# KÓDELMÉLET

A kódelmélet területei

1. Titkosítások

   (a) Rejtjelezés (Írás, Rabszolgák, "Shift" kódok, Sándor Mátyás, könyvek, matematikai módszerek)
   Példa: $A$ küldi $B$-nek az $u$ üzenetet:
   $A \xrightarrow{u} B$, de $A$ fél, hogy valaki lehallgatja.. ezért $f(u)$-t küld
   $A \xrightarrow{f(u)} B$ , és $f^{-1}$-t nem ismeri, csak $A$ Sajnos $B$ sem, ezért...
   $B \xrightarrow{g(f(u))} A$
   Legyen $f$ és $g$ olyan, hogy $g \circ f = f \circ g$ és természetesen létezzen az inverzük. Tehát
   $B \xrightarrow{g(f(u))} A$ írható a következő alakban is:
   $B \xrightarrow{f(g(u))} A$
   $A$ ismeri $f^{-1}$-t, ezért $A$ megkapva az $f(g(u))$ üzenetet:
   $f^{-1}(f(g(u))) = g(u)$
   $A \xrightarrow{g(u)} B$
   $g^{-1}(g(u)) = u$ eljutott $B$-hez

   (b) Kódfeltörés (nyilvános algoritmusút lehet csak, több megfejtett szöveg, social engeniring: Kevin Mitnik: The Art of Deception)
   Példa Neptun jelszavakra: Neptunkód, Barát/nő, születési dátum, titok
   Példa jelszavakra: Internet-Worm 432, Elendernél 64 találat
   Virasztó Tamás: Titkosítás és adatrejtés

2. Tömörítések

   (a) Veszteségmentes (exe, RLE, GIF, arj, stb..., redundancia, a tömöríthetőség határa, megfelelő algoritmus/tömörítő, "menetek", idő/hely)

   (b) Veszteséges (hang, kép, skálázható, többszöri ki- és betömörítés, szubjektív minőség)

3. Átvitel közben előforduló hibák kezelése

   (a) Hibafelismerés (alkalmazhatósága, paritásbit, hálózatoknál az elveszett csomagok)

   (b) Hibajavítás (alkalmazhatósága, triplázás, CD Reed-Solomon Code)

Tömörítés+titkosítás+hibakezelés=közlésre kész adat Kódolási alapfogalmak Az üzenetküldés modellje, $q$-adikus alak fogalma

1. Elsődleges közlés átalakítása $q$-adikus alakra

2. $q$-adikus alak átalakítása fizikai jellé

3. Fizikai jelek kiküldése

4. Fizikai jelek fogadása

5. Fizikai jelek átalakítása $q$-adikus alakra

6. $q$-adikus alak átalakítása elsődleges közléssé

Kódolás, dekódolás, modulálás, demodulálás

**Definíció:** A $\mathcal{K} : A^* \to B^*$ hozzárendelést kódolásnak nevezzük.
(Ahol

$$A^* = \bigcup_{i=0}^{\infty} A^i$$

$$\mathcal{K}(a_{i_1}, \ldots, a_{i_k}) = \mathcal{K}(a_{j_1}, \ldots, a_{j_l})$$

**Definíció:** Ha az elsődlegesközléshez tartozó ábécé minden egyes $a_i$ betűjének megfeleltetünk egy-egy $q$-adikus jelsorozatot, akkor betűszerinti kódolásról beszélünk.

**Definíciók:**

- Az $A = (a_1, \ldots, a_n)$ halmaz az *elsődlegesközléshez tartozó ábécé*
- $a_i$ az *elsődlegesközléshez tartozó ábécé szimbóluma*
- $a = a_{i_1} \cdots a_{i_m}$ szimbólumsorozat az *m hosszúságú elsődleges közlés*

- $K = (\alpha_1, \ldots, \alpha_n)$ halmaz röviden *kód*, vagy kódszavak halmaza

- $\alpha_i$ *kódszó*

- $\alpha = \alpha_{i_1} \cdots \alpha_{i_m}$ kódszósorozat *kódolt közlés*

- Egy szimbólumsorozat hossza a bennelévő szimbólumok számával egyenlő, jelölése $|\sigma| = l_\sigma$. Speciálisan $l_i = |\alpha_i|$.

