math.e

Hrvatski matematički elektronički časopis

Rešetke i samodualni kodovi

Sara Ban Martinović
Fakultet za matematiku,
Sveučilište u Rijeci,
e-mail: `sban@math.uniri.hr`

Margareta Crnčić
Fakultet za matematiku,
Sveučilište u Rijeci,
e-mail: `megipriv12@gmail.com`

1 Sažetak

U ovom radu se bavimo linearnim kodovima, s posebnim naglaskom na binarne samodualne linearne kodove. Promotrit ćemo njihova svojstva i primjenu u teoriji rešetki. Navest ćemo poveznicu binarnih linearnih kodova i rešetki, pod nazivom konstrukcija A.

Ključne riječi: samodualni kodovi, rešetke, generirajuća matrica, Gramova matrica, cjelobrojne rešetke, samodualne rešetke, konstrukcija A.

2 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.

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.

3 Linearni kodovi

Definicija 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 $\mathbb{F}_q$. Elemente koda $\mathcal{C}$ nazivamo **riječima koda** $\mathcal{C}$, a broj n **duljinom koda** $\mathcal{C}$.

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

Definicija 2. Neka je $\mathcal{C}$ linearan $[n, k]$ kod. **Generirajuća matrica** koda $\mathcal{C}$ je matrica reda $k \times n$ \v{c}iji su retci vektori baze prostora $\mathcal{C}$.

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.

3.1 Samodualni kodovi

Definicija 3. Neka je $\mathcal{C}[n, k]$ 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 $\mathbf{x} \cdot \mathbf{y} = \displaystyle\sum_{i=1}^{n} x_i y_i$, $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.

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

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

Definicija 5. Linearni kod $\mathcal{C}$ je **samoortogonalan** ako je $\mathcal{C} \subseteq \mathcal{C}^\perp$. Kažemo da je linearni kod $\mathcal{C}$ **samodualan** ako je $\mathcal{C} = \mathcal{C}^\perp$.

Napomena 6. Neka je $\mathcal{C}$ linearni $[n, k]$ kod s generirajućom matricom G.

(1) $\mathcal{C}$ je samoortogonalan ako i samo ako je $GG^\top = O$, gdje je O nulmatrica.
(2) $\mathcal{C}$ je samodualan ako i samo ako je samoortogonalan i $k = \frac{n}{2}$.

Primjer 7. Neka je $\mathcal{H}_3$ binarni kod zadan generirajućom matricom:

$$G_{\mathcal{H}_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Kod $\mathcal{H}_3$ se zove **Hammingov** $[7,4]$ **kod**. Ovim kodom podatke od četiri bita kodiramo u sedam bitova, dodajući tri bita provjere parnosti. Kod $\mathcal{H}_3$ može detektirati najviše dvije pogreške ukoliko su se dogodile ili ispraviti najviše jednu pogrešku (vidi više u \cite[Poglavlje 3.5]{l:3}). Dodavanjem bita provjere parnosti dobivamo matricu:

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

Kod e_8 generiran matricom G_{e_8} se zove **prošireni** $[8,4]$ **Hammingov kod**. Budući da vrijedi $k = \frac{n}{2}$ i

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

iz napomene 6 slijedi da je kod e_8 samodualan.

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 8. Neka je $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ baza za $\mathbb{R}^n$. **Rešetka** Λ u $\mathbb{R}^n$ generirana s B je

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

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

$$M = \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \ldots & v_{nn} \end{bmatrix}, \tag{1}$$

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

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

Koristit ćemo i sljedeći način označavanja rešetke Λ generirane s $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$:

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

Definicija 9. Neka je Λ rešetka u $\mathbb{R}^n$ s generirajućom matricom $M \in M_n(\mathbb{R})$. **Gramova matrica** rešetke Λ je matrica $A = MM^\top \in M_n(\mathbb{R})$.

Elementi Gramove matrice A su standardni skalarni produkti u $\mathbb{R}^n$ vektora baze rešetke Λ.

Definicija 10. 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

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

Determinanta rešetke Λ je n-dimenzionalni volumen od $\mathcal{F}$. Označava se sa $\det \Lambda$.

Propozicija 11. *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 $\mathrm{Vol}\,\mathcal{F}$, vrijedi sljedeća jednakost:*

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

Dokaz propozicije 11 može se naći u [2]. Iz propozicije 11 slijedi:

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

Definicija 12. Neka je Λ rešetka u $\mathbb{R}^n$. Kažemo da je rešetka Λ **cjelobrojna** ako vrijedi

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

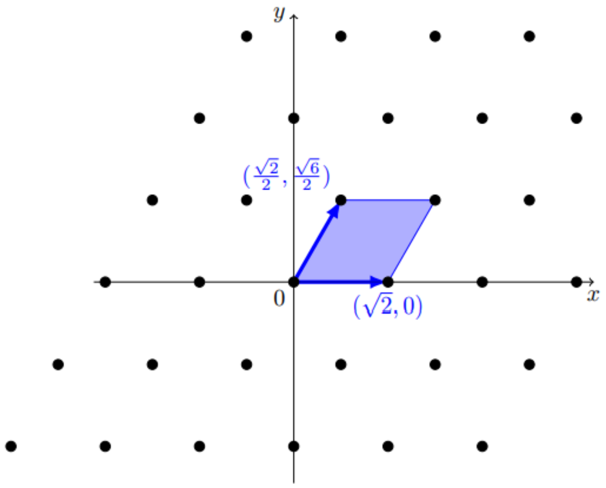
gdje je $\mathbf{x} \cdot \mathbf{y}$ standardni skalarni produkt u $\mathbb{R}^n$.

