# 3a. Hamming-kódok

Kódolástechnika

# A cél

Tervezzünk olyan kódot, amely képes egyetlen hibát kijavítani.

Motiváció: Ha a csatorna jó minőségű (pl. vezetékes összeköttetés), akkor a többszörös hibák generálásának valószínűsége kicsi. Ezért elegendő minden egyszeres hibát javítani, mert ezek fordulnak elő nagy valószínűséggel.

# Hamming-kódok

A Hamming-kódok egyetlen hiba javítására képesek.

A Hamming-kódok perfekt kódok:

$$n = 2^{n-k} - 1 \quad \Longleftrightarrow \quad \sum_{i=0}^{1} \binom{n}{i} = 2^{n-k}$$

A $C(n, k)$ Hamming-kódok konstrukciója:

- a $H$ paritás ellenőrző mátrix oszlopait úgy választjuk meg, hogy mind különböző legyen és a csupa nulla oszlop ne szerepeljen köztük;
- meghatározzuk a generátormátrixot;
- megtervezzük az "illesztő kapukat" a szindróma dekódoláshoz;
- implementáljuk az egész sémát.

# A $C(7,4)$ Hamming-kód

$n = 7, k = 4$, tehát $n + 1 = 8 = 2^{7-4}$ teljesül.

# A $C(7,4)$ Hamming-kód

$n = 7, k = 4$, tehát $n + 1 = 8 = 2^{7-4}$ teljesül.

A paritás ellenőrző mátrix konstrukciója:

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

# A $C(7,4)$ Hamming-kód

$n = 7, k = 4$, tehát $n + 1 = 8 = 2^{7-4}$ teljesül.

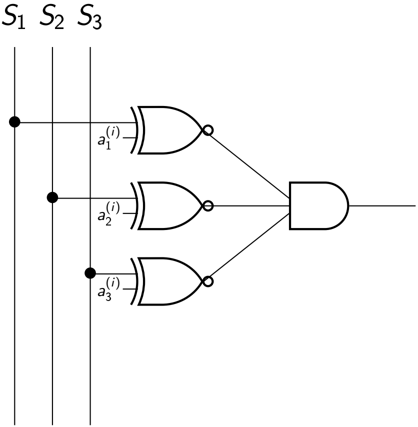
A paritás ellenőrző mátrix konstrukciója:

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

A generátormátrix:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

# Az "illesztő kapuk" konstrukciója

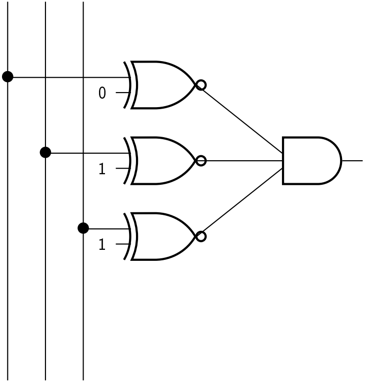



egyezés (1) $\rightarrow$ kimenet: $e$
eltérés (0) $\rightarrow$ kimenet: 0

# Az "illesztő kapuk" konstrukciója

Pl. $a^{(1)} = (011)$:

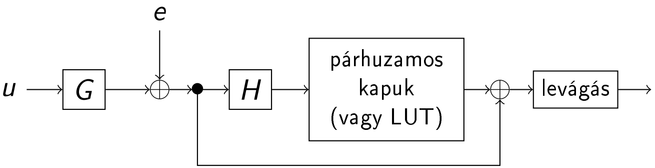
$S_1 \; S_2 \; S_3$




egyezés (1) $\to$ kimenet: (1000000)
eltérés (0) $\to$ kimenet: (0000000)

Hasonlóan $a^{(2)} = (101), \ldots, a^{(7)} = (001)$-re.

# A rendszer implementációja



# 1. feladat

Egy bináris csatorna bit hiba valószínűsége $P_b = 0.001$.

(a) Átküldünk egy 57 bit hosszú üzenetet a csatornán kódolás nélkül. Mennyi a blokk hiba valószínűsége (vagyis annak az esélye, hogy az üzenet hibásan érkezik meg)?

(b) Átküldünk egy 57 bit hosszú üzenetet a csatornán C(63,57) Hamming-kóddal kódolva. Mennyi a blokk hiba valószínűsége (vagyis annak az esélye, hogy hibás az üzenet dekódolása)?

# 1. feladat

Egy bináris csatorna bit hiba valószínűsége $P_b = 0.001$.

