Rešetke i samodualni kodovi

Crnčić, Margareta

Sveučilište u Rijeci

Fakultet za matematiku

Sveučilišni diplomski studij Diskretna matematika i primjene

Margareta Crnčić

REŠETKE I SAMODUALNI KODOVI

Diplomski rad

Rijeka, rujan 2024.

Sveučilište u Rijeci

Fakultet za matematiku

Sveučilišni diplomski studij Diskretna matematika i primjene

Margareta Crnčić

REŠETKE I SAMODUALNI KODOVI

Mentor: doc. dr. sc. Sara Ban Martinović

Diplomski rad

Rijeka, rujan 2024.

Sadržaj

Sažetak

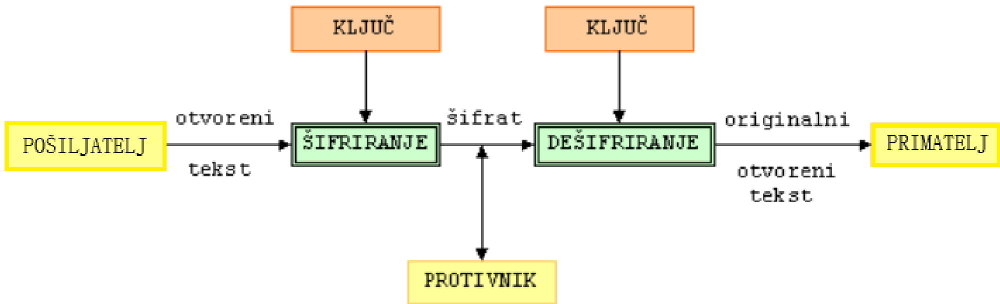
U ovom diplomskom radu bavit ćemo se linearnim kodovima, s posebnim naglaskom na binarne samodualne linearne kodove. Promotrit ćemo njihova svojstva i primjenu u teoriji rešetki. Pokrit ćemo osnovne pojmove i svojstva iz teorije rešetki za rešetke punog ranga nad poljem realnih brojeva. Nakon navođenja potrebnih osnovnih pojmova, navest ćemo poveznicu binarnih linearnih kodova i rešetki, pod nazivom konstrukcija A, te njezinu značajnu primjenu.

Ključne riječi

Linearni kodovi, binarni linearni kodovi, generirajuća matrica linearnog koda, samodualni kodovi, rešetke, generirajuća matrica rešetke, Gramova matrica rešetke, cjelobrojne rešetke, samodualne rešetke, konstrukcija A.

1 Uvod

Kodovi su osmišljeni kao sustav koji šifrira poruku prije slanja radi sigurnijeg prijenosa, kako bi se omogućila detekcija i ispravljanje pogrešaka uzrokovanih šumom i smetnjama u komunikacijskom kanalu (vidi sliku 1).



Slika 1: Komunikacijski sustav

Linearni kodovi, uključujući binarne linearne kodove, koriste generirajuće matrice za stvaranje kodnih riječi koje omogućuju učinkovito kodiranje i dekodiranje. Posebno su značajni samodualni kodovi zbog svojih svojstava koja poboljšavaju otpornost na pogreške.

Rešetke su matematičke strukture koje igraju ključnu ulogu u različitim područjima, uključujući teoriju brojeva, geometriju, kriptografiju i teoriju kodiranja. U kontekstu kriptografije, rešetke su se pokazale posebno korisnima za rješavanje problema koji su teški za klasične metode kao što su faktorizacija velikih brojeva ili diskretni logaritmi. Primjena rešetki u kriptografiji evoluirala je od inicijalnog korištenja za probijanje šifri do suvremenih primjena u kvantnoj kriptografiji, koja teži razvoju kriptosustava sigurnih protiv napada kvantnih računala.

Konstrukcija A je metoda koja povezuje teoriju linearnog kodiranja i teoriju rešetki. Ova metoda omogućuje konstrukciju rešetki iz linearnog koda. Svojstva kodova poput samodualnosti se prenose na rešetku, što omogućuje dodatnu otpornost na pogreške i sigurnosne prednosti. Konstrukcija A posebno je važna u kriptografiji i teoriji informacija, gdje omogućuje stvaranje rešetki otpornijih na kvantne napade.

2 Osnovni pojmovi iz linearne algebre

Prije no što krenemo na temu ovog diplomskog rada, navest ćemo pojmove iz linearne algebre koje ćemo koristiti u nastavku rada.

Definicija 2.1. Neka je G skup i $\circ : G \times G \to G$ binarna operacija na G. Uređeni par $(G, \circ)$ koji zadovoljava sljedeća svojstva:

1. $x \circ (y \circ z) = (x \circ y) \circ z \quad \forall x, y, z \in G$,
2. $(\exists e \in G)(\forall x \in G) \quad x \circ e = e \circ x = x$,
3. $(\forall x \in G)(\exists x^{-1} \in G) \quad x \circ x^{-1} = x^{-1} \circ x = e$,

zovemo **grupom**.

Definicija 2.2. Neka je $(G, \circ)$ grupa. Kažemo da je G **Abelova grupa** ako zadovoljava sljedeće svojstvo:

$$x \circ y = y \circ x \quad \forall x, y \in G.$$

Definicija 2.3. Neka je $(G, \circ)$ grupa i neka je $H \subseteq G$, $H \neq \emptyset$. Kažemo da je H **podgrupa** grupe G ako je $(H, \circ)$ grupa. Pišemo $H \leq G$.

Definicija 2.4. Neka je $\mathbb{F}$ neprazan skup na kojem su zadane dvije binarne operacije, zbrajanja $(+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F})$ i množenja $(\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F})$. Uređena trojka $(\mathbb{F}, +, \cdot)$ je **polje** ako vrijede sljedeća svojstva:

1. $(\mathbb{F}, +)$ je Abelova grupa,
2. $(\mathbb{F}\backslash\{0\}, \cdot)$, je Abelova grupa,
3. $x \cdot (y + z) = x \cdot y + x \cdot z$, za sve $x, y, z \in \mathbb{F}$.

Primjer 2.1. Primjeri polja:

1. $(\mathbb{R}, +, \cdot)$, gdje je $\mathbb{R}$ skup svih relanih brojeva, $+$ je zbrajanje, a $\cdot$ množenje realnih brojeva.
2. $(\mathbb{C}, +, \cdot)$, gdje je $\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$ skup svih kompleksnih brojeva, uz operacije:
   - zbrajanja: $z_1 + z_2 = x_1 + x_2 + (y_1 + y_2)i$,
   - množenja: $z_1 \cdot z_2 = (x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)i$,

   gdje su $z_1 = x_1 + y_1i, z_2 = x_2 + y_2i \in \mathbb{C}$.
3. $(\mathbb{F}_2, +_2, \cdot_2)$, gdje je $\mathbb{F}_2 = \{0, 1\}$, uz operacije:
   - zbrajanja: $x +_2 y = x + y \pmod 2$,
   - množenja: $x \cdot_2 y = x \cdot y \pmod 2$,

gdje su $x, y \in \mathbb{F}_2$.

Napomena 2.1. Neka je $z = a + bi \in \mathbb{C}$, gdje su $a, b \in \mathbb{R}$. Tada je njegov kompleksno konjugirani broj $\overline{z}$ definiran kao:

$$\overline{z} = a - bi.$$

Definicija 2.5. Neka je $\mathbb{F}$ polje i $m, n \in \mathbb{N}$. Svako preslikavanje $A : \{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\} \to \mathbb{F}$ se naziva **matrica** reda $m \times n$ nad poljem $\mathbb{F}$.
Pišemo $A(i, j) := a_{ij} \in \mathbb{F}$ ili kraće $A = [a_{ij}]$, te

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}.$$

Skup svih matrica reda $m \times n$ nad poljem $\mathbb{F}$ označavamo sa $M_{m,n}(\mathbb{F})$, a skup svih matrica reda $n \times n$ nad poljem $\mathbb{F}$ označavamo sa $M_n(\mathbb{F})$.

Definicija 2.6. Neka je $A = [a_{ij}] \in M_{m,n}(\mathbb{F})$ matrica i $\alpha \in \mathbb{F}$. Tada matricu $\alpha A = [b_{ij}]$ definiramo sa:

$$b_{ij} = \alpha a_{ij}, \quad i = 1, \ldots, m,\ j = 1, \ldots, n.$$

Definicija 2.7. Neka su $A = [a_{ij}], B = [b_{ij}] \in M_{m,n}(\mathbb{F})$ matrice. Tada matricu $A + B = [c_{ij}]$ definiramo sa:

$$c_{ij} = a_{ij} + b_{ij}, \quad i = 1, \ldots, m,\ j = 1, \ldots, n.$$

Definicija 2.8. Neka su $A = [a_{ij}] \in M_{m,n}(\mathbb{F})$ i $B = [b_{ij}] \in M_{n,p}(\mathbb{F})$ matrice. Matrica $AB = [c_{ij}]$ se definira sa:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \quad i = 1, \ldots, m,\ j = 1, \ldots, p.$$

Definicija 2.9. Jedinična matrica $I_n \in M_n(\mathbb{F})$ je matrica

$$I_n = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix}.$$

Definicija 2.10. Neka je S konačan skup. Svako bijektivno preslikavanje $\sigma : S \to S$ nazivamo **permutacijom**.

Definicija 2.11. Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$ matrica. **Determinanta matrice** A, u oznaci $\det A$ ili $\det(A)$, je:

$$\det(A) = \sum_{\sigma \in S_n} (-1)^{I(\sigma)} \prod_{i=1}^{n} a_{i,\sigma(i)},$$

gdje je S_n skup svih permutacija skupa $\{1, 2, \ldots, n\}$, a $I(\sigma)$ je broj inverzija [1] permutacije σ.

Primjer 2.2. Za matricu $A = [a_{ij}] \in M_2(\mathbb{F})$ vrijedi

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}.$$

Teorem 2.1. Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$, za $n \geq 2$. Tada $\det A$ možemo izračunati pomoću **Laplacovog razvoja**:

- duž i-tog retka: $\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \cdot M_{ij}$, $i = 1, \ldots, n$,
- duž j-tog stupca: $\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \cdot M_{ij}$, $j = 1, \ldots, n$,

matrice A, gdje je M_{ij} determinanta matrice koja se dobije iz A brisanjem i-tog reda i j-tog stupca, za $i, j = 1, \ldots, n$.

Definicija 2.12. Kažemo da je matrica $A \in M_n(\mathbb{F})$ **regularna matrica** ako postoji matrica $B \in M_n(\mathbb{F})$ za koju vrijedi:

$$AB = BA = I_n.$$

Ako postoji takva matrica B, zovemo je **inverzna matrica** matrice A, te ju označavamo sa A^{-1}.

Teorem 2.2. Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$ matrica. Tada vrijedi sljedeće: matrica A je regularna ako i samo ako je $\det(A) \neq 0$.

Dokaz teorema 2.2 može se pronaći u [6].

Definicija 2.13. Neka je $A \in M_{mn}(\mathbb{F})$. Tada matricu $A^\top = [b_{ij}] \in M_{nm}(\mathbb{F})$, gdje je $b_{ij} = a_{ji}$, za $i = 1, \ldots, n$, $j = 1, \ldots, m$, zovemo **transponiranom matricom** matrice A.

Teorem 2.3. Neka su $A \in M_{m,n}(\mathbb{F})$ i $B \in M_{n,m}(\mathbb{F})$ matrice. Tada vrijedi:

$$(AB)^\top = B^\top A^\top.$$

Teorem 2.4. Neka je $A \in M_n(\mathbb{F})$ matrica i $A^\top$ njena transponirana matrica. Tada vrijedi:

$$\det A = \det A^\top.$$

Dokaze teorema 2.3 i 2.4 može se pronaći u [6], kao i dokaz sljedećeg teorema.

Teorem 2.5. Neka je $M = \begin{bmatrix} A & C \\ O & B \end{bmatrix}$ blok matrica, gdje su $A \in M_n(\mathbb{F})$, $B \in M_m(\mathbb{F})$, $C \in M_{n,m}(\mathbb{F})$ i $O \in M_{m,n}(\mathbb{F})$ je **nulmatrica** (matrica kojoj su sve vrijednosti 0). Tada vrijedi:

$$\det(M) = \det(A) \cdot \det(B).$$

[1]Neka je $\sigma = (i_1, i_2, \ldots, i_n)$ permutacija na skupu $X = \{1, 2, \ldots, n\}$. Inverzija je uređeni par (i_k, i_l) takav da i_k prethodi i_l i $i_k > i_l$.

Definicija 2.14. Za matricu $A \in M_n(\mathbb{F})$ kažemo da je **ortogonalna** ako je $A^\top A = AA^\top = I_n$.

Definicija 2.15. Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$ matrica. Neka je M_{ij} determinanta matrice koja se dobije iz A brisanjem i-tog reda i j-tog stupca. Tada je **adjunkta** od A matrica

$$\mathrm{adj}(A) = [c_{ij}],$$

gdje je $c_{ij} = (-1)^{i+j} M_{ji}$, $i, j = 1, \ldots, n$.

Definicija 2.16. Neka je $A = [a_{ij}] \in M_n(\mathbb{R})$, gdje je $a_{ij} \in \mathbb{Z}$. Kažemo da je A **unimodularna matrica** ako je $\det A \in \{-1, 1\}$.

Teorem 2.6. (Binet-Cauchy) Neka su $A \in M_n(\mathbb{F})$ i $B \in M_n(\mathbb{F})$ matrice. Tada vrijedi sljedeće:

$$\det(AB) = \det A \det B.$$

Teorem 2.7. Neka je $A \in M_n(\mathbb{F})$ matrica i $\lambda \in \mathbb{F}$. Tada vrijedi:

$$\det(\lambda A) = \lambda^n \det(A).$$

Dokaze teorema 2.6 i 2.7 se može pronaći u [6].

Propozicija 2.1. Neka je $A = [a_{ij}] \in M_n(\mathbb{F})$ regularna matrica. Tada su i matrice $A^\top, A^{-1}$, $(A^\top)^{-1}$ te $AA^\top$ regularne matrice.

Dokaz propozicije slijedi iz teorema 2.2, 2.4 i 2.6.

