# Kodovi iz Hadamardovih matrica reda 48

Loredana Simčić
(loredana.simcic@riteh.hr)

- **D. Crnković, V. Mikulić**: Self-orthogonal doubly-even codes from Hadamard matrices of order 48, Advances and Applications in Discrete Mathematics. 1 (2008), 2; 159-170

# Uvod: Kodovi

**Definicija**

Kod $K$ duljine $n$ nad alfabetom $F_q$ veličine $q$ je podskup $K \subset F_q^n$.

Kod je binaran za $q = 2$.
Elementi koda zovu se riječi koda.

**Primjer**

$$K = \{00000, 01101, 10110, 11011\} \subset F_2^5$$

### Hammingova udaljenost

Neka je $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in F_q^n$.
Broj

$$d(x, y) = |\{i \,|\, 1 \leq i \leq n, x_i \neq y_i\}|$$

se naziva Hammingova udaljenost.

### Minimalna udaljenost

Minimalna udaljenost koda $K$ je broj

$$d = \{d(x, y) \,|\, x, y \in K, x \neq y\}$$

### Težina riječi koda

Za $x \in F_q^n$, težina $w(x)$ od $x$ je definirana sa

$$w(x) = d(x, 0)$$

## Težinski enumerator

Težinski enumerator koda $K$ je polinom

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

gdje je $A_i$ broj riječi koda težine $i$.

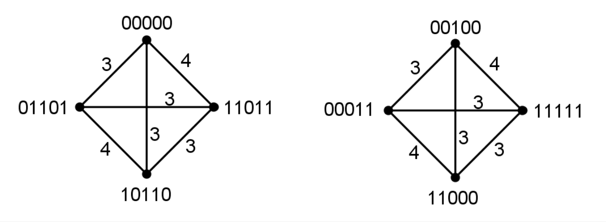
Kod je paran ako su sve težine parne i dvostruko paran ako su sve težine djeljive sa 4.

## Primjer

$$K = \{00000, 01101, 10110, 11011\} \subset F_2^5$$
$$d(01101, 10110) = 4$$
$$A(x) = x^4 + 2x^3 + 1$$

# Ekvivalentni kodovi

$$K_1 = \left\{ \begin{matrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{matrix} \right. \qquad K_2 = \left\{ \begin{matrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{matrix} \right.$$



### Ekvivalentni kodovi

Dva su koda ekvivalentna ako se jedan može dobiti iz drugoga permutacijom koordinata u svim riječima koda ili permutacijom simbola unutar jedne koordinate.

### Izomorfni kodovi

Dva su koda izomorfna ako se jedan može dobiti iz drugoga permutacijom koordinata u svim riječima koda.

# Linearni kodovi

**Definicija**

Neka je $q$ prim broj i neka je $F_q$ konačno polje reda $q$.
Linearan kod duljine $n$ je linearni podprostor vektorskog prostora $F_q^n$.
$k$-dimenzionalni potprostor od $F_q^n$ se naziva linearni $[n, k]$ kod nad $F_q$.

Za linearni kod $K$ minimalna udaljenost je jednaka minimalnoj težini,

$$d = min\{w(x) | x \in K, x \neq 0\}$$

Linearni $[n, k, d]$ kod je linearni $[n, k]$ kod s minimalnom udaljenošću (ili težinom) $d$.

## Generirajuća matrica linearnog koda

Matrica dimenzije $k \times n$ čiji se retci sastoje od vektora baze koda $[n, k, d]$ zove se generirajuća matrica.

## Primjer

$$K = \begin{cases} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{cases}$$

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

## Standardni oblik generirajuće matrice

Za generirajuću matricu $G$ linearnog $[n, k, d]$ koda kaže se da je u standardnom obliku ako je $G = [I_k|A]$, gdje je $I_k$ jedinična matrica reda $k$ i $A$ neka $k \times (n-k)$ matrica.

## Egzistencija standardnog oblika

Svaka generirajuća matrica $G$ linearnog $[n, k, d]$ koda može se operacijama zamjene redaka, zamjene stupaca i dodavanja jednog retka drugom retku svesti na oblik $G = [I_k|A]$.

