Totókulcsok, kódok és véges geometriák

Szakdolgozat

Készítette: Oli Barbara

Szak: Matematika BSc Tanári Szakirány

Témavezető: Kiss György Ph.D egyetemi docens

Geometriai Tanszék

Eötvös Loránd Tudományegyetem

Természettudományi Kar

2012.

Tartalomjegyzék

1. Bevezetés

Szakdolgozatomban különböző stratégiákat vizsgálok az ismert totó játékkal kapcsolatban, hogyan lehet minél jobb eredményt elérni minél kevesebb szelvény kitöltésével. Nem csak a telitalálat a cél, hanem a biztos 12, 11 stb. találat. Vizsgálom azt az esetet, amikor minden meccsnek három kimenetele van, amikor csak kettő, illetve a vegyes kimenetelű meccseket, ha egy játék során egy-egy mérkőzésnél biztosan tudjuk az eredményt, a többi meccsnél pedig kettő, vagy három kimenetellel számolunk.

Mindezek elméleti háttere a véges geometria és a kódelmélet. Dolgozatom elején ismertetem az alapvető fogalmakat, tételeket, melyeket a totókulcsok vizsgálatához felhasználtam. A véges geometriával foglalkozó fejezethez elsősorban Kiss György és Szőnyi Tamás könyvét vettem alapul [1.], a kódelméleti fejezethez pedig Hraskó András írását [3.].

A totóról szóló fejezethez a megadott cikkeken kívül [2-3-4.], a *http://www.sztaki.hu/~keri/codes/index.htm* honlapon találtam aktuális eredményeket. A totókulcsok megadása nyitott probléma, sok esetben nem ismert az optimális tippek pontos száma, csak alsó és felső becslés adható. Néhány konkrét konstrukció véges geometriai modellen szemléltethető. Ezeket az ábrákat *GeoGebra*-val készítettem el.

Dolgozatom végén a módszertani részben olyan feladatokat dolgoztam fel, melyek az egész egyszerűtől a gondolkodtató feladatokig középiskolás diákoknak is felkelthetik az érdeklődését, és megismertethetik őket a matematika bonyolultabb fejezeteivel is.

.

2. Véges geometriák

2.1 Síkok

2.1.1 Absztrakt projektív sík

Definiáljuk az absztrakt projektív síkot megtartva a klasszikus projektív sík illeszkedési tulajdonságait.

Definíció: A $\Pi = (P, E, I)$ hármast, ahol P és E diszjunkt halmazok, $I \subset P \times E$ pedig egy illeszkedésnek nevezett reláció, *absztrakt projektív sík*nak nevezzük, ha teljesül rá a következő négy axióma:

P1. P bármely két különböző eleméhez egyértelműen létezik E-nek olyan eleme, amely mindkettővel relációban áll.

P2. E bármely két különböző eleméhez egyértelműen létezik P-nek olyan eleme, amely mindkettővel relációban áll.

P3. E minden eleme legalább három különböző P-beli elemmel áll relációban.

P4. P minden eleme legalább három különböző E-beli elemmel áll relációban.

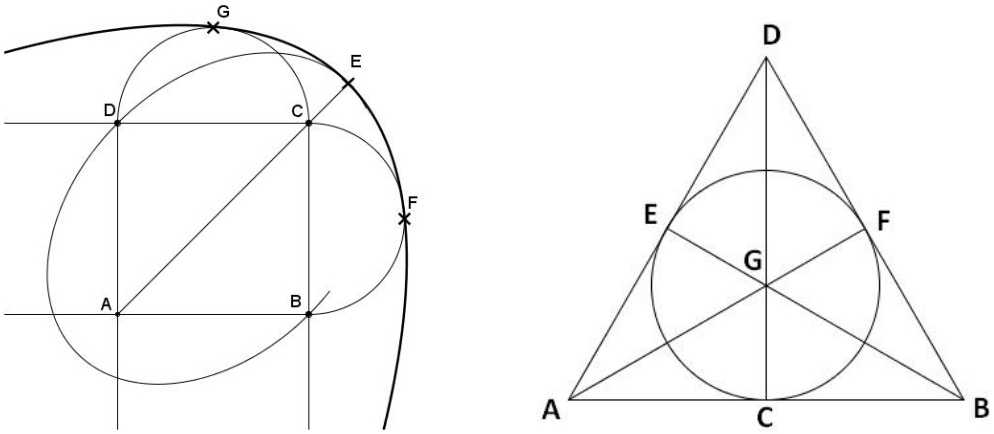
A klasszikus projektív sík pontjai, egyenesei és illeszkedése eleget tesznek a fenti axiómáknak, vagyis a klasszikus projektív sík is absztrakt projektív sík.

Algebrai modell:

Legyen K tetszőleges test, V pedig tetszőleges K feletti háromdimenziós vektortér. Ekkor legyen P a V egydimenziós, E a V kétdimenziós altereinek halmaza, az illeszkedés pedig a halmazelméleti tartalmazás. A lineáris algebrából tanultak alapján belátható, hogy erre a modellre teljesülnek az axiómák. Így megkaptuk a test fölötti vektortérből származó projektív síkok algebrai modelljét. A pontok koordinátái $x = (x_1, x_2, x_3) \neq (0,0,0)$, az egyenesek pedig az $u = [u_1, u_2, u_3] \neq [0,0,0]$ hármasok. Az $x = (x_1, x_2, x_3)$ pont és az $u = [u_1, u_2, u_3]$ egyenes pontosan akkor illeszkedik, ha $xu^T = \sum_{i=1}^{3} x_i u_i = 0$. Ezek a klasszikus projektív síknál megszokott homogén koordináták. Az egydimenziós altereket tehát egyik generáló vektorukkal adjuk meg, a kétdimenziós altereket pedig az ortogonális kiegészítőjük egy generáló vektorával.

Ezeket a síkokat $PG(2,K)$-val jelöljük, vagy $PG(2,q)$-val, ha K a q elemű véges test.

A legkisebb ilyen példa, ha $q = 2$. Ez a sík izomorf a *Fano-sík*kal, hiszen pontjaik és egyeneseik illeszkedéstartón megfeleltethetők egymásnak. A kételemű test fölött izomorfia erejéig csak egy projektív sík létezik.



1. ábra

A következő tétel a síkok pontjainak, illetve egyeneseinek számára vonatkozó fontos állítás.

Tétel: Ha egy absztrakt projektív síknak van olyan egyenese, amire pontosan $n + 1$ pont $(n \geq 2)$ illeszkedik, akkor

i. Minden egyenesnek $n + 1$ pontja van.
ii. Minden ponton $n + 1$ egyenes megy át.
iii. A sík összesen $n^2 + n + 1$ pontot, és ugyanennyi egyenest tartalmaz.

Definíció: Ekkor n-et a sík *rendjé*nek nevezzük.

Bizonyítás:

Először lássuk be, hogy létezik olyan pont, amin $n + 1$ egyenes megy át. Legyen e az az egyenes, amely $n + 1$ pontot tartalmaz. Jelöljük a pontjait $P_1, P_2, \dots, P_{n+1}$-gyel. **P3**

és **P4** miatt létezik olyan Q pont, mely nem eleme az egyenesnek. Ekkor Q-n minimum $n+1$ egyenes megy át, hiszen összeköthetem e pontjaival, és ezek mind különbözőek. Több egyenes nem mehet át rajta, hiszen **P2** miatt minden Q-n átmenő egyenes metszi e-t. Ebből az látszik, hogy ha (Q, e) nem illeszkedő pont és egyenes pár, akkor a Q-n átmenő egyenesek száma megegyezik az e pontjainak számával.

i. Az előző jelölésekkel bizonyítjuk az első állítást. **P4** axióma miatt létezik P_1-gyen átmenő f és g, e-től különböző egyenes. **P3** miatt pedig f-en létezik olyan Q pont, mely P_1-től különbözik, és tudjuk, hogy Q nem eleme e-nek, sem g-nek. Q-n ugyanannyi e-t metsző egyenes van, mint g-t metsző, így a metszéspontokat megszámolva látjuk, hogy ugyanannyi pontja van e-nek és g-nek.

ii. Ha m tetszőleges e-től különböző egyenes, melyre P_1 nem illeszkedik. Kössük össze P_1-et m pontjaival, ekkor e-vel együtt P_1-en $n+1$ egyenes megy át.

iii. Legyen Q egy tetszőleges pont, $n+1$ egyenes megy át rajta, és minden ilyen egyenes Q-n kívül n pontot tartalmaz. Ekkor látjuk, hogy a síkon pontosan $1 + (n+1) \cdot n$ különböző pont van.

Az előző bizonyítást duálizálva látjuk, hogy ha létezik egy e egyenes $n+1$ ponttal, akkor e minden pontján át e-n kívül n egyenes fut. Így megkapjuk az $1 + (n+1) \cdot n$ különböző egyenest.

□

2.1.2 Affin sík

Hagyjuk most el egy projektív sík egy tetszőleges egyenesét az összes rajta lévő ponttal együtt. Jelölje P' a megmaradt pontok halmazát, E' a pedig megmaradt egyenesekét, az illeszkedést $I' = I \cap (P' \times E')$ definiálja.

Definíció: Az $\mathcal{A} = (P', E', I')$ hármast, ahol P' és E' diszjunkt halmazok, $I' \subset P' \times E'$ pedig egy illeszkedésnek nevezett reláció, *affin sík*nak nevezzük, ha kielégíti a következő négy axiómát:

A1. P' bármely két különböző eleméhez egyértelműen létezik E'-nek olyan eleme, amely mindkettővel relációban áll.

A2. Ha $T \in P'$ nem áll relációban $e \in E'$ elemmel, akkor E' -nek pontosan egy olyan eleme van, amely relációban áll T-vel, de nem áll relációban egyetlen olyan P'-beli elemmel sem, amely e-vel relációban áll.

