2. A kódolás alapvető fogalmai és általános kódolási sémák

Kódolástechnika

1. feladat

Egy kód kódszavai

$$10100, 01111, 11110, 00000.$$

(a) Adjuk meg a kód n és k paramétereit.
(b) Mennyi a minimális Hamming-távolság a kódszavak között?
(c) Hány hibát képes a kód detektálni? Hány hibát képes a kód kijavítani?

1. feladat

Megoldás.

(a) A kódszavak hossza $n = 5$, és a kódszavak darabszáma $2^k = 4$ (minden k hosszú üzenetvektorhoz egy), tehát $k = 2$. Ez egy $C(5, 2)$ kód.

1. feladat

Megoldás.

(a) A kódszavak hossza $n = 5$, és a kódszavak darabszáma $2^k = 4$ (minden k hosszú üzenetvektorhoz egy), tehát $k = 2$. Ez egy $C(5, 2)$ kód.

(b) Páronkénti összehasonlítás alapján a minimális Hamming távolság

$$d_{\min} = 2.$$

1. feladat

Megoldás.

(a) A kódszavak hossza $n = 5$, és a kódszavak darabszáma $2^k = 4$ (minden k hosszú üzenetvektorhoz egy), tehát $k = 2$. Ez egy $C(5, 2)$ kód.

(b) Páronkénti összehasonlítás alapján a minimális Hamming távolság

$$d_{\min} = 2.$$

(c) $d_{\min} = 2$ alapján a kód

$$d_{\min} - 1 = 1$$

hibát képes detektálni, és

$$\left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = 0$$

hibát képes kijavítani.

2. feladat

(a) Tervezzünk egy C(5,2) kódot, melyre d_{min} a lehető legnagyobb.

(b) Adjuk meg a dekódolót Look-Up-Table (LUT) révén.

(c) Határozzuk meg a kód hibadetektáló és hibajavító képességeit.

2. feladat

(a) Tervezzünk egy C(5,2) kódot, melyre d_{min} a lehető legnagyobb.

(b) Adjuk meg a dekódolót Look-Up-Table (LUT) révén.

(c) Határozzuk meg a kód hibadetektáló és hibajavító képességeit.

Megoldás.

(a) $n = 5$ hosszúság esetén 32 bináris vektor van, melyek közül $2^k = 2^2 = 4$-et kell kiválasztanunk. Ezekre meg kell határoznunk a minimális páronkénti Hamming-távolságot, és kiválasztani 4 olyan vektort, melyekre a minimális Hamming-távolság a lehető legnagyobb.

2. feladat

(a) Az előző feladatbeli kódra $d_{\text{min}} = 2$ volt. Próbáljunk meg most $d_{\text{min}} = 3$-at elérni!

- Legyen az első kódszó a (00000).

2. feladat

(a) Az előző feladatbeli kódra $d_{\text{min}} = 2$ volt. Próbáljunk meg most $d_{\text{min}} = 3$-at elérni!

- Legyen az első kódszó a (00000).
- Minden más kódszó súlya legalább 3 kell legyen; (00111) egy természetes választás.

2. feladat

(a) Az előző feladatbeli kódra $d_{\min} = 2$ volt. Próbáljunk meg most $d_{\min} = 3$-at elérni!

- Legyen az első kódszó a (00000).
- Minden más kódszó súlya legalább 3 kell legyen; (00111) egy természetes választás.
- A következő kódszó súlya is legalább 3 kell legyen, és el kell térjen az előzőtől is legalább 3 helyen, legyen pl. (11100).

2. feladat

(a) Az előző feladatbeli kódra $d_{\text{min}} = 2$ volt. Próbáljunk meg most $d_{\text{min}} = 3$-at elérni!

- Legyen az első kódszó a (00000).
- Minden más kódszó súlya legalább 3 kell legyen; (00111) egy természetes választás.
- A következő kódszó súlya is legalább 3 kell legyen, és el kell térjen az előzőtől is legalább 3 helyen, legyen pl. (11100).
- A csupa 1-es nem jó utolsó kódszónak, mert az előző kettőtől a Hamming-távolsága csak 2, de ha a középső bitet 0-ra változtatjuk, már jó lesz: (11011).

