Kriptografija

Vizualna kriptografija in Hadamardjeve matrike

Aleš Zadravec
27004387

Ljubljana, 29.9.2004

Kazalo

1 Uvod

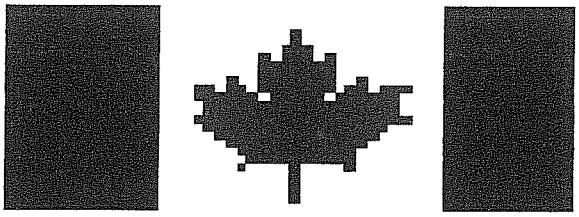
Cilj tega projekta je predstaviti, kako so Hadamardjeve matrike povezane z vizualno kriptografijo. Pri tem sem moral uporabiti snov o bločnih designih, zato jim je namenjeno krajše poglavje. Večji delež projekta predstavljajo Hadamardjeve matrike, ki so precej uporabne na več področjih v matematiki.

Vizualno shemo določimo, tako da konstruiramo bazne matrike iz bločnih designov. Slednje pa dobimo s pomočjo Hadamardjevih matrik, za katere je znanih veliko konstrukcij.

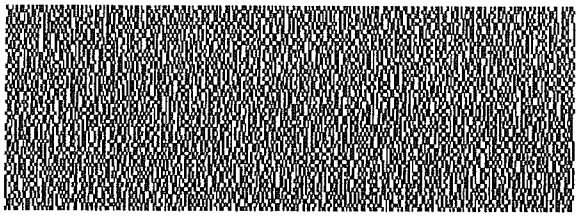
2 Osnove o vizualni kriptografiji

Naj bo $(2 \leq t \leq n)$. (n, t)-stopenjska shema za deljenje skrivnosti je rešitev problema, kako razdeliti med n ljudi take ključe, da lahko s t ključi oklenejo ključavnico, z manj ključi pa je ne morejo oz. ne dobijo nobenih podatkov, kako bi odklenili ključavnico. Varnost te sheme mora biti brezpogojna, torej neodvisna od kakšnega računsko zahtevnega problema.
Poseben primer te sheme sta leta 1994 odkrila M. Naor in A. Shamir. Vizualna shema je sestavljena iz prosojnic, na katerih se nahajajo črni in prozorni pravokotniki. Skrivnost je slika, ki jo dobimo, tako da prekrijemo t prosojnic, vseh pa je n. Če imamo samo $t-1$ prosojnic, ne moremo ugotoviti ničesar o sliki (shema je brezpogojno varna).
Slika je sestavljena iz črnih kvadratkov. Vsak kvadrat razdelimo na m delov.

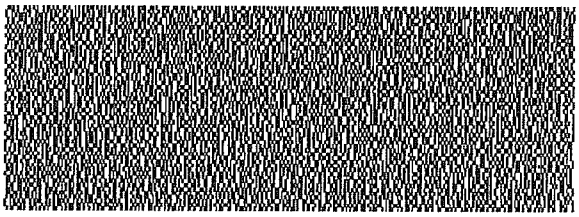
Na naslednji strani je primer $(2, 2)$-stopenjske vizualne sheme.



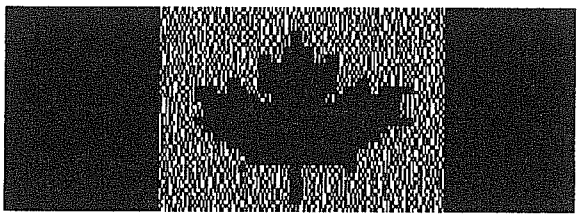
Slika 1: Originalna slika



Slika 2: 1. prosojnica



Slika 3: 2. prosojnica



Slika 4: Prekriti prosojnici

3 Bločni designi

Definicija 1 *Uravnotežen nepopoln bločni design je kombinatorični objekt, ki ga sestavlja b blokov (podmnožic univerzalne množice $S, |S| = v$), sestavljenih iz k ($k < v$) različnih elementov, tako da se vsak element pojavi v r blokih in vsak par različnih elementov se pojavi v λ blokih.*
Oznaka: (v, b, r, k, λ)-design.

Opomba: Pridevnik uravnotežen pomeni, da je število pojavitev poljubnega para iz različnih elementov v vseh blokih konstantno, torej λ = konstanta. Pridevnik nepopoln pomeni, da v blokih niso vsi elementi iz S, torej $k < v$.

