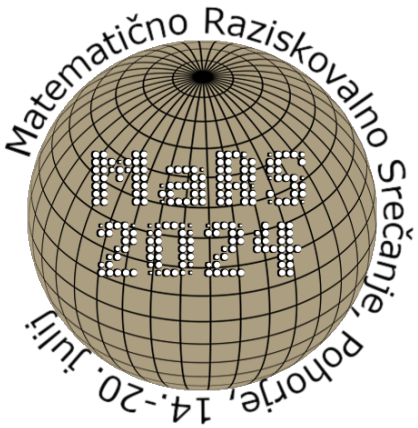
Teorija kodiranja in Hammingov kod

Val Filej, Janoš Ivanec
Mentor: Juš Kocutar



Povzetek

Obravnavane so osnove teorije kodiranja. Definirani so linearni kodi, dimenzija in minimalna razdalja. Predstavljen je Hammingov kod in kako je z njim povečana verjetnost pravilno poslanih sporočil.

1 Uvod

Želimo modelirati, kako lahko pošiljamo sporočila v resničnem življenju. Vsako sporočilo pretvorimo v zaporedje simbolov, ki so 0 ali 1. Pošiljatelj pošlje zaporedje preko nekega kanala in prejemnik ga dobi. V resničnem življenju se pri prenosu sporočila skozi vsak kanal lahko zgodijo napake. To pomeni, da se kakšen simbol spremeni iz 0 v 1, ali pa, da ga ne moremo določiti. Ideja teorije kodiranja je, da sporočilu, ki ga želimo poslati, dodamo nekaj bitov in s tem poskrbimo, da niso vse oblike sporočil dovoljene.

Poglejmo problem na preprostem primeru. Recimo, da želimo poslati sporočilo štirih bitov in vemo, da je verjetnost, da se vsak bit pokvari, enaka p. Predpostavimo tudi, da je verjetnost, da se en bit pokvari, neodvisna od tega, ali se drugi pokvarijo. Sledi, da je verjetnost, da se celo sporočilo štirih bitov prenese pravilno, enaka $(1-p)^4$. Za $p = 4\%$ to pomeni, da je verjetnost, da bo celotno sporočilo pravilno, enaka $\approx 85\%$. Naš cilj je, s čim manj dodanih bitov, povečati verjetnost pravilno prenesenega sporočila.

2 Osnovne definicije

2.1 Kodi

Najprej bomo definirali množico vseh možnih zaporedij neke dolžine. Elementu množice $\{0,1\}$ pravimo **bit**.

Definicija 1. *Označimo s $\mathbb{F}_2^n$ množico vseh možnih zaporedij dolžine n, kjer je n naravno število, s členi v $\{0,1\}$. Velja torej*

$$\mathbb{F}_2^n = \{(a_1, a_2, a_3, \ldots, a_n) : \ a \in \{0,1\}, \ n \in \mathbb{N}\}.$$

Za množico dovoljenih simbolov (t.i. abecedo) bi si namesto $\{0,1\}$ lahko izbrali poljubno množico, na primer slovensko abecedo $\{A, B, \ldots, Z, \check{Z}\}$. Dva razloga, zakaj si izberemo množico z dvema elementoma, sta, da je to najmanjše število simbolov, ki naredi zanimivo množico zaporedij dolžine n. Drugi razlog je, da sta 0 in 1 osnovna simbola v računalništvu, od koder izvirajo praktični problemi, ki so motivirali razvoj teorije kodiranja.

Na množici bitov $\{0,1\}$ definiramo operacijo seštevanja s predpisi

$$\begin{aligned} 1+1&=0,\\ 1+0&=1,\\ 0+1&=1,\\ 0+0&=0. \end{aligned}$$

Ta operacija je enaka operaciji seštevanja ostankov po modulu 2, ali pa logičnim vratom XOR. Lahko preverimo, da je zgornje seštevanje asociativno in komutativno.

Seštevanje na množici $\{0,1\}$ lahko prenesemo na množico $\mathbb{F}_2^n$ tako, da seštevamo komponente. Za poljubna elementa

$$x = (a_1, a_2, \ldots, a_n),\ y = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_2^n$$

definiramo njuno vsoto kot

$$x + y = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Definicija 2. ***Kod*** *C je podmnožica množice $\mathbb{F}_2^n$.*

Namen definicije „koda“ je, da predstavlja množico vseh *dovoljenih* zaporedij bitov. Zato, da lahko prejemnik sporočila zazna ali popravi potencialne napake, ki so nastale pri prenosu sporočila skozi kanal, je bistveno, da dovoljena zaporedja niso vsi elementi $\mathbb{F}_2^n$. Če bi vsa sporočila dolžine n bila dovoljena, bi prejemnik sporočila mislil, da so bila dejansko poslana sporočila z napakami.

