

Informacija in kodi

UN2-1-AV 2021/2022

Komunikacijski kanali II

Simon Dobrišek

15. februar 2022

Teme predavanja

Kodirnik in dekodirnik diskretnega komunikacijskega kanala

Kod kanala

Dekodiranje koda kanala

Zasnova dekodiranja z odkrivanjem napak

Zasnova dekodiranja s popravljanjem napak

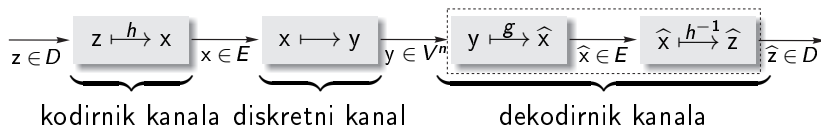
Funkcije odločanja

Optimalna dolžina kodnih zamenjav

Shannonova izreka o varnem kodiranju

Kodirnik in dekodirnik diskretnega komunikacijskega kanala

Obravnavali bomo modeliranje komunikacijskega kanala, ki ga sestavljajo kodirnik kanala, diskretni kanal in dekodirnik kanala.



Naloga kodirnika in dekodirnika kanala je, da naredita prevajanje informacije po kanalu odporno na motnje (šume).

Kodirnik in dekodirnik diskretnega komunikacijskega kanala

Kodirnik kanala obdeluje vhodne nize k znakov iz abecede koda vira $B = \{z_1, z_2, \dots, z_b\}$.

Vhodnemu nizu znakov pravimo *informacijski blok* in ga označimo z z .

Število vseh različnih blokov označimo z M , njihovo množico pa z D , pri čemer velja $M \leq b^k$.

Kodirnik kanala bijektivno preslika vsak informacijski blok z dolžine k v njegovo kodno zamenjavo x dolžine n , kjer je $n > k$.

Kodirnik in dekodirnik diskretnega komunikacijskega kanala

Kodna zamenjava x , pravimo ji tudi *vhodni vektor*, je sestavljena iz znakov abecede U .

Množico vseh kodnih zamenjav, teh je M , označimo z E .

Med prenosom po kanalu z motnjami se vhodni vektorji x naključno preslikajo v *izhodne vektorje* y , ki so sestavljeni iz znakov abecede V .

Iz sprejetega izhodnega vektorja y dekodirnik kanala oceni odposlano kodno zamenjavo $\hat{x} \in E$, ki jo nato bijektivno preslika v oceno odposlanega informacijskega bloka $\hat{z} \in D$.

DEFINICIJA 7.8 Kod $\mathcal{K}(n, k)$ kanala (U, P_K, V) sestavljajo:

1. Množica $M \leq b^k$ informacijskih blokov D , kjer je vsak blok zapisan z nizom k znakov iz abecede koda $B = \{z_1, z_2, \dots, z_b\}$.
2. Bijektivna kodirna funkcija h , ki preslika vsak informacijski blok znakov z iz množice $D \subseteq B^k$ v kodno zamenjavo x , sestavljeno iz $n > k$ znakov iz množice kodnih zamenjav $E \subset U^n$, to je

$$h : z \mapsto x.$$

3. Funkcija odločanja g , ki preslika vsak sprejeti niz znakov (vektor) $y \in V^n$ v v kodno zamenjavo \hat{x} iz množice kodnih zamenjav $E \subset U^n$, to je

$$g : y \mapsto \hat{x}.$$

4. Inverzna kodirna funkcija h^{-1} , ki preslika vsako kodno zamenjavo $\hat{x} \in E$ v informacijski blok znakov $\hat{z} \in D$, to je

$$h^{-1} : \hat{x} \mapsto \hat{z}.$$

Kod kanala

V zvezi s kodom $\mathcal{K}(n, k)$ kanala (U, P_K, V) definiramo tudi količino:

DEFINICIJA 7.9 *Hitrost koda $\mathcal{K}(n, k)$ je*

$$R = \frac{K \log_d M}{n} \quad \text{bitov (natov,...)/znak,} \quad (1)$$

kjer je $M \leq b^k$ število kodnih zamenjav koda, k število znakov v informacijskem bloku, b moč abecede koda (navadno $b = 2$), n število znakov v kodni zamenjavi koda, $K > 0$ poljubna konstanta ter $d > 1$ osnova logaritma, ki določa enoto hitrosti koda.

Opomba: $K \log_d M$ v števcu izraza (1) je lastna informacija enakoverjetnih kodnih zamenjav na vhodu v kanal.

Kod kanala

R lahko razumemo tudi kot *največjo količino informacije na en znak* v n -členi kodni zamenjavi $x \in E$.

Ker je navadno $M = 2^k$, $K = 1$ in $d = 2$, lahko hitrost koda izračunamo tudi kot

$$R = \frac{k}{n} \quad \text{bitov/znak.}$$

Varen prenos informacije po kanalu z motnjami lahko dosežemo s 'kontroliranim' zmanjšanjem hitrosti prevajanja informacije (hitrostjo koda) R ter s postopki dekodiranja z odkrivanjem napak ali s popravljanjem napak.

Pri načrtovanju kodirnika in dekodirnika kanala izberemo naravno število n ter funkciji g in h tako, da je število napačnih dekodiranj dovolj majhno.

Dekodiranje koda kanala

Če vzamemo, da je $U = V = \{0, 1\}$ oziroma $u = v = 2$, lahko ponazorimo vhodne in izhodne vektorje s točkami n -razsežnega vektorskega prostora $\{0, 1\}^n$.

