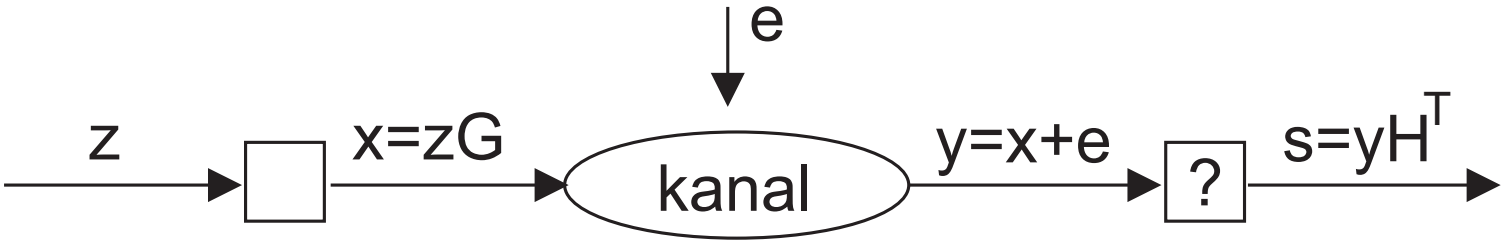
Teorija informacij in sistemov, predavanje 7

Uroš Lotrič

Univerza v Ljubljani,
Fakulteta za računalništvo in informatiko

5.5 Sindrom 1

- Poglejmo, kaj se zgodi, če v kanalu pride do napake:



- $\mathbf{yH^T} = (\mathbf{x}+\mathbf{e})\mathbf{H^T} = \mathbf{eH^T} = \mathbf{s}$ - vektor $\mathbf{s}$ velikosti $1 \times n-k$ je odvisen samo od napake. Imenujemo ga **sindrom**.
- Napako pri prenosu preprosto ugotavljamo tako, da pogledamo, če je $\mathbf{s} = \mathbf{0}$
- $\mathbf{s} = \mathbf{0}$ ne garantira, da pri prenosu ni prišlo do napake!

5.5 Sindrom 2

- Tabela enojnih napak in sindromov za trikotni kod:

e	s
000000	000
000001	001
000010	010
000100	100
001000	011
010000	110
100000	101

s = 111 - dobimo kadar v kanalu pride do dvojne ali trojne napake: (001100), (010001), (100010), (000111). Lahko jih zaznamo, ne moremo pa jih popraviti.

- primer: niz $\mathbf{z} = (110)$, napaka $\mathbf{e} = (001000)$, napako pravilno popravimo.
- primer: niz $\mathbf{z} = (110)$, napaka $\mathbf{e} = (000011)$, sprejemnik po popravljanju misli, da je bil poslan $\mathbf{z} = (111)$.

5.5 Sindrom 3

- Kako in kdaj popravljati? Ne moremo izbirati. Rešuje nas verjetnost
- Ker je verjetnost za napako običajno $p << 1$, je niz s t napakami veliko verjetnejši od niza s $t + 1$

5.6 Standardna tabela 1

- Spomnimo se ponavljalne kode $(0|00)$ in $(1|11)$. Opišimo jo z mehanizmom matrik
- $\mathbf{G} = (1|11), \mathbf{H} = \left(\begin{array}{c|cc} 1 & 1 & 0 \\ 1 & 0 & 1 \end{array}\right)$
- imamo 4 možne sindrome: (00), (01), (10), (11)
- na izhodu lahko dobimo $2^n = 8$ različnih nizov

y	e
000	00
001	01
010	10
011	11
100	11
101	10
110	01
111	00

5.6 Standardna tabela 2

- možne nize na izhodu in njihove sindrome običajno razvrstimo v standardno tabelo

sindrom	popravljalnik	
00	000	111
01	001	110
10	010	101
11	100	011

- v isti vrstici so nizi, ki dajo enak sindrom
- v prvi vrsti so vedno kodne zamenjave, ki imajo sindrom 0
- skrajno levo je vedno niz, ki ima najmanj enic, saj je najbolj verjeten. Imenujemo ga popravljalnik
- ostale nize dobimo tako, da popravljalnik prištevamo h kodnim zamenjavam v prvi vrsti
- Popravljanje je sedaj enostavno: izračunamo sindrom, popravljalnik odštejemo (prištejemo) od prejetega niza
- Ta postopek postane zelo kompleksen, če sta n in $n-k$ velika (velika matrika H in tabela

