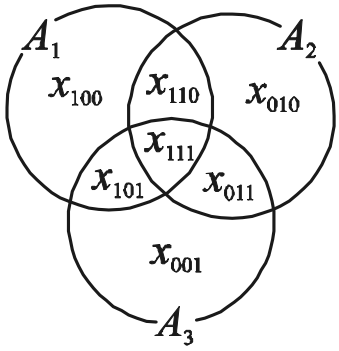
Megbeszéltük a bináris Hamming kód egy új interpretációját és megoldottuk az 5.11 feladatot (kém üzen a tv-n). Ezek után feltártuk az **"Ideális 1001-es"** és a **hétszögminták** mélyén rejlő algebrai struktúrákat és megismerkedtünk egy polinom-kóddal. A szakkör kódelméleti részének zárását a Mariner 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 $\boldsymbol{U}_1$-ben szereplő 0-1 sorozatok száma $\boldsymbol{n}_1$, akkor $\boldsymbol{n}_1 \cdot (64 + 1) \geq 2^{64}$. Ebből (mivel 65 nem osztja 2^{64}-t) $\boldsymbol{n}_1 > 2^{64}/65$. Ez bármely információra igaz, és az összes információhoz tartozó összes színezések legfeljebb 2^{64}-en vannak, így ha összesen $\boldsymbol{k}$-féle információt küldhetünk, akkor

$$\boldsymbol{k} \cdot 2^{64}/65 < \boldsymbol{n}_1 + \boldsymbol{n}_2 + ... + \boldsymbol{n}_{\boldsymbol{k}} \leq 2^{64},$$

azaz $\boldsymbol{k} < 65$.

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 $\boldsymbol{U}_{\boldsymbol{i}}$ 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 $\boldsymbol{n}_{\boldsymbol{i}} = 2^{64}/64$ legyen, tehát az adódó $\boldsymbol{k} \cdot 2^{63}/64 \leq \boldsymbol{n}_1 + \boldsymbol{n}_2 + ... + \boldsymbol{n}_{\boldsymbol{k}} \leq 2^{63}$ egyenlőtlenség nem zárja ki, hogy az üzenetek $\boldsymbol{k}$ száma 64 legyen.

63 mezőn csak akkor küldhetünk át 64 üzenetet, ha bármelyik üzenethez tartozó $\boldsymbol{U}_{\boldsymbol{i}}$ 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 $\boldsymbol{U}_{\boldsymbol{i}}$ halmaz egy-egy tökéletes 1-hiba javító kód.

Legyen az $\boldsymbol{u}_1$ információhoz tartozó $\boldsymbol{U}_1$ halmaz a 6 egyenlettel meghatározott 2^6 - 1 hosszú szavakból álló Hamming kód. Legyen továbbá $\underline{\boldsymbol{x}}$ tetszőleges 63 hosszú 0-1 sorozat. A sorozatokat a következőkben vektorokként kezeljük, koordinátánként mod 2 adjuk őket össze. Toljuk el $\boldsymbol{U}_1$-et $\underline{\boldsymbol{x}}$-szel. Ezen a következőt értjük: tekintsük $\boldsymbol{U}_1$ összes elemét (vektorát) és mindegyikhez külön-külön adjuk hozzá az $\underline{\boldsymbol{x}}$ vektort. Az így kapott vektorok halmazát $\boldsymbol{U}_1 + \underline{\boldsymbol{x}}$ -szel jelöljük. Képezzük ezt a halmazt minden lehetséges $\underline{\boldsymbol{x}}$-re. Így 2^{63} halmazt kapunk. Állítjuk, hogy

1') bármely $\underline{\boldsymbol{x}}$-re, az $\boldsymbol{U}_1 + \underline{\boldsymbol{x}}$ 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 $\boldsymbol{U}_{\boldsymbol{i}}$ halmazok.