**Definíció:** Egy $K$ bináris kódot felbonthatónak nevezünk, ha bármely$\sigma$ bináris jelsorozat legfeljebb egyféleképpen bontható kódszavak szorzatára.
Példák...
**Tétel:** Ha $K = \{\alpha_1, \ldots, \alpha_n\}$, és $\forall \quad i, j \leq n : \quad l_i = l_j$, akkor a kód felbontható.
**Bizonyítás:** !$\sigma$ tetszőleges bináris jelsorozat és $l_\sigma$ jelölje a hosszát, a kódszavak egyenlő hosszait pedig jelölje $l$! Ha $l|l_\sigma$ akkor egyszer vagy nullaszor felbontható, ha $l \not| l_\sigma$ akkor nullaszor felbontható. Ez kimeríti az összes esetet.
**Definíció:** Egy kódot prefixnek nevezünk, ha egyetlen kódszó sem valódi szelete egy másiknak.
Példák..
**Tétel:** Bármely prefix kód felbontható
**Bizonyítás:** Indirekt úton, ha prefix és létezik két felbontása, akkor nem lehet prefix.
**Tétel:** (Kraft – Mc Millan egyenlőtlenség) Bármely felbontható kódra teljesül

$$\sum_{i=1}^{n} 2^{-l_i} \leq 1$$

**Bizonyítás:** Emeljük $t$. hatványra, ahol $t$ elég nagy legyen ahhoz, hogy az átalakítások után kialakuló

$$\left(\sum_{i=1}^{n} 2^{-l_i}\right)^t \leq (M-1)t + 1$$

egyenlőtlenségben a baloldal és a jobboldal különbségének előjele egyetlen nagyobb értékre se változzon meg.
**Tétel:** Ha az $l_1, \ldots, l_n$ számokra igaz a $\sum_{i=1}^{n} 2^{-l_i} \leq 1$, akkor létezik prefix kód, melyben a kódszavak hosszai $l_1, \ldots, l_n$.
**Bizonyítás:** Legyen $q_1 = 0$ és konstruáljuk meg a $q_i = \sum_{j=1}^{i-1} 2^{-l_j}; \quad i = \{2, \ldots, n\}$ kettedes törteket. $\alpha_i$ ekkor a $q_i$ kettedestört alakjában a törtrész első $l_i$ darab számjegye lesz.
**Definíció:** Két (felbontható) kódot ekvivalensnek nevezünk, ha kódszavaik hosszai páronként azonosak.
**Tétel:** Bármely felbontható kódhoz létezik vele ekvivalens prefix kód.
**Bizonyítás:** Mivel felbontható igaz rá a Mc Millan, s emiatt az iménti tételből következik, hogy létezik a prefix kód.
Optimális kódok

Az $F$ jelforrás az $A = \{a_1, \ldots, a_n\}$ ábécé szimbólumait bocsájtja ki a $P = \{p_1, \ldots, p_n\}$ valószínűségekkel, ahol $p_i > 0$ és $\sum\limits_{i=1}^{n} p_i = 1$. Kódolva egy elsődleges közlést, a kódolt közlés hossza