Teorem 2.8. Neka je $A \in M_n(\mathbb{F})$ matrica i neka je $\det A \neq 0$. Tada vrijedi:

$$A^{-1} = (\det A)^{-1} \mathrm{adj}(A).$$

Dokaze prethodnog teorema može se pronaći u [6].

Definicija 2.17. Neka je $V \neq \emptyset$ i $(\mathbb{F}, +, \cdot)$ polje. Neka su zadane operacije zbrajanja $+ : V \times V \to V$ i vanjskog množenja $\cdot : \mathbb{F} \times V \to V$. Uređena trojka $(V, +, \cdot)$ se naziva **vektorski prostor** nad poljem $\mathbb{F}$ ako vrijedi:

(V1) $(V, +)$ Abelova grupa,

(V2) $(\alpha + \beta) \cdot \mathbf{x} = \alpha \cdot \mathbf{x} + \beta \cdot \mathbf{x}, \quad \forall \alpha, \beta \in \mathbb{F}, \forall \mathbf{x} \in V$,

(V3) $\alpha \cdot (\mathbf{x} + \mathbf{y}) = \alpha \cdot \mathbf{x} + \alpha \cdot \mathbf{y}, \quad \forall \alpha \in \mathbb{F}, \forall \mathbf{x}, \mathbf{y} \in V$,

(V4) $\alpha \cdot (\beta \cdot \mathbf{x}) = (\alpha\beta) \cdot \mathbf{x}, \quad \forall \alpha, \beta \in \mathbb{F}, \forall \mathbf{x} \in V$,

(V5) $1 \cdot \mathbf{x} = \mathbf{x}, \quad \forall \mathbf{x} \in V$.

Elemente vektorskog prostora nazivamo **vektorima**.

Primjer 2.3. Skup $\mathbb{F}^n = \{(x_1, x_2, \dots, x_n) \mid x_i \in \mathbb{F},\ i = 1, 2, \dots, n\}$ je vektorski prostor nad $\mathbb{F}$ uz sljedeće operacije:

$$\mathbf{u} + \mathbf{v} = (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n),$$
$$\alpha\mathbf{u} = (\alpha u_1, \alpha u_2, \dots, \alpha u_n),$$

za $\mathbf{u} = (u_1, u_2, \dots, u_n), \mathbf{v} = (v_1, v_2, \dots, v_n) \in \mathbb{F}^n$ i $\alpha \in \mathbb{F}$.

Definicija 2.18. Neka je V vektorski prostor i $U \subseteq V$, $U \neq \emptyset$. U je **vektorski potprostor** od V, u oznaci $U \leq V$, ako je U i sam vektorski prostor s naslijeđenim operacijama.

Teorem 2.9. (Kriterij za potprostor) Neka je V vektorski prostor nad $\mathbb{F}$ i $\emptyset \neq U \subseteq V$. Tada je $U \leq V$ ako i samo ako vrijedi:

$$\alpha\mathbf{x} + \beta\mathbf{y} \in U, \quad \forall \alpha, \beta \in \mathbb{F}, \forall \mathbf{x}, \mathbf{y} \in U.$$

Dokaz ovog teorema može se pronaći u [6]

Definicija 2.19. Neka je V vektorski prostor nad poljem $\mathbb{F}$, $\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n} \in V$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}$. Tada se vektor

$$\alpha_1\mathbf{v_1} + \alpha_2\mathbf{v_2} + \cdots + \alpha_n\mathbf{v_n}$$

naziva **linearna kombinacija vektora $\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n}$** s koeficijentima $\alpha_1, \alpha_2, \dots, \alpha_n$. Skup

$$\{\alpha_1\mathbf{v_1} + \alpha_2\mathbf{v_2} + \cdots + \alpha_n\mathbf{v_n} \mid \alpha_i \in \mathbb{F}, 1 \leq i \leq n\}$$

nazivamo **linearna ljuska** vektora $\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n}$, te je označavamo sa $[\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n}]$.

Definicija 2.20. Neka je V vektorski prostor nad poljem $\mathbb{F}$. Kažemo da je vektor **0 nulvektor** ako za svaki vektor $\mathbf{v} \in V$ vrijedi

$$\mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v} = \mathbf{v}.$$

Definicija 2.21. Neka je V vektorski prostor nad poljem $\mathbb{F}$. Skup vektora $\{\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n}\} \subseteq V$ je **linearno nezavisan** ako vrijedi

$$\alpha_1\mathbf{v_1} + \alpha_2\mathbf{v_2} + \cdots + \alpha_n\mathbf{v_n} = \mathbf{0} \Rightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0, \quad \alpha_i \in \mathbb{F}, 1 \leq i \leq n,$$

gdje je **0** nulvektor.
U suprotnom kažemo da je skup $\{\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n}\}$ **linearno zavisan**.

Definicija 2.22. Neka je V vektorski prostor nad poljem $\mathbb{F}$. Neka je $B \subseteq V$ bilo koji neprazan linearno nezavisan skup vektora iz V. Kažemo da je B **baza** vektorskog prostora ako vrijedi $[B] = V$. Broj vektora u bazi B zovemo **dimenzijom vektorskog prostora** V i označavamo je sa $\dim V$.

Definicija 2.23. Rang matrice A je maksimalni broj linearno nezavisnih redaka ili stupaca matrice.

Napomena 2.2. Skup svih matrica $M_{n,m}(\mathbb{F})$ je vektorski prostor uz prethodno definirano zbrajanje matrica i množenje matrica skalarom.

Definicija 2.24. Neka su U, V vektorski prostori nad poljem $\mathbb{F}$. Preslikavanje $f : U \to V$ naziva se **linearni operator** ako vrijedi:

1. $f(\mathbf{x}+\mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y}), \forall \mathbf{x}, \mathbf{y} \in U$,

2. $f(\alpha\mathbf{x}) = \alpha f(\mathbf{x}), \forall \alpha \in \mathbb{F}, \forall \mathbf{x} \in U$.

Definicija 2.25. Neka su U, V vektorski prostori nad poljem $\mathbb{F}$ dimenzije n i m, redom. Neka je $f : U \to V$ linearni operator. Neka je $B_1 = (a_1, \ldots, a_n)$ baza za U, a $B_2 = (b_1, \ldots, b_m)$ baza za V. Neka je

$$f(a_k) = \sum_{i=1}^{m} a_{ik} b_i, \quad k = 1, \ldots, n.$$

Kako je operator jednoznačno zadan svojim djelovanjem na bazi B_1 (za više o tome vidi [6]), on je jednoznačno određen matricom

$$F = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \ddots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}.$$

Matricu F nazivamo **matrični zapis** linearnog operatora f.

Definicija 2.26. Neka je $f : V \to W$ linearni operator. **Jezgra** linearnog operatora f, u oznaci $\mathrm{Ker}(f)$, je:

$$\mathrm{Ker}(f) = \{\mathbf{v} \in V \mid f(\mathbf{v}) = \mathbf{0}\}.$$

Defekt linearnog operatora f je $d(f) = \dim(\mathrm{Ker}(f))$.
Slika linearnog operatora f, u oznaci $\mathrm{Im}(f)$, je:

$$\mathrm{Im}(f) = \{f(\mathbf{v}) \mid \mathbf{v} \in V\}.$$

Nadalje, **rang** linearnog operatora f je $r(f) = \dim(\mathrm{Im}(f))$.

Teorem 2.10. (Teorem o rangu i defektu) Neka je $f : U \to V$ linearni operator. Tada vrijedi:

$$r(f) + d(f) = \dim U.$$

Dokaz prethodnog teorema može se pronaći u [6].

Definicija 2.27. Neka je V vektorski prostor nad poljem $\mathbb{F}$, gdje je $\mathbb{F} = \mathbb{R}$ ili $\mathbb{C}$. **Skalarni produkt** je preslikavanje $\cdot : V \times V \to \mathbb{F}$ sa svojstvima:

(S1) $\mathbf{x} \cdot \mathbf{x} \geq 0, \quad \forall \mathbf{x} \in V$, (S2) $\mathbf{x} \cdot \mathbf{x} = 0 \Leftrightarrow \mathbf{x} = \mathbf{0}$,

(S3) $\mathbf{x} \cdot \mathbf{y} = \overline{\mathbf{y} \cdot \mathbf{x}}, \quad \forall \mathbf{x}, \mathbf{y} \in V$,

(S4) $(\mathbf{x} + \mathbf{y}) \cdot \mathbf{z} = (\mathbf{x} \cdot \mathbf{z}) + \mathbf{y} \cdot \mathbf{z}, \quad \forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in V$,

(S5) $(\alpha \mathbf{x}) \cdot \mathbf{y} = \alpha(\mathbf{x} \cdot \mathbf{y}), \quad \mathbf{x}, \mathbf{y} \in V,\ \alpha \in \mathbb{F}$.

Primjer 2.4. **Standardni skalarni produkt** vektora u $\mathbb{R}^n$ je preslikavanje $\cdot : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ definirano s

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i, \quad \text{za } \mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{R}^n.$$

Definicija 2.28. Neka je X neprazan skup. Za funkciju $d : X \times X \to \mathbb{R}$ kažemo da je **metrika** na skupu X ako za sve $x, y, z \in X$ vrijedi:

(M1) $d(x, y) \geq 0$,

(M2) $d(x, y) = 0 \Leftrightarrow x = y$,

(M3) $d(x, y) = d(y, x)$,

(M4) $d(x, y) \leq d(x, z) + d(z, y)$.

Definicija 2.29. Neka je V vektorski prostor nad poljem $\mathbb{F} = \mathbb{R}$ ili $\mathbb{C}$. Kažemo da je preslikavanje $|| \cdot || : V \to \mathbb{R}$ **norma** na V ako vrijede sljedeća svojstva:

(N1) $||\mathbf{x}|| \geq 0, \forall \mathbf{x} \in V$,

(N2) $||\mathbf{x}|| = 0 \Leftrightarrow \mathbf{x} = \mathbf{0}$,

(N3) $||\alpha \mathbf{x}|| = |\alpha| \cdot ||\mathbf{x}||, \forall \mathbf{x} \in V, \forall \alpha \in \mathbb{F}$,

(N4) $||\mathbf{x} + \mathbf{y}|| \leq ||\mathbf{x}|| + ||\mathbf{y}||, \forall \mathbf{x}, \mathbf{y} \in V$.

3 Linearni kodovi

Definicija 3.1. Neka je $\mathbb{F}_q$ konačno polje s q elemenata, gdje je q potencija prostog broja i neka je $n \in \mathbb{N}$. Potprostor $\mathcal{C}$ od $\mathbb{F}_q^n$ dimenzije k nazivamo $[n.k]$ **linearnim kodom** nad $\mathbb{F}_q$. Vektorski prostor $\mathbb{F}_q^n$ nazivamo **prostorom koda** $\mathcal{C}$, elemente koda $\mathcal{C}$ nazivamo **riječima koda** $\mathcal{C}$, broj $|\mathcal{C}|$ **veličinom koda** $\mathcal{C}$, a broj n **duljinom koda** $\mathcal{C}$.

Teorem 3.1. Neka je $\mathcal{C}$ $[n,k]$ linearni kod nad $\mathbb{F}_q$. Tada je: $|\mathcal{C}| = q^k$.

Dokaz ovog teorema se može pronaći u [2].

Linearni kodovi nad poljem $\mathbb{F}_2$ se nazivaju **binarni kodovi**. U radu ćemo se baviti s takvim kodovima.

Primjer 3.1. Neka je $\mathcal{C}_1 = \{(0,0),(1,1)\}$. Tada je $\{(1,1)\}$ baza za $\mathcal{C}_1$ pa je $\mathcal{C}_1$ binarni $[2,1]$ kod.

Definicija 3.2. Neka su $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$. **Hammingova udaljenost** između riječi $\mathbf{x}$ i $\mathbf{y}$, u oznaci $d_H(\mathbf{x}, \mathbf{y})$, je broj pozicija na kojima se riječi $\mathbf{x}$ i $\mathbf{y}$ razlikuju:

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i \mid x_i \neq y_i, 1 \leq i \leq n\}|.$$

Hammingova udaljenost d_H zadovoljava svojstva iz definicije 2.28, pa je to metrika na $\mathbb{F}_q^n$.

Definicija 3.3. **Minimalna Hammingova udaljenost** $[n,k]$ koda $\mathcal{C}$ je broj

$$d = d(\mathcal{C}) = \min\{d_H(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}.$$

Tada kažemo da je $\mathcal{C}$ $[n,k,d]$ kod.

Napomena 3.1. U primjeru 3.1 možemo uočiti da je $d = 2$. Stoga je $\mathcal{C}_1$ binarni $[2,1,2]$ kod.

Definicija 3.4. **Težina riječi** $\mathbf{x} \in \mathcal{C}$ je broj:

$$w(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0}), \text{ gdje je } \mathbf{0} = (0, 0, \ldots, 0).$$

Težinski enumerator $[n,k]$ koda $\mathcal{C}$ je polinom

$$A(x) = \sum_{i=0}^{n} A_i x^i,$$

gdje je A_i broj riječi težine i u kodu $\mathcal{C}$, za $i = 0, \ldots, n$.

Lema 3.1. Neka je $\mathcal{C}$ $[n,k,d]$ kod. Tada vrijedi:

1. $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$, $\forall \mathbf{x}, \mathbf{y} \in \mathcal{C}$,
2. $d = \min\limits_{\mathbf{x} \in \mathcal{C} \setminus \{\mathbf{0}\}} w(\mathbf{x})$.

Dokaz prethodne leme se može pronaći u [1].

Najčešći način definiranja linearnih kodova je pomoću generirajuće matrice, kako bi izbjegli pisanje svih riječi koda.

Definicija 3.5. Neka je $\mathcal{C}$ linearan $[n,k]$ kod. **Generirajuća matrica** koda $\mathcal{C}$ je matrica reda $k \times n$ čiji su retci vektori baze prostora $\mathcal{C}$.

Primjer 3.2. Odredimo minimalnu udaljenost d binarnog koda $\mathcal{C}_2$ zadanog generirajućom matricom:

$$G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Odredimo i težinski enumerator zadanog koda.