Erre a kódra $d_{\text{min}} = 3$.

2. feladat

(a) Az előző feladatbeli kódra $d_{\min} = 2$ volt. Próbáljunk meg most $d_{\min} = 3$-at elérni!

- Legyen az első kódszó a (00000).
- Minden más kódszó súlya legalább 3 kell legyen; (00111) egy természetes választás.
- A következő kódszó súlya is legalább 3 kell legyen, és el kell térjen az előzőtől is legalább 3 helyen, legyen pl. (11100).
- A csupa 1-es nem jó utolsó kódszónak, mert az előző kettőtől a Hamming-távolsága csak 2, de ha a középső bitet 0-ra változtatjuk, már jó lesz: (11011).

Erre a kódra $d_{\min} = 3$.

$d_{\min} = 4$ viszont már nem lehetséges, azaz 5-hosszú kódszavakból nem lehet 4-et kiválasztani úgy, hogy $d_{\min} \geq 4$ teljesüljön. (Már 3-at sem lehet kiválasztani, hogy $d_{\min} \geq 4$ teljesüljön. Miért?)

2. feladat

(b) Ha az üzenet-kódszó hozzárendelés az alábbi módon történik, akkor a lookup-table (LUT) ugyanez fordítva:

$$\begin{array}{l} 00 \to 00000 \\ 01 \to 11100 \\ 10 \to 00111 \\ 11 \to 11011 \end{array} \quad \to$$

c'	u'
00000	00
11100	01
00111	10
11011	11

LUT

A fenti LUT-ben csak a kódszavak szerepelnek, minden más c' vett vektorhoz először megkeressük, melyik kódszótól minimális a Hamming-távolsága, és az alapján dekódoljuk.

($d = 2$ esetén előfordulhat, hogy a vett vektornak több kódszótól is minimális a távolsága, ilyenkor szabadságunk van abban, melyik kódszót detektáljuk a vett vektor alapján.)

2. feladat

(b) Ha az üzenet-kódszó hozzárendelés az alábbi módon történik, akkor a lookup-table (LUT) ugyanez fordítva:

$$\begin{aligned} 00 &\to 00000 \\ 01 &\to 11100 \\ 10 &\to 00111 \\ 11 &\to 11011 \end{aligned} \quad \to$$

c'	u'
00000	00
11100	01
00111	10
11011	11

LUT

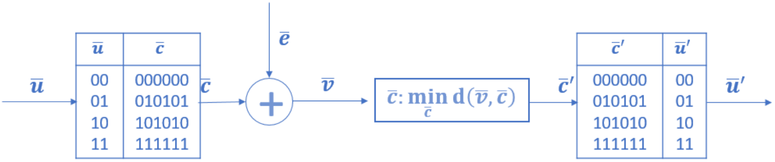
A fenti LUT-ben csak a kódszavak szerepelnek, minden más c' vett vektorhoz először megkeressük, melyik kódszótól minimális a Hamming-távolsága, és az alapján dekódoljuk.

($d = 2$ esetén előfordulhat, hogy a vett vektornak több kódszótól is minimális a távolsága, ilyenkor szabadságunk van abban, melyik kódszót detektáljuk a vett vektor alapján.)

(c) Hiba detekciós képesség: $d_{\min} - 1 = 2$.
Hiba javító képesség: $\lfloor \frac{d_{\min}-1}{2} \rfloor = 1$.

3. feladat

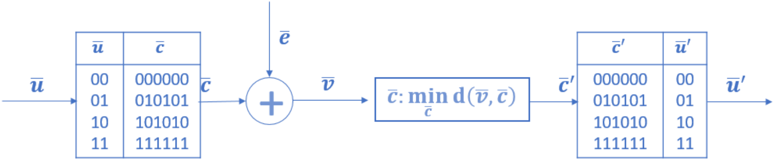
Adott a következő kódoló séma:



$u = (11)$ és $e = (001000)$; határozzuk meg a c, v, c', u' vektorokat.

