (-3x^2y + 6x^2 + 6x^3 + 9x^5 + 3x^6) + (-x^3y + 2x^3 + 2x^4 + 3x^6 + x^7) + \\ & (-2x^4y + 4x^4 + 4x^5 + 6x^7 + 2x^8), \end{aligned}$$

tj.

$$q(x, y) = -(y-2-2x-3x^3-x^4) + y(y-2-2x-3x^3-x^4) - 3x^2(y-2-2x-3x^3-x^4) \\ - x^3(y-2-2x-3x^3-x^4) - 2x^4(y-2-2x-3x^3-x^4).$$

Dobijamo:

$$q(x, y) = (-1 + y - 3x^2 - x^3 - 2x^4)(y - 2 - 2x - 3x^3 - x^4),$$

tj.

$$q(x, y) = (y - (1 + 3x^2 + x^3 + 2x^4))(y - (2 + 2x + 3x^3 + x^4)).$$

Konačno: $p_1(x) = 1 + 3x^2 + x^3 + 2x^4$ i $p_2(x) = 2 + 2x + 3x^3 + x^4$.

10 Zaključak

Glavni rezultat disertacije je karakterizacija svodljivih polinoma dve promenljive sa celobrojnim koeficijentima, čime je veza polinoma dve promenljive i njima pridruženih Newton-ovih poligona u smislu ispitivanja njihove svodljivosti u potpunosti zaokružena. Naime, formulisan je potreban i dovoljan uslov za egzistenciju netrivialne faktorizacije polinoma dve promenljive sa celobrojnim koeficijentima pomoću Newton-ovog poligona na faktor - polinome sa celobrojnim koeficijentima. S obzirom na to da bi se, na ovaj način, faktor - polinom koji ima netrivialnu faktorizaciju mogao dalje faktorisati, stvorena je teorijska osnova za faktorizaciju proizvoljnog polinoma dve promenljive sa celobrojnim koeficijentima na nesvodljive faktor - polinome.

Takođe, u disertaciji je prezentovan algoritam kojim se vrši provera svodljivosti proizvoljnog polinoma dve promenljive sa celobrojnim koeficijentima na faktor - polinome sa celobrojnim koeficijentima.

Dobijeni teorijski rezultati su omogućili i praktičnu primenu u teoriji kodiranja, za dekodiranje jedne specijalne klase Reed - Solomon kodova, miksa dve kodne reči.

11 Budući pravci istraživanja i dalji rad

Uspešna realizacija planiranih ciljeva disertacije omogućava dalja istraživanja u nekoliko različitih pravaca. Dobijeni teorijski rezultati otvaraju mogućnost primene u smislu daljeg istraživanja Newton-ovih poligona i njihove klasifikacije, sa ciljem formulacije stavova o nesvodljivosti. Dobijeni rezultati na polju primene mogu se fazifikacijom, tj. unošenjem neodređenosti u model, prilagoditi za rad sa zašumljenim podacima.

12 Literatura

- [1] BARVINOK A., *A course in convexity*, Graduate Studies in Mathematics, Volume 54, American Mathematical Society Providence, Rhode Island (2002).
- [2] BERLEKAMP E.R., *Algebraic coding theory*, McGraw-Hill, New York, (1968).
- [3] BIERBRAUER J., *Introduction to coding theory*, Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton, FL (2005).
- [4] BLEICHENBACHER D., KIAYIAS A., YUNG M., *Decoding of interleaved Reed Solomon codes over noisy data*, in Proceedings of the 30th International Colloquium on Automata, Languages and Programming, pp. (2003), 97–108.
- [5] COX D. A., *Galois Theory*, 2nd ed., Wiley, Hoboken (2012).
- [6] CRVENKOVIĆ S., PAVKOV I., *Factoring bivariate polynomials with integer coefficients via Newton polygons*, Filomat 27:2 (2013), 215–226.
- [7] DUMAS G., *Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels*, Journal de Math. Pures et Appliqués, no. 2 (1906), 191–258.
- [8] DUVAL D., *Absolute factorization of polynomials: a geometric approach*, SIAM J. Comput. 20 (1991), 1–21.
- [9] EISENSTEIN G., *Über die Irreduzibilität und einige andere Eigenschaften der Gleichungen*, J. Reine Angew. Math. 39 (1850), 160–179.
- [10] EWALD G., *Combinatorial Convexity and Algebraic Geometry*, GTM 168, Springer (1996).
- [11] FILASETA M., *The irreducibility of all but finitely many Bessel polynomials*, Acta Math. 174, no. 2 (1995), 383–397.
- [12] GAJIĆ LJ., *Predavanja iz uvoda u analizu*, Prirodno - matematički fakultet u Novom Sadu, Departman za matematiku i informatiku (2013).

