Blokkrendszerek és perfekt kódok

Diplomamunka

Koknya Péter

Alkalmazott matematikus szak

Témavezető:

Szőnyi Tamás, egyetemi tanár
Számítógéptudományi Tanszék

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2018

Tartalomjegyzék

1. Blokkrendszerek **1**
1.1. Illeszkedési struktúrák 1
1.2. Projektív terek 3
1.3. t-rendszerek 5
1.4. Négyzetes blokkrendszerek 7
1.5. Metszési háromszög 8
1.6. Konstrukciók 12

2. Hibajavító kódok **15**
2.1. Bevezetés 15
2.2. Lineáris kódok 19
2.3. Hamming-kódok 21
2.4. Súlypolinom 23
2.5. Kódkonstrukciók 27
2.6. Golay kódok 28

3. Kapcsolat **29**
3.1. Általános eset 29
3.2. Golay kódok 32

A. Függelék **40**
A.1. Programkód 40

Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek, Szőnyi Tamásnak, aki igen türelmesen segítette munkámat, és a leglehetetlenebb pillanatokban is tudott rám időt szakítani. Köszönöm továbbá Csajbók Bencének a LaTeX-hez nyújtott segítségét, és fáradságos lektori munkáját, valamint hogy valóban mindenkor lehetett rá számítani.

Előszó

A matematikában gyakran találkozunk nagy, bonyolult struktúrákkal. Ezek elemzésével könnyebben átláthatjuk őket. Az első fejezetben bizonyos szabályoknak eleget tevő struktúrákat fogok elemezni. A másdik részben a hibajavító kódolás témakörét vizsgáljuk. Egy zajos csatornán közölt információ gyakran megsérülhet, ezt a gyakorlatban úgy orvosolják, hogy több információt is küldenek ellenőrzés céljából. E területet nevezik a matematikában hibajavító kódolásnak. A harmadik fejezetben bemutatok néhány példát arra, hogyan kapcsolódik egymáshoz a két anyagrész. Így könnyebben fogjuk érteni, milyen szabályosságokat követ egy jó kódolási módszer. Szakdolgozatomban a tanult anyagrészek összegzésén kívül foglalkozom az úgynevezett metszési háromszögekkel, melyek nem képezik az alaptananyag részét, ám bizonyos esetekben igen hasznosak. Továbbá néhány speciális esetet általánosítok. Az algebrai fogalmak vizsgálatához [9] és [10] könyveket ajánlom.

1. fejezet

Blokkrendszerek

1.1. Illeszkedési struktúrák

A definíciók jelentős része [6]-t követi.

1.1.1. Definíció. Egy $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ hármast *illeszkedési struktúrának* nevezünk, ha $\mathcal{P}$ és $\mathcal{B}$ nemüres, diszjunkt halmazok, $\mathcal{I}$ pedig reláció $\mathcal{P}$ és $\mathcal{B}$ elemei között, azaz $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. $\mathcal{P}$ elemeit *pontoknak* , $\mathcal{B}$ elemeit *blokkoknak* nevezzük. Gyakran $(p, B) \in \mathcal{I}$ helyett $p\mathcal{I}B$ -t írunk, és azt mondjuk, hogy p *illeszkedik* B-re, vagy B *átmegy* p–n. $\mathcal{P}$ elemszámát v-vel, $\mathcal{B}$ elemszámát b-vel jelöljük.

Például:

- Legyen a G hipergráf csúcshalmaza $V(G)$, élhalmaza $E(G)$. Legyen $v \in V(G)$ és $e \in E(G)$. Továbbá $v\mathcal{I}e$, ha az e él átmegy a v csúcson. Ekkor G egy $(V(G), E(G), \mathcal{I})$ illeszkedési struktúra.
- Legyen V egy halmaz, $\mathcal{H}$ pedig néhány részhalmazának halmaza, azaz $\mathcal{H} \subseteq 2^V$. A $(V, \mathcal{H})$ halmazrendszer egy olyan $(V, \mathcal{H}, \in)$ illeszkedési struktúra, melyben különböző blokkok nem tartalmazhatják pontosan ugyanazokat a pontokat.

1.1.2. Definíció. Egy pont *foka* a rajta átmenő blokkok száma, egy blokk *foka* a benne lévő pontok száma. Ezt $\deg(p)$-vel illetve $\deg(B)$-vel jelöljük. Ha minden pont foka egyforma, a struktúrát *regulárisnak*, ha minden blokk foka egyforma, a struktúrát *uniformnak* nevezzük.

1.1.3. Definíció. Legyen $\mathbf{D}_1 = (\mathcal{P}_1, \mathcal{B}_1, \mathcal{I}_1)$ és $\mathbf{D}_2 = (\mathcal{P}_2, \mathcal{B}_2, \mathcal{I}_2)$ két illeszkedési struktúra. Az $\alpha : P_1 \cup B_1 \to P_2 \cup B_2$ leképezés *izomorfizmus*, ha bijektív, és $p_1\mathcal{I}_1B_1 \iff p_2\mathcal{I}_2B_2$. Ekkor azt mondjuk, hogy $\mathbf{D}_1$ és $\mathbf{D}_2$ *izomorfak*, és $\mathbf{D}_1 \cong \mathbf{D}_2$ -vel jelöljük.

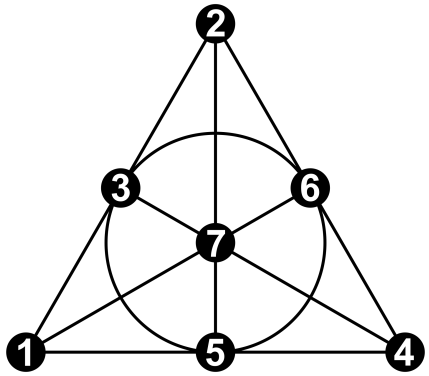
1.1.4. Definíció. Egy illeszkedési struktúrát *egyszerűnek* nevezünk, ha nincs két olyan blokk, amely ugyanazokra a pontokra illeszkedik. Ekkor a blokkok azonosíthatók a rájuk illeszkedő pontokkal, azaz $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ izomorf a $\mathbf{D}' = (\mathcal{P}, \mathcal{B}', \in)$ struktúrával, ahol $\mathcal{B}' := \{\{p\colon p\mathcal{I}B\}\colon B \in \mathcal{B}\}$.

A továbbiakban csak egyszerű struktúrákról lesz szó. Tegyük fel, hogy az előző azonosítást már elvégeztük, és reláción mindig az „$\in$” relációt értjük. Ekkor B blokk foka helyet B *méretét* mondunk, és $\deg(B)$ helyett $|B|$-vel jelöljük. Például:

- Egy többszörös él mentes hipergráf egyszerű illeszkedési struktúrát alkot.
- Egy egyszerű gráf olyan egyszerű illeszkedési struktúrát alkot, melyben minden blokk 2 elemű.
- Legyen $\mathcal{P} = \{1, \ldots, 7\}$, és

  $$\mathcal{B} = \Big\{\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\}\Big\}.$$

  Ez az úgynevezett Fano sík, melyet a leggyakrabban a alábbi ábrával szemléltetnek, ahol a blokkokat a következő vonalak reprezentálják: a három oldalvonal, a három magasságvonal valamint az egy darab beírt kör.



  Itt a pontok és a blokkok száma egyaránt 7, minden pont foka 3, minden blokk mérete 3.

1.1.5. Definíció. Tekintsük a $\bar{\mathcal{B}} = \{\bar{B}\colon B \in \mathcal{B}\}$ és $\bar{\mathcal{I}} := \{(p, B)\colon (p, B) \notin \mathcal{I}\}$ halmazokat. A $\bar{\mathbf{D}} := (\mathcal{P}, \bar{\mathcal{B}}, \bar{\mathcal{I}})$ struktúrát $\mathbf{D}$ *komplementerének* nevezzük.

Nyilván r-reguláris struktúra komplementere $(|\mathcal{B}| - r)$-reguláris, k-uniformé $(|\mathcal{P}| - k)$-uniform. Például a Fano sík komplementere 7 pontú, 7 blokkú, 4-reguláris, 4-uniform struktúra.

1.1.6. Definíció. Tekintsük a $\mathbf{D}^* = (\mathcal{P}^*, \mathcal{B}^*, \mathcal{I}^*)$ illeszkedési struktúrát, ahol $\mathcal{P}^* = \mathcal{B}$ és $\mathcal{B}^* = \mathcal{P}$, illetve $\mathcal{I}^*$ az $\mathcal{I}$ inverze. Ezt a struktúrát a $\mathbf{D}$ *duálisának* nevezzük. Ha $\mathbf{D}^*$ izomorf $\mathbf{D}$-vel, akkor *önduálisnak* nevezzük.

Ha $\mathbf{D}$ reguláris, akkor $\mathbf{D}^*$ uniform lesz, és fordítva. $\mathbf{D}^*$ akkor lesz egyszerű, ha a $\mathbf{D}$-ben nincs két olyan pont, melyek pontosan ugyanazokra a blokkokra illeszkednek.

1.1.7. Definíció. Készítsünk a $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ illeszkedési struktúrához egy M mátrixot a következőképpen. Legyenek a sorok címkéi $\mathcal{P}$ elemei, az oszlopoké $\mathcal{B}$ elemei. Legyen

$$m_{ij} := \begin{cases} 1, & \text{ha } p_i \mathcal{I} B_j, \\ 0, & \text{különben.} \end{cases}$$

Ezt az M mátrixot a $\mathbf{D}$ *illeszkedési mátrixának* hívjuk. $\mathbf{D}$ *szomszédsági mátrixa* az $MM^\top$ mátrix. Ennek i-edik sorának j-edik eleme azt mutatja meg, hogy hány olyan blokk van, mely az i-edik és j-edik pontot is tartalmazza. Speciálisan a főátlóban a pontok fokai szerepelnek. Hasonlóképpen vehetjük az $M^\top M$ *blokkszomszédsági mátrixot*, mely azt mutatja meg, hogy két blokk hány pontban metszi egymást, főátlójában az egyes blokkok mérete jelenik meg.

Számoljuk meg $\mathcal{I}$ elemeit ($p\mathcal{I}B$ párokat). Pontonként, vagy blokkonként számolva, azt kapjuk, hogy $|\mathcal{I}| = \sum_{p \in \mathcal{P}} \deg(p) = \sum_{B \in \mathcal{B}} \deg(B)$. Legyen $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ r-reguláris, k-uniform struktúrára, ekkor

$$|\mathcal{I}| = vr = bk. \tag{1.1}$$

1.1.8. Definíció. $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ illeszkedési struktúra *négyzetes*, ha $|\mathcal{P}| = |\mathcal{B}|$. Például a Fano-sík négyzetes.

1.2. Projektív terek

1.2.1. Definíció. Legyen $\mathbf{P} = (\Pi, \Lambda)$ pár, ahol Π nemüres halmaz, Λ pedig bizonyos részhalmazainak halmaza. Π elemeit *pontoknak*, Λ elemeit *egyeneseknek* fogjuk hívni. $\mathbf{P}$ -t *projektív síknak* nevezünk, ha:

- Bármely két különböző pontjához pontosan egy olyan egyenes van, mely mindkettőt tartalmazza.