A3. E' minden eleme legalább két különböző P'-beli elemmel áll relációban.

A4. P' minden eleme legalább három különböző E'-beli elemmel áll relációban.

Eljárásunkat megfordíthatjuk, vagyis affin síkból képezhető projektív sík ugyanúgy, ahogy a klasszikus affin síkhoz hozzávettük az ideális pontokat és az ideális egyenest. Az így kibővített síkot az affin sík *projektív lezártjá*nak nevezzük. Bármely affin sík projektív lezártja projektív sík.

Algebrai modell:

Ha $PG(2,K)$ síkból elhagyjuk az $x_3 = 0$ egyenletű egyenest a rajta lévő pontokkal együtt, akkor az $AG(2,K)$ affin síkot kapjuk. Feltehetjük ekkor, hogy az affin síkbeli pontok harmadik koordinátája 1, ezért elég a pontokat két koordinátával jelölni. Legyenek a pontok tehát $(x,y) \in K \times K$ rendezett párok, az egyenesek pedig azok az $[A,B,C]$ rendezett hármasok, ahol A és B egyszerre nem 0. Az (x,y) pont pontosan akkor illeszkedik $[A,B,C]$ egyenesre, ha $Ax + By + C = 0$.

Tétel: Ha az $\mathcal{A}$ affin síknak van olyan egyenese, amelyre n pont illeszkedik, akkor

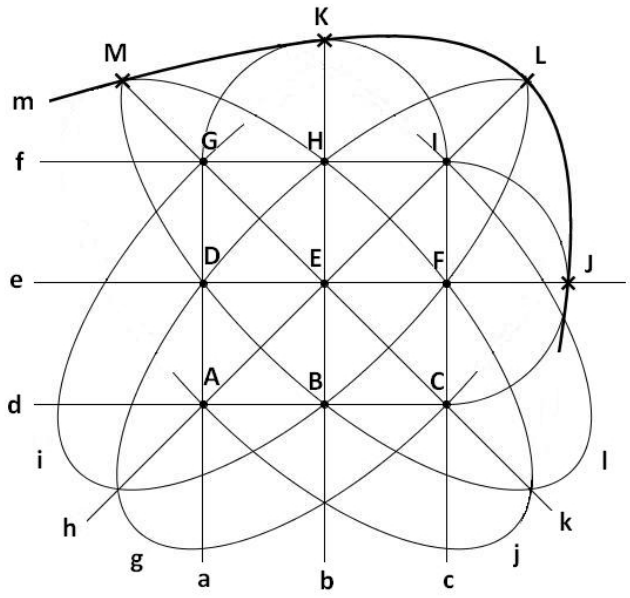
i. Minden egyenesnek n pontja van.

ii. Minden ponton $n+1$ egyenes megy át.

iii. A sík összesen n^2 pontot, és $n^2 + n$ egyenest tartalmaz.

Definíció: Az n számot az *affin sík rendjé*nek nevezzük.

A következő ábra $PG(2,3)$ és $AG(2,3)$ kapcsolatát szemlélteti. Ha $PG(2,3)$ projektív síkból elhagyjuk az m ideális egyenest a pontjaival együtt, megkapjuk az $AG(2,3)$ affin síkot. Az ábrán látható koordináták $AG(2,3)$ pontjainak és egyeneseinek a koordinátázása.



2. ábra

$A = (0,0)$	$a: x = 0$	$j: y = 2x$
$B = (1,0)$	$b: x = 1$	$k: y = 2x + 2$
$C = (2,0)$	$c: x = 2$	$l: y = 2x + 1$
$D = (0,1)$	$d: y = 0$	
$E = (1,1)$	$e: y = 1$	
$F = (2,1)$	$f: y = 2$	
$G = (0,2)$	$g: y = x + 1$	
$H = (1,2)$	$h: y = x$	
$I = (2,2)$	$i: y = x + 2$	

2.2 Magasabb dimenziós projektív terek

Legyen V_{n+1} $(n+1)$-dimenziós vektortér a $GF(q)$ véges test felett. Ekkor V egydimenziós altereit pontoknak, a kétdimenziós altereit egyeneseknek, a háromdimenziósakat síkoknak, az n-dimenziós altereit pedig *hipersíkok*nak nevezzük. Ezt a teret n-dimenziós *Galois-térnek* nevezzük, és $PG(n,q)$-val jelöljük. Ekkor V_{n+1} $(k+1)$-dimenziós alterei lesznek $PG(n,q)$ k-dimenziós alterei.

A V elemei n-dimenziós vektorok, melyekkel ugyanúgy számolunk, ahogy azt geometriában megszoktuk alacsonyabb dimenziós terek esetén. Néhány művelet ezek közül a következő:

Legyen $a = (a_1, a_2, \dots, a_n)$ és $b = (b_1, b_2, \dots, b_n)$ két vektor V-ből. Ekkor

- $a \pm b = (a_1 \pm b_1, a_2 \pm b_2, \dots, a_n \pm b_n)$
- Ha $\lambda \in GF(q)$, $\lambda \cdot a = (\lambda a_1, \lambda a_2, \dots, \lambda a_n)$
- A két vektor skaláris szorzata pedig $a \cdot b = \sum_{i=1}^{n} a_i\, b_i$.

Két vektor merőleges, ha a skaláris szorzatuk 0. Vagyis, ha $\sum_{i=1}^{n} a_i\, b_i = 0$.

Definíció: Egy V vektortérben egy H részhalmaz $H^{\perp}$ *merőleges kiegészítőjé*n a H minden elemére merőleges vektorok halmazát értjük, azaz

$$H^{\perp} = \{v \in V : h \cdot v = 0,\ \forall\, h \in H\}.$$

$H^{\perp}$ mindig altér V-ben. Ha H maga is altér, akkor igaz, hogy V a H és $H^{\perp}$ alterek direkt összege. Vagyis, ha vesszük H-ban $b_1, b_2, \dots, b_k$ ortonormált bázist, és ezt $b_{k+1}, b_{k+2}, \dots, b_n$ vektorokkal kiegészítjük V ortonormált bázisává, akkor minden $v \in V$ felírható $v = \sum_{j=1}^{n} \lambda_j\, b_j$ alakban, ahol $b_{k+1}, b_{k+2}, \dots, b_n$ bázisa $H^{\perp}$-nak. Egy k-dimenziós altér ortogonális kiegészítőjének dimenziója tehát $n-k$.

Mivel véges dimenziós vektorterekről beszélünk, az állítások nyilvánvalóak.

Ha egy projektív térnek elhagyjuk egy hipersíkját minden pontjával együtt, affin teret kapunk.

3. Kódelméleti háttér

A kódelmélet olyan kommunikációs modellel foglalkozik, melyben egy *adó* valamilyen *csatornán* keresztül *üzenetet* továbbít a *fogadónak*. Az adó kódolja az üzenetet, a fogadó pedig dekódolja azt. Tegyük most fel, hogy a kódolt üzenet valamilyen számjegyekből álló sorozat.

Az üzenet továbbítása során előfordulhat, hogy néhány adat megváltozik. Olyan kódok, eljárások kidolgozása a cél, melyek segítségével a fogadó észreveszi a hibát, és rekonstruálni tudja az eredeti üzenetet. Most csak azzal az esettel foglalkozom, ahol a számsorozat hossza nem változik, csak a számjegyek cserélődhetnek ki. A fogadónak ebben az esetben az a feladata, hogy a dekódolás során megkeresse a kapott rossz jelsorozathoz legközelebb álló kódszót, vagyis az eredeti üzenetet.

3.1 Matematikai modell

A kódolt üzenet, c, legyen a $V = (GF(q))^n$ vektortér eleme. Legtöbbször $q = 2$, vagyis a számsorozat n hosszúságú bináris sorozat. Hiba esetén egy e hibavektor adódik c-hez, tehát a fogadó $x = c + e$ üzenetet kapja meg, az eredeti c helyett. A vevő feladata a dekódolás során x-ből kideríteni c-t. Nem mindegy azonban, hogy mekkora az eltérés az eredeti üzenet vektora és a kapott vektor között. Ehhez fontos a következő két definíció.

Definíció: Két vektor *Hamming-távolságán* azt a számot értjük, ahány helyen a vektorok eltérnek egymástól. Vagyis ha $v = (v_1, v_2, \dots, v_n)$ és $w = (w_1, w_2, \dots, w_n)$ a két vektor, a távolság:

$$d(v, w) = |\{i : v_i \neq w_i\}|.$$

Megmutatjuk, hogy a Hamming-távolság V vektortéren metrika.

Bizonyítás: Nyilvánvaló, hogy a Hamming-távolság szimmetrikus. Az is könnyen látszik, hogy két vektor távolsága mindig pozitív, és csak akkor 0, ha a két vektor megegyezik.

Lássuk be a háromszög-egyenlőtlenséget. Legyen x, y, z három V-beli vektor. Meg kell mutatnunk, hogy $d(x,y) + d(y,z) \geq d(x,z)$. Legyen $d(x,z) = k$. Ekkor $x = (x_1, x_2, \dots, x_n)$ és $z = (z_1, z_2, \dots, z_n)$ koordinátái közül k darab különböző: $x_{i_1}, x_{i_2}, \dots, x_{i_k}$ és $z_{i_1}, z_{i_2}, \dots, z_{i_k}$. Mivel az y vektor megfelelő koordinátáiban legalább az egyiktől eltér, $d(x,y) + d(y,z) \geq k$ teljesül akkor is, ha csak ezt a k koordinátát vizsgáljuk.