Po definiciji 3.5, $w_1 = (1,0,1)$ i $w_2 = (0,1,1)$ su vektori baze koda $\mathcal{C}_2$, stoga su

$$\begin{aligned} 0 \cdot (1,0,1) + 0 \cdot (0,1,1) &= (0,0,0), \\ 1 \cdot (1,0,1) + 0 \cdot (0,1,1) &= (1,0,1), \\ 0 \cdot (1,0,1) + 1 \cdot (0,1,1) &= (0,1,1), \\ 1 \cdot (1,0,1) + 1 \cdot (0,1,1) &= (1,1,0) \end{aligned}$$

riječi koda $\mathcal{C}_2$, to jest $\mathcal{C}_2 = \{(0,0,0),(1,0,1),(0,1,1),(1,1,0)\}$. Odredimo sada težine svih nenul riječi u kodu $\mathcal{C}_2$:

$$w(1,0,1) = 2, \quad w(0,1,1) = 2, \quad w(1,1,0) = 2.$$

Prema lemi 3.1, minimalna udaljenost koda je $d = 2$. Dakle, $\mathcal{C}_2$ je binarni $[3,2,2]$ kod.
Zapišimo sada težinski enumerator koda $\mathcal{C}_2$:

$$A(x) = 1 \cdot x^0 + 0 \cdot x^1 + 3 \cdot x^2 + 0 \cdot x^3 = 1 + 3 \cdot x^2.$$

Definicija 3.6. Kažemo da je generirajuća matrica G $[n,k]$ koda u **standardnom obliku** ako postoji $k \times (n-k)$ matrica C takva da je: $G = [I_k \mid C]$, gdje je I_k jedinična matrica reda k.

Napomena 3.2. Uočimo da je generirajuća matrica G_2 binarnog $[3,2,2]$ koda $\mathcal{C}_2$ iz primjera 3.2 u standardnom obliku:

$$G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right].$$

Definicija 3.7. Neka su $\mathcal{C}_1$ i $\mathcal{C}_2$ dva linearna koda nad $\mathbb{F}_q$. Kažemo da su kodovi $\mathcal{C}_1$ i $\mathcal{C}_2$ **ekvivalentni** ako se jedan može dobiti iz drugoga:

1. proizvoljnom permutacijom koordinatnih mjesta u svim kodnim riječima,

2. množenjem s bilo kojim nenul elemenatom iz $\mathbb{F}_q$ na bilo kojoj koordinatnoj poziciji.

Napomena 3.3. Ekvivalentni kodovi imaju iste parametre $[n,k,d]$.

Teorem 3.2. Dvije generirajuće matrice iz $M_{n,k}(\mathbb{F}_q)$ generiraju ekvivalentne kodove ako se jedna matrica može dobiti iz druge pomoću sljedećih operacija:

1. permutacijom redaka,

2. množenjem retka s nenul elementom iz $\mathbb{F}_q$,

3. dodavanjem retka pomnoženog s elementom iz $\mathbb{F}_q$ nekom drugom retku,

4. permutacijom stupaca,

5. množenjem stupca s nenul elementom iz $\mathbb{F}_q$.

Teorem 3.3. Za generirajuću matricu G linearnog koda $\mathcal{C}$ postoji kod $\mathcal{C}_0$ koji je ekvivalentan kodu $\mathcal{C}$, čija generirajuća matrica je u standardnom obliku.

Dokazi teorema 3.2 i 3.3 se mogu pronaći u [5].

3.1 Samodualni kodovi

Definicija 3.8. Neka je $\mathcal{C}$ $[n,k,d]$ kod nad $\mathbb{F}_q$. **Dualni kod** koda $\mathcal{C}$ je:

$$\mathcal{C}^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x} \cdot \mathbf{c} = 0, \forall \mathbf{c} \in \mathcal{C}\},$$

gdje je $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i$, $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.

Primjer 3.3. Odredimo dualni kod $\mathcal{C}_1^{\perp}$ koda $\mathcal{C}_1$ iz primjera 3.1.

Uzmimo proizvoljan $\mathbf{x} = (x_1, x_2) \in \mathbb{F}_2^2$.

$$\begin{aligned} (x_1, x_2) \cdot (0,0) = (0,0) \quad &\Rightarrow \quad x_1,\, x_2 \in \mathbb{F}_2^2, \\ (x_1, x_2) \cdot (1,1) = (0,0) \quad &\Rightarrow \quad x_1 + x_2 = 0. \end{aligned}$$

Slijedi da je $\mathcal{C}_1^{\perp} = \{(0,0), (1,1)\}$.

Propozicija 3.1. Vrijedi: $(\mathcal{C}^{\perp})^{\perp} \supseteq \mathcal{C}$.

Dokaz. Neka je $\mathbf{c} \in \mathcal{C}$. Tada je za svaki $\mathbf{x} \in \mathcal{C}^{\perp}$ $\mathbf{c} \cdot \mathbf{x} = 0$. Slijedi da je: $\mathbf{c} \in (\mathcal{C}^{\perp})^{\perp}$. □

Propozicija 3.2. Za proizvoljan kod $\mathcal{C}$ njegov dualni kod $\mathcal{C}^{\perp}$ je linearan.

Dokaz. Neka je $\mathcal{C}$ linearni kod duljine n nad $\mathbb{F}_q$. Neka su $\mathbf{x}, \mathbf{y} \in \mathcal{C}^{\perp}$, te $\alpha, \beta \in \mathbb{F}_q$. Tada je i $\alpha\mathbf{x} + \beta\mathbf{y} \in \mathcal{C}^{\perp}$, zbog:

$$(\alpha\mathbf{x} + \beta\mathbf{y}) \cdot \mathbf{c} = \alpha(\mathbf{x} \cdot \mathbf{c}) + \beta(\mathbf{y} \cdot \mathbf{c}) = \alpha \cdot 0 + \beta \cdot 0 = 0, \forall \mathbf{c} \in \mathcal{C}.$$

Po teoremu 2.9, slijedi da je $\mathcal{C}^{\perp}$ vektorski prostor. □

Lema 3.2. Neka je $\mathcal{C}$ linearan $[n,k]$ kod nad poljem $\mathbb{F}_q$ s generirajućom matricom G i $\mathbf{v} \in \mathbb{F}_q^n$. Tada vrijedi:

$$\mathbf{v} \in \mathcal{C}^{\perp} \Leftrightarrow G\mathbf{v}^{\top} = 0.$$

Dokaz. Neka je $\mathbf{v} \in \mathcal{C}^\perp$. Budući da su retci od G riječi koda $\mathcal{C}$, tada očito vrijedi: $G\mathbf{v}^\top = 0$.
Obratno, neka je $G\mathbf{v}^\top = 0$. Označimo li retke od G sa $r_1, \ldots, r_k$, tada je: $\mathbf{v} \cdot r_i = 0, \forall i \in \{1, \ldots, k\}$.
Ako je $\mathbf{x} \in \mathcal{C}$, tada se može zapisati kao: $\mathbf{x} = \sum_{i=1}^{k} \lambda_i r_i$, za neke skalare $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_q$. Onda je:
$\mathbf{v} \cdot \mathbf{x} = \sum_{i=1}^{k} \lambda_i (\mathbf{v} \cdot r_i) = 0$. Slijedi da je $\mathbf{v} \in \mathcal{C}^\perp$. $\square$

Primjer 3.4. Odredimo dualni kod $\mathcal{C}_2^\perp$ koda $\mathcal{C}_2$ iz primjera 3.2.

Prema lemi 3.2 vrijedi:

$$\mathbf{v} \in \mathcal{C}_2^\perp \Leftrightarrow G_2 \cdot \mathbf{v}^\top = 0, \quad \mathbf{v} \in \mathbb{F}_2^3.$$

Uzmimo proizvoljan $\mathbf{v} = (v_1, v_2, v_3) \in \mathbb{F}_2^3$.

$$G_2 \cdot \mathbf{v}^\top = 0 \quad \Rightarrow \quad \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = 0$$

$$v_1 + v_3 = 0$$

$$v_2 + v_3 = 0$$

Slijedi da je $\mathcal{C}_2^\perp = \{(0,0,0), (1,1,1)\}$.

Teorem 3.4. Neka je $\mathcal{C}$ $[n,k]$ kod nad $\mathbb{F}_q$ s generirajućom matricom u standardnom obliku $G = [I_k \mid C]$. Tada njegov dualni kod $\mathcal{C}^\perp$ ima generirajuću matricu

$$G^\perp = [-C^\top \mid I_{n-k}].$$

Dokaz. Vrijedi:

$$G^\perp G^\top = \begin{bmatrix} -C^\top & I_{n-k} \end{bmatrix} \begin{bmatrix} I_k \\ C^\top \end{bmatrix} = -C^\top + C^\top = O,$$

gdje je O nulmatrica, iz čega slijedi tvrdnja teorema. $\square$

Lema 3.3. Neka je $\mathcal{C}$ linearan $[n,k]$ kod nad poljem $\mathbb{F}_q$. Tada je $\mathcal{C}^\perp$ linearan $[n, n-k]$ kod i $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Dokaz. Prema propoziciji 3.2 dualan kod $\mathcal{C}^\perp$ je linearan kod duljine n.
Pokažimo sada da je $\dim(\mathcal{C}^\perp) = n - k$. Prema lemi 3.2, vrijedi: $G \cdot \mathbf{v}^\top = 0, \quad \forall \mathbf{v} \in \mathcal{C}^\perp$. Prema teoremu 2.9 vrijedi: $r(G) + d(G) = \dim \mathbb{F}_q^n$, odnosno $\dim \mathcal{C} + \dim \mathcal{C}^\perp = n$, pa je $\dim \mathcal{C}^\perp = n - k$.
Pokažimo sada da je $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. Prema propoziciji 3.1, vrijedi $\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$ i $\dim \mathcal{C} = k$. Zbog $\dim(\mathcal{C}^\perp) = n - k$ slijedi $\dim(\mathcal{C}^\perp)^\perp = n - \dim(\mathcal{C}^\perp) = n - (n-k) = k$. Dakle, $\mathcal{C}$ je potprostor od $(\mathcal{C}^\perp)^\perp$ iste dimenzije kao $(\mathcal{C}^\perp)^\perp$, pa je: $\mathcal{C} = (\mathcal{C}^\perp)^\perp$. $\square$

Definicija 3.9. Linearni kod $\mathcal{C}$ je **samoortogonalan** ako je $\mathcal{C} \subseteq \mathcal{C}^\perp$.
Kažemo da je linearni kod $\mathcal{C}$ **samodualan** ako je $\mathcal{C} = \mathcal{C}^\perp$.

Teorem 3.5. Neka je $\mathcal{C}$ binarni samoortogonalni kod, tada je svim njegovim riječima težina paran broj.

Napomena 3.4. Uočimo da je kod $\mathcal{C}_1$ iz primjera 3.1 samodualan, dok kod $\mathcal{C}_2$ iz primjera 3.2 nije niti samoortogonalan niti samodualan kod.

Napomena 3.5. Neka je $\mathcal{C}$ binarni $[n, k]$ kod s generirajućom matricom G.

1. $\mathcal{C}$ je samoortogonalan ako i samo ako je $GG^\top = O$.

2. $\mathcal{C}$ je samodualan ako i samo ako je samoortogonalan i $k = \frac{n}{2}$.

Definicija 3.10. Kažemo da je binarni kod $\mathcal{C}$ **dvostruko paran** ako su mu težine svih riječi djeljive s 4.

Definicija 3.11. Kažemo da je binarni kod **tipa II** ako je on samodualan i dvostruko paran. Kažemo da je binarni kod **tipa I** ako je samodualan i nije dvostruko paran.

Napomena 3.6. Kako je kod $\mathcal{C}_1$ iz primjera 3.1 samodualan, a nije dvostruko paran, on je tipa I.

Teorem 3.6. Neka je $\mathcal{C}$ binarni linearni kod.

1. Ako je $\mathcal{C}$ samoortogonalan kod i ima generirajuću matricu čiji svaki redak ima težinu djeljivu s četiri, tada je $\mathcal{C}$ dvostruko paran.

2. Ako je $\mathcal{C}$ dvostruko paran, tada je $\mathcal{C}$ samoortogonalan kod.

Dokaz prethodnog teorema može se pronaći u [1].

Primjer 3.5. Neka je e_8 binarni kod zadan generirajućom matricom:

$$G_{e_8} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Kod e_8 se zove **prošireni** $[8, 4, 4]$ **Hammingov kod**. Provjerimo samodualnost koda e_8 pomoću napomene 3.5:

$$G_{e_8} G_{e_8}^\top = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Nadalje, iz parametara koda možemo vidjeti da vrijedi jednakost $k = \frac{n}{2}$, pa slijedi da je kod e_8 samodualan. Odredimo težine baznih riječi koda e_8:

$$w(1,0,0,0,1,1,0,1) = 4, \qquad w(0,1,0,0,1,0,1,1) = 4,$$
$$w(0,0,1,0,1,1,1,0) = 4, \qquad w(0,0,0,1,0,1,1,1) = 4.$$

Prema teoremu 3.6, vrijedi da je kod e_8 dvostruko paran. Stoga je kod e_8 tipa II.

4 Rešetke

Rešetka je skup točaka određenih cjelobrojnim linearnim kombinacijama podskupa neke baze u n-dimenzionalnom prostoru. Možemo je vizualizirati kao beskonačnu mrežu pravilno raspoređenih točaka.

Definicija 4.1. Neka su $n, m \in \mathbb{N}$, $m \leq n$, te $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ linearno nezavisan skup vektora iz $\mathbb{R}^n$. **Rešetka** Λ u $\mathbb{R}^n$ generirana skupom B je

$$\Lambda = \Lambda(B) = \left\{ \sum_{i=1}^{m} z_i \mathbf{v}_i \mid z_i \in \mathbb{Z},\, 1 \leq i \leq m \right\}.$$

Elemente rešetke Λ zovemo **točkama rešetke** Λ, dok skup B zovemo **bazom rešetke** Λ. Često se koristi sljedeći matrični zapis baze rešetke Λ:

$$M = \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{bmatrix}, \tag{1}$$

gdje je $\mathbf{v}_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, $i = 1, \ldots, m$. Matricu M nazivamo **generirajućom matricom** rešetke Λ. Nadalje, u radu ćemo definirati rešetke pomoću generirajuće matrice $M \in M_{m,n}(\mathbb{R})$ na sljedeći način:

$$\Lambda = \Lambda(M) = \{\mathbf{z}M \mid \mathbf{z} \in \mathbb{Z}^m\}.$$

Naime,

$$\begin{aligned} \mathbf{z}M &= \begin{bmatrix} z_1 & z_2 & \ldots & z_m \end{bmatrix} \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{bmatrix} \\ &= \begin{bmatrix} \sum_{i=1}^{m} z_i v_{i1} & \sum_{i=1}^{m} z_i v_{i2} & \ldots & \sum_{i=1}^{m} z_i v_{in} \end{bmatrix} \\ &= \sum_{i=1}^{m} z_i \mathbf{v}_i. \end{aligned}$$

Napomena 4.1. U radu ćemo koristiti i sljedeći način označavanja rešetke Λ generirane skupom $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$:

$$\Lambda = \Lambda(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m).$$

Definicija 4.2. Neka je Λ rešetka u $\mathbb{R}^n$ s generirajućom matricom $M \in M_{m,n}(\mathbb{R})$. **Gramova matrica** rešetke Λ je matrica $A = MM^\top \in M_m(\mathbb{R})$.

