Kvazisimetrični dizajni

V. Krčadinac, 2016./2017., 30 sati.

Dizajn s parametrima t-(v, k, λ) je skup od v točaka s familijom k-članih podskupova koje nazivamo blokovima, takvom da je svaki t-člani skup točaka sadržan u λ blokova. Dizajn nazivamo kvazisimetričnim ako se svaka dva bloka sijeku u x ili u y točaka, za neke konstante $x < y$. Riječ je o generalizaciji simetričnih dizajna, kod kojih je veličina presjeka blokova konstantna i jednaka λ.

Kvazisimetrični dizajni povezani su s drugim kombinatoričkim strukturama, poput jako regularnih grafova i samoortogonalnih kodova. Poznati su mnogi netrivijalni uvjeti na parametre i zanimljive konstrukcije beskonačnih serija i sporadičnih primjera kvazisimetričnih dizajna. Cilj ovog kolegija je dati kratak pregled rezultata i otvorenih problema o kvazisimetričnim dizajnima, služeći se monografijom [1] i novijim preglednim radom [2]. Poseban naglasak bit će stavljen na veze s drugim dijelovima kombinatorike.

Polaganje ispita predviđa se kroz individualne projektne zadatke koji se mogu izložiti usmeno na znanstvenom seminaru ili u obliku pisanog rada.

Literatura

1. M.S. Shrikhande, S.S. Sane, *Quasi-symmetric designs*, Cambridge University Press, 1991.

2. M.S. Shrikhande, *Quasi-symmetric designs*, u: *The Handbook of Combinatorial Designs, Second Edition* (urednici C.J. Colbourn i J.H. Dinitz), CRC Press, 2007., str. 578–582.

Quasi-symmetric designs

V. Krčadinac, 2016/2017, 30 hours.

A t-(v,k,λ) design is a set of v elements called points together with a family of k-element subsets called blocks such that any t-subset of points is contained in λ blocks. A design is called quasi-symmetric if any pair of blocks intersect in x or in y points, for non-negative integers $x < y$. The concept is a generalization of symmetric designs, which have block intersections of constant size, equal to λ.

Quasi-symmetric designs have important connections to other combinatorial structures, such as strongly regular graphs and self-orthogonal codes. Many non-trivial conditions on the parameters are known, as well as interesting constructions of infinite series and sporadic examples of quasi-symmetric designs. The goal of this course is to give a short overview of known results and open problems about quasi-symmetric designs. The monograph [1] and the survey paper [2] will be used. Emphasis will be put on connections with other parts of combinatorics.

The exam will be based on individual project assignments, that can be presented as scientific seminars or as written essays.

Bibliography

1. M.S. Shrikhande, S.S. Sane, *Quasi-symmetric designs*, Cambridge University Press, 1991.

2. M.S. Shrikhande, *Quasi-symmetric designs*, in: *The Handbook of Combinatorial Designs, Second Edition* (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, 2007, pp. 578–582.

Sadržaj

Verzija 11, 4.4.2017.

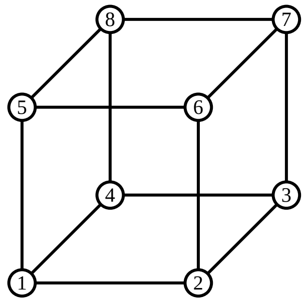
1 Dizajni

1.1 t-dizajni

Definicija 1.1. *Neka su $0 \leq t \leq k \leq v$ i $\lambda > 0$ cijeli brojevi.* Dizajn *s parametrima t-(v, k, λ) je konačna incidencijska struktura $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ sa svojstvima:*

1. *Broj točaka je $|\mathcal{P}| = v$.*
2. *Svaki blok $B \in \mathcal{B}$ je incidentan s k točaka.*
3. *Za svaki t-člani skup točaka $T \subseteq \mathcal{P}$ postoji točno λ blokova $B \in \mathcal{B}$ incidentnih s točkama iz T.*

Primjer 1.2. *Za točke dizajna uzmimo vrhove kocke $\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7, 8\}$:*



Blokove čine četveročlani podskupovi točaka dvije vrste. Osam blokova sastoji se od vrha kocke i tri njemu susjedna vrha: $\mathcal{B}_1 = \{\{1, 2, 4, 5\}, \{1, 2, 3, 6\}, \{2, 3, 4, 7\}, \{1, 3, 4, 8\}, \{1, 5, 6, 8\}, \{2, 5, 6, 7\}, \{3, 6, 7, 8\}, \{4, 5, 7, 8\}\}$. Još šest blokova dobivamo od po dva nasuprotna brida kocke: $\mathcal{B}_2 = \{\{1, 2, 7, 8\}, \{3, 4, 5, 6\}, \{2, 3, 5, 8\}, \{1, 4, 6, 7\}, \{1, 3, 5, 7\}, \{2, 4, 6, 8\}\}$. Incidencijska struktura $(\mathcal{P}, \mathcal{B}_1 \cup \mathcal{B}_2, \in)$ je dizajn s parametrima 3-(8, 4, 1).

Propozicija 1.3. *Svaki t-(v, k, λ) dizajn ujedno je i s-(v, k, λ_s) dizajn za sve $s \in \{0, \ldots, t\}$, pri čemu je*

$$\lambda_s = \lambda \cdot \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}.$$

Dokaz. Neka je $S \subseteq \mathcal{P}$ bilo koji s-člani skup točaka. Označimo s $\lambda(S)$ broj blokova koji sadrže S. Dvostrukim prebrojavanjem parova u skupu $\{(T, B) \mid S \subseteq T \subseteq B,\ |T| = t,\ B \in \mathcal{B}\}$ dobivamo jednakost $\binom{v-s}{t-s} \cdot \lambda = \lambda(S) \cdot \binom{k-s}{t-s}$. Slijedi da $\lambda(S)$ ne ovisi o izboru skupa S, nego samo o njegovoj kardinalnosti s i možemo ga izraziti kao u iskazu propozicije. $\square$

Prethodnu propoziciju dokazali smo metodom dvostrukog prebrojavanja. Ukupan broj blokova dizajna je $b = \lambda_0 = \lambda\binom{v}{t}/\binom{k}{t}$. Broj blokova kroz bilo koju točku je $r = \lambda_1 = \lambda\binom{v-1}{t-1}/\binom{k-1}{t-1}$. Iz propozicije također slijede nužni uvjeti djeljivosti za postojanje dizajna:

Korolar 1.4. *Ako postoji t-(v, k, λ) dizajn, onda $\binom{k-s}{t-s}$ dijeli $\lambda \cdot \binom{v-s}{t-s}$, za svaki $s \in \{0, \dots, t\}$.*

Uvjet 3. iz definicije dizajna je tim jači što je parametar t veći. Postavlja se pitanje postoje li t-dizajni za proizvoljno velike t? Trivijalni primjer čini familija $\mathcal{B}$ svih k-članih podskupova od $\mathcal{P}$. To je t-$(v, k, \binom{v-t}{k-t})$ dizajn za sve $0 \leq t \leq k \leq v$. Ako je veličina blokova k veća ili jednaka od $v - t$, jedini primjeri dizajna su trivijalni:

Propozicija 1.5. *Neka je $\mathcal{D}$ dizajn s parametrima t-(v, k, λ) i neka vrijedi $v \leq k + t$. Tada je $\mathcal{D}$ trivijalni dizajn ili njegov višekratnik (tj. $\mathcal{B}$ sadrži svaki k-člani podskup od $\mathcal{P}$ ponovljen m puta, za neki $m \geq 1$).*

U dokazu koristimo komplementarnu strukturu $\overline{\mathcal{D}}$ kojoj su blokovi komplementi blokova od $\mathcal{D}$, $\overline{\mathcal{B}} = \{\mathcal{P} \setminus B \mid B \in \mathcal{B}\}$.

Propozicija 1.6. *Ako je $\mathcal{D}$ dizajn s parametrima t-(v, k, λ) i vrijedi $v \geq k+t$, onda je komplementarna struktura $\overline{\mathcal{D}}$ dizajn s parametrima t-$(v, k - t, \overline{\lambda})$ za*

$$\overline{\lambda} = \sum_{s=0}^{t} (-1)^s \binom{t}{s} \lambda_s.$$

Dokaz. Neka je $T \subseteq \mathcal{P}$ bilo koji t-člani skup točaka. Broj blokova od $\overline{\mathcal{D}}$ koji sadrže T jednak je broju blokova od $\mathcal{D}$ koji su disjunktni s T. Možemo ga izraziti preko parametara λ_s iz propozicije 1.3 s pomoću formule uključivanja-isključivanja. $\square$

Dokaz propozicije 1.5. Uvjet $v \leq k + t$ ekvivalentan je s $t \geq v - k$. Zbog propozicije 1.3 možemo pretpostaviti da je $t = v - k$. U tom slučaju komplementarna struktura $\overline{\mathcal{D}}$ je t-$(v, t, \overline{\lambda})$ dizajn i sastoji se od svakog t-članog podskupa od $\mathcal{P}$ ponovljenog $\overline{\lambda}$ puta. No tada se i $\mathcal{D}$ sastoji od svakog k-članog podskupa od $\mathcal{P}$ ponovljenog $\overline{\lambda}$ puta. $\square$

Rick Wilson [141] je dokazao postojanje netrivijalnih t-dizajna za proizvoljno velike t:

Teorem 1.7. *Za sve prirodne brojeve t, k, v koji zadovoljavaju $t < k < v - t$ postoji netrivijalni t-(v, k, λ) dizajn za neki λ.*

Dokaz koristi linearnu algebru nad poljem $\mathbb{Q}$ i nije kompliciran. Nalazi se u knjigama [40, prop. 16.2.1 na str. 260] i [128, tm. 9.8 na str. 204]. Najpoznatiji Wilsonov rezultat iz 70-tih godina [142] tiče se postojanja dizajna s $t = 2$. Dokazao je da su nužni uvjeti za postojanje 2-dizajna "asimptotički dovoljni": za svaki k i λ postoji konstanta C takva da 2-(v, k, λ) dizajni postoje čim je $v > C$ i zadovoljava uvjete djeljivosti.

Dizajni iz teorema 1.7 mogu imati ponovljene blokove. Znatno je teže dokazati postojanje t-dizajna koji su *jednostavni*, tj. nemaju ponovljenih blokova. Postojanje takvih dizajna za proizvoljno velike t dokazao je Luc Teirlinck [130] 1987. godine.

Teirlinckovi dizajni imaju $k = t + 1$ i broj točaka v je jako velik. Prije njegovog rada najveći t za koji je bio poznat dizajn je $t = 5$. Prve konstrukcije dizajna s $t > 5$ i malim v uspjele su u 90-tim godinama grupi matematičara sa sveučilišta Bayreuth u Njemačkoj [15]. Najveći t za koji su dobili dizajne je $t = 9$ [92].

Posebno je teško konstruirati dizajne s parametrom $\lambda = 1$. Takvi dizajni nazivaju se *Steinerovim* i parametri se nekad zapisuju kao $S(t, k, v)$. Najpoznatiji primjeri su tzv. mali i veliki *Wittov dizajn* s parametrima 5-$(12, 6, 1)$ i 5-$(24, 8, 1)$. Sve do nedavno nije bilo poznato postoje li Steinerovi dizajni s $t > 5$. Peteru Keevashu [83] uspjelo je 2015. godine proširiti Wilsonovu asimptotičku teoriju na dizajne s $t > 2$: za dovoljno velike v, nužni uvjeti za postojanje ujedno su dovoljni. Iz toga slijedi postojanje Steinerovih t-dizajna s proizvoljno velikim t, ali dokaz nije konstruktivan. Još uvijek nisu konstruirani $S(t, k, v)$ dizajni za $t > 5$.

1.2 Simetrični i kvazisimetrični dizajni

Zbog uvjeta djeljivosti iz korolara 1.4 ne postoje 2-$(8, 3, 1)$ dizajni (imali bi $r = \frac{7}{2}$) i 2-$(11, 3, 1)$ dizajni (imali bi $b = \frac{55}{3}$). Parametri 2-$(16, 6, 1)$ zadovoljavaju uvjete djeljivosti ($r = 3$, $b = 8$), ali dizajni s tim parametrima ipak ne postoje zbog sljedećeg teorema.

Teorem 1.8 (Fisherova nejednakost)**.** *Ako postoji t-(v, k, λ) dizajn s $t \geq 2$ i $v \geq k + 1$, onda je $b \geq v$ (broj blokova ne može biti manji od broja točaka).*

Teorem dokazujemo linearnoalgebarskom metodom: elemente konačnog skupa S uložimo u vektorski prostor V (tj. definiramo injekciju $f : S \to V$). Ako je slika $f(S)$ linearno nezavisan skup, kardinalni broj od S ne može biti veći od dimenzije prostora ($|S| \leq \dim V$). Dualno, ako je $f(S)$ skup izvodnica za V, slijedi $|S| \geq \dim V$.

Dokaz. Zbog propozicije 1.3 možemo pretpostaviti da je $t = 2$. Označimo točke i blokove s $\mathcal{P} = \{P_1, \ldots, P_v\}$ i $\mathcal{B} = \{B_1, \ldots, B_b\}$. Točkama dizajna pridružimo incidencijske vektore $P_i \mapsto a_i = (a_{i1}, \ldots, a_{ib}) \in \mathbb{R}^b$ (retke incidencijske matrice $A = [a_{ij}]$), gdje je

$$a_{ij} = \begin{cases} 1, & \text{ako je } P_i \in B_j, \\ 0, & \text{inače.} \end{cases}$$

Pokazat ćemo da je skup $\{a_1, \ldots, a_v\} \subseteq \mathbb{R}^b$ linearno nezavisan, iz čega slijedi $v \leq b$. Pretpostavimo da je $\alpha_1 a_1 + \ldots + \alpha_v a_v = 0$ i pomnožimo jednakost skalarno sa samom sobom. Zbog svojstva da kroz svaku točku prolazi r blokova vrijedi $a_i \cdot a_i = r$, a zbog svojstva da kroz svake dvije točke prolazi λ blokova vrijedi $a_i \cdot a_j = \lambda$ za $i \neq j$. Slijedi $0 = \sum_{i=1}^{v} r\alpha_i^2 + \sum_{i \neq j} \lambda \alpha_i \alpha_j = (r - \lambda) \sum_{i=1}^{v} \alpha_i^2 + \lambda \left(\sum_{i=1}^{v} \alpha_i\right)^2$. Vidimo da obje sume moraju biti 0, posebno $\alpha_1 = \ldots = \alpha_v = 0$. □

Dualni dokaz, u kojem se pokazuje da stupci incidencijske matrice čine skup izvodnica za $\mathbb{R}^v$, nalazi se u [128, tm. 1.33 na str. 16]. Posebno su važni dizajni koji dostižu Fisherovu nejednakost.

Definicija 1.9. *Za dizajn koji ima jednako mnogo točaka i blokova kažemo da je* simetričan.

Uvjet $v = b$ očito je ekvivalentan s $r = k$, a ekvivalentan je i sljedećim uvjetima na presjeke blokova.

Teorem 1.10. *Za t-(v, k, λ) dizajn s $t \geq 2$ i $v \geq k + 1$ ekvivalentno je:*

1. *$v = b$,*
2. *svaka dva bloka sijeku se u $\lambda_2 = \lambda \binom{v-2}{t-2} / \binom{k-2}{t-2}$ točaka,*
3. *svaka dva bloka sijeku se u x točaka, za neku konstantu x.*

Dokaz je ilustracija primjene matričnog računa u kombinatorici.

Dokaz. Radi jednostavnijih oznaka pretpostavimo opet da je $t = 2$. Prvo dokazujemo da iz $v = b$ slijedi druga tvrdnja. Incidencijska matrica dizajna zadovoljava $A \cdot A^\tau = (r - \lambda)I + \lambda J$ i $A \cdot J = rJ$, $J \cdot A = kJ$ (ovdje je I jedinična matrica, a J je matrica čiji su svi unosi 1). Zbog $v = b$ sve matrice su kvadratne i vrijedi $r = k$, a iz dokaza Fisherove nejednakosti tada slijedi da je A regularna. Množenjem jednakosti $A \cdot A^\tau = (k - \lambda)I + \lambda J$ s lijeva s A^{-1} i zdesna s A dobivamo $A^\tau \cdot A = (k - \lambda)I + \lambda J$, iz čega slijedi da se svaka dva bloka sijeku u λ točaka.

Iz druge tvrdnje očito slijedi treća, pa preostaje dokazati da treća tvrdnja implicira prvu. Treću tvrdnju matrično možemo iskazati kao $A^\tau \cdot A = (k -$

$x)I + xJ$. Za $x < k$ ta matrica je regularna ($x = k$ nije moguće zbog $v > k$), što znači da su stupci matrice A linearno nezavisni i vrijedi $b \le v$. Iz Fisherove nejednakosti tada slijedi $v = b$. $\square$

Simetričnim dizajnima posvećene su knjige [69, 91] i cjelina II.6 u *Handbook of combinatorial designs* [70]. Glavna tema ove skripte je šira klasa dizajna, koja se dobiva generalizacijom treće tvrdnje prethodnog teorema.

Definicija 1.11. *Za dizajn kažemo da je* kvazisimetričan *ako postoje brojevi $0 \le x < y \le k$ takvi da se svaka dva bloka sijeku u x ili u y točaka. Brojeve x i y nazivamo* presječnim brojevima.

Simetrični dizajn možemo smatrati kvazisimetričnim za $x = \lambda$ i proizvoljan y (drugi presječni broj se ne pojavljuje). Pravi primjer je višekratnik simetričnog dizajna, kod kojeg svaki blok ponovimo $m \ge 2$ puta. On ima presječne brojeve $x = \lambda$ i $y = k$. Nadalje, svaki Steinerov 2-dizajn (dizajn s parametrima $t = 2$ i $\lambda = 1$) je kvazisimetričan s presječnim brojevima $x = 0$, $y = 1$.

U prethodnoj cjelini vidjeli smo da netrivijalni dizajni postoje za proizvoljno velike parametre t. Nasuprot tome, netrivijalni simetrični dizajni postoje samo za $t = 2$. Prvi dokaz dao je vjerojatno Dembowski [50]. Tvrdnja je jednostavna posljedica sljedeće generalizacije Fisherove nejednakosti, najavljene u [118] i dokazane u [119].

Teorem 1.12 (Ray-Chaudhuri, Wilson)**.** *Neka postoji t-(v, k, λ) dizajn. Ako je $t = 2s$ paran i vrijedi $v \ge k+s$, onda je $b \ge \binom{v}{s}$. Ako je $t = 2s+1$ neparan i vrijedi $v-1 \ge k+s$, onda je $b \ge 2\binom{v-1}{s}$.*

Korolar 1.13. *Ako postoji netrivijalni simetrični t-(v, k, λ) dizajn, onda je $t = 2$.*

Dokaz. Iz Ray-Chaudhuri-Wilsonovih nejednakosti slijedi da netrivijalni dizajni s $t \ge 3$ moraju imati $b > v$. Trivijalni primjeri simetričnih dizajna su v-(v, v, v) i $(v-1)$-$(v, v-1, 1)$ dizajni. $\square$

Iz teorema 1.12 također slijedi da netrivijalni kvazisimetrični dizajni mogu postojati samo za $t \le 4$, što je ranije dokazao Peter Cameron [39]. Ray-Chaudhuri i Wilson [119] nejednakosti dokazuju linearnoalgebarskom metodom i karakteriziraju dizajne koji dostižu nejednakost za parne t. U idućoj cjelini proći ćemo njihove dokaze i objasniti posljedice za kvazisimetrične dizajne.

1.3 Napeti dizajni

Sljedeći teorem je generalizacija propozicija 1.3 i 1.6.

Teorem 1.14. *Neka je $\mathcal{D}$ t-(v,k,λ) dizajn i neka su $i,j\in\mathbb{N}_0$, $i+j\leq t$. Tada je za sve $I,J\subseteq\mathcal{P}$, $|I|=i$, $|J|=j$, $I\cap J=\emptyset$ broj blokova koji sadrže I i disjunktni su s J jednak*

$$\lambda_i^j=\lambda\cdot\frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}.$$

Dokaz. Prvo dokazujemo tvrdnju za $i=0$, tj. $I=\emptyset$. Primjenom formule uključivanja-isključivanja, isto kao u dokazu propozicije 1.6, slijedi $\lambda_0^j=\sum_{s=0}^{j}(-1)^s\binom{j}{s}\lambda_s$. Sada znamo da λ_0^j ne ovisi o izboru skupa J i možemo ga izraziti jednostavnije, bez sume. Dvostrukim prebrojavanjem parova $\{\,(J,B)\mid J\subseteq\mathcal{P},|J|=j,B\in\mathcal{B},J\cap B=\emptyset\}$ dobivamo $\binom{v}{j}\lambda_0^j=b\binom{v-k}{j}$. Iz $b=\lambda\frac{\binom{v}{t}}{\binom{k}{t}}$ slijedi $\lambda_0^j=\lambda\frac{\binom{v}{t}\binom{v-k}{j}}{\binom{k}{t}\binom{v}{j}}$, što se može dalje pojednostavniti do $\lambda_0^j=\lambda\frac{\binom{v-j}{k}}{\binom{v-t}{k-t}}$. Opća formula za $i\geq 0$ slijedi primjenom formule za λ_0^j na strukturu $\mathrm{der}_I\,\mathcal{D}=(\mathcal{P}\setminus I,\{\,B\setminus I\mid B\in\mathcal{B},I\subseteq B\})$. To je derivirani dizajn od $\mathcal{D}$ u točkama iz I i prema propoziciji 1.27 ima parametre $(t-i)$-$(v-i,k-i,\lambda)$. Slijedi $\lambda_i^j=\lambda\frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}$. □

Primijetimo da smo dobili jednostavniju formulu za parametar $\overline{\lambda}$ komplementarnog dizajna nego u propoziciji 1.6: $\overline{\lambda}=\lambda_0^t=\lambda\frac{\binom{v-t}{k}}{\binom{v-t}{k-t}}$. Također, prema propoziciji 1.3 je $\lambda_i=\lambda\frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$, a sad smo dobili $\lambda_i=\lambda_i^0=\lambda\frac{\binom{v-i}{k-i}}{\binom{v-t}{k-t}}$. Izjednačavanjem slijedi $\binom{v-i}{k-i}\binom{k-i}{t-i}=\binom{v-i}{t-i}\binom{v-t}{k-t}$. To se može dokazati direktno tako da uzmemo neki skup S kardinalnosti $|S|=v-i$ te na dva načina brojimo parove $\{\,(A,B)\mid B\subseteq A\subseteq S,|B|=t-i,|A|=k-i\}$.

Teorem 1.15. *Ako postoji t-(v,k,λ) dizajn s parnim $t=2s$ i ako vrijedi $v\geq k+s$, onda je broj blokova $b\geq\binom{v}{s}$. Štoviše, ako dizajn nije jednostavan, broj različitih blokova također ne može biti manji od $\binom{v}{s}$.*

Dokaz. Neka je X skup svih s-članih podskupova od $\mathcal{P}$. Skup svih funkcija $V(X)=\{f:X\to\mathbb{R}\}$ je realni vektorski prostor dimenzije $|X|=\binom{v}{s}$. Bazu čine indikatorske funkcije

$$f_{S_0}(S)=\begin{cases}1, & \text{ako je } S=S_0,\\ 0, & \text{inače.}\end{cases}$$

Bloku $B \in \mathcal{B}$ pridružimo funkciju $\widehat{B} = \sum_{S \subseteq B, |S|=s} f_S$ iz $V(X)$. Primijetimo da pridruživanje $B \mapsto \widehat{B}$ nije injekcija za dizajne s ponovljenim blokovima. No ako dokažemo da je $\{\widehat{B} \mid B \in \mathcal{B}\}$ skup izvodnica od $V(X)$, slijedi da je broj različitih blokova bar $\dim V(X) = \binom{v}{s}$, što teorem i tvrdi.

Dovoljno je pokazati da se proizvoljni element baze f_{S_0}, $S_0 \in X$ može prikazati kao linearna kombinacija funkcija $\widehat{B}$, $B \in \mathcal{B}$, odnosno njihovih linearnih kombinacija $F_r = \sum_{|B \cap S_0|=s-r} \widehat{B}$, za $r = 0, 1, \ldots, s$. Izrazimo prvo vektore F_r preko vektora $E_i = \sum_{S \in X, |S \cap S_0|=s-i} f_S$ (primijetimo da je $E_0 = f_{S_0}$). Za proizvoljan $S_1 \in X$ sa svojstvom $|S_1 \cap S_0| = s - i$, koeficijent uz f_{S_1} u izrazu za F_r je broj blokova $B \in \mathcal{B}$ takvih da je $S_1 \subseteq B$ i $|B \cap S_0| = s - r$. Možemo ga izraziti preko brojeva iz teorema 1.14 kao $\binom{i}{r}\lambda^r_{s+i-r}$ (izabiremo r-člani podskup $A \subseteq S_0 \setminus S_1$ i blok B koji sadrži $S_1 \cup (S_0 \setminus A)$ i disjunktan je s A). Zato je $F_r = \sum_{i=r}^{s} \binom{i}{r}\lambda^r_{s+i-r} E_i$, za $r = 0, 1, \ldots, s$. Ovo je trokutasti sustav, pa ga možemo "obrnuti" i izraziti E_i preko F_r. Pritom je bitno da su dijagonalni koeficijenti $\lambda^r_s \neq 0$, što vrijedi zbog pretpostavke $v \geq k+s$. Prema tome, i $E_0 = f_{S_0}$ može se izraziti kao linearna kombinacija F_r, $r = 0, 1, \ldots, s$, odnosno razapet je vektorima $\widehat{B}$, $B \in \mathcal{B}$. Ti vektori razapinju cijeli prostor $V(X)$ i time je teorem dokazan. □

Korolar 1.16. *Ako postoji t-(v, k, λ) dizajn s neparnim $t = 2s + 1$ i ako vrijedi $v - 1 \geq k + s$, onda je broj blokova $b \geq 2\binom{v-1}{s}$.*

Dokaz. Koristimo definiciju 1.26 i propoziciju 1.27. Za bilo koju točku $T_0 \in \mathcal{P}$ derivirani dizajn $\operatorname{der}_{T_0} \mathcal{D}$ ima parametre $(2s)$-$(v-1, k-1, \lambda)$. Vrijedi uvjet $v - 1 \geq k - 1 + s$, pa prema teoremu 1.15 njegov broj blokova b_1 zadovoljava $b_1 \geq \binom{v-1}{s}$. Rezidualni dizajn $\operatorname{res}_{P_0} \mathcal{D}$ ima parametre $(2s)$-$(v-1, k, \lambda^1_{2s})$ i njegov broj blokova b_2 zadovoljava $b_2 \geq \binom{v-1}{s}$. Broj blokova dizajna $\mathcal{D}$ je $b = b_1 + b_2$ i zadovoljava $b \geq 2\binom{v-1}{s}$. □

Ray-Chaudhuri i Wilson u članku [119] dokazuju i druge rezultate linearno-algebarskom metodom. Wilson kasnije dokazuje nejednakost iz teorema 1.15 i slične nejednakosti raznim drugim metodama. U članku [143] koristi matrične tehnike. U članku [144] koristi tzv. Mendelsohnove jednadžbe i metodu momenata. Konačno, u zajedničkom članku s Peterom Dukesom [54] koristi matricu inkluzija W_{tk} između svih t-članih i k-članih podskupova od $\mathcal{P}$. Poznato je da t-(v, k, λ) dizajni odgovaraju 0-1 rješenjima sustava linearnih jednadžbi $W_{tk} \cdot x = (\lambda, \ldots, \lambda)$ (to je tzv. Kramer-Mesnerov sustav). Ako dizajni postoje, konus generiran stupcima matrice W_{tk} sadrži konstantni vektor $(\lambda, \ldots, \lambda)$. S pomoću Farkaseve leme Dukes i Wilson dokazuju da određeni vektori ne pripadaju tom konusu i na taj način dobivaju nejednakosti za parametre dizajna, među kojima i generalizaciju Ray-Chaudhuri-Wilsonove nejednakosti.

Simetrični dizajni dostižu Fisherovu nejednakost, odnosno Ray-Chaudhuri-Wilsonovu nejednakost za $t = 2$. Karakterizira ih svojstvo da presjek blokova poprima samo jednu veličinu. Idući cilj je dokazati generalizaciju: dizajne koji dostižu Ray-Chaudhuri-Wilsonovu nejednakost za $t = 2s$ karakterizira svojstvo da presjek blokova poprima s različitih veličina.

Definicija 1.17. *Za t-(v, k, λ) dizajn s parnim $t = 2s$ i $v \geq k + s$ kažemo da je* napet *(eng.* tight*) ako mu je broj blokova $b = \binom{v}{s}$.*

Za sljedeći teorem nije bitna balansiranost (svojstvo 3. iz definicije 1.1).

Teorem 1.18. *Neka je $\mathcal{P}$ v-člani skup točaka i $\mathcal{B}$ familija k-članih podskupova od $\mathcal{P}$ takva da za svaka dva $B_1, B_2 \in \mathcal{B}$ vrijedi $|B_1 \cap B_2| \in \{\mu_1, \ldots, \mu_s\}$, pri čemu su $k > \mu_1 > \ldots > \mu_s \geq 0$ zadani brojevi. Onda je $|\mathcal{B}| \leq \binom{v}{s}$.*

Dokaz. Gledamo vektorski prostor $V(\mathcal{B}) = \{f : \mathcal{B} \to \mathbb{R}\}$ dimenzije $|\mathcal{B}| = b$. Za svaki $S \subseteq \mathcal{P}$, $|S| = s$ definiramo $\widehat{S} = \sum_{B \in \mathcal{B}, S \subseteq B} f_B$. Takvih vektora ima $\binom{v}{s}$ i ako pokažemo da $\{\widehat{S} \mid S \subseteq \mathcal{P}, |S| = s\}$ razapinje $V(\mathcal{B})$, slijedi $b \leq \binom{v}{s}$.

Za čvrsti blok $B_0 \in \mathcal{B}$ želimo pokazati da je indikatorska funkcija f_{B_0} razapeta vektorima $\widehat{S}$, $S \subseteq \mathcal{P}$, $|S| = s$. Označimo $\mu_0 = k$ i definiramo vektore $H_i = \sum_{B \in \mathcal{B}, |B \cap B_0| = \mu_i} f_B$, $i = 0, 1, \ldots, s$ (očito je $H_0 = f_{B_0}$). Prvo vektore $G_r = \sum_{S \subseteq \mathcal{P}, |S| = s, |S \cap B_0| = r} \widehat{S}$, $r = 0, 1, \ldots, s$ izrazimo preko H_i:

$$G_r = \sum_{i=0}^{s} \binom{\mu_i}{r} \binom{k - \mu_i}{s - r} H_i.$$

Jednakost se vidi uspoređivanjem koeficijenata uz f_B na lijevoj i desnoj strani. Očito f_B ima koeficijent 1 u onim H_i za koje je $|B \cap B_0| = \mu_i$, a u ostalim H_i ima koeficijent 0. Koeficijent s lijeve strane je broj načina na koje možemo izabrati skup $S \subseteq \mathcal{P}$, $|S| = s$, $S \subseteq B$, $|S \cap B_0| = r$, a to je $\binom{\mu_i}{r}\binom{k-\mu_i}{s-r}$. Time je jednakost dokazana.

Sad želimo "obrnuti" vezu, tj. izraziti vektore H_i preko vektora G_r. Tada će $H_0 = f_{B_0}$ biti linearna kombinacija G_r, koji su očito razapeti sa $\widehat{S}$ i dokaz će biti gotov. Dovoljno je pokazati da je matrica koeficijenata $a_{ri} = \binom{\mu_i}{r}\binom{k-\mu_i}{s-r}$, $r, i \in \{0, 1, \ldots, s\}$ regularna. Označimo retke te matrice s $v_r = \left(\binom{\mu_0}{r}\binom{k-\mu_0}{s-r}, \ldots, \binom{\mu_s}{r}\binom{k-\mu_s}{s-r}\right)$, za $r = 0, 1, \ldots, s$. Dokazat ćemo da su reci linearno nezavisni, iz čega slijedi regularnost matrice.

Pretpostavimo $\alpha_0 v_0 + \ldots + \alpha_s v_s = 0$. To znači da polinom $p(x) = \sum_{r=0}^{s} \alpha_r \binom{x}{r}\binom{k-x}{s-r}$ ima $s + 1$ nultočaka $\mu_0, \ldots, \mu_s$. Stupanj tog polinoma nije veći od s, pa zaključujemo da je $p(x)$ nulpolinom. Uvrštavanjem $x = 0, 1, \ldots, s$ redom dobivamo $\alpha_0 = \alpha_1 = \ldots = \alpha_s = 0$. Dakle, $v_0, \ldots, v_s$ su linearno nezavisni i dokaz je gotov. $\square$

Korolar 1.19. *Kvazisimetrični dizajn bez ponovljenih blokova ima najviše* $b \le \binom{v}{2}$ *blokova.*

Dokaz. Primijenimo prethodni teorem za $s = 2$ i $\mu_1 = y$, $\mu_2 = x$. $\square$

Dva direktna dokaza ovog rezultata nalaze se u [124, tm. 3.15 na str. 39]. Za kvazisimetrične dizajne s ponovljenim blokovima ne možemo ograničiti broj blokova odozgo. Naprimjer, m-struki simetrični dizajn ima $b = mv$ blokova i m može biti proizvoljno velik. To su jedini primjeri kvazisimetričnih dizajna koji nisu jednostavni.

Propozicija 1.20. *Svaki kvazisimetrični dizajn s ponovljenim blokovima je višekratnik simetričnog dizajna.*

Dokaz. Neka je $B_0 \in \mathcal{B}$ čvrsti blok našeg dizajna. Svaki drugi blok $B \ne B_0$ siječe B_0 u x ili u y točaka; označimo broj takvih blokova s m_x, odnosno m_y. Očito je $m_x + m_y = b - 1$, a dvostrukim prebrojavanjem parova $\{(T, B) \mid T \in B_0 \cap B, B \ne B_0\}$ dobijemo jednadžbu $x\, m_x + y\, m_y = k(r - 1)$. Te dvije jednadžbe imaju jedinstveno rješenje

$$m_x = \frac{y(b-1) - k(r-1)}{y - x}, \quad m_y = \frac{k(r-1) - x(b-1)}{y - x}.$$

Vidimo da m_x i m_y ne ovise o izboru bloka B_0, nego samo o parametrima kvazisimetričnog dizajna i njegovim presječnim brojevima.

Ako kvazisimetrični dizajn ima ponovljene blokove, onda je $y = k$ i svaki blok se ponavlja $m = m_y + 1$ puta. Dakle, dizajn je m-struki višekratnik nekog t-$(v, k, \lambda/m)$ dizajna u kojem se svaka dva bloka sijeku u x točaka. Prema teoremu 1.10 taj dizajn je simetričan. $\square$

Teorem 1.21. *Ako postoji netrivijalni kvazisimetrični* t-(v, k, λ) *dizajn, onda je* $t \le 4$.

Dokaz. Ako dizajn ima ponovljene blokove, onda je višekratnik simetričnog i po korolaru 1.13 vijedi $t = 2$. U suprotnom možemo primijeniti korolar 1.19 i broj blokova ograničiti odozgo s $b \le \binom{v}{2}$. S druge strane, za $t \ge 5$ po korolaru 1.16 broj blokova je ograničen odozdo s $b \ge 2\binom{v-1}{2}$. Iz $2\binom{v-1}{2} \le \binom{v}{2}$ slijedi $v^2 - 5v + 4 \le 0$ i $v \le 4$, što ostavlja mogućnost samo za trivijalne dizajne. $\square$

Iz teorema 1.15 i 1.18 slijedi da t-(v, k, λ) dizajn $\mathcal{D}$ s parnim $t = 2s$ i $v \ge k + s$ ima bar s presječnih brojeva. Za karakterizaciju napetih dizajna nedostaje još ovaj rezultat.

Teorem 1.22. *Napeti t-(v, k, λ) dizajn ima najviše s presječnih brojeva, za $t = 2s$.*

Dakle, $\mathcal{D}$ ima točno s presječnih brojeva ako i samo ako je napet, tj. ima $b = \binom{v}{s}$ blokova. U [119] dokaz teorema 1.22 je linearnoalgebarski i koristi vektorski prostor $V(X)$ iz dokaza teorema 1.15. U tom dokazu $\{\widehat{B} \mid B \in \mathcal{B}\}$ je baza za $V(X)$ i pojavljuje se tzv. Delsarteov polinom, kojem su nultočke presječni brojevi. Direktna posljedica karakterizacije je

Korolar 1.23. *Kvazisimetrični t-(v, k, λ) dizajn s $4 \leq k \leq v - 4$ zadovoljava $b = \binom{v}{2}$ ako i samo ako je $t = 4$.*

U tom slučaju Delsarteov polinom može se zapisati preko parametara dizajna.

Teorem 1.24. *Presječni brojevi napetog 4-(v, k, λ) dizajna su nultočke kvadratnog polinoma*

$$f(x) = x^2 - \left(\frac{2(k-1)(k-2)}{v-3} + 1\right) x + \lambda \left(2 + \frac{4}{k-3}\right).$$

Dokaz se nalazi u [119, tm. 5]. Derivirani dizajn velikog Wittovog 5-$(24, 8, 1)$ dizajna ima parametre 4-$(23, 7, 1)$. Broj blokova je $b = 253 = \binom{23}{2}$, pa je kvazisimetričan s presječnim brojevima $x = 1$, $y = 3$ koje dobijemo kao nultočke polinoma $f(x) = x^2 - 4x + 3$. Komplement tog dizajna ima parametre 4-$(23, 16, 52)$. I on je napet i ima Delsarteov polinom $f(x) = x^2 - 22 + 120$, pa je kvazisimetričan s presječnim brojevima $x = 10$, $y = 12$. Ovo su jedina dva primjera netrivijalnih kvazisimetričnih 4-dizajna.