## Primjer

$$G^* = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

# Kodiranje linearnim kodovima

$G = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_k \end{bmatrix}$ - generirajuća matrica koda $K$ ($r_i$ - vektori baze)

$m = [m_1 m_2 \ldots m_k]$ - poruka

$$x = \sum_{i=1}^{k} m_i \cdot r_i = m \cdot G$$

## Primjer

$G$ nije u standardnom obliku

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$m = 0\,1$$

$$x = 1\,1\,0\,1\,1$$

$G$ je u standardnom obliku

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$m = 0\,1$$

$$x = \underbrace{0\,1}_{poruka}\ \underbrace{0\,1\,1}_{zalihost}$$

# Dekodiranje linearnog koda

## Suskup

Neka je $K \subset F_q^n$ $[n, k]$ kod i neka je $x \in F_q^n$. Podskup

$$x + K = \{x + y | y \in K\}$$

se naziva suskup od $K$.

## Propozicija

Neka je $K$ [n,k] kod.

- Svaki suskup $x + K$ ima $2^k$ elemenata.
- Ako je $y \in x + K$, tada je $x + K = y + K$.
- Svaki $x \in F_q^n$ pripada točno jednom suskupu.
- Različitih suskupa ima $2^{n-k}$.

## Standardni niz

$K = \{00000, 11100, 00111, 11011\}$

| | | | | |
|---|---|---|---|---|
| $K$ | 00000 | 11100 | 00111 | 11011 |
| $00001 + K$ | 00001 | 11101 | 00110 | 11011 |
| $00010 + K$ | 00010 | 11110 | 00101 | 11001 |
| $00100 + K$ | 00100 | 11000 | 00011 | 11111 |
| $01000 + K$ | 01000 | 10100 | 01111 | 10011 |
| $10000 + K$ | 10000 | 01100 | 10111 | 01011 |
| $10010 + K$ | 10010 | 01110 | 10101 | 01001 |
| $10001 + K$ | 10001 | 01101 | 10110 | 01010 |

# Dualni kod

## Skalarni produkt

Skalarni produkt vektora $x = (x_1 \dots x_n)$ i $y = (y_1 \dots y_n)$, $x, y \in F_q^n$ je skalar $\langle x, y \rangle = \sum_{i=1}^n x_i y_i \in F_q$.
Ako je $\langle x, y \rangle = 0$, kažemo da su $x$ i $y$ ortogonalni.

## Dualni kod

Za linearni kod $K \subset F_q^n$ definiramo dualni kod $K^\perp \subset F_q^n$ sa

$$K^\perp = \{x \in F_q^n \,|\, (\forall y \in K)\, \langle x, y \rangle = 0\}$$

Za $[n, k]$ kod $K$ se kaže da je samoortogonalan ako je $K \subset K^\perp$, a samodualan ako je $K = K^\perp$.
Za binarni kod se kaže da je samokomplementaran ako sadrži vektor $11 \dots 1$.

## Primjer dualnog koda

$$K = \begin{cases} 00000 \\ 11100 \\ 10111 \\ 01011 \end{cases} \quad K^{\perp} = \begin{cases} 00000 & 01110 \\ 10100 & 01101 \\ 11010 & 00011 \\ 11001 & 10111 \end{cases}$$

## Primjer samodualnog koda

$$K = \begin{cases} 0000 \\ 1100 \\ 0011 \\ 1111 \end{cases} \quad K^{\perp} = \begin{cases} 0000 \\ 1100 \\ 0011 \\ 1111 \end{cases}$$

Ako je $K$ $[n, k]$ kod, tada je $K^{\perp}$ $[n, n-k]$ kod.

### Paritetna matrica

Neka je $K \subset F_q^n$ kod. Paritetna matrica za kod $K$ je generirajuća matrica za dualni kod $K^{\perp}$.

### Lema

Neka je $G$ generirajuća i $H$ paritetna matrica koda $K$. Tada vrijedi

$$G \cdot H^T = 0$$

### Propozicija

Neka je $K$ $[n, k]$ kod i neka je $G = [I_k | A]$ njegova generirajuća matrica u standardnom obliku. Tada je

$$H = [A^T | I_{n-k}]$$

paritetna matrica koda $K$.