(a) Átküldünk egy 57 bit hosszú üzenetet a csatornán kódolás nélkül. Mennyi a blokk hiba valószínűsége (vagyis annak az esélye, hogy az üzenet hibásan érkezik meg)?

(b) Átküldünk egy 57 bit hosszú üzenetet a csatornán C(63,57) Hamming-kóddal kódolva. Mennyi a blokk hiba valószínűsége (vagyis annak az esélye, hogy hibás az üzenet dekódolása)?

Megoldás.

(a) Annak a valószínűsége, hogy minden bit helyesen érkezik meg,

$$(1 - P_b)^{57} \approx 0.9446,$$

a blokk hiba valószínűsége pedig

$$1 - (1 - P_b)^{57} \approx 0.0554.$$

# 1. feladat

(a) Hamming kód használata esetén a dekódolás helyes lesz, ha 0 vagy 1 hiba van a vett kódszóban. A helyes dekódolás valószínűsége

$$(1-P_b)^{63}+63(1-P_b)^{62}P_b = 0.99^{63}+62\cdot 0.999^{62}\cdot 0.001 \approx 0.99812,$$

a blokk hiba valószínűsége pedig

$$1-(1-P_b)^{63}-63(1-P_b)^{62}P_b \approx 0.00188.$$

# 1. feladat

(a) Hamming kód használata esetén a dekódolás helyes lesz, ha 0 vagy 1 hiba van a vett kódszóban. A helyes dekódolás valószínűsége

$$(1-P_b)^{63}+63(1-P_b)^{62}P_b = 0.99^{63}+62\cdot 0.999^{62}\cdot 0.001 \approx 0.99812,$$

a blokk hiba valószínűsége pedig

$$1-(1-P_b)^{63}-63(1-P_b)^{62}P_b \approx 0.00188.$$

Vagyis a C(63,57) Hamming kód használatával csökkentettük a blokk hiba valószínűségét 0.0554-ről 0.00188-re, ennek ára pedig az, hogy a kód ráta 57/63, vagyis az effektív csatorna kapacitás az eredeti kapacitás 57/63 részére csökkent.

# 2. feladat

(a) Egy bináris csatorna bit hiba velószínűsége $P_b = 0.01$. Átküldünk egy 4 bit hosszú üzenetet a csatornán C(7,4) Hamming kóddal kódolva. Mennyi a blokk hiba valószínűsége?

(b) Egy másik csatorna bit hiba valószínűsége $P'_b$. Átküldünk egy 4 bit hosszú üzenetet a csatornán kódolás nélkül. Számítsuk ki $P'_b$ értékét úgy, hogy a blokk hiba valószínűsége ugyanannyi legyen, mint az (a) részben.

## 2. feladat

(a) Egy bináris csatorna bit hiba velószínűsége $P_b = 0.01$. Átküldünk egy 4 bit hosszú üzenetet a csatornán C(7,4) Hamming kóddal kódolva. Mennyi a blokk hiba valószínűsége?

(b) Egy másik csatorna bit hiba valószínűsége $P_b'$. Átküldünk egy 4 bit hosszú üzenetet a csatornán kódolás nélkül. Számítsuk ki $P_b'$ értékét úgy, hogy a blokk hiba valószínűsége ugyanannyi legyen, mint az (a) részben.

Megoldás.

(a) A blokk hiba valószínűség

$$1 - (1 - P_b)^7 - 7(1 - P_b)^6 P_b \approx 0.00203.$$

## 2. feladat

(a) Egy bináris csatorna bit hiba velószínűsége $P_b = 0.01$. Átküldünk egy 4 bit hosszú üzenetet a csatornán C(7,4) Hamming kóddal kódolva. Mennyi a blokk hiba valószínűsége?

(b) Egy másik csatorna bit hiba valószínűsége $P'_b$. Átküldünk egy 4 bit hosszú üzenetet a csatornán kódolás nélkül. Számítsuk ki $P'_b$ értékét úgy, hogy a blokk hiba valószínűsége ugyanannyi legyen, mint az (a) részben.

Megoldás.