Teorem 1.25. *Derivirani Wittov dizajn 4-$(23, 7, 1)$ i njegov komplement 4-$(23, 16, 52)$ su jedini netrivijalni napeti 4-dizajni, prema tome jedini netrivijalni kvazisimetrični 4-dizajni.*

Dokaz koristi napredne tehnike iz teorije brojeva i objavljen je u nizu članaka i njihovih ispravaka [71, 72, 55, 29]. Uz simetrične dizajne, to su ujedno jedini poznati primjeri napetih dizajna. U [111] je dokazano da ne postoje napeti 6-dizajni (slučaj $s = 3$). U [11] je dokazano da za svaki $s \geq 5$ postoji najviše konačno mnogo napetih $(2s)$-dizajna, a u [53] da ne postoje za $5 \leq s \leq 9$. Ti rezultati zasnivaju se na cjelobrojnosti nultočaka Delsarteova polinoma. Slučaj $s = 4$ još je uvijek otvoren.

1.4 Proširenja dizajna i kvazisimetrični 3-dizajni

Definicija 1.26. *Neka je* $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ t-(v, k, λ) *dizajn i* $T_0 \in \mathcal{P}$ *jedna njegova točka. Definiramo* derivirani dizajn *kao incidencijsku strukturu*

$$\mathrm{der}_{T_0}\mathcal{D} = (\, \mathcal{P} \setminus \{T_0\},\ \{B \setminus \{T_0\} \mid B \in \mathcal{B}, T_0 \in B\}\,),$$

a rezidualni dizajn *kao incidencijsku strukturu*

$$\mathrm{res}_{T_0}\mathcal{D} = (\, \mathcal{P} \setminus \{T_0\},\ \{B \mid B \in \mathcal{B}, T_0 \notin B\}\,).$$

Propozicija 1.27. *Struktura* $\mathrm{der}_{T_0}\mathcal{D}$ *je* $(t-1)$-$(v-1, k-1, \lambda)$ *dizajn, a struktura* $\mathrm{res}_{T_0}\mathcal{D}$ *je* $(t-1)$-$(v-1, k, \lambda_{t-1} - \lambda)$ *dizajn.*

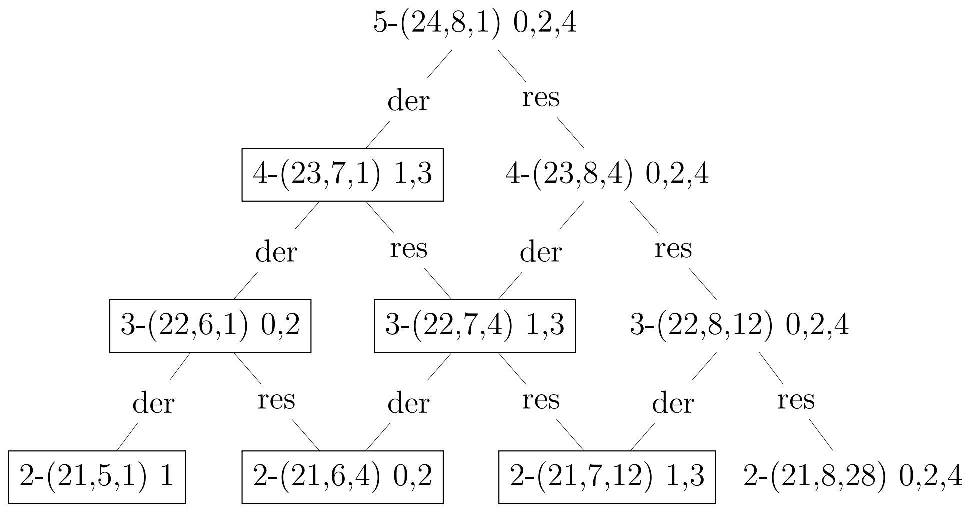
Dokaz. Očito $\mathrm{der}_{T_0}\mathcal{D}$ ima $v-1$ točaka, $k-1$ točaka na svakom bloku i λ blokova kroz bilo koji $(t-1)$-člani podskup od $\mathcal{P} \setminus \{T_0\}$ (to su blokovi od $\mathcal{D}$ koji sadrže taj podskup i točku T_0). Slično, $\mathrm{res}_{T_0}\mathcal{D}$ ima $v-1$ točaka, k točaka na svakom bloku i $\lambda_{t-1} - \lambda = \lambda_{t-1}^1$ blokova kroz bilo koji $(t-1)$-člani podskup od $\mathcal{P} \setminus \{T_0\}$ (to su blokovi od $\mathcal{D}$ koji sadrže taj podskup, a ne sadrže T_0). $\square$

Neka je $\mathcal{W}$ veliki Wittov 5-$(24, 8, 1)$ dizajn. On ima $b = \lambda_0 = \binom{24}{5}/\binom{8}{5} = 759$ blokova te parametre $r = \lambda_1 = \binom{23}{4}/\binom{7}{4} = 253$, $\lambda_2 = \binom{22}{3}/\binom{6}{3} = 77$, $\lambda_3 = \binom{21}{2}/\binom{5}{2} = 21$ i $\lambda_4 = \binom{20}{1}/\binom{4}{1} = 5$. U sljedećoj lemi dokazujemo da ima tri presječna broja 0, 2 i 4.

Lema 1.28. *Svaki blok* B_0 *od* $\mathcal{W}$ *siječe* 280 *blokova u* 4 *točke,* 448 *blokova u* 2 *točke i* 30 *blokova u* 0 *točaka.*

Dokaz. Dva bloka ne mogu se sjeći u 5 ili više točaka jer bismo tada imali više od $\lambda = 1$ blokova kroz tih 5 točaka. Broj parova u skupu $\mathcal{P}_i = \{(S, B) \mid S \subseteq B_0, |S| = i, B \neq B_0 \text{ blok}, S \subseteq B\}$ je $\binom{8}{i}(\lambda_i - 1)$. Iz $|\mathcal{P}_4| = 280$ zaključujemo da 280 blokova sijeku B_0 u 4 točke. Vrijedi $|\mathcal{P}_3| = 1120$, no blokovi koji sijeku B_0 u 4 točke već daju $280 \cdot \binom{4}{3} = 1120$ parova iz $\mathcal{P}_3$ pa nema blokova koji sijeku B_0 u 3 točke. Dalje vidimo da je $|\mathcal{P}_2| = 2128$, a blokovi koji sijeku B_0 u 4 točke daju $280 \cdot \binom{4}{2} = 1680$ parova iz $\mathcal{P}_2$. Zato blokova koji sijeku B_0 u 2 točke ima $2128 - 1680 = 448$. Iz $|\mathcal{P}_1| = 2016 = 280 \cdot \binom{4}{1} + 448 \cdot \binom{2}{1}$ zaključujemo da nema blokova koji sijeku B_0 u jednoj točki. Preostalih $b - 280 - 448 - 1 = 30$ blokova disjunktni su s B_0. $\square$

Iz ovoga direktno slijedi da je $\mathrm{der}\,\mathcal{W}$ kvazisimetrični 4-$(23, 7, 1)$ dizajn s presječnim brojevima $x = 1$, $y = 3$, bez pozivanja na napetost i teorem 1.24. Daljnjom primjenom operacija der i res dobivamo sljedeće dizajne s naznačenim presječnim brojevima.



Uokvireni su kvazisimetrični dizajni i simetrični 2-$(21, 5, 1)$ dizajn, tj. projektivna ravnina reda 4. Za t-(v, k, λ) dizajn $\mathcal{D}$ kažemo da je *proširiv* ako postoji $(t + 1)$-$(v + 1, k + 1, \lambda)$ dizajn $\mathcal{D}^*$ takav da je $\mathcal{D} = \mathrm{der}_{T_0} \mathcal{D}^*$ za neku točku T_0. Dizajn $\mathcal{D}^*$ nazivamo *proširenjem* od $\mathcal{D}$. Ovo je nuždan uvjet za proširivost dizajna.

Propozicija 1.29. *Ako je t-(v, k, λ) dizajn s b blokova proširiv, onda $k + 1$ dijeli $b(v + 1)$.*

Dokaz. Prošireni dizajn ima parametre $v^* = v+1$, $k^* = k+1$ i $r^* = b$. Uvjet dobivamo iz jednakosti $v^*r^* = b^*k^*$. $\square$

Posebno su zanimljiva proširenja simetričnih dizajna.

Propozicija 1.30. *Ako je simetrični* 2-(v, k, λ) *dizajn proširiv, onda je njegovo proširenje kvazisimetrični* 3-$(v+1, k+1, \lambda)$ *dizajn s presječnim brojevima* $x = 0$, $y = \lambda + 1$.

Dokaz. Neka je $\mathcal{D}^*$ proširenje simetričnog 2-(v, k, λ) dizajna i B_1, B_2 bilo koja dva njegova bloka. Neka B_1 i B_2 imaju bar jednu zajedničku točku T_0. Derivirani dizajn $\mathrm{der}_{T_0} \mathcal{D}^*$ je simetričan, pa se $B_1 \setminus \{T_0\}$ i $B_2 \setminus \{T_0\}$ sijeku u λ točaka. To znači da B_1 i B_2 imaju točno $y = \lambda + 1$ zajedničkih točaka. Mogućnost da B_1 i B_2 nemaju zajedničkih točaka također nastupa jer je $\mathcal{D}^*$ 3-dizajn i zato ne može biti simetričan. Dakle, realizira se i presječni broj $x = 0$. $\square$

Propozicija 1.31. *Svaki kvazisimetrični* 3*-dizajn s presječnim brojem* $x = 0$ *je proširenje simetričnog dizajna.*

Dokaz. Derivirani dizajn je 2-dizajn kojem se svaka dva bloka sijeku u $y-1$ točaka. Prema teoremu 1.10 on je simetričan. □

Dvije važne klase simetričnih dizajna su konačne projektivne ravnine i Hadamardovi dizajni. *Red* dizajna definira se kao broj $n = r - \lambda$, što je za simetrične dizajne jednako $k - \lambda$. Za simetrične dizajne čvrstog reda n dobivamo iz uvjeta $k(k-1) = \lambda(v-1)$ ocjenu za broj točaka $4n - 1 \leq v \leq n^2 + n + 1$ (vidi [129, tm. 4.4]). Konačne projektivne ravnine dostižu gornju granicu i imaju parametre oblika 2-$(n^2+n+1, n+1, 1)$ (možemo ih definirati kao simetrične dizajne s $\lambda = 1$). Hadamardovi dizajni dostižu donju granicu i imaju parametre oblika 2-$(4n-1, 2n-1, n-1)$. Promotrimo najprije što se zna o egzistenciji i proširenjima te dvije klase simetričnih dizajna.

Ako je q prim potencija, postoji konačno polje $\mathbb{F}_q$. Projektivnu ravninu reda $n = q$ možemo konstruirati iz trodimenzionalnog vektorskog prostora nad $\mathbb{F}_q$: točke su jednodimenzionalni potprostori, a pravci dvodimenzionalni. Tu projektivnu ravninu označavamo $PG(2, q)$ i zovemo *klasičnom* ili *Desarguesovom* ravninom. Poznati su mnogi drugi primjeri projektivnih ravnina reda q, neizomorfni s $PG(2, q)$. Nije poznat niti jedan primjer projektivne ravnine kojoj red nije prim potencija. Za neke redove koji nisu prim potencije se zna da projektivne ravnine ne postoje.

Teorem 1.32 (Bruck-Ryser)**.** *Ako postoji projektivna ravnina reda* $n \equiv 1$ *ili* $2 \pmod 4$*, onda je* n *zbroj dva kvadrata.*

Iz teorema slijedi nepostojanje projektivnih ravnina reda $n = 6$, 14, 21, 22, 30 i beskonačo mnogo drugih redova. Jedini red za koji je dokazano nepostojanje projektivne ravnine, a to nije posljedica Bruck-Ryserova teorema, je $n = 10$ [90]. Za beskonačno mnogo redova pitanje egzistencije projektivne ravnine je otvoreno, počevši s $n = 12$, 15, 18, 20, 24, 26, 28 ...

Samo dvije projektivne ravnine moguće je proširiti do 3-dizajna.

Propozicija 1.33. *Jedine proširive projektivne ravnine su reda* $n = 2$ *i* 4*.*

Dokaz. Uvjet iz propozicije 1.29 je da $n+2$ dijeli $(n^2+n+2)(n^2+n+1) = (n+2)(n-1)(n^2+n+5)+12$. Dakle, $n+2$ dijeli 12, što znači da je jednak 1, 2, 3, 4, 6 ili 12. Vidimo da su jedine mogućnosti $n = 2$ i $n = 4$. Ravnina reda 2 (tzv. Fanova ravnina) proširuje se do 3-$(8, 4, 1)$ dizajna iz primjera 1.2. Ravnina reda 4 je 2-$(21, 5, 1)$ dizajn. Vidjeli smo da se proširuje čak tri puta, sve do velikog Wittovog 5-$(24, 8, 1)$ dizana. □

Promotrimo sada Hadamardove dizajne. Oni su u vezi s matricama za koje je apsolutna vrijednost determinante maksimalna.

Teorem 1.34 (Hadamard)**.** *Neka je* $A = [a_{ij}] \in \mathbb{R}^{m\times m}$, $|a_{ij}| \le 1$. *Tada je* $|\det A| \le m^{m/2}$ *i jednakost vrijedi ako i samo ako su* $a_{ij} \in \{-1, 1\}$ *i* $A \cdot A^\tau = mI$.

Dokaz se može naći u [40, tm. 16.6.1 na str. 267]. Matrice koje dostižu jednakost nazivaju se *Hadamardovim matricama.* Poznato je da red Hadamardove matrice m mora biti jednak 1 ili 2 ili djeljiv s 4 [129, prop. 4.10]. Postojanje Hadamardove matrice reda $m = 4n$ ekvivalentno je postojanju Hadamardovog 2-$(4n-1, 2n-1, n-1)$ dizajna [129, tm. 4.12], [128, tm. 4.5]. Poznate su mnoge direktne i rekurzivne konstrukcije Hadamardovih matrica i dizajna. Naprimjer, ako je $q \equiv 3 \pmod 4$ prim potencija, onda postoji Hadamardov dizajn reda $n = (q+1)/4$ [129, tm. 6.12]. Ako postoje Hadamardovi dizajni reda n_1 i n_2, onda postoji Hadamardov dizajn reda $4n_1n_2$ [129, prop. 4.16]. Pretpostavlja se Hadamardovi dizajni postoje za sve redove $n \in \mathbb{N}$. Hipoteza nije dokazana, a najmanji otvoreni slučaj trenutačno je $n = 167$. Za razliku od projektivnih ravnina, svi Hadamardovi dizajni su proširivi.

Teorem 1.35. *Svaki* 2-$(4n-1, 2n-1, n-1)$ *dizajn proširiv je do* 3-$(4n, 2n, n-1)$ *dizajna. Svaki* 3-$(4n, 2n, n-1)$ *dizajn je kvazisimetričan s presječnim brojevima* $x = 0$, $y = n$.

Dokaz. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ simetrični 2-$(4n-1, 2n-1, n-1)$ dizajn sa skupom blokova $\mathcal{B} = \{B_1, \ldots, B_{4n-1}\}$. Definiramo $\mathcal{P}^* = \mathcal{P} \cup \{\infty\}$, $B_i^1 = B_i \cup \{\infty\}$, $B_i^2 = \mathcal{P} \setminus B_i$ i $\mathcal{B}^* = \{B_i^j \mid i = 1, \ldots, 4n-1,\ j = 1, 2\}$. Proširena struktura $\mathcal{D}^* = (\mathcal{P}^*, \mathcal{B}^*)$ je dizajn s parametrima 2-$(4n, 2n, 2n-1)$. Točka ∞ i bilo koja druga točka $P \in \mathcal{P}$ zajedno su sadržane u blokovima B_i^1 za koje je $P \in B_i$, a takvih je $2n-1$. Bilo koje dvije točke $P, Q \in \mathcal{P}$ zajedno su sadržane u $n-1$ blokova B_i^1 i n blokova B_i^2 (to su blokovi komplementarnog dizajna $\overline{\mathcal{D}}$ s parametrima 2-$(4n-1, 2n, n)$), dakle ukupno u $2n-1$ blokova iz $\mathcal{B}^*$.

Sada dokazujemo da je $\mathcal{D}^*$ zapravo 3-$(4n, 2n, n-1)$ dizajn. Uzmimo bilo koje tri točke $P, Q, R \in \mathcal{P}^*$ i definiramo a_1 kao broj blokova za koje je $\{P, Q, R\} \subseteq B_i^j$. Neka je a_2 broj blokova za koje je $\{P, Q\} \subseteq B_i^j$ i $R \notin B_i^j$, a_3 broj blokova za koje je $\{P, R\} \subseteq B_i^j$ i $Q \notin B_i^j$, te a_4 broj blokova za koje je $\{Q, R\} \subseteq B_i^j$ i $P \notin B_i^j$. Blokovi B_i^1 i B_i^2 čine particiju od $\mathcal{P}^*$, pa za svaki i nastupa točno jedan od ta četiri slučaja (ili su sve tri točke u jednom od blokova B_i^1, B_i^2, ili su dvije točke u jednom, a jedna u drugom). Zato je $a_1 + a_2 + a_3 + a_4 = 4n-1$. Ukupan broj blokova koji sadrže $\{P, Q\}$ je $a_1 + a_2$, što je jednako $2n-1$ jer je $\mathcal{D}^*$ 2-dizajn. Analogno slijedi $a_1 + a_3 = a_1 + a_4 = 2n-1$. Iz te četiri jednadžbe možemo izračunati $a_1 = n-1$ i zato je $\mathcal{D}^*$ 3-dizajn.

Druga tvrdnja teorema vrijedi jer derivirani 3-$(4n, 2n, n-1)$ dizajn ima parametre simetričnog Hadamardovog dizajna, pa primijenimo propoziciju 1.30. $\square$

Kvazisimetrični 3-dizajni iz prethodnog teorema također se nazivaju Hadamardovim. Cameron [38] je odredio sve moguće parametre proširivih simetričnih dizajna.

Teorem 1.36 (Cameron). *Ako je simetrični* 2-(v, k, λ) *dizajn* $\mathcal{D}$ *proširiv, onda vrijedi:*

1. $v = 4\lambda + 3$, $k = 2\lambda + 1$ *($\mathcal{D}$ je Hadamardov dizajn), ili*
2. $v = (\lambda + 2)(\lambda^2 + 4\lambda + 2)$, $k = \lambda^2 + 3\lambda + 1$, *ili*
3. $v = 495$, $k = 39$, $\lambda = 3$.

Dokaz. Parametri simetričnog dizajna $\mathcal{D}$ zadovoljavaju $(v-1)\lambda = k(k-1)$. Proširenje $\mathcal{D}^*$ je kvazisimetrični 3-$(v+1, k+1, \lambda)$ dizajn s presječnim brojevima $x = 0$, $y = \lambda + 1$. Njegov broj blokova je $b^* = \frac{\lambda(v+1)v(v-1)}{(k+1)k(k-1)} = \frac{v(v+1)}{k+1}$ i ima $\lambda_2 = \frac{\lambda(v-1)}{k-1} = k$ blokova kroz svake dvije točke. Za čvrsti blok $B_0 \in \mathcal{B}^*$ definiramo incidencijsku strukturu $\mathcal{D}' = (\mathcal{P} \setminus B_0, \{B \in \mathcal{B}^* \mid B \cap B_0 = \emptyset\})$. To je dizajn s parametrima 2-$(v-k, k+1, \frac{k-\lambda}{\lambda+1})$. Zaista, za svake dvije točke $P, Q \notin B_0$ i točku $T \in B_0$ postoji λ blokova od $\mathcal{D}^*$ koji ih sadrže. Zbog kvazisimetričnosti svaki takav blok siječe B_0 u $y = \lambda + 1$ točaka, pa imamo ukupno $\frac{(k+1)\lambda}{\lambda+1}$ blokova kroz P i Q koji sijeku B_0. Stoga je broj blokova kroz P i Q koji ne sijeku B_0 jednak $\lambda_2 - \frac{(k+1)\lambda}{\lambda+1} = \frac{k-\lambda}{\lambda+1}$.

Ako se $\mathcal{D}'$ sastoji samo od jednog bloka, onda on sadrži sve točke iz $\mathcal{P} \setminus B_0$ pa je $v + 1 = 2(k+1)$ i $k = 2\lambda + 1$. U tom slučaju $\mathcal{D}$ je Hadamardov dizajn i vrijedi 1. tvrdnja teorema. U suprotnom primijenimo Fisherovu nejednakost na parametre dizajna $\mathcal{D}'$ i dobivamo $b' = \frac{\lambda' v'(v'-1)}{k'(k'-1)} = \frac{(k-\lambda)(v-k)(v-k-1)}{(\lambda+1)k(k+1)} \geq v' = v - k$. Slijedi $(k-\lambda)(v-k-1) \geq (\lambda+1)k(k+1)$, što se uvrštavanjem $v = \frac{k(k-1)}{\lambda} + 1$ može zapisati kao $\frac{k^2}{\lambda}(k - 1 - \lambda(\lambda+3)) \geq 0$. Vidimo da je $k - 1 \geq \lambda(\lambda+3)$, odnosno $k + 1 \geq (\lambda+1)(\lambda+2)$. S druge strane, zbog cjelobrojnosti $b^* = \frac{v(v+1)}{k+1}$ slijedi da $k+1$ dijeli $2(\lambda+1)(\lambda+2)$. To se također vidi uvrštavanjem $v = \frac{k(k-1)}{\lambda} + 1$:

$$\begin{aligned} b^* &= \tfrac{[k(k-1)+\lambda]\cdot[k(k-1)+2\lambda]}{(k+1)\lambda^2} = \tfrac{[(k+1)(k-2)+\lambda+2]\cdot[(k+1)(k-2)+2(\lambda+1)]}{(k+1)\lambda^2} \\ &= \tfrac{(k+1)^2(k-2)^2+(k+1)(k-2)(\lambda+2)+2(k+1)(k-2)(\lambda+1)+2(\lambda+1)(\lambda+2)}{(k+1)\lambda^2}. \end{aligned}$$

Prva tri člana sume u brojniku djeljiva su s $k+1$, pa mora biti i četvrti član $2(\lambda+1)(\lambda+2)$. Dakle, vrijedi $k+1 = (\lambda+1)(\lambda+2)$ ili $k+1 = 2(\lambda+1)(\lambda+2)$.

U prvom slučaju je $k = \lambda^2 + 3\lambda + 1$, $v = (\lambda+2)(\lambda^2+4\lambda+2)$ i vrijedi 2. tvrdnja teorema. U drugom slučaju uvrštavanjem u $(v-1)\lambda = k(k-1)$ dobijemo $(v-1)\lambda = 6 + 30\lambda + 46\lambda^2 + 24\lambda^3 + 4\lambda^4$. Lijeva strana je djeljiva s λ, pa λ mora biti djelitelj od 6, tj. $\lambda = 1$, 2, 3 ili 6. Za $\lambda = 2$ i 6 parametar b^* nije cjelobrojan. Za $\lambda = 1$ dobijemo $v = 111$ i $k = 11$, a to su parametri konačne projektivne ravnine reda 10 koja ne postoji. Konačno, za $\lambda = 3$ dobijemo $v = 495$, $k = 39$ i vrijedi 3. tvrdnja teorema. □

Kao što smo vidjeli, Hadamardovi dizajni su uvijek proširivi i hipoteza je da postoje za sve $\lambda \in \mathbb{N}$. Za $\lambda = 1$ Hadamardov dizajn se podudara s Fanovom ravninom i njezinim proširenjem do 3-$(8,4,1)$ dizajna.

Druga serija iz Cameronova teorema za $\lambda = 1$ daje projektivnu ravninu reda 4, koja se proširuje do 3-$(22,6,1)$ dizajna. Iz teorema slijedi da je to jedini simetrični dizajn kojeg je moguće dva puta proširiti. Za $\lambda = 2$ druga serija daje parametre 2-$(56,11,2)$, takozvane dvoravnine reda 9. Poznato je da postoji točno 5 takvih dizajna [82], ali niti jedan nije moguće proširiti do 3-dizajna [8, 9]. Za $\lambda \geq 3$ nije poznato postoje li simetrični dizajni iz druge serije niti mogu li se proširiti. Isto vrijedi za 2-$(495,39,3)$ dizaje iz trećeg slučaja teorema.

Prema propoziciji 1.31, Cameronov teorem ujedno klasificira kvazisimetrične 3-dizajne s presječnim brojem $x = 0$. Poznato je vrlo malo kvazisimetričnih 3-dizajna s $x > 0$. To su derivirani Wittov dizajn 4-$(23,7,1)$, $x = 1$, $y = 3$ (koji je ujedno 3-$(23,7,5)$ dizajn), njegov rezidualni dizajn 3-$(22,7,4)$, $x = 1$, $y = 3$ i njihovi komplementi 4-$(23,16,52)$, $x = 10$, $y = 12$ i 3-$(22,15,52)$, $x = 9$, $y = 11$. Postavljena je hipoteza [120] da su to jedini kvazisimetrični 3-dizajni s $x > 0$. Dokazano je npr. da su jedini primjeri s $x = 1$ derivirani Wittov dizajn i njegov rezidual [37, 108].

Na kraju ove cjeline spomenimo generalizaciju teorema 1.35. Hadamardovi 2-$(4n-1, 2n-1, n-1)$ dizajni proširuju se do 3-dizajna tako da se na blokove doda točka ∞ i uz to se uzmu komplementi blokova. Slične konstrukcije dokazuju sljedeća dva teorema iz [4].

Teorem 1.37. *Svaki t-$(2k+1, k, \lambda)$ dizajn s parnim t proširiv je do $(t+1)$-$(2k+2, k+1, \lambda)$ dizajna.*

Teorem 1.38. *Svaki t-$(2k+1, k, \lambda)$ dizajn s neparnim t i $b = \frac{1}{2}\binom{2k+1}{k}$ blokova proširiv je do $(t+1)$-$(2k+2, k+1, \lambda)$ dizajna.*

2 Grafovi

2.1 Blokovni graf kvazisimetričnog dizajna

Neka je $\mathcal{D}$ dizajn s parametrima 2-$(v, k, 1)$ (Steinerov 2-dizajn). Znamo da je kvazisimetričan s presječnim brojevima $x = 0$, $y = 1$, a vrijedi i obrat: svaki kvazisimetrični 2-dizajn s presječnim brojevima $x = 0$, $y = 1$ ima parametar $\lambda = 1$.

Dizajnu $\mathcal{D}$ pridružimo graf $\Gamma(\mathcal{D})$ na sljedeći način. Vrhovi grafa su blokovi od $\mathcal{D}$. Dva vrha spojena su bridom ako se odgovarajući blokovi sijeku. Graf $\Gamma(\mathcal{D})$ ima b vrhova i svaki je stupnja $a = k(r-1)$ (kroz svaku od k točaka na bloku prolazi još $r-1$ drugih blokova). Nadalje, svaka dva susjedna vrha imaju $c = r - 2 + (k-1)^2$ zajedničkih susjeda (kroz zajedničku točku dvaju blokova prolazi $r-2$ drugih blokova, a ostali blokovi koji sijeku oba su spojnice parova točaka na jednom i drugom bloku). Konačno, svaka dva nesusjedna vrha imaju $d = k^2$ zajedničkih susjeda (spojnice parova točaka na jednom i drugom bloku). Grafove s tim svojstvima nazivamo jako regularnim.

Definicija 2.1. *Za graf Γ kažemo da je* jako regularan *s parametrima $SRG(b, a, c, d)$ (od eng. strongly regular graph) ako ima b vrhova, svaki vrh je stupnja a, svaka dva susjedna vrha imaju c zajedničkih susjeda i svaka dva nesusjedna vrha imaju d zajedničkih susjeda.*

Vidjeli smo da je graf pridružen 2-$(v, k, 1)$ dizajnu jako regularan s parametrima $SRG(b, k(r-1), r-2+(k-1)^2, k^2)$. Proširit ćemo taj rezultat na opće kvazisimetrične dizajne.

Definicija 2.2. *Neka je $\mathcal{D}$ kvazisimetrični 2-(v, k, λ) dizajn s presječnim brojevima $x < y$.* Blokovni graf $\Gamma(\mathcal{D})$ *ima kao vrhove blokove od $\mathcal{D}$. Dva vrha su spojena bridom ako se odgovarajući blokovi sijeku u y točaka.*

Komplement od $\mathcal{D}$ je kvazisimetrični 2-$(v, v-k, b-2r+\lambda)$ dizajn $\overline{\mathcal{D}}$ s presječnim brojevima $\overline{x} = v - 2k + x$ i $\overline{y} = v - 2k + y$, $\overline{x} < \overline{y}$. Primijetimo da je $\Gamma(\mathcal{D}) = \Gamma(\overline{\mathcal{D}})$, zato što se blokovi B_1 i B_2 sijeku u y točaka ako i samo ako se njihovi komplementi $\mathcal{P} \setminus B_1$ i $\mathcal{P} \setminus B_2$ sijeku u $\overline{y}$ točaka.

Teorem 2.3. *Blokovni graf kvazisimetričnog dizajna je jako regularan.*

Dokaz. Neka $\mathcal{D}$ ima parametre 2-(v, k, λ) i presječne brojeve $x < y$. Dvostrukim prebrojavanjem dokazat ćemo da je $\Gamma(\mathcal{D})$ jako regularan i odrediti mu parametre. Stupanj regularnosti a je broj blokova koji sijeku zadani blok B_0 u y točaka. U dokazu propozicije 1.20 vidjeli smo da $a = m_y = \frac{k(r-1)-x(b-1)}{y-x}$ ne ovisi o izboru bloka B_0. Osim toga iz uvjeta $m_x, m_y \geq 0$ slijedi $x \leq \frac{k(r-1)}{b-1} \leq y$.

Broj u sredini možemo interpretirati kao prosječnu veličinu presjeka dvaju blokova od $\mathcal{D}$.

Neka su B_1 i B_2 dva bloka koji se sijeku u y točaka, tj. susjedni vrhovi od $\Gamma(\mathcal{D})$. Označimo s c_{ij} broj blokova koji sijeku B_1 u i točaka, a B_2 u j točaka, za $i, j \in \{x, y\}$. Očito vrijedi

$$c_{xx} + c_{xy} + c_{yx} + c_{yy} = b - 2. \tag{1}$$

Dvostrukim prebrojavanjem parova $\{(P, B) \mid P \in B_1, P \in B, B \neq B_1, B_2\}$ dobijemo jednadžbu

$$xc_{xx} + xc_{xy} + yc_{yx} + yc_{yy} = k(r-1) - y. \tag{2}$$

Slično, brojanjem parova $\{(Q, B) \mid Q \in B_2, Q \in B, B \neq B_1, B_2\}$ dobijemo

$$xc_{xx} + yc_{xy} + xc_{yx} + yc_{yy} = k(r-1) - y. \tag{3}$$

Četvrta jednakost slijedi brojanjem trojki $\{(P, Q, B) \mid P \in B_1, Q \in B_2, P, Q \in B, B \neq B_1, B_2\}$:

$$x^2 c_{xx} + xyc_{xy} + xyc_{yx} + y^2 c_{yy} = DS. \tag{4}$$

Desnu stranu $DS = (k-y)^2\lambda + 2y(k-y)(\lambda-1) + y(r-2) + y(y-1)(\lambda-2)$ dobijemo kad prvo biramo P i Q. Prvi član odgovara slučaju $P \in B_1 \setminus B_2$ i $Q \in B_2 \setminus B_1$. Drugi član odgovara slučaju $P \in B_1 \setminus B_2$ i $Q \in B_1 \cap B_2$ ili $P \in B_1 \cap B_2$ i $Q \in B_2 \setminus B_1$. Treći član odgovara slučaju $P = Q \in B_1 \cap B_2$, a četvrti slučaju $P, Q \in B_1 \cap B_2$, $P \neq Q$.

Sustav (1)-(4) možemo zapisati matrično:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ x & x & y & y \\ x & y & x & y \\ x^2 & xy & xy & y^2 \end{bmatrix} \cdot \begin{bmatrix} c_{xx} \\ c_{xy} \\ c_{yx} \\ c_{yy} \end{bmatrix} = \begin{bmatrix} b-2 \\ k(r-1)-y \\ k(r-1)-y \\ DS \end{bmatrix}.$$

Determinanta matrice sustava je $-(x-y)^4 \neq 0$, pa sustav ima jedinstveno rješenje. To znači da varijable c_{ij} ne ovise o izboru blokova B_1, B_2. Broj zajedničkih susjeda od B_1 i B_2 u grafu $\Gamma(\mathcal{D})$ je

$$c = c_{yy} = \frac{x^2(b-2) + 2xy - 2k((r-1)x + y) + y(r-\lambda) + k^2\lambda}{(x-y)^2}. \tag{5}$$

Slično postupamo kad su B_1, B_2 dva bloka koji se sijeku u x točaka, tj. nesusjedni vrhovi od $\Gamma(\mathcal{D})$. Ozačimo s d_{ij} broj blokova koji B_1 sijeku u i

točaka, a B_2 u j točaka, za $i, j \in \{x, y\}$. Dobijemo sustav

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ x & x & y & y \\ x & y & x & y \\ x^2 & xy & xy & y^2 \end{bmatrix} \cdot \begin{bmatrix} d_{xx} \\ d_{xy} \\ d_{yx} \\ d_{yy} \end{bmatrix} = \begin{bmatrix} b-2 \\ k(r-1)-x \\ k(r-1)-x \\ DS \end{bmatrix}$$

za $DS = (k-x)^2\lambda + 2x(k-x)(\lambda-1) + x(r-2) + x(x-1)(\lambda-2)$. Sustav ima jedinstveno rješenje, a broj zajedničkih susjeda od B_1 i B_2 je

$$d = d_{yy} = \frac{x^2 b - rx(2k-1) + (k^2 - x)\lambda}{(x-y)^2}. \tag{6}$$

□

Time smo dokazali da je graf $\Gamma(\mathcal{D})$ jako regularan, ali su izrazi (5) i (6) za parametre c i d vrlo komplicirani. Moguće ih je jednostavnije zapisati s pomoću svojstvenih vrijednosti grafa $\Gamma(\mathcal{D})$. Na taj način dobit ćemo i uvjete djeljivosti na parametre i presječne brojeve kvazisimetričnog dizajna.

2.2 Spektralna karakterizacija jako regularnih grafova

Kao što dizajne i druge incidencijske strukture opisujemo incidencijskim matricama, grafove možemo opisati matricama susjedstva. Za graf Γ s v vrhova matrica susjedstva je $v \times v$ matrica $A = [a_{ij}]$ kojoj je unos a_{ij} broj bridova između i-tog i j-tog vrha. Ako je Γ neusmjeren jednostavan graf (bez petlji i višestrukih bridova), A je simetrična 0-1 matrica s nulama na dijagonali. Pod spektrom grafa Γ podrazumijevamo skup svih svojstvenih vrijednosti od A. Definicija je dobra, tj. ne ovisi o numeraciji vrhova grafa Γ, jer se matrice susjedstva izomorfnih grafova odnose kao $A' = P^{-1} \cdot A \cdot P = P^{\tau} \cdot A \cdot P$ za neku permutacijsku matricu P. Dakle, A i A' su slične i imaju iste spektre.

Propozicija 2.4. *Neka k-ta potencija matrice susjedstva A ima elemente $A^k = [a_{ij}^{(k)}]$. Onda je $a_{ij}^{(k)}$ broj šetnji duljine k od i-tog do j-tog vrha grafa Γ.*

Dokaz. Indukcijom po k. Tvrdnja očito vrijedi za $k = 1$. Šetnje duljine k podijelimo po predzadnjem vrhu l. Po pretpostavci indukcije $a_{il}^{(k-1)}$ je broj šetnji duljine $k-1$ od i-tog do l-tog vrha. Broj šetnji duljine k od i-tog do j-tog vrha je $\sum_{l=1}^{v} a_{il}^{(k-1)} \cdot a_{lj}$, a to je upravo $a_{ij}^{(k)}$. □

Propozicija 2.5. *Graf Γ je regularan stupnja a ako i samo ako je a svojstvena vrijednost matrice susjedstva A pridružena svojstvenom vektoru $j = (1, 1, \ldots, 1)$.*

Dokaz. Produkt $A \cdot j$ na i-toj komponenti ima $\sum_{l=1}^{v} a_{il}$, a to je stupanj i-tog vrha od Γ. Zato je $A \cdot j = aj$ ako i samo ako su svi vrhovi stupnja a. $\square$

Propozicija 2.6. *Graf Γ je regularan ako i samo ako matrica susjedstva A komutira s matricom J (kvadratnom matricom reda v popunjenom jedinicama).*

Dokaz. Označimo stupnjeve vrhova grafa Γ s $a_1, \dots, a_v$. Onda je

$$A \cdot J = \begin{bmatrix} a_1 & a_1 & \cdots & a_1 \\ a_2 & a_2 & \cdots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_v & a_v & \cdots & a_v \end{bmatrix}, \quad J \cdot A = \begin{bmatrix} a_1 & a_2 & \cdots & a_v \\ a_1 & a_2 & \cdots & a_v \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_v \end{bmatrix}.$$

Vidimo da je $A \cdot J = J \cdot A$ ako i samo ako je $a_1 = a_2 = \ldots = a_v$. $\square$

Propozicija 2.7. *Graf Γ je jako regularan s parametrima $SRG(v, a, c, d)$ ako i samo ako njegova matrica susjedstva zadovoljava $A^2 = aI + cA + d(J - I - A)$.*

Dokaz. Na lijevoj strani je kvadrat matrice susjedstva $A^2 = [a_{ij}^{(2)}]$. Dijagonalni element $a_{ii}^{(2)}$ je broj šetnji duljine 2 od i-tog do i-tog vrha, tj. stupanj i-tog vrha. Element $a_{ij}^{(2)}$ je broj šetnji duljine 2 od i-tog do j-tog vrha, tj. broj zajedničkih susjeda i-tog i j-tog vrha. Dijagonalni elementi matrice na desnoj strani su a, a na mjestu (i, j) izvan dijagonale je c ako su i-ti i j-ti vrh susjedni, a d inače. Vidimo da matrična jednakost vrijedi ako i samo ako su svi vrhovi stupnja a, susjedni vrhovi imaju c zajedničkih susjeda, a nesusjedni vrhovi imaju d zajedničkih susjeda. $\square$

Potpuni graf $\Gamma = K_v$ je jako regularan s parametrima $SRG(v, v-1, v-2, *)$. Za parametar d možemo staviti bilo što jer nema nesusjednih vrhova. Matrica susjedstva mu je $A = J - I$ (matrica s nulama na dijagonali i jedinicama izvan dijagonale).

