Samoortogonalni kodovi iz simetričnih dizajna

Loredana Simčić
(loredana.simcic@riteh.hr)

- **Masaaki Harada, Vladimir D. Tonchev**: Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms, Discrete Math. 264 (2003) 81-90.

Linearni kodovi

Definicija

Neka je q prim broj i neka je F_q konačno polje reda q, te neka je $n \in \mathbb{N}$. Linearan kod duljine n je linearni podprostor vektorskog prostora F_q^n.

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

Primjer

$$C = \{0000, 1010, 2020, 0122, 1102, 2201, 0211, 1221, 2112\} \subset F_3^4$$

Hammingova udaljenost

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

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

se naziva Hammingova udaljenost.

Težina riječi koda

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

$$w(x) = d(x, 0) = |\{i \in \mathbb{N} |\, i \leq n,\ x_i \neq 0\}|$$

Linearni kod C duljine n se naziva $[n, k, d]$ kod ako je k dimenzija od C i $d = \min\{w(c) |\, c \in C,\ c \neq 0\}$ je minimalna težina od C.

Optimalan kod

Linearni $[n, k, d]$ kod je optimalan ako je d najveća moguća minimalna težina za bilo koji $[n, k]$ kod nad odgovarajućim poljem.

Težinski enumerator

Težinski enumerator koda C je polinom

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

gdje je A_i broj riječi koda težine i.

Primjer

$$C = \{0000, 1010, 2020, 0122, 1102, 2201, 0211, 1221, 2112\} \subset F_3^4$$

$$A(x) = 2x^4 + 4x^3 + 2x^2 + 1$$

Generirajuća matrica linearnog koda

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

Primjer

$$C = \{0000,\ 1010,\ 2020,\ 0122,\ 1102, 2201,\ 0211,\ 1221,\ 2112\} \subset F_3^4$$

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 \end{bmatrix}$$

C je $[4, 2, 2]$ kod nad F_3.

Ekvivalentni kodovi

Dva koda iste duljine i nad istim poljem su ekvivalentna ako se jedan može dobiti iz drugoga permutacijom koordinata u svim riječima koda i množenjem koordinatne pozicije sa ne-nul elementom polja.

Primjer

Kodovi nad F_5 s generirajućim matricama

$$G_1 = \begin{bmatrix} 0 & 0 & 1 & 2 & 1 \\ 0 & 1 & 0 & 3 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} \quad G_2 = \begin{bmatrix} 1 & 0 & 4 & 1 & 0 \\ 1 & 1 & 0 & 4 & 0 \\ 1 & 0 & 4 & 0 & 1 \end{bmatrix}$$

Izomorfni kodovi

Dva koda iste duljine i nad istim poljem su izomorfna ako se jedan može dobiti iz drugoga permutacijom koordinata u svim riječima koda.

Dualni kod

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

$$C^\perp = \{x \in F_q^n \mid (\forall y \in C)\, x \cdot y = 0\}$$

Ako je C $[n, k]$ kod, tada je $C^\perp$ $[n, n-k]$ kod.

Za $[n, k]$ kod C se kaže da je samoortogonalan ako je $C \subset C^\perp$, a samodualan ako je $C = C^\perp$.

Primjer dualnog koda (nad F_3)

$$C = \begin{Bmatrix} 0000 \\ 1010 \\ 2020 \\ 0122 \\ 1102 \\ 2201 \\ 0211 \\ 1221 \\ 2112 \end{Bmatrix} \qquad C^{\perp} = \begin{Bmatrix} 0000 \\ 0101 \\ 0202 \\ 1220 \\ 2012 \\ 2110 \\ 1021 \\ 1122 \\ 2211 \end{Bmatrix}$$

Primjer samoortogonalnog koda

Kod s generirajućom matricom $G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 2 & 0 \end{bmatrix}$ nad F_3.

Dizajni

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 λ 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 je ukupni broj blokova jednak $b = \frac{\lambda v(v-1)}{k(k-1)}$ i svaka je točka incidentna s točno $r = \frac{\lambda(v-1)}{k-1}$ blokova.

Dizajn je simetričan ako je $v = b$, ili ekvivalentno $k = r$.