(a) A blokk hiba valószínűség

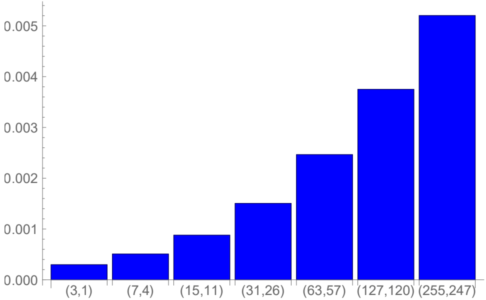
$$1 - (1 - P_b)^7 - 7(1 - P_b)^6 P_b \approx 0.00203.$$

(b) Kódolás nélkül pedig a blokk hiba valószínűség

$$1 - (1 - P'_b)^4 = 0.00203 \quad \rightarrow \quad P'_b \approx 0.000508.$$

# Módosított bit hiba valószínűség

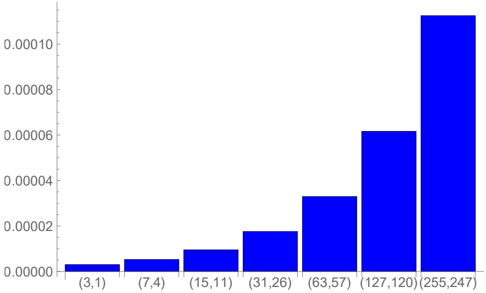
Megadjuk a módosított bit hiba valószínűséget a kód paramétereinek függvényében $P_b = 0.01$ esetén.




Sebesség csökkenés arányok:
$1/3; 4/7; 11/15; 57/63; 120/127; 247/255.$

# Módosított bit hiba valószínűség

Megadjuk a módosított bit hiba valószínűséget a kód paramétereinek függvényében $P_b = 0.001$ esetén.




Sebesség csökkenés arányok:
$1/3; 4/7; 11/15; 57/63; 120/127; 247/255.$

# Kód tervezés

Kód tervezés kommunikációs mérnöki szemszögből.

Feladat. Adott egy BSC $P_b$ bit hiba valószínűséggel és egy elérni kívánt QoS $\gamma$; tervezzünk kódot, melyre $P_b' < 10^{-\gamma}$.

# Kód tervezés

Kód tervezés kommunikációs mérnöki szemszögből.

Feladat. Adott egy BSC $P_b$ bit hiba valószínűséggel és egy elérni kívánt QoS $\gamma$; tervezzünk kódot, melyre $P_b' < 10^{-\gamma}$.

Megoldás.

(1) Kiszámítjuk $k$ értékét:

$$1 - (1 - P_b')^k = 1 - (1 - P_b)^n - nP_b(1 - P_b)^{n-1}.$$

Ha $n - k$ túl nagy, vagy $n > 2^{n-k} - 1$, akkor nem létezik olyan megoldás, amely csak egyetlen hibát javít (egy olyan kód, amely egynél több hibát javít, még segíthet).

# Kód tervezés

(2) Megkonstruáljuk a paritás ellenőrző mátrixot a következő szabályok alapján:
- minden oszlop különböző;
- egyik oszlop sem csupa 0;
- a kód szisztematikus.

(3) Implementáljuk a kód sémát.

# 3. Feladat

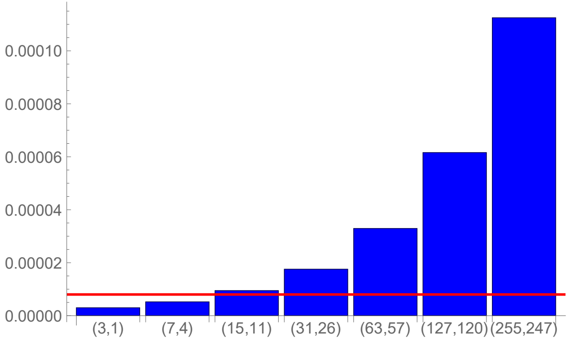
Egy BSC-re $P_b = 0.001$. Tervezzünk egy olyan hibajavító kódot a csatornához, melyre a módosított bit hiba valószínűsége $\leq 0.000008$.

# 3. Feladat

Egy BSC-re $P_b = 0.001$. Tervezzünk egy olyan hibajavító kódot a csatornához, melyre a módosított bit hiba valószínűsége $\leq 0.000008$.

Megoldás.

(1) A paraméterek kiválasztása: $n = 7, k = 4$ megfelelő.



# 4. Feladat

Egy bináris lineáris kód generátormátrixa

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Ez egy Hamming-kód?

# 4. Feladat

Egy bináris lineáris kód generátormátrixa

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Ez egy Hamming-kód?

Megoldás. $n = 5, k = 3$, tehát ez $C(5,3)$ kód. Viszont

$$n + 1 = 6 \neq 2^{n-k} = 4,$$

tehát ez nem Hamming-kód.

# 5. Feladat

Egy bináris Hamming-kódra $k = 11$. Mennyi $n$ értéke?

# 5. Feladat

Egy bináris Hamming-kódra $k = 11$. Mennyi $n$ értéke?