Izhodni vektorji \mathbf{y} lahko ustrezajo katerikoli točki prostora $\{0, 1\}^n$, teh točk je 2^n , M vhodnih vektorjev (kodnih zamenjav) \mathbf{x} pa lahko ustreza kvečjemu 2^k točkam.

Ker je $k < n$, je $E \subset \{0, 1\}^n$. Vsak $\mathbf{y} \neq \mathbf{x}_i$ ($i = 1, \dots, M$) je gotovo napačno sprejet.

Napake pri dekodiranju

Na znakih kodnih zamenjav lahko pride do dveh vrst napak:

- ▶ neodvisnih napak in/ali
- ▶ izbruho v napak.

Napaki, ki se pojavi na znaku odposlane kodne zamenjave neodvisno od morebitnih napak na sosednjih znakih, pravimo *neodvisna* napaka in te so posledica motenj, ki so krajše od trajanja signala enega znaka.

Pri *izbruhu* napak pa bo, če pride do napake na enem znaku kodne zamenjave, zelo verjetno prišlo do napake tudi na nekaj naslednjih znakih, ker je trajanje motenj daljše od trajanja signala enega znaka.

Številu znakov med prvim in zadnjim napačno sprejetim znakom v odposlani kodni zamenjavi pravimo *dolžina izbruha*.

Napake pri dekodiranju

Vektor napake

$$e = y - x_i \quad (2)$$

imenujemo vektor v prostoru $\{0, 1\}^n$, ki kaže iz x_i na y .

Vektor napake $e = (e_1, e_2, \dots, e_n)$ vsebuje enico na tistih mestih, kjer je prišlo v odposlani kodni zamenjavi do napake.

Primer 7.7

Naj bo kodna zamenjava vektor¹ $x = 11011$.

Če je sprejeti vektor $y = 10001$, je $e = 01010$.

Vektor e pove, da je do napake prišlo na drugem in četrtem znaku odposlane kodne zamenjave. □

¹ n -razsežne vektorje $x = (x_1, x_2, \dots, x_n)$ iz $\{0, 1\}^n$ strnjeno pišemo brez vejic in oklepajev.

Napake pri dekodiranju

Poznamo kanale, pri katerih prevladujejo neodvisne napake, ter kanale, pri katerih prevladujejo izbruhi napak.²

Primer 7.8

Vzemimo, da je $n = 20$. Vektor napake

$$e = 00010000010000000100$$

kaže, da je prišlo pri prenosu kodne zamenjave po kanalu do neodvisnih napak na treh znakih.

Vektor napake

$$e = 00000001011010000000$$

pa kaže, da je prišlo pri prenosu kodne zamenjave po kanalu do izbruha napak dolžine 6. □

²Če je znotraj izbruha več kot nek predpisan τ zaporednih znakov enakih nič, obravnavamo dani izbruh kot dva izbruha. Neodvisne napake so z veliko verjetnostjo oddaljene več kot τ .)

Dekodiranje koda kanala

Postopki dekodiranja lahko napake

- ▶ samo odkrivajo, ali pa
- ▶ odkrivajo in hkrati popravljajo.

Za natančno definiranje postopkov dekodiranja vpeljimo naslednje oznake:

$$\implies P(x_i)$$

za verjetnost i -tega vhodnega vektorja, kjer je $\sum_{i=1}^M P(x_i) = 1$,

$$\implies P(y \mid x_i)$$

za pogojno verjetnost izhodnega vektorja $y \in \{0, 1\}^n$, ko je vhodni vektor $x_i \in E$, kjer je $\sum_{y \in \{0, 1\}^n} P(y \mid x_i) = 1$,

Dekodiranje koda kanala

$$\implies P(x_i, y) = P(x_i)P(y | x_i) \quad (3)$$

za verjetnost urejenega para (vhodni vektor x_i , izhodni vektor y),
kjer je $\sum_{i=1}^M \sum_{y \in \{0,1\}^n} P(x_i, y) = 1$,

$$\implies P(y) = \sum_{i=1}^M P(x_i, y) \quad (4)$$

za verjetnost, da na izhodu dobimo vektor $y \in \{0, 1\}^n$, kjer je
 $\sum_{y \in \{0,1\}^n} P(y) = 1$,

$$\implies P(x_i | y) = \frac{P(x_i, y)}{P(y)} \quad (5)$$

za pogojno verjetnost vhodnega vektorja $x_i \in E$, ko je izhodni
vektor $y \in \{0, 1\}^n$, kjer je $\sum_{i=1}^M P(x_i | y) = 1$.

Zasnova dekodiranja z odkrivanjem napak

Dekodirnik, ki napake samo odkriva, ugotavlja, ali je sprejeti izhodni vektor enak kakšnemu vektorju iz množice kodnih zamenjav E .

- Če je $y \in E$, dekodirnik odloči, da ni prišlo do napake pri prenosu po kanalu. Dekodirnik nato posreduje prejemniku informacije tisti blok $z \in D$, ki ima kodno zamenjavo enako sprejetemu vektorju y .
- Če pa $y \notin E$, dekodirnik odloči, da je pri prenosu po kanalu prišlo do napake (napak) na odposlani kodni zamenjavi. V tem primeru dekodirnik zahteva ponovno pošiljanje iste kodne zamenjave x .

Zasnova dekodiranja z odkrivanjem napak

- Če je bila po kanalu odposlana kodna zamenjava x_i , sprejet pa izhodni vektor $y \notin E$, dekodirnik lahko nastalo napako odkrije. Vendar, če je sprejet vektor y , ki je enak neki drugi kodni zamenjavi iz E , na primer $y = x_j$, dekodirnik napake ne more odkriti.