Belátjuk a fenti 1'), 2) állításokat. Az $\boldsymbol{U}_1$ halmaz elemei köré írt 1 sugarú Hamming gömbök uniója az összes 63 hosszúságú 0-1 sorozat (vektor) halmaza, hiszen $\boldsymbol{U}_1$ tökéletes kód. Az $\boldsymbol{U}_1 + \underline{\boldsymbol{x}}$ elemei köré írt 1 sugarú Hamming gömböket úgy is képezhetjük, hogy az $\boldsymbol{U}_1$ elemei körüli gömböket toljuk el $\underline{\boldsymbol{x}}$-szel. Ezért az $\boldsymbol{U}_1 + \underline{\boldsymbol{x}}$ elemei köré írt 1 sugarú Hamming gömbök uniója $\boldsymbol{U}_1$ 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 $\boldsymbol{U}_1 + \underline{\boldsymbol{x}}$, $\boldsymbol{U}_1 + \underline{\boldsymbol{y}}$ halmazok nem diszjunktak, akkor van közös elemük, tehát valamely $\underline{\boldsymbol{a}}$, $\underline{\boldsymbol{b}}$ $\boldsymbol{U}_1$-beli vektorokkal $\underline{\boldsymbol{a}} + \underline{\boldsymbol{x}} = \underline{\boldsymbol{b}} + \underline{\boldsymbol{y}}$. Ebben az esetben az $\boldsymbol{U}_1 + \underline{\boldsymbol{x}}$ halmaz tetszőleges $\underline{\boldsymbol{a}}' + \underline{\boldsymbol{x}}$ elemére ($\underline{\boldsymbol{a}}'$ az $\boldsymbol{U}_1$-ben van) és az $\boldsymbol{U}_1 + \underline{\boldsymbol{y}}$ halmaz bármely $\underline{\boldsymbol{b}}' + \underline{\boldsymbol{y}}$ elemére ($\underline{\boldsymbol{b}}'$ az $\boldsymbol{U}_1$-ben van)

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

Mivel $\boldsymbol{U}_1$ lineáris kód, így $(\underline{\boldsymbol{a}}' - \underline{\boldsymbol{a}} + \underline{\boldsymbol{b}})$ és $(\underline{\boldsymbol{b}}' - \underline{\boldsymbol{b}} + \underline{\boldsymbol{a}})$ az $\boldsymbol{U}_1$ elemei, tehát $\underline{\boldsymbol{a}}' + \underline{\boldsymbol{x}}$ az $\boldsymbol{U}_1 + \underline{\boldsymbol{y}}$, $\underline{\boldsymbol{b}}' + \underline{\boldsymbol{y}}$ pedig az $\boldsymbol{U}_1 + \underline{\boldsymbol{x}}$ 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 $\underline{\boldsymbol{X}}$ számot kapunk. A fogadó fél is így fogja majd dekódolni az üzenetet. Legyen az információ, amit át akarunk adni $\underline{\boldsymbol{Y}}$ (szintén 6 biten tárolva). Képezzük az $\underline{\boldsymbol{X}} - \underline{\boldsymbol{Y}}$ 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 $\boldsymbol{I}_{1001}$ részhalmazát "ideális 1001-es"-nek nevezzük,

