7. fejezet

Kódoláselmélet

Huffman-kód, hibajavító kódok. Véges testek konstrukciója. Reed-Solomon kód és dekódolása.

7.1. A kódoláselmélet alapfogalmai

Az információról alkotott intuitív fogalmak nyomán számos definíció született – mi válasszuk azt, miszerint az információ *új ismeret*. Mérése a Shanon által bevezetett *bizonytalanság* segítségével történik.

7.1.1. Definíció (Entrópia). *Legyen egy információforrás által kibocsátott üzenetek száma n, az összes különböző üzenet pedig: $a_1, \ldots, a_m$ ($n \geq m \in \mathbb{N}^+$). Tegyük fel, hogy minden a_i üzenet k_i-szer fordul elő, és jelölje az a_i üzenet relatív gyakoriságát: $p_i = \frac{k_i}{n}$.*

Az a_i üzenet egyedi információtartalma $I_i = -\log_r p_i (1 < r \in \mathbb{R})$, az információforás entrópiája pedig $H_r(p_1, \ldots, p_m) = -\sum_{i=1}^{m} p_i \log_r p_i$.

Megjegyzés. Amennyiben a fenti logaritmus alapja $r = 2$, akkor az információ egységét *bit*nek nevezzük. Ilyen kor általában elhagyjuk a log alapjának jelölését.

7.1.2. Tétel. *Bármilyen eloszláshoz tartozó entrópiára $H_r(p_1, \ldots, p_m) \leq \log_r m$, és egyenlőség pontosan akkor teljesül, ha $p_1 = p_2 = \ldots = p_m = \frac{1}{m}$.*

Az átlagos információtartalom maximuma tehát $\log m$ bit.

7.1.1. Kódolások fajtái

A kódolás legáltalánosabban az üzenetek halmazának egy másik halmazba való leképezését jelenti (célja általában az információ hordozhatóvá tétele). Ha a leképezés injektív, akkor a kódolás *felbontható*, különben *veszteséges*.

A kódolások fajtái között megkülönböztetünk *betűnkénti*, illetve *szótár*kódokat attól függően, hogy a meglévő jelsorozatot milyen módon képezzük le a kódolás során.

A kódolásoknak az üzenet továbbíthatóságán túl még több célja lehet: az átvitel gazdaságossá tétele (*gazdaságos kódolás*), az átviteli hibák kivédése (*hibakorlátozó kódolás*), esetleg digitális aláírás vagy az üzenet titkosítása.

7.1.3. Definíció (Betűnkénti kódolás). *Legyen A és B két véges, nem üres ábécé. Ekkor betűnkénti kódolás egy $\varphi : A \to B^*$ leképezés. A leképezés természetesen kiterjeszthető $\psi : A^* \to B^*$ leképezéssé.*

A felbonthatóság érdekében általában feltesszük, hogy $\varphi : A \to B^+$ és injektív.

7.1.4. Definíció (Prefix, infix, szuffix). *Legyenek α, β és γ az A ábécé feletti szavak. Ekkor az $\alpha\beta\gamma$ szónak α prefixe, β infixe, γ pedig szuffixe.*

Az üres szó, illetve önmaga minden szónak triviális prefixe, infixe, illetve szuffixe. α-nak valódi prefixe, infixe, illetve szuffixe olyan prefix, infix, illetve szuffix, amely nem egyezik meg α-val.

7.1.5. Definíció (Prefixmentes halmaz). *Szavak egy halmaza prefixmentes, ha nincs benne két olyan különböző szó, amelyek közül az egyik a másiknak prefixe.*

7.1.6. Definíció (Prefix kód, egyenletes kód és vesszős kód). *Prefix kódolás egy φ injektív leképezés, melynek értékkészlete prefixmentes.*

Az egyenletes kód olyan kód, melynek kódszavai azonos hosszúságúak.

Vesszős kódnak nevezünk egy kódot, ha van olyan $\vartheta \in B^+$ szó, amely minden kódszónak szuffixe, de egynek sem infixe.