Lema 2.8. *Spektar kvadratne matrice $A = pI + q(J - I)$ reda v s elementom p na dijagonali i $q \neq 0$ izvan dijagonale je $\{p + (v-1)q, p - q\}$, pri čemu je svojstvena vrijednost $p + (v-1)q$ kratnosti 1, a $p - q$ kratnosti $v - 1$.*

Dokaz. Vrijedi $A \cdot j = (p + (v-1)q)j$, što znači da je $p + (v-1)q$ svojstvena vrijednost pridružena svojstvenom vektoru j. Nadalje, za vektor $x = (x_1, \dots, x_v)$ vrijedi $A \cdot x = (p - q)x$ ako i samo ako je $q(x_1 + \ldots + x_v) = 0$, a to znači da je $p - q$ svojstvena vrijednost čiji je svojstveni potprostor $(v-1)$-dimenzionalni potprostor zadan jednadžbom $x_1 + \ldots + x_v = 0$ (potprostor $[j]^{\perp}$ u standardnom skalarnom produktu na $\mathbb{R}^v$). $\square$

Dakle, potpun graf K_v ima dvije svojstvene vrijednosti: $v-1$ kratnosti 1 i -1 kratnosti $v-1$. Disjunktna unija potpunih grafova $\Gamma = m \cdot K_n$ također ima dvije svojstvene vrijednosti. Matrica susjedstva A je blok-dijagonalna s m blokova $J_n - I_n$ na dijagonali i karakterističnim polinomom $k_A(\lambda) = (-1)^{mn}(\lambda - (n-1))^m(\lambda+1)^{mn-m}$, pa joj je spektar $\{n-1, -1\}$ ($n-1$ kratnosti m, a -1 kratnosti $v-m = mn-m$). Graf $\Gamma = m \cdot K_n$ je jako regularan s parametrima $SRG(mn, n-1, n-2, 0)$.

Propozicija 2.9. *Jako regularni graf Γ ima parametar $d = 0$ ako i samo ako je oblika $\Gamma = m \cdot K_n$.*

Dokaz. Zbog uvjeta $d = 0$ relacija "postoji brid" na skupu svih vrhova je tranzitivna i možemo je proširiti do relacije ekvivalencije. Klase ekvivalencije particioniraju vrhove na disjunktnu uniju potpunih grafova, koji su jednako veliki zbog regularnosti. $\square$

Propozicija 2.10. *Jako regularni graf $\Gamma \neq K_v$ s parametrima $SRG(v, a, c, d)$ je povezan ako i samo ako je $d > 0$.*

Dokaz. Svaka dva susjedna vrha povezana su šetnjom duljine 1. Nesusjedne vrhove zbog $d > 0$ povezuje šetnja duljine 2. Obrnuto, povezani jako regularni graf $\Gamma \neq K_v$ mora imati $d > 0$ zbog prethodne karakterizacije. $\square$

Komplement grafa $\Gamma = m \cdot K_n$ je potpuni m-partitni graf $\overline{\Gamma} = K_{n,n,\ldots,n}$. Očito je jako regularan s parametrima $SRG(mn, mn-n, mn-2n, mn-n)$, što slijedi i iz sljedeće propozicije.

Propozicija 2.11. *Neka je Γ jako regularan s parametrima $SRG(v, a, c, d)$. Onda je njegov komplement $\overline{\Gamma}$ jako regularan s parametrima $SRG(v, v-1-a, v-2a+d-2, v-2a+c)$.*

Dokaz. Komplement je regularan stupnja $\overline{a} = v-1-a$. Dva nesusjedna vrha u Γ imaju d zajedničkih susjeda, a uz to svaki ima još $a-d$ susjeda. Znači da oba nisu susjedni s $v-2-2(a-d)-d = v-2a+d-2$ vrhova u Γ, što je parametar $\overline{c}$ komplementa. Slično dolazimo do parametra $\overline{d} = v-2a+c$. $\square$

Vidjeli smo da potpun graf i nepovezani jako regularni grafovi imaju dvije svojstvene vrijednosti (osim praznog grafa, koji ima samo jednu svojstvenu vrijednost 0). Svi ostali jako regularni grafovi mogu se karakterizirati kao regularni grafovi s točno tri svojstvene vrijednosti.

Teorem 2.12. *Neka je $\Gamma \neq K_v$ povezan a-regularan graf s matricom susjedstva A. Graf Γ je jako regularan s parametrima $SRG(v, a, c, d)$ ako i samo ako ima točno tri svojstvene vrijednosti $\theta_0 = a$, θ_1 i θ_2. U tom slučaju vrijedi $c = a + \theta_1 + \theta_2 + \theta_1\theta_2$ i $d = a + \theta_1\theta_2$.*

Za dokaz jednog smjera treba nam teorem o simultanoj dijagonalizaciji simetričnih matrica.

Teorem 2.13. *Neka su* $A_1, \ldots, A_k \in M_v(\mathbb{R})$ *kvadratne matrice reda* v. *Postoji ortonormirana baza od* $\mathbb{R}^v$ *sastavljena od njihovih zajedničkih svojstvenih vektora ako i samo ako su* $A_1, \ldots, A_k$ *simetrične i međusobno komutiraju* ($A_i \cdot A_j = A_j \cdot A_i$ *za sve* $i, j \in \{1, \ldots, k\}$).

Dokaz se može naći u [32, prop. 2.1.1]. Ako vektore te ortonormirane baze složimo u stupce ortogonalne matrice U, onda su matrice $U^{-1} \cdot A_i \cdot U = U^\tau \cdot A_i \cdot U$ dijagonalne, za $i = 1, \ldots, k$.

Dokaz teorema 2.12. ($\Longrightarrow$) Neka je Γ jako regularan s parametrima $SRG(v, a, c, d)$. Prema propoziciji 2.7 matrica susjedstva zadovoljava $A^2 = aI + cA + d(J - I - A)$. Neka je $\theta \neq a$ njezina svojstvena vrijednost. Matrice A, I, J su simetrične i međusobno komutiraju, pa po teoremu 2.13 postoji zajednički svojstveni vektor $x \in [j]^\perp$ pridružen svojstvenoj vrijednosti θ za A, 1 za I te 0 za J. Slijedi $\theta^2 x = ax + c\theta x + d(-x - \theta x)$, odnosno $(\theta^2 + (d-c)\theta + d - a)x = 0$. Zbog $x \neq 0$ vidimo da θ zadovoljava kvadratnu jednadžbu s pozitivnom diskriminantom $\theta^2 + (d-c)\theta + d - a = 0$, pa se podudara s jednim od njezina dva rješenja θ_1, θ_2. Iz Viéteovih formula slijedi $\theta_1\theta_2 = d - a$, $\theta_1 + \theta_2 = c - d$, odnosno $c = a + \theta_1 + \theta_2 + \theta_1\theta_2$ i $d = a + \theta_1\theta_2$. Oba rješenja kvadratne jednadžbe su svojstvene vrijednosti od A jer bi inače A imala samo dvije svojstvene vrijednosti i Γ bi bio oblika $m \cdot K_n$. □

Za dokaz drugog smjera teorema 2.12 trebaju nam još dva rezultata. Za kvadratne matrice A i B kažemo da su *permutacijski kongruentne* ako postoji permutacijska matrica P takva da je $A = P^\tau \cdot B \cdot P$. Za maricu A kažemo da je *reducibilna* ako je permutacijski kongruentna matrici oblika $\begin{bmatrix} B & C \\ 0 & D \end{bmatrix}$ za neke kvadratne matrice B i D (0 je nulmatrica). U suprotnom kažemo da je *ireducibilna.* Graf Γ je povezan ako i samo ako je njegova matrica susjedstva ireducibilna.

Teorem 2.14 (Perron-Frobenius)**.** *Neka je* A *kvadratna matrica reda* v *koja je ireducibilna i ima nenegativne unose (npr. matrica susjedstva povezanog grafa). Onda postoji jedinstveni broj* $a > 0$ *sa sljedećim svojstvima.*

1. *Broj* a *je svojstvena vrijednost matrice* A *algebarske kratnosti* 1.

2. *Ako je* λ *bilo koja druga svojstvena vrijednost od* A, *onda je* $|\lambda| \leq a$.

3. *Postoji svojstveni vektor s pozitivnim elementima pridružen svojstvenoj vrijednosti* a.

Dokaz se nalazi u [32, tm. 2.2.1]. Broj a iz Perron-Frobeniusova teorema naziva se *maksimalna svojstvnena vrijednost* od A. Naprimjer, ako je A matrica susjedstva a-regularnog povezanog grafa, onda je a njezina maksimalna svojstvena vrijednost, a $j = (1, \ldots, 1)$ je odgovarajući pozitivni svojstveni vektor. Perron-Frobeniusov teorem koristi se u dokazu sljedećeg teorema.

Teorem 2.15 (Hoffman)**.** *Neka je Γ graf s v vrhova i matricom susjedstva A. Postoji polinom $p \in \mathbb{Q}[x]$ takav da je $p(A) = J$ ako i samo ako je Γ regularan i povezan. Ako je Γ regularan stupnja a i ima (osim a) međusobno različite svojstvene vrijednosti $\beta_1, \ldots, \beta_t$, za polinom p možemo uzeti*

$$p(x) = \frac{v \cdot \prod_{i=1}^{t}(x - \beta_i)}{\prod_{i=1}^{t}(a - \beta_i)}.$$

Dokaz se nalazi u [124, tm. 2.4] i u [32, prop. 3.3.2]. Polinom $p(x)$ iz prethodnog teorema nazivamo *Hoffmanovim polinomom* grafa Γ.

Dokaz teorema 2.12. ($\Longleftarrow$) Neka je $\Gamma \neq K_v$ povezan a-regularan graf s matricom susjedstva A koja ima točno tri svojstvene vrijednosti $\theta_0 = a$, θ_1 i θ_2. Onda je njegov Hoffmanov polinom

$$p(x) = \frac{v(x - \theta_1)(x - \theta_2)}{(a - \theta_1)(a - \theta_2)}.$$

Vrijedi $p(A) = J$, tj.

$$(A - \theta_1 I)(A - \theta_2 I) = \frac{(a - \theta_1)(a - \theta_2)}{v} J.$$

To možemo zapisati kao

$$A^2 = (d - \theta_1\theta_2)I + (\theta_1 + \theta_2 + d)A + d(J - I - A)$$

za $d = (a - \theta_1)(a - \theta_2)/v$. Prema propoziciji 2.7 graf Γ je jako regularan s parametrima $SRG(v, a, c, d)$ za $d = a + \theta_1\theta_2$ i $c = \theta_1 + \theta_2 + d = a + \theta_1 + \theta_2 + \theta_1\theta_2$. $\square$

2.3 Spektralni dokaz teorema o blokovnom grafu

Koristeći se rezultatima iz prethodne cjeline možemo dokazati precizniju varijantu teorema 2.3.

Teorem 2.16. *Neka je $\mathcal{D}$ kvazisimetrični 2-(v, k, λ) dizajn s presječnim brojevima $x < y$ i neka je njegov blokovni graf $\Gamma(\mathcal{D})$ povezan. Onda je $\Gamma(\mathcal{D})$ jako regularan s parametrima $SRG(b, a, c, d)$ za $a = \frac{k(r-1)-x(b-1)}{y-x}$, $c = a+\theta_1+\theta_2+\theta_1\theta_2$ i $d = a+\theta_1\theta_2$. Pritom su $\theta_1 = \frac{r-\lambda-k+x}{y-x}$, $\theta_2 = \frac{x-k}{y-x}$ i $\{a, \theta_1, \theta_2\}$ je spektar od $\Gamma(\mathcal{D})$.*

Dokaz. Neka je N incidencijska matrica dizajna $\mathcal{D}$, a A matrica susjedstva pridruženog blokovnog grafa $\Gamma(\mathcal{D})$. Veza između te dvije matrice je $N^\tau \cdot N = kI + yA + x(J - I - A)$. Na mjestu (i, j) matrice $N^\tau \cdot N$ je veličina presjeka i-tog i j-tog bloka od $\mathcal{D}$. Za $i = j$ to je k, a u suprotnom je y ako su ta dva bloka susjedni u $\Gamma(\mathcal{D})$ i x inače.

Znamo da je $N \cdot N^\tau = (r - \lambda)I + \lambda J$, a to je $v \times v$ matrica koja ima r na dijagonali i λ izvan dijagonale. Prema lemi 2.8 ta matrica ima svojstvenu vrijednost $r + (v - 1)\lambda = rk$ kratnosti 1 i $r - \lambda$ kratnosti $v - 1$. Ako je α svojstvena vrijednost od $N \cdot N^\tau$ pridružena svojstvenom vektoru x, onda je α svojstvena vrijednost od $N^\tau \cdot N$ pridružena svojstvenom vektoru $N^\tau \cdot x$. Matrica $N^\tau \cdot N$ je dimenzija $b \times b$ i ranga v, pa uz to ima svojstvenu vrijednost 0 kratnosti $b - v$. Dakle, spektar od $N^\tau \cdot N$ je $\{rk, r - \lambda, 0\}$ kratnosti redom 1, $v - 1$ i $b - v$. Sad preko veze $(y - x)A = N^\tau \cdot N + (x - k)I - xJ$ možemo odrediti spektar od A: $\theta_0 = \frac{k(r-1)-x(b-1)}{y-x}$ kratnosti 1, $\theta_1 = \frac{r-\lambda-k+x}{y-x}$ kratnosti $v - 1$ i $\theta_2 = \frac{x-k}{y-x}$ kratnosti $b - v$.

Po teoremu 2.12 blokovni graf $\Gamma(\mathcal{D})$ je jako regularan s parametrima $SRG(b, a, c, d)$, $a = \theta_0$, $c = a + \theta_1 + \theta_2 + \theta_1\theta_2$ i $d = a + \theta_1\theta_2$. □

Korolar 2.17. *Ako postoji kvazisimetrični 2-(v, k, λ) dizajn s presječnim brojevima $x < y$, onda $y - x$ dijeli $k - x$ i $r - \lambda$.*

Dokaz. Iz izraza $\theta_1 = \frac{r-\lambda-k+x}{y-x}$ i $\theta_2 = \frac{x-k}{y-x}$ vidimo da su to racionalni brojevi. S druge strane, znamo da su θ_1, θ_2 nultočke normiranog polinoma $\theta^2 + (d - c)\theta + d - a$ s cjelobrojnim koeficijentima. Iz toga slijedi da θ_1, θ_2 moraju biti cijeli brojevi, što daje uvjete djeljivosti iskazane u korolaru. □

Ako su zadovoljeni uvjeti djeljivosti iz korolara, onda su i ostali parametri blokovnog grafa $\Gamma(\mathcal{D})$ cjelobrojni. Brojnik parametra a (stupnja regularnosti) je $k(r - 1) - x(b - 1) = k(r - b) + (k - x)(b - 1)$. Budući da je $k - x$ djeljiv s $y - x$, dovoljno je pokazati da $r - \lambda$ dijeli $k(r - b)$. Vrijedi $r - \lambda = \frac{\lambda(v-k)}{k-1}$ i $k(r - b) = \frac{\lambda(v-1)(k-v)}{k-1} = (r - \lambda)(1 - v)$, dakle $r - \lambda \mid k(r - b)$. Cjelobrojnost parametara c i d slijedi iz cjelobrojnosti a, θ_1, θ_2 i formula $c = a+\theta_1+\theta_2+\theta_1\theta_2$, $d = a + \theta_1\theta_2$.

Iz cjelobrojnosti izraza (5), (6) koje smo izveli u dokazu teorema 2.3 bilo bi teško izvesti uvjete djeljivosti iz korolara 2.17. Uvrštavanjem svojstvenih vrijednosti a, θ_1, θ_2 u formule za c i d iz teorema 2.16 dobijemo drugačije izraze nego u teoremu 2.3:

$$c = \frac{k^2 + y(r + x - \lambda) + k(r(-1 - x + y) + x(1 - x + y) - 3y + \lambda)}{(x - y)^2}, \tag{7}$$

$$d = \frac{(k(r + x - 1) - x)(y - x) + (k - x)(k - r - x + \lambda)}{(x - y)^2}. \tag{8}$$

Izjednačavanjem izraza (5) sa (7) i (6) sa (8) i sređivanjem dobili bismo još jedan nuždan uvjet na parametre kvazisimetričnog dizajna. Dokazat ćemo ga direktno u sljedećoj propoziciji.

Propozicija 2.18. *Ako postoji kvazisimetrični* 2-(v,k,λ) *dizajn s presječnim brojevima* $x < y$, *onda vrijedi*

$$k(r-1)(x+y-1) + xy(1-b) = k(k-1)(\lambda-1). \tag{9}$$

Dokaz. Neka je B_0 fiksni blok. Dvostrukim prebrojavanjem parova $\{(P,B) \mid B \neq B_0,\ P \in B \cap B_0\}$ dobijemo jednadžbu $ay + (b-1-a)x = k(r-1)$. Dvostrukim prebrojavanjem trojki $\{(P,Q,B) \mid B \neq B_0,\ P,Q \in B \cap B_0,\ P \neq Q\}$ dobijemo drugu jednadžbu $ay(y-1)+(b-1-a)x(x-1) = k(k-1)(\lambda-1)$. Množenjem prve jednadžbe s $x+y-1$ i oduzimanjem od druge slijedi (9). □

Iz uvjeta (9) vidimo da za zadane parametre (v,k,λ) iz jednog presječnog broja možemo jednoznačno odrediti drugi. Zanimljivo je pitanje određuju li već (v,k,λ) jednoznačno oba presječna broja (x,y)? Najmanji parametri za koje bi mogli postojati kvazisimetrični dizajni s različitim presječnim brojevima su $(v,k,\lambda) = (101,21,21)$. Presječni brojevi $(x,y) = (1,5)$ i $(3,6)$ zadovoljavaju sve nužne uvjete, ali nije poznato postoje li takvi kvazisimetrični dizajni. Pridruženi blokovni graf imao bi u prvom slučaju parametre $SRG(505, 420, 351, 340)$, a u drugom slučaju $SRG(505, 224, 108, 92)$. Prema Brouwerovoj tablici [30] otvorena je egzistencija i tih jako regularnih grafova.

U teoremu 2.16 imali smo pretpostavku da je blokovni graf $\Gamma(\mathcal{D})$ povezan, jer smo u dokazu koristili spektralnu karakterizaciju jako regularnih grafova (teorem 2.12). Ranije smo u teoremu 2.3 dokazali da je $\Gamma(\mathcal{D})$ jako regularan i bez pretpostavke o povezanosti. Primjer kvazisimetričnog dizajna s nepovezanim blokovnim grafom je simetrični 2-(v,k,λ) dizajn kojem svaki blok ponovimo $m \geq 2$ puta. To je kvazisimetrični 2-$(v,k,m\lambda)$ dizajn s presječnim brojevima $x = \lambda$, $y = k$. Pridruženi blokovni graf sastoji se od v disjunktnih kopija potpunog grafa K_m i ima parametre $SRG(mv, m-1, m-2, 0)$. Štoviše, to su jedini kvazisimetrični dizajni s nepovezanim blokovnim grafom.

Teorem 2.19. *Ako kvazisimetrični dizajn* $\mathcal{D}$ *ima kao blokovni graf disjunktnu uniju potpunih grafova* K_m, *onda se* $\mathcal{D}$ *sastoji od* m *kopija simetričnog dizajna.*

Dokaz. U dokazu teorema 2.16 vidjeli smo da blokovni graf kvazisimetričnog dizajna ima svojstvene vrijednosti $\theta_0 = \frac{k(r-1)-x(b-1)}{y-x}$ kratnosti 1, $\theta_1 = \frac{r-\lambda-k+x}{y-x}$ kratnosti $v-1$ i $\theta_2 = \frac{x-k}{y-x}$ kratnosti $b-v$ (za tu tvrdnju ne treba povezanost blokovnog grafa). Graf $\Gamma = n \cdot K_m$ ima $b = mn$ vrhova i svojstvene vrijednosti $m-1$ kratnosti n i -1 kratnosti $(m-1)n$ (vidi napomene iza leme 2.8). Iz toga slijedi da je $\theta_0 = \theta_1 = m-1$, $\theta_2 = -1$, $v = n$ i $y = k$. Prema propoziciji 1.20, $\mathcal{D}$ je višekratnik simetričnog $(v, k, \lambda/m)$ dizajna. $\square$

Iz teorema 2.19 i propozicija 2.9 i 2.10 slijedi

Korolar 2.20. *Kvazisimetrični dizajn s nepovezanim blokovnim grafom je višekratnik simetričnog dizajna.*

Teorem 2.19 dokazan je za $m = 2$ u članku [56], a od tamo potječe i matrični dokazi teorema 2.16. Goethals i Seidel [56] koriste drugačiju verziju matrice susjedstva, koja na dijagonali ima nule, a izvan dijagonale -1 ili 1 ovisno jesu li vrhovi susjedni ili nisu (tzv. Seidelovu matricu). Opći dokaz teorema 2.19 i korolara 2.20 dao je Neumaier [103] koristeći se pojmom regularnog skupa u jako regularnom grafu. Naš dokaz koristi spektar, a na sličan način dokazuje se idući rezultat.

Trokutni graf T_n $(n \geq 4)$ kao vrhove ima dvočlane podskupove od $\{1, \ldots, n\}$. Dva vrha spojena su bridom ako im je presjek neprazan. To je linijski graf potpunog grafa K_n, a komplement od T_5 je čuveni Petersenov graf. Graf T_n je jako regularan s parametrima $SRG(\binom{n}{2}, 2(n-2), n-2, 4)$.

Teorem 2.21. *Jedini kvazisimetrični dizajni kojima je blokovni graf T_n su trivijalni* 2-$(n, 2, 1)$ *dizajn i njegov komplement.*

Dokaz. Graf T_n ima svojstvene vrijednosti $2n-4$ kratnosti 1, $n-4$ kratnosti $n-1$ i -2 kratnosti $\binom{n}{2} - n$. Usporedbom sa spektrom $\{\theta_0^1, \theta_1^{v-1}, \theta_2^{b-v}\}$ vidimo da je $v = n$ i $b = \binom{n}{2}$. Prema korolaru 1.23 i teoremu 1.25 jedini netrivijalni kvazisimetrični dizajni s $b = \binom{v}{2}$ su derivirani Wittov 4-$(23, 7, 1)$ dizajn s $x = 1$, $y = 3$ i njegov komplement, ali njihov blokovni graf ima parametre $SRG(253, 140, 87, 65)$ i ne podudara se s T_{23}. Zato su mogući jedino trivijalni dizajni. $\square$

Idući cilj je karakterizirati kvazisimetrične dizajne kojima je blokovni graf potpuni multipartitni graf (komplement disjunktne unije potpunih grafova). Primjeri takvih dizajna su takozvani jako rastavljivi dizajni. Za dizajn $\mathcal{D}$ kažemo da je α-*rastavljiv* ako je blokove moguće particionirati u disjunktne klase $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_c$ tako da je svaka točka sadržana u α blokova iz svake klase. Brojanjem incidentnih parova vidimo da je $|\mathcal{B}_i|\, k = v\alpha$, tj. veličina svake klase je $m = |\mathcal{B}_i| = \frac{v\alpha}{k}$. Broj klasa c zadovoljava $b = mc$ i $r = \alpha c$. Nuždan uvjet za α-rastavljivost je djeljivost $k \mid v\alpha$, ili ekvivalentno $c \mid b$. Osim toga α-rastavljivi dizajni zadovoljavaju Boseovu nejednakost $b \geq v + c - 1$ (teorem 4.2).

Jaki α-rastav je onaj kod kojeg se svaka dva bloka iz iste klase sijeku u x točaka, a svaka dva bloka iz različitih klasa u y točaka. Jako rastavljivi dizajni očito su kvazisimetrični s presječnim brojevima x i y. Presječni brojevi mogu se izraziti kao $x = k - r + \lambda = k - n$, $y = k^2/v$ (propozicija 4.3), gdje je $n = r - \lambda$ red dizajna. Ako je $k < v$, iz toga slijedi da je $x < y$, pa je blokovni graf jako rastavljivog dizajna potpuni c-partitni graf $K_{m,\ldots,m}$ s parametrima $SRG(b, b - m, b - 2m, b - m)$. Pokazuje se da je α-rastav jak ako i samo ako se dostiže Boseova nejednakost, tj. vrijedi $b = v + c - 1$ (teorem 4.4). Sljedeći rezultat Majumdara [95] iz 1953. tiče se dizajna kod kojih se pojavljuje presječni broj $x = k - n$.

Teorem 2.22. *Neka je $\mathcal{D}$ jednostavni 2-(v, k, λ) dizajn reda $n = r - \lambda$. Za bilo koja dva bloka B_1, B_2 vrijedi $|B_1 \cap B_2| \geq k - n$. Jednakost se dostiže ako i samo ako za svaki blok $B \neq B_1, B_2$ vrijedi $|B \cap B_1| = |B \cap B_2|$.*

Dokaz. Označimo $z = |B_1 \cap B_2|$ i neka su ostali blokovi $B_3, \ldots, B_b$. Neka je $x_i = |B_i \cap (B_1 \setminus B_2)|$ i $y_i = |B_i \cap (B_2 \setminus B_1)|$, za $i = 3, \ldots, b$. Očito je $|B_i \cap B_1| = |B_i \cap (B_1 \cap B_2)| + x_i$ i $|B_i \cap B_2| = |B_i \cap (B_1 \cap B_2)| + y_i$, pa je $|B_i \cap B_1| = |B_i \cap B_2|$ ako i samo ako je $x_i = y_i$.

Dvostrukim prebrojavanjem trojki $\{(P, Q, B_i) \mid P, Q \in B_i \cap (B_1 \setminus B_2),\ i = 3, \ldots, b\}$ dobijemo

$$\sum_{i=3}^{b} x_i^2 = (k - z)(k - z - 1)(\lambda - 1) + (k - z)(r - 1). \tag{10}$$

Analogno slijedi

$$\sum_{i=3}^{b} y_i^2 = (k - z)(k - z - 1)(\lambda - 1) + (k - z)(r - 1), \tag{11}$$

a prebrojavanjem trojki $\{(P, Q, B_i) \mid P \in B_i \cap (B_1 \setminus B_2), Q \in B_i \cap (B_2 \setminus B_1),\ i = 3, \ldots, b\}$ dobijemo

$$\sum_{i=3}^{b} x_i y_i = (k - z)^2 \lambda. \tag{12}$$

Iz (10), (11) i (12) slijedi

$$\sum_{i=3}^{b} (x_i - y_i)^2 = 2(k - z)(z - (k - n)).$$

Budući da je lijeva strana nenegativna, slijedi $z \geq k - n$. Jednakost vrijedi ako i samo ako je $x_i = y_i$ za $i = 3, \ldots, b$. □

Beker i Haemers [13] dokazali su da su jako rastavljivi dizajni jedini kvazisimetrični dizajni kojima je blokovni graf potpuni multipartitni graf.

Teorem 2.23. *Za 2-dizajn $\mathcal{D}$ ekvivalentno je*

(*i*) *$\mathcal{D}$ je kvazisimetričan s presječnim brojem $x = k - n$,*

(*ii*) *$\mathcal{D}$ je jako rastavljiv,*

(*iii*) *$\mathcal{D}$ je kvazisimetričan i $\Gamma(\mathcal{D})$ je potpuni multipartitni graf.*

Dokaz. (*i*) $\Rightarrow$ (*ii*) Iz jednadžbe (9) slijedi da je veći presječni broj $y = k^2/v$. Na blokovima definiramo relaciju $B_1 \sim B_2$ ako je $B_1 = B_2$ ili $|B_1 \cap B_2| = k-n$. Iz teorema 2.22 slijedi da je $\sim$ relacija ekvivalencije, pa se $\mathcal{B}$ raspada na klase ekvivalencije $\mathcal{B}_1, \ldots, \mathcal{B}_c$. Veličina klasa je $m = m_x + 1 = \frac{y(b-1)-k(r-1)}{y-x} + 1 = \frac{n}{y-x}$ (vidi dokaz propozicije 1.20). Treba pokazati da je svaka točka sadržana u konstantnom broju α blokova iz svake klase. Neka je A_i incidencijska $v \times m$ matrica točaka i blokova iz klase $\mathcal{B}_i$. Vrijedi $A_i^\tau \cdot A_i = nI + (k-n)J_{m,m}$ i $A_i^\tau \cdot J_{v,m} = kJ_{m,m}$ ($J_{m,n}$ je $m \times n$ matrica popunjena jedinicama, a I jedinična matrica). Ako je j_m vektor dimenzija $m \times 1$ popunjen jedinicama, označimo $a = \left(A_i - \frac{k}{v} J_{v,m}\right) \cdot j_m$ (to je $v \times 1$ vektor). Vrijedi $a^\tau \cdot a = j_m^\tau \cdot \left(A_i^\tau - \frac{k}{v} J_{m,v}\right) \cdot \left(A_i - \frac{k}{v} J_{v,m}\right) \cdot j_m = j_m^\tau \cdot (nI + (x-y)J_{m,m}) \cdot j_m = m(n + m(x-y)) = 0$. Dakle, $a = 0$ i vrijedi $A_i \cdot j_m = \frac{k}{v} J_{v,m} \cdot j_m = \frac{km}{v} j_v$. To znači da je svaka točka sadržana u $\alpha = \frac{km}{v}$ blokova iz $\mathcal{B}_i$.

(*ii*) $\Rightarrow$ (*iii*) Već smo vidjeli da jako rastavljivi dizajn kvazisimetričan i blokovni graf mu je potpuni c-partitni graf $K_{m,\ldots,m}$.

(*iii*) $\Rightarrow$ (*i*) Neka su B_1 i B_2 dva bloka koja se sijeku u x točaka, tj. nesusjedni vrhovi u $\Gamma(\mathcal{D})$. Bilo koji treći blok iz iste klase siječe B_1 i B_2 u x točaka, a treći blok iz neke druge klase siječe B_1 i B_2 u y točaka. Zato se B_1 i B_2 po teoremu 2.22 sijeku u $k - n$ točaka, tj. $x = k - n$. $\square$

Neka su zadana $m - 2$ međusobno ortogonalna latinska kvadrata reda n (za definicije i osnovna svojstva vidi poglavlje 8 u [129]). Definiramo graf kojem su vrhovi n^2 parova iz Kartezijeva produkta $\{1, \ldots, n\}^2$. Dva vrha (i_1, j_1), (i_2, j_2) spojena su bridom ako je $i_1 = i_2$ ili je $j_1 = j_2$ ili se unosi na tim mjestima podudaraju u nekom od latinskih kvadrata. Svaki vrh je stupnja $a = m(n-1)$. Uzmimo dva susjedna vrha, recimo (i, j_1), (i, j_2) iz istog retka. Njihovi zajednički susjedi su preostalih $n-2$ vrhova u tom retku. Zatim, svaki latinski kvadrat $A = [a_{ij}]$ pridonosi zajedničkog susjeda u stupcu j_1 na kojem se nalazi element a_{ij_2} i zajedničkog susjeda u stupcu j_2 na kojem se nalazi element a_{ij_1}. Konačno, za svaki par latinskih kvadrata $A = [a_{ij}]$, $B = [b_{ij}]$ zbog ortogonalnosti postoji jedinstveno mjesto (i_3, j_3) takvo da je $a_{i_3 j_3} = a_{ij_1}$ i $b_{i_3 j_3} = b_{ij_2}$. To je još jedan zajednički susjed. Ukupan broj zajedničkih susjeda je $c = n-2+2(m-2)+(m-2)(m-3) = n+m^2-3m$. Isti broj dobije se za dva susjedna vrha u istom stupcu i za dva susjedna vrha u različitim recima i stupcima na kojima se unosi u nekom od kvadrata podudaraju. Ako uzmemo nesusjedne vrhove (i_1, j_1), (i_2, j_2), imamo dva zajednička susjeda (i_1, j_2) i (i_2, j_1). Svaki od latinskih kvadrata $A = [a_{ij}]$ pridonosi četiri zajednička susjeda: mjesta u retku i_1 i stupcu j_1 na kojima se nalazi element $a_{i_2 j_2}$ i mjesta u retku i_2 i stupcu j_2 na kojima se nalazi element $a_{i_1 j_1}$. Kao i prije, svaki par kvadrata pridonosi još jednog zajedničkog susjeda. Ukupan broj zajedničkih susjeda je $d = 2+4(m-2)+(m-2)(m-3) = m(m-1)$.

Time smo dokazali da je graf konstruiran od $m-2$ međusobno ortogonalna latinska kvadrata jako regularan s parametrima $SRG(n^2, m(n-1), n+m^2-3m, m(m-1))$. Svaki jako regularni graf s tim parametrima označavamo $L_m(n)$ (eng. *pseudo Latin square graph*). Goethals i Seidel [56, tm. 3.5] dokazali su da $L_2(n)$ i njegov komplement ne mogu biti blokovni grafovi niti jednog kvazisimetričnog dizajna. U radu [109] dokazano je da $L_3(n)$, $L_4(n)$ i njihovi komplementi ne mogu biti blokovni grafovi kvazisimetričnog dizajna, a u radu [110] za $L_5(n)$ i komplement. U radovima [109, 110] dokazano je i za mnoge druge jako regularne grafove da ne mogu biti blokovni grafovi kvazisimetričnog dizajna ili su klasificirani svi kvazisimetrični dizajni kojima je to blokovni graf. Coster i Haemers [47] proučavali su kvazisimetrične dizajne kojima je blokovni graf komplement trokutnog grafa $\overline{T}_n$. Napomenimo da jako regularni grafovi s istim parametrima ili čak izomorfni grafovi mogu biti blokovni grafovi različitih kvazisimetričnih dizajna. Naprimjer, grafovi s parametrima $SRG(63, 32, 16, 16)$ pridruženi su Steinerovim 2-$(28, 4, 1)$ dizajnima i kvazisimetričnim 2-$(28, 12, 11)$ dizajnima s $x = 4$, $y = 6$.

U ovom poglavlju mnoge rezultate dokazali smo s pomoću matrica i njihovih spektra. Pregled rezultata o dizajnima dokazanih matričnim tehnikama dan je u članku [122].

2.4 Dopustivi parametri kvazisimetričnih 2-dizajna

Neumaier [103] je sastavio tablicu dopustivih parametara kvazisimetričnih 2-dizajna s $v \leq 40$. Tablica sadrži 15 malih parametara za koje je egzistencija u tom trenutku bila otvorena, što je privuklo velik interes i potaknulo mnoge rezultate o kvazisimetričnim dizajnima. Obnovljene tablice objavljene su u [131] i [33], a obnovljene i proširene tablice za $v \leq 70$ u [35], [134] i [123]. Napravit ćemo sličnu tablicu za $v \leq 78$, zato da obuhvatimo i parametre $(78, 36, 30)$, $x = 15$, $y = 18$.

Zbog propozicije 1.6 i činjenice da je komplement kvazisimetričnog dizajna kvazisimetričan, parametar k možemo ograničiti s $3 \leq k \leq v/2$.

Izostavljamo dizajne s ponovljenim blokovima, pa iz korolara 1.19 dobivamo ocjenu $\lambda \leq \binom{k}{2}$. Uz te nejednakosti postoji 6575 trojki (v, k, λ) koje zadovoljavaju uvjete djeljivosti (korolar 1.4) i Fisherovu nejednakost (teorem 1.8). Među njima su 56 parametri simetričnih dizajna, koje smo izdvojili u tablicu 6.

Od preostalih 6519 trojki (v, k, λ), njih 1008 dostižu ocjenu $b = \binom{v}{2}$, odnosno $\lambda = \binom{k}{2}$. Zbog korolara 1.23 i teorema 1.25 možemo obrisati sve osim $(24, 7, 21)$, što su parametri deriviranog Wittova dizajna der $\mathcal{W}$ kao 2-dizajna. Za preostalih 5512 trojki tražimo moguće presječne brojeve x, y na sljedeći način. Za svaki $0 \leq x \leq \frac{k(r-1)}{b-1}$ odredimo odgovarajući y iz jednadžbe (9) (gornja granica za x je iz dokaza teorema 2.3). Ako je y cijeli broj i par (x, y) zadovoljava uvjete djeljivosti iz korolara 2.17, nadodamo ga na trojku (v, k, λ). Tako dobijemo 209 petorki (v, k, λ, x, y). Neke od njih možemo eliminirati na osnovi sljedećeg uvjeta Neumaiera [103].

