A szakkörön a Kódok feladatgyűjtemény **1.1**, **5.1**, **5.5**, **5.8**, **1.2**, **4.1**, **5.2**, **5.3** példái kerültek elő.

**1.1** Egy cég 10 szériában gyártott egész kg-os súlyokat. Az első szériában 1, a másodikban 2, a harmadikban 3, ... a tizedikben 10 kg-os súlyokat terveztek készíteni. Az azonos szériában készült egyforma súlyokat ugyanabban a ládában tartják, mind a 10 ládára rá van írva, hogy hanyadik szériában készült. Az egyik széria hibás lett, példányai egyforma súlyúak, de ez az érték nem egyezik meg az előre adott értékkel.

**a)** Egy kijelzős mérleg egyszeri használatával kell megtalálnunk, hogy mennyivel nehezebbek vagy könnyebbek a hibás súlyok az előírtnál.

**b)** Ezután határozzuk meg, hogy melyik súly szériája lett hibás!
Most is csak a kijelzős mérleget használhatjuk, és azt is csak még egyszer.

**c)** Próbáljuk meg általánosítani előző eredményeinket. Fontos volt-e, hogy épp 10 széria volt?
Lényeges-e, hogy rendre épp 1, 2, 3, ... 10 kg-osak a súlyok az egyes szériákban? Fogalmazzuk meg általánosan a feladatot, és adjunk választ az a), b) kérdésekre az általános esetben is!

**d)** Módosítunk az eredeti feladaton. Tegyük fel, hogy mindegyik súly megfelelő tömegű (az egyes szériákban rendre 1, 2, ... 10 kg), de előfordulhat, hogy amikor a ládákat a bennük lévő súlyok növekvő sorrendjében betolták a raktárba egymás mellé, akkor két szomszédos ládát felcseréltek. Ezután rakták rájuk sorban a szériaszámokat, amelyek így most növekvő sorrendben vannak, de lehet, hogy az egyik szomszédos párnál nem a ládában levő súlyok tömegét jelzik. Hány méréssel lehet megállapítani, hogy történt-e ilyen tévesztés?

**Megoldás:**
**a)** Rakjunk föl a mérlegre mindegyik súlyból egyet-egyet, és nézzük meg mennyivel tér el a tömeg 1+2+3+4+5+6+7+8+9+10=55 kg-tól.

**b)** Rakjunk a mérlegre az első szériából 1, a másodikból 2, ..., a tizedikből 10 súlyt és nézzük meg mennyivel tér el a tömeg $1\cdot1 + 2\cdot2 + 3\cdot3 + 4\cdot4 + 5\cdot5 + 6\cdot6 + 7\cdot7 + 8\cdot8 + 9\cdot9 + 10\cdot10$ kg-tól. Az eltérés és az előző mérésben kapott hiba hányadosa épp a hibás súlyok szériaszáma.
Nem ez az egyetlen jó megoldás. Az a lényeg, hogy mindegyik szériából különböző számú súlyt tegyünk föl a mérlegre.

**c)** Ha $n$ széria van, és az egyes szériákban a súlyok tervezett tömege rendre $x_1, x_2, x_3, .., x_n$, de az egyik széria hibás, akkor $x_1 + x_2 + x_2 + ... + x_n$, illetve $x_1 + 2x_2 + 3x_2 + ... + nx_n$ lekérdezése megoldja a két feladatot.

**d) I. mego.** A b)-ben adott mérés most is jó lesz. Ha pld a 4. és 5. szériát felcseréljük, akkor a várt és a tényleges tömeg különbsége:

$$4\cdot4 + 5\cdot5$$
$$4\cdot5 + 5\cdot4$$
$$4\cdot(-1)+5\cdot1 = 1.$$

**d) II. mego.** Tegyünk fel az elsőtől kezdve minden második szériából egyet-egyet a mérlegre!
Az 1+3+5+7+9 összeget várjuk eredménynek. Ha volt csere, akkor nem ennyit kapunk.

**d) Tanári kérdés:** a fenti két megoldás között van-e olyan, amely akkor is jó, ha nem szomszédos ládákat cseréltek föl? És olyan, ami akkor is kimutatja a tévedést, ha nem volt csere, de az egyik széria hibás? (Az I. megoldás mindkettőre jó.)

**5.1** (*Dobos Sándor példája*)
Számrontó Rezsőnek két módszere van egy szám elrontására. Vagy egy számjegyet tetszőlegesen megváltoztat (pld. 5437→5487), vagy két számjegyet kicserél (pld. 5437→3457). Egyszer véletlenül az asztalon hagytam egy cetlit a másológép négyjegyű belépési számával. Rezső ezt meglátta és rögtön átjavította 1323-ra. Szerencsére észrevettem, és visszajavítottam az eredeti számra. De, amikor legközelebb lehetősége adódott Rezső megint elrontotta a cetlin lévő számot, így most 1213 van ráírva. Mi lehet a másológép belépési száma?

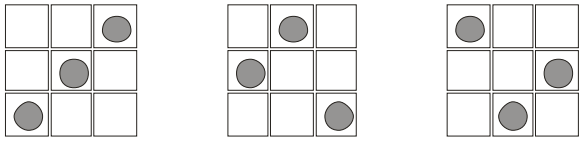
**Megoldás:**
Négy megoldás is van: 1223, 1313, 1233, 1123.

**5.5** A térbeli sakktáblán a bástya a tábla oldaléleivel párhuzamosan tud lépni. Legfeljebb hány bástya helyezhető el a táblán úgy, hogy semelyik kettő se üsse egymást, ha a tábla

**a)** 3×3-as?

**b)** 8×8-as?

**Megoldás:**
**a)** 9-nél több bástya nem helyezhető el, mert a 9 oszlop mindegyikében legfeljebb egy lehet. 9 elhelyezhető, az alábbi ábrán a kocka 3 rétege külön-külön látható, a korongok a bástyákat jelzik. Egy táblán belül semelyik két bástya sincs ugyanabban a sorban vagy oszlopban, a különböző táblákon lévő bástyák soha sincsenek a tábla ugyanazon mezőjén.



**b)** 64 a megoldás. A konstrukció az előzőhöz hasonló, a főátló nyolc bástyáját ciklikusan fölfelé toljuk.

**5.8 a)** Az 1, 2, 3, ... 16 számok közül kell kitalálni egyet barkochba kérdésekkel. Legalább hány kérdésre van szükség?
**b)** És ha a kérdéseket előre le kell írni, azaz a következő kérdés nem függhet az előzőre kapott választól?

**Megoldás:**
**a)** Egy-egy kérdés a szóbajövő számok halmazát két részhalmazra bontja: azokra, amelyekre igen a válasz (ha az a szám a gondolt szám) és azokra, amelyekre nem a válasz. "Rossz esetben" olyan választ kapunk, amely azt mutatja, hogy a nagyobb, pontosabban a nem kisebb részhalmazban van a gondolt szám. Ezért, ha biztosra megyünk nem tehetünk jobbat, minthogy kérdéseinkkel megfelezzük a lehetőségeket. 4 kérdés kell a kitaláláshoz, és ennyi elég is.

**b) Házi feladat**

**1.2** Egy cég 5 szériában gyártott súlyokat. Az egyes szériákon belül mindegyik súly egyforma tömegű, de nem ismert, hogy mekkorák. Az éppen távol levő cégvezető meg szeretné tudni, hogy milyen tömegű súlyokat gyártottak. Ezért egy mérési űrlapot küld egyik alkalmazottjának, majd annak kell elvégeznie a méréseket, és visszaküldeni az eredményekkel kitöltött űrlapot.

Legalább hány mérést kell elvégezni, és mik legyenek ezek a mérések (hogyan töltse ki a cégvezető az 1., 2., ..., 5. oszlopokat), ha várható, hogy (legfeljebb) egyszer az alkalmazott hibás értéket ír be a "Mért tömeg" rovatba?

Az űrlap így néz ki:

| | Hány súly legyen az egyes szériákból a mérlegen? | | | | | Mért tömeg |
|---|---|---|---|---|---|---|
| | 1. széria | 2. széria | 3. széria | 4. széria | 5. széria | (kg) |
| 1. mérés | | | | | | |
| 2. mérés | | | | | | |
| 3. mérés | | | | | | |
| 4. mérés | | | | | | |
| 5. mérés | | | | | | |
| 6. mérés | | | | | | |
| 7. mérés | | | | | | |
| 8. mérés | | | | | | |
| 9. mérés | | | | | | |
| 10. mérés | | | | | | |
| 11. mérés | | | | | | |

**I. megoldás** (*Mindent háromszor*)

15 mérés elég. Sorra vesszük a szériákat, mindig csak egy súlyt veszünk ki belőlük és azt a súlyt háromszor is megmérjük. Így a jó eredményt mindegyik szériánál legalább kétszer is megkapja a cégvezető, így tudni fogja a helyes eredményeket.

**Megjegyzés**: ez a módszer jó, de nem optimális.

**II. megoldás** (Az I. megoldás javítása)
Az előző módszert alkalmazom, de csak kétszer mérek meg minden súlyt, majd kizárólag azt teszem fel harmadszorra is, amelynél két különböző eredményt kaptam. Így 11 méréssel oldom meg a feladatot.

**Megjegyzés**: ez a módszer nem szabályos, mert nincs lehetőség a cégvezetőnek menet közben beleszólni, hogy melyiket mérje meg még egyszer az alkalmazott.

**III. megoldás**: (Újabb javítás)
Én is csak kétszer mérek meg minden súlyt, végül pedig mindegyik szériából egyet-egyet tetetek fel a mérlegre, így 11 méréssel oldom meg a feladatot. Ha az egyesével mért súlyok egyikénél a két mérés nem ugyanazt az eredményt adta, akkor tudhatjuk, hogy az utolsó mérés jó, így annak eredményéből, és a másik négy súly tömegéből meghatározható a bizonytalan eredmény is.

**IV. megoldás**: 7 méréssel oldom meg a feladatot. Az első öt mérésben csak egy-egy súlyt teszünk a mérlegre, az elsőben az első, a másodikban a második, ... az ötödikben az ötödik szériából. A hatodik mérésben öt súlyt, mindegyik szériából egyet-egyet teszünk a mérlegre. A hetedik mérésben 15 súlyt, az első szériából egyet, a másodikból kettőt, ... az ötödikből ötöt teszünk a mérlegre. Ha a hatodik vagy a hetedik mérés eredménye összhangban van az első öt mérés eredményével, akkor az első öt mérés mindegyikének jó az eredménye, tudjuk a tömegeket. Ha a hatodik és a hetedik mérés eredménye sincs összhangban az első öt mérés eredményével, akkor az első öt között van a hiba. Most az 1.1 feladat a) és b) része megoldásának alapján készen vagyunk.

Hat mérés nem elég. Ennek igazolására később térünk vissza.

**Házi feladat:** egy mérési tervhez meg kell adni az előírt mérések számát - a továbbiakban ezt $n$ jelöli - továbbá nemnegatív egész számokkal kell kitölteni az űrlap 1., 2., 3., 4., 5. oszlopait. Jelölje az így kapott számtáblázat $i$-edik sorának ($i = 1, 2, ..., n$) $j$-edik oszlopába ($j = 1, 2, 3, 4, 5$) írt számot $a_{ij}$ ($a_{ij}$ természetes szám). Tehát $a_{ij}$ -vel jelölöm az $i$-edik mérésnél a $j$-edik szériából vett súlyok számát. Határozzunk meg az $a_{ij}$ számokkal kapcsolatos olyan algebrai feltételt, amely azzal ekvivalens, hogy a mérésekből meghatározhatók a súlyok (feltéve, hogy legfeljebb egy hibás az eredmények közül).

**További házi feladatok:**

**4.1** (*Pálvölgyi Dömötör példája, Bergengóc példatár 2. 237. fel.*)
A budapesti telefonszámok hétjegyűek. Sokszor előfordul, hogy valaki két szomszédos számot felcserél, ezért téves a hívása. Keress minél egyszerűbb eljárást arra, hogy a hétjegyű számok végére még egy ellenőrző számot téve, a központ számcsere (két szomszédos felcserélése) esetén jelezni tudja, hogy a szám téves, és ne kapcsoljon!

**5.2** Egy hajó és utasai, összesen 100 fő, Ungabunga szigetén az emberevők fogságába esett. Tudják, hogy másnap reggel a kannibálok leültetik őket egymás mögé, és mindegyikük fejére egy-egy piros vagy kék sapkát húznak. Mindenki csak az összes előtte ülő ember fején lévő sapkát fogja látni, a sajátját és a mögötte ülőkét nem. A leghátsó embertől kezdve sorban mindenki hangosan mondhat majd egy színt: pirosat vagy kéket. A végén azt engedik szabadon, aki saját sapkája színét mondta, aki nem találta el, azt bizony megeszik. A kannibálok szigorúak, ha bárki mást tesz, minthogy a lehető legegyszerűbben kimondja a "piros" vagy a "kék" szót, akkor senkinek sem kegyelmeznek. A foglyoknak még egy esélye van. Most este még összebeszélhetnek. Szeretnék, hogy minél többen megszabaduljanak. Hány fogoly tud biztosan megmenekülni?

**Könnyítés**: oldjuk meg előbb a feladatot abban az esetben, ha tudjuk, hogy összesen pontosan

**a2)** két;

**a10)** tíz;

piros sapka van a 100 között!

**5.3** Gondoljuk végig az 5.2 feladatot kettő helyett három színnel! Minden rab fején háromféle sapka lehet, és mindenki háromféle színt is mondhat.

A szakkörön tovább folytattuk a Kódok feladatgyűjtemény feldolgozását. Megbeszéltük az **5.8** feladatot, visszatértünk az **1.1** példára és **1.2** megbeszélése után **5.5**-re is. Kielemeztük a **4.1** feladatot.

**Házi feladat** lesz: **5.3**, 1.2-nél az összes minimális megoldás jellemzése, **4.6** és **5.6**.
További gondolkodnivaló: az ISBN szám elemzése.

A következő alkalommal megbeszéljük a januári Kömal B feladatokat.

## A 16. szakkör részletezett anyaga

**5.8 a)** Az 1, 2, 3, ... 16 számok közül kell kitalálni egyet barkochba kérdésekkel. Legalább hány kérdésre van szükség?
**b)** És ha a kérdéseket előre le kell írni, azaz a következő kérdés nem függhet az előzőre kapott választól?

**Megoldás**
**a)** Egy-egy kérdés a szóbajövő számok halmazát két részhalmazra bontja: azokra, amelyekre igen a válasz (ha az a szám a gondolt szám) és azokra, amelyekre nem a válasz. "Rossz esetben" olyan választ kapunk, amely azt mutatja, hogy a nagyobb, pontosabban a nem kisebb részhalmazban van a gondolt szám. Ezért, ha biztosra megyünk nem tehetünk jobbat, minthogy kérdéseinkkel megfelezzük a lehetőségeket. 4 kérdés kell a kitaláláshoz, és ennyi elég is.

**b)** Most is szükséges a 4 kérdés, és elég is. Ehhez azt kell elérnünk, hogy a következő kérdés az előzőre adott bármely válasz esetén megfelezze a lehetőségeket.

**I. konstrukció**
Az alábbi megoldás négy kérdése mind így kezdődik: "A gondolt szám az itt megadott halmazban van?". A négy megadott halmaz:

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. halmaz | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | | | | | | |
| 2. halmaz | 1 | 2 | 3 | 4 | | | | | 9 | 10 | 11 | 12 | | | |
| 3. halmaz | 1 | 2 | | | 5 | 6 | | | 9 | 10 | | | 13 | 14 | |
| 4. halmaz | 1 | | 3 | | 5 | | 7 | | 9 | | 11 | | 13 | | 15 |

**II. konstrukció** Az iménti megoldást a diákok gyakran megtalálják, de ritkán veszik észre, hogy teljesen megegyezik a következővel. Írjuk fel a gondolt számnál eggyel kisebb számot kettes számrendszerben négy jeggyel (pótoljuk az elejét 0-kal, ha szükséges)! Ezek a felírások az alábbi táblázat oszlopaiban láthatók.

| *n* | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *n*-1 | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| 1. sor | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2. sor | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 3. sor | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 4. sor | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

Kérdéseink:

1. Az így kapott szám balról (a táblázatban fölülről) számított első jegye 0?

2. Az így kapott szám balról (a táblázatban fölülről) számított második jegye 0?

3. Az így kapott szám balról (a táblázatban fölülről) számított harmadik jegye 0?

4. Az így kapott szám balról (a táblázatban fölülről) számított negyedik jegye 0?

A négy válasz alapján megkapjuk a gondolt számnál eggyel kisebb szám kettes számrendszerbeli alakját, így ki tudjuk találni a gondolt számot. Látható, hogy táblázatunk négy sora, megfelel az I. konstrukció négy kérdésének. Az adott sorban az *n*-1 számnak megfelelő oszlopban pontosan akkor áll 0, ha az előző megoldás megfelelő kérdésében *n* benne volt a kijelölt halmazban.

**1.1+** Visszatérünk az 1.1 a), b) feladatokhoz, egy általánosító kérdés erejéig. Végezzünk két mérést: az elsőben az 1., 2., ... 10., széria súlyaiból rendre $a_1$, $a_2$, ..., $a_{10}$; a másodikban a szériákból rendre $b_1$, $b_2$, ..., $b_{10}$ darabot teszünk fel a mérlegre ($a_1$, $a_2$, ..., $a_{10}$, $b_1$, $b_2$, ..., $b_{10}$ nemnegatív egész számok). Adjunk meg olyan algebrai feltételt a felsorolt darabszámokra vonatkozólag, amely alapján eldönthető, hogy a két mérésből kitalálható-e hogy melyik széria adatai hibásak vagy nem található ki.