Namesto $(a_1, a_2, \ldots, a_n)$ bomo elemente množice $\mathbb{F}_2^n$ pisali kot $a_1a_2\ldots a_n$; na primer $(1,0,1) = 101$. Zaporedje $00\ldots00$ bomo pogosto označili kar s simbolom 0 in bo razvidno iz konteksta, ali mislimo na zaporedje z ničlami ali bit 0.

V naslednjem primeru bomo vzeli $n = 3$ in si ogledali kod $C \subset \mathbb{F}_2^3$, kjer je

$$\mathbb{F}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\},$$

$$C = \{000, 011, 101, 110\}.$$

Opazimo lahko, da je v zgornjemu kodu C zadnji bit v zaporedju enak vsoti prvih dveh bitov po prej definiranem seštevanju na množici $\{0,1\}$. Zaradi tega pravila je število vseh elementov v kodu enako $2 \cdot 2 = 4$, saj imamo dve možnosti za vsakega od prvih bitov, tretji pa je z njima že določen.

2.2 Hammingova razdalja

Poskusimo definirati razdaljo med dvema poljubnima zaporedjema v množici $\mathbb{F}_2^n$. Želimo, da sta si dve zaporedji blizu, če imata več enakih bitov na enakih mestih v zaporedju. To lahko storimo s pomočjo Hammingove razdalje, ki primerja dve zaporedji in zazna vsa mesta v zaporedjih, v katerih se razlikujeta. Razdalja je potem enaka številu vseh mest, v katerih se razlikujeta.

Definicija 3. *Za poljubna elementa $x = a_1a_2\ldots a_n$ in $y = b_1b_2\ldots b_n \in \mathbb{F}_2^n$ definiramo* ***Hammingovo razdaljo*** *$d(x,y)$ kot*

$$d(x,y) = |\{i :\ a_i \neq b_i,\ 1 \leq i \leq n\}|.$$

Za Hammingovo razdaljo velja trikotniška neenakost.

Izrek 1 (Trikotniška neenakost)**.** *Naj bodo $x, y, z \in \mathbb{F}_2^n$. Potem velja*

$$d(x,y) \leq d(x,z) + d(z,y).$$

Dokaz. Naj bodo $x = a_1a_2 \dots a_n,\ y = b_1b_2 \dots b_n$ in $z = c_1c_2 \dots c_n$. Trdimo, da velja

$$\{i :\ a_i \neq b_i\} \subseteq \{j :\ a_j \neq c_j\} \cup \{k :\ b_k \neq c_k\}.$$

Denimo, da imata x in y različna bita na mestu l, torej $l \in \{i;\ a_i \neq b_i\}$. Potem velja, da ima zaporedje z na mestu l različen bit ali od x ali od y. V nasprotnem primeru bi imeli vsi trije elementi enak bit na mestu l, kar vemo, da ne drži. Zato velja naslednja veriga neenakosti

$$\begin{aligned} d(x,y) &= |\{i :\ a_i \neq b_i\}| \\ &\leq |\{j :\ a_j \neq c_j\} \cup \{k :\ b_k \neq c_k\}| \\ &\leq |\{j :\ a_j \neq c_j\}| + |\{k :\ b_k \neq c_k\}| \\ &= d(x,z) + d(z,y), \end{aligned}$$

kar smo želeli dokazati. □

Na primer, zaporedji $10000, 10011 \in \mathbb{F}_2^5$ se razlikujeta v dveh bitih, in sicer na četrtem in petem mestu, zato je njuna Hammingova razdalja enaka

$$d(10000, 10011) = 2.$$

Na poseben način bomo poimenovali razdaljo do zaporedja $00 \dots 00$.

Definicija 4. ***Težo*** *zaporedja $w \in \mathbb{F}_2^n$, ki jo označimo z $|w|$, definiramo kot Hammingovo razdaljo med zaporedjem, ki ima vse člene 0, in zaporedjem w, torej*

$$|w| = d(0, w).$$

2.3 Minimalna razdalja

Minimalna razdalja koda je najmanjša možna razdalja med dvema različnima elementoma koda. Koncept minimalne razdalje je pomemben, ker bo igral vlogo pri številu napak, ki jih lahko kod zazna ali popravi. Večja kot je minimalna razdalja, več jih lahko popravi.