# Sindromsko dekodiranje

## Sindromsko preslikavanje

Neka je $H$ paritetna matrica $[n, k]$ koda $K$. Preslikavanje $S : F_q^n \to F_q^{n-k}$ definirano sa

$$S(y) = y \cdot H^T$$

naziva se sindromsko preslikavanje.
Vektor $S(y)$ naziva se sindrom riječi $y$.

## Propozicija

Neka je $S : F_q^n \to F_q^{n-k}$ sindromsko preslikavanje $[n, k]$ koda $K$. Tada je

$$Ker(S) = K$$

## Primjer

| | | | | Sindrom |
|---|---|---|---|---|
| 00000 | 11100 | 00111 | 11011 | 000 |
| 00001 | 11101 | 00110 | 11011 | 001 |
| 00010 | 11110 | 00101 | 11001 | 010 |
| 00100 | 11000 | 00011 | 11111 | 100 |
| 01000 | 10100 | 01111 | 10011 | 011 |
| 10000 | 01100 | 10111 | 01011 | 111 |
| 10010 | 01110 | 10101 | 01001 | 101 |
| 10001 | 01101 | 10110 | 01010 | 110 |

## Lema

Neka je $S : F_q^n \to F_q^{n-k}$ sindromsko preslikavanje $[n, k]$ koda $K$ i $x, y \in F_q^n$. Vrijedi $S(x) = S(y)$ akko $x$ i $y$ pripadaju istom koskupu.

## Tablica preslikavanja

| $e_i$ | $S(e_i)$ |
|---|---|
| 00000 | 000 |
| 00001 | 001 |
| 00010 | 010 |
| 00100 | 100 |
| 01000 | 011 |
| 10000 | 111 |
| 10010 | 101 |
| 10001 | 110 |

## Sindromsko dekodiranje

- Izračunaj sindrom primljene riječi $y$
- Iz tablice preslikavanja odredi vektor $e_i$
- Poslana riječ je $x = y - e_i$

# Dizajni. Hadamardove matrice

## Incidencijska struktura

Incidencijska struktura $\mathcal{D}$ je uređena trojka $(\mathcal{P}, \mathcal{B}, \mathcal{I})$, gdje su $\mathcal{P}$ i $\mathcal{B}$ neprazni disjunktni skupovi i $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$.

## Matrica incidencije

Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ konačna incidencijska struktura gdje je $\mathcal{P} = \{x_1, \ldots, x_v\}$ i $\mathcal{B} = \{B_1, \ldots, B_b\}$. Matrica incidencije incidencijske strukture $\mathcal{D}$ je $b \times v$ matrica $M = (m_{ij})$

$$m_{ij} = \begin{cases} 1, & (x_j, B_i) \in \mathcal{I} \\ 0, & (x_j, B_i) \notin \mathcal{I} \end{cases}$$

## Dizajn

Konačna incidencijska struktura $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ je $t - (v, k, \lambda)$ dizajn ako vrijedi sljedeće:

1. $|\mathcal{P}| = v$
2. svaki element skupa $\mathcal{B}$ incidentan je s točno $k$ elemenata skupa $\mathcal{P}$
3. svakih $t$ elemenata skupa $\mathcal{P}$ incidentno je s točno $\lambda$ elemenata skupa $\mathcal{B}$

Elementi skupa $\mathcal{P}$ nazivaju se točke, a elementi skupa $\mathcal{B}$ blokovi.

$2 - (v, k, \lambda)$ dizajn naziva se blok dizajn. U blok dizajnu svaka je točka incidentna s točno $r = \frac{\lambda(v-1)}{k-1}$ blokova.

Ako vrijedi $|\mathcal{P}| = |\mathcal{B}| = v$ i $2 \leq k \leq v - 2$, tada se $2 - (v, k, \lambda)$ dizajn naziva simetričan dizajn.

## Hadamardove matrice

Hadamardova matrica reda $m$ je $(m \times m)$ matrica $H = (h_{ij})$, $h_{ij} \in \{-1, 1\}$, takva da vrijedi $HH^T = H^T H = mI_m$, gdje je $I_m$ $(m \times m)$ jedinična matrica.