Če označimo s $P(y \mid x_i)$ pogojno verjetnost izhodnega vektorja $y \in \{0, 1\}^n$, ko je vhodni vektor $x_i \in E$, je *verjetnost neodkrite napake, ko je odposlana kodna zamenjava x_i* , enaka

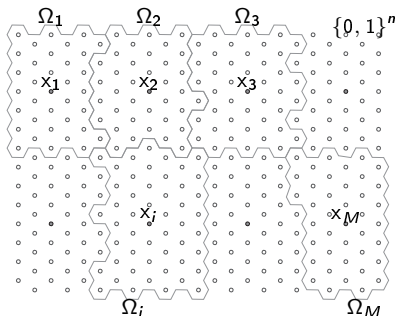
$$P_{NN}(x_i) = \sum_{\substack{y \in E \\ y \neq x_i}} P(y \mid x_i).$$

Zasnova dekodiranja s popravljanjem napak

Dekodirnik, ki odkrije napake tudi popravlja, udejanjimo z delitvijo prostora $\{0, 1\}^n$ na *odločitvena področja* (disjunktne podmnožice) $\Omega_1, \Omega_2, \dots, \Omega_M$, tako da je

$$\Omega_i = \{y : g(y) = x_i\} \quad (6)$$

in $\Omega_i \cap \Omega_j = \emptyset$ za $i \neq j$. Pri tem je g *funkcija odločanja*, ki vsakemu vektorju x_i priredi področje izhodnih vektorjev Ω_i .



Zasnova dekodiranja s popravljanjem napak

- Ker predpostavljamo, da sestavljajo področje Ω_i vsi tisti izhodni vektorji y , ki so posledica prenosa kodne zamenjave $x_i \in E$ po kanalu z motnjami, *odločimo*, da je odposlan x_i , če sprejmemo $y \in \Omega_i$.
- Odločitev bo očitno napačna, ko sprejmemo niz $y \in \Omega_i$, odposlan pa je bil niz $x \neq x_i$.

Zasnova dekodiranja s popravljanjem napak

Verjetnost pravilnega dekodiranja sprejetega vektorja \mathbf{y} , ko je odposlana kodna zamenjava \mathbf{x}_i , je

$$P_{PD}(\mathbf{x}_i) = \sum_{\mathbf{y} \in \Omega_i} P(\mathbf{y} \mid \mathbf{x}_i),$$

medtem ko sta verjetnost napačnega dekodiranja kodne zamenjave \mathbf{x}_i

$$\begin{aligned} P_{ND}(\mathbf{x}_i) &= \sum_{\substack{j=1 \\ j \neq i}}^M \sum_{\mathbf{y} \in \Omega_j} P(\mathbf{y} \mid \mathbf{x}_i) \\ &= 1 - P_{PD}(\mathbf{x}_i) \end{aligned}$$

in povprečna (celotna) verjetnost napake dekodiranja s popravljanjem napak

$$\bar{P}_{ND} = \sum_{i=1}^M P(\mathbf{x}_i) \left[1 - \sum_{\mathbf{y} \in \Omega_i} P(\mathbf{y} \mid \mathbf{x}_i) \right]. \quad (7)$$

Zasnova dekodiranja s popravljanjem napak

Primernost koda $\mathcal{K}(n, k)$ kanala (U, P_K, V) za uresničitev varnega prevajanja informacije ne opredeljuje povprečna verjetnost napake, temveč *največja verjetnost napake*

$$P_{ND}^{max} = \max_{1 \leq i \leq M} \{P_{ND}(x_i)\}. \quad (8)$$

Dekodirnik, ki na primer eno kodno zamenjavo dekodira vselej napačno, je neuporaben, kljub temu, da v povprečju nujno ne zgreši veliko napak (glej izraz (7)).

Zato bomo poiskali takšno funkcijo odločanja

$$g : V^n \rightarrow E,$$

ki čim bolj zmanjša največjo verjetnost napake P_{ND}^{max} .
V tem primeru bo namreč tudi \bar{P}_{ND} 'dovolj majhna'.

Funkcije odločanja

Naloga funkcij odločanja

$$g: V^n \rightarrow E,$$

kjer sta $V^n = \{0, 1\}^n$ in $E = \{x_1, x_2, \dots, x_M\}$, je, da sprejetim izhodnim vektorjem pridružijo najbolj verjetne vhodne vektorje.

Vzemimo, da za sprejeti vektor y dekodirnik odloči, da je odposlan vektor x_i .

- Verjetnost, da je ta odločitev pravilna, je enaka pogojni verjetnost vhodnega vektorja x_i , ko je dan izhodni vektor y , torej $P(x_i | y)$.
- Verjetnost, da je ta odločitev napačna, pa je enaka $1 - P(x_i | y)$.

Funkcija odločanja z najmanjšo verjetnostjo napake

Verjetnost napačne odločitve bo torej najmanjša, če funkcijo odločanja g definiramo kot:

DEFINICIJA 7.10 *Odločimo $\hat{x} = g(y)$, ko je*

$$P(\hat{x} | y) = \max_{1 \leq i \leq M} \{P(x_i | y)\}. \quad (9)$$

Če obstaja v množici E več vektorjev \hat{x} , za katere je pogojna verjetnost $P(x_i | y)$ največja, enega izmed njih poljubno izberemo.

Ker tako definirana preslikava g minimizira povprečno verjetnost napake dekodiranja \overline{P}_{ND} , jo imenujemo

*funkcija odločanja z najmanjšo verjetnostjo napake.*³

³Angleški izraz (najbolj pogosto): *Maximum A Posteriori (MAP) Decoding*.