Gramova matrica $A = [a_{ij}]$ rešetke $\Lambda = \Lambda(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m)$ ima elemente

$$a_{ij} = \mathbf{v}_i \cdot \mathbf{v}_j = \sum_{k=1}^{n} v_{ik} v_{jk}, \quad i, j = 1, \ldots, m,$$

gdje je $\mathbf{v}_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, $i = 1, \ldots, m$. Dakle, elementi Gramove matrice A su standardni skalarni produkti u $\mathbb{R}^n$ vektora baze rešetke Λ.

Definicija 4.3. Neka je Λ rešetka u $\mathbb{R}^n$ s bazom B. Broj $|B| = m$ zovemo **dimenzijom rešetke** Λ, a broj n **rangom rešetke** Λ. Ako vrijedi $n = m$, tada kažemo da je Λ **rešetka punog ranga**.

Napomena 4.2. Uočimo da su za rešetku punog ranga Λ, generirajuća matrica M i Gramova matrica A regularne matrice.

Napomena 4.3. U nastavku ovog rada bavit ćemo se rešetkama punog ranga $\Lambda \subseteq \mathbb{R}^n$.

Definicija 4.4. Neka je Λ rešetka u $\mathbb{R}^n$ s bazom $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$. **Fundamentalna domena** rešetke Λ je skup

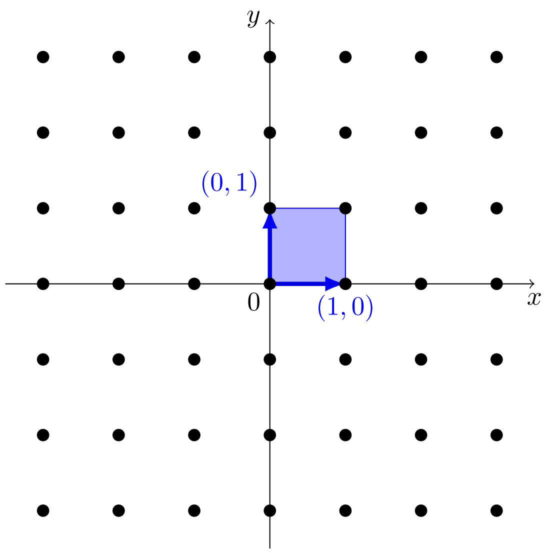
$$\mathcal{F} = \mathcal{F}(B) = \{t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_n\mathbf{v}_n \mid 0 \leq t_i < 1,\, 1 \leq i \leq n\}\,.$$

Primjer 4.1. Odredimo rešetku $\Lambda_1 = \Lambda_1(I_2)$ u $\mathbb{R}^2$.

Rešetka Λ_1 jednaka je:

$$\Lambda_1 = \Lambda_1(I_2) = \{\mathbf{z}I_2 \mid \mathbf{z} \in \mathbb{Z}^2\} = \{(z_1, z_2) \mid z_1, z_2 \in \mathbb{Z}\} = \mathbb{Z}^2,$$

to jest ona predstavlja skup svih točaka u ravnini s cjelobrojnim koordinatama. Na slici 2 prikazana je rešetka Λ_1 i njena fundamentalna domena obojena plavom bojom.



Slika 2: Fundamentalna domena rešetke $\mathbb{Z}^2$

Definicija 4.5. Neka je Λ rešetka u $\mathbb{R}^n$ s fundamentalnom domenom $\mathcal{F}$. **Determinanta rešetke** Λ je n-dimenzionalni volumen od $\mathcal{F}$. Označava se sa $\det \Lambda$.

Propozicija 4.1. Neka je Λ rešetka u $\mathbb{R}^n$ s generirajućom matricom M i fundamentalnom domenom $\mathcal{F}$. Tada za volumen od $\mathcal{F}$, u oznaci $\operatorname{Vol} \mathcal{F}$, vrijedi sljedeća jednakost:

$$\operatorname{Vol} \mathcal{F} = |\det M|.$$

Dokaz propozicije 4.1 može se naći u [2].

Iz propozicije 4.1 slijedi:

$$\det \Lambda = \text{Vol } \mathcal{F} = |\det M|. \tag{2}$$

Propozicija 4.2. Neka su M_1 i M_2 dvije generirajuće matrice rešetke Λ u $\mathbb{R}^n$, to jest neka je $\Lambda = \Lambda(M_1) = \Lambda(M_2)$. Tada postoji unimodularna matrica U takva da vrijedi:

$$M_1 = UM_2.$$

Dokaz. Neka su $B_1 = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ i $B_2 = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n\}$ dvije baze rešetke Λ u $\mathbb{R}^n$, $\mathbf{v}_i = (v_{1i}, \ldots, v_{in})$, $\mathbf{w}_i = (w_{i1}, \ldots, w_{in})$ za $i = 1, \ldots, n$, takve da su:

$$M_1 = \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \ldots & v_{nn} \end{bmatrix}, \quad M_2 = \begin{bmatrix} w_{11} & w_{12} & \ldots & w_{1n} \\ w_{21} & w_{22} & \ldots & w_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n1} & w_{n2} & \ldots & w_{nn} \end{bmatrix}.$$

Vektore iz B_2 možemo zapisati kao cjelobrojne linearne kombinacije vektora iz B_1, to jest:

$$\begin{aligned} \mathbf{w}_1 &= \alpha_{11}\mathbf{v}_1 + \alpha_{12}\mathbf{v}_2 + \cdots + \alpha_{1n}\mathbf{v}_n \\ \mathbf{w}_2 &= \alpha_{21}\mathbf{v}_1 + \alpha_{22}\mathbf{v}_2 + \cdots + \alpha_{2n}\mathbf{v}_n \\ &\vdots \\ \mathbf{w}_n &= \alpha_{n1}\mathbf{v}_1 + \alpha_{n2}\mathbf{v}_2 + \cdots + \alpha_{nn}\mathbf{v}_n, \end{aligned}$$

gdje su $\alpha_{ij} \in \mathbb{Z}$, $i, j \in \{1, 2, \ldots, n\}$. Matrični prikaz ovih jednadžbi je $M_2 = UM_1$, gdje je

$$U = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & & & \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{bmatrix}.$$

Želimo li odrediti vektore iz B_1 kao linearnu kombinaciju vektora iz B_2, dolazimo do jednakosti $M_1 = U^{-1}M_2$. Dakle, matrica U^{-1} postoji i ima cjelobrojne vrijednosti jer je B_2 baza rešetke Λ. Stoga,

$$1 = \det I_n = \det(UU^{-1}) = \det U \det U^{-1},$$

gdje su $\det U$ i $\det U^{-1}$ cijeli brojevi, iz čega slijedi $\det U = \pm 1$, pa je U unimodularna matrica. □

Napomena 4.4. Determinanta rešetke Λ u $\mathbb{R}^n$ ne ovisi o izboru baze rešetke Λ. Neka su M_1 i M_2 dvije različite generirajuće matrice rešetke Λ. Tada prema propoziciji 4.2 postoji unimodularna matrica U takva da $M_1 = UM_2$. Stoga vrijedi:

$$\det \Lambda = |\det M_1| = |\det(UM_2)| = |\det U||\det M_2| = |\det M_2|.$$

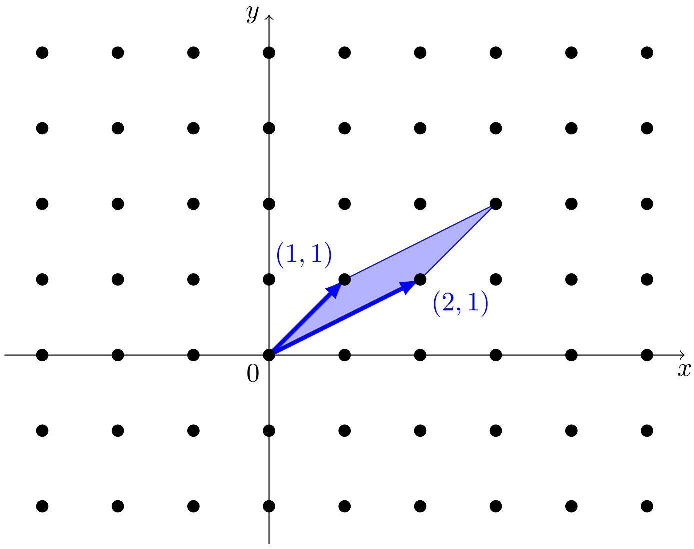
Primjer 4.2. Odredimo determinantu i fundamentalnu domenu rešetke

$$\Lambda_2 = \Lambda_2(M_2),\text{ gdje je } M_2 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}.$$

$$\det \Lambda_2 = \begin{vmatrix} 1 & 1 \\ 2 & 1 \end{vmatrix} = 1.$$

Uočimo da je determinanta rešetke Λ_2 jednaka površini paralelograma određenog vektorima baze rešetke Λ_2.

Na slici 3 prikazana je rešetka Λ_2, te njena fundamentalna domena obojena plavom bojom.



Slika 3: Fundamentalna domena rešetke Λ_2

Napomena 4.5. Iz slika 3 i 4, možemo uočiti da su rešetke $\mathbb{Z}^2$ i Λ_2 jednake. Matrica U iz propozicije 4.2 je jednaka:

$$U = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix},$$

te vrijedi $M_2 = UI_2$.

Definicija 4.6. Neka je Λ rešetka u $\mathbb{R}^n$. Kažemo da je rešetka Λ **cjelobrojna** ako vrijedi

$$\forall \mathbf{x}, \mathbf{y} \in \Lambda \quad \mathbf{x} \cdot \mathbf{y} \in \mathbb{Z},$$

gdje je $\mathbf{x} \cdot \mathbf{y}$ standardni skalarni produkt u $\mathbb{R}^n$.

Napomena 4.6. Ako Gramova matrica rešetke Λ ima cjelobrojne elemente, tada je skalarni produkt bilo koje dvije točke te rešetke cijeli broj, pa je rešetka Λ cjelobrojna.

Primjer 4.3. Odredimo determinantu, Gramovu matricu i fundamentalnu domenu rešetke

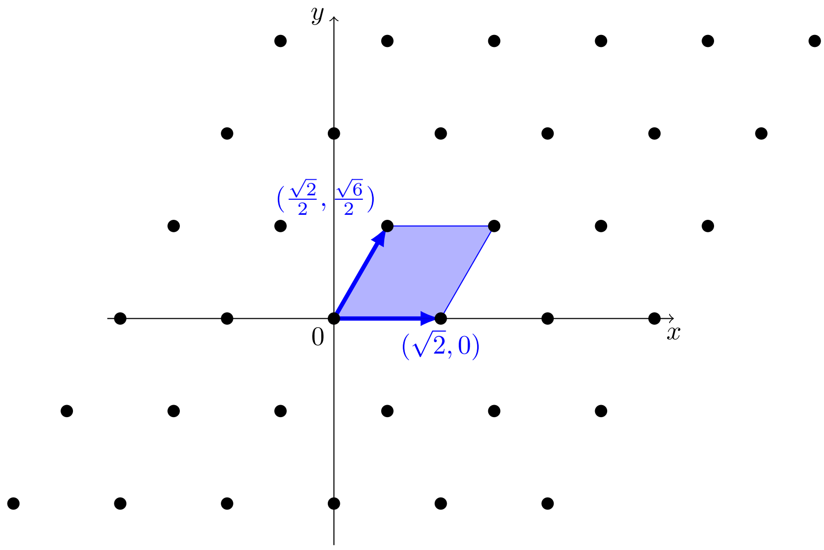
$$\Lambda_3 = \Lambda_3(M_3),\text{ gdje je } M_3 = \begin{bmatrix} \sqrt{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{2} \end{bmatrix}.$$

$$\det \Lambda_3 = \begin{vmatrix} \sqrt{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{2} \end{vmatrix} = \sqrt{2} \cdot \frac{\sqrt{6}}{2} = \sqrt{3},$$

$$M_3^\top = \begin{bmatrix} \sqrt{2} & \frac{\sqrt{2}}{2} \\ 0 & \frac{\sqrt{6}}{2} \end{bmatrix} \Rightarrow A_3 = M_3 M_3^\top = \begin{bmatrix} \sqrt{2}^2 & \frac{\sqrt{2}^2}{2} \\ \frac{\sqrt{2}^2}{2} & \left(\frac{\sqrt{2}}{2}\right)^2 + \left(\frac{\sqrt{6}}{2}\right)^2 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Budući da Gramova matrica A_3 ima cjelobrojne vrijednosti, prema napomeni 4.6 slijedi da je rešetka Λ_3 cjelobrojna.

Na slici 4 prikazana je rešetka Λ_3 te njena fundamentalna domena obojena plavom bojom. Ova rešetka naziva se **planarnom heksagonalnom rešetkom**.



Slika 4: Fundamentalna domena planarne heksagonalne rešetke Λ_3

Napomena 4.7. Neka je $\Lambda = \Lambda(B)$ rešetka u $\mathbb{R}^n$ s generirajućom matricom M, Gramovom matricom A i neka je $c \in \mathbb{R}$, rešetka $c\Lambda$ generirana bazom cB ima generirajuću matricu cM i Gramovu matricu:

$$cM(cM)^\top = c^2(MM^\top) = c^2 A.$$

Primjer 4.4. Neka je Λ_3 planarna heksagonalna rešetka s generirajućom matricom

$$M_3 = \begin{bmatrix} \sqrt{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{2} \end{bmatrix}, \qquad \text{te neka su} \qquad c_1 = 2 \quad \text{i} \quad c_2 = \frac{1}{2}.$$

Odredimo rešetke $c_1\Lambda_3 = 2\Lambda_3$ i $c_2\Lambda_3 = \frac{1}{2}\Lambda_3$.