- Bármely két különböző egyeneséhez pontosan egy olyan pont van, amelyet mindkét egyenes tartalmaz.
- Van négy olyan pont, amelyek közül semelyik hármat nem tartalmaz egy egyenes.

1.2.2. Definíció. Egy projektív sík *q-rendű* (véges), ha van olyan egyenese, ami $q+1$ pontot tartalmaz.

Idézzünk fel néhány aritmetikai tulajdonságot, mely megtalálható például [11]-ben.

1.2.1. Állítás. *q-rendű projektív síkban minden egyenesnek $q+1$ pontja van, minden pontot $q+1$ egyenes tartalmaz, valamint a pontok és az egyenesek száma egyaránt q^2+q+1.*

A homogén koordináták segítségével tetszőleges q-elemű testre tudunk projektív síkot építeni, melyet $\mathrm{PG}(2,q)$-val fogunk jelölni. Az eljárás a következő: Tekintsük a $\mathrm{GF}(q)^3 \setminus \mathbf{0}$ -beli vektorok alábbi ekvivalenciáját: $(x_1,x_2,x_3) \sim (y_1,y_2,y_3)$, ha $\exists\ 0 \neq \lambda \in \mathrm{GF}(q)$, hogy $x_i = \lambda y_i$, $i=1,2,3$ -ra. Legyenek Π elemei ennek a relációnak az ekvivalencia osztályai. Mindegyik osztályhoz hozzávéve $\mathbf{0}$-t ez nem más, mint a $\mathrm{GF}(q)^3$ 1-dimenziós altereinek halmaza. Λ elemei legyenek a $\{(x_1,x_2,x_3)\colon x_1u_1+x_2u_2+x_3u_3=0\}$ alakú halmazok. Λ minden eleméhez $\mathbf{0}$-t véve ez épp a 2-dimenziós alterekből áll. Ekkor (Π,Λ) projektív sík lesz. Ezt geometriailag úgy képzelhetjük el, mintha a 3-dimenziós térben Π lenne az origón átmenő „egyenesek", Λ pedig az origón átmenő „síkok" halmaza. Előbbieket irányvektorukkal, utóbbiakat normálvektorukkal adtuk meg. Ezek valóban teljesítik a projektív sík axiómáit. Például $\mathrm{PG}(2,2)$ épp a Fano-síkot adja.

1.2.3. Definíció. Jelölje $\begin{bmatrix} n \\ k \end{bmatrix}_q$ a q elemű véges test feletti n-dimenziós vektortér k-dimenziós altereinek számát. Ezeket *Gauss-féle binomiális együtthatóknak* hívjuk.

Egy ilyen altér bázisának első elemét q^n-1 féle képpen választhatom, a következő nem lehet az előző skalárszorosa, azaz q^n-q féle képpen választhatom, az $i+1$-edik bázisvektor nem lehet az előző i darabb lineáris kombinációja, tehát q^n-q^i féle képpen választhatom... Hasonlóan számolhatjuk ki, hogy k-dimenziós vektortérben $(q^k-1)(q^k-q)\dots(q^k-q^{k-1})$ féle képpen választhatunk bázist. Tehát

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{\Pi_{i=0}^{k-1}(q^n-q^i)}{\Pi_{i=0}^{k-1}(q^k-q^i)} = \frac{\Pi_{i=0}^{k-1}(q^{n-i}-1)}{\Pi_{i=0}^{k-1}(q^{k-i}-1)}.$$

Hasonlóan meghatározható például egy adott r-dimenziós alteret tartalmazó k-dimenziós alterek száma: $\begin{bmatrix} n-r \\ k-r \end{bmatrix}_q$. A projektív síkokhoz hasonlóan tekintsük most a $\mathrm{GF}(q)^{n+1}$ vektortérben „pontnak" az 1-dimenziós altereket, „egyenesnek" a 2-dimenziós altereket, és így tovább. Ezen alterek hálóját $\mathrm{PG}(n,q)$-val jelöljük, és n-dimenziós *projektív térnek* nevezzük. Például $\mathrm{PG}(4,q)$-ban a „síkok" száma $\begin{bmatrix} 5 \\ 3 \end{bmatrix}_q$.

1.3. t-rendszerek

1.3.1. Definíció. Egy $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ illeszkedési struktúrát $t-(v,k,\lambda)$ *rendszernek* hívunk, ha léteznek $t \leq k \leq v$ és λ nem negatív egészek úgy, hogy:

- $|P| = v$,
- Minden blokk mérete k,
- Bármely t pontra pontosan λ darab olyan blokk van, mely mindegyiket tartalmazza.

Megjegyezzük, hogy nem csak az egyszerű struktúrák elégíthetik ki az axiómákat. Például ha összesen 2 olyan blokkom van, ami minden pontot tartalmaz, akkor $v-(v,v,2)$ rendszert kapnék. Mi azonban csak az egyszerű struktúrákat vizsgáljuk. A továbbiakban nem fogunk foglalkozni a $k = v$ és $k \leq 1$ esetekkel, ezek a struktúrák könnyen áttekinthetőek. Megjegyezzük továbbá, hogy $t = 1$ esetben csak annyit tudunk, hogy a struktúra reguláris, $t = k$ esetben pedig minden k elemű részhalmaz blokk.

Tekintsünk egy $t-(v,k,\lambda)$ rendszert. Vegyünk, egy $i \leq t$ elemű $I \subseteq \mathcal{P}$ ponthalmazt, és vizsgáljuk meg az I-n átmenő blokkok számát. Egészítsük ki I-t t-elemű halmazzá, ekkor pontosan λ blokk megy át rajta. Ezt $\binom{v-i}{t-i}$ féleképpen tehetjük meg, de ekkor minden blokkot $\binom{k-i}{t-i}$-szer számoltunk. Tehát az i ponton átmenő blokkok száma:

$$\lambda_i := \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} = \lambda \frac{\frac{(v-i)!}{(t-i)!(v-t)!}}{\frac{(k-i)!}{(t-i)!(k-t)!}} = \lambda \frac{\frac{(v-i)!}{(k-i)!(v-k)!}}{\frac{(v-t)!}{(k-t)!(v-k)!}} = \lambda \frac{\binom{v-i}{k-i}}{\binom{v-t}{k-t}}. \tag{1.2}$$

Megjegyezzük, hogy $\lambda_0 = |\mathcal{B}|$, a blokkok száma, ezt b-vel jelöltük. $\lambda_1 = \deg(p)$ minden $p \in \mathcal{P}$ re, vagyis minden t-rendszer reguláris. λ_1-et r-rel fogjuk jelölni, $\lambda_t = \lambda$. Nyilván $0 < i \leq t \leq k$ esetén egy adott blokk i pontját választva, $\lambda_i > 0$.

1.3.1. Következmény. *Ha létezik* $t-(v,k,\lambda)$ *rendszer, akkor a* $\lambda\frac{\binom{v-i}{k-i}}{\binom{v-t}{k-t}}$ *szám pozitív egész minden* $i=0,\dots,t$*-re.*

Tehát $i=0,\dots,t$-re

$$\lambda_i=\lambda\frac{(v-i)\dots(v-t+1)}{(k-i)\dots(k-t+1)}, \text{ amiből}$$

$$\lambda_i=\lambda_{i+1}\frac{(v-i)}{(k-i)} \qquad (i=0,\dots,t-1). \tag{1.3}$$

$\lambda=1$ esetén a $t-(v,k,1)$ rendszereket *Steiner rendszereknek* nevezzük. Ezekről bővebben [4]-ben és [5]-ben olvashatunk.

$t=2$ esetén röviden csak *blokkrendszerről* beszélünk. Ekkor

$$\lambda_1=r=\lambda\frac{v-1}{k-1}, \qquad \lambda_0=b=\lambda\frac{v(v-1)}{k(k-1)}.$$

1.3.2. Következmény. *Ha létezik* $2-(v,k,\lambda)$ *blokkrendszer, akkor*

$$\lambda(v-1)\equiv 0 \pmod{k-1},$$

$$\lambda v(v-1)\equiv 0 \pmod{k(k-1)}.$$

Például:

- Minden $t-(v,k,\lambda)$ rendszer $s-(v,k,\lambda_s)$ rendszer is egyben minden $s\le t$-re.
- Egy v elemű halmaz összes k elemű részhalmaza $t-(v,k,\binom{v-t}{k-t})$ rendszert alkot minden $t\le k$-ra. Ezeket *triviális rendszereknek* nevezzük.
- A Fano-sík $2-(7,3,1)$-rendszert alkot.
- A véges projektív síkok $2-(q^2+q+1,q+1,1)$-rendszert alkotnak.
- Legyen $\mathcal{P}$ a $\mathrm{PG}(n,q)$ pontjai, $\mathcal{B}$ a $\mathrm{PG}(n,q)$ d-dimenziós alterei, vagyis az $(n+1)$-dimenziós vektortérben az 1 és $(d+1)$-dimenziós alterek. Ekkor bármely két különböző 1-dimenziós altér kifeszít egy 2-dimenziós alteret, melyet pontosan $\begin{bmatrix}n+1-2\\ d+1-2\end{bmatrix}_q$ darab $(d+1)$-dimenziós altér (vagyis blokk) tartalmaz. Így tehát egy $2-(\begin{bmatrix}n+1\\ 1\end{bmatrix}_q,\begin{bmatrix}d+1\\ 1\end{bmatrix}_q,\begin{bmatrix}n-1\\ d-1\end{bmatrix}_q)$ blokkrendszert definiáltunk, amit $\mathrm{PG}_d(n,q)$-val jelölünk. Ennek további paraméterei $r=\begin{bmatrix}n\\ d\end{bmatrix}_q$ és $b=\begin{bmatrix}n+1\\ d+1\end{bmatrix}_q$. Ez pontosan akkor lesz négyzetes, ha $d=n-1$. Például $\mathrm{PG}_1(2,q)$-ra épp az előző példát kapjuk.

- A $2-(4\lambda+3, 2\lambda+1, \lambda)$ paraméterű blokkrendszereket *Hadamard-féle blokkrendszereknek* nevezzük. Ezekről [3] és [6] tartalmaz bővebb leírást.

A következő tételek [6]-ból származnak, bizonyításukhoz is ezt ajánljuk.

1.3.1. Tétel. *(Fisher-egyenlőtlenség)* $2-(v,k,\lambda)$ *blokkrendszerben* $k<v$ *esetén* $b \geq v$.

További feltételeket bizonyított Ray-Chaudhuri és Wilson.

1.3.2. Tétel. *Legyen* $\mathbf{D}$ $t-(v,k,\lambda)$*-rendszer, ahol* $t=2s$ *és* $k \leq v-s$. *Ekkor* $b \geq \binom{v}{s}$.

1.3.3. Tétel. *Legyen* $s \leq k \leq v-s$ *és legyen* $\mathbf{B}$ *egy* v *pontú* V *halmaz* k *elemű részhalmazainak olyan családja, melyre* $|B \cap B'|$ *legfeljebb* s *értéket vesz fel, ha* $B \neq B' \in \mathbf{B}$. *Ekkor* $\mathbf{B} \leq \binom{v}{s}$.

1.4. Négyzetes blokkrendszerek

Ezt a témát csak érintjük, a legtöbb állítást bizonyítás nélkül mondjuk ki. Bővebb tanulmányozásukhoz [6]-t és [3]-t érdemes átnézni.

