Grafički prikaz binarnih kvadratnih formi

Vidolin, Marina

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marina Vidolin

GRAFIČKI PRIKAZ BINARNIH KVADRATNIH FORMI

Diplomski rad

Voditelj rada:
doc.dr.sc. Tomislav Pejković

Zagreb, veljača 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Teoriju kvadratnih formi, kao područje teorije brojeva, razvio je francuski matematičar Joseph-Louis Lagrange u 18. stoljeću. Postavio je mnoge fundamentalne tvrdnje o kvadratnim formama. Ovu teoriju je nastavio razvijati francuski matematičar Adrien-Marie Legendre. Legendre je sintetizirao Lagrangeov rad i dao cjelovit prikaz jednadžbi oblika $ax^2 + bxy + cy^2 = N$, gdje su a, b, c, N cijeli brojevi. Veći napredak u području kvadratnih formi ostvario je njemački matematičar i astronom Johann Karl Friedrich Gauss u 19. stoljeću. On je proučavao diskriminantu, ekvivalenciju i broj klasa kvadratnih formi. Svojim doprinosima je snažno utjecao i na teoriju kvadratnih formi s više varijabli, te na kasniji razvoj teorije brojeva. U devedesetim godinama 20. stoljeća engleski matematičar John Horton Conway je osmislio grafički pristup rješavanju jednadžbi oblika $ax^2+bxy+cy^2 = N$ u cijelim brojevima.

U ovom radu u središtu proučavanja je upravo Conwayev grafički pristup rješavanju spomenutih jednadžbi. U prvom poglavlju iskazujemo osnovne pojmove kao što su ekvivalencija formi, njihov matrični zapis i dokazujemo osnovne tvrdnje vezane uz njih. Također se bavimo i reprezentacijom cijelog broja zadanom binarnom kvadratnom formom te redukcijom kvadratnih formi.

U drugom poglavlju se upoznajemo s pojmom *topografa* te načinom na koji je nastao kako bismo mogli grafički prikazivati kvadratne forme. Definiramo bazu, primitivne i slabe vektore te iskazujemo i dokazujemo tvrdnje koje nam koriste u daljnjem razumijevanju pojma topografa. Razlikujemo topograf domene i topograf slike. Topograf domene je grafički prikaz svih primitivnih slabih vektora, slabih baza i njihovih međusobnih veza, dok je topograf slike grafički prikaz vrijednosti binarnih kvadratnih formi u primitivnim vektorima.

U posljednja dva poglavlja detaljnije ispitujemo topograf slike, koristeći ga za proučavanje ekvivalencije kvadratnih formi i njihovih izometrija što nas vodi na algoritam za rješavanje kvadratnih diofantinskih jednadžbi u dvije varijable. Jedno poglavlje je posvećeno definitnim formama, tj. onima s negativnom diskriminantom, a drugo indefinitnim formama koje imaju pozitivnu diskriminantu.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Poglavlje 1

Binarne kvadratne forme

Definicija 1.1. ***Binarna kvadratna forma*** *je preslikavanje* $f : \mathbb{R}^2 \to \mathbb{R}$ *oblika*

$$f(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}.$$

Drugim riječima, binarne kvadratne forme su homogeni polinomi dviju varijabli drugog stupnja s cjelobrojnim koeficijentima.

Diskriminanta od f je broj $d = d(f) = b^2 - 4ac$.

Nadopunjavanjem do potpunog kvadrata na dva načina dobivamo

$$4af(x, y) = (2ax + by)^2 - dy^2, \tag{1.1}$$

$$4cf(x, y) = (2cy + bx)^2 - dx^2. \tag{1.2}$$

Diskriminanta d je cijeli broj te iz (1.1) i (1.2) vidimo da ako je

$d < 0$, onda f poprima ili samo pozitivne ili samo negativne vrijednosti te kažemo da je f *pozitivno*, odnosno *negativno definitna*,

$d > 0$, onda f poprima i pozitivne i negativne vrijednosti te kažemo da je f *indefinitna*,

$d = 0$, onda f poprima samo nenegativne ili samo nepozitivne vrijednosti te kažemo da je f *pozitivno*, odnosno *negativno semidefinitna.*

Ako je f negativno (semi)definitna forma, onda je $-f$ pozitivno (semi)definitna i obratno, pa ćemo u nastavku promatrati pozitivno (semi)definitne forme. Zanimat će nas vrijednosti koje forma poprima na $\mathbb{Z}^2 \setminus (0, 0)$. U točki $(0, 0)$ forma uvijek poprima vrijednost 0, koja nam nije od interesa pa ju isključujemo.

1.1 Ekvivalencija formi

Od koristi nam je znati kada su dvije binarne kvadratne forme jednake, to jest ekvivalentne.

Definicija 1.2. *Za dvije kvadratne forme f i g kažemo da su **ekvivalentne** ako se jedna može transformirati u drugu pomoću cjelobrojnih unimodularnih transformacija, tj. supstitucija oblika*

$$x = px' + qy', \qquad y = rx' + sy',$$

gdje je $p, q, r, s \in \mathbb{Z}$ i $ps - qr = 1$. Pišemo $f \sim g$.

Primjer 1.1. *Binarne kvadratne forme $3x^2 + 4y^2$ i $4x^2 + 3y^2$ su ekvivalentne.*

Rješenje: Uvedemo supstituciju $x = -y'$ i $y = x'$, tj. $q = -1,\ r = 1,\ p = s = 0$.

$$ps - qr = 0 \cdot 0 - (-1) \cdot 1 = 1.$$

Ekvivalenciju formi možemo kraće zapisati kao $(3, 0, 4) \sim (4, 0, 3)$. □

1.2 Matrični zapis formi

Binarnu kvadratnu formu $f(x, y) = ax^2 + bxy + cy^2$ matrično možemo zapisati kao $f(x, y) = X^\tau F X$, gdje su

$$F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}, \qquad X = \begin{pmatrix} x \\ y \end{pmatrix}.$$

Napomenimo da smo ovdje prešutno identificirali 1×1 matricu s elementom koji sadrži. I u nastavku ćemo tako raditi.

Simetrična matrica F pridružena je kvadratnoj formi $f(x, y)$ dok je X^τ transponirana matrica matrice X. Primijetimo da je diskriminanta forme f povezana s determinantom pripadne matrice F,

$$d = b^2 - 4ac = -(4ac - b^2) = -4\left(ac - \frac{b^2}{4}\right) = -4 \det F.$$

Supstituciju varijabli matrično zapisujemo

$$X = UX' = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Tada je uvjet unimodularnosti $\det U = 1$. Ako je G matrični zapis kvadratne forme g i $f \sim g$, onda je $G = U^\tau F U$. Naime, vrijedi

$$f(x,y) = X^\tau F X = (UX')^\tau F(UX') = X'^\tau (U^\tau F U)X' = X'^\tau G X' = g(x',y').$$

Označimo s Γ skup svih matrica oblika $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$, $p,q,r,s \in \mathbb{Z}$, $ps - qr = 1$.

Skup Γ čini grupu s obzirom na množenje matrica koju nazivamo *specijalna linearna grupa* $\mathrm{SL}_2(\mathbb{Z})$. Zaista, neka su $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \Gamma$. Tada je

$$AB^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} s & -q \\ -r & p \end{pmatrix} = \begin{pmatrix} as - br & -aq + bp \\ cs - dr & -cq + dp \end{pmatrix}$$

i $\det(AB^{-1}) = \det A \cdot (\det B)^{-1} = 1$, pa je $AB^{-1} \in \Gamma$. Elemente grupe Γ zovemo *unimodularne matrice.*

Teorem 1.1. *Neka su f, g i h binarne kvadratne forme. Tada vrijedi:*

1. $f \sim f$,
2. $f \sim g \Rightarrow g \sim f$,
3. $f \sim g, g \sim h \Rightarrow f \sim h$.

Drugim riječima, $\sim$ je relacija ekvivalencije.

Dokaz. 1. Očito je $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$.

2. Ako je $f \sim g$, onda postoji $U \in \Gamma$ tako da je $G = U^\tau F U$. Odavde je $F = (U^{-1})^\tau G U^{-1}$. Ali, Γ je grupa pa je $U^{-1} \in \Gamma$, a to znači da je $g \sim f$.

3. Ako je $f \sim g$ i $g \sim h$, onda je $G = U^\tau F U$, $H = V^\tau G V$ za neke $U, V \in \Gamma$. Odavde je $H = (UV)^\tau F(UV)$, a budući je $UV \in \Gamma$, to je $f \sim h$. □

1.3 Reprezentacija cijelog broja

Definicija 1.3. *Kažemo da kvadratna forma **reprezentira** cijeli broj n ako postoje cijeli brojevi x_0, y_0 takvi da je $f(x_0, y_0) = n$. Ako je još k tome najveći zajednički djelitelj $(x_0, y_0) = 1$, onda kažemo da je reprezentacija **prava**, inače je **neprava**.*

Propozicija 1.2. *Neka su f i g ekvivalentne kvadratne forme, te $n \in \mathbb{Z}$. Tada:*

1. *f reprezentira n ako i samo ako g reprezentira n,*
2. *f pravo reprezentira n ako i samo ako g pravo reprezentira n,*

3. diskriminante od f i g su jednake.

Dokaz. 1. Zbog Teorema 1.1, dovoljno je provjeriti jednu implikaciju. Neka je $G = U^\tau F U$. Ako je $n = X_0^\tau F X_0$, onda je $n = X_1^\tau G X_1$, gdje je $X_1 = U^{-1} X_0$.

2. Neka je $X_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$. Pretpostavimo da je $(x_0, y_0) = 1$. Iz $x_0 = px_1 + qy_1$, $y_0 = rx_1 + sy_1$ slijedi da je $(x_1, y_1) = 1$.

3. Označimo sa d_0 i d_1 diskriminante od f i g. Tada je

$$d_0 = -4 \det F, \quad d_1 = -4 \det G,$$

$$\det G = \det U^\tau \det F \det U = \det F.$$

Zaključujemo $d_0 = d_1$. □

Ako neki cijeli broj n želimo reprezentirati kvadratnom formom $f(x, y) = ax^2 + bxy + cy^2$, tada zapravo rješavamo diofantsku jednadžbu

$$ax^2 + bxy + cy^2 = n.$$

Diofantske jednadžbe mogu se ugrubo podijeliti prema broju rješenja, na one koje imaju konačno mnogo rješenja, na one koje imaju beskonačno mnogo rješenja te na one koje nemaju rješenja.

Primjer 1.2. *Riješimo diofantsku jednadžbu $x^2 - y^2 = 71$.*

Rješenje: Uočimo ako je $(x_0, y_0) \in \mathbb{Z}^2$ rješenje jednadžbe, tada su i $(\pm x_0, \pm y_0)$ sa svim kombinacijama predznaka rješenja jednadžbe.

Znamo da vrijedi $x > y > 0$ jer bi u suprotnom, tj. za $y > x$, lijeva strana jednadžbe bila negativna, a desna pozitivna. Također je $x, y \neq 0$ jer broj 71 nije potpun kvadrat.

Vidimo da je lijeva strana početne jednadžbe zapravo razlika kvadrata pa jednadžbu možemo zapisati kao

$$(x - y)(x + y) = 71.$$

Broj 71 je prost te znamo da postoji jedinstvena faktorizacija u $\mathbb{Z}$, pa slijedi da je

$$x + y = 71 \text{ i } x - y = 1, \text{ tj. } x = 36, y = 35.$$

Dakle, skup rješenja jednadžbe $x^2 - y^2 = 71$ je $\{(\pm 36, \pm 35)\}$. Kažemo da forma $f(x, y) = x^2 - y^2$ reprezentira broj 71, te da je broj reprezentacija konačan. □

Primjer 1.3. *Riješimo diofantsku jednadžbu* $x^2 - 5y^2 = 4$.

Rješenje: Jednadžba $x^2 - 5y^2 = 4$ je tzv. Pellova jednadžba. U skupu $\mathbb{Z}$ Pellova jednadžba ima beskonačno mnogo rješenja.

Ako gledamo u skupu prirodnih brojeva $\mathbb{N}$, njeno najmanje rješenje je $(x_1, y_1) = (3, 1)$. Kod određivanja najmanjeg rješenja Pellove jednadžbe u pravilu se koristi teorija verižnih razlomaka.

Sva rješenja jednadžbe $x^2 - 5y^2 = 4$ u $\mathbb{N}$ dana su sa

$$\frac{x_n + y_n\sqrt{4}}{2} = \left(\frac{x_1 + y_1\sqrt{4}}{2}\right)^n, \quad n \in \mathbb{N},$$

gdje je (x_1, y_1) fundamentalno (tj. najmanje) rješenje te jednadžbe. Sva rješenja u $\mathbb{Z}$ dobivamo varijacijom predznaka $\{(\pm x_n, \pm y_n) : n \in \mathbb{N}_0\}$.

Dakle, forma $x^2 - 5y^2$ reprezentira broj 4 na beskonačno mnogo načina. □

Primjer 1.4. *Riješimo diofantsku jednadžbu* $x^2 + y^2 = 2006$.

Rješenje: Prije nego što krenemo s rješavanjem diofantske jednadžbe prisjetimo se da je kvadrat parnog broja uvijek djeljiv s 4 jer je $(2k)^2 = 4 \cdot k^2$, dok kvadrat neparnog broja pri dijeljenju s 4 daje ostatak 1 jer je $(2k + 1)^2 = 4(k^2 + k) + 1$.

Budući da broj 2006 pri dijeljenju s 4 daje ostatak 2, slijedi da su i x i y neparni. Označimo $x = 2m + 1$, $y = 2n + 1$ $(m, n \in \mathbb{Z})$, pa uvrštavanjem u početnu jednadžbu dobivamo

$$\begin{aligned}(2m + 1)^2 + (2n + 1)^2 &= 2006,\\ 4m^2 + 4m + 1 + 4n^2 + 4n + 1 &= 2006,\\ 4(m^2 + m + n^2 + n) &= 2004,\\ m(m + 1) + n(n + 1) &= 501.\end{aligned}$$

Lijeva i desna strana posljednje jednakosti različite su parnosti. Naime, $m(m + 1)$ i $n(n + 1)$ su parni brojevi te je njihov zbroj paran broj, dok je broj 501 neparan. Iz toga slijedi da jednadžba nema cjelobrojnih rješenja, tj. forma $x^2 + y^2$ ne reprezentira broj 2006. □

1.4 Redukcija pozitivno definitnih kvadratnih formi

Kao što smo spomenuli na početku ovog poglavlja, binarne kvadratne forme dijelimo na pozitivo i negativno (semi)definitne te indefinitne.

U ovom potpoglavlju ćemo se baviti pozitivno definitnim formama te ćemo opisati njihovu redukciju.

Definicija 1.4. *Kažemo da je pozitivno definitna kvadratna forma* $f(x,y) = ax^2 + bxy + cy^2$ ***reducirana*** *ako je* $-a < b \leq a < c$ *ili* $0 \leq b \leq a = c$.

Teorem 1.3. *Svaka pozitivno definitna kvadratna forma je ekvivalentna nekoj reduciranoj formi.*

Dokaz. Neka je f pozitivno definitna kvadratna forma s pripadnom matricom

$$F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

Znamo da je $a > 0$ i $d < 0$, a iz $d = b^2 - 4ac < 0$ slijedi da je $c > 0$. Označimo s U i V unimodularne matrice:

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ i } V = \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}.$$

Sada ćemo pokazati da korištenjem konačno mnogo transformacija s ovim matricama možemo postići da vrijedi

$$|b| \leq a \leq c. \tag{1.3}$$

Uočimo da se transformacijom pomoću U, tj. $U^\tau F U = \begin{pmatrix} c & \frac{-b}{2} \\ \frac{-b}{2} & a \end{pmatrix}$ koeficijenti a i c zamjenjuju.

Dakle, ako smo u F imali $a > c$, onda u $U^\tau F U$ imamo $a < c$.

Pogledajmo što se događa transformacijom pomoću V.

$$V^\tau F V = \begin{pmatrix} a & \pm a + \frac{b}{2} \\ \pm a + \frac{b}{2} & a \pm b + c \end{pmatrix},$$

što znači da V zamjenjuje b s $b \pm 2a$, dok a ostavlja nepromijenjenim. Koristeći ovu transformaciju konačno mnogo puta možemo postići da je $|b| \leq a$.

Neka smo sada došli do forme za koju vrijedi (1.3). Ako je $b = -a$, onda primjenom supstitucije s matricom V možemo postići da je $b = a$, uz nepromijenjeni c. Ako je $a = c$, onda primjenom supstitucije s matricom U možemo postići da je $b \geq 0$. Tako dobivamo reduciranu formu ekvivalentnu početnoj. □

Primjer 1.5. *Nađimo reduciranu formu ekvivalentnu formi* $f(x,y) = 166x^2 + 136xy + 28y^2$.

Rješenje: Neka je F matrični zapis dane kvadratne forme f, odnosno $F = \begin{pmatrix} 166 & 68 \\ 68 & 28 \end{pmatrix}$. Kako bi proveli redukciju kvadratne forme koristit ćemo se unimodularnim matricama navedenim u Teoremu 1.3:

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad V^+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad V^- = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Na matricu F primjenjujemo transformaciju U i dobivamo $F_1 = \begin{pmatrix} 28 & -68 \\ -68 & 166 \end{pmatrix}$.

Budući je $b > a$, na matricu F_1 dva puta primjenjujemo matricu V^+ kako bi postigli $-a < b \leq a$, pa dobivamo $F_2 = \begin{pmatrix} 28 & -40 \\ -40 & 58 \end{pmatrix}$ i $F_3 = \begin{pmatrix} 28 & -12 \\ -12 & 6 \end{pmatrix}$.

Ponovo primjenjujemo U i dobivamo $F_4 = \begin{pmatrix} 6 & 12 \\ 12 & 28 \end{pmatrix}$.

Sada dva puta primjenjujemo matricu V^-, pa dobivamo $F_5 = \begin{pmatrix} 6 & 6 \\ 6 & 10 \end{pmatrix}$ i $F_6 = \begin{pmatrix} 6 & 0 \\ 0 & 4 \end{pmatrix}$.

Konačno, primjenom U dobivamo $F_7 = \begin{pmatrix} 4 & 0 \\ 0 & 6 \end{pmatrix}$.

Matrici F_7 odgovara forma $4x^2 + 6y^2$ koja je očito reducirana, $b = 0 < a = 4 < c = 6$, i ekvivalentna početnoj. □

Teorem 1.4. *Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.*

Dokaz. Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa je c, a onda i a i $|b|$ manje od $\frac{1}{3}|d|$. □

Definicija 1.5. *Broj reduciranih kvadratnih formi s diskriminantom d zove se* ***broj klasa*** *od d i označava s h(d).*

Primjer 1.6. *Izračunajmo* $h(-16)$.

Rješenje: Neka je d diskriminanta naše forme, $d = -16$, tada je $-d = 4ac - b^2 \geq 3ac \geq 3a^2$. Slijedi da je $a \leq 2$. Imamo dva slučaja.

$a = 1$. Tada je $b \in \{0, 1\}$. Kada uvrstimo $a = 1$ dobivamo $4c - b^2 = 16$ odakle slijedi da je b paran. Za $b = 0$ je $c = 4$.

$a = 2$. Tada je $b \in \{-1, 0, 1, 2\}$ zbog $-a < b \leq a$. Iz $8c - b^2 = 16$ slijedi da je b paran. Uvrštavanjem b u jednadžbu vidimo da za $b = 2$ nemamo rješenja, dok za $b = 0$ dobivamo $c = 2$.

Dakle, postoje dvije reducirane forme s diskriminantom -16, a to su $x^2 + 4y^2$ i $2x^2 + 2y^2$. Stoga je $h(-16) = 2$. □

1.5 Redukcija indefinitnih kvadratnih formi

U prethodnom potpoglavlju smo opisali redukciju pozitivno definitnih formi, a sada ćemo isto napraviti za indefinitne forme.

Definicija 1.6. *Kažemo da je indefinitna kvadratna forma* $f(x,y) = ax^2 + bxy + cy^2$ *s diskriminantom* d ***reducirana*** *ako je*

$$0 < \sqrt{d} - b < 2\,|a| < \sqrt{d} + b. \tag{1.4}$$

Uvjet reduciranosti (1.4) je ekvivalentan

$$\Big|\sqrt{d} - 2\,|a|\Big| < b < \sqrt{d}. \tag{1.5}$$

Zbog $\Big(\sqrt{d} - b\Big)\Big(\sqrt{d} + b\Big) = -4ac$ je uvjet reduciranosti ekvivalentan i

$$0 < \sqrt{d} - b < 2\,|c| < \sqrt{d} + b. \tag{1.6}$$

Iz uvjeta reduciranosti (1.4) vidimo da za fiksirani d postoji samo konačno mnogo reduciranih indefinitnih formi s cjelobrojnim koeficijentima kojima je diskriminanta d.

Propozicija 1.5. *Indefinitna forma* $f(x,y) = ax^2 + bxy + cy^2 = a(x - \vartheta y)(x - \varphi y)$ *je reducirana ako i samo ako je*

$$|\vartheta| < 1, \quad |\varphi| > 1 \quad i \quad \vartheta\varphi < 0, \tag{1.7}$$

gdje su ϑ *i* φ *korijeni od* $f(x,1)$ *određeni s*

$$\vartheta = \frac{-b + \sqrt{d}}{2a}, \quad \varphi = \frac{-b - \sqrt{d}}{2a}.$$

Dokaz. Pretpostavimo da je f reducirana. Dijeljenjem (1.4) s $2|a|$ dobivamo $|\vartheta| < 1$ i $|\varphi| > 1$. Također je $0 < b < \sqrt{d}$, pa zbog $d = b^2 - 4ac$ imamo $ac < 0$. Odatle je $\vartheta\varphi = \frac{c}{a} < 0$.

Pretpostavimo sada da vrijedi (1.7). Iz $\frac{c}{a} = \vartheta\varphi < 0$ su a i c suprotnih predznaka te je $|b| < \sqrt{d}$. Nadalje, $(-b + \sqrt{d})(-b - \sqrt{d}) = 4a^2\vartheta\varphi < 0$ povlači da su $-b + \sqrt{d}$ i $b + \sqrt{d}$ istog predznaka, odnosno zbog $b < \sqrt{d}$, moraju biti pozitivni. Iz $|\vartheta| < 1$ je $|-b + \sqrt{d}| < 2|a|$, dok iz $|\varphi| > 1$ slijedi $2|a| < |b + \sqrt{d}|$. Dakle, vrijedi (1.4), pa je f reducirana. □

Teorem 1.6. *Svaka indefinitna forma je ekvivalentna nekoj reduciranoj formi.*

Dokaz teorema nećemo navoditi, a može se naći u skripti [5, str. 28].

U prethodnom potpoglavlju smo vidjeli da za definitne forme u svakoj klasi ekvivalencije postoji jedinstvena reducirana forma. Za indefinitne forme može postojati više ili čak beskonačno mnogo reduciranih formi u istoj klasi.

Definicija 1.7. *Desna susjedna forma od $f(x,y) = a^2+bxy+cy^2$ je njoj ekvivalentna forma f_d koja se dobiva supstitucijom s matricom $U_s = \left(\begin{smallmatrix} 0 & 1 \\ -1 & s \end{smallmatrix}\right)$, tj.*

$$f_d(x,y) = f(y,-x+sy) = cx^2 - (b+2cs)xy + c'y^2$$

za neki cijeli broj s. Analogno, lijeva susjedna forma od f dobiva se supstitucijom s matricom $\left(\begin{smallmatrix} s & -1 \\ 1 & 0 \end{smallmatrix}\right) = U_s^{-1}$, odnosno

$$f_l(x,y) = f(sx-y,x) = a'x^2 - (b+2as)xy + ay^2.$$

Vidimo da su kvadratne forme $ax^2+bxy+cy^2$ i $cx^2+b'xy+c'y^2$ s istom diskriminantom susjedne ako i samo ako je $\frac{b+b'}{2c} \in \mathbb{Z}$.