□

Definíció: A c középpontú r sugarú gömb, úgynevezett *Hamming-gömb*, azon pontok halmaza, melyek c-től való távolsága legfeljebb r, azaz:

$$S_r(c) = \{v \in V : d(c,v) \leq r\}.$$

Definíció: A V vektortér $C \subset V$ részhalmazát *t-hibajavító kód*nak nevezzük (t pozitív egész szám), ha bármely két különböző $v, w \in C$ vektor esetén

$$d(v,w) \geq 2t + 1.$$

A C elemeit *kódszavak*nak nevezzük. A t-hibajavító kód elnevezést a következő lemma indokolja:

Lemma: Ha C t-hibajavító kód, akkor minden $v \in V$ vektorhoz legfeljebb egy olyan $c \in C$ kódszó van, amelyre $d(c,v) \leq t$.

Bizonyítás: Legyen C t-hibajavító kód. Indirekt tegyük fel, hogy létezik két különböző $c, c' \in C$ vektor, melyekre $d(c,v) \leq t$ és $d(c',v) \leq t$. A háromszög-egyenlőtlenségből ekkor azt kapjuk, hogy $d(c,c') \leq 2t$. Ami ellentmondás, hiszen $d(c,c') \geq 2t + 1$.

□

Tehát ha a küldő kódszavakat továbbít, és maximum t hiba lép fel, akkor a fogadó ki tudja javítani, dekódolni tudja az eredeti üzenetet. Hiszen a kapott hibás üzenet

pontosan egy kódszó köré írt t sugarú gömbben lesz benne, melynek középpontja az eredeti üzenet.

Látjuk tehát, hogy t-hibajavító kód esetén a kódszavak köré írt t sugarú gömbök diszjunktak. Lehetséges azonban, hogy ezek a gömbök nem fedik le teljesen a V vektorteret. Ilyenkor kimarad néhány vektor a gömbökből, melyeket nem tudunk egyértelműen dekódolni.

Definíció: Az olyan t-hibajavító kód, melyre teljesül, hogy minden $v \in V$-hez létezik legfeljebb t távolságra lévő kódszó, *perfekt kód*nak nevezzük.

Hány kódszó lehet egy t-hibajavító kódban?

Tétel: (Hamming-korlát) Ha C t-hibajavító kód a q elemű ábécé felett, akkor

$$|C| \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} \cdot (q-1)^i}$$

Bizonyítás: Először vizsgáljuk meg, hány vektor van egy t sugarú Hamming-gömbben. Ha $t = 0$, csak a középpont van a gömbben, ha $t = 1$, akkor a középponton kívül $\binom{n}{1} \cdot (q-1)$ vektor, hiszen $\binom{n}{1}$-féle helyen térhetünk el a középponti vektortól, és minden helyre a test elemszámánál eggyel kevesebb féle számot írhatunk, mely eltér a középpont megfelelő koordinátájától. Ha t$= 2$, akkor $1 + \binom{n}{1} \cdot (q-1) + \binom{n}{2} \cdot (q-1)^2$ pont van a gömbben, a középpont, az egy távolságra lévő pontok és a két távolságra lévőek. Ezt általánosítva látjuk, hogy egy t sugarú gömbben $\sum_{i=0}^{t} \binom{n}{i} \cdot (q-1)^i$ vektor van.

Ha $|C|$ darab kódszavunk van, akkor $|C| \cdot \sum_{i=0}^{t} \binom{n}{i} \cdot (q-1)^i \leq q^n$, hiszen tudjuk, hogy a gömbök diszjunktak, és lehetnek olyan elemei a vektortérnek, amik nincsenek benne egy gömbben sem.

□

Egyenlőség nyilván csak akkor van, ha a kód perfekt.

Definíció: Egy kódszó nem nulla koordinátáinak számát a *kódszó súlyá*nak nevezzük és $w(v)$-vel jelöljük.

A $d(C) = min\{d(v,w): v,w \in C, v \neq w\}$ számot pedig C *minimális távolság*ának nevezzük. Ha C t-hibajavító, akkor $d(C) \geq 2t+1$.

A gyakorlatban használt kódok dekódolásánál meg kell határozni a kapott üzenet kódszavaktól való távolságát. A kódok egy speciális fajtái esetén ezt könnyebben meg tudjuk tenni.

Definíció: A $C \subset V$ kód *lineáris kód*, ha C lineáris altere V vektortérnek. Ha C dimenziója k, akkor lineáris $[n,k]$-*kód*nak nevezzük.

Ha $c_1, c_2, \dots, c_k$ a C egy bázisa, akkor azt a $k \times n$-es G mátrixot, melynek i-edik sora a c_i vektor $(i = 1,2,\dots,k)$, C *generátor mátrixá*nak nevezzük.

A lineáris kódok dekódolásához néhány további fogalomra van szükség.

Definíció: A $C \subset V$ tetszőleges kód *duális kód*ja a

$$C^{\perp} = \{v \in V: v \cdot c = 0, \forall\, c \in C\},$$

ahol $\cdot$ a skaláris szorzatot jelenti. A 2.2 fejezetben láttuk, hogy ha C lineáris $[n,k]$-kód, akkor $C^{\perp}$ lineáris $[n, n-k]$-kód.

Definíció: A fenti $C^{\perp}$ kódnak egy H generátor mátrixát a C kód *paritásellenőrző mátrixá*nak nevezzük. Ekkor tetszőleges $v \in V$ esetén az $s(v) = vH^T$ vektort a v vektor *tünetének* nevezzük.

Egy $c \in V$ vektor akkor és csak akkor kódszó ($c \in C$), ha a tünete 0, vagyis ha

$$cH^T = 0.$$

3.2 Hamming-kód

Legyen $q = 2$ és $t = 1$. Ha perfekt kódot akarunk szerkeszteni, a Hamming-korlátból kapjuk, hogy $n + 1$ osztója kell legyen 2^n-nek, vagyis $n = 2^r - 1$. Készítsünk egy olyan $r \times (2^r - 1)$-es H mátrixot, melynek i-edik oszlopa legyen az i kettes számrendszerbeli alakja. Ekkor látszik, hogy a csupa nullából álló sorozaton kívül minden különböző r hosszú $0 - 1$ sorozat szerepel az oszlopokban, és csak ezek szerepelnek. Formálisan $i = \sum_{j=1}^{r} h_{ij} 2^{r-j}$. A Hamming-kód definíciója tehát a következő:

Definíció: Legyen r tetszőleges pozitív egész szám, $n = 2^r - 1$, H pedig az az $(r \times n)$-es mátrix, melynek oszlopai a csupa 0-ból álló sorozat kivételével az összes különböző $0 - 1$ sorozatot tartalmazzák. Az *n-hosszú bináris Hamming-kód* az a kód, melynek H a paritásellenőrző mátrixa. Jelöljük ezt $Ham(r)$-rel.

Mivel $Ham(r)$ $(n - r)$-dimenziós altér $GF(2)^n$ vektortérben, az altérre merőleges vektorok egy r-dimenziós G alteret alkotnak, melynek H a generátormátrixa. A v kódszó, vagyis eleme $Ham(r)$-nek, ha merőleges a G altérre, tehát ha $v \cdot H^T = 0$.

Ha $r = 1$ vagy 2, a kód triviális. Nézzük meg az $r = 3$ esetet! Ekkor a paritásellenőrző mátrix:

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

Látszik, hogy H maximális rangú, hiszen átrendezhető úgy, hogy legyen 3×3-as identikus részmátrixa. Ebből következik, hogy egy 3-dimenziós alteret generál, H^T pedig 4-dimenziós alteret.

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

Ekkor $|Ham(3)| = 2^{n-3} = 16$, mert $v \cdot H^T = 0$ egyenletrendszernek ennyi megoldása van.

A 7-hosszú Hamming-kód kódszavai a következők:

$0000000,\ 1110000,\ 0101010,\ 1001100,\ 0011001,\ 0100101,\ 1000011,\ 0010110,$
$1111111,\ 0001111,\ 1010101,\ 0110011,\ 1100110,\ 1011010,\ 0111100,\ 1101001$

3.2.1 Mi a kapcsolata $\boldsymbol{Ham}(3)$-nak a Fano-síkkal?

*Karakterisztikus vektor*nak nevezzük az olyan $v = (v_{1,}, v_2, \dots, v_n)$ vektort, melynek egyes koordinátái a pontokat jelképezik, $v_i = 1$, ha az i-edik pont benne van a sík egy adott részhalmazában, $v_i = 0$, ha nem.

A fenti kódszavak az 1. ábrán látható Fano-sík egyeneseinek karakterisztikus vektorai, a vektorok komplementerei, és az üres halmaznak, valamint az egész síknak a karakterisztikus vektora. Ezen a geometriai modellen szemléltethető, hogy a 7-hosszú Hamming-kód 1-hibajavító. Mutassuk meg tehát, hogy minden $v \in V$ vektor pontosan 1 darab kódszótól lesz 1 Hamming-távolságra.

Tekintsük V elemeit karakterisztikus vektoroknak, azonosítsuk őket a sík pontjainak részhalmazaival. Ha egy részhalmaz legfeljebb egy, vagy legalább hat pontot tartalmaz, akkor legfeljebb 1 távolságra csak az üres halmaz, vagy a teljes sík van. Ha kettő vagy öt pontot tartalmaz, akkor egyértelműen kiegészíthető egy egyenessé vagy egy egyenes komplementerévé. Ha három pont nem kollineáris, akkor minden egyenestől legalább 2 távolságra van az általuk alkotott részhalmaz, viszont 1 távolságra van annak az egyenesnek a komplementerétől, amelyik a három pont által meghatározott háromszög oldalait a pontoktól különböző pontokban metszi. Ha pedig négy pont nem egy egyenes komplementere, akkor köztük van három kollineáris, ettől az egyenestől ekkor 1 a távolságuk, minden más egyenestől és az egyenesek komplementereitől pedig legalább 2.