Emlékezzünk, hogy definíció szerint egy illeszkedési struktúra négyzetes, ha $|P| = |B|$. Blokkrendszerek esetében ez azt jelenti, hogy $b = v$, ami az (1.1) összefüggés miatt ekvivalens azzal, hogy $r = k$, illetve a

$$v = \frac{k(k-1)}{\lambda} + 1 \tag{1.4}$$

összefüggéssel.

1.4.1. Lemma. *Jelölje* $\mathbf{I}$ *az* $n \times n$ *-es egységmátrixot,* $\mathbf{J}$ *pedig az* $n \times n$ *-es csupa 1-esből álló mátrixot. Ekkor* $\det(x\mathbf{I} + y\mathbf{J}) = (x+yn)x^{n-1}$.

Bizonyítás. Legyen $A = x\mathbf{I} + y\mathbf{J}$. A csupa egyesből álló $\mathbf{j}$ vektor sajátvektora lesz az A-nak, méghozzá $x+yn$ sajátértékkel. Mivel A szimmetrikus, így létezik olyan sajátvektorokból álló ortogonális bázisa, ami tartalmazza $\mathbf{j}$-t. Bármely másik $\mathbf{v}$ báziselemre tehát igaz lesz, hogy $\mathbf{vJ} = \mathbf{0}$. Tehát $\mathbf{v}(x\mathbf{I} + y\mathbf{J}) = x\mathbf{v}$, azaz a $\mathbf{v}$-hez tartozó x sajátérték $n-1$-szeres lesz. □

1.4.1. Következmény. *Blokkrendszer szomszédsági mátrixának determinánsa:* $\det(MM^\top) = rk(r-\lambda)^{v-1}$.

Mivel tudjuk, hogy $r = k$ és $\det(M) = \det(M^\top)$, azt kapjuk, hogy $\det(M)^2 = k^2(k-\lambda)^{v-1}$, így a következőt kapjuk:

1.4.2. Következmény. *(Shützenberger)* $2-(v,k,\lambda)$ *négyzetes blokkrendszerben* $(k-\lambda)^{v-1}$ *négyzetszám (azaz* v *páratlan vagy* $k-\lambda$ *négyzetszám).*

1.4.1. Tétel. *Négyzetes* $2-(v,k,\lambda)$*, és* $1<k<v$ *esetén*

$$4(k-\lambda)-1 \leq v \leq (k-\lambda)^2+(k-\lambda)+1.$$

Az alsó határ élességét az Hadamard blokkrendszerek, míg a felső határ élességét a projektív síkok igazolják.

1.4.2. Tétel. *Négyzetes* $2-(v,k,\lambda)$ *blokkrendszer esetén bármely két különböző blokk metszete* λ *elemű.*

1.4.3. Következmény. *Négyzetes* $2-(v,k,\lambda)$ *blokkrendszer duálisa is egy négyzetes* $2-(v,k,\lambda)$ *blokkrendszer lesz, mely azonban nem feltétlenül izomorf az eredetivel.*

1.5. Metszési háromszög

E szakaszhoz [7], [2], és [5] nyújtottak segítséget. Egy $t-(v,k,\lambda)$ rendszerben tekintsünk egy i elemű I, és egy tőle diszjunkt j elemű J ponthalmazt. Jelölje $\mathrm{b}(I,J)$ azon blokkok számát, amik tartalmazzák az I halmazt, és diszjunktak a J halmazzal.

1.5.1. Állítás. $i+j \leq t$ *esetén* $b(I,J)=\lambda c(i,j,t,v,k)$*, ahol* $c(i,j,t,v,k)$ *csak az* i,j,t,v,k *paraméterektől függ.*

Bizonyítás. $|J|$ szerinti indukcióval: $|I| \leq t$ esetén $\mathrm{b}(I,\emptyset)=\lambda\frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$. Tegyük fel, hogy $|J|-1$-re már beláttuk. Vegyünk egy $p \in J$ pontot, és számoljuk meg az I-t tartalmazó, de $J\setminus\{p\}$ -vel diszjunkt blokkok számát. p vagy benne van egy ilyen blokkban, vagy nincs, tehát $\mathrm{b}(I,J\setminus\{p\})=\mathrm{b}(I\cup\{p\},J\setminus\{p\})+\mathrm{b}(I,J)$. Az indukciós feltevés miatt

$$\mathrm{b}(I,J)=\mathrm{b}(I,J\setminus\{p\})-\mathrm{b}(I\cup\{p\},J\setminus\{p\})=$$
$$=\lambda\Big(c(i,j-1,t,v,k)-c(i+1,j-1,t,v,k)\Big),$$

ahol $c(i,j-1,t,v,k)-c(i+1,j-1,t,v,k)$ csak az i,j,t,v,k paraméterektől függ. □

$c(i,j,t,v,k)$ nem függ a λ paramétertől. Triviális rendszerek esetén (ahol minden k elemű részhalmaz blokk) $\mathrm{b}(I,J)=\binom{v-i-j}{k-i}$. Azaz

$$c(i,j,t,v,k)=\frac{\mathrm{b}(I,J)}{\lambda}=\frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}.$$

1.5.1. Definíció. $0 \leq i+j \leq t$ esetén jelölje λ_i^j egy $t-(v,k,\lambda)$ rendszerben azon blokkok számát, melyek egy i elemű halmazt tartalmaznak, és egy tőle diszjunkt j elemű halmazzal diszjunktak.

Ekkor tehát

$$\lambda_i^j = \lambda \frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}, \tag{1.5}$$

$$\lambda_i^j = \lambda_i^{j-1} - \lambda_{i+1}^{j-1} \quad (0 < j, i < t \text{ esetén}). \tag{1.6}$$

Megjegyezzük, hogy az (1.5) képlet indukcióval is belátható (1.2) és (1.6) miatt.

Vagyis $\lambda \neq 0$, $t-(v,k,\lambda)$ rendszer esetén minden $0 \leq i+j \leq t$-re a λ_i^j-nek pozitív egésznek kell lennie. Ez azonban, mint azt láni fogjuk, már következik abból, hogy a λ_i-k pozitív egészek.

1.5.1. Lemma. *Legyenek $0 \leq t \leq k \leq v$ és $0 < \lambda$ rögzített egész számok. Azon i, j egész számokra, ahol $i+j \leq v$ és $i \leq k$, legyen*

$$c(i,j) := \lambda \frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}.$$

Ekkor $c(i,j) > 0$, valamint minden $i+j \leq v$ és $i < k$ esetén

$$c(i,j) = c(i,j-1) - c(i+1,j-1).$$

Továbbá ha léteznek z_1, z_2, j_0 (nem feltétlenül pozitív) egész számok úgy hogy minden $z_1 \leq i \leq z_2$ és $j = j_0$ esetén a $c(i,j)$ számok egészek, akkor minden $i \geq z_1$, $j \geq j_0$, $i+j \leq z_2$ esetén is a $c(i,j)$ egész sám lesz.

Bizonyítás. $c(i,j) > 0$ triviális. A rekurzióhoz a $\lambda/\binom{v-t}{k-t}$ konstans szorzó miatt azt kell belátnunk, hogy

$$\binom{v-i-j}{k-i} = \binom{v-i-j+1}{k-i} - \binom{v-i-j}{k-i-1},$$

ami a binomiális együtthatók összefüggése miatt igaz.

Az utolsó részt képzeljük el szemléletesen. Vegyünk egy (i,j) koordináta-rendszert. Ekkor a rekrzió azt jelenti, hogy minden (i,j) ponthoz tartozó $c(i,j)$ az alatta, és jobbra-alatta levő, $c(i,j-1)$-nek és $c(i+1,j-1)$-nek a különbsége. Így ha van egy vízszintes szakaszom, ahol a $c(i,j)$ függvény értéke egész, akkor arra tudok építeni egy olyan háromszöget, ahol szintén minden függvényérték egész lesz. Ezt a háromszöget épp az állításban leírt

tartományok határolják. □

Legyen **D** egy $t-(v,k,1)$ Steiner-rendszer, és B egy blokkja. Legyen $I,J \subseteq B$. Ekkor a $\mathrm{b}(I, J\setminus\{p\}) = \mathrm{b}(I\cup\{p\}, J\setminus\{p\}) + \mathrm{b}(I,J)$ rekurzió ugyanúgy igaz minden $p\in J$-re. Mivel itt $|I|>t$ esetén $\mathrm{b}(I,\emptyset)=1$, így Steiner rendszerek esetén kiterjeszthető a λ_i^j definíciója:

1.5.2. Definíció. Legyen **D** egy $t-(v,k,1)$ Steiner-rendszer, és B egy blokkja. Legyen $I,J\subseteq B$, és $I\cap J=\emptyset$. $i:=|I|$, $j:=|J|$. Jelölje λ_i^j azon blokkok számát, melyek I-t tartalmazzák, és J-vel diszjunktak.

Ekkor tehát

$$\begin{array}{ll}\lambda_i^j = 1\cdot\frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}} & \text{, ha } i+j\le t,\\ \lambda_i^0 = 1 & \text{, ha } t<i\le k,\\ \lambda_i^j = \lambda_i^{j-1}-\lambda_{i+1}^{j-1} & \text{, ha } 0<j\le k, i<k.\end{array}$$

1.5.3. Definíció. Legyen B egy $t-(v,k,\lambda)$ rendszer blokkja. Jelölje $n_i(B)$ azon blokkok számát, melyek a B blokkot pontosan i pontban metszik. ($n_k(B)=1$.)

Láttuk, hogy Steiner-rendszer esetén $n_i(B)$ nem függ B választásától, ekkor ugyanis $n_i(B)=\binom{k}{i}\lambda_i^{k-i}$.

1.5.2. Állítás. $\lambda_i^j = \sum_{l=0}^{j}(-1)^l\binom{j}{l}\lambda_{i+l}$

Bizonyítás. j szerinti indukcióval: $j=0$-ra $\lambda_i^0=\lambda_i$, j=1-re pedig $\lambda_i^1=\lambda_i-\lambda_{i+1}$, ami az (1.6) összefüggés miatt szintén igaz. Tegyük fel, hogy j-ig már beláttuk. Ekkor:

$$\lambda_i^{j+1}=\lambda_i^j-\lambda_{i+1}^j=\sum_{l=0}^{j}(-1)^l\binom{j}{l}\lambda_{l+i}-\sum_{l=0}^{j}(-1)^l\binom{j}{l}\lambda_{l+i+1}.$$

Az első szummából hozzuk ki az első tagot, ami $\binom{j}{0}\lambda_i=\lambda_i$. A második szummát átparaméterezve

$$-\sum_{l'=1}^{j+1}(-1)^{l'-1}\binom{j}{l'-1}\lambda_{l'+i}\text{ -t kapunk.}$$

Végezzük el a (-1)-gyel való szorzást, és hozzuk ki az utolsó tagot, vagyis

$$\sum_{l'=1}^{j}(-1)^{l'}\binom{j}{l'-1}\lambda_{l'+i}+(-1)^{j+1}\lambda_{j+i+1}.$$

Így tehát:

$$\lambda_i^{j+1} = \lambda_i + \sum_{l=1}^{j} (-1)^l \binom{j}{l} \lambda_{l+i} + \sum_{l=1}^{j} (-1)^l \binom{j}{l-1} \lambda_{l+i} + (-1)^{j+1} \lambda_{j+i+1}.$$

Ami a binomiális együtthatók összefüggése miatt éppen:

$$\lambda_i^{j+1} = \lambda_i + \sum_{l=1}^{j} (-1)^l \binom{j+1}{l} \lambda_{l+i} + (-1)^{j+1} \lambda_{j+i+1} = \sum_{l=0}^{j+1} (-1)^l \binom{j+1}{l} \lambda_{l+i}.$$

□

A $\lambda_i^j = \lambda_{i+1}^j + \lambda_i^{j+1}$ rekurzió miatt ezeket a számokat háromszög formába szokták rendezni, ahol minden szám az alatta lévő kettőnek az összege (az angol nyelvű szakirodalmoban ezt *intersection triangle*-nek hívják).

$$\lambda_0$$

$$\lambda_1 \quad \lambda_0^1$$

$$\lambda_2 \quad \lambda_1^1 \quad \lambda_0^2$$

$$\dots$$

Ezzel tehát egy nagyon könnyen programozható algoritmust kapunk. Az A.1 függelékben egy olyan egyszerű, VBA Excel makrót láthatunk, mely adott paraméterek esetén leelenőrzi az 1.3.1 következmény feltételeit, és kiírja a kiterjesztett metszési háromszöget (λ_i^j-t az $(i+1)$-dik sor $(j+1)$-dik cellájába).