Teorem 2.24. *Parametri kvazisimetričnog 2-dizajna $\mathcal{D}$ zadovoljavaju*

$$B(B - A) \leq AC, \tag{13}$$

gdje je $A = (v-1)(v-2)$, $B = r(k-1)(k-2)$, $C = rV(y-1)(y-2) + r(r-1-V)(x-1)(x-2)$ i $V = \frac{(k-1)(\lambda-1)-(r-1)(x-1)}{y-x}$. Jednakost se dostiže ako i samo ako je $\mathcal{D}$ 3-dizajn.

Dokaz. Neka je (P_0, B_0) incidentni par točka-blok. Broj V je broj blokova kroz P_0 koji sijeku B_0 u y točaka. Ako s V_x i V_y označimo broj blokova kroz P_0 koji sijeku B_0 u x, odnosno y točaka, vrijedi $V_x + V_y = r - 1$. Prebrojavanjem parova (P_1, B_1) točke $P_1 \neq P_0$ i bloka $B_1 \neq B_0$ takvih da su $P_0, P_1 \in B_0 \cap B_1$ dobijemo drugu jednadžbu $(x-1)V_x + (y-1)V_y = (k-1)(\lambda-1)$. Iz te dvije jednadžbe slijedi formula $V = V_y = \frac{(k-1)(\lambda-1)-(r-1)(x-1)}{y-x}$. Neumaier taj broj naziva *valencijom* regularnog skupa induciranog točkom P_0 u jako regularnom grafu $\Gamma(\mathcal{D})$.

Za dvije točke $Q, R \neq P_0$ označimo s λ_{QR} broj blokova koji sadrže P_0, Q i R. Sumiranjem po svim parovima (Q, R) dobijemo

$$\sum 1 = (v-1)(v-2) = A,$$

$$\sum \lambda_{QR} = r(k-1)(k-2) = B,$$

$$\sum \lambda_{QR}(\lambda_{QR} - 1) = rV_x(x-1)(x-2) + rV_y(y-1)(y-2) = C.$$

Prosječni λ_{QR} je $\overline{\lambda} = B/A$ i vrijedi $0 \leq \sum(\lambda_{QR} - \overline{\lambda})^2 = \frac{(B+C)A-B^2}{A} = \frac{AC-B(B-A)}{A}$. Zbog $A > 0$ to je ekvivalentno s nejednakosti (13), a jednakost se dostiže ako i samo ako je $\lambda_{QR} = \overline{\lambda}$ za sve parove (Q, R). Budući da je P_0 proizvoljna točka, to je ekvivalentno s tvrdnjom da je $\mathcal{D}$ 3-dizajn. $\square$

Uvjet iz prethodnog teorema eliminira 36 od 209 petorki (v, k, λ, x, y). Neumaier je u [103] uvjet (13) nazvao analogonom Kreinovih uvjeta.

Teorem 2.25 (Kreinovi uvjeti)**.** *Neka je Γ jako regularan graf s parametrima $SRG(v, a, c, d)$ i svojstvenim vrijednostima $\theta_1, \theta_2 \neq a$ takav da su Γ i njegov komplement $\overline{\Gamma}$ povezani. Onda vrijedi*

$$(\theta_1 + 1)(a + \theta_1 + 2\theta_1\theta_2) \leq (a + \theta_1)(\theta_2 + 1)^2,$$

$$(\theta_2 + 1)(a + \theta_2 + 2\theta_1\theta_2) \leq (a + \theta_2)(\theta_1 + 1)^2.$$

Dokaz se može naći u [41, tm. 2.26]. Iz teorema 2.16 možemo odrediti parametre i svojstvene vrijednosti blokovnog grafa pridruženog kvazisimetričnom dizajnu s parametrima (v, k, λ, x, y). Kreinovi uvjeti eliminiraju 34 grafova pridruženih našim petorkama i slabiji su od uvjeta (13). Naprimjer, petorka $(76, 10, 12, 0, 2)$ ne zadovoljava uvjet (13), ali blokovni graf bi imao parametre $SRG(760, 495, 334, 300)$ i svojstvene vrijednosti $\{\theta_1, \theta_2\} = \{-5, 39\}$ koji zadovoljavaju Kreinove uvjete. Calderbank [34] je izveo uvjet ekvivalentan Neumaierovom uvjetu (13). Definirao je sljedeće polinome:

$$\begin{aligned} f_3(v, k, x, y) = {} & (v-1)(v-2)(k-x)(k-y) - k(v-k)(v-2)(2k-x-y) \\ & +k(v-k)(k(v-k)-1), \end{aligned}$$

$$\begin{aligned} f_4(v, k, x, y) = {} & -(v-6)(v-3)(v-1)(k-x)(k-y)(2k-x-y) \\ & +(v-6)(v-3)k(v-k)(2k-x-y)^2 \\ & -2(v-3)k(v-k)(2k(v-k)-3v)(2k-x-y) \\ & +(v-3)(k(v-k)(3v+2)-6v(v-1))(k-x)(k-y) \\ & +k(v-k)(3k(v-k)(k(v-k)-2(v-1))+5v-3). \end{aligned}$$

Teorem 2.26. *Parametri kvazisimetričnog 2-dizajna $\mathcal{D}$ zadovoljavaju*

(i) $f_3(v, k, x, y) \geq 0$,

(ii) $f_4(v, k, x, y) \geq 0$.

Jednakost u (i) se dostiže ako i samo ako je $\mathcal{D}$ 3-dizajn.

Uvjet *(i)* ekvivalentan je uvjetu (13) i eliminira istih 36 od 209 petorki. Uvjet *(ii)* eliminira još dvije petorke $(28, 7, 16, 1, 3)$ i $(29, 7, 12, 1, 3)$, ali uključit ćemo ih u tablicu dopustivih parametara zbog usporedivosti s tablicom iz [123]. Neke od 173 dopustivih petorki izdvojit ćemo u druge tablice, po uzoru na [103, 131, 33, 35, 134, 123]. Tablice iz tih članka ne sadrže parametre jako rastavljivih dizajna, Steinerovih 2-dizajna i reziduala dvoravnina. Od naših 173 petorki, 29 su parametri jako rastavljivih dizajna; prepoznajemo ih npr. po uvjetu $x = k - n$ iz teorema 2.23. Izdvojili smo ih u tablicu 7. Od preostalih 144 petorki, 41 odgovaraju Steinerovim 2-dizajnima, tj. imaju $\lambda = 1$. Njih smo izdvojili u tablicu 9. Primijetimo da među njima nema konačnih projektivnih ravnina, koje su simetrični dizajni i već smo ih izdvojili u tablicu 6, niti konačnih afinih ravnina, koje su jako rastavljive i izdvojili smo ih u tablicu 7. Tablica 9 sadrži samo Steinerove 2-dizajne s $v > k^2$. Konačno, od preostalih 103 petorki 9 odgovara rezidualima dvoravnina (prepoznajemo ih po $\lambda = 2$). Izdvojili smo ih u tablicu 10. Ostalo je 94 dopustivih petorki (v, k, λ, x, y) koje navodimo u tablici 1.

Osim parametara (v, k, λ, x, y) u tablici navodimo parametar r i parametre $SRG(b, a, c, d)$ pridruženog blokovnog grafa. U stupcu 'Nqsd' navodimo broj međusobno neizomorfnih kvazisimetričnih dizajna ili ocjenu za taj broj, a u stupcu 'Nsrg' broj odgovarajućih jako regularnih grafova. U stupcu 'Ref.' je referenca za broj Nqsd. Brojevi Nsrg preuzeti su iz Brouwerove tablice [30]. Konačno, u stupcu 'Napomene' navodimo familije kvazisimetričnih dizajna kojima pripadaju parametri, opis dizajna ili razlog zašto ne postoje.

Br.	v	k	λ	x	y	r	b	a	c	d	Nqsd	Nsrg	Ref.	Napomene
1	19	7	7	1	3	21	57	42	31	30	0	0	[103]	Teorem 3.35
2	19	9	16	3	5	36	76	45	28	24	0	0	[33]	
3	20	8	14	2	4	38	95	54	33	27	0	0	[36]	
4	20	10	18	4	6	38	76	35	18	14	0	0	[36]	
5	21	6	4	0	2	16	56	45	36	36	1	1	[131]	res(der$^2\mathcal{W}$)
6	21	7	12	1	3	40	120	77	52	44	1	1	[131]	res^2(der$\mathcal{W}$)
7	21	8	14	2	4	40	105	52	29	22	0	?	[33]	Teorem 3.35
8	21	9	12	3	5	30	70	27	12	9	0	≥1	[33]	Teorem 3.35
9	22	6	5	0	2	21	77	60	47	45	1	1	[145]	der$^2\mathcal{W}$
10	22	7	16	1	3	56	176	105	68	54	1	1	[131]	res(der$\mathcal{W}$)
11	22	8	12	2	4	36	99	42	21	15	0	?	[33]	
12	23	7	21	1	3	77	253	140	87	65	1	≥1	[145]	der$\mathcal{W}$
13	24	8	7	2	4	23	69	20	7	5	0	?	[31]	
14	28	7	16	1	3	72	288	105	52	30	0	?	[131]	Teorem 2.26(ii)
15	28	12	11	4	6	27	63	32	16	16	≥58891	≥1	[89]	QSDP
16	29	7	12	1	3	56	232	77	36	20	0	?	[131]	Teorem 2.26(ii)
17	31	7	7	1	3	35	155	42	17	9	5	≥1	[132]	$PG_2(4,2)$
18	33	9	6	1	3	24	88	60	41	40	0	?	[33]	
19	33	15	35	6	9	80	176	45	18	9	?	≥1		
20	35	7	3	1	3	17	85	14	3	2	0	?	[33]	Teorem 3.35

Tablica 1: Dopustivi parametri kvazisimetričnih dizajna.

Br.	v	k	λ	x	y	r	b	a	c	d	Nqsd	Nsrg	Ref.	Napomene
21	35	14	13	5	8	34	85	14	3	2	?	?		
22	36	16	12	6	8	28	63	30	13	15	≥522079	≥1	[89]	QSDP
23	37	9	8	1	3	36	148	84	50	44	?	?		
24	39	12	22	3	6	76	247	54	21	9	?	≥1		
25	41	9	9	1	3	45	205	96	50	40	?	?		
26	41	17	34	5	8	85	205	136	93	84	0	?	[35]	Teorem 3.36
27	41	20	57	8	11	120	246	140	85	72	?	?		
28	42	18	51	6	9	123	287	160	96	80	?	?		
29	42	21	60	9	12	123	246	119	64	51	?	?		
30	43	16	40	4	7	112	301	192	128	112	?	?		
31	43	18	51	6	9	126	301	150	83	66	0	?	[35]	Teorem 3.36
32	45	9	8	1	3	44	220	84	38	28	≥1	≥1	[132]	der^3 5-$(48, 12, 8)$
33	45	15	42	3	6	132	396	260	178	156	?	?		
34	45	18	34	6	9	88	220	84	38	28	?	≥1		
35	45	21	70	9	13	154	330	63	24	9	?	≥1		
36	46	16	8	4	6	24	69	48	32	36	?	?		
37	46	16	72	4	7	216	621	320	184	144	?	?		
38	49	9	6	1	3	36	196	60	23	16	≥49	≥1	[27]	
39	49	13	13	1	4	52	196	156	125	120	?	?		
40	49	16	45	4	7	144	441	176	85	60	?	?		
41	51	15	7	3	5	25	85	54	33	36	0	?	[33]	Teorem 3.35
42	51	21	14	6	9	35	85	70	57	60	0	?	[35]	Teorem 3.36
43	52	16	20	4	7	68	221	64	24	16	?	≥1		
44	55	15	7	3	5	27	99	48	22	24	?	≥1		
45	55	15	63	3	6	243	891	320	148	96	?	?		
46	55	16	40	4	8	144	495	78	29	9	?	≥1		
47	56	12	9	0	3	45	210	176	148	144	?	?		
48	56	15	42	3	6	165	616	205	90	57	?	?		
49	56	16	6	4	6	22	77	16	0	4	≥2	1	[102]	res$(78, 22, 6)$
50	56	16	18	4	8	66	231	30	9	3	≥3	≥1	[89]	
51	56	20	19	5	8	55	154	105	72	70	?	?		
52	56	21	24	6	9	66	176	105	64	60	?	?		
53	57	9	3	1	3	21	133	24	5	4	?	?		
54	57	12	11	0	3	56	266	220	183	176	0	?	[82]	
55	57	15	30	3	6	120	456	140	58	36	?	?		
56	57	21	10	7	9	28	76	21	2	7	0	0	[59]	
57	57	21	25	6	9	70	190	105	60	55	?	?		
58	57	24	23	9	12	56	133	44	15	14	0	?	[35]	Teorem 3.36
59	57	27	117	12	17	252	532	81	30	9	0	≥1	[35]	Teorem 3.36
60	60	15	14	3	6	59	236	55	18	11	?	?		

Tablica 1: Dopustivi parametri kvazisimetričnih dizajna (nastavak).

Br.	v	k	λ	x	y	r	b	a	c	d	Nqsd	Nsrg	Ref.	Napomene
61	60	30	58	14	18	118	236	55	18	11	0	?	[36]	
62	61	21	21	6	9	63	183	70	29	25	?	≥1		
63	61	25	160	9	13	400	976	300	128	76	?	?		
64	63	15	35	3	7	155	651	90	33	9	≥1	≥1		$PG_3(5,2)$
65	63	18	17	3	6	62	217	150	105	100	?	?		
66	63	24	92	8	12	248	651	182	73	42	?	?		
67	64	24	46	8	12	126	336	80	28	16	≥28826	≥1	[79]	BH
68	65	20	19	5	8	64	208	75	30	25	?	≥1		
69	66	30	29	12	15	65	143	72	36	36	≥10000	≥1	[89]	Teorem 3.15
70	69	18	30	3	6	120	460	255	150	130	?	?		
71	69	33	176	15	21	374	782	99	36	9	0	≥1	[33]	Teorem 3.35
72	70	10	6	0	2	46	322	225	160	150	?	?		
73	70	30	58	10	14	138	322	225	160	150	?	?		
74	71	14	39	2	5	210	1065	266	103	54	?	?		
75	71	31	93	11	15	217	497	310	201	180	?	?		
76	71	35	136	15	19	280	568	315	186	160	?	?		
77	72	18	34	3	6	142	568	279	150	124	?	?		
78	72	32	124	12	16	284	639	350	205	175	?	?		
79	72	36	140	16	20	284	568	279	150	124	?	?		
80	73	10	15	1	4	120	876	105	38	9	?	≥1		
81	73	28	126	10	16	336	876	105	38	9	?	≥1		
82	73	32	124	12	16	288	657	328	179	148	?	?		
83	75	27	117	9	15	333	925	108	39	9	?	≥1		
84	76	16	12	1	4	60	285	220	171	165	?	?		
85	76	26	52	6	10	156	456	325	236	220	?	?		
86	76	30	116	10	14	300	760	345	176	140	?	?		
87	76	36	21	16	18	45	95	40	12	20	0	0	[6]	
88	76	36	42	16	20	90	190	45	12	10	?	?		
89	76	36	105	16	21	225	475	96	32	16	?	≥1		
90	77	33	24	12	15	57	133	88	57	60	?	?		
91	78	26	100	6	10	308	924	611	418	376	?	?		
92	78	28	216	8	12	616	1716	875	490	400	?			
93	78	33	64	13	18	154	364	66	20	10		?		
94	78	36	30	15	18	66	143	70	33	35	≥10000	≥1	[89]	Teorem 3.15

Tablica 1: Dopustivi parametri kvazisimetričnih dizajna (nastavak).

Dizajn broj 54 ima parametre 2-$(57, 12, 11)$, $x = 0$, $y = 3$. Oni dostižu jednakost u (13) i zato je to 3-$(57, 12, 2)$ dizajn koji je proširenje dvoravnine 2-$(56, 11, 2)$. Takvo proširenje ne postoji kao posljedica klasifikacije [82]. Nepostojanje dizajna broj 54 i postojanje dizajna broj 50 su jedini novi rezultati o egzistenciji kvazisimetričnih dizajna s $v \leq 70$ u odnosu na tablicu [123].

Konstrukcije dizajna navedenih u tablici 1 opisat ćemo u poglavlju 4 o familijama kvazisimetričnih dizajna. Nekoliko dizajna iz tablice dobiveni su sporadičnim konstrukcijama. Dizajn broj 32 konstruiran je u [132] kao tri puta derivirani 5-$(48, 12, 8)$ dizajn s presječnim brojevima 0, 2, 4 i 6. Dizajni 38 konstruirani su u [67] od samodualnih $[50, 25, 10]$ kodova (vidi također [27]). Dizajni 56 konstruirani su u [133, 102] kao reziduali simetričnih $(78, 22, 6)$ dizajna; reći ćemo više o toj konstrukciji u cjelini 4.4. Konačno, dizajni 50 konstruirani su u [89] Kramer-Mesnerovom metodom uz pretpostavku da imaju određenu grupu automorfizama.

3 Kodovi

3.1 Ocjene za parametre kodova

Neka je Q skup od q elemenata koji zovemo *abecedom*. *Kod* s parametrima (n, M, d, q) je skup uređenih n-torki $C \subseteq Q^n$. Pritom je $M = |C|$ *veličina* koda, a $d = \min\{\, d(x, y) \mid x, y \in C, x \neq y \,\}$ je *minimalna udaljenost* kodnih riječi u Hammingovoj metrici $d(x, y) = |\{\, i \mid x_i \neq y_i \,\}|$. Parametar n nazivamo *duljinom* koda.

Ako je $Q = \mathbb{F}_q$ konačno polje i $C \leq \mathbb{F}_q^n$ potprostor vektorskog prostora, govorimo o *linearnom kodu*. Za linearne kodove minimalna udaljenost jednaka je minimalnoj težini $w(C) = \min\{\, w(x) \mid x \in C, x \neq 0 \,\}$, gdje je $w(x) = |\{\, i \mid x_i \neq 0 \,\}|$. Parametre linearnog koda zapisujemo kao $[n, m, d, q]$ za $m = \dim C$. *Generirajuća matrica* je $m \times n$ matrica kojoj reci čine bazu od C. *Produkt* vektora $x, y \in Q^n$ je $x \cdot y = \sum_{i=1}^{n} x_i y_i$. Vektori su *ortogonalni* ako je $x \cdot y = 0$. *Dualni kod* od $C \leq Q^n$ je $C^\perp = \{x \in Q^n \mid x \cdot y = 0,\, \forall y \in C\}$.

Propozicija 3.1. *Ako je* $\dim C = m$*, onda je* $C^\perp$ *linearni kod dimenzije* $n - m$*. Nadalje, vrijedi* $(C^\perp)^\perp = C$*.*

Matrica provjere parnosti od C je generirajuća matrica od $C^\perp$. Neka je to $(n - m) \times n$ matrica P. Vektor $x \in Q^n$ pripada kodu C ako i samo ako je $x \cdot P^\tau = 0$. Iz matrice provjere parnosti možemo odrediti i minimalnu težinu od C.

Teorem 3.2. *Neka je C linearni kod s matricom provjere parnosti P. Minimalna težina od C jednaka je minimalnom broju linearno zavisnih stupaca od P. Točnije, vrijedi $w(C) = d$ ako i samo ako u P postoji d linearno zavisnih stupaca, a bilo kojih $d - 1$ ili manje stupaca su linearno nezavisni.*

U teoriji kodiranja cilj je konstruirati kodove što manje duljine n (zbog brzine prijenosa), što veće veličine M ili dimenzije m (zbog manje redundancije) i što veće minimalne udaljenosti d (zbog mogućnosti otkrivanja i ispravljanja više pogrešaka). Ocjene za parametre kodova predstavljaju ograničenja na te zahtjeve. Kodovi koji dostižu neku od ocjena obično su povezani sa zanimljivim kombinatoričkim strukturama.

Propozicija 3.3 (Singletonova ocjena)**.** *Ako postoji (n, M, d, q) kod, onda vrijedi $M \leq q^{n-d+1}$.*

Kodove koji dostižu Singletonovu ocjenu nazivamo *MDS kodovima* (prema eng. *maximum distance separable*). Povezani su s ortogonalnim latinskim kvadratima.

Propozicija 3.4 (Ocjena pakiranja kugli)**.** *Ako postoji* (n, M, d, q) *kod i ako je* $e = \lfloor \frac{d-1}{2} \rfloor$*, onda vrijedi* $M \leq \frac{q^n}{\sum_{i=0}^{e} \binom{n}{i} (q-1)^i}$.

Kodove koji dostižu ocjenu pakiranja kugli nazivamo *savršenim kodovima.* Za vektor $x \in (\mathbb{F}_q)^n$ njegov *nosač* je skup $\{i \mid x_i \neq 0\}$. Nosači vektora minimalne težine u savršenom linearnom $[n, m, d, q]$ kodu s $d = 2e + 1$ čine dizajn s parametrima $(e + 1)$-$(n, d, (q - 1)^e)$.

Propozicija 3.5 (Plotkinova ocjena)**.** *Ako postoji binarni* $(n, M, d, 2)$ *kod s* $2d > n$*, onda vrijedi* $M \leq 2 \left\lfloor \dfrac{d}{2d - n} \right\rfloor$.

Kodovi koji dostižu Plotkinovu ocjenu povezani su s Hadamardovim matricama. Uvod u teoriju kodiranja i dokazi navedenih tvrdnji prikazani su u 9. poglavlju skripte [129]. Ovdje ćemo dokazati još jednu ocjenu i karakterizirati kodove koji je dostižu s pomoću kvazisimetričnih dizajna. *Komplement* binarnog vektora $x \in \{0, 1\}^n$ je vektor $\overline{x}$ dobiven zamjenom nula i jedinica. Za kod $C \subseteq \{0, 1\}^n$ kažemo da je *samokomplementaran* ako iz $x \in C$ slijedi $\overline{x} \in C$.

Teorem 3.6 (Grey-Rankinova ocjena)**.** *Ako postoji samokomplementarni binarni* $(n, M, d, 2)$ *kod s* $n - \sqrt{n} < 2d < n + \sqrt{n}$*, onda vrijedi*

$$M \leq \frac{8d(n - d)}{n - (n - 2d)^2}.$$

Jednakost se dostiže ako i samo ako su jedine udaljenosti između kodnih riječi 0*,* d*,* $n - d$ *i* n *te projekcija koda* C *na bilo koje dvije koordinate sadrži svaki od parova* 00*,* 01*,* 10 *i* 11 *jednako mnogo puta.*

Dokaz. Neka je $C' \subseteq C$ podkod koji se sastoji od po jedne riječi za svaki komplementarni par $x, \overline{x} \in C$. Onda je $|C'| = M/2$ i udaljenost kodnih riječi iz C' je između d i $n - d$ (uključujući granice). Ocijenit ćemo na dva načina broj uređenih parova $(\{x, y\}, \{i, j\})$, pri čemu su $x, y \in C'$, $1 \leq i, j \leq n$, $x_i = x_j$, $y_i \neq y_j$ ili $x_i \neq x_j$, $y_i = y_j$. Neka je N broj takvih parova. Ako prvo biramo kodne riječi $\{x, y\}$ i ako je $t = d(x, y)$, onda koordinate $\{i, j\}$ na kojima se x slaže, a y ne slaže, ili obrnuto, možemo izabrati na $t(n - t)$ načina. To se lako vidi za $x = 0$, a opći slučaj vrijedi jer se broj takvih koordinata ne mijenja translacijom, tj. kodne riječi $\{x, y\}$ možemo zamijeniti s $\{x + x, y + x\} = \{0, x + y\}$. Vrijedi $t(n - t) \geq d(n - d)$ jer kvadratna funkcija $t \to t(n-t)$ poprima minimume na rubovima intervala $[d, n-d]$, pa je $N \geq \binom{M/2}{2} d(n - d)$.

S druge strane, ako prvo izaberemo koordinate $\{i, j\}$, onda kodne riječi $\{x, y\}$ možemo izabrati najviše na $(M/4)^2$ načina. Označimo s $a_{00} = |\{x \in C' \mid x_i = 0, x_j = 0\}|$ i analogno a_{01}, a_{10}, a_{11}. Onda je broj izbora $(a_{00} + a_{11})(a_{10} + a_{01})$, a ta funkcija poprima maksimum uz uvjet $a_{00} + a_{01} + a_{10} + a_{11} = M/2$ kad je $a_{00} + a_{11} = a_{01} + a_{10} = M/4$. Dakle, $N \leq \binom{n}{2}(M/4)^2$.

Dokazali smo da je $\binom{M/2}{2}d(n-d) \leq N \leq \binom{n}{2}(M/4)^2$. Sređivanjem dobivamo $[n - (n-2d)^2] \cdot M \leq 8d(n-d)$. Ako je izraz u uglatoj zagradi pozitivan, što je ekvivalentno s $n - \sqrt{n} < 2d < n + \sqrt{n}$, možemo podijeliti i dobiti Grey-Rankinovu ocjenu. Jednakost vrijedi ako i samo ako se obje ocjene za N dostižu. Prva jednakost $N = \binom{M/2}{2}d(n-d)$ znači da udaljenosti različitih vektora iz C' mogu biti samo d ili $n-d$, tj. udaljenosti u C su 0, d, $n-d$ i n. Druga jednakost $N = \binom{M/2}{2}d(n-d)$ znači da je $a_{00} + a_{11} = a_{01} + a_{10} = M/4$ za proizvoljne koordinate $\{i, j\}$. To je broj pojavljivanja parova 00, 01, 10 i 11 u projekciji koda C na te koordinate. $\square$

Rankin je u [116, 117] dokazao rezultate o pakiranju n-dimenzionalnih sfernih odsječaka i minimumu pozitivno definitnih kvadratnih formi, iz kojih je Grey [57] izveo ocjenu za parametre kodova. Gornji dokaz je iz [100], gdje je pripisan R. Wilsonu. Svojstvo kodova koji dostižu Grey-Rankinovu ocjenu da projekcija na bilo koje dvije koordinate sadrži svaki od parova 00, 01, 10 i 11 jednako mnogo puta je definicijsko svojstvo strukture koja se na engleskom naziva *orthogonal array* (OA).

Definicija 3.7. $\mathrm{OA}(M, n, q, t)$ *je $M \times n$ matrica popunjena elementima iz q-članog skupa Q takva da se u bilo kojih t stupaca svaki od q^t mogućih vektora iz Q^t javlja jednako mnogo puta.*

Broj pojavljivanja svakog vektora iz Q^t očito je $\lambda = M/q^t$. Parametar t nazivamo *jakost* OA i ima sličnu ulogu kao parametar t dizajna. Svaki OA jakosti t ujedno je OA jakosti $s \leq t$. Ako kao retke matrice uzmemo riječi koda koji dostiže Grey-Rankinovu ocjenu, dobivamo $\mathrm{OA}(M, n, 2, 2)$. Općenito OA može imati ponovljene retke, ali kad ga konstruiramo uzimajući riječi nekog koda onda se reci ne ponavljaju. Takve OA nazivamo *jednostavnim.* Ako je $Q = \mathbb{F}_q$ konačno polje i reci OA čine potprostor od Q^n, kažemo da je OA *linearan.* Gary McGuire [100] karakterizirao je kodove koji dostižu Grey-Rankinovu ocjenu.

Teorem 3.8. *Neka n i d zadovoljavaju $n - \sqrt{n} < 2d < n$.*

(i) Ako je n neparan, samokomplementarni kod koji dostiže Grey-Rankinovu ocjenu postoji ako i samo ako postoji Hadamardova matrica reda $n+1$.

(*ii*) *Ako je n paran, samokomplementarni kod koji dostiže Grey-Rankinovu ocjenu postoji ako i samo ako postoji kvazisimetrični 2-(n,d,λ) dizajn s presječnim brojevima $x = \dfrac{3d-n}{2}$, $y = \dfrac{d}{2}$, za $\lambda = \dfrac{d(d-1)}{n-(n-2d)^2}$.*

Vidjeli smo da riječi koda koji dostiže Grey-Rankinovu ocjenu čine OA jakosti 2. Važan korak u dokazu teorema 3.8 je pokazati da čine OA jakosti 3. Za dokaz trebamo objasniti vezu između kodova i OA, što je najlakše u linearnom slučaju.

Teorem 3.9. *Neka je C linearni $[n,m,d,q]$ kod i $d^\perp$ minimalna težina dualnog koda $C^\perp$. Onda vektori u C čine $OA(q^m,n,q,d^\perp-1)$. Obrnuto, ako vektori u C čine $OA(q^m,n,q,t)$, onda je minimalna težina dualnog koda $d^\perp \geq t+1$. Ako je taj OA jakosti t i nije jakosti $t+1$, minimalna težina dualnog koda je točno $d^\perp = t+1$.*

Dokaz se može naći u [128, tm. 10.17 na str. 231]. Tvrdnja da kodne riječi čine OA jakosti t slijedi iz svojstva da su bilo kojih t stupaca generirajuće matrice linearno nezavisni. To je zbog $(C^\perp)^\perp = C$ i teorema 3.2 ekvivalentno s $d^\perp \geq t+1$. Međutim, kodovi koji dostižu Grey-Rankinovu ocjenu ne moraju biti linearni, pa trebamo općenitiju verziju teorema 3.9, koja vrijedi i za nelinearne kodove.

Važnu ulogu u teoriji kodiranja igra takozvani *težinski polinom.* Neka je $C \leq Q^n$ linearni kod i $A_i = |\{x \in C \mid w(x) = i\}|$ broj kodnih riječi težine i. Definiramo $W_C(x,y) = \sum_{i=0}^n A_i x^{n-i} y^i$, homogeni polinom stupnja n u varijablama x i y kojem su koeficijenti distribucija težina $(A_0,\ldots,A_n)$ koda C. Primijetimo da težinski polinom možemo zapisati i u obliku $W_C(x,y) = \sum_{x\in C} x^{n-w(x)} y^{w(x)}$. MacWilliams je izveo vezu između težinskog polinoma koda C i dualnog koda $C^\perp$.

Teorem 3.10 (MacWilliamsov identitet)**.** *Za linearni kod $C \leq Q^n$ veličine M i njegov dual $C^\perp$ vrijedi*

$$W_{C^\perp}(x,y) = \frac{1}{M} W_C(x+(q-1)y, x-y).$$

Dokaz u binarnom slučaju nalazi se u [93, tm. 5.2.1 na str. 127]. Ako distribuciju težina u dualnom kodu označimo $(A'_0,\ldots,A'_n)$, raspisivanjem desne strane MacWilliamsova identiteta dobijemo vezu

$$A'_i = \frac{1}{M} \sum_{j=0}^{n} A_j P_i(j), \tag{14}$$

gdje su $P_i(x) = \sum_{r=0}^{i} (-1)^r (q-1)^{i-r} \binom{x}{r} \binom{n-x}{i-r}$ *Kravčukovi polinomi*, jedna familija diskretnih ortogonalnih polinoma. Minimalna težina koda C je $d = \min\{\, i \in \mathbb{N} \mid A_i > 0 \,\}$, a dualnog koda $d^\perp = \min\{\, i \in \mathbb{N} \mid A_i' > 0 \,\}$. Za nelinearni kod C i vektor $x \in C$ definiramo $A_i(x) = |\,\{\, y \in C \mid d(x,y) = i \,\}\,|$ te $A_i = \frac{1}{M} \sum_{x \in C} A_i(x)$. To su nenegativni racionalni brojevi koji na isti način određuju minimalnu udaljenost $d = \min\{\, i \in \mathbb{N} \mid A_i > 0 \,\}$ nelinearnog koda. U linearnom slučaju za svaku kodnu riječ $x \in C$ vrijedi $A_i(x) = A_i$, $i = 0, \ldots, n$. MacWilliamsonov identitet ne vrijedi za nelinearne kodove, ali nam formule (14) omogućuju da distribuciji prosječnih udaljenosti $(A_0, \ldots, A_n)$ pridružimo niz $(A_0', \ldots, A_n')$ koji nazivamo *MacWilliamsonovom transformacijom.* Philippe Delsarte je u svojoj disertaciji [48] dokazao da su komponente pridruženog vektora nenegativne.

Teorem 3.11. *Za opći (n, M, q, d) kod s distribucijom prosječnih udaljenosti $(A_0, \ldots, A_n)$, brojevi definirani formulama (14) zadovoljavaju $A_i' \geq 0$, $i = 0, \ldots, n$.*

Iz ovog teorema slijedi *ocjena linearnog programiranja*, još jedan nuždan uvjet za egzistenciju OA i kodova (vidi [65, tm. 4.15 na str. 73]). Sad možemo definirati formalnu dualnu težinu $d^\perp = \min\{\, i \in \mathbb{N} \mid A_i' > 0 \,\}$ općeg koda preko MacWilliamsonove transformacije distribucije prosječnih udaljenosti. Za linearne kodove formalna dualna težina podudara se s minimalnom težinom od $C^\perp$. Delsarte [49] je dokazao da i u općem slučaju ima istu ulogu kao u teoremu 3.9.

Teorem 3.12 (Delsarte)**.** *Neka je C opći (n, M, d, q) kod i $d^\perp$ njegova formalna dualna težina. Onda vektori u C čine $OA(q^m, n, q, d^\perp - 1)$. Obrnuto, ako vektori u C čine $OA(q^m, n, q, t)$, onda formalna dualna težina zadovoljava $d^\perp \geq t+1$. Ako je taj OA jakosti t i nije jakosti $t+1$, formalna dualna težina je točno $d^\perp = t+1$.*

Dokaz za $q = 2$ nalazi se u [65, tm. 4.9 na str. 70]. Slijedi dokaz da riječi koda koji dostiže Grey-Rankinovu ocjenu čine OA jakosti 3.

Lema 3.13. *Neka je C samokomplementarni kod s parametrima $(n, M, d, 2)$ koji dostiže Grey-Rankinovu ocjenu. Kodne riječi od C čine $OA(M, n, 2, 3)$.*

Dokaz. Neka je $x \in C$ čvrsti vektor. Promotrimo kod $x + C = \{\, x + y \mid y \in C \,\}$. Distribucija težina u kodu $x + C$ odgovara distribuciji udaljenosti od vektora x u kodu C. Kod $x + C$ ima istu minimalnu udaljenost kao C (zbog $d(x+y_1, x+y_2) = d(y_1, y_2)$) i također je samokomplementaran (zbog $\overline{x+y} = x + \overline{y}$). Očito je $0 \in x + C$, pa zbog samokomplementarnosti $x + C$ sadrži i vektor $j = (1, \ldots, 1)$. Kod $x + C$ ima iste parametre kao C i također dostiže Grey-Rankinovu ocjenu. Zbog teorema 3.6 jedine udaljenosti u $x + C$ su 0, d, $n - d$ i n, a zbog $0 \in x + C$ to su i jedine težine kodnih riječi. Iz samokomplementarnosti slijedi da je broj vektora težine d jednak broju vektora težine $n - d$. Time smo odredili distribuciju težina u $x + C$: $A_0 = A_n = 1$, $A_d = A_{n-d} = \frac{M-2}{2}$ te $A_i = 0$ za sve ostale i. U kodu C vrijedi $A_i(x) = A_i$ za svaki i, tj. distribucija udaljenosti od vektora $x \in C$ ne ovisi o izboru tog vektora (kao i u linearnim kodovima).

Odredimo sada MacWilliamsonovu transformaciju niza $(A_0, \ldots, A_n)$, definiranu s $M \cdot A_i' = \sum_{j=0}^{n} A_j P_i(j)$ gdje je $P_i(x) = \sum_{r=0}^{i} (-1)^r \binom{x}{r}\binom{n-x}{i-r}$ binarni Kravčukov polinom stupnja i. Zbog svojstva $P_i(0) = \binom{n}{i}$ i $P_i(j) = (-1)^i P_i(n-j)$ vidimo da vrijedi

$$\begin{aligned} M \cdot A_i' &= \binom{n}{i} + \frac{M-2}{2} P_i(d) + \frac{M-2}{2} P_i(n-d) + P_i(n) \\ &= \begin{cases} 2\binom{n}{i} + (M-2)P_i(d), & \text{za } i \text{ paran,} \\ 0, & \text{za } i \text{ neparan.} \end{cases} \end{aligned}$$

Posebno, $A_1' = A_3' = 0$. Iz teorema 3.6 znamo da kodne riječi od C čine OA jakosti 2, pa iz Delsarteova teorema 3.12 zaključujemo $A_2' = 0$. Vidimo da je formalna dualna težina koda C barem $d^\perp \geq 4$. Iz drugog smjera Delsarteova teorema slijedi da kodne riječi od C čine OA jakosti 3. □

Dokaz teorema 3.8. Neka je C samokomplementarni kod koji dostiže Grey-Rankinovu ocjenu. Kao što smo vidjeli u dokazu leme 3.13, možemo pretpostaviti da je $0 \in C$. Tada je distribucija težina u tom kodu $A_0 = A_n = 1$, $A_d = A_{n-d} = \frac{M-2}{2}$, $A_i = 0$ za sve ostale i. Pokažimo prvo da nosači vektora težine d čine dizajn $\mathcal{D}$ s parametrima 2-(n, d, λ) za $\lambda = \frac{d(d-1)}{n-(n-2d)^2}$. Za $k \in \{d, n-d\}$ i bilo koje dvije koordinate $i_1, i_2 \in \{1, \ldots, n\}$ neka je λ_k broj kodnih riječi težine k koje ih pokrivaju (tj. nosači im sadrže i_1 i i_2). Kodna riječ $j = (1, \ldots, 1)$ pokriva sve koordinate, a budući da kod čini OA jakosti 2 vrijedi

$$\lambda_d + \lambda_{n-d} = \frac{M}{4} - 1. \tag{15}$$

Drugu jednadžbu dobijemo prebrojavanjem parova (x, c), gdje je x vektor težine 3 koji pokriva i_1, i_2, a $c \in C \setminus \{0, j\}$ je kodna riječ koja pokriva x:

$$(d-2)\lambda_d + (n-d-2)\lambda_{n-d} = (n-2)\left(\frac{M}{8} - 1\right). \tag{16}$$

Za desnu stranu koristimo lemu 3.13, tj. svojstvo da kod čini OA jakosti 3. Sustav (15), (16) ima jedinstveno rješenje

$$\lambda_d = \frac{d(d-1)}{n-(n-2d)^2}, \quad \lambda_{n-d} = \frac{(n-d)(n-d-1)}{n-(n-2d)^2}.$$

Dakle, broj vektora težine d i $n-d$ koji pokrivaju i_1 i i_2 ne ovisi o izboru tih koordinata. Nosači vektora težine d čine 2-(n, d, λ_d) dizajn $\mathcal{D}$, a nosači vektora težine $n-d$ čine komplementarni 2-$(n, n-d, \lambda_{n-d})$ dizajn $\overline{\mathcal{D}}$.

