Diszkrét matematika II. feladatok

Tizenegyedik alkalom

Bemelegítő feladatok

1. Tekintsük az alábbi bináris kódolást:

$$00 \mapsto 00000, \quad 01 \mapsto 01110, \quad 10 \mapsto 10101, \quad 11 \mapsto 11011.$$

a) Mekkora a 01110 és az 10101 kódszavak távolsága?

Megoldás: Az 1.,2.,4.,5. karakterek térnek el, ezért $d\begin{pmatrix}01110\\10101\end{pmatrix} = 4$ a két szó távolsága.

b) Mekkora a kód távolsága?

Megoldás: $d\begin{pmatrix}00000\\01110\end{pmatrix} = 3$, $d\begin{pmatrix}00000\\10101\end{pmatrix} = 3$, $d\begin{pmatrix}00000\\11011\end{pmatrix} = 4$, $d\begin{pmatrix}01110\\10101\end{pmatrix} = 4$, $d\begin{pmatrix}01110\\11011\end{pmatrix} = 3$, $d\begin{pmatrix}10101\\11011\end{pmatrix} = 3$, ezek között a $d = 3$ a legkisebb, ez a kód távolsága.

c) Mennyi az 11011 kódszó súlya?

Megoldás: $w(11011) = 4$, hiszen négy nemnulla karakter van benne.

d) Mennyi a kód súlya?

Megoldás: A legkisebb súlyú (nemcsupanulla) kódszó súlya $w = 3$, ez a kód súlya.

e) Adja meg a 00000 kódszóhoz legfeljebb 1 távolságra levő $\mathbb{Z}_2^5$-beli szavak halmazát!

Megoldás: $\big\{(10000), (01000), (00100), (00010), (00001), (00000)\big\}$

f) A 01000 szót mire dekódoljuk minimális távolságú dekódolással?

Megoldás: Mivel Hamming-metrikában a (00000) kódszó van hozzá a legközelebb, ezért erre dekódoljuk.

Gyakorló feladatok

2. Az alábbi bináris kódok esetében állapítsa meg a kód távolságát, hibajelző és hibajavító képességét!

a) $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1 + c_2 + c_3 + 1)$;

Megoldás: Ha $c_1' \neq c_1, c_2' = c_2, c_3' = c_3$, akkor $c_1' + c_2' + c_3' + 1 \neq c_1 + c_2 + c_3 + 1$ azaz ekkor KÉT koordináta tér el. Hasonlóan $c_1' = c_1, c_2' \neq c_2, c_3' = c_3$ és $c_1' = c_1, c_2' = c_2, c_3' \neq c_3$ esetén is két-két koordináta tér el a kódszavakban.

Ha c_1, c_2, c_3 és c_1', c_2', c_3' közül kettő is eltér, akkor is legalább két koordinátában különbözik a két kódszó.

Mivel $(0, 0, 0, 1)$ és $(1, 0, 0, 0)$ kódszavak pontosan két koordinátában különböznek, ezért $d = 2$-nél nem nagyobb a kódtávolság. Vagyis $d = 2$ a kód távolsága.

$d = 2$ távolságú kód $d - 1 = 1$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibát tud javítani.

b) $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1, c_2 + c_3)$;

Megoldás: $d = 2$ a kód távolsága. $d = 2$ távolságú kód $d - 1 = 1$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibát tud javítani.

c) $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1, 1 - c_2c_3)$.

Megoldás: $(1, 1, 0, 1, 1)$ és $(1, 0, 1, 1, 1)$ kódszavak távolsága $d = 1$, így $d = 1$ a kód távolsága. $d = 1$ távolságú kód $d - 1 = 0$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibát tud javítani.

d) $(c_1, c_2) \mapsto (c_1, c_2, c_1 + c_2)$.
Megoldás: A kód $K = \{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\}$, $d = 2$ a kód távolsága, azaz $d - 1 = 1$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibát tud javítani.

e) $(c_1, c_2) \mapsto (c_1, c_2, c_1 + c_2, \max\{c_1, c_2\})$.
Megoldás: $K = \{(0,0,0,0), (1,0,1,1), (0,1,1,1), (1,1,0,1)\}$, $d = 2$ a kód távolsága, azaz $d - 1 = 1$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibát tud javítani.