Funkcija odločanja z najmanjšo verjetnostjo napake

Iz (7) sledi

$$\begin{aligned} \sum_{i=1}^M P(x_i) \left[1 - \sum_{y \in \Omega_i} P(y | x_i) \right] &= \sum_{i=1}^M P(x_i) \sum_{y \notin \Omega_i} P(y | x_i) = \sum_{i=1}^M \sum_{y \notin \Omega_i} P(x_i, y) = \\ &= \sum_{y \in V^n} \sum_{x_i \neq g(y)} P(x_i, y) = \sum_{y \in V^n} P(y) \sum_{x_i \neq g(y)} P(x_i | y) = \sum_{y \in V^n} P(y) [1 - P(\hat{x} | y)], \end{aligned}$$

zato je \overline{P}_{ND} najmanjša, če velja (9) za vsak $y \in V^n$.

Če upoštevamo (5) in (3), lahko zapišemo a posteriori verjetnost x -a kot

$$P(x_i | y) = \frac{P(x_i)P(y | x_i)}{P(y)}. \quad (10)$$

Ker je imenovalec izraza (10) neodvisen od i , je iskanje največje vrednosti a posteriori verjetnosti $P(x_i | y)$ v (9) enakovredno iskanju največje vrednosti števca $P(x_i)P(y | x_i)$.

Funkcija odločanja z največjim verjetjem

Funkcijo odločanja g , ki sicer ne zagotavlja najmanjše verjetnosti napačne odločitve, vendar jo za kanale brez spomina lažje udejanjimo kot funkcijo (9), definiramo takole:

DEFINICIJA 7.11 *Odločimo $\hat{x} = g(y)$, ko je*

$$P(y \mid \hat{x}) = \max_{1 \leq i \leq M} \{P(y \mid x_i)\}. \quad (11)$$

Če obstaja v množici E več vektorjev \hat{x} , za katere je pogojna verjetnost $P(y \mid x_i)$ največja, enega izmed njih poljubno izberemo.

Tako definirano funkcijo g imenujemo

*funkcija odločanja z največjim verjetjem.*⁴

⁴Angleški izraz (najbolj pogosto): *Maximum Likelihood (ML) Decoding*.

Idealna funkcija odločanja

Funkcija odločanja z največjim verjetjem ni optimalna, ker ne upošteva porazdelitve vhodnih vektorjev $P(x_i)$ ($i = 1, 2, \dots, M$), lažje pa jo udejanjimo zato, ker pogojne verjetnosti $P(y | x_i)$ lahko izračunamo s podatki, ki jih vsebuje matrika kanala P_K .

Če so vhodni vektorji enako verjetni, to je, če velja

$$P(x_i) = \frac{1}{M}, \quad i = 1, 2, \dots, M,$$

iz (9), (10) in (11) sledi, da je funkcija odločanja z najmanjšo verjetnostjo napake enaka funkciji odločanja z največjim verjetjem, in v tem primeru govorimo o

idealni funkciji odločanja

Idealna funkcija zaporednega odločanja

Pri kanalu brez spomina se z idealno funkcijo odločanja sprejeti vektor dekodira preprosto tako, da se dekodira vsak znak sprejetega vektorja posebej, zato preslikavo g imenujemo tudi

*idealna funkcija zaporednega odločanja*⁵.

Primer 7.8 Za dano matriko kanala

$$P_K = \begin{bmatrix} P(y_1 | x_1) & P(y_2 | x_1) & P(y_3 | x_1) \\ P(y_1 | x_2) & P(y_2 | x_2) & P(y_3 | x_2) \\ P(y_1 | x_3) & P(y_2 | x_3) & P(y_3 | x_3) \end{bmatrix} = \begin{bmatrix} 0,3 & 0,2 & 0,5 \\ 0,5 & 0,3 & 0,2 \\ 0,2 & 0,5 & 0,3 \end{bmatrix}$$

zapišemo idealno funkcijo odločanja takole:

$$y_1 \mapsto x_2, \quad y_2 \mapsto x_3, \quad y_3 \mapsto x_1.$$



⁵Angleški izraz: *Symbol-by-symbol Decoding*.

Idealna funkcija odločanja za dvojiški simetrični kanal

Idealno funkcijo odločanja za dvojiški simetrični kanal brez spomina (DSK), lahko udejanjimo tudi brez računanja pogojnih verjetnosti $P(y | x_i)$ ($i = 1, 2, \dots, M$), če nad množico n -razsežnih vektorjev iz $\{0, 1\}^n$ definiramo funkcijo razdalje

$$d : \{0, 1\}^n \times \{0, 1\}^n \implies \mathbb{R},$$

ki za poljubne $x, y, z \in \{0, 1\}^n$ zadošča pogojem:

- a) $d(x, y) \geq 0$
- b) $d(x, y) = 0 \iff x = y$
- c) $d(x, y) = d(y, x)$
- d) $d(x, z) \leq d(x, y) + d(y, z)$.

Tem pogojem zadošča Hammingova razdalja.