Prvo pretpostavimo da je n neparan. Međusobna udaljenost riječi težine d iz koda C je d ili $n-d$. Vrijedi formula

$$d(x, y) = w(x-y) = w(x+y) = w(x) + w(y) - 2w(x \cap y), \qquad (17)$$

gdje je $x \cap y$ vektor koji dobijemo množenjem x i y po komponentama i odgovara presjeku nosača od x i y. Za vektore težine d desna strana je uvijek parna, pa je $d(x,y) = d$ ako je d paran, a $d(x,y) = n-d$ ako je d neparan. Budući da je udaljenost vektora težine d konstantna, iz formule (17) slijedi da je i $w(x \cap y)$ konstanta, tj. presjek blokova u dizajnu $\mathcal{D}$ je konstantne veličine. Iz teorema 1.10 slijedi da je $\mathcal{D}$ simetrični dizajn, tj. vrijedi $n = \frac{M-2}{2}$, odnosno $M = 2n+2$. Izjednačavanjem sa $M = \frac{8d(n-d)}{n-(n-2d)^2}$ dobijemo $n = 2d \pm 1$. Zbog uvjeta $2d < n$ slijedi $n = 2d+1$, što znači da dizajn $\mathcal{D}$ ima parametre $(2d+1, d, \frac{d-1}{2}) = (4m-1, 2m-1, m-1)$ za $d = 2m-1$. To je simetrični Hadamardov dizajn ekvivalentan Hadamardovoj matrici reda $4m = n+1$. Obrnuto, ako postoji Hadamardova matrica reda $4m$, znamo da postoji simetrični $(4m-1, 2m-1, m-1)$ dizajn. Kod C koji se sastoji od incidencijskih vektora njegovih blokova i blokova komplementarnog dizajna te vektora 0 i j je samokomplementaran i ima parametre $(4m-1, 8m, 2m-1, 2)$ koji dostižu Grey-Rankinovu ocjenu.

Promotrimo sada slučaj kad je n paran. Tada zbog parnosti desne strane u (17) slijedi da i d mora biti paran. Za neparni d mogla bi postojati samo jedna kodna riječ težine d, tj. kod bi bio oblika $C = \{0, x, \overline{x}, j\}$, ali $M = 4$ vodi u kontradikciju. Za parni d udaljenost kodnih riječi težine d je d ili $n-d$, pa iz (17) slijedi da je $\mathcal{D}$ kvazisimetričan s presječnim brojevima $x = \frac{3d-n}{2}$, $y = \frac{d}{2}$. Obrnuto, od kvazisimetričnog 2-$(n, d, \frac{d(d-1)}{n-(n-2d)^2})$ dizajna s presječnim brojevima $x = \frac{3d-n}{2}$, $y = \frac{d}{2}$ možemo napraviti samokomplementarni kod C koji se sastoji od incidencijskih vektora njegovih blokova i blokova komplementarnog dizajna te vektora 0 i j. Dizajn ima n točaka i $b = \frac{n(n-1)}{n-(n-2d)^2}$ blokova, pa je kod duljine n i veličine $M = 2b+2 = \frac{8d(n-d)}{n-(n-2d)^2}$. Zbog kvazisimetričnosti i formule (17) vidimo da je minimalna udaljenost od C jednaka d, dakle C dostiže Grey-Rankinovu ocjenu. $\square$

U tablici 2 navedeni su parametri kvazisimetričnih dizajna s $v \leq 136$ koji odgovaraju kodovima koji dostižu Grey-Rankinovu ocjenu. U prvom retku je trivijalni 2-$(6, 2, 1)$ dizajn, koji za blokove ima sve dvočlane podskupove 6-članog skupa. U drugom retku su rezidualni dizajni dvoravnina $(16, 6, 2)$, koji su također navedeni u tablici 10. U idućih osam redaka su parametri iz tablice 1 i redni brojevi odgovaraju recima u toj tablici. U zadnjih pet redaka tablice 2 su parametri s $v > 78$, koji nisu obuhvaćeni drugim tablicama.

Br.	n	d	λ	x	y	M	Nqsd	Nlin
	6	2	1	0	1	32	1	1
	10	4	2	1	2	32	3	1
3	20	8	14	2	4	192	0	0
15	28	12	11	4	6	128	$\geq$58891	4
22	36	16	12	6	8	128	$\geq$522079	4
28	42	18	51	6	9	576	?	0
69	66	30	29	12	15	288	$\geq$10000	0
78	72	32	124	12	16	1280	?	0
87	76	36	21	16	18	192	0	0
94	78	36	30	15	18	288	$\geq$10000	0
	88	40	65	16	20	640	?	0
	110	50	245	20	25	2400	?	0
	120	56	55	24	28	512	$\geq$14668	$\geq$4668
	130	60	118	25	30	1120	?	0
	136	64	56	28	32	512	$\geq$14668	$\geq$4668

Tablica 2: Dizajni i kodovi koji dostižu Grey-Rankinovu ocjenu.

U sedmom stupcu tablice navedena je veličina koda M. Ako je M potencija od 2, moguće je da kod bude linearan. McGuire [100] je karakterizirao linearnost samokomplementarnih kodova koji dostižu Grey-Rankinovu ocjenu.

Propozicija 3.14. *Neka je C samokomplementarni $(n, M, d, 2)$ kod parne duljine n koji dostiže Grey-Rankinovu ocjenu i $\mathcal{D}$ odgovarajući kvazisimetrični 2-(n, d, λ) dizajn s $\lambda = \frac{d(d-1)}{n-(n-2d)^2}$, $x = \frac{3d-n}{2}$, $y = \frac{d}{2}$. Kod C je linearan ako i samo ako dizajn $\mathcal{D}$ ima sljedeće svojstvo: za svaka dva bloka B_1, B_2 simetrična razlika $B_1 \Delta B_2$ je blok ili komplement bloka.*

Dokaz. Kao i ranije, pretpostavljamo da C sadrži nulvektor i vektor j. Budući da radimo nad poljem $\mathbb{F}_2$, za linearnost je nužno i dovoljno da kod bude zatvoren na zbrajanje. Primijetimo da zbroj vektora nad $\mathbb{F}_2$ odgovara simetričnoj razlici njihovih nosača. Kod osim 0 i j sadrži incidencijske vektore blokova iz $\mathcal{D}$ i njihovih komplementa. Stoga je jasno da u slučaju linearnog koda dizajn $\mathcal{D}$ ima svojstvo iz propozicije. Obrnuto, ako dizajn $\mathcal{D}$ ima to svojstvo, onda je C zatvoren na zbrajanje vektora težine d. Zatvorenost na zbrajanje svih vektora slijedi iz $x + \overline{y} = \overline{x + y}$ i $\overline{x} + \overline{y} = x + y$. $\square$

Svojstvo dizajna $\mathcal{D}$ iz prethodne propozicije zovemo *QSDP svojstvom.* Dizajne s tim svojstvom susrest ćemo ponovo u cjelini 4.4. Oni su nužno rezidualni ili derivirani dizajni tzv. simetričnih SDP dizajna i imaju parametre oblika $(n, d, \lambda) = (2^{2m-1} + 2^{m-1}, 2^{2m-2}, 2^{2m-2} - 2^{m-1})$ ili $(2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}, 2^{2m-2} - 2^{m-1} - 1)$ ili njima komplementarne parametre. McGuire [100, tm. B] je karakterizirao i linearnost kodova neparne duljine n. U tom slučaju linearni kodovi odgovaraju tzv. Hadamardovim matricama Sylvesterovog tipa, kojima je red uvijek potencija od 2 [93, str. 45].

U zadnja dva stupca tablice 2 naveden je ukupan broj samokomplementarnih kodova koji dostižu Grey-Rankinovu ocjenu (odnosno odgovarajućih dizajna) i broj takvih kodova koji su linearni (odnosno QSDP dizajna). Kad je M potencija od 2, mogu postojati linearni i nelinearni kodovi. Kada M nije potencija od 2, mogu postojati samo nelinearni kodovi, odnosno dizajni koji nemaju QSDP svojstvo. Jedini poznati primjeri kod kojih M nije potencija od 2 su dizajni i kodovi br. 69 i 94 s parametrima $(66, 288, 30, 2)$ i $(78, 288, 36, 2)$, konstruirani u [28].

Teorem 3.15 (Bracken-McGuire-Ward)**.** *Neka je $u \in \mathbb{N}$ paran prirodan broj.*

(*i*) *Ako postoji Hadamardova matrica reda $2u$ i skup od $u - 2$ međusobno ortogonalna latinska kvadrata reda $2u$, onda postoji kvazisimetrični 2-$(2u^2 - u, u^2 - u, u^2 - u - 1)$ dizajn s presječnim brojevima $x = \frac{u(u-2)}{2}$, $y = \frac{u(u-1)}{2}$.*

(*ii*) *Ako postoji Hadamardova matrica reda $2u$ i skup od $u - 1$ međusobno ortogonalna latinska kvadrata reda $2u$, onda postoji kvazisimetrični 2-$(2u^2 + u, u^2, u^2 - u)$ dizajn s presječnim brojevima $x = \frac{u(u-1)}{2}$, $y = \frac{u^2}{2}$.*

Dokaz. Opisat ćemo konstrukciju samokomplementarnih kodova koji su ekvivalentni prema teoremu 3.8. U slučaju (*i*) takav kod ima parametre $(2u^2 - u, 8u^2, u^2 - u, 2)$, a u slučaju (*ii*) parametre $(2u^2 + u, 8u^2, u^2, 2)$. Prvo od Hadamardove matrice reda $2u$ napravimo binarni kod na sljedeći način. Pretpostavimo da je matrica normalizirana, tj. prvi redak i stupac sadrže samo jedinice. Izbrišemo prvi stupac, zamijenimo jedinice simbolom 0, a minus jedinice s 1 i uzmemo retke kao kodne riječi. Zbog ortogonalnosti redaka Hadamardove matrice, svake dvije kodne riječi razlikuju se na u koordinata. Dakle, dobili smo ekvidistantni kod s parametrima $(2u - 1, 2u, u, 2)$.

U slučaju (i) skup od $u-2$ međusobno ortogonalnih latinskih kvadrata transformiramo u MDS kod s parametrima $(u, 4u^2, u-1, 2u)$ (vidi [129, tm. 9.35]). Abeceda tog koda je veličine $2u$ pa uspostavimo bijekciju s kodnim riječima dobivenim od Hadamardove matrice (to možemo napraviti na $(2u)!$ načina). Zatim supstituiramo te kodne riječi u MDS kod i dobijemo binarni kod duljine $u(2u-1) = 2u^2 - u$ i veličine $4u^2$. Kad dodamo komplementarne vektore, dobijemo samokomplementarni binarni kod s $n = 2u^2 - u$ i $M = 8u^2$. Još treba pokazati da se svake dvije kodne riječi razlikuju na bar $d = u^2 - u$ koordinata. Riječi MDS koda razlikuju se na $u-1$ ili u koordinata, a vektori dobiveni od Hadamardove matrice na u koordinata. Zato se kodne riječi dobivene supstitucijom razlikuju na $(u-1)u = u^2 - u$ ili u^2 koordinata. Međusobna udaljenost komplementiranih vektora je ista $(d(\overline{x}, \overline{y}) = d(x, y))$, a udaljenost komplementiranog od nekomplementiranog vektora je zbog $d(\overline{x}, y) + d(x, y) = n$ jednaka u^2, $u^2 - u$ ili n ako je $x = y$. Dakle, minimalna udaljenost je $u^2 - u$ i dobili smo kod s parametrima $(2u^2 - u, 8u^2, u^2 - u, 2)$.

U slučaju (ii) skup od $u-1$ ortogonalnih latinskih kvadrata ekvivalentan je MDS kodu s parametrima $(u+1, 4u^2, u, 2u)$. Supstitucijom kodnih riječi dobivenih od Hadamardove matrice dobijemo kod duljine $(u+1)(2u-1) = 2u^2 + u - 1$ i veličine $4u^2$. Njegove kodne riječi proširimo koordinatom 0 i dodamo komplementarne vektore, pa dobijemo samokomplementarni kod s parametrima $(2u^2 + u, 8u^2, u^2, 2)$. □

Ekvivalentna konstrukcija kvazisimetričnih dizajna opisana je u članku [99] direktno, bez posredstva kodova. Hadamardove matrice vjerojatno postoje za sve redove djeljive s 4, ali "usko grlo" ove konstrukcije su veliki skupovi međusobno ortogonalnih latinskih kvadrata. Za prim potenciju q lako je konstruirati potpun skup od $q-1$ međusobno ortogonalnih latinskih kvadrata reda q. U teoremu 3.15 je $q = 2u$, pa je q prim potencija samo ako je u potencija od 2. U tom slučaju teorem 3.15 daje dizajne s istim parametrima kao QSDP dizajni (konstruirani dizajni ne moraju imati QSDP svojstvo, tj. odgovarajući kodovi nisu nužno linearni). Jedini slučaj kad u nije potencija od 2, a poznato je dovoljno međusobno ortogonalnih latinskih kvadrata, je $u = 6$. Poznat je skup od 5 međusobno ortogonalnih latinskih kvadrata reda 12 [2, tm. 3.44]. Od tog skupa i Hadamardove matrice reda 12 možemo konstruirati dizajne br. 69 i 94 s parametrima 2-$(66, 30, 29)$, $x = 12$, $y = 15$ i 2-$(78, 36, 30)$, $x = 15$, $y = 18$.

U dokazu teorema 3.15 pridruživanje abecede MDS koda riječima koda dobivenog od Hadamardove matrice možemo napraviti na bilo koji od $(2u)!$ načina. Eksperimenti na računalu pokazuju da za različita pridruživanja često dobivamo neizomorfne dizajne te da konstruirani dizajni obično nemaju dodatne pravilnosti (nemaju QSDP svojstvo i puna grupa automorfizama im je trivijalna). U članku [89] konstruirano je po 10000 neizomorfnih dizajna s parametrima br. 69 i 94, a isto možemo napraviti za $u = 8$. Uzeli smo Hadamardovu matricu reda 16 i potpuni skup od 15 međusobno ortogonalnih latinskih kvadrata reda 16 te izabrali podskup veličine 6 ili 7. Različitim pridruživanjem simbola konstruirali smo po 10000 dizajna s parametrima 2-$(120, 56, 55)$, $x = 24$, $y = 28$ i 2-$(136, 64, 56)$, $x = 28$, $y = 32$. S pomoću računala provjerili smo da su svi konstruirani dizajni neizomorfni, imaju trivijalnu grupu automorfizama i nemaju QSDP svojstvo, tj. odgovarajući kodovi su nelinearni. Linearni kodovi s parametrima $(120, 512, 56, 2)$ i $(136, 512, 64, 2)$ konstruirani su u člancima [58, 25]. Uz pretpostavku da imaju automorfizam reda 3 konstruirano je po 4668 neizomorfnih linearnih kodova. To znači da je ukupan broj takvih dizajna i kodova barem 14668. Napomenimo da su to vrlo grube ocjene. Točan broj tih dizajna i kodova, kao i dizajna i kodova br. 69 i 94, vjerojatno je puno veći.

3.2 Samoortogonalni i samodualni kodovi

Za linearni kod $C \leq \mathbb{F}_q^n$ kažemo da je *samoortogonalan* ako je $C \leq C^\perp$, tj. za sve kodne riječi $x, y \in C$ vrijedi $x \cdot y = \sum_{i=1}^n x_i y_i = 0$. Nuždan i dovoljan uvjet za samoortogonalnost je ortogonalnost redaka generirajuće matrice.

Lema 3.16. *Neka je C linearni kod s generirajućom matricom $G \in \mathbb{F}_q^{m\times n}$. Kod C je samoortogonalan ako i samo ako za retke $g_1, \ldots, g_m$ matrice G vrijedi $g_i \cdot g_j = 0$, $\forall i, j \in \{1, \ldots, m\}$.*

Dokaz. Nužnost vrijedi jer su reci od G sadržani u C. Za dovoljnost primijetimo da vektore $x, y \in C$ možemo zapisati kao $x = \sum_{i=1}^m \alpha_i g_i$, $y = \sum_{j=1}^m \beta_j g_j$, pa je $x \cdot y = \sum_{i=1}^m \sum_{j=1}^m \alpha_i \beta_j \, g_i \cdot g_j = 0$. $\square$

Lema 3.17. *Ako je $C \leq \mathbb{F}_q^n$ samoortogonalni kod dimenzije m, onda je $m \leq n/2$.*

Dokaz. Vrijedi $m = \dim C \leq \dim C^\perp = n - m$ (prema propoziciji 3.1). Dakle, $2m \leq n$. $\square$

Samoortogonalne kodove koji dostižu nejednakost nazivamo *samodualnim.* To su kodovi za koje je $C = C^\perp$ i mogući su samo ako je duljina koda n parna. Iduću teorem iz [94] pokazuje da svaki samoortogonalni binarni kod (tj. kod nad poljem $\mathbb{F}_2$) parne duljine možemo proširiti do samodualnog koda.

Teorem 3.18. *Neka je C samoortogonalni binarni kod duljine $n = 2t$ i dimenzije $m \geq 1$. Broj samodualnih kodova $D \leq \mathbb{F}_2^n$ koji sadrže C je $\prod_{i=1}^{t-m}(2^i + 1)$.*

Dokaz. Označimo sa σ_i broj samoortogonalnih kodova dimenzije i koji sadrže C, za $i = m, \ldots, t$. Neka je D takav kod dimenzije $i < t$; pogledajmo na koliko ga načina možemo proširiti do samoortogonalnog koda E dimenzije $i+1$. Zbog samoortogonalnosti vrijedi $D < D^\perp$ i kvocijentni prostor $D^\perp/D$ sastoji se od klasa $D, d_1+D, \ldots, d_l+D$ za $l = 2^{n-i}/2^i - 1 = 2^{n-2i} - 1$. Svako proširenje je oblika $E = D \cup (d_j + D)$ za $j = 1, \ldots, l$. Međutim, isti kod E dobivamo i od bilo kojeg drugog i-dimenzionalnog koda D' sa $C \leq D' < E$. Broj takvih međukodova je $2^{i+1-m} - 1$ i time smo dokazali rekurziju

$$\sigma_{i+1} = \sigma_i \cdot \frac{2^{n-2i} - 1}{2^{i+1-m} - 1}, \quad i = m, \ldots, t-1.$$

Počevši od $\sigma_m = 1$ iz rekurzije se rastavljanjem brojnika kao razlike kvadrata i kraćenjem s nazivnicima dobije $\sigma_t = \prod_{i=m}^{t-1}(2^{t-i}+1) = \prod_{i=1}^{t-m}(2^i+1)$. To je broj samoortogonalnih kodova dimenzije t koji sadrže C, a oni su zbog $n = 2t$ samodualni. $\square$

Na isti način dokazuje se da svaki samoortogonalni binarni kod neparne duljine $n = 2t+1$ možemo proširiti do samoortogonalnog koda dimenzije t. Vektori samoortogonalnog koda okomiti su na same sebe, pa im je težina u binarnom slučaju parna. Posebno su važni samoortogonalni binarni kodovi kojima su težine svih kodnih riječi djeljive s 4, takozvani *dvostruko parni* kodovi (eng. *doubly even*). Ako je duljina n djeljiva s 8, moguće je proširiti svaki dvostruko parni samoortogonalni kod do dvostruko parnog samodualnog koda.

Teorem 3.19. *Neka je C samoortogonalni dvostruko parni binarni kod duljine $n = 2t$ i dimenzije $m \geq 1$. Ako je n djeljiv s 8, broj samodualnih dvostruko parnih kodova $D \leq \mathbb{F}_2^n$ koji sadrže C je $2\prod_{i=1}^{t-m-1}(2^i+1)$.*

Dokaz je kompliciraniji od teorema 3.18 i nalazi se u [94]. Primjenom teorema na $C = \{0, j\}$ (j je vektor sa svim komponentama 1) slijedi da samodualni dvostruko parni kodovi postoje uvijek kad je n djeljiv s 8. Nužnost tog uvjeta također je dokazana u [94], a slijedi direktno iz Gleasonova teorema 3.31. Dvostruko parni samodualni binarni kodovi nazivaju se kodovima *tipa II*, a samodualni binarni kodovi u kojima postoje riječi težine $\equiv 2 \pmod 4$ kodovima *tipa I*. Nazivi dolaze od klasifikacije samodualnih kodova u kojima su težine višekratnici nekog broja $t > 1$ (vidi [93, tm. 19.1.1]).

Vratimo se kodovima nad bilo kojim konačnim poljem $\mathbb{F}_q$. Dizajnu $\mathcal{D}$ s parametrima 2-(v, k, λ) pridružujemo linearni kod $C \leq \mathbb{F}_q^v$ duljine v tako da razapnemo potprostor s incidencijskim vektorima njegovih blokova, tj. za generirajuću matricu uzmemo transponiranu incidencijsku matricu $G = A^\tau$. Ako je p karakteristika polja $\mathbb{F}_q$, dimenziju koda C nazivamo *p-rangom* od $\mathcal{D}$

i označavamo $\operatorname{rang}_p \mathcal{D}$. To je rang incidencijske matrice nad bilo kojim poljem karakteristike p. Zbog iduće propozicije kod C je zanimljiv samo ako p dijeli red dizajna $n = r - \lambda$.

Propozicija 3.20. *Neka je $\mathcal{D}$ 2-(v, k, λ) dizajn i p prost broj koji ne dijeli njegov red $n = r - \lambda$. Onda vrijedi $\operatorname{rang}_p \mathcal{D} \geq v - 1$. Jednakost vrijedi ako i samo ako p dijeli k i tada je $C = [j]^\perp$, za $j = (1, \ldots, 1)$.*

Dokaz. Zbrajanjem stupaca incidencijske matrice koji na i-toj koordinati imaju jedinicu (tj. incidencijskih vektora blokova kroz i-tu točku) dobijemo vektor $ne_i + \lambda j$. Vektor e_i na i-toj koordinati ima 1, a na ostalim koordinatama 0. Kod C sadrži vektore $ne_i + \lambda j$, pa sadrži i njihove razlike $n(e_i - e_1)$. Budući da p ne dijeli n, vrijedi $e_i - e_1 \in C$, $i = 2, \ldots, v$. To su linearno nezavisni vektori pa je $\dim C \geq v - 1$. Nadalje, zbog $(e_i - e_1) \cdot j = 0$ vrijedi $[j]^\perp \leq C$, a jednakost $\dim C = v - 1$ vrijedi ako i samo ako je $C = [j]^\perp$. To je ekvivalentno s $p \mid k$ jer je produkt stupaca incidencijske matrice s vektorom j jednak k. □

O slučaju kada p dijeli n govori teorem M. Klemma [85]. Dokaz se može naći i u [5, tm. 2.4.2].

Teorem 3.21 (Klemm)**.** *Ako je $\mathcal{D}$ 2-(v, k, λ) dizajn i p prost broj koji dijeli njegov red $n = r - \lambda$, onda vrijedi $\operatorname{rang}_p \mathcal{D} \leq \frac{b+1}{2}$. Ako uz to p^2 ne dijeli n i p ne dijeli λ, onda kod pridružen dizajnu zadovoljava $C^\perp \leq C$ i vrijedi $\operatorname{rang}_p \mathcal{D} \geq \frac{v}{2}$.*

Prema lemi 3.16, kod C razapet stupcima incidencijske matrice dizajna $\mathcal{D}$ nad poljem $\mathbb{F}_q$ je samoortogonalan ako su skalarni produkti stupaca djeljivi s p (karakteristikom polja). Skalarni produkt dvaju stupaca je veličina presjeka odgovarajućih blokova, a skalarni produkt stupca sa sobom je k. Ako presječne brojeve označimo $x_1, \ldots, x_s$, uvjet za samoortogonalnost je $x_1 \equiv \ldots \equiv x_s \equiv 0 \pmod{p}$ i $k \equiv 0 \pmod{p}$. Prema sljedećem teoremu Calderbanka [33], drugi uvjet slijedi iz prvog.

Teorem 3.22. *Neka je p prost broj i $\mathcal{D}$ dizajn s parametrima 2-(v, k, λ) koji nije simetričan i ima presječne brojeve $x_1, \ldots, x_s$. Ako je $x_1 \equiv \ldots \equiv x_s \equiv x \pmod{p}$, onda je $k \equiv x \pmod{p}$ i $n \equiv 0 \pmod{p}$.*

Dokaz. Neka je A incidencijska matrica dizajna $\mathcal{D}$. Matrica $A^\tau \cdot A$ je kvadratna reda b i ima dijagonalne elemente k, a izvan dijagonale ima presječne brojeve. Modulo p to je matrica oblika kao u lemi 2.8. Ako je $k \not\equiv x \pmod{p}$, rang te matrice nad poljem $\mathbb{F}_p$ je b ili $b - 1$. Iz $v \geq \operatorname{rang}_p(A) \geq \operatorname{rang}_p(A^\tau \cdot A) \geq b - 1$ slijedi $b = v + 1$, pa iz $bk = vr$ dobijemo kontradikciju $k = v$. Dakle, $k \equiv x \pmod{p}$.

Ako je $n \not\equiv 0 \pmod p$, tj. $r \not\equiv \lambda \pmod p$, matrica $A \cdot A^\tau = nI + \lambda J$ zbog leme 2.8 ima p-rang v ili $v-1$. Ako je $k \equiv x \equiv 0 \pmod p$, stupci matrice A (incidencijski vektori blokova) generiraju nad poljem $\mathbb{F}_p$ samoortogonalni kod C (lema 3.16). Ako je pak $k \equiv x \not\equiv 0 \pmod p$, kod C generiran vektorima $a_i - a_1$, $i = 2, \ldots, b$ je samoortogonalan (a_i su stupci incidencijske matrice). Samoortogonalni kod u $\mathbb{F}_p^v$ ima dimenziju najviše $v/2$ (lema 3.17), pa je $\mathrm{rang}_p(A) - 1 \le v/2$. To je kontradikcija s $v - 1 \le \mathrm{rang}_p(A \cdot A^\tau) \le \mathrm{rang}_p(A) \le v/2 + 1$. Dakle, $n \equiv 0 \pmod p$. □

Vidimo da dizajn kojem su svi presječni brojevi kongruentni modulo p zadovoljava uvjet Klemmova teorema, tj. red n mu je djeljiv s p. U dokazu teorema vidjeli smo kako mu pridružiti samoortogonalni kod:

Korolar 3.23. *Neka je $\mathcal{D}$ nesimetrični 2-(v, k, λ) dizajn s presječnim brojevima $x_1, \ldots, x_s$ i neka vrijedi $x_1 \equiv \ldots \equiv x_s \equiv x \pmod p$. Ako je $x = 0$, onda je kod C razapet stupcima incidencijske matrice $a_1, \ldots, a_b$ nad poljem $\mathbb{F}_q$ karakteristike p samoortogonalan. Ako je $x \neq 0$, onda je kod razapet vektorima $a_i - a_1$, $i = 2, \ldots, b$ nad $\mathbb{F}_q$ samoortogonalan.*

U slučaju $p = 2$, $x = 1$, drugi način za dobiti samoortogonalni binarni kod je proširiti generirajuću matricu stupcem jedinica:

$$G_1 = \begin{bmatrix} & 1 \\ A^\tau & \vdots \\ & 1 \end{bmatrix}. \tag{18}$$

Ako su presječni brojevi $x_1, \ldots, x_s$ neparni, po teoremu 3.22 parametar k je također neparan. Skalarni produkti redaka proširene matrice G_1 su parni, tj. nula u polju $\mathbb{F}_2$. Zato je kod C_1 generiran tom matricom nad poljem $\mathbb{F}_2$ samoortogonalni kod duljine $v + 1$. Idući rezultat Toncheva [131] je ocjena za dualnu težinu binarnog koda pridruženog dizajnu.

Propozicija 3.24. *Neka je C binarni kod razapet stupcima incidencijske matrice 2-(v, k, λ) dizajna. Minimalna težina dualnog koda $C^\perp$ zadovoljava $d^\perp \ge (r + \lambda)/\lambda$.*

Dokaz. Prema teoremu 3.2, minimalna težina koda $C^\perp$ je najmanji broj stupaca transponirane incidencijske matrice $G = A^\tau$ koji su linearno zavisni nad $\mathbb{F}_2$. Neka je S minimalni skup linearno zavisnih stupaca od G. Suma stupaca iz S je nulvektor u $\mathbb{F}_2^b$. To znači da svaki redak od G ima paran broj jedinica u stupcima iz skupa S. Označimo s n_{2i} broj redaka od G koji imaju $2i$ jedinica u stupcima iz S. Ukupan broj jedinica u stupcima iz S je

$$\sum 2i\, n_{2i} = r\,|S| = rd^\perp. \tag{19}$$

Brojanjem parova jedinica dobijemo

$$\sum 2i(2i-1)n_{2i} = d^{\perp}(d^{\perp}-1)\lambda, \tag{20}$$

a oduzimanjem (19) od (20) slijedi

$$\sum 2i(2i-2)n_{2i} = d^{\perp}[(d^{\perp}-1)\lambda - r].$$

Lijeva strana je nenegativna i zato je $(d^{\perp}-1)\lambda - r \geq 0$, tj. $d^{\perp} \geq (r+\lambda)/\lambda$. □

Primijetimo da za ovaj rezultat nije bitna samoortogonalnost koda C. Tonchev [131] je ocijenio i dualnu težinu binarnog koda generiranog proširenom incidencijskom matricom.

Propozicija 3.25. *Neka je C_1 binarni kod razapet proširenom incidencijskom matricom* (18) *dizajna s parametrima* 2-(v,k,λ). *Minimalna težina dualnog koda $C_1^{\perp}$ zadovoljava $d^{\perp} \geq \min\{(r+\lambda)/\lambda, (b+r)/r\}$.*

Dokaz. Kao i u prethodnoj propoziciji, neka je S minimalni skup linearno zavisnih stupaca od G_1. Ako među njima nije dodani stupac jedinica, slijedi $d^{\perp} \geq (r+\lambda)/\lambda$. Ako je dodani stupac u S, u svakom retku od G_1 nalazi se neparan broj jedinica iz redaka u S bez dodatnog stupca. Označimo s n_{2i+1} broj redaka od G_1 u kojima je broj jedinica $2i+1$. Vrijedi $\sum n_{2i+1} = b$ i $\sum(2i+1)n_{2i+1} = (d^{\perp}-1)r$, iz čega oduzimanjem dobijemo $\sum 2i\, n_{2i+1} = (d^{\perp}-1)r - b$. Lijeva strana je nenegativna, pa je $d^{\perp} \geq (b+r)/r$. □

Samodualni binarni kodovi duljina $n \leq 40$ potpuno su klasificirani [113, 115, 45, 46, 18, 19, 63, 3, 14, 23, 24, 26]. Generirajuće matrice dostupne su na web stranici japanskih matematičara M. Harade i A. Munemase [64]. Informacije o kodovima prenose se preko opisanih rezultata na kvazisimetrične dizajne. Kao prvi primjer provest ćemo klasifikaciju afino rastavljivih dizajna br. 5 iz tablice 7.

Teorem 3.26. *Postoji točno pet neizomorfnih kvazisimetričnih* 2-$(16,8,7)$ *dizajna s presječnim brojevima $x=0$, $y=4$. Podaci o dimenziji m, minimalnoj težini d i težinskom polinomu $W(x,y)$ pridruženog koda te redu pune grupe automorfizama dani su u tablici 3.*

Dokaz. Binarni kod C generiran transponiranom incidencijskom matricom $G = A^{\tau}$ je duljine $n=16$ i samoortogonalan je jer su x i y parni. Kodne riječi su sume redaka od G. Indukcijom se dokaže generalizacija formule (17):

$$\begin{aligned} w(x_1+\ldots+x_k) &= \sum_{i_1} w(x_{i_1}) - 2\sum_{i_1<i_2} w(x_{i_1}\cap x_{i_2}) + \\ &+ 4\sum_{i_1<i_2<i_3} w(x_{i_1}\cap x_{i_2}\cap x_{i_3}) + \ldots + (-2)^{k-1}\, w(x_1\cap\cdots\cap x_k). \end{aligned} \tag{21}$$

Dizajn	m	d	$W(x,y)$	$\lvert\,\mathrm{Aut}\,\rvert$
$\mathcal{D}_1$	5	8	$x^{16}+30x^8y^8+y^{16}$	322560
$\mathcal{D}_2$	6	4	$x^{16}+4x^{12}y^4+54x^8y^8+4x^4y^{12}+y^{16}$	9216
$\mathcal{D}_3$	7	4	$x^{16}+12x^{12}y^4+102x^8y^8+12x^4y^{12}+y^{16}$	1536
$\mathcal{D}_4$	8	4	$x^{16}+28x^{12}y^4+198x^8y^8+28x^4y^{12}+y^{16}$	2688
$\mathcal{D}_5$	8	4	$x^{16}+28x^{12}y^4+198x^8y^8+28x^4y^{12}+y^{16}$	2688

Tablica 3: Kvazisimetrični 2-$(16,8,7)$ dizajni s $x=0$, $y=4$.

Budući da su težine redaka od G i "presjeka" parova redaka od G djeljive s 4, iz formule (21) slijedi da su težine svih kodnih riječi iz C djeljive s 4, tj. C je dvostruko parni samoortogonalni kod. Po teoremu 3.19 možemo ga proširiti do dvostruko parnog samodualnog koda D koji zadovoljava $C \leq D \leq C^{\perp}$. Po propoziciji 3.24 minimalna težina od $C^{\perp}$ je bar 4, a minimalna težina potkoda D ne može biti manja. S druge strane, po teoremu 3.34 minimalna težina od D ne može biti veća od 4. Dakle, D je dvostruko parni samodualni kod s parametrima $[n,m,d,q]=[16,8,4,2]$. Prema [64], postoje točno dva takva neekvivalentna koda (binarni kodovi su ekvivalentni ako se jedan može dobiti od drugog permutacijom koordinata). Oba imaju težinski polinom $W_D(x,y)=x^{16}+28x^{12}y^4+198x^8y^8+28x^4y^{12}+y^{16}$. Vidimo da postoji točno 198 kodnih riječi težine 8. Blokovi dizajna su nosači nekih 30 od tih kodnih riječi. Vidimo također da kod D sadrži vektor $j=(1,\dots,1)$, što znači da je samokomplementaran. Nosače riječi težine 8 možemo podijeliti u 99 komplementarnih parova, tj. klasa paralelnosti. Dizajn je afino rastavljiv i sastoji se od 15 takvih klasa.

Problem izbora $\binom{99}{15}$ klasa paralelnosti koje pokrivaju svaki od $\binom{16}{2}$ parova točaka točno $\lambda=7$ puta možemo riješiti Kramer-Mesnerovom metodom, kako je opisano u članku [89]. Koristimo se matricom kompatibilnosti, koja sadrži informaciju da se blokovi iz različitih klasa sijeku u $y=4$ točaka. Kramer-Mesnerov sustav je dimenzija 120×99 i za prvi kod D ima 5040 rješenja, a za drugi 7200 rješenja. Od prvog koda dobivamo četiri neizomorfna dizajna $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{D}_3$ i $\mathcal{D}_4$, a od drugog također četiri, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{D}_3$ i $\mathcal{D}_5$. Dizajn $\mathcal{D}_1$ je izomorfan afinom dizajnu $AG_3(4,2)$ i ima najmanji 2-rang $m=5$. Dizajni $\mathcal{D}_4$ i $\mathcal{D}_5$ imaju 2-rang $m=8$. Za njih se kodovi C i D podudaraju. □

Na sličan način V. Tonchev [132] je klasificirao kvazisimetrične dizajne br. 17 iz tablice 1.