3. Tekintsük az alábbi kódokat adott ábécé felett: Határozza meg a kódok távolságát, hibajelző, hibajavító képességét, ellenőrizze, hogy MDS kódok-e?

a) $(c_1, c_2) \mapsto (c_1, c_2, c_1 + c_2)$, $c_1, c_2 \in \mathbb{F}_5$;
Megoldás: $d = 2$ a kód távolsága, azaz $d-1 = 1$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibát tud javítani. A $|K| \leq q^{n-d+1}$ Singleton-korlát itt $25 \leq 5^{3-2+1}$ egyenlőséggel teljesül, tehát MDS-kód.

b) $(c_1, c_2) \mapsto (c_1, c_2, c_1 + c_2)$, $c_1, c_2 \in \mathbb{F}_7$;
Megoldás: $d = 2$ a kód távolsága, azaz $d-1 = 1$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibát tud javítani. A $|K| \leq q^{n-d+1}$ Singleton-korlát itt $49 \leq 7^{3-2+1}$ egyenlőséggel teljesül, tehát MDS-kód.

c) $(c_1, c_2) \mapsto (c_1, c_2, c_1 + c_2, c_1 \cdot c_2)$, $c_1, c_2 \in \mathbb{F}_7$;
Megoldás: $d = 2$ a kód távolsága, azaz $d - 1 = 1$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibát tud javítani. A $|K| \leq q^{n-d+1}$ Singleton-korlát itt $49 \leq 7^{4-2+1}$ NEM egyenlőséggel teljesül, tehát NEM MDS-kód.

d) $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1 + c_2, c_1 + c_3)$, $c_1, c_2, c_3 \in \mathbb{F}_3$;
Megoldás: $d = 2$ a kód távolsága, azaz $d - 1 = 1$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibát tud javítani. A $|K| \leq q^{n-d+1}$ Singleton-korlát itt $27 \leq 3^{5-2+1}$ NEM egyenlőséggel teljesül, tehát NEM MDS-kód.

e) $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1 + c_2, c_1 + c_3, c_2 + c_3)$, $c_1, c_2, c_3 \in \mathbb{F}_3$.
Megoldás: $d = 3$ a kód távolsága, azaz $d-1 = 2$ hibát jelez, és $\lfloor \frac{d-1}{2} \rfloor = 1$ hibát tud javítani. A $|K| \leq q^{n-d+1}$ Singleton-korlát itt $27 \leq 3^{5-3+1}$ egyenlőséggel teljesül, tehát MDS-kód.

4. Tekintsük a $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1 + c_2 + c_3, c_1 + 2c_2 + 3c_3)$ kódot! Mennyi a kód távolsága, ha modulo 5 ill. modulo 4 értelmezzük a kódot?

Megoldás: Modulo 5 nincsenek nullosztók, így ha az üzenetszegmensben egy-egy eltérés van, akkor a paritásszegmens mindkét karaktere elér, és így 3 lesz a távolság. Ha az üzenetszemensben két karakter tér el, a paritásszegmens két karaktere közül legalább az egyik el fog térni, így ekkor is legalább 3 lesz a távolság, ha mindhárom első karakter eltér, akkor nyilván legalább 3 a távolság, azaz a kód távolsága $d = 3$.

Modulo 4 viszont vannak nullosztók, így $2c_2 \equiv 0$ akkor is, ha $c_2 = 0$ és akkor is, ha $c_2 = 2$. Tehát a $(0,0,0,0,0)$ és a $(0,2,0,2,0)$ kódszavak távolsága csak $d = 2$. (A negyedik karakter biztsan eltér, ha az első három karakter közül csak egy tér el, így lealább 2 lesz két kódszó távolsága.) Azaz ekkor a kód távolsága $d = 2$.