U primjeru 4.3 izračunali smo Gramovu matricu A_3 rešetke Λ_3:

$$A_3 = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Generirajuća matrica rešetke $2\Lambda_3$ jednaka je

$$2M_3 = \begin{bmatrix} 2\sqrt{2} & 0 \\ \sqrt{2} & \sqrt{6} \end{bmatrix},$$

dok je generirajuća matrica rešetke $\frac{1}{2}\Lambda_3$ jednaka

$$\frac{1}{2}M_3 = \begin{bmatrix} \frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{2}}{4} & \frac{\sqrt{6}}{4} \end{bmatrix}.$$

Odredimo sada redom pripadne Gramove matrice rešetki $2\Lambda_3$ i $\frac{1}{2}\Lambda_3$:

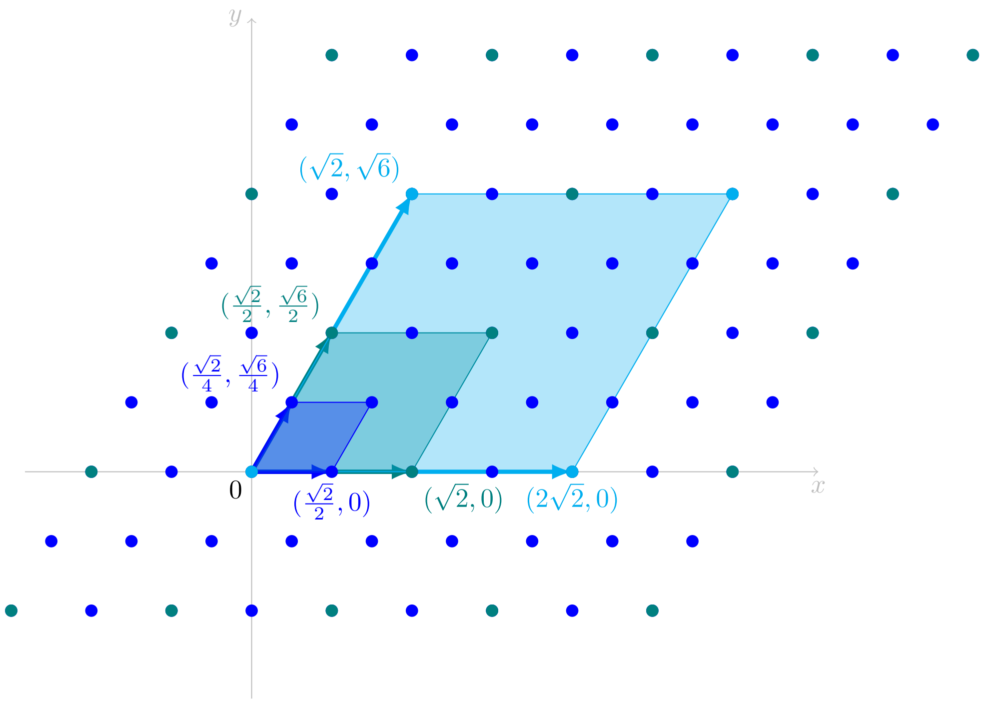
$$2^2 A_3 = 4 \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 8 & 4 \\ 4 & 8 \end{bmatrix},$$

$$\left(\frac{1}{2}\right)^2 A_3 = \frac{1}{4} \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} \end{bmatrix}.$$

Možemo uočiti da je rešetka $2\Lambda_3$ također cjelobrojna, kako su sve vrijednosti njene Gramove matrice cjelobrojne, dok rešetka $\frac{1}{2}\Lambda_3$ nije cjelobrojna.

Na slici 5 prikazane su fundamentalne domene rešetki $\frac{1}{2}\Lambda_3$, Λ_3 i $2\Lambda_3$. Površinom najmanja fundamentalna domena rešetke $\frac{1}{2}\Lambda_3$ obojena je tamno plavom bojom, zatim je fundamentalna domena rešetke Λ_3 obojena tirkiznom bojom, dok je površinom najveća fundamentalna domena rešetke $2\Lambda_3$ obojena svjetlo plavom bojom. Možemo uočiti sa slike da vrijedi sljedeće:

$$2\Lambda_3 \subseteq \Lambda_3 \subseteq \frac{1}{2}\Lambda_3.$$



Slika 5: Fundamentalne domene rešetki $\frac{1}{2}\Lambda_3$, Λ_3 i $2\Lambda_3$

Napomena 4.8. Neka je $\Lambda = \Lambda(M)$ rešetka u $\mathbb{R}^2$ i $c \in \mathbb{R}$, gdje je $M = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}$. Tada je

$$\det \Lambda = |\det M| = |v_{11}v_{22} - v_{12}v_{21}|, \text{ pa slijedi}$$
$$\det c\Lambda = |\det(cM)| = |c^2(v_{11}v_{22} - v_{12}v_{21})| = c^2|v_{11}v_{22} - v_{12}v_{21}| = c^2 \det \Lambda.$$

U primjeru 4.3 smo izračunali $\det \Lambda_3 = \sqrt{3}$, pa prema napomeni 4.8 vrijedi:

$$\det \frac{1}{2}\Lambda_3 = \frac{\sqrt{3}}{4}, \quad \det 2\Lambda_3 = 4\sqrt{3}.$$

Definicija 4.7. Neka su $\Lambda_1 = \Lambda_1(M_1)$ i $\Lambda_2 = \Lambda_2(M_2)$ rešetke. Kažemo da su rešetke Λ_1 i Λ_2 **ekvivalentne** ako postoji $c \in \mathbb{R}$, unimodularna matrica U te ortogonalna matrica D tako da vrijedi

$$cUM_1D = M_2.$$

Matrica D djeluje kao niz rotacija, a matrica U djeluje kao niz zrcaljenja.

Napomena 4.9. Pri odabiru predstavnika rešetki u klasi ekvivalencije, cilj je odabrati cjelobrojnog predstavnika s najmanjom determinantom.

Napomena 4.10. Primijetimo da su rešetke $\frac{1}{2}\Lambda_3$, Λ_3 i $2\Lambda_3$ iz primjera 4.4 međusobno ekvivalentne.

4.1 Samodualne rešetke

Definicija 4.8. Neka je Λ rešetka u $\mathbb{R}^n$. Njena **dualna rešetka** Λ^* je

$$\Lambda^* = \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{x} \cdot \mathbf{y} \in \mathbb{Z}, \forall \mathbf{x} \in \Lambda\}.$$

Definicija 4.9. Kažemo da je cjelobrojna rešetka Λ **samodualna (unimodularna)** ako vrijedi $\Lambda = \Lambda^*$.

Teorem 4.1. Neka je Λ rešetka u $\mathbb{R}^n$ s bazom $B = \{\mathbf{v}_1, \mathbf{v}_2 \ldots, \mathbf{v}_n\}$, te s pripadnom generirajućom matricom M i Gramovom matricom A. Tada vrijedi sljedeće:

(i) $\Lambda^* = \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{v}_i \cdot \mathbf{y} \in \mathbb{Z}, \forall 1 \le i \le n\} = \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{y}M^\top \in \mathbb{Z}^n\}$.

(ii) Generirajuća matrica od Λ^* je $(M^{-1})^\top$.

(iii) Gramova matrica od Λ^* je A^{-1}.

(iv) $\det \Lambda^* = 1/\det \Lambda$.

(v) Λ je cjelobrojna ako i samo ako je $\Lambda \subseteq \Lambda^*$.

(vi) Ako je Λ cjelobrojna, tada vrijedi

$$\Lambda \subseteq \Lambda^* \subseteq \frac{1}{\det \Lambda}\Lambda = (\det \Lambda^*)\Lambda.$$

(vii) Ako je Λ cjelobrojna, tada je Λ samodualna ako i samo ako je $\det \Lambda = 1$.

Dokaz. Neka je $\Lambda = \Lambda(\mathbf{v}_1, \mathbf{v}_2 \ldots, \mathbf{v}_n)$ rešetka u $\mathbb{R}^n$ s generirajućom matricom M i Gramovom matricom A.

(i) Uočimo da jednakost

$$\{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{x} \cdot \mathbf{y} \in \mathbb{Z}, \forall \mathbf{x} \in \Lambda\} = \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{v_i} \cdot \mathbf{y} \in \mathbb{Z}, \forall 1 \leq i \leq n\}$$

vrijedi zbog linearnosti skalarnog produkta u $\mathbb{R}^n$.

Nadalje, dokažimo drugu jednakost:

$$\{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{v_i} \cdot \mathbf{y} \in \mathbb{Z}, \forall 1 \leq i \leq n\} = \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{y}M^\top \in \mathbb{Z}^n\}.$$

Neka je $\mathbf{y} \in \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{v_i} \cdot \mathbf{y} \in \mathbb{Z}, \forall 1 \leq i \leq n\}$. Za $\mathbf{y} = (y_1, \ldots, y_n)$ i $\mathbf{v}_i = (v_{i1}, \ldots, v_{in})$, $i = 1, \ldots, n$, možemo pisati:

$$\begin{aligned}
\mathbf{y}M^\top &= \begin{bmatrix} y_1 & y_2 & \ldots & y_n \end{bmatrix} \begin{bmatrix} v_{11} & v_{21} & \ldots & v_{n1} \\ v_{12} & v_{22} & \ldots & v_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ v_{1n} & v_{2n} & \ldots & v_{nn} \end{bmatrix} \\
&= \begin{bmatrix} \sum_{i=1}^{n} y_i v_{1i} & \sum_{i=1}^{n} y_i v_{2i} & \ldots & \sum_{i=1}^{n} y_i v_{ni} \end{bmatrix} \\
&= \begin{bmatrix} \mathbf{v}_1 \cdot \mathbf{y} & \mathbf{v}_2 \cdot \mathbf{y} & \ldots & \mathbf{v}_n \cdot \mathbf{y} \end{bmatrix}.
\end{aligned}$$

Budući da za $\mathbf{y}$ vrijedi $\mathbf{v_i} \cdot \mathbf{y} \in \mathbb{Z}, \forall 1 \leq i \leq n$, slijedi da su svi elementi vektora $\mathbf{y}M^\top$ cijeli brojevi, što znači da je $\mathbf{y}M^\top \in \mathbb{Z}^n$.

Neka je sada $\mathbf{y} \in \mathbb{R}^n$ takav da je $\mathbf{y}M^\top \in \mathbb{Z}^n$. To znači da su svi elementi vektora $\mathbf{y}M^\top$ cijeli brojevi, pa tako i za proizvoljan $i \in \{1, \ldots, n\}$ vrijedi da je i-ta komponenta vektora $\mathbf{y}M^\top$, koja je jednaka $\mathbf{v_i} \cdot \mathbf{y}$, također cijeli broj. Stoga slijedi: $\mathbf{y} \in \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{v_i} \cdot \mathbf{y} \in \mathbb{Z}, \forall 1 \leq i \leq n\}$.

(ii) Prema propoziciji 2.1, matrica $(M^{-1})^\top$ je regularna. Neka su $\mathbf{w_1}, \ldots, \mathbf{w_n}$ retci matrice $(M^{-1})^\top$. Tada je $\{\mathbf{w_1}, \ldots, \mathbf{w_n}\}$ baza za $\mathbb{R}^n$. Budući da je $(M^{-1})^\top M^\top = (MM^{-1})^\top = I_n$, vrijedi

$$\mathbf{w}_i \cdot \mathbf{v}_j = \begin{cases} 1 & \text{ako je } i = j, \\ 0 & \text{ako je } i \neq j. \end{cases} \tag{3}$$

Posebno, $\mathbf{w_1}, \ldots, \mathbf{w_n} \subseteq \Lambda^*$, prema svojstvu (i). Neka je $\mathbf{w} \in \Lambda^*$. Tada je

$\mathbf{w} = a_1\mathbf{w}_1 + \ldots + a_n\mathbf{w}_n$, budući da je $\{\mathbf{w_1}, \ldots, \mathbf{w_n}\}$ baza za $\mathbb{R}^n$. Kako je $\mathbf{w} \in \Lambda^*$, $\mathbf{w} \cdot \mathbf{v}_j \in \mathbb{Z}$, za $j \in \{1, \ldots, n\}$. No, $\mathbf{w} \cdot \mathbf{v}_j = a_j$, za $1 \leq j \leq n$, prema (3). Stoga je $a_j \in \mathbb{Z}$. Iz ovoga slijedi da svaku točku rešetke Λ^* možemo zapisati kao cjelobrojnu linearnu kombinaciju vektora $\mathbf{w_1}, \ldots, \mathbf{w_n}$. Dakle, vrijedi

$$\Lambda^* = \{\mathbf{z}\,(M^{-1})^\top \mid \mathbf{z} \in \mathbb{Z}^n\}.$$

(iii) Odredimo sada Gramovu matricu rešetke Λ^*. Prema svojstvu (ii), vrijedi

$$(M^{-1})^\top M^{-1} = (MM^\top)^{-1} = A^{-1},$$

iz čega slijedi da je A^{-1} Gramova matrica rešetke Λ^*.

(iv) Odredimo sada determinantu rešetke Λ^*. Iz jednadžbe (2) i iz svojstva (ii) slijedi da je $\det \Lambda^* = |\det(M^{-1})^\top| = |\det(M^{-1})|$, te kako je M regularna matrica, prema teoremu 2.6, vrijedi

$$\det \Lambda^* = |\det(M^{-1})| = \frac{1}{|\det M|} = \frac{1}{\det \Lambda}.$$

(v) Dokažimo tvrdnju: ako je rešetka Λ cjelobrojna , tada vrijedi $\Lambda \subseteq \Lambda^*$. Neka je Λ je cjelobrojna rešetka. Tada vrijedi

$$\forall \mathbf{x} \in \Lambda \Rightarrow \mathbf{x} \in \Lambda^*,$$

kako se dualna rešetka sastoji od vektora $\mathbf{y}$ takvih da $\mathbf{x} \cdot \mathbf{y} \in \mathbb{Z}$, $\forall \mathbf{x} \in \Lambda$.

