HADAMARDOVE MATRIKE IN MISIJA MARINER 9

ALEKSANDAR JURIŠIĆ

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

Math. Subj. Class. (2000): 05B20, 05B25, 05B30, 05C12, 05C62, 05C50, 05E20, 05E30, 05E35, 68R05, 68R10, 68R141, 11T71, 51E, 52C

J. Hadamard (1865–1963) je bil eden izmed pomembnejših matematikov na prehodu iz 19. v 20. stoletje. Njegova najpomembnejša dela zajemajo področja teorije analitičnih funkcij in matematične fizike. Najbolj znan pa je po dokazu izreka o gostoti praštevil (leta 1896, hkrati s C. J. De La Vallée-Poussinom). V tem članku predstavljamo Hadamardove matrike, njihove karakterizacije s Hadamardovimi grafi, geometrijami in Hadamardovimi kodami ter nekaj zanimivih konstrukcij in uporabo Hadamardovih matrik v praksi.

HADAMARD MATRICES AND MARINER 9 MISSION

J. Hadamard (1865–1963) was one of more important mathematicians at the turn of the 19$^{\text{th}}$ century. His is most celebrated for his contributions in analtycal functions and mathematical physics. His most important result is the prime number theorem, which he proved in 1896 (at the same time as C. J. De La Vallée-Poussin). In this article we introduce Hadamard matrices, their characterizations with Hadamard graphs, geometries and Hadamard codes, some interesting constructions and applications of Hadamard matrices in practice.

Hadamardove matrike

Naj bo A kvadratna matrika z n stolpci, za katero velja $|(A)_{ij}| \leq 1$. Kako velika je lahko $\det A$? Če si vrstice (oziroma stolpce) matrike A predstavljamo kot vektorje v $\mathbb{R}^n$, potem je njihova dolžina navzgoraj omejena s $\sqrt{n}$. Po drugi strani pa vemo, da absolutna vrednost determinante predstavlja prostornino paralelepipeda, ki ga določajo ti vektorji, torej velja $|\det A| \leq n^{n/2}$. Ali lahko v tej neenakosti velja enakost? V tem primeru so vsi elementi matrike enaki ± 1, vsaki dve različni vrstici (oziroma stolpca) pa morata biti paroma pravokotni. To je bila motivacija Brennerja (1972) za naslednjo definicijo.

Kvadratni matriki H z n vrsticami in z elementi ± 1, za katero velja

$$HH^T = nI_n, \tag{1}$$

pravimo *Hadamardova matrika* reda n. Glede na to, da matrični produkt v (1) sestavljajo produkti vrstic matrike H, lahko stolpce (oziroma vrstice)

Hadamardove matrike poljubno premešamo (permutiramo) ali pa pomnožimo z -1, pa bo nova matrika še vedno Hadamardova. Rekli bomo, da sta si taki Hadamardovi matriki *ekvivalentni*. Na prvi pogled se zdi, da identiteta (1) zagotavlja le pravokotnost vrstic. Vendar jo lahko pomnožimo z desne s H in dobimo $HH^TH = nI_nH$ oziroma $HH^TH = HnI_n$. Upoštevamo še obrnljivost matrike H, in že smo pri identiteti $H^TH = nI_n$, v kateri sta vlogi vrstic in stolpcev zamenjani glede na identiteto (1). To pomeni med drugim tudi, da so različni stolpci matrike H paroma pravokotni. Predstavimo nekaj manjših Hadamardovih matrik:

$$(1)\,,\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \text{ in } \begin{pmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{pmatrix}$$

(v slednji smo ± 1 zamenjali s $+$ in $-$). Zgornje Hadamardove matrike označimo zaporedoma s H_1, H_2, H_4 in H_8 (indeks torej kaže njihovo velikost). Opazimo, da sta v vseh štirih primerih prva vrstica in prvi stolpec sestavljena iz samih enic. Same enice v prvem stolpcu oziroma vrstici Hadamardove matrike dobimo tako, da vrstice oziroma stolpce matrike H, ki se začnejo z negativnim številom, pomnožimo z -1. Temu postopku pravimo *normalizacija*. Če je $n > 1$, potem mora imeti v normalizirani matriki vsaka preostala vrstica polovico pozitivnih in polovico negativnih elementov, kar pomeni, da je n sod. S podobnim razmislekom pridemo do še močnejšega sklepa.

Trditev. *Če je H Hadamarova matrika reda n, potem je $n = 1$, $n = 2$ ali pa $4 \mid n$.*

Dokaz. Naj bo $n > 2$. Normaliziramo H, potem pa s permutacijo stolpcev spravimo prve tri vrstice matrike H v naslednjo obliko:

$$\begin{array}{ll} \text{1. vrstica} & \underbrace{+\,+\,+\,\ldots\,+\,++}_{a} \ \underbrace{+\,+\,+\,\ldots\,+\,++}_{b} \ \underbrace{+\,+\,+\,\ldots\,+\,++}_{c} \ \underbrace{+\,+\,+\,\ldots\,+\,++}_{d} \\ \text{2. vrstica} & \underbrace{+\,+\,+\,\ldots\,+\,++}_{a} \ \underbrace{+\,+\,+\,\ldots\,+\,++}_{b} \ \underbrace{-\,-\,-\,\ldots\,-\,--}_{c} \ \underbrace{-\,-\,-\,\ldots\,-\,--}_{d} \\ \text{3. vrstica} & \underbrace{+\,+\,+\,\ldots\,+\,++}_{a} \ \underbrace{-\,-\,-\,\ldots\,-\,--}_{b} \ \underbrace{+\,+\,+\,\ldots\,+\,++}_{c} \ \underbrace{-\,-\,-\,\ldots\,-\,--}_{d} \end{array}$$