Propozicija 1.7. *Svaka reducirana forma ima jedinstvenu reduciranu desnu susjednu formu i jedinstvenu reduciranu lijevu susjednu formu.*

Dokaz propozicije nećemo navoditi, a može se naći u skripti [5, str. 29].

Poglavlje 2

Topograf

U prethodnom smo poglavlju definirali binarne kvadratne forme, iskazali i dokazali određene tvrdnje koje vrijede, no forme nismo grafički prikazivali.

Da bismo mogli grafički prikazivati kvadratne forme, prvo se trebamo upoznati s pojmom *topografa* te kako je nastao.

Kroz povijest su se mnogi matematičari bavili rješavanjem diofantskih jednadžbi oblika $ax^2 + by^2 = c$ gdje su a, b, c cijeli brojevi.

U 18. stoljeću, točnije 1733. godine, Leonhard Euler, poznati švicarski matematičar, fizičar i astronom, dao je jedno rješenje jednadžbe $31x^2 + 1 = y^2$.

Eulerovo rješenje dane jednadžbe je uređeni par prirodnih brojeva (x, y) tako da je x najmanji mogući i ono glasi $(x, y) = (273, 1520)$.

Dva stoljeća kasnije, 1990-ih, engleski matematičar **John Horton Conway** osmislio je izvanredan grafički pristup rješavanju spomenutih jednadžbi.

Da bismo bolje razumjeli Conwayevo grafičko rješavanje, najprije ćemo objasniti tzv. *problem malih i velikih skokova* u ravnini.

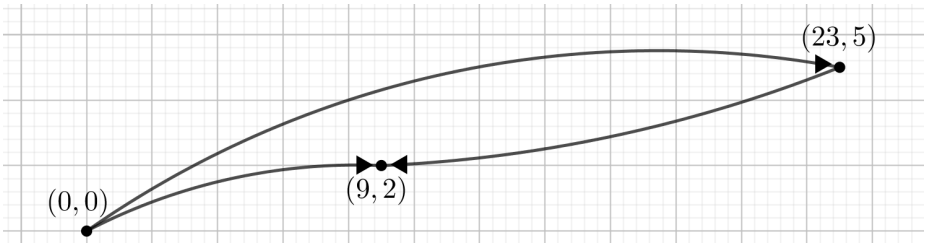
2.1 Problem malih i velikih skokova

Zamislimo da se nalazimo u pravokutnom koordinatnom sustavu te da se možemo kretati samo po određenim pravilima.

Možemo napraviti *mali skok* za vektor $(14, 3)$ ili $(-14, -3)$ te *veliki skok* za vektor $(23, 5)$ ili $(-23, -5)$.

Zanima nas koje sve točke možemo posjetiti u pravokutnom koordinatnom sustavu ako krećemo iz njegova ishodišta $(0, 0)$ i jedini dopušteni koraci su prethodno opisani mali i veliki skokovi.

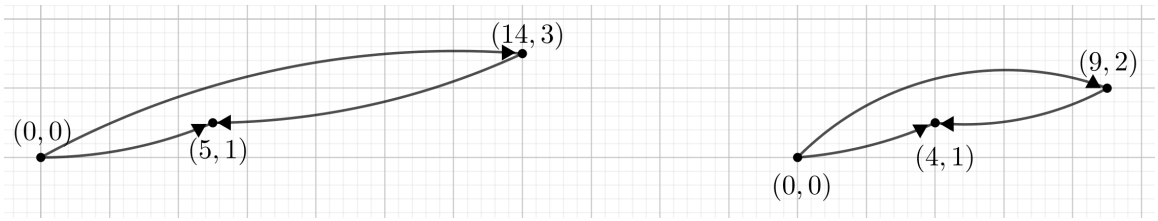
Rješenje: Ako možemo napraviti veliki skok za vektor $\pm(23, 5)$ i mali za vektor $\pm(14, 3)$ tada kombinacijom velikog skoka $(23, 5)$ i malog skoka $(-14, -3)$ dobivamo novi pomak za vektor $\pm(9, 2)$ kojeg nazivamo *skok*. Skok je prvi složeni pomak kojeg dobivamo.



Slika 2.1: Skok, dobiven kombinacijom velikog i malog skoka u suprotnim smjerovima.

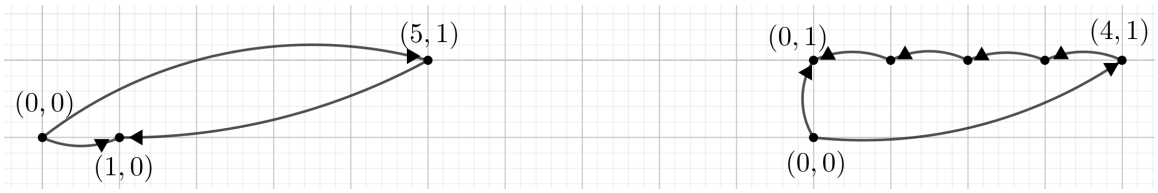
Kombinacijom malog skoka za vektor $(14, 3)$ i skoka za vektor $(-9, -2)$ dobivamo sljedeći složeni pomak za vektor $\pm(5, 1)$ kojeg nazivamo *doskok*.

Ako pak kombiniramo skok i doskok dobit ćemo pomak za vektor $\pm(4, 1)$ nazvan *odskok*.



Slika 2.2: Doskok i odskok

Doskokom i odskokom možemo zakoračiti desno za vektor $(1, 0)$ ili lijevo za vektor $(-1, 0)$. A ako odskočimo i zakoračimo lijevo tada možemo zakoračiti prema gore za vektor $(0, 1)$ ili dolje za vektor $(0, -1)$.



Slika 2.3: Korak desno i korak gore

Kombinacijom osnovnih pomaka došli smo do pomaka za 1 prema gore, dolje, lijevo ili desno, tj. dopušteno nam je kretanje po svim cjelobrojnim točkama pravokutnog koordinatnog sustava.

Pri rješavanju problema malih i velikih skokova koristimo *Euklidov algoritam* tako da algoritam prvo primijenimo na x-koordinatu vektora, a potom, ako je potrebno, i na y-koordinatu.

Teorem 2.1. ***(Euklidov algoritam).*** *Neka su b i $c > 0$ cijeli brojevi. Pretpostavimo da je uzastopnom primjenom teorema o dijeljenju s ostatkom dobiven niz jednakosti*

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c, \\ c &= r_1q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\ldots \\ r_{j-2} &= r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1}. \end{aligned}$$

Tada je najveći zajednički djelitelj brojeva b i c, tj. $\operatorname{nzd}(b, c)$ *jednak r_j, posljednjem ostatku različitom od nule. Vrijednosti od x_0 i y_0 u izrazu* $\operatorname{nzd}(b, c) = bx_0 + cy_0$ *mogu se dobiti izražavanjem svakog ostatka r_i kao linearne kombinacije od b i c.*

Primijetimo da ćemo u konačno mnogo koraka doći do ostatka $r_{j+1} = 0$ jer ostatci r_1, r_2, r_3, ... čine padajući niz prirodnih brojeva.

Za dokaz ovog teorema potrebna nam je sljedeća propozicija.

Propozicija 2.2. *Vrijedi* $\operatorname{nzd}(a, b) = \operatorname{nzd}(a, b + ax)$ *gdje je* $x \in \mathbb{Z}$.

Dokaz propozicije nećemo navoditi, a može se naći u skripti [4, str. 3]

Dokaz teorema. Po propoziciji 2.2 imamo

$$\begin{aligned} \operatorname{nzd}(b, c) = \operatorname{nzd}(b - cq_1, c) = \operatorname{nzd}(r_1, c) = \operatorname{nzd}(r_1, c - r_1q_2) = \operatorname{nzd}(r_1, r_2) = \\ \operatorname{nzd}(r_1 - r_2q_3, r_2) = \operatorname{nzd}(r_3, r_2). \end{aligned}$$

Nastavljajući ovaj proces, dobivamo: $\operatorname{nzd}(b, c) = \operatorname{nzd}(r_{j-1}, r_j) = \operatorname{nzd}(r_j, 0) = r_j$. Indukcijom ćemo dokazati da je svaki r_i linearna kombinacija od b i c. Za r_1 i r_2 to vrijedi, pa pretpostavimo da vrijedi i za r_{i-1} i r_{i-2}. Kako je $r_i = r_{i-2} - r_{i-1}q_i$, po pretpostavci indukcije dobivamo da je r_i linearna kombinacija od b i c. □

Vratimo se sad rješavanju problema malih i velikih skokova primjenom Euklidovog algoritma. Počevši velikim skokom $(23, 5)$ i malim skokom $(14, 3)$, Euklidov algoritam primijenjen na te vektore izgleda ovako:

$$\begin{aligned}(23,5) &= 1 \cdot (14,3) + (9,2),\\ (14,3) &= 1 \cdot (9,2) + (5,1),\\ (9,2) &= 1 \cdot (5,1) + (4,1),\\ (5,1) &= 1 \cdot (4,1) + (1,0),\\ (4,1) &= 4 \cdot (1,0) + (0,1).\end{aligned}$$

Ovdje su kvocijenti određeni Euklidovim algoritmom primijenjenim na x-koordinatu vektora. Primjerice, u prvom retku $(23, 5) = 1 \cdot (14, 3) + (9, 2)$ vidimo da je kvocijent 1 dobiven primjenom teorema o dijeljenju s ostatkom na x-koordinatu, $23 = 1 \cdot 14 + 9$. Koristeći kvocijent 1, prvi redak glasi $(23, 5) = 1 \cdot (14, 3) + (9, ?)$. Iz $5 = 1 \cdot 3 + 2$ slijedi da je y-koordinata vektora $(9, ?)$ jednaka 2.

Napomenimo da Euklidov algoritam primijenjen na vektore ne daje uvijek poželjne rezultate.

Primjer 2.1. *Primijenimo Euklidov algoritam na vektore* $(87, 16)$ *i* $(32, 19)$.

Rješenje. Primjenjujemo algoritam na x-koordinatu vektora $(87, 16)$.

$$\begin{aligned}(87,16) &= 2 \cdot (32,19) + (23,-22),\\ (32,19) &= 1 \cdot (23,-22) + (9,41),\\ (23,-22) &= 2 \cdot (9,41) + (5,-104),\\ (9,41) &= 1 \cdot (5,-104) + (4,145),\\ (5,-104) &= 1 \cdot (4,145) + (1,-249),\\ (4,145) &= 4 \cdot (1,-249) + (0,1141).\end{aligned}$$

Vidimo da ovim posljednjim pomacima, $(1, -249)$ i $(0, 1141)$, ne možemo doći u svaku cjelobrojnu točku pravokutnog koordinatnog sustava, pa isto vrijedi i za početni par vektora. □

Primijetimo da je u Primjeru 2.1 najveći zajednički djelitelj $\text{nzd}(87, 16) = 1$ i $\text{nzd}(32, 19) = 1$, ali koristeći te vektore ne možemo doći do svake cjelobrojne točke koordinatnog sustava. Naime, do točke $(0, y)$ možemo doći ako i samo ako je y djeljiv sa 1141.

U jednoj dimenziji ključna invarijanta kod primjene Euklidovog algoritma bio je najveći zajednički djelitelj, ako je $a = q \cdot b + r$, tada je $\text{nzd}(a, b) = \text{nzd}(b, r)$.

U dvije dimenzije to nije slučaj, već je invarijanta determinanta.

Definicija 2.1. *Neka su* (a, b) *i* (c, d) *dva vektora. Determinanta toga para vektora je broj* $ad - bc$*, a označavamo je s*

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

Propozicija 2.3. *Neka su* (a, b) *i* (c, d) *vektori s cjelobrojnim koordinatama. Pretpostavimo da je* q *cijeli broj i* (r, s) *vektor koji zadovoljavaju*

$$(a, b) = q \cdot (c, d) + (r, s).$$

Tada vrijedi

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = -\det\begin{pmatrix} c & d \\ r & s \end{pmatrix}.$$

Dokaz. Znamo da vrijedi $a = qc + r,\ b = qd + s$. Tada je

$$\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = ad - bc = (qc + r)d - (qd + s)c = qcd + rd - qdc - sc = -(cs - rd) = -\det\left(\begin{smallmatrix} c & d \\ r & s \end{smallmatrix}\right)$$

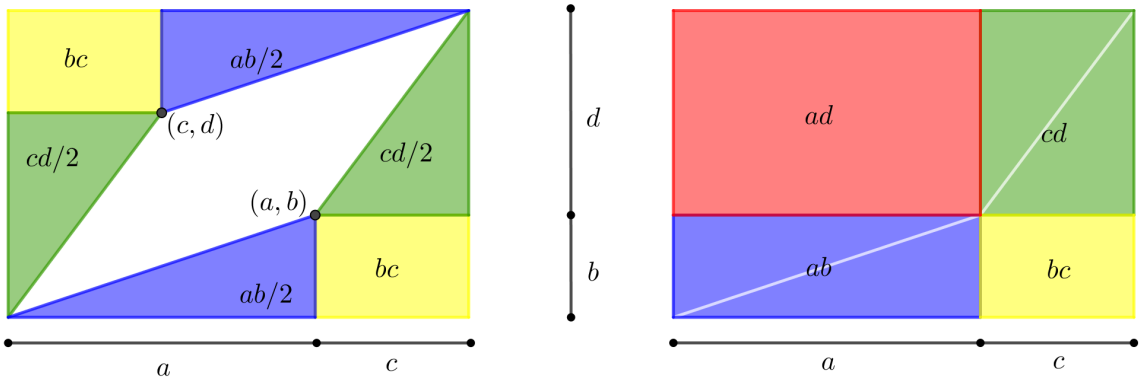
□

Vratimo se nakratko Primjeru 2.1. Determinanta para vektora $(87, 16)$ i $(32, 19)$ jednaka je $87 \cdot 19 - 16 \cdot 32 = 1141$ pa bi i determinanta para vektora $(1, -249)$ i $(0, 1141)$ također trebala biti jednaka 1141, što uistinu i jest, $1 \cdot 1141 - (-249) \cdot 0 = 1141$.

Geometrijska interpretacija determinante

Teorem 2.4 (Interpretacija determinante kao površine). *Neka su* (a, b) *i* (c, d) *nenul vektori. Pretpostavimo da je kut između vektora* (a, b) *i* (c, d) *(u pozitivnom smislu) manji od* $180°$*. Tada je determinanta* $ad - bc$ *jednaka površini paralelograma čije su stranice vektori* (a, b) *i* (c, d)*.*

Dokaz. Nacrtajmo pravokutnik duljina stranica $a+c$ i $b+d$ te ga podijelimo na dva različita načina na pravokutne trokute i pravokutnike kao na Slici 2.4.



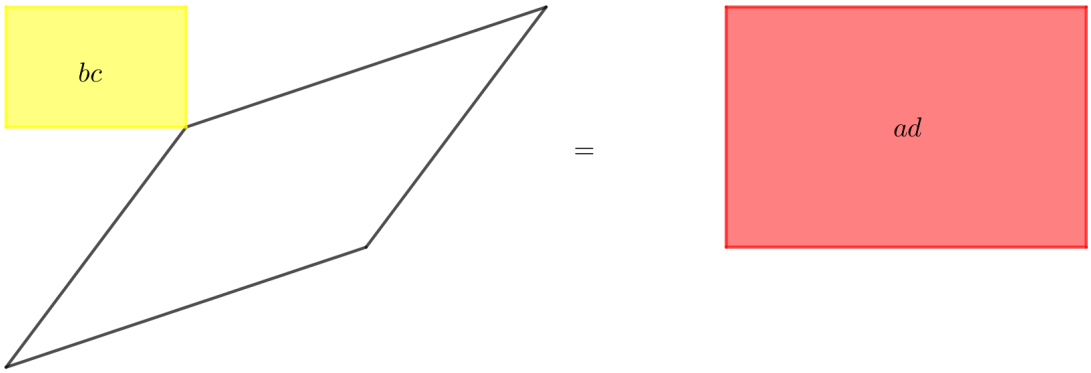
Slika 2.4: Teorem 2.4

Sa Slike 2.4 vidimo da dva plava trokuta površina $\frac{ab}{2}$ na lijevoj strani imaju jednaku površinu kao plavi pravokutnik, površine ab, na desnoj strani.

Isto vrijedi i za zelene trokute površina $\frac{cd}{2}$ na lijevoj strani i zeleni pravokutnik, površine cd, na desnoj strani.

Žuti pravokutnici u donjim desnim kutovima su jednaki, površine bc.

Tada preostali dijelovi, paralelogram i pravokutnik na lijevoj strani i pravokutnik na desnoj, moraju biti jednake površine.



Slika 2.5: Teorem 2.4

Oduzimanjem pravokutnika površine bc s obje strane, vidimo da je površina paralelograma jednaka $ad - bc$. □

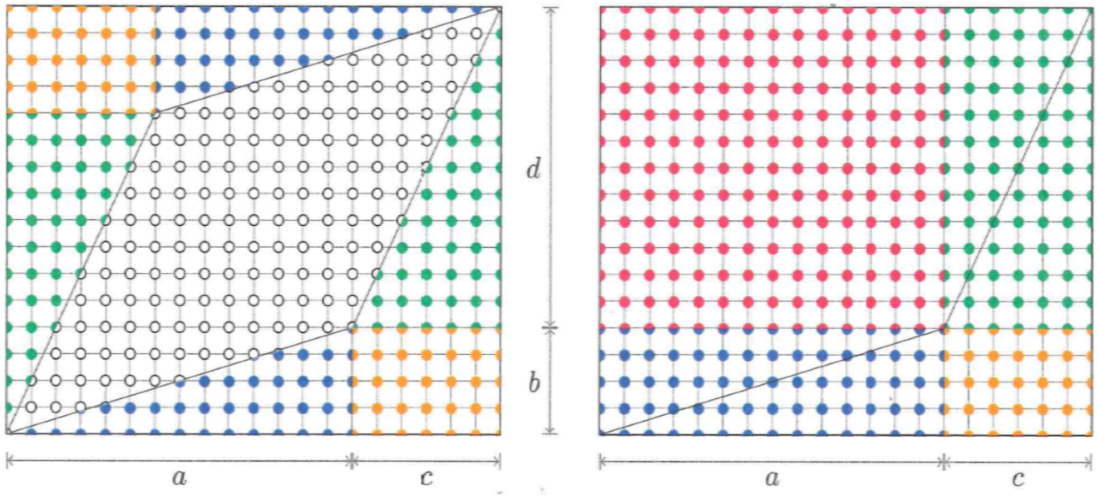
Što se događa s površinom paralelograma, odnosno determinantom, ako vektori (a, b) i (c, d) pripadaju istom pravcu?

Paralelogram se degenerira u dužinu, čija je površina jednaka 0 kao i determinanta, $\det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = 0$.

Da bismo izračunali determinantu, to jest površinu paralelograma, paralelogram možemo postaviti na cjelobrojnu mrežu točaka te površinu računamo brojanjem točaka unutar paralelograma. O toj metodi nam više govori sljedeći teorem.

Teorem 2.5 (**Pickov teorem za paralelograme**). *Neka je dan paralelogram u pravokutnom koordinatnom sustavu tako da su vrhovi paralelograma točke s cjelobrojnim koordinatama. Tada je površina paralelograma jednaka* $I + \frac{1}{2}E + 1$, *gdje je* I *broj točaka s cjelobrojnim koordinatama koje se nalaze unutar paralelograma, a* E *broj točaka kroz koje prolaze stranice paralelograma (ne uključujući vrhove).*

Dokaz. Nacrtajmo pravokutnik duljina stranica $a+c$ i $b+d$ pazeći da stranice paralelograma rasijecaju cjelobrojne točke koje su ovdje prikazane kao mali kružići.



Slika 2.6: Teorem 2.5

Plave i zelene točke na lijevoj strani Slike 2.6, cijele ili prepolovljene, mogu se posložiti i, ako je potrebno, spojiti tako da tvore plave i zelene točke na desnoj strani. Žutih točaka u donjim desnim kutovima ima jednak broj na obje strane slike.

Preostale točke, bijele i žute na lijevoj strani i crvene na desnoj, su jednakobrojne. Broj žutih točaka u gornjem lijevom kutu je

$$(c-1)(b-1) + (c-1) + (b-1) + 1 = bc.$$

Na isti način brojimo crvene točke na desnoj strani

$$(a-1)(d-1)+(a-1)+(d-1)+1=ad.$$

Stoga je broj bijelih točaka jednak broju crvenih točaka na desnoj strani umanjen za broj žutih na lijevoj i jednak je $ad-bc$, a to je po Teoremu 2.4 upravo površina paralelograma.

Broj bijelih točaka jednak je $I+\frac{1}{2}E+1$. Primijetimo da svaka točka presječena stranicama paralelograma daje polovicu bijele točke, dok vrhovi paralelograma zajedno tvore točno jednu bijelu točku.

Stoga je $I+\frac{1}{2}E+1=ad-bc$ površina paralelograma. □

2.2 Baza, primitivan i slab vektor

U rješavanju problema malih i velikih skokova vidjeli smo da kombinacijom tih osnovnih pomaka možemo doći do složenijih koji nam dopuštaju kretanje po svim cjelobrojnim točkama pravokutnog koordinatnog sustava. Takvi pomaci, odnosno parovi vektora, su nam od koristi te ćemo ih stoga definirati.

Definicija 2.2. *Neka su (a,b) i (c,d) vektori s cjelobrojnim koordinatama. Kažemo da ti vektori čine **bazu** ako kombinacijom malih skokova za vektore $\pm(a,b)$ i velikih skokova za vektore $\pm(c,d)$ možemo doći do svake točke pravokutnog koordinatnog sustava.*

Teorem 2.6 (Kriterij provjere baze pomoću determinante). *Neka su (a,b) i (c,d) vektori s cjelobrojnim koordinatama. Vektori (a,b) i (c,d) čine bazu ako i samo ako je*

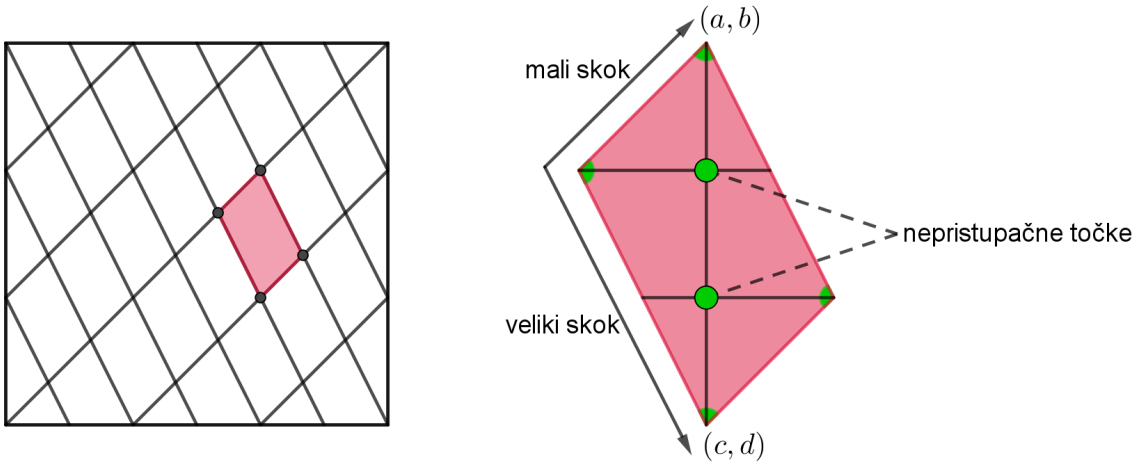
$$\det\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\{1,-1\}.$$

Dokaz. Cjelobrojne točke koordinatnog sustava u koje možemo doći malim i velikim skokovima za vektore $\pm(a,b)$ i $\pm(c,d)$ tvore mrežu paralelograma u ravnini. Kao u Pickovom teoremu, 2.5, sa I označavamo točke koje se nalaze unutar paralelograma, a s E označavamo točke kroz koje prolaze stranice istog. Obje vrste točaka, I i E, su nepristupačne u svakom paralelogramu, tj. ne možemo doći do njih pomoću malih i velikih skokova počevši iz ishodišta. Stoga vektori (a,b) i (c,d) čine bazu ako i samo ako vrijedi $I=0$ i $E=0$.