3. feladat

Adott a következő kódoló séma:



$u = (11)$ és $e = (001000)$; határozzuk meg a c, v, c', u' vektorokat.

Megoldás.

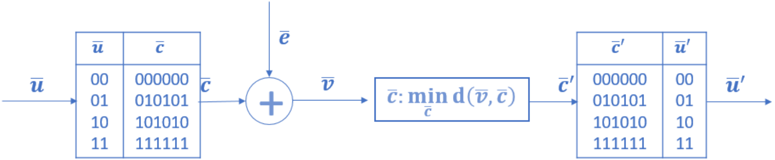
$$c = (111111)$$

$$v = c + e = (111111) + (001000) = (110111),$$

$$c' = \{c : \min_{c} d(v, c)\} = (111111)$$

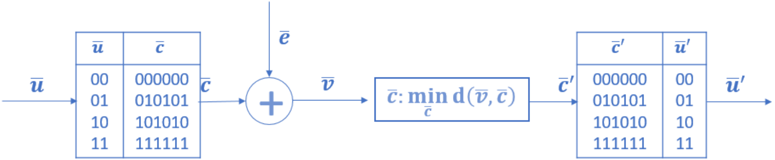
$$u' = (11)$$

4. feladat



Ugyanerre a kódolási sémára ezúttal $u = (01)$ és $e = (001011)$. Határozzuk meg a c, v, c', u' vektorokat.

4. feladat



Ugyanerre a kódolási sémára ezúttal $u = (01)$ és $e = (001011)$. Határozzuk meg a c, v, c', u' vektorokat.

Megoldás.

$$c = (010101)$$

$$v = c + e = (010101) + (001011) = (011110),$$

$$c' = \{c : \min_{c} d(v, c)\} = (111111)$$

$$u' = (11)$$

5. feladat

A következő kódszó halmazok mindegyikére adjuk meg az (n, k, d) értékeket, ahol n a kódszavak hossza, k az, hogy egy kódszó hány bit információt továbbít, és $d = d_{\text{min}}$ a minimális Hamming távolság a kódszavak között. Adjuk meg a kódolási rátát is.

(a) $\{111, 100, 010, 001\}$

(b) $\{00000, 01111, 10100, 11011\}$

(c) $\{00000\}$

5. feladat

Megoldás.

(a) $\{111, 100, 010, 001\}$

- $n = 3$ (a kódszavak hossza);
- $k = 2$ (a kódszavak száma $4 = 2^k$);
- $d = d_{\min} = 2$ (páronkénti összehasonlítás alapján);
- a kód ráta $k/n = 2/3$.

5. feladat

Megoldás.

(a) $\{111, 100, 010, 001\}$

- $n = 3$ (a kódszavak hossza);
- $k = 2$ (a kódszavak száma $4 = 2^k$);
- $d = d_{\min} = 2$ (páronkénti összehasonlítás alapján);
- a kód ráta $k/n = 2/3$.

(b) $\{00000, 01111, 10100, 11011\}$

$n = 5, k = 2, d = 2$, a kód ráta $2/5$.

5. feladat

Megoldás.

(a) $\{111, 100, 010, 001\}$

- $n = 3$ (a kódszavak hossza);
- $k = 2$ (a kódszavak száma $4 = 2^k$);
- $d = d_{\min} = 2$ (páronkénti összehasonlítás alapján);
- a kód ráta $k/n = 2/3$.

(b) $\{00000, 01111, 10100, 11011\}$

$n = 5, k = 2, d = 2$, a kód ráta $2/5$.

(c) $\{00000\}$

Némileg beugratós kérdés. $n = 5, k = 0$, d nem definiált. A kód ráta 0.

Mivel csak egy kódszó van, nem lehet információt továbbítani, mivel a vevő eleve tudja, milyen kódszót kell kapnia.

6. feladat

Az Irattáros szeretne egy kódolást évfolyamok szerint („gólya", „másodéves", „junior", „senior"), amely képes egy hibát kijavítani. Adjunk megfelelő 5-bites bináris kódolást a 4 évfolyamra.