$$M \sum_{i=1}^{n} p_i l_i$$

**Definíció:** A $\sum\limits_{i=1}^{n} p_i l_i$ számot a $K$ kód $F$ jelforrás melletti költségének nevezzük és $L(K)$-val jelöljük.
**Definíció:** Egy kódot optimálisnak nevezünk egy adott jelforrásra nézve, ha az adott jelforrás melletti költsége nem nagyobb egyetlen más kódétól sem. Jelölése: $K^o$
**Tétel:** Tetszőleges jelforráshoz létezik prefix kód
**Bizonyítás:** Legyen $|P| = n$, akkor a $0, \ldots, n-1$ számok $\lceil \log_2 n \rceil$ bites kettesszámrendszerbeli alakjai lesznek a megfelelő kódszavak.
**Tétel:** Tetszőleges jelforráshoz létezik optimális prefix kód
**Bizonyítás:** Legyen $K'$ tetszőleges felbontható kód $L(K')$ költséggel. Az előző tétel miatt biztos létezik ilyen. Ha $L(K) \leq L(K')$ akkor

$$\forall i : \quad 1 \leq l_i \leq \left[\frac{L(K')}{p_i} + 1\right] \text{ és}$$

$$\sum_{i=1}^{n} 2^{-l_i} \leq 1$$

**Definíció:** A $H(F) = \sum\limits_{i=1}^{n} p_i \log_2 \frac{1}{p_i}$ számot az $F$ jelforrás entrópiájának nevezzük. Az információ átlaga, azaz várható értéke:

$$\sum_{i=1}^{n} p(X_i) I(X_i) = \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i} = H(X)$$

**Tétel:** $H(F) \leq L(K)$
**Bizonyítás:** $H(F) - L(K) \leq 0$
**Tétel:** $L(K^o) < H(F) + 1$
**Bizonyítás:** Vajon létezik-e kód: $l_i = \left\lceil \log_2 \frac{1}{p_i} \right\rceil$? Igen, mert teljesül a McMillan, s ennek a költsége épp kisebb, mint az entrópia$+1$.
**Definíció:** Egy kódot teljesnek nevezünk, ha tetszőleges $\sigma$ esetén vagy $\sigma$ kezdődik kódszóval, vagy valamely kódszó kezdődik $\sigma$-val.
**Tétel:** $K$ teljes $\iff$ $K$ prefix és $\sum\limits_{i=1}^{n} 2^{-l_i} = 1$
**Tétel:** Ha $K$ optimális prefix kód, akkor $K$ teljes.

**Tétel:** Ha $K$ optimális, akkor $K$-ra teljesül a $\sum_{i=1}^{n} 2^{-l_i} = 1$.

**Bizonyítás:** Ekvivalens kódok költsége egyenlő.

Optimális kódok konstrukciója

Az egyszerűsített *Shannon–Fano* kód

A kódot a halmozott valószínűség kettedestört törtrészéből vesszük, a hossza az eredeti kettedestört törtrészében az első egyes helye

Huffmann–féle konstrukció:

**Tétel:** Az optimális kódok között létezik olyan, hogy a két leghosszabb kódszava azonos hosszú és csak az utolsó jegyben térnek el egymástól.

**Tétel:** Ha a $K_1 = \{\alpha_1, \ldots, \alpha_n\}$ optimális az $F_1 = \{p_1, \ldots, p_n\}$ $p_i \geq p_{i+1}$ jelforrásra és szét tudjuk bontani úgy egy valségét két részre, hogy mindkét rész kisebb egyenlő lesz a többinél ($\exists j : p_j = q_1 + q_2$ és $\forall i : p_i \geq q_1, q_2$), akkor erre az új $F_2 = \{p_1, \ldots, p_{j-1}, p_{j+1}, \ldots, p_n, q_1, q_2\}$ forrásra nézve optimális lesz a $K_2 = \{\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_n, \alpha_j 0, \alpha_j 1\}$ kód. Ez lehetőséget biztosít arra, hogy visszavezessük a problémát triviális $n = 2$ esetre. Ez a Huffmann-kódolás.

Példa: Hibajavítások, hibafelismerések

Mindegyik kódszó azonos hosszú, ez a blokkméret

**Definíció:** A csatorna (legfeljebb) $t$ egyedi hibát okoz, ha legfeljebb $t$ bit változik meg egy blokkban.

**Definíció:** Kódsűrűség: $\frac{\log_2 m}{n}$, ahol $m$ a kódszavak száma, $n$ pedig a blokkméret.

**Definíció:** Két kódszó Hamming–távolságán a különböző pozíciók számát értjük és $\varrho(\alpha, \beta)$-val jelöljük.

