HADAMARDOVE MATRIKE IN HADAMARDOVE KODE

Vincenc Petruna
Gimnazija Črnomelj
Kidričeva 18a, Črnomelj

21. junij 2007

Povzetek

Sestavek govori o kodah za odpravo napak pri prenosu informacij, ki nastanejo zaradi šuma v informacijskem kanalu. Posebej se ukvarja s Hadamardovimi matrikami in njim pripadajočimi Hadamardovimi kodami.

Povzetek

Article describes about error detecting codes on noisy communication channels. Hadamard matrices and correndsponding Hadamard codes are particulary discussed.

1 Uvod

Pri prenosu informacij najprej priprava (Koder) informacijo zakodira tako, da v binarni obliki (0 in 1) potuje po informacijske kanalu. Na koncu kanala pa druga priprava (Dekoder) pretvori prejeto informacijo iz binarne v razumljivo obliko.

V praksi nastopijo v informacijskem kanalu motnje, ki vplivajo na to, da se biti pokazijo (0 v 1 in obratno).

Govora bo o kodah, ki napake odkrijejo in popravijo.

Ena od preprostih možnosti za odkrivanje napak je parnostni bit. To je bit, ki ga dodamo sporočilu, in sicer 1, če je v sporocilu liho število enk, sicer pa 0. To preverjanje funkcionira, če je v sporočilu zelo malo napak, odpove pa že, če sta se spremenila 2 bita. Po zaznavi napake te-te ne znamo odpraviti.

Druge možnosti so še večkratno pošiljanje sporočila ter uporaba *kod, ki odkrivajo in popravljajo napake*.

2 Kode za odkrivanje in popravljanje napak

Najprej definiramo pojem koda:

Definicija: Naj bo V^n množica vseh zaporedij ničel in enic dolžine n. *Binarna koda* je podmnožica v V^n. Elementi kode so *kodne besede.*

Primeri:

1. C_1=00,01,10,11 $n = 2 \quad \delta = 1$
2. C_2=000,110,011,101 $n = 3 \quad \delta = 2$
3. C_3=000000,111000,001110,110011 $n = 6 \quad \delta = 3$

Problem teorije kodiranja je poiskati dobre kode. Dobre kode so tiste, katerih kodne besede so čim kraše, pa vendar tako izbrane, da odpravijo čimveč napak. Če pogledamo prejšnje primere, vidimo da je:

1. C_1 je slaba koda, ker ne opazi niti ne odpravi nobene napake.
2. C_2 opazi napako, vendar ne vemo, kako jo odpraviti. Denimo, da se je pokvaril en bit v kodni besedi 011. Nastalo je 010 ali 100 ali 111. Vendar npr. 010 lahko nastane tako, da se pokvari 1 bit v kodnih besedah 000, 110 ali 011, tako da ne moremo odpraviti napake.
3. C_3 pa odpravi eno napako. Če se denimo pokvari kodna beseda 001110, dobimo 101110, 011110, 000110, 001010, 001100, 001111. Vendar katerakoli od teh besed razlikuje od 001110 samo za en bit, od ostalih kodnih besed pa za 2 bita ali več. Besedo popravimo po *principu bližnjega soseda,* ki pravi: Če se prejeta beseda od kodne besede u razlikuje v enem bitu, od ostalih kodnih besed pa za dva bita in več, je največja verjetnost, da je bila poslana kodne beseda u.

Definicija: *Hammingova razdalja* $\partial(u, v)$ med besedama u in v je število mest, v katerih se besedi u in v razlikujeta.

Pokažemo lahko, da ima Hammingova razdalja vse lastnosti razdalje:

$$\partial(u, u) = 0$$
$$\partial(u, v) = \partial(v, u)$$
$$\partial(u, v) \leq \partial(u, v) + \partial(u, v)$$

Princip bližnjega soseda lahko potem z uporabo Hammingove razdalje povemo takole:
Naj bo u prejeta beseda. Če velja

$$\partial(u,v) < \partial(u,w) \quad za \forall w \neq v, \quad (v, w \epsilon \mathcal{C}, 0$$

tedaj je najbolj verjetno, da je bila v poslana beseda.