Például a $2-(7,3,1)$ Fano-sík esetén a háromszög:

$$7$$

$$3 \quad 4$$

$$1 \quad 2 \quad 2$$

$$1 \quad 0 \quad 2 \quad 0$$

Nem csak a paraméterek határozzák meg a háromszöget, ez visszafelé is igaz. Ha például egy másik struktúrából kapott t-rendszert keresünk, és már ismerjük a háromszöget, abból kiolvashatóak a paraméterek ($t > 1$ esetén). (1.3) miatt

$$\begin{aligned}
\lambda_0 = \frac{v}{k}\lambda_1 \quad &\text{és} \quad \lambda_1 = \frac{v-1}{k-1}\lambda_2, \\
\lambda_1(k-1) &= (\frac{\lambda_0 k}{\lambda_1} - 1)\lambda_2, \\
\lambda_1^2 k - \lambda_1^2 &= \lambda_0\lambda_2 k - \lambda_1\lambda_2, \\
(\lambda_1^2 - \lambda_0\lambda_2)k &= \lambda_1^2 - \lambda_1\lambda_2.
\end{aligned}$$

Azaz

$$b = \lambda_0, \quad r = \lambda_1, \quad \lambda = \lambda_t, \quad k = \tfrac{\lambda_1(\lambda_1-\lambda_2)}{\lambda_1^2-\lambda_0\lambda_2}, \quad v = \tfrac{\lambda_0(\lambda_1-\lambda_2)}{\lambda_1^2-\lambda_0\lambda_2}.$$

Ekkor azonban oda kell figyelnünk arra, hogy ezek csak szükséges feltételek! Habár meg tudjuk határozni, hogy adott számok esetén milyen paraméterű t-rendszernek lenne ez a metszési háromszöge, ebből egyáltalán nem következik az, hogy ilyen rendszer létezik. Ráadásul vannak azonos paraméterű, nem izomorf rendszerek is. Tehát a metszési háromszög nem határozza meg a struktúrát, csak jellemzi.

1.6. Konstrukciók

Legyen $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \in)$ egy $t-(v,k,\lambda)$ rendszer.

- $\mathbf{D}^* = (\mathcal{B}, \mathcal{P}, \in^*)$ a $\mathbf{D}$ duálisa. A $\mathbf{D}^*$ struktúra pontjainak száma b, valamint (mivel $\mathbf{D}$ r-reguláris volt) r-uniform. Nem biztos azonban, hogy $t^* > 1$ -re $t^*-(b,r,\lambda^*)$ rendszert kapunk.

  Tegyük fel, hogy mégis így van. Ha $k = v$, akkor minden blokk minden pontot tartalmaz, ami a duálisra is igaz, viszont ekkor csak v=1-re lesz a duális egyszerű. Mivel $\mathbf{D}$ egy $2-(v,k,\lambda_2)$ rendszer is, így $v > k$ esetén a Fisher egyenlőtlenség miatt $b \geq v$. Tudjuk, hogy $b = r\frac{v}{k}$, azaz $v > k$ -ból következik $b > r$, így a duális rendszerre a Fisher-egyenlőtlenség $v \geq b$ -t ad. Ekkor tehát $b = v$, azaz a $\mathbf{D}$ négyzetes. Az 1.4.3 következmény miatt tehát $\mathbf{D}$ blokkrendszer duálisa akkor és csak akkor lesz blokkrendszer, ha $\mathbf{D}$ négyzetes, és ekkor a duálisnak ugyanazok lesznek a paraméterei, amiből $\lambda^{*j}_i = \lambda^j_i$ következik.

- $\bar{\mathbf{D}} = (\mathcal{P}, \bar{\mathcal{B}}, \notin)$ egy $t-(v, v-k, \lambda_0^t)$ rendszer. Ebben tehát egy $I \subseteq \mathcal{P}$ halmazon pontosan azok a blokkok mennek át, amik az eredetiben nem, azaz $\bar{\lambda}^j_i = \lambda^i_j$. Ez szemléletesen azt jelenti, hogy a metszési háromszöget tükrözzük.

Vizsgáljuk meg, hogy mikor lesz a háromszög szimmetrikus (nem Steiner rendszer esetén). Ehhez az kell tehát, hogy $\lambda_i^j = \lambda_j^i$, azaz

$$\lambda\frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}} = \lambda\frac{\binom{v-j-i}{k-j}}{\binom{v-t}{k-t}},$$

$$\frac{(v-i-j)!}{(k-i)!(v-k-j)!} = \frac{(v-i-j)!}{(k-j)!(v-k-i)!},$$

$$(k-i)!(v-k-j)! = (k-j)!(v-k-i)!.$$

Látszik, hogy $v = 2k$ esetén ez teljesül. Mindazonáltal, ha $\mathbf{D}$ háromszöge szimmetrikus, akkor $\bar{\mathbf{D}}$ háromszöge ezzel megegyezik, és láttuk, hogy ekkor a paramétereik is, így k=v-k. Tehát $\lambda \neq 1$ esetben $\mathbf{D}$ háromszöge akkor és csak akkor szimmetrikus, ha v=2k.

- Minden $0 \leq s \leq t$-re a $\mathbf{D}$ $s-(v,k,\lambda_s)$ rendszer is egyben. Ezekben ugyanazok lesznek a λ_i^j-k $i+j \leq s$-re. Ennek tehát a (nem kiterjesztett) metszési háromszöge ugyanúgy néz ki, mint az eredetié, csak hiányzik az alsó $t-s$ sor (illetve Steiner-rendszerek esetén a kiterjesztett, $k-t$ sor).

- **1.6.1. Definíció.** Legyen $p \in \mathcal{P}$. $\mathcal{P}_p := \mathcal{P}\backslash\{p\}$, $\mathcal{B}_p := \{B \in \mathcal{B}\colon p \in B\}$. Ekkor $\mathbf{D}_p = (\mathcal{P}_p, \mathcal{B}_p, \in)$-t a $\mathbf{D}$ p pontra vonatkozó *derivált rendszerének* hívjuk.

  Ez egy $(t-1)-(v-1,k-1,\lambda)$-rendszer, ahol $(\lambda_p)_i^j = \lambda_{i+1}^j$. Ennek metszési háromszöge úgy néz ki, hogy az eredetiből elhagyjuk a „jobb szélső oldalt".

  Például a Fano-sík deriváltjának háromszöge:

  3

  1 2

  1 0 2

- **1.6.2. Definíció.** Legyen $p \in \mathcal{P}$. $\mathcal{P}^p := \mathcal{P} \setminus \{p\}$, $\mathcal{B}^p := \{B \in \mathcal{B}\colon p \notin B\}$. Ekkor $\mathbf{D}^p = (\mathcal{P}^p, \mathcal{B}^p, \in)$-t a $\mathbf{D}$ p pontra vonatkozó *pont-reziduális rendszerének* hívjuk.

  Ez egy $(t-1)-(v-1,k,\lambda_{t-1}^1)$-rendszer, ahol $(\lambda^p)_i^j = \lambda_i^{j+1}$. Itt tehát a háromszögből a „bal szélső oldalt" kell elhagyni (illetve Steiner rendszer esetén a plusz sorokat). (1.5) miatt

$$\lambda_{t-1}^1 = \lambda\frac{\binom{v-t}{k-t+1}}{\binom{v-t}{k-t}} = \lambda\frac{\frac{(v-t)!}{(k-t+1)!(v-k-1)!}}{\frac{(v-t)!}{(k-t)!(v-k)!}} = \lambda\frac{v-k}{k-t+1}.$$

Láttuk tehát, hogy a metszési háromszög jól szemlélteti a konstrukcióknál a kapcsolatot az eredeti struktúrával. Utóbbi 3 esetben azonban csökkentettük a rendszer méretét, ami önmagában nem túl hasznos. Sokkal izgalmasabb feladat megvizsgálni annak a lehetőségét, hogy az adott rendszerünk egy nagyobb rendszerből keletkezett a fenti konstrukciók valamelyikével. Az 1.5.1 lemma miatt az 1.3.1 következmény és (1.3) összefüggés segítségével könnyen meghatározhatjuk, mik a szükséges feltételei annak, hogy ezeket visszafelé alkalmazzuk. Duális esetén láttuk, hogy csak négyzetes struktúráknál kapunk blokkrendszert, ekkor azonban nem változnak a paraméterek. Komplementer komplementere az eredeti, így itt sem érdemes a visszafele irányt vizsgálni.

Nézzük a harmadik konstrukciót. Tegyük fel, hogy $s < k$ esetén van egy $s-(v,k,\lambda_s)$ rendszerünk, ami azonban egy nagyyobb $(s+1)-(v,k,\lambda_{s+1})$ rendszert is alkot. Ekkor tehát a λ_{s+1} -nek is egésznek kell lennie, azaz (1.3) miatt

$$\lambda_{s+1} = \lambda_s \frac{(k-s)}{(v-s)}, \text{ vagyis}$$

$$\lambda_s(k-s) \equiv 0 \pmod{v-s}.$$

Az 1.5.1 lemma miatt ahhoz, hogy a nagyobb háromszögben minden szám pozitív egész legyen, a fenti feltétel teljesülése már elegendő.

A deriválás visszafordításánál arra lesz szükségünk, hogy a nagyobb rendszerben a blokkok száma legyen egész, itt is az 1.5.1 lemma miatt ebből már következik, hogy a többi szám is pozitív egész lesz. Azaz $\lambda_0(v+1) \equiv 0 \pmod{k+1}$ -nek kell teljesülnie. (Kiszámolható, hogy q-adrendű projektív síkoknál ez csak $q = 2$ vagy 4-re teljesül.)