## Primjer

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

### Teorem

Postoji Hadamardova matrica reda $m$ ako i samo ako postoji (simetričan) $(m-1, \frac{1}{2}m-1, \frac{1}{4}m-1)$ dizajn.

### Hadamardov dizajn

Simetrični dizajn s parametrima $(m-1, \frac{1}{2}m-1, \frac{1}{4}m-1)$ naziva se Hadamardov dizajn.

### Primjer: Matrica incidencije Hadamardovog (7,3,1) dizajna

$$M = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

## Hadamardov 3-dizajn

Dizajn $\mathcal{D}^* = (\mathcal{P}^*, \mathcal{B}^*, \mathcal{I}^*)$ dobiven iz Hadamardovog $(m-1, \frac{1}{2}m-1, \frac{1}{4}m-1)$ dizajna na sljedeći način:

- $\mathcal{P}^* = \mathcal{P} \cup \{\infty\}$
- $\mathcal{B}^* = \{B \cup \{\infty\} | B \in \mathcal{B}\} \cup \{\mathcal{P} \backslash B | B \in \mathcal{B}\}$

je $3-(m, \frac{1}{2}m, \frac{1}{4}m-1)$ i naziva se Hadamardov 3-dizajn.

Neka je $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ incidencijska struktura. Kod od $\mathcal{S}$ nad poljem $F$ je podprostor $K_F(\mathcal{S})$ od $F^{\mathcal{P}}$ razapet vektorima koji odgovaraju karakterističnim funkcijama blokova od $\mathcal{S}$.

**Teorem**

Za svaki prim broj $p$ i svaku klasu ekvivalencije Hadamarovih matrica postoji, do na ekvivalentnost koda, točno jedan $p$-narni kod povezan sa 3-dizajnom dobivenim iz klase ekvivalencije.

Ako je $H$ Hadamardova matrica, tada je $p$-narni kod od $H$ (oznaka: $K_p(H)$) $p$-narni kod povezan sa bilo kojim 3-dizajnom dobivenim iz $H$.

# Kodovi iz Hadamardovih matrica reda 48

Iz Hadamardovih matrica reda 48 dobivamo $(47, 23, 11)$ Hadamardove dizajne.
Postoji 54 takva simetrična dizajna.

- **D. Crnković, S. Rukavina**: Some Symmetric (47,23,11) Designs, Glas. Mat. Ser. III 38(58), No. 1 (2003), 1-9

### Teorem

Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn sa kardinalnostima presjeka blokova $s_1,\ldots,s_m$. Označimo sa $K$ binarni kod razapet incidencijskom matricom dizajna $\mathcal{D}$. Tada vrijedi:

1. Ako su $k,s_1,\ldots,s_m$ svi parni, tada je $K$ samoortogonalan.
2. Ako su $v,k,s_1,\ldots,s_m$ svi parni, tada je $K$ sadržan u samodualnom kodu duljine $v$.
3. Ako je $v\equiv 0(mod 8)$, $k\equiv 0(mod 4)$ i $s_1,\ldots,s_m$ su svi parni, tada je $K$ sadržan u dvostruko parnom samodualnom kodu duljine $v$.
4. Dualni kod $K^{\perp}$ ima minimalnu udaljenost $d^{\perp}\geq\dfrac{r+\lambda}{\lambda}$.

### Lema

Neka je $K$ kod iz Hadamardove matrice reda 48. Tada je $K$ samoortogonalan dvostruko parni kod. $K$ je i samokomplementaran kod. Nadalje, $K^{\perp}$ je paran samokomplementaran kod.

**Dokaz**

Dva bloka $3-(48,24,11)$ dizajna se sijeku u 12 ili 0 točaka, pa možemo primjeniti teorem. Dakle, $K$ je samoortogonalan dvostruko paran kod.
Za svaki blok Hadamardovog 3-dizajna, njegov komplement je također blok dizajna, pa je binarni kod $K$ samokomplementaran, iz čega slijedi i da je $K^{\perp}$ paran kod.
S obzirom da su sve težine koda $K$ parne, $K^{\perp}$ sadrži vektor $11\ldots1$.

### Ekvivalencija Hadamardovih matrica

Matrice $A$ i $B$ su izomorfne ako se $B$ može dobiti iz $A$ permutacijama redaka i stupaca.