Definicija: *Razdalja kode $\mathcal{C}$ je minimalna razdalja med vsemi pari kodnih besed*

$$\delta = min_{\substack{u,v \epsilon \mathcal{C} \\ u \neq v}} \{\partial(u,v)\}.$$

Brez dikaza navajam naslednji izrek:

Izrek: Naj bo $\mathcal{C}$ koda, ki ima $\delta = 2e+1$. Tedaj Koda $\mathcal{C}$ odpravi (po principu bližnjega soseda) e napak.
Dokaz lahko najdemo v bibliografiji.

3 Hadamardove matrike

Definicija. *Hadamardova matrika* H reda n je taka matrika dimenzije nxn, ki ima za elemente samo števila -1 in 1 ter zanjo velja

$$HH^T = nI.$$

Iz definicije vidimo, da je skalarni produkt poljubnih različnih vrstic matrike H enak 0, poljubnih enakih vrstic pa n. Vrstice matrike H so torej med seboj ortogonalne. Enaka trditev velja za stolpce matrike H.

Če pomnožimo poljubno vrstico ali stolpec Hadamardove matrike z -1, dobimo spet Hadamardovo matriko. To lahko počnemo tolikokrat, da dobimo v prvi vrstici in prvem stolpcu same enke.

Definicija. Hadamardova matrika je *normalizirana*, če ima v prvi vrstici in v prvem stolpcu same enke. Za katera števila n Hadamardove matrike obstajajo? Iskanje nam olajša naslednji izrek:

Izrek. *Če Hadamardova matrika H reda n obstaja, potem je n 1, 2 ali mnogokratnik števila 4.*

n=1;

$$H_1 = \| \, 1 \, \|$$

n=2;

$$H_2 = \begin{Vmatrix} 1 & 1 \\ 1 & -1 \end{Vmatrix}]$$

n=4;

$$H_4 = \begin{Vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{Vmatrix}$$

n=8;

$$H_8 = \begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{Vmatrix}$$

Slika 1: Hadamardove matrike reda 1, 2, 4 in 8.

Dokaz: Brez škode za splošnost lahko predpostavimo, da je H normalizirana. Naj bo $n \geq 3$, prve tri vrstice matrike H pa naj bodo sestavljene takole:

$$\begin{array}{cccc} 1\ 1\cdots\ 1 & 1\ 1\cdots\ 1 & 1\ 1\cdots\ 1 & 1\ 1\cdots\ 1 \\ 1\ 1\cdots\ 1 & 1\ 1\cdots\ 1 & -1-1\cdots-1 & -1-1\cdots-1 \\ \underbrace{1\ 1\cdots\ 1}_{\text{i}} & \underbrace{-1-1\cdots-1}_{\text{j}} & \underbrace{1\ 1\cdots\ 1}_{\text{k}} & \underbrace{-1-1\cdots-1}_{\text{l}} \end{array}$$

Pri tem je $i + j + k + l = n$. Ker pa so vrstice med seboj ortogonalne, dobimo tudi

produkt 1. in 2. vrstice i+j-k-l=0
produkt 1. in 3. vrstice i-j+k-l=0
produkt 2. in 3. vrstice i-j-k+l=0

Rešitev tega sistema enačb je $i = j = k = l$, torej n=4i, kar je bilo treba dokazati.

Domnevamo, da Hadamardove matrike obstajajo za vsak n, ki je mnogokratnik števila 4. Vendar ta domneva dosedaj še ni dokazana. Dosedaj je znanih veliko število konstrukčij Hadamardovih matrik. Najmanjši n, za katerega do 1977 Hadamardova matrika še ni bila znana, je 268.

4 Sylvestrova konstrukcija

V nadaljevanju bomo spoznali dve konstrukciji Hadamardovih matrik, ki sta v teoriji kodiranja pomembni.