Érdekes feladatok

5. Alice gondolt egy számra 1 és 16 között, amit Bob szeretne kitalálni barkochbában (kérdésekre a lehetséges válsz: igen/nem).

a) Bobnak hány kérdést kell feltenni, ha kérdéseit előre, írásban kell elküldenie Alicenak (azaz az adott kérdés nem függhet Alice korábbi válaszaitól).
Megoldás: Négy kérdés kell, és annyi elég is. Ha n az Alice által gondolt szám, akkor Bob kérdezze végig $n - 1$ (ez már 0 és 15 közötti szám) kettes számrendszerbeli alakjának számjegyeit.

b) Bob tudja, hogy Alice megbízhatatlan, és bizonyos kérdésekre elfelejt válaszolni. Hány kérdést kell feltenni, ha Alice legfeljebb egy kérdésre felejt el válaszolni?

Megoldás: Öt kérdés elég lesz, ha elsőre azt a négy bitet kérdezi meg, mint az előző feladat négy kérdésében, ötödiknek pedig a paritásbitet (az $n-1$ kettes számrendszerbeli alakjában az 1-esek számának paritását).

Ha Alice az utolsó kérdésre nem válaszol, akkor megvan az $n-1$ összes számjegye. Ha ezek közül felejt el valamit, akkor a másik három ismeretében és a paritásbit ismretében tudni lehet, hogy az elflejtett bit mi lehet.

c) És ha Alice legfeljebb két kérdésre felejt el válaszolni? Adja meg a kérdéseket is!

Megoldás: Olyan bináris kód kell, amiben bármely két kódszó megkülönböztethető akkor is, ha mindkettőből ugyanazt a két karaktert töröljük (ezt felejti el Alice). Azaz a kód távolsága legalább $d = 3$.

Singleton korlát szerint $16 = |K| \leq 2^{n-3+1}$, azaz $4 \leq n-2$, vagyis $n \geq 6$. A Hamming-korlát szerint (mivel $d = 3$ és így $t = 1$), $16 = |K| \cdot (1+n) \leq 2^n$, azaz $n+1 \leq 2^{n-4}$. Ez $n = 6$ esetén sérül, hiszen $6+1 > 2^2$, de $n = 7$-re már teljesül, hiszen $7+1 = 2^3$, méghozzá egyenlőséggel. Azt a bináris kódot, ami $n = 7$ hosszú bitsorozatokból áll, és bármely két kódszó távolsága legalább $d = 3$, Hamming-kódnak nevezik. És például a következő mátrix a paritásellenőrzőmátrixa:

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

Azaz, ha (c_1, c_2, c_3, c_4) az $n-1$ szám kettes számrendszerbeli alakjának számjegyei, mint bitek, akkor a következő hét bitet kérdezzük meg:

$$c_1, \quad c_2, \quad c_3, \quad c_4, \quad c_1+c_2+c_3 \pmod 2, \quad c_1+c_2+c_4 \pmod 2, \quad c_1+c_3+c_4 \pmod 2$$

6. Most Bob Cecile-el játszik barkochbát, aki azonban nem feledékeny, hanem rosszindulatú: néha hazudik.

a) Bobnak hány kérdést kell feltenni, hogy kitalálja a Cecile által gondolt számot 1 és 16 között, ha Cecile legfeljebb egyszer hazudik. Adja meg a kérdéseket is!

Megoldás: Ha egyszer hazudik Cecil, akkor $t = 1$ hibajavító kód kell, ami $d = 3$ távolságú, azaz pont jó lesz ugyanaz, mint az előző feladat c) részében.

b) Bobnak hány kérdést kell feltenni, ha Cecile legfeljebb 2-szer hazudik? És ha legfeljebb 16-szor?

Megoldás: Ha Cecil legfeljebb 2-szer hazudik, akkor $t = 2$ hibajavító, azaz $d = 5$ távolságú kód kell. Ha 16-szor is hazudhat, akkor $t = 16$ hibajavító kód kell, ami $d = 2t+1 = 33$ távolságú.

Szorgalmi feladatok

7. Tekintsük a 6 hosszú bináris sztringeket, amikben pontosan 3 darab 1-es van. Hány darab választható ki közülük, hogy a páronkénti távolságuk legalább 3 legyen?