Golay-kódos feladatok megoldásai

2. A G_{24} Golay-kód egy $[24, 12, 8]_2$ paraméterű kód. Egy koordinátáját elhagyva kapjuk a G_{23} $[23, 12, 7]_2$ paraméterű Golay-kódot. Mutasd meg, hogy G_{23} perfekt kód.

Megoldás: A G_{23} kód perfektsége következik abból, hogy a Hamming-korlátot egyenlőséggel teljesíti :

$$\frac{2^{23}}{1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}} = \frac{2^{23}}{2^{11}} = 2^{12}.$$

3. (a) Legyen A_i az i súlyú szavak száma G_{23}-ban. A G_{23} kód perfektségét felhasználva mutasd meg, hogy $A_0 = A_{23} = 1$, $A_7 = A_{16} = 253$, $A_8 = A_{15} = 506$, $A_{11} = A_{12} = 1288$.

(b) Legyen $\overline{A_i}$ a G_{24} Golay-kódban a i súlyú szavak száma G_{24}-ban. Határozd meg az $\overline{A_i}$ számokat.

Megoldás: A G_{23} kód perfekt ami azt jelenti, hogy minden 23 hosszú $0-1$ sorozat pontosan egy kódszó körüli három Hamming-sugarú gömbben van benne. Jelölje A_i az i hosszú kódszavak számát, ekkor az előbbi észrevétel szerint

$$\binom{23}{i} = \sum_{j=i-3}^{i+3} \left(\sum_{\substack{r+s\leq 3 \\ r-s=j-i}} \binom{j}{r}\binom{23-j}{s} \right) A_j.$$

Ebből rekurziót kapunk A_i-re $A_0 = 1$-t felhasználva. Ebből kapjuk, hogy $A_0 = A_{23} = 1$, $A_7 = A_{16} = 253$, $A_8 = A_{15} = 506$ és $A_{11} = A_{12} = 1288$. Ebből az eredeti C kód súlypolinomjának $\bar{A}_i$ együtthatói:

$$\bar{A}_0 = \bar{A}_{24} = 1 \qquad \bar{A}_8 = \bar{A}_{16} = 759 \qquad \bar{A}_{12} = 2576$$

(Az eredeti kódban nem lehet például 7 súlyú szó, mert akkor az egyik ilyen szó 1-est tartalmazó helyén lyukasztva a kapott 23 hosszú kódban lennének 6 súlyú szavak is. Hasonlóan $\bar{A}_9 = \bar{A}_{15} = \bar{A}_{17} = \bar{A}_{23} = 0$.)

4. Tekintsük a G_{24} Golay-kód 8 súlyú szavait és tekintsük ezeket egy blokkrendszer elemeinek. Mutasd meg, hogy az $\{1, 2, \ldots, 24\}$ bármely 5 elemére pontosan egy blokk illeszkedik. (Ez a blokkrendszer a *Witt-design*.)

Megoldás: Bármely 5 pontra legfeljebb egy blokk illeszkedhet, mert ha valamely 5 pontra két blokk is illeszkedne akkor lenne $c_1, c_2 \in C$ kódok 8 súllyal, melyekre $c_1 + c_2$ súlya legfeljebb 6 lenne, ez pedig nem lehet, mert a Golay-kód lineáris kód, így minden nem $\underline{0}$ kódszavának a súlya legalább 8. Most számoljuk meg kétféleképpen az (M, B) párokat, ahol $M \subset \{1, 2, \ldots, 24\}$ $|M| = 5$ és $M \subset B$ ahol B egy blokk. Mivel ezutóbbiak száma $\bar{A}_8 = 759$, így az ilyen párok száma $759 \cdot \binom{8}{5}$. Másrészt az ilyen párok száma legfeljebb $\binom{24}{5}$, mert minden 5 elemű halmazra legfeljebb egy blokk illeszkedik.

Mivel $759 \cdot \binom{8}{5} = \binom{24}{5}$ így minden 5 elemű halmazra pontosan egy blokknak kell illeszkednie.

