19. alkalom

Folytattuk a Kódok feladatgyűjtemény feldolgozását. Bemelegítésként a **Pénzes barkochbá**val foglalkoztunk, majd ismétlésként megoldottuk a **4.11** feladatot. "Kitöltöttünk" 3^{10} szelvényt, amelyekkel a 13-as totón biztosan elérünk 12 vagy 13 találatot. Ennek kapcsán megismerkedtünk a tökéletes kód, valamint a bináris és a ternér Hamming-kód fogalmával. Leellenőriztük a Golay-kódok paramétereit. A **"Jó 30-as"** feladat folytatásaként, a **Hétszögminták** előkészítése kedvéért megkerestük az **"Ideális 101-es"** sorozatokat.

Házi feladatnak a múlt óráról megmaradt: **hétszögminták**, **5.11**, új példa: **Általános Hamming-kód**, **"Ideális 1001-es"**.

A 19. szakkör részletezett anyaga

Pénzes barkochba (***Pósa Lajos feladata***) Az 1, 2, 3, ... 16 számok közül kell kitalálni egyet barkochba-kérdésekkel. A válaszokért fizetnünk kell: az IGEN válaszért 1 Ft-ot, a NEM válaszért 2-t. Legalább hány Ft-ra van szükség ahhoz, hogy biztosan kitaláljuk a gondolt számot?

Megoldás
Fordítsuk meg a kérdést! Próbáljuk meg kitalálni, hogy n Ft felhasználásával legfeljebb hány dolgot tudunk megkülönböztetni, azaz legfeljebb hány szám közül tudjuk biztosan kitalálni a gondoltat. Jelölje ezt a számot s_n. Ha adott egy s_n elemből álló S halmaz, akkor első kérdésünk két részre osztja S-t: az I részhalmaz azokból az elemekből áll, amelyekre - mint gondolt számokra - "igen" a válasz, az N részhalmaz pedig azokból, amelyekre "nem" a válasz. Ha "igen" választ kapunk, akkor még (n - 1) Ft maradt meg kérdésekre, "nem" válasz esetén azonban csak (n - 2), így $|I| = s_{n-1}$, $|N| = s_{n-2}$, azaz $s_n = s_{n-1} + s_{n-2}$. Világos, hogy $s_1 = 1$, míg $s_2 = 2$, így $s_3 = 3$, $s_4 = 5$, $s_5 = 8$, $s_6 = 13$, $s_7 = 21$, tehát 16 szám közül 7 Ft-tal tudjuk biztosan kitalálni a gondolt számot. Az első kérdésünk lehet pld ez: "a gondolt szám az {1, 2, 3 ..., 13} halmazban van?".

4.11 Bizonyítsd be, hogy egy kód pontosan akkor
a) k-hiba javító, ha minimális távolsága legalább $2k+1$;
b) k-hiba jelző, ha minimális távolsága legalább $k+1$;
c) k-törlés javító, ha k-hiba jelző!

Megoldás
a) Ha bármelyik két kódszó minimális távolsága legalább $(2k+1)$, akkor bármelyik kódszóban k betűt elrontva, attól csak k Hamming távolságra jutunk, míg az összes többitől legalább $(k+1)$ Hamming távolágnyira leszünk. Így a szó kijavítható.
Ha két kódszó távolsága csak $2k$ lenne, akkor azokat a szavakat nem tudnánk kijavítani, amely a $2k$ hely közül k helyen az egyik kódszóval, k helyen a másik kódszóval, a többi helyen pedig mindkét kódszóval megegyeznek. Ezek a szavak mindkét kódszóból megkaphatók k betű elírásával.

b) Ha bármelyik két kódszó távolsága legalább $(k+1)$, akkor hiába rontunk el egy kódszót k, vagy annál kevesebb helyen, nem kapunk másik kódszót, hanem tudni fogjuk, hogy hiba történt. Másrészt, ha van két olyan különböző kódszó, amelyek távolsága legfeljebb k, akkor az egyiket legfeljebb k helyen "elírva" megkaphatjuk a másikat, és ilyenkor nem veszi észre a hibát a rendszer.

c) Használjuk fel a b) állítást! Ha a két kódszó távolsága legfeljebb k, akkor az egyik kódszóból azt a legfeljebb k betűt törölve, ahol különböznek, olyan "szó"-hoz jutunk, amelynek rekonstruálása nem egyértelmű. Tehát k-törlés javító kód minimális távolsága legalább $(k+1)$.
Ha egy kódszó minden más kódszótól k-nál több helyen eltér, akkor bármelyik k betűjének törlődése esetén sem keverhető össze másik kódszóval. Tehát egy legalább $(k+1)$ minimális távolságú kód egyben k-törlés javító is.