Teorem 3.27. *Postoji točno pet neizomorfnih kvazisimetričnih* 2-$(31,7,7)$

dizajna s presječnim brojevima $x = 1$, $y = 3$. Njihov 2-rang je $m = 16$, a redovi pune grupe automorfizama su $|\operatorname{Aut}(\mathcal{D})| = 9999360$*,* 322560*,* 2688*,* 720 *i* 465*.*

Dokaz. Binarni kod C_1 generiran proširenom matricom (18) je duljine $n = 32$. Zbog $x \equiv y \equiv 1 \pmod 2$, kod C_1 je samoortogonalan. Težine redaka generirajuće matrice G_1 su 8, a "presjeci" redaka su parni (imaju 2 ili 4 zajedničkih jedinica). Iz relacije (21) slijedi da su težine svih kodnih riječi djeljive s 4, tj. C_1 je dvostruko parni kod. Po teoremu 3.19 možemo ga proširiti do dvostruko parnog samodualnog koda D koji zadovoljava $C_1 \leq D \leq C_1^\perp$. Po propoziciji 3.25 minimalna težina koda $C_1^\perp$ je bar 6. Minimalna težina od D nije manja, a zbog djeljivosti s 4 mora biti bar 8. Po teoremu 3.34 minimalna težina od D ne može biti veća od 8. Dakle, D je kod s parametrima $[n, m, d, q] = [32, 16, 8, 2]$. Samodualni kodovi s tim parametrima klasificirani su u [45] i dvostruko parnih ima točno 5. Generirajuće matrice dostupne su na web stranici [64]. Svih pet kodova imaju težinski polinom $W_D(x, y) = x^{32} + 620\, x^{24}y^8 + 13888\, x^{20}y^{12} + 36518\, x^{16}y^{16} + 13888\, x^{12}y^{20} + 620\, x^8y^{24} + y^{32}$. Nosači vektora težine 8 čine dizajn s parametrima 3-$(32, 8, 7)$. To se može provjeriti računalom, a slijedi i iz teorema Assmusa i Matsona (vidi [93, tm. 6.9.29] ili [5, tm. 2.11.2]). Kvazisimetrične 2-$(31, 7, 7)$ dizajne dobivamo od tih 3-dizajna deriviranjem. U terminima kodova, fiksiramo koordinatu i uzmemo sve kodne riječi težine 8 koje na toj koordinati imaju jedinicu. Takvih vektora ima 155 i nosači (bez fiksirane koordinate) čine kvazisimetrični 2-$(31, 7, 7)$ dizajn. Za različite fiksirane koordinate (tj. različit izbor točaka obzirom na koje deriviramo) dobivamo izomorfne dizajne, jer grupe automorfizama 3-$(32, 8, 7)$ dizajna djeluju tranzitivno na točkama. Dakle, dobijemo pet kvazisimetričnih 2-$(31, 7, 7)$ dizajna za koje se računalom provjeri da su neizomorfni, imaju 2-rang jednak $m = 16$ (što znači da je $C_1 = D = C_1^\perp$) i pune grupe automorfizama veličina navedenih u teoremu. Prvi od njih, s najvećom grupom automorfizama, izomorfan je projektivnom dizajnu $PG_2(4, 2)$. $\square$

U teoremu 3.26 afini dizajn $AG_3(4, 2)$ karakteriziran je minimalnim 2-rangom, ali u teoremu 3.27 to nije slučaj za projektivni dizajn $PG_2(4, 2)$. Ovo je bio prvi potuprimjer za tzv. Hamadinu slutnju, koju ćemo opisati u cjelini 4.5. Istom tehnikom može se dokazati jedinstvenost kvazisimetričnih dizajna vezanih uz veliki Wittov 5-$(24, 8, 1)$ dizajn $\mathcal{W}$, tj. dizajna br. 5, 6, 9, 10 i 12 iz tablice 1. Jedinstvenost dizajna br. 5, 6 i 10 dokazao je Tonchev [131], a dizajna br. 9 i 12 Witt [145] na drugi način.

Teorem 3.28. *Svi kvazisimetrični dizajni sa sljedećim parametrima međusobno su izomorfni:*

1. 2-$(22, 6, 5)$*,* $x = 0$*,* $y = 2$ *(izomorfni su* 3-$(22, 6, 1)$ *dizajnu* $\mathrm{der}^2 \mathcal{W}$*),*

2. 2-$(21, 6, 4)$*,* $x = 0$*,* $y = 2$ *(izomorfni su dizajnu* $\mathrm{res}(\mathrm{der}^2 \mathcal{W})$*),*

3. 2-$(21, 7, 12)$*,* $x = 1$*,* $y = 3$ *(izomorfni su dizajnu* $\mathrm{der}(\mathrm{res}^2 \mathcal{W})$*),*

4. 2-$(23, 7, 21)$*,* $x = 1$*,* $y = 3$ *(izomorfni su* 4-$(23, 7, 1)$ *dizajnu* $\mathrm{der}\, \mathcal{W}$*),*

5. 2-$(22, 7, 16)$*,* $x = 1$*,* $y = 3$ *(izomorfni su* 3-$(22, 7, 4)$ *dizajnu* $\mathrm{res}(\mathrm{der}\, \mathcal{W})$*).*

Dokaz. Neka je C binarni kod generiran transponiranom incidencijskom matricom prvog dizajna iz iskaza teorema, s parametrima 2-$(22, 6, 5)$, $x = 0$, $y = 2$. Zbog parnosti od x i y kod C je samoortogonalan, a zbog propozicije 3.24 minimalna težina od $C^\perp$ je $d^\perp \geq 6$. Po teoremu 3.18 kod C se može proširiti do samodualnog koda D, $C \leq D \leq C^\perp$, minimalne težine $d \geq 6$. S druge strane, zbog teorema 3.33 vrijedi $d \leq 6$. Dakle, D je samodualni kod s parametrima $[n, m, d, q] = [22, 11, 6, 2]$. Prema [115] i [64], jedini takav kod je skraćeni Golayev kod G_{22} s težinskim polinomom $W_D(x, y) = x^{22} + 77x^{16}y^6 + 330x^{14}y^8 + 616x^{12}y^{10} + 616x^{10}y^{12} + 330x^8y^{14} + 77x^6y^{16} + y^{22}$. Nosači riječi težine 6 su blokovi 3-$(22, 6, 1)$ dizajna $\mathrm{der}^2 \mathcal{W}$ s kojim je polazni dizajn izomorfan.

Neka je A incidencijska matrica drugog dizajna iz iskaza teorema, s parametrima 2-$(21, 6, 4)$, $x = 0$, $y = 2$. Promotrimo binarni kod C_0^+ generiran matricom

$$G_0^+ = \begin{bmatrix} 1 \cdots 1 & 1 \\ & 0 \\ A^\tau & \vdots \\ & 0 \end{bmatrix}.$$

To je samoortogonalni kod duljine $n = 22$, a $(C_0^+)^\perp$ se dobije od koda $C^\perp$ s matricom provjere parnosti A^τ dodavanjem koordinate 0 vektorima parne težine i koordinate 1 vektorima neparne težine ("proširivanjem po parnosti"). Po propoziciji 3.24 minimalna težina od $C^\perp$ je bar 5, pa je zbog parnosti minimalna težina od $(C_0^+)^\perp$ bar 6. Po teoremu 3.18 kod C_0^+ možemo proširiti do samodualnog koda D, $C_0^+ \leq D \leq (C_0^+)^\perp$, s parametrima $[n, m, d, q] = [22, 11, 6, 2]$. Kao i ranije, D je skraćeni Golayev kod G_{22}, a polazni dizajn je izomorfan rezidualnom dizajnu $\mathrm{res}(\mathrm{der}^2 \mathcal{W})$. Grupa automorfizama od $\mathrm{der}^2 \mathcal{W}$ djeluje tranzitivno, pa je svejedno obzirom na koju točku uzimamo rezidualni dizajn.

Od trećeg dizajna iz iskaza teorema, s parametrima 2-$(21, 7, 12)$, $x = 1$, $y = 3$, napravimo binarni kod C_1 s generirajućom matricom (18). Kod C_1 je samoortogonalan, ali po propoziciji 3.25 dobijemo slabiju ocjenu za dualnu težinu $d^\perp \geq 4$. Dokažimo direktno da je $d^\perp > 4$. Zbog $(r+\lambda)/\lambda = 52/12 > 4$, među četiri linearno zavisna stupca od G_1 mora biti dodani stupac jedinica. To znači da imamo tri retka incidencijske matrice A čija je suma nad $\mathbb{F}_2$ vektor $j = (1, \ldots, 1)$ duljine $b = 120$. Označimo s n_i broj stupaca od A koji u ta tri retka imaju i jedinica. Očito je $n_2 = 0$ i vrijede jednadžbe $n_1 + n_3 = b = 120$, $n_1 + 3n_3 = 3r = 120$, $3n_3 = 3\lambda = 36$, a taj sustav nema rješenja. Dakle, $d^\perp \geq 5$ i kod C_1 se po teoremu 3.18 može proširiti do samodualnog koda D, $C_1 \leq D \leq C_1^\perp$, kojem je minimalna težina zbog parnosti $d \geq 6$. To je ponovo skraćeni Golayev kod G_{22} u kojem nosači vektora težine 8 čine 3-$(22, 8, 12)$ dizajn $\mathrm{res}^2 \mathcal{W}$. Polazni dizajn izomorfan je deriviranom dizajnu $\mathrm{der}(\mathrm{res}^2 \mathcal{W})$ (svejedno obzirom na koju točku zbog tranzitivnosti grupe automorfizama od $\mathrm{res}^2 \mathcal{W}$).

Od četvrtog dizajna s parametrima 2-$(23, 7, 21)$, $x = 1$, $y = 3$ generiramo samoortogonalni binarni kod C_1 s proširenom matricom (18). Iz relacije (21) slijedi da je C_1 dvostruko parni, a iz propozicije 3.25 da je minimalna težina od $C_1^\perp$ barem 5. Po teoremu 3.19 možemo proširiti C_1 do dvostruko parnog samodualnog koda D, $C_1 \leq D \leq C_1^\perp$. Zbog dvostruke parnosti minimalna težina mu je bar 8, a zbog teorema 3.34 je točno 8. Dakle, D je kod s parametrima $[n, m, d, q] = [24, 12, 8, 2]$. Prema [112] i [64], jedini takav kod je prošireni Golayev kod G_{24} s težinskim polinomom $W_D(x, y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$. Nosači riječi težine 8 čine veliki Wittov dizajn $\mathcal{W}$, a polazni dizajn je izomorfan s $\mathrm{der}\, \mathcal{W}$.

Transponiranu incidencijsku matricu petog dizajna s parametrima 2-$(22, 7, 16)$, $x = 1$, $y = 3$ proširimo s dva stupca i jednim retkom do matrice

$$G_{10}^+ = \begin{bmatrix} 1 \cdots 1 & 1 & 1 \\ & 1 & 0 \\ A^\tau & \vdots & \vdots \\ & 1 & 0 \end{bmatrix}. \tag{22}$$

Kod C_{10}^+ generiran tom matricom nad $\mathbb{F}_2$ je samoortogonalan i dvostruko paran, a njegov dual $(C_{10}^+)^\perp$ dobiva se od koda $C_1^\perp$ proširivanjem po parnosti. Po propoziciji 3.25 minimalna težina od $C_1^\perp$ je bar 5, pa je minimalna težina od $(C_{10}^+)^\perp$ bar 6. Po teoremu 3.19 možemo proširiti C_{10}^+ do dvostruko parnog samodualnog koda D, $C_{10}^+ \leq D \leq (C_{10}^+)^\perp$, kojem je minimalna težina 8. To je ponovo prošireni Golayev kod G_{24}, a polazni dizajn je izomorfan s $\mathrm{res}(\mathrm{der}\, \mathcal{W})$. □

Tonchev je u [131] istom tehnikom dokazao nepostojanje sljedećih kvazisimetričnih dizajna.

Teorem 3.29. *Ne postoje kvazisimetrični dizajni s parametrima* 2-$(29, 7, 12)$, $x = 1$, $y = 3$ *i* 2-$(28, 7, 16)$, $x = 1$, $y = 3$.

Dokaz. Neka je C_1 binarni kod generiran proširenom matricom (18) od kvazisimetričnog 2-$(29, 7, 12)$ dizajna s $x = 1$, $y = 3$. Taj kod je samoortogonalan, ima dualnu težinu $d^\perp \geq 6$ i možemo ga proširiti do samodualnog koda D s parametrima $[n, m, d, q] = [30, 15, d, 2]$, $d \geq 6$. Od kvazisimetričnog 2-$(28, 7, 16)$ dizajna s $x = 1$, $y = 3$ dolazimo preko dvostruko proširene generirajuće matrice (22) do samodualnog koda D s istim parametrima. Prema [46] i [64], postoji 13 neekvivalentnih kodova s takvim parametrima, opisanih u tablici 4. Svi imaju minimalnu težinu $d = 6$, a težinski polinom im je $W(x, y) = x^{30} + A_6 x^{24} y^6 + A_8 x^{22} y^8 + A_{10} x^{20} y^{10} + A_{12} x^{18} y^{12} + A_{14} x^{16} y^{14} + A_{14} x^{14} y^{16} + A_{12} x^{12} y^{18} + A_{10} x^{10} y^{20} + A_8 x^8 y^{22} + A_6 x^6 y^{24} + y^{30}$. Neka je $\mathcal{B}$ incidencijska struktura kojoj su blokovi nosači vektora težine 8 u D. Blokovi polaznog 2-$(29, 7, 12)$ dizajna su neki od 7-članih skupova iz $\operatorname{der} \mathcal{B}$, a polaznog 2-$(28, 7, 16)$ dizajna iz $\operatorname{res}(\operatorname{der} \mathcal{B})$. U zadnjem stupcu tablice 4 navedeni su stupnjevi točaka u strukturi $\mathcal{B}$. Vidimo da su uvijek manji ili jednaki 112, a to znači da u $\operatorname{der} \mathcal{B}$ i $\operatorname{res}(\operatorname{der} \mathcal{B})$ nikad nema više od 112 podskupova veličine 7. Polazni dizajni imali bi $b = 232$ i $b = 288$ blokova i zato nisu mogući. □

Kod	d	A_6	A_8	A_{10}	A_{12}	A_{14}	Stupnjevi
D_1	6	35	345	1848	5320	8835	92
D_2	6	35	345	1848	5320	8835	92
D_3	6	27	369	1848	5256	8883	66, 102
D_4	6	35	345	1848	5320	8835	92
D_5	6	35	345	1848	5320	8835	92
D_6	6	35	345	1848	5320	8835	92
D_7	6	35	345	1848	5320	8835	92
D_8	6	35	345	1848	5320	8835	92
D_9	6	35	345	1848	5320	8835	92
D_{10}	6	19	393	1848	5192	8931	76, 112
D_{11}	6	19	393	1848	5192	8931	76, 112
D_{12}	6	35	345	1848	5320	8835	92
D_{13}	6	19	393	1848	5192	8931	76, 112

Tablica 4: Samodualni $[30, 15, d, 2]$ kodovi s $d \geq 6$.

Lema 4.1 iz [131] tvrdi da je stupanj točaka u $\mathcal{B}$ uvijek 92, što nije točno. Dokaz se poziva na pogrešnu klasifikaciju samodualnih kodova duljine 30 iz [114], koja je ispravljena u [46]. Međutim, isti argument za nepostojanje kvazisimetičnih dizajna s parametrima iz teorema 3.29 prolazi i za ispravljenu listu samodualnih kodova u tablici 4. Prema [134], nepostojanje kvazisimetričnih 2-$(29, 7, 12)$ dizajna ranije je dokazao W. Haemers u svojem diplomskom radu, koristeći se svojstvenim vrijednostima pridruženog jako regularnog grafa. Neposredni dokaz nepostojanja za jedne i druge parametre skiciran je u [124, napomena 10.12 na str. 198], a nepostojanje slijedi i iz teorema 2.26 (*ii*). Kao zadnji primjer primjene Tonchevljeve tehnike, dokazat ćemo nepostojanje dizajna br. 1–4 iz tablice 1.

Teorem 3.30. *Ne postoje kvazisimetrični dizajni s ovim parametrima:*

1. 2-$(20, 8, 14)$, $x = 2$, $y = 4$,
2. 2-$(20, 10, 18)$, $x = 4$, $y = 6$,
3. 2-$(19, 7, 7)$, $x = 1$, $y = 3$,
4. 2-$(19, 9, 16)$, $x = 3$, $y = 5$.

Dokaz. Binarni kod generiran transponiranom incidencijskom matricom prvog i drugog dizajna je samoortogonalan i ima dualnu težinu $d^\perp \geq 4$. Možemo ga proširiti do samodualnog koda D s parametrima $[n, m, d, q] = [20, 10, d, 2]$, $d \geq 4$. Do istog takvog koda D dolazimo preko proširene incidencijske matrice (18) trećeg i četvrtog dizajna iz iskaza teorema. Prema [64], postoji 7 neekvivalentnih kodova s takvim parametrima, opisanih u tablici 5. Imaju minimalnu težinu $d = 4$ i težinski polinom $W(x, y) = x^{20} + A_4 x^{16} y^4 + A_6 x^{14} y^6 + A_8 x^{12} y^8 + A_{10} x^{10} y^{10} + A_8 x^8 y^{12} + A_6 x^6 y^{14} + A_4 x^4 y^{16} + y^{20}$. Blokove

Kod	d	A_4	A_6	A_8	A_{10}
D_1	4	29	32	226	448
D_2	4	45	0	210	512
D_3	4	13	64	242	384
D_4	4	5	80	250	352
D_5	4	17	56	238	400
D_6	4	21	48	234	416
D_7	4	9	72	246	368

Tablica 5: Samodualni $[20, 10, d, 2]$ kodovi s $d \geq 4$.

prvog dizajna čine nekih $b = 95$ nosača vektora težine 8 u kodu D, a drugog dizajna nekih $b = 76$ nosača vektora težine 10. Problem izbora tih nosača tako da svaki od $\binom{20}{2}$ parova točaka bude pokriven točno $\lambda = 14$, odnosno $\lambda = 18$ puta rješavamo Kramer-Mesnerovom metodom. Niti za jedan od 7 kodova iz tablice 5 problem nema rješenja. Za treći i četvrti dizajn prvo uzimamo nosače vektora težine 8 ili 10 koji na čvrstoj koordinati imaju jedinicu, a zatim biramo $b = 57$ ili $b = 76$ punktiranih nosača koji pokrivaju svaki od $\binom{19}{2}$ parova točaka točno $\lambda = 7$ ili $\lambda = 16$ puta. Niti jedan od tih Kramer-Mesnerovih sustava također nema rješenja. Za traženje 0-1 rješenja sustava linearnih jednadžbi koristimo LLL solver A. Wassermanna [139]. $\square$

Nepostojanje kvazisimetričnih 2-$(19, 7, 7)$ dizajna slijedi direktno iz nepostojanja odgovarajućih jako regularnih grafova $SRG(57, 42, 31, 30)$ [140], ili iz teorema 3.35. Nepostojanje kvazisimetričnih 2-$(19, 9, 16)$ dizajna dokazao je bez računala Calderbank [33, tm. 12], a kvazisimetričnih 2-$(20, 8, 14)$ i 2-$(20, 10, 18)$ dizajna Calderbank i Frankl [36].

3.3 Calderbankovi teoremi

Teorem 3.31 (Gleason)**.** *Neka je C samodualni binarni kod.*

1. *Težinski polinom $W_C(x, y)$ može se izraziti kao polinom u varijablama $g = x^2 + y^2$ i $h = x^2y^2(x^2 - y^2)^2$.*

2. *Ako je C dvostruko paran, onda se težinski polinom $W_C(x, y)$ može izraziti kao polinom u varijablama $e = x^8 + 14x^4y^4 + y^8$ i $f = x^4y^4(x^4 - y^4)^4$.*

Korolar 3.32. *Duljina dvostruko parnog samodualnog binarnog koda djeljiva je s* 8.

Teorem 3.33. *Minimalna težina samodualnog binarnog koda duljine n zadovoljava $d \leq 2\lfloor n/8 \rfloor + 2$.*

Teorem 3.34 (Mallows, Sloane)**.** *Minimalna težina dvostruko parnog samodualnog binarnog koda duljine n zadovoljava $d \leq 4\lfloor n/24 \rfloor + 4$.*

Calderbank [33]: ne postoje 2-$(19, 9, 16)$, 2-$(22, 8, 12)$, 2-$(33, 9, 6)$ i kriterij

Teorem 3.35. *Neka postoji 2-(v, k, λ) dizajn kojem su svi presječni brojevi kongruentni x modulo 2. Onda vrijedi bar jedna od tvrdnji*

(1) $r \equiv \lambda \pmod 4$,

(2) $x = 0$, $k \equiv 0 \pmod 4$, $v \equiv \pm 1 \pmod 8$,

(3) $x = 1$, $k \equiv v \pmod 4$, $v \equiv \pm 1 \pmod 8$.

Calderbank [35]:

Teorem 3.36. *Neka je p neparan prost broj i neka postoji 2-(v, k, λ) dizajn kojem su svi presječni brojevi kongruentni x modulo p. Onda vrijedi bar jedna od tvrdnji*

(1) $r \equiv \lambda \pmod{p^2}$,

(2) *v je paran,* $v \equiv k \equiv x \equiv 0 \pmod p$, $(-1)^{v/2}$ *je kvadrat u* $\mathbb{F}_p$,

(3) *v je neparan,* $v \equiv k \equiv x \not\equiv 0 \pmod p$, $(-1)^{(v-1)/2}x$ *je kvadrat u* $\mathbb{F}_p$,

(4) $r \equiv \lambda \equiv 0 \pmod p$ *i vrijedi bar jedna od tvrdnji*

   (a) *v je paran,* $v \equiv k \equiv x \not\equiv 0 \pmod p$,
   (b) *v je paran,* $k \equiv x \not\equiv 0 \pmod p$, *$v/x$ je nekvadrat u* $\mathbb{F}_p$,
   (c) $v \equiv 1 \pmod{2p}$, $r \equiv 0 \pmod{p^2}$, $k \equiv x \not\equiv 0 \pmod p$,
   (d) $v \equiv p \pmod{2p}$, $k \equiv x \equiv 0 \pmod p$,
   (e) *v je neparan,* $k \equiv x \equiv 0 \pmod p$, *$v$ je nekvadrat u* $\mathbb{F}_p$,
   (f) *v je neparan,* $k \equiv x \equiv 0 \pmod p$, *$v$ i* $(-1)^{(v-1)/2}$ *su kvadrati u* $\mathbb{F}_p$.

4 Familije kvazisimetričnih dizajna

4.1 Simetrični dizajni

Simetrični dizajni mogu se smatrati kvazisimetričnim s jednakim presječnim brojevima $x = y$. Osim uvjeta $\lambda(v-1) = k(k-1)$, poznat je sljedeći netrivijalni nužni uvjet za egzistenciju.

Teorem 4.1 (Bruck-Ryser-Chowla)**.** *Neka postoji simetrični (v, k, λ) dizajn reda $n = k - \lambda$.*

(1) *Ako je v paran, onda je n kvadrat prirodnog broja.*

(2) *Ako je v neparan, onda jednadžba $nx^2 + (-1)^{\frac{v-1}{2}}\lambda y^2 = z^2$ ima netrivijalno cjelobrojno rješenje.*

Teorem 4.1 je generalizacija teorema 1.32. Dokaz je prikazan u poglavlju 7 skripte [129]. U članku [70] opisano je 21 beskonačnih familija simetričnih dizajna i mnogi sporadični primjeri. U tablici 6 navodimo dopustive parametre simetričnih dizajna s $v \leq 78$. Podaci o broju neizomorfnih dizajna u stupcu 'Nd' preuzeti su iz [97]. Primijetimo da za $v \leq 78$ nema niti jedne trojke (v, k, λ) za koju je egzistencija simetričnih dizajna otvoreno pitanje. Najmanji simetrični dizajni za koje je egzistencija nepoznata su troravnine $(81, 16, 3)$.

Br.	v	k	λ	Nd	Napomene
1	7	3	1	1	$PG(2,2)$
2	11	5	2	1	
3	13	4	1	1	$PG(2,3)$
4	15	7	3	5	$PG_2(3,2)$
5	16	6	2	3	
6	19	9	4	6	
7	21	5	1	1	$PG(2,4)$
8	22	7	2	0	Teorem 4.1 (1)
9	23	11	5	1106	
10	25	9	3	78	
11	27	13	6	208310	
12	29	8	2	0	Teorem 4.1 (2)
13	31	6	1	1	$PG(2,5)$
14	31	10	3	151	
15	31	15	7	$\geq$22478260	$PG_3(4,2)$
16	34	12	4	0	Teorem 4.1 (1)

Tablica 6: Dopustivi parametri simetričnih dizajna.

Br.	v	k	λ	Nd	Napomene
17	35	17	8	$\geq$108131	
18	36	15	6	$\geq$25634	
19	37	9	2	4	
20	39	19	9	$\geq 5.87 \cdot 10^{14}$	
21	40	13	4	$\geq$1108800	$PG_2(3,3)$
22	41	16	6	$\geq$115307	
23	43	7	1	0	Teorem 4.1 (2)
24	43	15	5	0	Teorem 4.1 (2)
25	43	21	10	$\geq$82	
26	45	12	3	$\geq$3752	
27	46	10	2	0	Teorem 4.1 (1)
28	47	23	11	$\geq$55	
29	49	16	5	$\geq$12146	
30	51	25	12	$\geq$1	
31	52	18	6	0	Teorem 4.1 (1)
32	53	13	3	0	Teorem 4.1 (2)
33	55	27	13	$\geq$1	
34	56	11	2	5	[82]
35	57	8	1	1	$PG(2,7)$
36	58	19	6	0	Teorem 4.1 (1)
37	59	29	14	$\geq$1	
38	61	16	4	$\geq$6	
39	61	21	7	0	Teorem 4.1 (2)
40	61	25	10	$\geq$24	
41	63	31	15	$\geq 10^{17}$	$PG_4(5,2)$
42	64	28	12	$\geq$8784	
43	66	26	10	$\geq$588	
44	67	12	2	0	Teorem 4.1 (2)
45	67	22	7	0	Teorem 4.1 (2)
46	67	33	16	$\geq$1	
47	69	17	4	$\geq$4	
48	70	24	8	$\geq$28	
49	71	15	3	$\geq$72	
50	71	21	6	$\geq$2	
51	71	35	17	$\geq$9	
52	73	9	1	1	$PG(2,8)$
53	75	37	18	$\geq$1	
54	76	25	8	0	Teorem 4.1 (1)
55	77	20	5	0	Teorem 4.1 (2)
56	78	22	6	$\geq$3	

Tablica 6: Dopustivi parametri simetričnih dizajna (nastavak).

4.2 Jako rastavljivi dizajni

Za dizajn kažemo da je *α-rastavljiv* ako se skup blokova može particionirati na disjunktne klase $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_c$ tako da je svaka točka sadržana u α blokova iz svake klase. U slučaju $\alpha = 1$ govorimo o *rastavljivosti*, a klase nazivamo *klasama paralelnosti.* Za rastavljive dizajne vrijedi poboljšanje Fisherove nejednakosti poznato kao Boseova nejednakost.

Teorem 4.2. *Ako je dizajn α-rastavljiv na c klasa, onda vrijedi $b \geq v + c - 1$.*

Dokaz. Dvostrukim prebrojavanjem vidimo da je $|\mathcal{B}_i|\, k = v\alpha$, tj. veličina svake klase je $m = |\mathcal{B}_i| = \frac{v\alpha}{k}$. Neka je A incidencijska matrica dizajna. Proširimo je do $(v+c) \times (b+1)$ matrice na sljedeći način:

$$A_1 = \left[\begin{array}{cccc|c} & & & & 1 \\ & & A & & \vdots \\ & & & & 1 \\ \hline 1\cdots 1 & & & & 0 \\ & 1\cdots 1 & & & 0 \\ & & \ddots & & \vdots \\ \underbrace{}_{m} & \underbrace{}_{m} & & \underbrace{1\cdots 1}_{m} & 0 \end{array}\right].$$

Pretpostavljamo da prvih m stupaca incidencijske matrice odgovara blokovima iz klase $\mathcal{B}_1$, idućih m stupaca blokovima iz klase $\mathcal{B}_2$ itd. Pokazuje se da vrijedi

$$A_1 \cdot A_1^{\tau} = \left[\begin{array}{ccc|ccc} & & & \alpha & \cdots & \alpha \\ & nI + (\lambda+1)J & & \vdots & & \vdots \\ & & & \alpha & \cdots & \alpha \\ \hline \alpha & \cdots & \alpha & m & & 0 \\ \vdots & & \vdots & & \ddots & \\ \alpha & \cdots & \alpha & 0 & & m \end{array}\right].$$

Ovdje je I jedinična matrica reda v, J je $v \times v$ matrica popunjena jedinicama, a $n = r - \lambda$ je red dizajna. Determinanta te matrice je $\det(A_1 \cdot A_1^{\tau}) = vn^{v-1}m^c \neq 0$ i ona je punog ranga $v + c$. Zato je i matrica A_1 ranga $v + c$, pa joj je broj stupaca $b + 1 \geq v + c$. $\square$

R.C. Bose [21] dokazao je nejednakost za $\alpha = 1$, kad je broj klasa $c = r$. Gornji dokaz za opći α je iz [68]. Za α-rastavljivi dizajn kažemo da je *jako rastavljiv* ako se svaka dva bloka iz iste klase sijeku u x točaka, a svaka dva bloka iz različitih klasa sijeku se u y točaka. Jako rastavljivi dizajn je kvazisimetričan i pridruženi blokovni graf je potpun c-partitini graf $K_{m,\ldots,m}$. U teoremu 2.23 vidjeli smo da vrijedi i obrat te tvrdnje. Sad ćemo izraziti presječne brojeve jako rastavljivog dizajna preko ostalih parametara.

Propozicija 4.3. *Presječni brojevi jako rastavljivog dizajna su* $x = k - n$ *i* $y = k^2/v$.

Dokaz. Brojanjem trojki (P, B_1, B_2), gdje je P točka incidentna s blokovima $B_1 \in \mathcal{B}_i$, $B_2 \in \mathcal{B}_j$ iz različitih klasa, dobijemo $v\alpha^2 = m^2 y$. Iz te jednadžbe i $mk = v\alpha$ slijedi $y = k^2/v$. Formulu za x dobijemo iz jednadžbe (9). $\square$

Idući teorem iz [68] karakterizira jako rastavljive dizajne kao one koji dostižu Boseovu nejednakost (slučaj $\alpha = 1$ dokazan je već u [21]). Jako rastavljive dizajne s $\alpha = 1$ nazivamo *afino rastavljivim.*

Teorem 4.4. *Neka je* $\mathcal{D}$ α*-rastavljivi dizajn s klasama* $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_c$. *Rastav je jak ako i samo ako vrijedi jednakost* $b = v + c - 1$.

Dokaz. Neka vrijedi $v + c = b + 1$. Tada je matrica A_1 iz dokaza teorema 4.2 kvadratna. Množenjem zdesna $(A_1 \cdot A_1^{-1})$ provjeri se da joj je inverzna matrica

$$A_1^{-1} = \left[\begin{array}{c|cccc}
 & \frac{1}{m} & & & \\
 & \vdots & & & \\
 & \frac{1}{m} & & & \\
 & & \frac{1}{m} & & \\
 & & \vdots & & \\
\frac{1}{n}A^\tau - \frac{k}{nv}J_{b,v} & & \frac{1}{m} & & \\
 & & & \ddots & \\
 & & & & \frac{1}{m} \\
 & & & & \vdots \\
 & & & & \frac{1}{m} \\
\hline
\frac{1}{v} \quad \cdots \quad \frac{1}{v} & -\frac{k}{nv} & -\frac{k}{nv} & \cdots & -\frac{k}{nv}
\end{array}\right]
\begin{array}{l}
\left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\}m \\
\left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\}m \\
\\
\left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\}m \\
\\
\end{array}.$$

Ovdje je $J_{b,v}$ matrica dimenzija $b \times v$ popunjena jedinicama. Množenjem s lijeva $(A_1^{-1} \cdot A_1)$ i izjednačavanjem s jediničnom matricom dobijemo

$$A^\tau \cdot A = nI_b + \frac{k^2}{v}J_b - \frac{n}{m}\begin{bmatrix} J_m & 0 & \cdots & 0 \\ 0 & J_m & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_m \end{bmatrix}.$$

Desno je matrica koja na dijagonali ima $m \times m$ podmatrice popunjene jedinicama, a ostali unosi su nule. To znači da se blokovi iz različitih klasa sijeku u $y = k^2/v$ točaka, a blokovi iz iste klase u $x = k^2/v - n/m$ točaka.

Obrnuto, neka je $\mathcal{D}$ jako rastavljiv i pretpostavimo da blokovi iz istih klasa odgovaraju uzastopnim stupcima incidencijske matrice A. Tada je

$$A^\tau \cdot A = \begin{bmatrix} D & yJ_m & \cdots & yJ_m \\ yJ_m & D & \cdots & yJ_m \\ \vdots & \vdots & \ddots & \vdots \\ yJ_m & yJ_m & \cdots & D \end{bmatrix},$$

gdje su na dijagonali matrice $D = (k - x)I_m + xJ_m$. To je matrica punog ranga b, pa za matricu A_1 iz dokaza teorema 4.2 vrijedi da je $A_1^\tau \cdot A_1$ ranga $b + 1$. No tada je i A_1 ranga $b + 1$, pa je $v + c = b + 1$. $\square$

Korolar 4.5. *Ako postoji jako rastavljivi dizajn s parametrima (v, k, λ) i c klasa veličine m, onda je $vn^{v-1}m^c$ kvadrat prirodnog broja.*

Dokaz. Matrica A_1 iz dokaza teorema 4.2 je kvadratna, pa je $vn^{v-1}m^c = \det(A_1 \cdot A_1^\tau) = (\det A_1)^2$. $\square$

Naprimjer, ne postoji $(45, 15, 7)$ dizajn sa $c = 22$ klasa veličine $m = 3$, jer $vn^{v-1}m^c = 3^{68}\,5^{45}$ nije kvadrat. Afini dizajni $AG_d(n, q)$ opisani u propoziciji 4.20 su rastavljivi. Za $d = n-1$ dostižu Boseovu nejednakost, pa su afino rastavljivi. U tom slučaju parametri su $(v, k, \lambda) = (q^n, q^{n-1}, \left[{n-1 \atop 1}\right]_q)$, $\alpha = 1$, $m = q$, $c = \left[{n \atop 1}\right]_q$, $x = 0$ i $y = q^{n-2}$. Još jedna familija afino rastavljivih dizajna su Hadamardovi 3-dizajni. U teoremu 1.35 vidjeli smo kako ih konstruirati od blokova B_i simetričnog $(4n-1, 2n-1, n-1)$ dizajna. Parovi $\{B_i^1, B_i^2\}$ čine particiju skupa točaka proširenog dizajna, pa je on rastavljiv s parametrima 2-$(4n, 2n, 2n-1)$, $b = 8n-2$, $\alpha = 1$, $m = 2$, $c = 4n-1$. Dostižu Boseovu nejednakost i presječni brojevi su $x = 0$, $y = n$. Hadamardovi dizajni postoje ako i samo ako postoji Hadamardova matrica reda $4n$, a afini dizajni $AG_{n-1}(n, q)$ postoje za svaki $n \geq 2$ i prim potenciju q. Pregled rezultata o afino rastavljivim dizajnima dan je u [125]. U [12] je karakterizirana generalizacija pojma jakog rastava, tzv. jaka taktička dekompozicija dizajna, i dokazano je da su jedini jako rastavljivi 3-dizajni Hadamardovi.

Parametre jako rastavljivih dizajna možemo zapisati u sljedećem obliku. Presječni broj blokova iz različitih klasa je $y = k^2/v$. Broj blokova u svakoj klasi je $m = \alpha v/k = \alpha k/y$, pa je $k = my/\alpha$. Nadalje, $v = k^2/y = m^2y/\alpha^2$ i $\lambda = (my - \alpha)/(m - 1)$. Dakle, svaki jako rastavljivi dizajn ima parametre oblika $(v, k, \lambda) = (\frac{m^2y}{\alpha^2}, \frac{my}{\alpha}, \frac{my-\alpha}{m-1})$. Obrnuto, svaki rastavljivi dizajn s

Br.	v	k	λ	x	y	r	b	α	m	c	Nr	Napomene
1	8	4	3	0	2	7	14	1	2	7	1	$AG_2(3,2)$, Hadamard
2	9	3	1	0	1	4	12	1	3	4	1	$AG(2,3)$
3	12	6	5	0	3	11	22	1	2	11	1	Hadamard
4	16	4	1	0	1	5	20	1	4	5	1	$AG(2,4)$
5	16	8	7	0	4	15	30	1	2	15	5	$AG_3(4,2)$, Hadamard
6	20	10	9	0	5	19	38	1	2	19	3	Hadamard
7	24	12	11	0	6	23	46	1	2	23	130	Hadamard
8	25	5	1	0	1	6	30	1	5	6	1	$AG(2,5)$
9	27	9	4	0	3	13	39	1	3	13	68	$AG_2(3,3)$
10	28	14	13	0	7	27	54	1	2	27	7570	Hadamard
11	32	16	15	0	8	31	62	1	2	31	$\geq$1	$AG_4(5,2)$, Hadamard
12	36	6	1	0	1	7	42	1	6	7	0	
13	36	18	17	0	9	35	70	1	2	35	$\geq$91	Hadamard
14	40	20	19	0	10	39	78	1	2	39	$\geq$1	Hadamard
15	44	22	21	0	11	43	86	1	2	43	$\geq$1	Hadamard
16	45	15	7	0	5	22	66	1	3	22	0	Korolar 4.5
17	48	24	23	0	12	47	94	1	2	47	$\geq$1	Hadamard
18	49	7	1	0	1	8	56	1	7	8	1	$AG(2,7)$
19	49	21	10	7	9	24	56	3	7	8	$\geq$10000	Teorem 4.6
20	52	26	25	0	13	51	102	1	2	51	$\geq$1	Hadamard
21	56	28	27	0	14	55	110	1	2	55	$\geq$1	Hadamard
22	60	30	29	0	15	59	118	1	2	59	$\geq$1	Hadamard
23	63	21	10	0	7	31	93	1	3	31	0	Korolar 4.5
24	64	8	1	0	1	9	72	1	8	9	1	$AG(2,8)$
25	64	16	5	0	4	21	84	1	4	21	$\geq$157	$AG_2(3,4)$
26	64	32	31	0	16	63	126	1	2	63	$\geq$1	Hadamard
27	68	34	33	0	17	67	134	1	2	67	$\geq$1	Hadamard
28	72	36	35	0	18	71	142	1	2	71	$\geq$1	Hadamard
29	76	38	37	0	19	75	150	1	2	75	$\geq$1	Hadamard

Tablica 7: Dopustivi parametri jako rastavljivih dizajna.

parametrima tog oblika je jako rastavljiv. Dopustive parametre jako rastavljivih dizajna s $2k \leq v \leq 78$ izdvojili smo u tablicu 7. Vidimo da su svi osim dizajna br. 19 afino rastavljivi, tj. imaju parametar $\alpha = 1$. Broj neizomorfnih dizajna naveden je u stupcu 'Nr'. Za afino rastavljive dizajne podatak je preuzet iz [97], a dizajne br. 19 dobivamo s pomoću sljedeće konstrukcije iz [126].