6. feladat

Az Irattáros szeretne egy kódolást évfolyamok szerint („gólya”, „másodéves”, „junior”, „senior”), amely képes egy hibát kijavítani. Adjunk megfelelő 5-bites bináris kódolást a 4 évfolyamra.

Megoldás. Egy $C(5,2,3)$ blokk-kódra van szükség. Egy ilyen kód szerepelt a 2. feladatban, azt használhatjuk:

$$\{(00000),(00111),(11100),(11011)\}.$$

7. feladat

A Páronkénti Kommunikáció egy olyan kódot fejlesztett, melyben a három adatbit (D_1, D_2, D_3) és három paritás bit (P_1, P_2, P_3) szerepel:

$$P_1 = D_1 + D_2, \quad P_2 = D_2 + D_3, \quad P_3 = D_3 + D_1.$$

(a) Számítsuk ki (n, k) értékét erre a kódra.

(b) Mik a kódszavak?

(c) Mi a minimális Hamming távolság a kódszavak között?

7. feladat

Megoldás.

(a) $n = 6, k = 3.$

7. feladat

Megoldás.

(a) $n = 6, k = 3$.

(b) 8 lehetséges kódszó van:

$$(000000), \quad (001011), \quad (010110), \quad (011101),$$
$$(100101), \quad (101110), \quad (110011), \quad (111000).$$

(Például a (001) üzenet esetén $D_1 = D_2 = 0, D_3 = 1$, így $P_1 = 0, P_2 = P_3 = 1$, az ehhez tartozó kódszó a (001011).)

7. feladat

Megoldás.

(a) $n = 6, k = 3$.

(b) 8 lehetséges kódszó van:

$$\begin{array}{cccc} (000000), & (001011), & (010110), & (011101), \\ (100101), & (101110), & (110011), & (111000). \end{array}$$

(Például a (001) üzenet esetén $D_1 = D_2 = 0, D_3 = 1$, így $P_1 = 0, P_2 = P_3 = 1$, az ehhez tartozó kódszó a (001011).)

Egyébként itt minden kódszó első k bitje pont maga az üzenet. Az ilyen kódokat szisztematikus kódnak hívjuk.

7. feladat

Megoldás.

(a) $n = 6, k = 3$.

(b) 8 lehetséges kódszó van:

$$\begin{array}{cccc} (000000), & (001011), & (010110), & (011101), \\ (100101), & (101110), & (110011), & (111000). \end{array}$$

(Például a (001) üzenet esetén $D_1 = D_2 = 0, D_3 = 1$, így $P_1 = 0, P_2 = P_3 = 1$, az ehhez tartozó kódszó a (001011).)

Egyébként itt minden kódszó első k bitje pont maga az üzenet. Az ilyen kódokat szisztematikus kódnak hívjuk.

(c) Páronkénti összehasonlítás alapján a minimális Hamming távolság $d_{\min} = 3$.

7. feladat

Megoldás.

(a) $n = 6, k = 3.$

(b) 8 lehetséges kódszó van:

$$\begin{array}{llll} (000000), & (001011), & (010110), & (011101), \\ (100101), & (101110), & (110011), & (111000). \end{array}$$

(Például a (001) üzenet esetén $D_1 = D_2 = 0, D_3 = 1$, így $P_1 = 0, P_2 = P_3 = 1$, az ehhez tartozó kódszó a (001011).)

Egyébként itt minden kódszó első k bitje pont maga az üzenet. Az ilyen kódokat szisztematikus kódnak hívjuk.

