Diszkrét matematika II. feladatok

Tizenkettedik alkalom

Bemelegítő feladatok

1. Tekintsük az alábbi kódokat. Ellenőrizze, hogy lineáris-e a kód, és abban az esetben írja fel a kód generátor és ellenőrzőmátrixát! Adja meg az n, k paramétereket!

   a) $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1 + c_2 + c_3)$, $c_1, c_2, c_3 \in \mathbb{F}_2$;
   Megoldás: Ez a legegyszerűbb paritásbites kód. Lineáris, hiszen $(c_1, c_2, c_3, c_1 + c_2 + c_3) = c_1 \cdot (1, 0, 0, 1) + c_2 \cdot (0, 1, 0, 1) + c_3 \cdot (0, 0, 1, 1)$, azaz minden kódszó három vektor lineáris kombinációjaként áll elő, és minden ilyen lineáris kombináció kódszó, azaz a kód egy altér. Oszlopvektorokkal felírva: $K = \text{Span}\left\{\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\end{pmatrix}\right\}$, vagyis $G = \left(\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\right)$ a generátormátrix. Ez egy szisztematikus kód, azaz az ellenőrzőmátrixa a generátormátrixából úgy készül, hogy az (itt 3×3-as) egységmátrix-blokk alatti blokk (mínusz egyszerese, de modulo 2 az ugyanaz) mellé írunk egy (itt 1×1-es) egységmátrixot: $H = \big([1 \quad 1 \quad 1] \quad [1]\big)$.
   $n = 4$ a kódszavak hossza (ennyi sora van a generátormátrixnak), $k = 3$ a kód, mint altér dimenziója (ennyi oszlopa van a generátormátrixnak).

   b) $(c_1, c_2) \mapsto (c_1, c_2, c_1 + c_2, \max\{c_1, c_2\})$, $c_1, c_2 \in \mathbb{F}_2$;
   Megoldás: NEM lineáris a kód, mert nem altér a kódszavak halmaza:

   $$K = \{(0, 0, 0, 0),\ (1, 0, 1, 1),\ (0, 1, 1, 1),\ (1, 1, 0, 1)\},$$

   ebben a halmazban ugyan benne van a nullvektor, de például a második és harmadik kódszó koordinátánkénti összege $(1, 0, 1, 1) + (0, 1, 1, 1) = (1, 1, 0, 0)$ NEM kódszó, azaz lineáris kombináció műveletére NEM zárt a K halmaz, így nem lehet altér.
   Nem lineáris a kód, így nincs neki sem generátormátrixa, sem ellenőrzőmátrixa, és k paramétere sem. ($n = 4$ a kódszavak hossza, ez a paraméter megadható.)

   c) $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, 2c_1 + 3c_2, c_1 + 4c_3)$, $c_1, c_2, c_3 \in \mathbb{F}_5$;
   Megoldás: Lineáris a kód, hiszen oszlopvektorokkal felírva a következő mátrix oszlopvektorai által feszített alteret alkotják a kódszavak:

   $$G = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\2&3&0\\1&0&4\end{pmatrix} = \left(\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\right), \quad \text{mivel} \quad \begin{pmatrix}c_1\\c_2\\c_3\\2c_1+3c_2\\c_1+4c_3\end{pmatrix} = c_1 \cdot \begin{pmatrix}1\\0\\0\\2\\1\end{pmatrix} + c_2 \cdot \begin{pmatrix}0\\1\\0\\3\\0\end{pmatrix} + c_3 \cdot \begin{pmatrix}0\\0\\1\\0\\4\end{pmatrix}$$

   Mivel a G generátormátrix egy 3×3-as egységmátrix-blokkból és azalatt egy 2×3-as blokkból áll, ez egy szisztematikus kód, aminek az ellenőrzőmátrixa könnyen elkészíthető:

   $$H = \left(\begin{bmatrix}-2&-3&0\\-1&0&-4\end{bmatrix}\begin{bmatrix}1&0\\0&1\end{bmatrix}\right) \equiv \begin{pmatrix}3&2&0&1&0\\4&0&1&0&1\end{pmatrix} \pmod 5, \text{ hiszen } \mathbb{F}_5 \text{ fölött vagyunk.}$$

   A kódszavak hossza $n = 5$, a kód dimenziója $k = 3$ (ennyi oszlopa van a generátormárixnak).

   d) $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1, 1 - c_2c_3)$, $c_1, c_2, c_3 \in \mathbb{F}_5$;
   Megoldás: Ez NEM lineáris kód, hiszen a csupa nulla vektor nem kódszó: ha az első három koordináta $c_1 = c_2 = c_3 = 0$, akkor az utolsó koordináta $1 - 0 \cdot 0 = 1$ NEM lehet nulla.
   Ezért NINCS sem generátormátrixa, sem ellenőrzőmátrixa, és nincs k paramétere sem. $n = 5$ a kódszavak hossza.

e) $(c_1, c_2, c_3) \mapsto (c_1 + 2c_2, c_2 + 3c_3, 4c_1 + c_3, 3c_2 + c_3)$, $c_1, c_2, c_3 \in \mathbb{F}_5$.