Teorem 4.6. *Ako postoji simetrični (v_1, k_1, λ_1) dizajn $\mathcal{D}_1$ i afino rastavljivi (v_2, k_2, λ_2) dizajn $\mathcal{D}_2$ reda $n_2 = r_2 - \lambda_2$ s v_1 blokova u svakoj klasi paralel-*

nosti, onda postoji jako rastavljivi $(v_2, k_1k_2, \lambda_2k_1 + n_2\lambda_1)$ *dizajn* $\mathcal{D}$ *s* $\alpha = k_1$ *i presječnim brojevima* $x = k_2\lambda_1$, $y = k_1^2k_2/v_1$.

Dokaz. Neka su blokovi dizajna $\mathcal{D}_2$ particionirani u klase $\mathcal{B}_1 \cup \dots \cup \mathcal{B}_c$, gdje je $c = r_2$ broj blokova kroz svaku točku od $\mathcal{D}_2$. Blokove iz klase $\mathcal{B}_i$ bijektivno pridružimo točkama dizajna $\mathcal{D}_1$ i definiramo novu klasu $\mathcal{B}_i'$ na sljedeći način. Za svaki blok B simetričnog dizajna $\mathcal{D}_1$ napravimo uniju k_1 blokova iz $\mathcal{B}_i$ koje odgovaraju točkama na B. Nova klasa $\mathcal{B}_i'$ sastoji se od v_1 blokova veličine k_1k_2 koje pokrivaju svaku točku $\alpha = k_1$ puta. Neka je $\mathcal{D}$ incidencijska struktura s istim skupom točaka kao $\mathcal{D}_2$ i blokovima $\mathcal{B}_1' \cup \dots \cup \mathcal{B}_c'$. Kroz svake dvije njezine točke T_1 i T_2 prolazi λ_2 blokova dizajna $\mathcal{D}_2$, a svaki je sadržan u k_1 blokova nove strukture $\mathcal{D}$. Osim toga točka T_1 sadržana je u $n_2 = r_2 - \lambda_2$ blokova od $\mathcal{D}_2$ koji ne sadrže T_2, a svaki od njih sadržan je u λ_1 novih blokova koji sadrže i T_2. Dakle, kroz T_1 i T_2 prolazi ukupno $\lambda = \lambda_2k_1 + n_2\lambda_1$ blokova od $\mathcal{D}$, pa je nova struktura rastavljivi 2-dizajn. Dva bloka iz iste klase $\mathcal{B}_i'$ očito se sijeku u $x = k_2\lambda_1$ točaka. Zbog afine rastavljivosti od D_2, njegovi blokovi iz različitih klasa $\mathcal{B}_i$, $\mathcal{B}_j$ sijeku se u $\frac{k_2^2}{v_2}$ točaka. Zato se blokovi od $\mathcal{D}$ iz različitih klasa $\mathcal{B}_i'$, $\mathcal{B}_j'$ sijeku u $y = k_1^2 \cdot \frac{k_2^2}{v_2} = k_1^2k_2/v_1$ točaka. Dakle, $\mathcal{D}$ je jako rastavljiv. $\square$

Ako za $\mathcal{D}_1$ uzmemo Fanovu ravninu $PG(2,2)$, a za $\mathcal{D}_2$ afinu ravninu $AG(2,7)$, dobivamo afino rastavljive dizaje br. 19 iz tablice 7. Točke od $\mathcal{D}_1$ možemo bijektivno pridružiti blokovima pojedinih klasa od $\mathcal{D}_2$ na $(v_1!)^c$ načina. Pritom općenito dobivamo neizomorfne dizajne. Konstruirali smo 10000 dizajna s parametrima br. 19 i s pomoću računala provjerili neizomorfnost. Druge jako rastavljive dizajne s $\alpha > 1$ dobivamo kao komplemente afino rastavljivih dizajna. Komplement jako rastavljivog (v, k, λ)

v	k	λ	x	y	r	b	α	m	c	Egzistencija
49	21	10	7	9	24	56	3	7	8	Tm. 4.6: $\mathcal{D}_1 = PG(2,2)$, $\mathcal{D}_2 = AG(2,7)$
121	55	27	22	25	60	132	5	11	12	Tm. 4.6: $\mathcal{D}_1 = (11,5,2)$, $\mathcal{D}_2 = AG(2,11)$
169	52	17	13	16	56	182	4	13	14	Tm. 4.6: $\mathcal{D}_1 = PG(2,3)$, $\mathcal{D}_2 = AG(2,13)$
225	105	52	45	49	112	240	7	15	16	?
256	96	38	32	36	102	272	6	16	17	Tm. 4.6: $\mathcal{D}_1 = (16,6,2)$, $\mathcal{D}_2 = AG(2,16)$
343	147	73	49	63	171	399	3	7	57	Tm. 4.6: $\mathcal{D}_1 = PG(2,2)$, $\mathcal{D}_2 = AG_2(3,7)$
441	105	26	21	25	110	462	5	21	22	?
961	186	37	31	36	192	992	6	31	32	Tm. 4.6: $\mathcal{D}_1 = PG(2,5)$, $\mathcal{D}_2 = AG(2,31)$
1849	301	50	43	49	308	1892	7	43	44	?

Tablica 8: Jako rastavljivi dizajni s $\alpha > 1$ i $x \leq 55$.

dizajna s parametrima α, m, c i presječnim brojevima x, y ima parametre $(\overline{v}, \overline{k}, \overline{\lambda}) = (v, v-k, b-2r+\lambda)$, $\overline{\alpha} = m-\alpha$, $\overline{m} = m$, $\overline{c} = c$, $\overline{x} = v-2k+x$ i $\overline{y} = v-2k+y$. U radu [16] navedeni su svi dopustivi parametri jako rastavljivih dizajna s $\alpha > 1$ i $x \leq 55$. U tablici 8 navodimo one koji uz to zadovoljavaju $2k \leq v$ s podacima o egzistenciji iz [16].

4.3 Steinerovi 2-dizajni

Steinerovim nazivamo dizajne s parametrom $\lambda = 1$. Ako je uz to $t = 2$, dizajn je automatski kvazisimetričan s presječnim brojevima $x = 0$, $y = 1$. Egzistencija Steinerovih 2-dizajna obično se razmatra za fiksni k. Za $k = 3$ uvjeti djeljivosti iz korolara 1.4 svode se na $v \equiv 1$ ili $3 \pmod 6$, a Fisherova nejednakost (teorem 1.8) na $v \geq 7$. To su nužni uvjeti za postojanje *Steinerovih sustava trojki*. Još je Kirkman [84] dokazao da su oni dovoljni za egzistenciju, prije nego što je Steiner [127] postavio pitanje. Za $k = 4$ nužni uvjeti su $v \equiv 1$ ili $4 \pmod{12}$, $v \geq 13$, a za $k = 5$ nužni uvjeti su $v \equiv 1$ ili $5 \pmod{20}$, $v \geq 21$. Haim Hanani [62] dokazao je da su ti uvjeti ujedno dovoljni za egzistenciju 2-$(v, 4, 1)$ i 2-$(v, 5, 1)$ dizajna.

Za $k = 6$ nužni uvjeti su $v \equiv 1$ ili $6 \pmod{15}$, $v \geq 31$ i oni nisu dovoljni za egzistenciju. Poznato je da ne postoje 2-$(36, 6, 1)$ dizajni (afina ravnina reda 6) i 2-$(46, 6, 1)$ dizajni [66]. Prema tablici 3.4 u [1], egzistencija 2-$(v, 6, 1)$ dizajna je otvorena za 29 parametara $v \in \{51, 61, 81, 166, 226, 231, 256, 261, 286, 316, 321, 346, 351, 376, 406, 411, 436, 441, 471, 501, 561, 591, 616, 646, 651, 676, 771, 796, 801\}$, a za sve ostale dopustive v poznato je da dizajni postoje. Za $k = 7$ poznato je da ne postoje 2-$(43, 7, 1)$ dizajni (projektivna ravnina reda 6) i egzistencija je otvorena za 21 dopustivih parametara v, za $k = 8$ egzistencija je otvorena za 38 dopustivih v, a za $k = 9$ za 91 dopustivih v [1]. Prema Wilsonovom rezultatu [142] za svaki k može biti samo konačno mnogo dopustivih v za koje 2-$(v, k, 1)$ dizajni ne postoje.

Poznate su i druge beskonačne familije Steinerovih 2-dizajna pored projektivnih ravnina 2-$(n^2+n+1, n+1, 1)$ i afinih ravnina 2-$(n^2, n, 1)$. Jedna takva familija su *unitali* s parametrima 2-$(n^3+1, n+1, 1)$. Oni postoje uvijek kad je n prim potencija i za $n = 6$ [96, 10, 89], a za sve ostale n egzistencija je otvorena. Unitalima je posvećena skripta [87].

U tablici 9 navodimo dopustive parametre Steinerovih 2-dizajna s $v \leq 78$ i rezultate o broju neizomorfnih dizajna prema [97] i odgovarajućih jako regularnih grafova prema [30]. Isključili smo projektivne i afine ravnine, koje su pokrivene tablicama 6 i 7. Sa $PG(n, q)$ označen je dizajn točaka i pravaca u n-dimenzionalnom projektivnom prostoru nad poljem $\mathbb{F}_q$, sa $AG(n, q)$ dizajn točaka i pravaca u n-dimenzionalnom afinom prostoru nad $\mathbb{F}_q$, a $U(n)$ označava unital 2-$(n^3+1, n+1, 1)$.

Br.	v	k	λ	r	b	a	c	d	Nd	Nsrg	Napomene
1	13	3	1	6	26	15	8	9	2	10	
2	15	3	1	7	35	18	9	9	80	3854	$PG(3,2)$
3	19	3	1	9	57	24	11	9	11084874829	$\geq$1	
4	21	3	1	10	70	27	12	9	$\geq$62336617	$\geq$1	
5	25	3	1	12	100	33	14	9	$\geq 10^{14}$	$\geq$1	
6	25	4	1	8	50	28	15	16	18	$\geq$1	
7	27	3	1	13	117	36	15	9	$\geq 10^{11}$	$\geq$1	$AG(3,3)$
8	28	4	1	9	63	32	16	16	$\geq$4747	$\geq$1	$U(3)$
9	31	3	1	15	155	42	17	9	$\geq 6 \cdot 10^{16}$	$\geq$1	$PG(4,2)$
10	33	3	1	16	176	45	18	9	$\geq 10^{13}$	$\geq$1	
11	37	3	1	18	222	51	20	9	$\geq 10^{10}$	$\geq$1	
12	37	4	1	12	111	44	19	16	$\geq$51402	$\geq$1	
13	39	3	1	19	247	54	21	9	$\geq 10^{44}$	$\geq$1	
14	40	4	1	13	130	48	20	16	$\geq 10^{6}$	$\geq$1	$PG(3,3)$
15	41	5	1	10	82	45	24	25	$\geq$15	$\geq$1	
16	43	3	1	21	301	60	23	9	$\geq 5 \cdot 10^{64}$	$\geq$1	
17	45	3	1	22	330	63	24	9	$\geq 6 \cdot 10^{76}$	$\geq$1	
18	45	5	1	11	99	50	25	25	$\geq$16	$\geq$1	
19	46	6	1	9	69	48	32	36	0	?	
20	49	3	1	24	392	69	26	9	$\geq 6 \cdot 10^{14}$	$\geq$1	
21	49	4	1	16	196	60	23	16	$\geq$769	$\geq$1	
22	51	3	1	25	425	72	27	9	$\geq 6 \cdot 10^{53}$	$\geq$1	
23	51	6	1	10	85	54	33	36	?	?	
24	52	4	1	17	221	64	24	16	$\geq$206	$\geq$1	
25	55	3	1	27	495	78	29	9	$\geq 6 \cdot 10^{76}$	$\geq$1	
26	57	3	1	28	532	81	30	9	$\geq 10^{90}$	$\geq$1	
27	61	3	1	30	610	87	32	9	$\geq 2 \cdot 10^{24}$	$\geq$1	
28	61	4	1	20	305	76	27	16	$\geq$18132	$\geq$1	
29	61	5	1	15	183	70	29	25	$\geq$10	$\geq$1	
30	61	6	1	12	122	66	35	36	?	$\geq$1	
31	63	3	1	31	651	90	33	9	$\geq 10^{42}$	$\geq$1	$PG(5,2)$
32	64	4	1	21	336	80	28	16	$\geq 1.4 \cdot 10^{31}$	$\geq$1	$AG(3,4)$
33	65	5	1	16	208	75	30	25	$\geq$1777	$\geq$1	$U(4)$, [88]
34	66	6	1	13	143	72	36	36	$\geq$3	$\geq$1	[86]
35	67	3	1	33	737	96	35	9	$\geq 10^{35}$	$\geq$1	
36	69	3	1	34	782	99	36	9	$\geq 4 \cdot 10^{41}$	$\geq$1	
37	73	3	1	36	876	105	38	9	$\geq 10^{34}$	$\geq$1	
38	73	4	1	24	438	92	31	16	$\geq 10^{7}$	$\geq$1	
39	75	3	1	37	925	108	39	9	$\geq 10^{196}$	$\geq$1	
40	76	4	1	25	475	96	32	16	$\geq$169574	$\geq$1	
41	76	6	1	15	190	84	38	36	$\geq$1	$\geq$1	

Tablica 9: Dopustivi parametri Steinerovih 2-dizajna s $v > k^2$.

4.4 Rezidualni i derivirani simetrični dizajni

Definicija 4.7. *Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ simetrični (v, k, λ) dizajn i $B_0 \in \mathcal{B}$ jedan njegov blok. Definiramo* rezidualni dizajn *kao incidencijsku strukturu*

$$\mathrm{res}_{B_0}\mathcal{D} = (\,\mathcal{P} \setminus B_0,\ \{B \setminus B_0 \mid B \in \mathcal{B}, B \neq B_0\}\,),$$

a derivirani dizajn *kao incidencijsku strukturu*

$$\mathrm{der}_{B_0}\mathcal{D} = (\,B_0,\ \{B \cap B_0 \mid B \in \mathcal{B}, B \neq B_0\}\,).$$

Propozicija 4.8. *Struktura* $\mathrm{res}_{B_0}\,\mathcal{D}$ *je 2-dizajn s parametrima $v' = v - k$, $k' = k - \lambda$, $\lambda' = \lambda$, $r' = k$ i $b' = v - 1$.*

Dokaz. Izbacivanjem točaka koje pripadaju B_0 preostaje $v' = v - k$ točaka i $k' = k - \lambda$ točaka na svakom bloku (svaka dva bloka simetričnog dizajna sijeku se u λ točaka). Kroz svake dvije preostale točke prolazi $\lambda' = \lambda$ blokova, a kroz jednu točku $r' = k$. Ukupan broj preostalih blokova je $b' = v - 1$. □

Parametri rezidualnog dizajna zadovoljavaju $r' = k' + \lambda'$. Svaki 2-dizajn s tim svojstvom nazivamo *kvazirezidualnim.*

Propozicija 4.9. *Struktura* $\mathrm{der}_{B_0}\,\mathcal{D}$ *je 2-dizajn s parametrima $v' = k$, $k' = \lambda$, $\lambda' = \lambda - 1$, $r' = k - 1$ i $b' = v - 1$.*

Dokaz. Izbacivanjem točaka koje ne pripadaju B_0 preostaje $v' = k$ točaka i $k' = \lambda$ točaka na svakom bloku. Kroz svake dvije preostale točke prolazi $\lambda' = \lambda - 1$ blokova različitih od B_0, a kroz jednu točku $r' = k - 1$. Ukupan broj preostalih blokova je $b' = v - 1$. □

Parametri deriviranog dizajna zadovoljavaju $k' = \lambda' + 1$. Svaki 2-dizajn s tim svostvom nazivamo *kvaziderivirani m.* Kvazirezidualni i kvaziderivirani dizajni ne moraju biti rezidualni i derivirani, tj. ne može ih se uvijek proširiti do simetričnog dizajna. Naprimjer, postoji 2-$(16, 6, 3)$ dizajn s $r = 9$, $b = 24$ i s blokovima koji se sijeku u 4 točke. Zato ga ne možemo proširiti do simetričnog $(25, 9, 3)$ dizajna, tj. nije rezidualni. Daljnji primjeri kvazirezidualnih dizajna koji nisu rezidualni konstruirani su u članku [137], a primjeri kvaziderviranih dizajna koji nisu derivirani u članku [136].

Kvazirezidualni dizajni s $\lambda = 1$ su afine ravnine (iz $r = k + 1$ slijedi $v = k^2$). Uvijek ih je moguće proširiti do simetričnog dizajna poznatom konstrukcijom dodavanja točaka i pravca u beskonačnosti. Naime, iz $r = k+1$ slijedi Playfairov aksiom o paralelama, zbog kojeg je paralelnost relacija ekvivalencije. Pravcima iz svake od r klasa paralelnosti dodajemo jednu novu točku i r dodanih točaka stavimo na pravac u beskonačnosti. Tako dobivamo projektivnu ravninu čiji se rezidualni dizajn obzirom na pravac u beskonačnosti podudara s polaznom afinom ravninom.

Promotrimo sada rezidualne dizajne dvoravnina, tj. simetričnih dizajna s $\lambda = 2$. Za čvrsti blok B_0 dvoravnine možemo uspostaviti bijekciju između blokova različitih od B_0 i parova točaka iz B_0. Svaki drugi blok siječe B_0 u dvije točke i za svake dvije točke iz B_0 postoji točno jedan drugi blok koji ih sadrži. Zato dvoravnina ima $b = v = \binom{k}{2} + 1$ blokova i točaka.

Rezidualni dizajn dvoravnine ima parametre $v' = v - k = \frac{k^2-3k+2}{2}$, $k' = k - 2$, $\lambda' = 2$, $r' = k$ i $b' = \binom{k}{2}$. Blokovi dvoravnine sijeku se u dvije točke, pa se blokovi rezidualnog dizajna sijeku u najviše dvije točke. Ne mogu biti disjunktni jer bi to značilo da oba sijeku B_0 u istom paru točaka, pa bismo imali tri bloka kroz dvije točke. Zato se blokovi rezidualnog dizajna sijeku u jednoj ili dvije točke, tj. rezidualni dizajn dvoravnine je kvazisimetričan s presječnim brojevima $x = 1$, $y = 2$.

Kvazirezidualni dizajn s $\lambda = 2$ ima parametar $r = k + 2$, iz čega slijedi $v = \binom{k+1}{2}$, $b = \binom{k+2}{2}$ (iste parametre dobijemo zamjenom $k' \leftrightarrow k$ u gornjim formulama). Connor [44] je dokazao da i takvi dizajni moraju biti kvazisimetrični.

Lema 4.10. *Svaki kvazirezidualni dizajn s $\lambda = 2$ je kvazisimetričan s presječnim brojevima $x = 1$, $y = 2$.*

Dokaz. Za čvrsti blok B_0 označimo s n_i broj blokova koji sijeku B_0 u točno i točaka. Onda je

$$\sum_{i=0}^{k-1} n_i = b - 1 = \binom{k+2}{2} - 1 = \frac{k(k+3)}{2}. \tag{23}$$

Prebrojavanjem parova $\{(P, B) \mid P \in B \cap B_0, B \neq B_0\}$ dobijemo

$$\sum_{i=0}^{k-1} i\, n_i = k(r-1) = k(k+1). \tag{24}$$

Prebrojavanjem trojki $\{(P_1, P_2, B) \mid P_1, P_2 \in B \cap B_0, P_1 \neq P_2, B \neq B_0\}$ slijedi

$$\sum_{i=0}^{k-1} i(i-1)n_i = k(k-1). \tag{25}$$

Promotrimo izraz $Q = \sum_{i=0}^{k-1}(i-1)(i-2)n_i = 2n_0 + 2n_3 + 6n_4 + \ldots + (k-2)(k-3)n_{k-1}$. Uvrštavanjem (23), (24) i (25) slijedi

$$Q = \sum_{i=0}^{k-1} i(i-1)n_i - 2\sum_{i=0}^{k-1} i\, n_i + 2\sum_{i=0}^{k-1} n_i = k(k-1) - 2k(k+1) + k(k+3) = 0.$$

Dakle, $n_0 = n_3 = n_4 = \ldots = n_{k-1} = 0$ i dizajn je kvazisimetričan s $x = 1$, $y = 2$. Iz (23) i (24) dobijemo da $n_1 = 2k$ blokova sijeku B_0 u jednoj točki, a $n_2 = \binom{k}{2}$ blokova sijeku B_0 u dvije točke. □

Uz jednu iznimku, vrijedi i obrat prethodne leme.

Teorem 4.11. *Svaki kvazisimetrični dizajn s presječnim brojevima $x = 1$, $y = 2$ je kvazirezidualan s $\lambda = 2$, ili je trivijalni 2-$(5,3,3)$ dizajn.*

Dokaz. Iz uvjeta $vr = bk$ i $r(k-1) = \lambda(v-1)$ izrazimo $b = \frac{r(r(k-1)+\lambda)}{k\lambda}$. Uvrstimo taj b, $r = n + \lambda$ i $x = 1$, $y = 2$ u jednadžbu (9) iz propozicije 2.18, sredimo i dobijemo kvadratnu jednadžbu za red dizajna n:

$$2n^2 - 2(k-1)\lambda n + k(k-2)\lambda(\lambda-1) = 0. \tag{26}$$

Diskriminanta te jednadžbe je $\Delta = 4\lambda[2k(k-2) - \lambda(k^2 - 2k - 1)] \geq 0$, iz čega dobijemo uvjet $\lambda \leq \frac{2k(k-2)}{k^2-2k-1}$. Za $k = 3$ slijedi $\lambda \leq 3$, a za $k > 3$ slijedi $\lambda \leq 2$, tj. $\lambda = 2$ (Steinerovi 2-dizajni imaju presječne brojeve $x = 0$, $y = 1$, a ne $x = 1$, $y = 2$). U slučaju $k = \lambda = 3$ jednadžba (26) ima dvostruko rješenje $n = 3$, iz čega slijedi $r = 6$, $v = 5$, $b = 10$. To su parametri dizajna svih tročlanih podskupova 5-članog skupa, koji je zaista kvazisimetričan s $x = 1$, $y = 2$. U slučaju $\lambda = 2$ jednadžba (26) ima rješenja $n_1 = k-2$, $n_2 = k$. Prvo rješenje nije moguće jer bismo dobili $r = k$, a dizajn nije simetričan. Drugo rješenje daje $r = k + 2$, što znači da je dizajn kvazirezidualan s $\lambda = 2$. □

Prethodni teorem dokazao je Neumaier [103, tm. Q (iv)]. Naš dokaz je prilagođen iz Pawaleovog rada [105, tm. 3.2]. Pawale je dokazao općenitiji teorem, u kojem je klasificirao sve kvazisimetrične dizajne s $y - x = 1$. Osim dizajna iz teorema 4.11, to su još samo Steinerovi 2-dizajni i komplementi spomenutih dizajna. Istraživanje mogućih parametara kvazisimetričnih dizajna nastavljeno je u [106] za $y - x = 2$ i u [98, 107] za $y - x = 3$.

Hall i Connor [60] su s pomoću leme 4.10 dokazali da se svaki kvazirezidualni dizajn s $\lambda = 2$ može proširiti do simetričnog dizajna, isto kao kvazirezidualni dizajni s $\lambda = 1$ (afine ravnine).

Teorem 4.12 (Hall-Connor)**.** *Svaki kvazirezidualni dizajn s $\lambda = 2$ može se na jedinstven način proširiti do dvoravnine, tj. rezidualan je.*

Ovaj teorem svodi pitanje egzistencije kvazirezidualnih dizajna s $\lambda = 2$ na egzistenciju dvoravnina. Zbog teorema 4.11 isti zaključak vrijedi za kvazisimetrične dizajne s $x = 1$, $y = 2$. U tablici 10 navedeni su dopustivi parametri tih dizajna za $v \leq 78$. Ako dvoravnine s određenim parametrima ne postoje, isto vrijedi za odgovarajuće (kvazi)rezidualne dizajne. Ako dvoravnine postoje, broj neizomorfnih rezidualnih dizajna može biti veći od

Br.	v	k	λ	x	y	r	b	a	c	d	Nd	Nsrg	Napomene
1	10	4	2	1	2	6	15	6	1	3	3	1	
2	15	5	2	1	2	7	21	10	3	6	0	1	Teorem 4.1 (1)
3	21	6	2	1	2	8	28	15	6	10	0	4	Teorem 4.1 (2)
4	28	7	2	1	2	9	36	21	10	15	8	1	
5	36	8	2	1	2	10	45	28	15	21	0	1	Teorem 4.1 (1)
6	45	9	2	1	2	11	55	36	21	28	16	1	[82]
7	55	10	2	1	2	12	66	45	28	36	0	1	Teorem 4.1 (2)
8	66	11	2	1	2	13	78	55	36	45	$\geq$8	1	
9	78	12	2	1	2	14	91	66	45	55	0	1	Teorem 4.1 (1)

Tablica 10: Dopustivi parametri reziduala dvoravnina.

broja dvoravnina. Naime, $\mathrm{res}_{B_1}\mathcal{D}$ i $\mathrm{res}_{B_2}\mathcal{D}$ mogu biti neizomorfni za različite blokove B_1, B_2 od $\mathcal{D}$. Naprimjer, od ukupno 5 dvoravnina $(56, 11, 2)$ klasificiranih u [82] dobivamo $16 = 1 + 3 + 3 + 4 + 5$ kvazisimetričnih 2-$(45, 9, 2)$ dizajna s $x = 1$, $y = 2$. Najveće poznate dvoravnine imaju parametre $(79, 13, 2)$ i poznate su dvije neizomorfne (nisu potpuno klasificirane, tj. moglo bi ih biti više). Od njih dobivamo $8 = 4 + 4$ kvazisimetričnih 2-$(66, 11, 2)$ dizajna s $x = 1$, $y = 2$. Najmanji parametri za koje je egzistencija dvoravnina otvorena su $(168, 16, 2)$. Sukladno tome, nije poznato postoje li kvazisimetrični 2-$(152, 14, 2)$ dizajni s $x = 1$, $y = 2$.

Spomenimo poznatu *Hallovu slutnju* da za čvrsti $\lambda > 1$ postoji samo konačno mnogo simetričnih (v, k, λ) dizajna. Ako je slutnja istinita za $\lambda = 2$, onda postoji i samo konačno mnogo kvazisimetričnih dizajna s $x = 1$, $y = 2$. U radu [7] proučavani su parametri kvazirezidualnih kvazisimetričnih dizajna. Dokazano je da za čvrsti $\lambda \geq 3$ postoji samo konačno mnogo takvih dizajna, kao i za čvrste presječne brojeve $(x, y) \neq (0, 1)$ i $(1, 2)$.

Primijetimo da je blokovni graf kvazisimetričnog 2-$(\binom{k+1}{2}, k, 2)$ dizajna s $x = 1$, $y = 2$ komplement trokutnog grafa $\overline{T}_{k+2}$ s parametrima $SRG(\binom{k+2}{2}, \binom{k}{2}, \binom{k-2}{2}, \binom{k-1}{2})$. Coster i Haemers [47] dokazali su da kvazisimetrični dizajn kojemu je blokovni graf $\overline{T}_{m+2}$ ima parametre oblika $v = \binom{m+1}{2}$, $k = \frac{1}{2}am$, $\lambda = \frac{a(am-2)}{2(m-1)}$, $r = \frac{1}{2}a(m + 2)$, $b = \binom{m+2}{2}$, $x = \binom{a}{2}$, $y = \frac{a(am-2a+2)}{2(m-1)}$ za neki prirodni broj a. Za $a = 2$ to su kvazisimetrični dizajni s $x = 1$, $y = 2$, tj. reziduali dvoravnina. U [47] izvedeni su netrivijalni nužni uvjeti za egzistenciju takvih dizajna s općim a, slični teoremu 4.1. Napomenimo da nije poznat niti jedan primjer za $2 < a < m - 1$, a autori su u [47] izrazili skepsu da će ikad biti konstruiran (iako kažu da nema dovoljno informacija za hipotezu da takvi dizajni ne postoje). Najmanji otvoreni slučaj je $a = 8$, $m = 25$, što odgovara kvazisimetričnim 2-$(325, 100, 33)$ dizajnima s $x = 28$, $y = 31$.

Vidjeli smo da kvazirezidualni dizajni s $\lambda \geq 3$ ne moraju biti rezidualni. No zbog sljedećeg teorema iz [22], za čvrsti λ može biti samo konačno mnogo iznimaka, a svi ostali kvazirezidualni dizajni s parametrom λ su rezidualni.

Teorem 4.13. *Postoji funkcija $f(\lambda)$ takva da se svaki kvazirezidualni dizajn s parametrima λ i $k \geq f(\lambda)$ na jedinstven način proširuje do simetričnog dizajna.*

Funkcija $f(\lambda)$ iz [22] je dosta komplicirana i može se ograničiti odozdo polinomom petog stupnja. Metsch [101] je dokazao da tvrdnja teorema vrijedi i za polinom četvrtog stupnja $f(\lambda) = (\frac{8}{\sqrt{3}}\lambda + \lambda + 5)\lambda^2(\lambda + 1)$.

Rezidualni dizajni simetričnih dizajna s $\lambda = 1$ ili 2 uvijek su kvazisimetrični, ali za $\lambda \geq 3$ ne moraju biti. Najmanji primjer su reziduali simetričnih $(15, 7, 3)$ dizajna. Do na izomorfizam postoji 5 takvih simetričnih dizajna, a njihovi reziduali su 4 neizomorfna 2-$(8, 4, 3)$ dizajna. Jedan od njih je kvazisimetričan s presječnim brojevima $x = 0$, $y = 2$, a ostali nisu kvazisimetrični. Kvazisimetrični rezidual je zapravo Hadamardov 3-$(8, 4, 1)$ dizajn i pojavljuje se kao rezidualni dizajn u 4 od 5 simetričnih $(15, 7, 3)$ dizajna. To je ujedno primjer kvazirezidualnog dizajna kojeg se može na više načina proširiti do simetričnog dizajna.

Propozicija 4.14. *Neka je $\mathcal{D}$ simetrični (v, k, λ) dizajn i B_0 njegov blok. Rezidualni dizajn $\mathrm{res}_{B_0}\mathcal{D}$ je kvazisimetričan s presječnim brojevima x, y ako i samo ako je odgovarajući derivirani dizajn $\mathrm{der}_{B_0}\mathcal{D}$ kvazisimetričan s presječnim brojevima $\lambda - y$, $\lambda - x$.*

Dokaz. Neka su $B_1, B_2 \neq B_0$ dva bloka simetričnog dizajna. Vrijedi $|B_1 \cap B_2| = \lambda$ i $\{\mathcal{P} \setminus B_0, B_0\}$ je particija od $\mathcal{P}$, pa je $|(B_1 \cap B_2) \cap (\mathcal{P} \setminus B_0)| + |(B_1 \cap B_2) \cap B_0| = \lambda$. $\square$

Naprimjer, od simetričnih $(64, 28, 12)$ dizajna dobivamo rezidualne 2-$(36, 16, 12)$ dizajne i derivirane 2-$(28, 12, 11)$ dizajne. Rezidualni dizajn je kvazisimetričan s $x = 6$, $y = 8$ ako i samo ako je odgovarajući derivirani dizajn kvazisimetričan s $x = 4$, $y = 6$. U radu [52] konstruirani su svi kvazisimetrični 2-$(28, 12, 11)$ dizajni s $x = 4$, $y = 6$ koji imaju automorfizam reda 7 bez fiksnih točaka i blokova. Postoji točno 246 takvih dizajna (konstruirani su s pomoću orbitnih matrica). Zatim su ih u [52] na sve moguće načine proširivali do simetričnog $(64, 28, 12)$ dizajna. Četiri dizajna nije moguće proširiti i to su primjeri kvazisimetričnih kvaziderivirani dizajna koji nisu derivirani. Preostalih 242 dizajna proširuju se do 8784 neizomorfnih $(64, 28, 12)$ dizajna, a odgovarajući rezidualni dizajni su isto toliko neizomorfnih kvazisimetričnih 2-$(36, 16, 12)$ dizajna s $x = 6$, $y = 8$.

Na sličan način konstruiran je u [133] kvazisimetrični 2-$(56, 16, 6)$ dizajn s presječnim brojevima $x = 4$, $y = 6$. Dva puta derivirani Wittov dizajn s parametrima 3-$(22, 6, 1)$ (odnosno 2-$(22, 6, 5)$) i presječnim brojevima $x = 0$, $y = 2$ uložen je kao derivirani dizajn u simetrični $(78, 22, 6)$ dizajn. Odgovarajući rezidualni dizajn ima parametre 2-$(56, 16, 6)$, $x = 4$, $y = 6$. Drugi takav dizajn konstruiran je u [102] s pomoću kodova.

Jedna familija simetričnih dizajna za koje su rezidualni i derivirani dizajni uvijek kvazisimetrični su takozvani SDP dizajni (prema eng. *symmetric difference property*). Za simetrični dizajn kažemo da je *SDP dizajn* ako je za svaka tri bloka B_1, B_2, B_3 simetrična razlika $B_1 \Delta B_2 \Delta B_3$ blok ili komplement bloka. Kantor [80, tm. 3] je dokazao da SDP dizajni imaju parametre oblika $(v, k, \lambda) = (2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ ili komplementarne parametre $(2^{2m}, 2^{2m-1} + 2^{m-1}, 2^{2m-2} + 2^{m-1})$. Komplementarni dizajn SDP dizajna također je SDP dizajn, pa se možemo ograničiti na prvi slučaj. Kantor je u [80] konstruirao beskonačnu seriju SDP dizajna na kojima djeluje simplektička grupa $Sp(2m, 2)$, a u [81] je dokazao da broj neizomorfnih SDP dizajna raste eksponencijalno s m.

Propozicija 4.15. *Rezidualni i derivirani SDP dizajni imaju sljedeće svojstvo: za svaka dva bloka B_1, B_2, simetrična razlika $B_1 \Delta B_2$ je blok ili komplement bloka.*

Dokaz. Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ SDP dizajn i B_0 njegov blok. Blokovi rezidualnog dizajna $\mathrm{res}_{B_0} \mathcal{D}$ su oblika $B \setminus B_0$, $B \in \mathcal{B}$. Za dva takva bloka $B_1 \setminus B_0$, $B_2 \setminus B_0$ vrijedi $(B_1 \setminus B_0) \Delta (B_2 \setminus B_0) = (B_0 \Delta B_1 \Delta B_2) \setminus B_0$. Ako je $B_0 \Delta B_1 \Delta B_2 = B \in \mathcal{B}$, to je blok rezidualnog dizajna $B \setminus B_0$. Ako je pak $B_0 \Delta B_1 \Delta B_2 = \mathcal{P} \setminus B$ za $B \in \mathcal{B}$, onda je to komplement bloka rezidualnog dizajna $(\mathcal{P} \setminus B) \setminus B_0 = (\mathcal{P} \setminus B_0) \setminus (B \setminus B_0)$. Blokovi deriviranog dizajna su oblika $B \cap B_0$, $B \in \mathcal{B}$. Za dva takva bloka $B_1 \cap B_0$, $B_2 \cap B_0$ vrijedi $(B_1 \cap B_0) \Delta (B_2 \cap B_0) = B_0 \setminus [(B_0 \Delta B_1 \Delta B_2) \cap B_0]$. Ako je $B_0 \Delta B_1 \Delta B_2 = B \in \mathcal{B}$, to je komplement bloka deriviranog dizajna $B_0 \setminus (B \cap B_0)$. Ako je pak $B_0 \Delta B_1 \Delta B_2 = \mathcal{P} \setminus B$ za $B \in \mathcal{B}$, onda je to blok deriviranog dizajna $B_0 \setminus [(\mathcal{P} \setminus B) \cap B_0] = B \cap B_0$. □

Dizajne koji imaju svojstvo iz prethodne propozicije zovemo *QSDP dizajnima.* Takvi dizajni nužno su kvazisimetrični.

Propozicija 4.16. *Neka je $\mathcal{D}$ 2-(v, k, λ) dizajn sa svojstvom da je za svaka dva bloka B_1, B_2 simetrična razlika $B_1 \Delta B_2$ blok ili komplement bloka. Onda je $\mathcal{D}$ kvazisimetričan s presječnim brojevima $k/2$ i $(3k - v)/2$.*

Dokaz. Tvrdnja slijedi iz $|B_1 \Delta B_2| = |B_1| + |B_2| - 2|B_1 \cap B_2|$. □

Iz Kantorovog rezultata [80, tm. 3], propozicija 4.8, 4.9 i prethodne dvije propozicije dobivamo sljedeći korolar.