Matrica incidencije dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ je $v \times b$ matrica $A = (a_{ij})$

$$a_{ij} = \begin{cases} 1, & (x_i, B_j) \in \mathcal{I} \\ 0, & (x_i, B_j) \notin \mathcal{I} \end{cases}$$

Komplementaran dizajn se dobije zamjenom svih blokova njihovim komplementima.

Dva dizajna su izomorfna ako se matrica incidencije jednog dizajna može dobiti iz matrice incidencije drugog permutacijom redaka i stupaca.

Automorfizam dizajna je izomorfizam dizajna sa samim sobom, tj. permutacija točaka koja permutira i blokove.

Djelovanje grupe na skup

Grupa G djeluje na konačan skup Ω ako postoji preslikavanje $f : G \times \Omega \to \Omega$ takvo da vrijedi

1. $f(g_1, f(g_2, x)) = f(g_1 g_2, x),\ \forall x \in \Omega,\ \forall g_1,\ g_2 \in G,$
2. $f(1, x) = x,\ \forall x \in \Omega.$

Slika djelovanja elementa $g \in G$ na element $x \in \Omega$ označava se $g.x$ ili x^g.

Skup $G_x = \{g \in G \mid g.x = x\} \leq G$ naziva se **stabilizator** elementa x za djelovanje grupe G.

Na skupu Ω na kojeg djeluje grupa G može se definirati relacija

$$x \sim y \Leftrightarrow (\exists g \in G) \text{ t.d. } g.x = y.$$

Relacija $\sim$ je relacija ekvivalencije na skupu Ω.

Klasa ekvivalencije elementa x s obzirom na relaciju $\sim$,
$G.x = \{g.x \mid g \in G\}$, naziva se orbita elementa x za djelovanje grupe G.

Teorem

Ako grupa G djeluje na skup Ω, tada je za $x \in \Omega$

$$|G.x| = [G : G_x]$$

Metoda konstrukcije samoortogonalnih kodova

Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn sa automorfizmom Φ reda p, gdje je p prim broj, koji ne fiksira niti jednu točku i niti jedan blok dizajna.

Tada je matrica incidencije dizajna $\mathcal{D}$ blok matrica oblika

$$A = \begin{bmatrix} A_{1,1} & \cdots & A_{1,b/p} \\ \vdots & & \vdots \\ A_{v/p,1} & \cdots & A_{v/p,b/p} \end{bmatrix},$$

gdje je $A_{i,j}$ kvadratna cirkularna matrica reda p kojoj su retci indeksirani točkama u i-toj orbiti točaka pod djelovanjem cikličke grupe $\langle\Phi\rangle$, i stupci indeksirani blokovima u j-toj orbiti blokova.

Primjer. 2-(9,3,2) dizajn

Točke:

$$\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Blokovi:

1. $\{1, 2, 3\}$	9. $\{2, 3, 6\}$	17. $\{3, 5, 9\}$
2. $\{1, 2, 4\}$	10. $\{2, 4, 5\}$	18. $\{3, 6, 7\}$
3. $\{1, 3, 5\}$	11. $\{2, 5, 7\}$	19. $\{3, 7, 8\}$
4. $\{1, 4, 6\}$	12. $\{2, 6, 9\}$	20. $\{4, 5, 8\}$
5. $\{1, 5, 7\}$	13. $\{2, 7, 8\}$	21. $\{4, 6, 7\}$
6. $\{1, 6, 8\}$	14. $\{2, 8, 9\}$	22. $\{4, 7, 9\}$
7. $\{1, 7, 9\}$	15. $\{3, 4, 8\}$	23. $\{5, 6, 8\}$
8. $\{1, 8, 9\}$	16. $\{3, 4, 9\}$	24. $\{5, 6, 9\}$

Automorfizam reda 3:

$$\Phi = (1, 3, 8)(2, 4, 9)(5, 7, 6)$$

Primjer-nastavak

$$\Phi = (1,3,8)(2,4,9)(5,7,6)$$

Orbite točaka pod djelovanjem grupe $\langle\Phi\rangle$:

$\{1,3,8\}$
$\{2,4,9\}$
$\{5,7,6\}$

Orbite blokova pod djelovanjem grupe $\langle\Phi\rangle$:

$\{1,15,8\}$
$\{2,16,14\}$
$\{3,19,6\}$
$\{4,17,13\}$
$\{5,18,23\}$
$\{7,9,20\}$
$\{10,22,12\}$
$\{11,21,24\}$

Primjer-nastavak

1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	1	0	0	0	0	0	1	1	1	1	1	0	0	0	0	0
0	1	0	1	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0	1	1	1	0	0
0	0	1	0	1	0	0	0	0	1	1	0	0	0	0	0	1	0	0	1	0	0	1	1
0	0	0	1	0	1	0	0	1	0	0	1	0	0	0	0	0	1	0	0	1	0	1	1
0	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	0	1	1	0	1	1	0	0
0	0	0	0	0	1	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	1	0
0	0	0	0	0	0	1	1	0	0	0	1	0	1	0	1	1	0	0	0	0	1	0	1

Primjer-nastavak

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.	19.	20.	21.	22.	23.	24.
1.	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.	1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0
3.	1	0	1	0	0	0	0	0	1	0	0	0	0	0	1	1	1	1	1	0	0	0	0	0
4.	0	1	0	1	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0	1	1	1	0	0
5.	0	0	1	0	1	0	0	0	0	1	1	0	0	0	0	0	1	0	0	1	0	0	1	1
6.	0	0	0	1	0	1	0	0	1	0	0	1	0	0	0	0	0	1	0	0	1	0	1	1
7.	0	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	0	1	1	0	1	1	0	0
8.	0	0	0	0	0	1	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	1	0
9.	0	0	0	0	0	0	1	1	0	0	0	1	0	1	0	1	1	0	0	0	0	1	0	1

Primjer-nastavak

	1.	15.	8.	2.	16.	14.	3.	19.	6.	4.	17.	13.	5.	18.	23.	7.	9.	20.	10.	22.	12.	11.	21.	24.
1.	1	0	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0
3.	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0
8.	0	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0
2.	1	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	1	0	1	0	1	1	0	0
4.	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0	1	0
9.	0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1	1	0	0	1
5.	0	0	0	0	0	0	1	0	0	0	1	0	1	0	1	0	0	1	1	0	0	1	0	1
7.	0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	1	0	0	0	1	0	1	1	0
6.	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	0	0	0	1	0	1	1

Primjer-nastavak

1	0	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0
1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0
0	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0
1	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	1	0	1	0	1	1	0	0
0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0	1	0
0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1	1	0	0	1
0	0	0	0	0	0	1	0	0	0	1	0	1	0	1	0	0	1	1	0	0	1	0	1
0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	1	0	0	0	1	0	1	1	0
0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	0	0	0	1	0	1	1

Orbitna matrica

Matrica dimenzija $(v/p) \times (b/p)$

$$M = \begin{bmatrix} m_{1,1} & \cdots & m_{1,b/p} \\ \vdots & & \vdots \\ m_{v/p,1} & \cdots & m_{v/p,b/p} \end{bmatrix},$$

gdje je $m_{i,j}$ broj jedinica u retku od $A_{i,j}$ se naziva orbitna matrica od $\mathcal{D}$ s obzirom na Φ.

Primjer-nastavak

1	0	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0
1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0
0	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0
1	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	1	0	1	0	1	1	0	0
0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0	1	0
0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1	1	0	0	1
0	0	0	0	0	0	1	0	0	0	1	0	1	0	0	1	1	0	0	0	1	1	0	1
0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	1	0	0	0	1	0	1	1	0
0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	0	0	0	1	0	1	1

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

Propozicija 1.

Neka je $\mathcal{D}$ $2-(v,k,\lambda)$ dizajn sa automorfizmom Φ reda p, gdje je p prim broj, bez fiksnih točaka i blokova. Neka su matrice A i M kao što je opisano ranije. Ako je q prim broj koji dijeli r i λ, tada orbitna matrica M generira samoortogonalni kod duljine b/p nad F_q.