Ako Gramova matrica rešetke Λ ima cjelobrojne elemente, tada je rešetka Λ cjelobrojna.

Primjer 13. Odredimo determinantu, Gramovu matricu i fundamentalnu domenu rešetke

$$\Lambda_2 = \Lambda_2(M_2), \text{ gdje je } M_2 = \begin{bmatrix} \sqrt{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{2} \end{bmatrix}.$$

$$\det \Lambda_2 = \begin{vmatrix} \sqrt{2} & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{2} \end{vmatrix} = \sqrt{3}, \ A_2 = M_2 M_2^\top = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$



Slika 1: Fundamentalna domena planarne heksagonalne rešetke

Budući da matrica A_2 ima cjelobrojne vrijednosti, slijedi da je rešetka Λ_2 cjelobrojna. Na slici 1 prikazana je rešetka Λ_2 te njena fundamentalna domena obojena plavom bojom. Ova rešetka naziva se **planarnom heksagonalnom rešetkom**.

4.1 Samodualne rešetke

Definicija 14. 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 15. Kažemo da je cjelobrojna rešetka Λ **samodualna (unimodularna)** ako vrijedi $\Lambda = \Lambda^*$.

Teorem 16. *[3, Teorem 10.6.3] Neka jeΛ rešetka u $\mathbb{R}^n$ s bazom $B = \{\mathbf{v}_1, \mathbf{v}_2 \dots, \mathbf{v}_n\}$ te s pripadnom generirajućom matricom M i Gramovom matricom A. Tada vrijedi:*

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

(i) Uočimo da jednakost

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

vrijedi zbog linearnosti skalarnog produkta u $\mathbb{R}^n$.
Nadalje, dokažimo drugu jednakost:

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

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

$$\mathbf{y}M^\top = \begin{bmatrix} \mathbf{v}_1 \cdot \mathbf{y} & \mathbf{v}_2 \cdot \mathbf{y} & \dots & \mathbf{v}_n \cdot \mathbf{y} \end{bmatrix}.$$

Budući da vrijedi $\mathbf{v}_i \cdot \mathbf{y} \in \mathbb{Z}, \forall 1 \le i \le n$, slijedi 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 je $\mathbf{y} \in \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{v}_i \cdot \mathbf{y} \in \mathbb{Z}, \forall 1 \le i \le n\}$.

(ii) Neka su $\mathbf{w}_1, \dots, \mathbf{w}_n$ retci matrice $(M^{-1})^\top$. Tada je $\{\mathbf{w}_1, \dots, \mathbf{w}_n\}$ 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, $\mathbf{w}_1, \dots, \mathbf{w}_n \subseteq \Lambda^*$, prema svojstvu (i). Neka je $\mathbf{w} \in \Lambda^*$. Tada je

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

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

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

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

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 koji vrijedi

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

Matricu A^{-1} možemo zapisati na sljedeći način:

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

gdje je $\mathrm{adj}(A) = \left[(-1)^{i+j}M_{ij}\right]^\top$. Kako je Λ cjelobrojna rešetka, matrica A je cjelobrojna, pa su minore $M_{ij} \in \mathbb{Z}$, za $1 \leq i, j \leq n$.

Nadalje,

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

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 17. Odredimo dualnu rešetku Λ_2^* planarne heksagonalne rešetke $\Lambda_2 = \Lambda_2(M_2)$ te njenu determinantu i fundamentalnu domenu.

Prema teoremu 16 (ii), generirajuća matrica dualne rešetke Λ_2^* je

$$(M_2^{-1})^\top = \begin{bmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{6}}{6} \\ 0 & \frac{\sqrt{6}}{3} \end{bmatrix}.$$