1.konstrukcija *Če je H_n Hadamardova matrika reda n, potem je*

$$H_{2n} = \begin{Vmatrix} H_n & H_n \\ H_n & -H_n \end{Vmatrix} \textit{ Hadamardova matrika reda 2n.}$$

Dokaz: Matrika H_{2n} je simetrična, njene vrstice so ortogonalne, ker so ortogonalne vrstice v H_n. Ker je skalarni produkt vrstice z isto vrstico v H_n enak n, je v H_{2n} enak 2n. Torej velja

$$H_{2n} H_{2n}^T = 2nI.$$

Če pričnemo konstrukcijo s $H_1 = \|1\|$, dobimo H_2, H_4, H_8 (prikazane na Sliki 1) in tako naprej Hadamardove matrike reda, ki je potenca števila 2. Take Hadamardove matrike imenujemo *Sylvestrove matrike*.

5 Paleyeva konstrukcija

Za naslednjo konstrukcijo pa potrebujemo nekaj znanja iz teorije števil o kvadratnih ostankih.

5.1 Kvadratni ostanki

Definicija: Naj bo p liho praštevilo. *Kvadratni ostanki po modulu p* (kratko ostanki po modulu p) so neničelni kvadrati 1^2, 2^2, $3^2 \ldots$.

Ostanke po modulu p poiščemo tako, da poiščemo kvadrate števil od 1 do p-1. Če pa upoštevamo, da je

$$(p-a)^2 \equiv (-a)^2 \equiv a^2 (mod\ p)$$

, vidimo, da je dovolj že, če izračunamo ostanke kvadratov do

$$p-1$$

$$1^2, 2^2, \ldots, (\frac{p-1}{2})^2 \qquad (mod\ p).$$

Lahko se prepričamo, da so ti ostanki vsi med seboj različni. Iz kongruence $i^2 \equiv j^2 (mod\ p)$, pri čemer sta $1 \leq i, j \leq \frac{1}{2}(p-1)$, namreč lahko sklepamo, da p deli $(i-j)(i+j)$. To pa je mogoče le, če je $i = j$. Obstaja torej $\frac{1}{2}(p-1)$ kvadratnih ostankov po modulu p. Preostalih $\frac{1}{2}(p-1)$ števil po modulu p imenujemo neostanki. Število 0 ni ne ostanek ne neostanek.

Primer: Če je p=11, so kvadratni ostanki po modulu 11 naslednja števila

$$1^2 = 1, \qquad 2^2 = 4, \qquad 3^2 = 9, \qquad 4^2 = 16 \equiv 5\ in \qquad 5^2 = 25 \equiv 3. (mod\ 110$$

Preostala števila 2,6,7,8 in 10 pa so neostanki.

5.2 Lastnosti kvadratnih neostankov

Sedaj lahko naštejemo nekaj lastnosti kvadratnih ostankov.

Izrek: *Produkt dveh kvadratnih ostankov ali dveh kvadratnih neostankov je kvadratni ostanek, produkt kvadratnega ostanka in kvadratnega neostanka pa kvadratni neostanek.*

Izrek: Če je p oblike $4k+1$, je -1 kvadratni ostanek po modulu p. Če pa je p oblike $4k+3$, je -1 neostanek po modulu p. Dokaza teh izrekov najdemo npr. v Graselli, Teorija števil.

Definicija: Naj bo p liho praševilo. Funkcija χ, imenovana *Legendrov simbol*, je nad celimi števili definirana takole:

$$\chi(i) = \begin{cases} 0, & \text{če je i mnogokratnik p,} \\ 1, & \text{če je i mod p kvadratni ostanek po modulu p,} \\ -1, & \text{če je i mod p neostanek po modulu p.} \end{cases}$$

Izrek: Za vsak $c \neq 0$ velja

$$\sum_{b=0}^{p-1} \chi(b)\chi(b+c) = -1.$$

Dokaz: Iz prejšnjega izreka sledi, da je

$$\chi(xy) = \chi(x)\chi(y)$$

za poljuben par x,y, za katerega velja $0 \leq x, y \leq p-1$. Člen z $b = 0$ ne prispeva k vsoti. Predpostavimo torej da $b \neq 0$ in naj bo $z \equiv \frac{b+c}{b}(mod\ p)$. Za vsak b obstaja enoličen $z, 0 \leq z \leq p-1$. Ko teče b od 0 do p-1, zavzame z vrednosti $0, 2, \cdot, p-1$, samo 1 ne. Potem pa velja

$$\sum_{b=0}^{p-1} \chi(b)\chi(b+c) = \sum_{b=1}^{p-1} \chi(b)\chi(bz) = \sum_{b=1}^{p-1} \chi(b)^2\chi(z) = \sum_{\substack{z=0 \\ z\neq 1}}^{p-1} \chi(z) = 0 - \chi(1) = -1,$$

kar je bilo treba dokazati.
Opomba: Podobno velja, če p nadomestimo s poljubno potenco lihega praštevila p^m, ťevila $0, 1, \cdots, p-1$ pa z elementi končnega obsega $GF(p^m)$. Kvadratični ostanki so definirani kot neničelni kvadrati v tem obsegu.