-
- [13] GAO S., *Factoring multivariate polynomials via partial differential equations*, Mathematics of Computation 72, 242 (2003), 801–822.
- [14] GAO S., *Absolute irreducibility of polynomials via Newton polytopes*, Journal of Algebra 237, No.2 (2001), 501–520.
- [15] GAO S., LAUDER A. G. B., *Decomposition of polytopes and polynomials*, Discrete and Computational Geometry 26 (2001), 89–104.
- [16] GOODMAN J.E., O’ROURKE J., *Handbook of Discrete and Computational Geometry*, Elsevier Science, Amsterdam (1997).
- [17] GRAHAM R. L., *An efficient algorithm for determining the convex hull of a finite planar set*, Information Processing Letters 1 (1972), 132–133.
- [18] GRIGORYEV D. YU, CHISTOV A. L., *Fast factorization of polynomials into irreducible ones and the solution of systems of algebraic equations*, Dokl. Akad. Nauk SSSR 275, no. 6 (1984), 1302–1306.
- [19] GRÜNBAUM B., *Convex Polytopes*, Interscience Publ., London, New York, Sydney, (1967).
- [20] GURUSWAMI V., *Algorithmic Results in List Decoding*, Foundations and Trends in Theoretical Computer Science Vol. 2, No. 2 (2006), 107–195.
- [21] GURUSWAMI V., RUDRA A., *Limits to list decoding Reed-Solomon codes*, IEEE Transactions on Information Theory, vol. 52, no. 8 (2006).
- [22] GURUSWAMI V., SUDAN M., *Improved decoding of Reed-Solomon and algebraic-geometric codes*, IEEE Transactions on Information Theory, vol. 45 (1999), 1757–1767.
- [23] HAMMING R. W., *Error detecting and error correcting codes*, Bell System Technical Journal, vol. 29 (1950), 147–160.
- [24] HIRSCHFELD J. W. P., *Projective Geometries over Finite Fields*, Clarendon Press, Oxford (1979).
- [25] KALLAY M., *Indecomposable polytopes*, Israel J. Math. 41, no. 3 (1982), 235–243.

-
- [26] KALTOFEN E., *Polynomial factorization 1987-1991*, Proc. LATIN '92 (Sao Paulo, 1992), I. Simon (Ed.), Lecture Notes Comput. Sci., vol. 583, Springer, Berlin (1992), 294–313.
- [27] KALTOFEN E., *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization*, SIAM J. Comput. 14 (1985), no. 2, 469–489.
- [28] KOETTER R., VARDY A., *Algebraic soft-decision decoding of Reed-Solomon codes*, IEEE Transactions on Information Theory, vol. 49, no. 11 (2003), 2809–2825.
- [29] KOYUNCU F., *A geometric approach to absolute irreducibility of polynomials*, doctoral thesis, The Middle East Technical University - The Department of Mathematics (2004).
- [30] KOYUNCU F., *An application of the polytope method*, JFS, Vol 28 (2005), 13–19.
- [31] KOVAČEVIĆ I., RALEVIĆ N., *Funkcionalna analiza*, Fakultet tehničkih nauka u Novom Sadu (2004).
- [32] KURSCHAK J., *Irreduzible formen*, J. Reine Angew. Math. 152 (1923), 180–191.
- [33] LANG S., *Algebra*, Addison-Wesley (1974).
- [34] LENSTRA A. K., *Factoring multivariate polynomials over finite fields*, J. Comput. System Sci. 30, no. 2 (1985), 235–248.
- [35] LIDL R., NIEDERREITER H., *Finite Fields*, Encyclopedia of Math. and Its Appl., Vol. 20, Addison-Wesley, Reading, MA (1983).
- [36] LIPKOVSKI A., *Newton polyhedra and irreducibility*, Math. Z. 199 (1988) 119–127.
- [37] MCELIECE R. J., SWANSON L., *On the decoder error probability for Reed Solomon codes*, IEEE Transactions on Information Theory, vol. 32, no. 5 (1986), 701–703.
- [38] MCMULLEN P., *Indecomposable convex polytopes*, Israel J. Math. 58, no.3 (1987), 321–323.