Megoldás: Lineáris: $c_1 \cdot (1,0,4,0) + c_2 \cdot (2,1,0,3) + c_3 \cdot (0,3,1,1)$, oszlopvektorokra áttérve $G = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 3 \\ 4 & 0 & 1 \\ 0 & 3 & 1 \end{pmatrix}$ a generátormátrix. Ez NEM szisztematikus kód. De ugyanezt az alteret egy *másik* mátrix képtereként is előállíthatjuk. A fenti G mátrix oszlopaiból új oszlpokat lineárisan kombinálva, hogy ugyanaz legyen a feszített alterük (oszlopokra alkalmazott Gauß-Jordan eljárással):

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 3 \\ 4 & 0 & 1 \\ 0 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 4 & -8 & 1 \\ 0 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & -8 & 25 \\ 0 & 3 & -8 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & -8 & 1 \\ 0 & 3 & \frac{-8}{25} \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \frac{32}{25} & \frac{11}{25} & \frac{-8}{25} \end{pmatrix} = G'$$

G' mátrix oszlopai ugyanazt az alteret generálják, mint G mátrix oszlopai, ezért ez egy alternatív generátormátrixa ugyanannak a kódnak. Ezzel viszont már szisztematikus a kód, és ehhez könnyedén elkészíthető az ellenőrzőmátrix: $H = (-\frac{32}{25}, -\frac{11}{25}, \frac{8}{25}, 1)$, vagy ennek számszorosa: $H' = (-32, -11, 8, 25)$. A kód hossza $n = 4$, dimenziója $k = 3$.

2. Tekintsük a kódszavak következő halmazát:

$$\mathcal{C} = \{(c_1, c_2 \ldots, c_7) \in \mathbb{F}_7 : \{c_1, c_2 \ldots, c_7\} = \{1, 2, \ldots, 7\}\}.$$

Lineáris-e a kód? Mi lesz a kódtávolság?

Megoldás: Vagyis az $(1,2,3,4,5,6,0)$ héthosszú sorozat összes lehetséges permutációi (mind a 7!) alkotják a kódszavat. Mivel a $(0,0,0,0,0,0,0)$ nyilvánvalóan NEM permutációja $\mathbb{F}_7$ elemeinek, ezért a nullvektor nem kódszó, így a kód nem altér, vagyis a kód NEM lineáris kód.

Az nem lehet, hogy ugyanazon 7 elem két különböző permuációja csak egyik pozícióban térjen el egymástól: ha $(c_1, c_2 \ldots, c_7)$ és $(a_1, a_2 \ldots, a_7)$ is kódszavak, azaz az $\mathbb{F}_7$ elemeinek permutációi, és $c_k \neq a_k$, akkor $\exists j \in \{1, \ldots, 7\} : j \neq k$, hogy $c_k = a_j$, de akkor $a_j \neq c_j$, azaz legalább kettő a Hamming-távolság bármely két különböző kódszó között. Mivel van két olyan kódszó, aminek pontosan kettő a Hamming-távolsága (például $(1,2,3,4,5,6,0)$ és $(1,2,3,4,5,0,6)$ távolsága épp kettő), ezért a kód távolsága $d = 2$.

3. Tekintsük a következő mátrixokat:

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad G_3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

Tekintsük az adott mátrixokhoz, mint generátormátrixokhoz tartozó (n, k) lineáris kódokat. Adja meg az n, k és a kódtávolság értékeit! Add meg valamelyik ellenőrző mátrixát!

Megoldás: Az n a generátormátrix sorainak száma, a k pedig a generátormátrix oszlopainak száma (tényleg teljes rangú mátrixokról van szó, ez könnyen látható, lineárisan függetlenek az oszlopaik). Tehát az első esetben $[n, k] = [7, 4]$, a második esetben $[n, k] = [7, 3]$, az utolsó esetben $[n, k] = [5, 3]$.