5.7 Hammingov kod 1

- **Hammingovi kodi** so družina linearnih bločnih kodov, ki lahko popravijo eno napako
- najlažje jih predstavimo z matriko za preverjanje sodosti, v kateri so vsi stolpci neničelni vektorji
- kod z m varnostnimi biti ima kodne zamenjave dolžine $2^m - 1$. Oznaka koda je $H(2^m - 1, 2^m - 1 - m)$
- če stolpce v matriki H interpretiramo kot števila v binarni obliki, nam oznaka stolpca določa položaj napake
- če je sindrom $\mathbf{s} = (s_1, s_2, s_3)$, ga želimo interpretirati kot število, za $m = 3$: $S = 4s_1 + 2s_2 + s_3$.
- stolpci v Hammingovem kodu so lahko poljubno razmetani. Pomembno je le to, da nastopajo vsa števila od 1 do $2^m - 1$
- Hamminov kod je lahko
  - leksikografski (oznake stolcev si sledijo po vrsti, v splošnem ni sistematičen)
  - sistematični (oznale stolpcev so pomešane)

5.7 Hammingov kod 2

- Napake in njihovi sindromi na leksikografskem kodu H(7,4)

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

  pokaži z različnimi vektorji e!!!
- V Hammingovem kodu se za varnostne bite običajno vzamejo tisti stolpci, ki imajo samo eno enico (1, 2, 4, 8, 16, ...).
- V nekaterih primerih lahko varnostne in podatkovne bite postavimo tudi drugače (Luenberger) vendar postopkov ne moremo posplošiti.

5.7 Hammingov kod 3

- Primer za $H(7,4)$: če postavimo $\mathbf{x} = (x_1, x_2, z_1, x_4, z_2, z_3, z_4)$, dobimo iz matrike $\mathbf{H}$ za vsak varnostni bit svojo enačbo:

$$\begin{aligned} x_4 + z_2 + z_3 + z_4 = 0 \quad &\rightarrow \quad x_4 = z_2 + z_3 + z_4 \\ x_2 + z_1 + z_3 + z_4 = 0 \quad &\rightarrow \quad x_2 = z_1 + z_3 + z_4 \\ x_1 + z_1 + z_2 + z_4 = 0 \quad &\rightarrow \quad x_1 = z_1 + z_2 + z_4 \end{aligned}$$

- enačbe opisujejo stolpce varnostnih bitov v matriki $\mathbf{G}$:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

5.7 Hammingov kod 4

- Če vir nima spomina, lahko stolpce v matrikah $\mathbf{H}$ in $\mathbf{G}$ sinhrono premečemo.
- Primer: matriki za sistematični ciklični kod H(7,4)

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \rightarrow$$

$$\mathbf{H}' = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \rightarrow$$

$$\mathbf{G}' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

- Če na matriki $\mathbf{G}'$ naredimo obratne premike kot na matriki $\mathbf{H}$ dobimo matriko $\mathbf{G}$, ki smo jo določili iz enačb.

5.7 Hammingov kod 5

- Dekodiranje leksikografskega Hammingovega koda je preprosto:
  - Izračunamo sindrom $\mathbf{s} = \mathbf{y}\mathbf{H}^{\mathbf{T}}$
  - Če je $\mathbf{s} = \mathbf{0}$, je $\mathbf{x}' = \mathbf{y}$
  - Če $\mathbf{s} \neq \mathbf{0}$, decimalno število S predstavlja mesto napake.
- Za kod, ki ni leksikografski rabimo tabelo povezav med indeksi sindromov in stolpci
- Hammingovi kodi spadajo med **popolne kode** - sfere z radijem 1 okrog kodnih zamenjav ravno zapolnijo ves prostor z 2^n točkami. Taki linearni kodi so še ponavljajoči kodi in Golayevi kodi.