Hadamardove matrice $H_1$ i $H_2$ su ekvivalentne ako i samo ako su matrice $H_1^*$ i $H_2^*$ izomorfne, pri čemu je

$$H^* = \begin{bmatrix} H & -H \\ -H & H \end{bmatrix}$$

Iz 54 Hadamardova (47,23,11) dizajna dobije se 27 neekvivalentnih Hadamardovih matrica.

# Rezultati

Iz 27 neekvivalentnih Hadamardovih matrica reda 48 dobije se 15 neekvivalentnih binarnih linearnih kodova.

$C_1$ - $[48, 13, 8]$ kod dobiven iz dizajna $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_5$ i $\mathcal{D}_8$

$$A(x) = x^0 + 66x^8 + 494x^{16} + 7068x^{24} + 495x^{32} + 66x^{40} + x^{48}$$

$C_2$ - $[48, 23, 4]$ kod dobiven iz dizajna $\mathcal{D}_3, \mathcal{D}_4, \mathcal{D}_6, \mathcal{D}_7, \mathcal{D}_{12}, \mathcal{D}_{13}, \mathcal{D}_{15}$ i $\mathcal{D}_{16}$

$$A(x) = x^0 + 132x^4 + 5346x^8 + 67188x^{12} + 367983x^{16} + 980232x^{20} + 5546844x^{24} + 980232x^{28} + 367983x^{32} + 67188x^{36} + 5346x^{40} + 132x^{44} + x^{48}$$

$C_3$ - $[48, 13, 12]$ kod dobiven iz dizajna $\mathcal{D}_9$ i $\mathcal{D}_{18}$

$$A(x) = x^0 + 66x^{12} + 275x^{16} + 1342x^{20} + 4824x^{24} + 1342x^{28} + 275x^{32} + 66x^{36} + x^{48}$$

$C_4$ - $[48, 23, 4]$ kod dobiven iz dizajna $\mathcal{D}_{10}, \mathcal{D}_{11}$ i $\mathcal{D}_{17}$

$$A(x) = x^0 + 66x^4 + 90x^8 + 29018x^{12} + 283679x^{16} + 1733732x^{20} + 4293812x^{24} + 1733732x^{28} + 283679x^{32} + 29018x^{36} + 902x^{40} + 66x^{44} + x^{48}$$

$C_5$ - $[48, 13, 16]$ kod dobiven iz dizajna $\mathcal{D}_{14}$

$$A(x) = x^0 + 759x^{16} + 6672x^{24} + 759x^{32} + x^{48}$$

$C_6$ - $[48, 14, 12]$ kod dobiven iz dizajna $\mathcal{D}_{19}$ i $\mathcal{D}_{36}$

$$A(x) = x^0 + 136x^{12} + 495x^{16} + 2904x^{20} + 9312x^{24} + 2904x^{28} + 495x^{32} + 136x^{36} +$$

$C_7$ - $[48, 24, 4]$ kod dobiven iz dizajna $\mathcal{D}_{20}, \mathcal{D}_{21}$ i $\mathcal{D}_{35}$

$$A(x) = x^0 + 66x^4 + 1254x^8 + 55642x^{12} + 546975x^{16} + 3581028x^{20} + 8407284x^{24} + 3581028x^{28} + 546975x^{32} + 55642x^{36} + 1254x^{40} + 66x^{44} + x^{48}$$

$C_8$ - $[48, 14, 8]$ kod dobiven iz dizajna $\mathcal{D}_{22}, \mathcal{D}_{23}, \mathcal{D}_{26}$ i $\mathcal{D}_{27}$

$$A(x) = x^0 + 66x^8 + 4x^{12} + 759x^{16} + 1980x^{20} + 10764x^{24} + 1980x^{28} + 759x^{32} + 4x^{36} + 66x^{40} + x^{48}$$

$C_9$ - $[48, 24, 4]$ kod dobiven iz dizajna $\mathcal{D}_{24}, \mathcal{D}_{25}, \mathcal{D}_{28}, \mathcal{D}_{29}, \mathcal{D}_{30}, \mathcal{D}_{31}, \mathcal{D}_{32}$ i $\mathcal{D}_{34}$

$$A(x) = x^0 + 132x^4 + 5346x^8 + 71284x^{12} + 638319x^{16} + 3007752x^{20} + 9331548x^{24} + 3007752x^{28} + 638319x^{32} + 71284x^{36} + 5346x^{40} + 132x^{44} + x^{48}$$