Za $a, b, c, d \in \mathbb{N}_0$ velja:

$$\begin{aligned} &a+b+c+d = n, \\ &a-b+c-d = 0 \quad \text{(produkt tretje vrstice s prvo vrstico)}, \\ &a+b-c-d = 0 \quad \text{(produkt druge vrstice s prvo vrstico)}, \\ &a-b-c+d = 0 \quad \text{(produkt druge in tretje vrstice)}, \end{aligned}$$

vsota zgornjih štirih enačb pa nam da $4a = n$. ∎

Če se v zgornjem sistemu enačb osredotočimo samo na predznake, v njem zagledamo matriko, ki je ekvivalentna H_4. Kot bomo videli, lahko pridemo do H_4 na več načinov. Do naslednjega si v naslednjem razdelku pomagamo z grafi, bolj natančno s 4-razsežno kocko.

Karakterizaciji z grafi in geometrijami

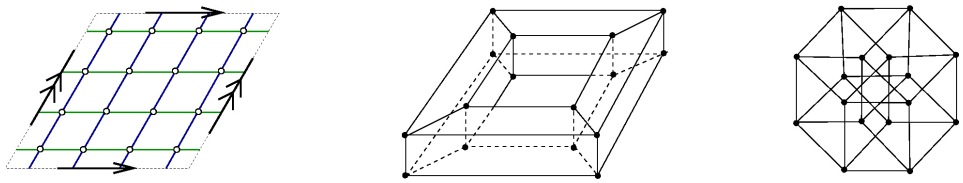
V povezanem grafu je *razdalja* med dvema vozliščema definirana kot število povezav najkrajše poti med njima, njegov *premer* pa je enak največji razdalji med njegovimi vozlišči. V povezanem grafu premera $d \in \mathbb{N}$ izberimo vozlišči u in v, ki sta na razdalji $i \in \{0, 1, \ldots, d\}$, ter opazujmo sosede vozlišča v glede na razdaljo od vozlišča u. Zaradi trikotniške neenakosti velja, da so le-ta od u lahko oddaljena bodisi $i-1$ (kadar je $i > 0$), i ali pa $i+1$ (kadar je $i < d$). Število teh sosedov na razdalji $i-1$, i in $i+1$ označimo zaporedoma s c_i, a_i in b_i. Očitno je $a_0 = 0$ in $c_1 = 1$, smiselno pa je privzeti še $c_0 = 0 = b_d$. Če števila a_i, b_i in c_i niso odvisna od izbire vozlišč u in v na razdalji i za vsak $i \in \{0, \ldots, d\}$, bomo rekli, da je graf *razdaljno-regularen*. Tak graf je seveda regularen, saj je število sosedov vsakega njegovega vozlišča enako b_0. Zato velja tudi $b_0 = a_i + b_i + c_i$ in v njegovem *presečnem zaporedju*: $\{b_0, \ldots, b_{d-1}; c_1, \ldots, c_d\}$ običajno izpustimo števila $a_1, \ldots, a_d$ (vseeno pa je treba omeniti, da število a_i predstavlja ravno regularnost grafa, ki ga inducirajo vozlišča na razdalji i od poljubnega vozlišča).

Hadamardov graf reda $2n$, $n \in \mathbb{N}$, je razdaljno-regularen graf s presečnim zaporedjem

$$\{2n, 2n-1, n, 1;\ 1, n, 2n-1, 2n\}.$$

Pri Hadamardovem grafu torej velja $a_i = 0$ za $i = 1, 2, 3, 4$. Za $n = 1$ dobimo 8-cikel (C_8), za $n = 2$ pa 4-razsežno kocko (Q_4). Glej sliko 1, s katere se lahko hitro prepričamo, da gre pri $n = 2$ res za Hadamardov graf.

Če pa se želimo prepričati, da je za $n = 2$ vsak Hadamardov graf izomorfen Q_4, je morda smiselno preučiti še kakšno lastnost teh grafov. Za

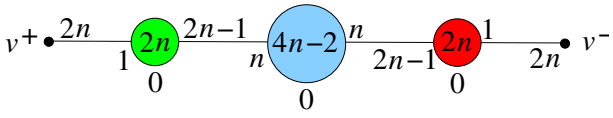


Slika 1. 4-razsežna kocka, predstavljena na tri načine (prva dva sta povezana z vložitvijo na torus): zaradi simetrije lahko izberemo za vozlišče u iz definicije razdaljno-regularnega grafa poljubno vozlišče. Potem je očitno $b_0 = 4$. Ker v tem grafu ni trikotnikov, velja $a_1 = 0$ in zato tudi $b_1 = 3$. Sledi $c_2 = 2$, $a_2 = 0$ (glede na to, da v grafu ni niti petkotnikov) ter $b_2 = 2$. Tako nadaljujemo vse do konca.

graf premera d pravimo, da je *antipoden*, če je biti na razdalji d ali 0 ekvivalenčna relacija na množici vozlišč. Če pa je v antipodnem grafu velikost vsakega antipodnega razreda enaka 2, rečemo, da je G 2-*krov*. In v resnici gre za topološke 2-krove. Npr. C_8 krije C_4, Q_8 pa poln dvodelen graf $K_{4,4}$, kot bomo videli v nadaljevanju.

