Eötvös Loránd Tudományegyetem
Természettudományi Kar

---

Alekszievv Rita Antónia
Matematika BSc
Alkalmazott matematikus szakirány

# Golay-kódok

Szakdolgozat

Témavezető: Szőnyi Tamás
Számítógéptudományi Tanszék


Budapest, 2015.

# Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek, Szőnyi Tamásnak, hogy elvállalta a konzulensi teendőket. A készülő munka többszöri figyelmes átolvasásával, hasznos formai és tartalmi tanácsaival nagy segítséget nyújtott a szakdolgozat írásában. Köszönöm továbbá Héger Tamásnak, hogy észrevételeivel segítette a munkámat.

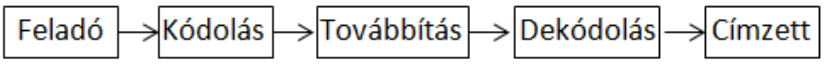
# Tartalomjegyzék

# Előszó

A hibajavító kódolás a lineáris algebra egyik hasznos és érdekes alkalmazása. Jelen dolgozat célja, hogy általánosságban bemutassa a hibajavítás alapjait, majd részletesen tárgyaljon egy példát: a Golay-kódokat. A bináris Golay-kódnak hat, a ternér Golay-kódnak három különböző előállítását mutatom be részletes bizonyításokkal együtt. A dolgozat ezen kívül kitér az algebrai kódok és a blokkrendszerek kapcsolatára is.

# 1. A kódokról általában

A kommunikációban a **kódolás** egy olyan eljárás, amely során a feladó az információt adattá alakítja, amelyet aztán valamilyen csatornán keresztül elküld a vevőnek. A vevő ezután **dekódolja** a kódolt adatot, azaz visszaállítja értelmezhető információvá.




Az üzenet útja a feladótól a címzettig

Kódolás használatának egyik tipikus oka az, hogy a csatorna, amelyen a két ember (vagy gép) kommunikál, nem alkalmas kézírás, kép vagy hang átvitelére. A matematikában a kódok többféle célt szolgálnak. A kódolás egyik célja lehet, hogy a kommunikáló feleken kívül más ne értse, amit egymással közölni akarnak. Ilyenkor *titkosítás*ról beszélünk. Ha minél kevesebb adat átvitelével szeretnénk az információt célba juttatni, ezt *tömörítés*sel érjük el. A *hibajavítás* az adó és a vevő közötti átvitel folyamán a zaj vagy egyéb zavar okozta rendellenességek miatti torzulások javítása.

# 2. Alapfogalmak

**2.1. Definíció.** *Ahhoz, hogy üzenetet tudjunk továbbítani, szükségünk van egy* $q(<<\infty)$ *elemszámú* $Q$ ***ábécé****re. A* $Q$ *elemeiből álló véges sorozatokat* ***szavak****nak nevezzük.* $V = Q^n = \{(x_1, ..., x_n) | x_i \in Q \ \forall i = 1, ..., n\}$ *a* $Q$ *elemeiből álló,* $n$ *elemű sorozatok halmaza.* $V$ *két elemének (*$x$ *és* $y$*)* ***Hamming-távolság****át* $d(x, y)$*-nal jelöljük, és a két sorozat különböző tagjainak számát értjük rajta. Legyen* $C \subseteq V$*. Ekkor* $C$*-t* ***kód****nak,* $C$ *elemeit* ***kódszavak****nak nevezzük,* $n$ *a kód* ***hossz****a. A* $C$ *kód* ***minimális távolság****a* $d = \min\{d(c, c') : c, c^{'} \in C, c \neq c^{'}\}$*, azaz a különböző kódszavak közötti Hamming-távolságok minimuma. Egy* $x$ *szóra és* $r$ *természetes számra az* $x$ *középpontú,* $r$ *sugarú* ***gömb (Hamming-gömb)*** *a következő halmaz:* $B(x, r) = \{y \in V | d(x, y) \leq r\}$*. [9]*

Nagyon gyakran előfordul, hogy a kódolt üzenetek 0-1-sorozatok, hiszen ezt elektromos berendezéssel könnyű megvalósítani (folyik áram – nem folyik áram). Ugyancsak gyakori, hogy egy-egy üzenet hossza valamilyen műszaki okból rögzítve van, ezt használtuk a fenti definícióban is.

A továbbiakban több helyen használni fogunk véges testeket. Az ilyenek elemszáma mindig prímhatvány, továbbá minden prímhatványra pontosan egy véges test létezik, aminek ő az elemszáma. A $q = p^\alpha$ elemű véges testet a továbbiakban $GF(q)$-val fogom jelölni.

**2.2. Definíció.** *Ha $Q = GF(q)$, akkor $Q^n = V(n, q)$ az $n$ dimenziós vektortér $GF(q)$ felett. Ennek a lineáris altereit* ***lineáris kód****nak nevezzük. Egy kódszó* ***súly****a a nullától különböző koordinátáinak száma. Ha a kód lineáris, akkor a kód minimális távolsága a csupa nulla sorozattól számított legkisebb távolság, hiszen a kódhoz egy tetszőleges kódszót hozzáadva visszakapjuk a kódot. Lineáris kódok esetén tehát a minimális távolság megegyezik a minimális súllyal, mert a Hamming-távolság az eltolásokra nézve invariáns. Ha $C$ egy $k$ dimenziós altér, és a minimális súlya $d$, akkor $C$-t $[n, k, d]_q$ kódnak nevezzük. Ha $C$ nem lineáris, akkor a kódszavak $M = |C|$ számát tüntetjük fel, a minimális súly helyett pedig a minimális távolságot, így ilyenkor $(n, M, d)_q$ kódról beszélünk. Ha a minimális súlyt vagy a minimális távolságot nem ismerjük, akkor szokásos az $[n, k]_q$ és az $(n, M)_q$ jelölés. [9]*

A Hamming-távolság bizonyos szempontból hasonlít a geometriai távolságra:

- szimmetrikus,
- nemnegatív, és $d(x, y) = 0$ akkor és csak akkor lehet, ha $x = y$,
- teljesül a háromszög-egyenlőtlenség, azaz $\forall x, y, z \in V : d(x, z) \leq d(x, y) + + d(y, z)$.

Az előzőekből következik, hogy ha két szó távolsága nagyobb $2r$-nél, ahol $r$ természetes szám, akkor a szavak $r$ sugarú gömbjei diszjunktak

# 3. Hibajavítás

A hibajavító kódolás célja az, hogy a fogadó fél akkor is értelmezni tudja az üzenetet, ha az valamilyen zavar vagy zaj hatására a továbbítás során megváltozott.

Azokban az esetekben, amikor a küldő képes a küldött üzenetet vagy annak egy részét ismételten elküldeni, elég detektálni a hibát. Ilyenkor a címzett felismeri, hogy nem az eredeti üzenetet kapta meg, és újraküldést kér.

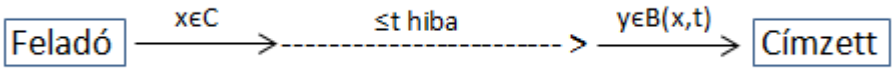
**Példa**( [8] alapján): Számítógépünk két részegysége kábellel van összekötve, ezen keresztül küldenek adatokat egymásnak. Legyen a továbbítandó üzenet a $\mathbf{c} = = (c_1, ..., c_{n-1})$ bináris vektor. Számítunk rá, hogy valamelyik 0 vagy 1 megváltozik

(például mert bekapcsoljuk a porszívót), ezért a részegységek egy $c_n = \sum_{i=1}^{n-1} c_i$ **paritásbit**et illesztenek az üzenet végére. Így egy olyan $C$ kódot kapunk, amelyben minden kódszó páros darab 1-est tartalmaz, azaz minden $c = (c_1, \cdots c_{n-1}, c_n) \in C$ kódszóra teljesül, hogy $c_1 + \cdots + c_n \equiv 0 \mod 2$. Ha egyetlen helyen változott meg az üzenet, akkor a sorozatban szereplő egyesek száma eggyel változik, azaz páratlan sok egyes lesz az $n$ elem között. Ekkor a fogadó részegység jelzést küld az adónak, hogy küldje újra az üzenetet.

Ugyanezt megtehetjük másmilyen ábécé felett: az utolsó bit olyan legyen, hogy a kódszóban a koordináták összege nulla legyen. Az ötletet általánosan is alkalmazhatjuk, egyetlen paritásbit helyett több paritásbitet (pl. a koordináták valamilyen lineáris kombinációját) is hozzáfűzhetünk az üzenethez.

Az adatok újraküldésére azonban nem minden esetben van lehetőség. Például, amikor egy űrhajóról képeket akarnak küldeni a Földre, akkor ezeket elektromos impulzusokká alakítják, és így továbbítják őket. Az elküldött üzenet azonban zaj hatására eltorzulhat az űrben, az esetleges hibákat pedig a fogadó félnek kell visszaállítania.

Gondolhatunk arra is, hogy az adatok átvitele mondjuk telefonvonalon történik, de ott hálózati zavar, recsegés következhet be, vagy egyéb üzenetek részei hozzákeveredhetnek. Ugyanez a helyzet, ha rádióhullámmal történik az adatátvitel.




Az üzenet meghibásodása

A probléma megoldásának alapkoncepciója az, hogy egymástól nagyban különböző kódszavakat választunk. Így lehetetlen összekeverni őket, ha csak kis mértékben változtak meg. Ha tehát a fogadó olyan szót vesz, amely nem kódszó, akkor a dekódolás során megkeresi a hozzá - valamilyen szempontból - legközelebb eső kódszót, és azt tekinti beérkezett üzenetnek. Persze ahhoz, hogy a kódszavak megfelelő mértékben eltérhessenek egymástól, redundánssá kell tennünk őket, tehát hosszabb üzeneteket kell közvetítenünk. Minél hosszabb üzeneteket küldünk, annál több hibát tudunk javítani, de annál több hiba is keletkezhet. Ugyanígy, adott kódhossz mellett egy jó kódnak egyszerre kell sok kódszót tartalmaznia és sok hibát javítania. A kódelmélet alapproblémája, hogy minél rövidebb kóddal és minél több kódszóval minél

több hibát javítsunk. Ezek egymásnak ellentmondó célok, így a kompromisszumot a konkrét feladatnak megfelelően kell megkeresni.

**3.1. Definíció.** *Egy lehetséges dekódolás, amelyet* ***maximum likelihood****nak neveznek, azon $x$ üzenet megtalálása, melyre a legnagyobb a valószínűsége, hogy a beérkezett $y$-t kapjuk. Ez a módszer tehát adott $y$-ra a*

$$P(y \text{ a beérkezett üzenet} \mid x \text{ az elküldött üzenet})$$

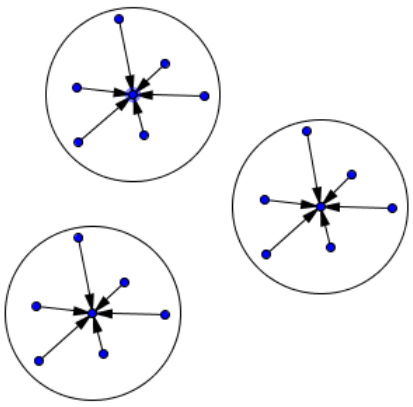
*valószínűséget maximalizálja (ezért legnagyobb valószínűség elvének is nevezik). [10]*

**3.2. Definíció.** *A* ***minimum distance decoding****nak nevezett dekódolás azt az $x$ kódszót keresi, amelynek a beérkezett szótól vett Hamming-távolsága a lehető legkisebb. [10]*

Ezt a dekódolást akkor értelmes használni, ha feltehetőek a következők:

1. minden koordináta ugyanolyan valószínűséggel romlik el,
2. a hibák egymástól függetlenek: egy hiba nem befolyásolja a szó többi karakterét.

Ha ezen felül még az is teljesül, hogy egy adott helyen $p < \frac{1}{2}$ valószínűséggel történik hiba, akkor a minimum distance decoding éppen megfelel a legnagyobb valószínűség elvének, hiszen $\mathrm{P}(y \text{ a beérkezett üzenet} \mid x \text{ az elküldött üzenet}) = \prod_{i=1}^{n} \begin{cases} 1-p & \text{ha } x_i = y_i \\ p & \text{ha } x_i \neq y_i \end{cases} = (1-p)^{n-d}p^d = (1-p)^n(\frac{p}{1-p})^d$, ahol $d = d(x,y)$. Ez a kifejezés akkor maximális, ha $x$ olyan, amire $d$ a lehető legkisebb, hiszen $\frac{p}{1-p} < 1$.



Dekódolás

A fenti feltételek nem teljesülnek például egy DVD esetében: ekkor ha hiba történik (a lemez szennyeződik vagy megkarcolódik), akkor egyszerre keletkezik sok egymásutáni hiba is.