Elemezzük pld az alábbi három tervet:

**A)**

| széria: | **1.** | **2.** | **3.** | **4.** | **5.** | **6.** | **7.** | **8.** | **9.** | **10.** |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. mérés ($a_i$) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 2. mérés ($b_i$) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

**B)**

| széria: | **1.** | **2.** | **3.** | **4.** | **5.** | **6.** | **7.** | **8.** | **9.** | **10.** |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. mérés ($a_i$) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 2. mérés ($b_i$) | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 |

**C**)

| széria: | **1.** | **2.** | **3.** | **4.** | **5.** | **6.** | **7.** | **8.** | **9.** | **10.** |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. mérés ($a_i$) | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2. mérés ($b_i$) | 0 | 1 | 2 | 3 | 4 | 4 | 3 | 2 | 1 | 0 |

**Megoldás**
Az A) terv jó, mert a két mérés különbsége, épp az 1.1 a) feladat megoldásában adott mérést állítja elő, az 1. mérés pedig az 1.1 b) feladat megoldásának mérése.
A B) terv nem jó, a 2. és 3. szériákkal van a gond. Ha a 2. széria súlyai 2 kg-mal nehezebbek az előírt értéknél, akkor ugyanazokat az eltéréseket érzékeljük, mint amikor a 3. széria súlyai 1 kg-mal nehezebbek az előírtnál.
A C) tervnél hasonló jellegű a hiba az 1. és a 10., a 2. és a 9., stb. szériapárok viszonyában.

Általában, akkor nem tudjuk eldönteni, hogy a $k$-adik vagy a $j$-edik széria a hibás, ha van olyan $\varepsilon_k$ és olyan $\varepsilon_j$ nemnulla hibatag, amelyre $a_k \cdot \varepsilon_k = a_j \cdot \varepsilon_j$ és ugyanakkor $b_k \cdot \varepsilon_k = b_j \cdot \varepsilon_j$. Pontosan akkor vannak ilyen ε-ok, ha $a_k : a_j = b_k : b_j$, azaz ha az $(a_k; b_k)$, $(a_j; b_j)$ vektorok egyállásúak.

Továbbra is **házi feladat** az 1.2 feladatra vonatkozó hasonló jellegű diszkusszió: ott egy mérési tervhez meg kell adni az előírt mérések számát - a továbbiakban ezt $n$ jelöli - továbbá nemnegatív egész számokkal kell kitölteni az űrlap 1., 2., 3., 4., 5. oszlopait. Jelölje az így kapott számtáblázat $i$-edik sorának ($i$ = 1, 2, ..., $n$) $j$-edik oszlopába ($j$ = 1, 2, 3, 4, 5) írt számot $a_{ij}$ ($a_{ij}$ természetes szám). Tehát $a_{ij}$ -vel jelölöm az $i$-edik mérésnél a $j$-edik szériából vett súlyok számát. Határozzunk meg az $a_{ij}$ számokkal kapcsolatos olyan algebrai feltételt, amely azzal ekvivalens, hogy a mérésekből meghatározhatók a súlyok (feltéve, hogy legfeljebb egy hibás az eredmények közül).

**5.2** Egy hajó és utasai, összesen 100 fő, Ungabunga szigetén az emberevők fogságába esett. Tudják, hogy másnap reggel a kannibálok leültetik őket egymás mögé, és mindegyikük fejére egy-egy piros vagy kék sapkát húznak. Mindenki csak az összes előtte ülő ember fején lévő sapkát fogja látni, a sajátját és a mögötte ülőkét nem. A leghátsó embertől kezdve sorban mindenki hangosan mondhat majd egy színt: pirosat vagy kéket. A végén azt engedik szabadon, aki saját sapkája színét mondta, aki nem találta el, azt bizony megeszik. A kannibálok szigorúak, ha bárki mást tesz, minthogy a lehető legegyszerűbben kimondja a "piros" vagy a "kék" szót, akkor senkinek sem kegyelmeznek. A foglyoknak még egy esélye van. Most este még összebeszélhetnek. Szeretnék, hogy minél többen megszabaduljanak. Hány fogoly tud biztosan megmenekülni?

**I. megoldás**
50 rabot szabadítok meg, hátulról számítva minden párosadikat. A páratlan sorszámú rabok bemondják az előttük levő sapkájának színét, a páros sorszámú rabok pedig a saját sapkájuk színét. Így az utóbbiak mind megszabadulnak, a többiek csak szerencsés esetben menekülhetnek meg.

**II. megoldás**
93 rabot szabadítok meg. A leghátsó hét rab csak az első 93-mal törődik. Megszámolják, hogy azokon összesen hány piros sapka van, ezt a számot felírják maguknak kettes számrendszerben (ez legfeljebb hétjegyű), és ennek jegyeit mondják be sorban (pld "piros" jelenti az "1"-et). Az első 93 mindegyike tudja, hogy rajtuk összesen hány piros sapka van, mindegyik hallja a mögötte levők sapkájának színét (a 93-ból), látja az előtte levőkét, így a sajátját ki tudja találni és bemondja.

**III. megoldás**
Az előző megoldás javítható. 99 rabot is ki lehet szabadítani.
Az embereknek szükségtelen tudni az összes piros sapka pontos számát, elég tudni a piros sapkák számának paritását. Megállapodnak pld abban, hogy a leghátsó ember "piros"-at mond, ha az előtte levő 99 ember közül összesen páratlan soknak a fején lát piros sapkát, és kéket mond az ellenkező esetben. Így a 99 emberből már mindenki tudja, hogy rajtuk összesen páros vagy páratlan db piros sapka van, látja az előtte levők sapkáját, hallja a mögötte levők sapkájának színét, így a sajátját is kitalálhatja és bemondja.
100 rab nyilván csak szerencsés esetben szabadulhat, a leghátsó nem kap információt saját sapkájáról.

**4.1** (*Pálvölgyi Dömötör példája, Bergengóc példatár 2. 237. fel.*)
A budapesti telefonszámok hétjegyűek. Sokszor előfordul, hogy valaki két szomszédos számot felcserél, ezért téves a hívása. Keress minél egyszerűbb eljárást arra, hogy a hétjegyű számok végére még egy ellenőrző számot téve, a központ számcsere (két szomszédos szám felcserélése) esetén jelezni tudja, hogy a szám téves, és ne kapcsoljon!

**I. megoldás**
Legyen $x_8 \equiv x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 \pmod{10}$. Az 1.1 d) feladat I. megoldásának mintájára látható, hogy két szomszédos jegy felcserélődése esetén a jobb oldali kifejezés értéke változik, így az összefüggés nem marad érvényben.

**Megjegyzés**
Sajnos baj van a 7. és 8. jegyek cseréjénél. Ilyenkor a bal oldal is változik, nem csak a jobb, az összefüggés esetleg érvényben marad. Lehetséges, hogy egyszerre teljesüljön az

$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 \equiv x_8 \pmod{10} \text{ és a}$$
$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_8 \equiv x_7 \pmod{10}$$

összefüggés is. Valóban a két kongruencia kivonása és rendezés után

$$8(x_8 - x_7) \equiv 0 \pmod{10},$$

ami teljesül pld $x_8 = 6$, $x_7 = 1$ esetén, tehát ha egy jó nyolcjegyű szám utolsó két jegye 6 és 1, akkor az utolsó két jegy cseréjét nem veszi hibának a rendszer.

**II. megoldás**
Legyen $x_8 \equiv x_1 + x_3 + x_5 + x_7 \pmod{10}$. Két szomszédos jegy felcserélődése esetén a jobb oldali kifejezés értéke változik, így az összefüggés nem marad érvényben.

**Megjegyzés**
Sajnos most is baj van a 7. és 8. jegyek cseréjénél. Lehetséges, hogy egyszerre teljesüljön az

$$x_1 + x_3 + x_5 + x_7 \equiv x_8 \pmod{10} \text{ és a}$$
$$x_1 + x_3 + x_5 + x_8 \equiv x_7 \pmod{10}$$

összefüggés is. Valóban a két kongruencia kivonása és rendezés után

$$2(x_8 - x_7) \equiv 0 \pmod{10},$$

ami az előzőével analóg hibát okoz.

**I'. megoldás**
Legyen $x_8 \equiv 0x_1 + 1x_2 + 2x_3 + 3x_4 + 4x_5 + 5x_6 + 6x_7 \pmod{10}$. Most a 7. és 8. jegy felcserélését firtató kongruencia-rendszer a

$$7(x_8 - x_7) \equiv 0 \pmod{10}$$

kongruenciához vezet, amelyből már következik, hogy $x_8 \equiv x_7 \pmod{10}$, azaz $x_8 = x_7$, azaz nincs igazi csere.

**II'. megoldás**
Legyen $x_8 \equiv x_2 + x_4 + x_6 \pmod{10}$. Az első hét jegyből két szomszédos cseréjénél csak a jobb oldal, az utolsó két jegy cseréjénél csak a bal oldal értéke változik, tehát a kongruencia nem marad fenn.

**Házi feladat**
**4.2** Nézd meg sok különböző könyv azonosítóját, az úgynevezett ISBN (International Standard Book Number) számot! Próbáldd meg kideríteni, milyen részekből áll, hogyan épül fel ez az azonosító! (Segítség: a legutolsó jegy egy ellenőrző jegy, segítségével kiszűrhető bármelyik két számjegy felcserélése, illetve bármelyik jegy elírása. A többi jegy három csoportba osztható és a könyv azonosítására szolgál.)

**Elméleti összefoglaló a kódokról:**

Legyen adva egy tetszőleges *abc* (betűkészlet, a kódolásnál tipikusan {0,1}) és egy *n* pozitív egész (a szavak hossza). Az *abc* elemeiből készíthető *n* hosszúságú sorozatokat *szavak*nak nevezzük.
Két szó távolságán (*Hamming távolság*) azoknak a helyeknek a számát értjük, amelyeken különböznek egymástól. (Az *AABC*, *CBBC* szavak távolsága pld. 2, mert az első és a második helyen térnek el egymástól.)

Az általános megközelítésben *kód*on a szavak egy tetszőleges részhalmazát értjük. A kódba tartozó szavak a kódszavak. Úgy képzeljük, hogy két fél kommunikál egymással és a kódszavak az értelemmel bíró jelek. Előfordulhat, hogy a kommunikáció során egy kódszó sérül (a küldő hibázott, a kommunikációs csatorna zaja módosította az üzenetet vagy a fogadó fél hibásan olvasta ki a szót). A kapott szót úgy javítjuk, hogy átírjuk a tőle legkisebb (Hamming) távolságra lévő egyik kódszóra.

A kód *k-hiba javító*, ha bármelyik kódszavában *k* vagy annál kevesebb betű módosulása esetén a fenti hibajavító módszer mindig egyértelműen helyreállítja az eredeti üzenetet.

A kód *k-hiba jelző*, ha bármelyik kódszavában *k* vagy annál kevesebb betű módosulása esetén nem juthatunk másik kódszóhoz, azaz a fogadó fél észre tudja venni, hogy hiba van, mert nem kódszót olvas.

A kód *k-törlés javító*, ha bármelyik kódszavában *k* vagy annál kevesebb betű törlődése (olvashatatlansága) esetén a hiányzó *k* betű csak egyféleképpen tölthető ki úgy, hogy kódszót kapjunk.

A kód minimális távolsága a kódszavai között fellépő legkisebb pozitív Hamming távolság.

Régen, amikor a számítógépeknek kazettán adtak információt, akkor az üzenetet hetes bitcsomagokban tárolták, és minden hetest egy további bittel egészítettek ki egy byte-tá. Ez az egy bit volt az úgynevezett *paritásjelző bit*, amelyet úgy állítottak be, hogy a byteban összesen páros darab 1-es legyen. Ha egy kiolvasott byteban nem ez volt a helyzet, akkor újra lekérték az adatot. Ebben a megközelítésben egy 1-hiba jelző kódról van szó.

Az **5.2** feladatban egy hasonló eljárást 1-törlés javításra alkalmaztunk. A "törlés" itt azt jelenti, hogy (az első 99 ember közül) mindenki látja vagy hallja a többiek sapkájának színét, számára egy sapka színe - a sajátjáé - van törölve.

Az **5.5** feladat (térbeli sakktábla) megoldása is felfogható ilyen módon. Nézzük pld a 8×8-as esetet! A "tábla" mezőit nevezzük meg a {0, 1, 2, ..., 7} halmazból képzett számhármasokkal. (2, 0, 3) pld a 2. emelet 0. sor 3. oszlopában álló mező kódja. A 64 bástya mezőinek koordinátáit (*x*, *y*, *z*) megadhatjuk pld az alábbi feltétellel:

$$x + y + z \equiv 0 \pmod 8.$$

Ennek 64 mező felel meg, hiszen *x* és *y* értéke tetszőlegesen megadható. Két bástya akkor üti egymást, ha koordinátáik közül kettő is megegyezik egymással. Ez a fenti feltételnek eleget tevő mezők közül semelyik kettőre sem teljesülhet, ugyanis, ha *x*, *y* és *z* közül kettőt megadunk, akkor a harmadik már egyértelműen meghatározható, nincs két lehetőség.

További **házi feladatok:**

**4.6** Keress háromféle betű alkalmazásával minél több szóból álló négybetűs 1-hibajavító kódot!

**5.6** Bergengóciában a totó, a bajnokságnak megfelelően csak 4 mérkőzést tartalmaz. Minden mérkőzés eredményére háromféleképpen lehet tippelni: 1-gyel, 2-vel vagy X-szel. Egy szelvényen csak egy tipposzlop van.

**a)** Hány szelvényt kell venni ahhoz, hogy biztosan legyen telitalálatunk?

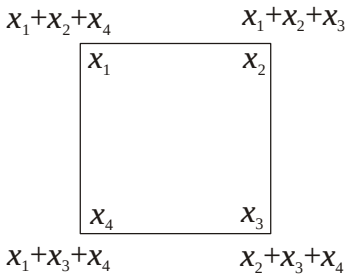
**b)** És ahhoz, hogy biztosan legyen olyan szelvényünk, amely legalább 3 találatos?

A szakkörön mégsem a Kömal példák kerültek terítékre, hanem tovább folytattuk a Kódok feladatgyűjtemény feldolgozását. Egy bemelegítő feladat után tisztáztuk az ISBN szám felépítését (**4.2**), majd 1-hiba javító kódot gyártottunk (**4.6**) és totóztunk is (**5.6, 5.7**). Menet közben megismerkedtünk a Hamming távolság fogalmával, és néhány egyszerű lemmát fogalmaztunk meg a kódok minimális távolsága és hibajelző, illetve javító képessége között (pld **4.5**).

**Házi feladat** lesz: **5.9**, és egy szokatlan példa a 7-szög bináris mintáiról.

## A 17. szakkör részletezett anyaga

**Négyzetminta** Egy négyzet csúcsaiba egy-egy egész számot írtunk, majd mindegyik csúcs mellé még odaírtuk az abba a csúcsba írt számnak a szomszédos csúcsokba írt számokkal vett összegét. Hány páratlan szám lehet az így kapott nyolc szám között? Adjuk meg az összes lehetőséget!




**Megoldás**
A feladat nem nehéz, 0, 4 vagy 8 páratlan számot kaphatunk.
Ez az egyszerű példa a későbbiekben egészen más összefüggésben elő fog bukkanni, az lesz az igazi feladat, hogy észrevegyük, mikor.

**3.2** Nézzük meg sok különböző könyv azonosítóját, az úgynevezett ISBN (International Standard Book Number) számot! Próbáljuk meg kideríteni, milyen részekből áll, hogyan épül fel ez az azonosító! (Segítség: a legutolsó jegy egy ellenőrző jegy, segítségével kiszűrhető bármelyik két számjegy felcserélése, illetve bármelyik jegy elírása. A többi jegy három csoportba osztható és a könyv azonosítására szolgál.)

**Megoldás**
Nagy segítséget jelent, ha észrevesszük, hogy néhány ISBN számban az utolsó jegy nem is szám, hanem az X jel. Innen sejthető, hogy az ellenőrző jegy a múlt órai **4.1** feladat megoldásához hasonlóan adható meg, csak annyi a különbség, hogy mod 11 kell számolni.

A Bergengóc példatár első kiadásának kódja pld ISBN 963 9132 31 4. Ebből az első három jegy, 963, Magyarország kódja. Nagyobb országoknak kevesebb jegyből áll a kódja, hogy több maradjon a könyv azonosítására. A következő négy jegy, 9132, a Typotex kiadót jelöli. Ez egy viszonylag kis kiadó, ezért ilyen hosszú a kódja. A következő két szám, a 32, a könyv sorszáma. Ha a Typotex túllépi a kódjához tartozó 100 könyv kiadására lehetőséget adó keretet, akkor majd új kódot kap. Az utolsó jegy, a 4-es az ellenőrző jegy, ez a korábbiakból így számítható ki:

$$4 \equiv 1\cdot 9 + 2\cdot 6 + 3\cdot 3 + 4\cdot 9 + 5\cdot 1 + 6\cdot 3 + 7\cdot 2 + 8\cdot 3 + 9\cdot 1 \pmod{11}.$$

Ha a szorzatösszeg 11-es maradéka 10 lenne, akkor az X betű lenne az ellenőrző jegy.