13-as totó "Adjunk meg" 59049 szelvénykitöltést a 13 mérkőzésből álló totón úgy, hogy biztosan legyen olyan szelvényünk, amely legalább 12 találatos!

Emlékeztetünk rá, hogy az 5.7 feladat megoldásában már megmutattuk, hogy ennyi szelvényre valóban szükség van. A megoldásból az is kiderül, hogy 59049 szelvény pontosan akkor lesz megfelelő, ha a kitöltések 1-hiba javító kódot alkotnak, azaz bármelyik két különböző kitöltés Hamming távolsága legalább 3. Konstrukciónk az 5.9 feladatra adott III. konstrukciót, illetve az azt követő - az 5.6 feladatra vonatkozó - Megjegyzést követi.

Konstrukció
Lineáris kódot keresünk, azaz olyan

$$\begin{aligned} a_1 \cdot y_1 + a_2 \cdot y_2 + \ldots + a_{13} \cdot y_{13} &= 0, \\ b_1 \cdot y_1 + b_2 \cdot y_2 + \ldots + b_{13} \cdot y_{13} &= 0, \\ c_1 \cdot y_1 + c_2 \cdot y_2 + \ldots + c_{13} \cdot y_{13} &= 0 \end{aligned}$$

alakú egyenletrendszert, amelynek egyenletei, változói, műveletei mod 3 értendők. A kódszavak az egyenletrendszer megoldásai lesznek. Azért van szükség épp három egyenletre, mert 3^{13} szóból csak 3^{10}-t akarunk kódszónak választani, azaz a 13 változóból csak 10-et akarunk szabadnak tekinteni, 3 pedig kiküszöbölendő. Láttuk, hogy a kód akkor lesz 1-hiba javító, ha az együtthatók

$$A = \begin{pmatrix} a_1 & a_2 & \ldots & a_{13} \\ b_1 & b_2 & \ldots & b_{13} \\ c_1 & c_2 & \ldots & c_{13} \end{pmatrix}$$

mátrixában egyik oszlop sem azonosan 0, és semelyik két oszlop sem azonos vagy egymás ellentettje (azaz -1-szerese, vagy másképp: kétszerese). Ilyen mátrixot tudunk választani, hiszen az oszlopok három elemből álló bináris sorozatok, amelyekből $3^3 = 27$ van, az azonosan 0 nélkül 26, az ellentett párokat nem megkülönböztetve épp 13.

Tapasztalataink alapján kimondhatjuk, hogy az alább definiált kódok 1-hiba javító tökéletes kódok.

Megjegyzés (***Bináris és ternér Hamming-kód***)
Legyen r tetszőleges pozitív egész. Az előbbiek általánosításaként értelmezhető egy bináris (tehát kétféle jelet használó), valamint egy ternér (azaz háromféle jelet használó) lineáris kód. A kódot definiáló egyenletrendszer egyenleteinek száma mindkét esetben r. A kódszavak hossza a bináris, illetve a ternér esetben rendre

$$2^r - 1, \quad \text{illetve} \quad \frac{3^r - 1}{2},$$

a kódszavak száma pedig

$$2^{2^r - 1 - r}, \quad \text{illetve} \quad 3^{\frac{3^r - 1}{2} - r}.$$

Az egyenletrendszer egyenleteinek sorrendjét rögzítjük, és így az egyes változók együtthatói egy-egy r komponensű bináris, illetve ternér (oszlop)vektort alkotnak. Ezeket a vektorokat úgy választjuk meg, hogy különbözzenek a nullvektortól, egymástól, illetve egymás ellentettjeitől (-1-szereseitől).

Házi feladat: Általános Hamming-kód Általánosítsunk tovább! Mely q esetén lehet az előbbiekhez hasonló módon értelmezni q jelet használó 1-hiba javító tökéletes kódot? Pontosan hogyan?

Tétel (***Tietäväinen, Van Lint***) t-hiba javító tökéletes kódból $t > 1$ esetén csak kettő van, az úgynevezett Golay-kódok, ezek egyike bináris, 3-javító, szavainak hossza 23; a másik ternér, 2-javító, szavainak hossza 11.

A tételt itt nem bizonyítjuk. A ternér Golay kóddal az 5.7 feladat táblázatában is találkozunk, hiszen létezése ideális totókulcsot jelent annak számára, aki a 11 mérkőzésből álló totón legalább 9 találatra tör.