**3.3. Definíció.** *A $C$ kód **t-hibajelző**, ha $\forall x \in C, y \in B(x,t)$ esetén a címzett $y$-ból meg tudja állapítani, hogy $y \in C$ vagy sem. $C$ **t-hibajavító**, ha $\forall x \in C$, $y \in$ $\in B(x,t)$ esetén a címzett $y$-ból meg tudja állapítani, hogy mi az $x$. Tehát minden, $x$-től legfeljebb $t$ helyen különböző szóhoz pontosan egy legközelebbi kódszó létezik, és ez $x$.*

**Példa:** A 3. oldalon szereplő paritásbit egy hibát jelez, de egyet sem javít: ha olyan szót kaptunk, amelyben a koordináták összege nem nulla, és a szó legfeljebb $t = 1$ koordinátájában romolhat el, akkor tudjuk, hogy nem a küldött szót kaptuk. Ebből azonban még nem tudunk következtetni arra, hogy pontosan melyik koordináta változott meg az üzenet továbbítása során. Ha a koordináták összege nulla, az csak úgy lehet, hogy páros sok helyen módosult a szó. Ha tehát $t = 1$, akkor biztosan az eredeti üzenetet kaptuk meg.

**3.0.1. Állítás.** *(i) Egy $d$ minimális távolságú kód $d-1$ hibát képes jelezni. (ii) A $t$-hibajavítással ekvivalens tulajdonság: $d \geq 2t+1$.*

*Bizonyítás.* (i) Ha $x$ kódszó továbbítása során $t$ hiba keletkezik, akkor olyan $x'$ szót kapunk, amire $d(x,x') = t$. Ha $t < d$, akkor olyan szót kaptunk, ami nem lehet kódszó, tehát a hibát detektáltuk.

(ii) Ha $d > 2t$, akkor a kódszavak körüli $t$ sugarú gömbök diszjunktak: ha lenne egy $u$ szó, ami benne van két különböző kódszó ($x$ és $y$) $t$ sugarú gömbjében, akkor a háromszög-egyenlőtlenség miatt $2t \geq d(x,u) + d(u,y) \geq d(x,y) \geq 2t+1$ adódna, ami ellentmondás. Tehát minden szóhoz egyértelmű az a kódszó, amiből őt legfeljebb $t$ koordináta megváltoztatásával kaptuk. □

# 4. Perfekt kódok

A Hamming-távolság és a geometriai távolság hasonlósága miatt a kódelmélet gyakran az $n$-dimenziós gömbök modelljét használja. A $t$-hibajavító tulajdonságot úgy is megfogalmazhatjuk, hogy a kódszavak köré írt $t$ sugarú gömbök diszjunktak, azaz

minden szó legfeljebb egy ilyen gömbnek az eleme. Ebből megkapható a **Hamming-korlát** [9], vagy más néven a gömbkitöltési korlát, mely a kód paraméterei között határoz meg összefüggést, és korlátot ad a kódszavak számára:

**4.0.2. Tétel.** *Ha egy GF(q) test feletti $(n, M, d)$ kód $t$ hibát javít, akkor*

$$M \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n.$$

*Bizonyítás.* $M$ darab kódszó van, mindegyikhez $\binom{n}{i}$ hely, ahol tőle $i$ helyen különbözhet egy szó. Ezekere a helyekre a kódszó megfelelő elemétől különböző karaktert kell írnunk, ami $q-1$-féle lehet. Azaz összesen $\binom{n}{i}(q-1)^i$ szó van egy adott kódszóhoz, amely tőle $i$ helyen különbözik. Így a bal oldalon lévő kifejezés a $t$ sugarú gömbökben lévő vektorok számát adja meg. Mivel ez nem haladhatja meg a tér számosságát, ezért az egyenlőtlenség fennáll. □

A $Q^n$ teret egy nagy gömbnek tekintve, szemléletesen az a célunk, hogy minél több $t$ sugarú golyót helyezzünk bele, azaz minél kevesebb „hely" maradjon kitöltetlenül. Optimális esetben ezek a kisebb gömbök hézagmentesen lefedik a teret.

**4.1. Definíció.** *A C kódot **perfekt**nek nevezzük, ha eléri a Hamming-korlátot.*

Ha ismerjük egy kód paramétereit, akkor automatikusan adódik, hogy perfekt-e. Perfekt $t$-hibajavító kód esetén minden $y$ szóhoz van tőle legfeljebb $t$ Hamming-távolságra kódszó. Ebből következik, hogy a kódszavak körüli $t$ sugarú gömbök diszjunkt uniója éppen $Q^n$. Ez azt is jelenti, hogy ha egy kódszó $t$-nél több helyen romlik el a továbbítás során, akkor a beérkezett szót biztosan rosszul fogjuk dekódolni.

Triviális példát könnyű adni perfekt kódra: az egyetlen kódszóból álló, illetve az összes $Q^n$-beli szót használó kód is ilyen. Ezek a gyakorlatban természetesen használhatatlanok.

A legegyszerűbb sok hibát javító perfekt kód az ismétlés-kód: az elküldött adatok bitsorozatát bitek blokkjaira tördelik, és küldésnél minden blokkot egy előre megadott számszor újraküldenek. Például, úgy küldjük el az „1011" bitsorozatot, hogy minden bitet háromszor küldünk el. Tegyük fel, hogy elküldtük az „111 000 111 111" sorozatot, amit „110 101 111 111" sorozatnak veszünk. Mivel van olyan csoport, amelyben nem csak 1 vagy csak 0 szerepel, megállapítható, hogy az átvitel hibás volt.

**4.2. Definíció.** *Az (1,...,1) által generált egydimenziós lineáris kódot* $[n,1,n]$ ***ismétléskód****nak nevezzük.*

Ez a kód $\lfloor n/2 \rfloor$ hibát képes javítani, azaz páratlan $n$-re perfekt.

A Hamming-korlátból és a perfektségből következik a következő összefüggés:

**4.0.3. Állítás.** *Ha létezik $n$ hosszú, perfekt, $t$-hibajavító kód $q$ elemű ábécé felett, akkor $\sum_{i=0}^{t}\binom{n}{i}(q-1)^i$ osztója $q^n$-nek. Ha $q=p^\alpha$ prímhatvány is, akkor $\sum_{i=0}^{t}\binom{n}{i}(q-1)^i = q^a$ is teljesül, azaz a $t$ sugarú gömbök elemszáma nemcsak $p$-hatvány, hanem $q$-nak is hatványa.*

*Bizonyítás.* A perfekt kódok elérik a Hamming-korlátjukat, azaz az $M\sum_{i=0}^{t}\binom{n}{i}(q-1)^i = q^n$ egyenlőség teljesül. Mivel $M$ a kódszavak száma, ezért egész, tehát $\sum_{i=0}^{t}\binom{n}{i}(q-1)^i$ osztója $q^n$-nek. Legyen $a$ az a legnagyobb kitevő, amelyre $q^a$ osztója az előbbi összegnek, azaz

$$\sum_{i=0}^{t}\binom{n}{i}(q-1)^i = 1+n(q-1)+\binom{n}{2}(q-1)^2+...+\binom{n}{t}(q-1)^t = p^\lambda q^a,$$

ahol $p^\lambda < q$. Ebből $n$-et kifejezve a következőt kapjuk: $n = \frac{p^\lambda q^a - \sum_{i=2}^{t}\binom{n}{i}(q-1)^i - 1}{q-1} =$ $= \frac{p^\lambda q^a-1}{q-1} - \frac{\sum_{i=2}^{t}\binom{n}{i}(q-1)^i}{q-1} = p^\lambda\frac{q^a-1}{q-1} + \frac{p^\lambda-1}{q-1} - \sum_{i=2}^{t}\binom{n}{i}(q-1)^{i-1}$. Az egyenlőség jobb oldalának az első tagja egész, mert egy prímhatvány szorzata egy egészekből álló mértani sorozat első néhány tagjának összegével. A harmadik tag is egész, és az egyenlőség bal oldala is, ebből következik, hogy az összeg középső tagjának is egésznek kell lennie. Ez csak úgy lehetséges, ha $\lambda = 0$. □

# 5. Lineáris kódok

Emlékeztetőül: A $C$ kód **lineáris**, ha $Q$ a GF($q$) véges test, és $C$ lineáris altere a $V(n,q)$ GF($q$) fölötti $n$ dimenziós vektortérnek. Az altér dimenzióját $k$ jelölte.

A lineáris kódok egyik előnye, hogy $d$ meghatározásához nem kell mind az $\frac{1}{2}q^k(q^k-$ $-1)$ darab távolságot megvizsgálnunk, elég a kódszavak súlyát nézni. Továbbá, mivel a kód egy lineáris altér, ezért a megadásához nem kell minden kódszót felsorolni, elegendő egy bázist.

**5.1. Definíció.** *Ha egy $C$ lineáris $[n,k]_q$-kód bázisának elemeit egy mátrix soraiba írjuk, akkor a $C$ kód egyik* ***generátormátrixát*** *kapjuk. Ez tehát egy $k\times n$-es mátrix.*

A $G$ generátormátrix rangja $k$, hiszen a sorai lineárisan függetlenek. Mivel $C$ elemei a $G$ sorainak lineáris kombinációi, ezért egy $GF(q)$ fölötti $k$ hosszú üzenet *kódolás*a a mátrixszal való jobbról szorzás: $u \mapsto uG$.

**Példa:** Egy egyszerű, bináris paritásbit, amely a $G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ generátormátrixszal van megadva, az $(u_1, u_2) \mapsto (u_1, u_2, u_1 + u_2)$ leképezéssel kódol.

Ha el akarjuk dönteni, hogy egy $w \in GF_q^n$ szó hozzátartozik-e a $C$ kódhoz, akkor a $w = xG$ egyenletet kellene megoldanunk. Erre azonban létezik egyszerűbb módszer, ha ismerjük $C$ ortogonális kiegészítőjét.

**5.2. Definíció.** *A $C$ kód **duálisa** a $C^\perp = \{w \in V : (w, x) = 0, \forall x \in C\}$ kód, ahol $(.,.)$ a szokásos skaláris szorzás: $x = (x_1, \ldots, x_n)$ és $y = (y_1, \ldots, y_n)$ skaláris szorzata $(x, y) = \sum_{i=1}^{n} x_i y_i$. $H$ a $C$ kód **ellenőrző mátrix**a, ha $C^\perp$-nek egy generátormátrixa.*

A definíció alapján $H$ sorai ortogonálisak a kódszavakra, sőt, $C^\perp$-nek egy bázisát alkotják, azaz $C$ elemei éppen azok az $x$ vektorok, amelyekre $xH^\top = 0$ teljesül.

**5.0.4. Állítás.** *Ha egy $n$ hosszú, $k$ dimenziós lineáris kód generátormátrixa $G = \begin{pmatrix} I_k & A \end{pmatrix}$ alakú, akkor ugyanezen kód ellenőrző mátrixa megadható a következő alakban: $H = \begin{pmatrix} -A^\top & I_{n-k} \end{pmatrix}$. [9]*

*Bizonyítás.* $H$ a duális kódot generálja, mert $GH^\intercal$ $i$. sorának $j$. eleme $-a_{ij} + a_{ij} = 0$, azaz $GH^\intercal = 0$, és a $H$ által generált lineáris kód dimenziója $n - k$. □

**Példa (Hamming-kód):** Válasszunk egy tetszőleges $m$ természetes számot, és legyen $n = \frac{q^m - 1}{q - 1}$. Az $[n, n - m]_q$ Hamming-kód olyan kód, melynek $H$ ellenőrző mátrixában a $h_i$ $(i = 1...n)$ oszlopok a $GF(q)$ test feletti $m$ hosszú nemnulla vektorok, méghozzá úgy, hogy két oszlop ne legyen egymás skalárszorosa. Ezt elérhetjük úgy, hogy pontosan azokat a vektorokat vesszük be a mátrixba, amelyeknek az első nullától különböző koordinátája 1. $H$ tehát egy $m \times n$-es mátrix, és az oszlopok permutálásával (esetleg másik bázisra áttérve) elérhető, hogy valahol legyen benne egy $m \times m$-es egységmátrix, ezért a rangja $m$. Általában bináris ($q = 2$) esetben az oszlopok pontosan az 1,2, ...,$2^{m-1}$ számok kettes számrendszerbeli alakjai. Az $[n, n - m]_q$ Hamming-kódot $Ham_q(m)$-mel, $q = 2$ esetén $Ham(m)$-mel jelöljük.

A legegyszerűbb ilyen kód a $q = 2$, $m = 3$ paraméterekkel rendelkező bináris [7, 4] kód. Ekkor az ellenőrző mátrix a

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

A **Hamming-kódok dekódolása** a következő függvény:

$$\Psi : V(q, n) \mapsto C$$

$$\Psi(y) = \begin{cases} y & \text{ha } yH^\intercal = 0 \\ y - \lambda e_i & \text{ha } yH^\intercal = \lambda h_i^\intercal, \end{cases}$$

ahol $h_i$ a $H$ mátrix $i$-edik oszlopa, $e_i$ pedig az az $n$ hosszú sorvektor, amelynek az $i$-edik koordinátája 1, a többi 0.

**1. Példa:** Ha a kételemű test feletti,

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

ellenőrző mátrixú (ahol $H$ oszlopai az 1, ..., 7 számok kettes számrendszerbeli alakjai fordított sorrendben) Hamming-kód használatakor a címzett az

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

szót kapta meg, akkor feltéve, hogy legfeljebb egy helyen történt hiba, az elküldött szót a következőképpen találhatjuk ki:

$yH^\intercal = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} = h_2^\intercal$, tehát nem $y$ az elküldött szó, és $\lambda = 1$, $i = 2$.

$\Psi(y) = y - \lambda e_i = y - 1e_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$ volt az elküldött szó.