(c) Páronkénti összehasonlítás alapján a minimális Hamming távolság $d_{\min} = 3$. VAGY (kicsit előreutalva): ez egyébként egy lineáris kód, és lineáris kódokra

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

8. feladat

A vevő kiszámít három szindróma bitet (E_1, E_2 és E_3) az (esetleg hibás) adatbitekből és paritásbitekből:

$$E_1 = D_1 + D_2 + P_1, \quad E_2 = D_2 + D_3 + P_2, \quad E_3 = D_3 + D_1 + P_3.$$

A vevő maximum likelihood dekódolást végez a szindróma bitek alapján. Határozzuk meg az eredményt a következő lehetőségek közül:

- nincs hiba, vagy
- egyetlen hiba van (azt is határozzuk meg, hogy melyik bitben), vagy
- több hiba van,

a következő szindrómák mindegyikére:

$$E_1E_2E_3 = 000, \qquad E_1E_2E_3 = 010,$$
$$E_1E_2E_3 = 101, \qquad E_1E_2E_3 = 111.$$

8. feladat

Megoldás. A fő észrevételek:

- hibák a vett $D_1, D_2, D_3, P_1, P_2, P_3$ között lehetnek.
- ha nincs bennük hiba, akkor $E_1E_2E_3 = 000$.
- ha egyetlen hiba van, és az P_1, P_2 vagy P_3 valamelyikében, akkor E_1, E_2 és E_3 közül egy lesz egyes.
- ha egyetlen hiba van, és az D_1, D_2 vagy D_3 valamelyikében, akkor E_1, E_2 és E_3 közül kettő lesz egyes.
- A ML dekódoló minden $E_1E_2E_3$ szindróma esetén azt a lehetséges hiba-konfigurációt választja, amelyikben a legkevesebb hiba van.

8. feladat

Megoldás. A fő észrevételek:

- hibák a vett $D_1, D_2, D_3, P_1, P_2, P_3$ között lehetnek.
- ha nincs bennük hiba, akkor $E_1E_2E_3 = 000$.
- ha egyetlen hiba van, és az P_1, P_2 vagy P_3 valamelyikében, akkor E_1, E_2 és E_3 közül egy lesz egyes.
- ha egyetlen hiba van, és az D_1, D_2 vagy D_3 valamelyikében, akkor E_1, E_2 és E_3 közül kettő lesz egyes.
- A ML dekódoló minden $E_1E_2E_3$ szindróma esetén azt a lehetséges hiba-konfigurációt választja, amelyikben a legkevesebb hiba van.

Ha $E_1E_2E_3 = 000$, az eredmény az, hogy nincs hiba.

8. feladat

Megoldás. A fő észrevételek:

- hibák a vett $D_1, D_2, D_3, P_1, P_2, P_3$ között lehetnek.
- ha nincs bennük hiba, akkor $E_1E_2E_3 = 000$.
- ha egyetlen hiba van, és az P_1, P_2 vagy P_3 valamelyikében, akkor E_1, E_2 és E_3 közül egy lesz egyes.
- ha egyetlen hiba van, és az D_1, D_2 vagy D_3 valamelyikében, akkor E_1, E_2 és E_3 közül kettő lesz egyes.
- A ML dekódoló minden $E_1E_2E_3$ szindróma esetén azt a lehetséges hiba-konfigurációt választja, amelyikben a legkevesebb hiba van.

Ha $E_1E_2E_3 = 000$, az eredmény az, hogy nincs hiba.

Ha $E_1E_2E_3 = 010$, az eredmény 1 hiba P_2-ben.

8. feladat

Megoldás. A fő észrevételek:

- hibák a vett $D_1, D_2, D_3, P_1, P_2, P_3$ között lehetnek.
- ha nincs bennük hiba, akkor $E_1 E_2 E_3 = 000$.
- ha egyetlen hiba van, és az P_1, P_2 vagy P_3 valamelyikében, akkor E_1, E_2 és E_3 közül egy lesz egyes.
- ha egyetlen hiba van, és az D_1, D_2 vagy D_3 valamelyikében, akkor E_1, E_2 és E_3 közül kettő lesz egyes.
- A ML dekódoló minden $E_1 E_2 E_3$ szindróma esetén azt a lehetséges hiba-konfigurációt választja, amelyikben a legkevesebb hiba van.

Ha $E_1 E_2 E_3 = 000$, az eredmény az, hogy nincs hiba.

Ha $E_1 E_2 E_3 = 010$, az eredmény 1 hiba P_2-ben.