Primjer-nastavak

Iz $2-(9,3,2)$ dizajna dobijemo samoortogonalni $[8,3,4]$ kod nad F_2 s generirajućom matricom

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

i težinskim enumeratorom

$$A(x) = 1 + 6x^4 + x^8$$

Rezultati.
Samoortogonalni kodovi nad F_7 iz $2-(24,17,7)$ dizajna

- **K. Mackenzie-Fleming, K.W. Smith**: (27,13,6) designs with an automorphism of order 3, J.Combin. Math. Combin.Comput. 22 (1996) 241-253

Postoji točno 22 neizomorfnih simetričnih $2-(27,13,6)$ dizajna sa automorfizmom reda 3 bez fiksnih točaka.

Iz 22 dizajna dobiju se četiri neekvivalentne orbitne matrice, označimo ih sa A_1, A_2, A_3 i A_4.

Komplementaran dizajn $2-(27,13,6)$ dizajna s automorfizmom reda 3 bez fiksnih točaka i orbitnom matricom A_i je $2-(27,14,7)$ dizajn s automorfizmom reda 3 bez fiksnih točaka i orbitnom matricom $3J-A_i$.

Koristeći Propoziciju 1., iz orbitnih matrica $3J-A_1$, $3J-A_2$, $3J-A_3$ i $3J-A_4$ dobiveni su $[9,4]$ samoortogonalni kodovi nad F_7 s težinskim enumeratorima

$$A_1(x) = 1+12x^3+36x^5+246x^6+594x^7+936x^8+576x^9,$$
$$A_2(x) = 1+72x^5+258x^6+522x^7+972x^8+576x^9,$$
$$A_3(x) = 1+54x^5+288x^6+540x^7+918x^8+600x^9,$$
$$A_4(x) = 1+18x^3+270x^6+648x^7+864x^8+600x^9$$

Propozicija 2.

Samoortogonalni $[9,4]$ kodovi nad F_7 dobiveni iz 22 neizomorfna simetrična $2-(27,14,7)$ dizajna s automorfizmom reda 3 bez fiksnih točaka su podijeljeni u četiri klase ekvivalencije. Dva od njih su optimalni kodovi.

Samoortogonalni kodovi nad F_3 iz $2-(40,27,18)$ dizajna

- **V. Ćepulić**: On symmetric block designs (40,13,4) with automorphisms of order 5, Discrete Math. 128 (1994) 45-60.

Postoji 13 neizomorfnih simetričnih $2-(40,13,4)$ dizajna sa automorfizmom reda 5 bez fiksnih točaka.

Tih je 13 dizajna dobiveno iz tri orbitne matrice, označimo ih sa A_1, A_2 i A_3.

Komplementaran dizajn $2-(40,13,4)$ dizajna s automorfizmom reda 5 bez fiksnih točaka i orbitnom matricom A_i je $2-(40,27,18)$ dizajn s automorfizmom reda 5 bez fiksnih točaka i orbitnom matricom $5J-A_i$.

Koristeći Propoziciju 1., iz orbitnih matrica $5J - A_1$, $5J - A_2$ i $5J - A_3$ dobiveni su kodovi nad F_3:

C_1 i C_2

-parametri: $[8, 2, 6]$ (optimalni samoortogonalni kodovi)
-težinskim enumerator: $1 + 8x^6$
-generirajuće matrice:

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 & 2 & 2 & 1 & 1 \end{bmatrix} \text{ i } G_2 = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 1 & 2 & 1 & 0 & 2 \end{bmatrix}$$

C_3

-parametri: $[8, 3, 3]$
-težinskim enumerator: $1 + 4x^3 + 22x^6$
-generirajuća matrica:

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Samoortogonalni kodovi nad F_3 iz $2-(45,12,3)$ dizajna

- **V. Ćepulić**: On symmetric block designs (45,12,3) with automorphisms of order 5, Ars Combin. 37 (1994) 33-48.

Postoji 13 neizomorfnih simetričnih $2-(45,12,3)$ dizajna sa automorfizmom reda 5 bez fiksnih točaka.

Tih je 13 dizajna dobiveno iz jedanaest orbitnih matrica, označimo ih sa $A_1, \ldots, A_{11}$.