Postoje dva načina izražavanja površine paralelograma.

$$|\det\begin{pmatrix}a & b\\ c & d\end{pmatrix}|=Površina=I+\frac{1}{2}E+1.$$

Vektori (a,b) i (c,d) čine bazu ako i samo ako vrijedi $I=0$ i $E=0$, tj. ako i samo ako je $Površina=1$, tj. ako i samo ako je determinanta jednaka ±1. □



Slika 2.7: Mali skok za vektor $(1,1)$ i veliki za vektor $(1,-2)$ nam omogućuju kretanje po stranicama paralelograma. No, u unutrašnjosti svakog paralelograma su dvije nepristupačne točke. Upravo iz nepristupačnih točaka vidimo da je površina paralelograma veća od 1, točnije *Površina* $= |\det\left(\begin{smallmatrix}1 & 1\\ 1 & -2\end{smallmatrix}\right)| = |-3| = 3$, te vektori $(1,1)$ i $(1,-2)$ ne čine bazu.

Čine li dva vektora (a,b) i (c,d) bazu možemo provjeriti na više, međusobno ekvivalentnih, načina.

- *Algebarski*: $ad - bc = \pm 1$.
- *Geometrijski*: Površina paralelograma čije su stranice vektori (a,b) i (c,d) jednaka je 1.
- *Dinamički*: Koristeći male skokove za vektore $\pm(a,b)$ i velike za vektore $\pm(c,d)$ možemo se pomicati po svim cjelobrojnim točkama pravokutnog koordinatnog sustava.

No, ne mogu svi vektori biti dio neke baze. Na primjer, vektor $(3,6)$ neće nikad biti član neke baze, kao ni vektor $(9,-18)$. Zašto je tomu tako nam govori sljedeća propozicija.

Propozicija 2.7. *Vektor* (a,b) *je član neke baze ako i samo ako je* $\text{nzd}(a,b) = 1$*, tj. ako i samo ako je* (a,b) ***primitivan vektor***.

Za dokaz navedene propozicije, potreban nam je sljedeći teorem.

Teorem 2.8. *Neka su a, b, c cijeli brojevi i $d = \text{nzd}(a, b)$. Ako $d \nmid c$, onda jednadžba $ax + by = c$ nema cjelobrojnih rješenja. Ako $d \mid c$, onda jednandžba ima beskonačno mnogo rješenja. Ako je (x_1, y_1) jedno rješenje, onda su sva rješenja dana sa $x = x_1 + \frac{b}{d} \cdot t$, $y = y_1 - \frac{a}{d} \cdot t$, gdje je $t \in \mathbb{Z}$.*

Dokaz ovog teorema može se pronaći u skripti [4, str. 75]

Dokaz propozicije. Zadan je vektor (a, b) te tražimo odgovarajući vektor (c, d) koji sa zadanim vektorom čini bazu. Traženje vektora (c, d) ekvivalentno je rješavanju jednadžbe

$$ad - bc = \pm 1.$$

Uvođenjem supstitucija $x = d$ i $y = -c$ dobivamo linearnu diofantsku jednadžbu

$$ax + by = \pm 1. \tag{2.1}$$

Prema Teoremu 2.8 jednadžba (2.1) ima rješenje ako i samo ako je $\text{nzd}(a, b) = 1$. □

Primjer 2.2. *Odredimo neku bazu koja sadrži vektor* $(31, 13)$.

Rješenje: Prema prethodnoj propoziciji, rješavanje problema započinjemo rješavanjem diofantske jednadžbe $31x + 13y = 1$. Znamo da rješenje postoji jer je $\text{nzd}(31, 13) = 1$. Primjenom Euklidovog algoritma na 31 i 13 dobivamo

$$\begin{aligned} 31 &= 2 \cdot 13 + 5, \\ 13 &= 2 \cdot 5 + 3, \\ 5 &= 1 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Uvrštavajući unazad dobivamo

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (5 - 3) = 2 \cdot 3 - 5 \\ &= 2 \cdot (13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 5 \\ &= 2 \cdot 13 - 5 \cdot (31 - 2 \cdot 13) = 12 \cdot 13 - 5 \cdot 31. \end{aligned}$$

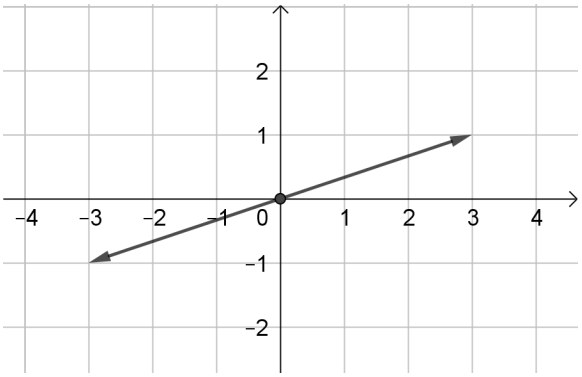
Iz jednakosti $1 = 12 \cdot 13 - 5 \cdot 31$, tj. $-1 = 5 \cdot 31 - 12 \cdot 13$ možemo odrediti vektor koji zajedno sa zadanim čini bazu. To je vektor $(12, 5)$. □

Proizvoljan vektor označavamo s $\vec{v}$. Vektor suprotan vektoru $\vec{v}$ dobivamo tako da promijenimo predznak objema koordinatama vektora $\vec{v}$. Na primjer, ako nam je zadan vektor $\vec{v} = (3, -4)$ njemu suprotan vektor je vektor $-\vec{v} = (-3, 4)$. Vektore zbrajamo (oduzimamo)

tako da zbrojimo (oduzmemo) x-koordinate i y-koordinate posebno. Ako su zadani vektori $\vec{v} = (2, 3)$ i $\vec{w} = (2, 4)$ tada je $\vec{v} + \vec{w} = (4, 7)$ i $\vec{v} - \vec{w} = (0, -1)$.

Bilo koji nenul vektor $\vec{v}$ u pravokutnom koordinatnom sustavu možemo prikazati tako da mu je početna točka $(0, 0)$, ishodište koordinatnog sustava. Na isti način prikazujemo par vektora $\{\vec{v}, -\vec{v}\}$, u oznaci $\pm\vec{v}$. Dakle, par vektora $\pm\vec{v}$ prikazujemo kao dva vektora jednake duljine i smjera, ali suprotne orijentacije s početnom točkom u ishodištu koordinatnog sustava. Takav par vektora, $\pm\vec{v}$, nazivamo *slabi vektor*.

Slabi vektor zapisujemo kao $\pm(x, y)$, gdje su x, y cijeli brojevi. Poželjno je da je x-koordinata pozitivan cijeli broj, ali nije pravilo. Ako je x-koordinata jednaka nuli, preferira se zapis $(0, y)$ u kojemu je y pozitivan.



Slika 2.8: Slabi vektor $\pm(3, 1)$.

Slaba baza je neuređeni par slabih vektora, $\{\pm\vec{v}, \pm\vec{w}\}$, od kojih svaka dva vektora, bez obzira na predznak, čine bazu.

Tako, primjerice, neuređeni par vektora $\{\pm(31, 13), \pm(12, 5)\}$ iz Primjera 2.2 čini slabu bazu.

2.3 Topograf domene

Topograf domene je grafički prikaz svih primitivnih slabih vektora, slabih baza te njihovih međusobnih veza.

U topografu domene slabu bazu prikazujemo dužinom (bridom topografa) koja razdvaja slabe vektore, članove navedene baze.

Na primjer, slabu bazu koju čine slabi vektori $\pm(x_1, y_1)$ i $\pm(x_2, y_2)$ prikazujemo kao

$$\frac{\pm(x_1, y_1)}{\pm(x_2, y_2)}.$$

Od svih slabih baza, izdvaja se jedna slaba baza, $\{\pm(1,0), \pm(0,1)\}$ koju nazivamo *osnovnom bazom*.

Nove baze nastaju zbrajanjem i oduzimanjem već postojećih baza.

Propozicija 2.9. *Pretpostavimo da vektori $\vec{v}$ i $\vec{w}$ čine bazu. Tada vrijedi da su i*

$$\{\vec{v}, \vec{v}+\vec{w}\}, \quad \{\vec{v}, \vec{v}-\vec{w}\}, \quad \{\vec{v}+\vec{w}, \vec{w}\}, \quad \{\vec{v}-\vec{w}, \vec{w}\} \quad \textit{baze}.$$

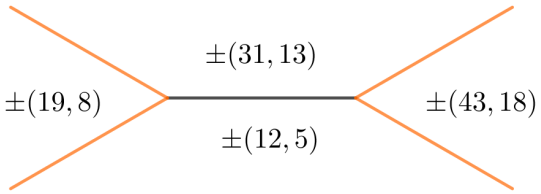
Dokaz. Da bismo dokazali da navedeni parovi vektora čine baze, koristimo se dinamičkom interpretacijom baze.

Ako vektori $\vec{v}$ i $\vec{w}$ čine bazu, tada kombinacijom malih skokova za vektor $\vec{v}$ i velikih skokova za vektor $\vec{w}$ možemo doći do bilo koje cjelobrojne točke koordinatnog sustava.

Iz rješenja problema malih i velikih skokova znamo da je doskok pomak dobiven spajanjem osnovnih pomaka, malog i velikog skoka. Očito su mali skokovi za vektor $\vec{v}$ i doskoci za vektor $\vec{v}+\vec{w}$ dovoljni pomaci pomoću kojih možemo doći do svake cjelobrojne točke. Iz toga slijedi da vektori $\{\vec{v}, \vec{v}+\vec{w}\}$ čine bazu.

Analogno pokazujemo preostala tri slučaja. □

Topograf domene prikazuje posljedice Propozicije 2.9. Svaka slaba baza, uz pomoć dva nova vektora, daje četiri **susjedne slabe baze**.



Slika 2.9: Grafički prikaz slabih vektora i baza iz Primjera 2.2. U sredini se nalaze dva slaba vektora $\pm(31,13)$ i $\pm(12,5)$ koji čine slabu bazu. S lijeve i desne strane su dva slaba vektora $\pm(19,8)$ i $\pm(43,18)$ dobivena oduzimanjem i zbrajanjem slabih vektora $\pm(31,13)$, $\pm(12,5)$. Narančastim dužinama su označene četiri nove slabe baze.

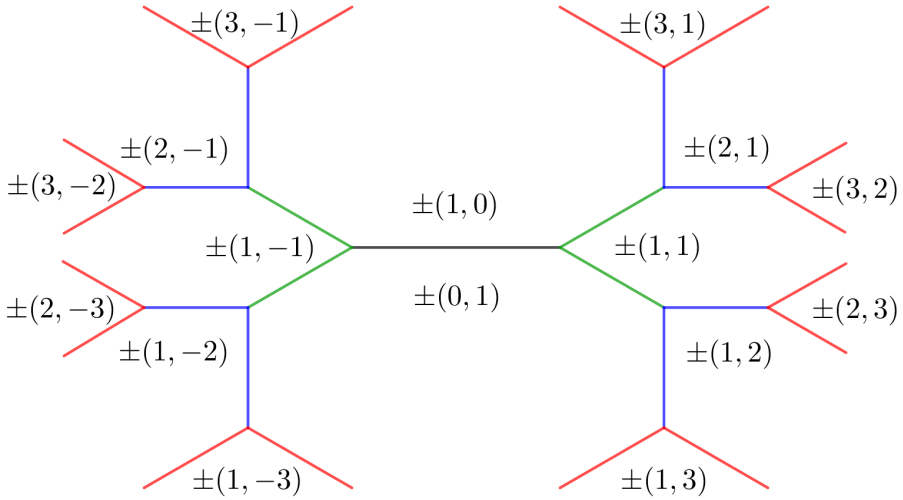
Topograf domene sadrži beskonačno mnogo slabih baza. Iz Propozicije 2.9 znamo da zbrajanjem i oduzimanjem slabih baza dobivamo nove slabe baze te na taj način granamo topograf.

Na sljedećoj Slici 2.10, vidimo grananje topografa domene koje smo započeli od osnovne baze $\pm(1,0)$ i $\pm(0,1)$. Zbrajanjem i oduzimanjem slabih vektora koji čine osnovnu bazu dobivamo dva nova slaba vektora, $\pm(1,1)$ i $\pm(1,-1)$ i četiri nove slabe baze, označene zelenim dužinama. Zbrajanjem i oduzimanjem svih četiriju slabih vektora dobivamo još

četiri nova slaba vektora $\pm(2,1)$, $\pm(1,2)$, $\pm(2,-1)$, $\pm(1,-2)$ i osam novih slabih baza označenih plavim dužinama. Ako još jednom ponovimo ovaj postupak zbrajanja i oduzimanja, dobivamo osam novih slabih vektora $\pm(3,1)$, $\pm(3,2)$, $\pm(2,3)$, $\pm(1,3)$, $\pm(3,-1)$, $\pm(3,-2)$, $\pm(2,-3)$, $\pm(1,-3)$ i šesnaest novih slabih baza označenih crvenim dužinama.

Dakle, počevši s osnovnom bazom proširili smo topograf domene tri puta, rekurzivno, te dobili 29 slabih baza između 16 slabih vektora.

Primijetimo da je determinanta bilo kojeg para slabih vektora, koje dijeli jedna dužina, jednaka ± 1.



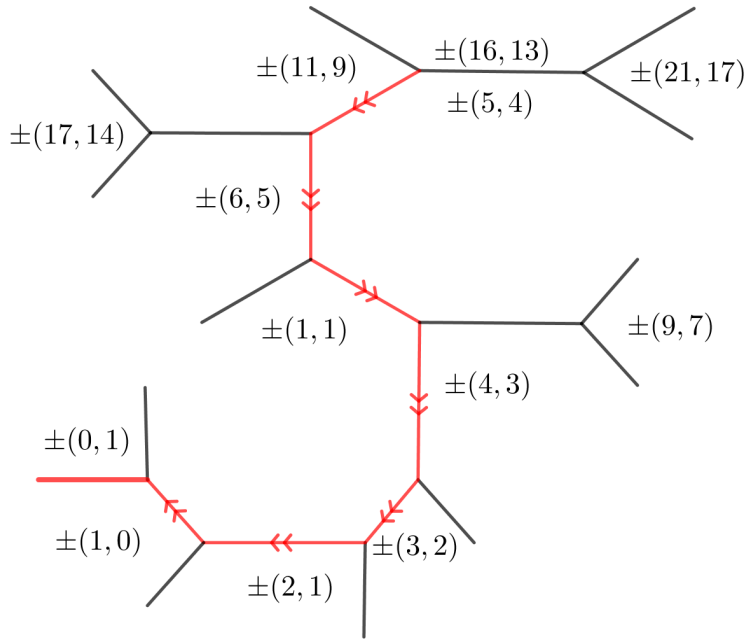
Slika 2.10: Grananje topografa domene.

Topograf domene sadrži sve slabe baze. Ako krenemo od osnovne baze, grananjem ćemo pronaći sve slabe baze. U sljedećem primjeru ćemo pokazati kako od bilo koje slabe baze šetnjom po topografu možemo doći do osnovne baze $\{\pm(1,0), \pm(0,1)\}$. Obrnuvši dobiveni put nalazimo kako iz osnovne baze doći do odabrane slabe baze.

Primjer 2.3. *Krećući se bridovima topografa, pronađimo put od slabe baze* $\{\pm(16,13), \pm(5,4)\}$ *do osnovne baze.*

Rješenje: Nacrtajmo bridove slabih baza susjednih zadanoj bazi $\{\pm(16,13), \pm(5,4)\}$. Primijetimo da se koordinate slabih vektora smanjuju ako se krećemo prema donjem lijevom kutu zato sada promatramo slabu bazu $\{\pm(11,9), \pm(5,4)\}$ i docrtavamo bridove njoj susjednih slabih baza. Ponavljamo ovaj postupak praćenja manjih koordinata vektora i docrtavanja bridova susjednih baza sve dok ne dođemo do osnovne baze $\{\pm(1,0), \pm(0,1)\}$.

Kada dođemo do osnovne baze prekidamo postupak te je zadatak izvršen. □



Slika 2.11: Prikaz puta u topografu domene od slabe baze $\{\pm(16,13), \pm(5,4)\}$ do osnovne baze $\{\pm(1,0), \pm(0,1)\}$.

Povezanost topografa domene nam omogućuje kretanje od bilo koje slabe baze do osnovne baze.

Teorem 2.10. *Topograf je povezan, tj. postoji put od bilo koje slabe baze do osnovne baze.*

Za dokaz ovog teorema, potrebna nam je sljedeća lema.

Lema 2.11. *Ako je $\{\vec{v}, \vec{w}\}$ baza, tada primjenom Euklidovog algoritma na vektore $\vec{v}$ i $\vec{w}$ dobivamo bazu oblika $\{\pm(1,s), \pm(0,1)\}$.*

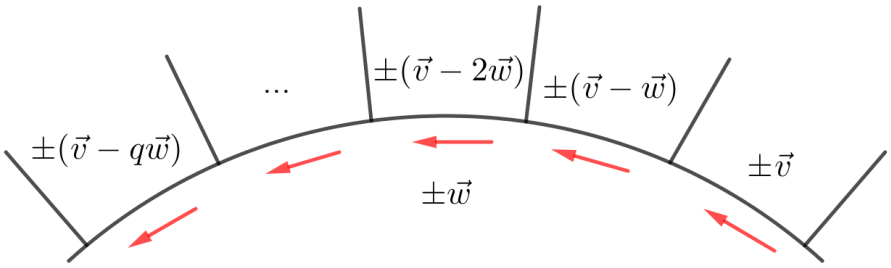
Dokaz. Pretpostavimo da je $\vec{v} = (a,b)$ i $\vec{w} = (c,d)$. Budući da je $\{\vec{v}, \vec{w}\}$ baza, znamo da je $ad - bc = \pm 1$. Upravo zato je $x = d$, $y = -b$ rješenje diofantske jednadžbe $ax + cy = \pm 1$, te je $\text{nzd}(a,c) = 1$.

Sada primijenimo Euklidov algoritam na x-koordinate vektora $\pm\vec{v}$ i $\pm\vec{w}$. Znamo da je $\text{nzd}(a,c) = 1$ pa su zadnja dva vektora, koja dobivamo primjenom Euklidovog algoritma, oblika $(1,s)$ i $(0,t)$ za neke cijele brojeve s i t. No, apsolutna vrijednost determinante se ne mijenja kroz Euklidov algoritam te dobivamo

$$\pm 1 = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det\begin{pmatrix} 1 & s \\ 0 & t \end{pmatrix} = t.$$

Stoga je $t = \pm 1$ i tvrdnja je dokazana. □

Dokaz teorema. Neka je $\{\pm\vec{v}, \pm\vec{w}\}$ slaba baza. Primijenimo Euklidov algoritam na vektore $\vec{v}$ i $\vec{w}$. Svaki korak Euklidovog algoritma odgovara jednom luku u topografu domene. Korak $\vec{v} = q \cdot \vec{w} + \vec{r}$ odgovara luku topografa na Slici 2.12 od slabe baze $\{\pm\vec{v}, \pm\vec{w}\}$ do $\{\pm\vec{w}, \pm\vec{r}\}$.

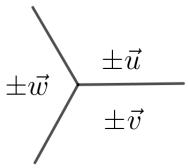


Slika 2.12: Teorem 2.10

Prema Lemi 2.11, od slabe baze $\{\pm\vec{v}, \pm\vec{w}\}$ do $\{\pm(1, s), \pm(0, 1)\}$ možemo doći nizom ovakvih lukova. Primijetimo da je $(1, s) = s \cdot (0, 1) + (1, 0)$. Stoga još jedan luk u topografu domene vodi do osnovne baze. □

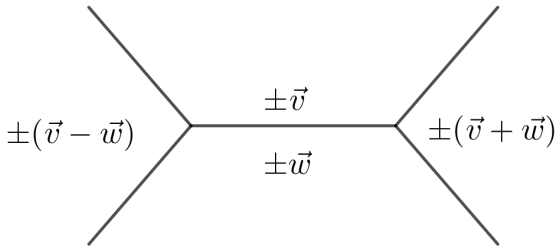
Beskonačan topograf domene je nemoguće nacrtati na papiru pa se fokusiramo na njegove manje elemente: *vrhove (ili čvorove), bridove i područja.*

Vrh je točka u kojoj se sastaju bridovi topografa. Ako se fokusiramo na jedan vrh, uočavamo tzv. *trobrid*. Svaki trobrid okružuju tri slaba vektora od kojih bilo koja dva čine slabu bazu. Takvu ćemo trojku nazivati slabom superbazom.



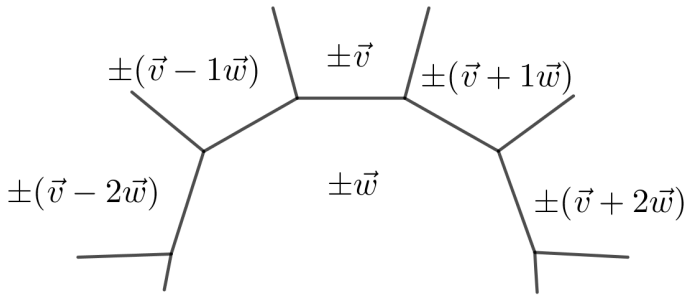
Slika 2.13: Trobrid s trima slabim vektorima $\pm\vec{u}$, $\pm\vec{v}$, $\pm\vec{w}$ i trima slabim bazama.

Ako obratimo pažnju na jedan brid topografa, vidimo *ćeliju*. U svakoj ćeliji se nalaze četiri slaba vektora, $\pm\vec{v}$, $\pm\vec{w}$, $\pm(\vec{v}-\vec{w})$, $\pm(\vec{v}+\vec{w})$, pet slabih baza i dva trobrida.



Slika 2.14: Ćelija s četirima slabim vektorima i pet slabih baza.

Gledajući jedno *područje* topografa, uočavamo lik kojeg nazivamo *beskonačnim poligonom*. U području vidimo slabi vektor $\pm\vec{w}$ te beskonačan niz slabih vektora oblika $\pm(\vec{v}+n\vec{w})$, gdje je $n \in \mathbb{Z}$.



Slika 2.15: Jedan dio beskonačnog poligona.

Vratimo se spomenutom pojmu superbaze. J. H. Conway je osmislio superbazu koju koristimo u proučavanju presjeka baza te u praćenju orijentacije unutar topografa domene. Kako razlikujemo vektore i slabe vektore, tako razlikujemo *jaku* i *slabu* superbazu.