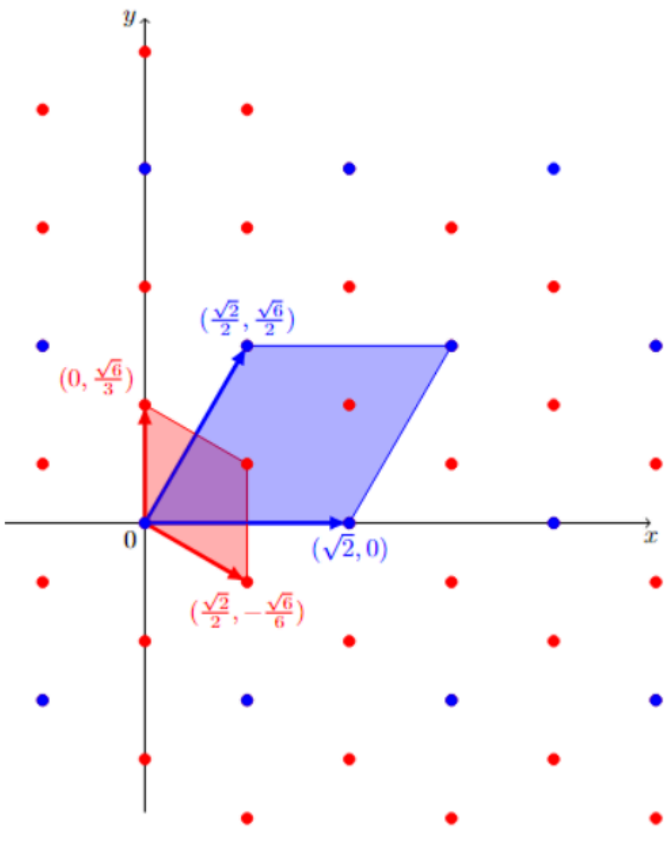
Stoga vrijedi:

$$\Lambda_2^* = \{\mathbf{z}\,(M_2^{-1})^\top \mid \mathbf{z} \in \mathbb{Z}^2\} = \left\{\left(\frac{\sqrt{2}}{2}z_1, -\frac{\sqrt{6}}{6}z_1 + \frac{\sqrt{6}}{3}z_2\right) \mid z_1, z_2 \in \mathbb{Z}\right\}.$$

Nadalje, po teoremu 16 (iv) slijedi

$$\det \Lambda_2^* = \frac{1}{\det \Lambda_2} = \frac{\sqrt{3}}{3}.$$

Podskupovnost $\Lambda_2 \subseteq \Lambda_2^*$



Slika 2: Fundamentalne domene rešetki Λ_2 i Λ_2^*

slijedi iz teorema 16 (v) i \v{c}injenice da je rešetka Λ_2 cjelobrojna. Nadalje, prema teoremu 16 (vii) i iz \v{c}injenice da je $\det \Lambda_2 = \sqrt{3}$, slijedi da Λ_2 nije samodualna rešetka. Na slici 2 su točke dualne rešetke Λ_2^* i njena fundamentalna domena obojene crvenom bojom.

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

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

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:

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

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

$$A = \frac{1}{2} \begin{bmatrix} I_k + CC^\top & 2C \\ 2C^\top & 4I_{n-k} \end{bmatrix}.$$

Teorem 18. *[3, Teorem 10.6.4] Neka je $\mathcal{C}$ binarni $[n, k]$ kod. Tada vrijedi:*

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

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

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

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

Dokaz. Neka je $\mathcal{C}$ binarni $[n, k]$ 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.

(i) Vrijedi:

$$\det M = 2^{-\frac{n}{2}} \det I_k \cdot \det(2I_{n-k}) = 2^{\frac{n-2k}{2}}.$$

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

(ii) Budući da je $G^\perp = [C^\top \mid I_{n-k}]$ 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. Slijedi da je realni skalarni produkt retka iz M s retkom iz $M^\perp$ cijeli broj. Tada je $M^\perp M^\top$ matrica s cjelobrojnim vrijednostima, te vrijedi $\Lambda(\mathcal{C}^\perp) \subseteq \Lambda(\mathcal{C})^*$.

Neka je sada $\mathbf{y} \in \Lambda(\mathcal{C})^*$. Tada je $\mathbf{y}M^\top \in \mathbb{Z}^n$, prema teoremu 16 (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

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

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

(iii) 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.

(iv) Neka je rešetka $\Lambda(\mathcal{C})$ samodualna. Tada je rešetka $\Lambda(\mathcal{C})$ cjelobrojna iz čega slijedi da je kod $\mathcal{C}$ samoortogonalan, prema (iii). Zatim, prema teoremu 16 (vii), vrijedi $\det \Lambda(\mathcal{C}) = 1$, \v{s}to implicira $k = \frac{n}{2}$. Prema napomeni 6, kod $\mathcal{C}$ je samodualan.

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

□

Primjer 19. Odredimo rešetku $\Lambda(e_8)$ konstrukcijom A iz proširenog $[8,4]$ Hammingovog koda e_8. Generirajuća i Gramova matrica rešetke $\Lambda(e_8)$ su jednake:

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

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

Prema teoremu 18 (iv), slijedi da je rešetka $\Lambda(e_8)$ samodualna, kako je kod e_8 samodualan.

6 Zaključak

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 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.

Napomena: Članak je nastao iz diplomskog rada studentice Margarete Crnčić, pod mentorstvom doc. dr. sc. Sare Ban Martinović, na diplomskom studiju Diskretna matematika i primjene Fakulteta za matematiku Sveučilišta u Rijeci.

Bibliografija

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

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

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

[4] M. Lukanović, *Teorija kodiranja i linearni kodovi*, diplomski rad, Osijek, 2017.

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

---

[1]email: sban@math.uniri.hr
[2]email: megipriv12@gmail.com

ISSN 1334-6083