Általánosabban: az ISBN kód első kilenc jele egy-egy számjegy, ezek az országot, azon belül a kiadót, illetve a könyvet azonosítják; ezen belül nincs rögzítve, hogy e három jellemző melyike hány helyen tárolódik; nagyobb országok, nagyobb kiadók rövidebb, kisebb országok, kisebb kiadók hosszabb karaktersort kapnak; összesen mindig 9 jegyből áll ez a három rész. A tizedik jegy meghatározására az alábbi egymással ekvivalens feltételek bármelyike alkalmazható.

$$x_{10} \equiv 2\cdot x_9 + 3\cdot x_8 + 4\cdot x_7 + 5\cdot x_6 + 6\cdot x_5 + 7\cdot x_4 + 8\cdot x_3 + 9\cdot x_2 + 10\cdot x_1 \pmod{11};$$
$$x_{10} \equiv 1\cdot x_1 + 2\cdot x_2 + 3\cdot x_3 + 4\cdot x_4 + 5\cdot x_5 + 6\cdot x_6 + 7\cdot x_7 + 8\cdot x_8 + 9\cdot x_9 \pmod{11};$$
$$0 \equiv 1\cdot x_{10} + 2\cdot x_9 + 3\cdot x_8 + 4\cdot x_7 + 5\cdot x_6 + 6\cdot x_5 + 7\cdot x_4 + 8\cdot x_3 + 9\cdot x_2 + 10\cdot x_1 \pmod{11};$$
$$0 \equiv 1\cdot x_1 + 2\cdot x_2 + 3\cdot x_3 + 4\cdot x_4 + 5\cdot x_5 + 6\cdot x_6 + 7\cdot x_7 + 8\cdot x_8 + 9\cdot x_9 + 10\cdot x_{10} \pmod{11}.$$

Az utolsó alakból könnyen leolvasható, hogy az ellenőrző jegy kiszűri bármely két jegy cseréjét vagy bármelyik jegy elírását. Ha pld az ötödik jegyet $x_5$-ről $x_5'$-re módosítjuk, akkor nem állhat fenn a

$$0 \equiv 1\cdot x_1 + 2\cdot x_2 + 3\cdot x_3 + 4\cdot x_4 + 5\cdot x_5 + 6\cdot x_6 + 7\cdot x_7 + 8\cdot x_8 + 9\cdot x_9 + 10\cdot x_{10} \pmod{11},$$
$$0 \equiv 1\cdot x_1 + 2\cdot x_2 + 3\cdot x_3 + 4\cdot x_4 + 5\cdot x_5' + 6\cdot x_6 + 7\cdot x_7 + 8\cdot x_8 + 9\cdot x_9 + 10\cdot x_{10} \pmod{11}$$

közül mindkettő, mert különbségük:

$$0 \equiv 5\cdot(x_5 - x_5') \pmod{11},$$

és mivel 11 prím, így ez csak akkor állhat fenn, ha

$$0 \equiv x_5 - x_5' \pmod{11},$$

azaz $x_5 = x_5'$, tehát ha nem is történt módosítás. Ehhez hasonlóan, ha feltételezzük, hogy az $i$-edik és $j$-edik jegy cseréje érvényes számot eredményez, akkor a

$$0 \equiv (i - j)\cdot(x_i - x_j) \pmod{11}$$

kongruenciához jutunk, amelyben $|i - j| < 10$ és $|x_i - x_j| < 10$, tehát $i = j$ vagy $x_i = x_j$, azaz nem történt valódi csere.

Néhány további azonosító leírását is összegyűjtöttük.

Most következzék egyszerre két feladat:

**4.6** Keress háromféle betű alkalmazásával minél több szóból álló négybetűs 1-hiba javító kódot (lásd az előző szakkör anyagát)!

**5.6** Bergengóciában a totó, a bajnokságnak megfelelően csak 4 mérkőzést tartalmaz. Minden mérkőzés eredményére háromféleképpen lehet tippelni: 1-gyel, 2-vel vagy *X*-szel. Egy szelvényen csak egy tipposzlop van.
**a)** Hány szelvényt kell venni ahhoz, hogy biztosan legyen telitalálatunk?
**b)** És ahhoz, hogy biztosan legyen olyan szelvényünk, amely legalább 3 találatos?

**Definíció** (*Hamming távolság*)
Ha adott két szó (azaz két azonos hosszúságú jelsorozat), akkor sorban összehasonlíthatjuk a bennük lévő jeleket: először a két szó első jeleit vetjük össze, azután a szavakban másodiknak következő jeleket, ..., végül az utolsókat. Azoknak a helyeknek a számát, ahol egymástól különböző jeleket találunk, a két szó Hamming távolságának nevezzük. Formálisan:

$$d_H(x_1x_2x_3...x_n, y_1y_2y_3...y_n) = |\{i|\ x_i \neq y_i\}|,$$

Pld $d_H(AABC, ABBA) = 2$, mert a második helyen (*A* ill. *B*) és a negyediken (*C* és *A*) van eltérés.

**Történeti megjegyzés**
Claude E. Shannon (lásd pld Györfi László cikkét, Charles A. Gimon írását vagy a MacTutor Matematikatörténeti Arhívumot) a Bell Laboratórium munkatársaként 1948-ban publikálta a modern kommunikáció elvi megalapozását jelentő "A Mathematical Theory of Communication" című cikkét. 1950-ben a cég műszaki folyóiratának másik számában R. W. Hamming (lásd a MacTutor Matematikatörténeti Arhívumot) "Error Detecting and Error Correcting Codes" című írásában konkrét kódolási módszereket javasolt.

**Definíció** (*Kód minimális távolsága*)
Egy adott kód minimális távolságán a különböző kódszavai között fellépő legkisebb Hamming távolságot értjük.

**Lemma**
Egy kód pontosan akkor 1-hiba javító, ha minimális távolsága legalább 3.

**Bizonyítás**
Ha a kód nem 1-hiba javító, akkor van olyan *p* kódszó (pld *AABA*), amit egy betűjében megváltoztatva egy $c_1$ kódszóhoz jutunk (pld *AABC*), de meg lehet *p*-t úgy is változtatni egy betűvel, hogy egy *c*2 kódszót kapjunk (pld *ABBA*). Ebben az esetben a *c*1, *c*2 kódszavak Hamming távolsága egy vagy kettő attól függően, hogy a két esetben a változtatás ugyanazon a helyen történt vagy nem. Tehát 1-hiba javításra alkalmatlan kódok minimális távolsága kisebb 3-nál.
Másrészt, ha egy kód minimális távolsága kisebb, mint 3, akkor van a kódban két olyan kódszó, $c_1$, $c_2$ (pld *AABC* és *ABBA*), amelyek Hamming távolsága 2 vagy 1. Ha a távolság 2, akkor könnyen készíthetünk olyan *p* szót, amely mindkét kódszótól csak egy helyen tér el: *p* egyezzen meg $c_1$-gyel és $c_2$-vel mindazokon a helyeken, ahol $c_1$ és $c_2$ megegyezik egymással (*p* = *A_B_*), az eltérést okozó két hely egyikén pedig *p* egyezzen meg $c_1$-gyel (*p* = *AAB_*, vagy *A_BC*), a másikon $c_2$-vel (*p* = *AABA*, vagy *p* = *ABBC*). Ha véletlenül a *p* üzenet érkezik hozzánk, akkor nem tudjuk kijavítani. Ha $c_1$ és $c_2$ Hamming távolsága csak 1, akkor $c_1$-et kapva bizonytalanságban vagyunk, hogy $c_1$-et vagy $c_2$-t küldték, ha egy hibát megengedünk.

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

Most visszatérünk a **4.6** feladat megoldásához.

**4.6 I. megoldása** (*A minimális távolság alapján*)

Tegyük fel, hogy már van egy ilyen kódunk! Legyenek a betűk 0, 1, 2, és gyűjtsük össze a 0-val kezdődő kódszavakat! Legfeljebb három lehet belőlük, mert ha már négy volna, akkor volna közöttük kettő, amelyek a második "betűben" is megegyeznek, és így legfeljebb csak két helyen térnek el egymástól. Teljesen hasonlóan az 1-gyel és a 2-vel kezdődő szavakból is legfeljebb három-három lehet, tehát összesen legfeljebb csak 9 ilyen kódszó van.

Találtam is 9 megfelelő kódszót:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | | 1 | 0 | 1 | 2 | | 2 | 0 | 2 | 1 |
| 0 | 1 | 1 | 1 | | 1 | 2 | 0 | 1 | | 2 | 1 | 0 | 2 |
| 0 | 2 | 2 | 2 | | 1 | 1 | 2 | 0 | | 2 | 2 | 1 | 0 |

Először a 0-val kezdődőket írtam össze (első oszlop). Egyszerűnek tűnt a maradék három jegyet mindig egyformának választani. Ezután már alig volt szabadságom. Kellett még három-három 1-gyel és 2-vel kezdődő kódszó. Ezeknek az utolsó három helyén 0-ból, 1-ből és 2-ből is csak egy-egy fordulhatott elő szavanként, hogy a már kijelölt három kódszó egyikével se egyezzenek meg két helyen. Három jelnek épp hat permutációja van, ez adja az esélyt. Miután leírtam az 1021 kódszót is már csak egyféleképpen lehetett folytatni: 021 ciklikus elforgatottjait kellett leírni az 1-es mögé, hogy ne legyen újabb egyezés, a másik három permutációt pedig a 2-es mögé.

**4.6 II. megoldása** (*Algebrai konstrukció az* 1.1 *feladat analógiájára*)

Ha a kódszavakat 1-1 helyen az összes lehetséges módon megváltoztatjuk, akkor csupa különböző szóhoz kell jutnunk. Egy kódszónak négy betűje van, mindegyiket kétféleképpen változtathatjuk meg, így egy kódszóhoz önmagával együtt 9 szó tartozik. Mivel összesen $3^4 = 81$ szó van, így legfeljebb 81/9 = 9 kódszó lehetséges.

Megadunk 9 megfelelő kódszót. Legyen a négy betű sorban $x_1$, $x_2$, $x_3$ és $x_4$.
Válasszuk meg $x_1$-et és $x_2$-t az összes lehetséges módon! Ez összesen épp 9 lehetőség.
$x_3$-at és $x_4$ számítsuk ki $x_1$-ből és $x_2$-ből az 1.1 feladat megoldása alapján, csak modulo 3 számolva:

$$x_3 \equiv x_1 + x_2 \pmod 3, \qquad x_4 \equiv x_1 + 2\cdot x_2 \pmod 3.$$

Tehát a kódszavak: 0000, 0112, 0221, 1011, 1120, 1202, 2022, 2101, 2210.

Ha kapunk egy négybetűs szót, akkor "betűit" helyettesítsük be a fenti egyenletekbe. Ha mindkettő teljesül, akkor nincs hiba (vagy egy hibánál több van). Ha csak az egyik nem teljesül, akkor annak bal oldala a hibás és kijavítható. Ha egyik se teljesül, akkor $x_1$ és $x_2$ egyike a hibás, az első egyenletből kiderül mennyivel, a másodikból, hogy melyik.

**Megjegyzés**
Ha a II. megoldást úgy módosítjuk, hogy $x_3$-at és $x_4$-et az

$$x_3 \equiv x_1 + x_2 \pmod 3, \qquad x_4 \equiv 2\cdot x_1 + x_2 \pmod 3$$

képletekkel értelmezzük, akkor épp az I. megoldásban kapott 9 kódszóhoz jutunk.

**5.6 a) megoldása**
$3^4 = 81$-féleképpen alakulhat a négy mérkőzés eredménye, ezért ennyi, azaz 81 szelvényt kell kitölteni a biztos telitalálat érdekében.

**5.6 b) I. megoldása**
Összesen 9-féleképpen lehet úgy kitölteni a totószelvényt, hogy legalább háromtalálatos legyen:
van 1 négytalálatos;
van 2 olyan, amelyen az 1., a 2., és a 3. mérkőzésre adott tipp talált (a 4. mérkőzés eredményre adott tipp kétféleképpen lehet rossz);
és még 2-2-2 olyan szelvény képzelhető el, amelyen az 1., 2., 4.; az 1., 3., 4.; illetve a 2., 3., 4. mérkőzés eredményét találtuk el.

Ezért csak 81-9=72 olyan kitöltés lehetséges, amely legfeljebb kéttalálatos. Tehát 73 szelvényt kell ahhoz venni, hogy biztosan legyen egy legalább háromtalálatos.

**Megjegyzés** Ez a megoldás hibás, mert nem a feltett kérdésre válaszol, hanem a következőre: hány szelvényt kell vennie a nagyon buta totózónak, ha azt akarja, hogy azokat gondolkodás nélkül, de csupa különböző módon kitöltve legyen egy legalább háromtalálatos szelvénye.

Egy gondolkodó totózó kevesebb szelvénnyel is el tud érni három (vagy több) találatot.

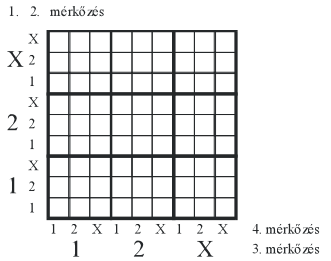
**5.6 b) II. megoldása**
Ha háromtalálatosat szeretnénk, a következőképpen járunk el. Mivel a negyedik tipp nem számít, csak az első hármat nézzük. Ezeket 3·3·3-féleképpen tölthetjük ki. Tehát bármilyen is a telitalálatos, biztos lesz a kitöltöttek között háromtalálatos. Így 27 szelvényt kell ehhez kitölteni.

**Megjegyzés**
Ez a megoldás is hibás, ugyanis nem derül ki belőle, hogy 27-nél kevesebb szelvénnyel nem oldható meg a feladat (szerencse nélkül).

**5.6 b) III. megoldása**
A négy mérkőzés együttes eredményét röviden "eredmény"-nek fogjuk hívni.

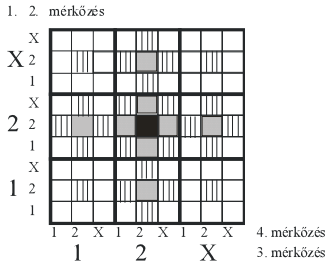
Ha egy szelvényt kitöltünk, akkor 9 olyan eredmény van, amely mellett van három találatunk: a telitalálat, valamint ha a 3 mérkőzés közül pontosan egynél hibáztunk (2-féle hiba lehetséges): 1+4·2=9. Nem úszhatjuk meg tehát 81/9=9 szelvénynél kevesebbel. Nézzük meg, hogy 9 szelvénnyel boldogulhatunk-e!

A szelvények mindegyike 9 eredmény esetén nyer (azaz 3 vagy 4 találatos). Ahhoz, hogy mind a 81 lehetséges eredmény esetén legyen nyerő szelvényünk az kell, hogy egyik eredménynél se nyerjen 2 szelvény. Próbáljunk meg így kitölteni 9 szelvényt! A próbálkozáshoz egy (3×3)×(3×3)-as táblázatban ábrázoljuk a lehetséges eredményeket, illetve tippeket.



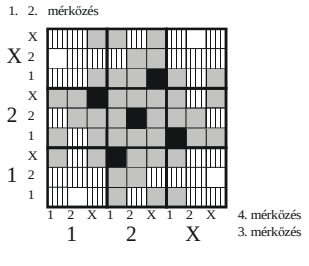

A táblázatban összesen 81 mező van, minden mező egy lehetséges eredménynek felel meg. Az, hogy az adott mező melyik "sorhármasban" van, megmondja, hogy mi az első mérkőzés végeredménye; a sorhármason belüli sor a második mérkőzés végeredményére utal; az oszlophármas a harmadik, azon belül az oszlopszám a negyedik meccs végeredményét jelzi.

A kitöltött szelvénynek megfelelő mezőt befeketítjük. Ennél az eredménynél lenne a szelvény telitalálatos. Szürkével jelöljük azokat az eredményeket, amelyek 3 találatosak lennének. Ezeket nem szabad befeketíteni. Bevonalkázzuk azokat a mezőket, amelyek a szürkéktől csak 1 mérkőzés végeredményében térnek el. Ezeket a továbbiakban nem szabad befeketíteni, mivel minden eredménynél csak egy szelvény nyerhet (lehet 3 vagy 4 találatos).

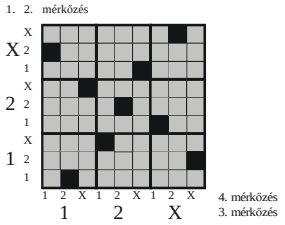



Röviden a szabályok: a fekete mezőtől csak egy adatban eltérő mezők szürkék, a pontosan két adatban eltérők vonalazottak.

Mivel az 1-2-X eredmények egyenértékűek, és a mérkőzések egymástól függetlenek, mindegy, hogy melyik az első kitöltött szelvény, ezért szimmetriaokokból válasszuk elsőnek a középső mezőt (2222)! Ezután is tarthatjuk magunkat a szimmetriához, még 4-4 szelvény kellene, esélyünk van 90°-os forgásszimmetriára. Ezért bejelölünk a középponthoz legközelebb lévő még kitölthető szelvényt, rögtön a forgásszimmetria szerint négyet (1X21, 21X1, X12X, 2X1X).




Lám, még szerencsénk is van: a négy mező együttes bejelölése sem okoz átfedést. Mint látható, pont annyi lyuk van, amennyi szelvényt még el kell helyeznünk. Sikerült! Megelégedéssel olvashatjuk le a megfelelő tippeket:
2222
1X21, 21X1, X12X, 2X1X
X211, 1112, 12XX, XXX2
E szelvényekkel biztos a legalább 3 találat, így 9 szelvény szükséges és elégséges.



**5.6 b) IV. megoldása**
Az előző megoldásban elején láttuk, hogy legalább 9 szelvény szükséges, és 9 szelvény pontosan akkor oldja meg a feladatot, ha nincs olyan "eredmény", amely a 9 szelvény közül kettőtől is csak egy mérkőzés eredményében tér el. Ez épp azt jelenti, hogy a 9 szelvény 1-hiba javító kódot alkot. Ezek szerint a 4.6 feladatra adott megoldások bármelyike optimális szelvényeket szolgáltat, csak a 0-kat kell X-re cserélni.
**Megjegyzés** (*Tökéletes kódok*)
Tekintsünk $k$ különböző karaktert, és a belőlük alkotható összes $n$ hosszú sorozatok, "szavak", $H$ halmazát. Úgy is tekinthetjük, mintha $n$ mérkőzésünk lenne és mindegyiknek $k$-féle eredménye lehetne. Legyen $r$ rögzített pozitív egész, és $h \in H$ tetszőleges szó. "$h$ középpontú $r$ sugarú körlapon" azoknak a szavaknak a halmazát értjük, amelyeknek $h$-tól való Hamming távolsága legfeljebb $r$. A "kódelmélész" arra törekszik, hogy minél több szót találjon úgy, hogy a köréjük írt $r$ sugarú körlapok diszjunktak legyenek. $r = 1$ esetén pld így 1-hiba javító kódot kap. A "totózó" célja ezzel némileg ellentétes: ő szavaknak egy olyan készletét keresi, amelyek köré írt $r$ sugarú körlapok lefednek minden szót, nem marad ki egy "eredmény" sem. Így ő olyan optimális szelvény-készletet állít elő, amellyel biztosan nyer, ha $r$ találatot enged a telitalálatból. Bizonyos ($k$, $n$, $r$) számhármasoknál céljukat ugyanannyi szóval, ugyanazzal a szókészlettel érik el. Az ilyen szókészletek a tökéletes kódok.