Lema 1 *Za (v, b, r, k, λ)-design velja:*
a) $bk = vr$
b) $r(k-1) = \lambda(v-1)$

Dokaz: a) Enakost dobimo, tako da na dva različna načina preštejemo vse elemente designa. Vsak od b blokov vsebuje k elementov in vsak od v elementov se pojavi v r blokih.
b) Drugo enakost dobimo, tako da preštejemo vse pare, ki vsebujejo določen element t na dva različna načina. Element t se pojavi v r blokih in v vsakem od teh tvori par z ostalimi $k-1$ elementi. Po drugi strani pa t nastopa v paru λ-krat z vsakim od ostalih $v-1$ elementov.

■

Definicija 2 *(v, b, r, k, λ)-design je simetričen, če velja $v = b$.*
Oznaka: (v, k, λ)-design.

Opomba: Iz prve enakosti iz leme sledi, da za simetrični bločni design velja tudi $k = r$.

Primer: $S = \{1, 2, 3, 4, 5, 6, 7\}$, $(7, 3, 1)-$ design:

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 4 \\ 5 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 6 \\ 7 \end{pmatrix} \quad \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} \quad \begin{pmatrix} 2 \\ 5 \\ 7 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 4 \\ 7 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix}$$

Definicija 3 *Označimo* $S = \{t_1, \ldots, t_v\}$ *in z* $B_1, \ldots, B_b$ *bloke* (v, b, r, k, λ)-*designa. Incidenčna matrika* $A = [a_{ij}]_{i,j=1}^{v,b}$ *designa je definirana z*

$$a_{ij} = \begin{cases} 1 & ; \text{ če } t_i \in B_j \\ 0 & ; \text{ sicer} \end{cases}$$

Primer: Incidenčna matrika $(7, 3, 1)$-designa iz prejšnjega primera je

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

Izrek 1 *Če je* A *incidenčna matrika* (v, b, r, k, λ)-*designa, potem velja*

$$AA^T = (r - \lambda)I_v + \lambda J_v \text{ in} \tag{1}$$

$$J_v = kJ_{v \times b}, \tag{2}$$

kjer je I_n *identiteta velikosti* $n \times n$ *in* $J_{m \times n}$ *matrika samih enic velikosti* $m \times n$.
Obratno: Če obstaja $v \times b$ *matrika* A *z elementi 0 ali 1, ki zadošča* (1) *in* (2), *in če je* $k < v$, *potem velja:*

$$v = \frac{r(k-1)}{\lambda} + 1,$$

$$b = \frac{vr}{k}$$

in A *je incidenčna matrika* (v, b, r, k, λ)-*designa.*

Dokaz: Predpostavimo, da je A incidenčna matrika (v, b, r, k, λ)-designa. Najprej dokažimo enakost (1). (i, j)-ti element matrike AA^T je enak

$$\sum_{n=1}^{b} a_{in} a_{jn}.$$

$a_{in}a_{jn}$ je enak 1, ko oba elementa designa t_i in t_j pripadata bloku B_n, sicer pa je 0. Torej je $\sum_{n=1}^{b} a_{in}a_{jn}$ enaka številu blokov, ki vsebujejo t_i in t_j; to je r, ko je $i = j$ in λ sicer. Sledi:

$$AA^T = \begin{bmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda \\ \lambda & \cdots & \lambda & r \end{bmatrix} = rI + \lambda(J - I) = (r - \lambda)I + \lambda J$$

Za dokaz druge enakosti označimo $s_j = \sum_{k=1}^{v} a_{kj}$, to je vsota elementov j-tega stolpca matrike A. Iz definicije incidenčne matrike sledi, da je v vsakem stolpcu matrike A natanko k enic, ostali elementi pa so enaki 0. Torej $s_j = k, \forall j = 1, \ldots, b$.

$$JA = \begin{bmatrix} s_1 & s_2 & \cdots & s_b \\ s_1 & s_2 & \cdots & s_b \\ \vdots & \vdots & & \vdots \\ s_1 & s_2 & \cdots & s_b \end{bmatrix} = \begin{bmatrix} k & \cdots & k \\ \vdots & \ddots & \vdots \\ k & \cdots & k \end{bmatrix} = kJ$$

Pokažimo še drugi del izreka. Definiramo bločni design z elementi $t_i, i = 1, \ldots, v$ in bloki $B_j, j = 1, \ldots, b$, tako da velja

$$t_i \in B_j \Leftrightarrow a_{ij} = 1.$$

Brez težav vidimo, da je to (v, b, r, k, λ)-design (upoštevati še je treba $k < v$). Torej veljata tudi enakosti za v in b (glej lemo) in A je incidenčna matrika za ta design.