**2. Példa:** Tekintsük a háromelemű test fölötti,

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

ellenőrző mátrixú Hamming-kódot, ahol tehát $H'$ oszlopai az 1, 3, 4, 5 számok hármas számrendszerben. Ha ezen kód használatakor a címzett az

$$y' = \begin{pmatrix} 2 & 1 & 1 & 1 \end{pmatrix}$$

szót kapta meg, akkor a dekódolás a következő: $y'H'^{\intercal} = \begin{pmatrix} 1 & 2 \end{pmatrix} = 2 \cdot h_1'^{\intercal}$ miatt $y'$ nem kódszó, és $\lambda = 2$, $i = 1$ adódik. Tehát $\Psi(y') = y' - \lambda e_i = y' - 2e_1 = \begin{pmatrix} 0 & 1 & 1 & 1 \end{pmatrix}$ volt a küldött szó, ha feltesszük, hogy legfeljebb egy helyen hibásodott meg.

A következő állítás értelmében minden kód minimális távolsága leolvasható az ellenőrző mátrixból.

**5.0.5. Állítás.** *A $C$ kód minimális távolsága pontosan akkor $d$, ha az ellenőrző mátrixban minden $d-1$ oszlop lineárisan független, de van $d$ olyan oszlop, amelyek összefüggenek. [9]*

*Bizonyítás.* A kód egy $d$ súlyú $y$ vektora $d$ oszlopra ad meg lineáris összefüggést, hiszen $yH^{\intercal} = 0$ teljesül minden kódszóra. Nincs $d$-nél kisebb súlyú szó, ez ekvivalens azzal, hogy minden $d-1$ oszlop lineárisan független. Viszont van $d$ súlyú kódszó, ez akkor és csak akkor lehetséges, ha van $d$ összefüggő oszlop. □

Az állításban adott feltételt csak látszólag egyszerű ellenőrizni. Elwyn R. Berlekamp, Robert J. McEliece és Henk C.A. van Tilborg 1978-as cikkükben megmutatták, hogy az általános lineáris kódok dekódolása és egy lineáris kód súlyainak meghatározása NP-teljes probléma.

**5.0.6. Állítás.** *A Hamming-kódok 1-hibajavító perfekt kódok.*

*Bizonyítás.* A minimális súly 3, mert $H$ bármely két oszlopa független, de van 3 összefüggő oszlop, például az $(1, 0, \dots 0)^{\intercal}$, a $(0, 1, 0, \cdots 0)^{\intercal}$ és ezek összege, az $(1, 1, 0, \dots 0)^{\intercal}$. Az 1 sugarú gömbök mérete $\sum_{i=0}^{1} \binom{n}{i}(q-1)^i = 1 + n(q-1) = = 1 + (q^m - 1) = q^m$. A kódszavak száma $M = q^{n-m}$, mert a kódot $C$-vel jelölve $C = ker(H)$ lineáris altere $V(n, q)$-nak, és $dim(C) = n - rang(H) = n - m$. A kód tehát valóban eléri a Hamming-korlátot. □

**5.0.7. Tétel** (Singleton-korlát)**.** *Ha $C$ lineáris $[n, k, d]_q$ kód,akkor $d \leq n - k + 1$. [9]*

*Bizonyítás.* Az ellenőrző mátrix $(n-k) \times n$-es, így a rangja legfeljebb $n-k$, ennél több oszlop nem lehet független. □

**5.3. Definíció.** *Ha egy lineáris kódra a Singleton-korlát egyenlőséggel teljesül, azaz $d = n - k + 1$, akkor a kódot **MDS**-nek (Maximum Distance Separable) nevezzük.*

**5.0.8. Állítás.** *MDS kód duálisa is MDS. [9]*

*Bizonyítás.* Ha $C$ egy $[n,k,d]_q$ kód, akkor $C^\perp$ egy $[n,n-k,d']_q$ kód. Azt kell belátnunk, hogy $d'=k+1$. Legyen $H$ az eredeti kód egyik ellenőrző mátrixa, amely egyben az ortogonális kód generátormátrixa. Legyenek $h_1,\ldots,h_k$ ezen mátrix sorai. Ezek lineáris kombinációi a duális kód szavai, tehát azt kell megmutatnunk, hogy bármely $\lambda_1,\ldots,\lambda_k$ együtthatókra $\sum_{i=1}^{k}\lambda_i h_i$ súlya szigorúan nagyobb $k$-nál. Először lássuk be, hogy $w(h_i)\geq k+1$ minden $i$-re 1-től $k$-ig. Tegyük fel, hogy $h_i$ súlya legfeljebb $k$. Ekkor legalább $n-k$ olyan oszlop van $H$-ban, ahol 0 áll az $i$-edik helyen. Ekkor viszont a megfelelő $(n-k)\times(n-k)$-as részmátrix determinánsa 0, azaz a sorai összefüggőek. Ez azonban nem lehetséges, mert a sorokban egy $n-k$ dimenziós altér bázisa van. Ellentmondáshoz jutottunk, tehát $w(h_i)\geq k+1$. Tetszőleges lineáris kombinációra úgy térhetünk át, hogy a $H$ helyett egy olyan generátormátrixát vizsgáljuk $C^\perp$-nek, amely első sora a kívánt lineáris kombináció. Ezzel beláttuk, hogy $C$ minimális súlya legalább $k+1$. A Singleton-korlát miatt a másik irányú egyenlőtlenség is teljesül, ebből $d'=k+1$ következik. □

# 6. Kódok módosításai

Számos módja van annak, hogy már meglévő kódok megváltoztatásával új, lehetőleg jobb tulajdonságokkal rendelkezőeket hozzunk létre. A korábban már látott paritásbit általánosítása egy egyszerű eljárás, amellyel a kódot hosszabbá tehetjük.

**6.1. Definíció.** *Ha $C$ egy $n$ hosszú kód a $GF(q)$ ábécé felett, akkor*

$$\overline{C}=\{(c_1,c_2,...,c_n,c_{n+1}):(c_1,c_2,...,c_n)\in C,\textstyle\sum_{i=1}^{n+1}c_i\equiv 0\ \ GF(q)\text{-ban}\}$$

*kód a $C$ **kibővítettje**.*

Bináris esetben ezzel az eljárással a paritásellenőrző bitet kapjuk. Szintén a bináris esetben világos, hogy ha $C$ minimális távolsága $d$, és ez páratlan, akkor $\overline{C}$-é $d+1$ lesz. A $C$ kód $H$ ellenőrző mátrixából $\overline{C}$ $H'$ ellenőrző mátrixát a következőképpen kapjuk:

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

**1. Példa:** A Ham(3) Hamming-kód ellenőrző mátrixa

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

Ebből leolvasható, hogy a kódnak olyan $y = (y_1, y_2, \ldots, y_7)$ vektorok az elemei, amelyekre $y_4 + y_5 + y_6 + y_7 \equiv 0 \mod 2$, $y_2 + y_3 + y_6 + y_7 \equiv 0 \mod 2$, illetve $y_1 + y_3 + y_5 + y_7 \equiv 0 \mod 2$ egyszerre teljesül. Ha most a fent leírtak szerint módosítjuk $H$-t, tehát a

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

ellenőrző mátrixra térünk át, akkor az új kód szavai éppen azok a 8 hosszú vektorok lesznek, amelyek első 7 koordinátája tartja az előző tulajdonságokat, és emellett még $\sum_{i=1}^{8} y_i \equiv 0 \mod 2$ is teljesül. Tehát tényleg a kibővített kódot kaptuk.

**2. Példa:** Tekintsük a $q = 3$, $m = 2$ paraméterekkel konstruált Hamming-kódot. Ennek az ellenőrző mátrixa a

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

A kódszavak pedig olyan $y = (y_1, y_2, y_3, y_4)$ vektorok, amelyekre $y_2 + y_3 + y_4 \equiv 0 \mod 3$ és $y_1 + y_3 + 2y_4 \equiv 0 \mod 3$ teljesül. A módosított kód ellenőrző mátrixa a

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

Az előző példához hasonlóan itt is megkaptuk, hogy ez éppen a kibővített kód ellenőrző mátrixa, hiszen minden kódszó egy olyan koordinátával bővül, amelyre $\sum_{i=1}^{5} y_i \equiv 0 \mod 3$ teljesül.

A kód rövidítésére szolgál a **lyukasztás**, amely néhány koordináta törlését jelenti. Ha egy $d$ minimális távolságú kódot $l$ helyen lyukasztjuk, akkor az új kód minimális távolsága legalább $d - l$ lesz.

A következő konstrukció csak lineáris kódokra vonatkozik, és függ a generátormátrixtól.

**6.2. Definíció.** *Legyen $C$ lineáris $[n, k, d]_2$-kód, $w_0 < 2d$ valamely $c_0$ kódszó súlya.*

*Permutálva a koordinátákat feltehető, hogy* $c_0 = \big(1 \dots 1 \quad 0 \dots 0\big)$. *Vetítsük* $C$*-t* $c_0$ *nulla koordinátáira, azaz írjuk be* $c_0$*-t egy mátrix első sorába, és egészítsük ki* $C$ *generátormátrixává. Ekkor a mátrix*

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

*alakú lesz.* $A$ $(k-1) \times (n-w_0)$ *méretű* $B$ *mátrix által generált kódot nevezzük a* $C$ $c_0$*-ra vonatkozó* ***reziduális kód****jának.*

**6.0.9. Állítás.** *Ha a kód, amiből kiindulunk, egy* $[n,k,d]_2$*-kód, akkor reziduális kód* $[n-w_0, k-1, d']_2$*-kód, ahol* $d' \geq d - \frac{w_0}{2}$.

*Bizonyítás.* Az első két paraméter változása a generátormátrix definíciójából következik. Az új minimális távolságot a következőképpen kapjuk. Legyen $c'$ egy kódszó a reziduális kódban. Létezik hozzá $c \in C$, amelynek ő a vetülete. Ekkor $c$ és $c_0 + c$ közül tekintsük azt, amelyre az első $w_0$ koordinátában $\frac{w_0}{2}$, vagy annál kevesebb 1-es van. Bármelyik is az, a súlya $d$-nél nagyobb vagy egyenlő. Ebből következik, hogy $c'$ súlya $\geq d - \frac{w_0}{2}$. □

# 7. Golay-kódok

A Voyager űrszondák küldetései során 24 hosszú, 3-hibajavító kódot használtak. A képet itt 800 × 800 darab 8 bites képpontra osztották. Ez egy kissé különbözik attól a kódtól, amelyet Marcel Golay mutatott be 1949-ben. Az eredeti kód szintén három hibát javít, de szavai eggyel rövidebbek. A továbbiakban a Golay-kódok egyértelműségét fogjuk igazolni.

A fejezet első fele főként a [9] jegyzetre támaszkodik. Az ebben szereplő vázlatos bizonyításokat bővítettem ki, megoldottam a hozzájuk kapcsolódó feladatokat. A tételeket, állításokat példákkal illusztráltam.

**7.1. Lemma.** *Legyenek* $x$, $y \in V(n,2)$ *olyan vektorok, amelyekre* $4|w(x)$ *és* $4|w(y)$. *Ekkor* $x+y$ *súlya pontosan akkor osztható 4-gyel, ha* $x$ *és* $y$ *ortogonális.*

*Bizonyítás.* Jelölje $c$ azon helyek számát, ahol mindkét szóban 1-es áll. Ekkor $w(x+y) = w(x) + w(y) - 2c$, és $(x,y) = c$. Mindkét állítás pontosan akkor igaz, ha $c$ páros. □

**7.1. Definíció.** *A $C$ $(n, M, d)_q$-kód* ***súlyeloszlás****a az $A_i$ $(i = 1 \dots n)$ egész számsorozat, ha minden $i$-re $A_i$ darab $i$ súlyú szó van $C$-ben.*

**7.2. Lemma.** *Tetszőleges, a 0-t tartalmazó bináris perfekt kód súlyeloszlását paraméterei meghatározzák. [7]*

*Bizonyítás.* Legyenek $C$ paraméterei $(n, M, d = 2e + 1)$. Jelöljük $A_j$-vel a $j$ súlyú kódszavak számát, a célunk ezek meghatározása a paraméterekkel. Világos, hogy $M = \sum_{i=0}^{n} A_i$. A perfektség miatt minden $x$ szó pontosan egy $C$-beli kódszótól lesz legfeljebb $e$ távolságra. Egy $i$ súlyú kódszó esetén a hozzá tartozó szavak súlya $i - e$ és $i + e$ közé esik. Jelöljük $C_{i,j}$-vel azon $i$ súlyú szavak számát, amelyek egy $j$ súlyú kódszótól vannak legfeljebb $e$ távolságra. Ekkor kétféleképpen összeszámolva az $i$ súlyú szavakat a következő rekurziót kapjuk:

$$\binom{n}{i} = C_{i,i-e}A_{i-e} + \ldots + C_{i,i}A_i + \ldots + C_{i,i+e}A_{i+e} \qquad (e \le i \le n - e).$$

A $C_{i,i-k}$ együtthatókat, amelyek tehát azt jelentik, hogy rögzített $i - k$ súlyú kódszótól hány $i$ súlyú szó van legfeljebb $e$ távolságra, a következőképp kapjuk meg: a kijelölt kódszóhoz úgy találjuk meg az összes, nála $k$-val nagyobb súlyú szót, hogy $j$ darab koordinátáját 1-ről 0-ra változtatjuk, $k + j$ koordinátáját pedig 0-ról 1-re. Így tehát $k + 2j$ távolságra lesz a kapott szó a kódszótól, és ennek legfeljebb $e$-nek kell lennie, ezért a futóindex 0-tól $\lfloor \frac{e-k}{2} \rfloor$-ig fut.

$$C_{i,i-k} = \sum_{j=0}^{\lfloor \frac{e-k}{2} \rfloor} \binom{n - (i-k)}{k+j} \binom{i-k}{j} \qquad k = e, \ldots, 0$$

A $C_{i,i+k}$ együtthatókat hasonló gondolatmenet alapján a

$$C_{i,i+k} = \sum_{j=0}^{\lfloor \frac{e-k}{2} \rfloor} \binom{i+k}{k+j} \binom{n - (i+k)}{j} \qquad k = 1, \ldots, e$$

összeg adja. Ekkor $k+j$ koordinátát állítunk 1-ről 0-ra, és $j$ darabot 0-ról 1-re. Ezen kívül tudjuk, hogy a kód tartalmazza a csupa nulla szót, tehát $A_0 = 1$, $A_1 = \ldots = A_{2e} = 0$. Ebből már minden $A_j$ kifejezhető. □

**Példa:** A Ham(3) Hamming-kód súlyeloszlására a következőt kapjuk. $A_0 = 1$, $A_1 = A_2 = 0$, hiszen $e = 1$. Most $i = 2$-re a rekurzió a következőt adja:

$$21 = \binom{7}{2} = C_{2,1}A_1 + C_{2,2}A_2 + C_{2,3}A_3 = 0 + 0 + 3 \cdot A_3,$$

azaz $A_3 = 7$. $i = 3$-ra:

$$35 = \binom{7}{3} = C_{3,2}A_2 + C_{3,3}A_3 + C_{3,4}A_4 = 0 + 1 \cdot 7 + 4 \cdot A_4,$$

amiből $A_4 = 7$ következik. Az ellenőrző mátrixból leolvasható, hogy a csupa egyesből álló szó eleme a kódnak, azaz $A_7 = 1$, továbbá az 1-hibajavítás miatt $A_5 = A_6 = 0$.