**Tétel:** $\varrho$ metrika.

**Bizonyítás:**

1. $\varrho(\alpha, \beta) \geq 0$
2. $\varrho(\alpha, \beta) = 0 \iff \alpha = \beta$
3. $\varrho(\alpha, \beta) = \varrho(\beta, \alpha)$
4. $\varrho(\alpha, \beta) + \varrho(\beta, \gamma) \geq \varrho(\alpha, \gamma)$

**Definíció:** Egy $K$ kód távolságán kódszavai távolságainak minimumát értjük és $d(K)$-val jelöljük.

**Tétel:** *A hibafelismerés alaptétele*
$K$ kóddal $t$ hibát tudunk felismerni $\iff d(K) > t$.

**Bizonyítás:** A hibát onnan ismerjük fel, hogy nem kódszó érkezett, tehát egyik kódszó sem változhat más kódszóvá $t$ hiba hatására.

**Tétel:** *A hibajavítás alaptétele*
$K$ kóddal $t$ hibát tudunk javítani $\iff d(K) > 2t$.

**Bizonyítás:** A hibát úgy tudjuk javítani, hogy tudjuk melyik kódszóból származik, azaz különböző kódszavak sem változhatnak át ugyanazon jelsorozattá $t$ hiba hatására. Lineáris kódok

**Definíció:** Két kódszó összege alatt a szimbólumainak $modulo 2$ szerinti összegeiből kialakuló kódszót értjük.

**Definíció:** Ha egy $K$ kódban bármely két kódszó összege is kódszó, akkor $K$-t lineárisnak nevezzük.

**Tétel:** A null kódszó mindig eleme egy lineáris kódnak.

**Bizonyítás:** Triviális

**Tétel:** A lineáris kódra teljesül: $|K| = 2^n$

**Definíció:** Egy kódszó súlya alatt nem nulla szimbólumainak számát értjük és $w(\alpha)$-val jelöljük.

**Tétel:** $\varrho(\alpha, \beta) = w(\alpha + \beta)$

**Definíció:** Egy kód súlya alatt nem nulla kódszavai súlyainak minimumát értjük és $w(K)$-val jelöljük.

**Tétel:** Ha $K$ lineáris, akkor $d(K) = w(K)$

**Bizonyítás:** $d(K) = \varrho(\alpha, \beta) = w(\alpha + \beta) \geq w(K)$
$w(K) = w(\alpha) = w(\alpha + 0) = \varrho(\alpha, 0) \geq d(K)$.

**Definíció:** Egy $K$ kód bázisán független kódszavai együttesét értjük.

**Definíció:** Egy kód generátormátrixán azt a mátrixot értjük, amelyet balról beszorozva tetszőleges vektorral a kód egy kódszavát kapjuk.

**Definíció:** Egy kód szisztematikus generátormátrixán azt a generátor mátrixot értjük, amelyet balról beszorozva tetszőleges vektorral a kód olyan kódszavát kapjuk, melynek a szorzó vektor prefix része.

**Tétel:** A szisztematikus generátor mátrix $I\,A$ alakú.

**Definíció:** A $H$ mátrixot a $K$ kód ellenőrző mátrixának nevezzük, ha $Hx^T = 0$ minden kódszóra.

**Tétel:** A $K$ lineáris kóddal $t$ hibát lehet javítani $\iff$ az ellenőrző mátrix tetszőleges $2t$ számú oszlopa lineárisan független.

**Definíció:** Ha $H = (1, 2, \ldots, 2^n - 1)$ akkor az általa meghatározott kódot *Hamming–kód*-nak nevezzük.

Jelentősége: Látható, hogy egy hibát tud javítani, de azt nagyon ügyesen: $H(\alpha + \varepsilon)^T = n$, ahol n a hiba helye.