**5.7** A szenvedélyes játékosok már régóta keresik az olyan nyerőesélyes tipprendszereket, úgynevezett *totókulcsokat*, mint amilyet az 5.6 feladatban is kerestünk. Mégis, már "kicsinek" tűnő esetekben sem ismeretes, hogy legkevesebb hány szelvény kell bizonyos számú találat eléréséhez.

Az alábbi táblázat[1] mutatja, hogy mit tudott a világ 1995-ben. $n$ a mérkőzések számát jelöli, $r$ pedig azt mutatja, hogy legfeljebb hány találatot engedünk ki a kezünkből. Az 5.6 feladat az $n = 4$, $r = 1$ esetnek felel meg ($k = 3$).

| $n/r$ | **1** | **2** | **3** |
|---|---|---|---|
| 1 | 1 | | |
| 2 | 3 | 1 | |
| 3 | 5 | 3 | 1 |
| 4 | 9 | 3 | 3 |
| 5 | 27 | 8 | 3 |
| 6 | 63-73 | 12-17 | 6 |
| 7 | 150-186 | 26-34 | 7-12 |
| 8 | 393-486 | 52-81 | 13-27 |
| 9 | 1048-1356 | 128-219 | 25-54 |
| 10 | 2818-3645 | 323-558 | 57-108 |
| 11 | 7767-9477 | 729 | 115-729 |
| 12 | 21395-27702 | 1919-2187 | 282-729 |
| 13 | 59049 | 5062-6561 | 609-1215 |

Látható, hogy elég kevés konkrét eredmény ismert. Az alábbi kérdés az egyik pontos eredményre kérdez rá.

Mutassuk meg, hogy a 13 mérkőzésből álló totón legalább 59049 szelvényt kell kitölteni ahhoz, hogy biztosan elérjünk legalább 12 találatot!

**Megoldás**
Összesen $3^{13}$-féle szelvény lehetséges. Egy szelvénnyel $1 + 2 \cdot 13 = 27 = 3^3$ esetben van legalább 12 találatunk, így legalább $3^{13}/3^3 = 3^{10} = 59049$ szelvényre van szükség.

**2. Házi feladat**
Kísérelünk meg konstruálni 59049 megfelelő szelvényt.

**Megjegyzés**
Látható, hogy $k = 3$ esetén akkor van lehetőség 1-hiba javító tökéletes kódra ($r = 1$), ha $1 + 2n = 3^s$. Ha tehát $s$ tetszőleges pozitív egész,

$$n = \frac{3^s - 1}{2}, \qquad k = \frac{3^n}{1+2n} = \frac{3^n}{3^s} = 3^{n-s} = 3^{\frac{3^s-1}{2}-s},$$

[1] Forrás: H. Hämäläinen, I. Honkala, S. Lytsin, P. Östergøard, Football Pools - A Game for Mathematicians, *American Math. Monthly*, August-Sept 1995, 579-588.

akkor az egyszerű leszámlálás nem zárja ki tökéletes kód létezését.

**3. Házi feladat**

**5.9** Most is az 1, 2, 3, ...16 számok közül kell kitalálni egyet barkochba kérdésekkel. Kérdéseinket előre le kell írni és nincs befolyásunk arra, hogy a gondoló milyen sorrendben nézi és válaszolja meg azokat.[2]
Hány kérdéssel tudjuk biztosan kitalálni a gondolt számot, ha várhatóan egyszer (legfeljebb egyszer) téves választ kapunk?

**4. Házi feladat**

**Hétszögminták** Ebben a feladatban egy szabályos hétszög csúcsaira írunk 0-t vagy 1-et. Összesen $2^7=128$ ilyen kitöltés van. A kitöltések egy $I_7$ részhalmaza "7-szögre ideális", ha
1. Ha $h\in I_7 \Rightarrow h$ bármely ($n\cdot 360°/7$-kal való) elforgatottja is $I_7$-ben van.
2. Bármely két $I_7$-beli kitöltés csúcsonként és mod 2 számított összege is $I_7$-ben van.
A kitöltéseknek hány "7-szögre ideális" részhalmaza van?

[2] Ezzel az "Előző válaszod igaz volt?" - típusú kérdéseket akarjuk kiszűrni. Tehát kérdés nem vonatkozhat a válaszok igazságtartalmára.

Folytattuk a Kódok feladatgyűjtemény feldolgozását, leginkább az 5.9. feladattal foglalkoztunk. Menet közben megismerkedtünk a lineáris kód fogalmával, és több példán is láttuk, hogyan lehet 1-hiba javító lineáris kódot konstruálni.

**Házi feladat**nak a múlt óráról megmaradt: **hétszögminták**, **13-as totó**, új példák: **5.11, fizetős barkochba**.

## A 18. szakkör részletezett anyaga

**5.9** Most is az 1, 2, 3, ...16 számok közül kell kitalálni egyet barkochba-kérdésekkel. Kérdéseinket előre le kell írni és nincs befolyásunk arra, hogy a gondoló milyen sorrendben nézi és válaszolja meg azokat.[3] Hány kérdéssel tudjuk biztosan kitalálni a gondolt számot, ha várhatóan egyszer (legfeljebb egyszer) téves választ kapunk?

**Megoldás (Alsó korlát)**
Tegyük fel, hogy $k$ előre leírt kérdéssel ki lehet találni a gondolt számot. Tekintsük ezt a $k$ kérdést, és válasszuk ki a 16 szám egyikét, mintha az lenne a gondolt szám. Válaszoljuk meg a $k$ db kérdést hazugság nélkül. Írjunk 0-t az "igen", 1-est a "nem" válasz helyett. Így egy $k$ hosszúságú 0-1 sorozatot kapunk, amit a kiválasztott szám ***kód***jának fogok nevezni. Ha a válaszoló egyszer hazudik, akkor nem a szám kódját kapjuk, hanem egy olyan sorozatot, amely egy helyen különbözik a szám kódjától. Az ilyen sorozatokat a szám ***álkód***jának fogom nevezni. Álkódból éppen $k$ darab van, mert a $k$ kérdésből egyre kaphatunk rossz választ, és mindegyik kérdésre egyféle rossz választ kaphatunk. A 16 számhoz 16 kód és 16$k$ álkód tartozik. Ezeknek mind különbözőeknek kell lennie, mert ha volna közös elemük, akkor az annak a 0-1 sorozatnak megfelelő válaszok esetén nem tudnánk kitalálni a gondolt számot. Összesen $2^k$ darab $k$ hosszú 0-1 sorozat van, így biztosan teljesül a $16\cdot(k+1) \le 2^k$ egyenlőtlenség. A két oldal értékét $k = 1, 2, \ldots$ esetén táblázatban írom fel.

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $16\cdot(k+1)$ | 32 | 48 | 64 | 80 | 96 | 112 | 128 | 144 |
| $2^k$ | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |

Látható, hogy az egyenlőtlenség a $k = 7$ esetben teljesül először. Tehát legalább 7 előre leírt kérdésre van szükség.

**I. konstrukció** ("Mohó algoritmus")
7 előre leírt kérdéssel megoldható a feladat.
Ennek igazolásához 16 db olyan 7 hosszúságú 0-1 sorozatot kell megadni, amelyek közül bármelyik kettő legalább három helyen eltér egymástól. Ebből ugyanis következik, hogy a 16 kód és $16\cdot7$ álkód mind különböző lesz: ha két különböző kódhoz tartozó álkód megegyezik, akkor a két kód csak két helyen tér el egymástól.

Mohó algoritmussal dolgozunk. A 0000000 sorozattól kezdve a lexikografikusan legkisebb olyan sorozatot keressük, amelyik mindegyik korábban már kiválasztott sorozattól legalább 3 helyen különbözik. Az eredményül kapott 16 db 0 - 1 sorozat az alábbi táblázat oszlopaiban található:

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. sor | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2. sor | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 3. sor | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 4. sor | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 5. sor | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 6. sor | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 7. sor | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |

A 7 kérdés a 7 sorból olvasható ki. Egy oszlophoz tartozó kérdés, azokra az 1 és 16 közti számokra kérdez rá, amelyek sorában az adott oszlopban 0 áll. A hét kérdés mindegyike így kezdődik: "A gondolt szám az itt megadott halmazban van?". A hét megadott halmaz az alábbi sorokban olvasható:

[3] Ezzel az "Előző válaszod igaz volt?" - típusú kérdéseket akarjuk kiszűrni. Tehát kérdés nem vonatkozhat a válaszok igazságtartalmára.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. kérdés: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | | | | | |
| 2. kérdés: | 1 | 2 | 3 | 4 | | | | | 9 | 10 | 11 | 12 | | |
| 3. kérdés: | 1 | 2 | | | 5 | 6 | | | 9 | 10 | | | 13 | 14 |
| 4. kérdés: | 1 | 2 | | | | | 7 | 8 | | | 11 | 12 | 13 | 14 |
| 5. kérdés: | 1 | | 3 | | 5 | | 7 | | 9 | | 11 | | 13 | | 15 |
| 6. kérdés: | 1 | | 3 | | | 6 | | 8 | | 10 | | 12 | 13 | | 15 |
| 7. kérdés: | 1 | | | 4 | 5 | | | 8 | | 10 | 11 | | | 14 | 15 |

Érdekes, hogy a fenti 1., 2., 3., 5. kérdések rendre megegyeznek az **5.8 b)** feladatra adott megoldások kérdéseivel (lásd a 16. szakkört).

**II. konstrukció** (*Algebra I.*)
Az **5.8 b)** feladatra adott II. konstrukcióra építve az **1.2** feladat IV. megoldásának mintájára (lásd a 15. szakkört) dolgozunk.
Legyen ($n$-1) kettes számrendszerbeli alakja $x_8x_4x_2x_1$ ($n \in 1, 2, ..., 16$, $x_i \in 0, 1$). Ebben a megközelítésben az **5.8 b)** feladatra adott II. konstrukció kérdései így írhatók:

"$x_8 = 0$?"; "$x_4 = 0$?"; "$x_2 = 0$?"; "$x_1 = 0$?".

Állítjuk, hogy a jelen feladat megoldását kapjuk, ha a fenti négy kérdést kiegészítjük az alábbi hárommal:

"$x_4+x_2+x_1 = 0$?"; "$x_8+x_2+x_1 = 0$?"; "$x_8+x_4+x_1 = 0$?",

ahol az összeadás és az egyenlőség mindenütt mod 2 értendő.
A válaszokat elfogadva megállapíthatjuk $x_8$, $x_4$, $x_2$, $x_1$, $x_4+x_2+x_1$, $x_8+x_2+x_1$, $x_8+x_4+x_1$ értékeit és az első négyre kapott értékkel leellenőrizhetjük az utolsó hármat. Ha egyik ellenőrzés sem teljesül, akkor biztosan $x_1$ volt a ludas, értékét kijavíthatjuk. Ha két ellenőrzésnél sem stimmelt az összeg, akkor $x_2$, $x_4$ vagy $x_8$ értéke volt hibás, attól függően, hogy melyik két egyenlettel volt baj. Mindegyik változó legalább két összegben szerepel, így ha csak egy ellenőrzésnél jutottunk ellentmondáshoz, akkor biztosan annak az összegnek az értékét kaptuk rosszul, a változók értékei helyesek. Végül, ha minden ellenőrzés klappolt, akkor nem is kaptunk hamis választ, tudjuk a változók értékeit.

**Megjegyzés**
Mutassuk meg, hogy az I. konstrukcióban megadott kérdések is megfogalmazhatók a II. konstrukcióban adott algebrai alakban!

**III. konstrukció** (*Algebra II.*, Hamming kód)
Az I. konstrukció gondolatmenete alapján, de a II. konstrukcióban szereplő algebrai módszerhez hasonló megoldást keresünk.
16 db olyan hét hosszúságú 0 - 1 sorozatot kell megadni, amelyek közül bármelyik kettő legalább három helyen eltér egymástól. Szeretnénk ezeket a sorozatokat egy

$$a_1 \cdot y_1 + a_2 \cdot y_2 + ... + a_7 \cdot y_7 = 0,$$
$$b_1 \cdot y_1 + b_2 \cdot y_2 + ... + b_7 \cdot y_7 = 0,$$
$$c_1 \cdot y_1 + c_2 \cdot y_2 + ... + c_7 \cdot y_7 = 0$$

homogén lineáris egyenletrendszer megoldásaként előállítani. (Itt, és az alábbiakban a +, · műveletek és az egyenlőség is mod 2 értendő, az együtthatók, változók értékei 0 és 1 lehetnek.) Azaz olyan $a_1$, $a_2$, ..., $a_7$, $b_1$, $b_2$, ..., $b_7$, $c_1$, $c_2$, ..., $c_7$ együtthatókat keresünk, amelyek esetén a fenti egyenletrendszert kielégítő $y_1\, y_2\, ...\, y_7$ sorozatok közül bármelyik kettő legalább 3 helyen eltér egymástól. Az ilyen kódot *lineáris kód*nak nevezik.

A lineáris kódnak a következő előnye van. Az egyenletrendszer egyik megoldása, tehát az egyik kódszó a 00...0 sorozat. Tegyük fel, hogy sikerül olyan az egyenletrendszer együtthatóit úgy megválasztani, hogy bármelyik másik megoldás 00...0-tól legalább három helyen térjen el, azaz legalább három 1-es legyen benne. Állítjuk, hogy ebben az esetben bármelyik két megoldás legalább három helyen eltér egymástól. Valóban, ha az $y_{11}\, y_{21}\, ...\, y_{71}$ és az $y_{12}\, y_{22}\, ...\, y_{72}$ sorozat is teljesíti a fenti egyenletrendszert, azaz

$$a_1 \cdot y_{11} + a_2 \cdot y_{21} + ... + a_7 \cdot y_{71} = 0, \qquad a_1 \cdot y_{12} + a_2 \cdot y_{22} + ... + a_7 \cdot y_{72} = 0,$$
$$b_1 \cdot y_{11} + b_2 \cdot y_{21} + ... + b_7 \cdot y_{71} = 0, \qquad b_1 \cdot y_{12} + b_2 \cdot y_{22} + ... + b_7 \cdot y_{72} = 0,$$
$$c_1 \cdot y_{11} + c_2 \cdot y_{21} + ... + c_7 \cdot y_{71} = 0, \qquad c_1 \cdot y_{12} + c_2 \cdot y_{22} + ... + c_7 \cdot y_{72} = 0,$$

akkor a megfelelő egyenletek kivonása révén kapjuk, hogy

$$a_1\cdot(y_{11}-y_{12})+a_2\cdot(y_{21}-y_{22})+\ldots+a_7\cdot(y_{71}-y_{72})=0,$$
$$b_1\cdot(y_{11}-y_{12})+b_2\cdot(y_{21}-y_{22})+\ldots+b_7\cdot(y_{71}-y_{72})=0,$$
$$c_1\cdot(y_{11}-y_{12})+c_2\cdot(y_{21}-y_{22})+\ldots+c_7\cdot(y_{71}-y_{72})=0,$$

azaz az $(y_{11}-y_{12})\,(y_{21}-y_{22})\ldots(y_{71}-y_{72})$ sorozat is teljesíti az eredeti egyenletrendszert. Ebben a sorozatban feltételünk szerint legalább három 1-es van, de pontosan ott van benne 0-tól különböző szám, ahol az $y_{11}\,y_{21}\ldots y_{71}$, $y_{12}\,y_{22}\ldots y_{72}$ sorozatok eltérnek egymástól. Tehát ha egy lineáris kódban nincs olyan kódszó, amelyikben egy vagy két 0-tól különböző jel van, akkor bármely két kódszó távolsága legalább három.

Feltételi egyenlet nélkül az $y_1, y_2, \ldots, y_7$ bináris változók értékei $2^7$-féleképpen választhatók meg, hiszen mind a hét változó szabadon és egymástól függetlenül fölveheti a 0, 1 értékek bármelyikét. Egy egyenlet lehetőséget ad, hogy az egyik változót kifejezzük a többiből, így a szabad változók száma eggyel csökken. Azt szeretnénk elérni, hogy az egyenletrendszernek $16 = 2^4$ megoldása legyen, ehhez 3 (független) egyenletet kell megadni.

Az

$$a_1\cdot y_1+a_2\cdot y_2+\ldots+a_7\cdot y_7=0,$$
$$b_1\cdot y_1+b_2\cdot y_2+\ldots+b_7\cdot y_7=0,$$
$$c_1\cdot y_1+c_2\cdot y_2+\ldots+c_7\cdot y_7=0$$

egyenletrendszer tehát pontosan akkor megfelelő, ha (egyenletei függetlenek és) nincs olyan megoldása, amelyben az ismeretlenek közül egynek vagy kettőnek az értéke 1-es (és a többi 0).

$y_1 = 1, y_2 = \ldots = y_7 = 0$ pontosan akkor megoldása a fenti egyenletrendszernek, ha az

$$A=\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 \end{pmatrix}$$

mátrix első oszlopában mindenütt 0 áll. Általában, egyenletrendszerünknek pontosan akkor van olyan megoldása, amelyben az egyik változó értéke 1, a többié 0, ha $A$-nak van azonosan 0 oszlopa.
$y_1 = y_2 = 1$, $y_3 = \ldots = y_7 = 0$ pontosan akkor megoldása az egyenletrendszernek, ha az $A$ mátrix első két oszlopa egyenlő egymással. Általában, pontosan akkor van olyan megoldás, amelyben két változó értéke 1, a többié 0, ha $A$-nak van két egyforma oszlopa. Az $A$ mátrix tehát pontosan akkor ad megfelelő egyenletrendszert, ha egyik oszlopa sem egyezik meg az azonosan 0 oszloppal vagy egy másik oszloppal (és az egyenletek függetlenek).