Hammingova razdalja

DEFINICIJA 7.12 Hammingova razdalja $d_H(x,y)$ vektorjev $x \in \{0,1\}^n$ in $y \in \{0,1\}^n$ je enaka številu komponent, na katerih se vektorja razlikujeta. Torej:

$$x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \implies d_H(x,y) = \sum_{i=1}^n |x_i - y_i|. \quad (12)$$

Primer 7.9

Če je $n = 5$, $x = 00110$ in $y = 10101$, je $d_H(x,y) = 3$. Vektorja x in y se namreč razlikujeta na prvem, četrtem in petem mestu. \square

Hammingova razdalja

Da Hammingova razdalja $d_H(x, y)$ zadošča pogojem a), b) in c), je očitno. Dokažimo še, da zadošča tudi trikotniški neenakosti d):

$$\begin{aligned}d_H(x, y) + d_H(y, z) &= \sum_{i=1}^n (|x_i - y_i| + |y_i - z_i|) \geq \sum_{i=1}^n |x_i - y_i + y_i - z_i| \\&= \sum_{i=1}^n |x_i - z_i| \\&= d_H(x, z).\end{aligned}$$

TRDITEV 7.1 *Hammingova razdalja $d_H(x, y)$ vektorjev $x \in \{0, 1\}^n$ in $y \in \{0, 1\}^n$ je enaka številu enic v vektorju $(x + y) \in \{0, 1\}^n$, to je*

$$d_H(x, y) = w(x + y),$$

kjer funkcija $w(\cdot)$ prešteje enice v danem vektorju oziroma njegovo 'težo'.

Hammingova razdalja

Pri računanju teže upoštevamo, da ima vsota $x + y$ enico na mestih, kjer se vektorja x in y razlikujeta, na ostalih mestih pa ničlo.

Primer 7.10

Na primer:

$$d_H(00110, 10101) = w(00110 + 10101) = w(10011) = 3. \quad \square$$

Idealna funkcija odločanja za dvojiški simetrični kanal

Za določitev idealne funkcije odločanja za dani DSK brez računanja pogojnih verjetnosti $P(y | x_i)$ ($i = 1, 2, \dots, M$) moramo dokazati še naslednji izrek:

IZREK 7.2 *Za diskretni simetrični kanal, ki je dan z matriko⁶*

$$P_K = \begin{bmatrix} 1 - \varepsilon & \varepsilon \\ \varepsilon & 1 - \varepsilon \end{bmatrix}, \quad \text{kjer je } 0 < \varepsilon < \frac{1}{2},$$

velja

$$P(y | x_1) > P(y | x_2) \iff d_H(x_1, y) < d_H(x_2, y)$$

za vsak $y \in \{0, 1\}^n$ in ustrezna $x_1 \in E$ in $x_2 \in E$.

⁶Pogoj za verjetnost napake ε smo postavili tako, da kanal sicer ni brezizguben, se je pa po njem mogoče sporazumevati.

Idealna funkcija odločanja za dvojiški simetrični kanal

Dokaz: Naj bo Hammingova razdalja med x in y enaka

$$d_H(x, y) = m \text{ pri } (0 \leq m \leq n).$$

Pogojno verjetnost

$$P(y | x) = P((y_1, y_2, \dots, y_n) | (x_1, x_2, \dots, x_n)) = P(y_1 | x_1) \cdot P(y_2 | x_2) \cdots P(y_n | x_n)$$

za dani DSK lahko zapišemo kot

$$P(y | x) = \varepsilon^m (1 - \varepsilon)^{n-m} \quad (0 \leq m \leq n). \quad (13)$$

Za poljubna x_1 in x_2 je tedaj

$$P(y | x_1) = \varepsilon^{m_1} (1 - \varepsilon)^{n-m_1},$$

kjer je $m_1 = d_H(x_1, y)$ in

$$P(y | x_2) = \varepsilon^{m_2} (1 - \varepsilon)^{n-m_2},$$

kjer je $m_2 = d_H(x_2, y)$.

Idealna funkcija odločanja za dvojiški simetrični kanal

Velja

$$\frac{P(y | x_1)}{P(y | x_2)} = \frac{\varepsilon^{m_1}(1 - \varepsilon)^{n-m_1}}{\varepsilon^{m_2}(1 - \varepsilon)^{n-m_2}} = \left(\frac{1 - \varepsilon}{\varepsilon}\right)^{m_2 - m_1}. \quad (14)$$

Ker je $0 < \varepsilon < 1/2$, je $(1 - \varepsilon)/\varepsilon > 1$.

Zato bo $P(y | x_1)/P(y | x_2) > 1$ le, če je $m_1 < m_2$. ■

Idealna funkcija odločanja za dvojiški simetrični kanal

Za dani DSK in dano množico vhodnih vektorjev

$E = \{x_1, x_2, \dots, x_M\}$ idealno funkcijo odločanja g udejanjimo takole:

Za vsak izhodni vektor $y \in \{0, 1\}^n$ poiščemo tisti vhodni vektor $\hat{x} \in E$, za katerega je Hammingova razdalja $d_H(\hat{x}, y)$ najmanjša. Če obstaja več takšnih vektorjev $\hat{x} \in E$, enega izmed njih poljubno izberemo.

Torej lahko *idealno funkcijo odločanja*

$$\max_{1 \leq i \leq M} \{P(y \mid x_i)\} = P(y \mid \hat{x}) \implies g(y) = \hat{x}$$

za dvojiški simetrični kanal zapišemo kot

$$\min_{1 \leq i \leq M} \{d_H(x_i, y)\} = d_H(\hat{x}, y) \implies g(y) = \hat{x}. \quad (15)$$

Idealna funkcija odločanja za dvojiški simetrični kanal

Opazimo, da moramo zaradi varnega prenosa informacije po DSK-ju *izbrati* $M \leq 2^k$ *kodnih zamenjav* vektorjev informacijskih znakov, *tako da so Hammingove razdalje med njimi v prostoru* $\{0, 1\}^n$ *čim večje*.

V tem primeru, tudi če pride pri prenosu do nekaj napak, se vektor na izhodu iz kanala ne bo oddaljil od odposlanega vektorja toliko, da bi bil bližji kakšnemu drugemu vhodnemu vektorju (drugi kodni zamenjavi) iz E .