Definicija 2.3. ***Jaka superbaza*** *je neuređena trojka vektora* $\{\vec{u}, \vec{v}, \vec{w}\}$ *za koje vrijedi* $\vec{u}+\vec{v}+\vec{w}=0$*, te bilo koja dva vektora čine bazu.*

Prema Propoziciji 2.9, uvjet da vektori $\vec{u}$ i $\vec{v}$ čine bazu te da vrijedi $\vec{u}+\vec{v}+\vec{w}=0$ povlači da vektori $\vec{u}$ i $\vec{w}$ čine bazu, kao i vektori $\vec{v}$ i $\vec{w}$.

Lema 2.12. *Ako bilo koja dva slaba vektora iz skupa* $\{\pm\vec{u}, \pm\vec{v}, \pm\vec{w}\}$ *čine slabu bazu, tada vrijedi* $\pm\vec{u}\pm\vec{v}\pm\vec{w}=0$ *za određeni izbor predznaka.*

Dokaz. Neka je $\{\vec{v}, \vec{w}\}$ baza te $\vec{v} = (a, b)$ i $\vec{w} = (c, d)$. Ako $\vec{u} = (x, y)$ čini bazu s oba vektora, $\vec{v}$ i $\vec{w}$, tada je

$$bx - ay = \pm 1 \quad i \quad dx - cy = \pm 1.$$

Navedene četiri jednadžbe su jednadžbe četiriju pravaca; dva pravca s koeficijentom smjera $\frac{b}{a}$ i dva pravca s koeficijentom smjera $\frac{d}{c}$. Sjecišta tih četiriju pravaca su vrhovi paralelograma koji određuju točno četiri moguća vektora $\vec{u}$ (odnosno dva para slabih vektora).

S druge strane, sva četiri vektora $\vec{u} = \pm\vec{v} \pm \vec{w}$ zadovoljavaju uvjet leme, tj. čine bazu s oba zadana vektora, $\vec{v}$ i $\vec{w}$.

Stoga, ako $\{\pm\vec{u}, \pm\vec{v}, \pm\vec{w}\}$ zadovoljava pretpostavku leme, tada je $\vec{u} = \pm\vec{v} \pm \vec{w}$ za određeni izbor predznaka, iz čega slijedi tvrdnja. □

Definicija 2.4. ***Slaba superbaza*** *je neuređena trojka slabih vektora* $\{\pm\vec{u}, \pm\vec{v}, \pm\vec{w}\}$ *od kojih svaka dva čine slabu bazu.*

Uočimo da prema Lemi 2.12 svaka slaba superbaza nastaje iz jake superbaze, točnije, nastaje iz točno dvije jake superbaze. Ako je $\{\vec{u}, \vec{v}, \vec{w}\}$ jaka superbaza, tada od osam mogućih odabira predznaka u $\{\pm\vec{u}, \pm\vec{v}, \pm\vec{w}\}$, jedino odabir svih pozitivnih ili svih negativnih predznaka daje jaku superbazu.

Orijentacija topografa domene ovisi o njegovom početku, tj. slaboj bazi od koje granamo topograf. Ako krećemo od osnovne baze, te vektor $\pm(1, 1)$ postavljamo zdesna osnovne baze, time je određena orijentacija svake slabe superbaze.

Drugim riječima, za svaku slabu superbazu $\{\pm\vec{u}, \pm\vec{v}, \pm\vec{w}\}$, tri slaba vektora su smještena oko jednog vrha topografa ili u smjeru kazaljke na satu ili u obrnutom smjeru.

No, postavlja se pitanje kako pronaći orijentaciju slabe superbaze ako topograf ne počinjemo granati od osnovne baze?

Lema 2.13. *Pretpostavimo da je* $\{\vec{u}, \vec{v}, \vec{w}\}$ *jaka superbaza gdje je* $\vec{u} = (a, b)$, $\vec{v} = (c, d)$ *i* $\vec{w} = (e, f)$. *Tada su determinante svih triju parova vektora međusobno jednake*

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det\begin{pmatrix} c & d \\ e & f \end{pmatrix} = \det\begin{pmatrix} e & f \\ a & b \end{pmatrix}.$$

Dokaz. Uvjeti jake superbaze, $a + c + e = 0$ i $b + d + f = 0$, povlače $e = -a - c$ i $f = -b - d$. Stoga vrijedi $\det\left(\begin{smallmatrix} c & d \\ e & f \end{smallmatrix}\right) = cf - de = c(-b - d) - d(-a - c) = ad - bc$.

Pogledajmo sada determinantu para vektora $\vec{w} = (e, f)$ i $\vec{u} = (a, b)$,

$$\det\left(\begin{smallmatrix} e & f \\ a & b \end{smallmatrix}\right) = eb - fa = (-a - c)b - (-b - d)a = ad - bc.$$

Dakle, $\det\left(\begin{smallmatrix} e & f \\ a & b \end{smallmatrix}\right) = \det\left(\begin{smallmatrix} c & d \\ e & f \end{smallmatrix}\right) = \det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = ad - bc$, čime je tvrdnja dokazana. □

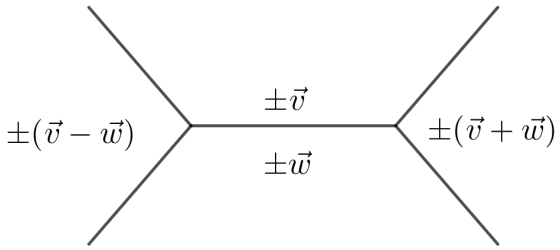
Teorem 2.14 (**Orijentacija topografa domene pomoću determinanti**). *U svakom vrhu topografa domene odaberimo predznake slabih vektora kako bismo formirali jake superbaze. Tada su sve determinante u smjeru obrnutom od kazaljke na satu, jednake* 1.

Dokaz. Moguća su samo dva izbora predznaka kojima iz slabe superbaze dobivamo jaku superbazu. Determinante koje tako dobivamo su međusobno jednake.

Ako gledamo osnovnu bazu, jaka superbaza sadrži vektore $(1,0)$, $(0,1)$ i $(-1,-1)$ te su determinante parova vektora, u smjeru obrnutom od kazaljke na satu, jednake 1,

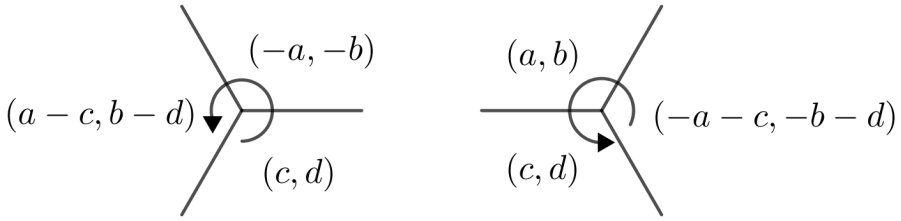
$$\det\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \det\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix} = \det\begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix} = 1.$$

Pogledajmo sada jednu ćeliju u topografu domene, gdje je $\vec{v} = (a,b)$ i $\vec{w} = (c,d)$.



Slika 2.16: Jedna ćelija topografa domene.

Da bismo formirali jaku superbazu trebamo odabrati predznake slabih vektora kao na Slici 2.17.



Slika 2.17: Izbor predznaka slabih vektora za formiranje jake superbaze.

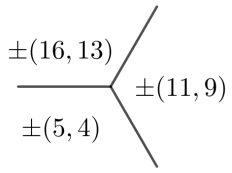
Izravnim računanjem determinanti parova vektora, vidimo da vrijedi

$$\det\begin{pmatrix}c & d\\ -a & -b\end{pmatrix} = \det\begin{pmatrix}a & b\\ c & d\end{pmatrix}.$$

Dakle, determinante parova vektora, u smjeru obrnutom od kazaljke na satu, u oba trobrida su jednake. Budući da je topograf domene povezan, možemo doći iz jednog trobrida u drugi pa su sve determinante parova vektora, u smjeru obrnutom od kazaljke na satu, jednake 1. □

Primjer 2.4. *Odredimo orijentaciju slabe superbaze* $\{\pm(16,13), \pm(5,4), \pm(11,9)\}$ *u topografu domene.*

Rješenje: Prvo odabiremo predznake slabih vektora tako da čine strogu superbazu: $(-16,-13)$, $(5,4)$, $(11,9)$. Determinanta para vektora $(5,4)$ i $(11,9)$ iznosi $\det\left(\begin{smallmatrix}5 & 4\\ 11 & 9\end{smallmatrix}\right) = 45 - 44 = 1$, stoga smjer kretanja, oko vrha, od slabog vektora $\pm(5,4)$ do $\pm(11,9)$ mora biti suprotan od smjera kazaljke na satu. □



Slika 2.18: Za slabu superbazu $\{\pm(16,13), \pm(5,4), \pm(11,9)\}$ u topografu domene od vektora $(5,4)$ do $(11,9)$ krećemo se u smjeru suprotnom od smjera kazaljke na satu.

Pogledajmo sada kako neke transformacije vektora utječu na topograf.

Matricu $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ možemo promatrati kao transformaciju vektora. Transformacija vektora (x,y) pomoću matrice M određena je pravilom da se (x,y) preslikava u

$$(x,y) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ax + cy, bx + dy).$$

Posebno, ako vektor $(1,0)$ transformiramo pomoću matrice $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, dobivamo vektor (a,b). Isto tako se vektor $(0,1)$ transformira u vektor (c,d).

Lema 2.15. *Neka je M matrica i neka su $\vec{v}$ i $\vec{w}$ vektori. Pretpostavimo da M preslikava vektore $\vec{v}$ i $\vec{w}$ redom u vektore $\vec{v}'$ i $\vec{w}'$. Tada M preslikava vektor $\vec{v} \pm \vec{w}$ u vektor $\vec{v}' \pm \vec{w}'$.*

Dokaz. Neka je $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $\vec{v} = (x,y)$ i $\vec{w} = (s,t)$. Tada M transformira $\vec{v}$ u vektor $(ax+cy, bx+dy)$, a $\vec{w}$ u vektor $(as+ct, bs+dt)$. Također, M transformira vektor $(x \pm s, y \pm t)$ u vektor $(a(x \pm s) + c(y \pm t), b(x \pm s) + d(y \pm t))$. Zbrajanjem ili oduzimanjem vektora slijedi tvrdnja

$$\begin{aligned}(ax + cy, bx + dy) \pm (as + ct, bs + dt)& \\ = (a(x \pm s) + c(y \pm t), b(x \pm s) + d(y \pm t)).&\end{aligned}$$

Drugim riječima matrica M predstavlja linearni operator. □

Automorfizam je matrica M s cjelobrojnim elementima čija determinanta iznosi ± 1. Ako je M automorfizam, tada M preslikava osnovnu bazu u neku drugu slabu bazu, čiji su vektori redovi matrice M. Takve matrice transformiraju topograf domene.

Propozicija 2.16. *Neka je M automorfizam i $\{\vec{v}, \vec{w}\}$ baza. Pretpostavimo da M preslikava vektor $\vec{v}$ u vektor $\vec{v}'$ i vektor $\vec{w}$ u vektor $\vec{w}'$. Tada je $\{\vec{v}', \vec{w}'\}$ također baza.*

Dokaz. Neka je $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ automorfizam i $\{\vec{v}, \vec{w}\}$ baza. Tada kombinacijom malog skoka za vektor $\vec{v}$ i velikog skoka za vektor $\vec{w}$ možemo dobiti vektor $(1, 0)$. Automorfizmom M transformiramo vektor $(1, 0)$ u vektor (a, b). Prema Lemi 2.15 prvo smo mogli provesti transformaciju vektora $(1, 0)$, a zatim kombinacijom malih i velikih skokova za $\vec{v}'$ i $\vec{w}'$ dobiti vektor (a, b).

Na isti način, kombinacijom malog skoka za vektor $\vec{v}$ i velikog skoka za vektor $\vec{w}$ možemo dobiti vektor $(0, 1)$. Tada automorfizmom M transformiramo vektor $(0, 1)$ u vektor (c, d). Dakle, kao i prije, prema Lemi 2.15 kombinacijom malih i velikih skokova za vektore $\vec{v}'$ i $\vec{w}'$ možemo dobiti vektor (c, d).

Kako je $\det M = \pm 1$, neuređeni par vektora $\{(a, b), (c, d)\}$ čini bazu. Budući da malim skokom za vektor $\vec{v}'$ i velikim skokom za vektor $\vec{w}'$ možemo dobiti oba vektora baze, (a, b) i (c, d), to tim pomacima možemo doći do bilo koje cjelobrojne točke koordinatnog sustava. Slijedi da je $\{\vec{v}', \vec{w}'\}$ baza. □

Korolar 2.17. *Neka je M automorfizam i $\vec{v}$ primitivan vektor. Tada M preslikava $\vec{v}$ u primitivan vektor.*

Dokaz. Primitivan vektor $\vec{v}$ čini bazu s nekim vektorom $\vec{w}$. Ako M preslikava $\vec{v}$ u $\vec{v}'$ i $\vec{w}$ u $\vec{w}'$, tada par vektora $\{\vec{v}', \vec{w}'\}$ također čini bazu. Dakle, vektor $\vec{v}'$ je primitivan vektor. □

Korolar 2.18. *Ako je $\{\vec{u}, \vec{v}, \vec{w}\}$ superbaza i automorfizam M preslikava $\vec{u}$ u $\vec{u}'$, $\vec{v}$ u $\vec{v}'$ i $\vec{w}$ u $\vec{w}'$, tada je $\{\vec{u}', \vec{v}', \vec{w}'\}$ superbaza.*

Dokaz. Prema Propoziciji 2.16 neuređena trojka $\{\pm\vec{u}', \pm\vec{v}', \pm\vec{w}'\}$ je slaba superbaza. Štoviše, izbor predznaka slabih vektora daje jaku superbazu: budući da je $\vec{u} + \vec{v} + \vec{w} = (0, 0)$ i M preslikava $(0, 0)$ u $(0, 0)$, vidimo da M preslikava $\vec{u} + \vec{v} + \vec{w}$ u $(0, 0)$. Prema Lemi 2.15 slijedi da je $\vec{u}' + \vec{v}' + \vec{w}' = (0, 0)$. □

Ako su A i B automorfizmi, tada postoji automorfizam C koji je kompozicija automorfizama A i B. Dakle, ako A preslikava vektor $\vec{v}$ u $\vec{v}'$ i B preslikava vektor $\vec{v}'$ u $\vec{v}''$ tada C direktno preslikava $\vec{v}$ u $\vec{v}''$.

Ako je M automorfizam, tada postoji automorfizam N za koji vrijedi sljedeće: ako M preslikava vektor $\vec{v}$ u vektor $\vec{v}'$, tada N preslikava vektor $\vec{v}'$ natrag u vektor $\vec{v}$. Automorfizam N nazivamo **inverznim automorfizmom**.

Automorfizmi preslikavaju područja u područja, bridove u bridove, trobride u trobride i ćelije u ćelije. Upravo zbog toga je topograf domene uniforman, posvuda izgleda jednako.

Teorem 2.19 (**Uniformnost topografa**). *Neka su* $\{\vec{u}, \vec{v}, \vec{w}\}$ *i* $\{\vec{u}', \vec{v}', \vec{w}'\}$ *dvije jake superbaze u topografu domene. Tada postoji automorfizam koji preslikava* $\vec{u}$ *u* $\vec{u}'$, $\vec{v}$ *u* $\vec{v}'$ *i* $\vec{w}$ *u* $\vec{w}'$.

Dokaz. Neka je $\vec{u} = (a, b)$ i $\vec{v} = (c, d)$. Tada $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ preslikava osnovnu bazu u bazu $\{\vec{u}, \vec{v}\}$. Slijedi da vektor $(-1, -1)$ matrica M preslikava u vektor $\vec{w} = (-a - c, -b - d)$.

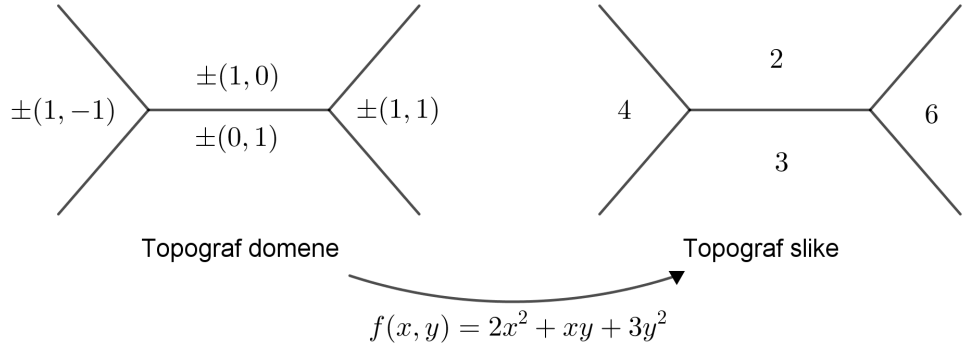
Stoga, postoji automorfizam M koji preslikava osnovni trobrid $\{(1, 0), (0, 1), (-1, -1)\}$ u $\{\vec{u}, \vec{v}, \vec{w}\}$. Također, postoji i automorfizam M' koji preslikava osnovni trobrid u $\{\vec{u}', \vec{v}', \vec{w}'\}$. Neka je N automorfizam inverzan automorfizmu M. Tada je traženi automorfizam kompozicija automorfizama N i M'. □

2.4 Topograf slike

Topograf slike je grafički prikaz binarnih kvadratnih formi koji je osmislio J. H. Conway.

U potpoglavlju 1.3 *Reprezentacija cijelog broja*, spomenuli smo da ako neki cijeli broj n želimo reprezentirati kvadratnom formom $f(x, y) = ax^2 + bxy + cy^2$, tada zapravo rješavamo diofantsku jednadžbu $ax^2 + bxy + cy^2 = n$. U ovom potpoglavlju ćemo grafički prikazivati rješenja diofantskih jednadžbi koristeći topograf slike.

Za proizvoljnu kvadratnu formu $f(x, y)$, topograf slike dobivamo crtanjem topografa domene i označavanjem područja ne primitivnim slabim vektorima $\pm\vec{v}$, već cijelim brojevima $f(\pm\vec{v})$.



Slika 2.19: Topograf slike binarne kvadratne forme $f(x, y) = 2x^2 + xy + 3y^2$. Uvrštavajući slabe vektore osnovne baze i vektore njoj susjednih slabih baza u formu f dobivamo $f(1, 0) = 2$, $f(0, 1) = 3$, $f(1, 1) = 6$, $f(1, -1) = 4$.

Pogledajmo topograf slike kvadratne forme $f(x, y) = 2x^2 - 2y^2$ na Slici 2.20.

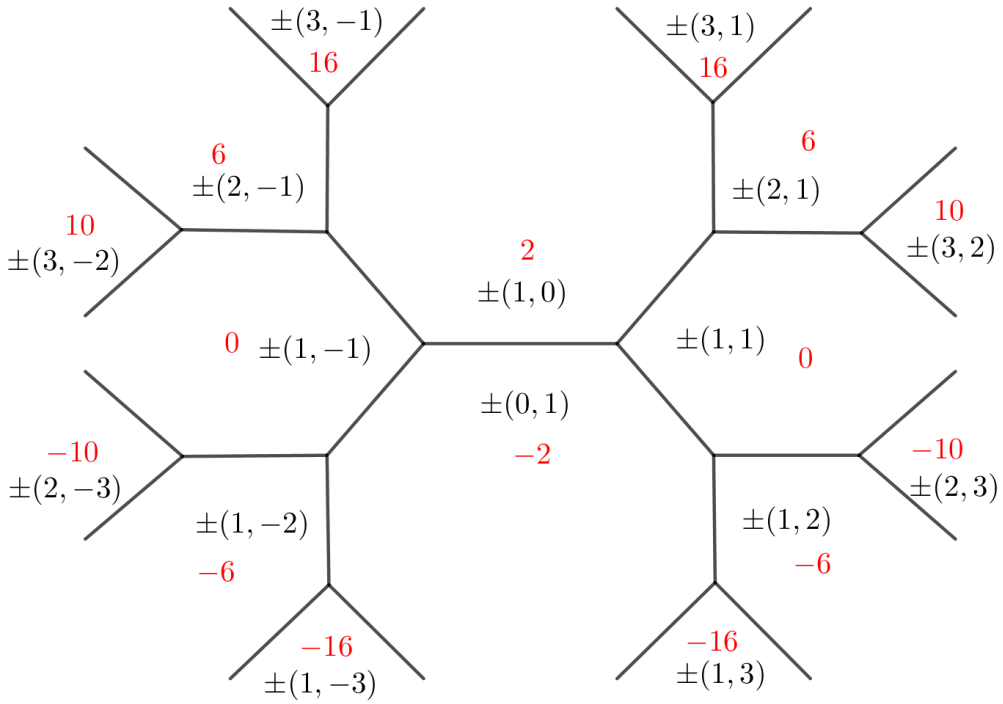
Vidimo da postoje dvije simetrije topografa slike. Simetrija s obzirom na vertikalni pravac preslikava lijevu u desnu stranu topografa slike i obratno te vidimo da su vrijednosti u simetričnim područjima jednake. Osno simetrična područja s obzirom na horizontalni pravac sadrže vrijednosti koje su suprotnog predznaka.

Ove dvije simetrije topografa slike odražavaju sljedeća dva svojstva kvadratne forme $f(x, y) = 2x^2 - 2y^2$.

1. Promjena predznaka bilo koje koordinate, x ili y, ne mijenja formu $f(x, y)$. Drugim riječima $f(x, y) = f(x, -y)$.

2. Zamjena x i y koordinate mijenja predznak forme $f(x, y)$. Vrijedi $f(x, y) = -f(y, x)$.

Da bismo prepoznali još ovakvih svojstava unutar topografa slike, trebamo proučiti manje elemente topografa, trobride, ćelije i beskonačne poligone.



Slika 2.20: Šesnaest područja topografa domene uz osnovnu bazu i odgovarajuće vrijednosti u topografu slike kvadratne forme $f(x, y) = 2x^2 - 2y^2$.

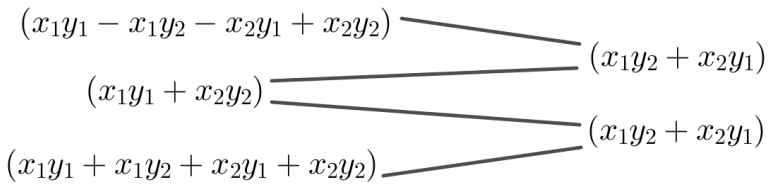
Ćelija u topografu slike sadrži četiri cijela broja od kojih bilo koja tri određuju četvrti, koristeći Conwayevo *pravilo aritmetičkog niza*. Da bismo dokazali ovo pravilo koristit ćemo sljedeću lemu.

Lema 2.20. *Neka su x_1, x_2, y_1, y_2 realni brojevi. Tada je niz*

$$(x_1 - x_2)(y_1 - y_2), \quad x_1y_1 + x_2y_2, \quad (x_1 + x_2)(y_1 + y_2)$$

aritmetički niz s razlikom $d = x_1y_2 + x_2y_1$.

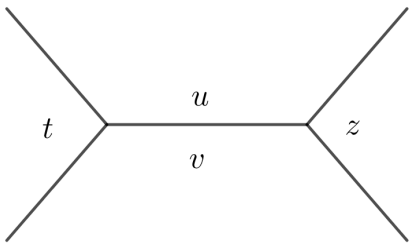
Dokaz. Na Slici 2.21 u lijevom stupcu se nalaze raspisani članovi niza, dok se u desnom stupcu nalaze razlike dvaju susjednih članova tog niza.