A kódtávolság könyebben meghatározható, ha ismerjük az ellenőrzőmátrixoat, ezért előbb azokat adjuk meg. G_1 és G_2 szisztematikus generátormátrixok, azokhoz azonnal tudunk ellenőrzőmátrixot megadni: a 4×4-es, illetve 3×3-as egységmátrix-blokk alatti blokk mínusz egyszerese mellé kell 3×3-as, illetve 4×4-es egységmátrix-blokkokat illeszteni:

$$H_1 = \begin{pmatrix} -1 & -1 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 & 1 & 0 \\ -1 & -1 & -1 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad H_2 = \begin{pmatrix} -1 & -1 & -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & -1 & -1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A harmadik generátormátrixot előbb célszerű átalakítani szisztematikussá az oslopaira alkalmzott Gauß-Jordan eljárással (első lépésben a második oszlopot kivonva a harmadikból, utána az első oszlopot a másodikból):

$$G_3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix} = G_3' \qquad H_3 = \begin{pmatrix} -1 & 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

A kódtávolság az ellenőrzőmátrixból úgy olvasható le, hogy a legkevesebb olyan oszlop száma, amik már lineárisan összefüggők. (Ha nincs H-ban csupa nulla oszlop, akkor $d > 1$, ha nincs két olyan oszlop, amik egymás skalárszorosai, akkor $d > 2$, és így tovább.) Egyik ellenőrző mátrixban sincs csupa nulla oszlop, de H_1-ben a harmadik és az utolsó oszlop egymás számszorosa, tehát az első kód távolsága $d = 2$.

H_2-ben nincs két oszlop, ami számszorosa lenne egymásnak, de van három, ami lineárisan összefüggő (a harmadik oszlophoz hozzáadva a negyedik és hatodik oszlopot a csupanulla oszlopvektort kapjuk), ezért a második kód távolsága $d = 3$.

A harmadik kód ellenőrző mátrixában van két azonos oszlop (például második és a negyedik, de az ötödik és a harmadik is megegyezik), ezért a harmadik kód távolsága $d = 2$.

Gyakorló feladatok

4. Tekintsük az 1. feladatban szereplő kódokat! Ellenőrizze, hogy a kódok MDS ill. perfekt kódok-e!

   Megoldás: Emlékeztetőül a Singleton-korlát $|K| \leq q^{n-d+1}$, ahol $|K|$ a kódszavak száma. Lineáris kódokra $k \leq n - d + 1$, mivel ott $|K| = q^k$. Az a kód MDS, amire egyenlőség teljesül.

   Az 1/a) kód a paritásbites lineáris kód, $n = 4$, $k = 3$, $d = 2$ (mert a $H = (1, 1, 1, 1)$ sormátrixnak van két azonos oszlopa), a Singleton-korlát $3 \leq 4 - 2 + 1$ egyenlőséggel teljesül, azaz MDS-kód.

   Az 1/b) kód nem lineáris, a négy kódszó között a legkisebb távolság kettő, azaz $d = 2$, a Singleton-korlát $4 \leq 2^{4-2+1}$ NEM egyenlőséggel teljesül.

   Az 1/c) kód lineáris, az ellenőrző mátrixából leolvasható, hogy $d = 2$, hiszen a harmadik és ötösik oszlopa egymás számszorosa (sőt: megegyeznek). A Singleton-korlát $3 \leq 5 - 2 + 1$ NEM egyenlőséggel teljesül.

   Az 1/d) kód nem lineáris, $|K| = 7!$, $n = 7$, $d = 2$, azaz a Singleton-korlát $7! \leq 7^{7-2+1}$, azaz $5040 \leq 117647$, NEM egyenlőséggel teljesül.

   Az 1/e) kód lineáris, $n = 4$, $k = 3$, $d = 2$, azaz Singleton-korlát $3 \leq 4 - 2 + 1$ egyenlőséggel teljesül, azaz MDS-kód.

   Emlékeztetőül a Hamming-korlát t-hibajavító kódokra $|K| \cdot \sum_{j=0}^{t} \binom{n}{j} \cdot (q-1)^j \leq q^n$. Az a kód perfekt, amire egyenlőséggel teljesül. Ha $d = 1, 2$, akkor $t = 0$, ha $d = 3$, akkor $t = 1$. A $t = 0$ esetben (és mindegyik esetben $d = 2$, azaz $t = 1$) a Hamming-korlát triviális: $|K| \cdot 1 \leq q^n$,

ez csak akkor teljesülhet egyenlőséggel, ha minden lehetséges karaktersorozat kódszó. Ez sem 1/a), sem 1/b), sem 1/c), sem 1/d), sem 1/e) esetén nem teljesül, azaz egyik kód sem perfekt az 1. feladatban.