Lema. *Hadamardov graf reda* $2n$ *je dvodelen* 2-*krov premera* 4 *z* $8n$ *vozlišči.*

Dokaz. Naj bo G Hadamardov graf reda $2n$. Ker je $c_4 = b_0$, je premer grafa G enak štiri.



Slika 2. Razdaljna particija Hadamardovega grafa glede na izbrano vozlišče: na levi je vozlišče v^+, nato proti desni sledijo v prvem krogu zbrani njegovi sosedi, v drugem zbrana vozlišča na razdalji 2 od v^+, v tretjem vozlišča na razdalji 3 in končno še vozlišče v^- na maksimalni razdalji. Povezave lahko potekajo le med zaporednimi krogi ali znotraj njih. Števila znotraj krogov predstavljajo števila k_i, tik nad črto so števila b_i, pod njo pa števila c_i. Pod krogi pa so še števila a_i.

Naj bo k_i oznaka za število vozlišč na razdalji i od fiksnega vozlišča. Ker poznamo presečno zaporedje grafa G, lahko izračunamo iz rekurzivne zveze $k_i c_i = k_{i-1} b_{i-1}$ (ki na dva načina šteje povezave med vozlišči, ki so na razdalji i in $i+1$): $k_1 = b_0 = 2n$, $k_2 = 4n - 2$, $k_3 = 2n$ in končno $k_4 = 1$. To pomeni, da ima G res $8n$ vozlišč in da za vsako vozlišče v^+ v grafu G obstaja natanko eno vozlišče v^-, ki je na razdalji 4 od vozlišča v^+, torej je graf G 2-krov. Sedaj izberemo poljubno vozlišče v, nato pa množico vseh vozlišč grafa G razdelimo na dva dela glede na to, ali je razdalja do

vozlišča v soda oziroma liha. Vozlišča, ki so na razdalji $i \in \{1,2,3,4\}$ od vozlišča v, inducirajo graf stopnje a_i. Ker pa je $a_i = 0$, to pa pomeni, da nam je uspelo razdeliti vozlišča grafa G na dva dela, tako da vsak del zase ne vsebuje sosednjih vozlišč, tj. graf G mora biti dvodelen. ∎

Za vozlišči v^+ in v^- iz zgornjega dokaza bomo rekli, da sta *antipodni*, saj sestavljata antipodni razred. Mimogrede, tudi 1-skeleti Platonovih teles so razdaljno-regularni 2-krovi.

Konstrukcija. *Naj bo G Hadamardov graf reda $2n$. Ker je G dvodelen graf, obstaja delitev njegovih vozlišč na množici A in B, od katerih nobena ne vsebuje sosednjih vozlišč. Potem je $|A| = |B| = k_1+k_3 = 1+k_2+k_4 = 4n$. Ker sta antipodni vozlišči na medsebojni razdalji 4, morata obe ležati bodisi v množici A bodisi v množici B. V posamezni množici A oziroma B imamo torej $2n$ parov antipodnih vozlišč. Pare iz A označimo z $a_1, a_2, \ldots, a_{2n}$, iz B pa z $b_1, b_2, \ldots, b_{2n}$. Potem je vsako vozlišče para $a_i = \{a_i^+, a_i^-\}$ sosednje natanko enemu izmed vozlišč para $b_j = \{b_j^+, b_j^-\}$. Naj bo H $(2n \times 2n)$-razsežna matrika, za katero je $H_{ij} = 1$, če je vozlišče a_i^+ sosednje vozlišču b_j^+ in $H_{ij} = -1$ sicer.*

Opomba. Naj bo G antipoden graf. Potem dobimo *antipodni kvocient* grafa G tako, da vzamemo za njegova vozlišča antipodne razrede, dva razreda pa sta sosednja, če je v G med njima kakšna povezava. Iz priprave na zgornjo konstrukcijo je razvidno, da je antipodni kvocient Hadamardovega grafa reda $2n$ res poln dvodelen graf $K_{2n,2n}$. Kaj pa so antipodni kvocienti 1-skeletov Platonovih teles?

Trditev. *Matrika H iz zgornje konstrukcije je Hadamardova.*

Dokaz. Ker je skalarni produkt vsake vrstice te matrike s seboj enak $k_1 = 2n$, je dovolj pokazati, da sta poljubni različni vrstici, npr. $i \neq i'$, med seboj pravokotni. Vrednosti, ki jih imata ti vrstici v j-tem stolpcu, se ujemata, če sta para vozlišč a_i in $a_{i'}$ povezana s parom b_j na enak način, se pravi, če je z obema vozliščema a_i^+ in $a_{i'}^+$ povezano bodisi vozlišče b_j^+ bodisi b_j^-. Ujemanje vrednosti vrstic v j-tem stolpcu torej pomeni, da imata vozlišči a_i^+ in $a_{i'}^+$ skupnega soseda (če pa ga nimata, ga morata imeti a_i^+ in $a_{i'}^-$). Skalarni produkt dveh različnih vrstic je zato enak $c_2 - (2n - c_2) = 2(c_2 - n) = 0$. ∎

Prišli smo na pol poti do naslednjega izreka.