■

4 Hadamardjeve matrike

Definicija 4 *Kvadratna matrika H reda n je Hadamardjeva matrika, če so njeni elementi* 1 *ali* -1 *in velja*

$$HH^T = nI.$$

Opomba: Zadnja enakost je ekvivalentna trditvi, da sta poljubni dve vrstici matrike ortogonalni.

4.1 Lastnosti Hadamardjevih matrik

- Če Hadamardjevi matriki permutiramo vrstice, ostane Hadamardjeva.
  Dokaz: Sledi iz definicije Hadamardjeve matrike.

- Če Hadamardjevi matriki permutiramo stolpce, ostane Hadamardjeva.
  Dokaz: Vzemimo i-to in j-to vrstico matrike H, ki sta ortogonalni. Torej velja $\sum_{k=1}^{n} h_{ik}h_{jk} = 0$. Če stolpce od H permutiramo s poljubno permutacijo π, vidimo $\sum_{k=1}^{n} h_{i\pi(k)}h_{j\pi(k)} = \sum_{k=1}^{n} h_{ik}h_{jk} = 0$.

- Če poljubno vrstico(ali stolpec) Hadamardjeve matrike pomnožimo z -1, ostane Hadamardjeva.
  Dokaz: Sledi iz definicije ortogonalnosti dveh vektorjev.

- Velja: $HH^T = H^TH$. Dokaz:

$$\begin{aligned} H(\frac{1}{n}H^T) = I \quad &\Rightarrow \quad \frac{1}{n}H^T = H^{-1} \\ H^{-1}H \quad &= \quad \frac{1}{n}H^TH = I \\ HH^T \quad &= \quad nI = H^TH \end{aligned}$$

- Če je H Hadamardjeva, je H^T tudi Hadamardjeva.
  Dokaz: Iz prejšnje lastnosti sledi: $nI = HH^T = H^TH = H^T(H^T)^T$.

- Velja: $|\det H| = n^{n/2}$. Dokaz:

$$\begin{aligned} \det(HH^T) &= \det(nI) \\ (\det H)^2 &= n^n \det I \\ |\det H| &= n^{n/2} \end{aligned}$$

Definicija 5 *Hadamardjevi matrika je normalizirana, če sta prva vrstica in prvi stolpec matrike sestavljena samo iz enic.*

Opomba: Hadamardjevo matriko normaliziramo, tako da pomnožimo tiste stolpce in vrstice, katerih prvi element je -1, z -1.

Trditev 1 *Če Hadamardjeve matrike obstajajo, so reda* $1, 2$ *ali* $4k, k \in \mathbb{N}$.

Dokaz: Hadamardjeva matrika reda 1 je [1], reda 2 pa $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Za $n \geq 3$ naprej matriko H reda n normalizirajmo in si poglejmo prve tri vrstice le-te. Vrstice so sestavljene iz stolpcev oblike

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix},$$

kjer se prvi pojavi x-krat, drugi y-krat, tretji z-krat in četrti w-krat. Sedaj upoštevamo, da je vseh stolpcev n, in ortogonalnost vrstic. Dobimo naslednje enakosti:

$$\begin{aligned} x + y + z + w &= n \\ x + y - z - w &= 0 \\ x - y + z - w &= 0 \\ x - y - z + w &= 0. \end{aligned}$$

Rešitev tega sistema je $x = y = z = w = \frac{n}{4}$. Ker so $x, y, z, w \in \mathbb{N}$, velja $n = 4k$.

■

Primer: Hadamardjeva matrika reda 12

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

4.2 Zgodovina raziskovanja o Hadamardjevih matrikah

S Hadamardjevimi matrikami se je prvi ukvarjal J. J. Sylvester, ki je obravnaval matrike, ki so ortogonalne svojim transponirankam. Leta 1867 je izdal članek, v katerem omenja matrike z elementi 1 in -1 in konstrukcijo Hadamardjevih matrik reda $2^n, n \in \mathbb{N}$.