Dokažimo sada tvrdnju: ako vrijedi $\Lambda \subseteq \Lambda^*$, tada je rešetka Λ cjelobrojna. Neka je $\Lambda \subseteq \Lambda^*$. Tada vrijedi:

$$\forall \mathbf{x}, \mathbf{y} \in \Lambda \subseteq \Lambda^* \Rightarrow \mathbf{x} \cdot \mathbf{y} \in \mathbb{Z},\ \forall \mathbf{y} \in \Lambda,$$

pa je rešetka Λ cjelobrojna.

(vi) Neka je rešetka Λ cjelobrojna. Prema svojstvu (v) vrijedi $\Lambda \subseteq \Lambda^*$. Uzmimo proizvoljan $\mathbf{y} \in \Lambda^*$. Tada je $\mathbf{y}M^\top \in \mathbb{Z}^n$ prema (i), stoga postoji $\mathbf{z} \in \mathbb{Z}^n$ za kojeg vrijedi

$$\mathbf{y} = \mathbf{z}\,(M^\top)^{-1} = \mathbf{z}\,(M^\top)^{-1} M^{-1} M = \mathbf{z}\,(MM^\top)^{-1} M = \mathbf{z}\,A^{-1} M.$$

Prema teoremu 2.8, matricu A^{-1} možemo zapisati na sljedeći način:

$$A^{-1} = (\det A)^{-1} \mathrm{adj}(A).$$

Stoga,

$$\mathbf{y} = \mathbf{z}\,(\det A)^{-1} \mathrm{adj}(A) M = \mathbf{z}'\,(\det A)^{-1} M,$$

gdje je $\mathbf{z}' = \mathbf{z}\,\mathrm{adj}(A) \in \mathbb{Z}^n$ budući da $\mathrm{adj}(A)$ ima cjelobrojne vrijednosti. Dakle, $\mathbf{y} \in (\det \Lambda)^{-1}\Lambda$ pa vrijedi svojstvo (vi).

(vii) Neka je Λ cjelobrojna rešetka. Dokažimo najprije tvrdnju: ako je Λ samodualna, tada vrijedi $\det \Lambda = 1$. Prema svojstvu (iv), vrijedi

$$\det \Lambda = \det \Lambda^* = \frac{1}{\det \Lambda},$$

iz čega slijedi $\det \Lambda = 1$, jer je $\det \Lambda > 0$.

Neka sada vrijedi $\det \Lambda = 1$. Prema svojstvu (vi) vrijedi

$$\Lambda \subseteq \Lambda^* \subseteq \frac{1}{\det \Lambda} \Lambda = \Lambda,$$

pa je $\Lambda^* = \Lambda$.

$\square$

Primjer 4.5. Odredimo dualnu rešetku Λ_3^* planarne heksagonalne rešetke

$$\Lambda_3 = \Lambda_3(M_3), \text{ gdje je } M_3 = \begin{bmatrix} \sqrt{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{2} \end{bmatrix}.$$

Nadalje, odredimo determinantu i fundamentalnu domenu rešetke Λ_3^*.

Odredimo najprije inverznu matricu generirajuće matrice M_3 koristeći teorem 2.8:

$$\begin{aligned} M_3^{-1} &= (\det M_3)^{-1}\mathrm{adj}(M_3) \\ &= \frac{\sqrt{3}}{3}\begin{bmatrix} \frac{\sqrt{6}}{2} & 0 \\ -\frac{\sqrt{2}}{2} & \sqrt{2} \end{bmatrix} \\ &= \begin{bmatrix} \frac{\sqrt{2}}{2} & 0 \\ -\frac{\sqrt{6}}{6} & \frac{\sqrt{6}}{3} \end{bmatrix}. \end{aligned}$$

Prema teoremu 4.1 (ii), generirajuća matrica dualne rešetke Λ_3^* je

$$(M_3^{-1})^\top = \begin{bmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{6}}{6} \\ 0 & \frac{\sqrt{6}}{3} \end{bmatrix}.$$

Stoga vrijedi:

$$\Lambda_3^* = \{\mathbf{z}\,(M_3^{-1})^\top \mid \mathbf{z} \in \mathbb{Z}^2\}.$$

Nadalje, odredimo determinantu dualne rešetke Λ_3^*:

$$\det \Lambda_3^* = \begin{vmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{6}}{6} \\ 0 & \frac{\sqrt{6}}{3} \end{vmatrix} = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{6}}{3} = \frac{\sqrt{3}}{3}.$$

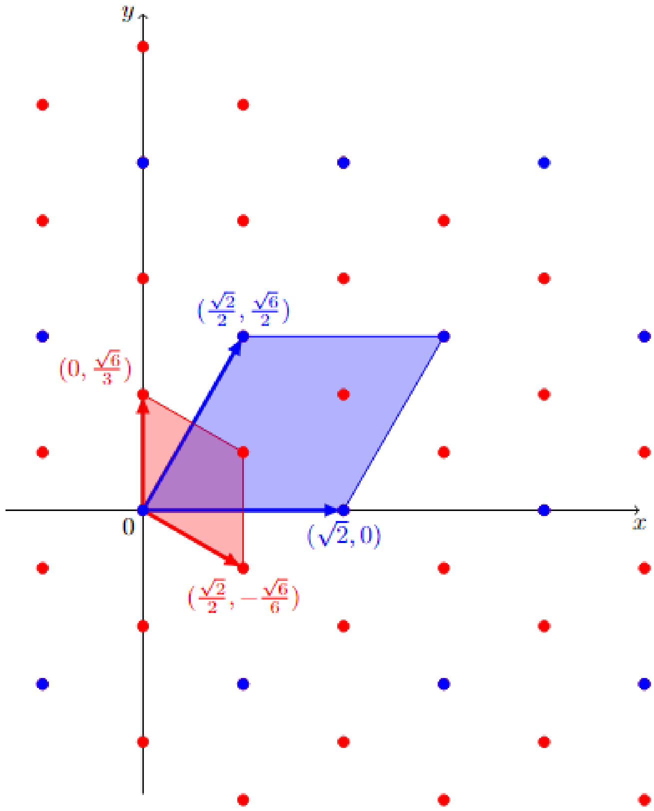
Determinantu možemo računati i na sljedeći način: u primjeru 4.3 smo izračunali determinantu rešetke Λ_3, koja iznosi $\det \Lambda_3 = \sqrt{3}$, pa po teoremu 4.1 (iv) slijedi

$$\det \Lambda_3^* = \frac{1}{\det \Lambda_3} = \frac{1}{\sqrt{3}} = \frac{\sqrt{3}}{3}.$$

Na slici 6 možemo vidjeti točke rešetke Λ_3 obojene plavom bojom te njenu fundamentalnu domenu, obojenu također plavom bojom. Točke dualne rešetke Λ_3^* obojene su crvenom bojom, te je njena fundamentalna domena na slici 6 obojena crvenom bojom. Nadalje, sa slike 6 možemo uočiti da vrijedi sljedeća podskupovnost:

$$\Lambda_3 \subseteq \Lambda_3^*.$$

Ova podskupovnost također slijedi iz teorema 4.1 (v) i činjenice da je rešetka Λ_3 cjelobrojna. Nadalje, prema teoremu 4.1 (vii) i iz činjenice da je $\det \Lambda_3 = \sqrt{3} \neq 1$ slijedi da Λ_3 nije samodualna rešetka.



Slika 6: Fundamentalne domene rešetki Λ_3 i Λ_3^*

Definicija 4.10. Kažemo da je cjelobrojna rešetka Λ **parna** ako je $\mathbf{x} \cdot \mathbf{x}$ paran broj za svaki $\mathbf{x} \in \Lambda$. U suprotnom kažemo da je cjelobrojna rešetka Λ **neparna**.

Napomena 4.11. Neka je $\Lambda = \Lambda(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ parna cjelobrojna rešetka s pripadnom Gramovom matricom $A = [a_{ij}]$. Kako je Λ parna rešetka, skalarni produkt svake dvije točke rešetke Λ je paran broj, pa to vrijedi i za točke baze. Stoga je $a_{ii} = v_i \cdot v_i$ je paran broj, za svaki $1 \leq i \leq n$.

Dakle, ako je Λ cjelobrojna parna rešetka, tada njezina Gramova matrica A ima parne elemente na svojoj glavnoj dijagonali.

Definicija 4.11. Ako je Λ parna samodualna rešetka, kažemo da je Λ rešetka **tipa II**, a ako je Λ neparna samodualna rešetka, kažemo da je ona **tipa I**.

Dokaz sljedeće propozicije možemo pronaći u [3].

Propozicija 4.3. Rešetke $\Lambda \subseteq \mathbb{R}^n$ tipa I postoje za svaku dimenziju n. Rešetke $\Lambda \subseteq \mathbb{R}^n$ tipa II postoje ako i samo ako je $n \equiv 0 \pmod 8$.

Primjer 4.6. Pokažimo da je $\mathbb{Z}^2$ rešetka tipa I.

Rešetka $\mathbb{Z}^2$ ima generirajuću matricu I_2, te je njena Gamova matrica jednaka $I_2 I_2^\top = I_2 I_2 = I_2$. Tada prema napomeni 4.6 slijedi da je $\mathbb{Z}^2$ cjelobrojna rešetka. Nadalje, prema teoremu 4.1 (vii), kako je $\det \mathbb{Z}^2 = 1$, slijedi da je $\mathbb{Z}^2$ samodualna. Zatim, prema napomeni 4.11, slijedi da je to neparna rešetka. Stoga je $\mathbb{Z}^2$ rešetka tipa I.

Definicija 4.12. Neka je $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{R}^n$. Definiramo **normu** vektora $\mathbf{v}$ kao

$$N(\mathbf{v}) = \mathbf{v} \cdot \mathbf{v} = \sum_{i=1}^{n} v_i^2.$$

Napomena 4.12. Uočimo da funkcija iz prethodne definicija ne zadovoljava svojstva iz definicije 2.29.

Definicija 4.13. **Minimalna norma** rešetke Λ, u oznaci μ, je

$$\mu = \mu(\Lambda) = \min\{N(\mathbf{x} - \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \Lambda,\, \mathbf{x} \neq \mathbf{y}\} = \min\{N(\mathbf{x}) \mid \mathbf{x} \in \Lambda,\, \mathbf{x} \neq \mathbf{0}\}.$$

Neka je Λ samodualna rešetka u $\mathbb{R}^n$. Može se pokazati da vrijedi:

$$\mu = \mu(\Lambda) \leq \begin{cases} \lfloor \frac{n}{8} \rfloor + 1, & \text{ako je } \Lambda \text{ tipa I,} \\ 2\lfloor \frac{n}{24} \rfloor + 2, & \text{ako je } \Lambda \text{ tipa II.} \end{cases} \tag{4}$$

Više o ovoj gornjoj ogradi se može pronaći u [4].
Za rešetke se definira red potencija pod imenom theta red, koji je analogon težinskom enumeratoru koda iz definicije 3.4.

Definicija 4.14. **Theta red** $\Theta(q)$ rešetke Λ je

$$\Theta(q) = \sum_{\mathbf{x} \in \Lambda} q^{\mathbf{x} \cdot \mathbf{x}}.$$

Ako je Λ cjelobrojna i N_m je broj točaka rešetke norme m, tada je

$$\Theta(q) = \sum_{m=0}^{\infty} N_m q^m.$$

Primjer 4.7. Neka je Λ_3 planarna heksagonalna rešetka iz primjera 4.3.

(a) Odredimo minimalnu normu rešetke Λ_3.

(b) Pokažimo da je norma bilo koje točke rešetke Λ_3 paran cijeli broj.

(c) Odredimo točke $\mathbf{x} \in \Lambda_3$ za koje je $N(\mathbf{x})$ jednaka:
(i) 2, (ii) 4, (iii) 6.

Vrijedi $\Lambda_3 = \{\mathbf{x} = z_1\mathbf{v}_1 + z_2\mathbf{v}_2 \mid z_1, z_2 \in \mathbb{Z}\}$, gdje su $\mathbf{v}_1 = (\sqrt{2}, 0)$ i $\mathbf{v}_2 = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{6}}{2}\right)$.

(a) Na slici 4 možemo uočiti da je dovoljno odrediti normu točaka baze:

$$N(\mathbf{v}_1) = (\sqrt{2}, 0) \cdot (\sqrt{2}, 0) = 2,$$
$$N(\mathbf{v}_2) = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{6}}{2}\right) \cdot \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{6}}{2}\right) = \frac{2}{4} + \frac{6}{4} = 2,$$
$$\mu = \mu(\Lambda_3) = \min\{N(\mathbf{v}_1), N(\mathbf{v}_2)\} = 2.$$

(b) Uzmimo proizvoljnu točku $\mathbf{x} = z_1\mathbf{v}_1 + z_2\mathbf{v}_2 \in \Lambda_3$, gdje su $z_1, z_2 \in \mathbb{Z}$.

$$\begin{aligned}
\mathbf{x} &= z_1(\sqrt{2}, 0) + z_2\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{6}}{2}\right) \\
&= \left(z_1\sqrt{2} + z_2\frac{\sqrt{2}}{2}, z_2\frac{\sqrt{6}}{2}\right).
\end{aligned}$$

$$\begin{aligned}
\text{Nadalje, } N(\mathbf{x}) &= \mathbf{x} \cdot \mathbf{x} \\
&= \left(z_1\sqrt{2} + z_2\frac{\sqrt{2}}{2}, z_2\frac{\sqrt{6}}{2}\right) \cdot \left(z_1\sqrt{2} + z_2\frac{\sqrt{2}}{2}, z_2\frac{\sqrt{6}}{2}\right) \\
&= 2z_1^2 + 2z_1z_2 + \frac{1}{2}z_2^2 + \frac{3}{2}z_2^2 \\
&= 2z_1^2 + 2z_1z_2 + 2z_2^2 \\
&= 2(z_1^2 + z_1z_2 + z_2^2),
\end{aligned}$$

pa je $N(\mathbf{x})$ paran broj, za svaku točku $\mathbf{x} \in \Lambda_3$.