$C_{10}$ - $[48, 14, 12]$ kod dobiven iz dizajna $\mathcal{D}_{33}$

$$A(x) = x^0 + 4x^{12} + 1023x^{16} + 1980x^{20} + 10368x^{24} + 1980x^{28} + 1023x^{32} + 4x^{36} + x^{48}$$

$C_{11}$ - $[48, 14, 4]$ kod dobiven iz dizajna $\mathcal{D}_{37}, \mathcal{D}_{40}, \mathcal{D}_{51}$ i $\mathcal{D}_{54}$

$$A(x) = x^0 + 12x^4 + 66x^8 + 220x^{12} + 495x^{16} + 792x^{20} + 13212x^{24} + 792x^{28} + 495x^{32} + 220x^{36} + 66x^{40} + 12x^{44} + x^{48}$$

$C_{12}$ - $[48, 24, 4]$ kod dobiven iz dizajna $\mathcal{D}_{38}, \mathcal{D}_{39}, \mathcal{D}_{42}, \mathcal{D}_{43}, \mathcal{D}_{46}, \mathcal{D}_{49}, \mathcal{D}_{52}$ i $\mathcal{D}_{53}$

$$A(x) = x^0 + 276x^4 + 10626x^8 + 134596x^{12} + 735471x^{16} + 1961256x^{20} + 11092764x^{24} + 1961256x^{28} + 735471x^{32} + 134596x^{36} + 10626x^{40} + 276x^{44} + x^{48}$$

$C_{13}$ - $[48, 14, 4]$ kod dobiven iz dizajna $\mathcal{D}_{41}$ i $\mathcal{D}_{44}$

$$A(x) = x^0 + x^4 + 11x^8 + 121x^{12} + 451x^{16} + 3014x^{20} + 9186x^{24} + 3014x^{28} + 451x^{32} + 121x^{36} + 11x^{40} + x^{44} + x^{48}$$

$C_{14}$ - $[48, 14, 4]$ kod dobiven iz dizajna $\mathcal{D}_{45}$

$$\begin{aligned}A(x) =& x^0 + x^4 + 77x^{12} + 1111x^{16} + 946x^{20} + 12112x^{24}\\ &+ 946x^{28} + 1111x^{32} + 77x^{36} + x^{44} + x^{48}\end{aligned}$$

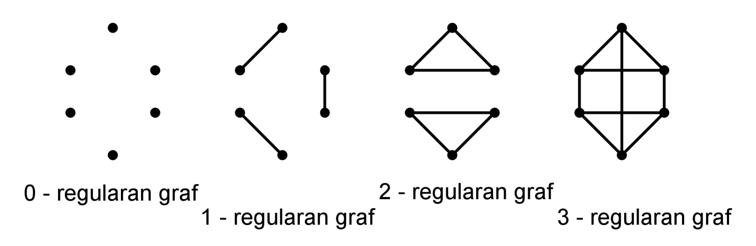
$C_{15}$ - $[48, 24, 4]$ kod dobiven iz dizajna $\mathcal{D}_{47}, \mathcal{D}_{48}$ i $\mathcal{D}_{50}$

$$\begin{aligned}A(x) =& x^0 + 78x^4 + 2046x^8 + 58102x^{12} + 564927x^{16} + 3474108x^{20}\\ &+ 8578692x^{24} + 3474108x^{28} + 564927x^{32} + 58102x^{36} + 2046x^{40}\\ &+ 78x^{44} + x^{48}\end{aligned}$$

# Jako regularni grafovi

## Regularan graf

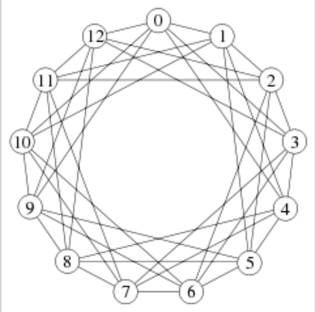
Regularan graf je graf u kojem svaki vrh ima isti stupanj.
Regularan graf sa vrhovima stupnja $k$ naziva se $k$-regularan graf ili regularan graf stupnja $k$.