**7.0.10. Tétel.** *Nemtriviális, bináris, 3-hibajavító perfekt kódokra csak $n = 23$ lehet.*

Megjegyzés: Később látni fogjuk, hogy ezek csak a Golay-kódok lehetnek.

*Bizonyítás.* A 3 sugarú gömbben $1 + n + \binom{n}{2} + \binom{n}{3} = 2^k$ szó van. Ebből az $(n + +1)(n^2 - n + 6) = (n+1)[(n+1)(n-2)+8] = 3 \cdot 2^{k+1}$ egyenletet kapjuk. Az $(n+1)$ prímtényezős felbontásában legfeljebb 3 darab kettes lehet, mert ha $(n+1)$ osztható lenne 16-tal, akkor a 8 lenne a legmagasabb 2-hatvány, ami osztja $n^2 - n + 6$-ot. Továbbá $(n^2 - n + 6)$ 24-nek osztója kell hogy legyen, amiből $(n+1)(n-2)+8 \leq 24$, azaz $(n + 1) < 16$ következik, ami ellentmondás. Tehát ha $(n + 1)$ prímtényezős felbontását tekintjük, abban legfeljebb egy hármas és legfeljebb 3 kettes lehet, azaz osztója 24-nek. Ez alapján $n$ a következő értékek valamelyike:

- $n = 0, 1, 2$: nem tartozik hozzájuk kód,
- $n = 3$: egy szóból álló triviális kód,
- $n = 7$: ismétlés-kód,
- $n = 23$: Golay-kód.

□

**7.0.11. Tétel.** *A [23, 12, 7] bináris Golay-kódok 3-hibajavító perfekt kódok.*

*Bizonyítás.* Mivel $2^{12} \cdot (1 + 23 + \binom{23}{2} + \binom{23}{3}) = 2^{23}$, ezért a kód eléri a Hamming-korlátot, tehát perfekt. □

Mivel a bináris, 0-t tartalmazó perfekt kódok súlyeloszlását a paraméterekből ki tudjuk számolni, ezért a Golay-kódokét is. A 7.2 lemmában kapott képlet nélkül is látszik, hogy $A_0 = 1$, $A_1 = A_2 = A_3 = A_4 = A_5 = A_6 = 0$. Mivel minden 4 súlyú szó pontosan egy 7 súlyú kódszó 3 sugarú gömbjében van benne, ezért a $\binom{23}{4} = \binom{7}{3} \cdot A_7$ egyenlőség fennáll. Ebből $A_7 = 253$. Egy 5 súlyú szó vagy 7, vagy 8 súlyú kódszóhoz tartozik, ezért felírható a következő egyenlőség: $\binom{23}{5} = A_7 \cdot \binom{7}{2} + + A_8 \cdot \binom{8}{3}$, amiből azt kapjuk, hogy $A_8 = 506$. 6 súlyú szó négyféleképpen lehet

kódszó 3 sugarú gömbjében: egy 9 súlyútól különbözik 3 helyen, egy 8 súlyútól 2 helyen, egy 7 súlyútól 1 helyen, vagy egy 7 súlyútól 3 helyen (2 egyest nullára változtatunk, és egy nullát egyesre).Tehát $\binom{23}{6} = A_7 \cdot \binom{7}{2} \cdot 16 + A_7 \cdot \binom{7}{2} + A_8 \cdot \binom{8}{2} + + A_9 \cdot \binom{9}{3}$, ebből $A_9 = 0$. Ezt a gondolatmenetet folytathatnánk, de lényegében ez a 7.2 lemma rekurziója, amiből a [7] jegyzet alapján a következő súlyeloszlást kapjuk: $A_0 = A_{23} = 1, A_7 = A_{16} = 253, A_8 = A_{15} = 506, A_{11} = A_{12} = 1288$, a többi $j$-re $A_j = 0$.

Lássuk a Golay-kódok néhány konstrukcióját. Minden esetben kulcsfontosságú belátni, hogy a kód duplán páros, azaz minden kódszó súlya osztható 4-gyel, illetve hogy a kód duálisa önmaga. A linearitás általában a konstrukcióból következik. Ezen kívül minden esetben ki kell zárnunk a 4 súlyú szavak létezését. Először a kibővített Golay-kód egyértelműségét látjuk be. Ebből az utolsó koordináta törlésével (lyukasztással) kapjuk a perfekt Golay-kódot.

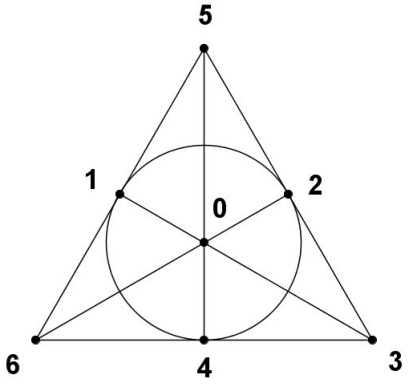
**7.2. Definíció.** *Egy $(H, \mathcal{H})$, $\mathcal{H} \subseteq 2^H$ halmazrendszert $t-(v,k,\lambda)$* ***t-rendszer****nek nevezünk, ha $|H| = v$, $\forall B \in \mathcal{H} : |B| = k$, és $H$ minden $t$ elemű részhalmazát $\mathcal{H}$-nak pontosan $\lambda$ eleme tartalmazza. $\lambda = 1$ esetén a $t$-rendszer* ***Steiner-rendszer****. $t = 2$ esetén a $t$-rendszer* ***blokkrendszer****. Ekkor $H$ elemeit pontoknak, $\mathcal{H}$ elemeit pedig blokkoknak nevezzük.*

**Példa:** Legyen $H = \{0, \dots 6\}$, és $\mathcal{H} = \{\{0;1;3\};\ \{1;2;4\};\ \{2;3;5\};\ \{3;4;6\};\ \{4;5;0\};\ \{5;6;1\};\ \{6;0;2\}\}$. Ezt a blokkrendszert Fano-síknak nevezik.

**7.0.12. Állítás.** *Legyen $C$ egy 0-t tartalmazó $e$-hibajavító bináris perfekt kód. Tekintsük pontnak a koordináta-pozíciókat, és blokknak a $(2e+1)$ súlyú (tehát minimális súlyú) kódszavak tartóit. Ekkor ezek egy $(e+1)-(n, 2e+1, 1)$ blokkrendszert alkotnak.*

*Bizonyítás.* A koordináta-pozíciók száma $n$. Egy pont legyen eleme egy blokknak, ha a blokkhoz tartozó kódszóban az adott helyen egyes áll. Minden blokk elemszáma megegyezik: $|B| = 2e+1$. A pontok egy $(e+1)$ elemű részhalmaza egy $(e+1)$ súlyú szó. A perfektség miatt minden ilyenhez létezik pontosan egy olyan kódszó, amely tőle legfeljebb $e$ távolságra van. Ez pontosan $e$ távolságra van, mert annál közelebb csak $2e+1 = d$-nél kisebb súlyú szavak vannak, ezek viszont nem kódszavak. Ahol az $e+1$ súlyú szóban egyes áll, ott a hozzá tartozó $2e+1$ súlyú kódszóban is egyesnek kell állnia, különben kisebb lenne a súlya. Tehát bármely $e+1$ koordináta-pozícióhoz pontosan egy blokk létezik, amely tartalmazza őket. □

**Példa:** A Ham(3) Hamming-kód minimális súlyú kódszavai 2-(7, 3, 1) blokkrendszert alkotnak, azaz Fano-síkot.




Fano-sík

**7.0.13. Állítás.** *Egy $t-(v,k,\lambda)$ t-rendszer blokkjainak száma $b=\frac{\binom{v}{t}\lambda}{\binom{k}{t}}$.*

*Bizonyítás.* Tekintsük az illeszkedő $P$-$B$ párokat, ahol $P$ a pontok egy $t$ elemű részhalmaza, $B$ pedig egy blokk, és számoljuk őket össze kétféleképpen. Egy rögzített blokkban $\binom{k}{t}$ pont $t$-es van, tehát $b\binom{k}{t}$ ilyen pár létezik. Másrészt viszont minden $t$ darab pont pontosan $\lambda$ közös blokknak eleme, tehát az illeszkedő párok száma $\binom{v}{t}\lambda$. Ebből átrendezéssel kapjuk a fenti egyenlőséget. □

**7.0.14. Állítás.** *Ha egy $(H, \mathcal{H})$, $\mathcal{H}\subseteq 2^H$ halmazrendszerre teljesül, hogy $|H|=v$, $\forall B\in\mathcal{H}: |B|=k$, annyi halmaz van, amennyi a blokkok száma egy $2-(v,k,\lambda)$ blokkrendszerben (azaz b), és $H$ minden kételemű részhalmazát $\mathcal{H}$-nak legfeljebb $\lambda$ eleme tartalmazza, akkor $(H, \mathcal{H})$ egy $2-(v,k,\lambda)$ blokkrendszer.*

*Bizonyítás.* Jelölje minden $p_1$ és $p_2$ pontra $\lambda(p_1,p_2)$ azon blokkok számát, amelyek átmennek $p_1$-en és $p_2$-n is. Ekkor $\sum_{p_1\neq p_2}\lambda(p_1,p_2)=|\{(p_1,p_2,B)|p_1\neq p_2, p_1,p_2\in \in B\}|\leq b\binom{k}{2}=\binom{v}{2}\lambda$. Ha lenne két olyan pont, amelyek kevesebb, mint $\lambda$ közös blokknak elemei, akkor a bal oldalon lévő kifejezés szigorúan kisebb lenne, mint $\binom{v}{2}\lambda$, hiszen $\binom{v}{2}$ pontpárt vizsgálunk. □

Ugyanezt a gondolatmenetet követve hasonló állítás mondható ki $t-(v,k,\lambda)$ rendszerekre.

**7.0.15. Állítás.** *A 2-(11, 5, 2) blokkrendszer létezik és egyértelmű.*

Az állítást nem bizonyítjuk, a [2] jegyzet 24. oldalán ábrázolt Hussain-gráfok (és a mindjárt következő Paley-konstrukció) adják a létezést. A Hussain-gráfok egyértelműségét is meg lehet mutatni.

A **Paley-konstrukció** egy ilyen blokkrendszert ad meg: legyen a pontok halmaza a $H$=\{mod 11 maradékosztályok\}, legyen $S=\{0,1,3,4,5,9\}$, és legyenek

a blokkok a $\mathcal{H} = \{S + x | x \in H\}$ halmaz elemei. Ekkor $(H, \mathcal{H})$ egy $2 - (11, 5, 2)$ blokkrendszer.

## 7.1. Bináris Golay-kódok

**7.1.1. Tétel.** *Legyen $C$ egy 0-t tartalmazó $(24, 2^{12}, 8)_2$ kód. Ekkor $C$ a koordináták permutációjától eltekintve egyértelmű.*

*Bizonyítás.* A bizonyítás első felében megmutatjuk, hogy a kód önortogonális. Bár a tétel feltételei között nem szerepel a linearitás, látni fogjuk, hogy a kód lineáris. A második részben belátjuk az egyértelműséget: reziduális kódot képezünk, és ennek a generátormátrixát felelteljük meg egy blokkrendszernek, amelyről tudjuk, hogy egyértelműen létezik.