5. Tekintsük a G_{23} Golay-kód 7 súlyú szavait. Hány közös 1-es lehet két ilyen kódszóban? Konstruálj egy $(253, 140, 87, 65)$ paraméterű erősen reguláris gráfot. Mi a komplementerének, mint erősen reguláris gráfnak a paraméterei?

Megoldás: Vegyük észre, hogy G_{23} minden 7-súlyú szava úgy keletkezik, hogy a G_{24} kód letörölt koordinátájaban 1-es állt ezen kódszavakban. A G_{24} kódban $0, 8, 12, 16, 24$ súlyú szavak voltak, ez a kód linearitása miatt azt jelenti, hogy két 8 súlyú szónak $0, 2$ vagy 4 közös 1-ese volt. Tehát a G_{23} két 7 súlyú szavában 1 vagy 3 darab közös 1 van.

Legyen G az a gráf, melynek csúcsai a G_{23} 7-súlyú szavai és kettő össze van kötve ha pontosan 3 darab közös 1-esük van. Megmutatjuk, hogy ez egy $(253, 140, 87, 65)$ paraméterű erősen reguláris gráfot határoz meg.

Azt már láttuk a 2. feladatban, hogy ennek a gráfnak 253 csúcsa van.

Mielőtt belekezdenénk a további paraméterek bizonyításába, két dolgot megjegyzünk. Mostantól a kódszavakat azonosítjuk azon 7-elemű halmazokkal, ahol 1-eseik vannak és $\mathcal{B}$ blokkrendszerbeli halmazokról fogunk beszélni az esetükben. A továbbiakban aktívan használni fogjuk, hogy minden 4-elemű halmazra pontosan egy ilyen blokkrendszerbeli 7-elemű halmaz illeszkedik, ez következik a 4. feladatból. Azt is használni fogjuk implicite, hogy ha két $\mathcal{B}$-beli halmaznak legalább két közös eleme van és ők nem egyeznek meg akkor valójában pontosan három közös elemük van.

Belátjuk, hogy a gráf 140-reguláris. Rögzítsünk egy A 7-elemű halmazt a blokkrendszerből. Legyen $S \subset A$, melyre $|S| = 3$. Vegyünk még egy $p \notin A$ elemet. Ekkor $S \cup \{p\}$-re illeszkedik pontosan egy B 7-elemű blokkrendszerbeli halmaz. Viszont minden ilyet pontosan 4-szer számoltunk, mert $|B \setminus A| = 4$. Mivel S-t $\binom{7}{3} = 35$, p-t pedig $23 - 7 = 16$ féleképpen választhattuk, így az ilyen B halmazok száma $35 \cdot 16/4 = 140$. Ezek éppen azon halmazok, amelyek A-t pontosan 3 elemben metszik. Tehát beláttuk, hogy a G gráf 140-reguláris.

Legyen $A, B \in \mathcal{B}$, melyekre $|A \cap B| = 3$. Keressük azon $C \in \mathcal{B}$ halmazok számát, melyekre $|A \cap C| = |B \cap C| = 3$. Legyen $A \cap B \cap C = T$. Ha $|T| = 3$ akkor ezeket úgy kaphatjuk, meg, hogy veszünk egy $p \notin A \cup B$ elemet és $T \cup \{p\}$-re pontosan egy ilyen halmaz illeszkedik, viszont minden ilyet 4 elemnél is megszámoltunk. Tehát $(23 - |A \cup B|)/4 = 12/4 = 3$ ilyen halmaz van. Ha $|T| = 2$ akkor $|C \cap (A \setminus B)| = |C \cap (B \setminus A)| = 1$, így erre a $2+1+1 = 4$ elemre éppen pontosan egy $\mathcal{B}$-beli halmaz illeszkedik. Mivel T-t 3, a $C \cap (A \setminus B)$ és $C \cap (B \setminus A)$ halmazokat (igazából elemeket) $4-4$ féleképpen választhatjuk meg, így ilyenből $3 \cdot 4 \cdot 4 = 48$ darab van. Ha $|T| = 1$ akkor $|C \cap (A \setminus B)| = |C \cap (B \setminus A)| = 2$, így ezutóbbi $2+2$ elemre illeszkedik éppen egy $\mathcal{B}$-beli halmaz. Ilyenből $\binom{4}{2}\binom{4}{2} = 36$ halmaz van. Maradt az az eset, hogy $|T| = 0$. Valójában ilyen nem lehet, mert ekkor a $v_A + v_B + v_C$ vektorban $|A \Delta B \Delta C| = 3$ darab 1-es lenne, de ilyen vektor nincs a G_{23} Golay-kódban. Tehát két összekötött csúcsnak $3 + 48 + 36 = 87$ közös szomszédja van.