Megjegyzések. Az egyenletes kód egyben prefix kód. A prefix, egyenletes, illetve vesszős kódok triviálisan felbonthatók.

7.1.7. Definíció (Kódfa). *A betűnkénti kódolás szemléltető eszköze a kódfa. Ez a kódolás értékkészlete összes prefixeinek Hasse-diagramja (a „prefixe” részbenrendezési relációra). Az élek címkézése: legyen egy β-ból α-ba vezető él címkéje b, ha $\beta = \alpha b$.*

7.2. Huffman-kód

A Huffman-kód optimális kód, célja, hogy a lehető legkevesebb jellel írjuk le a kódolni kívánt információt.

7.2.1. Definíció (Optimális kód). *Legyen a kódolás során az $\{a_1, \ldots, a_n\}$ betűk eloszlása $p_1, \ldots, p_n$, és a_i kódjának hossza l_i. Ha egy kód $\bar{l} = \sum_{i=1}^{n} p_i l_i$ átlagos hossza minimális, akkor optimális kódról beszélünk.*

7.2.2. Tétel (Shannon tétele zajmentes csatornára). *Legyen egy betűnkénti kódolásban a kódábécé elemeinek száma r. Ha a betűnkénti kódolás felbontható, akkor $H_r(p_1, \ldots, p_n) \leq \bar{l}$, ahol $\bar{l}$ a kód átlagos hossza, H_r pedig az eloszlás entrópiája.*

7.2.3. Tétel (Shannon-kód létezése). *Az előző tétel jelöléseivel $n > 1$ esetén létezik olyan prefix kód, melyre $\bar{l} < H_r(p_1, \ldots, p_n) + 1$.*

7.2.1. A Huffman-kód konstrukciója

Huffman-kódot (és így optimális kódot) állíthatunk elő egy kódolandó szóhalmazhoz a következő lépések segítségével (legyen n a kódolandó betűk száma, r pedig a kódábécé elemszáma):

1. rendezzük a betűket relatív gyakoriságuk szerinti csökkenő sorrendben,
2. legyen $t = ((n-2) \bmod (r-1)) + 2$,
3. első lépésben helyettesítsük a legkevésbé gyakori t betűt egy új betűvel, melyhez relatív gyakoriságként az elhagyott betűk relatív gyakoriságainak összegét rendeljük, és ezt helyezzük el a sorozatban,
4. ismételjünk az előzőhöz hasonló redukciót úgy, hogy minden alkalommal r betűt hagyunk el és helyettesítünk a sorozat végéről – ezután a redukált ábécé legfeljebb r betűt tartalmaz,
5. ezután rendeljünk miden összevont betűhöz egy elemet a kódábécéből,
6. végül az összevonások mentén „visszafelé” haladva az összevont betű kódjához fűzzünk hozzá még egy jelet a kódábécéből,
7. folytassuk a felbontást addig, amíg vissza nem kapjuk az eredeti ábécét!

Megjegyzés. A Huffman-kódolt szöveggel együtt általában továbbítanunk kell a kódszótárat is, ami plusz költséget jelent.

7.3. Hibakorlátozó kódok

A hibakorlátozó kódok célja a csatorna esetleges hibáinak kiküszöbölése. Megkülönböztetünk *hibajelző* és *hibajavító* kódokat.

7.3.1. Alapfogalmak

7.3.1. Definíció (Kód távolsága és súlya). *A kódábécé két egyforma hosszúságú szavának $d(u, v)$ távolsága az azonos pozícióban lévő, különböző jelek száma. Kód $d(C)$ távolsága a kód szópárjai távolságának minimuma.*

Ha a kódábécé additív Abel-csoport, akkor a kódábécé egy u szavának $w(u)$ Hamming-súlya a nullától különböző jegyeinek száma, a kód $w(C)$ súlya pedig a nem nulla kódszavak súlyainak minimuma.

Megjegyzés. A Hamming-távolság rendelkezik a távolság szokásos tulajdonságaival, azaz

- $d(u, v) \geq 0$,
- $d(u, v) = 0 \Leftrightarrow u = v$,
- $d(u, v) = d(v, u)$ (szimmetrikus),
- $d(u, z) \leq d(u, v) + d(v, z)$ (háromszög-egyenlőtlenség).