Az önortogonalitás bizonyításához tekintsük $C$ súlyeloszlását. Mivel a perfekt $(23, 2^{12}, 7)$ kódokét ismerjük, ezért lyukasszuk ki $C$-t egy tetszőleges helyen, így épp egy ilyent kapunk. Ekkor a korábban vizsgált súlyeloszlás miatt csak 0, 7, 8, 11, 12, 15, 16 és 23 súlyú szavak lehetnek a kilyukasztott kódban. Az eredetiben tehát csak 0, 8, 12, 16 és 24 súlyú szavak lehettek, különben rosszul lyukasztva nem megengedett súlyt kapnánk. Például ha egy 11 súlyú szóból 1-est törlünk, 10 súlyút kapunk, ha 13 súlyúból 0-t, akkor 13 súlyút. Most toljuk el a kódot az egyik szavával, azaz tekintsük az $u + C$ kódot, ahol $u \in C$. Erre is igaz minden, amit eddig észrevettünk. Ez azt jelenti, hogy $C$-ben bármely két kódszó távolsága 0, 8, 12, 16 vagy 24. Mivel minden kódszó súlya osztható néggyel, ezért a fejezet első lemmáját alkalmazva $C$ bármely két szava ortogonális, azaz $C \subseteq C^\perp$. Ekkor $\langle C \rangle \subseteq C^\perp$ is teljesül. Tudjuk, hogy $C$ elemszáma $2^{12}$, ebből következik, hogy az általa generált altér legalább 12 dimenziós. Ugyanakkor $\dim(\langle C \rangle) \leq \dim(C^\perp) = 24 - \dim(\langle C \rangle)$ miatt $\dim(\langle C \rangle) = 12$ következik, ezért $C = \langle C \rangle = C^\perp$. Tehát $C$ önortogonális, lineáris kód.

Ezután írjuk fel a kód generátormátrixát. Ehhez először képezzünk reziduális kódot egy 12 súlyú $c_0$ kódszóra vonatkozóan (korábbról tudjuk, hogy ilyenből 1288+1288=2576 darab van), és vizsgáljuk ennek a generátormátrixát. A 6.0.9 állítás miatt a reziduális kód paraméterei $[12, 11, d]_2$ lesznek, ahol $d \geq 2$. Ugyanakkor a Singleton-korlát miatt $d \leq n - k + 1 = 12 - 11 + 1 = 2$, tehát $d = 2$. Most tekintsük a reziduális kód duálisát. Ez egy $[12, 1, 12]_2$ kód, ami csak úgy lehet, ha a csupa nulla és csupa 1 szavakból áll, tehát az ismétlés-kód. A reziduális kód szavai ezekre merőlegesek, azaz pontosan a páros súlyú szavak. Ennek a generátormátrixa

$$\begin{pmatrix} & & 1 \\ & I_{11} & \vdots \\ & & 1 \end{pmatrix},$$

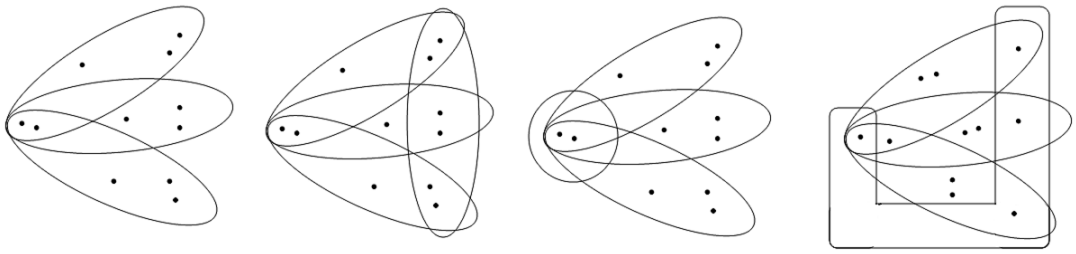
ezért az eredeti $C$ generátormátrixa felírható

$$\begin{pmatrix} 1 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & & & & & 1 \\ \vdots & A & & & I_{11} & \vdots \\ 0 & & & & & 1 \end{pmatrix}$$

alakban, ahol A egy $11 \times 11$-es mátrix. Az első oszlopban a nullákat úgy tudjuk elérni, hogy ahol egyes áll, ahhoz hozzáadjuk az első sort.

A továbbiakban azt fogjuk belátni, hogy $A$ egy $2-(11,6,3)$ blokkrendszer illeszkedési mátrixa. Belátjuk, hogy minden sorban pontosan 6 helyen áll egyes, és hogy bármelyik két sorhoz pontosan 3 olyan index létezik, ahol mindkettőben 1-es áll. Mivel $C$ minimális súlya 8, és $A$-n kívül minden sorban 2 darab 1-es van, ezért $A$ minden sorában legalább 6 helyen áll 1-es. 7, 8, 9 és 11 db 1-es nem lehet, mert 9, 10, 11 és 13 súlyú szavak nincsenek a kódban. 10 helyen szintén nem lehet 1-es $A$ egyik sorában sem, mert akkor ehhez a sorhoz az elsőt hozzáadva 4 súlyú szó keletkezne, ami szintén nincs $C$-ben. Tehát $A$ minden sorában 6 helyen áll egyes. Most tekintsük két tetszőleges sorát $A$-nak. Tegyük fel, hogy 3-nál több közös helyen van bennük 1-es, ami azt jelenti, hogy mindkettőnek legfeljebb 2 olyan koordinátája van, ahol 1-es áll, a másik sor megfelelő helyén pedig 0. Ekkor ezt a két sort összeadva egy olyan kódszót kapunk, aminek az $A$-ra eső részén legfeljebb 4 egyes van, az $I_{11}$-re eső részén pedig pontosan kettő. Ennek a kódszónak a súlya tehát 6-nál kisebb vagy egyenlő, ilyen szó azonban a 0-n kívül nincs $C$-ben, tehát ellentmondáshoz jutottunk. Most tegyük fel, hogy a két sornak 3-nál kevesebb közös 1-es koordinátája van. Nem lehet, hogy nincs közös 1-es koordinátájuk, mert akkor legalább 6+6=12 hosszúnak kellene lenniük, de $A$-nak csak 11 oszlopa van. Tehát vagy 1, vagy 2 közös koordinátájukon áll 1-es. Adjuk össze ezt a két sort, és még adjuk hozzá $c_0$-t is. Ha csak egy közös 1-es volt a két sorban, akkor a kapott összeg súlya 1 az $A$ koordinátáin, ha pedig két helyen is egyes állt mindkettőben, akkor a három sor összege 3 súlyú az $A$-ra eső részen. Ebből azt kapjuk, hogy a három sor összegeként kapott kódszó súlya 3 vagy 5, ilyenek azonban nincsenek $C$-ben, tehát megint ellentmondáshoz jutottunk. Ezzel beláttuk, hogy bármely két sorban 3 közös helyen áll egyes. További 3-3 egyes van bennük, tehát bármely két sorban két közös helyen áll nulla. Most térjünk át a komplementerre, azaz tekintsük azt az $A'$ mátrixot, amelyet $A$-ból a nullák és egyesek felcserélésével kaptunk. Erről fogjuk belátni, hogy egy $2-(11,5,2)$ paraméterű

blokkrendszer illeszkedési mátrixa. Tudjuk, hogy minden sorában 5 egyes van, és bármely két sorban két közös helyen áll 1-es. Ahhoz, hogy ez a megfelelő blokkrendszer illeszkedési mátrixa legyen, azt kell megmutatnunk, hogy bármely két pont két közös blokkban van. Tekintsünk két tetszőleges pontot. Ha ehhez lenne három blokk úgy, hogy mindháromnak elemei, akkor a blokkok maradék 3-3 pontja kívül esne a másik két blokkon. Ezzel meglenne a 11 pont, tehát további pontok nincsenek. Ekkor azonban egy negyedik blokk csak úgy metszhetné őket 2-2 pontban, hogy 2, 4 vagy 6 elemű lenne, ami ellentmondás.

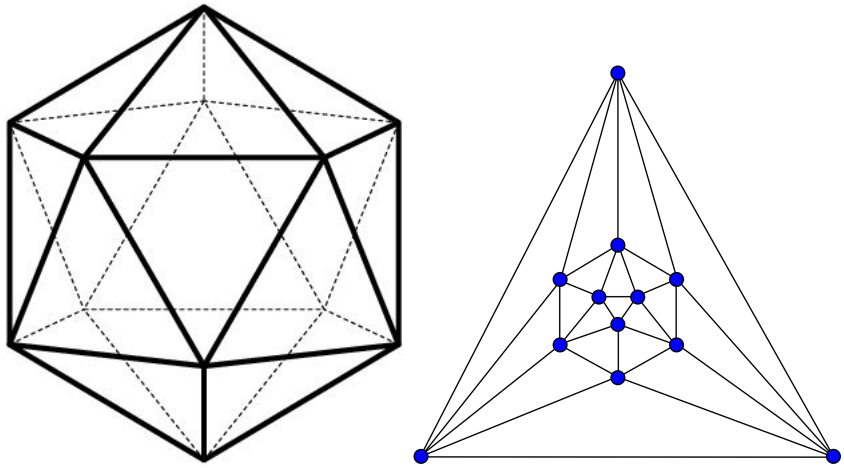


Nem lehet két pont három közös blokkban.

Ha bármely két pont legfeljebb két közös blokknak eleme, akkor a 7.0.14 állítás miatt pontosan annyinak eleme, mert $A$ $11 \times 11$-es, tehát 11 blokk van, ez éppen megegyezik a 7.0.13 állításból kapott számmal. Ezzel megmutattuk, hogy $A'$ egy 2-(11, 5, 2)-blokkrendszer illeszkedési mátrixa, ami 7.0.15 állítás alapján egyértelműen létezik. Ebből adódik a Golay-kódok egyértelműsége. □

$C$ a kibővített Golay-kód, amelyet $G_{24}$-gyel jelölünk.

A kibővített Golay-kódot megkaphatjuk az ikozaéder szomszédsági mátrixa segítségével is. A most következő rész a [8] könyvre támaszkodik.



Ikozaéder és szomszédsági gráfja

**7.1.2. Tétel.** *Legyen $N'$ az ikozaéder ($12 \times 12$-es) adjacencia-mátrixa, és legyen $N$ az $N'$-ből a 0-k és 1-esek felcserélésével kapott mátrix. Ekkor*

$$G = (I_{12} \quad N)$$

*a $G_{24}$ generátormátrixa.*

*Bizonyítás.* Legyen $C$ a kód, amelynek $G$ a generátormátrixa. Először belátjuk, hogy $C$ önortogonális. $N'$ minden sorában pontosan öt 1-es van, tehát $N$ minden sorában pontosan 5 nulla. $N'$ két sorának skaláris szorzata a két kijelölt csúcs közös szomszédainak száma modulo 2. Két csúcs vagy átellenes, és ekkor nincs közös szomszédjuk, vagy nem, ekkor kettő van. Ezért $N'$ két sorában nulla vagy két közös 1-es van, $N$ két sorában nulla vagy két közös nulla. Ha nincs közös nulla, akkor 5-5 olyan nulla van a két sorban, amelyek mind különböző helyeken állnak, a skaláris szorzat tehát $2(\equiv 0 \mod 2)$. Ha kettő közös nulla van, akkor 3-3 van, ami nem közös, tehát összesen $3 + 3 + 2 = 8$ darab 0 tényező lesz az összegben, és 4 egyes, azaz a skaláris szorzat $4(\equiv 0 \mod 2)$. Mivel $G$ minden sorában 8 helyen szerepel 1-es, és a kód önortogonális, ezért a már korábban is használt lemma miatt minden kódszó súlya osztható 4-gyel. Már csak azt kell belátnunk, hogy nincsen 4 súlyú kódszó $C$-ben. Ha lenne ilyen kódszó, az $G$ néhány sorának összege kellene hogy legyen. A 4 nemnulla koordináta közül lennie kell legalább egynek az első 12 koordinátán, hiszen a kódszó néhány sor összegeként áll elő. Pontosan egy nem lehet, mert akkor az a generátormátrix egy sora lenne, de azok közül egyiknek sem 4 a súlya. A 5.0.4 állításból következik, hogy pontosan 3 sem lehet, mert ekkor az ellenőrző mátrixszal szorozva kapnánk egy 1-es koordinátát. Tehát 4 súlyú szó csak úgy fordulhat elő a kódban,

ha 2 egyes koordináta esik az első 12 helyre, és 2 a második 12-re. Két sor összege viszont az előbbiek miatt vagy 12 súlyú, ha az $N$-re eső részen nincs közös nulla, vagy 8 súlyú, ha az $N$-re eső részen két helyen áll mindkettőben 0. □

**Megjegyzés:** A 4 súlyú szavak létezését az 5.0.4 állítás használata nélkül is be tudtuk volna látni úgy, hogy egyszerűen megvizsgáljuk az összegeket. Egyik sor sem 4 súlyú. Két sor összege vagy 12, vagy 8 súlyú. Három sor esetén az összegben azokon a helyeken lesz 1-es az utolsó 12 koordinátán, amely csúcsok a három kiválasztott csúcs közül egyikkel sem szomszédosak, illetve amelyek pontosan kettővel. Ezekből bármely három csúcsra létezik legalább kettő, ezért az összeg teljes súlya nagyobb 4-nél. Ha négy sort adunk össze, akkor pedig ahhoz, hogy négy súlyú szót kapjunk, olyan négy csúcsot kell választanunk, amelyekhez nincs ötödik, ami pontosan eggyel vagy pontosan hárommal szomszédos közülük. Ilyen négy csúcsa nincs az ikozaédernek. Ha négynél több sort adunk össze, akkor már az első 12 koordinátában legalább 5 egyes lesz.