(c) Budući da je norma točke $\mathbf{x} \in \Lambda_3$ jednaka

$$N(\mathbf{x}) = 2(z_1^2 + z_1z_2 + z_2^2),$$

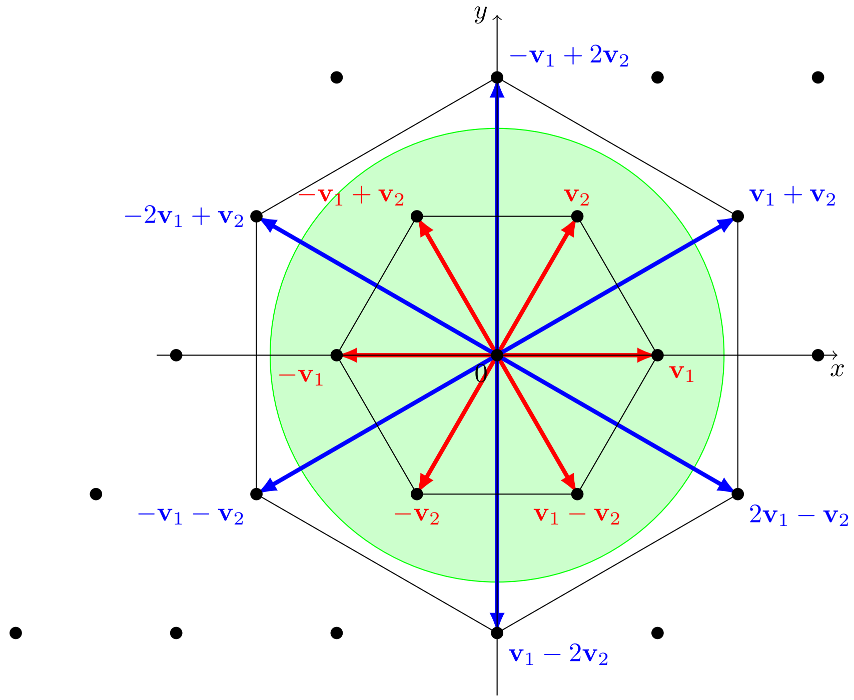
dobivamo:

(i) $2 = N(\mathbf{x}) = 2(z_1^2 + z_1z_2 + z_2^2) \Rightarrow 1 = z_1^2 + z_2^2 + z_1z_2$
$\Rightarrow (z_1, z_2) \in \{\pm(1,0), \pm(0,1), \pm(1,-1)\}$
$\Rightarrow \mathbf{x} \in \{\pm\mathbf{v}_1, \pm\mathbf{v}_2, \pm(\mathbf{v}_1 - \mathbf{v}_2)\}$.

(ii) $4 = N(\mathbf{x}) = 2(z_1^2 + z_1z_2 + z_2^2) \Rightarrow 2 = z_1^2 + z_2^2 + z_1z_2$
$\Rightarrow$ nema cjelobrojnih rješenja za z_1 i z_2
$\Rightarrow$ nema takvih točaka $\mathbf{x} \in \Lambda_3$.

(iii) $6 = N(\mathbf{x}) = 2(z_1^2 + z_1z_2 + z_2^2) \Rightarrow 3 = z_1^2 + z_2^2 + z_1z_2$
$\Rightarrow (z_1, z_2) \in \{\pm(1,1), \pm(2,-1), \pm(1,-2)\}$
$\Rightarrow \mathbf{x} \in \{\pm(\mathbf{v}_1 + \mathbf{v}_2), \pm(2\mathbf{v}_1 - \mathbf{v}_2), \pm(\mathbf{v}_1 - 2\mathbf{v}_2)\}$.

Na slici 7 prikazana je planarna heksagonalna rešetka Λ_3, crvenom bojom označeni su radij vektori točaka $\mathbf{x} \in \Lambda_3$ za koje vrijedi $N(\mathbf{x}) = 2$, dok su plavom bojom označeni radij vektori točaka $\mathbf{y} \in \Lambda_3$ za koje vrijedi $N(\mathbf{y}) = 6$. Zelena kružnica predstavlja točke u ravnini s normom 4.



Slika 7: Točke norme 2 i 6 planarne heksagonalne rešetke Λ_3

Pojam minimalne norme rešetke koristi se u definiciji pakiranja rešetke.

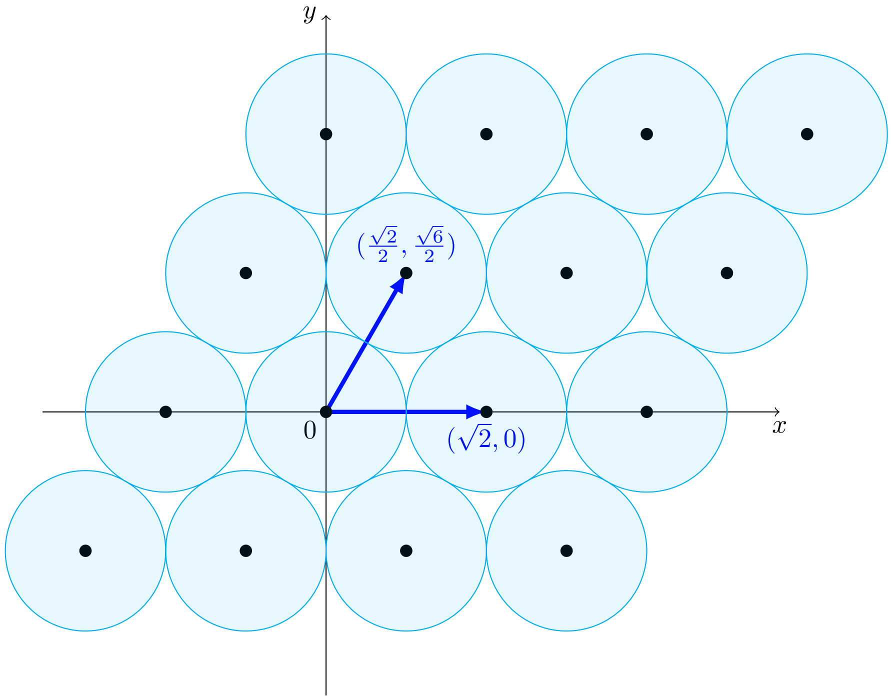
Definicija 4.15. Ako je Λ rešetka u $\mathbb{R}^n$ s minimalnom normom μ, tada n-dimenzionalne sfere polumjera $\rho = \frac{\sqrt{\mu}}{2}$ sa središtem u točkama rešetke tvore **pakiranje rešetke** Λ u $\mathbb{R}^n$.

Primjer 4.8. Odredimo pakiranje planarne heksagonalne rešetke Λ_3.

U primjeru 4.7 odredili smo minimalnu normu rešetke Λ_3: $\mu = \mu(\Lambda_3) = 2$. Tada je

$$\rho = \frac{\sqrt{\mu}}{2} = \frac{\sqrt{2}}{2}.$$

Na slici 8 prikazano je pakiranje planarne heksagonalne rešetke Λ_3, to jest oko svake točke rešetke Λ_3 konstruirana je kružnica polumjera $\frac{\sqrt{2}}{2}$, obojena svijetlo plavom bojom.



Slika 8: Pakiranje planarne heksagonalne rešetke Λ_3

Napomena 4.13. Primjetimo da svake dvije sfere iz definicije 4.15 imaju najviše jednu zajedničku točku.

Definicija 4.16. **Priljubljujući broj** rešetke Λ je broj sfera u pakiranju rešetke Λ koje dodiruju sferu sa središtem u ishodištu.

Napomena 4.14. Priljubljujući broj rešetke Λ jednak je broju točaka rešetke Λ s minimalnom normom μ.

Priljubljujući broj rešetke je analogon broju riječi minimalne težine u kodu. Iz raznih razloga zanimljivo je pronaći rešetke s velikim priljubljujućim brojem.

Napomena 4.15. Iz slike 8 možemo uočiti da je priljubljujući broj rešetke Λ_3 jednak 6.

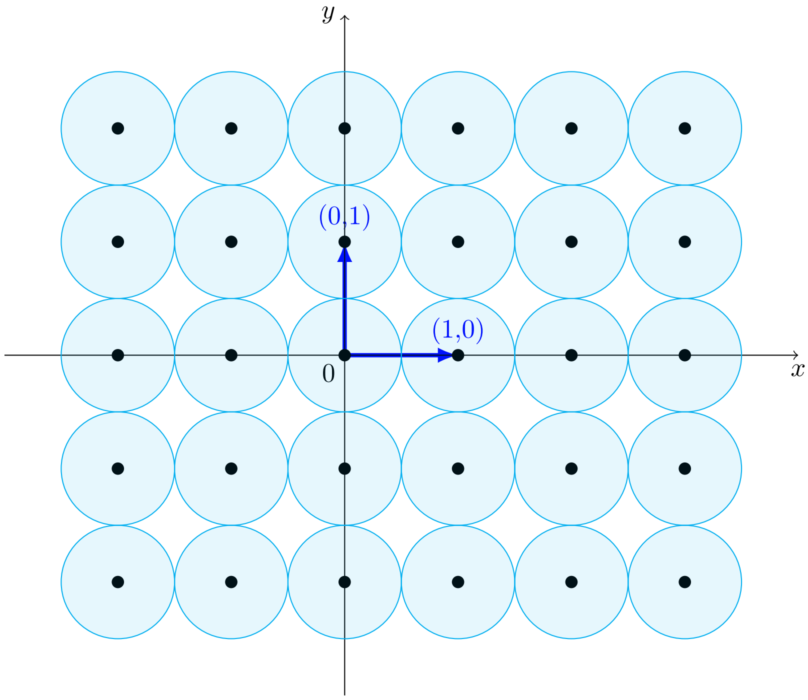
Primjer 4.9. Odredimo pakiranje rešetke $\mathbb{Z}^2$ i njen priljubljujući broj. Dovoljno je odrediti normu za točke baze:

$$N(\mathbf{v}_1) = 1, \quad N(\mathbf{v}_2) = 1,$$

gdje je $\mathbf{v}_1 = (1,0), \mathbf{v}_2 = (0,1)$. Dakle, $\mu = \mu(\mathbb{Z}^2) = 1$. Nadalje, slijedi da je polumjer sfera u pakiranju rešetke $\mathbb{Z}^2$ jednak

$$\rho = \frac{\sqrt{\mu}}{2} = \frac{1}{2},$$

dok je priljubljujući broj rešetke $\mathbb{Z}^2$ jednak 4, što možemo vidjeti na slici 9.



Slika 9: Pakiranje rešetke $\mathbb{Z}^2$

5 Konstrukcija A

Sada navodimo konstrukciju rešetki iz binarnih kodova, poznatu pod nazivom *Konstrukcija A*. Neka je $\mathcal{C}$ binarni kod duljine n. Tada je rešetka određena kodom $\mathcal{C}$ jednaka

$$\Lambda(\mathcal{C}) = \{\mathbf{x} \in \mathbb{R}^n \mid \sqrt{2}\mathbf{x} \pmod 2 \in \mathcal{C}\}.$$

Primjer 5.1. Odredimo rešetku $\Lambda(\mathcal{C}_1)$ pomoću konstrukcije A iz binarnog koda $\mathcal{C}_1$ iz primjera 3.1.

Uzmimo proizvoljan $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$ i neka je $\mathbf{c} = (c_1, c_2) \in \mathcal{C}_1$.

$$\sqrt{2}\mathbf{x} \pmod 2 = \mathbf{c} \quad \Rightarrow \quad \sqrt{2}x_i \pmod 2 = c_i \in \{0,1\},\ i = 1, 2.$$

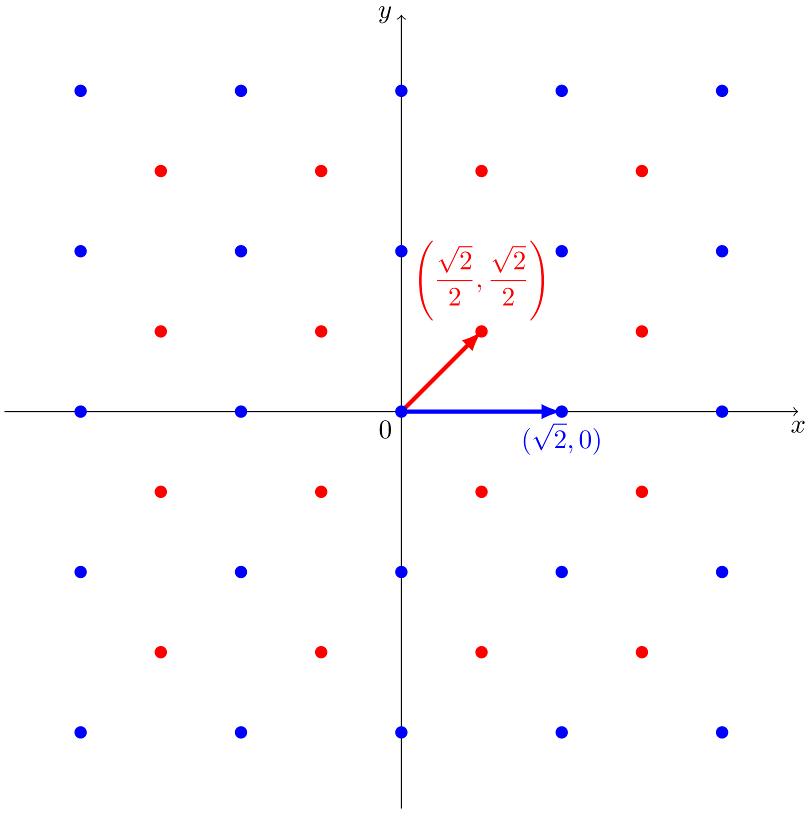
Imamo sljedeća dva slučaja:

$$\begin{aligned}
\sqrt{2}x_i \pmod 2 = 0 \quad &\Rightarrow \quad x_i = \frac{1}{\sqrt{2}}2z = \sqrt{2}z,\ z \in \mathbb{Z}, \\
\sqrt{2}x_j \pmod 2 = 1 \quad &\Rightarrow \quad x_j = \frac{1}{\sqrt{2}}(2z+1) = \sqrt{2}z + \frac{\sqrt{2}}{2} = \sqrt{2}\left(z + \frac{1}{2}\right),\ z \in \mathbb{Z}.
\end{aligned}$$

Kako je $\mathcal{C}_1 = \{(0,0), (1,1)\}$, točke rešetke $\Lambda(\mathcal{C}_1)$ će biti sljedećeg oblika:

$$\begin{aligned}
(0,0) \in \mathcal{C}_1 \quad &\Rightarrow \quad (\sqrt{2}z_1, \sqrt{2}z_2) \in \Lambda(\mathcal{C}_1),\ z_1, z_2 \in \mathbb{Z}, \\
(1,1) \in \mathcal{C}_1 \quad &\Rightarrow \quad \left(\sqrt{2}z_1 + \frac{\sqrt{2}}{2}, \sqrt{2}z_2 + \frac{\sqrt{2}}{2}\right) \in \Lambda(\mathcal{C}_1),\ z_1, z_2 \in \mathbb{Z}.
\end{aligned}$$

Na slici 10 prikazane su točke rešetke $\Lambda(\mathcal{C}_1)$, plavom bojom obojene su točke oblika $(\sqrt{2}z_1, \sqrt{2}z_2)$, dok su crvenom bojom obojene točke oblika $\left(\sqrt{2}z_1 + \frac{\sqrt{2}}{2}, \sqrt{2}z_2 + \frac{\sqrt{2}}{2}\right)$, gdje su $z_1, z_2 \in \mathbb{Z}$.