Golay Ellenőrizzük le, hogy a fenti Tételben említett kódok adatai megfelelhetnek tökéletes kódnak!

Megoldás A ternér esetben 11 hosszúságú szóból összesen 3^{11} van. Egy szótól 1 Hamming távolságnyira $2 \cdot 11 = 22$, míg 2 Hamming távolságnyira $2^2 \cdot 11 \cdot 10/2 = 220$ szó van. Egy szótól legfeljebb 2 távolságnyira tehát épp $243 = 3^5$ szó található. Így nincs kizárva, hogy $3^{11}/3^5 = 3^6 = 729$ kódszóval 2-hiba javító kódot találjunk.
A bináris esetben 23 hosszúságú szóból összesen 2^{23} van. Egy szótól 0, 1, 2, ill. 3 Hamming távolságnyira rendre

$$\binom{23}{0} = 1, \quad \binom{23}{1} = 23, \quad \binom{23}{2} = 253, \quad \binom{23}{3} = 1771$$

szó van, ami összesen $2048 = 2^{11}$. Így nincs kizárva, hogy $2^{23}/2^{11} = 2^{12} = 4096$ kódszóval 2-hiba javító kódot találjunk.

Megjegyzések
1. A Golay-kódokról is olvashatunk a Typotex Kiadónál megjelent Új matematikai mozaik című kötet Hibajavító kódok című írásában, amelyet Szőnyi Tamás és Hraskó András írt.
2. A Golay-kódokat manapság is használják. Lásd pld 4i2i.com,
3. A Golay kódokról még olvashatunk a Univ. of Illinois at Chicago honlapján.
4. Érdemes olvasni J. H. v. Lint könyveit, pld a Course in Combinatorics című könyvét, amely az amazon.com-on meg is rendelhető, vagy a Designs, Graphs, Codes and their Links, illetve az Introducion to Coding Theory című könyveit.

"Ideális 101-es"
Ebben a feladatban a természetes számok bizonyos részhalmazait keressük. A számokat mindig kettes számrendszerben leírva képzeljük, illetve alább így is említjük őket. Két számot nem a szokásos módon adunk össze, hanem kettes számrendszerbeli alakjuk megfelelő jegyeit modulo 2, és átvitel nélkül adjuk össze (pld 1100110 + 10011 = 1110101). A természetes számok (pontosabban azok kettes számrendszerbeli alakjainak) egy $\boldsymbol{I}_{101}$ részhalmazát "ideális 101-es"-nek nevezzük,

1. ha $\boldsymbol{h}\in\boldsymbol{I}_{101} \Rightarrow \boldsymbol{h}0\in\boldsymbol{I}_{101}$; ($\boldsymbol{h}0$ a $\boldsymbol{h}$ dupláját, tehát azt a számot jelöli, amelyet úgy kapunk, hogy $\boldsymbol{h}$ mögé írunk egy 0-t)
2. ha $\boldsymbol{h}\in\boldsymbol{I}_{101}$ és $\boldsymbol{j}\in\boldsymbol{I}_{101} \Rightarrow \boldsymbol{h}+\boldsymbol{j}\in\boldsymbol{I}_{101}$;
3. ha $101\in\boldsymbol{I}_{101}$ (itt 101 az egy-nulla-egy számot, azaz az 5-öt és nem a százegyet jelenti).

Hány "ideális 101-es" részhalmaza van a természetes számok halmazának?

Példák Némi próbálkozás után három példát találhatunk:
A) A természetes számok halmaza. Ha feltesszük, hogy $1\in\boldsymbol{I}_{101}$ és alkalmazzuk az 1., 2. szabályokat, akkor ezt a "részhalmazt" kapjuk.
B) Ha csak annyit teszünk fel, hogy $101\in\boldsymbol{I}_{101}$ és alkalmazzuk az 1., 2. szabályokat, akkor egy kisebb részhalmazt kapunk. Ez pontosan azokból a számokból áll, amelyek kettes számrendszerbeli alakjában a párosadik helyiértékeken és a páratlanadik helyiértékeken külön-külön az 1-esek száma páros.
C) Az a részhalmaz is jó, amelynek elemei az olyan számok, amelyek kettes számrendszerbeli alakjában az 1-esek száma páros. Ezt a részhalmazt az 11 elem "generálja".