Izrek (Darke, Shad, Delorme). *Za $n \in \mathbb{N}$ obstaja Hadamardov graf reda $2n$ natanko tedaj, ko obstaja Hadamardova matrika reda $2n$.*

Pri drugem delu dokaza tega izreka pa nam pomaga konstrukcija iz naslednje trditve:

Trditev. *Naj bo H Hadamardova matrika reda $2n$, $n \in \mathbb{N}$. Potem je graf $G(H)$ z vozlišči $a_i^+, a_i^-, b_i^+, b_i^-$, $i \in \{1, \dots, 2n\}$ in povezavami $\{a_i^\varepsilon, b_j^\eta\}$, kjer je $\varepsilon = \eta$, če je $H_{ij} = 1$ in $\varepsilon \neq \eta$, če je $H_{ij} = -1$, Hadamardov graf.*

Dokaz. Zaradi očitne simetrije v definiciji grafa $G(H)$ med vozlišči a_i^+, a_i^-, b_i^+ in b_i^- je dovolj opazovati vozlišča glede na njihovo razdaljo od vozlišča $u = a_i^+$. Potem je $\{b_j^\varepsilon \mid \varepsilon = \operatorname{sgn}(H_{ij})\}$ množica sosedov vozlišča u, $\{a_j^\varepsilon \mid i \neq j\}$ množica vozlišč na razdalji 2 od u, $\{b_j^\varepsilon \mid \varepsilon = -\operatorname{sgn}(H_{ij})\}$ množica vozlišč na razdalji 3 od u, edino preostalo vozlišče a_i^- pa je potem na razdalji 4 od u.

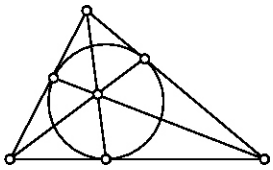
Torej je $G(H)$ antipoden graf premera 4 s presečnimi števili $b_0(G) = 2n = c_4$, $c_1(G) = 1 = b_3$, $b_1(G) = 2n - 1 = c_3$ in $c_2(G) = n = b_2$. ∎

Iz Hadamardovih grafov je Nomura [10] skonstruiral objekte, ki se imenujejo *spin modeli* in so povezani tako s fiziko kot tudi s teorijo vozlov, glej npr. [4].

Na kratko omenimo še eno karakterizacijo Hadamardovih matrik. Le-ta je povezana s *končnimi geometrijami*. Naj bo H Hadamardova matrika, ki smo jo normalizirali tako, da so v prvem stolpcu in prvi vrstici same enice. Če zbrišemo prvi stolpec in prvo vrstico, dobimo kvadratno matriko N reda $4n - 1$, ki je $(-1, 1)$ točka/premica incidenčna matrika *Hadamardovega 2-načrta*. Predstavlja kvadratni 2-$(4n - 1, 2n - 1, n - 1)$ načrt, tj. končno geometrijo, sestavljeno iz

- množice $4n - 1$ točk in enako velike množice blokov (premic),
- velikost vsakega bloka je $2n - 1$, kar je hkrati tudi število blokov, ki vsebujejo poljubno točko,
- poljubni dve točki ležita v $n - 1$ blokih (to število pa hkrati pomeni tudi velikost preseka poljubnih dveh blokov).

Naj bo I relacija incidenčnosti med točkami in bloki. *Paleyjev načrt* definiramo takole: če je $4n - 1 = q$ potenca praštevila, potem vzamemo za točke in bloke elemente končnega obsega s q elementi, tj. $\mathrm{GF}(q)$, ter $x \, I \, y$



Slika 3. Fanova ravnina

natanko tedaj, ko $x + y$ ni popoln kvadrat. Za $q = 7$ dobimo znano *Fanovo ravnino* (glej sliko 3), iz nje pa H_8.

Geometrija, ki jo dobimo za $q = 11$, pa je povezana z enostavno končno grupo M_{12}, znano pod imenom *Mathieujeva grupa*, in že smo pri Hadamardovi matriki reda 12. Omenimo še, da lahko tedaj, ko je q praštevilo, za incidenčno matriko izberemo cirkulant, tj. matriko, katere vrstice dobimo s cikličnim zamikom prve.

Konstrukcije in Hadamardova matrična domneva

Iz n-razsežne Hadamardove matrike U in m-razsežne Hadamardove matrike V lahko s tenzorskim produktom matrik, ki je definiran z

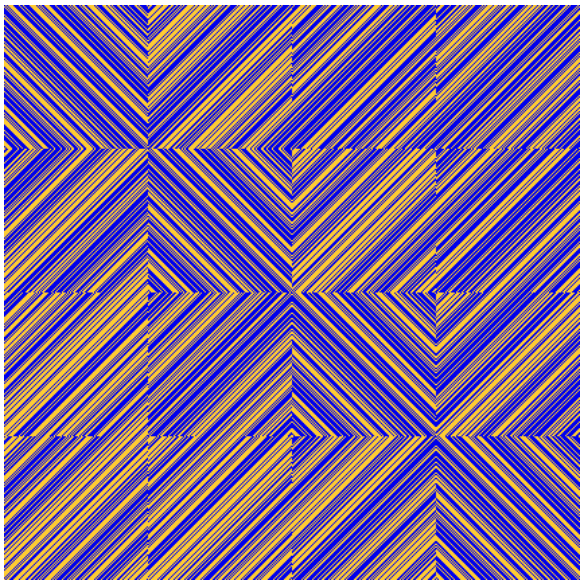
$$U \otimes V = \begin{bmatrix} u_{11}V & u_{12}V & \dots \\ u_{21}V & u_{22}V & \\ \vdots & & \ddots \end{bmatrix} = \begin{bmatrix} u_{11}v_{11} & u_{11}v_{12} & \dots & u_{12}v_{11} & u_{12}v_{12} & \dots \\ u_{11}v_{21} & u_{11}v_{22} & & u_{12}v_{21} & u_{12}v_{22} & \\ \vdots & & \ddots & & & \\ u_{21}v_{11} & u_{21}v_{12} & & & & \\ u_{21}v_{21} & u_{21}v_{22} & & & & \\ \vdots & & & & & \end{bmatrix},$$