Definicija 5. *Naj bo $C \subset \mathbb{F}_2^n$ kod.* ***Minimalna razdalja*** *koda C je najmanjša možna razdalja d med poljubnima različnima elementoma $x, y \in C$, torej*

$$d = \min\{d(x,y) :\ x \neq y,\ x, y \in C\}.$$

Rečemo, da lahko kod $C \subset \mathbb{F}_2^n$ *popravi* m napak, če lahko prejemnik sporočila ob predpostavki, da se je zgodilo največ m napak, točno določi, katero sporočilo je bilo poslano. Podobno pravimo, da lahko kod $C \subset \mathbb{F}_2^n$ *zazna* l napak, če lahko prejemnik sporočila ob predpostavki, da se je zgodilo največ l napak, določi, da se je pri prenosu sporočila zgodila napaka.

Izrek 2. *Naj bo $C \subset \mathbb{F}_2^n$ kod z minimalno razdaljo d. Največje število napak, ki jih kod C lahko zazna, je $d-1$. Največje število napak, ki pa jih lahko popravi, je $\left\lfloor \frac{d-1}{2} \right\rfloor$.*

Dokaz. Najprej dokažimo, da lahko kod popravi $\left\lfloor \frac{d-1}{2} \right\rfloor$ napak. Predpostavimo, da je napak največ $\left\lfloor \frac{d-1}{2} \right\rfloor$. Radi bi pokazali, da lahko vsakemu zaporedju z, ki ima največ toliko napak, priredimo enoličen element koda, ki je temu sporočilu najbližji. To sporočilo je tisto, ki ga je pošiljatelj poslal, preden je prišlo v kanal.

Enoličnost takega elementa iz koda lahko dokažemo s protislovjem. Recimo da za dva različna elementa x, y v kodu velja

$$d(x,z) \leq \left\lfloor \frac{d-1}{2} \right\rfloor \quad \text{in} \quad d(y,z) \leq \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Po definiciji minimalne razdalje velja $d \leq d(x,y)$. Dobimo naslednjo verigo neenakosti

$$\begin{aligned} d &\leq d(x,y) \\ &\leq d(x,z) + d(z,y) \\ &\leq \left\lfloor \frac{d-1}{2} \right\rfloor + \left\lfloor \frac{d-1}{2} \right\rfloor \\ &\leq \frac{d-1}{2} + \frac{d-1}{2} \\ &= d-1. \end{aligned}$$

Sledi, da velja $d \leq d-1$, kar je protislovje, zato obstaja največ en element koda C, ki je zaporedju z najbližji.

Naslednje, kar bomo pokazali, je, da lahko ob predpostavki največ $d-1$ napak, zaznamo, ali se je zgodila napaka.

Recimo, da prejemnik prejme sporočilo $z \in \mathbb{F}_2^n$ in ve, da se je zgodilo največ $d-1$ napak. Če zaporedje z ni v kodu, prejemnik ve, da se je zgodila napaka. Če pa element z je v kodu, pa je nemogoče, da je bilo dejansko poslano neko drugo sporočilo iz koda, saj bi potem razdalja med poslanim in prejetim sporočilom bila manjša ali enako $d-1$, kar je manj od minimalne razdalje. Idejno to preprosto pomeni, da ne moremo „skočiti“ od enega kodnega sporočila do drugega.

□

2.4 Linearni kodi

Sedaj bomo definirali posebne vrste kodov, ki jih bomo obravnavali do konca članka.

Definicija 6. ***Linearen kod*** *$C \subset \mathbb{F}_2^n$ je kod z lastnostjo, da za poljubna $x, y \in C$ velja $x + y \in C$.*

Definicija pravi, da če dva elementa iz koda C seštejemo, potem bo tudi njun seštevek element kode. Njihova prednost je, da lahko iz majhnega števila baznih elementov sestavimo poljubni element koda z uporabo seštevanja.

Primer linearnega koda je $C \subset \mathbb{F}_2^4$ z elementi $C = \{0000, 0011, 1100, 1111\}$. Če seštejemo elementa $\{0011\}$ in $\{1100\}$, dobimo $\{1111\}$, ki je v kodu.

Primer koda, ki ni linearen, je $C = \{10, 01\}$, saj elementa $10 + 01 = 11$ ni v tem kodu.

Izkaže se, da pri linearnem kodu za določitev minimalne razdalje ni potrebno primerjati vsakega elementa z vsakim, temveč je dovolj primerjati en element z vsemi.