Végül tegyük fel, hogy $t < k$ esetén a $\mathbf{D}$ $t-(v,k,\lambda)$ rendszer az $\mathbf{M}$ pont-reziduálisa. Ekkor $\mathbf{M}$ paraméterei $(t+1)-(v+1,k,\hat{\lambda})$, ahol

$$\begin{aligned} \lambda &= \hat{\lambda}\frac{(v+1)-k}{k-(t+1)+1}, \text{ vagyis} \\ \hat{\lambda} &= \lambda\frac{k-t}{v-k+1}, \end{aligned}$$

azaz $\lambda(k-t) \equiv 0 \pmod{v-k+1}$ kell, hogy teljesüljön. A többi érték már (1.3) miatt pozitív, (1.6) miatt pedig egész lesz.

Ezek a szükséges feltételek szintén könnyedén programozhatók, így adott t-rendszer esetén akár egyből meghatrozhatjuk annak a legagyobb rendszernek (ha létezik) a metszési háromszögét is, amiből az adott t-rendszer a fenti konstrukciókkal létrejött.

2. fejezet

Hibajavító kódok

2.1. Bevezetés

Egy hosszú cikket olvasva előfordul, hogy félregépelést fedezünk fel. Jó esetben a hibásan leírt szó nagyon hasonlít az eredeti szóhoz, így könnyen értelmezhető marad a szöveg. Azonban például egy igekötőt viszonylag könnyű elírni, és ez szerencsétlenebb esetben akár a mondat értelmét is megváltoztathatja. Célunk olyan „nyelvet" használni, amiben az értelmes szavak eléggé különböznek egymástól, hogy az esetleges hibák könnyen felismerhetők legyenek.

Alapvetően tehát információt szeretnénk küldeni egy zajos csatornán keresztül, akár térben (például telekommunikáció, űrkutatás), akár időben (például adattároló eszközök) úgy, hogy az esetleges torzulások ne okozzanak információveszteséget. Ezt, mint később látni fogjuk, úgy tudjuk elérni, ha az eredeti információt bizonyos szabályokat követve plusz karakterekkel egészítjük ki. Gyakorlatban a küldendő üzenetet adott hosszúságú (általában bináris) számsorozattá alakítjuk, ezt hívjuk kódolásnak.

A következő motiváló példákhoz [8] nyújtott segítséget.
Például:

- Ha egy távolban lévő embernek háromszor kiabálom el ugyanazt, jó eséllyel legalább kétszer jól érti meg, és így még akkor is tudni fogja, mit akartam mondani, ha legfeljebb egyszer nem hallotta rendesen. Ennek viszont az a hátránya, hogy az eredeti mondanivaló hosszát háromszorosára növeltem, így annak közlése háromszor annyi időt, energiát igényel. Arról nem is beszélve, hogy megbízható csatorna esetén ez felesleges többletet jelent.
  A kódolással tehát kettős célunk van, minél rövidebb szavakkal, minél megbízhatóbb „nyelvet" kreálni. A kettő ellentmond egymásnak, mindig

az adott feladat határozza meg, melyiket válasszuk.

- A számítógép részegységei kábellel vannak összekötve, ami megbízható csatornának minősül. Az ASCII jelkészletet használva 128 féle adatot közölhetünk, amit egy 7 hosszú bináris vektor jelképez. Olykor azonban itt is előfordulhatnak jeltorzulások (mondjuk ha valaki felkapcsol a közelben egy neon fénycsövet), ezért a kódot egy nyolcadik bittel egészítik ki úgy, hogy a 8 elem között páros sok egyes szerepeljen. Ekkor, ha pontosan 1 helyen megváltozik az üzenet, akkor azt a fogadó látni fogja, mivel olyan sorozatot kapott, amiben páratlan sok egyes van. (Azt mondjuk, hogy ez a kód 1 hibát jelez.)

- Az Európában használt EAN-13 vonalkódok esetében a 12, információt tároló számhoz egy 13-dik, ellenőrző számjegyet adnak. A számokat egy speciális módon is ábrázolják, melyet a megfelelő készülék gyorsan le tud olvasni. Itt is előfordul azonban, hogy felületi sérülés, gyűrődés miatt a precíz optikai műszer „másnak látja" a számsort. Ilyenkor felismeri, hogy amit lát, nem egy érvényes vonalkód, és hibát jelez. Ekkor néhány újabb, sikertelen kísérlet után a megbízhatóbb csatornára kell váltani, és szemmel leolvasni az arab számokat.
  Ezeknél a példáknál fontosabb volt a csatornán a gyors információáramlás, valamint a ritkán előforduló hibákat gyorsan fel lehetett ismerni, és javítani. (Hasonló a helyzet a személyigazolvány szám, adószám, a könyvek ISBN száma, stb. esetén is.)

- Van viszont, amikor a megbízhatóság a fontosabb. A Mariner űrszonda 1969-ben a Marsról készített fotókat, melyeket a Földre sugárzott. Minden képkocka a szürke 64 árnyalatának egyike volt, amiket egy 32 hosszú bináris vektorral helyettesítettek (ami nagyjából 4,3 millió lehetőséget jelent). Erre azért volt szükség, mert a beérkezett jel nagyon gyenge volt, az óhatatlanul jelenlévő zaj gyakran megváltoztatta a beérkezett üzenetek egy-egy bitjét. Ugyanakkor, mivel az adatokat csak jóval később dolgozták föl, továbbá lehetetlen volt újrapróbálkozni, ezért jobban megérte egy sokkal hosszabb, ámde megbízhatóbb kódolást használni.

- Akadnak olyan helyzetek is, amikor a zaj jellege a meghatározóbb. Például a CD megkarcolásakor egymás melletti biteket rongálunk, úgynevezett csomós hibát hozunk létre. Ezt a kódátfűzésnek nevezett eljárással küszöbölik ki, így a fizikailag közeli bitek valójában logikailag távol vannak egymástól, így karcolás esetén is nagy hosszúságú, ép szakaszok maradnak a kódból.

A továbbiakban az úgynevezett blokk-kódokról beszélünk, ahol az üzenetet hossza rögzített.

2.1.1. Definíció. Legyen Q egy véges halmaz. Q-t *ábécének* fogjuk hívni, az elemeiből képzett n hosszú sorozatokat (vagy sorvektorokat) pedig *szavaknak*. Néhány szót kitüntetünk, ezeket *kódszavaknak*, ezek halmazát pedig *kódnak* hívjuk, és C-vel jelöljük. Azaz $C \subseteq Q^n$.

Elküldjük tehát a $c \in C$ kódszót, azonban a fogadó egy $c' \in Q^n$ szót kap, amiből vissza kell nyernie c-t. Ezt hívjuk dekódolásnak, ez általában nehéz feladat, ezért úgy kell megválasztanunk a C halmazt, hogy ez egyszerű legyen. A dekódolás módszereivel ebben a dolgozatban nem foglalkozunk.

2.1.2. Definíció. Két szó *Hamming-távolságán* az eltéréseik számát értjük, azaz $x, y \in Q^n$ esetén $d(x, y) := |\{i \colon x_i \neq y_i, i = 1, \ldots, n\}|$.

Könnyen ellenőrizhető, hogy ez valóban távolság. Akkor járunk tehát jól, ha a C elemei elég messze vannak egymástól, és csoportosítani tudjuk a Q^n halamazt a kódszavak szerint. Ekkor ugyanis bármely kapott x szóhoz a hozzá legközelebb lévő $c \in C$ -t gondoljuk a küldött üzenetnek.

2.1.3. Definíció. C kód *minimális vávolsága*: $\min\{d(c_1, c_2) \colon c_1, c_2 \in C, c_1 \neq c_2\}$. Egy C kód *paraméterei*: $(n, M, d)_q$, ahol n az üzenet hossza, M a kódszavak száma ($|C|$), d a minimális távolsága, q pedig az ábécé elemszáma ($|Q|$). Legyen $0 \in Q$. Egy x szó *súlya* a nem nulla karaktereinek a száma, vagyis $\mathrm{w}(x) := d(x, \mathbf{0})$. C kód *minimális súlya*: $\min\{\mathrm{w}(c) \colon \mathbf{0} \neq c \in C\}$.

2.1.4. Definíció. Vegyünk egy c kódszót, és tekintsük azokat a szavakat, amelyek maximum e helyen különböznek tőle. Ezt a c középpontú, e sugarú *Hamming-gömbnek* hívjuk: $\mathrm{B}(c, e) = \{x \colon d(x, c) \leq e\}$.

2.1.5. Definíció. Egy C kód *t-hibajelző*, ha a kiindulási c kódszót legfeljebb t helyen megváltoztatva a kapott x szó csak akkor lesz kódszó, ha nem történt változtatás, különben nem. Azaz, ha a minimális távolság $> t$.

2.1.6. Definíció. Egy C kód *e-hibajavító*, ha a kiindulási c kódszót legfeljebb e helyen megváltoztatva a kapott x szóból egyértelműen ki tudom találni az eredeti c-t. Azaz minden $x \in Q^n$ szóhoz legfeljebb egy olyan $c \in C$ kódszó létezik, amire $d(x, c) \leq e$. A C kód éppen akkor e-hibajavító, ha a $\mathrm{B}(c, e)$ gömbök minden $c \in C$-re páronként diszjunktak. Másképpen, ha a minimális távolság $> 2e$.

2.1.1. Tétel. *(Hamming-korlát): e-hibajavító kód esetén*

$$M \leq \frac{q^n}{\sum_{i=0}^{e} \binom{n}{i}(q-1)^i}. \tag{2.1}$$

Bizonyítás. A nevezőben szereplő kifejezés éppen azt mutatja, hogy hányféleképpen tudok egy kódszót maximum e helyen megváltoztatni (a Hamming-gömb térfogata). Mivel a gömbök páronként diszjunktak, ezért $|C| \cdot |\mathrm{B}(c, e)| \leq |Q^n|$. □

Látható, hogy minél nagyobb az e (és így a d is), annál több nem-kódszó lesz a szavak között. Például legyen a C az azonos karakterekből álló sorozatok, azaz egy $b \in Q$ karaktert n-szer fogunk elküldeni. Ezt *ismétlő kódnak* nevezzük, a paraméterei: $(n, q, n)_q$. Ez nyilván $\lfloor \frac{n-1}{2} \rfloor$ hibát javít, ugyanakkor n-szeresére növeltem az eredeti információt. *Triviális kódoknak* hívjuk az ismétlő, és az egyelemű kódokat. A kódolásnál kettős célunk van: Nem túl hosszú, sok hibát javító kódot előállítani. Ahogy a bevezetőben is említettük, mindig az adott feladat határozza meg, melyiket részesítjük előnyben.

2.1.7. Definíció. Egy e-hibajavító kódot *perfektnek* nevezünk, ha minden szóhoz pontosan egy olyan kódszó létezik, ami tőle legfeljebb e távolságra van.

Például az ismétlő kód $q = 2$ és páratlan n esetén perfekt, $q > 2$ esetén azonban nem.
Ez tehát azt jelenti, hogy a Hamming gömbök (azon túl, hogy egyrétűen) hézagmentesen is lefedik a szavakat (a „szükséges" nem-kódszavakon kívül nem lesznek „felesleges" nem-kódszavak). Vagyis a Hamming korlát egyenlőséggel teljesül, azaz

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

Láttuk, hogy e-hibajavító kód esetén $d > 2e$. Ha a kód perfekt, e-hibajavító, akkor $d = 2e+1$. Vegyünk ugyanis egy c_1 kódszót, és változtassuk meg $e + 1$ helyen. Az így kapott x szóhoz egyértelműen létezik kódszó tőle legfeljebb e távolságban. Ez nem lehet a c_1, illetve ő maga sem lehet kódszó. Tehát egy másik, c_2 kódszó van tőle legfeljebb e távolságra. Ekkor azonban a háromszög-egyenlőtlenségből $2e + 1 \leq d \leq d(c_1, c_2) \leq d(c_1, x) + d(x, c_2) \leq e + 1 + e$, azaz mindenhol egyenlőség áll.