Optimalna dolžina kodnih zamenjav

Osnovni problem, ki ga sedaj želimo rešiti je, da za dano število možnih informacijskih blokov M najdemo *najmanjšo* dolžino kodnih zamenjav.

To je, najmanjše število n , ki omogoča, da je ob uporabi idealnega pravila odločanja prenos informacije po DSK-ju pravilen (brez napake) tudi v primeru, ko pri prenosu nastopi e ($0 \leq e \leq n$) napak⁷.

Za dano množico $E = \{x_1, \dots, x_M\} \subset \{0, 1\}^n$ naj bo n takšen, da za Hammingovo razdaljo poljubnega para vhodnih vektorjev $x_i \neq x_j$ velja

$$d_H(x_i, x_j) \geq 2e + 1. \quad (16)$$

(Različna elementa iz E sta torej oddaljena vsaj $2e + 1$ enot Hammingove razdalje.) Razdaljo $d_H(x_i, x_j) = 2e + 1$ imenujemo *najmanjša razdalja koda* in jo navadno označujemo z d_{min} .

⁷Napaka pomeni spremembo znaka kodne zamenjave 0 v 1 oziroma 1 v 0.

Optimalna dolžina kodnih zamenjav

V tem primeru lahko ob uporabi idealnega pravila odločanja dosežemo pravilen sprejem odposlanega vektorja, če pri prenosu nastopi e ali manj napak.

Očitno je namreč, da lahko za vsak $x_i \in E$ oblikujemo množico Ω_i vseh tistih vektorjev $y \in \{0, 1\}^n$, za katere je $d_H(x_i, y) \leq e$, to je

$$\Omega_i = \{y \in \{0, 1\}^n : d_H(x_i, y) \leq e\}, \quad i = 1, \dots, M, \quad (17)$$

ter da z idealnim pravilom odločanja

$$g(y) = x_i \quad \text{za} \quad y \in \Omega_i \quad (i = 1, \dots, M)$$

dosežemo pravilen sprejem odposlanih vektorjev, če nastopi pri prenosu e ali manj napak. Množice $\Omega_1, \Omega_2, \dots, \Omega_M$ so paroma disjunktne.

To očitno dejstvo je razvidno tudi iz geometrične razlage (pod)množic $\Omega_1, \Omega_2, \dots, \Omega_M$.

Optimalna dolžina kodnih zamenjav

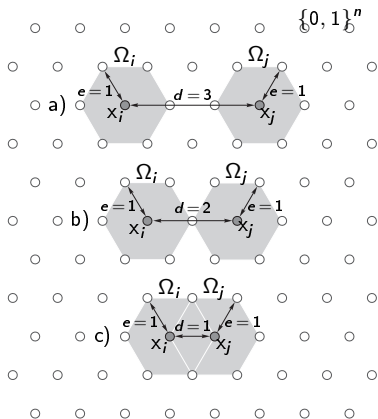
Množico Ω_i , ki smo jo definirali s (17), si lahko geometrijsko predstavljamo kot (hiper)kroglo polmera e s središčem v “točki” x_i v n -razsežnem vektorskem prostoru $\{0, 1\}^n$ vseh n -razsežnih dvojiških vektorjev z definirano Hammingovo razdaljo.

Če je najmanjša razdalja med središči krogel vsaj $2e + 1$ (glej (16)), se krogle v prostoru ne sekajo.

Zato velja, da če na odposlanem vektorju nastane e ali manj napak, se ta sicer ‘oddalji’ od središča krogle, vendar ne zapusti krogle, da bi ga z uporabo Hammingove razdalje napačno ‘dekodirali’.

Optimalna dolžina kodnih zamenjav

Slika 1 ponazarja primer: a) krogle, ki so v prostoru dovolj narazen, da se ne dotikajo, b) dotikanja krogel ter c) sekanja krogel.



Slika: Množice Ω_i kot (hiper)krogle v prostoru.

Optimalna dolžina kodnih zamenjav - primer

Primer 7.11

Vzemimo, da je dana množica kodnih zamenjav

$$E = \{000, 111\}.$$

Ker je najmanjša razdalja med kodnimi zamenjavami $d_{min} = 3$, kod lahko popravi vse enojne napake.

Odločitveni področji (množici) za kodni zamenjavi $x_1 = 000$ in $x_2 = 111$ sta:

$$\Omega_1 = \{000, 100, 010, 001\} \text{ in}$$

$$\Omega_2 = \{111, 011, 101, 110\}.$$

Optimalna dolžina kodnih zamenjav - primer

Da bi se prepričali, da kod lahko popravi enojne napake na kodnih zamenjavah, vzemimo, da odpošljemo po kanalu $x_2 = 111$ ter da pride do napake na tretjem znaku kodne zamenjave, torej $e = 001$.

Sprejeli smo torej vektor $y = x_2 + e = 110$.

Ker je $y = 110 \in \Omega_2$, ga dekodiramo kot x_2 .

Vendar, če bi pri prenosu po kanalu na kodni zamenjavi prišlo do dveh napak, bi kodirnik sprejeti vektor napačno dekodiral.

Na primer, če je odposlana kodna zamenjava x_2 in je vektor napake $e = 011$, bi dekodirnik napačno dekodiral sprejeti vektor $y = 100 \in \Omega_1$ kot odposlano kodno zamenjavo x_1 . □

Hammingov pogoj

Naslednja izreka vzpostavljata zvezo med številom vektorjev, ki se prenašajo po kanalu, M , številom napak e in dolžino vektorjev na vhodu v dvojiški kanal n .

IZREK 7.3 (Hammingov pogoj) Če lahko kod $\mathcal{K}(n, k)$ popravi e ali manj napak, število kodnih zamenjav M ustreza pogoju

$$M \leq \frac{2^n}{\sum_{i=0}^e \binom{n}{i}}. \quad (18)$$

Dokaz: Glej učbenik *Informacija in kodi*, str. 174.