Megoldás. Az

$$n + 1 = 2^{n-k},$$

egyenlet megoldása $n = 15$.

# 6. Feladat

Egy bináris lineáris kód paritás ellenőrző mátrixa

$$H = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Ez egy Hamming-kód?

# 6. Feladat

Egy bináris lineáris kód paritás ellenőrző mátrixa

$$H = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Ez egy Hamming-kód?

Megoldás. $n = 7, k = 4$, tehát $n + 1 = 2^{n-k}$ teljesül, viszont az első és a negyedik oszlop megegyezik, tehát ez nem egy Hamming-kód.

# 7. feladat

Egy szisztematikus bináris lineáris kód paritás ellenőrző mátrixa

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

(a) Mik a kód paraméterei?
(b) Ez egy Hamming-kód?
(c) Számítsuk ki a $G$ generátor mátrixot.
(d) Mik a kód hibadetektálási és hibajavítási képességei?
(e) Adjuk meg a (011) hibavektorhoz tartozó szindrómát és hibacsoportot.

# 7. feladat

Megoldás.

(a) $H = H_{(n-k)\times n}$ egy $2 \times 3$-as mátrix, tehát $n - k = 2$ és $n = 3$, azaz ez egy C(3,1) kód.

# 7. feladat

Megoldás.

(a) $H = H_{(n-k)\times n}$ egy $2 \times 3$-as mátrix, tehát $n - k = 2$ és $n = 3$, azaz ez egy C(3,1) kód.

(b) $H$ oszlopai éppen a különböző 2 hosszú bináris vektorok, azaz ez egy Hamming kód.

# 7. feladat

Megoldás.

(a) $H = H_{(n-k)\times n}$ egy $2\times 3$-as mátrix, tehát $n-k=2$ és $n=3$, azaz ez egy C(3,1) kód.

(b) $H$ oszlopai éppen a különböző 2 hosszú bináris vektorok, azaz ez egy Hamming kód.

(c)

$$H = (B^T, I_{n-k}) = \left[\underbrace{\boxed{\begin{matrix}1\\1\end{matrix}}}_{B^T}\begin{matrix}1 & 0\\0 & 1\end{matrix}\right].$$

$$G = (I_k, B) = \left[\,1\;\underbrace{\boxed{1\quad 1}}_{B}\right].$$

# 7. feladat

(d) A kódszavak

$$(000), \quad (111)$$

so

$$d_{\min} = \min_{c \neq (00\ldots0)} w(c) = 3,$$

tehát a kód $d_{\min} - 1 = 2$ hibát képes detektálni és $\lfloor (d_{\min} - 1)/2 \rfloor = 1$ hibát képes javítani.

# 7. feladat

(d) A kódszavak

$$(000), \quad (111)$$

so

$$d_{\min} = \min_{c \neq (00\ldots0)} w(c) = 3,$$

tehát a kód $d_{\min} - 1 = 2$ hibát képes detektálni és $\lfloor (d_{\min} - 1)/2 \rfloor = 1$ hibát képes javítani.

(e) $s^T = He^T = \begin{bmatrix} 110 \\ 101 \end{bmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$

$E_{(11)} = \{(011), (011) + (111)\} = \{(011), (100)\}$

# 8. Feladat

Adott egy $C(7,4)$ bináris szisztematikus Hamming-kód.

(a) Töltsük ki a paritás ellenőrző mátrix hiányzó elemeit:

$$H = \begin{bmatrix} 0 & 1 & 1 & * & * & 0 & 0 \\ 1 & 0 & 1 & * & * & 1 & 0 \\ 1 & 1 & 0 & * & * & 0 & 1 \end{bmatrix}.$$

(b) Mi az (1111) üzenetvektorhoz tartozó kódszó?

# 8. Feladat

Megoldás.

(a) A kód szisztematikus $\rightarrow$ $H$-ban a jobb szélső négyzet alakú blokk az identitás mátrix. Az utolsó hiányzó oszlop pedig az utolsó kimaradó nemnulla vektor kell legyen.

$$H = \left[\begin{array}{cccc|c} 0 & 1 & 1 & 1 & \boxed{\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}} \\ 1 & 0 & 1 & 1 & \\ 1 & 1 & 0 & 1 & \end{array}\right].$$

# 8. Feladat

Megoldás.

(b) A generátormátrixhoz pedig használjuk, hogy

$$H = \Bigg[ \underbrace{\boxed{\begin{matrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{matrix}}}_{B^T} \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \Bigg].$$

jelöléssel $G = (I; B)$ alakú:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

végül

$$(1111) \cdot G = (1111111).$$