Slika 2.21: Lema 2.20

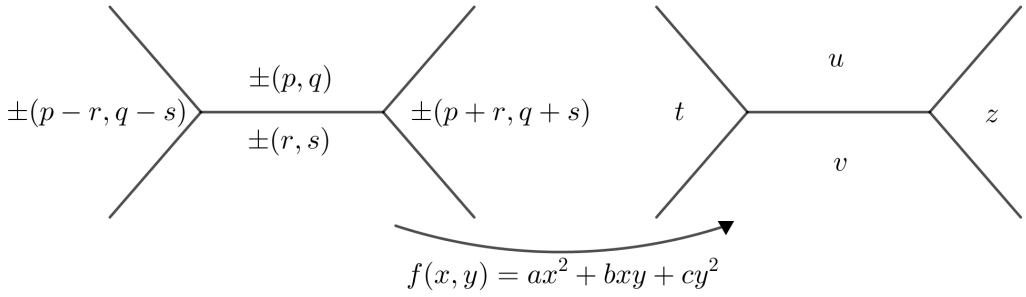
□

Teorem 2.21 (**Pravilo aritmetičkog niza**). *U svakoj ćeliji topografa slike neke binarne kvadratne forme, uz oznake kao na Slici 2.22, brojevi t, (u + v), z čine aritmetički niz.*



Slika 2.22: Ćelija topografa slike neke binarne kvadratne forme.

Dokaz. Neka je $f(x, y) = ax^2 + bxy + cy^2$ binarna kvadratna forma. Promotrimo ćeliju topografa domene koja sadrži slabu bazu $\{\pm(p, q), \pm(r, s)\}$ te pridruženu ćeliju topografa slike.



Slika 2.23: Ćelija topografa domene i pridružena ćelija topografa slike.

Vrijednosti t, $u + v$ i z su navedene u sljedećoj tablici na Slici 2.24.

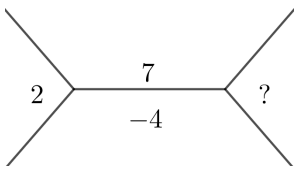
$f(x,y) =$	ax^2	$+$	bxy	$+$	cy^2
$t =$	$a(p-r)^2$	$+$	$b(p-r)(q-s)$	$+$	$c(q-s)^2$
$u+v =$	$a(p^2+r^2)$	$+$	$b(pq+rs)$	$+$	$c(q^2+s^2)$
$z =$	$a(p+r)^2$	$+$	$b(p+r)(q+s)$	$+$	$c(q+s)^2$

Slika 2.24: Vrijednosti t, $u + v$ i z.

Lema 2.20 povlači da tri stupca u tablici, plavi, crveni i zeleni čine aritmetičke nizove. Zbroj triju aritmetičkih nizova je ponovo aritmetički niz, stoga t, $u + v$ i z čine aritmetički niz. □

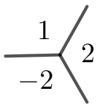
Pravilo aritmetičkog niza nam dopušta brzo skiciranje topografa slike sa samo tri zadane vrijednosti.

Primjer 2.5. *Koristeći pravilo aritmetičkog niza odredimo vrijednost koja nedostaje u ćeliji na Slici 2.25.*



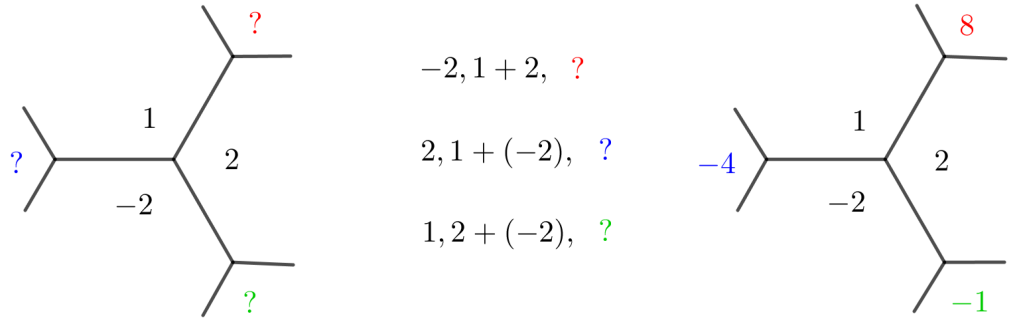
Slika 2.25: Ćelija topografa slike kojoj nedostaje jedna vrijednost.

Rješenje: Prema pravilu aritmetičkog niza, niz brojeva 2, (7 + (−4)) i ? mora biti aritmetički. Stoga, vrijednost ? u aritmetičkom nizu 2, 3, ? iznosi 4. □

Primjer 2.6. *Skicirajmo topograf slike koji sadrži trobrid* 

.

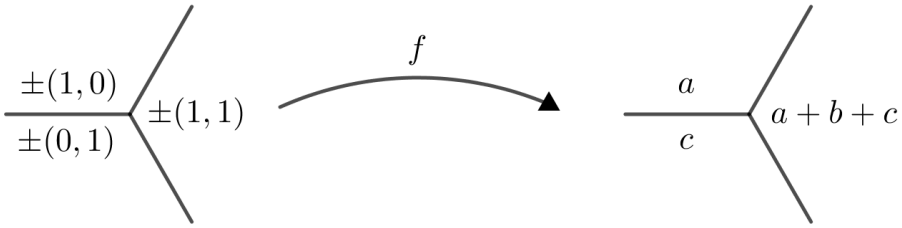
Rješenje: Da bismo skicirali traženi topograf, moramo odrediti tri nepoznate vrijednosti sa Slike 2.26 tako da čine aritmetičke nizove s već zadanim vrijednostima u trobridu. □



Slika 2.26:

Na ovaj način topograf slike možemo proširiti u beskonačnost.

Svaka trojka cijelih brojeva se pojavljuje u trobridu topografa slike za neku binarnu kvadratnu formu. Promotrimo trobrid uz osnovnu bazu u topografu slike kvadratne forme $f(x, y) = ax^2 + bxy + cy^2$.

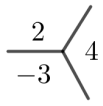


Slika 2.27: Vidimo da je $f(1,0) = a$, $f(1,1) = a + b + c$, $f(0,1) = c$.

Ako znamo vrijednosti a, $a+b+c$, i c tada možemo odrediti vrijednosti a, b i c. Iz toga slijedi sljedeća tvrdnja.

Propozicija 2.22. *Kvadratna forma je određena svojim vrijednostima u* $(1,0)$*,* $(0,1)$*,* $(1,1)$*.*

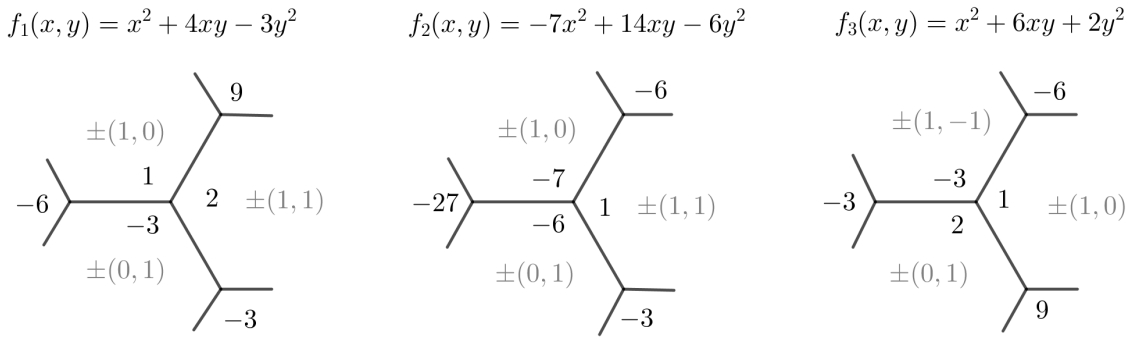
Ako je $f(1,0) = p$, $f(0,1) = q$ i $f(1,1) = r$ tada je $f(x,y) = px^2 + (r-p-q)xy + qy^2$.

Primjer 2.7. *Odredimo kvadratnu formu u čijem se topografu slike uz osnovnu bazu nalazi trobrid* 

.

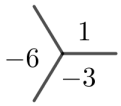
Rješenje: Tražimo kvadratnu formu $f(x,y) = ax^2 + bxy + cy^2$ za koju vrijedi $a = 2$, $c = -3$ i $a+b+c = 4$. Uvrštavanjem $a = 2$ i $c = -3$ u posljednju jednakost dobivamo $2+b-3 = 4$ iz čega slijedi $b = 5$. Tražena kvadratna forma je $f(x,y) = 2x^2 + 5xy - 3y^2$. □

Ponekad različite kvadratne forme imaju gotovo jednak topograf slike. Na Slici 2.28 se nalaze topografi slika triju međusobno različitih kvadratnih formi, $f_1(x,y) = x^2+4xy-3y^2$, $f_2(x,y) = -7x^2 + 14xy - 6y^2$, $f_3(x,y) = x^2 + 6xy + 2y^2$.



Slika 2.28: Topografi slika kvadratnih formi f_1, f_2 i f_3.

Vidimo da koeficijenti kvadratnih formi f_1, f_2, f_3 nemaju nikakvu očitu međusobnu vezu.

No, trobrid 

se pojavljuje u sva tri topografa slike. Prema pravilu aritmetičkog niza, vrijednosti u trobridu određuju sve vrijednosti topografa slike. Stoga, tri zadane kvadratne forme f_1, f_2, f_3 reprezentiraju isti skup cijelih brojeva.

Automorfizam, kojeg smo spominjali u potpoglavlju 2.3 *Topograf domene*, nam dopušta transformacije binarnih kvadratnih formi. Neka je $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ automorfizam. Ako je $f(x,y)$ binarna kvadratna forma, tada možemo definirati novu formu $f'(x,y) = f(ax+cy, bx+dy)$. Drugim riječima, ako M preslikava vektor $\vec{v}$ u vektor $\vec{v}'$, tada je $f'(\vec{v}) = f(\vec{v}')$.

Ako su f i f' u takvom odnosu, kažemo da je M ekvivalencija f u f'. Ako je još k tome $\det M = 1$, kažemo da je M **prava ekvivalencija** f u f'. Prema tome, dvije kvadratne forme f i f' zovemo (pravo) ekvivalentnima ako postoji (prava) ekvivalencija M koja ih povezuje. O ekvivalenciji formi smo govorili više s algebarskog stanovišta u Poglavlju 1. Ondje smo ekvivalencijom zvali ono za što ovdje koristimo pojam prave ekvivalencije, tj. dopuštali smo samo determinantu jednaku 1. Ovdje koristimo širi pojam ekvivalencije gdje determinanta matrice zamjene varijabli može imati determinantu ± 1, no to ne bi trebalo izazvati probleme.

Ako su dvije kvadratne forme ekvivalentne njihovi topografi slika su praktički jednaki. Svaki trobrid koji se pojavljuje u topografu slike forme f mora se pojaviti negdje u topografu slike njoj ekvivalentne forme f'.

Propozicija 2.23. *Neka su p, q i r cijeli brojevi te neka je $\{\vec{u}, \vec{v}, \vec{w}\}$ jaka superbaza. Tada postoji jedinstvena binarna kvadratna forma f za koju vrijedi*

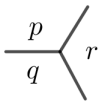
$$f(\vec{u}) = p, \quad f(\vec{v}) = q, \quad f(\vec{w}) = r.$$

Dokaz. Neka je f' binarna kvadratna forma koja poprima vrijednosti p, q, r za vektore $(1,0)$, $(0,1)$ i $(-1,-1)$, redom. Neka je M automorfizam koji vektore $(1,0)$, $(0,1)$ i $(-1,-1)$ preslikava u vektore jake superbaze $\vec{u}$, $\vec{v}$, $\vec{w}$ (prema Teoremu 2.19). Neka je f binarna kvadratna forma koju automorfizam M preslikava u f'. Tada je

$$f'(1,0) = f(\vec{u}), \quad f'(0,1) = f(\vec{v}), \quad f'(-1,-1) = f(\vec{w}).$$

Stoga je f tražena binarna kvadratna forma.

Jedinstvenost forme f dokazujemo na sljedeći način. Prema pravilu aritmetičkog niza i povezanosti topografa domene, vrijednosti koje forma f postiže za vektore $\vec{u}$, $\vec{v}$, $\vec{w}$ određuju sve ostale vrijednosti koje forma poprima. Stoga određuju i vrijednosti koje f poprima za vektore $(1,0)$, $(0,1)$ i $(-1,-1)$. Prema Propoziciji 2.22 koeficijenti forme f su jedinstveno određeni tim vrijednostima. □



Teorem 2.24 (**Kriterij ekvivalencije pomoću trobrida**). *Ako se trobrid* *pojavljuje u topografima slika dviju binarnih kvadratnih formi f_1 i f_2, tada su forme ekvivalentne. Ako se navedeni trobrid pojavljuje u istoj orijentaciji u obje forme, f_1 i f_2, tada je ekvivalencija prava.*

Dokaz. Neka je f binarna kvadratna forma u čijem se topografu slike pojavljuje navedeni trobrid na osnovnoj superbazi. Prema prethodnom dokazu vidimo da je forma f ekvivalentna formama f_1 i f_2. Stoga su forme f_1 i f_2 ekvivalentne. □

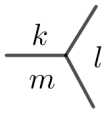
Kako bismo pronašli određena svojstva koja vrijede za kvadratnu formu, do sada smo promatrali njezin topograf slike i njegove manje elemente, trobride i ćelije. Pogledajmo sada što možemo saznati iz diskriminante kvadratne forme.

Diskriminanta kvadratne forme je cijeli broj iz kojeg možemo iščitati neka, ali ne sva njezina važna svojstva. Binarne kvadratne forme s različitim diskriminantama se međusobno dosta razlikuju.

Diskriminantu binarne kvadratne forme $d(f)$ lako računamo. No, za ono što nam slijedi bilo bi korisno povezati $d(f)$ s topografom slike i to činimo na dva načina. Prvo definirajmo diskriminantu trobrida.

Definicija 2.5. *Neka je zadan trobrid sa Slike 2.29. Tada je diskriminanta tog trobrida jednaka*

$$d(trobrid) = k^2 + l^2 + m^2 - 2(kl + lm + mk).$$



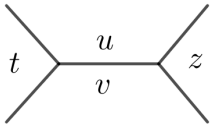
Slika 2.29: Trobrid

Primijetimo da se iznos $k^2 + l^2 + m^2 - 2(kl + lm + mk)$ ne mijenja pri permutaciji k, l, m na bilo koji način, tj. nakon rotacije ili zrcaljenja trobrida.

Ćelija također ima diskriminantu.

Definicija 2.6. *Neka je zadana ćelija sa Slike 2.30. Tada je diskriminanta te ćelije jednaka*

$$d(ćelija) = (u - v)^2 - tz.$$



Slika 2.30: Ćelija

Kao i kod trobrida, iznos $(u - v)^2 - tz$ se ne mijenja ni nakon zamjene u i v niti nakon zamjene t i z.

Prema pravilu aritmetičkog niza vrijednosti bilo koje ćelije topografa slike zadovoljavaju jednakost $t = 2(u + v) - z$. Stoga zaključujemo da se prethodne dvije definicije slažu što dokazujemo u sljedećoj tvrdnji.

Lema 2.25. *U topografu slike, diskriminanta ćelije je jednaka diskriminanti bilo kojeg trobrida kojeg sadrži.*

Dokaz. Koristeći identitet $t = 2(u + v) - z$, jednostavnije zapisujemo diskriminantu ćelije.

$$\begin{aligned} d(\text{ćelija}) &= (u - v)^2 - tz \\ &= u^2 - 2uv + v^2 - (2(u + v) - z)z \\ &= u^2 + v^2 + z^2 - 2uv - 2uz - 2vz = d(\text{trobrid}). \end{aligned}$$

Zbog simetrije kod zamjene t, z slijedi tvrdnja leme. □

Teorem 2.26 (**Jednakost diskriminanti u svim ćelijama i trorubima**)**.** *U topografu slike binarne kvadratne forme $f(x, y) = ax^2 + bxy + cy^2$, diskriminante svih ćelija i svih trobrida su jednake $d(f)$.*

Dokaz. Diskriminantu trobrida uz osnovnu bazu računamo direktno $a^2 + (a+b+c)^2 + c^2 - 2a(a + b + c) - 2c(a + b + c) - 2ac = b^2 - 4ac$ te dobivamo upravo $d(f)$.

Prema prethodnoj lemi, diskriminante svih triju susjednih ćelija spomenutog trobrida su jednake $d(f)$. Stoga su diskriminante svih susjednih trobrida ovim ćelijama jednake $d(f)$. Budući da su svi trobridi i ćelije međusobno vezani za osnovnu bazu, diskriminanta svakog trobrida i diskriminanta svake ćelije moraju biti jednake $d(f)$. □

U Propoziciji 1.2 smo naveli i dokazali jednakost diskriminanti dviju ekvivalentnih kvadratnih formi. Sada ćemo pokazati nešto drugačiji dokaz te tvrdnje.

Korolar 2.27. *Dvije ekvivalentne binarne kvadratne forme imaju jednake diskriminante.*

Dokaz. Ako su dvije binarne kvadratne forme ekvivalentne, tada imaju zajednički trobrid u topografu slike. Stoga je diskriminanta tog trobrida jednaka diskriminantama obiju kvadratnih formi. □

Svaka binarna kvadratna forma je ekvivalentna samoj sebi, što je trivijalno. No, binarna kvadratna forma može biti ekvivalenta sama sebi i na netrivijalan način.

Definicija 2.7. *Neka je f binarna kvadratna forma. Prava izometrija forme f je prava ekvivalencija $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ forme f u samu sebe. Drugim riječima, a, b, c, d su cijeli brojevi za koje vrijedi $ad - bc = 1$ te za sve cijele brojeve x, y vrijedi*

$$f(x, y) = f(ax + cy, bx + dy).$$

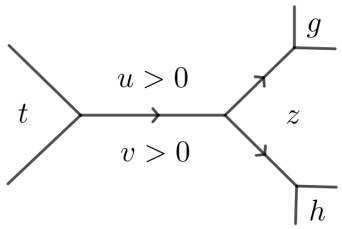
Pravu izometriju možemo često vidjeti u topografu slike kao rotacijsku ili translacijsku simetriju.

Poglavlje 3

Definitne kvadratne forme

Da bismo pronašli traženi broj u topografu slike, krećemo se prateći sve manje brojeve. Ako pogriješimo u praćenju brojeva te oni postaju sve veći, dovoljno je promijeniti smjer kretanja u topografu slike.

Teorem 3.1 (**Conwayev princip uspona**). *Neka je zadano područje topografa slike sa Slike 3.1.*



Slika 3.1: Dio topografa slike s dva susjedna područja u kojima su pozitivni brojevi.

Ako je aritmetički niz t, u + v, z rastući te su brojevi u i v pozitivni, tada su i aritmetički nizovi v, u + z, g i u, v + z, h također rastući.

Dokaz. Pretpostavimo da je niz t, $u + v$, z rastući. Tada vrijedi $t < u + v < z$.

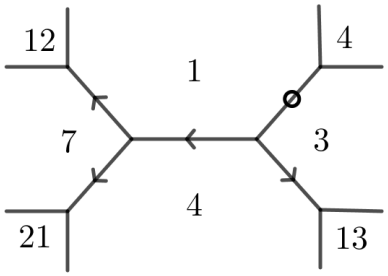
Nejednakosti $0 < u$ i $u + v < z$ povlače

$$v < u + u + v < u + z.$$

Dakle, niz v, $u + z$, g je rastući.

Analogno pokazujemo da je i niz u, $v + z$, h rastući. □

Da bismo pratili porast brojeva unutar topografa slike, bridove topografa označavamo strelicama. Strelice pokazuju smjer od manjih prema većim brojevima u svim nekonstantnim aritmetičkim nizovima. Ako je niz brojeva konstantan, tada odgovarajući brid topografa označavamo kružićem.



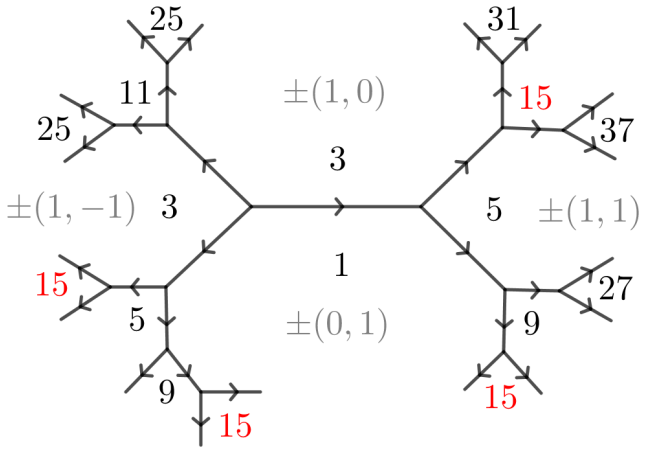
Slika 3.2: Označavanje bridova topografa slike kvadratne forme $f(x, y) = x^2 - 2xy + 4y^2$.

Ako su brojevi pozitivni, onda prema principu uspona znamo da strelice zadržavaju tok stalnog porasta. Ako se brojevi počnu povećavati, tada se nastavljaju povećavati.

Koristeći princip uspona možemo naći sva rješenja nekih diofantskih jednadžbi.

Primjer 3.1. *Riješimo diofantsku jednadžbu* $3x^2 + xy + y^2 = 15$.

Rješenje: U topografu slike kvadratne forme $f(x, y) = 3x^2 + xy + y^2$ tražimo broj 15.



Slika 3.3: Topograf slike kvadratne forme $f(x, y) = 3x^2 + xy + y^2$.

Broj 15 nalazimo na četiri mjesta u topografu slike. Prema principu uspona, grananjem topografa slike brojevi postaju sve veći. Dakle, ako u topografu slike nađemo broj 15 i nastavimo granati topograf, brojevi postaju sve veći i više nećemo naići na broj 15.

Broj 15 nalazimo na četiri mjesta u topografu slike koja odgovaraju četirima slabim vektorima u topografu domene: $\pm(1,-4)$, $\pm(2,-3)$, $\pm(2,1)$, $\pm(1,3)$.

Navedeni slabi vektori daju osam rješenja diofantske jednadžbe $3x^2 + xy + y^2 = 15$, $(-1,4)$, $(1,-4)$, $(-2,3)$, $(2,-3)$, $(-2,-1)$, $(2,1)$, $(-1,-3)$, $(1,3)$.

Primijetimo da u topografu slike vidimo samo cijele brojeve dobivene uvrštavanjem primitivnih slabih vektora u kvadratnu formu. No, što je s neprimitivnim vektorima kao što su $(0,0)$, $(2,-4)$, $(3,12)$?

Ako je $m \neq \pm 1$ i (ma, mb) neprimitivan vektor, tada imamo $f(ma,mb) = m^2 f(a,b)$. No, broj 15 je kvadratno slobodan te $m^2 f(a,b)$ ne može biti jednako 15. Stoga su osam rješenja koje smo pronašli u topografu slike sva rješenja diofantske jednadžbe $3x^2+xy+y^2 = 15$. □

Na isti način, koristeći pravilo aritmetičkog niza, možemo zaključiti da jednadžbe $3x^2 + xy + y^2 \in \{2,6,7,8,10,13,14\}$ nemaju rješenja.