Korolar 4.17. *Rezidualni SDP dizajn ima parametre oblika* 2-$(2^{2m-1}+2^{m-1}$, $2^{2m-2}, 2^{2m-2}-2^{m-1})$ *i presječne brojeve* $x = 2^{2m-3}-2^{m-2}$, $y = 2^{2m-3}$. *Derivirani SDP dizajn ima parametre oblika* 2-$(2^{2m-1}-2^{m-1}, 2^{2m-2}-2^{m-1}, 2^{2m-2}-2^{m-1}-1)$ *i presječne brojeve* $x = 2^{2m-3}-2^{m-1}$, $y = 2^{2m-3}-2^{m-2}$.

Ward [138] je direktno dokazao da QSDP dizajni moraju imati parametre tog oblika. Jungnickel i Tonchev [76] dokazali su da rezidualni i derivirani dizajni neizomorfnih SDP dizajna ne mogu biti izomorfni. Iz toga i iz Kantorovog rezultata [81] slijedi da broj neizomorfnih QSDP dizajna raste eksponencijalno s m. Tonchev [135] je dokazao da se svaki QSDP dizajn proširuje na jedinstven način do simetričnog SDP dizajna, tj. da je uvijek rezidualni ili derivirani (jedinstvenost slijedi već iz [76]). Primijetimo da je ukupan broj simetričnih dizajna s parametrima $(2^{2m}, 2^{2m-1}-2^{m-1}, 2^{2m-2}-2^{m-1})$ i kvazisimetričnih dizajna s parametrima iz korolara 4.17 puno veći od broja SDP i QSDP dizajna. Naprimjer, za $m = 3$ dobivamo parametre $(64, 28, 12)$ i 2-$(36, 16, 12)$, $x = 6$, $y = 8$ te 2-$(28, 12, 11)$, $x = 4$, $y = 6$. Poznato je da postoji točno četiri simetrična SDP dizajna i točno četiri rezidualna i derivirana QSDP dizajna s tim parametrima [104]. S druge strane, ukupan broj simetričnih $(64, 28, 12)$ dizajna je bar 8784 [52], kvazisimetričnih 2-$(36, 16, 12)$ dizajna s $x = 6$, $y = 8$ bar 522079, a kvazisimetričnih 2-$(28, 12, 11)$ dizajna s $x = 4$, $y = 6$ bar 58891 [89].

4.5 Projektivni i afini dizajni

Neka je $V = (\mathbb{F}_q)^n$ vektorski prostor dimenzije n nad poljem $\mathbb{F}_q$. Broj d-dimenzionalnih potprostora od V označavamo $\begin{bmatrix} n \\ d \end{bmatrix}_q$ i zovemo *q-binomni* ili *Gaussov* koeficijent.

Lema 4.18. $\begin{bmatrix} n \\ d \end{bmatrix}_q = \dfrac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-d+1}-1)}{(q^d-1)(q^{d-1}-1)\cdots(q-1)}$.

Dokaz. Potprostor A dimenzije d zadajemo linearno nezavisnim podskupom od d vektora iz V. Za prvi vektor biramo bilo koji osim nulvektora ($q^n - 1$ izbora), za drugi bilo koji vektor koji nije u potprostoru razapetom s prvim ($q^n - q$ izbora), za treći bilo koji vektor koji nije u potprostoru razapetom s prva dva ($q^n - q^2$ izbora) itd. Produkt tih brojeva treba podijeliti s brojem baza od A, što je na sličan način $(q^d-1)(q^d-q)\cdots(q^d-q^{d-1})$. Formula slijedi kraćenjem $q^{1+2+\ldots+d-1}$ iz brojnika i nazivnika. □

Gaussovi koeficijenti imaju mnoga svojstva analogna svojstvima binomnih koeficijenata, npr. simetriju $\begin{bmatrix} n \\ d \end{bmatrix}_q = \begin{bmatrix} n \\ n-d \end{bmatrix}_q$, Pascalov identitet $\begin{bmatrix} n+1 \\ d \end{bmatrix}_q =$

$q^d \begin{bmatrix} n \\ d \end{bmatrix}_q + \begin{bmatrix} n \\ d-1 \end{bmatrix}_q$ i q-binomni teorem $\prod_{d=0}^{n-1}(1-q^d x) = \sum_{d=0}^{n} q^{d(d-1)/2} \begin{bmatrix} n \\ d \end{bmatrix}_q x^d$. Trebaju nam da izrazimo parametre dizajna točaka i d-dimenzionalnih potprostora u n-dimenzionalnom projektivnom i afinom prostoru nad poljem $\mathbb{F}_q$.

Propozicija 4.19. *Neka je $V = (\mathbb{F}_q)^{n+1}$ vektorski prostor dimenzije $n+1$ nad poljem $\mathbb{F}_q$. U incidencijskoj strukturi $PG_d(n,q)$ točke su 1-dimenzionalni potprostori od V, blokovi $(d+1)$-dimenzionalni potprostori od V, a incidencija je inkluzija $\subseteq$. Ta struktura je 2-dizajn s parametrima $v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q$, $k = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q$, $\lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$, $r = \begin{bmatrix} n \\ d \end{bmatrix}_q$ i $b = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q$.*

Dokaz. Bilo koja dva jednodimenzionalna potprostora $P, Q \leq V$ razapinju dvodimenzionalni potprostor $A = \langle P, Q \rangle \leq V$. Potprostori dimenzije $d+1$ od V koji sadrže A su u bijektivnom odnosu s potprostorima dimenzije $d-1$ od V/A. Zato ih ima $\lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$. Slično se odredi parametar r, a parametri v, k i b slijede direktno iz definicije Gaussovih koeficijenata. $\square$

Za $d = 1$ projektivni dizajn označavamo $PG(n,q)$. Budući da je $\lambda = \begin{bmatrix} n-1 \\ 0 \end{bmatrix}_q = 1$, riječ je o Steinerovom 2-dizajnu. Za $d = n-1$ vrijedi $v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q = \begin{bmatrix} n+1 \\ n \end{bmatrix}_q = b$, pa je dizajn točaka i hiperravnina projektivnog prostora simetričan. Za $d = n-2$ presjek bilo koja dva potprostora A, B kodimenzije 2 je kodimenzije 3 ili 4. To slijedi iz Grassmanove formule $\dim(A \cap B) = \dim A + \dim B - \dim(A+B) = 2(n-1) + \dim(A+B)$. Budući da je $A+B$ hiperravnina ili cijeli prostor V, rezultat je $n-2$ ili $n-3$. Dakle, dizajn $PG_{n-2}(n,q)$ je kvazisimetričan s presječnim brojevima $x = \begin{bmatrix} n-3 \\ 1 \end{bmatrix}_q$, $y = \begin{bmatrix} n-2 \\ 1 \end{bmatrix}_q$.

Propozicija 4.20. *Neka je $V = (\mathbb{F}_q)^n$ vektorski prostor dimenzije n nad poljem $\mathbb{F}_q$. U incidencijskoj strukturi $AG_d(n,q)$ točke su vektori iz V, blokovi su translati d-dimenzionalnih potprostora od V (linearne mnogostrukosti), a incidencija je relacija pripadanja $\in$. Ta struktura je 2-dizajn s parametrima $v = q^n$, $k = q^d$, $\lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$, $r = \begin{bmatrix} n \\ d \end{bmatrix}_q$ i $b = q^{n-d} \begin{bmatrix} n \\ d \end{bmatrix}_q$.*

Dokaz. Za svaka dva vektora $P, Q \in V$ postoji $\begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$ potprostora dimenzije d koji sadrže $P-Q$ (u bijektivnom su odnosu s potprostorima dimenzije $d-1$ od $V/\langle P-Q \rangle$). Za svaki od tih potprostora točno jedan translat sadrži P i Q, pa je $\lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$. Slična argumentacija vrijedi za parametar r, a formule za v i k su očite. Formula za b slijedi jer d-dimenzionalni potprostor ima $q^n/q^d = q^{n-d}$ translata. $\square$

Afini dizajn $AG_d(n,q)$ je rastavljiv. Blokove možemo particionirati u paralelne klase (translate istog potprostora), a svaka klasa čini particiju skupa točaka. Za $d = 1$ afini dizajn označavamo $AG(n, d)$ i ima parametar $\lambda = \begin{bmatrix} n-1 \\ 0 \end{bmatrix}_q = 1$, pa je Steinerov 2-dizajn. Za $d = n - 1$ dostiže se Boseova nejednakost $b = v + r - 1$ i dizajn je afino rastavljiv. Slijedi da je dizajn točaka i hiperravnina afinog prostora $AG_{n-1}(n, q)$ kvazisimetričan s presječnim brojevima $x = 0$, $y = k^2/v = q^{n-2}$.

Projektivni i afini dizajni $PG_d(n, q)$ i $AG_d(n, q)$ nisu jedini dizajni s tim parametrima. Poznato je da za fiksne d i q broj neizomorfnih dizajna s istim parametrima kao $PG_d(n, q)$ raste eksponencijalno s n [78, 75]. Broj neizomorfnih simetričnih dizajna s istim parametrima kao $PG_{n-1}(n, q)$ također raste eksponencijalno s n [73]. Ista tvrdnja vrijedi za $AG_d(n, q)$ i $AG_{n-d}(n, q)$, čak i kad se ograničimo na rastavljive dizajne s tim parametrima [42]. Posebno, broj afino rastavljivih dizajna s istim parametrima kao $AG_{n-1}(n, q)$ raste eksponencijalno s n.

Zanimljivo je pitanje karakterizacije projektivnih i afinih dizajna među svim dizajnima s odgovarajućim parametrima [74, 75]. Jedna od hipoteza o tome je takozvana *Hamadina slutnja*. Noboru Hamada [61] izračunao je p-rang incidencijskih matrica dizajna $PG_d(n, q)$ i $AG_d(n, q)$ za prim potenciju $q = p^s$. Formule su vrlo komplicirane, a u specijalnom slučaju $d = n-1$ rang je $\binom{p+n-1}{n}^s + 1$ za projektivni i $\binom{p+n-1}{n}^s$ za afini dizajn. Hamada je proučavao p-rang drugih dizajna s istim parametrima i postavio hipotezu da ne može biti manji od p-ranga $PG_d(n, q)$ i $AG_d(n, q)$, te da se minimalne vrijednosti dostižu samo za projektivne i afine dizajne. Prvi dio Hamadine slutnje i dalje je otvoren, a za drugi su pronađeni protuprimjeri.

Najmanji protuprimjer su dizajni s parametrima 2-$(31, 7, 7)$ koji odgovaraju projektivnom dizajnu $PG_2(4, 2)$. Prema ocjeni iz [78], ukupan broj neizomorfnih 2-$(31, 7, 7)$ dizajna veći je od $5 \cdot 10^{28}$. Tonchev [132] je dokazao da postoji točno pet kvazisimetričnih dizajna s tim parametrima (vidi teorem 3.27). Jedan od njih je $PG_2(4, 2)$, a svih pet imaju 2-rank jednak 16. Proučavajući strukturu jednog od tih protuprimjera, Jungnickel i Tonchev [77] konstruirali su familiju dizajna s istim parametrima kao $PG_n(2n, q)$, ali s njima neizomorfnih. Ti dizajni su kvazisimetrični ako je $n = 2$ i imaju isti p-rang kao $PG_n(2n, q)$ ako je $q = p$ primbroj. Druga beskonačna serija protuprimjera za Hamadinu slutnju su dizajni s istim parametrima kao $AG_{d+1}(2d+1, 2)$ konstruirani u [43].

Vidjeli smo da broj afino rastavljivih (posebno, kvazisimetričnih) dizajna s istim parametrima kao $AG_{n-1}(n, q)$ raste eksponencijalno s n. S druge strane, iako ukupan broj dizajna s parametrima kao $PG_{n-2}(n, q)$ također raste eksponencijalno, poznato je vrlo malo kvazisimetričnih dizajna s tim parametrima. Osim projektivnih dizajna, jedini poznati primjeri su kvazisimetrični dizajni iz serije Jungnickela i Toncheva [77] s parametrima kao

$PG_2(4,q)$ i još tri takva dizajna za $q=2$ opisana u teoremu 3.27. Dakle, poznato je pet neizomorfnih kvazisimetričnih dizajna s parametrima kao $PG_{n-2}(n,q)$ za $(n,q)=(4,2)$, dva za $n=4$ i $q>2$ i samo jedan za sve $n>4$. U radu [121] dokazano je za $(n,q)=(5,2)$ da je projektivni dizajn jedini primjer s cikličkom grupom automorfizama.

Zanimljiva karakterizacija projektivnog dizajna među svim dizajnima s parametrima kao $PG_{n-2}(n,q)$ dokazana je u [75]. *Pravac* u 2-(v,k,λ) dizajnu je presjek svih blokova kroz dvije točke. Za $\lambda=1$ pravci se podudaraju s blokovima, a u $PG_d(n,q)$ podudaraju se s 1-dimenzionalnim projektivnim potprostorima i svi su veličine $q+1$.

Teorem 4.21. *Neka je $\mathcal{D}$ dizajn s parametrima kao $PG_{n-2}(n,q)$, pri čemu je $n\geq 4$ i q ne mora biti prim potencija (formula za Gaussove koeficijente ima smisla za sve prirodne brojeve $q\geq 2$). Ako se svaka dva bloka od $\mathcal{D}$ sijeku bar u $\left[{n-3 \atop 1}\right]_q$ točaka i svi pravci su veličine $q+1$, onda je $\mathcal{D}$ izomorfan dizajnu $PG_{n-2}(n,q)$ (posebno, q je prim potencija).*

Uvjet da se blokovi sijeku bar u $\left[{n-3 \atop 1}\right]_q$ točaka ispunjen je u kvazisimetričnom dizajnu s presječnim brojevima $x=\left[{n-3 \atop 1}\right]_q$, $y=\left[{n-2 \atop 1}\right]_q$. Dakle, ako su u kvazisimetričnom dizajnu s istim parametrima kao $PG_{n-2}(n,q)$ svi pravci veličine $q+1$, onda je izomorfan s $PG_{n-2}(n,q)$.

4.6 Familija Blokhuisa i Haemersa

Literatura

[1] R.J.R. Abel, M. Greig, *BIBDs with small block size*, u: *The Handbook of Combinatorial Designs, Second Edition* (urednici C.J. Colbourn i J.H. Dinitz), CRC Press, 2007., str. 72–70.

[2] R.J.R. Abel, C.J. Colbourn, J.H. Dinitz, *Mutually orthogonal Latin squares (MOLS)*, u: *The Handbook of Combinatorial Designs, Second Edition* (urednici C.J. Colbourn i J.H. Dinitz), CRC Press, 2007., str. 160–193.

[3] C. Aguilar-Melchor, P. Gaborit, J.-L. Kim, L. Sok, P. Solé, *Classification of extremal and s-extremal binary self-dual codes of length* 38, IEEE Trans. Inform. Theory **58** (2012), 2253–2262.

[4] W.O. Alltop, *Extending t-designs*, J. Combinatorial Theory Ser. A **18** (1975), 177–186.

[5] E.F. Assmus Jr, J.D. Key, *Designs and their codes*, Cambridge University Press, 1992.

[6] J. Azarija, T. Marc, *There is no* $(95, 40, 12, 20)$ *strongly regular graph*, arXiv:1603.02032v2 (2016), 14 str.
`https://arxiv.org/pdf/1603.02032v2`

[7] A. Baartmans, K. Danhof, S.T. Tan, *Quasi-residual quasi-symmetric designs*, Discrete Math. **30** (1980), 69–81.

[8] B. Bagchi, *No extendable biplane of order nine*, J. Combin. Theory Ser. A **49** (1988), 1–12.

[9] B. Bagchi, *Corrigendum: "No extendable biplane of order nine"*, J. Combin. Theory Ser. A **57** (1991), 162.

[10] S. Bagchi, B. Bagchi, *Designs from pairs of finite fields. I. A cyclic unital $U(6)$ and other regular Steiner* 2*-designs*, J. Combin. Theory Ser. A **52** (1989), 51–61.

[11] E. Bannai, *On tight designs*, Quart. J. Math. Oxford Ser. (2) **28** (1977), 433–448.

[12] H. Beker, *On strong tactical decompositions*, J. London Math. Soc. (2) **16** (1977), 191–196.

[13] H. Beker, W. Haemers, 2-*designs having an intersection number* $k-n$, J. Combin. Theory Ser. A **28** (1980), 64–81.

[14] K. Betsumiya, M. Harada, A. Munemasa, *A complete classification of doubly even self-dual codes of length* 40, Electron. J. Combin. **19** (2012), #P18, 12 str.

[15] A. Betten, A. Kerber, R. Laue, A. Wassermann, *Es gibt* 7*-Designs mit kleinen Parametern! [There are* 7*-designs with small parameters!]*, Bayreuth. Math. Schr. **49** (1995), 213.

[16] A. Beutelspacher, U. Porta, *On the parameters of strongly resolvable designs*, J. Geom. **19** (1982), 115–129.

[17] A. Beutelspacher, U. Rosenbaum, *Projective geometry: from foundations to applications*, Cambridge University Press, 1998.

[18] R.T. Bilous, G.H.J. van Rees, *An enumeration of binary self-dual codes of length* 32, Des. Codes Cryptogr. **26** (2002), 61–86.

[19] R.T. Bilous, *Enumeration of the binary self-dual codes of length* 34, J. Combin. Math. Combin. Comput. **59** (2006), 173–211.

[20] A. Blokhuis, W.H. Haemers, *An infinite family of quasi-symmetric designs*, J. Statist. Plann. Inference **95** (2001), 117–119.

[21] R.C. Bose, *A note on the resolvability of balanced incomplete designs*, Sankhya **6** (1942), 105–110.

[22] R.C. Bose, S.S. Shrikhande, N.M. Singhi, *Edge regular multigraphs and partial geometric designs with an application to the embedding of quasi-residual designs*, u *Colloquio Internazionale sulle Teorie Combinatorie, Tomo I*, Atti dei Convegni Lincei **17**, Accad. Naz. Lincei, 1976., str. 49–81.

[23] S. Bouyuklieva, I. Bouyukliev, *An algorithm for classification of binary self-dual codes*, IEEE Trans. Inform. Theory **58** (2012), 3933–3940.

[24] S. Bouyuklieva, I. Bouyukliev, M. Harada, *Some extremal self-dual codes and unimodular lattices in dimension* 40, Finite Fields Appl. **21** (2013), 67–83.

[25] I. Bouyukliev, S. Bouyuklieva, S. Dodunekov, *On binary self-complementary* $[120, 9, 56]$*-codes having an automorphism of order* 3*, and associated SDP designs*, Probl. Inf. Transm. **43** (2007), 89–96.

[26] I. Bouyukliev, M. Dzhumalieva-Stoeva, V. Monev, *Classification of binary self-dual codes of length* 40, IEEE Trans. Inform. Theory **61** (2015), 4253–4258.

[27] S. Bouyuklieva, M. Harada, *Extremal self-dual* $[50, 25, 10]$ *codes with automorphisms of order* 3 *and quasi-symmetric* 2-$(49, 9, 6)$ *designs*, Des. Codes Cryptogr. **28** (2003), 163–169.

[28] C. Bracken, G. McGuire, H. Ward, *New quasi-symmetric designs constructed using mutually orthogonal Latin squares and Hadamard matrices*, Des. Codes Cryptogr. **41** (2006), 195–198.

[29] A. Bremner, *A Diophantine equation arising from tight* 4*-designs*, Osaka J. Math. **16** (1979), 353–356.

[30] A.E. Brouwer, *Parameters of strongly regular graphs.* `https://www.win.tue.nl/~aeb/graphs/srg/srgtab.html`

[31] A.E. Brouwer, A.R. Calderbank, *An Erds-Ko-Rado theorem for regular intersecting families of octads*, Graphs Combin. **2** (1986), 309–316.

[32] A.E. Brouwer, W.H. Haemers, *Spectra of graphs*, Springer, 2012. `http://homepages.cwi.nl/~aeb/math/ipm/`

[33] A.R. Calderbank, *The application of invariant theory to the existence of quasisymmetric designs*, J. Combin. Theory Ser. A **44** (1987), 94–109.

[34] A.R. Calderbank, *Inequalities for quasisymmetric designs*, J. Combin. Theory Ser. A **48** (1988), 53–64.

[35] A.R. Calderbank, *Geometric invariants for quasisymmetric designs*, J. Combin. Theory Ser. A **47** (1988), 101-110.

[36] A.R. Calderbank, P. Frankl, *Binary codes and quasisymmetric designs*, Discrete Math. **83** (1990), 201–204.

[37] A.R. Calderbank, P. Morton, *Quasi-symmetric* 3*-designs and elliptic curves*, SIAM J. Discrete Math. **3** (1990), 178–196.

[38] P.J. Cameron, *Extending symmetric designs*, J. Combinatorial Theory Ser. A **14** (1973), 215–220.

[39] P.J. Cameron, *Near-regularity conditions for designs*, Geometriae Dedicata **2** (1973), 213–223.

[40] P.J. Cameron, *Combinatorics: topics, techniques, algorithms*, Cambridge University Press, 1994.

[41] P.J. Cameron, J.H. van Lint, *Designs, graphs, codes and their links*, Cambridge University Press, 1991.

[42] D. Clark, D. Jungnickel, V.D. Tonchev, *Correction to: "Exponential bounds on the number of designs with affine parameters"*, J. Combin. Des. **19** (2011), 156–166.

[43] D. Clark, D. Jungnickel, V.D. Tonchev, *Affine geometry designs, polarities, and Hamada's conjecture*, J. Combin. Theory Ser. A **118** (2011), 231–239.

[44] W.S. Connor, Jr., *On the structure of balanced incomplete block designs*, Ann. Math. Statistics **23** (1952), 57–71.

[45] J.H. Conway, V. Pless, *On the enumeration of self-dual codes*, J. Combin. Theory Ser. A **28** (1980), 26–53.

[46] J.H. Conway, V. Pless, N.J.A. Sloane, *The binary self-dual codes of length up to* 32*: a revised enumeration*, J. Combin. Theory Ser. A **60** (1992), 183–195.

[47] M.J. Coster, W.H. Haemers, *Quasi-symmetric designs related to the triangular graph*, Des. Codes Cryptogr. **5** (1995), 27–42.

[48] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. No. 10, 1973.

[49] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Information and Control **23** (1973), 407–438.

[50] P. Dembowski, *Kombinatorische Eigenschaften endlicher Inzidenzstrukturen*, Math. Z. **75** (1960/1961), 256–270.

[51] P. Dembowski, *Finite geometries*, Springer, 1968.

[52] Y. Ding, S. Houghten, C. Lam, S. Smith, L. Thiel, V. D. Tonchev, *Quasi-symmetric* 2-$(28, 12, 11)$ *designs with an automorphism of order* 7, J. Combin. Des. **6** (1998), 213–223.

[53] P. Dukes, J. Short-Gershman, *Nonexistence results for tight block designs*, J. Algebraic Combin. **38** (2013), 103–119.

[54] P. Dukes, R.M. Wilson, *The cone condition and t-designs*, European J. Combin. **28** (2007), 1610–1625.

[55] H. Enomoto, N. Ito, R. Noda, *Tight* 4*-designs*, Osaka J. Math. **16** (1979), 39–43.

[56] J.-M. Goethals, J.J. Seidel, *Strongly regular graphs derived from combinatorial designs*, Canad. J. Math. **22** (1970), 597–614.

[57] L.D. Grey, *Some bounds for error-correcting codes*, IRE Trans. IT-8 (1962), 200–202.

[58] T.A. Gulliver, M. Harada, *Codes of lengths* 120 *and* 136 *meeting the Grey-Rankin bound and quasi-symmetric designs*, IEEE Trans. Inform. Theory **45** (1999), 703-706.

[59] W.H. Haemers, *There exists no* $(76, 21, 2, 7)$ *strongly regular graph*, u: Finite geometry and combinatorics (Deinze, 1992), London Math. Soc. Lecture Note Ser. **191**, Cambridge Univ. Press, 1993., str. 175–176.

[60] M. Hall, Jr., W.S. Connor, *An embedding theorem for balanced incomplete block designs*, Canadian J. Math. **6** (1954), 35–41.

[61] N. Hamada, *On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes*, Hiroshima Math. J. **3** (1973), 153–226.

[62] H. Hanani, *The existence and construction of balanced incomplete block designs*, Ann. Math. Statist. **32** (1961), 361–386.

[63] M. Harada, A. Munemasa, *Classification of self-dual codes of length* 36, Adv. Math. Commun. **6** (2012), 229–235.

[64] M. Harada, A. Munemasa, *Database of binary self-dual codes*, 2013. `http://www.math.is.tohoku.ac.jp/~munemasa/research/codes/sd2.htm`

[65] A.S. Hedayat, N.J.A. Sloane, J. Stufken, *Orthogonal arrays. Theory and applications*, Springer-Verlag, 1999.

[66] S.K. Houghten, L.H. Thiel, J. Janssen, C.W.H. Lam, *There is no* $(46, 6, 1)$ *block design*, J. Combin. Des. **9** (2001), 60–71.

[67] W.C. Huffman, V.D. Tonchev, *The existence of extremal self-dual* $[50, 25, 10]$ *codes and quasi-symmetric* 2-$(49, 9, 6)$ *designs*, Des. Codes Cryptogr. **6** (1995), 97–106.

[68] D.R. Hughes, F.C. Piper, *On resolutions and Bose's theorem*, Geometriae Dedicata **5** (1976), 129–133.

[69] Y.J. Ionin, M.S. Shrikhande, *Combinatorics of symmetric designs*, Cambridge University Press, 2006.

[70] Y.J. Ionin, T. van Trung, *Symmetric designs*, u: *The Handbook of Combinatorial Designs, Second Edition* (urednici C.J. Colbourn i J.H. Dinitz), CRC Press, 2007., str. 110–124.

[71] N. Ito, *On tight* 4*-designs*, Osaka J. Math. **12** (1975), 493–522.

[72] N. Ito, *Corrections and supplements to: "On tight 4-designs"*, Osaka J. Math. 15 (1978), 693–697.

[73] D. Jungnickel, *The number of designs with classical parameters grows exponentially*, Geom. Dedicata **16** (1984), 167–178.

[74] D. Jungnickel, *Characterizing geometric designs*, Rend. Mat. Appl. **(7) 30** (2010), 111–120.

[75] D. Jungnickel, *Characterizing geometric designs, II*, J. Combin. Theory Ser. A **118** (2011), 623–633.

[76] D. Jungnickel, V.D. Tonchev, *Exponential number of quasi-symmetric SDP designs and codes meeting the Grey-Rankin bound*, Des. Codes Cryptogr. **1** (1991), 247–253.

[77] D. Jungnickel, V.D. Tonchev, *Polarities, quasi-symmetric designs, and Hamada's conjecture*, Des. Codes Cryptogr. **51** (2009), 131–140.

[78] D. Jungnickel, V.D. Tonchev, *The number of designs with geometric parameters grows exponentially*, Des. Codes Cryptogr. **55** (2010), 131–140.

[79] D. Jungnickel, V.D. Tonchev, *Maximal arcs and quasi-symmetric designs*, Des. Codes Cryptogr. **77** (2015), 365–374.

[80] W.M. Kantor, *Symplectic groups, symmetric designs, and line ovals*, J. Algebra **33** (1975), 43-58.

[81] W.M. Kantor, *Exponential numbers of two-weight codes, difference sets and symmetric designs*, Discrete Math. **46** (1983), 95-98.

[82] P. Kaski, P. Östergard, *There are exactly five biplanes with* $k = 11$, J. Combin. Des. **16** (2008), 117–127.

[83] P. Keevash, *The existence of designs*, arXiv:1401.3665 (2015), 56 str. `https://arxiv.org/pdf/1401.3665v1`

[84] T.P. Kirkman, *On a problem in combinations*, The Cambridge and Dublin Mathematical Journal **2** (1847), 191–204.

[85] M. Klemm, *Über den p-Rang von Inzidenzmatrizen*, J. Combin. Theory Ser. A **43** (1986), 138–139.

[86] V. Krčadinac, *Steiner* 2*-designs*, 2010. `https://web.math.pmf.unizg.hr/~krcko/results/steiner.html`

[87] V. Krčadinac, *Unitali*, skripta, PMF-Matematički odsjek, 2010. `https://web.math.pmf.unizg.hr/~krcko/nastava/unitali10.pdf`

[88] V. Krčadinac, A. Nakić, M.O. Pavčević, *The Kramer-Mesner method with tactical decompositions: some new unitals on 65 points*, J. Combin. Des. **19** (2011), 290–303.

[89] V. Krčadinac, R. Vlahović, *New quasi-symmetric designs by the Kramer-Mesner method*, Discrete Math. **339** (2016), 2884–2890.

[90] C.W.H. Lam, L. Thiel, S. Swiercz, *The nonexistence of finite projective planes of order* 10, Canad. J. Math. **41** (1989), 1117–1123.

[91] E.S. Lander, *Symmetric designs: an algebraic approach*, Cambridge University Press, 1983.

[92] R. Laue, *Constructing objects up to isomorphism, simple* 9*-designs with small parameters*. Algebraic combinatorics and applications (Gössweinstein, 1999), 232–260, Springer, 2001.

[93] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes I, II*, North-Holland Publishing Co., 1977.

[94] F.J. MacWilliams, N.J.A. Sloane, J.G. Thompson, *Good self dual codes exist*, Discrete Math. **3** (1972), 153–162.

[95] K.N. Majumdar, *On some theorems in combinatorics relating to incomplete block designs*, Ann. Math. Statistics **24** (1953), 377–389.

[96] R. Mathon, *Constructions for cyclic Steiner* 2*-designs*, Ann. Discrete Math. **34** (1987), 353–362.

[97] R. Mathon, A. Rosa, 2-(v, k, λ) *designs of small order*, u: *The Handbook of Combinatorial Designs, Second Edition* (urednici C.J. Colbourn i J.H. Dinitz), CRC Press, 2007., str. 25–58.

[98] V.C. Mavron, T.P. McDonough, M.S. Shrikhande, *On quasi-symmetric designs with intersection difference three*, Des. Codes Cryptogr. **63** (2012), 73-86.

[99] T.P. McDonough, V.C. Mavron, H.N. Ward, *Amalgams of designs and nets*, Bull. Lond. Math. Soc. **41** (2009), 841–852.

[100] G. McGuire, *Quasi-symmetric designs and codes meeting the Grey-Rankin bound*, J. Combin. Theory Ser. A **78** (1997), 280–291.

[101] K. Metsch, *Quasi-residual designs,* $1\frac{1}{2}$*-designs, and strongly regular multigraphs*, Discrete Math. **143** (1995), 167–188.

[102] A. Munemasa, V.D. Tonchev, *A new quasi-symmetric* 2-$(56, 16, 6)$ *design obtained from codes* Discrete Math. **284** (2004), 231–234.

[103] A. Neumaier, *Regular sets and quasi-symmetric* 2*-designs*, Combinatorial theory (Schloss Rauischholzhausen, 1982), 258–275, Lecture Notes in Math. **969**, Springer, 1982.

[104] C. Parker, E. Spence, V.D. Tonchev, *Designs with the symmetric difference property on* 64 *points and their groups*, J. Combin. Theory Ser. A **67** (1994), 23–43.

[105] R.M. Pawale, *Quasi-symmetric designs with fixed difference of block intersection numbers*, J. Combin. Des. **15** (2007), 49–60.

[106] R.M. Pawale, *Quasi-symmetric designs with the difference of block intersection numbers two*, Des. Codes Cryptogr. **58** (2011), 111–121.

[107] R.M. Pawale, *A note on quasi-symmetric designs*, Australas. J. Combin. **57** (2013), 245–250.

[108] R.M. Pawale, S.S. Sane, *A short proof of a conjecture on quasi-symmetric* 3*-designs*, Discrete Math. **96** (1991), 71–74.

[109] R.M. Pawale, M.S. Shrikhande, S.M. Nyayate, *Conditions for the parameters of the block graph of quasi-symmetric designs*, Electron. J. Combin. **22** (2015), #P1.36, 30 str.

[110] R.M. Pawale, M.S. Shrikhande, S.M. Nyayate, *Non-derivable strongly regular graphs from quasi-symmetric designs*, Discrete Math. **339** (2016), 759–769.

[111] C. Peterson, *On tight* 6*-designs*, Osaka J. Math. **14** (1977), 417–435.

[112] V. Pless, *On the uniqueness of the Golay codes*, J. Combinatorial Theory **5** (1968), 215–228.

[113] V. Pless, *A classification of self-orthogonal codes over* $GF(2)$, Discrete Math. **3** (1972), 209–246.

[114] V. Pless, *The children of the* $(32, 16)$ *doubly even codes*, IEEE Trans. Inform. Theory **24** (1978), 738–746.

[115] V. Pless, N.J.A. Sloane, *On the classification and enumeration of self-dual codes*, J. Combinatorial Theory Ser. A **18** (1975), 313–335.

[116] R.A. Rankin, *The closest packing of spherical caps in* n *dimensions*, Proc. Glasgow Math. Assoc. **2** (1955), 139–144.

[117] R.A. Rankin, *On the minimal points of positive definite quadratic forms*, Mathematika **3** (1956), 15–24.

[118] D. Ray-Chaudhuri, R. Wilson, *Generalisation of Fisher's inequality to* t*-designs*, Notices Amer. Math. Soc. **18** (1971), 805.

[119] D. Ray-Chaudhuri, R. Wilson, *On* t*-designs*, Osaka J. Math. **12** (1975), 737-744.

[120] S.S. Sane, M.S. Shrikhande, *Quasisymmetric* 2,3,4*-designs*, Combinatorica **7** (1987), 291–301.

[121] C. Sarami, V.D. Tonchev, *Cyclic quasi-symmetric designs and self-orthogonal codes of length* 63, J. Statist. Plann. Inference **138** (2008), 80–85.

[122] M. Shrikhande, *A survey of some problems in combinatorial designs – a matrix approach*, Linear Algebra Appl. **79** (1986), 215–247.

[123] M.S. Shrikhande, *Quasi-symmetric designs*, u: *The Handbook of Combinatorial Designs, Second Edition* (urednici C.J. Colbourn i J.H. Dinitz), CRC Press, 2007., str. 578–582.

[124] M.S. Shrikhande, S.S. Sane, *Quasi-symmetric designs*, Cambridge University Press, 1991.

[125] S.S. Shrikhande, *Affine resolvable balanced incomplete block designs: a survey*, Aequationes Math. **14** (1976), 251–269.

[126] S.S. Shrikhande, D. Raghavarao, *A method of construction of incomplete block designs*, Sankhya Ser. A **25** (1963), 399–402.

[127] J. Steiner, *Combinatorische Aufgaben*, J. Reine Angew. Math. **45** (1853), 181–182.

[128] D.R. Stinson, *Combinatorial designs. Construction and analysis*, Springer, 2004.

[129] J. Šiftar, V. Krčadinac, *Konačne geometrije*, skripta, PMF-Matematički odsjek, 2013.
`https://web.math.pmf.unizg.hr/nastava/kg/kg-skripta.pdf`

[130] L. Teirlinck, *Nontrivial t-designs without repeated blocks exist for all t*, Discrete Math. **65** (1987), 301–311.

[131] V.D. Tonchev, *Quasi-symmetric designs and self-dual codes*, European J. Combin. **7** (1986), 67–73.

[132] V.D. Tonchev, *Quasi-symmetric* 2-$(31,7,7)$ *designs and a revision of Hamada's conjecture*, J. Combin. Theory Ser. A **42** (1986), 104-110.

[133] V.D. Tonchev, *Embedding of the Witt-Mathieu system* $S(3,6,22)$ *in a symmetric* 2-$(78,22,6)$ *design*, Geom. Dedicata **22** (1987), 49–75.

[134] V. Tonchev, *Self-orthogonal designs*, u: Finite geometries and combinatorial designs (urednici E.S. Kramer i S.S. Magliveras), Contemp. Math. **111**, Amer. Math. Soc., 1990., str. 219–235.

[135] V.D. Tonchev, *Quasi-symmetric designs, codes, quadrics, and hyperplane sections*, Geom. Dedicata **48** (1993), 295–308.

[136] J.H. van Lint, V.D. Tonchev, *A class of nonembeddable designs*, J. Combin. Theory Ser. A **62** (1993), 252–260.

[137] T. van Trung, *Nonembeddable quasi-residual designs*, u *Finite geometries and combinatorial designs* (urednici E.S. Kramer, S.S. Magliveras), Contemp. Math. **111**, Amer. Math. Soc., 1990., str. 237–278.

[138] H.N. Ward, *Block designs with SDP parameters*, Electron. J. Combin. **19** (2012), #P11, 7 str.

[139] A. Wassermann, *Finding simple t-designs with enumeration techniques*, J. Combin. Des. **6** (1998), 79–90.

[140] H.A. Wilbrink, A.E. Brouwer, *A* $(57, 14, 1)$ *strongly regular graph does not exist*, Nederl. Akad. Wetensch. Indag. Math. **45** (1983), 117–121.

[141] R.M. Wilson, *The necessary conditions for t-designs are sufficient for something*, Utilitas Math. **4** (1973), 207–215.

[142] R.M. Wilson, *An existence theory for pairwise balanced designs. III. Proof of the existence conjectures*, J. Combinatorial Theory Ser. A **18** (1975), 71–79.

[143] R.M. Wilson, *Incidence matrices of t-designs*, Linear Algebra Appl. **46** (1982), 73–82.

[144] R.M. Wilson, *Inequalities for t-designs*, J. Combin. Theory Ser. A **34** (1983), 313–324.

[145] E. Witt, *Über Steinersche Systeme*, Abh. math. Sem. Hansische Univ. **12** (1938), 265–275.