Desni strani neenačbe (18) pravimo *Hammingova zgornja meja* števila kodnih zamenjav M koda $\mathcal{K}(n, k)$, ki lahko popravi e napak na sprejetih kodnih zamenjavah (vektorjih y).

IZREK 7.4 (Gilbertov pogoj) Če lahko kod $\mathcal{K}(n, k)$ popravi e ali manj napak, število kodnih zamenjav M ustreza pogoju

$$M \geq \frac{2^n}{\sum_{i=0}^{2e} \binom{n}{i}}. \quad (19)$$

Dokaz: Glej učbenik *Informacija in kodi*, str. 175.

Desni strani neenačbe (19) pravimo *Gilbertova spodnja meja* števila kodnih zamenjav M koda $\mathcal{K}(n, k)$, ki lahko popravi e napak na sprejetih kodnih zamenjavah (vektorjih y).

Spodnje in zgornje meje dolžine kodnih zamenjav

Vrednosti Gilbertove spodnje meje (GSM) in Hammingove zgornje meje (HZM) števila kodnih zamenjav M za nekaj izbranih vrednosti n in e ponazarja spodnja tabela.

$e = 1$			$e = 2$		
n	GSM	HZM	n	GSM	HZM
3	$8/7 \approx 1,1$	2	5	$32/31 \approx 1,0$	2
4	$16/11 \approx 1,5$	$16/5 = 3,2$	6	$64/57 \approx 1,1$	$32/11 \approx 2,9$
5	$32/16 = 2$	$16/3 \approx 5,3$	7	$128/99 \approx 1,3$	$128/29 \approx 4,4$
6	$32/11 \approx 2,9$	$64/7 \approx 9,1$	8	$256/163 \approx 1,6$	$256/37 \approx 6,9$
7	$128/29 \approx 4,4$	16	9	$512/256 = 2$	$256/23 \approx 11,1$
8	$256/37 \approx 6,9$	$256/9 \approx 28,5$	10	$512/193 \approx 2,7$	$128/7 \approx 18,3$

Hammingov pogoj

Hammingov pogoj (18) je potreben, ne pa hkrati tudi zadosten pogoj za gradnjo koda $\mathcal{K}(n, k)$, ki lahko popravi e ali manj napak na kodni zamenjavi dolžine n .

V to se lahko prepričamo, če v (18) vstavimo na primer $n = 4$ in $e = 1$. Pogoj (18) dovoljuje $M = 3$, to je $k = 2$.

Da bi kod $\mathcal{K}(4, 2)$ lahko popravljal enojne napake, mora biti razdalja med vsakim parom kodnih zamenjav vsaj $d_{min} = 2e + 1 = 2 \cdot 1 + 1 = 3$ enote Hammingove razdalje, vendar je med štirirazsežnimi dvojiškimi vektorji 0000, 0001, ..., 1111 mogoče najti le dva vektorja na Hammingovi razdalji vsaj 3, ne pa treh ($M = 3$).

Gilbertov pogoj

Gilbertov pogoj (19) je zadosten, ni pa vedno tudi potreben pogoj za gradnjo koda $\mathcal{K}(n, k)$, ki lahko popravi e ali manj napak.

To pomeni, če za dana n in e določimo najmanjši M , ki ustreza pogoju (19), tedaj bo kod $\mathcal{K}(n, k)$ lahko popravil e ali manj napak.

Je pa hkrati možno, da obstaja še kakšen kod $\mathcal{K}(n, k)$ z več kot M kodnimi zamenjavami, ki lahko ravno tako popravi e ali manj napak.

Na primer, če v (19) vstavimo $n = 10$ in $e = 2$, dobimo $\approx 2,7$. Najmanjše število kodnih zamenjav (vektorjev, ki se prenašajo po kanalu) M je torej enako 3. Vendar je možno sestaviti kod $\mathcal{K}(10, k)$ za $e = 2$ tudi z osmimi kodnimi zamenjavami v E .

Spodnja in zgornja meja dolžine kodnih zamenjav

Če pišemo $M = 2^k$ in $2^n = 2^{k+m}$, lahko omenjena pogoja zapišemo kot

$$2^m \geq \sum_{i=0}^e \binom{n}{i} \quad (20)$$

in

$$2^m \leq \sum_{i=0}^{2e} \binom{n}{i}. \quad (21)$$

Nenačbi (20) pravimo Hammingova spodnja meja, nenačbi (21) pa Gilbertova zgornja meja števila m *odvečnih* (neinformacijskih) znakov v kodnih zamenjavah koda $\mathcal{K}(n, k)$, ki lahko popravi vse e ali manjkratne napake.

Spodnja in zgornja meja dolžine kodnih zamenjav - primer

Primer 7.12

Vzemimo, da želimo zgraditi kod $\mathcal{K}(n, 4)$, ki lahko popravi vse enojne napake. Torej, $k = 4$ in $n = k + m = 4 + m = ?$

Potrebno število odvečnih znakov v kodnih zamenjavah m določimo iz neenačb (20) in (21). Kod $\mathcal{K}(n, 4)$, ki lahko popravi vse enojne napake ($e = 1$), obstaja za tiste m , za katere je 2^m med Hammingovo spodnjo in Gilbertovo zgornjo mejo števila m :

$$\text{HSM} = \sum_{i=0}^1 \binom{n}{i} = 1 + n \quad \text{in} \quad \text{GZM} = \sum_{i=0}^2 \binom{n}{i} = 1 + n + \binom{n}{2}.$$

Spodnja in zgornja meja dolžine kodnih zamenjav - primer

Iskanje potrebnega števila preverjalnih znakov m ponazarja spodnja tabela.

m	n	HSM	2^m	GZM
1	5	6	2	16
2	6	7	4	22
3	7	8	8	29
4	8	9	16	37
5	9	10	32	46
6	10	11	64	56
\vdots	\vdots	\vdots	\vdots	\vdots


Tabela: Hammingova spodnja meja (HSM) in Gilbertova zgornja meja (GZM) števila m odvečnih znakov v kodnih zamenjavah x koda $\mathcal{K}(n = 4 + m, 4)$, ki lahko popravi eno napako ($e = 1$).