Koristeći Propoziciju 1., iz orbitnih matrica $A_1, \ldots, A_{11}$ dobiveni su kodovi $C_1, \ldots, C_{11}$ nad F_3:

Kod	Parametri	Težinski enumerator
C_1	$[9,1,9]$	$1+2x^9$
C_2	$[9,2,3]$	$1+2x^3+2x^6+4x^9$
C_3, C_{11}	$[9,2,6]$	$1+6x^6+2x^9$
C_4	$[9,3,3]$	$1+2x^3+20x^6+4x^9$
$C_5, C_7, C_8, C_9, C_{10}$	$[9,4,3]$	$1+6x^3+66x^6+8x^9$
C_6	$[9,3,6]$	$1+24x^6+2x^9$

Propozicija 3.

Ternarni samoortogonalni kodovi dobiveni iz 13 neizomorfnih simetričnih $2-(45,12,3)$ dizajna s automorfizmom reda 5 bez fiksnih točaka su podijeljeni u šest klasa ekvivalencije.

Ternarni $[63, 20, 21]$ kod

- **Z. Janko**: The existance of symmetric designs with parameters (189,48,12), J.Combin. Theory Ser. A 80 (1997) 334-338.

Postoji simetričan $2-(189, 48, 12)$ dizajn s automorfizmom reda 3 bez fiksnih točaka.

Njegova orbitna matrica generira samoortogonalan ternarni $[63, 20, 21]$ kod čija je težinski enumerator

$$\begin{aligned} A(x) =& 1 + 942x^{21} + 24766x^{24} + 594832x^{27} + 8443890x^{30} + 67603172x^{33} + \\ &+ 307398672x^{36} + 787009356x^{39} + 1110234948x^{42} + 832430718x^{45} + \\ &+ 314109012x^{48} + 54952604x^{51} + 3893639x^{54} + 87066x^{57} + 784x^{60}. \end{aligned}$$

- $[63, 20]$ kod s najvećom dosad poznatom minimalnom težinom.
- Ima podkodove koji su ternarni $[63, 19, 21]$ kodovi.

Kodovi iz cikličkih diferencijskih skupova

Diferencijski skup

Neka je G grupa reda v. (v, k, λ) diferencijski skup u G je podskup $D \subset G$ sa sljedećim svojstvima:

1. $|D| = k$
2. $\forall g \in G$, $g \neq 1$, postoji točno λ uređenih parova $(x, y) \in D \times D$ takvih da je $xy^{-1} = g$

Diferencijski skup je abelov (neabelov, ciklički) ako je grupa abelova (neabelova, ciklička).

Ako grupa G ima diferencijski skup D tada je skup $\{g.D | \, g \in G\}$ skup blokova simetričnog (v, k, λ) dizajna sa skupom točaka G.

Iz diferencijskih skupova danih u

- **L.D. Baumert**: Cyclic difference sets, Springer, Berlin, 1971.

dobiju se simetrični dizajni s parametrima $(156, 31, 6)$, $(400, 57, 28)$ i $(820, 91, 10)$.

Iz njihovih komplementarnih dizajna, odnosno simetričnih dizajna s parametrima $(156, 125, 100)$, $(400, 343, 294)$ i $(820, 729, 648)$, dobiveni su sljedeći kodovi:

$[78, 16, 38]$ kod nad F_5 ($[78, 16]$ kod s najvećom poznatom minimalnom težinom)

$[52, 9, 28]$ kod nad F_5

$[164, 16, 84]$ kod nad F_3 ($[164, 16]$ kod s najvećom poznatom minimalnom težinom)

$[80, 16, 42]$ kod nad F_7

- **K.W. Smith**: Non-Abelian Hadamard difference sets, J. Combin. Theory Ser. A 70 (1995) 145-156.

Nađen ne-Abelov $(100, 45, 20)$ diferencijski skup.

Kod iz njegove orbitne matrice za automorfizam reda 5 bez fiksnih točaka je $[20, 4, 14]$ kod nad F_5. Kod je optimalan.

Težinski enumerator:

$$A(x) = 1 + 120x^{14} + 96x^{15} + 300x^{16} + 80x^{19} + 28x^{20}$$

- **Vladimir D. Tonchev**: Hadamard matrices of order 28 with automorphisms of order 7, J. Combin. Theory Ser A 40 (1985) 62-81.