1. ha $\boldsymbol{h} \in \boldsymbol{I}_{1001} \Rightarrow \boldsymbol{h}0 \in \boldsymbol{I}_{1001}$; ($\boldsymbol{h}0$ a $\boldsymbol{h}$ duplláját, tehát azt a számot jelöli, amelyet úgy kapunk, hogy $\boldsymbol{h}$ mögé írunk egy 0-t)
2. ha $\boldsymbol{h} \in \boldsymbol{I}_{1001}$ és $\boldsymbol{j} \in \boldsymbol{I}_{1001} \Rightarrow \boldsymbol{h} + \boldsymbol{j} \in \boldsymbol{I}_{1001}$;
3. ha $1001 \in \boldsymbol{I}_{1001}$ (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 $\boldsymbol{p}$ polinomból és $\boldsymbol{p}$ összes többszöröséből (azaz polinom-szorosából) áll. A 3. tulajdonság pedig pontosan akkor teljesül, ha $\boldsymbol{p}$ az $\boldsymbol{x}^3 + 1$ polinom osztója, azaz $\boldsymbol{x}^3 + 1$ előáll $\boldsymbol{p}$-nek egy (F_2 feletti) polinommal vett szorzataként. Tehát az "ideális 1001-es halmazok" leszámlálása ekvivalens az $\boldsymbol{x}^3 + 1$ polinom osztóinak leszámlálásával. F_2 felett, azaz mod 2 számolva is teljesül az $\boldsymbol{x}^3 + 1 = (\boldsymbol{x} + 1) \cdot (\boldsymbol{x}^2 + \boldsymbol{x} + 1)$ 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 $\boldsymbol{x}^3 + 1$ összes osztója, tehát az összes lehetséges $\boldsymbol{p}$ polinom $\boldsymbol{x}^3 + 1$ irreducibilis osztóiból állítható össze. A két irreducibilis osztóból összesen négy osztó állítható össze: $\boldsymbol{p}_1 = 1$, $\boldsymbol{p}_2 = \boldsymbol{x} + 1$, $\boldsymbol{p}_3 = \boldsymbol{x}^2 + \boldsymbol{x} + 1$ és $\boldsymbol{p}_4 = (\boldsymbol{x} + 1) \cdot (\boldsymbol{x}^2 + \boldsymbol{x} + 1) = \boldsymbol{x}^3 + 1$. Tehát négy "ideális 1001-es halmaz" van. A $\boldsymbol{p}_1$-nek megfelelő halmaz az összes természetes számból áll, a $\boldsymbol{p}_2$ által meghatározott pedig azokból a természetes számokból, amelyeknek kettes számrendszerbeli alakjában páros darab 1-es van. A $\boldsymbol{p}_3$ és $\boldsymbol{p}_4$ 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:

$$\underline{1}\ \boldsymbol{0}\ 0\ \underline{1}\ \boldsymbol{1}\ 1\ \underline{0}\ \boldsymbol{1}\ 1\ \underline{0}\ \boldsymbol{0}\ 0\ \underline{1},$$

tehát minden harmadik jegy tartozik ugyanabba a csoportba. A $\boldsymbol{p}_3$ 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 $\boldsymbol{p}_4$ 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 $\boldsymbol{I}_7$ részhalmaza "7-szögre ideális",

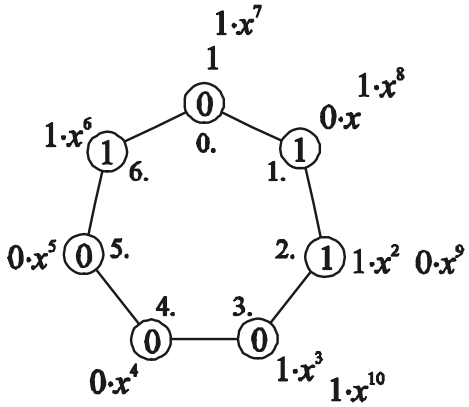
1. ha $\boldsymbol{h} \in \boldsymbol{I}_7 \Rightarrow \boldsymbol{h}$ bármely ($\boldsymbol{n} \cdot 360°/7$-kal való) elforgatottja is $\boldsymbol{I}_7$-ben van.
2. ha bármely két $\boldsymbol{I}_7$-beli kitöltés csúcsonként és mod 2 számított összege is $\boldsymbol{I}_7$-ben van.

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

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 $F_2[\boldsymbol{x}]$ 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 $\boldsymbol{p}$ poli-

nom 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 $\boldsymbol{p}$ polinomhoz rendelt kitöltésének értéke egy adott csúcson legyen egyenlő a $\boldsymbol{p}$ polinomnak az ahhoz a csúcshoz írt tagjai együtthatóinak összegével. A $\boldsymbol{p}$ polinomhoz így rendelt kitöltést $\varphi(\boldsymbol{p})$ fogja jelölni. Tehát $\varphi(\boldsymbol{p})$-ben az $\boldsymbol{i}$. csúcshoz írt érték a $\boldsymbol{p}$ polinom azon tagjai együtthatóinak összegével egyenlő, amely tagok kitevője 7-tel osztva $\boldsymbol{i}$ maradékot ad. Például a $\boldsymbol{p}(\boldsymbol{x}) = 1 + 0\cdot\boldsymbol{x} + 1\cdot\boldsymbol{x}^2 + 1\cdot\boldsymbol{x}^3 + 0\cdot\boldsymbol{x}^4 + 0\cdot\boldsymbol{x}^5 + 1\cdot\boldsymbol{x}^6 + 1\cdot\boldsymbol{x}^7 + 1\cdot\boldsymbol{x}^8 + 0\cdot\boldsymbol{x}^9 + 1\cdot\boldsymbol{x}^{10}$ polinomhoz rendelt kitöltésnél a 0. csúcshoz írt szám a 0, mert az $1 + 1\cdot\boldsymbol{x}^7$ polinom együtthatóinak összege 0. Ehhez hasonlóan az 1. csúcshoz írt szám 1, mert $0\cdot\boldsymbol{x}+1\cdot\boldsymbol{x}^8$ együtthatóinak összege 1. A 2., 3., 4., 5., 6. csúcsokhoz írt számok $\varphi(\boldsymbol{p})$-ben rendre 1, 0, 0, 0, 1.



