Diszkrét matematika 2

9. előadás
Kódelmélet

Mérai László
merai@inf.elte.hu
https://sites.google.com/view/laszlomerai

Komputeralgebra Tanszék

2023 ősz

Kódelméleti áttekintő

1. feladat: Szavak, információ reprezentálása jelsorozatként.

Példa ábécé, Morze-kód, UTF-8, . . .

$\longrightarrow$ forráskódolás

2. feladat: Adott üzenet gazdaságos kódolása

Példa zip, tiff,. . .

$\longrightarrow$ veszteségmentes kódok és forráskódolás hűségkritériummal

3. feladat: Adott jelsorozat adattovábítás során sérülhet. A megkapott jelsorozatban hiba ellenörzése, javítása

Példa $0 \mapsto 000$, $1 \mapsto 111$

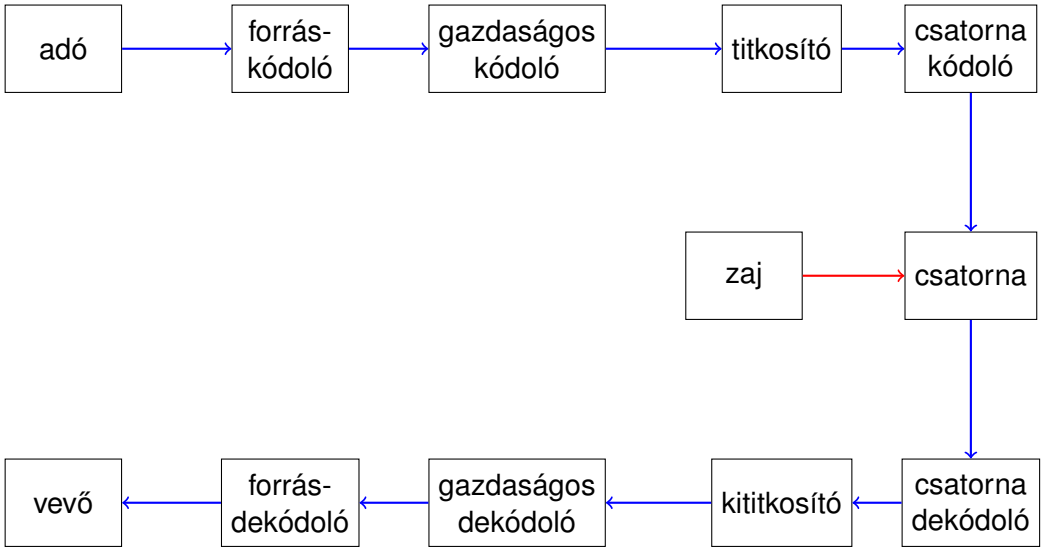
$\longrightarrow$ csatornakódolás: hibajelző, hibajavító kódok

4. feladat: Jelsorozat manipulálása, hogy harmadik fél ne tudja azt értelmezni

Példa $\texttt{helló} \mapsto \texttt{5b@!r\%g)j\$f}$

$\longrightarrow$ nem kódelmélet, kriptográfia

Kommunikációs csatorna



Kódelméleti áttekintő

- **Most**: forráskódolás (1. feladat)
- **Utána**: csatornakódolás (3. feladat)
- **Esetleg**: gazdaságos kódolás (2. feladat)

Forráskódolás

Betűnkénti kódolás

Definíció

Legyen $\mathcal{X} = \{x_1, x_2 \dots, x_n\}$ halmaz a forrásábécé és $\mathcal{Y} = \{y_1, y_2, \dots, y_k\}$ a kódábécé. Ekkor egy $\varphi : \mathcal{X} \to \mathcal{Y}^*$ injektív függvényt kódolásnak (vagy betűnkénti kódolásnak) hívunk.
Itt $\mathcal{Y}^*$ az $\mathcal{Y}$ elemeiből álló véges szavak halmaza.
A φ függvényt kiterjesztjük az $\mathcal{X}^*$ halmazra betűnként:
$\varphi(u_1 u_2 \dots u_r) = \varphi(u_1)\varphi(u_2) \dots \varphi(u_r)$.

Példa

- Morze-kód: $\mathcal{X} = \{a, b, c \dots\}$, $\mathcal{Y} = \{\cdot, -\}$, $a \mapsto \cdot-$, $b \mapsto -\cdots$, $c \mapsto -\cdot-\cdot$,...
- ASCII: $\mathcal{X} = \{\text{latin ábécé+}\}$, $\mathcal{Y} = \{0, 1\}$
- UTF-8: $\mathcal{X} = \{\text{latin ábécé+}\} \cup \{\text{görög ábécé}\} \cup \{\text{cirill ábécé}\} \cup \dots$, $\mathcal{Y} = \{0, 1\}$

Felbontható kódolás

Figyelem, attól, hogy φ injektív, még nem, biztos, hogy egyértelműen dekódolható.

Definíció

Egy $\varphi : \mathcal{X} \mapsto \mathcal{Y}^*$ kódolás felbontható (vagy egyértelműen dekódolható), ha $\mathbf{u}, \mathbf{v} \in \mathcal{X}^*$, $\mathbf{u} = u_1 u_2 \dots u_r$, $\mathbf{v} = v_1 v_2 \dots v_s$ esetén, ha $\mathbf{u} \neq \mathbf{v}$, akkor

$$\varphi(u_1)\varphi(u_2)\dots\varphi(u_r) \neq \varphi(v_1)\varphi(v_2)\dots\varphi(v_s).$$

Példa

- A Morze-kód nem felbontható: $\varphi(s) = \cdots = \varphi(e)\varphi(i)$ (u.i. $\varphi(e) = \cdot$, $\varphi(i) = \cdot\cdot$)
- ASCII és UTF-8 felbontható.