5. Tekintsük az alábbi lineáris kódolást: $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1 + c_2, c_3, c_1 + c_3)$.

   Adja meg a kód két-két különböző generátor- és ellenőrző mátrixát!

   Megoldás: Először a legkézenfekvőbb szisztematikus generátormátrixot adjuk meg, és a belőle elkészíthető ellenőrzőmátrixot:

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

   A fenti G mátrix egyik oszlopát hozzáadva egy másik oszlopához ugyanannak az altérnek egy másik bázisát adja az új mátrix három oszlopa, azaz jó lesz másik generátormátrixnak. Az ellenőrzőmátrix esetén a sorokkal lehet ugyanezt az eljárást csinálni, hogy másik ellenőrző mátrixát kapjuk ugyanazon kódnak:

$$G' = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \qquad H' = \begin{pmatrix} -1 & -1 & 0 & 1 & 0 & 0 \\ -1 & -1 & -1 & 1 & 1 & 0 \\ -1 & 0 & -1 & 0 & 0 & 1 \end{pmatrix}$$

Érdekes feladatok

6. Tekintsünk a $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1 + c_2, c_1 + c_3, c_2 + c_3)$ bináris kódolást! Mennyi lesz a kód távolsága? Hány olyan *tetszőleges* szó (azaz nem feltételenül kódszó) van $\mathbb{F}_2^5$-ben, ami minden kódszótól legalább 2 távolságra van?

   Megoldás: Készítsük el a generátormátrixot, annak segítségével az ellenőrzőmátrixot,és mivel modulo 2 a plusz és a mínusz ugyaaz, az előjeleket ki sem írjuk:

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

   Az ellenőrzőmátrixban nincs csupa nulla oszlop, és nincs két oszlop, ami egymás számszorosa lenne (viszont van három összefüggő oszlopa, például az első, a negyedik és az ötödik), ezért a kód távolsága $d = 3$, amiből követezoik, hogy $t = 1$ a hibajavító képessége.

   A Hamming-korlát $t = 1$ esetben, $q = 2$ bináris kódokra: $|K| \cdot \left(\binom{n}{0} \cdot 1^0 + \binom{n}{1} \cdot 1^1 \right) \leq 2^n$. Vagyis $2^k \cdot \big(1 + n\big) \leq 2^n$, ha k-dimenziós lineáris a kódról van szó. Átrendezve $n + 1 \leq 2^{n-k}$. Akkor perfekt a kód, ha egyenlőséggel teljesül. Itt most $n = 6$, $k = 3$, $n - k = 3$, $n + 1 = 7$, és a $7 \leq 8$ nem egyenlőséggel teljesül, ezért NEM perfekt a fenti kód.

7. Döntse el, hogy az alábbi n, k, d választással létezik-e $\mathbb{F}_q$ feletti $[n, k, d]$ lineáris kód! Ha nem, indokoljon, ha igen, mutasson példát!

   a) $[7, 6, 2]$, $q = 5$ b) $[8, 6, 3]$, $q = 2$ c) $[8, 6, 3]$, $q = 9$ d) $[6, 4, 3]$, $q = 2$ e) $[6, 4, 3]$, $q = 5$

   Megoldás: Lineáris kódok esetén a Singleton-korlát $k \leq n - d + 1$, a Hamming-korlát $t = 1$ ($d = 3$) esetén pedig $|K| \cdot \left(\binom{n}{0} \cdot (q-1)^0 + \binom{n}{1} \cdot (q-1)^1 \right) \leq q^n$. Vagyis $q^k \cdot \big(1 + n \cdot (q-1)\big) \leq q^n$, átrendezve $n \cdot (q-1) + 1 \leq q^{n-k}$.

   a) $[7, 6, 2]_5$ esetén $6 \leq 7 - 2 + 1$ teljesül, a Hamming-korlát triviális, az is teljesül, és tényleg létezik ilyen kód: a paritásbit kódjához hasonló, csak nem bináris, hanem modulo 5 számolva: $(c_1, \ldots, c_6) \mapsto (c_1, \ldots, c_6, c_1 + \cdots + c_6)$.

   b) $[8, 6, 3]_2$ NEM létezik, mert sérül a Hamming korlát: $8 + 1 \leq 2^{8-6}$, de $9 > 4$.

   c) $[8, 6, 3]_9$ csak a $q = 9$ ($q = 2$ helyett) a különbség, de ezzel már teljesül a Hamming-korlát: $8 \cdot (9-1) + 1 \leq 9^{8-6}$, azaz $65 \leq 81$, a Singleton-korlát is teljesül: $6 \leq 8 - 3 + 1$, méghozzá egyenlőséggel.