Az, hogy egy kód e-hibát javít, vagy hogy perfekt, a paraméterektől függ, nem kell hozzá ismernünk a kód szerkezetét.

2.2. Lineáris kódok

2.2.1. Definíció. Legyen Q test. Ekkor Q^n vektortér. Ha $C \subseteq Q^n$ kód altér is egyben, a kódot *lineárisnak* evezzük.

Míg lineáris algebrában általában oszlopvektorokról beszélünk, a kódelmélet lináris részében a szavakat sorvektoroknak tekintjük. Legyen $u, v, x \in Q^n$, ekkor $u + x$ és $v + x$ pontosan azokon a helyeken egyeznek meg, ahol u és v megegyeztek. Tehát a Hamming-távolság az eltolásra nézve invariáns. Továbbá ha C altér, akkor $\mathbf{0} \in C$, tehát lineáris kód minimális távolsága megegyezik a minimális súlyával. Lineáris kód esetén $M = q^k$, így C elemszáma helyett, inkább a C altér dimenzióját szoktuk megadni, és a paramétereket szögletes zárójelbe írjuk, azaz: $[n, k, d]_q$.

2.2.2. Definíció. $n - k$ azt jelenti, hogy mennyivel hosszabb a kódunk, mint az eredeti információnk (azaz az ellenőrző bitek száma). Ezt a számot *redundanciának* nevezzük, és r-rel jelöljük.

Ha C altér, akkor lesz bázisa.

2.2.3. Definíció. Egy C $[n, k, d]_q$ lineáris kód *generátormátrixa* egy $G \in Q^{k\times n}$ mátrix, melynek sorai a C egy bázisát alkotják.

C tehát a bázisvektorok lineáris kombinációiból áll, azaz $C = \{xG \colon x \in Q^k\}$, vagyis C az $x \mapsto xG$ leképezés képtere.

Nyilván egy lineáris kódnak több bázisa lehet, G és G' ugyanazt a kódot generálják, ha létezik $B \in Q^{k\times k}$ nem szinguláris mátrix (bázistranszformáció), hogy $G' = BG$.

2.2.4. Definíció. Két nemlineáris kód *ekvivalens*, ha az egyik megkapható a másikból a koordinátáik permutációjával. Két lineáris kód *ekvivalens*, ha az előzőeken kívül, egy nemnulla Q-beli elemmel való szorzást is megengedünk.

C es C' lineáris kódok tehát akkor ekvivalensek ha létezik $\alpha : C \to C'$ bijektív leképezés, hogy $\alpha(c) = cPD$, ahol P és D $n \times n$-es mátrixok, P permutációmátrix, D diagonális mátrix (az ilyen PD mátrixokat „monomiálisnak" szokták nevezni).G és G' tehát ekvivalens kódokat generálnak, ha $G' = BGM$, ahol B nemszinguláris, M monomiális.

2.2.5. Definíció. Egy C (nem feltétlenül lineáris) kód *duálisa* a rá merőleges vektorok altere. Azaz $C^\perp := \{y \in Q^n \colon \langle c, y\rangle = 0, c \in C\}$.

A $c \mapsto \langle c, y\rangle$ leképezés lineáris, így $C^\perp$ mindig altér lesz, tehát a duális kód lineáris. Vigyáznunk kell azonban , hogy $C \cap C^\perp$ nem csak a $\mathbf{0}$ vektor lehet, például bináris esetben minden páros súlyú szó merőleges önmagára.

Ugyanakkor $C^{\perp\perp} = \langle C\rangle$ és $\dim(\langle C\rangle) + \dim(C^\perp) = n$.

2.2.6. Definíció. Ha $C^\perp = C$, a kódot *önduálisnak* nevezzük.

2.2.1. Lemma. *Ha C bármely két eleme ortogonális, akkor* $\dim(\langle C\rangle) \leq \frac{n}{2}$.

Bizonyítás. Ekkor $C \subseteq C^\perp$, tehát $\langle C\rangle \leq C^\perp$ és így $\dim(\langle C\rangle) \leq \dim(C^\perp) = n - \dim(\langle C\rangle)$, amit átrendezve a keresett kifejezést kapjuk. □

2.2.7. Definíció. C lineáris kód *ellenőrző mátrixa* a dulális kód egy generátormátrixa. Vagyis egy olyan $H \in Q^{(n-k)\times n}$ mátrix, hogy minden $x \in Q^{n-k}$ estén $\langle c, (xH)\rangle = 0$, minden $c \in C$-re.

Ha B' nem szinguláris, és M' monomiális, akkor H és $B'HM'$ ekvivalens kódokat generálnak.

Ha $c \in C$, akkor $0 = c(xH)^\top = (cH^\top)x^\top$ minden $x \in Q^{n-k}$, vagyis $cH^\top = \mathbf{0}$. Fordítva, ha $cH^\top = \mathbf{0}$, akkor c merőleges a H által generált kódra, ezért $c \in C^{\perp\perp} = C$.

2.2.1. Következmény. *Legyen H a C ellenőrzőmátrixa. Ekkor $c \in C \iff cH^\top = \mathbf{0}$.*

$cH^\top = \mathbf{0}$ éppen azt jelnti, hogy van H oszlopainak egy olyan 0 értékű lineáris kombinációja, ahol az együtthatók rendre c koordinátái. Azaz ha $c \in C$, akkor H-nak van w(c) darab lineárisan összefüggő oszlopa. Fordítva ha van H-nak w darab összefüggő oszlopa, a lineáris kombinációból már le is olvashatunk egy w súlyú kódszót. Tudjuk továbbá, hogy liináris kód minimális súlya megegyezik a minimális távolságával, ezért:

2.2.1. Tétel. *Lineáris kód minimális távolsága nagyobb s-nél $\iff$ ellenőrzőmátrixának bármely s db oszlopa lineárisan független.*

H a duális kód generátormátrixa, és így rangja $n - k$. Következésképp:

2.2.2. Tétel. *Singleton-korlát: Tetszőleges C $[n, k, d]_q$ lineáris kódra $d \leq n - k + 1$.*

Megint csak az látszik, hogy adott redundanciára nem fogunk tudni túl sok hibát javító kódot konstruálni. Lássuk a tétel nem lineáris változatát is.

2.2.3. Tétel. *Legyen C egy $(n, M, d)_q$ kód. Ekkor $M \leq q^{n-d+1}$.*

Bizonyítás. Töröljünk C-ből $d-1$ koordinátát. Mivel a minimális távolság d, így nincs két olyan kódszó, ami a maradék $n-d+1$ helyen megegyezne. Vagyis az előző $C \to Q^{n-d+1}$ leképezés injektív, ezért $|C| \leq |Q^{n-d+1}|$. □

2.2.8. Definíció. Azokat a kódokat, ahol $M = q^{n-d+1}$, *MDS kódoknak* hívjuk.

2.3. Hamming-kódok

Vizsgáljuk meg a lineáris, perfekt, 1-hibajavító $[n,k,d]_q$ kódokat. Korábban láttuk, hogy $d = 2e+1 = 3$. Mivel a kód perfekt, ezért $q^k(1+n(q-1)) = q^n$, azaz $n = \frac{q^{n-k}-1}{q-1}$. Tehát a kód paraméteri: $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]_q$. A kód ellenőrző mátrixa n db r-dimenziós oszlopvektorokból áll. A 2.2.1 tételből kapjuk, hogy mivel $d > 2$, ezért bármely 2 oszlopa lineárisan független kell legyen. Azaz az oszlopvektorok által külön-külön kifeszített 1-dimenziós alterek különbözőek. A Q^r vektortérben az 1-dimenziós alterek száma éppen $\begin{bmatrix} r \\ 1 \end{bmatrix}_q$, azaz $\frac{q^r-1}{q-1}$, ami éppen n. Az oszlopvektorok tehát nem mások, mint az $(r-1)$-dimenziós projektív tér pontjainak reprezentánsai.

2.3.1. Definíció. r-edrendű *Hamming-kódnak* a $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]_q$ paraméterű kódot nevezzük. Ez 1-hibajavító perfekt, ellenőrző mátrixának oszlopai pedig az $(r-1)$-rendű projektív tér pontjai.

Tehát H oszlopai a $\mathrm{GF}(q)^r$ minden $\mathbf{0}$-n átmenő egyeneséből tartalmaz egy-egy pontot. Tehát ha H és H' is ilyen, akkor létezik M monomiális mátrix, hogy $H' = HM$, azaz a lineáris, 1-hibajavító perfekt kódok ekvivalencia erejéig egyértelműek. Megjegyezzük, hogy léteznek nem lineáris 1-hibajavító perfekt kódok is.

2.3.1. Állítás. *e-hibajavító perfekt kódoknál, ha q prímhatvány, akkor a $B(c,e)$ Hamming gömb térfogata q-nak a hatványa.*

Bizonyítás. Nyilván $\mathrm{B}(c,e) \mid q^n$. Tegyük fel, hogy $q = p^\alpha$, és $\mathrm{B}(c,e) = q^k p^\beta$, ahol $0 \leq \beta < \alpha$. Ekkor

$$q^n = (1+(q-1))^n = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i,$$

$$q^k p^\beta = \sum_{i=0}^{e} \binom{n}{i} (q-1)^i,$$

$$q^n - q^k p^\beta = \sum_{i=e+1}^{n} \binom{n}{i} (q-1)^i \equiv 0 \pmod{q-1},$$

$$q^n - q^k p^\beta = q^k(q^{n-k} - p^\beta) = q^k(q^{n-k} - 1 - p^\beta + 1) \equiv 0 \pmod{q-1}.$$

Mivel q^k és $q-1$ relatív prímek, továbbá

$$q^{n-k} - 1 = (q-1)(q^{n-k-1} + q^{n-k-2} + \ldots + q + 1),$$

azt kapjuk, hogy $p^\beta - 1 \equiv 0 \pmod{q-1}$. Mivel $p^\beta \leq q$, ezért ez csak úgy lehet, ha $\beta = 0$. □

2.3.2. Állítás. *Bináris, 3-hibajavító perfekt kódok esetén $n = 3, 7$ vagy 23.*

Bizonyítás. Ekkor a 3-sugarú Hamming gömb térfogata

$$1 + n + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)}{6} = 2^s,$$

$$6 + 6n + 3n(n-1) + n(n-1)(n-2) = 3 \cdot 2^{s+1},$$

$$(n+1)(n^2 - n + 6) = 3 \cdot 2^{s+1},$$

$$(n+1)((n+1)^2 - 3(n+1) + 8) = 3 \cdot 2^{s+1}.$$

Vagyis $(n^2 - n + 6) \equiv 8 \pmod{n+1}$. Ha $16 \mid n+1$ akkor $n^2 - n + 6 \mid 24$, de ez nem lehet. Ha $16 \nmid n+1$, akkor $n+1 \mid 24$. Ekkor tehát mivel $e = 3$, ezért $n \geq 3$, vagyis a lehetséges megoldások $n = 3, 7$ vagy 23. □

Mivel az előző állításban $q = 2, e = 3$, így $n = 3$ esetén $|C| = 1$. $n = 7$-re a $(7, 2^1, 7)_2$ paraméterű, ismétlő kódot kapjuk, míg $n = 23$-ra a később vizsgált bináris perfekt Golay kódot.