Spodnja in zgornja meja dolžine kodnih zamenjav - primer

Iz tabele 1 izhaja, da naravna števila $m \leq 2$ in $m \geq 6$ ne zadoščajo neenačbam (20) in (21).

Za kod je najbolj ugoden najmanjši $3 \leq m \leq 5$ (optimalna dolžina kodnih zamenjav), zato najprej poskusimo zgraditi kod $\mathcal{K}(7, 4)$.

Ker pa je Hammingov pogoj le potreben, ne pa tudi zadosten, ni nujno da nam bo to tudi uspelo⁸. □

⁸Navadno je vprašljiv samo tisti m , ki je najbližji HSM. 

Popolni kod

DEFINICIJA 7.13 Kod $\mathcal{K}(n, k)$, za katerega sta izpolnjena pogoja:

1. $\Omega_i \cap \Omega_j = \emptyset$ za vsak $i, j = 1, 2, \dots, M$ ($i \neq j$) in

2. $\bigcup_{i=1}^M \Omega_i = \{0, 1\}^n$,

imenujemo popolni kod.

Za popolni kod lahko Hammingov pogoj (18) zapišemo kot

$$M \sum_{i=0}^e \binom{n}{i} = 2^n$$

oziroma kot

$$\sum_{i=0}^e \binom{n}{i} = 2^m,$$

če je število kodnih zamenjav $M = 2^k = 2^{n-m}$.

Popolni kod

Število odvečnih znakov v kodnih zamenjavah popolnih kodov je torej najmanjše, zato so med vsemi kodi, ki lahko popravijo e ali manj napak, popolni kodi '*najhitrejši*'.

Shannonova izreka o varnem kodiranju

Eden izmed glavnih problemov gradnje varnih kodov je, da ugotovimo pogoje, ki jim morata zadostiti kodirnik in dekodirnik kanala, da prenese znak po kanalu vso informacijo, ki jo je prevzel od vira informacije, z verjetnostjo, čim bližje vrednosti ena.

Shannonova izreka o diskretnem kanalu brez spomina s kapaciteto $C > 0$ pravita, pod katerimi pogoji je možno pravilno (brez napak) prenašati informacijo po kanalu, ki je moten s šumom.

Shannonova izreka o varnem kodiranju

Prvi Shannonov izrek o varnem kodiranju (izrek 7.5) pravi, da

- ▶ če je $R < C$, tedaj obstaja kod $\mathcal{K}(n, k)$, ki zagotavlja takšno prevajanje informacije, da je verjetnost napake pri dekodiranju poljubno majhna;

drugi (izrek 7.6) pa, da

- ▶ če je $R > C$, ne obstaja nobeno kodiranje, ki bi omogočalo, da bi bilo prevajanje informacije brez napake z verjetnostjo poljubno blizu nič.

Shannonov izrek o varnem kodiranju

IZREK 7.5 (Shannonov izrek o varnem kodiranju) *Dana sta diskretni kanal brez spomina s kapaciteto $C > 0$ in realno število R ($0 < R < C$). Obstaja takšen kod $\mathcal{K}(n, k)$ in takšna funkcija odločanja g , da velja:*

$$\begin{aligned} P_{ND}^{\max} &\leq \delta + d^{-\rho n}, \\ M &\geq d^{nR}, \end{aligned}$$

kjer sta δ in ρ poljubno majhni pozitivni števili, M število kodnih zamenjav v množici E , R hitrost koda (glej (1)), d osnova logaritma pri računanju C in R ter P_{ND}^{\max} največja verjetnost napake (glej (8)) koda $\mathcal{K}(n, k)$.

Dokaz: Glej učbenik *Informacija in kodi*, str. 179.

Obrat Shannonovega izreka o varnem kodiranju

IZREK 7.6 (Obrat Shannonovega izreka o varnem kodiranju)

Če je hitrost koda R za poljuben kod $\mathcal{K}(n, k)$ in dani diskretni kanal brez spomina s kapaciteto $C > 0$ večja od kapacitete kanala ($R > C$), največja verjetnost P_{ND}^{\max} (glej (8)) ne teži k nič, ko narašča dolžina kodnih zamenjav n čez vse meje.

Dokaz: Glej učbenik *Informacija in kodi*, str. 180.

Vprašanja

- ▶ Kako je definirana hitrost koda?
- ▶ Kako je definirana shema odločanja z najmanjšo verjetnostjo napake?
- ▶ Kako je definirana shema odločanja z največjo verjetnostjo?
- ▶ Kdaj govorimo o idealni shemi odločanja?
- ▶ Kako je definirana Hammingova razdalja?
- ▶ Kako se udejanji idealna shema odločanja za binarni simetrični kanal?
- ▶ Kako je definirana najmanjša razdalja koda?
- ▶ Kaj sta spodnja in zgornja meja intervala, v katerem je vklenjeno število kodnih zamenjav koda?
- ▶ Kaj trdita Shannonova izreka o varnem kodiranju?