- [39] MEYER W., *Indecomposable polytopes*, Trans. Amer. Math. Soc. 190 (1974), 77–86.
- [40] MILIĆ S., *Elementi algebre*, Carić, Beograd (1995).
- [41] ORE O., *Zur Theorie der Algebraischen Körper*, Acta Math. 44 (1924), 219–314.
- [42] ORE O., *Zur Theorie der Eisensteinschen Gleichungen*, Math. Z. 20 (1924), 267–279.
- [43] ORE O., *Zur Theorie der Irreduzibilitätskriterien*, Math. Z. 18 (1923), 278–288.
- [44] OSTROWSKI A. M., *On multiplication and factorization of polynomials I*, Lexicographic ordering and extreme aggregates of terms, Aequationes Math. 13 (1975), 201–228.
- [45] OSTROWSKI A. M., *On multiplication and factorization of polynomials II*, Irreducibility discussion, Aequationes Math. 14 (1976), 1–32.
- [46] PAVKOV I., *Nesvodljivost polinoma dve promenljive*, master teza, Univerzitet u Novom Sadu, Prirodno-matematiki fakultet, Departman za matematiku i informatiku, Novi Sad (2010).
- [47] PAVKOV I., RALEVIĆ N., NEDOVIĆ LJ., *An application of bivariate polynomial factorization on decoding of Reed - Solomon based codes*, submitted (2017).
- [48] PRASOLOV, V., *Polynomials*, Springer (2009).
- [49] REED I. S., SOLOMON G., *Polynomial codes over certain finite fields*, J. Soc. Ind. Appl. Math., vol. 9 (1960), 300–304.
- [50] RELLA T., *Ordnungsbestimmungen in Integritätsbereichen und Newtonsche Polygone*, J. Riene Angew. Math. 158 (1927), 33–48.
- [51] SCHMIDT W. M., *Equations over Finite Fields: an Elementary Approach*, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin/New York, (1976).

- [52] SCHNEIDER R., *Convex bodies: the Brunn-Minkowski theory*, Encyclopedia of Mathematics and its Applications, 44. Cambridge University Press, Cambridge (1993).
- [53] SCHÖNEMANN T., *Von denjenigen moduln, welche potenzen von primzahlen sind*, Journal für die Reine und Angew. Math. 32 (1846), 93–105.
- [54] SHANOK C., *Convex polyhedra and criteria for irreducibility*, Duke Mathematical Journal 2 (1936), 103–111.
- [55] SHEN B.-Z., *Algebraic-geometric codes and their decoding algorithm*, Ph.D. Thesis, Eindhoven Univ. Techn. (1992).
- [56] SHEPHARD G. C., *Decomposable convex polyhedra*, Mathematika 10 (1963), 89–95.
- [57] SMILANSKY Z., *An indecomposable polytope all of whose facets are decomposable*, Mathematika 33, no. 2 (1986), 192–196.
- [58] SMILANSKY Z., *Decomposability of polytopes and polyhedra*, Geometriae Dedicata 24, no.1 (1987), 29–49.
- [59] STEPANOV S. A., *Congruences with two unknowns*, Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 683–711 (in Russian)
- [60] STEPANOV S. A., *Rational points of algebraic curves over finite fields*, Current Problems of Analytic Number Theory, Proc. Summer School, Minsk (1972), 223–243, 272, Nauka, Minsk (1974) (in Russian)
- [61] STURMFELS B., *Gröbner Bases and Convex Polytopes*, University Lecture Series Vol. 8, American Mathematical Society (1996).
- [62] SUDAN M., *Decoding of Reed Solomon Codes beyond the Error-Correction Bound*, Journal of Complexity 13 (1997), 180–193.
- [63] 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).
- [64] TSFASMAN M.A., VLADUT S.G., *Algebraic-geometric codes*, Kluwer Academic Publishers, Dordrecht-Boston-London (1991).

-
- [65] VAN LINT J. H., *Introduction to coding theory*, Graduate Texts in Mathematics, vol. 86, 3rd Edition, Springer-Verlag, Berlin (1999).
- [66] VAN LINT J.H., VAN DER GEER G., *Introduction to coding theory and algebraic geometry*, DMV Seminar vol. 12, Birkhäuser Verlag, Basel Boston Berlin (1988).
- [67] VON ZUR GATHEN J., KALTOFEN E., *Factorization of multivariate polynomials over finite fields*, Math. Comp. 45, no. 171 (1985), 251–261.
- [68] WEBSTER R., *Convexity*, Oxford University Press, Oxford (1994).
- [69] ZIEGLER G. M., *Lectures on Polytopes*, Graduate Texts in Mathematics, Vol. 152, Springer-Verlag, Berlin/New York (1995).