Nem létezik sokféle perfekt kód nagyobb e esetén sem, ezt a következő tétel igazolja, mely [6]-ból van:

2.3.1. Tétel. *Tietäväinen-van Lint: Ha q prímhatvány, akkor olyan nem triviális perfekt kód, amely legalább két hibát javít csak a bináris vagy a ternér Golay-kód lehet.*

Ezeket a kódokat később vizsgáljuk.

2.3.2. Definíció. Egy C kód *szimplex*, ha bármely két kódszó távolsága állandó.

Lineáris esetben $\mathrm{GF}(q)^r$ vektoraiból $q^{r-1}-1$ darab olyan nem $\mathbf{0}$ van, amik egy adott koordinátapozícióban 0-t vesznek fel. Ezek közül az egy egyenesen lévők száma $q-1$.

Tekintsük a Hamming kód H ellenőrzőmátrixának egy sorát, ez tehát pontosan $\frac{q^{r-1}-1}{q-1}$ darab 0-t, és q^{r-1} nem 0-t tartalmaz. Ha $\mathbf{0} \neq v \in C^\perp = \langle H \rangle$, akkor lesz olyan H', hogy $\langle H \rangle = \langle H' \rangle$, és aminek első sora v. Azaz v súlya q^{r-1} minden $v \in C^\perp \setminus \{\mathbf{0}\}$ -re. Vagyis $c_1, c_2 \in C^\perp$ esetén $d(c_1, c_2) = \mathrm{w}(c_1 - c_2) = q^{r-1}$, mivel $c_2 - c_1 \in C^\perp$. Tehát a Hamming kód duálisa szimplex.

2.4. Súlypolinom

2.4.1. Definíció. Egy C kód *súlypolinomja*

$$A(z) := \sum_{c \in C} z^{\mathrm{w}(c)} = \sum_{i=0}^{n} A_i z^i,$$

ahol A_i az i súlyú kódszavak száma.

Vizsgáljuk meg az e-hibajavító perfekt kódok súlypolinomját. Ehhez számoljuk meg az i súlyú szavakat a hozzájuk legközelebb álló kódszavak szerint. Tudjuk, hogy a c kódszó legfeljebb e távolságban lehet, és így a háromszög-egyenlőtlenség miatt $i - e \leq \mathrm{w}(c) \leq i + e$.

Tekintsünk először egy i-nél kisebb, $i-j$ súlyú kódszót. Ebből úgy kaphatunk i súlyú szót, ha x db 0 elemet nem 0-ra cserélünk, $x-j$ db nem 0 elemet pedig 0-ra. Az esetleg maradt $e-2x+j$ lehetőségből pedig y db nem 0 elemet másik nem 0 elemre cserélünk. Az x db $0 \mapsto$ nem 0 cserét $\binom{n-i+j}{x}(q-1)^x$ féleképpen hajthatjuk végre, az $x-j$ db nem $0 \mapsto 0$ cserét $\binom{i-j}{x-j}$ féleképpen, az y db nem $0 \mapsto$ nem 0 cserét pedig $\binom{i-j}{y}(q-2)^y$ féleképpen. Ezt összegezve x-re (j-től $\min\{i, \lfloor \frac{e+j}{2} \rfloor\}$-ig) és y-ra (0-tól $e-2x+j$-ig) kapunk

$$\sum_{x=j}^{\min\{i, \lfloor \frac{e+j}{2} \rfloor\}} \sum_{y=0}^{e-2x+j} \binom{n-i+j}{x}(q-1)^x \binom{i-j}{x-j}\binom{i-j}{y}(q-2)^y$$

db i súlyú szót.

Ha i-nél nagyobb, $i+j$ súlyú kódszóból indulunk ki, x db nem $0 \mapsto 0$ cserét, $x-j$ db $0 \mapsto$ nem 0 cserét, és y db nem $0 \mapsto$ nem 0 cserét hajthatunk végre. Az előzőhöz hasonlóan összegezve kapunk

$$\sum_{x=j}^{\min\{i, \lfloor \frac{e+j}{2} \rfloor\}} \sum_{y=0}^{e-2x+j} \binom{n-i+j}{x-j}(q-1)^{x-j} \binom{i+j}{x}\binom{i+j}{y}(q-2)^y$$

db i súlyú szót.

Végül i súlyú kódszóból kiindulva x db $0 \mapsto$ nem 0, x db nem $0 \mapsto 0$, és y db nem $0 \mapsto$ nem 0 cserét végrehajtva kapunk

$$\sum_{x=0}^{\min\{i,\lfloor \frac{e}{2} \rfloor\}} \sum_{y=0}^{e-2x} \binom{n-i}{x} (q-1)^x \binom{i}{x} \binom{i}{y} (q-2)^y$$

db i súlyú szót.

Mivel az i súlyú szavak száma összesen $\binom{n}{i}(q-1)^i$, így j-re összegezve:

$$\binom{n}{i}(q-1)^i = \tag{2.2}$$

$$\begin{aligned}
= & \sum_{j=1}^{\min(e,i)} \sum_{x=j}^{\min(\lfloor \frac{e+j}{2} \rfloor, i)} \sum_{y=0}^{e-2x+j} \binom{n-i+j}{x} (q-1)^x \binom{i-j}{x-j} \binom{i-j}{y} (q-2)^y A_{i-j} + \\
& + \sum_{x=0}^{\min(\lfloor \frac{e}{2} \rfloor, i)} \sum_{y=0}^{\min(e-2x,i)} \binom{n-i}{x} (q-1)^x \binom{i}{x} \binom{i}{y} (q-2)^y A_i + \\
& + \sum_{j=1}^{\min(e,n-i)} \sum_{x=j}^{\min(\lfloor \frac{e+j}{2} \rfloor, n-i)} \sum_{y=0}^{e-2x+j} \binom{n-i+j}{x-j} (q-1)^{x-j} \binom{i+j}{x} \binom{i+j}{y} (q-2)^y A_{i+j}.
\end{aligned}$$

Ha $\mathbf{0} \in C$, akkor $A_0 = 1$, és $1 \leq i \leq 2e$-re $A_i = 0$, azaz a rekurzió el tud indulni. Tehát ha C e-hibajavító perfekt kód, ami tartalmazza $\mathbf{0}$-t, akkor a súlypolinomját a paraméterei meghatározzák.

Például minimális súly esetén az $e+1$ súlyú szavakra felírva az első két szummában minden $A_{i-j} = A_i = 0$, a harmadik szummában $(i = e+1, j = e, x = e, y = 0)$:

$$\binom{n}{e+1}(q-1)^{e+1} = \binom{2e+1}{e} A_{2e+1}.$$

Tehát a minimális súlyú kódszavak száma:

$$A_{2e+1} = \frac{\binom{n}{e+1}(q-1)^{e+1}}{\binom{2e+1}{e}}.$$

Például a Hamming kódokra

$$\binom{n}{i}(q-1)^i = (n-i+1)(q-1)A_{i-1} + (1+i(q-2))A_i + (i+1)A_{i+1}.$$

Ezt z^i-nel szorozva, és i-re összegezve (0-tól n-ig) az

$$(1+(q-1)z)^n = (q-1)nzA(z)-(q-1)z^2A'(z)+A(z)+(q-2)zA'(z)+A'(z)$$

elsőrendű lineáris differenciálegyenletet kapjuk. Ennek megoldásának részletezése a témakörön kívülre eseik, mi inkább egy más megközelítéssel számoljuk ezt ki. Megjegyezzük, hogy persze konkrét q esetén a rekurzió is könnyedén használható.

F. J. MacWilliams egy fontos eredménye volt, hogy feltárta a kapcsolatot duális kódok súlypolinomjai közt. Mielőtt erre rátérnénk, tekintsünk át egy algebrai fogalmat.

2.4.2. Definíció. *Karakternek* hívunk egy Abel csoportból az 1 abszolút értékű komplex számokba képző homomorfizmust.

Azaz $\chi : (G,+) \to \mathbb{C}$, és $\chi(g_1+g_2) = \chi(g_1)\chi(g_2)$. Ekkor

$$\sum_{g\in G}\chi(g) = \begin{cases} |G| & \text{, ha } \chi \equiv 1, \\ 0 & \text{, különben.} \end{cases}$$

Ugyanis tetszőleges $h \in G$-re:

$$\chi(h)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(h+g) = \sum_{g'\in G}\chi(g').$$

Például legyen $G = \langle g\rangle$ ciklikus, $\chi(g^k) := \cos(k\frac{2\Pi}{|G|}) + i\sin(k\frac{2\Pi}{|G|})$.

2.4.1. Tétel. *Legyen C kód súlypolinomja $A(z)$, $C^\perp$-é $B(z)$. Ekkor*

$$B(z) = q^{-k}\Big(1+(q-1)z\Big)^n A\Big(\frac{1-z}{1+(q-1)z}\Big).$$

Bizonyítás. Ez a bizonyítás [1]-t követi. Legyen χ nemkonstans karakter $(Q,+)$-n. Legyen

$$\mathrm{g}(u) := \sum_{v\in Q^n}\chi(\langle u,v\rangle)z^{\mathrm{w}(v)},$$

$$\sum_{u\in C}\mathrm{g}(u) = \sum_{u\in C}\sum_{v\in Q^n}\chi(\langle u,v\rangle)z^{\mathrm{w}(v)} = \sum_{v\in Q^n}z^{\mathrm{w}(v)}\sum_{u\in C}\chi(\langle u,v\rangle).$$

Itt $v \in C^\perp$ esetén

$$\sum_{u\in C}\chi(\langle u,v\rangle) = \sum_{u\in C}\chi(0) = |C|,$$

$v \notin C^\perp$ esetén, mivel $u \mapsto \langle u, v\rangle$ lineáris leképezés $C \to Q$, ezért Q minden eleme ugyanannyiszor fordul elő, azaz

$$\sum_{u\in C} \chi(\langle u, v\rangle) = \sum_{q\in Q} \chi(q)m = 0 \cdot m.$$

Tehát

$$\sum_{u\in C} \mathrm{g}(u) = \sum_{v\in C^\perp} z^{\mathrm{w}(v)}|C| = |C|B(z). \tag{2.3}$$

Terjesszük ki a súlyfüggvényt Q elemeire: $\mathrm{w}(0) := 0$, és $\mathrm{w}(q) := 1$, ha $q \neq 0$. Ekkor definíció szerint

$$\begin{aligned}
\mathrm{g}(u_1, \ldots, u_n) &= \sum_{(v_1,\ldots,v_n)\in Q^n} \chi(u_1v_1 + \ldots + u_nv_n) z^{\mathrm{w}(v_1)+\ldots+\mathrm{w}(v_n)} = \\
&= \sum_{(v_1,\ldots,v_n)\in Q^n} \chi(u_1v_1) z^{\mathrm{w}(v_1)} \ldots \chi(u_nv_n) z^{\mathrm{w}(v_n)} = \\
&= \prod_{i=1}^{n} \sum_{v\in Q} \chi(u_iv) z^{\mathrm{w}(v)}.
\end{aligned}$$

