Teorija kodiranja in kriptografija

Osnovne definicije. Kod C nad končno abecedo Σ je končna podmnožica Σ^*. Množico Σ imenujemo kodna abeceda, elemente C kodne besede in elemente Σ kodni simboli. Kod C je bločni, če za nek n velja $C \subset \Sigma^n$, torej vse besede so enako dolge. Razmaknjenost koda C je minimalna razdalja med dvema različnima besedama.

(n,M,d) kod je kod z M besedami dolžine n in razmaknjenostjo d. Kod z razmaknjenostjo d odkrije $d-1$ napak in popravi $\lfloor \frac{d-1}{2} \rfloor$ napak.

Dvojiški simetrični kanal. Pri pošiljanju se dolžina binarne besede ne spremeni, na vsakem mestu pa se bit pokvari z enako verjetnostjo $p < 1/2$.

Postopek dekodiranja. Pravilo najmanjše napake. Pri prejetem $y \in \Sigma^n$ je x tista beseda iz C, da je $P(x|y)$ največja. Pravilo največje verjetnosti. x je tista beseda pri kateri je $(y|x)$ največja. Če so vse besede enako verjetne dajeta pravili enak rezultat. Pravilo najbližjega soseda. y dekodiramo v tisto besedo x kjer je $d(x,y)$ najmanjša. V BSC s $p < 1/2$ sta pravilo največje verjetnosti in pravilo najbližjega soseda ekvivalentni.

Malo verjetnosti $P(x|y) = \frac{P(y|x)P(x)}{P(y)}$. $P(y) = \sum_{c \in C} P(y|c)P(c)$. $P(y|x) = p^{d(x,y)}(1-p)^{n-d(x,y)}$.

Linearni kodi. Kod je linearen, če je vektorski podprostor Σ^n, torej zaprt za seštevanje in množenje s skalarjem. Označimo [n,k,d] kod je kod z besedami dolžine n, ki je k dimenzionalen vektorski prostor nad Σ z razmaknjenostjo d. Če je kod nad $GF(q)$ potem $M = q^k$. Generatorska matrika je matrika dimenzije $k \times n$, ki ima v vrsticah linearno neodvisne kodne besede. Matrika je v standardni obliki, če je na začetku $k \times k$ identiteta. Kodiramo tako, da besedilo dolžine k pomnožimo z matriko: $s \cdot G$. V standardni obliki se besedilo ohrani doda se le nekaj solate na konec.

$C^\perp = \{x \in \Sigma^n, C \cdot x = \{0\}\}$ je dualni kod koda C. Njegovo generatorsko matriko označimo s H in jo imenujemo nadzorna matrika, in je dimenzije $n - k \times n$. Velja $GH^\top = 0$ in $x \in C \iff Hx^\top = 0$. Če je G v standardni obliki $[I_k|A]$ je $H = [-A^\top|I_{n-k}]$ ena izmed nadzornih matrik te matrike.

Ekvivalentni kodi. Gaussove operacije po vrsticah koda ne spremenijo. Menjavanje stolpcev in množenje stolpcev s skalarjem pa spremeni kod v ekvivalenten kod, potem lahko npr. zračunamo nadzorno matriko, ki jo pretvorimo z enakimi operacijami nazaj v nadzorno matriko originalnega koda.

Dekodiranje s sindromi. Za vse možne napake (primerne teže) izračunamo sindrome: $He^\top$. Za dano prejeto besedo y prav tako izračunamo njen sindrom $Hy^\top$ in vidimo s katero napako se ujema (ali pa je 0, kar pomeni da smo dobili veljavno besedo, ali pa se ne ujema z nobeno, kar pomeni da te napake ne moremo popraviti). Nato od prejetega sporočila odštejemo to napako.

Razmaknjenost linearnega koda C je največji tak d, da je vsakih $d-1$ stolpcev nadzorne matrike H še linearno neodvisnih. Ekvivalentno, d je najmanjša teža neničelne besede v C.

Meje za kode. Naj bo $A_q(n,d) = \max\{M; \exists (n,M,d)\text{-kod nad } GF(q)\}$. $A_q(n,1) = q^n$ $A_q(n,2) = q^{n-1}$. Kod je popoln če dosega Hammingovo mejo.
Hammingova meja: $A_q(n,d) \leq \frac{q^n}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k}(q-1)^k}$. Singeltonova meja: $A_q(n,d) \leq q^{n-d+1}$.
Gilbert-Varshamova meja: $A_q(n,d) \geq \frac{q^n}{\sum_{k=0}^{d-1} \binom{n}{k}(q-1)^k}$. Linearni kod lahko popravi največ $\lfloor \frac{n-k}{2} \rfloor$ napak.

Ciklični kodi. [n,k,d]-kod je cikličen, če je linearen in vsebuje vse cikične pomike vseh besed. Ciklični pomik je množenje s t v $(GF(q)[t])/(t^n - 1)$ in vsak cikličen kod ustreza nekemu idealu, ki je glavni ($g(t)$). Torej $g(t)$ deli $t^n - 1$. Baza koda $\{g(t), tg(t), \ldots, t^{k-1}g(t)\}, k = n - \deg(g)$.

Reed-Salomonovi kodi. β primitivni element $GF(2^k)$. $RS(n,k)$ je cikličen linearen kod dolžine $n = 2^r - 1$ dimenzije $k = n - \delta + 1$ nad $GF(2^r)$ generiran s polinomom $g(t) = (t-\beta)(t-\beta^2)\cdots(t-\beta^{\delta-1})$. Za RS-kode velja, da je razmaknjenost $d = n - k + 1 = \delta$. RS kodi dosežejo Singeltonovo mejo – popravijo največ napak glede na število dodanih bitov.

Shanonova teorija. Nope.