Izrek 3. *Naj bo $C \subset \mathbb{F}_2^n$ linearen kod. Potem je minimalna razdalja koda C enaka*

$$d = \min\{|z| : \ z \in C, \ z \neq 0\}.$$

Dokaz. Po definiciji obstajata različna elementa $u = u_1u_2 \cdots u_n$ in $v = v_1v_2 \cdots v_n, \in C$, za katera velja $d(u,v) = d$. Prištejemo elementoma u in v poljuben element $w = w_1w_2 \ldots w_n \in \mathbb{F}_2^n$ in izračunajmo $d(u+w, v+w)$.

Opazimo, da za poljubno koordinato i velja $u_i = v_i$, če in samo če je $u_i + w_i = v_i + w_i$, zato sta množici $\{i : \ a_i \neq b_i\}$ in $\{j : \ a_j + w_j \neq b_j + w_j\}$ enaki in po definiciji velja $d(u,v) = d(u+w, v+w)$.

Če izberemo $w = v$, vemo, da je $u + v$ element C, saj je kod C linearen. Vemo torej naslednje

$$d = d(u,v) = d(u+v, v+v) = d(u+v, 0).$$

Sklepamo, da je minimalna razdalja enaka teži elementa $u + v$ iz C, kar smo želeli dokazati. □

Za primer vzamimo naslednji linearen kod $C \subset \mathbb{F}_2^3$

$$C = \{000000, 111111, 111000, 000111\}; \quad |111000| = 3.$$

Minimalna razdalja je po izreku 3 enaka najmanjši teži elementa koda C. Hitro preverimo, da je najmanjša teža elementa koda C enaka 3, zato je minimalna razdalja koda C enaka 3.

2.5 Dimenzija

Izkaže se, da linearni kodi ne morejo imeti poljubne velikosti, ampak da je njihova velikost vedno potenca števila 2.

Izrek 4. *Naj bo $C \subset \mathbb{F}_2^n$ linearni kod. Potem velja $|C| = 2^k$ za neko naravno število $0 \leq k \leq n$.*

Dokaz. Definirajmo kod $C' \subset \mathbb{F}_2^{n-1}$ kot kod, ki ga sestavljajo zaporedja iz prvih $n-1$ bitov koda C. Kod C' je linearen, saj ima enake lastnosti kot kod C, samo da pozabimo na zadnji bit. Na C' lahko gledamo kot sliko preslikave $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$, ki slika element $(a_1, a_2, \ldots, a_{n-1}, a_n)$ v element $(a_1, a_2, \ldots, a_{n-1})$. Obravnavamo lahko dve možnosti.

1. Če je zožitev preslikave π na C injektivna, potem velja $|C'| = |C|$.

2. Zožitev preslikave π na C ni injektivna. V kodu C sta potem po definiciji različna elementa u in v, za katera velja $u = t_1 t_2 \ldots t_{n-1} 0$ in $v = t_1 t_2 \ldots t_{n-1} 1$. Ker je C linearen kod je njuna vsota $u + v = 00 \cdots 001$ v C. Po definiciji C' za vsak $w \in C'$ obstaja vsaj en element iz C, ki ga π slika v w. Velja tudi, da za vsak $w \in C'$ obstajata največ dva elementa iz C, ki se slikata v w, saj je prvih $n-1$ bitov že določenih, zadnji pa je lahko ali 0 ali 1.

   Trdimo, da za vsak $w \in C'$ obstajata natanko dva elementa $z_1, z_2 \in C$, ki ju π slika v w. V kodu C je element $00 \cdots 001$ in kod C je linearen. Če torej za $z \in C$ velja $\pi(z) = w$, potem je drugi element iz C, ki se slika v w, enak $z + 00 \cdots 001$.

   Zato je v kodu C natanko dvakrat toliko elementov kot v kodu C'.

Vemo torej, da je moč množice C' enaka

$$|C'| = \begin{cases} |C|; & \pi|_C \text{ je injektivna,} \\ \frac{1}{2}|C|; & \pi|_C \text{ ni injektivna.} \end{cases}$$

Postopek lahko ponovimo na kodu C', saj je kod C' linearen in ima dolžino $n-1$. Nato postopek ponovimo še $(n-1)$-krat. V zadnjem koraku dobimo kod, ki je enak $\{0\}$ ali $\{0, 1\}$. Moč teh množic je enaka 1 ali 2, obe sta potenci 2, v vsakem koraku pa smo ali obdržali moč prejšnje množice ali pa jo razpolovili. Zato je moč prvotnega koda C enaka potenci števila 2.