6 Paleyeva konstrukcija Hadamardove matrike

Ta konstrukcija nam da Hadamardovo matriko poljubnega reda n=p+1, ki je mnogokratnik števila 4 (ali reda $n = p^m + 1$, če uporabljamo kvadratične ostanke iz $GF(p^m)$).

Najprej konstruiramo *Jakobsthalovo matriko.* $Q = (q_{ij})$. To je matrika reda pXp, vrstice in stolpci so označeni $0, 1, \ldots, p-1$, $q_{ij} = \chi(j-i)$. Za p je 7 ima matrika Q naslednje elemente:

$$Q = \begin{Vmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 0 \end{Vmatrix}$$

Slika 2: Jakobsthalova matrika reda reda 7.

Ker je p oblike 4k-1, je $q_{ij} = \chi(i-j) = \chi(-1)\chi(j-i) = q_{ji}$ in matrika je poševno simetrična. Zato je $Q^T = -Q$.

Izrek: *Naj bo J matrika istega reda kot Q, za elemente pa naj ima same enice. Potem je* $QQ^T = pI - J$ *in* $QJ = JQ = 0$.

Dokaz: Naj bo P=$(p)_{ij} = QQ^T$. Potem velja

$$p_{ii} = \sum_{k=0}^{p-1} q_{ik}^2 = p - 1.$$

Upoštevali smo, da je v vsaki vrstici p-1 elementov, enakih 1 ali -1. Po prejšnjem izreku pa je za $i \neq j$

$$p_{ij} = \sum_{k=0}^{p-1} q_{ik}q_{jk} = \sum_{k=0}^{p-1} \chi(k-i)\chi(k-j) = -1.$$

Ker ima vsaka vrstica matrike Q $\frac{1}{2}(p-1)$ enk in ravno toliko -1, je tudi $QJ = JQ = 0$.

Hadamardovo matriko reda p+1 tvorimo takole:

$$H = \begin{Vmatrix} 1 & \mathbf{1} \\ \mathbf{1^T} & Q - I \end{Vmatrix}$$

Pri tem je $\mathbf{1}$ vektor z p enkami. Da je matrika H res Hadamardova, uvidimo takole:

$$HH^T = \begin{Vmatrix} 1 & \mathbf{1} \\ \mathbf{1^T} & Q - I \end{Vmatrix} \begin{Vmatrix} 1 & \mathbf{1} \\ \mathbf{1^T} & Q^T - I \end{Vmatrix} = \begin{Vmatrix} p+1 & 0 \\ 0 & J + (Q-I)(Q^T - I) \end{Vmatrix}$$

Toda po prejšnjem izreku je

$$J + (Q - I)(Q^T - I) = J + pI - J - Q - Q^T + I = (p+1)I.$$

Torej je $HH^T = (p+1)I_{p+1}$. Ta konsrukcija Hadamardovih matrik se imenuje Paleyeva konstrukcija. Definicija:Hadamardovi matriki sta *ekvivalentni*, če lahko dobimo eno iz druge s permutacijo vrstic in stolpcev ter množenjem vrstic in stolpcev z -1.

Relacija razdeli Hadamardove matrike reda n v ekvivalenčne razrede. Za matrike reda 1, 2, 4 in 8 obstaja en sam ekvivalenčni razred. Pri matrikah reda 16 je 5 razredov, pri 20 trije. Stevilo ekvivalenčnih razredov pri redu 24 je neznano.(1977).