Slika 10: Rešetka $\Lambda(\mathcal{C}_1)$

Neka je $\mathcal{C}$ binarni $[n,k]$ kod s generirajućom matricom u standardnom obliku $G = [I_k \mid C]$. Tada rešetka $\Lambda(\mathcal{C})$ konstruirana konstrukcijom A iz koda $\mathcal{C}$, ima generirajuću matricu:

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} I_k & C \\ O & 2\,I_{n-k} \end{bmatrix}, \tag{5}$$

gdje je O nulmatrica, a I_n jedinična matrica reda n. Gramova matrica rešetke $\Lambda(\mathcal{C})$ jednaka je:

$$\begin{aligned} A = MM^\top &= \left(\frac{1}{\sqrt{2}} \begin{bmatrix} I_k & C \\ O & 2I_{n-k} \end{bmatrix}\right) \left(\frac{1}{\sqrt{2}} \begin{bmatrix} I_k & O \\ C^\top & 2I_{n-k} \end{bmatrix}\right) \\ &= \frac{1}{2} \begin{bmatrix} I_k \cdot I_k + C \cdot C^\top & I_k \cdot O + C \cdot 2I_{n-k} \\ O \cdot I_k + 2I_{n-k} \cdot C^\top & O \cdot O + 2I_{n-k} \cdot 2I_{n-k} \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} I_k + CC^\top & 2C \\ 2C^\top & 4I_{n-k} \end{bmatrix}. \end{aligned}$$

Napomena 5.1. Budući da je generirajuća matrica koda $\mathcal{C}_1$ iz primjera 3.1 jednaka $G_1 = \begin{bmatrix} 1 & 1 \end{bmatrix}$, te je generirajuća matrica rešetke $\Lambda(\mathcal{C}_1)$ iz primjera 5.1 jednaka:

$$M_1 = \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ 0 & \sqrt{2} \end{bmatrix},$$

prema jednakosti (5).

Teorem 5.1. Neka je $\mathcal{C}$ binarni $[n, k, d]$ kod. Tada vrijedi:

(i) $\mu = \mu(\Lambda(\mathcal{C})) = \begin{cases} \frac{d}{2}, & d \leq 4, \\ 2, & d > 4. \end{cases}$

(ii) $\det \Lambda(\mathcal{C}) = 2^{\frac{n-2k}{2}}$.

(iii) $\Lambda(\mathcal{C}^{\perp}) = \Lambda(\mathcal{C})^*$.

(iv) Rešetka $\Lambda(\mathcal{C})$ je cjelobrojna ako i samo ako je kod $\mathcal{C}$ samoortogonalan.

(v) Rešetka $\Lambda(\mathcal{C})$ je samodualna ako i samo ako je kod $\mathcal{C}$ samodualan.

(vi) Rešetka $\Lambda(\mathcal{C})$ je tipa I ako i samo ako je kod $\mathcal{C}$ tipa I.

(vii) Rešetka $\Lambda(\mathcal{C})$ je tipa II ako i samo ako je kod $\mathcal{C}$ tipa II.

Dokaz. Neka je $\mathcal{C}$ binarni $[n, k, d]$ kod s generirajućom matricom u standardnom obliku $G = [I_k \mid C]$ i $\Lambda(\mathcal{C})$ rešetka konstruirana iz koda $\mathcal{C}$ konstrukcijom A s generirajućom matricom M, te neka je M_i i-ti redak matrice M, za $i = 1, \ldots, n$.

(i) Uočimo da je $N(M_i) = 2$, za $i = k+1, \ldots, n$. Iz ove činjenice slijedi tvrdnja (i).

(ii) Prema (5), generirajuća matrica rešetke $\Lambda(\mathcal{C})$ jednaka je:

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} I_k & C \\ O & 2I_{n-k} \end{bmatrix}.$$

Stoga vrijedi, prema teoremu 2.5:

$$\begin{aligned} \det M = \det \left(\frac{1}{\sqrt{2}} \begin{bmatrix} I_k & C \\ O & 2I_{n-k} \end{bmatrix} \right) &= \frac{1}{\sqrt{2}^n} \det \begin{bmatrix} I_k & C \\ O & 2I_{n-k} \end{bmatrix} \\ &= 2^{-\frac{n}{2}} \det I_k \cdot \det(2I_{n-k}) = 2^{-\frac{n}{2}} \cdot 2^{n-k} = 2^{\frac{n-2k}{2}}. \end{aligned}$$

Tada, prema (2), $\det \Lambda(\mathcal{C}) = |\det M| = 2^{\frac{n-2k}{2}}$.

(iii) Budući da je $G^{\perp} = \begin{bmatrix} C^{\top} & I_{n-k} \end{bmatrix}$ generirajuća matrica od $\mathcal{C}^{\perp}$, $\Lambda(\mathcal{C}^{\perp})$ ima generirajuću matricu

$$M^{\perp} = \frac{1}{\sqrt{2}} \begin{bmatrix} C^{\top} & I_{n-k} \\ 2I_k & O \end{bmatrix}.$$

Skalarni produkt retka iz G s retkom iz $G^\perp$ je 0. Stoga, slijedi da je skalarni produkt retka iz M s retkom iz $M^\perp$ cijeli broj. Tada je $M^\perp M^\top$ matrica s cjelobrojnim vrijednostima, te vrijedi $\Lambda(\mathcal{C}^\perp) \subseteq \Lambda(\mathcal{C})^*$.

Da bismo dokazali (iii), moramo još pokazati $\Lambda(\mathcal{C})^* \subseteq \Lambda(\mathcal{C}^\perp)$. Neka je $\mathbf{y} \in \Lambda(\mathcal{C})^*$. Tada je $\mathbf{y}M^\top \in \mathbb{Z}^n$, prema teoremu 4.1 (i). Dakle, postoji $\mathbf{z} \in \mathbb{Z}^n$ takav da je

$$\mathbf{y} = \mathbf{z}(M^\top)^{-1} = \mathbf{z}(M^\top)^{-1}(M^\perp)^{-1}M^\perp = \mathbf{z}(M^\perp M^\top)^{-1}M^\perp.$$

Kako je $M^\perp M^\top$ matrica s cjelobrojnim vrijednostima, vrijedi:

$$\det(M^\perp M^\top) = \det(M^\perp)\det(M^\top) = \pm 2^{\frac{2k-n}{2}} \cdot (2^{\frac{n-2k}{2}}) = \pm 1$$

pa i matrica

$$(M^\perp M^\top)^{-1} = \frac{1}{\det(M^\perp M^\top)} \operatorname{adj}(M^\perp M^\top)$$

ima cjelobrojne vrijednosti. Dakle, $\mathbf{y} = \mathbf{z}' M^\perp$ za neki $\mathbf{z}' \in \mathbb{Z}^n$. Stoga, $\mathbf{y} \in \Lambda(\mathcal{C}^\perp)$, pa smo dokazali (iii).

(iv) Ova tvrdnja slijedi iz činjenice da je realni skalarni produkt dvaju redaka iz M cijeli broj ako i samo ako je binarni skalarni produkt redaka iz G jednak 0.

(v) Neka je rešetka $\Lambda(\mathcal{C})$ samodualna. Tada je rešetka $\Lambda(\mathcal{C})$ cjelobrojna iz čega slijedi da je kod $\mathcal{C}$ samoortogonalan, prema teoremu 5.1 (iv). Zatim, prema teoremu 4.1 (vii), vrijedi $\det \Lambda(\mathcal{C}) = 1$, što implicira $k = \frac{n}{2}$. Prema napomeni 3.5, kod $\mathcal{C}$ je samodualan.

Neka je kod $\mathcal{C}$ samodualan. Tada vrijedi, prema teoremu 5.1 (iii), $\Lambda(\mathcal{C}) = \Lambda(\mathcal{C}^\perp) = \Lambda(\mathcal{C})^*$, iz čega slijedi da je $\Lambda(\mathcal{C})$ samodualna rešetka.

Tvrdnje (vi) i (vii) slijede iz prethodnih tvrdnji teorema 5.1, kao i činjenice da binarne riječi težine djeljive s 2, ali ne i s 4, odgovaraju točkama rešetke s neparnom normom, dok riječi težine djeljive s 4 odgovaraju točkama s parnom normom. □

Primjer 5.2. Odredimo rešetku $\Lambda(\mathcal{C}_2)$ pomoću konstrukcije A iz binarnog $[3, 2, 2]$ koda $\mathcal{C}_2$ iz primjera 3.2.

Prema (5) znamo da je generirajuća matrica rešetke $\Lambda(\mathcal{C}_2)$ jednaka:

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix},$$

a njena Gramova matrica jednaka je:

$$A = \frac{1}{2} \begin{bmatrix} 2 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 2 & 4 \end{bmatrix}.$$

Prema teoremu 5.1 (i) i (ii) slijedi da je minimalna norma konstruirane rešetke $\mu = 1$, a njena $\det(\Lambda(\mathcal{C}_2)) = 2^{\frac{3-2\cdot 2}{2}} = 2^{-\frac{1}{2}} = \frac{1}{\sqrt{2}}$.
Zatim odredimo $\Lambda(\mathcal{C}_2^{\perp})$. Po teoremu 4.1 (iii) vrijedi da je generirajuća matrica rešetke $\Lambda(\mathcal{C}_2)^*$ jednaka:

$$(M^{-1})^{\top} = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix}^{-1} \right)^{\top} = \frac{1}{\sqrt{2}} \begin{bmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ 0 & 0 & 1 \end{bmatrix}^{\top} = \frac{1}{\sqrt{2}} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ -1 & -1 & 1 \end{bmatrix}.$$

Tada prema teoremu 5.1 (iii) slijedi da je to generirajuća matrica rešetke $\Lambda(\mathcal{C}_2^{\perp})$.

Primjer 5.3. Odredimo rešetku $\Lambda(e_8)$ konstrukcijom A iz binarnog koda e_8 tipa II iz primjera 3.5.

Generirajuća matrica binarnog $[8, 4, 4]$ koda e_8 u standarnom obliku je

$$G_{e_8} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix},$$

pa su generirajuća i Gramova matrica rešetke $\Lambda(e_8)$ jednake:

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}, \quad A = \begin{bmatrix} 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 \end{bmatrix}.$$

Prema teoremu 5.1 (vii) slijedi da je rešetka $\Lambda(e_8)$ tipa II, kako je kod $\Lambda(e_8)$ tipa II.
Odredimo sada minimalnu normu, determinantu i rešetku $\Lambda(e_8^{\perp})$ koristeći teorem 5.1:

$$\mu = \mu(\Lambda(e_8)) = 2,$$
$$\det(\Lambda(e_8)) = 2^{\frac{8-2\cdot 4}{2}} = 1.$$

Iz teorema 4.1 (iii) slijedi da je generirajuća matrica rešetke $\Lambda(e_8^{\perp})$ jednaka:

$$(M^{-1})^{\top} = \left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}^{-1}\right)^{\top} = \frac{1}{\sqrt{2}}\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & -1 & -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & -1 & 0 & 0 & 1 & 0 \\ -1 & -1 & 0 & -1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

6 Zaključak

U ovom radu istraženi su ključni aspekti linearnih kodova i rešetki, naglašavajući njihovu međusobnu povezanost i primjene. Binarni linearni kodovi, uz pomoć generirajućih matrica, omogućuju učinkovitu izgradnju kodnih riječi, dok samodualni kodovi pružaju dodatna svojstva koja su korisna u različitim kontekstima, kao na primjer ispravljanju grešaka, kriptografiji te u teoriji rešetki i kvantnoj teoriji.

Rešetke, definirane generirajućim i Gramovim matricama, proširuju primjene teorije kodiranja u područjima poput kriptografije i teorije brojeva. Imaju široku primjenu kod bežične komunikacije u mobilnim komunikacijskim sustavima poput 4G i 5G mreža, u satelitskoj komunikaciji, kod digitalne televizije i radija, te pohrane podataka na memorijskim uređajima.

Konstrukcija A predstavlja ključnu metodu za povezivanje linearnih kodova s rešetkama, omogućujući prijenos korisnih svojstava između ovih dvaju područja. Koristi se u računskim algoritmima i optimizaciji, teoriji informacija te kod skladištenja podataka. Buduća istraživanja mogu dodatno unaprijediti razumijevanje i primjenu ovih matematičkih struktura, otvarajući nove mogućnosti u teoriji informacija i drugim područjima.

Popis slika

Literatura

[1] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[2] J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, 2008.

[3] E. Bannai, S. T. Dougherty, M. Harada, M. Oura, *Type II codes, even unimodular lattices, and invariant rings*, IEEE Trans. Inf. Theory, 45(4), 1194-1205, 1999.

[4] J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* 3rd ed., Springer-Verlag, 1999.

[5] I. S. Pandžić, A. Bažant, Ž. Ilić, Z. Vrdoljak, M. Kos, V. Sinković, *Uvod u teoriju informacija i kodiranja*, Element, 2009.

[6] K. Horvatić, *Linearna algebra*, Golden marketing - Tehnička knjiga, 2004.