## Jako regularan graf

Neka je $\mathcal{G}$ graf sa $n$ vrhova. Graf $\mathcal{G}$ je jako regularan graf s parametrima $(n, k, \lambda, \mu)$ ako vrijedi:

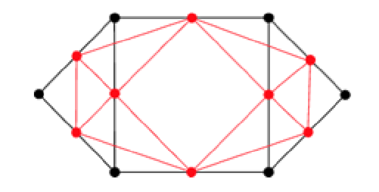
1. $\mathcal{G}$ je jednostavan $k$-regularan graf
2. svaka dva susjedna vrha imaju točno $\lambda$ zajedničkih susjednih vrhova
3. svaka dva nesusjedna vrha imaju točno $\mu$ zajedničkih susjednih vrhova




Slika: Payleyjev graf reda 13 (jako regularan graf s parametrima (13,6,2,3))

## Linijski graf

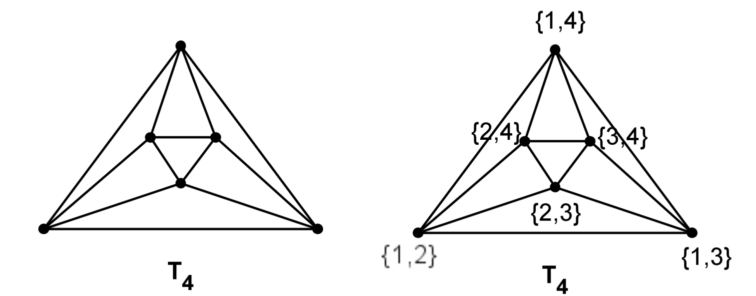
Linijski graf grafa $G$ je graf dobiven pridruživanjem vrha svakom bridu grafa $G$ i povezivanjem dva vrha bridom ako i samo ako odgovarajući bridovi grafa $G$ imaju barem jednu krajnju točku zajedničku.



## Triangularan graf

Triangularan graf $T_m$ je linijski graf potpunog grafa $K_m$.
Triangularan graf $T_m$ je jako regularan graf s parametrima $(\frac{m(m-1)}{2}, 2(m-2), m-2, 4)$.

Vrhovi grafa $T_m$ se mogu identificirati sa $2-$podskupovima skupa $\{1, 2, \ldots, m\}$. Vrhovi su susjedni ako i samo ako $2-$podskupovi imaju neprazan presjek.



# Dizajn nositelj

Nositelj ne-nul vektora $x = (x_1, \ldots, x_n) \in F_q^n$ je skup indeksa njegovih ne-nul koordinata,

$$supp(x) = \{i \mid x_i \neq 0\}$$

Dizajn nositelj koda duljine $n$ za danu težinu $w \neq 0$ je dizajn čije su točke indeksi koordinata, a blokovi nositelji svih riječi koda težine $w$.

Primjer

$K = \{000000, 001110, 010101, 011011, 100011, 101101, 110110, 111000\}$
$w = 3$

$$\mathcal{P} = \{1, 2, 3, 4, 5, 6\}$$
$$\mathcal{B} = \{345, 246, 156, 123\}$$

# Jako regularni grafovi dobiveni iz kodova

$\mathcal{S}_1$ - dizajn nositelj koda $C_1$ za $w = 8$
$\mathcal{S}_1$ ima 48 točaka i 66 blokova; bilo koja dva bloka se sijeku u 0 ili 4 točke
$\mathcal{G}_1$ - graf čiji su vrhovi blokovi dizajna $\mathcal{S}_1$, pri čemu su dva vrha susjedna akko odgovarajući blokovi u presjeku imaju 4 točke
$\mathcal{G}_1$ je jedinstven jako regularan graf s parametrima $(66, 20, 10, 4)$, odnosno triangularan graf $\binom{12}{2}$ kojemu je grupa automorfizama simetrična grupa $S_{12}$

$\mathcal{S}_2$ - dizajn nositelj koda $C_1$ za $w = 16$
$\mathcal{S}_2$ ima 495 blokova; bilo koja dva bloka se sijeku u 0, 4, 8 ili 12 točaka
$\mathcal{G}_2$ - graf čiji su vrhovi blokovi dizajna $\mathcal{S}_2$, pri čemu su dva vrha susjedna akko odgovarajući blokovi u presjeku imaju 0 ili 8 točaka
$\mathcal{G}_2$ je jedinstven jako regularan graf s parametrima $(495, 238, 109, 119)$ kojemu je grupa automorfizama ortogonalna grupa $O^-_{10}(2)$.