□

3.2.2 $Ham(r)$ tetszőleges r esetén

Legyen most r tetszőleges pozitív egész. Az $r = 3$ esethez hasonlóan belátható, hogy H maximális rangú, vagyis r a rangja. Ebből következik, hogy $|Ham(r)| = 2^{n-r}$, és dimenziója $2^r - 1 - r$.

Állítás: A Hamming-kódok lineáris 1-hibajavító kódok.

Az előző állítás bizonyításához a következő segédtételre van szükség.

Lemma: Lineáris kódoknál a minimális távolság megegyezik a legkisebb nem nulla súlyú kódszó súlyával.

Bizonyítás: (Lemma) Legyen C lineáris kód, ekkor $0 \in C$. Ezért

$d(C) = \min\{d(v,w): v,w \in C, v \neq w\} \leq \min\{d(v,0): v \in C, v \neq 0\} = w(v)$

A minimális távolság tehát nem nagyobb a legkisebb súlyú nem nulla vektor súlyánál.

Másrészt, ha v és w olyan vektorok, melyekre $d(C) = d(v,w)$, akkor a linearitás miatt $v - w \in C$. Mivel

$w(v-w) = d(v-w,0) = d(v-w,w-w) = d(v,w) = d(C)$,

ezért van olyan kódszó, melynek súlya éppen a minimális távolság. □

Bizonyítás (Állítás): Megmutatjuk, hogy a minimális távolság $Ham(r)$-ben legalább 3, vagyis nem létezik 1 vagy 2 súlyú kódszó. Legyen $x, y \in Ham(r)$ két tetszőleges vektor. Tudjuk, hogy $(x-y) \in Ham(r)$, mivel $Ham(r)$ lineáris altér. Ekkor $x \cdot H^T = y \cdot H^T = (x-y) \cdot H^T = 0$.

Tegyük fel, hogy $d(x,y) = 1$. Ekkor $x - y = (0,0,\dots,m,\dots 0)$ 1 súlyú vektor, vagyis az i-edik koordinátája nem 0. Az $(x-y) \cdot H^T$ skaláris szorzat ebben az esetben a H i-edik oszlopának transzponáltja, ami nem lehet a nullvektor, mert nincs csupa 0-ból álló oszlopa H-nak.

Most azt tegyük fel, hogy $d(x,y) = 2$. Ekkor a 2 súlyú $x - y = (0,0,\dots,m.\dots,n,\dots 0)$ vektor i-edik és j-edik koordinátája nem 0. Legyen v vektor a H i-edik oszlopának transzponálja, w pedig a j-edik oszlop transzponáltja. Ha

$0 = (x - y) \cdot H^T$, akkor $n \cdot v + m \cdot w = 0$, vagyis $w = -\frac{n}{m} \cdot v$. Ez ellentmondás, mert a különböző oszlopvektorok nem lehetnek egymás skalárszorosai.

Valóban legalább 3 a minimális távolság, vagyis 1-hibajavító a kód.

□

Állítás: A Hamming-kódok perfekt kódok.

Bizonyítás: Mivel $2^{n-r}(2^r - 1 + 1) = 2^n$, ezért a Hamming-kód szavai köré írt 1 sugarú gömbök a V vektortér diszjunkt befedését adják.

□

3.2.3 Kódolás és dekódolás

Kódolás:

Az n-hosszú bináris Hamming-kód esetén a kódolást a következőképpen végezhetjük. Legyen $c = (x_1, x_2, \dots, x_n)$ kódszó. Írjunk az x_i $(i \neq 2^j, j = 0,1, \dots, r-1)$ koordináták helyére tetszőleges számot, a többi koordinátát pedig számoljuk ki a $c \cdot H^T = 0$ egyenletrendszerből.

Dekódolás:

Ha a fogadó $x \notin Ham(r)$ üzenetet kapja c kódszó helyett, akkor a dekódolás során ki kell számolnia az e hibavektort. Ki kell számolni a $(c + e) \cdot H^T$ szorzatot, mely egyenlő lesz $e \cdot H^T$-tal, a linearitás miatt. Ekkor H j-edik oszlopvektorát kapjuk eredményül, mely megadja, hogy e j-edik koordinátája nem nulla, tehát a j-edik koordinátában történt a hiba. Innen már visszafejthető az üzenet.

3.2.4 Általánosítás p-re

Legyen $V = GF(p)$ tetszőleges véges test (p prím). Ekkor a H mátrix konstrukcióját módosítjuk. Az oszlopokba az $1,2, \dots, p^r - 1$ számok p alapú számrendszerbeli alakját írjuk. Az olyan oszlopok közül, amelyek egymás skalárszorosai lennének, csak azt írjuk le, amelynek az első nem nulla számjegye 1. Mivel ez a számjegy $(p-1)$-féle lehet, $\frac{p^r-1}{p-1}$ oszlopot tartunk meg. Ezek az oszlopok éppen $GF(p)$ feletti $(r-1)$-dimenziós projektív tér pontjainak felelnek meg.

A $p = 2$ esethez hasonlóan bizonyítható, hogy ezek perfekt 1-hibajavító kódok.

3.3 Golay-kódok

Nagyon kevés perfekt kód van. A Hamming-kódon kívül ilyenek még a Golay-kódok.

Tétel: (Tietäväinen, van Lint) Ha $t > 1$, akkor csak két perfekt kód létezik. Ezek a *Golay-kódok*. A $q = 2$ esetén $n = 23$, $t = 3$ a bináris Golay-kód paraméterei, $q = 3$ esetén pedig $n = 11$, $t = 2$ a ternér kód paraméterei.

A tétel bizonyítása kívül esik dolgozatom témáján.

3.3.1 A ternér Golay-kód

A következő fejezetben a totókulcsok megadásánál szerepel majd a ternér Golay-kód, így ezzel részletesebben foglalkozom.

A kód paritásellenőrző mátrixa a következő:

$$\begin{pmatrix} 1 & 0 & 1 & 2 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 2 & 0 & 0 & 2 & 0 & 0 \\ 1 & 2 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 2 & 0 \\ 1 & 1 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Ekkor a perfekt kódunkat a következő 5 egyenlet definiálja, ahol x_i értékeit $i = 1,2, \dots ,6$ esetén szabadon megválaszthatjuk:

$$\begin{aligned} x_7 &= x_1 + x_3 + 2x_4 + 2x_5 + x_6 \\ x_8 &= x_1 + x_2 + x_4 + 2x_5 + 2x_6 \\ x_9 &= x_1 + 2x_2 + x_3 + x_5 + 2x_6 \\ x_{10} &= x_1 + 2x_2 + 2x_3 + x_4 + x_6 \\ x_{11} &= x_1 + x_2 + 2x_3 + 2x_4 + x_5 \end{aligned}$$

4. Lehet-e nyerni a totón?

A klasszikus totó játéknál focimeccsek kimenetelére fogadhatunk. $13+1$ mérkőzést játszanak a csapatok, és minden meccs esetén háromféle kimenetel lehetséges. A telitalálattal sok pénzt nyerhetünk, 10-nél kevesebb találattal azonban nincs nyeremény. Mivel a szervezők csak egy részét osztják szét a játék során befizetett pénznek, játékosként csak szerencsével nyerhetünk több pénzt, mint amit beinvesztáltunk. Néhány lehetőséget azonban ki lehet zárni, ezzel csökkenthetjük a kitöltendő szelvények számát.

Ebben a részben módszerek szerepelnek arra, hogy egyforma valószínűségű kimenetelek mellett hogyan érhetünk el biztosan előre meghatározott számú találatot a lehető legkevesebb tippel.

4.1 Matematikai megfogalmazás $\mathbb{Z}_3$ fölött

Tegyük fel, hogy a meccsek száma N. Mivel lehetséges, hogy néhány meccs kimenetelét már előre tudjuk, legyen n $(n \leq N)$ azon meccsek száma, melyeknél több kimenetellel számolunk. A lehetséges kimenetelek száma ekkor valamilyen m pozitív egész, legyen most $m = 3$.

Legyen r egy rögzített egész szám. Tekintsük az n hosszú $0, 1, 2$ számjegyekből álló sorozatok halmazát, vagyis a $\mathbb{Z}_3^n$ vektorteret. Adjuk meg a lehető legkevesebb elemszámú $C \subset \mathbb{Z}_3^n$ részhalmazt, melyre teljesül, hogy $\mathbb{Z}_3^n$ bármely v eleméhez van olyan C-beli c elem, amely v-től legfeljebb r helyen tér el. C elemeit nevezzük *tippvektor*oknak, a meccsek végeredményeiből létrejött vektort pedig *eredményvektor*nak.

Ha r tetszőleges egész, biztos $n-r$ találatot akkor tudunk elérni $|C|$ darab tippvektorral, ha a C elemei köré írt r sugarú Hamming-gömbök lefedik az egész $\mathbb{Z}_3^n$ vektorteret. Ekkor bármilyen e eredményvektor benne lesz legalább egy alkalmas gömbben. Tehát lesz olyan c tippünk, melyre $d(c, e) \leq r$, azaz c az eredményvektorral legalább $n-r$ koordinátában megegyezik.

Tétel: (Gömbpakolási korlát) Ha az n meccset tartalmazó totón a C tipphalmazzal biztosan elérünk legalább $n-r$ találatot, akkor a tipphalmaz $|C|$ elemszámára teljesülnie kell, hogy

$$|C| \geq \frac{3^n}{\sum_{i=0}^{r}\binom{n}{i}\cdot 2^i}$$

Bizonyítás: A Hamming-korlát bizonyításánál láttuk, hogy egy gömbben $\sum_{i=0}^{r}\binom{n}{i}\cdot(q-1)^i$ darab vektor van. Ahhoz, hogy az egész vektorteret le tudjuk fedni a $|C|\cdot\sum_{i=0}^{r}\binom{n}{i}\cdot 2^i \geq 3^n$ egyenlőtlenségnek kell teljesülnie.