Segítség a teljes megoldáshoz: feleltessük meg a természetes számok kettes számrendszerbeli alakjait F_2 testbeli együtthatós (azaz mod 2 számolunk) polinomoknak! Az $\boldsymbol{a} = \boldsymbol{a}_n\cdot 2^n + \boldsymbol{a}_{n-1}\cdot 2^{n-1} + ... + \boldsymbol{a}_1\cdot 2^1 + \boldsymbol{a}_0\cdot 2^0 = \boldsymbol{a}_n\boldsymbol{a}_{n-1}...\boldsymbol{a}_1\boldsymbol{a}_0$ számnak az $\boldsymbol{a}_n\cdot\boldsymbol{x}^n + \boldsymbol{a}_{n-1}\cdot\boldsymbol{x}^{n-1} + ... + \boldsymbol{a}_1\cdot\boldsymbol{x} + \boldsymbol{a}_0$ polinom feleljen meg.

Megoldás
A megfeleltetés után már a polinomok részhalmazait keressük. Az 1. tulajdonság azt jelenti, hogy $\boldsymbol{I}_{101}$-beli polinom $\boldsymbol{x}$-szerese is $\boldsymbol{I}_{101}$-ben van, 2. szerint pedig $\boldsymbol{I}_{101}$-beli polinomok összege is ott van. Ezekből az is következik, hogy $\boldsymbol{I}_{101}$-beli polinom tetszőleges polinomszorosa is $\boldsymbol{I}_{101}$-ben van, hiszen bármely polinommal való szorzás felépíthető $\boldsymbol{x}$-szel való szorzásokból és polinomok összeadásából. Az $\boldsymbol{x}^4 + \boldsymbol{x}$ polinommal például úgy szorzunk meg egy másik polinomot, hogy egymás után négyszer megszorozzuk $\boldsymbol{x}$-szel és az eredményhez hozzáadjuk az $\boldsymbol{x}$-szel szorzott polinomot.

A feladat megoldása innentől kezdve már nagyon hasonló a "Jó 30-as" feladatéhoz, csak míg ott az egész számok halmaza volt a főszereplő, itt a polinomok halmaza játszik. Lényeges közös vonás, hogy mindkét halmazban lehet maradékosan osztani.

Legyen most $\boldsymbol{I}_{101}$ legkisebb fokú (az azonosan 0-tól különböző) eleme a $\boldsymbol{p}$ polinom. Ha $\boldsymbol{q}\in\boldsymbol{I}_{101}$, akkor $\boldsymbol{p}|\boldsymbol{q}$, mert a $\boldsymbol{q}$ polinom $\boldsymbol{p}$-vel való osztási maradéka is $\boldsymbol{I}_{101}$-ben van és $\boldsymbol{p}$-nél kisebb fokú, így 0. Tehát $\boldsymbol{I}_{101}$ a $\boldsymbol{p}$ összes többszöröséből, és csakis azokból áll. Annyi megoldás van, ahány osztója van az $\boldsymbol{x}^2 + 1$ polinomnak. Az osztók: 1, $\boldsymbol{x} + 1$, $\boldsymbol{x}^2 + 1$, amiből látható, hogy a fenti A), B) és C) eset az összes megoldást lefedi.

Házi feladatok: "Ideális 1001-es" Oldjuk meg az "ideális 101-es" feladatot 101 helyett mindenütt 1001-gyel!

Még a múltkori óráról:
Hétszögminták Ebben a feladatban egy szabályos hétszög csúcsaira írunk 0-t vagy 1-et. Összesen 2^7=128 ilyen kitöltés van. A kitöltések egy $\boldsymbol{I}_7$ részhalmaza "7-szögre ideális",
1. ha $\boldsymbol{h}\in\boldsymbol{I}_7 \Rightarrow \boldsymbol{h}$ bármely ($\boldsymbol{n}\cdot$360°/7-kal való) elforgatottja is $\boldsymbol{I}_7$-ben van.
2. ha bármely két $\boldsymbol{I}_7$-beli kitöltés csúcsonként és mod 2 számított összege is $\boldsymbol{I}_7$-ben van.
A kitöltéseknek hány "7-szögre ideális" részhalmaza van?

5.11 (***Juhász Istvántól és Szegedy Balázstól is hallottam***)
Egy kém az ellenséges ország televíziójánál dolgozik. Esténként alkalma van az adásba kerülő 8×8-as fekete fehér tábla egyetlen mezőjének színét megváltoztatni. Nem feltétlenül szükséges változtatnia. Sajnos sohasem tudja előre, hogy milyen mintázatú lesz a 64 mező, amikor eléje kerül. Hányféle információt tud így küldeni a TV-n keresztül?