$A$ egy-egy oszlopa egy három elemből álló bináris sorozat, amely $2^3 = 8$-féleképpen választható meg. A 8 közül az egyik azonosan 0, ez nem lehet $A$-ban, tehát $A$ oszlopai - a sorrendtől eltekintve - egyértelműen meghatározottak:

$$A=\begin{pmatrix} 1&1&1&0&1&0&0 \\ 1&1&0&1&0&1&0 \\ 1&0&1&1&0&0&1 \end{pmatrix}.$$

Tehát a megfelelő egyenletrendszer:

$$1\cdot y_1+1\cdot y_2+1\cdot y_3+0\cdot y_4+1\cdot y_5+0\cdot y_6+0\cdot y_7=0,$$
$$1\cdot y_1+1\cdot y_2+0\cdot y_3+1\cdot y_4+0\cdot y_5+1\cdot y_6+0\cdot y_7=0,$$
$$1\cdot y_1+0\cdot y_2+1\cdot y_3+1\cdot y_4+0\cdot y_5+0\cdot y_6+1\cdot y_7=0,$$

Ennek valóban 16 megoldása van (azaz egyenletei függetlenek) hiszen $y_1, y_2, y_3, y_4$ értékei szabadon választhatók és

$$y_5=1\cdot y_1+1\cdot y_2+1\cdot y_3+0\cdot y_4,$$
$$y_6=1\cdot y_1+1\cdot y_2+0\cdot y_3+1\cdot y_4,$$
$$y_7=1\cdot y_1+0\cdot y_2+1\cdot y_3+1\cdot y_4.$$

A 16 megoldás itt látható:

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_1$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $y_2$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| $y_3$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| $y_4$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $y_5$ | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| $y_6$ | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| $y_7$ | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |

Látható, hogy - két sor felcserélődésétől eltekintve - ugyanahhoz a táblázathoz jutottunk, mint az I. konstrukció esetén.

**Megjegyzés**
Az előbb látottak alapján új konstrukciót adunk a múlt órai **4.6**, **5.6** példákhoz. Most tehát háromféle jelünk van, pld 0, 1, 2 és négyes sorozatokat kell gyártanunk. Számoljunk mod 3 (tehát 2 = -1), és keressünk olyan

$$a_1 \cdot y_1 + a_2 \cdot y_2 + a_3 \cdot y_3 + a_4 \cdot y_4 = 0,$$
$$b_1 \cdot y_1 + b_2 \cdot y_2 + b_3 \cdot y_3 + b_4 \cdot y_4 = 0$$

alakú egyenletrendszert , amely megoldáshalmaza 1-hiba javító lineáris kód! Azért van szükség most csak két egyenletre, mert 4 változónk van, de 9 kódszót keresünk, tehát két szabad változót kell hagynunk, kettőt kell tudni kiküszöbölni az egyenletekkel. Most is úgy kell megválasztani az egyenletrendszer együtthatóinak

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{pmatrix}$$

mátrixát, hogy az egyenletrendszernek ne legyen olyan megoldása, amelyben csak egy vagy két változó értéke különbözik 0-tól. Az egy darab 0-tól különböző elemet tartalmazó sorozatokat most is úgy tudjuk kizárni, hogy nem engedünk meg a mátrixban olyan oszlopot, amelyben mindkét elem 0. Tekintsünk most két darab nullától különböző elemet tartalmazó sorozatokat, legyen pld $y_1 = y_2 \neq 0$, $y_3 = y_4 = 0$. Ez pontosan akkor megoldás, ha $a_1 = -a_2$ és $b_1 = -b_2$, azaz ha az

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}, \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$$

oszlopvektorok egymás ellentettjei. Az $y_1 = 1$, $y_2 = -1$, $y_3 = y_4 = 0$ valamint az $y_1 = -1$, $y_2 = 1$, $y_3 = y_4 = 0$ számnégyesek pontosan akkor megoldások, ha $a_1 = a_2$ és $b_1 = b_2$, azaz ha

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}.$$

Ha nem akarunk olyan megoldásokat, amelyek legfeljebb két helyen térnek el egymástól, akkor olyan $A$ mátrixot kell választani, amelynek nincsenek azonosan 0, egymással egyenlő, illetve egymással ellentétes oszlopai. Pld egy ilyen mátrix:

$$\begin{pmatrix} 1120 \\ 2102 \end{pmatrix},$$

amely az

$$y_1 + y_2 + 2 \cdot y_3 = 0,$$
$$2 \cdot y_1 + y_2 + 2 \cdot y_4 = 0$$

egyenletrendszert, azaz a

$$y_1 + y_2 = y_3,$$
$$2 \cdot y_1 + y_2 = y_4$$

összefüggéseket határozza meg. Épp ezeket "találtuk ki" az előző órán a 4.6 feladat II. megoldásában.

**IV. konstrukció** (*Négyzetminta*)
Térjünk vissza a "Négyzetminta" feladathoz, az előző foglalkozás első példájához! Egész számok helyett számoljunk binárisan (mod 2), azaz a "páros" és "páratlan" szavakat 0 és 1 helyettesítse! A négyzet csúcsaihoz írt 8 számot 16-féleképpen adhatjuk meg, hiszen a csúcsokhoz először írt egy-egy szám összesen $2^4$-féle lehet és ezek már meghatározzák a további négy számot. Így tehát összesen 16 db 0-1 sorozatot kapunk, amelyek egy lineáris halmazt alkotnak, azaz a 16 közül bármelyik két sorozat összege (természetesen koordinátánként és mod 2 értve) is a 16 sorozat között van. A "Négyzetminta" feladatban azt láttuk, hogy e sorozatokban 0, 4 vagy 8 db 1-es lehet, tehát a 16 sorozat egy olyan lineáris kódot alkot, amelynek minimális távolsága 4. Ha a nyolcelemű sorozatok egyik, pld az utolsó elemét mindegyikben elhagyjuk, akkor 16 olyan hételemű 0-1 sorozatot kapunk, amelyek közül bármelyik kettő Hamming távolsága legalább 3. Az I. konstrukció elején leírtak szerint éppen ilyen sorozatokat kerestünk.

Végül két levezető feladat:
**Jó-30-as** Az egész számok egy $I_{30}$ részhalmazát "jó 30-as"-nak nevezzük, ha teljesülnek rá az alábbi feltételek:

1. Ha $h \in I_{30}$ és $n$ tetszőleges egész szám, akkor $n \cdot h \in I_{30}$.
2. Ha $h_1 \in I_{30}$ és $h_2 \in I_{30}$, akkor $h_1 + h_2 \in I_{30}$.
3. $30 \in I_{30}$.

Az egész számok halmazának hány "jó 30-as" részhalmaza van?

**Megoldás**
Az 1. - 2. tulajdonságokból következik, hogy jó 30-as halmazban lehet maradékosan osztani, azaz, ha $h_1 \in I_{30}$ és $h_2 \in I_{30}$ és $h_1 = n \cdot h_2 + m$ ahol $n$, $m$ egész számok, akkor $m \in I_{30}$. Legyen $k$ egy jó 30-as halmaz (egyik) legkisebb abszolút-értékű, de 0-tól különböző eleme. (Ilyen elem biztos van, hiszen 30 benne van a halmazban, így csak az 1, 2, ... 30 eseteket kell végignézni.) Ekkor $k$ minden többszöröse is a jó 30-as halmazban van, de más elem nem is lehet a halmazban, mert a maradékos osztás $k$-nál kisebb abszolút-értékű elemet eredményezne. Tehát minden jó 30-as halmaz egy elem összes többszöröséből áll. 30 pontosan akkor lesz egy ilyen halmaznak eleme, ha a szóbanforgó elem 30 osztója. 8 megfelelő halmaz van, ezek rendre 30, 15, 10, 6, 5, 3, 2, 1 összes többszöröseiből állnak.

**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?

Ez a feladat **házi feladat**nak maradt. További gondolkodnivalók:

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 $I_7$ részhalmaza "7-szögre ideális", ha
1. Ha $h \in I_7 \Rightarrow h$ bármely ($n \cdot 360°/7$-kal való) elforgatottja is $I_7$-ben van.
2. Bármely két $I_7$-beli kitöltés csúcsonként és mod 2 számított összege is $I_7$-ben van.
A kitöltéseknek hány "7-szögre ideális" részhalmaza van?

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

Új feladat:
**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?

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 feladat**nak 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

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

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 $I_{101}$ részhalmazát "ideális 101-es"-nek nevezzük,

1. ha $h \in I_{101} \Rightarrow h0 \in I_{101}$; ($h0$ a $h$ dupláját, tehát azt a számot jelöli, amelyet úgy kapunk, hogy $h$ mögé írunk egy 0-t)
2. ha $h \in I_{101}$ és $j \in I_{101} \Rightarrow h + j \in I_{101}$;
3. ha $101 \in I_{101}$ (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 $1 \in I_{101}$ és alkalmazzuk az 1., 2. szabályokat, akkor ezt a "részhalmazt" kapjuk.
B) Ha csak annyit teszünk fel, hogy $101 \in I_{101}$ 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 $a = a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + ... + a_1 \cdot 2^1 + a_0 \cdot 2^0 = a_n a_{n-1} ... a_1 a_0$ számnak az $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0$ polinom feleljen meg.

**Megoldás**
A megfeleltetés után már a polinomok részhalmazait keressük. Az 1. tulajdonság azt jelenti, hogy $I_{101}$-beli polinom $x$-szerese is $I_{101}$-ben van, 2. szerint pedig $I_{101}$-beli polinomok összege is ott van. Ezekből az is következik, hogy $I_{101}$-beli polinom tetszőleges polinomszorosa is $I_{101}$-ben van, hiszen bármely polinommal való szorzás felépíthető $x$-szel való szorzásokból és polinomok összeadásából. Az $x^4 + x$ polinommal például úgy szorzunk meg egy másik polinomot, hogy egymás után négyszer megszorozzuk $x$-szel és az eredményhez hozzáadjuk az $x$-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 $I_{101}$ legkisebb fokú (az azonosan 0-tól különböző) eleme a $p$ polinom. Ha $q \in I_{101}$, akkor $p|q$, mert a $q$ polinom $p$-vel való osztási maradéka is $I_{101}$-ben van és $p$-nél kisebb fokú, így 0. Tehát $I_{101}$ a $p$ összes többszöröséből, és csakis azokból áll. Annyi megoldás van, ahány osztója van az $x^2 + 1$ polinomnak. Az osztók: 1, $x + 1$, $x^2 + 1$, 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 $I_7$ részhalmaza "7-szögre ideális",
1. ha $h \in I_7 \Rightarrow h$ bármely ($n \cdot 360°/7$-kal való) elforgatottja is $I_7$-ben van.
2. ha bármely két $I_7$-beli kitöltés csúcsonként és mod 2 számított összege is $I_7$-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?

Az előadó betegsége miatt az óra kissé szokatlan volt. A nebulók a **4.7**, **5.10** feladatok megoldásával folytatták a Kódok feladatgyűjtemény feldolgozását, majd egy esszét olvashattak a CD működésének matematikai alapjairól.
Új házi feladat nincs, de korábbról megmaradt még a **hétszögminták**, **5.11**, az **Általános Hamming-kód** és az **"Ideális 1001-es"**.

## A 20. szakkör részletezett anyaga

**4.7** Összehasonlítunk három kódot! Mindhárom kód kilenc szóból áll, mindegyik egy hárombetűs ABC-t használ.
$k_1$) *A legegyszerűbb*: A szavak kétbetűsek, a kilenc kódszó az összes kétbetűs szó.
$k_2$) *Mindent háromszor*: A szavak hatbetűsek és úgy készülnek, hogy a kétbetűs szót háromszor írjuk le egymás után.
$k_3$) *A sűrű*: A szavak négybetűsek, a 4.6 feladatban meghatározott 1-hiba javító tökéletes kódot alkotják.

Tegyük fel, hogy egy betű a kommunikáció során 10% eséllyel megváltozik és 90% eséllyel jól továbbítódik. $k_2$ és $k_3$ esetén a kiolvasott jelsorozatot mindig a tőle legkevesebb jelben eltérő kódszóra változtatjuk. Ha ez nem egyértelmű, akkor nem javítunk. Határozzuk meg a három esetben külön-külön, hogy mi az esélye, hogy egy szót úgy olvasunk ki, ahogy elküldték!

**Megoldás**
$k_1$ esetén mindkét jelet jól kell kiolvasni, így $0{,}9^2 = 0{,}81$ alapján 81% az esély.
$k_2$ esetén mindkét jel három példányából háromnak vagy kettőnek kell helyesen megérkeznie, tehát a számolás: $(0{,}9^3 + 3\cdot 0{,}1\cdot 0{,}9^2)^2 = 0{,}944784$, azaz 94,4784% az esély.
$k_3$ esetén a négy jelből négynek vagy háromnak kell helyesnek lennie, így $0{,}9^4 + 4\cdot 0{,}1\cdot 0{,}9^3 = 0{,}9477$ alapján 94,77% az esély.

**5.10** (*Dienes Péter javaslata*)
Hanyag Hugó az 1, 2, 3, ..., 16 számok egyikére gondolt. Egy-egy cetlire kell fölírni kérdéseinket, s mind odaadni neki, majd amikor ráér egyszerre mindegyikre válaszol fog. De lehet rá számítani, hogy az egyik választ elveszti mielőtt az eljutna hozzánk. Legalább hány kérdésre van így szükség ahhoz, hogy kitaláljuk a gondolt számot?

**Megoldás**
Öt kérdés nyilván szükséges, de ennyi elég is. Öt megfelelő kérdés megkapható az 5.9 feladatra adott bármelyik konstrukció mintájára (lásd a 18. szakkör anyagát).

Most 16 db olyan 5 hosszúságú 0 - 1 sorozatot keresünk, amelyek közül bármelyik kettő legalább két helyen eltér egymástól. Ha ugyanis az egyik kérdésre nem érkezik válasz, azaz a sorozatokban az egyik helyen álló elem eltűnik, akkor továbbra is 16 különböző sorozatot kell kapjunk. Ez felel meg annak, hogy a négy megmaradt kérdésre adott válaszból minden esetben kitalálható a gondolt szám. Az alábbi táblázat oszlopaiba 16 megfelelő sorozatot írtunk be.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. sor | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2. sor | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 3. sor | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 4. sor | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 5. sor | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |

Látható, hogy az utolsó sor az előzőekhez hozzátett paritásjelző-bit. Az öt kérdés közül az első négy megegyezik az 5.8 b) feladat megoldásaként konstruált négy kérdéssel, az ötödik
pedig azokra a számokra kérdez rá, amelyekre addig páratlan sokszor kérdeztünk rá. Így összességében minden számra páros sokszor kérdezünk rá, tehát ha mind az öt kérdésre kapnánk választ, akkor páros sok "Igen"-t hallanánk. Ezért, ha egy válasz hiányzik, akkor az már kitalálható a többi négyből.

**Megjegyzések**
1. Az 5.9 feladatra (hazudós barkochba) adott II. konstrukció szellemében fenti kérdéseink így is írhatók:
"$x_8 = 0$?"; "$x_4 = 0$?"; "$x_2 = 0$?"; "$x_1 = 0$?"; "$x_8 + x_4 + x_2 + x_1 = 0$?".

2. Táblázatunk oszlopai most egy 16 kódszóból álló ötbetűs 1-törlés javító kódot alkotnak.

A CD-ről szóló esszé előtt felelevenítjük a **házi feladatokat:**

**"Ideális 1001-es"** Oldjuk meg az "ideális 101-es" feladatot 101 helyett mindenütt 1001-gyel!

**Hétszögminták** Ebben a feladatban egy szabályos hétszög csúcsaira írunk 0-t vagy 1-et. Összesen $2^7=128$ ilyen kitöltés van. A kitöltések egy $I_7$ részhalmaza "7-szögre ideális",
1. ha $h \in I_7 \Rightarrow h$ bármely ($n \cdot 360°/7$-kal való) elforgatottja is $I_7$-ben van.
2. ha bármely két $I_7$-beli kitöltés csúcsonként és mod 2 számított összege is $I_7$-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?

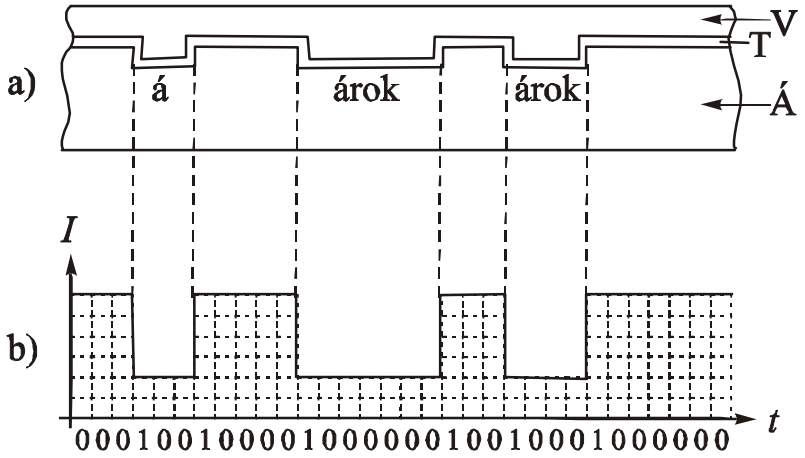
**A CD matematikája**

Ennek a fejezetnek az anyagát nagyrészt a J. H. van Lint, The Mathematics of the Compact Disc, *DMV-Mitteilungen* 4/98, 25--29. és a Compact disc digital audio, *Philips technical review*, Vol. 40, 1982, No. 6. művek alapján állítottuk össze.

**A pálya**

A CD lejátszót a Philips és a Sony cég fejlesztette ki.
Maga a lemez egyetlen egy pályából áll, ami 5 km hosszú. Ezen binárisan van tárolva az információ. "Síkságok" és "árkok" követik egymást, de az árok alja is sík. Az 1-es bitet a változás, az árok széle, a 0-át az egységnyi hosszúságú vízszintes rész jelöli, amely lehet síkságon vagy az árok alján is.

A kódolt üzenetnek nagyon sok feltételt tudnia kell:




a) A CD lemez keresztmetszete a pálya irányában
V: védőréteg; T: tükrözőfelület; Á: átlátszó réteg.
b) *I*: Az optikai olvasófej által érzékelt jel intenzitása az idő (*t*) függvényében.