$\mathcal{S}_3$ - dizajn nositelj koda $C_3$ za $w = 12$
$\mathcal{S}_3$ ima 66 blokova; bilo koja dva bloka se sijeku u 2,4 ili 6 točaka
Graf čiji su vrhovi blokovi dizajna $\mathcal{S}_3$, pri čemu su dva vrha susjedna akko odgovarajući blokovi u presjeku imaju 6 točaka, je izomorfan grafu $\mathcal{G}_1$

Iz dizajna nositelja kodova $C_4$, $C_7$ i $C_8$ za minimalne težine mogu se konstruirati jako regularni grafovi izomorfni grafu $\mathcal{G}_1$.

$\mathcal{S}_4$ - dizajn nositelj koda $C_{11}$ za $w = 8$
$\mathcal{S}_4$ ima 66 blokova; bilo koja dva bloka se sijeku u 0 ili 4 točke
Graf čiji su vrhovi blokovi dizajna $\mathcal{S}_4$, pri čemu su dva vrha susjedna akko odgovarajući blokovi u presjeku imaju 4 točke, je izomorfan grafu $\mathcal{G}_1$

$\mathcal{S}_5$ - dizajn nositelj koda $C_{11}$ za $w = 16$
$\mathcal{S}_5$ ima 495 blokova; bilo koja dva bloka se sijeku u 0, 4, 8 ili 12 točaka
Graf čiji su vrhovi blokovi dizajna $\mathcal{S}_5$, pri čemu su dva vrha susjedna akko odgovarajući blokovi u presjeku imaju 0 ili 8 točaka, je izomorfan grafu $\mathcal{G}_2$

$\mathcal{S}_6$ - dizajn nositelj koda $C_{12}$ za $w = 4$
$\mathcal{S}_6$ ima 276 blokova; bilo koja dva bloka se sijeku u 0 ili 2 točke
$\mathcal{G}_3$ - graf čiji su vrhovi blokovi dizajna $\mathcal{S}_6$, pri čemu su dva vrha susjedna akko odgovarajući blokovi u presjeku imaju 2 točke
$\mathcal{G}_3$ je jako regularan graf s parametrima $(276, 44, 22, 4)$, odnosno triangularan graf $\binom{24}{2}$ kojemu je grupa automorfizama simetrična grupa $S_{24}$

$\mathcal{S}_7$ - dizajn nositelj koda $C_{14}$ za $w = 12$
$\mathcal{S}_7$ ima 77 blokova; bilo koja dva bloka se sijeku u 0 ili 4 točke
$\mathcal{G}_4$ - graf čiji su vrhovi blokovi dizajna $\mathcal{S}_7$, pri čemu su dva vrha susjedna akko su odgovarajući blokovi disjunktni
$\mathcal{G}_4$ je jedinstven jako regularan graf s parametrima $(77, 16, 0, 4)$, kojemu je grupa automorfizama grupa $Aut(M_{22}) \cong M_{22} : Z_2$

$\mathcal{S}_8$ - dizajn nositelj koda $C_{15}$ za $w = 4$
$\mathcal{S}_8$ ima 78 blokova; bilo koja dva bloka se sijeku u 0 ili 2 točke
$\mathcal{G}_5$ - graf čiji su vrhovi blokovi dizajna $\mathcal{S}_8$, pri čemu su dva vrha susjedna akko odgovarajući blokovi u presjeku imaju 2 točke
$\mathcal{G}_5$ je jako regularan graf s parametrima $(78, 22, 11, 4)$, odnosno triangularan graf $\binom{13}{2}$ kojemu je grupa automorfizama simetrična grupa $S_{13}$