7.3.2. Definíció (Hibajelző kód, hibajavító kód). *Egy kódot* t-hibajelző*nek* (t-hibajavító*nak) nevezünk, ha minden esetben jelez (illetve a hiba biztosan javítható), ha az elküldött kódszó legfeljebb t helyen változik meg.*

Egy kód pontosan t-hibajelző (pontosan t-hibajavító), ha t-hibajelző (t-hibajavító), és nem $t + 1$-hibajelző ($t + 1$-hibajavító).

7.3.3. Tétel (Hibajelzés, hibajavítás és a Hamming-távolság). *Egy C kód akkor és csak akkor t-hibajelző, ha $t < d(C)$, illetve akkor és csak akkor pontosan t-hibajelző, ha $t = d(C) - 1$.*

Hasonlóan egy C kód akkor és csak akkor t-hibajavító, ha $t < \frac{d(C)}{2}$, illetve akkor és csak akkor pontosan t-hibajavító, ha $t = \lfloor \frac{d(C)-1}{2} \rfloor$.

Ismétléses kód. Az ismétléses kód olyan kód, melyben minden bitet páratlan sokszor elküldünk egymás után. Ekkor az egy bitet jelző bitsorozatban valamelyik bit többször szerepel, ekként értelmezzük a sorozatot. A kódnak elméleti jelentősége van, mivel a többszörözés növelésével a döntési hiba 0-hoz tart.

7.3.2. Paritáskódok

7.3.4. Definíció (Paritásbites kód). *A paritásbites kód olyan kód, mely a (tegyük fel, azonos n hosszú) kódszavakat kiegészíti egy $n+1$-edik* paritásbit*tel úgy, hogy a paritásbit értéke* 0*, ha a bitsorozatban az* 1*-esek száma páratlan, különben* 1 *(vagy fordítva, de a kódolás során következetesen kell eljárni).*

Megjegyzés. A paritásbites kód pontosan 1-hibajelző.

7.3.5. Definíció (Kétdimenziós paritáskód). *Legyenek az üzenetek n bites szavak. Egészítsünk ki minden kódszót egy paritásbittel páratlan paritásúra, és rendezzünk m ilyen kódszót egymás alá! Írjuk minden bitoszlop aljára az oszlop paritásbitjét páros paritás szerint!*

Megjegyzés. A kétdimenziós paritáskód pontosan 1-hibajavító egy $(m+1)(n+1)$ blokkra nézve.

7.3.3. Lineáris kód

7.3.6. Definíció (Lineáris kód). *Ha K test, akkor a K elemeiből képzett rendezett n-esek a komponensenkénti összeadással, illetve az ugyanazzal az elemmel való szorzással lineáris teret alkotnak. Ennek bármely alterét lineáris kódnak nevezzük.*

Megjegyzés. A paritásellenőrző kód párosra való kiegészítéssel lineáris.

A lineáris kódok alapfogalmai

7.3.7. Definíció (Generátormátrix, ellenőrző mátrix). *A K véges test feletti $[n,k]$ lineáris kódnál, ha a kódolási eljárás $K^k \to C (C \subset K^n)$ lineáris leképezés, akkor a leképezés mátrixát generátormátrixnak nevezzük.*

A dekódolásra ekkor használható egy $H : K^n \to K^k$ szürjektív lineáris leképezés, melynek magja C. A leképezés mátrixa az ellenőrző mátrix.

Ellenőrzés ellenőrző mátrixszal. Ha $v \in K^n$ fogadott szó, akkor az $s = Hv$ szindróma pontosan akkor 0, ha v kódszó.