1) A digitalizálás ellenére az emberi fül számára hűen adja vissza a felvett zenét;
2) Az elszórt véletlenszerű bithibákat képes legyen kijavítani;
3) A csomóban keletkező hibák --- ujjlenyomatok, karcolások, anyaghibák --- korrigálását is megoldja;
4) A hallgató számára információt tudjon nyújtani, hogy hol tart;
5) A lézeres leolvasószerkezet hatékonyan olvasni tudja az információt;
6) A szerkezet működése ne keltsen az emberi fül számára hallható zajt (a lejátszandó zenén kívül).

**Audiobit**

A zene felvételekor az érzékelő bizonyos időnként "mintát vesz", azaz egy-egy pillanatban megméri milyen a beérkező hullám nyomása. Lényegében ez az érték a tárolt információ.
A felvétel lejátszásakor keletkező hang a pillanatnyi minták visszaadásából áll össze, így természetesen nem pont ugyanaz, mint amit fel szándékoztak venni. A mintavételezés gyakoriságától függően, a zenei hang bizonyos hullámhosszú összetevői hűen hallhatók.
Egy fizikai elv, Nyquist tétele, kapcsolatot teremt a mintavételezés gyakorisága, és az abból hűen rekonstruálható hanghullámok frekvenciája között. Ennek a tételnek az alapján és abból kiindulva, hogy az emberi fül kb. 20 000 Hz-ig hall jól másodpercenként 44 100-nek adódik a szükséges mintavételezési gyakoriság.

Minden minta eredményét 16 bitté alakítja a rendszer. A felvétel általában sztereó, így máris 32 bit - úgynevezett *audiobit* - tartozik egyetlen pillanatnyi mintához. A 32 bit 4 byte-ba van rendezve (egy byte az nyolc egymást követő bit).

**2-hiba javító kód**

Ha nem volnának hibajavító kódok hozzátéve a felvett audiobitekhez, akkor a CD lemez lejátszhatatlan minőségű lenne. A leggyakoribb "károkozók" az ujjlenyomatok, az apró karcolások, a lemezben vagy rajta lévő idegen anyagok, a műanyagban óhatatlanul meglévő légbuborékok, az eredeti felületi egyenetlenségek és a felvételkor vétett pontatlanságok.

Tegyük fel, hogy nem alkalmazunk hibajavító kódot. Ha a byte-hiba valószínűsége csupán 0,01% lenne, akkor az egy mintavételnek megfelelő információban, azaz 4 byte-ban megbúvó hiba esélye $1-0{,}9999^4 \approx 0{,}9996$ alapján kb. 0,04%-os lenne. Ez másodpercenként több mint 17 hibás lejátszott hangot okozna.

Tegyük fel először, hogy csak 1-hiba javítást alkalmazunk. A CD-n használt Reed-Solomon-féle kódolási eljárás egy-egy byte-ot egyben, egyetlen "számként" kezel. Ennek részleteibe most nem megyünk bele, inkább egyszerűsítésként képzeljük azt, mintha egy byte-on csak 31-féle információ lenne szállítható. Feleltessünk meg minden lehetőségnek egy 0 és 30 közötti számot és számoljunk velük mod 31.[4]

Az 1-hiba javítás megoldható úgy, hogy minden mintavételnek megfelelő byte-négyeshez még 2 byte-ot veszünk hozzá. Az R-S kódolás ezt az 1.1 feladathoz kicsit hasonlóan oldja meg. Az $x_1$, $x_2$, $x_3$, $x_4$ eredeti byte-ok mellé az $x_5$ és $x_6$ ellenőrző biteket úgy kell választani, hogy teljesüljön az alábbi két összefüggés:

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \equiv 0 \pmod{31},$$
$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 \equiv 0 \pmod{31}.$$

Ha a dekódolásnál kiderül, hogy nem teljesül ez a két összefüggés, mondjuk a felső
bal oldali kifejezés értéke 2, az alsóé pedig 41, azaz 10 (mod 31), akkor - abban bízva, hogy csak 1 hiba történt - kiszámolhatjuk a kódolt információt. Tudjuk, hogy a hiba értéke 2, tehát azt kell megkeresnünk, hogy melyik 1 és 26 közötti szám kétszerese ad 10 maradékot 31-gyel osztva. Ez a szám az 5, tehát az $x_5$ byte hibás, 2-vel nagyobb a kelleténél (mod 31).

Nézzük, most mennyi hibára számíthatunk! Sajnos azzal, hogy megnöveltük a bitsorozat hosszát vagy kevesebb zenét kell rögzítenünk a lemezen, vagy kisebb jeleket sűrűbben kell írnunk a CD-re, ami növeli a hiba valószínűségét. Az első lehetőséget ne fogadjuk el. Tegyük fel, hogy a byte-hiba valószínűsége 0,02%-ra nő. Annak esélye, hogy egy mintavételnek megfelelő, most már 6 byte-ból álló adatsor hibás lesz, tehát 2 hiba kerül bele:

$$1-0{,}9998^6 - 6\cdot 0{,}0002\cdot 0{,}9998^5 \approx 0{,}0000006.$$

Ez másodpercenként csak átlagosan kb. 0,0264 hibás lejátszott hangot okozna, ami lényegesen jobb, mintha nem alkalmaztunk volna kódolást.

Egy, az előzőnél jobb, két hibát javító kóddal még sokkal jobb eredményt érhetünk el. Most byte-négyesek helyett byte-ok nyolcas csoportjaira osztjuk a kódolandó üzenetet, és ezekhez négy további byte-ot illesztünk. Nevezetesen, az eredeti byte-oknak megfelelő 8 szám legyen
$x_1$, $x_2$, ..., $x_8$, a négy ellenőrző szám pedig $x_9$, $x_{10}$, $x_{11}$, $x_{12}$. Szabályaink legyenek

$$x_1 + x_2 + x_3 + x_4 + ... + x_{11} + x_{12} \equiv 0 \pmod{31},$$
$$x_1 + 2x_2 + 3x_3 + 4x_4 + ... + 11x_{11} + 12x_{12} \equiv 0 \pmod{31},$$
$$x_1 + 4x_2 + 9x_3 + 16x_4 + ... + 121x_{11} + 144x_{12} \equiv 0 \pmod{31},$$
$$x_1 + 8x_2 + 27x_3 + 64x_4 + ... + 1331x_{11} + 1728x_{12} \equiv 0 \pmod{31}.$$

Annak részletes vizsgálatát, hogy így 2-hibajavító kódot kapunk, feladatnak hagyjuk. Jegyezzük meg, hogy ebben az esetben is csak másfélszer annyi üzenetet kell átküldenünk, mint kódolás nélkül. Ha tehát itt is a 0,02%-os hibájú berendezést használjuk, akkor a legalább 3
hibát tartalmazó csoportok lesznek azok, amelyeket nem tudunk javítani. Ennek valószínűsége

$$1-0{,}9998^{12} - 12\cdot 0{,}0002\cdot 0{,}9998^{11} - 66\cdot 0{,}0002^2\cdot 0{,}9998^{10} \approx 0{,}000000002.$$

Ha úgy számolunk, hogy ilyenkor a 8 byte-hoz tartozó mindkét hang rossz, akkor is másodpercenként átlagosan csak kb. 0,0000774 hibás lejátszott hangot kapnánk, az egy órányi zene alatt összesen 0,28-at. Ez már elfogadható eredmény.

Lényeges, hogy a CD-n olyan kódot használjunk, amely a lehető legkisebb arányban növeli meg az adatsor hosszát, és nagyon gyorsan dekódolható.

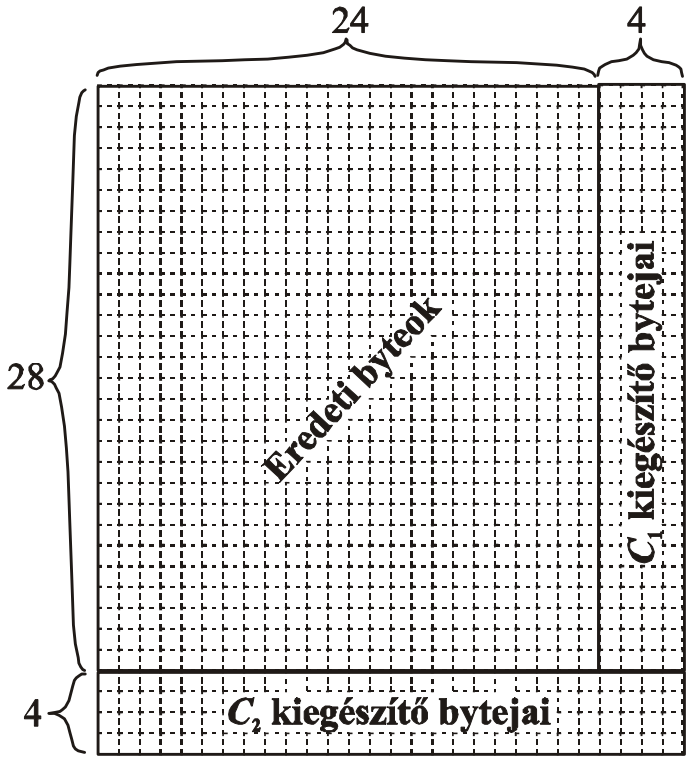
[4] Az egyszerűsítésre azért van szükség, mert a természetesen adódó mod 256 számolás $256=2^8$ esetén az osztással baj van, pl.: a 2 fele az 1 és a 129 is, a 3-nak viszont nincsen fele. Lehet a 256 elemű halmazon úgy értelmezni az alapműveleteket, hogy ne forduljon elő hasonló probléma, ezt láttuk az első félévben.

**"Keresztbe font" kódok**

Eddig csak a véletlenszerű, elszórt hibák kiszűréséről volt szó. Sajnos, a hibák jelentős része csomóban jelentkezik. Ezek ellenében a CD-n két "keresztbe font" (Cross-Interleaved) Reed-Solomon kód biztosítja az információ megmaradását.

Ez egyrészt azt jelenti, hogy az egymáshoz kapcsolódó információk a lemez különböző helyein vannak elhelyezve, az egymás mellé kerülő jelek pedig a lejátszandó zenében valójában egymástól nagyobb időkülönbséggel következnek. Így a hibafolt ugyan több információba "belepiszkít", de mindegyikbe csak egy picit.

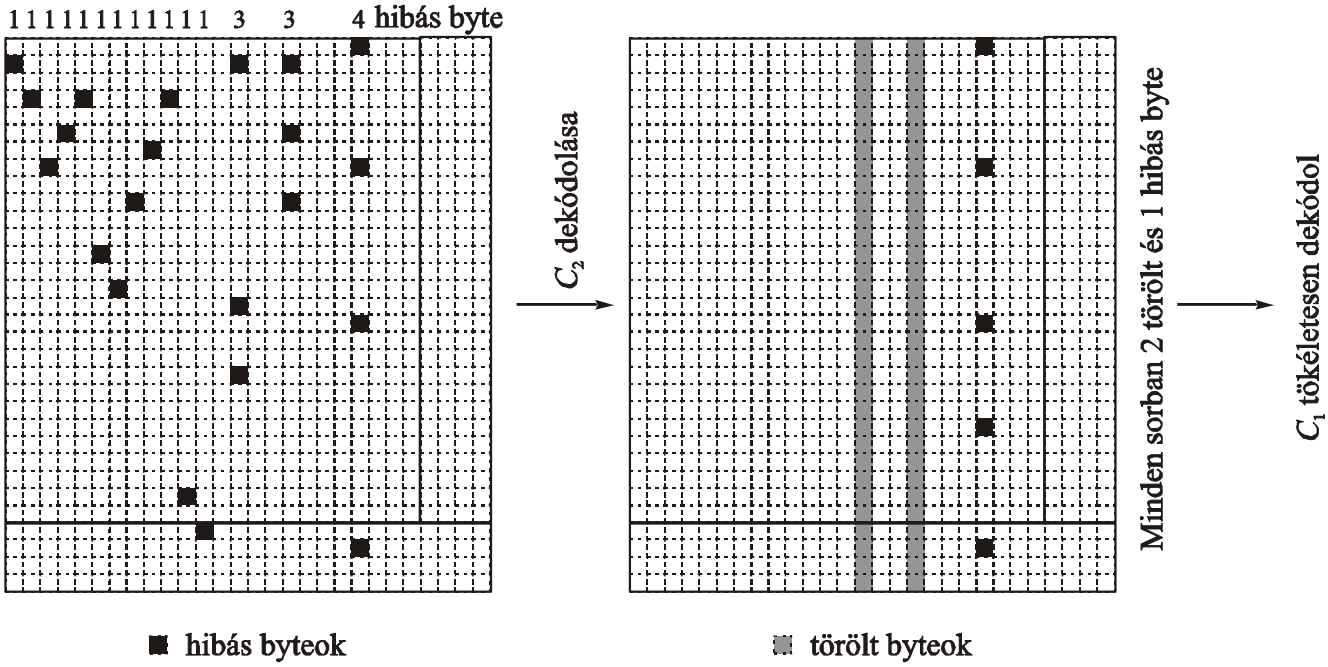
A másik trükk az, hogy a két kódolás az alábbi táblázatos formához hasonló módon működik együtt. Az első, C1 kód 24 byte-ot kezel együtt, ezekhez 4 byte-ot tesz hozzá 2-hiba javító módon, tehát a létrejövő 28 byte-os kódszavak minimális távolsága 5 lesz. Rendezzünk el 28 ilyen, már C1-gyel kódolt 28 byte-os adatsort egy táblázat soraiban! A második, C2 kód 28 byte-ot kezel együtt, a táblázat minden oszlopát további 4 byte-tal egészíti ki 2-hiba javító módon,




Keresztbefont kódok

tehát a létrejövő 32 byte-os oszlopkódok minimális távolsága 5 lesz.

A két kód alkalmazásával lényegében egy 24×28-as táblázat adatait kódoltuk át egy 28×32-es táblázattá. Bebizonyítható, hogy az így létrejövő táblázatok minimális távolsága 25, tehát a kettős kód alkalmas a 28×32 adatban keletkező 12 hiba kijavítására.




Keresztbefont kódok dekódolása

Képzeljünk el egy ennél sokkal rosszabb esetet, amikor 22 hiba van a táblázatban: tizenkét oszlopban 1-1 hiba, két oszlopban 3, egyben pedig 4 hiba is előfordul. Nem várható el, hogy ki tudjuk javítani a hibákat, hiszen az oszlopok 2-hiba javítása után még elképzelhető, hogy marad sor 3 hibával. Úgy döntünk, hogy a C2 kódot a dekódolásnál csak 1-hiba javításra használjuk.
Fel tudjuk ismerni a 3 hibát tartalmazó oszlopokat, mert azok legalább 2 távolságra vannak a legközelebbi kódszótól. Könnyen elképzelhető viszont, hogy a 4 hibát tartalmazó oszlop csak 1 távolságra került egy kódszótól, így azt "kijavítjuk" 5 hibásra. A trükk az, hogy kijavítjuk (legalábbis így képzeljük) az 1 hibát tartalmazó oszlopokat, azokat viszont, amelyekről látjuk, hogy ennél több hibát tartalmaznak csak megjelöljük, hogy "törlendő", ne vegyék figyelembe. Korábbi feladatainknak nyelvén a "hazugságot" "hanyagsággá" változtatjuk. Ez azt jelenti, hogy a 32 oszlopból C2 dekódolása után 29 jó, 2 törlendő, 1-ben pedig 5 hiba is van. Nézzük most a sorokat, amelyeket C1-gyel kódoltunk! Mindegyikben 2 jel törölve van, öt sorban pedig van egy-egy hibás is. Mivel C1 minimális távolsága 5, így mindegyiket ki tudja javítani.

Előfordulhat mégis, hogy a dekódoló észreveszi a hibát, de nem tudja kijavítani. Ez a helyzet pl. akkor, amikor túl sok legalább 2-hibás oszlop van. Ekkor a C2 dekóder végül is a "törlendő" jelet mellékeli jónéhány byte-hoz.
A dekóderből kimenő byte-ok még mindig nem a lejátszás sorrendjében következnek egymás után, hanem összefonódva. A visszarendezéskor az "épségben" lévő társai közé érkező "törlendő" byte helyettesíthető szomszédai átlagával. Ilyen interpolációval, ami szukcesszíven is alkalmazható elérhető, hogy ahelyett, hogy "mute"-ra kapcsolna a zenegép, egy-egy pillanatban amolyan "kitöltő" hangot ad. Ez, ha tényleg csak pillanatokról van szó valószínűleg észre sem vehető.

A csomóhiba maximális hossza, amit a dekodolással még ki tud javítani a rendszer 4000 adatbit. Tehát ha ennyi egymást követő bit elromlik, akkor azt nem fogjuk észrevenni. Ez a disc-en 2,5 mm-nyi torzulást jelent a pálya irányában.
Az interpoláció segítségével pótolható egybefüggő bitsorozat maximális hossza 12 000.

**A barázda-jelek**

Láttuk, hogy a mintavételből keletkező byte-ok 24-es csoportját az egyik kód 28, majd a másik 32 byte hosszúságúra növeli. (A "keresztbe fonás" miatt ez ennél valamivel bonyolultabb, csak a számarányok tekintetében pontos a megállapítás.) A 32 byte-hoz hozzátesznek egy 33.-at, egy kontrol byte-ot, amely lehetővé teszi, hogy tudjuk, hogy hol tartunk.