Ha $E_1 E_2 E_3 = 101$, az eredmény 1 hiba D_1-ben.

8. feladat

Megoldás. A fő észrevételek:

- hibák a vett $D_1, D_2, D_3, P_1, P_2, P_3$ között lehetnek.
- ha nincs bennük hiba, akkor $E_1 E_2 E_3 = 000$.
- ha egyetlen hiba van, és az P_1, P_2 vagy P_3 valamelyikében, akkor E_1, E_2 és E_3 közül egy lesz egyes.
- ha egyetlen hiba van, és az D_1, D_2 vagy D_3 valamelyikében, akkor E_1, E_2 és E_3 közül kettő lesz egyes.
- A ML dekódoló minden $E_1 E_2 E_3$ szindróma esetén azt a lehetséges hiba-konfigurációt választja, amelyikben a legkevesebb hiba van.

Ha $E_1 E_2 E_3 = 000$, az eredmény az, hogy nincs hiba.

Ha $E_1 E_2 E_3 = 010$, az eredmény 1 hiba P_2-ben.

Ha $E_1 E_2 E_3 = 101$, az eredmény 1 hiba D_1-ben.

Ha $E_1 E_2 E_3 = 111$, az eredmény több hiba.

Elméleti korlátok

Singleton-korlát: tetszőleges $C(n, k)$ kódra

$$d_{\min} \leq n - k + 1.$$

Ha egy kódra a Singleton-korlátban egyenlőség áll, azt Maximum Distance Separable (MDS) kódnak nevezzük.

Elméleti korlátok

Singleton-korlát: tetszőleges $C(n, k)$ kódra

$$d_{\min} \leq n - k + 1.$$

Ha egy kódra a Singleton-korlátban egyenlőség áll, azt Maximum Distance Separable (MDS) kódnak nevezzük.

Hamming-korlát: ha egy $C(n, k)$ bináris kód t hibát tud javítani, akkor

$$\sum_{i=0}^{t} \binom{n}{i} \leq 2^{n-k}.$$

Ha egy kódra a Hamming-korlátban egyenlőség áll, azt perfekt kódnak nevezzük.

9. feladat

A következő kódra teljesül-e az MDS (Maximum Distance Separable) tulajdonság?

$$c_1 = (00000), \qquad c_2 = (11111)$$

9. feladat

A következő kódra teljesül-e az MDS (Maximum Distance Separable) tulajdonság?

$$c_1 = (00000), \qquad c_2 = (11111)$$

Megoldás. $n = 5$, $2^k = 2$, tehát $k = 1$, és $d_{\text{min}} = 5$;

$$d_{\text{min}} = 5 = n - k + 1 = 5 - 1 + 1$$

teljesül, tehát a kód MDS.

10. feladat

A következő kódra teljesül-e a MDS tulajdonság? (Ez a 7. feladat kódja.)

$$\begin{array}{cccc} (000000), & (001011), & (010110), & (011101) \\ (100101), & (101110), & (110011), & (111000) \end{array}$$

10. feladat

A következő kódra teljesül-e a MDS tulajdonság? (Ez a 7. feladat kódja.)

$$\begin{matrix} (000000), & (001011), & (010110), & (011101) \\ (100101), & (101110), & (110011), & (111000) \end{matrix}$$

Megoldás. $n = 6, k = 3, d_{\text{min}} = 3.$

$$n - k + 1 = 6 - 3 + 1 \neq d_{\text{min}} = 3$$

Nem, ez nem egy MDS kód.

11. feladat

Egy perfekt kódra $n = 15$, és a kód $t = 1$ hibát képes javítani. Mennyi k értéke?

11. feladat

Egy perfekt kódra $n = 15$, és a kód $t = 1$ hibát képes javítani. Mennyi k értéke?

Megoldás. Perfekt kódokra a Hamming-korlátban egyenlőség áll:

$$\begin{aligned} \sum_{i=0}^{t} \binom{n}{i} &= 2^{n-k} \\ n + 1 &= 2^{n-k} \\ 16 &= 2^{15-k}, \end{aligned}$$

tehát $k = 11$.