□

4.2 Jó tipphalmazok $\mathbb{Z}_3$ fölött

Ha biztos telitalálatot szeretnénk, vagyis $r=0$, akkor triviális a megoldás. A tippvektorok köré írt 0 sugarú gömbök uniójának tartalmaznia kell az egész $\mathbb{Z}_3^n$ vektorteret, vagyis $C=\mathbb{Z}_3^n$. Ekkor minden lehetséges módon ki kell tölteni a szelvényeket. $|C|=3^n$.

Kombinatorikából ismert, hogy egy 13 mérkőzésből álló totón a biztos 5 találathoz 3 szelvény elég. Legyenek a tippvektorok azon c_i vektorok $(i=0,1,2)$, melyek mindegyik koordinátája i. A skatulyaelv szerint a 13 hosszú vektoroknak van legalább 5 darab azonos koordinátája, hiszen egy vektor mindhárom lehetséges koordinátából 4-et tartalmazva maximum 12 hosszú lehetne. Ez a három szelvény tehát valóban biztos 5 találatot eredményez. Két szelvény pedig nem elég, mert ha kitöltünk két, minden koordinátában különböző szelvényt, lehet, hogy az eredményvektor 0 találatos lesz, mert minden koordinátában pont a lehetséges harmadik kimenetel fog szerepelni.

Sajnos az 5 találatos szelvénnyel nem lehet nyerni. A továbbiakban tehát azokkal az esetekkel érdemes foglalkozni, ahol r kicsi.

A következő táblázat az ismert eredményeket tartalmazza $n \leq 13$ és $r = 1,2,3$ esetén. Az első szám a legjobb ismert tipphalmaz elemszámát jelöli, a zárójelben pedig az optimális tipphalmaz méretére vonatkozó legjobb alsó becslés szerepel, mely itt minden olyan esetben, amikor nincs egyenlőség, jobb a Gömbpakolási korlátnál.

n	$r = 1$	$r = 2$	$r = 3$
2	3	1	
3	5	3	1
4	9	3	3
5	27	8	3
6	73 (71)	17 (15)	6
7	186 (156)	34 (26)	12 (11)
8	486 (402)	81 (54)	27 (14)
9	1269 (1060)	219 (130)	54 (27)
10	3645 (2854)	555 (323)	105 (57)
11	9477 (7832)	729	243 (117)
12	27702 (21531)	2187 (1919)	657 (282)
13	59049	6561 (5062)	1215 (612)

1. táblázat

Látszik, hogy nagy n-ekre csak nagyon kevés esetben ismert a jó tipphalmazok elemszáma. Én most csak azokkal az esetekkel foglalkozom, ahol ismert az optimális konstrukció.

4.2.1 Biztos $n - 1$ találat

Nézzük az $r = 1$ esetet. Ha $n = 2$ a szelvények: $(0,0)$, $(1,1)$, $(2,2)$. Ugyanúgy belátható, mint fentebb az $n = 13, r = 8$ esetén.

Az $n = 3$ esetet dolgozatom végén feladatként oldottam meg.

Vizsgáljuk a 4 mérkőzéses totót. Az $AG(2,3)$ véges affin sík segítségével adható egy optimális konstrukció.

A tippvektorok legyenek az affin sík pontjai, rendeljünk minden ponthoz egy 4 hosszú vektort. Minden P ponton 4 egyenes megy át, melyek mind különböző párhuzamossági osztályba tartoznak. A tippvektor egyes koordinátái megfeleltethetőek a P-n átmenő egyeneseknek, melyek a következők:

$$X = c, \qquad Y = d, \qquad Y = X + e, \qquad Y = 2X + f$$

Ekkor rendeljük minden P ponthoz a következő 4 hosszú vektort:

$$P \mapsto p = (c, d, e, f)$$

Ez a konstrukció jó. 9 tippel biztos 3 találatot érhetünk el.

Bizonyítás: A Gömbpakolási korlát szerint minimum 9 tippvektor kell. Megmutatjuk, hogy ennyi elég is. Bármely két különböző P, Q pont Hamming-távolsága 3, mert pontosan 1 koordinátában egyeznek meg, ugyanis egyértelműen létezik őket összekötő egyenes. Vagyis a pontok köré írt 1 sugarú gömbök diszjunktak lesznek, a becslés tehát éles.

□

Kódelmélet segítségével megfogalmazva létezik 4 hosszú perfekt 1-hibajavító kód $\mathbb{Z}_3$ fölött. A kódszavai, vagyis a szükséges tippek a következők:

A: $(0,0,0,0)$, B: $(1,0,2,1)$, C: $(2,0,1,2)$, D: $(0,1,1,1)$, E: $(1,1,0,2)$,

F: $(2,1,2,0)$, G: $(0,2,2,2)$, H: $(1,2,1,0)$, I: $(2,2,0,1)$

A pontokat a 2. ábrán (7. oldal) szereplő jelölések alapján adtam meg.

Meglepő, hogy a táblázatban $n = 13$ esetén pontos számot látunk. Létezik tehát optimális konstrukció ebben az esetben. Ez a $\frac{3^3-1}{3-1}$ hosszú ternér Hamming-kód. Nézzük tehát a 13 mérkőzéses TOTÓ-n hány szelvény kell a biztos 12 találathoz.

Tekintsük a $\mathbb{Z}_3$ feletti 13 hosszú Hamming-kódot. A bináris esethez hasonlóan vegyük a $3 \times \frac{3^3-1}{2}$-as H mátrixot. A H oszlopaiban a $1,2,\dots,3^3-1$ számok hármas számrendszerbeli alakja szerepel, de csak azoké, amelyeknek föntről lefelé az első nemnulla koordinátája 1. Mivel az első nemnulla koordináta kétféle lehet, pontosan a számok fele szerepel. A mátrix a következő:

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

Ahogy 3.2.4.-ben láttuk, az oszlopok épp a $PG(2,3)$ projektív sík pontjainak homogén koordinátái.

A bináris esethez hasonlóan a mátrix átrendezhető, rangja így maximális, vagyis 3. Az $x \cdot H^T = 0$ egyenletrendszernek tehát 3^{13-3} megoldása van, 59049 szelvényt kell kitöltenünk. A Gömbpakolási korlát szerint ennyi kódszó köré írt 1 sugarú gömbbel már lefedhető a vektortér. A gömbök pedig diszjunktak, mert a minimális távolság legalább 3, ahogy ezt már a 3.2 fejezetben beláttuk.

4.2.2 Biztos $n-2$ és $n-3$ találat

Ha $r = 2$ és $n = 3, 4$, akkor 3 szelvény kell. A csupa 0-ból, a csupa 1-ből és a csupa 2-ből álló szelvények jók. A 3 mérkőzéses totó esetén triviális, 4 mérkőzés esetén pedig a skatulyaelvből következik. Ugyanígy könnyen látható az $r = 3$, $n = 4, 5$ eset is.

Az $r = 3$, $n = 6$ totókulcs a feladatoknál szerepel.

Feltűnő, hogy $r = 2$, $n = 11$ esetén létezik optimális megoldás. A konstrukció a fentebb említett ternér Golay-kódhoz kapcsolódik. Ebben az esetben egy kódszó köré írt 2 sugarú gömbben $1 + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 2^2 = 243 = 3^5$ darab vektor van, így a 3^{11} vektort legalább 3^6 gömb fed le. Mivel a kódunk perfekt, elég is ennyi gömb.

A 3.3.1-ben megadott egyenletrendszer geometriailag is szemléltethető. Vegyünk egy szabályos ötszög alapú gúlát, és számozzuk meg a csúcsait. Legyenek az alap csúcsai a $2,3,4,5,6$ csúcsok, a hatodik csúcsot pedig jelölje az 1. A $(x_1 x_2, \dots, x_{11})$ vektor első hat koordinátája szabadon megadható modulo 3, jelképezze x_i-t $(i = 1,2, \dots, 6)$ az i-edik csúcshoz rendelt érték.

Tekintsük a 2 csúcsot. Ekkor az $1,3$ és a 6 csúcsok szomszédai, a 4 és 5 csúcsok nem-szomszédai az adott csúcsnak. Az x_7 koordináta úgy számolható ki, hogy összeadjuk a 2 csúcs szomszédjaihoz rendelt számokat és kivonjuk belőle a nem-szomszédokhoz rendelt értékeket. Tehát $x_7 = x_1 + x_3 + x_6 + 2x_4 + 2x_5$, hiszen modulo 3 számolunk. Az x_i-k $(i = 8,9,10,11)$ értékei rendre kiszámítható a $3,4,5,6$ csúcsok szomszédait és nem-szomszédait véve.

4.3 Jó tipphalmazok $\mathbb{Z}_2$ fölött

Abban az estben, ha egy mérkőzésnek csak 2 kimenetele van (pl. egyenes kieséses bajnokság), olyan $C \subseteq \mathbb{Z}_2^n$ részhalmazt keresünk, ahol minden $x \in \mathbb{Z}_2^n$ vektor r Hamming-távolságra van minimum egy $c \in C$ tippvektortól. Bináris esetben a Gömbpakolási korlát a következő:

$$|C| \geq \frac{2^n}{\sum_{i=0}^{r} \binom{n}{i}}$$

Ez ugyanúgy belátható, mint ternér esetben.

Vizsgáljuk most csak azt a lehetőséget, amikor $r = 1$. Ez a becslés csak akkor éles, ha $n = 2^h - 1$, vagyis Hamming-kódok esetén.

A következő táblázat az ismert eredményeket tartalmazza $n \leq 13$ és $r = 1$ esetén. Ugyanúgy, mint az első táblázatnál, az első szám a legjobb ismert tipphalmaz elemszámát jelöli, a zárójelben pedig az optimális tipphalmaz méretére vonatkozó legjobb alsó becslés szerepel.