sestavimo (nm)-razsežno Hadamardovo matriko (namig: uporabi identiteti $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ in $(A \otimes B)^T = A^T \otimes B^T$). Bralec lahko hitro preveri, da velja $H_4 = H_2 \otimes H_2$ in $H_8 = H_2 \otimes H_4$, ter rekurzivno konstruira še Hadamardovo matriko H_n reda $n = 2^k$ za vsak $k \in \mathbb{N}$. Omenimo še, da je vsaka Hadamardova matrika velikosti n, $n \leq 8$, ekvivalentna H_1, H_2, H_4 ali H_8. Tudi Hadamardova matrika reda 12 je enolično določena (do ekvivalentnosti), po drugi strani pa obstaja natanko pet neekvivalentnih Hadamardovih matrik reda 16, tri reda 20, 60 reda 24 in 487 reda 28. Dobljeno zaporedje $1, 1, 1, 5, 3, 60, 487, \dots$ ima oznako Sloan A007299.

Za konstrukcijo Hadamardovih matrik lahko uporabimo tudi *konferenčne matrike*, ki jih je leta 1950 vpeljal Belevitch [1] (za uporabo v telefoniji).

Drugače od Hadamardovih matrik ima n-razsežna konferenčna matrika C na diagonali same ničle in velja $CC^T = (n-1)I$. Posebno enostavni sta konstrukciji, če je C

- antisimetrična: v tem primeru vzamemo $H = I + C$, ali pa
- simetrična: dvakrat večja matrika H je v tem primerub sestavljena iz štirih blokov, na diagonali $I + C$ in $-I - C$, preostala bloka pa sta enaka $I - C$.



Slika 4. (428×428)-razsežna Hadamardova matrika, tj. matrika s paroma pravokotnimi stolpci in elementi, enakimi bodisi $+1$ (svetli piksli) bodisi -1 (temnni piksli). Ta primer sta odkrila H. Kharaghani in B. Tayfeh-Rezaie leta 2004 kot prvo tako matriko te velikosti. Še vedno pa ne vemo, ali obstaja (668×668)-razsežna Hadamardova matrika, čeprav je bila postavljena domneva, da $(4n \times 4n)$-razsežni primeri obstajajo za vsak $n \in \mathbb{N}$.

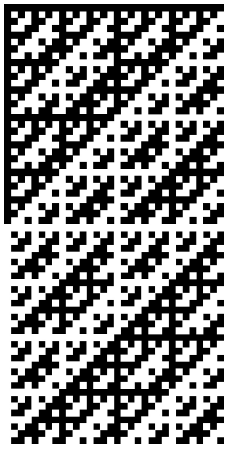
Konferenčne matrike reda $q+1$ (oziroma $2(q+1)$), kjer je q potenca praštevila in je $q \equiv 3 \pmod 4$ (oziroma $q \equiv 1 \pmod 4$), pa je konstruiral Paley leta 1933 [11] iz končnih obsegov (in popolnih kvadratov, ki jih je ravno polovica med neničelnimi elementi). Že samo pravkar opisane konstrukcije so dovolj, da skonstruiramo Hadamardove matrike do reda 100, z izjemo $n = 92$.[1] V slednjem primeru pa so L. Baumert, S. W. Golomb in M. Hall

[1]Bolj natančno znamo s Paleyjevim izrekom skonstruirati Hadamardovo matriko reda n, ko $2^e \mid n$ za $e > 1$ in je $(n/2^e) - 1$ potenca lihega praštevila. Za $n < 1000$ nam potem

leta 1962 poleg Williamsonove bločne metode [12], ta je prvi skonstruiral Hadamardovo matriko reda 172, že uporabili računalnike. Slavna *Hadamardova matrična domneva* iz leta 1893 pravi, da obstaja Hadamardova matrika reda $4n$ za vsako naravno število n. Leta 2004 sta iranska matematika H. Kharaghani in B. Tayfeh-Rezaie [7] konstruirala Hadamardovo matriko reda 428 (na sliki 4 je lepo razvidna tudi Williamsonova bločna metoda). Najmanjši odprti primeri obstoja Hadamardove matrike so sedaj matrike reda 668, 716, 876, 892. Najnovejšo konstrukcijo (Hadamardova matrika reda 764) pa je lansko leto odkril Djoković [3].

Hadamardove kode in ekspedicija Mariner 9

Definicija Hadamardovih matrik nam zagotavlja nekakšno „uravnoteženost“, zato jih lahko uporabimo na številnih področjih. Tu predstavljamo sestavljanje učinkovitih kod za odpravljanje napak. Spomnimo se, da je *koda* podmnožica nekega prostora, v katerem je definirana razdalja [6]. Na prostoru m-teric najbolj pogosto uporabljamo Hammingovo razdaljo, ki je enaka številu različnih koordinat med dvema n-tericama. Morebitne napake v tem primeru odpravljamo po principu *najbližjega soseda*, ki dani m-terici izbere najbližji element kode.



Slika 5. H-koda

ostanejo še naslednje velikosti: 92, 116, 156, 172, 184, 188, 232, 236, 260, 268, 292, 324, 356, 372, 376, 404, 412, 428, 436, 452, 472, 476, 508, 520, 532, 536, 584, 596, 604, 612, 652, 668, 712, 716, 732, 756, 764, 772, 808, 836, 852, 856, 872, 876, 892, 904, 932, 940, 944, 952, 956, 964, 980, 988, 996.