□

Definicija 7. *Naj bo $C \subset \mathbb{F}_2^n$ linearen kod. Vemo, da je število elementov v kodu $C = 2^k$ za nek $k \in \mathbb{N}_0$. Eksponentu k pravimo **dimenzija** koda C.*

Za poljuben linearen kod definirajmo dimenzijo, ki je enaka eksponentu v potenci števila 2, ki nastopa v njeni moči. Lahko jo interpretiramo tudi kot število mest, ki jih zavzame sporočilo pri prenosu. Za primer lahko vzamemo naslednji linearen kod

$$C \subset \mathbb{F}_2^n, \quad C = \{0000, 0011, 1100, 1111\}.$$

Število elementov v C je 4, torej je dimenzija enaka 2.

Definicija 8. *Linearnemu kodu $C \subset \mathbb{F}_2^n$ z minimalno razdaljo d in dimenzijo k pravimo $[n, k, d]$-kod.*

3 Primeri kodov

3.1 Sodi kod

Definicija 9. ***Sodi kod*** *$E \subset \mathbb{F}_2^n$ je kod, ki vsebuje vsa zaporedja iz $\mathbb{F}_2^n$ s sodo težo, torej*

$$E = \{u \in \mathbb{F}_2^n : \ |u| \text{ je sodo število}\}.$$

Izrek 5. *Za vsak $n \in \mathbb{N}$ je sodi E kod linearen kod.*

Dokaz. Naj bosta $x, y \in E$ poljubna elementa. Želimo, dokazati, da je $x+y$ v E, kar po definiciji pomeni, da je $|x+y|$ sodo število.

Označimo število vseh mest v zaporedju, kjer ima zaporedje x bit 1 in zaporedje y bit 0, z a ter označimo število mest, kjer ima x bit 0 in y bit 1, z b. Nato dobimo

$$|x| = a + c,$$

$$|y| = b + c,$$

kjer c označuje število mest, na katerih imata x in y hkrati bit 1. Obe števili $|x|$ in $|y|$ sta sodi. Preštejemo število enic v $x + y$. Ugotovimo, da je to natanko $|x + y| = a + b$. To velja, ker se na vseh c mestih, kjer imata oba x in y bit 1, tisto mesto sešteje v 0.

Parnost števila $a+b$ je enaka parnosti $a+b+2c = (a+c)+(b+c) = |x|+|y|$, ki pa je vsota dveh sodih števil po predpostavki in zato sodo število. Zato velja, da je $|x + y|$ sodo število s čimer smo pokazali, da je sodi kod E linearen kod. □

Primer sodega koda je $C \subset \mathbb{F}_2^3$,

$$C = \{000, 011, 101, 110\}.$$

Za $n \geq 2$ velja, da je minimalna razdalja sodega koda enaka $d = 2$, ker vedno obstaja element teže 2. Dimenzija k pa je za $n \geq 1$ enaka $n - 1$. To lahko vidimo, tako da pogledamo preslikavo

$$f \colon \mathbb{F}_2^n \to \mathbb{F}_2^n, \quad u \to u + 100 \ldots 00.$$

Opazimo, da je preslikava f bijektivna in da slika elemente s sodo Hammingovo težo v elemente z liho Hammingovo težo, in obratno.

Vemo torej, da je za $n \geq 2$ sodi kod vedno $[n, n-1, 2]$-kod, kar z uporabo izreka 2 pravi, da lahko vedno zaznamo največ eno napako, popraviti pa jih ne moremo.

3.2 Hammingov kod

Hammingov kod ima sedem bitov. Prvi štirje biti v njegovih zaporedjih so poljubni, naslednji trije pa so biti za določitev parnosti. Poljuben element H je oblike $d_1d_2d_3d_4p_1p_2p_3$, kjer so zadnji trije biti podani z naslednjimi enačbami

$$\begin{aligned} p_1 &= d_1 + d_2 + d_4, \\ p_2 &= d_1 + d_3 + d_4, \\ p_3 &= d_2 + d_3 + d_4. \end{aligned}$$

Pokazali bomo, da je Hammingov kod linearen kod, in določili njegovo minimalno razdaljo in dimenzijo.