$\boldsymbol{n}$	$\boldsymbol{r = 1}$
1	1
2	2
3	2
4	4
5	7
6	12
7	16
8	32
9	62
10	120 (107)
11	192 (180)
12	380 (342)
13	704 (598)

2. táblázat

Példa: Ha $n = 4$, biztos három találatot elérhetünk a következő négy tippel:

$0000, 1000, 0111, 1111.$

Bizonyítás: Összesen $|\mathbb{Z}_2^4| = 16$ darab vektorunk van. Az 1 súlyú vektorok 1 Hamming-távolságra vannak a 0000 tippvektortól, így a tipp köré írt 1-sugarú gömb lefedi ezt a 4 vektort, és a középpontot. Az 1100, 1010, 1001 vektorokat az 1000 tippvektor köré írt gömb fedi le, az összes 3-súlyút pedig az 1111 köré írt gömb. Eddig lefedtünk $5 + 3 + 5$ vektort. Kimaradt még néhány 2 súlyú: a 0011, 0110, 0101 vektorok, melyeket a 0111 köré írt gömb lefed. Ezzel beláttuk, hogy a fenti 4 tippvektor jó. □

4.3.1 $n = 11, r = 1$ paraméterű bináris eset

Most adjunk egy konstrukciót $n = 11$ esetén, mely bizonyítja, hogy 192 szelvény elég a biztos 10 találathoz. (Az nem bizonyított, hogy nincs ennél jobb konstrukció.)

Definíció: Egy $(H; \mathcal{H})$, $\mathcal{H} \subseteq 2^H$ halmazrendszer $t - (v, k, \lambda)$ *blokkrendszer*, ha $|H| = v$, $\forall B \in \mathcal{H}: |B| = k$, és H minden t elemű részhalmazát $\mathcal{H}$-nak pontosan λ eleme tartalmazza. $\mathcal{H}$ elemeit blokkoknak nevezzük. Ha $\lambda = 1$, akkor az $S(t, k, v)$ *Steiner rendszert* kapjuk.

Ismert, hogy létezik az $S(4,5,11)$ Steiner rendszer. Megmutatjuk, hogy ez 66 elemű.

Vegyük a blokkok karakterisztikus vektorait. Ugyanúgy járunk el, mint a 3.2.1. fejezetben a Fano-sík esetén.

Rögzítsünk le 4 koordinátát. $\mathcal{H}$ elemei között pontosan 1 olyan vektor van, melynek a rögzített koordinátáiban 1-es szerepel, és akárhogy választhatom ki a 4 koordinátát, lesz ilyen vektor. $\binom{11}{4}$-féleképpen rögzíthetem a koordinátákat. Mivel $\mathcal{H}$ elemei 5-súlyú vektorok, minden vektort az 5 darab 1-es koordinátájából 4-nek a megadásával már megkapunk. Ha minden lehetséges módon lerögzítünk 4 koordinátát, akkor $\binom{5}{4} = 5$-ször számolunk minden vektort. Tehát $|\mathcal{H}| = \frac{\binom{11}{4}}{\binom{5}{4}} = 66.$

Legyenek ezek a vektorok a komplementereikkel együtt tippvektorok. Eddig van 132 vektorunk tehát. Ennek a Steiner rendszernek megvan az a tulajdonsága, hogy a komplementerek által lefedhető 5-súlyú vektorok egyike sem egyezik meg az 5-súlyú tippvektorok valamelyikével [7.].

Belátható, hogy minden $4, 5, 6$ és 7 súlyú bináris vektor 1 Hamming-távolságra van a fenti tippvektoroktól. A 4 súlyú vektorok lefedése könnyen adódik a fentiekből. Hiszen pont úgy definiáltuk a Steiner rendszert, hogy minden koordinátanégyes szerepeljen a kiválasztott 5-súlyú vektorok között.

Ugyanígy a komplementerek között szerepel minden 7 koordináta lehetséges kombinációja úgy, hogy közülük csak egy 0, vagyis a 7-súlyúak is lefedhetők.

Az 5-súlyú vektorok vagy az $S(4,5,11)$ elemei, vagy a komplementerekkel lefedhetőek. Összesen $\binom{11}{5} = 462$ darab 5-súlyú vektor van, melyből 66 eleme a Steiner-rendszernek, $66 \cdot 6 = 396$ pedig 1 távolságra van a komplementerek valamelyikétől. Tudjuk, hogy $S(4,5,11)$ elemeinek halmaza és a komplementerek által lefedett vektorok halmaza diszjunkt.

Meg kell még mutatnunk, hogy a komplementerek által lefedett vektorok mind különbözőek. Ha lenne két olyan komplementer, ami ugyanazt az 5-súlyú vektort fedné le, akkor az eredeti vektorok tartalmaznák ugyanazt a négyest, ami nem lehetséges. Tehát a fenti 5-súlyú vektorok mind különbözőek, és lefedhetőek.

A 6-súlyú vektorok lefedése könnyen adódik, ha az előző gondolatmenetben szereplő vektoroknak mindig a komplementerét vesszük.

A kimaradt vektorokat fedjük le a következőképpen: Osszuk fel H-t egy 5 és egy 6-elemű részhalmazra. Vegyük az összes kételemű részhalmazát ezeknek, és az 5-elemű részhalmaz egyelemű részhalmazait. Ez az $\binom{5}{2} + \binom{6}{2} + \binom{5}{1} = 30$ részhalmaz a komplementereivel együtt már lefedi a kimaradt elemeket. Összesen tehát 192 tippvektorral lefedhető a $\mathbb{Z}_2^{11}$ vektortér.

4.4 A vegyes eset

A valóságban általában nem ilyen egységes a totó játék. Néhány mérkőzés esetén kizárhatunk egy lehetséges kimenetelt, néhány mérkőzésnél azonban nem. Legyen n_1 azon mérkőzések száma, ahol 3 esélyt játszunk meg, n_2 pedig, ahol 2 kimenetellel számolunk. Ekkor a következő becslés érvényes a tippek számára:

$$|C| \geq \frac{2^{n_2} 3^{n_1}}{\sum_{j=0}^{r} \sum_{i=0}^{j} \binom{n_2}{i} \binom{n_1}{j-i} 2^{j-i}}$$

ahol r a gömbök sugara, vagyis r hibát engedünk meg.

Az alábbi táblázat az eddig ismert minimális tippszámot mutatja. A számok mögött a felkiáltójel jelzi, hogy az adott érték optimális.

n_1/n_2	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	2 (!)	3 (!)	6 (!)	8 (!)	16 (!)	24 (!)	48	84	160	284	548	992
2	4 (!)	6 (!)	12 (!)	20 (!)	36	64	122	232	408	768	1472	
3	9 (!)	16 (!)	24 (!)	48	92	171	312	576	1056	2016		
4	18 (!)	36 (!)	72	128	238	432	852	1296	2592			
5	54	96	168	324	624	1184	1944	3888				
6	132	252	468	864	1620	2916	5832					
7	333	648	1296	2304	4374	8532						
8	948	1728	3374	6408	11664							
9	2520	4752	9450	17496								
10	6804	13122	25272									
11	18954	34992										
12	52488											

3. táblázat

Jelölje $\mathbb{Z}_3^k \mathbb{Z}_2^l$ az olyan $k+l$ hosszú vektorokat, melyek első k koordinátája $\mathbb{Z}_3$ eleme, az utolsó l koordinátája pedig $\mathbb{Z}_2$ eleme.

Vizsgáljuk megint az $n = 4$ és $k = l = 2$ esetet. Minden $\mathbb{Z}_3^2 \mathbb{Z}_2^2$-beli vektor legfeljebb 1 Hamming-távolságra van a következő 6 tippvektor valamelyikétől:

$0011, 0200, 1000, 1211, 2101, 2110$

Bizonyítás: A 2200, 2211, 2201, 2210 vektorok 1 távolságra vannak a fenti tippvektorok valamelyikétől, hiszen az utolsó két koordináta minden lehetséges módon szerepel az olyan tippvektorokban, ahol van egy 2-es az első két koordinátában. Ugyanígy lefedhetők azok a vektorok, melyek 11-gyel kezdődnek. A 00-val kezdődő vektorok vagy a 0011 tipptől, vagy az 1000 tipptől vannak maximum 1 távolságra. Az 10 kezdetű vektorok a 0011, 1000 vektoroktól vannak maximum 1 távolságra, a 01 kezdetűek pedig a 0011 vektortól, és azon vektoroktól, melyek második koordinátája 1. Az $12, 21, 20$ és 02 kezdetű $4-4$ vektor esetén szintén könnyen látható a távolság. Így mind a $9 \cdot 4 = 36$ vektor benne lesz a tippek köré írt valamelyik 1-sugarú gömbben.

□

4.5 Többszörös lefedés

Tegyük fel, hogy nem egyedül játszunk, hanem csapatban. A μ darab játékos célja, legalább μ helyezés elérése, melyek mindegyike legalább az $(r+1)$-edik. Magától értetődő stratégia lenne, ha mindenki külön-külön a biztos $(r+1)$-edik helyért küzdene, de nem mindig ez a legolcsóbb megoldás.

Legyen $n=4$ és $r=1$. Lefedhetjük $\mathbb{Z}_2^4$-et kétszeresen és háromszorosan úgy, hogy az egyszeres lefedéshez szükséges tippeket 2-szer, 3-szor megjátsszuk. Így $8, 12$ tippre lenne szükségünk, de van ennél jobb megoldás 7, illetve 11 tippel, melyek a következők.

$0001, 0010, 0011, 1100, 1100, 0111, 1011$

$0001, 0010, 0100, 0011, 0101, 1001, 1010, 1100, 0111, 1101, 1110$

A bizonyítás könnyen adódik, ha megvizsgáljuk, hogy a $\mathbb{Z}_2^4$-beli vektorokat 2 vagy 3 különböző gömb fedi le.