Primjer 3.2. *Riješimo diofantsku jednadžbu* $3x^2 + xy + y^2 = 12$.

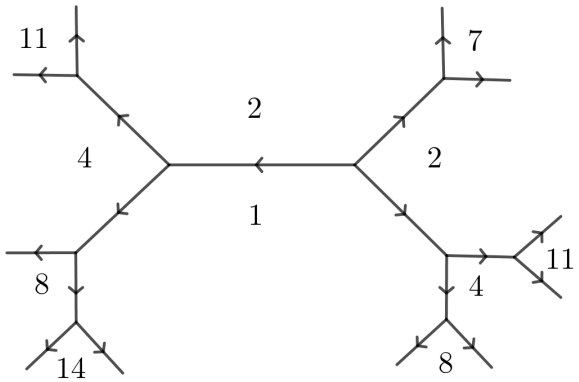
Rješenje: U topografu slike na prethodnoj stranici nigdje ne vidimo broj 12, a na svim krajevima topografa smo dobili brojeve veće od 12. Dakle, broj 12 nećemo nikad pronaći u ovom topografu slike.

Primijetimo da se broj 3 pojavljuje na dva mjesta u topografu slike: $\pm(1,0)$ i $\pm(1,-1)$. Prema formuli $f(ma,mb) = m^2 f(a,b)$ slijedi da je $3x^2+xy+y^2 = 12$ kada je $\pm(x,y)$ jednak jednom od sljedećih neprimitivnih vektora: $\pm(2,0)$ i $\pm(2,-2)$. Na ovaj način smo pronašli sva četiri rješenja zadane diofantske jednadžbe: $(-2,0)$, $(2,0)$, $(-2,2)$, $(2,-2)$.

Sva četiri rješenja koja smo dobili metodom kvadratnog skaliranja su neprimitivna. Budući da broj 12 možemo dobiti kvadratnim skaliranjem samo na jedan način, množenjem broja 3 faktorom 4, ne postoji drugo rješenje. □

Primjer 3.3. *Riješimo diofantsku jednadžbu* $2x^2 - xy + y^2 = 8$.

Rješenje: U topografu slike kvadratne forme $f(x,y) = 2x^2 - xy + y^2$, na Slici 3.4, nalazimo broj 2 na mjestima $\pm(1,0)$ i $\pm(1,1)$ te broj 8 na mjestima $\pm(1,-2)$ i $\pm(1,3)$. Znamo da vrijedi $2 \cdot 2^2 = 8$. Dakle, metodom kvadratnog skaliranja dobivamo osam rješenja: $(-2,0)$, $(2,0)$, $(-2,-2)$, $(2,2)$, $(-1,2)$, $(1,-2)$, $(-1,-3)$ i $(1,3)$.



Slika 3.4: Topograf slike kvadratne forme $f(x, y) = 2x^2 - xy + y^2$.

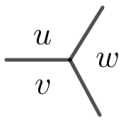
Prema principu uspona znamo da su to sva moguća rješenja dane diofantske jednadžbe. □

Promotrimo sada pozitivno definitnu binarnu kvadratnu formu $f(x, y) = ax^2 + bxy + cy^2$. Znamo da je $f(x, y) > 0$ za svaki primitivan vektor (x, y), te da u bilo kojem skupu prirodnih brojeva postoji najmanji broj, minimum tog skupa. Stoga se najmanji pozitivan broj pojavljuje i u topografu slike kvadratne forme. Označimo taj minimum s u.

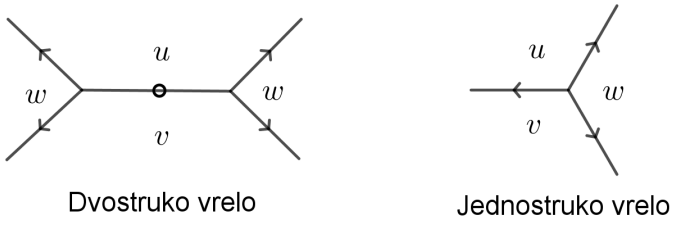
Napomenimo da u topografu slike mogu postojati dva ili više područja u kojima se pojavljuje minimalna vrijednost.

Promatramo u topografu slike, duž beskonačnog poligona koji okružuje vrijednost u vrijednosti $f(x, y)$. Budući da su navedene vrijednosti također pozitivne, to postoji vrijednost v koja je najmanja među vrijednostima susjednima vrijednosti u. Uočimo da je $u \leq v$.

Postoje dvije vrijednosti susjedne objema vrijednostima u i v. Neka je w manji od ta dva broja.



Budući je v najmanja susjedna vrijednost od u, to je $v \leq w$. Kako je w manja od dviju vrijednosti susjednih objema u i v, slijedi da aritmetički niz $w, u + v, ?$ mora biti konstantan ili rastući. Uočimo da je $w \leq u + v$. Ovisno o tome je li $w = u + v$ ili $w < u + v$, na Slici 3.5 vidimo dva moguća slučaja porasta brojeva unutar topografa slike.



Slika 3.5: Jednostruko i dvostruko vrelo. Strelice su pravilno postavljene zbog činjenice da je $0 < u \leq v \leq w$.

Definicija 3.1. ***Jednostruko vrelo*** *u topografu slike je trobrid čije su sve strelice na bridovima, koje pokazuju smjer porasta brojeva, usmjerene prema van.* ***Dvostruko vrelo*** *u topografu slike je ćelija čije su četiri strelice vanjskih bridova usmjerene prema van, a središnji brid ćelije je neutralan. Pod pojmom* ***vrela*** *podrazumijevamo jednostruko ili dvostruko vrelo.*

Prema principu uspona, vrijednosti koje se nalaze izvan vrela u topografu slike moraju biti veće od onih unutar vrela. Sve strelice na bridovima topografa slike su usmjerene od vrela. Stoga u svakom drugom trobridu imamo jednu ulaznu i dvije izlazne strelice. Tako dobivamo sljedeći teorem.

Teorem 3.2 (**Egzistencija i jedinstvenost vrela**)**.** *Svaka pozitivno definitna binarna kvadratna forma ima točno jedno vrelo unutar svog topografa slike.*

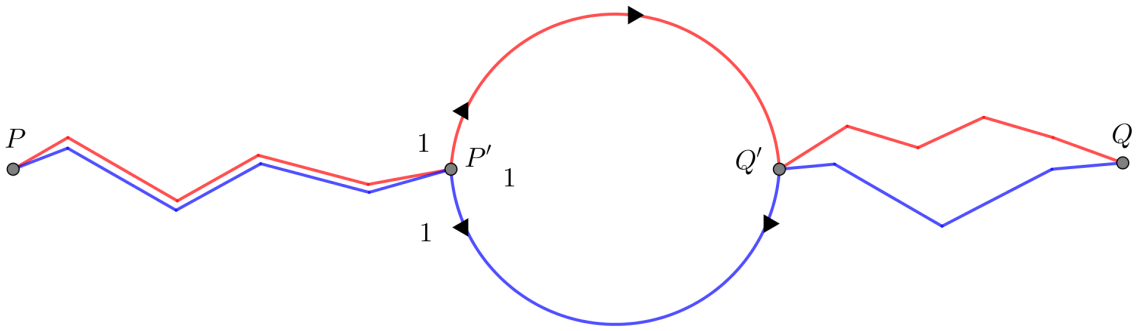
Koristeći princip uspona možemo dokazati važno svojstvo topografa domene. Do sada smo uzimali zdravo za gotovo da se vrhovi i bridovi topografa dalje granaju i izvode bez ikakvog ponovnog spajanja, tj. da u topografu domene nema petlji. Slijedi preciznije objašnjenje.

Jednostavan put u topografu domene, od vrha P do vrha Q, je šetnja duž bridova topografa koja nikada ne prolazi istim vrhom ili istim bridom dva puta. **Jednostavna petlja** u topografu domene jednostavan je put koji počinje i završava u istom vrhu.

Teorem 3.3 (**Topograf ne sadrži petlje**)**.** *Za bilo koja dva vrha P i Q u topografu domene, postoji samo jedan jednostavan put od P do Q. Posebno, u topografu domene nema jednostavnih petlji.*

Dokaz. Pretpostavimo da postoje dva jednostavna puta od P do Q. Pratimo oba puta sve do vrha njihova razilaženja, kojeg označavamo s P'. Od P' pratimo svaki od puteva do prvog ponovnog susreta te označimo taj vrh susretanja s Q'. Naravno, postoji mogućnost da je $P = P'$ ili $Q = Q'$ ili oboje. Na ovaj način smo konstruirali jednostavnu petlju u

topografu domene, krećući se najprije prvim putom od P' do Q', a zatim unazad drugim putom od Q' do P'.



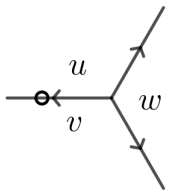
Slika 3.6: Teorem 3.3.

Promotrimo kvadratnu formu čije su vrijednosti unutar trobrida oko P' jednake 1, 1, 1 (prema Propoziciji 2.23 znamo da takva forma postoji). U nastavku promatramo topograf slike navedene kvadratne forme. Princip uspona podrazumijeva da, dok putujemo jednostavnom petljom od P' do Q' i natrag do P', vrijednosti s kojima se susrećemo (s desne ili lijeve strane) moraju rasti. No, nije moguće da vrijednosti neprestano rastu, a da se na kraju vratimo u isti vrh iz kojeg smo krenuli. □

Ovaj rezultat završava dokaz da topograf domene tvori **stablo**. Stablo je mreža vrhova i bridova, koja ne sadrži jednostavne petlje, i gdje šetanjem po bridovima možemo iz nekog vrha doći do svakog drugog vrha.

Propozicija 3.4. *Ako je f definitna binarna kvadratna forma tada je $d(f) < 0$.*

Dokaz. Ako je f negativno definitna, tada je $-f$ pozitivno definitna i vrijedi $d(f) = d(-f)$. Stoga bez smanjenja općenitosti možemo pretpostaviti da je f pozitivno definitna. Da bismo izračunali diskriminantu kvadratne forme, fokusiramo se na vrelo.



Slika 3.7: Vrelo.

Lijevi brid trobrida sa Slike 3.7 označavamo s kružićem i sa strelicom, kako bismo ukazali da je $u + v \geq w$, odnosno vrelo može biti jednostruko ili dvostruko.

Iz $u + v \geq w$ i $v \leq w$ slijedi da je

$$0 \leq w - v \leq u.$$

Kvadriranjem prethodnog izraza dobivamo sljedeće nejednakosti

$$0 \leq w^2 - 2vw + v^2 \leq u^2.$$

Diskriminanta kvadratne forme f jednaka je diskriminanti trobrida u vrelu.

$$d(f) = u^2 + v^2 + w^2 - 2uv - 2vw - 2wu.$$

Koristeći prethodnu nejednakost dobivamo

$$d(f) \leq u^2 + u^2 - 2uv - 2wu = 2u(u - (v + w)).$$

Budući je $v + w > u$, imamo da je $u - (v + w)$ negativan broj. Stoga vrijedi

$$d(f) \leq 2u(u - (v + w)) < 0.$$

□

Za jednostruka vrela moguće je dati geometrijski dokaz korištenjem Hadwiger-Finslerove nejednakosti. Nejednakost nam govori da ako je zadan trokut sa stranicama duljina u, v, w, tada se površina zadanog trokuta može odozgo ograničiti,

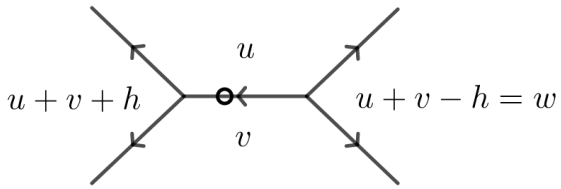
$$4\sqrt{3} \cdot \textit{Površina} \leq 2uv + 2vw + 2wu - u^2 - v^2 - w^2.$$

Uvjet postojanja jednostrukog vrela su nejednakosti trokuta: $u + v > w$, $v + w > u$ i $w + u > v$. Stoga znamo da postoji trokut sa stranicama duljina u, v, w i pozitivnom površinom. Hadwiger-Finslerova nejednakost povlači $4\sqrt{3} \cdot \textit{Površina} \leq -d$. Slijedi da je $d \leq -4\sqrt{3} \cdot \textit{Površina}$, tj. diskriminanta d je negativna.

Iz diskriminante pozitivno definitne kvadratne forme možemo saznati dosta informacija o topografu slike te forme. Primjerice, pomoću diskriminante možemo dobiti ogradu minimalne (nenul) vrijednosti pozitivno definitne kvadratne forme. Koristeći to, razvijamo algoritam za pronalaženje svih pozitivno definitnih binarnih kvadratnih formi sa zadanom diskriminantom.

Teorem 3.5 (**Ograda minimalne vrijednosti definitne forme**). *Neka je f pozitivno definitna binarna kvadratna forma s diskriminantom d. Najmanja nenul vrijednost koju f postiže je manja ili jednaka $\sqrt{|d|/3}$.*

Dokaz. Kao i prije, promotrimo vrelo kvadratne forme f. Opet je $u \leq v \leq w$, pa je u najmanja nenul vrijednost koju f postiže. Neka je $h = (u + v) - w$, pa ćelija koja sadrži vrelo ima oblik



Diskriminantu forme f možemo izračunati pomoću u, v i h. Naime, ista se ćelija pojavljuje u topografu slike od $ux^2 - hxy + vy^2$ kod osnovne baze. Stoga je

$$d = h^2 - 4uv < 0.$$

Nejednakost $u + v \geq w$ povlači da je $h \geq 0$. Nadalje, zbog $0 \leq u \leq v \leq w$ je $0 \leq u \leq v \leq u + v - h$. Budući je $v \leq u + v - h$, vrijedi $0 \leq u - h$, tj. $h \leq u$. Slijedi

$$0 \leq h \leq u \leq v.$$

Stoga je $|d| = 4uv - h^2 \geq 4u^2 - h^2 \geq 4u^2 - u^2 = 3u^2$. Iz toga slijedi tvrdnja teorema, $u \leq \sqrt{|d|/3}$. □

Sada nam četiri svojstva omogućuju popisivanje svih vrela određene (negativne) diskriminante.

1. $1 \leq u \leq \sqrt{d/3}$. (Teorem 3.5)
2. $0 \leq h \leq u$. (Dokaz Teorema 3.5)
3. $h^2 - 4uv = d$. (Definicija diskriminante)
4. Broj h je iste parnosti kao d.

Primjer 3.4. *Pronađimo sva vrela čije su diskriminante jednake* -80.

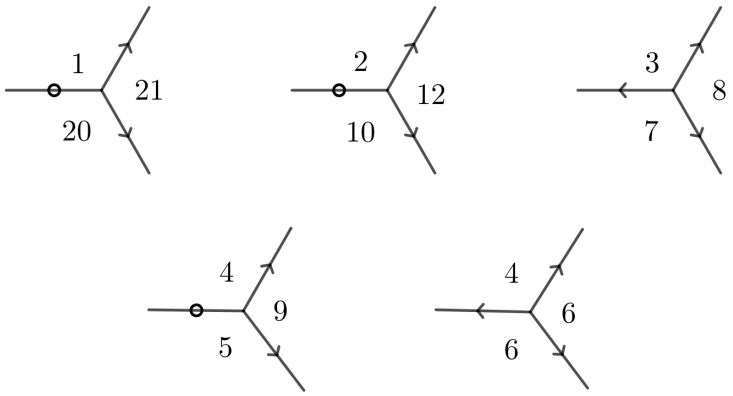
Rješenje: Promotrimo vrelo s diskriminantom -80, te kao i prije uzmimo da je $u \leq v \leq w$ i $h = (u + v) - w$.

Budući je $\sqrt{|-80|/3} = \sqrt{26.666...} < 6$ vrijedi $1 \leq u \leq 5$. Za svaki takav u vrijedi $0 \leq h \leq u$. Diskriminanta je parna, $d = -80$, pa je i h paran broj. Vrijednost v dobivamo uvrštavanjem vrijednosti u i h u formulu $h^2 - 4uv = -80$. Na Slici 3.8 je prikazana tablica s vrijednostima u, v i h.

u	h	v	
1	0	20	+
2	0	10	+
2	2	21/2	−
3	0	20/3	−
3	2	7	+
4	0	5	+
4	2	21/4	−
4	4	6	+
5	0	4	−
5	2	21/5	−
5	4	24/5	−

Slika 3.8: Tablica vrijednosti u, h, v.

Od svih navedenih vrijednosti u, v i h moguće je dobiti pet vrela prikazanih na Slici 3.9. □



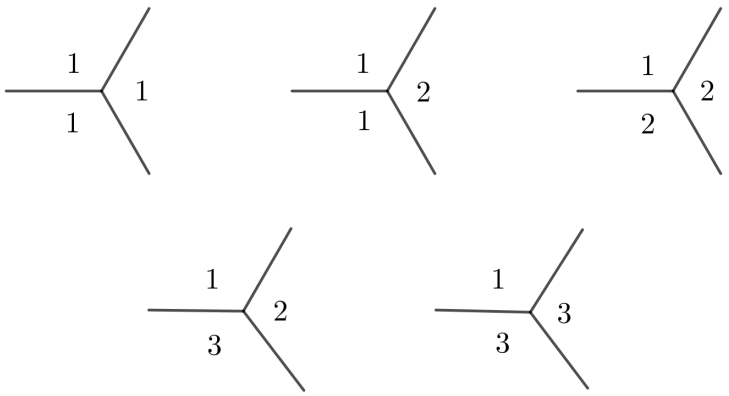
Slika 3.9: Vrela čije su diskriminante −80.

Ovo rješenje, zajedno sa svojstvom egzistencije jedinstvenog vrela za svaku pozitivno definitivnu binarnu kvadratnu formu, daje sljedeći rezultat. Ako je f pozitivno definitna binarna kvadratna forma s diskriminantom -80, onda je f ekvivalentna jednoj od sljedećih pet formi: $x^2 + 20y^2$, $2x^2 + 10y^2$, $3x^2 - 2xy + 7y^2$, $4x^2 + 5y^2$, $4x^2 - 4xy + 6y^2$.

Dakle, možemo reći da esencijalno postoji samo pet različitih pozitivno definitnih binarnih kvadratnih formi s diskriminantom -80. Svaka takva binarna kvadratna forma ima vrelo, a to vrelo mora biti jedno od pet navedenih na Slici 3.9.

Lema 3.6. *Ako je $d = -3, -4, -7, -8, -11$, tada postoji točno jedno vrelo čija je diskriminanta jednaka d.*

Dokaz. Da bismo dokazali ovu tvrdnju koristimo metodu opisanu u prethodnom primjeru. U svih pet slučajeva je $|d| < 12$, dakle $\sqrt{|d|/3} < 2$ pa vrijedi da je $u = 1$. Stoga je $h = 0$ ili $h = 1$, ovisno o tome je li d parno ili neparno. Tada vrijednosti u i h određuju v budući da je $h^2 - 4uv = d$. Dobivamo vrela kao na Slici 3.10. □



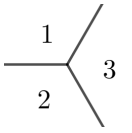
Slika 3.10: Vrela s diskriminantama -3, -4, -7, -8, -11.

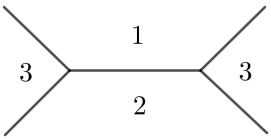
Teorem 3.7. *Ako je f pozitivno definitna binarna kvadratna forma s diskriminantom $d = -3, -4, -7, -8$ ili -11, tada vrijedi*

- *$d = -3$: f je pravo ekvivalentna formi $x^2 + xy + y^2$.*
- *$d = -4$: f je pravo ekvivalentna formi $x^2 + y^2$.*
- *$d = -7$: f je pravo ekvivalentna formi $x^2 + xy + 2y^2$.*
- *$d = -8$: f je pravo ekvivalentna formi $x^2 + 2y^2$.*
- *$d = -11$: f je pravo ekvivalentna formi $x^2 + xy + 3y^2$.*

Dokaz. Prethodna lema kaže da postoji jedinstveno vrelo za svaku od ovih diskriminanti. Svako od pet vrela pojavljuje se redom u navedenih pet kvadratnih formi. Pa je f ekvivalentna navedenim formama. Treba još pokazati da je ekvivalencija prava, tj. da se svako

vrelo pojavljuje u istoj orijentaciji u f kao i u pet navedenih formi. Sva su vrela simetrična (ista bilo da ih gledamo u smjeru kazaljke na satu ili obrnuto), osim vrela





s diskriminantom -8. No, to vrelo se pojavljuje u ćeliji i u smjeru kazaljke na satu i u smjeru suprotnom od kazaljke na satu. Dakle, svaka pozitivno definitna kvadratna forma f s diskriminantom -8 sadrži ovo vrelo u obje orijentacije i pravo je ekvivalentna formi $x^2 + 2y^2$. □

Kod manjih diskriminanti se pojavljuje jedinstveno vrelo, ali za svaku diskriminantu može ih se pojaviti samo konačno mnogo.

Teorem 3.8. *Ako je d negativan cijeli broj, tada postoji najviše konačno mnogo vrela čije su diskriminante jednake d. Takvih vrela ima najviše $|d|/3$.*

Dokaz. Svako vrelo čija je diskriminanta jednaka d nastaje od triju cijelih brojeva u, v, h za koje vrijedi $h^2 - 4uv = d$ i $0 \leq h \leq u \leq v$.

Budući je u omeđen s $\sqrt{|d|/3}$, vidimo da je broj mogućih parova (h, u) omeđen s $|d|/3$. Za svaki takav par postoji najviše jedan cijeli broj v koji zadovoljava $h^2 - 4uv = d$. Slijedi da je broj vrela s diskriminantom d omeđen s $|d|/3$. □

Budući da se prava ekvivalencija pozitivno definitne binarne kvadratne forme može vidjeti iz vrela, prethodni teorem povlači sljedeći rezultat o konačnosti koji je zapravo posljedica Teorema 1.3 i Teorema 1.4.

Korolar 3.9. *Neka je zadan negativan cijeli broj d. Tada postoji konačno mnogo binarnih kvadratnih formi $\{f_1,...,f_t\}$, takvih da je svaka pozitivno definitna binarna kvadratna forma f s diskriminantom d pravo ekvivalentna jednoj od navedenih formi.*

U sljedećem teoremu koristimo kongruencije pa se prisjetimo tog pojma. Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, onda kažemo da je *a kongruentan b* modulo m i pišemo $a \equiv b \pmod{m}$. U protivnom, kažemo da *a nije kongruentan b* modulo m i pišemo $a \not\equiv b \pmod{m}$.

Teorem 3.10 (Fermat). *Neka je p prost broj za koji vrijedi $p \equiv 1 \pmod{4}$. Tada diofantska jednadžba $x^2 + y^2 = p$ ima rješenje, tj. p možemo prikazati kao sumu dva kvadrata.*

Dokaz. Prema Gaussovom kvadratnom zakonu reciprociteta za ostatak -1, kojeg možemo naći u skripti [4], postoje cijeli brojevi u, n takvi da vrijedi $u^2 + 1 = pn$. Promotrimo kvadratnu formu

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

Koeficijenti forme f su cijeli brojevi, a diskriminanta iznosi

$$d = (2u)^2 - 4pn = 4u^2 - 4(u^2 + 1) = -4.$$

Budući je $f(1, 0) = p > 0$ i $d = -4 < 0$, kvadratna forma je pozitivno definitna. Prema Teoremu 3.7, f je ekvivalentna formi $x^2 + y^2$. Budući da f reprezentira p, tada i forma $x^2 + y^2$ također reprezentira p. □

Sličan rezultat možemo dokazati koristeći jedinstvenost vrela s diskriminantom -3.