Az így kapott adatsor nem alkalmas arra, hogy a "síkságok" és "árkok" módszerével az anyagba vive, azt a lézer olvasófej biztonságosan ki tudja olvasni. Az árok mélysége és a síkság magassága úgy van beállítva, hogy az árokból sokkal kisebb intenzitású fény verődik vissza a leolvasófejbe, mint a síkságról. Az egymáshoz túl közeli 1-esek, tehát közeli falak, olyan interferenciát okoznának, amely megzavarná a leolvasást. A túl távoli falak esetén nagy a bizonytalanság, hogy pontosan mennyi ideje tart a lapos rész, hány 0-t jelent ez. Ilyen megfontolások alapján a lemezen olyan jelsorozatokat érdemes tárolni, amelyben két 1-es között legalább két, de legfeljebb tíz 0 van. Az ilyen elrendezésű jelsorozatok a ***barázda-jelek*** (channel-bits).
A byte-ok 256 lehetséges értékét hány barázda-biten lehet tárolni? Ennek meghatározásához a mérnököknek az alábbi feladatot kellett megoldaniuk:

*Ha $F_n$ az n hosszúságú barázda-jelek száma, akkor melyik az a legkisebb n érték, amelyre $F_n \geq 256$?*

A helyes eredmény 14. Tehát a byte-okat 14 bitre bővítik. Ez az eljárás az EFM átalakítás (Eight-to-Fourteen Modulation).
Problémát okoz, hogy két szomszédos barázda-jel együtt már nem feltétlenül teljesíti a barázda-jelekre kirótt követelményeket. Segítséget jelent viszont, hogy $F_{14}$ értéke 267, tehát 11 darab 14 hosszúságú barázda-jel kidobható. 10-et azért hagytak ki, mert "nem jöttek volna jól ki a szomszédaikkal", 1-et pedig véletlenszerűen választottak. Ezután az EFM átalakítást úgy tervezték meg, hogy a szükséges logikai kapuk száma minimális legyen.

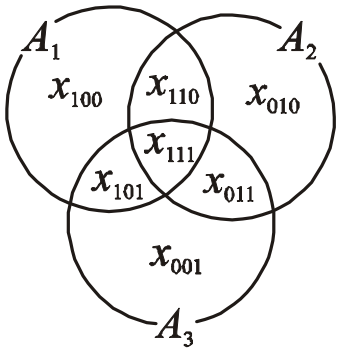
Az egymás mellé kerülő barázda-jelek problémáját nem teljesen oldotta meg a 10 kellemetlen sorozat kidobása. További 3-3 bitet kellett berakni a byte-oknak megfelelő 14 hosszúságú bitsorozatok közé.
A 3 bit egy kicsit túlbiztosított. Beállításukkor arra is törekednek, hogy a pálya kezdetétől a síkságok és az árkok hosszának különbsége minél kisebb legyen. Az ezt a különbséget leíró hullámszerű függvényt ugyanis a berendezés "érzi": annak megfelelő zaj indukálódik a berendezésben. Ebből ki kell küszöbölni az emberi fül számára hallható nagyobb amplitudójú komponenseket, tehát minél kisebb kitéréseket kell elérni.

Végül a 33 byte-ból adódó 33×17 bit után 27 szinkronizáló bit jön. Ez a 27 bitsorozat olyan, hogy nem keverhető össze a kódolt zenével, csak arra szolgál, hogy az egyik 33-as egység végét, a következő kezdetét jelölje.
Mindebből kiszámolható, hogy egyetlen másodpercnyi zenét 4 321 800 biten tárol a CD.

Megbeszéltük a bináris Hamming kód egy új interpretációját és megoldottuk az 5.11 feladatot (kém üzen a tv-n). Ezek után feltártuk az **"Ideális 1001-es"** és a **hétszögminták** mélyén rejlő algebrai struktúrákat és megismerkedtünk egy polinom-kóddal. A szakkör kódelméleti részének zárását a Mariner szonda kódjának leírása, és néhány ajánlott olvasmány jelenti.

## A 21. szakkör részletezett anyaga

**Megjegyzés** (*bináris Hamming kód*)
Új interpretációt adunk a bináris Hamming kódhoz. Lássuk példaként a 16 db hétbetűs kódszóból álló kódot! Ez szolgáltatta az 5.9 "hazudós barkochba" feladat megoldását is és ott a III. konstrukcióban a




$$1\cdot x_1 + 1\cdot x_2 + 1\cdot x_3 + 0\cdot x_4 + 1\cdot x_5 + 0\cdot x_6 + 0\cdot x_7 = 0,$$
$$1\cdot x_1 + 1\cdot x_2 + 0\cdot x_3 + 1\cdot x_4 + 0\cdot x_5 + 1\cdot x_6 + 0\cdot x_7 = 0,$$
$$1\cdot x_1 + 0\cdot x_2 + 1\cdot x_3 + 1\cdot x_4 + 0\cdot x_5 + 0\cdot x_6 + 1\cdot x_7 = 0$$

egyenletrendszer állította elő. Az ismeretlenek indexei itt 1, 2, ..., 7; ezek helyett "beszédesebb", ha az indexszel a változó együtthatóira utalunk:

$$1\cdot x_{111} + 1\cdot x_{110} + 1\cdot x_{101} + 0\cdot x_{011} + 1\cdot x_{110} + 0\cdot x_{010} + 0\cdot x_{001} = 0,$$
$$1\cdot x_{111} + 1\cdot x_{110} + 0\cdot x_{101} + 1\cdot x_{011} + 0\cdot x_{110} + 1\cdot x_{010} + 0\cdot x_{001} = 0,$$
$$1\cdot x_{111} + 0\cdot x_{110} + 1\cdot x_{101} + 1\cdot x_{011} + 0\cdot x_{110} + 0\cdot x_{010} + 1\cdot x_{001} = 0.$$

Tehát a változókat $x_{ijk}$ jelöli, ahol az $i, j, k$ bitek nem mindegyike 0 és ahol $x_{ijk}$ együtthatója az egyes egyenletekben rendre $i, j, k$. Az első egyenletben azok a változók szerepelnek 1-es együtthatóval, amelyek indexének első jegye 1-es, a második egyenletben azok, amelyek második jegye 1-es, végül a harmadikban azoknak a változóknak 1 az együtthatója, amelyek indexében az utolsó bit 1-es. Az ábrán a változókat Venn-diagrammba rendeztük, a Hamming kódba a változók olyan értékrendszere tartozik, amelynél a három halmaz közül bármelyikben szereplő négy változó értékének összege zérus (mod 2).

Ehhez hasonlóan adhatjuk meg az általános esetben is a bináris Hamming kódot. Annál a kódnál, amelyben a szavak hossza, az egyenletek száma és a kódszavak száma rendre

$$2^r - 1, \quad r, \quad 2^{2^r - 1 - r},$$

a változókat $r$ hosszú bináris sorozatokkal indexeljük (a csupa 0 sorozatot nem engedjük meg indexként) és az $i$-edik egyenlet azt fejezi ki, hogy azon változók értékeinek összege, amelyek indexében az $i$-edik jegy 1-es, zérussal egyenlő (mod 2).

**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?

**I. Megoldás**
Tekintsünk egy lehetséges információt! Legyen pld $u_1$ az az információ, üzenet, hogy "támadás várható északról". Az üzenet vevőjénél és az azt közvetítő kémnél kell lennie egy a dekódolást illetve a kódolást segítő iratnak, amelyben föl van sorolva, hogy az $u_1$ üzenetet mely sakktáblaszínezések jelentik. Bonyolult lenne mindig lerajzolni a sakktáblát. Ehelyett rakjuk inkább sorba a 64 mezőt, és minden sakktáblaszínezésnek feleltessünk meg egy-egy 64 hosszúságú 0-1 sorozatot, pld 0 jelentheti a fehér színt, 1 a feketét. Ha a sorozat 11. eleme 1-es, akkor a megfeleltetett színezésben a sakktábla 11. mezője fekete. Az $u_1$ üzenetet ezek után a 64 hosszúságú 0-1 sorozatok egy $U_1$ részhalmaza továbbítja. Megpróbáljuk meghatározni egy megfelelő $U_1$ részhalmaz tulajdonságait.

Az $u_1$ üzenetet el kell tudnia küldeni a kémnek, bármilyen minta is kerül elé. Ez azt jelenti, hogy bármely 64 hosszúságú 0-1 sorozathoz található $U_1$-ben azzal teljesen megegyező vagy tőle csak egy helyen eltérő sorozat. Másképpen:

1) az $U_1$ elemei köré írt 1 sugarú Hamming gömbök lefedik az összes 64 hosszúságú 0-1 sorozatot.

Tudjuk, hogy bármely 1 sugarú Hamming gömbben éppen 1 + 64 = 65 elem (0-1 sorozat) van, összesen pedig $2^{64}$ darab 0-1 sorozat van. Ennek alapján, ha az $U_1$-ben szereplő 0-1 sorozatok száma $n_1$, akkor $n_1 \cdot (64 + 1) \geq 2^{64}$. Ebből (mivel 65 nem osztja $2^{64}$-t) $n_1 > 2^{64}/65$. Ez bármely információra igaz, és az összes információhoz tartozó összes színezések legfeljebb $2^{64}$-en vannak, így ha összesen $k$-féle információt küldhetünk, akkor

$$k\cdot 2^{64}/65 < n_1 + n_2 + ... + n_k \le 2^{64},$$

azaz $k < 65$.

Megmutatjuk, hogy 64 információ átküldése lehetséges. 64 helyet próbálkozhatunk 1, 2, 4, 8 mezővel, ezekben az esetekben a kém által elküldhető információk száma 1, 2, 4, 8, és viszonylag könnyű is megtalálni a színezések, illetve a 0-1 sorozatok megfelelő $U_i$ részhalmazait. Az általánosítás azonban nehezen észrevehető. Ennek oka az, hogy túl sok szabadságunk van, valójában a fenti esetekben mindig elég eggyel kevesebb mező is ugyanannyi üzenet átküldésére. Ennek esélyét beláthatjuk, ha az előző bekezdésben leírtakat 64 mező helyett 63-mal is végiggondoljuk. Valóban, ilyenkor a Hamming gömb elemeinek száma 64, $2^{64}/64$ most egész, így lehetséges, hogy $n_i = 2^{64}/64$ legyen, tehát az adódó $k\cdot 2^{63}/64 \le n_1 + n_2 + ... + n_k \le 2^{63}$ egyenlőtlenség nem zárja ki, hogy az üzenetek $k$ száma 64 legyen.

63 mezőn csak akkor küldhetünk át 64 üzenetet, ha bármelyik üzenethez tartozó $U_i$ halmaz egyes elemei köré írt Hamming gömbök egymáshoz diszjunktak (nincs közös elemük) és lefedik az összes 63 hosszú 0-1 sorozatot. Ez éppen azt jelenti, hogy mindegyik $U_i$ halmaz egy-egy tökéletes 1-hiba javító kód.

Legyen az $u_1$ információhoz tartozó $U_1$ halmaz a 6 egyenlettel meghatározott $2^6$ - 1 hosszú szavakból álló Hamming kód. Legyen továbbá $\underline{x}$ tetszőleges 63 hosszú 0-1 sorozat. A sorozatokat a következőkben vektorokként kezeljük, koordinátánként mod 2 adjuk őket össze. Toljuk el $U_1$-et $\underline{x}$-szel. Ezen a következőt értjük: tekintsük $U_1$ összes elemét (vektorát) és mindegyikhez külön-külön adjuk hozzá az $\underline{x}$ vektort. Az így kapott vektorok halmazát $U_1 + \underline{x}$ -szel jelöljük. Képezzük ezt a halmazt minden lehetséges $\underline{x}$-re. Így $2^{63}$ halmazt kapunk. Állítjuk, hogy

1') bármely $\underline{x}$-re, az $U_1 + \underline{x}$ elemei köré írt 1 sugarú Hamming gömbök lefedik az összes 63 hosszúságú 0-1 sorozatot.

2) bármelyik kettő halmaz vagy megegyezik egymással vagy diszjunkt.

Ha állításaink igazak, akkor készen vagyunk, az egymástól diszjunkt eltoltak lesznek az üzeneteknek megfelelő $U_i$ halmazok.

Belátjuk a fenti 1'), 2) állításokat. Az $U_1$ halmaz elemei köré írt 1 sugarú Hamming gömbök uniója az összes 63 hosszúságú 0-1 sorozat (vektor) halmaza, hiszen $U_1$ tökéletes kód. Az $U_1 + \underline{x}$ elemei köré írt 1 sugarú Hamming gömböket úgy is képezhetjük, hogy az $U_1$ elemei körüli gömböket toljuk el $\underline{x}$-szel. Ezért az $U_1 + \underline{x}$ elemei köré írt 1 sugarú Hamming gömbök uniója $U_1$ elemei körüli gömbök uniójának, azaz az összes sorozatnak (vektornak) az eltoltja. Ha az összes sorozatot (vektort) eltoljuk ugyanazzal a sorozattal (vektorral), akkor az összes sorozatot (vektort) megkapjuk, így az 1') állítás igaz.
Ha az $U_1 + \underline{x}$, $U_1 + \underline{y}$ halmazok nem diszjunktak, akkor van közös elemük, tehát valamely $\underline{a}$, $\underline{b}$ $U_1$-beli vektorokkal $\underline{a} + \underline{x} = \underline{b} + \underline{y}$. Ebben az esetben az $U_1 + \underline{x}$ halmaz tetszőleges $\underline{a}' + \underline{x}$ elemére ($\underline{a}'$ az $U_1$-ben van) és az $U_1 + \underline{y}$ halmaz bármely $\underline{b}' + \underline{y}$ elemére ($\underline{b}'$ az $U_1$-ben van)

$$\underline{a}' + \underline{x} = (\underline{a}' - \underline{a}) + (\underline{a} + \underline{x}) = (\underline{a}' - \underline{a}) + (\underline{b} + \underline{y}) = (\underline{a}' - \underline{a} + \underline{b}) + \underline{y},$$
$$\underline{b}' + \underline{y} = (\underline{b}' - \underline{b}) + (\underline{b} + \underline{y}) = (\underline{b}' - \underline{b}) + (\underline{a} + \underline{x}) = (\underline{b}' - \underline{b} + \underline{a}) + \underline{x}.$$

Mivel $U_1$ lineáris kód, így $(\underline{a}' - \underline{a} + \underline{b})$ és $(\underline{b}' - \underline{b} + \underline{a})$ az $U_1$ elemei, tehát $\underline{a}' + \underline{x}$ az $U_1 + \underline{y}$, $\underline{b}' + \underline{y}$ pedig az $U_1 + \underline{x}$ halmazban van, azaz a két halmaz valóban megegyezik egymással. A 2) állítást is bebizonyítottuk.

**II. megoldás** (csak konstrukció, *Pósa Lajos*)
Konstrukciót adunk 64 információra. Az egyik mezőt kidobhatjuk. A maradék mezőkre írjuk rá 1-tól 63-ig a számokat kettes számrendszerben 6 biten (000001-111111)! Ha adott a tábla színezése, akkor adjuk össze a fekete mezők számait bitenként mod 2. Így egy $\underline{X}$ számot kapunk. A fogadó fél is így fogja majd dekódolni az üzenetet. Legyen az információ, amit át akarunk adni $\underline{Y}$ (szintén 6 biten tárolva). Képezzük az $\underline{X}$ - $\underline{Y}$ bitenkénti differenciát! Ha ez 000000, akkor nem kell változtatnunk, egyébként változtassuk meg a neki megfelelő mező színét.

**Megjegyzések**
**I.** Ha átgondoljuk a bináris Hamming kódnak a szakkör elején ismertetett interpretációját, akkor észrevehetjük, hogy a II. megoldásban adott konstrukció az I. megoldás konstrukciójának frappáns átfogalmazása, amellett, hogy konkrét kódolási-dekódolási algoritmust is ad.

**II.** A II. megoldásból az is kiderül, hogy 64 mezővel akkor is megoldható 64 információ továbbítása, ha kapott mintán a kémnek mindenképpen kell változtatnia. A 64. mező száma lehet 000000, és ha a 63 mezőre vonatkozó módszer esetén nem kellene változtatni, akkor a 000000 mező színét módosítja a kém.

**"Ideális 1001-es"** (emlékeztető: lásd az "ideális 101-es" feladatot és megoldását a 19. szakkör anyagában!)

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 $I_{1001}$ részhalmazát "ideális 1001-es"-nek nevezzük,

1. ha $h \in I_{1001} \Rightarrow h0 \in I_{1001}$; ($h0$ a $h$ dupláját, tehát azt a számot jelöli, amelyet úgy kapunk, hogy $h$ mögé írunk egy 0-t)
2. ha $h \in I_{1001}$ és $j \in I_{1001} \Rightarrow h + j \in I_{1001}$;
3. ha $1001 \in I_{1001}$ (itt 1001 az egy-nulla-nulla-egy számot, azaz a 9-et és nem az ezeregyet jelenti).

Hány "ideális 1001-es" részhalmaza van a természetes számok halmazának?

**Megoldás**
Az "ideális 101-es" feladat "Segítség" részében leírt megfeleltetésből indulunk ki, természetes számok helyett $F_2$ feletti (azaz az együtthatók és a műveletek mod 2 értendők) polinomokról beszélünk. Az ottani megoldásból kiderül, hogy 1. és 2. azzal ekvivalens, hogy az "ideális 1001-es" halmaz valamely $p$ polinomból és $p$ összes többszöröséből (azaz polinom-szorosából) áll. A 3. tulajdonság pedig pontosan akkor teljesül, ha $p$ az $x^3 + 1$ polinom osztója, azaz $x^3 + 1$ előáll $p$-nek egy ($F_2$ feletti) polinommal vett szorzataként. Tehát az "ideális 1001-es halmazok" leszámlálása ekvivalens az $x^3 + 1$ polinom osztóinak leszámlálásával. $F_2$ felett, azaz mod 2 számolva is teljesül az $x^3 + 1 = (x + 1) \cdot (x^2 + x + 1)$ azonosság, és itt már egyik tényezőt sem lehet tovább bontani kisebb fokú polinomok szorzatára, a két tényező már felbonthatatlan, idegen szóval *irreducibilis*. Az $F_2$ test feletti polinomok körében is igaz a számelmélet alaptétele (ezt a szakkör őszi félévében igazoltuk, de a szakköri anyagban egyelőre nincs részletesen leírva). Ennek következményeként $x^3 + 1$ összes osztója, tehát az összes lehetséges $p$ polinom $x^3 + 1$ irreducibilis osztóiból állítható össze. A két irreducibilis osztóból összesen négy osztó állítható össze: $p_1 = 1$, $p_2 = x + 1$, $p_3 = x^2 + x + 1$ és $p_4 = (x + 1) \cdot (x^2 + x + 1) = x^3 + 1$. Tehát négy "ideális 1001-es halmaz" van. A $p_1$-nek megfelelő halmaz az összes természetes számból áll, a $p_2$ által meghatározott pedig azokból a természetes számokból, amelyeknek kettes számrendszerbeli alakjában páros darab 1-es van. A $p_3$ és $p_4$ által generált "ideális 1001-es halmazokat" bonyolultabb leírni, szükség van hozzá, hogy a természetes számok kettes számrendszerbeli alakjának jegyeit három csoportba osszuk. Alább aláhúzással, dőlt szedéssel, illetve normál szedéssel jelöltük a csoportokat egy példaként vett szám kettes számrendszerbeli alakján:

$$\underline{1}\,\textit{0}\;0\;\underline{1}\,\textit{1}\;1\;\underline{0}\,\textit{1}\;1\;\underline{0}\,\textit{0}\;0\;\underline{1},$$

tehát minden harmadik jegy tartozik ugyanabba a csoportba. A $p_3$ által generált "ideális 1001-es halmaz" azokból a kettes számrendszerbeli alakokból áll, amelyeknél ha felírjuk a három csoportba tartozó 1-esek számát, akkor három ugyanolyan paritású számot kapunk. A $p_4$ által generált halmaz pedig azokból a kettes számrendszerbeli alakokból áll, amelyek mindhárom csoportban páros darab 1-est tartalmaznak.