**Következmény:** A $G_{23}$ perfekt Golay-kód egyértelmű.

*Bizonyítás.* Tekintsük $G_{23}$ kibővítettjét. Ennek a paraméterei megegyeznek $G_{24}$ paramétereivel. Az ikozaéder szomszédsági mátrixa szimmetrikus, így $G_{24}^{\perp} = G_{24}$ generátormátrixa $N = N^{\intercal}$ miatt $(N|I_{12})$. Ez azt jelenti, hogy az $i$-edik és a $(12+i)$-edik koordináta felcserélhető minden $i$-re 1 és 12 között. Továbbá az ikozaéder automorfizmuscsoportja (ahol a leképezések a csúcsok permutációi) tranzitív a 12 csúcson. Ezekből következik, hogy $G_{24}$ automorfizmuscsoportja tranzitív a koordinátákon, azaz bárhol lyukasztjuk ki a kódot, permutáció erejéig ekvivalens kódokat kapunk. Mivel $G_{24}$-ból a paritásbit törlésével kapjuk vissza $G_{23}$-at, így $G_{24}$ egyértelműségéből $G_{23}$ egyértelműsége következik. □

A következő két előállítás az [1] könyvben szerepel vázlatos bizonyítással. Ezeket a bizonyításokat fejtettem ki bővebben.

Ezek közül az első konstrukció J. H. Conwaytől ered. Az ábécé most a négyeleműtest, azaz $GF(4) = \{0, 1, \omega, \overline{\omega}\}$, ahol $\overline{\omega} = \omega + 1 = \omega^2$. $\omega$ és $\overline{\omega}$ gyökei az $x^2 + x + 1$ polinomnak, amely irreducibilis GF(2) fölött. Ebből következik, hogy $\omega + \overline{\omega} = 1$, illetve hogy $\omega$ és $\overline{\omega}$ egymás négyzetei. Az előállításhoz először definiálunk egy segédkódot.

**7.3. Definíció.** *A*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & \overline{\omega} & \omega \\ 0 & 1 & 0 & 1 & \omega & \overline{\omega} \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

*mátrix által generált kód a $H_6$ kód.*

**7.1.3. Állítás.** *A $H_6$ kód ekvivalens a $H := \{(a, b, c, f(1), f(\omega), f(\overline{\omega}))|f(x) = ax^2 + + bx + c; a, b, c \in GF(4)\}$ kóddal.*

*Bizonyítás.* $H_6$ elemei azok a vektorok, amelyek előállnak $G$ sorainak lineáris kombinációjaként, azaz

$$y = \alpha \begin{pmatrix} 1 & 0 & 0 & 1 & \overline{\omega} & \omega \end{pmatrix} + \beta \begin{pmatrix} 0 & 1 & 0 & 1 & \omega & \overline{\omega} \end{pmatrix} + \gamma \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

alakúak, ahol $(\alpha, \beta, \gamma) \in V(3,4)$. A műveleteket elvégezve a következőt kapjuk a kódszavak általános alakjára:

$$y = \begin{pmatrix} \alpha, & \beta, & \gamma, & \alpha + \beta + \gamma, & \alpha\overline{\omega} + \beta\omega + \gamma, & \alpha\omega + \beta\overline{\omega} + \gamma \end{pmatrix},$$

ez pedig éppen $H$ definíciójának felel meg. □

Ebből az alakból látszik, hogy ha $a$, $b$ és $c$ közül pontosan kettő nulla, akkor a kódszó súlya 4. Ha pontosan egy nulla van köztük, akkor $f(x) = 0$ pontosan egy $x \neq 0$-ra, tehát a súly megint 4. Ha egyik sem nulla az együtthatók közül, akkor $f$ vagy két helyen vesz fel nullát, vagy egy helyen sem. $H_6$ egy szavának súlya tehát 0, 4 vagy 6.

**7.4. Definíció.** *Legyen $C$ az a kód, amelynek a kódszavai azok a $4\times6$-os bináris mátrixok, amelyekre teljesülnek a következők: egy $M$ mátrix, melynek sorai $m_0, m_1, m_2$ és $m_3$, akkor és csak akkor kódszó, ha*

– *$M$ minden oszlopának a paritása megegyezik $m_0$ paritásával, és*

– *$m_1 + \omega m_2 + \overline{\omega} m_3 \in H_6$.*

**Megjegyzés:** Egy vektor paritása alatt a koordinátái összegének a paritását értjük.

**7.1.4. Tétel.** *A fent definiált $C$ kód ekvivalens a kibővített Golay-kóddal.*

*Bizonyítás.* A kód linearitása a definícióban adott tulajdonságokból következik. Számoljuk össze a kódszavakat! A paritást kétféleképpen választhatjuk meg, azt a $c \in$ $\in H_6$ szót pedig, amit a második tulajdonság ad, $4^3$-féleképpen. Ez a két paraméter még nem határoz meg egyértelműen egy kódszót, ugyanis $c$ minden koordinátájához 2 különböző oszlop tartozik: ha $c_i$, azaz az $i$-edik koordináta előáll $0 + \alpha\omega + \beta\overline{\omega}$ alakban, akkor előáll $1 + (\alpha + 1)\omega + (\beta + 1)\overline{\omega}$ alakban is, tehát minden oszlopnak van kiegészítője. Az első 5 oszlopot ezek szerint $2^5$-féleképpen választhatjuk, a hatodikat pedig az első öt oszlop és a paritás már egyértelműen meghatározza. Ebből $|C| = 2 \cdot 4^3 \cdot 2^5 = 2^{12}$ következik, vagyis $C$ egy 12 dimenziós lineáris kód.

A minimális súly meghatározásához külön vizsgáljuk $C$ páros és páratlan kódszavait. Ha egy páros súlyú kódszót tekintünk, és a hozzá tartozó $c \in H_6$ nem a csupa nulla vektor, akkor $c$-nek legalább 4 nemnulla koordinátája van. Az ezeknek megfelelő oszlopok nem lehetnek tehát csupa 0-k. Mivel páros sok 1-esnek kell lennie minden oszlopban, ezért itt legalább 2 helyen áll egyes. Az egész mátrix súlya tehát legalább 8. Ha a paritás páros, és a $c = 0$ vektor tartozik hozzá, de maga a mátrix nem a csupa nulla mátrix, akkor kell lennie olyan oszlopnak, ahol az utolsó három koordináta egyes, hiszen így lesz a második tulajdonságban szereplő összeg adott koordinátája 0. Ha viszont egy oszlopban van 3 egyes, akkor négynek is lennie kell a paritás miatt. Így az első sorba került egy egyes. Azonban ennek a sornak páros súlyúnak kell lennie, ezért legalább két csupa 1-es oszlop van, a mátrix súlya tehát ebben az esetben is legalább 8. Tekintsük most a páratlan súlyú kódszavakat. Ebben az esetben a 8-nál kisebb súlyú kódszavak kizárásához elég belátnunk, hogy nem lehetséges, hogy minden oszlopban pontosan 1 helyen álljon egyes. Mivel $c$ páros súlyú, és páros sok koordinátája van, ezért páros sok helyen áll benne 0. Ha minden oszlopban pontosan egy darab 1-es lenne, akkor ott és csak ott lehetne $c$-ben nulla, ahol a mátrix első sorában szerepel az egyes. Ha ebből páros sok lenne, akkor $m_0$ páros súlyú lenne, tehát ellentmondásra jutottunk.

Megkaptuk, hogy $C$ egy $[24, 12, 8]_2$ kód, tehát ekvivalens a korábban $G_{24}$-gyel jelölt kibővített Golay-kóddal. □

A Golay-kód legegyszerűbb előállítása a következő mohó eljárás, amely az [1] irodalomban szerepel. Induljunk ki a 24 hosszú csupa nulla szóból, és egymás után vegyük be a kódba a lexikografikusan legkisebb szót, ami még nincs benne, és minden eddig bevett szótól legalább 8 távolságra van. A második szó tehát a $(0, \cdots, 0, 1, \cdots, 1)$ lesz, ahol az utolsó 8 koordináta egyes. Nehéz bebizonyítani, de igaz, hogy $2^{12}$ lépés után éppen a $G_{24}$ kódot kapjuk.

A következő konstrukció R. J. Turyntól ered, és a Hamming-kódokra épül. Legyen

$H$ a bináris $[7,4,3]$ Hamming-kód, amelynek ellenőrző mátrixa

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

és jelölje $\overline{H}$ a kibővítettjét. Legyen $H^*$ az a kód, amelyet $H$-ból a szavak megfordításával kapunk, és legyen $\overline{H^*}$ ennek a kibővítettje. A 7.0.12 állítás miatt $H$ minimális súlyú kódszavai $2-(7,3,1)$ blokkrendszert alkotnak, azaz Fano-síkot.

Ebből következik, hogy $H$ elemei a 0, az 1, a Fano-sík egyeneseinek, illetve az egyenesek komplementereinek karakterisztikus vektorai. Tehát $H$ a 0 szóból, az $(1,1,0,1,0,0,0)$ hét ciklikus eltoltjából, illetve ezek komplementumaiból áll. A kibővített kód elemei tehát a csupa nulla, a csupa 1, a fenti vektor és az eltoltjai egy 1-essel kiegészítve, és a komplemeterek 0-val bővítve. $\overline{H}$ és $\overline{H^*}$ 8 hosszú, 4 dimenziós kódok, metszetük a $\{\underline{0},\underline{1}\}$. Más szó akkor lehetne a metszetben, ha $H$-ban lenne a középső koordinátára szimmetrikus kódszó. Mindkét kód önduális, és minimális súlyuk 4.

**7.1.5. Állítás.** *Legyen $C$ a következő 24 hosszú kód:*

$$C = \{(a+x, b+x, a+b+x) : a,b \in \overline{H}, x \in \overline{H^*}\}.$$

*Ekkor $C$ ekvivalens a $G_{24}$ kibővített Golay-kóddal.*

*Bizonyítás.* $C$ egy [24,12] kód, hiszen az $(a,0,a)$, $(0,b,b)$ és $(x,x,x)$ szavak, ahol $a$ és $b$ a $\overline{H}$, $x$ pedig a $\overline{H^*}$ egy bázisát futja be, $C$ egy bázisát adják. $C$ önortogonális is, mert $\overline{H}$ és $\overline{H^*}$ önörtogonális, és az előbb felsorolt vektorok páronként ortogonálisak: $(a,0,a)\cdot(x,x,x) = a\cdot x + a\cdot x = 0$, $(0,b,b)\cdot(x,x,x) = b\cdot x + b\cdot x = 0$.

A fenti bázisvektorok súlya osztható néggyel. Két bázisvektor összegében ott lesz egyes, ahol pontosan az egyikben volt eredetileg. Ennek mérete két néggyel osztható szám összege mínusz kétszer az a szám, ahány helyen mindkettőben egyes állt. Ennek a metszetnek a mérete az öndualitás miatt páros. $C$ tehát duplán páros, azaz minden kódszó súlya osztható néggyel.

Most azt fogjuk belátni, hogy a minimális súly 8, amihez már csak az kell, hogy nincs 4 súlyú szó a kódban. Indirekte tegyük fel, hogy $c = (a+x, b+x, a+b+x)$ súlya 4. A három komponensből valamelyiknek a csupa nullának kell lennie, mert mindhárom rész súlya páros. Ez csak úgy lehetséges, hogy $a = x$ vagy $b = x$ vagy $a+b = x$ teljesül. Mivel $\overline{H} \cap \overline{H^*} = \{0,1\}$, ezért $x$ 0 vagy 1. Ha $x = 0$, akkor mindhárom részben $\overline{H}$ egy-egy szava áll. Ezek súlya legalább 4, és közülük legfeljebb

egy lehet nullvektor, ezért $c$ súlya legalább 8, ami ellentmondás. Ha $x = 1$, akkor $c = (0; b+1; b)$ vagy $c = (a+1; 0; a)$. Mindkét esetben $c$ súlya 8.

$C$ tehát $[24, 12, 8]_2$ kód, azaz ekvivalens a $G_{24}$ kibővített Golay-kóddal. □

A következő előállításban a $G_{23}$ Golay-kódot egy polinom többszöröseiként fogjuk megkapni. Ehhez be kell vezetnünk a ciklikus kód és a generátorpolinom fogalmát.

**7.5. Definíció.** *A $C$ lineáris kódot **ciklikus**nak nevezzük, ha bármely $(c_0, c_1, \ldots c_{n-1})$ kódszavára $(c_{n-1}, c_0, \ldots c_{n-2})$ is eleme a kódnak.*

Ezek a kódok kényelmesen leírhatóak polinomokkal: a $c = (c_0, c_1, \cdots c_{n-1})$ kódszónak feleltessük meg a $c(x) = \sum_{i=0}^{n-1} c_i x^i$ polinomot. Ekkor a fenti eltolás annak felel meg, hogy $c(x)$-et szorozzuk $x$-szel, majd az eredményt redukáljuk modulo $(x^n - -1)$. Eszerint minden polinomot érdemes a $GF(q)[x]/(x^n - 1)$ faktorgyűrű elemének tekinteni. A szóban forgó polinomok halmaza vektortér, ezért a lineáris kódok felírhatóak ebben a reprezentációban.