Legyen most adva egy $\boldsymbol{I}_7$ halmaz, ehhez hozzá fogjuk rendelni az $F_2[\boldsymbol{x}]$-beli polinomok egy részhalmazát, amelyet - később világossá váló okokból - $\boldsymbol{I}_{10000001}$-gyel jelölünk. $\boldsymbol{I}_{10000001}$ álljon az összes olyan polinomból, amelyhez a fenti hozzárendelés $\boldsymbol{I}_7$-beli kitöltést feleltet meg. Röviden: $\boldsymbol{I}_{10000001} = \varphi^{-1}(\boldsymbol{I}_7)$. "7-szögre ideális" $\boldsymbol{I}_7$ halmaz lehet az üres halmaz is, de állítjuk, hogy az összes ettől különböző "7-szögre ideális" $\boldsymbol{I}_7$ halmazhoz rendelt $\boldsymbol{I}_{10000001}$ polinom-halmaz rendelkezik az alábbi három tulajdonsággal:

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

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 $\boldsymbol{x}^7 + 1$ polinomhoz rendelt $\varphi(\boldsymbol{x}^7 + 1)$ 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 φ leképezésnél "7-szögre ideális";
B) egymástól különböző "ideális 10000001-es" halmazok képe különbözik egymástól.

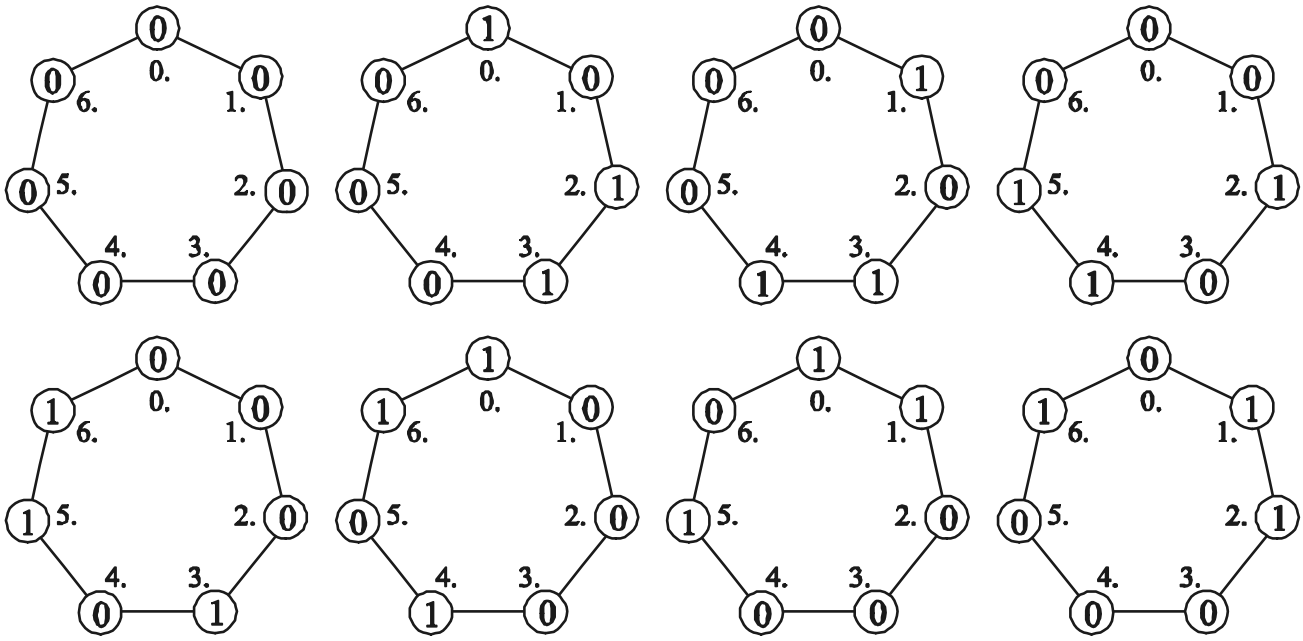
Valóban, az 1'), 2') tulajdonságból következnek az 1), 2) tulajdonságok, így az A) állítás igaz. B) igazolásához 3'.-re is szükség van. Ha valamely $\boldsymbol{p}$, $\boldsymbol{q}$ polinomokra $\varphi(\boldsymbol{p}) = \varphi(\boldsymbol{q})$, akkor $\boldsymbol{p} - \boldsymbol{q}$ előáll a $\boldsymbol{x}^7 + 1$, $\boldsymbol{x}^8 + \boldsymbol{x}$, $\boldsymbol{x}^9 + \boldsymbol{x}^2$, ... polinomok összegeként, azaz $\boldsymbol{p} - \boldsymbol{q} = \boldsymbol{r}(\boldsymbol{x})\cdot(\boldsymbol{x}^7 + 1)$, ahol $\boldsymbol{r}(\boldsymbol{x})$ is polinom. Az 1'., 2'., 3'. tulajdonságokból következik, hogy $\boldsymbol{r}(\boldsymbol{x})\cdot(\boldsymbol{x}^7 + 1)$ minden "ideális 10000001-es" halmazban benne van, így 2'. szerint $\boldsymbol{q}$ pontosan akkor van benne egy "ideális 10000001-es" halmazban, ha abban $\boldsymbol{p} = \boldsymbol{q} + \boldsymbol{r}(\boldsymbol{x})\cdot(\boldsymbol{x}^7 + 1)$ 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 $\boldsymbol{x}^7 + 1$ polinom irreducibilis felbontásának segítségével határozhatók meg. A felbontás:

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

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

	generáló polinom	**leírás**	**elemszám**
1.	$\boldsymbol{p}_1 = 1$	az összes kitöltés	2^7
2.	$\boldsymbol{p}_2 = \boldsymbol{x} + 1$	az 1-esek száma páros	2^6
3.	$\boldsymbol{p}_3 = \boldsymbol{x}^3 + \boldsymbol{x}^2 + 1$	az ábrán látható 8, és ugyanezek a 0 és 1 felcserélésével.	2^4
4.	$\boldsymbol{p}_4 = \boldsymbol{x}^3 + \boldsymbol{x} + 1$	3. tükörképe	2^4
5.	$\boldsymbol{p}_5 = (\boldsymbol{x} + 1)\cdot(\boldsymbol{x}^3 + \boldsymbol{x}^2 + 1)$	2. és 3. közös része	2^3
6.	$\boldsymbol{p}_6 = (\boldsymbol{x} + 1)\cdot(\boldsymbol{x}^3 + \boldsymbol{x} + 1)$	2. és 4. közös része	2^3
7.	$\boldsymbol{p}_7 = \boldsymbol{x}^6 + \boldsymbol{x}^5 + \boldsymbol{x}^4 + \boldsymbol{x}^3 + \boldsymbol{x}^2 + \boldsymbol{x} + 1$	azonosan 0, és azonosan 1.	2^1
8.	$\boldsymbol{p}_8 = \boldsymbol{x}^7 + 1$	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 $\boldsymbol{p}_3 = \boldsymbol{x}^3 + \boldsymbol{x}^2 + 1$ polinommal. $\boldsymbol{p}_3$-at legfeljebb harmad-fokú polinommal szorozva kapunk legfeljebb hatod-fokú polinomot. Összesen 2^4 darab legfeljebb harmad-fokú polinom van F_2 felett, így $\boldsymbol{p}_3$-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 $\boldsymbol{p}_3$ 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 $\boldsymbol{p}_3$-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 $\boldsymbol{p}_3$-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, $\boldsymbol{x}, \boldsymbol{x}^2, \boldsymbol{x}^3, \boldsymbol{x}^4, \boldsymbol{x}^5, \boldsymbol{x}^6$ polinomok valamelyikével eltérő polinomot dekódoltuk. Ebben az esetben lesz maradék, méghozzá éppen annyi amennyi az 1, $\boldsymbol{x}, \boldsymbol{x}^2, \boldsymbol{x}^3, \boldsymbol{x}^4, \boldsymbol{x}^5, \boldsymbol{x}^6$ polinomok közül megfelelőnek a $\boldsymbol{p}_3$-mal való osztási maradéka. Állítjuk, hogy