Naj bo H Hadamardova matrika reda $4m$. Vzemimo vrstice matrike H in matrike $-H$ ter zamenjajmo vse „-1“ z „0“, glej sliko 5. Tako dobimo $8m$ vektorjev dolžine $4m$ nad binarnim obsegom $\mathbb{Z}_2$ (pri dolžini mislimo na število koordinat in ne evklidske razdalje). Neposredno iz definicije Hadamardove matrike sledi, da je Hammingova razdalja med poljubnima različnima vektorjema bodisi $2m$ ali $4m$ (razdalja do svojega negativa je $4m$, do vseh drugih pa $2m$). Te vrstice generirajo vektorski podprostor v $(\mathbb{Z}_2)^{4m}$, ki predstavlja kodo. Potem je njena najmanjša razdalja $2m$, koda pa lahko popravi do $(m-1)$-napak.

Tako dobljenim kodam pravimo *Hadamardove kode*. Če pa dobimo iz Hadamardove matrike reda 2 Hadamardovo matriko s tenzorskim produktom, potem kodo imenujemo tudi *Reed-Mullerjeva koda prve vrste*.

Proces uporabe kod bomo preverili na aplikaciji iz realnega sveta. Mariner 9 je bila vesoljska sonda iz leta 1971, katere namen je bil leteti do Marsa in pošiljati črno-bele slike na Zemljo (prva sonda, ki je letela v orbiti drugega planeta). Čez vsako sliko je bila nameščena podrobna mreža in za vsak kvadratek v tej mreži (piksel) je bila izmerjena sivina na skali od 0 do 63 (tj. 2^6 možnosti oziroma 6 bitov informacije). Ta števila, zapisana v binarni obliki, so bili podatki, ki so bili poslani na Zemljo (bolj natančno v laboratorij kalifornijskega instituta za tehnologijo v Pasadeni). Ob prihodu je bil signal šibek in je moral biti ojačan. Motnje iz vesolja ter termične motnje iz ojačevalca povzročijo, da včasih poslano enico preberemo kot ničlo (in obratno ničlo kot enico). Že če je verjetnost napake le 5 %, bo ob predpostavki, da ne bomo uporabili nobenih kod, kvaliteta slik izredno slaba (le 26 % pravilna, velja namreč $1-0,95^6 \approx 0,26$). Torej ni dvoma, da moramo uporabiti kode za odpravljanje napak. Vprašamo pa se lahko tudi, katere kode naj uporabimo. Vsaka koda bo povečala velikost podatkov, ki jih moramo poslati.

Mariner 9 je bilo majhno vozilo, ki ni moglo nositi velikega oddajnika, tako da je moral biti signal usmerjen, vendar je na velikih razdaljah signal težko uspešno usmeriti. Poleg tega pa je bila omejena tudi maksimalna velikost podatkov, ki se jih da poslati v danem trenutku (ko je oddajnik naravnan). Le-ta je bila enaka petkratni velikosti originalnih podatkov. Ker so bili podatki sestavljeni iz šestih bitov, so bile lahko kodne besede sestavljene iz tridesetih bitov.

Kode s ponavljanjem smo predstavili že v [5] (če vsak simbol ponovimo m-krat, lahko z večinskim pravilom odkodiramo pravilno, če je pri prenosu prišlo do manj kot $m/2$ napak). Koda s petimi ponovitvami je bila ena izmed

možnosti, saj jo je enostavno implementirati, vendar pa le-ta lahko popravi le 2 napaki. Hadamardova koda, ki je zasnovana na Hadamardovi matriki reda 32, pa je lahko popravila 7 napak, tako da je bila vredna nekoliko bolj zapletene implementacije. Z uporabo te kode je verjetnost napake na sliki zreducirana na samo 0,01 % (v primeru kode s petimi ponovitvami pa bi bila verjetnost približno 1 %).

Predpostavimo, da je verjetnost, da se spremeni en bit, enaka $p = 0,01$. Potem je verjetnost, da je sprejeti piksel napačen $1 - 0,99^6 \approx 0,06$. Verjetnost v primeru kode s ponavljanjem pa je:

$$1 - \left[\binom{5}{0}(1-p)^5 + \binom{5}{1}p(1-p)^4 + \binom{5}{2}p^2(1-p)^3\right]^6$$

in v našem primeru verjetnost $6 \cdot 10^{-5}$, da bo prejeti piksel napačen. V primeru Hadamardove kode pa imamo:

$$1 - \sum_{i=0}^{7}\binom{32}{i}p^i(1-p)^{32-i} = \sum_{i=8}^{32}\binom{32}{i}p^i(1-p)^{32-i},$$

kar nam da bistveno boljšo verjetnost $8 \cdot 10^{-10}$. Reed-Mullerjeva koda sicer res potrebuje približno enako količino dodane informacije, je pa zato skoraj 70 000-krat zanesljivejša.

Sedaj pa preusmerimo našo pozornost k problemu kodiranja in odkodiranja z uporabo Hadamardove kode. Na prvi pogled kodiranje ne bi smelo povzročati težav. Imamo namreč 64 različnih podatkov in 64 kodnih besed, kar pomeni, da bi morala delovati že poljubna bijekcija. Težava pa je v tem, da je Mariner 9 majhna naprava, ta način pa bi zahteval hranjenje vseh 64 32-bitnih kodnih besed. Veliko bolj ekonomično v smislu prostora in lažje je bilo narediti hardware, ki dejansko izračuna kodno besedo, namesto da jo prebere iz pomnilnika.