Leta 1893 je Jaques Hadamard odkril, da za poljubno matriko $A = [a_{ij}]_{i,j=1}^n$ velja naslednja neenakost:

$$|\det(A)|^2 \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |a_{ij}|^2,$$

in ugotovil, da matrike z elementi 1 in -1, katerih vrstice so paroma ortogonalne, zadoščajo enakosti v zgornji neenakosti. Res, leva stran neenakosti je n^n (glej lastnosti Hadamardjevih matrik), desna pa

$$\prod_{i=1}^{n} \sum_{j=1}^{n} 1 = \prod_{i=1}^{n} n = n^n.$$

Torej imajo Hadamardjeve matrike maksimalno determinanto med vsemi kompleksnimi matrikami A, za katere velja $|a_{ij}| \leq 1$. Prvi je pokazal, da morajo biti Hadamardjeve matrike reda $1, 2$ ali $4k, k \in \mathbb{N}$ in domneval, da za vse te rede tudi obstajajo (Hadamarjeva domneva). Ta domneva še danes ni

potrjena ali ovržena. Trenutno so znane kontrukcije Hadamardjevih matrik do reda 424, torej je neznana matrika reda 428.

Veliko je prispeval leta 1933 mlad matematik R. E. A. C. Paley, ki se je žal kmalu zatem ubil v smučarski nesreči. Njegovo konstrukcijo Hadamardjevih matrik, ki je dala rešitve za precej redov, je leta 1944 in 1947 izboljšal Williamson in dodal nekaj svojih prijemov. Zaradi obsežnosti teh konstrukcij ne bom obravnaval.

Po drugi svetovni vojni se je s Hadamardjevimi matrikami ukvarjalo veliko matematikov, saj so uporabne v kriptografiji, teoriji kodiranja, statistiki in optiki.

4.3 Sylvestrova konstrukcija Hadamardjevih matrik z direktnim produktom

Naj bo A matrika velikosti $p \times q$ in B matrika reda $r \times s$. Potem je direktni produkt matrik definiran kot

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1q}B \\ a_{21}B & a_{22}B & \cdots & a_{2q}B \\ \vdots & \vdots & & \vdots \\ a_{p1}B & a_{p2}B & \cdots & a_{pq}B \end{bmatrix},$$

ki je velikosti $pr \times qs$.

Lema 2 *Velja:*

$$\begin{aligned} &a) \quad \alpha(A \otimes B) = (\alpha A) \otimes B = A \otimes (\alpha B), \\ &b) \quad (A \otimes B)^T = A^T \otimes B^T, \\ &c) \quad (A \otimes B)(C \otimes D) = AC \otimes BD, \end{aligned}$$

kjer sta A in C $n \times n$ matriki, B in D pa $m \times m$ matriki.

Dokaz:
a)Enakost sledi iz definicije direktnega produkta.

b)Transponiranje katerekoli bločne matrike se vrši po pravilu:

$$\begin{bmatrix} X & Y \\ Z & W \end{bmatrix}^T = \begin{bmatrix} X^T & Z^T \\ Y^T & W^T \end{bmatrix}.$$

Torej $(A \otimes B)^T = [(a_{ij}B)^T] = [a_{ji}B^T] = A^T \otimes B^T$
c)Poljuben produkt $XY = [X_{ij}][Y_{ij}]$ dveh bločnih matrik ima na ij-tem mestu blok

$$\sum_k X_{ik}Y_{kj},$$

če je število stolpcev v bloku X_{ij} enako številu vrstic v bloku Y_{ij} in je število blokov v X po vrsticah enako številu blokov v Y po stolpcih.
Torej je ij-ti blok matrike $(A \otimes B)(C \otimes D)$ enak

$$\sum_{k=1}^{n}(a_{ik}B)(c_{kj}D) = \left(\sum_{k=1}^{n} a_{ik}c_{kj}\right) BD = (AC)_{ij}BD$$

Torej velja $(A \otimes B)(C \otimes D) = AC \otimes BD$.

