1 Kode za odkrivanje in odpravljanje napak

1.1 Dobro je vedeti

Koda $\mathcal{C}$ je podmnožica množice $\{0,1\}^n$ elementom katere pravimo *kodne besede*. Za kodni besedi $u, v \in \mathcal{C}$ je *Hammingova razdalja*, $H(u,v)$, definirana kot število istoležnih bitov v katerih se besedi razlikujeta. *Minimalna razdalja* kode $\mathcal{C}$ je $\delta(\mathcal{C}) = \min\{H(u,v); u, v \in \mathcal{C}\}$.

Princip bližnjega soseda: Naj bo $\mathcal{C} \subseteq \{0,1\}^n$ poljubna koda in w prejeta beseda. Če obstaja taka kodna beseda u, da je $H(u,w) < H(v,w)$ za vsak $v \in \mathcal{C}$, $v \neq u$, tedaj w dekodiramo v u. Če je $\delta(\mathcal{C}) \geq 2e+1$, tedaj $\mathcal{C}$ po principu bližnjega soseda odpravlja do e napak.

Linearne kode

Neprazna koda $\mathcal{C}$ je *linearna*, če za vsak $u, v \in \mathcal{C}$ velja, da je $u + v \in \mathcal{C}$.

Linearno kodo opišejo trije parametri: n (dolžina besed), k (dimenzija kode, ki nam pove število kodnih besed, saj velja $|\mathcal{C}| = 2^k$) in δ (minimalna razdalja kode, ki nam pove koliko napak odpravlja koda).

Teža besede $u \in \mathcal{C}$, $\omega(u)$, je števio enic besede u, to je $\omega(u) = H(u, \mathbf{0})$. *Teža kode* $\mathcal{C}$ je $\omega(\mathcal{C}) = \min\{w(u); u \in \mathcal{C}, u \neq \mathbf{0}\}$. Za linearno kodo $\mathcal{C}$ velja: $\delta(\mathcal{C}) = \omega(\mathcal{C})$.

Za linearno kodo $\mathcal{C}$ dolžine n in dimenzije k, ki odpravlja e napak velja: $2^{n-k} \geq 1 + \binom{n}{1} + \ldots + \binom{n}{e}$.

Konstrukcije linearnih kod

Naj bo N binarna matrika. Tedaj je jedro matrike N linearna koda ($ker(N) = \{x; Nx = 0\}$). Matriki N pravimo *preveritvena matrika* kode $ker(N)$.

Naj bo N $r \times n$ preveritvena matrika oblike

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & b_{1,r+1} & \cdots & b_{1,n} \\ 0 & 1 & \cdots & 0 & b_{2,r+1} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & b_{r,r+1} & \cdots & b_{r,n} \end{bmatrix}.$$

Če so vsi stolpci v N neničelni in paroma različni, tedaj je $\mathcal{C} = ker(N)$ $(n, n-r, 3)$ koda in $\mathcal{C}$ odpravlja eno napako. Spoznajmo še postopek, ki v $\mathcal{C}$ odpratvi do eno napako. V ta namen naj bo u poslana in w prejeta beseda.

- Izračunaj Nw;
- Če je $Nw = 0$, potem dekodiraj w v w, torej $u = w$.

- Če $Nw \neq 0$, potem poišči stolpec v N, naj bo to N^i, ki je enak Nw. V tem primeru $u = w + e_i$.
- Sicer je prišlo do več kot ene napake.

Če ima N $2^r - 1$ neničelnih in paroma različnih stolpcev, potem je $Ker(N)$ $(2^{r-1}, 2^r - 1 - r, 3)$ koda, ki ji pravimo *Hammingova koda*. Pri dani dolžini n (in $\delta(\mathcal{C}) = 3$) so Hammingove kode optimalne, kar pomeni, da imejo največ kodnih besed med vsemi kodami, ki odpravljajo eno napako.

Ciklične kode

Koda $\mathcal{C}$ je *ciklična*, če je linearna in iz $a = a_0 a_1 \ldots a_{n-1} \in \mathcal{C}$ sledi $\hat{a} = a_{n-1} a_0 \ldots a_{n-2} \in \mathcal{C}$. Z $V^n[x]$ označimo kolobar polinomov po modulu $x^n - 1$ s koeficienti v $\mathbb{Z}_2$. Vsaki kodni besedi $a = a_0 \ldots a_{n-1}$ ciklične kode $\mathcal{C}$ priredimo polinom $a(x) = a_0 + a_1 x + \ldots a_{n-1} x^{n-1} \in V^n[x]$. Potem je $a(x) + b(x)$ polinom generiran iz kode $a + b$ in $xa(x)$ polinom generiran iz kode $\hat{a}$.

Naj bo $f(x)$ poljuben polinom v $\mathbb{Z}_2[x]$ s stopnjo manj od n. Potem z $\langle f(x) \rangle$ označujemo ideal generiran s $f(x)$, to je $\langle f(x) \rangle = \{p(x) f(x) \pmod{x^n - 1}\}$.

Koda v V^n je ciklična natanko tedaj, ko ustreza idealu v $V^n[x]$.