S pravilno izbiro Hadamardove matrike postane Hadamardova koda linearna (o linearnih kodah si lahko preberete več v [8]), tako da je ta izračun v resnici množenje podatkov z generatorsko matriko kode. Prava izbira za Hadamardovo matriko je tista, ki jo dobimo iz tenzorskega produkta Hadamardove matrike reda 2. Z matematično indukcijo lahko preverimo, da je taka koda linearna. Sedaj pa si oglejmo pobliže še problem odkodiranja. Prejeti signal, tj. zaporedje 32-ih ničel in enic, je najprej spremenjen v obliko ± 1 (tako da zamenjamo „0“ z „-1“). Tako dobimo vektor $\boldsymbol{x}$, in če ni bilo napak, potem je $\boldsymbol{x}H^T$, kjer je H originalna Hadamardova matrika, vektor z 31-imi koordinatami enakimi 0 in eno koordinato enako ± 32.

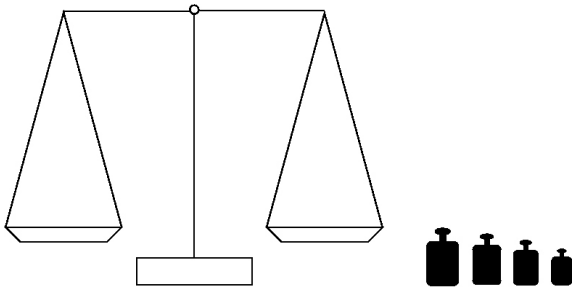
Slika 6. Površina Marsa

Če pa nastanejo napake, potem se ta števila spremenijo. Vendar pa največ 7 napak poveča vrednost z 0 na največ 14, vrednost 32 pa se zmanjša kvečjemu do 18 (v tem primeru prejeta beseda spominja na poslano kodno bolj kot katera koli izmed preostalih 63 kodnih besed). Torej nam mesto, na katerem se pojavi po absolutni vrednosti največja vrednost vektorja $\boldsymbol{x}H^T$, pove, katera vrstica matrike H (oziroma $-H$, če je originalna vrednost negativna) je bila poslana. Ker je bil originalni algoritem za odkodiranje signalov sonde Mariner 9 počasen (potreboval je 322 množenj in ustrezna seštevanja za vsako kodno besedo), so na Zemlji uporabili številne računske trike in tako zreducirali računanje na vsega eno tretjino.

Hadamardove matrike v kemiji in statistiki

Hadamardove matrike se uporabljajo tudi za izboljšavo natančnosti pri merjenjih podobnih objektov. Problem kemijskega ravnotežja, pri katerem lahko objekte postavimo na katero koli stran tehtnice, glej sliko 7, je skoraj popolnoma rešen s Hadamardovimi načrti, ki jih lahko dobimo iz Hadamardovih matrik [9].

Brez tega postopka bi morali v nekaterih primerih tehtati tudi do $\binom{n}{n/2}$-krat oziroma $\binom{n}{(n+1)/2}$-krat, pri čemer je n število objektov. Npr. stolpce lahko interpretiramo kot uteži na inštrumentu z dvema skalama, vrstice pa kot objekte, ki jih želimo tehtati. Med vsakim izmed n tehtanj uporabimo vseh n objektov. Ko merimo j, postavimo i-ti objekt na levo stran, če je $H_{ij} = 1$, sicer pa na desno. Ta način merjenja bo natančnejši (manjša varianca/sprememba), kot če bi merili vsak objekt posebej.



Slika 7

Kompleksne Hadamardove matrike

Če namesto $H_{ij} = \pm 1$ zahtevamo pri definiciji Hadamardove matrike raje $|H_{ij}| = 1$, transponiranje pa pomeni hermitsko transponiranje, dobimo kompleksne Hadamardove matrike. Podobno kot pri običajnih Hadamardovih matrikah imamo v bistvu natanko eno kompleksno Hadamardovo matriko reda 3 (t. i. Butson-Hadamardovo matriko) in jo sestavimo s primitivnim kubičnim korenom števila 3, ki ga označimo z w:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{pmatrix}.$$

Kompleksne Hadamardove matrike obstajajo za vsako naravno število n (medtem ko pri realnih ni tako). Npr. Fourierove matrike $(F_n)_{jk} := e^{2\pi i(j-1)(k-1)/n}$, za $j, k = 1, 2, \ldots, n$, pripadajo temu razredu.

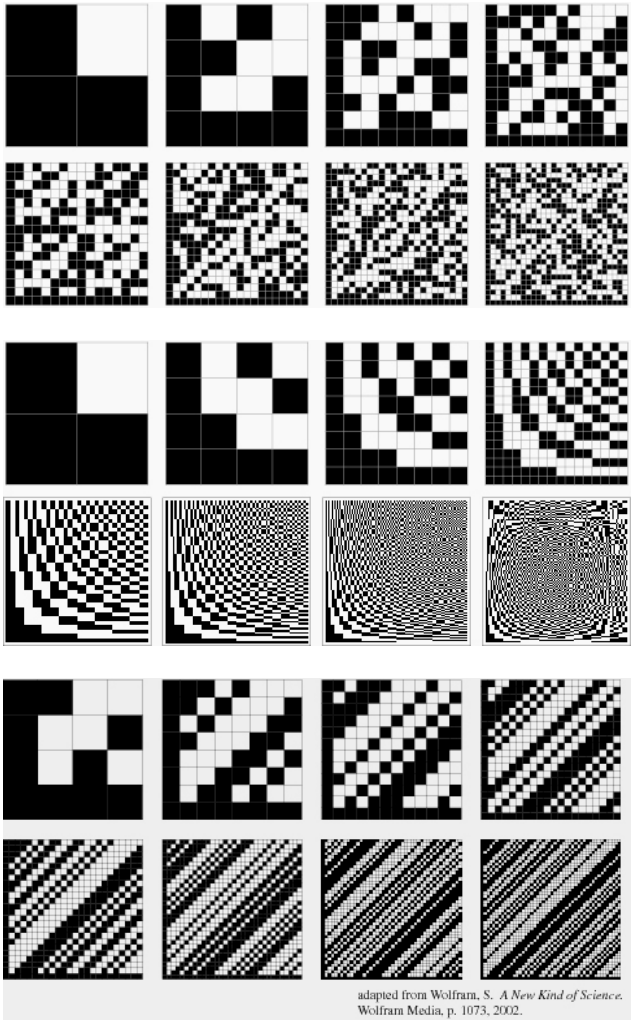
Za konec pa postavimo bralcem še nekaj zanimivih nalog:

Naloga 1. Za $n = 2^m$ in $1 \leq i \leq m$ definiramo matriko $M_n^{(i)}$ z $M_n^{(i)} := I_{2^{m-i}} \otimes H_2 \otimes I_{2^{i-1}}$. Dokaži, da je produkt $M_n^{(1)} M_n^{(2)} \ldots M_n^{(m)}$ enak Hadamardovi matriki H_n, ki smo jo skonstruirali s tenzorskim produktom.

Naloga 2. V primeru Reed-Mulerjeve kode prve vrste je sprejeta beseda $\boldsymbol{x}$ odkodirana tako, da izračunamo $\boldsymbol{x} H_n^T$. Če ni prišlo do prevelikega števila napak, potem bodo vse vrednosti vseh koordinat tega produkta blizu 0, z izjemo tiste, katere absolutna vrednost bo blizu n. Tako bomo vedeli, kateri vektor je bil v resnici poslan. Množenje s ± 1 imenujemo operacija. Primerjaj število operacij, ki so potrebne za odkodiranje, če

(a) uporabimo matriko H_n, (b) uporabimo reprezentacijo iz prve naloge.

Drugi primer je poznan kot *hitra Fourierova transformacija*.



Slika 8. Še nekaj predstavitev Hadamardovih matrik iz različnih rekurzivnih konstrukcij (nakljućne, Walshove in Paleyjeve Hadamardove matrike). Več o Hadamardovih matrikah lahko najdete v priročniku [2] (v katerem je 5. del posvečen prav Hadamardovim matrikam) ter na Wikipediji in Wolframovem raziskovalnem centru.

Naloga 3. Naj bo M $(m \times n)$-razsežna binarna matrika, v kateri je Hammingova razdalja med poljubnima dvema različnima vrsticama vsaj d (če postavimo Hadamardovo matriko H nad matriko $-H$ in zamenjamo simbole

± 1 v ničle in enice, dobimo primer z $m = 2n$ in $d = n/2$). Preštej število urejenih trojic (i, j, k), za katere sta i in j (indeksa) različni vrstici, k pa je tak stolpec, da je $M(i, k) \neq M(j, k)$, na dva načina – tako da nam en da neenakost, ki vsebuje d, drugi pa stolpčne vsote matrike M. Če privzamemo $2d > n$, potem dokaži oceno

$$m \leq \frac{2d}{2d - n},$$

ki ji pravimo v teoriji kodiranja tudi *Plotkinova ocena*. Kateri pogoj nam zagotovi enakost?

Naloga 4. V prejšnji nalogi privzemi $d = n/2$ in dokaži, da je potem $m \leq 2n$ ter da enakost implicira eksistenco Hadamardove matrike reda n.

LITERATURA

[1] V. Belevitch, *Theory of 2n-terminal networks with applications to conference telephony*, Electrical Communication **27** (1950), str. 231–244.

[2] C. J. Colbourn in J. H. Dinitz, *Handbook of Combinatorial designs*, druga izdaja, Chapman&Hall/CRC, 2007.

[3] D. Ž. Djoković, *Hadamard matrics of order 764 exist*, Combinatorica **28** (2008), str. 487–489.

[4] P. de la Harpe, *Spin models for link polynomials, strongly regular graphs and Jaeger's Higman-Sims model*, Pacific J. Math. **162** (1994) 1, str. 57–96.

[5] A. Jurišić, *Napake niso večne – Presek, zgoščenke, planeti in kode*, Presek **30** (2002/2003) 6, str. 361–366.

[6] A. Jurišić in A. Žitnik, *Reed-Solomonove kode*, Obzornik mat. fiz. **51** (2004) 5, str. 129–143.

[7] H. Kharaghani, *A Hadamard matrix of order 428*, J. Combin. Des. **13** (2005), str. 435–440.

[8] S. Klavžar, *O teoriji kodiranja, linearnih kodah in slikah z Marsa*, Obzornik mat. fiz. **45** (1998) 4, str. 97–106.

[9] A. M. Mood, *On Hotelling's Weighing Problem*, Ann. Math. Statist. **17** (1946), str. 432–446.

[10] K. Nomura, *Spin models constructed from Hadamard matrices*, J. Combin. Th. Ser. A **68** (1994), str. 251–261.

[11] R. E. A. C. Paley, *On orthogonal matrices*, J. Math. Phys. **12** (1933), str. 311–320.

[12] J. Williamson, *Hadamard's determinant theorem and the sum of 4 squares*, Duke Math. J. **11** (1944), str. 65–81.