■

Trditev 2 *Če obstajata Hadamardjevi matriki H_1 reda n in H_2 reda m, je njun direktni produkt $H_1 \otimes H_2$ tudi Hadamardjeva matrika reda $n \times m$.*

Dokaz:

$$\begin{aligned}(H_1 \otimes H_2)(H_1 \otimes H_2)^T &= (H_1 \otimes H_2)(H_1^T \otimes H_2^T) = \\ H_1H_1^T \otimes H_2H_2^T &= nI_n \otimes mI_m = mnI_{mn}\end{aligned}$$

Vsi elementi matrik H_1 in H_2 so -1 ali 1, zato sledi iz definicije direktnega produkta, da so tudi elementi $H_1 \otimes H_2$ le 1 ali -1.

■

Primer:

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

Posledica 1 *Če obstajata Hadamardjevi matriki reda m in n, potem obstaja Hadamardjeva matrika reda nm.*

4.4 Hadamardjeve matrike in bločni designi

Izrek 2 *Hadamardjeva matrika reda $4n$ obstaja natanko takrat, ko obstaja $(4m-1, 2m-1, m-1)$-design.*

Dokaz: Predpostavimo, da je H Hadamardjeva matrika reda $4n$. Brez škode za splošnost lahko predpostavimo, da je H normalizirana. Ker je H Hadamardjeva, vemo, da velja

$$\sum_{k=1}^{4n} h_{1k}h_{jk} = 0, \text{če } j \neq 1,$$

torej $\sum_{k=1}^{4n} h_{jk} = 0$. Podobno lahko sklepamo: $\sum_{k=1}^{4n} h_{kj} = 0$, če je $j \neq 1$. Torej so vsote elementov v poljubni vrstici oziroma stolpcu, razen v prvi oziroma prvem, enake nič.
Naj bo A matrika velikosti $(4n-1)\times(4n-1)$, ki jo dobimo iz H z odstranitvijo prve vrstice in prvega stolpca.

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{bmatrix}.$$

Tedaj je vsota poljubne vrstice ali stolpca matrike A enaka -1 ali ekvivalentno

$$AJ = JA = -J,$$

kjer je J matrika velikosti $(4n-1)\times(4n-1)$, katere elementi so vsi 1.
Ker je $HH^T = 4nI$, vidimo, da velja

$$AA^T = \begin{bmatrix} 4n-1 & -1 & \cdots & -1 \\ -1 & 4n-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \cdots & -1 & 4n-1 \end{bmatrix} = 4nI - J.$$

Sedaj poglejmo matriko $B = (A + J)/2$. Tedaj imamo

$$BJ = \frac{1}{2}(AJ + JJ) = \frac{1}{2}(-J + (4n-1)J) = (2n-1)J$$

in podobno

$$JB = (2n-1)J. \qquad (*)$$

Velja

$$\begin{aligned} BB^T &= \frac{1}{4}(A+J)(A^T+J) = \frac{1}{4}(AA^T + JA^T + AJ + JJ) = \\ &= \frac{1}{4}((4nI - J) - J - J + (4n-1)J) = nI + (n-1)J. \qquad (+) \end{aligned}$$

Iz enačb $(*)$ in $(+)$ po izreku 1 sledi, da je matrika B incidenčna matrika $(4n-1, 2n-1, n-1)$-designa.
Predpostavimo sedaj, da obstaja $(4n-1, 2n-1, n-1)$-design. Naj bo C njegova incidenčna matrika in definirajmo $A = 2C - J$. Skonstruirajmo matriko H, tako da pripnemo matriki A novo prvo vrstico in stolpec samo iz enic. Ni se težko prepričati, da je H Hadamardjeva matrika.

■

Literatura

[1] Članki iz internetne strani Douglasa R. Stinsona (www.cacr.math.uwaterloo.ca/~dstinson/visual.html)

[2] W. D. Wallis, Combinatorial Designs, Monographs and textbooks in pure and applied mathematics, Marcel Dekker, 1988

[3] Marshall Hàll Jr., Combinatorial Theory, Second Edition, John Wiley & Sons, 1986

[4] Jeffrey H. Dinitz, Douglas R. Stinson, Contemporary Design Theory, A Collection of Surveys, John Wiley & Sons, 1992

[5] D. Cvetković, S. Simić, Kombinatorika, klasična i moderna, Drugo izmenjeno i dopunjeno izdanje, Načna knjiga, 1990