5.8 Ciklični kodi

- Ciklični kod $C(n, k)$ je linearni bločni kod, v katerem vsak krožni premik kodne zamenjave da drugo kodno zamenjavo.
- Primer cikličnega koda sestavljenega iz 4 različnih ciklov kodnih zamenjav:
  (000)
  (001), (010), (100)
  (011), (110), (101)
  (111)
- Zapis cikličnih kodov s polinomi zelo poenostavi njihovo obravnavo
- Polinome bomo zapisovali po padajočih potencah, seštevali pa bomo po $\mod 2$, kot do sedaj
- $\mathbf{x} = (x_{n-1}, \ldots, x_1, x_0) \Leftrightarrow x(p) = x_{n-1}p^{n-1} + \ldots + x_1 p + x_0$
- Primer: $\mathbf{x} = (110101) \Leftrightarrow x(p) = p^5 + p^4 + p^2 + 1$

5.8.1 Zapis s polinomi 1

- Zapis krožnega premika za eno mesto
  - Osnovni vektor: $\mathbf{x} = (x_{n-1}, x_{n-2}, \ldots, x_0) \Leftrightarrow x(p) = x_{n-1}p^{n-1} + x_{n-2}p^{n-2} + \ldots + x_0$
  - **Pozor - oznake indeksov tečejo kontra kot prej!!!**
  - Premik za eno mesto: $\mathbf{x}' = (x_{n-2}, \ldots, x_0, x_{n-1}) \Leftrightarrow x'(p) = x_{n-2}p^{n-2} + \ldots + x_0 p + x_{n-1}$
  - Zveza: $x'(p) = px(p) - x_{n-1}(p^n - 1)$
  - Delamo v $\mod 2$ aritmetiki ($-$ je enakovreden $+$): $x'(p) = px(p) + x_{n-1}(p^n + 1)$
  - V aritmetiki $\mod (p^n + 1)$ sledi: $x'(p) = px(p) \mod (p^n + 1)$
  - **Pozor: aritmetika po** $\mod 2$ **na istih stopnjah polinoma (na bitih) in aritmetika po** $\mod (p^n + 1)$ **na polinomu**
- Krožni premik za i mest:

$$x^i(p) = p^i x(p) \mod (p^n + 1)$$

5.8.2 Generatorski polinom 1

- Vrstice generatorske matrike lahko razumemo kot kodne zamenjave
- Za ciklične kode velja splošno: **generatorski polinom** je stopnje m, kjer je m število varnostnih bitov, in ga označimo kot

$$g(p) = p^m + g_{m-1}p^{m-1} + \ldots + g_1 p + 1$$

- Pokaži za poseben primer: sistematični kod $\mathbf{G} = [\mathbf{I}_k | \mathbf{A}_{k,n-k}]$.

5.8.2 Generatorski polinom 2

- Kako dobimo generatorsko matriko?
- $g(p)$ je kodna zamenjava, enako tudi $pg(p), \ldots, p^{k-1}g(p)$, vse $\mod p^n + 1$
- Torej

$$\mathbf{G} = \begin{pmatrix} 1 & g_{m-1} & \ldots & g_1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & g_{m-1} & \ldots & g_1 & 1 & 0 & \ldots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & \ldots & 0 & 1 & g_{m-1} & \ldots & g_1 & 1 \end{pmatrix}$$

- Sistematični lahko dobimo z linearnimi operacijami nad vrsticami

5.8.2 Generatorski polinom 3

- Polinom $g(p)$ deli polinom $p^n + 1$. Dokaz.
- Velja torej
$$p^n + 1 = g(p)h(p)$$
- Vsak polinom, ki polinom $p^n + 1$ deli brez ostanka, je generatorski polinom.
- Primer: generatorski polinomi za $n = 7$:
  - Faktorji: $1, p + 1, p^3 + p + 1, p^3 + p^2 + 1, p^7 + 1$
  - Polinomi: 1, $p + 1$, $p^3 + p + 1$, $p^3 + p^2 + 1$, $(p + 1)(p^3 + p + 1)$, $(p + 1)(p^3 + p^2 + 1)$, $(p^3 + p + 1)(p^3 + p^2 + 1)$, $p^7 + 1$
- Primer: kakšna kodna zamenjava ustreza $\mathbf{z} = (0101)$, če je $g(p) = p^3 + p^2 + 1$? $\mathbf{x} = (0111001)$ - z matriko in s polinomi!