Teorem 3.11. *Neka je p prost broj za koji vrijedi $p \equiv 1 \pmod 3$. Tada diofantska jednadžba $x^2 + xy + y^2 = p$ ima rješenje.*

Dokaz. Prema Gaussovom kvadratnom zakonu reciprociteta, dobivamo

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = 1.$$

Dakle, postoji cijeli broj v takav da vrijedi $v^2 \equiv -3 \pmod p$. Zamjenom v sa $p - v$ ako je potrebno, možemo pretpostaviti da je v neparan. Stoga je $v^2 + 3 = pn$ za neki cijeli broj n, i štoviše, $v^2 + 3 \equiv 0 \pmod 4$ jer su kvadrati neparnih brojeva $\equiv 1 \pmod 4$. Budući da je p neparan, a $4 \mid (v^2 + 3) = pn$, vidimo da $4 \mid n$. Označimo $m = n/4$ pa imamo $v^2 + 3 = 4pm$.

Sada promotrimo kvadratnu formu $f(x, y) = px^2 + vxy + my^2$. Koeficijenti su cijeli brojevi, a diskriminanta je $d = v^2 - 4pm = -3$. Forma f je pozitivno definitna, jer je $f(1, 0) = p$, a diskriminanta je negativna. Prema Teoremu 3.7, f je ekvivalentna kvadratnoj formi $x^2 + xy + y^2$. Dakle, $x^2 + xy + y^2$ također reprezentira p. □

Prave izometrije pozitivno definitne kvadratne forme moraju nastati iz pravih simetrija njezina vrela. Promotrimo pravu izometriju M kvadratne forme f i vrelo u njezinom topografu slike. Ako pomoću M preslikavamo vrelo, tada moramo naći iste vrijednosti, a time i cijelo vrelo. Jedinstvenost vrela podrazumijeva da M preslikava vrelo u vrelo, pa nemamo mnogo mogućnosti.

Teorem 3.12. *Ako je f pozitivno definitna binarna kvadratna forma s netrivijalnim pravim izometrijama, tada je ili*

f kvadratna forma s rotacijskom izometrijom za $120°$, te je f ekvivalentna višekratniku forme $x^2 + xy + y^2$ ili

f kvadratna forma s rotacijskom izometrijom za $180°$, te je f ekvivalentna višekratniku forme $x^2 + y^2$.

Dokaz teorema nećemo navoditi, a može se naći u [6, str. 270].

Pozitivno semidefinitne kvadratne forme

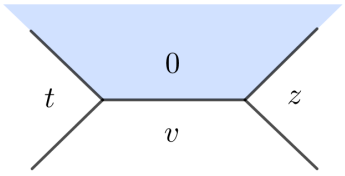
Pozitivno semidefinitne forme su binarne kvadratne forme koje u topografu slike poprimaju pozitivne vrijednosti i nulu, ali nikako negativne vrijednosti. Kada se u topografu slike pojavi nula, prema Conwayevom pristupu bojimo područje u plavo i nazivamo ga *jezerom*.

Definicija 3.2. ***Jezero*** *je područje u topografu slike u kojem je vrijednost jednaka nuli.*

U nastavku promatramo kvadratnu formu f s diskriminantom d.

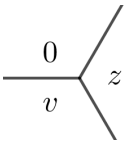
Propozicija 3.13. *Uz obalu jezera u topografu slike kvadratne forme f, vrijednosti tvore aritmetički niz s razlikom $\sqrt{d}$. Posebno, diskriminanta d je potpun kvadrat.*

Dokaz. Promotrimo tri područja susjedna jezeru.



Slika 3.11: Jezero

Prema Teoremu 2.21, t, v, z čine aritmetički niz koji se nastavlja oko bridova jezera. Razlika aritmetičkog niza iznosi $z - v$. Računamo diskriminantu koristeći trobrid sa slike ispod.



$$d(trobrid) = z^2 + v^2 - 2zv = (z - v)^2.$$

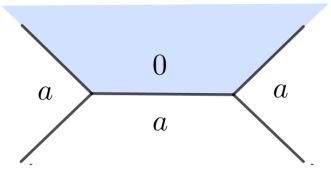
Stoga je razlika aritmetičkog niza $z - v$ jednaka $\pm\sqrt{d}$, tj. $d = (z - v)^2$ je potpun kvadrat. □

Korolar 3.14. *Ako je f pozitivno semidefinitna forma koja nije pozitivno definitna, tada je $d(f) = 0$ i topograf slike sadrži jezero okruženo konstantnim nizom.*

Dokaz. Budući da je f semidefinitna, u topografu slike se pojavljuje jezero. Obostrano beskonačni aritmetički niz duž bridova jezera ne može sadržavati negativan broj, jer je f pozitivno semidefinitna. No takav niz mora biti konstantan niz. Zbog toga nalazimo pozitivnu konstantu a uz bridove jezera. Iz prethodne propozicije slijedi $d = 0$. □

Korolar 3.15 (**Klasifikacija formi s diskriminantom nula**). *Ako je f pozitivno semidefinitna forma koja nije pozitivno definitna, tada je f ekvivalentna kvadratnoj formi ax^2 za neki pozitivan cijeli broj a.*

Dokaz. Ćelija prikazana na Slici 3.12 se pojavljuje u topografu slike binarne kvadratne forme $f'(x, y) = ax^2$. Prethodni korolar povlači da je f ekvivalentna formi ax^2. □



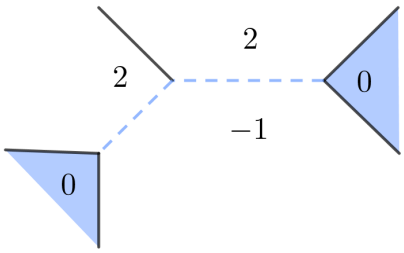
Slika 3.12: Poseban slučaj kad je $d = 0$.

Poglavlje 4

Indefinitne kvadratne forme

Za mnoge kvadratne forme, u topografu slike nalazimo i pozitivne i negativne vrijednosti. Te forme nazivamo **indefinitnim** formama. Svojstva indefinitnih formi, promjena predznaka i vrijednost nula, u topografu slike se označavaju **vodom**. Podsjetimo da se područja u topografu slike s vrijednošću nula nazivaju jezera i obojena su plavom bojom. Proširivši ovu metaforu, Conway definira rijeku.

Definicija 4.1. ***Rijeka*** *je skup bridova topografa slike koji odvajaju pozitivne vrijednosti od negativnih vrijednosti.*



Slika 4.1: Topograf slike s dva jezera i rijekom.

U ovom poglavlju ćemo vidjeti da za indefinitne forme, topografi slika bez jezera imaju beskrajne periodične rijeke.

Prema Propoziciji 3.13, ako se u topografu slike kvadratne forme pojavljuje jezero, tada je diskriminanta te forme potpun kvadrat. Obrat ove tvrdnje se može dokazati algebarski.

Propozicija 4.1. *Ako je f binarna kvadratna forma čija je diskriminanta d potpun kvadrat, tada topograf slike forme f ima barem jedno jezero.*

Dokaz. Neka je $f(x,y) = ax^2 + bxy + cy^2$ binarna kvadratna forma za koju vrijedi da je $d = b^2 - 4ac$ potpun kvadrat. Ako je $a = 0$, tada je

$$f(1,0) = 0(1)^2 + b(1)(0) + c(0)^2 = 0.$$

Dakle, ako je $a = 0$, tada topograf slike ima jezero na mjestu $\pm(1,0)$.

Ako je $a \neq 0$, neka je $x = \sqrt{d} - b$ i $y = 2a$. Direktno računamo

$$\begin{aligned} f(x,y) &= a(\sqrt{d} - b)^2 + b(\sqrt{d} - b)(2a) + c(2a)^2 \\ &= a(d - 2b\sqrt{d} + b^2) + a(2b\sqrt{d} - 2b^2) + a(4ac) \\ &= a(d - b^2 + 4ac) = 0. \end{aligned}$$

Neka je $g = \text{nzd}(x,y)$. Budući je $a \neq 0$, slijedi da je $y \neq 0$ i $g \neq 0$. Tada kvadratnim skaliranjem za faktor g dobivamo

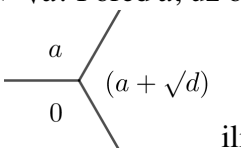
$$f(\frac{x}{g}, \frac{y}{g}) = \frac{1}{g^2} f(x,y) = 0 \qquad \text{i} \qquad \pm(\frac{x}{g}, \frac{y}{g}) \text{ je primitivan slab vektor.}$$

Stoga topograf slike forme f ima jezero na mjestu $\pm(\frac{x}{g}, \frac{y}{g})$. □

Propozicija 4.2. *Ako topograf slike binarne kvadratne forme f ima jezero, tada je f ekvivalentna $ax^2 + \sqrt{d}xy$ za neki cijeli broj a. Ako je $d \neq 0$, tada postoji takav cijeli broj a za koji vrijedi $0 \leq a < \sqrt{d}$.*

Dokaz. Uz obalu jezera vrijednosti čine aritmetički niz s razlikom $\sqrt{d}$. Ako je $d = 0$, sve vrijednosti uz obalu jezera su jednake pa tu vrijednost možemo označiti s a. Tada tvrdnja slijedi iz Korolara 3.15.

Ako je $d \neq 0$, tada je u nizu uz obalu jezera, najmanja nenegativna vrijednost cijeli broj a koji zadovoljava nejednakosti $0 \leq a < \sqrt{d}$. Pored a, uz obalu jezera, nalazimo vrijednost $a + \sqrt{d}$. Tako topograf f sadrži trobrid



ili njegovu zrcalnu sliku.

Taj se trobrid također pojavljuje u topografu slike forme $ax^2 + \sqrt{d}xy$ (kod osnovne baze). Stoga je f ekvivalentna s $ax^2 + \sqrt{d}xy$. □

Teorem 4.3 (**Diskriminanta određuje broj jezera**). *Neka je f nenul binarna kvadratna forma s diskriminantom d. Broj jezera u topografu slike forme f jednak je*

$$\begin{cases} 0 & \textit{ako } d \textit{ nije potpun kvadrat}; \\ 1 & \textit{ako je } d\textit{=0}; \\ 2 & \textit{ako je } d \textit{ potpun kvadrat različit od nule}. \end{cases}$$

Dokaz. Prema Propoziciji 3.13, ako d nije potpun kvadrat, topograf slike forme f ne može imati jezero. Obratno prema Propoziciji 4.1, ako topograf slike forme f nema jezero, tada d nije potpun kvadrat. Ostaje dokazati da postoji točno jedno jezero ako je $d = 0$, te da postoje točno dva jezera ako je d pozitivan potpun kvadrat. U oba slučaja f je ekvivalentna $ax^2 + \sqrt{d}xy$ za neki cijeli broj a.

Ako je $d = 0$, tada je f ekvivalentna ax^2. No, jedini slab primitivan vektor $\pm(x, y)$ za koji vrijedi $ax^2 = 0$ je $\pm(0, 1)$. Dakle, jedino jezero u topografu slike forme ax^2 je na mjestu $\pm(0, 1)$. Zbog ekvivalencije dviju formi, postoji samo jedno jezero u topografu slike forme f.

Ako je d pozitivan potpun kvadrat, tada je f ekvivalentna $ax^2 + \sqrt{d}xy$. Jezera forme $ax^2 + \sqrt{d}xy$ odgovaraju slabim primitivnim vektorima $\pm(x, y)$ za koje vrijedi $ax^2 + \sqrt{d}xy = 0$. Faktorizacijom prethodnog izraza dobivamo njemu ekvivalentan izraz

$$x(ax + \sqrt{d}y) = 0.$$

Ova jednakost vrijedi ako je $x = 0$ ili $x/y = -\sqrt{d}/a$. Jedini slab primitivan vektor za koji je $x = 0$ je vektor $\pm(0, 1)$. Jedini slab primitivan vektor $\pm(x, y)$ koji zadovoljava $x/y = -\sqrt{d}/a$ je rezultat skraćivanja toga razlomka, tj.

$$x = \frac{-\sqrt{d}}{\text{nzd}(\sqrt{d}, a)}, \quad y = \frac{a}{\text{nzd}(\sqrt{d}, a)}.$$

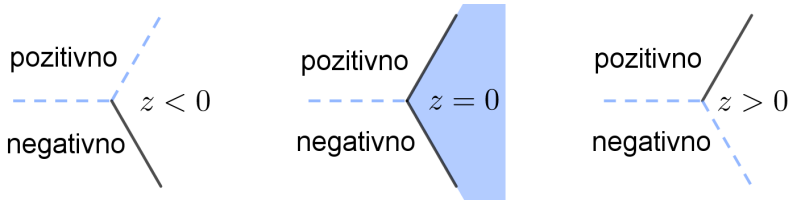
Dakle, točno dva jezera se pojavljuju u topografu slike forme f: jedno na mjestu $(\pm 1, 0)$ i drugo na mjestu $\pm(x, y)$, gdje su x, y dani gornjim jednakostima. □

U nastavku ćemo proučavati topografe jezera i rijeka.

Rijeke u topografu slike odvajaju pozitivne vrijednosti od negativnih.

Propozicija 4.4 (**Topologija rijeka**). *Rijeke se ne mogu odjednom zaustaviti niti se mogu račvati. Njihov tok može prestati samo u jezeru.*

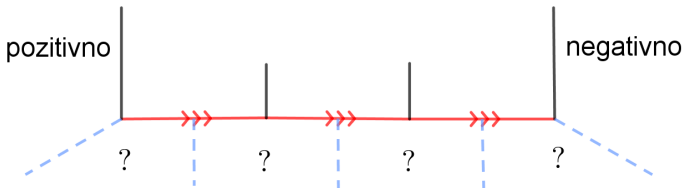
Dokaz. Promotrimo trobrid koji sadrži jedan dio rijeke. Stoga trobrid sadrži pozitivnu vrijednost, negativnu vrijednost, i još jednu vrijednost koju označavamo sa z. Za vrijednost z vrijedi da je $z < 0$ ili $z = 0$ ili $z > 0$. Na Slici 4.2 su prikazana sva tri slučaja te vidimo da vrijedi tvrdnja propozicije. □



Slika 4.2: Topologija rijeka.

Propozicija 4.5. *Ako se pozitivna vrijednost i negativna vrijednost pojavljuju u topografu slike, tada topograf slike mora sadržavati jezero ili rijeku (ili oboje).*

Dokaz. Prema Teoremu 2.10, povezanost topografa nam omogućuje kretanje od pozitivne do negativne vrijednosti po bridovima topografa slike. Promotrimo vrijednosti s jedne strane toga puta kao na slici dolje.



Slika 4.3: Propozicija 4.5

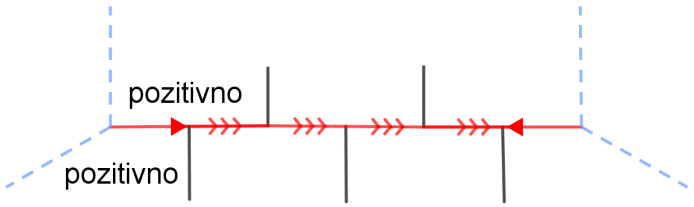
Duž puta moramo naći jezero ili pak direktan prijelaz iz pozitivne u negativnu vrijednost, tj. rijeku. Jedan od iscrtkanih bridova mora biti rijeka ili jedno od područja s oznakama ? mora biti jezero. □

Korolar 4.6. *Neka je f binarna kvadratna forma s diskriminantom d. Ako je $d > 0$ i d nije potpun kvadrat, tada topograf slike forme f sadrži beskrajnu rijeku.*

Dokaz. Budući da je $d > 0$, forma f nije definitna niti semidefinitna, i zbog toga što d nije potpun kvadrat, topograf slike forme f ne sadrži jezera. Stoga se i pozitivne i negativne vrijednosti pojavljuju u topografu slike forme f, dok se vrijednost 0 ne pojavljuje. Prema Propoziciji 4.5, rijeka se mora pojaviti. Kao što smo ranije vidjeli, rijeka ne može završiti budući da u topografu slike forme f nema jezera, pa je rijeka beskrajna. □

Propozicija 4.7 (**Jedinstvenost rijeke**). *Topograf može imati najviše jednu rijeku.*

Dokaz. Ako se u topografu pojavljuju dvije rijeke, krenimo od jedne prema drugoj kao što je prikazano na Slici 4.4.

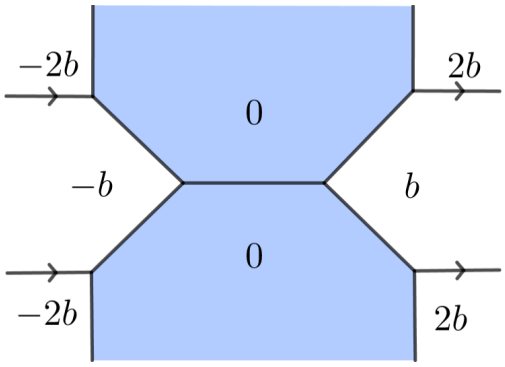


Slika 4.4: Ako se put od jedne rijeke do druge nalazi na pozitivnoj strani rijeke, tada vrijednosti postaju sve veće i veće kako se krećemo udesno. Topograf prikazan na ovoj slici ne može se pojaviti ni za jednu formu.

Ako se pomaknemo od rijeke, vrijednosti s obje strane puta su ili obje pozitivne ili obje negativne. Prema principu uspona vrijednosti po modulu moraju rasti (moraju se povećavati ako su pozitivne ili smanjivati ako su negativne) dok se krećemo ovim putem. Stoga ne možemo tim putom doći do druge rijeke. □

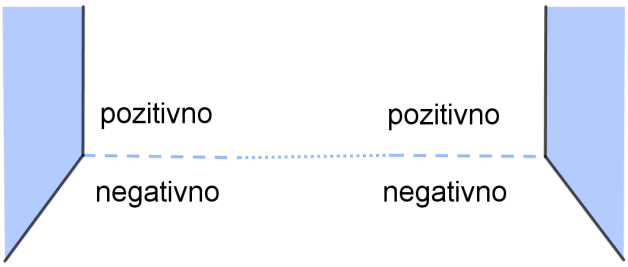
Propozicija 4.8. *Ako je d pozitivan potpun kvadrat, tada u topografu slike postoji dvostruko jezero (dva jezera koja imaju zajednički brid) bez rijeke ili postoje dva jezera povezana rijekom.*

Dokaz. Kada je d pozitivan potpun kvadrat, u topografu se nalaze dva jezera. Ako postoji dvostruko jezero, princip uspona pokazuje nemogućnost postojanja rijeke kako vidimo na Slici 4.5.



Slika 4.5: Dvostruko jezero mora imati vrijednosti $\pm b$ na obje strane, prema pravilu aritmetičkog niza. Takva forma je ekvivalentna $\sqrt{d}xy$. Aritmetički nizovi uz obale jezera jamče da se s jedne strane obale dvostrukog jezera nalaze pozitivne vrijednosti, a s druge strane negativne vrijednosti. Prema principu uspona vrijednosti će se povećavati ili smanjivati dok se odmičemo dalje od dvostrukog jezera.

Ako postoje dva nesusjedna jezera, tada nekonstantan aritmetički niz oko svakog jezera ne sadrži nulu. Na mjestu gdje svaki od nizova mijenja predznak, dio rijeke strši iz obale jezera.

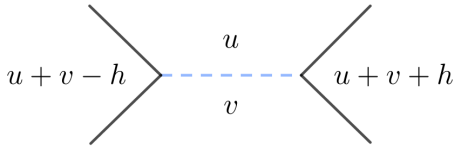


Slika 4.6: Propozicija 4.8

Prema Propoziciji 4.7 dijelovi rijeka koji strše se spajaju u jednu rijeku. □

Propozicija 4.9. *Topograf koji sadrži rijeku ima pozitivnu diskriminantu.*

Dokaz. Promotrimo ćeliju uz rijeku. Neka je h razlika aritmetičkog niza kojeg čine vrijednosti u zadanoj ćeliji.



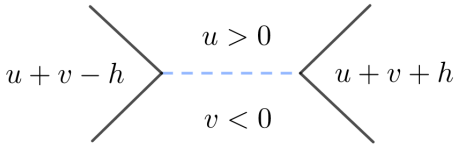
Slika 4.7: Ćelija uz rijeku.

Diskriminanta je jednaka $d = h^2 - 4uv$. Budući da su vrijednosti u i v suprotnih predznaka, slijedi da je $-4uv > 0$. Zbog $h^2 \geq 0$ je $d > 0$. □

Pomnija analiza riječnih dijelova pokazuje da je tek konačno mnogo takvih sa zadanom diskriminantom.

Lema 4.10. *Fiksirajmo pozitivan cijeli broj d. Tada postoji najviše konačno mnogo različitih dijelova rijeke s diskriminantom d.*

Dokaz. Promotrimo dio rijeke s diskriminantom d.



Vrijedi da je $h^2 - 4uv = d$. Kako je $u > 0$ i $v < 0$ slijedi da je $-4uv > 0$. Stoga je $0 \leq h^2 < d$ i $0 < |u| \cdot |v| \leq d/4$.

Iz toga slijedi da ne postoji više od $\sqrt{d}$ mogućih vrijednosti h. Slično tome, broj mogućih vrijednosti u omeđen je s $\frac{d}{4}$. Vrijednosti h i u određuju vrijednost v kad je d fiksno. Zato za $d > 0$ ne može postojati više od $\frac{1}{4}d^{3/2}$ dijelova rijeke s diskriminantom d. □

Teorem 4.11 (**Periodičnost rijeke**). *Ako je d pozitivan i nije potpun kvadrat, tada svaki topograf slike s diskriminantom d ima beskrajnu **periodičnu** rijeku.*

Dokaz. Kada je d pozitivan i nije potpun kvadrat, tada svaki topograf slike s diskriminantom d ima beskrajnu rijeku. Ako pratimo rijeku, dio po dio, prema Lemi 4.10 moramo naići na ponavljanje. No, kad nađemo ponavljanje, uzorak se stalno ponavlja. □

Korolar 4.12. *Neka je $f(x, y)$ binarna kvadratna forma čija je diskriminanta pozitivan broj koji nije potpun kvadrat. Neka je N cijeli broj različit od nule. Ako diofantska jednadžba $f(x, y) = N$ ima jedno rješenje, tada ima beskonačno mnogo rješenja.*

Dokaz. Neka je zadana kvadratna forma $f(x, y) = N$ te neka su $g = \text{nzd}(x, y)$, $u = \frac{x}{g}$ i $v = \frac{y}{g}$. Neka je $n = f(u, v)$. Tada je $\pm(u, v)$ primitivan slab vektor i vrijedi

$$N = f(x, y) = f(gu, gv) = g^2 f(u, v) = g^2 n.$$

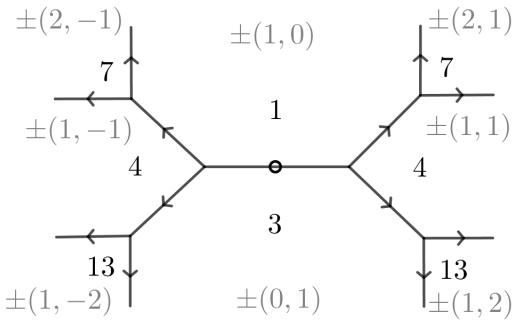
Budući da je rijeka periodična, cijeli topograf je periodičan pa se vrijednost n pojavljuje beskonačno mnogo puta u topografu. Svaki put kada se n pojavi na mjestu slabog vektora $\pm(u', v')$, pronalazimo novo rješenje $x' = gu'$, $y' = gv'$ koje zadovoljava jednadžbu $f(x', y') = N$. □

Rezultat prethodnog korolara ilustrirajmo rješavajući dvije kvadratne diofantske jednadžbe.