A) az 1, $\boldsymbol{x}, \boldsymbol{x}^2, \boldsymbol{x}^3, \boldsymbol{x}^4, \boldsymbol{x}^5, \boldsymbol{x}^6$ polinomok nem oszthatók $\boldsymbol{p}_3$-mal;
B) az 1, $\boldsymbol{x}, \boldsymbol{x}^2, \boldsymbol{x}^3, \boldsymbol{x}^4, \boldsymbol{x}^5, \boldsymbol{x}^6$ polinomok különböző maradékot adnak $\boldsymbol{p}_3$-mal osztva.

A) azt jelenti, hogy észrevehetjük, hogy 1 hiba történt, B) pedig azt, hogy ki is tudjuk javítani. A) igaz, hiszen $\boldsymbol{p}_3$ osztja az $\boldsymbol{x}^7 + 1$ polinomot, így az attól 1-gyel eltérő $\boldsymbol{x}^7$ polinomhoz, és annak minden osztójához (tehát az 1, $\boldsymbol{x}$, ..., $\boldsymbol{x}^7$ polinomokhoz) relatív prím. B) azért igaz, mert ha $\boldsymbol{x}^m$ és $\boldsymbol{x}^n$ ($\boldsymbol{m} < \boldsymbol{n}$) azonos maradékot ad $\boldsymbol{p}_3$-mal osztva, akkor $\boldsymbol{x}^m - \boldsymbol{x}^n = \boldsymbol{x}^m + \boldsymbol{x}^n = \boldsymbol{x}^m \cdot (1 + \boldsymbol{x}^{n-m})$ osztható $\boldsymbol{p}_3$-mal, azaz $\boldsymbol{q} = (\boldsymbol{x}^{n-m} + 1)$ osztható $\boldsymbol{p}_3$-mal ($\boldsymbol{n-m}<7$). Ebben az esetben a

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

polinom is osztható $\boldsymbol{p}_3$-mal, ami azért nem lehetséges, mert $\boldsymbol{p}_3$ harmadfokú, és $\boldsymbol{q}$ és $\boldsymbol{q}^*$ közül az egyik legfeljebb harmadfokú, de különbözik $\boldsymbol{p}_3$-tól.

Ha tehát előre felírjuk az 1, $\boldsymbol{x}, \boldsymbol{x}^2, \boldsymbol{x}^3, \boldsymbol{x}^4, \boldsymbol{x}^5, \boldsymbol{x}^6$ polinomok $\boldsymbol{p}_3$-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 $\boldsymbol{H_i}$ számtáblázat, akkor elkészíthetjük a kétszer akkora oldalhosszúságú

$$\boldsymbol{H}_{2\boldsymbol{i}} = \begin{pmatrix} \boldsymbol{H_i} & \boldsymbol{H_i} \\ \boldsymbol{H_i} & -\boldsymbol{H_i} \end{pmatrix}$$

számtáblázatot. Induljunk ki az 1×1-es $\boldsymbol{H}_1$ = (1) "számtáblázat"-ból, és képezzük a

$$\boldsymbol{H}_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

majd a $\boldsymbol{H}_4$, $\boldsymbol{H}_8$, $\boldsymbol{H}_{16}$, $\boldsymbol{H}_{32}$ számtáblázatokat. $\boldsymbol{H}_{32}$-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![1]

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.

[1] 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.