Most legyen $A, B \in \mathcal{B}$, melyekre $|A \cap B| = 1$. Keressük azon $C \in \mathcal{B}$ halmazok számát, melyekre $|A \cap C| = |B \cap C| = 3$. Legyen $A \cap B \cap C = T$. Ha r azon C halmazok száma, melyre $|T| = 1$ és s azon halmazok száma, melyre $|T| = 0$. Ha kiválasztjuk $A \cap B$ elemet és még két elemet $B \setminus A$-ból illetve 1 elemet $A \setminus B$-ból akkor ezekre illeszkedik pontosan egy $\mathcal{B}$-beli halmaz. Ekkor $|T| = 1$, de minden halmazt kétszer számoltunk meg, mert $|C \cap (B \setminus A)| = 2$. Tehát $2r = \binom{6}{2}\binom{6}{1}$, így $r = 45$. Ha kiválasztunk két-két elemet $A \setminus B$ és $B \setminus A$-ból akkor ezzel 9-szer számoltuk meg azon halmazokat, melyekre $|T| = 0$ és pontosan 1-szer azokat, melyekre $|T| = 1$. Így $\binom{6}{2}^2 = 9s + r$, azaz $s = 20$. Tehát $r + s = 65$ közös szomszédja van a gráfban két összekötetlen csúcsnak a gráfban.

Általaban egy (n, k, λ, μ) paraméterű erősen reguláris gráf komplementere erősen reguláris gráf $(n, n-k-1, n-2k+\mu-2, n-2k+\lambda)$ paraméterekkel. Tehát G komplementerének a paraméterei $(253, 112, 36, 60)$.

6. Legyen N az ikozaéder élgráfjának adjacencia mátrixa. J a csupa 1 mátrix. Mutasd meg, hogy az $(I_{12}, J - N)$ mátrix a G_{24} generátormátrixa.

Megoldás: Az ikozaéder minden csúcsának 5 szomszédja van, továbbá két átellenes csúcsának nincs, két nem átellenes csúcsának pontosan két közös szomszédja van. Ebből következik, hogy $H = (I_{12}, J - N)$ bármely sorában 8 darab 1-es van és bármely két sor merőleges egymásra . Ezutóbbiból következik, hogy bármely két kódszó is merőleges egymásra.

Így a kód minden szava 4-gyel osztható súlyú, ez teljesül C soraira és ha c_1, c_2-re teljesül, akkor $c_1 + c_2$-re is :

$$|\mathrm{supp}(c_1 + c_2)| = |\mathrm{supp}(c_1)| + |\mathrm{supp}(c_2)| - 2|\mathrm{supp}(c_1) \cap \mathrm{supp}(c_2)|$$

hiszen $|\mathrm{supp}(c_1) \cap \mathrm{supp}(c_2)|$ páros, mert $(c_1, c_2) = 0$.

Az is világos, hogy a mátrix 12 dimenziós teret generál, hiszen az első 12 oszlop mutatja, hogy a 12 generáló vektor lineárisan független. Ebből következik, hogy a $C = C^{\perp}$. Ha C kódot a $H = (I, A)$ mátrix generálja akkor a $C^{\perp}$ altere $H^* = (-A^T, I)$ mátrix által generált altér. Most azonban $C = C^{\perp}$ 12 dimenziós, F_2 felett vagyunk és A szimmetrikus így C-t generálja a $(J - N, I_{12})$ mátrix is.