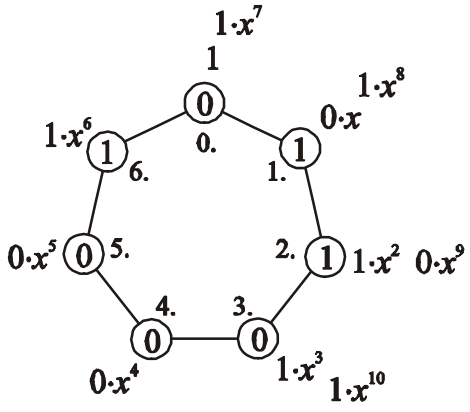
**Hétszögminták** Ebben a feladatban egy szabályos hétszög csúcsaira írunk 0-t vagy 1-et. Összesen $2^7$=128 ilyen kitöltés van. A kitöltések egy $I_7$ részhalmaza "7-szögre ideális",

1. ha $h \in I_7 \Rightarrow h$ bármely ($n \cdot 360°/7$-kal való) elforgatottja is $I_7$-ben van.
2. ha bármely két $I_7$-beli kitöltés csúcsonként és mod 2 számított összege is $I_7$-ben van.

A kitöltéseknek hány "7-szögre ideális" részhalmaza van?

**Megoldás**
A feladat megoldható az esetek alapos elemzésével, de a tapasztalat azt mutatja, hogy a diákok gyakran elnézik a két legizgalmasabb "7-szögre ideális" részhalmazt. Alább egy, az absztrakt algebrába hajló megoldást ismertetünk.

Visszavezetjük a feladatot az "ideális 101-es", "ideális 1001-es" problémákkal analóg kérdésre. Tekintsük az $F_2$ test feletti polinomok $F_2[x]$ halmazát. Minden polinomhoz hozzárendeljük a hétszög egy "kitöltését" a következő módon. A hétszög csúcsait számozzuk meg az egyik forgásirányban a 0., 1., 2., ..., 6. sorszámokkal, és a $p$ polinom tagjait írjuk fel sorban, körkörösen a hétszög csúcsaira. A polinom konstans tagja kerüljön a 0., az elsőfokú tag az 1. csúcshoz és így tovább, a hetedfokú tag értelem szerint megint a 0. csúcshoz kerül. A hétszögnek a $p$ polinomhoz rendelt kitöltésének értéke egy adott csúcson legyen egyenlő a $p$ polinomnak az ahhoz a csúcshoz írt tagjai együtthatóinak összegével. A $p$ polinomhoz így rendelt kitöltést $\varphi(p)$ fogja jelölni. Tehát $\varphi(p)$-ben az $i$. csúcshoz írt érték a $p$ polinom azon tagjai együtthatóinak összegével egyenlő, amely tagok kitevője 7-tel osztva $i$ maradékot ad. Például a $p(x) = 1 + 0\cdot x + 1\cdot x^2 + 1\cdot x^3 + 0\cdot x^4 + 0\cdot x^5 + 1\cdot x^6 + 1\cdot x^7 + 1\cdot x^8 + 0\cdot x^9 + 1\cdot x^{10}$ polinomhoz rendelt kitöltésnél a 0. csúcshoz írt szám a 0, mert az $1 + 1\cdot x^7$ polinom együtthatóinak összege 0. Ehhez hasonlóan az 1. csúcshoz írt szám 1, mert $0\cdot x+1\cdot x^8$ együtthatóinak összege 1. A 2., 3., 4., 5., 6. csúcsokhoz írt számok $\varphi(p)$-ben rendre 1, 0, 0, 0, 1.




Legyen most adva egy $I_7$ halmaz, ehhez hozzá fogjuk rendelni az $F_2[x]$-beli polinomok egy részhalmazát, amelyet - később világossá váló okokból - $I_{10000001}$-gyel jelölünk. $I_{10000001}$ álljon az összes olyan polinomból, amelyhez a fenti hozzárendelés $I_7$-beli kitöltést feleltet meg. Röviden: $I_{10000001} = \varphi^{-1}(I_7)$. "7-szögre ideális" $I_7$ halmaz lehet az üres halmaz is, de állítjuk, hogy az összes ettől különböző "7-szögre ideális" $I_7$ halmazhoz rendelt $I_{10000001}$ polinom-halmaz rendelkezik az alábbi három tulajdonsággal:

1'. ha $h \in I_{10000001} \Rightarrow h\cdot x \in I_{10000001}$;
2'. ha $h \in I_{10000001}$ és $j \in I_{10000001} \Rightarrow h + j \in I_{10000001}$;
3'. $x^7 + 1 \in I_{10000001}$.

Valóban, 1'. az 1., 2'. a 2. tulajdonság közvetlen következménye, 3'. pedig abból adódik, hogy nem üres "7-szögre ideális" halmazban a 2. tulajdonság miatt (azt két egymással megegyező polinomra alkalmazva) benne van az azonosan 0 kitöltés, és az $x^7 + 1$ polinomhoz rendelt $\varphi(x^7 + 1)$ kitöltés is azonosan 0. Nevezzük az 1'., 2'., 3'. tulajdonsággal rendelkező polinom-halmazokat "ideális 10000001-es"-nek. Állítjuk, hogy

A) "ideális 10000001-es" halmaz képe a $\varphi$ leképezésnél "7-szögre ideális";
B) egymástól különböző "ideális 10000001-es" halmazok képe különbözik egymástól.

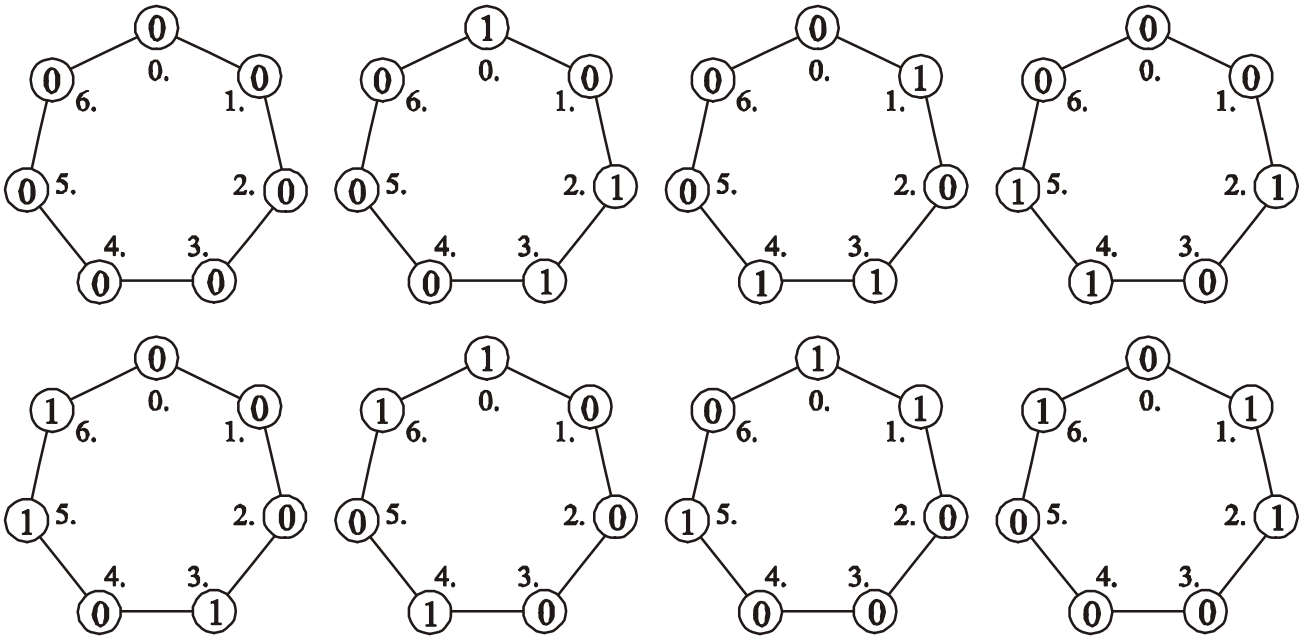
Valóban, az 1'), 2') tulajdonságból következnek az 1), 2) tulajdonságok, így az A) állítás igaz. B) igazolásához 3'.-re is szükség van. Ha valamely $p$, $q$ polinomokra $\varphi(p) = \varphi(q)$, akkor $p - q$ előáll a $x^7 + 1$, $x^8 + x$, $x^9 + x^2$, ... polinomok összegeként, azaz $p - q = r(x)\cdot(x^7 + 1)$, ahol $r(x)$ is polinom. Az 1'., 2'., 3'. tulajdonságokból következik, hogy $r(x)\cdot(x^7 + 1)$ minden "ideális 10000001-es" halmazban benne van, így 2'. szerint $q$ pontosan akkor van benne egy "ideális 10000001-es" halmazban, ha abban $p = q + r(x)\cdot(x^7 + 1)$ is benne van. Ezzel megmutattuk, hogy ha két "ideális 10000001-es" halmaz képe megegyezik egymással, akkor a két "ideális 10000001-es" halmaz is megegyezik egymással.

Mindezekből következik, hogy az üres halmaztól különböző "hétszögre ideális" kitöltés-halmazok kölcsönösen egyértelmű megfeleltetésben állnak az "ideális 10000001-es" halmazokkal. Ez utóbbiak az "ideális 101-es" feladat megoldásának mintájára az $x^7 + 1$ polinom irreducibilis felbontásának segítségével határozhatók meg. A felbontás:

$$x^7 + 1 = (x + 1)\cdot(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x + 1)\cdot(x^3 + x^2 + 1)\cdot(x^3 + x + 1).$$

Ebből következik, hogy 9 db "7-szögre ideális" kitöltéshalmaz van, az üres halmazon kívül az alábbi nyolc:

| | **generáló polinom** | **leírás** | **elemszám** |
|---|---|---|---|
| 1. | $p_1 = 1$ | az összes kitöltés | $2^7$ |
| 2. | $p_2 = x + 1$ | az 1-esek száma páros | $2^6$ |
| 3. | $p_3 = x^3 + x^2 + 1$ | az ábrán látható 8, és ugyanezek a 0 és 1 felcserélésével. | $2^4$ |
| 4. | $p_4 = x^3 + x + 1$ | 3. tükörképe | $2^4$ |
| 5. | $p_5 = (x + 1)\cdot(x^3 + x^2 + 1)$ | 2. és 3. közös része | $2^3$ |
| 6. | $p_6 = (x + 1)\cdot(x^3 + x + 1)$ | 2. és 4. közös része | $2^3$ |
| 7. | $p_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ | azonosan 0, és azonosan 1. | $2^1$ |




| | | | |
|---|---|---|---|
| 8. | $p_8 = x^7 + 1$ | azonosan 0 | $2^0$ |

**Megjegyzés** (*polinom-kódok*)
A táblázatban található 3. (és 4.) "hétszögre ideális" halmaz régi ismerős: bináris, lineáris, 1-hiba javító, tökéletes kód. "Hétszögre ideális" halmaz definíciója szerint bináris és lineáris. Ez a halmaz azért 1-hiba javító kód, mert lineáris kód, és az azonosan 0 kitöltésen kívül mindegyik kitöltésben legalább három darab 1-es van. Tökéletessége egyszerű leszámlálásból adódik.

Ezt a kódot tehát a következőképpen is értelmezhetjük. Tekintsük a 0, 1 jelekből képezhető hétbetűs szavak halmazát. Minden szónak feleltessünk meg egy $F_2$ feletti legfeljebb hatod-fokú polinomot. Egy szó pontosan akkor kódszó, ha a neki megfeleltetett polinom osztható a $p_3 = x^3 + x^2 + 1$ polinommal. $p_3$-at legfeljebb harmad-fokú polinommal szorozva kapunk legfeljebb hatod-fokú polinomot. Összesen $2^4$ darab legfeljebb harmad-fokú polinom van $F_2$ felett, így $p_3$-nak összesen $2^4$ legfeljebb hatod-fokú többszöröse van. Ezek a kódszavak.

Az így értelmezett *polinom-kód* előnye, hogy nem kell megjegyeznünk a kódszavakat, csak a $p_3$ polinomot kell fejben tartanunk. Minden legfeljebb harmadfokú polinomhoz (azaz lényegében minden négy hosszú 0-1 sorozathoz) rendelünk egy információt, és a kívánt információt úgy küldjük el, hogy a neki megfelelő polinomot megszorozzuk $p_3$-mal, és az így kapott polinom együtthatóit továbbítjuk. A fogadó fél egyszerű polinom-osztással fejtheti vissza az üzenetet: a kapott 0-1 sorozatot legfeljebb hatod-fokú polinomként értelmezi és $p_3$-mal osztja. Ha nem történt hiba, akkor nem lesz maradék és a hányados együtthatói alkotják az információt. Ha 1 hiba történt akkor az elküldeni kívánt polinom helyett az attól az 1, $x$, $x^2$, $x^3$, $x^4$, $x^5$, $x^6$ polinomok valamelyikével eltérő polinomot dekódoltuk. Ebben az esetben lesz maradék, méghozzá éppen annyi amennyi az 1, $x$, $x^2$, $x^3$, $x^4$, $x^5$, $x^6$ polinomok közül megfelelőnek a $p_3$-mal való osztási maradéka. Állítjuk, hogy

A) az 1, $x$, $x^2$, $x^3$, $x^4$, $x^5$, $x^6$ polinomok nem oszthatók $p_3$-mal;
B) az 1, $x$, $x^2$, $x^3$, $x^4$, $x^5$, $x^6$ polinomok különböző maradékot adnak $p_3$-mal osztva.

A) azt jelenti, hogy észrevehetjük, hogy 1 hiba történt, B) pedig azt, hogy ki is tudjuk javítani. A) igaz, hiszen $p_3$ osztja az $x^7 + 1$ polinomot, így az attól 1-gyel eltérő $x^7$ polinomhoz, és annak minden osztójához (tehát az 1, $x$, ..., $x^7$ polinomokhoz ) relatív prím. B) azért igaz, mert ha $x^m$ és $x^n$ $(m < n)$ azonos maradékot ad $p_3$-mal osztva, akkor $x^m - x^n = x^m + x^n = x^m \cdot (1 + x^{n-m})$ osztható $p_3$-mal, azaz $q = (x^{n-m} + 1)$ osztható $p_3$-mal ($n$-$m$<7). Ebben az esetben a

$$q^* = x^{7-(n-m)} \cdot (x^{n-m} + 1) + (x^7 + 1) = x^{7-(n-m)} + 1$$

polinom is osztható $p_3$-mal, ami azért nem lehetséges, mert $p_3$ harmadfokú, és $q$ és $q^*$ közül az egyik legfeljebb harmadfokú, de különbözik $p_3$-tól.

Ha tehát előre felírjuk az 1, $x$, $x^2$, $x^3$, $x^4$, $x^5$, $x^6$ polinomok $p_3$-mal való osztási maradékait, akkor az üzenet dekódolásakor, a polinom-osztás során nyert maradék alapján azonnal rájöhetünk, hogy hol volt a hiba.

Házi feladat:

**4.10** Ha adott egy négyzet alakú $H_i$ számtáblázat, akkor elkészíthetjük a kétszer akkora oldalhosszúságú

$$H_{2i} = \begin{pmatrix} H_i & H_i \\ H_i & -H_i \end{pmatrix}$$

számtáblázatot. Induljunk ki az 1×1-es $H_1$ = (1) "számtáblázat"-ból, és képezzük a

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

majd a $H_4$, $H_8$, $H_{16}$, $H_{32}$ számtáblázatokat. $H_{32}$-nek már 32 sora van, mindegyikben egy 32 hosszú számsorozat, csupa 1-gyel és (-1)-gyel. Tekintsük ezt a 32 sorozatot és (-1)-szereseiket. Álljon kódunk ebből a 64 sorozatból, csak a (-1)-eket cseréljük ki 0-kra. Határozzuk meg az így kapott bináris kód minimális távolságát![5]

Ajánlott olvasmányok:

Freud Róbert: Lineáris algebra, ELTE Eötvös Kiadó, Budapest, 1998.

A 10. fejezetben sok kódelméleti feladatot olvashatunk, és a Hamming kódokon túl a BCH kódokkal is megismerkedhetünk. A gimnazisták többségének azonban a könyv nagy részét el kell olvasni az utolsó fejeezt megértéséhez. Érdemes.

Hraskó András és Szőnyi Tamás: Hibajavító kódok, az Új matematikai mozaik című kötetben, Typotex kiadó, Budapest, 2002.

A cikkben a Hamming kódok dekódolásának leírása és a Golay kódok leírása jelent lényegesen új információt.

[5] Ennek a kódnak az alkalmazásával küldte a fényképeket a Mariner 10 szonda a Földre. A 64 sorozat 64 színnek felelt meg, egy sorozat egy képpont (pixel) színét határozta meg.