Ha $n=11$, $r=1$, $\mathbb{Z}_2^{11}$ háromszoros lefedését 2^9 tippel érhetjük el. Tetszőlegesen megválasztjuk x_i $(i=1,2,\dots,9)$ értékét, a többi vektort pedig a következő egyenletek adják:

$$x_{10} = x_1 + x_2 + x_3 + x_4 + x_5$$

$$x_{11} = x_1 + x_2 + x_3 + x_6 + x_7$$

Ez a konstrukció optimális is, mert eléri a Gömbpakolási korlátot.

Vizsgálhatunk olyan eseteket is, ahol az a cél, hogy elérjünk vagy egy nagy nyereményt, vagy sok kicsit. Például a következő hat tippel $\mathbb{Z}_2^4$-ben vagy telitalálatot, vagy két második helyezést (egy hibát) érünk el minden esetben.

$$1111, 1111, 1000, 0100, 0010, 0001$$

5. Feladatok

5.1 Feladat: Hányféleképpen lehet kitölteni egy $13+1$ meccses totószelvényt úgy, hogy az első négy kimenetel között legfeljebb egy 0-s legyen? Hányféleképpen tölthetjük ki a szelvényeket úgy, hogy legyen legalább egy 0 köztük?

Rögzítsünk le egy koordinátát az első négy közül, ahol a 0 álljon. Ezt 4-féleképpen tehetjük meg. A többi három helyre 1-es vagy 2-es kerülhet 2^3-féleképpen. A fennmaradó 10 koordináta esetén három lehetőség közül választhatunk, 3^{10} különböző módon. Eddig összeszámoltuk azokat az eseteket, ahol egy darab 0 szerepel az első 4 koordinátában. Hozzávesszük még azokat a vektorokat, ahol az elején nem szerepel 0, $2^4 \cdot 3^{10}$ darab ilyen létezik. Összesen $(2^3 \cdot 4 + 2^4) \cdot 3^{10}$-féle szelvény tölthető ki.

A feladat második részét szintén esetszétválasztással oldjuk meg. Ha az első koordináta 0, a többit tetszés szerint, 3^{13}-féleképpen adhatjuk meg. Ha a második koordináta 0, akkor az első koordinátát kétféleképp választhatjuk, a többit háromféleképpen, hogy ne számítsunk kétszer azt az esetet, ahol az első két koordináta 0. Ha a harmadik koordináta 0, az első kettőt 2-féleképp, a többit 3-féleképp, ha pedig a negyedik koordináta 0, az első hármat 2-féleképp, a többit 3-féleképp választhatjuk. Összesen $3^{13} + 2 \cdot 3^{12} + 2^2 \cdot 3^{11} + 2^3 \cdot 3^{10}$ különböző szelvény tölthető ki.

5.2 Feladat: Hány szelvényt kell kitöltenünk a biztos 13 találathoz, ha tudjuk, hogy lesz 0? Hány szelvényt kell kitöltenünk, ha 5 találattal is megelégszünk?

Vegyük sorba azokat az eseteket, amikor a 0-k száma $1,2,\dots,13$.
$\binom{13}{1} \cdot 2^{12}$ különböző szelvényünk van, mely egy darab 0-t tartalmaz, hiszen a 0 13-féle helyen szerepelhet, a többi 12 koordináta pedig tetszőlegesen 1 vagy 2 lehet. Ugyanígy belátható, hogy i darab 0-t tartalmazó szelvényből $\binom{13}{i} \cdot 2^{13-i}$ darab van. Az i minden lehetséges értékére kiszámolva a következő összeget kapjuk:

$\sum_{i=1}^{13}\binom{13}{i}\cdot 2^{13-i}$ darab szelvényt kell kitölteni, az összes olyat, ami 0-t tartalmaz. Ha csak egyet is kihagynánk, lehet, hogy nem nyerünk, mert pont az lesz az eredményvektor.

Ha megelégszünk 5 találattal, akkor 3 szelvény elég: a csupa 0-ból, csupa 1-ből és a csupa 2-ből álló. Fentebb már láttuk, hogy ezzel a 3 szelvénnyel biztosan elérünk 5 találatot, lényegtelen, hogy van-e 0 az eredményben vagy nem. 2 szelvény pedig nem elég, mert minden mérkőzésnél 3 lehetséges kimenetel van, lehet, hogy mindig a harmadik lesz a jó eredmény, amivel nem számoltunk, és 0 találatunk lesz.

5.3 Feladat: Lássuk be, hogy a 3 mérkőzéses totón nem elég 4 szelvény a biztos 2 találathoz! Adjunk meg 5 tippet, ami már elég!

Ha $n = 3$, a Gömbpakolási korlátból azt kapjuk, hogy legalább 4 tippre van szükségünk a biztos 2 találathoz. Tegyük fel, hogy ennyi elég.

Ebben az esetben minden gömb 7 vektort tartalmaz. 4 gömbbel tehát maximum 28 vektor fedhető le. Mivel $|\mathbb{Z}_3^3| = 27$, csak egy olyan vektor lehet, ami két gömb közös eleme. Nézzük meg, hogy létezhet-e két olyan gömb, melyek metszete pontosan egy vektort tartalmaz.

Vegyük az (a, b, c) vektort, legyen ez az egyik gömb középpontja. A másik gömb középpontja vagy (a', b, c), vagy (a', b', c), vagy (a', b', c') lehet ($a \neq a'$ stb.). Ha (a', b', c') a másik középpont, nem lehet közös elemük a gömböknek, mert az egyik gömb vektorai egy darab ’-vel jelölt koordinátát tartalmazhatnak maximum, a másik gömbben lévőek pedig minimum kettőt.

(a, b, c) és (a', b', c) középpontok esetén, (a', b, c) és (a, b', c) is közös eleme a gömböknek. (a, b, c) és (a', b, c) esetén pedig közösek az (a', b, c) és az (a, b, c) vektorok. Nem létezik tehát két olyan gömb, aminek pontosan egy közös eleme van.

A feladat tehát csak 4 darab diszjunkt gömbbel lenne megoldható. $\mathbb{Z}_3^3$-ban azonban a Hamming-korlátból következően maximum 3 diszjunkt gömb létezhet. Ezzel

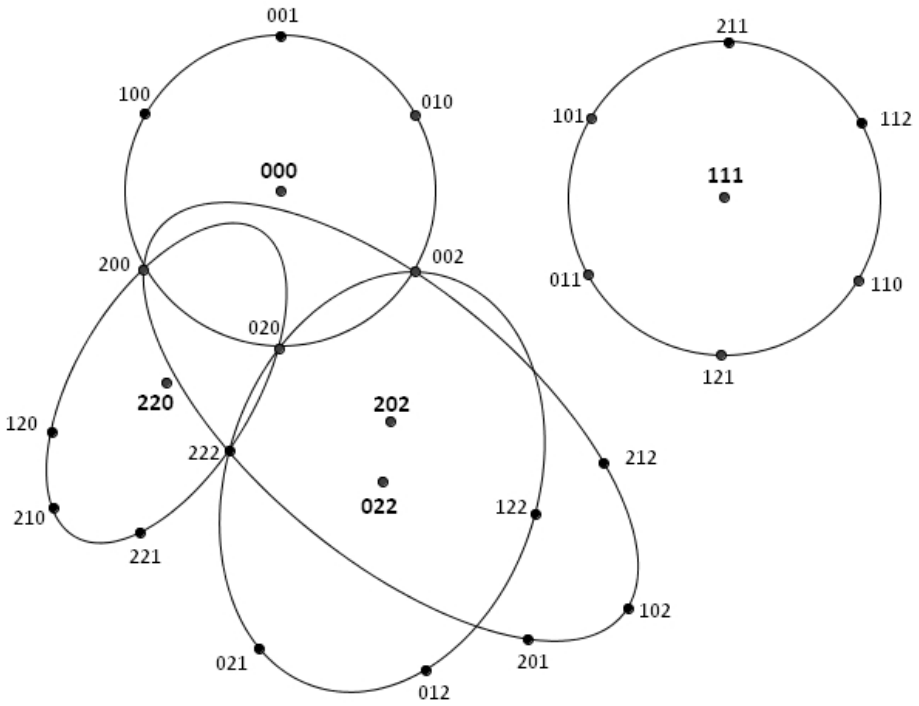
beláttuk, hogy négy gömbbel nem fedhető le a vektortér, vagyis négy szelvény nem elég a biztos 2 találathoz.

□

A következő 5 tippel azonban biztos 2 találatot érhetünk el:

$$000, 111, 220, 202, 022$$

Az alábbi ábra szemlélteti, hogy az 5 tipp köré írt 1-sugarú gömbök valóban lefedik a teret.



3. ábra

5.4 Feladat: Lássuk be a vegyes esetre vonatkozó Gömbpakolási korlátot!

Legyen n_1 azon mérkőzések száma, ahol 3 esélyt játszunk meg, n_2 pedig, ahol 2 kimenetellel számolunk. Ekkor összesen $2^{n_2}3^{n_1}$ féle különböző szelvény tölthető ki. Tekintsük úgy a vektorokat, hogy az első n_2 koordináta 2-féle lehet, a többi n_1 koordináta pedig 3-féle.

Egy adott tipptől 1-távolságra $n_2 + n_1 \cdot 2$ vektor van, mert vagy az első n_2 koordinátában térek el 1-féleképpen, vagy a többiben 2-féleképpen.

Nézzük most azokat a vektorokat, melyek 2-távolságra vannak egy adott vektortól. $\binom{n_2}{2}$ darab olyan vektor létezik, amely az első n_2 helyen kétszer tér el, $\binom{n_1}{2} \cdot 2^2$ olyan, ami az utolsó n_1 helyen tér el kétszer, és $n_2 \cdot n_1 \cdot 2$ olyan, ami az elején és a végén is eltér egyszer. 2-távolságra tehát $\binom{n_2}{2} + \binom{n_1}{2} \cdot 2^2 + n_2 \cdot n_1 \cdot 2$ darab vektor van egy adott vektortól.