7 Hadamardove kode

Naj bo H_n normalizirana Hadamardova matrika reda n. Če zamenjamo enice z 0, -1 pa z 1, postane H_n *binarna Hadamardova matrika* A_n. Ker so vrstice H_n ortogonalne, se poljubni dve vrstici matrike A_n razlikujeta v n/2 mestih, tako da je Hammingova razdalja med njima $\frac{n}{2}$.

A_n pa nam da 3 *Hadamardove kode*. To so:

1. $\mathcal{A}_n \equiv (n-1, n, \frac{1}{2}n)$ dobimo iz vrstic matrike A_n, kateri smo prej odstranili 1.stolpec. Primer te kode je npr. (7,8,4) koda, ki jo dobimo iz $\mathcal{A}_8$:

$$\mathcal{A}_8 = \left\| \begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \right\|$$

2. $\mathcal{B}_n \equiv (n-1, 2n, \frac{1}{2}n - 1)$ je unija kodnih besed iz $\mathcal{A}_n$ in komplementov teh besed. Primer: $\mathcal{B}_{12}$ je (11,24,5)-koda.

$\mathcal{B}_{12} =$

0	1	2	3	4	5	6	7	8	9	10	
0	0	0	0	0	0	0	0	0	0	0	
1	1	0	1	1	1	0	0	0	1	0	
0	1	1	0	1	1	1	0	0	0	1	
1	0	1	1	0	1	1	1	0	0	0	
0	1	0	1	1	0	1	1	1	0	0	
0	0	1	0	1	1	0	1	1	1	0	
0	0	0	1	0	1	1	0	1	1	1	
1	0	0	0	1	0	1	1	0	1	1	
1	1	0	0	0	1	0	1	1	0	1	
1	1	1	0	0	0	1	0	1	1	0	
0	1	1	1	0	0	0	1	0	1	1	
1	0	1	1	1	0	0	0	1	0	1	
0	0	1	0	0	0	1	1	1	0	1	
1	0	0	1	0	0	0	1	1	1	0	
0	1	0	0	1	0	0	0	1	1	1	
1	0	1	0	0	1	0	0	0	1	1	
1	1	0	1	0	0	1	0	0	0	1	
1	1	1	0	1	0	0	1	0	0	0	
0	1	1	1	0	1	0	0	1	0	0	
0	0	1	1	1	0	1	0	0	1	0	
0	0	0	1	1	1	0	1	0	0	1	
1	0	0	0	1	1	1	0	1	0	0	
0	1	0	0	0	1	1	1	0	1	0	
1	1	1	1	1	1	1	1	1	1	1	height

3. $\mathcal{C}_n \equiv (n, 2n, \frac{1}{2}n)$ je unija vrstic matrike A_n in komplementov teh vrstic.

8 Sklep

Hadamardove kode so primeri nelinearnih kod. Linearne kode imajo mnoge praktične prednosti. Vendar ko želimo dobiti maksimalno število kodnih besed z dano kodno razdaljo, moramo včasih uporabiti nelinearno kodo.

Za primer vzemimo, da želimo kodo dolžine 11, ki odpravlja dve napaki. Najdaljša linearna koda ima 16 kodnih besed. Obstaja pa nelinearna koda, ki ima 24 besed, kar je 50% več. To je Hadamardova koda $\mathcal{B}_{12}$.

Vendar ni vsaka koda, dobljena iz Hadamardovih matrik, nelinearna. Koda, dobljena iz matrik Sylvestrove konstrukcije je linearna za vsak n. Nelinearna je koda, dobljena iz matrik Paleyeve konstrukcije za $n > 8$.

9 Literatura:

1. N.L.Biggs,*Discrete Mathematics*, Clarendon Press, Oxford, 1989.
2. P.J.Cameron, J.H.Van Lint, *Graphs, Codes and Designs*, London Math. Soc. Lecture Notes Ser. 43, Cambridge University Press, Cambridge, 1980.
3. D.G.Hoffman, D.A.Leonard, C.C.Lindner,K.T.Phelps,C.A.Rodger,J.R.Wall, *Coding Theory, the Essentials*, Marcer Dekker, Inc., 1991.
4. J.H.Van Lint, Introduction to Coding Theory, Springer-Verlag, Berlin, 1992.
5. F.J.MaxWilliams,N.J.A.Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam,1977.