Szindróma-dekódolás. Ha a fenti jelölésekkel $s \in K^{n-k}$, akkor legyen $e(s)$ a $\{v : Hv = s\}$ halmaz egy minimális súlyú vektora – ez a *mellékosztályvezető*. c kódszó és v fogadott szó esetén $e = v - c$ a hiba. Tegyük fel, hogy a hibavektor súlya kisebb, mint $\frac{d}{2}$, azaz a hiba javítható! Ekkor $He(s) = s = Hv = He$, melyből a Hamming-súly tulajdonságai alapján következik, hogy $e = e(s)$.

A hiba javítása tehát $c = v - e(s)$ számítással javítható.

7.3.8. Tétel (Singleton-korlát). *Ha egy adott C kód, mely egy q elemű ábécé betűiből álló n hosszú kódszavakat tartalmaz, és $d(C) =: d$, akkor minden kódszóból elhagyva $d-1$ betűt ugyanazon pozíciókról, a kapott halmaz kód marad. Ekkor a kódszavak száma $|C| \leq q^{n-d+1}$.*

Következmény. Lineáris kód esetén a Singleton-korlátból adódik a $d \leq n - k + 1$ összefüggés. Ha egyenlőség áll fenn, a kódot *maximális távolságú szeparábilis kód*nak (MDS) nevezzük. Az elnevezést az indokolja, hogy a kódolást ekkor választhatjuk úgy, hogy a kódolt szó betűi a kódban rögzített helyeken álljanak, így a kiolvasás egyszerű.

CRC (Cyclic Redundancy Check)

A CRC egy gyakorlatban széles körben használt, hibajelző lineáris kód. Az által használt test kételemű (pl. $\{0, 1\}$), és erősen támaszkodik a rendezett n-esek és polinomok közötti megfeleltetésre (ahol az n-esek elemei rendre a polinom egyre magasabb fokú együtthatóit jelölik).

A CRC nem a fent bemutatott szindróma-módszerrel, hanem annál nagyonbb hatékonysággal működik, azonban hiba javítására nem alkalmas.

A CRC konstrukciója. Legyen n a teljes lineáris tér dimenziója, k bites a kódolandó szó, $m = n-k$! Adott még egy m-edfokú polinom, a *kódpolinom*. Ekkor a CRC-kód a következőképpen áll elő:

1. a kódolandó szó elejére írjunk m darab nullát, és tekintsük a megfelelő polinomot,

2. osszuk el az így kapott polinomot a kódpolinommal,

3. az osztás maradékát írjuk a kiegészített szóban a 0-k helyére!

Így a kódszavakat az jellemzi, hogy oszthatók a kódpolinommal. Ha tehát egy fogadott szó nem osztható a kódpolinommal, akkor az átvitel során hiba keletkezett.

Megjegyzés. A CRC-1 kód kódpolinomja $x + 1$, ami a paritásbites kódolást állítja elő. Ezen kívül még számos, a gyakorlatban elterjedt CRC-kódpolinom van használatban.

A CRC használata. A CRC általában csak hibajelzésre használható fel, és itt is nagy súlyt kell fektetni a generátorpolinom megválasztására. Általában ajánlott, hogy a generátorpolinom konstans tagja ne legyen 0. Ezen kívül más megfontolásokat is figyelembe véve a CRC hatékonysága tovább fokozható (például minden páratlan számú bitet érintő hiba felismerhető).

Hamming-kód

A Hamming-kód egy hiba javítására alkalmas lineáris kód.

Legyen $r \geq 2$ egész szám, $n = 2^r - 1$ és $k = n - r$. Készítsünk egy $r \times n$ méretű mátrixot, melynek minden oszlopában az oszlop számának bináris alakjának számjegyei állnak (a számjegyek a fenti korlátok miatt biztosan elférnek a mátrixban).

Pl. legyen $r = 3 \Rightarrow n = 7$, ekkor :

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Ekkor van $r - 1$ darab olyan oszlop, mely egy kettő hatvány számjegyeit tartalmazza, tehát pontosan 1 darab egyes található benne. Ezek az oszlopok egységmátrixot alkotnak, azaz függetlenek, tehát a mátrix rangja r. Így a mátrix által meghatározott H lineáris leképezés szürjektív.