Naj bo $\mathcal{C}$ ciklična koda (ideal) v $V^n[x]$. Potem obstaja polinom $g(x) \in \mathcal{C}$, da je $\mathcal{C} = \langle g(x) \rangle$. Polinom $g(x)$ z najmanjšo stopnjo za katerega je $\mathcal{C} = \langle g(x) \rangle$ imenujemo *kanonični generator* kode $\mathcal{C}$.

Kanonični generator $g(x)$ ciklične kode $\mathcal{C}$ v $V^n[x]$ je delitelj polinoma $x^n - 1$ v $\mathbb{Z}_2[x]$. Naj bo $g(x) = g_0 + g_1 x + \ldots + g_{n-k} x^{n-k}$ kanonični generator in naj bo $h(x) = h_0 + h_1 x + \ldots + h_k x^k \in V^n[x]$ tak, da velja $g(x)h(x) = x^n - 1$ v $\mathbb{Z}_2[x]$. Naj bo $h = h_k h_{k-1} \ldots h_0 \underbrace{0 \ldots 0}_{n-k-1}$ in naj bo H matrika z vrsticami h in $n - k - 1$ cikličnimi premiki od h. Potem je H preveritvena matrika ciklične kode $\mathcal{C} = \langle g(x) \rangle$ in dimenzija $\mathcal{C}$ je enaka k.

1.2 Naloge

1. Za kodi $\mathcal{C}_1$ in $\mathcal{C}_2$ določi minimalno razdaljo ter zapiši koliko napak odkrije oz. popravi.

   (a) $\mathcal{C}_1 = \{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$

   (b) $\mathcal{C}_2 = \{000000, 101010, 010101\}$.

2. Ali lahko katero kodo iz naloge 1 razširimo tako, da dodamo eno kodno besedo in ne spremenimo minimalne razdalje?

3. Konstruiraj kodo $\mathcal{C} \subseteq V^6$, ki kodira 5 sporočil in odpravi eno napako.

4. Naj bo $\mathcal{C}$ koda (ne nujno linearna) dolžine 8, ki popravlja dve napaki. Dokaži, da je $|\mathcal{C}| \leq 6$.

5. Naj bo $\mathcal{C}$ linearna koda in $u, v \in C$ poljubni kodni besedi. Dokaži, da je $\omega(u+v)$ sodo število natanko tedaj, ko sta u in v bodisi obe sodi bodisi obe lihi.

6. Naj bo $\mathcal{C}$ linearna koda. Dokaži, da je podmnožica X od $\mathcal{C}$, ki vsebuje vse sode besede iz $\mathcal{C}$, linearna koda.

7. Naj bo $\mathcal{C}$ linearna koda dimenzije k, $X = \{C \in \mathcal{C};\ \omega(C) \text{ je sodo}\}$. Dokaži, da je $|X| = 2^k$ ali $|X| = 2^{k-1}$.

8. Poišči kodne besede kode določene z nazorno matriko:
$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

9. Poišči parametre n, k, δ in kodne besede kode določene z nazorno matriko:
$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

10. Radi bi poslali 128 sporočil, kjer bo vsako sporočilo predstavljeno z binarno kodo dolžine 11. Kako bi konstruirali takšno kodo? Ali je možno konstruirati takšno kodo, ki ima $\delta \geq 3$?

11. Naj bo $\mathcal{C}$ linearna koda določena z nazorno matriko:
$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$
Če je prejeta beseda 110110 in je storjena samo ena napaka, katera beseda je bila poslana?

12. Naj bo $\mathcal{C}$ linearna koda dolžine n. Kodo $\mathcal{C}'$ dolžine $n+1$ konstruiramo na naslednji način: $x = x_1 \dots x_n \in \mathcal{C} \Rightarrow x_1 \dots x_n x_{n+1} \in \mathcal{C}'$, kjer je
$$x_{n+1} = \begin{cases} 0 & \omega(x) \text{ je sodo} \\ 1 & \omega(x) \text{ je liho.} \end{cases}$$
Dokaži, da je tudi $\mathcal{C}'$ linerana koda.

13. Naj bosta $C_1, C_2 \subseteq V^n$ dve kodi dolžine n z $|C_1| = m_1$, $|C_2| = m_2$, $\delta(C_1) = d_1$ in $\delta(C_2) = d_2$. Koda $C_3 = C_1 * C_2$ je definirana kot $C_3 = \{u_1 \dots u_n u_1{+}v_1 \dots u_n{+}v_n; u = u_1 \dots u_n \in C_1, v = v_1 \dots v_n \in C_2\}$.

    (a) Izračunaj število kodnih besed kode C_3.

    (b) Dokaži, da je $\delta(C_3) = \min\{2d_1, d_2\}$.

    (c) Naj bosta kodi C_1 in C_2 linearni. Ali je koda C_3 linearna?

14. Katere izmed naslednjih kod so ciklične?

    (a) $\{000, 100, 010, 001\}$

    (b) $\{000, 111\}$

    (c) $\{0000, 1010, 0101, 1111\}$.

15. Zapiši kodne besede ciklične kode, ki ustreza idealu generiranim z $< 1 + x + x^2 >$ v $V^3[X]$. Poišči še nazorno matriko te kode.

16. S pomočjo faktorizacije polinoma $x^5 - 1$ v $\mathbb{Z}_2[X]$ določi vse ciklične kode dolžine 5.

17. Naj bo C ciklična koda, ki vsebuje besedo z liho težo. Dokaži, da C vsebuje besedo samih enic.