   Olyan ellenőrzőmátrixot kell megadni, aminek $n - k = 2$ sora és $n = 8$ oszlopa van, és semelyik két oszlopa sem számszorosa egymásnak. Ha $\alpha \in \mathbb{F}_9$ egy generátoreleme a kilenc elemű testnek (aminek a hatványaiként az összes nemulla testelem előáll és $\alpha^8 = 1$), akkor például:

$$H = \begin{pmatrix} \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

   azaz az első sorban fel van sorolva majdem minden testelem, ez teljesíti a kívánt feltételeket.

   d) $[6, 4, 3]_2$ NEM létezik, mert sérül a Hamming-korlát: $6 + 1 \leq 2^{6-4}$, de $7 > 4$.

   e) $[6, 4, 3]_5$ csak a $q = 5$ ($q = 2$ helyett) a különbség, de ezzel már teljesül a Hamming-korlát: $6 \cdot 4 + 1 \leq 5^{6-4}$, azaz $25 \leq 25$, méghozzá egyenlőséggel, ez perfekt kód, ha létezik ilyen. A Singleton-korlát is teljesül: $4 \leq 6 - 3 + 1$, ez is egyenlőséggel, ez MDS-kód is, ha létezik.

   Olyan ellenőrzőmátrix kell megint, aminek $n - k = 2$ sora ls $n = 6$ oszlopa van, és semelyik két oszlopa sem számszorosa egymásnak.

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

   azaz az egységmátrix előtti blokkban az első sorban fel van sorolva minden testelem, ez teljesíti a kívánt feltételeket.

8. Legyen $n = 5, k = 2, d = 4$. Milyen q esetén létezik $[n, k, d]$ paraméterű lineáris kód $\mathbb{F}_q$ fölött? Válaszát indokolja!

   Megoldás: $2 = k \leq n - d + 1 = 5 - 4 + 1$ Singleton-korlát teljesül. A Hamming-korlát $d = 4$ esetén is csak $t = 1$-re mondható ki: $n \cdot (q-1) + 1 \leq q^{n-k}$, vagyis itt $5 \cdot (q-1) + 1 \leq q^{5-2}$, vagyis $5 \cdot q - 4 \leq q^3$. Vagyis $q^3 - 5q + 4 \geq 0$. Az egyenlőtlenségben szereplő harmadfokú polinomnak látványosan gyöke a $q = 1$, azaz $q^3 - 5q + 4 = (q-1) \cdot (q^2 + q - 4)$, ha $q > 1$, akkor ennek az előjele $q^2 + q - 4$ előjelétől függ, ami $\frac{-1-\sqrt{5}}{2}$ és $\frac{-1+\sqrt{5}}{2}$ között negatív, azaz $q > 1$ esetén mindig pozitív. Tehát sem a Singleton-korlátból, sem a Hamming-korlátból nem jön ki ellentmondás semmilyen $q = p^m$ prímhatvány esetére. Viszont a Hamming-korlát $d = 3$-ra is ugyanez lenne, ezért az, hogy nem sérül, nem sokat jelent.

   Ha tudunk olyan ellenőrzőmátrixot konstruálni, aminek $n - k = 3$ sora és $n = 5$ oszlopa van, és bármelyik három oszlopa lineárisan függelten, akkor van ilyen kód. Ha nincs ilyen mátrix, akkor annak ellenére sincs ilyen kód, hogy nem sérti a két tanult korlátot.

Ha létezik olyan α testelem, amire $\alpha+1 \neq 0$ és $\alpha \neq 0$, akkor $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ \alpha & 1 & 0 & 1 & 0 \\ 1+\alpha & 1 & 0 & 0 & 1 \end{pmatrix}$ mátrix bármly három oszlopa lineárisan független lesz. Minden $q > 2$ esetén léterzik ilyen testelem, de $q = 2$ esetén nem.

Szorgalmi feladatok

9. Írjon programot, mely egy adott szisztematikus kódoláshoz tartozó G generátormátrix esetén meghatározza a kód minimális távolságát!