Legyen C kód azon bináris, n-dimenziós vektorok halmaza, melyekre $Hc = 0$. Ekkor a $k = n - r$ bites kódolandó szavakat egészítsük ki r bittel úgy, hogy a kapott szó eleme legyen C-nek.

Ha pontosan egy hiba lépett fel, akkor a v vett szóval: $s := Hv = He$, így a konstrukció miatt s-et bináris számként értelmezve megkapjuk a hiba pozícióját.

7.3.4. Véges testek konstrukciója

7.3.9. Tétel (A véges testek alaptétele). *Minden véges test elemszáma prímhatvány, ahol a prím a test karakterisztikája. Az azonos (prímhatvány) elemszámú véges testek izomorfak.*

7.3.10. Tétel (Maradékosztályok és véges testek). *Ha p prímszám, akkor $\mathbb{Z}_p$ maradékosztály test.*

...

7.3.5. Reed-Solomon kód

A Reed-Solomon kód maximális távolságú lineáris kód, melyben lehetőség van nagy hatékonyságú kódolásra és dekódolásra. A Reed-Solomon kód változatait alkalmazzák például optikai lemezeken az írási és olvasási hibák javítására. A gyakorlatban kettő hatvány-elemszámú testekkel (pl. K_{2^8}) használják.

Reed-Solomon kód előállítása

7.3.11. Definíció (Reed-Solomon kódolás). *Legyen K véges test, $0 \neq \alpha \in K$, α multiplikatív rendje n, $0 < k < n$! Legyen még $m = n - k$, $g = \prod_{i=1}^{m}(x - \alpha^i)$ generátorpolinom. Ekkor $C = \{ag | a \in K[x], deg(a) < k\}$ halmaz az α által generált Reed-Solomon kód, melynek leképezése $\varphi(a) = ag$.*

Magyarázat. $K[x] \ni x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i)$, mivel $\alpha^i minden 0 \leq i < n$-re különböző elemek, és mindegyik gyöke az $x^n - 1 \in K[x]$ polinomnak, azaz megadják a polinom összes gyökét. A generátorpolinom osztója az $x^n - 1$ polinomnak. $\varphi : K^k \to C$ injektív leképzés, C a K^n k-dimenziós altere.

A Reed-Solomon kód ellenőrző mátrixa. A CRC-kódoláshoz hasonlóan a Reed-Solomon kód esetében is elmondhatjuk, hogy egy v kódszónak akkor és csak akkor osztója g, ha $v \in C$. Ez alapján belátható, hogy $h_{i,j} = \alpha^{ij} (1 \leq i \leq m, 0 \leq j \leq n - 1)$ a kód egy ellenőrző mátrixa.

7.3.12. Tétel (Reed-Solomon kód távolsága). *Reed-Solomon kód távolsága a fenti jelölésekkel: $d = n - k + 1$, azaz a kód maximális távolságú.*

Reed-Solomon kód dekódolása

A Reed-Solomon kód javítása történhet szindróma-dekódolással is, de az alábbi megoldás hatékonyabb.

A fenti jelöléseket egészítsük ki a következőkkel: e legyen a keresett hibavektor, $L(z) = \prod_{e_j \neq 0}(1 - \alpha^j z)$ az ún. hibahelypolinom.

A hibák helye a következő módon határozható meg: ha megkeressük azon α^{-j}-ket, melyek L-nek gyökei, akkor a j-k megadják a hibák pozícióját.

A hibák javításához vezessük be a hibaérték-polinomot:

$$E(z) = \sum_{e_j \neq 0} \alpha^j e_j L_j(z)$$

, ahol $L_j(z) = \frac{L(z)}{1-\alpha^j z}$, ha $e_j \neq 0$. Ennek ismeretében a hibák javíthatók: $e_j = \frac{E(\alpha^{-j})}{\alpha^j L_j(\alpha^{-j})}$. A nevező itt nem nulla, mivel $\alpha^j \neq 0$, illetve $L_i(\alpha^{-j})$ pontosan akkor nem nulla, ha $i = j$.

A fenti polinomok meghatározásának lehetőségét tétel biztosítja a szindróma segítségével.