Ezt általánosítva kapjuk, hogy egy adott vektortól j-távolságra $\sum_{i=0}^{j} \binom{n_2}{i} \binom{n_1}{j-i} 2^{j-i}$ vektor van.

Egy r-sugarú gömb $\sum_{j=0}^{r} \sum_{i=0}^{j} \binom{n_2}{i} \binom{n_1}{j-i} 2^{j-i}$ vektort tartalmaz, mert benne van a középpont és a tőle $1,2, \dots, r$ távol lévő pontok. Ha le akarjuk fedni az egész vektorteret $|C| \geq \frac{2^{n_2} 3^{n_1}}{\sum_{j=0}^{r} \sum_{i=0}^{j} \binom{n_2}{i} \binom{n_1}{j-i} 2^{j-i}}$ tippvektorra van szükségünk.

□

5.5 Feladat: Lássuk be, hogy a 6 meccses totó esetén az $111111, 222222$, 000000, 211111, 011111, 122222 tippekkel biztos elérünk 3 találatot!

Az olyan vektorokat, melyeknek legalább 3 koordinátája azonos, lefedi az első 3 tippvektor közül legalább az egyik. Csak azokkal a vektorokkal kell foglalkoznunk, amelyekben mindhárom lehetséges számjegy kétszer szerepel.

Vizsgáljuk meg ezen vektorokat az első koordinátájuk szerint. Ha 1-gyel kezdődik, akkor az 122222 köré írt 3-sugarú kör lefedi, mert szerepelni fog még két darab kettes, ha 2-vel kezdődik, jó a 211111 tipp, ha 0-val, akkor pedig a 011111 tippvektor.

□

5.6 Feladat: Lássuk be, hogy a ternér Golay-kód 2 hibát javít!

Meg kell mutatni, hogy a kódszavak köré írt 2-sugarú gömbök diszjunktak, vagyis tetszőleges $v, w \in C \subset \mathbb{Z}_3^{11}$ esetén $d(v, w) \geq 5$.

Kódunkat úgy definiáltuk, hogy az első 6 koordináta tetszőleges, a többi 5 pedig már egyértelműen kiszámítható egy egyenletrendszerrel. Ha tehát két vektor első hat koordinátában megegyezik, akkor azonosak. Az első hat koordináta változtatását kell csak vizsgálnunk.

Ha 5 vagy 6 koordinátát változtatunk meg, nyilván minimum 5 lesz a távolság. Azt kell tehát megvizsgálnunk, hogy, ha az első hat koordinátából 1-et, 2-t, 3-at, vagy 4-et megváltoztatunk, változik-e az utolsó 5 koordináta közül minimum $4, 3, 2$, vagy 1.

A továbbiakban legyen $i = 1,2, \dots ,6$ és $j = 7,8, \dots ,11$, és nézzük a 4.2.2.-ben megadott geometriai modellt. Mivel minden x_i legalább négy egyenletben tagként szerepel, pontosan egy x_i megváltoztatásával minimum négy x_j értéke változik meg.

Ha két különböző x_i-t megváltoztatunk, több esetet kell végiggondolnunk. Változzon x_1 és x_k $(k = 2,3,4,5,6)$. Ekkor az 5 egyenletből egyben csak x_1, kettőben $x_1 + x_k$, kettőben pedig $x_1 + 2x_k$ fog szerepelni. Ezek a tagok pedig 3 különböző maradékosztályban lesznek modulo 3. Ezért az öt utolsó koordinátából legalább három biztosan más maradékosztályba fog kerülni, mint volt.

Vegyünk két x_k, x_l $(k, l = 2,3,4,5,6$ és $l \neq k)$ koordinátát, vagyis az ötszögem $2,3,4,5,6$ csúcsa közül kettőt. Ha ezek szomszédosak, akkor a két tag a következőképpen szerepel az öt egyenletben: x_k, x_l, $2x_k + 2x_l$, $2x_k + x_l$, $x_k + 2x_l$. Hiszen ha közülük az egyik csúcs szerint írjuk fel az egyenletet, akkor az adott koordináta nem szerepel az egyenletben, a másik koordinátát pedig hozzáadjuk. Ha az egyikkel sem szomszédos csúcs szerint definiáljuk az egyenletet, akkor mindkét koordináta értékét kivonjuk. Ha pedig egy olyan csúcs szerint írjuk fel, mely az adott csúcsok közül csak az egyikkel szomszédos, akkor az egyik koordináta értékét hozzáadjuk, a másikét kivonjuk.

Ha x_k és x_l nem szomszédosak, akkor az egyenletekben a $2x_k$, $2x_l$, $x_k + x_l$, $2x_k + x_l$, $x_k + 2x_l$ tagok szerepelnek. Ez a fenti módon belátható.

Mindkét fent említett esetben x_k, x_l $(k, l = 2,3,4,5,6$ és $l \neq k)$ értékének megváltoztatásával legalább három x_j $(j = 7,8, \dots ,11)$ megváltozik, hiszen az első esetben x_k, x_l a másodikban $2x_k$, $2x_l$ tagok miatt az egyenletek eredményei más maradékosztályba kerülnek, mint voltak, a többi három-három tag közül pedig legalább egy értéke változik modulo 3.

Ha három koordinátát változtatunk meg, a következő eseteket kell meggondolnunk:

1) az egyik csúcs az 1 csúcs, a másik kettő szomszédos;
2) az egyik csúcs az 1 csúcs, a másik kettő nem szomszédos;
3) három egymást követő csúcs és egyik sem az 1 csúcs;
4) két csúcs szomszédos, a harmadik egyikkel sem szomszédos, és egyik sem az 1 csúcs.

Legyenek a megváltoztatott koordináták $x_k,\ x_l, x_m$. Az egyenletekben szereplő tagok a különböző esetekben a következők:

Esetek/ egyenletek	**1.**	**2.**	**3.**	**4.**	**5.**
1)	$x_1 + x_l$	$x_1 + x_m$	$x_1 + 2x_l + 2x_m$	$x_1 + 2x_l + x_m$	$x_1 + x_l + 2x_m$
2)	$x_1 + 2x_l$	$x_1 + 2x_m$	$x_1 + x_l + x_m$	$x_1 + 2x_l + x_m$,	$x_1 + x_l + 2x_m$
3)	$x_k + 2x_l$	$x_l + 2x_m$	$x_m + 2x_k$	$x_k + 2x_l + 2x_m$	$2x_k + 2x_l + x_m$
4)	$x_k + 2x_l$	$x_m + 2x_l$	$2x_k + 2x_m$	$x_k + 2x_l + x_m$,	$2x_k + x_l + x_m$,

Elemi számolással belátható, hogy minden esetben legalább 2 egyenlet eredménye meg fog változni.

Ha négy koordinátát változtatunk meg a következő három eset lehetséges:

1) az egyik csúcs az 1 csúcs, az ötszögből kimaradt kettő szomszédos;
2) az egyik csúcs az 1 csúcs, az ötszögből kimaradt két csúcs nem szomszédos;
3) egyik csúcs sem az 1 csúcs, az ötszögemből egy csúcs maradt ki

Legyenek a megváltoztatott koordináták $x_k,\ x_l,\ x_m$ és x_n. Az egyenletekben szereplő tagok a különböző esetekben a következők:

	1.	2.	3.	4.	5.
1)	$x_1 + x_k + 2x_l$	$x_1 + x_m + x_l$	$x_1 + 2x_k + x_m$	$x_1 + 2x_k + x_l + 2x_m$	$x_1 + 2x_k + 2x_l + x_m$
2)	$x_1 + x_k + 2x_l$	$x_1 + x_m + 2x_l$	$x_1 + x_k + x_l + 2x_m$	$x_1 + 2x_k + 2x_m$,	$x_1 + 2x_k + x_l + x_m$
3)	$2x_n + x_k + 2x_l$	$2x_n + x_m + x_l$	$x_n + x_k + 2x_m$	$2x_m + 2x_k + x_l$	$x_n + 2x_k + 2x_l + x_m$

Meggondolható, hogy a fenti táblázat minden sorában legalább egy összefüggés értéke megváltozik, ha négy változót megváltoztatunk.

Ezzel beláttuk, hogy az első hat közül n darab koordináta megváltoztatása, legalább további $5 - n$ koordináta megváltoztatását vonja maga után.

□

Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek, Kiss György egyetemi docensnek, a tanításért, irányításért és a matematikai problémák feldolgozásában nyújtott segítségéért.

Bibliográfia

[1.] *Kiss György, Szőnyi Tamás*: Véges geometriák, Polygon, Szeged, 2001: 1., 4., 13. fejezet

[2.] *Kiss György*: Hogyan nyerjünk a TOTÓ-n?, KöMaL, 2007. május

[3.] *Hraskó András, Szőnyi Tamás*: Hibajavító kódok, in: Hraskó András: Új matematikai mozaik, Typotex, Budapest, 2002. 139-170.

[4.] *H. Hämäläinen, I. Honkala, S. Lytsin, P. Östergøard*: Football Pools – A Game for Mathematicians, in: American Math. Monthly, 1995. augusztus, szeptember, 579-588.

[5.] *Freud Róbert*: Lineáris algebra, ELTE Eötvös Kiadó, Budapest, 2007.

[6.] *Lovász László, Pelikán József, Vesztergombi Katalin*: Diszkrét matematika, Typotex, Budapest, 2010.

[7.] *P. J. Cameron, J. H. van Lint*: Designs, Graphs, Codes and their Links, Cambridge University Press, 1991.

[8.] http://www.sztaki.hu/~keri/codes/index.htm

[9.] http://www.cs.elte.hu/~szonyi/Golay.pdf