Primjer 4.1. *Riješimo diofantsku jednadžbu $x^2 + 3y^2 = 7$.*

Rješenje: Kvadratna forma $f(x, y) = x^2 + 3y^2$ je pozitivno definitna. Uz osnovnu bazu nalazimo dvostruko vrelo i četiri rješenja dane jednadžbe:

$$(x, y) = (2, 1), (-2, 1), (2, -1), (-2, -1).$$

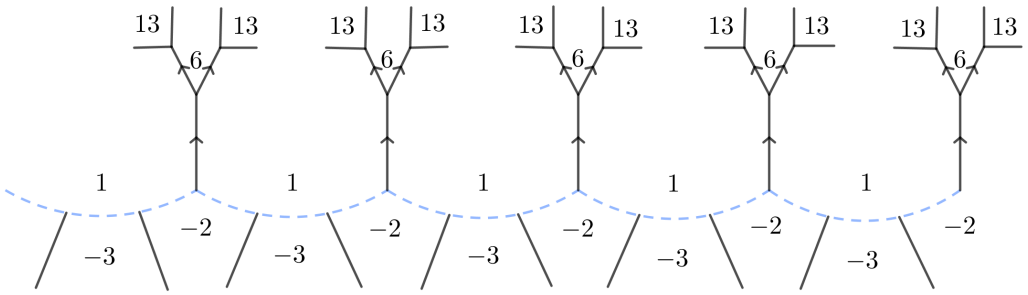


Slika 4.8: Topograf slike kvadratne forme $f(x, y) = x^2 + 3y^2$.

Princip uspona osigurava da nema drugih rješenja. □

Primjer 4.2. *Riješimo diofantsku jednadžbu* $x^2 - 3y^2 = 7$.

Rješenje: Kvadratna forma $f(x, y) = x^2 - 3y^2$ je indefinitna s diskriminantom 12, koja je pozitivan broj i nije potpun kvadrat. Stoga topograf slike forme f nema jezera, ali ima periodičnu beskraju rijeku, koja je prikazana na slici dolje.



Ako postoje primitivni slabi vektori $\pm(x, y)$ za koje vrijedi $f(x, y) = 7$, onda se takvi nalaze s pozitivne strane rijeke. No, prema principu uspona i periodičnosti rijeke vidimo da se broj 7 ne pojavljuje nigdje u topografu slike. Stoga diofantska jednadžba $x^2 - 3y^2 = 7$ nema rješenja. □

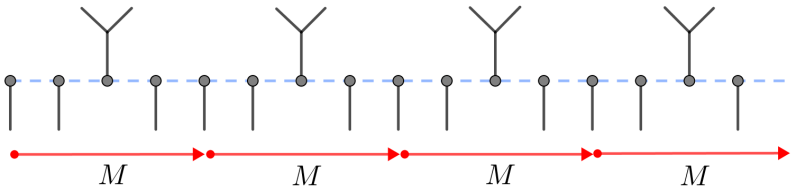
Uočimo da jednadžba $x^2 - 3y^2 = 1$ ima beskonačno mnogo rješenja. Takva jednadžba je poseban slučaj Pellove jednadžbe.

Teorem 4.13 (Beskonačnost rješenja Pellove jednadžbe). *Ako je N pozitivan broj koji nije potpun kvadrat, tada diofantska jednadžba $x^2 - Ny^2 = 1$ ima beskonačno mnogo rješenja.*

Dokaz. Diskriminanta kvadratne forme $f(x, y) = x^2 - Ny^2$ jednaka je $4N$. Ako je N pozitivan broj koji nije potpun kvadrat, tada je i $4N$ pozitivan broj koji nije potpun kvadrat. Stoga topograf slike kvadratne forme f sadrži beskrajnu periodičnu rijeku. Budući da $x^2 - Ny^2 = 1$ ima jedno rješenje, $x = 1$, $y = 0$, diofantska jednadžba ima beskonačno mnogo rješenja. □

Topograf slike ne samo da ilustrira postojanje beskonačno mnogo rješenja, već pruža i metodu njihovog pronalaska prateći rijeku.

Prave izometrije indefinitne binarne kvadratne forme nastaju iz pravih simetrija njezine rijeke. Neka je f kvadratna forma s pozitivnom diskriminantom koja nije potpun kvadrat, te neka je M prava izometrija forme f. Tada M preslikava rijeku u rijeku i pozitivne vrijednosti u pozitivne vrijednosti te stoga M translatira topograf duž rijeke. Ako rastegnemo rijeku u ravnu liniju i odredimo da je duljina svakog brida jednaka 1, tada M mora biti translacija duž rijeke za cijeli broj jedinica.



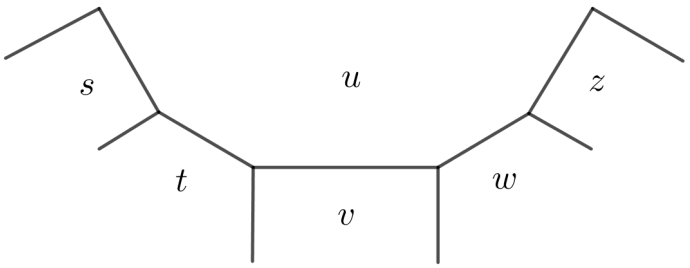
Slika 4.9: Prikazana je translacija M duž rijeke za četiri jedinice.

Ako je t najmanja pozitivna duljina za koju translatiramo duž rijeke, onda je svaka izometrija translacija za višekratnik broja t.

Zanimljivije su neprave izometrije forme f. Geometrijski, to su simetrije topografa slike koje obrću orijentaciju, tj. to su zrcalne simetrije. Algebarski, to su matrice s cjelobrojnim elementima $T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ za koje vrijedi $f(x, y) = f(ax + cy, bx + dy)$ i čija je determinanta jednaka -1. **Dvoznačne forme** su kvadratne forme koje imaju nepravu izometriju. Dvoznačne indefinitne forme stoga imaju, kako translacijsku simetriju M svoje rijeke, tako i zrcalnu simetriju T.

Kao i prave izometrije, i neprave moraju preslikavati rijeku u rijeku, pozitivne vrijednosti u pozitivne vrijednosti. Da bi se orijentacija obrnula, neprava izometrija mora promijeniti tok rijeke u jednom smjeru u tok suprotnog smjera. Iz toga slijedi da ako neprava izometrija T preslikava točku p na rijeci u točku q, tada izometrija T mora djelovati kao zrcaljenje s obzirom na pravac koji prolazi polovištem m, dužine $\overline{pq}$. Više o ovoj temi možete pronaći u [6, str. 288, 289].

Sve rijeke zavijaju te se zavoji koji nastaju mogu koristiti za klasifikaciju indefinitnih formi. Polazna točka klasifikacije je pomnija analiza vrijednosti u beskonačnom poligonu topografa slike.



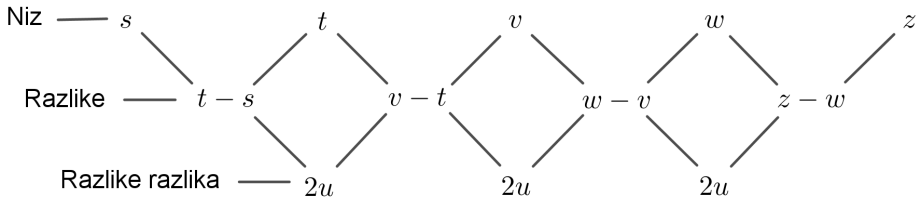
Propozicija 4.14. *Oko vrijednosti u, vrijednosti topografa slike čine kvadratni niz s* ***ubrzanjem*** $2u$*. Drugim riječima, niz razlika tvori aritmetički niz s konstantnom razlikom* $2u$*.*

Dokaz. Svojstvo aritmetičkog niza povlači

$$\begin{aligned}(v-t) &= (t-s)+2u\\ (w-v) &= (v-t)+2u\\ (z-w) &= (w-v)+2u\end{aligned}$$

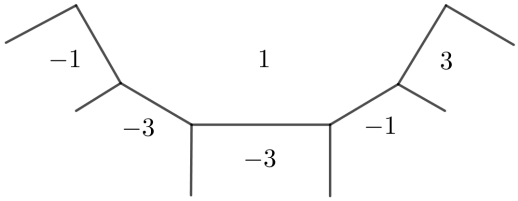
Naime, budući da t, $u+v$, w, čine aritmetički niz, vrijedi $w-(u+v)=(u+v)-t$. Iz toga slijedi $(w-v)=(v-t)+2u$. Preostale dvije jednakosti dobivamo analogno.

Otuda vidimo da je niz razlika za s, t, v, w, z aritmetički niz s razlikom $2u$.

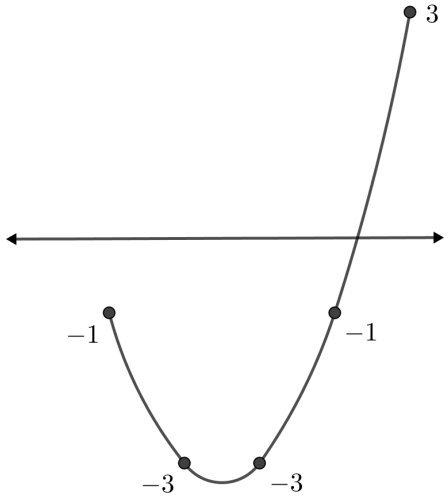


□

Vrijednosti kvadratnog niza leže na paraboli pri čemu jedinični pomak lijevo ili desno odgovara prethodnom ili idućem članu niza. Primjerice, na Slici 4.11 je grafički prikaz kvadratnog niza sa Slike 4.10.



Slika 4.10: Kvadratni niz

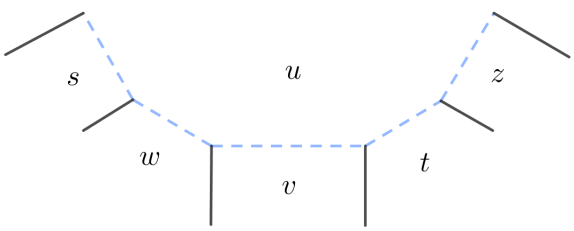


Slika 4.11: Grafički prikaz kvadratnog niza sa Slike 4.10.

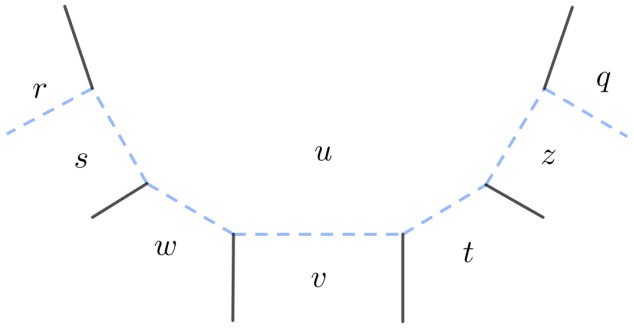
Degenerirani slučaj se događa kada je $u = 0$. U ovom slučaju, vrijednosti oko u čine kvadratni niz s ubrzanjem 0 te je ovo aritmetički niz. Ovaj slučaj smo vidjeli kada smo primijetili da vrijednosti oko jezera čine aritmetički niz. U nastavku će nas zanimati samo slučaj kada je $u \neq 0$.

Korolar 4.15. *Rijeka može zauzeti samo konačno mnogo bridova beskonačnog poligona.*

Dokaz. Slijedimo rijeku duž bridova beskonačnog poligona.



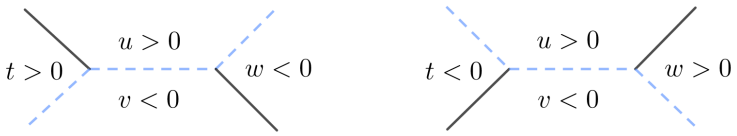
Ako je vrijednost u pozitivna, tada su vrijednosti preko rijeke negativne. Ali vrijednosti s, w, v, t, z čine kvadratni niz s pozitivnim ubrzanjem. Dakle, ako se dovoljno daleko udaljimo ulijevo i udesno, vrijednosti nasuprot u moraju promijeniti predznak s negativnih na pozitivne. Na tim prijelazima rijeka zavija.



Slika 4.12: Ako je $r > 0$ i $q > 0$, rijeka zavija kao što je ovdje prikazano.

Analogno rješavamo slučaj kada je $u < 0$. Tada dobivamo kvadratni niz s negativnim ubrzanjem. □

Riječni zavoji su orijentiri koji nam omogućuju razumijevanje indefinitnih binarnih kvadratnih formi bez jezera. Kvadratna forma f s diskriminantom $d > 0$, koja nije potpun kvadrat, mora sadržavati jedinstvenu beskrajnu rijeku, koja zavija lijevo i desno duž svog toka. Na svakom zavoju se nalaze dvije pozitivne i dvije negativne vrijednosti. Postoje dvije moguće orijentacije za riječne zavoje, koje su prikazane na slici dolje.



Riječni zavoji su orijentiri u topografima indefinitnih formi, slično kao što su vrela orijentiri za definitne forme. Ali ključna razlika čini indefinitne forme težima i zanimljivijima za proučavanje. Indefinitna forma može imati više riječnih zavoja duž rijeke, dok definitna forma ima jedinstveno vrelo.

Teorem 4.16 (Ograda minimalne vrijednosti indefinitne forme). *Neka je f binarna kvadratna forma s diskriminantom $d > 0$, koja nije potpun kvadrat. Najmanja (po apsolutnoj vrijednosti) nenul vrijednost koju f postiže je po apsolutnoj vrijednosti manja ili jednaka od $\sqrt{d/5}$.*

Dokaz. Takva kvadratna forma sadrži riječni zavoj u topografu slike. Računamo diskriminantu d kod riječnog zavoja, $d = (u - v)^2 - tw$. Raspisivanjem dobivamo

$$d = u^2 - uv - vu + v^2 - tw.$$

U bilo kojoj orijentaciji, vrijednosti u i v imaju suprotne predznake, kao i t i w. Iz toga slijedi da gornja jednakost prikazuje prirodan broj d kao zbroj pet prirodnih brojeva. Dakle, barem jedan od tih pet brojeva ne može biti veći od $d/5$. Uzimajući apsolutne vrijednosti, dobivamo

$$|u| \cdot |u| \leq \frac{d}{5} \quad \text{ili} \quad |u| \cdot |v| \leq \frac{d}{5} \quad \text{ili} \quad |v| \cdot |v| \leq \frac{d}{5} \quad \text{ili} \quad |t| \cdot |w| \leq \frac{d}{5}.$$

U svakom slučaju, umnožak dvaju prirodnih brojeva omeđen je s $d/5$. Stoga, barem jedan od dva cijela broja ne može biti veći od $\sqrt{d/5}$.

$$0 < |u| \leq \sqrt{\frac{d}{5}} \quad \text{ili} \quad 0 < |v| \leq \sqrt{\frac{d}{5}} \quad \text{ili} \quad 0 < |t| \leq \sqrt{\frac{d}{5}} \quad \text{ili} \quad 0 < |w| \leq \sqrt{\frac{d}{5}}.$$

Time smo dokazali teorem. □

Sada nam četiri svojstva omogućuju popisivanje svih riječnih zavoja (bilo koje orijentacije) određene pozitivne diskriminante koja nije potpun kvadrat.

1. Budući da je $u \geq 1$, $v \leq -1$, $tw \leq -1$ i $d = (u-v)^2 - tw$, vrijedi $2 \leq (u-v) \leq \sqrt{d-1}$.
2. Za svaku moguću vrijednost $(u - v)$ postoji $(u - v - 1)$ mogućih vrijednosti u i v koje zadovoljavaju nejednakosti $u \geq 1$ i $v \leq -1$.
3. Za svaku vrijednost $u - v$, imamo $tw = (u - v)^2 - d$.
4. Niz t, $(u + v)$, w je aritmetički niz.

Korolar 4.17 (**Konačnost broja klasa indefinitnih formi**). *Za dani prirodan broj d koji nije potpun kvadrat broj riječnih zavoja s diskriminantom d, a samim time i broj neekvivalentnih kvadratnih formi s diskriminantom d, je manji od* $2d - 2$.

Dokaz. Ima najviše $\sqrt{d-1}$ mogućnosti za vrijednost $(u - v)$ i za svaki izbor te razlike, postoji manje od $\sqrt{d-1}$ mogućih parova (u, v). Stoga, postoji manje od $d - 1$ mogućih parova (u, v). Svaki par (u, v) određuje najviše dva moguća para (t, w), jednog od svake orijentacije, budući da sustav jednadžbi

$$tw = (u - v)^2 - d, \quad \frac{t + w}{2} = u + v$$

u t i w predstavlja pravac i hiperbolu koji se sijeku u najviše dvije cjelobrojne točke. Dakle, postoji manje od $2(d - 1)$ riječnih zavoja. □

Sustav jednadžbi $tw = (u-v)^2 - d$ i $\frac{1}{2}(t+w) = u+v$ možemo riješiti izražavanjem t i w pomoću u i v.

$$t = u + v \pm \sqrt{d+4uv}.$$
$$w = u + v \mp \sqrt{d+4uv}.$$

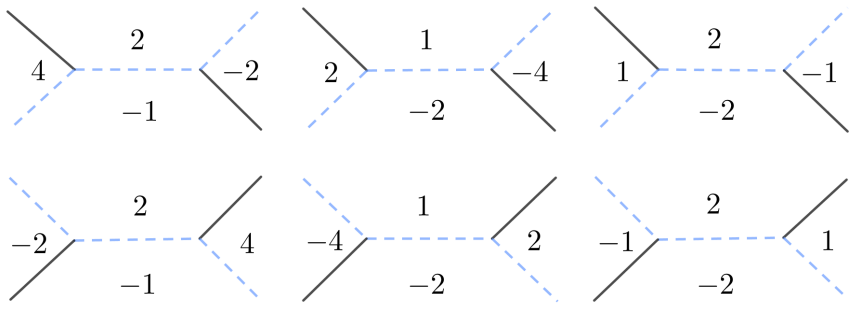
Stoga, da bismo pomoću vrijednosti u i v formirali riječni zavoj, nužno je da je broj $d+4uv$ potpun kvadrat.

Primjer 4.3. *Nađimo sve riječne zavoje s diskriminantom* 17.

Rješenje: Promotrimo riječni zavoj, bilo koje orijentacije, s diskriminantom 17. Budući da je $\sqrt{17-1} = 4$, vrijedi da je $2 \leq (u-v) \leq 4$. Na slici dolje, prikazujemo sve mogućnosti za vrijednosti u i v.

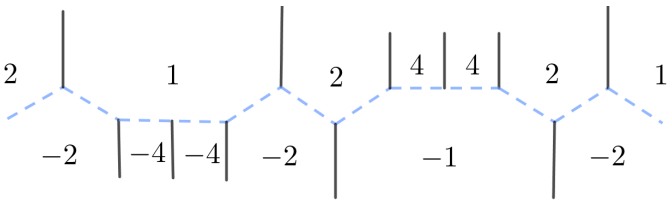
$u-v$	u	v	$d+4uv$	
2	1	-1	13	$-$
3	2	-1	9	$+$
3	1	-2	9	$+$
4	3	-1	5	$-$
4	2	-2	1	$+$
4	1	-3	5	$-$

Pojavljuju se tri mogućnosti za vrijednosti u, v kod kojih je $d+4uv$ potpun kvadrat. Svaka od njih ima dva izbora za orijentaciju, iz kojih dobivamo šest mogućih riječnih zavoja prikazanih na Slici 4.13. □



Slika 4.13: Mogući riječni zavoji.

Ako započnemo granati topograf slike s jednim od gornjih riječnih zavoja, i pratimo rijeku kroz cijeli jedan period, dobivamo donji topograf slike.



Svih šest riječnih zavoja se pojavljuje na istoj rijeci. Iz toga slijedi da esencijalno postoji samo jedna binarna kvadratna forma s diskriminantom 17. Svaka binarna kvadratna forma s diskriminantom 17 je pravo ekvivalentna formi $2x^2 + xy - 2y^2$. Drugim riječima, broj klasa diskriminante 17 je jednak 1.

Bibliografija

[1] D.A. Buell, *Binary quadratic forms. Classical theory and modern computations*, Springer-Verlag, New York, 1989.

[2] J.H. Conway, *The sensual (quadratic) form*, With the assistance of Francis Y. C. Fung. Carus Mathematical Monographs, 26. Mathematical Association of America, Washington, 1997.

[3] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb 2019.

[4] A. Dujella, *Uvod u teoriju brojeva*, dostupno na
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf` (prosinac 2019.)

[5] T. Pejković, *Lagrangeov i Markovljev spektar*, dostupno na
`https://web.math.pmf.unizg.hr/~pejkovic/files/lm.pdf` (prosinac 2019.)

[6] M.H. Weissman, *An Illustrated Theory of Numbers*, American Mathematical Society, Providence, 2017.

Sažetak

Binarna kvadratna forma je preslikavanje $f : \mathbb{R}^2 \to \mathbb{R}$ oblika

$$f(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z},$$

tj. homogeni polinom dviju varijabli drugog stupnja s cjelobrojnim koeficijentima.

U prvom poglavlju rada predstavljamo osnovne pojmove i rezultate o binarnim kvadratnim formama, poput ekvivalencije formi, njihovog matričnog zapisa i diskriminante. Također se bavimo problemom reprezentacije cijelog broja nekom kvadratnom formom i redukcijom pozitivno definitnih i indefinitnih formi. U drugom poglavlju opisujemo pojam topografa kojeg je osmislio engleski matematičar J. H. Conway. Topograf je izvanredan grafički pristup kvadratnim formama pomoću kojeg u trećem i četvrtom poglavlju opisujemo osnovna svojstva definitnih, semidefinitnih i indefinitnih kvadratnih formi s cjelobrojnim koeficijentima.

Summary

A binary quadratic form is a function $f : \mathbb{R}^2 \to \mathbb{R}$ of the general form

$$f(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}.$$

In other words, binary quadratic form is a homogeneous polynomial of degree two in two variables with integer coefficients.

In the first chapter of this master's thesis we present the basic concepts and results on binary quadratic forms, such as the equivalence of forms, their matrix notation, and the discriminant. We also deal with the problem of the representation of an integer by some quadratic form and the reduction of positive definite and indefinite forms. In the second chapter, we describe the concept of topograph invented by the English mathematician J. H. Conway. A topograph is an extraordinary visual approach to quadratic forms by which we describe in the third and fourth chapter the basic properties of definite, semidefinite and indefinite quadratic forms with integer coefficients.

Životopis

Rođena sam 19.4.1995. godine u Zadru. Osnovnu školu Petra Preradovića i opći smjer Gimnazije Franje Petrića pohađala sam u Zadru. Po završetku srednje škole, 2013. godine, upisala sam nastavnički smjer preddiplomskog studija Matematike na Prirodoslovno-matematičkom fakultetu u Zagrebu. Godine 2017. završila sam preddiplomski studij i upisala diplomski studij Matematika, smjer nastavnički na istom fakultetu.

Tijekom srednjoškolskog i fakultetskog obrazovanja radila sam za ljetnih sezona u uslužnim djelatnostima. Na tim poslovima sam poboljšala znanje engleskog i talijanskog jezika te stekla bolje komunikacijske vještine.