Most már bebizonyíthatjuk, hogy C nem tartalmaz 4-súlyú szót. Tegyük fel, hogy $c \in C$ és $w(c) = 4$. Írjuk fel c-t $c = (a, b)$ alakban ahol a és b két 12 hosszú vektor, $w(a) + w(b) = 4$. Ha $w(a) = 0$ akkor H mátrixból látszik, hogy $c = 0$, ez nem lehet. Ha $w(a) = 1$ akkor szintén H mátrixból látszik, hogy c a H egyik sora, de ekkor $w(c) = 8$, ez sem lehet. Ha $w(a) = 3$ vagy $w(a) = 4$ akkor $w(b) = 1$ vagy $w(b) = 0$ és H helyett H^* mátrixot használva jutnánk ellentmondásra. Ha $w(a) = 2$ akkor c két bázis vektor összege, de a bizonyítás első mondatából következik, hogy ezen vektorok súlya 8 vagy 12 aszerint, hogy két nem átellenes vagy két átellenes csúcshoz tartozó vektorokról van szó. Tehát C-ben nincs 4 súlyú szó, de minden szó súly osztható 4-gyel, így a minimális súly 8. Mivel a kód 12 dimenziós, így a Golay-kód egyértelműségéből következik, hogy C a Golay-kód.

7. Mutasd meg, hogy az alábbi mátrix egy $[11, 6, 5]_3$ paraméterű perfekt kód generátormátrixa

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 & 1 & 0 \end{pmatrix}$$

Ez a G_{11} ternáris Golay-kód. Hogy kapunk ebből egy G_{12} $[12, 6, 6]_3$ paraméterű kódot?

Megoldás: Tegyünk be egy 7. oszlopot a mátrixba az alábbi módon. Megmutatjuk, hogy a kapott mátrix egy $[12, 6, 6]_3$ paraméterű kód generátormátrixa.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & -1 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & 1 & 0 \end{pmatrix}$$

Először is vegyük észre, hogy ezen új mátrix minden sorában 6 darab nem 0 elem van vagyis minden vektor merőleges önmagára ($\mathbb{F}_3$ felett számolunk!). Sőt ez a 6 vektor egymásra is merőleges: elég leellenőrizni, hogy az első és a második sor merőleges az összes többire, mert a bal alsó 5×5 mátrix ciklikus. Ez mindössze 9 gyorsan ellenőrizhető dolog. Tehát a generátormátrix bármely két sora merőleges egymásra, így ez igaz tetszőleges két kódszóra is. Speciálisan minden kódszó súlya 3-mal osztható.

Ahhoz, hogy megmutassuk, hogy minden kódszó súlya legalább 6, elég megmutatni, hogy minden kódszó súlya legalább 4. Ez igaz a generátormátrix soraira és ha két ilyen sorvektort előjelesen összeadunk akkor az első 6 helyen is lesz két nem 0 és az utolsó két helyen is lesz két nem 0 elem a generátormátrix utolsó 6 helyében található 0-k miatt. Már csak azt kell megmutatni, hogy három vektort előjelesen összeadva nem kaphatunk az utolsó három koordinátaban csupa $\underline{0}$ vektort. Megállapítottuk, hogy a sorvektorok merőlegesek egymásra, így ez igaz az utolsó 6 koordináta által meghatározott vektorokra is. Így az általuk meghatározott 6×6 A mátrixra $AA^T = -I$. Vagyis A invertálható, tehát a 6 vektor lineárisan független, speciálisan bármely 3 vektor is lineárisan független. Ezzel megmutattuk, hogy a kapott mátrix egy $[12, 6, 6]_3$ paraméterű kód generátormátrixa.

Elhagyva a 7. koordinátát kapjuk egy $[11, 6, 5]_3$ paraméterű kód generátormátrixát. Ez perfekt, mert egyenlőséggel teljesíti a Hamming-becslést:

$$3^6 = \frac{3^{11}}{1 + 11 \cdot 2 + \binom{11}{2} \cdot 2^2},$$

mert $1 + 11 \cdot 2 + \binom{11}{2} \cdot 2^2 = 1 + 22 + 220 = 243 = 3^5$.