**Példa:** A Ham(3) Hamming-kód ciklikus, hiszen a csupa nulla és a csupa egyes vektort önmagába viszi az eltolás, a kód többi szava pedig az $(1, 1, 0, 1, 0, 0, 0)$ összes ciklikus eltoltja. Ha például a $(0, 0, 0, 1, 1, 0, 1)$ kódszónak megfelelő $x^3 + x^4 + x^6$ polinomot megszorozzuk $x$-szel, és redukáljuk modulo $x^7 - 1$, akkor az $x^5 + x^4 - 1 \equiv$ $\equiv x^5 + x^4 + 1$ ( mod 2) polinomot kapjuk, ami valóban az $(1, 0, 0, 0, 1, 1, 0)$ szónak felel meg.

Mivel a $GF(q)[x]/(x^n - 1)$ gyűrű főideálgyűrű, azaz minden ideáljának van egy elemből álló generátorrendszere. Minden ciklikus kód ideál, mert tartja az $x$-szel való szorzást, ami a kódszavak eltolása eggyel, és a konstanssal való szorzást. Minden polinom előállítható $x$-szel és konstanssal való szorzással, és ezek összegével. ezért minden ciklikus kódhoz találhatunk egy $g(x)$ generátorpolinomot. Ez a legkisebb $C$-beli egy főegyütthatós polinom. Ez a polinom egyértelmű, és osztója $(x^n - 1)$-nek, mert ellenkező esetben $g(x)$ és $(x^n - 1)$ legnagyobb közös osztója egy $g(x)$-nél alacsonyabb fokú polinom lenne $C$-ben. A kód ekkor $g$ legfeljebb $n - 1$-edfokú többszöröseiből áll. A generátorpolinom együtthatóiból felírható a kód generátormátrixa is. Ha $g(x) = \sum_{i=0}^{n-k} g_i x^i$, akkor

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & & \ddots & & & & 0 \\ \vdots & & & & \ddots & & & \vdots \\ 0 & \cdots & & & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}.$$

**7.6. Definíció.** *A $C$ ciklikus kód **ellenőrző polinom**ja az a $h(x)$ polinom, melyre a kód szavai pontosan azok a polinomok, amelyeket $h(x)$-szel szorozva nullát kapunk a $GF(q)[x]/(x^n-1)$ gyűrűben.*

**7.1.6. Állítás.** *A $g(x)$ polinom által generált ciklikus kód ellenőrzőpolinomja $h(x) = \frac{x^n-1}{g(x)}$. $C$ duálisának az ellenőrzőpolinomja $h(\frac{1}{x})x^{deg(h(x))}$.*

**7.1.7. Állítás** (BCH-korlát)**.** *Legyen $g(x)$ a $C$ ciklikus kód generátorpolinomja. Tekintsük $g(x)$ gyökeit $GF(q)$ egy olyan $K = GF(q^m)$ testbővítésében, amely tartalmazza az $n$-edik egységgyököket. Ha $\alpha$ primitív $n$-edik egységgyök, és $\alpha$-nak egymást követő $\delta - 1$ hatványa mind gyöke $g(x)$-nek, akkor $C$ minimális súlya legalább $\delta$.*

A következő állítás bizonyításához az [5] jegyzet bináris Golay-kódokhoz kapcsolódó feladatsorát oldottam meg.

A Golay-kód előállításához tekintsük az $x^{23}-1$ polinomot. Ez $GF(2)$ felett három irreducibilis tényező szorzatára bomlik: $x^{23}-1 = (x-1)(x^{11}+x^9+x^7+x^6+x^5+$ $+x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1) = (x-1)g(x)f(x)$. Természetesen a $+$ és $-$ előjeleket szabadon cserélgethetjük, mert a kételemű test minden eleme a saját ellentettje.

**7.1.8. Állítás.** *A $g(x)$ által generált $C$ kód, amely $g(x)$ legfeljebb 22-edfokú többszöröseiből áll, ekvivalens a $G_{23}$ Golay-kóddal.*

*Bizonyítás.* Mivel a 23 osztója $(2^{11}-1)$-nek, ezért az $x^{23}-1$ polinom gyökei $GF(2^{11})$ elemei. Legyen $\alpha$ primitív 23-adik egységgyök $K = GF(2^{11})$-ben. Itt a négyzetre emelés automorfizmus, így $\alpha$ minimálpolinomjának további gyökei $\alpha^2$, $\alpha^4$, $\alpha^8$, $\alpha^{16}$, $\alpha^{32}(=\alpha^9)$, $\alpha^{18}$, $\alpha^{36}(=\alpha^{13})$, $\alpha^{26}(=\alpha^3)$, $\alpha^6$ és $\alpha^{12}$, tehát $\alpha$ minimálpolinomja egy 11-edfokú $g(x)$ polinom. Az $\frac{1}{\alpha} = \alpha^{11}$ nem szerepel ezek között. Ennek a minimálpolinomja $f(x) = g(\frac{1}{x})x^{\deg(g)}$. Ennek az együtthatói $g$ együtthatói fordított sorrendben.

Most megmutatjuk, hogy $C^\perp$ a $C$-nek egy 1 kodimenziós altere. Általában egy ciklikus kód ellenőrző polinomja $h(x) = \frac{x^n-1}{g(x)}$ polinom, ahol $g$ a generátorpolinom. $C$ ellenőrző polinomja tehát a $h(x) = \frac{x^{23}-1}{g(x)} = (x-1)f(x) = (x+1)f(x) =$ $= (x+1)g(\frac{1}{x})x^{11}$. A duális kód generátorpolinomja $h(x)$ reciprokpolinomja, azaz $h(\frac{1}{x})x^{\deg(h)}$, ebben az esetben $h(\frac{1}{x})x^{12} = (\frac{1}{x}+1)g(x)\frac{1}{x^{11}}x^{12} = (\frac{1}{x}+1)g(x)x = (x+$ $+1)g(x)$. Az ez által generált kód altere a $g$ által generált kódnak. Mivel elsőfokú polinommal szorzunk, ezért a kodimenzió 1.

Ezt felhasználva kapjuk a kibővített kód önortogonalitását. $C^\perp$ minden kódszava (polinomként tekintve) többszöröse $(1+x)$-nek, azaz a súlya páros. Az előzőek miatt $C^\perp$ éppen a $C$ páros súlyú szavaiból áll. Tekintsük most két tetszőleges szavát $\overline{C}$-nek.

Ezek egyike álljon egy $c_1$ $C$-beli vektorból és egy $p_1$ paritásbitből, a másik pedig $c_2$-ből és $p_2$-ből. Vizsgáljuk a skaláris szorzatukat! Ha valamelyik paritásbit 0, akkor az ahhoz tartozó $C$-beli szó eleme $C^\perp$-nek is, tehát a skaláris szorzat 0. Ha a $p_1 = p_2 = 1$ eset áll fenn, akkor tekintsük az $(1 + c_1)c_2$ szorzatot. A csupa 1-esből álló szó eleme $C$-nek, és hozzáadva egy páratlan súlyú szóhoz párost kapunk, tehát $(1 + c_1) \in C^\perp$, ezért a szorzat nulla. Felbontva a zárójelet kapjuk, hogy $0 = 1c_1 + c_1c_2 = 1 + c_1c_2$, amiből $c_1c_2 = 1$ következik. Tudjuk, hogy $p_1p_2 = 1$, tehát a két $C$-beli szó skaláris szorzata 0.

$\overline{C}$ önortogonalitását a generátormátrixból is megkaphattuk volna. Ezt a $G'$ generátormátrixot úgy kapjuk $G$-ből, hogy egy csupa egyes oszlopot írunk mellé. Ha $G$ bármely két sora ortogonális, akkor ez $G'$-re is teljesül. Ahhoz, hogy $G$-nek ezt a tulajdonságát ellenőrizzük, a ciklikusság miatt elég az első sort összevetni a többivel. Ebből $\overline{C} \subseteq \overline{C}^\perp$ következik. Mindkettő altér, és $12 = \dim(\overline{C}) \leq \dim(\overline{C}^\perp)$ miatt a duális kód dimenziója is 12. A két altér tehát megegyezik, így a kibővített kód önduális. Az előző érvelés ezt a hosszadalmas ellenőrzést hivatott megkerülni.

A 7.1.7 állítást alkalmazva $\alpha$-ra, aminek az első négy hatványa gyöke $g$-nek, azt kapjuk, hogy $C$ minimális súlya legalább 5. Mivel a $g(x)$, $xg(x)$, $\ldots$, $x^{11}g(x)$ polinomok egy bázisát adják a kódnak, és mindegyiknek a súlya 7, ezért a paritásbittel kibővítve a súlyuk 8 lesz. 7.1 lemma miatt ebből következik, hogy minden kódszó súlya néggyel osztható. Mivel a minimális súly legalább 5, ezért legalább 8 is. Eszerint $\overline{C}$ $[24, 12, 8]_2$ kód, azaz $G_{24}$, amiből $C = G_{23}$ következik.

□

## 7.2. Ternér Golay-kódok

Most pedig térjünk át a ternér Golay-kódok vizsgálatára. Ez annyiban fog hasonlítani a bináris esethez, hogy itt is a kibővített kódot vizsgáljuk, amelyről azt látjuk majd be, hogy önortogonális és minden kódszó súlya osztható hárommal, majd kizárjuk a három súlyú szavak létezését.

A jelen alfejezetben szereplő állítások bizonyításához az [1] könyv bizonyításvázlatait egészítettem ki, írtam le részletesen.

Az első előállításhoz definiáljuk az $S_5$ mátrixot (Paley-mátrix) a következőképpen: a mátrix $i$. sorának $j$. eleme legyen 1, ha $i - j$ kvadratikus maradék modulo 5, -1, ha $i - j$ kvadratikus nemmaradék, és 0, ha $i = j$:

$$S_5 = \begin{pmatrix} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \end{pmatrix}.$$

Könnyen ellenőrizhető, hogy erre a mátrixra $S_5 S_5^\intercal = 5I - J$ teljesül, ahol $J$ a csupa egyesből álló mátrix.

Legyen $C$ az a (11 hosszú, 6 dimenziós) lineáris kód a háromelemű test felett, amelynek generátormátrixa a következő:

$$G = \begin{pmatrix} & & & 1 & 1 & 1 & 1 & 1 \\ & & & & & & & \\ & & I_6 & & & S_5 & & \\ & & & & & & & \end{pmatrix}.$$

Mivel $G$ első sorában a koordináták összege 0, a többiben pedig 1 (mod 3), ezért ebből $C$ kibővített kódjának, $\overline{C}$-nek a generátormátrixát úgy kapjuk $G$-ből, hogy az első sor végére 0-t, a többi sor végére -1-et írunk. Jelöljük $\overline{C}$ generátormátrixát $\overline{G}$-vel. Először belátjuk, hogy a kibővített kód önduális. Tekintsük $\overline{G}$ két tetszőleges sorát, és használjuk fel, hogy $S_5 S_5^\intercal = 5I - J$. Ha a két sor azonos, akkor könnyen ellenőrizhető, hogy a skaláris szorzat nulla. Ellenkező esetben az első 6 koordinátán a skaláris szorzat mindig nulla, a következő 5 koordinátán pedig -1, ha nincs köztük az első sor, és nulla, ha igen. Az utolsó koordinátán 1 a skaláris szorzat, ha egyik sem az első sor, és nulla, ha valamelyik az első sor. Ebből $\overline{C} \subseteq \overline{C}^\perp$ következik. Tekintsük az alterek dimenzióit. Ekkor $6 = \dim(\overline{C}) \leq \dim(\overline{C}^\perp)$ miatt $\dim(\overline{C}^\perp) = 6$ teljesül, és ebből $\overline{C} = \overline{C}^\perp$.

Mivel $\overline{C}$ önortogonális, ezért bármely $x$ kódszavát önmagával skalárisan összeszorozva 3-mal osztható számot kapunk. Ez az érték éppen megegyezik $x$ súlyával. Ebből következik, hogy $\overline{C}$ minden kódszavának súlya osztható hárommal.

$\overline{G}$ minimális súlyának megállapításához tekintsük a sorok lineáris kombinációit. Belátjuk, hogy nincs 3 súlyú kódszó. Ha lenne ilyen, akkor annak legalább egy nemnulla koordinátája az első hat hely valamelyikére kell, hogy essen, hiszen néhány sor lineáris kombinációjaként áll elő. Pontosan egy nem eshet az első 6 helyre, mert az $G$ egy sora lenne, ezek között pedig nincs 3 súlyú. Pontosan 2 sem lehet az első 6 koordinátán, mert akkor pontosan egynek kellene lennie az utolsó 5-ön, ekkor viszont az 5.0.4 állításból kapott ellenőrzőmátrixszal megszorozva kapnánk egy nemnulla koordinátát. Tehát ha van 3 súlyú szó a kódban, akkor az három sor lineáris kombi-

nációja nemnulla együtthatókkal. A mátrixból leolvasható, hogy minden ilyennek az utolsó 5 koordinátáján van legalább egy nullától különböző elem, mert nincs olyan két sor, amelynek az összege egy harmadik, vagy egy harmadik -1-szerese.

Ebből az következik, hogy a minimális súly legalább 4, de a hárommal való oszthatóság miatt legalább 6. Nagyobb nem lehet, mert 6 súlyú szó van a kódban, például az első sor. Tehát $\overline{G}$ minimális súlya 6. Mivel $C$-t az utolsó koordináta elhagyásával kapjuk $\overline{C}$-ből, ezért $C$ minimális súlya 5.