Izrek 6. *Hammingov kod je linearen kod.*

Dokaz. Naj bosta $x = a_1a_2a_3a_4p_1p_2p_3 \in H$ in $y = b_1b_2b_3b_4q_1q_2q_3 \in H$ poljubna elementa. Želimo pokazati, da je $x + y$ element H. Prvi štirje biti vsote $x + y$ so enaki $a_1 + b_1, \ldots, a_4 + b_4$ in so lahko poljubni. Dejstvo, da so zadnji trije primerne oblike, pa je posledica komutativnosti in asociativnosti seštevanja na $\{0, 1\}$. Na primer, bit na petem mestu vsote $x + y$ je enak

$$\begin{aligned} p_1 + q_1 &= (a_1 + a_2 + a_4) + (b_1 + b_2 + b_4) \\ &= (a_1 + b_1) + (a_2 + b_2) + (a_4 + b_4), \end{aligned}$$

kar je natanko enako vsoti prvega, drugega in četrtega mesta vsote zaporedji $x + y$. Sklepanje ponovimo še za šesti in sedmi bit in ugotovimo, da je $x + y$ po definiciji element H. □

Izrek 7. *Hammingov kod H je $[7, 4, 3]$-kod.*

Dokaz. Po definiciji je $n = 7$. Dimenzija k je enaka 4, ker so prvi štirje biti poljubni, zadnji trije pa so točno določeni glede na prve štiri, torej je vseh elementov koda natanko $2 \cdot 2 \cdot 2 \cdot 2 = 16 = 2^4$.

Vemo, da je H linearen kod, zato lahko minimalno razdaljo d določimo z najmanjšo težo vseh 16 elementov koda. Vemo da je d največ 3, ker imamo v H element 1000110. Preveriti moramo vse elemente v kodu, ki imajo na prvih štirih mestih največ dva bita enaka 1. Ugotovimo, da je teža vseh takšnih elementov 3 ali 4. Zato je minimalna razdalja d natanko 3. □

Zadnji presenetljiv rezultat, ki nakazuje na uporabnost Hammingovega koda, je, da lahko H vedno popravi največ eno napako. To se na prvi pogled zdi presentetljivo, ker nismo niti podvojili števila vseh bitov prvotnega sporočila, ki je dolgo štiri bite. Velja namreč, da prvi štirje biti predstavljajo sporočilo, zadnji trije pa so dodatek.

Izrek 8. *Hammingov kod H lahko zazna 2 napaki in popravi 1.*

Dokaz. Uporabimo izrek 2 in dejstvo, da je minimalna razdalja $d = 3$, zato je $d-1 = 2$ in $\left\lfloor \frac{d-1}{2} \right\rfloor = 1$. □

Sedaj lahko poskusimo rešiti problem iz uvoda. Želimo torej poslati sporočilo štirih bitov. Naj bo verjetnost, da se pri prenašanju sporočila en bit pokvari, enaka p in predpostavimo, da je verjetnost neodvisna od drugih bitov. Izračunajmo, kolikšna je verjetnost, da pravilno prenesemo sporočilo, če sporočilo prenesemo v Hammingovem kodu.

Verjetnost, da je celotno sporočilo brez napak, je $(1-p)^7$, kar je manj kot $(1-p)^4$ za sporočilo brez dodatka. Vendar so zdaj sprejemljiva tudi vsa sporočila, ki imajo natanko eno napako, ker jo lahko popravimo. Verjetnost da se bit pokvari pri poljubnem mestu je $p(1-p)^6$, torej je skupna verjetnost pravilnega sporočila enaka

$$(1-p)^7 + 7p(1-p)^6.$$

Če vstavimo $p = 4\%$ kot v uvodu, sedaj verjetnost, da lahko prenesemo pravilno sporočilo, naraste na kar 97%. Torej nam je uspelo z uporabo Hammingovega koda povečati verjetnost pravilno poslanega sporočila iz 85% na 97%. Verjetnost je še veliko boljša za manjše p.

4 Zaključek

Predstavili smo problem napak pri prenašanju podatkov, sestavljenih iz zaporedij bitov. Definirali smo koncept koda in linearnega koda. Nato smo definirali dimenzijo koda, ki meri velikost dejanskega sporočila in minimalne razdalje, od katere je odvisno število napak, ki jih lahko zaznamo ali popravimo. Na koncu smo predstavili sodi kod in Hammingov kod. Slednji lahko zmeraj popravi eno napako, kljub temu, da niti ne podvojimo velikost sporočila.

Literatura

[1] J. Top, *Security & Codes*, dostopno na `https://www.rug.nl/staff/steffen.muller/security-and-codes-updated.pdf`