**7.2.1. Állítás.** *$C$ 2-hibajavító perfekt kód.*

*Bizonyítás.* $C$ paramétereire a következő adódik: $\binom{11}{0}2^0 + \binom{11}{1}2 + \binom{11}{2}2^2 = 243 = 3^5$. Az egyenlőség mindkét oldalát $3^6$-nal szorozva kapjuk, hogy a kód eléri a Hamming-korlátot. □

$C$ tehát $[11, 6, 5]_3$-kód. $C$ a ternér Golay-kód, amelyet $G_{11}$-gyel jelölünk, a kibővítettjét pedig $G_{12}$-vel. $G_{11}$ és $G_{12}$ is egyértelmű [1], ezek bizonyítása lényegesen nehezebb, mint a bináris esetben.

**7.2.2. Állítás.** *$G_{11}$-ben a minimális súlyú kódszavak tartói 4-(11,5,1) blokkrendszert alkotnak. A pontoknak a koordináta-pozíciók felelnek meg.*

*Bizonyítás.* Egy 4-(11,5,1) blokkrendszer blokkjainak száma $b = \frac{\binom{11}{4}}{\binom{5}{4}} = 66$. Számoljuk össze az 5 súlyú tartókat! 5 súlyú kódszóból $A_5$ db van, amelyre teljesül, hogy $A_5\binom{5}{2} = \binom{11}{3}(3-1)^3$, mert minden 3 súlyú szóhoz egyértelműen létezik 5 súlyú szó, amely tőle legfeljebb 2 (azaz a súlykülönbség miatt pontosan 2) távolságra van. Ezeket egyrészt összeszámoltuk úgy, hogy az 5 súlyú kódszavakban 2 nemnulla koordinátát nullára állítunk, ez az egyenlet bal oldala, másrészt minden lehetséges módon letettünk a 11 helyre 3 darab nullától különböző koordinátát, ez a jobb oldal. Ebből $A_5 = 132$ adódik. Most megmutatjuk, hogy minden 5 súlyú tartóhoz pontosan két kódszó tartozik. Legalább kettő biztosan tartozik hozzá, hiszen ha $v$-nek ez a tartója, akkor $-v$-nek is. Egy harmadik kódszónak már nem lehet ugyanez a tartója, mert ha lenne egy ilyen $v'$, akkor az vagy $v$-vel, vagy $-v$-vel legalább 3 helyen megegyezne, de ekkor $v + v'$ vagy $-v + v'$ súlya 4-nél kisebb lenne, ami lehetetlen, mert az összegnek is kódszónak kell lennie. Ebből következik, hogy 66 tartó van, tehát éppen annyi, amennyi blokk a megfelelő blokkrendszerben. Már csak azt kell megmutatnunk, hogy bármely 4 koordináta-pozícióhoz legfeljebb egy közös 5 súlyú tartó van, amelyben benne vannak. Indirekt módon tegyük fel, hogy 4 adott pozícióhoz legalább két tartó tartozik. Tudjuk, hogy a két tartóra pontosan négy kódszó illeszkedik. Ezek közül kell lennie kettőnek, amelyek legalább két helyen azonosak.

Ezt a kettőt kivonva egymásból egy olyan kódszót kapnánk, amely legfeljebb 4 súlyú, ez ellentmondás. A 7.0.14 állítás miatt valóban egy 4-(11,5,1) blokkrendszert kaptunk. □

**7.2.3. Állítás.** *$G_{12}$-ben a minimális súlyú kódszavak tartói 5-(12,6,1) blokkrendszert alkotnak.*

A következő konstrukció a $[4, 2, 3]_3$ Hamming-kódot használja. Jelöljük ennek az ellenőrző mátrixát $H$-val, azaz legyen

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

**7.2.4. Állítás.** *A*

$$G := \begin{pmatrix} J_4 + I_4 & I_4 & I_4 \\ 0 & H & -H \end{pmatrix}$$

*mátrix által generált kód ekvivalens $G_{12}$-vel.*

*Bizonyítás.* Legyen $C$ a $G$ által generált kód. Először megmutatjuk, hogy $G$ sorai lineárisan függetlenek, tehát $C$ valóban 6 dimenziós. $J_4 + I_4$ teljes rangú, mert az oszlopai páronként ortogonálisak. $G$ első hat oszlopa tehát lineárisan független:

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

$G$ bármely két sorának skaláris szorzata nulla, mert az első négy koordinátán 0+0+0+0 vagy 2+2+1+1 az eredmény, a második négy koordinátán 1+0+0+0 vagy 0+1+2+0, az utolsó négyen pedig 2+0+0+0 vagy 0+0+4+2. Ebből és a linearitásból következik, hogy $C$ önduális.

Az öndualitásból ismét következik, hogy minden kódszó súlya osztható hárommal, így már csak azt kell megmutatni, hogy 3 súlyú szó nincs a kódban. Az öndualitás miatt a fenti mátrix nemcsak a generátormátrix, hanem a paritásellenőrző mátrix is. Így azt kell belátnunk, hogy nincs három összefüggő oszlop. Ehhez az kell, hogy nincs két olyan oszlop, amelyek összege egy harmadik, vagy annak a $-$ $-1$-szerese. Ha az első négy oszlop közül adunk össze kettőt, annak az első négy koordinátája között lesz 2 db 0 és 2 db 2-es. Nincs harmadik oszlop, amelyre (vagy

az ellentettjére) ez igaz lenne. Ha egy oszlopot választunk az első négy közül, egy másikat pedig a többiből, akkor az összeg utolsó két koordinátája meg fog egyezni a másodikként választott oszlop utolsó két koordinátájával. Minden ilyenhez van pontosan egy olyan harmadik oszlop, aminek az utolsó két koordinátája ezek ellentettje, de annak az oszlopnak az ellentettje pontosan 3 helyen tartalmaz nullát az első négy koordinátán, míg az összeg legfeljebb 1 helyen. Ha két olyan oszlopot választunk, amelyek közül mindkettő az utolsó nyolc valamelyike, akkor az összeg első négy koordinátája vagy egy kettesből és három nullából, vagy két egyesből és két nullából áll. Egyik esetben sincs harmadik oszlop, amely ezeknek megfelelne. □

A következő, és egyben utolsó előállításhoz definiálnunk kell egy segédkódot. Legyen $\alpha$ primitív 8. egységgyök $GF(9)$-ben, és legyen $i = \alpha^2$. Ekkor $i^2 = \alpha^4 = -1$. Minden $x \in GF(9)$-re $\overline{x} := x^3$. $GF(9)$ minden elemét tekintsük $a + bi$ alakban, ahol $a$ és $b$ a háromelemű test elemei. Ebből $\overline{a + bi} = a^3 + 3a^2bi - 3ab^2 + b^3i^3 = a^3 - b^3i = a - bi$ következik, hiszen $GF(3)$ minden elemének a köbe saját maga. A konjugálás műveletét terjesszük ki a kódszavakra is: $c = (c_1, \ldots, c_n)$ esetén $\overline{c} = (\overline{c_1}, \ldots, \overline{c_n})$.

**7.7. Definíció.** *Egy $C$ kód **konjugáltan duális**, ha belőle a szavai konjugálásával kapott kód $C^\perp$.*

**7.8. Definíció.** *Egy $n$ hosszú $C$ kód **vetítése** az a $2n$ hosszú kód, amelyet úgy kapunk, hogy minden $a + bi$ koordinátát az $(a, b)$ koordináta-párra cserélünk.*

**7.2.5. Állítás.** *Egy $GF(9)$ feletti konjugáltan duális lineáris kód vetítése önduális kód $GF(3)$ felett.*

*Bizonyítás.* Legyen $C$ egy $GF(9)$ feletti konjugáltan duális lineáris kód, $D$ pedig a vetítése. Ahhoz, hogy $D$ öndualitását belássuk, azt kell megmutatnunk, hogy bármely $d_1$, $d_2 \in D$-re $(d_1, d_2) = 0$. Legyen $c_1$ az a $C$-beli kódszó, amelyből $d_1$-et kaptuk vetítéssel, $c_2$ pedig az, amelyből $d_2$-t. Tudjuk, hogy bármely $x$, $y \in C$ kódszavakra az $(\overline{x}, y)$ skaláris szorzat nulla. Legyen $c_1$ $k$-adik koordinátája $a_{1,k} + b_{1,k}i$, $c_2$ $k$-adik koordinátája pedig $a_{2,k} + b_{2,k}i$. Ekkor tehát kapjuk, hogy $(a_{1,1} - b_{1,1}i)(a_{2,1} + b_{2,1}i) + (a_{1,2} - b_{1,2}i)(a_{2,2} + b_{2,2}i) + \ldots + (a_{1,n} - b_{1,n}i)(a_{2,n} + b_{2,n}i) = 0$. Ez a szorzat is $a + bi$ alakú, és csak úgy lehet nulla, ha $a$ és $b$ is nulla. Ebből adódóan $a_{1,1}a_{2,1} + b_{1,1}b_{2,1} + a_{1,2}a_{2,2} + b_{1,2}b_{2,2} + \ldots + a_{1,n}a_{2,n} + b_{1,n}b_{2,n} = 0$, mert a zárójeleket felbontva ezek lesznek az $i$-t nem tartalmazó tagok. Ez az összeg éppen a $(d_1, d_2)$ skaláris szorzat, tehát $D$ valóban önduális.

□

Legyen $C$ a $G := \begin{pmatrix} I & \alpha A \end{pmatrix}$ által generált kód, ahol $A = I + iJ$, $I$ és $J$ mérete $3 \times 3$, $J$ csupa egyesből álló mátrix, $\alpha$ pedig primitív 8. egységgyök. $C$ tehát $GF(9)$ fölötti 6 hosszú, 3 dimenziós kód. Az $A$ mátrixról ellenőrizhető, hogy $A\overline{A^\intercal} = I$.

**7.2.6. Állítás.** *$C$ vetítése ekvivalens $G_{12}$-vel.*

*Bizonyítás.* Jelöljük $C$ vetítését $C'$-vel. $C$ konjugáltan duális, hiszen $G\overline{G^{\mathsf{T}}}$ a csupa nulla mátrix. Ebből a 7.2.5 állítás miatt következik, hogy $C'$ önduális.

A 5.0.4 állítás és $A$ szimmetriája miatt $C$ ellenőrző mátrixa előáll $H = \begin{pmatrix} -\alpha A & I \end{pmatrix}$ alakban. Mivel az ellenőrző mátrix a duális kód egyik generátormátrixa, és $C$ duálisa a kódszavakból konjugálással kapott kód, ezért a $\begin{pmatrix} -\alpha\overline{A} & I \end{pmatrix}$ mátrix szintén $C$-t generálja. A két generátormátrix felhasználásával megmutatjuk, hogy 4-nél kisebb súlyú kódszó nem lehet $C$-ben. Egy súlyú nem lehet, mert akárhogy kombináljuk a sorokat, az első három és a második három koordinátán is lesz legalább egy nemnulla elem. 2 súlyú kódszót szintén nem kaphatunk, mert az az előbbiek miatt csak úgy lenne lehetséges, ha egy nemnulla elem esne az első 3 koordinátára, és egy a másik háromra, tehát bármelyik generátormátrixot tekintjük, egy sor skalárszorosának kellene lennie, azok azonban 4 súlyúak. A 3 súlyú szavak létezését hasonlóképpen lehet kizárni. A három nemnulla koordináta nem lehet az első három vagy az utolsó három. Ha egy esik az első három koordinátára, akkor az $G$ egyik sora kellene, hogy legyen, ha 2, akkor pedig a másik generátormátrixé, de ezek mind 4 súlyú kódszavak. $C$ minimális távolsága tehát legalább 4, amiből az is látszik, hogy $C'$ minimális távolsága szintén legalább 4. Mivel $C'$ önortogonális, ezért bármely $x$ kódszavát önmagával skalárisan összeszorozva 3-mal osztható számot kapunk. Ez az érték éppen megegyezik $x$ súlyával. Ebből következik, hogy $C'$ minden kódszavának súlya osztható hárommal, a minimális távolság tehát minimum 6. A Singleton-korlátból kapjuk, hogy legfeljebb 7, ezért a hárommal való oszthatóság miatt pontosan 6. □

# Hivatkozások


[1] P.J. Cameron and J.H. van Lint, *Designs, graphs, codes and their links*, London Mathematical Society Student Texts, Cambridge University Press, 1991.

[2] F. De Clerck, Gy. Károlyi, and M.J. de Resmini, *Combinatorial structures*, 1993.

[3] P.M. Cohn, *Algebra. volume 2*, John Wiley and Sons Ltd, 1977.

[4] Kiss Emil, *Bevezetés az algebrába*, Typotex Kft, 2007.

[5] Ivanyos Gábor, *Matematikai kriptográfia és kódelmélet*, Egyetemi előadásjegyzet, 2008-2009 tavasz.

[6] Frenkel Péter, *Algebra*, Egyetemi előadás, 2013-2014 ősz.

[7] Vrana Péter, *Golay-kódok*, Egyetemi előadásjegyzet.

[8] Hraskó András, Szőnyi Tamás, *Hibajavító kódok*, Új matematikai mozaik, Typotex Kft, 2002.

[9] Szőnyi Tamás, *Szimmetrikus struktúrák*, 2013.

[10] Wikipedia, *Decoding methods — wikipedia, the free encyclopedia*, 2015, [Online; accessed 29-May-2015].