Itt, ha $u_i = 0$, akkor $\chi(u_iv) = 1$, és így

$$\sum_{v\in Q} \chi(u_iv) z^{\mathrm{w}(v)} = 1 + (q-1)z.$$

Ha pedig $u_i \neq 0$, akkor

$$\sum_{v\in Q} \chi(u_iv) z^{\mathrm{w}(v)} = 1 + z \sum_{0\neq q\in Q} \chi(q) = 1 - z.$$

Azaz

$$\mathrm{g}(u) = \Big(1 + (q-1)z\Big)^{n-\mathrm{w}(u)} (1-z)^{\mathrm{w}(u)} = \Big(1 + (q-1)z\Big)^{n} \Big(\frac{1-z}{1+(q-1)z}\Big)^{\mathrm{w}(u)},$$

$$\sum_{u\in C} \mathrm{g}(u) = \Big(1 + (q-1)z\Big)^{n} A\Big(\frac{1-z}{1+(q-1)z}\Big). \tag{2.4}$$

(2.3)-ből és (2.4)-ből pedig épp azt kapjuk, hogy

$$B(z) = q^{-k}\Big(1 + (q-1)z\Big)^{n} A\Big(\frac{1-z}{1+(q-1)z}\Big).$$

□

Alkalmazzuk ezt a Hamming kód súlypolinomjának meghatározásához. Tudjuk, hogy az r-edrendű Hamming kód duálisa $[\frac{q^m-1}{q-1}, r, q^{m-1}]$ paraméterű szimplex kód, súlypolinomja

$$A(z) = 1 + (q^r - 1)z^{q^{r-1}}.$$

Ennek duálisa az eredeti Hamming kód, melynek így súlypolinomja

$$B(z) = q^{-r}\Big(1 + (q-1)z\Big)^{\frac{q^r-1}{q-1}}\Big(1 + (q^r-1)(\frac{1-z}{1+(q-1)z})^{q^{r-1}}\Big) =$$

$$= q^{-r}\bigg(\Big(1 + (q-1)z\Big)^{\frac{q^r-1}{q-1}} + (q^r-1)(1-z)^{q^{r-1}}\Big(1 + (q-1)z\Big)^{\frac{q^{r-1}-1}{q-1}}\bigg).$$

2.5. Kódkonstrukciók

2.5.1. Definíció. Ha Q test, C egy $(n, M, d)_q$ kód, akkor legyen a *kibővített kódja*

$$\bar{C} := \{(c_1, \ldots, c_n, c_{n+1}) \colon (c_1, \ldots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}.$$

Például bináris esetben ez a paritásellenőrző bit hozzáadását jelenti, ahogy a bevezetőben említett második példában is láthattuk. Ekkor, ha d páratlan, $\bar{C}$ minimális távolsága d+1 lesz.

2.5.2. Definíció. A C $(n, M, d)_q$ kódból töröljünk egy olyan koordinátát, ahol nem minden kódszó 0-t vesz fel. Azaz vegyük C vetületét alkalmas $n-1$ darab koordinátára. Ezt *lyukasztásnak* hívjuk. Ekkor a minimális távolság eggyel csökken. Ha a $d \geq 1$, akkor a kódszavak száma nem változik.

2.5.3. Definíció. A C $(n, M, d)_q$ kódból töröljünk egy olyan koordinátát, ahol minden kódszó 0. Ezt *rövidítésnek* hívjuk. Ez nem válttoztat a minimális távolságon.

2.5.4. Definíció. Legyen C lineáris $[n, k, d]_2$ kód, $w_0 := \mathrm{w}(c_0)$, ahol $c_0 \in C$, és $w_0 < 2d$. Koordinátapermutációkkal elérhető, hogy c_0 elején álljanak az 1-esek, és végén a 0-k. Ekkor választható olyan bázis, melynek első eleme c_0, azaz olyan generátormátrix, ami

$$\begin{bmatrix} 1\ldots1 & 0\ldots0 \\ A & B \end{bmatrix} \text{ alakú.}$$

Ekkor a $B \in 2^{(k-1)\times(n-w_0)}$ mátrix által generált kódot a C w_0-ra vonatkozó *reziduális kódjának* hívjuk.

2.5.1. Állítás. *Ekkor a reziduális kód paraméterei* $[n - w_0, k - 1, d']_2$ *ahol* $d' \geq d - \frac{w_0}{2}$.

Bizonyítás. Egy c kódszó vetülete az első w_0 koordinátára legyen w_1 súlyú, az utolsó $n - w_0$ koordinátára legyen w_2 súlyú. Ekkor

$$\begin{array}{ll} w_1 \leq \frac{w_0}{2} & \text{esetén} \quad d(c, \mathbf{0}) \leq w_2 + \frac{w_0}{2}, \\ w_1 \geq \frac{w_0}{2} & \text{esetén} \quad d(c, c_0) \leq w_2 + \frac{w_0}{2}. \end{array}$$

Tehát $d' \geq w_2 \geq d - \frac{w_0}{2}$. □

2.6. Golay kódok

2.6.1. Definíció. A $[23, 12, 7]_2$ lineáris kódot a *perfekt bináris Golay kódnak* hívjuk, és $\mathcal{G}_{23}$-mal jelöljük. A $[24, 12, 8]_2$ lineáris kódot a *kiterjesztett bináris Golay kódnak* hívjuk, és $\mathcal{G}_{24}$-gyel jelöljük. A $[11, 6, 5]_3$ lineáris kódot a *ternér Golay kódnak* hívjuk.

A ternér és perfekt bináris Golay kódok egyértelműségét S. L. Snover látta be, a kiterjesztett bináris esetre a harmadik fejezetben visszatérünk.

2.6.1. Állítás. *A* $(23, 2^{12}, 7)_2$ *és a* $(11, 3^6, 5)_3$ *paraméterű kódok perfektek.*

Bizonyítás.

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 1 + 23 + 253 + 1771 = 2048 = 2^{23-12},$$

$$\binom{11}{0} + \binom{11}{1}2 + \binom{11}{2}4 = 1 + 22 + 220 = 243 = 3^{11-6}.$$

□

3. fejezet

Kapcsolat

3.1. Általános eset

Egy **0**-t tartalmazó, e-hibajavító perfekt kód esetén láttuk, hogy a minimális súly $2e+1$, valamint igaz a (2.4) összefüggés:

$$\binom{n}{e+1}(q-1)^{e+1} = \binom{2e+1}{e}A_{2e+1}.$$

Ezt a súlypolinom képlete nélkül is meghatározhattuk volna, ugyanis, mivel a kód perfekt, minden szóhoz egyértelműen tarozik egy kódszó, ami tőle legfeljebb e távolságban van. $e+1$ súlyú szó esetén ez csak minimális $(2e+1)$ súlyú kódszó lehet, ami pontosan e távolságban van tőle. Tehát az $e+1$ súlyú szavakat megszámolhatjuk úgy is, hogy a hozzá legközelebb lévő kódszavak szerint csoportosítjuk. Ebben (ahogy a súlypolinomnál is láttuk) e db nem 0 elemet kell 0-ra cserélnünk, azaz:

$$\binom{n}{e+1}(q-1)^{e+1} = \binom{2e+1}{e}A_{2e+1}.$$

Láttuk tehát, hogy minden $e+1$ súlyú szóhoz egyértelműen tarozik egy $2e+1$ súlyú kódszó. Mivel bináris esetben kölcsönösen egyértelmű kapcsolat van a szavak, és a tartóik közt, így a **0**-t tartalmazó, bináris, e-hibajavító perfekt kódok esetén a minimális súlyú kódszavak tartói egy $(e+1)-(n, 2e+1, 1)$ Steiner rendszert határoznak meg.

Például a $[7,4,3]_2$ paraméterű Hamming kód egy $2-(7,3,1)$ rendszert határoz meg, mely épp a $\mathrm{PG}_1(2,2)$.

3.1.1. Definíció. Legyen $\sim$ reláció a szavak közt. $x_i \sim x_j$, ha x_i és x_j „összefüggőek", vagyis létezik olyan $0 \neq q \in Q$, hogy $qx_i = x_j$.

Ez ekvivalencia relácó, így a szavakat partícionálhatjuk ennek osztályaira. Egy osztályba tartozó szavaknak ugyanaz a tartója.

3.1.1. Állítás. *Egy nem egyelemű $[n,k,d]_q$ lineáris, e-hibajavító perfekt kód esetén a minimális súlyú kódszavak tartói egy $(e+1)-(n,2e+1,(q-1)^e)$ rendszer blokkjai.*

Bizonyítás. Az, hogy egy $e+1$ súlyú szó egyértelműen kiegészíthető $2e+1$ súlyú kódszóvá, az ellenőrzőmátrix oszlopvektoraival kifejezve azt jelenti, hogy $q_1v_1+\ldots+q_ev_e+q_{e+1}v_{e+1}$ lineáris kombinációt egyértelműen tudom kibővíteni e darab vektorral 0 értékű lineáris kobinációvá:

$$q_1v_1+\ldots+q_ev_e+q_{e+1}v_{e+1}+\underbrace{q_{e+2}v_{e+2}+\ldots+q_{2e+1}v_{2e+1}}_{e \text{ darab}}=0.$$

A továbbiakban legyen x_1 és x_2 két azonos tartójú, $e+1$ súlyú szó. Ezek egyértelműen kiegészíthetőek $2e+1$ súlyú kódszavakká, jelölje ezeket c_1 és c_2.

Ha $x_1\sim x_2$, azaz létezik olyan $0\neq q'\in Q$, hogy $q'x_1=x_2$, akkor $q'c_1$ is kódszó lesz, melynek vetülete az adott $e+1$ koordinátapozícióra $q'x_1=x_2$, azaz az x_2-höz tartozó c_2 kódszó éppen $q'c_1$ lesz. Tehát ha $x_1\sim x_2$, akkor $c_1\sim c_2$ (ugyanazzal a skalárral), és így c_1 és c_2 tartói megegyeznek.

Ha $x_1\nsim x_2$, akkor legyen x_1 első nem 0 koordinátája l_1, x_2-é pedig l_2. Mivel Q test, ezért $\exists l_2^{-1}$, $x_3:=l_1l_2^{-1}x_2$. Így x_3 és x_1 leagalább 1 koordinátában megegyeznek, de nem az összesben. Tegyük fel, hogy x_1 és x_3 $0<j<e+1$ helyen megegyeznek, azaz $\mathrm{d}(x_1,x_3)=e+1-j$. Ekkor a hozzájuk tartozó c_1 és c_3 kódszavakra a lineáris kombinációk legyenek

$$\underbrace{q_1v_1+\ldots+q_jv_j}_{j \text{ darab}}+\underbrace{q_{j+1}v_{j+1}+\ldots+q_{e+1}v_{e+1}}_{e+1-j \text{ darab}}+\underbrace{q_{e+2}v_{e+2}+\ldots+q_{2e+1}v_{2e+1}}_{e \text{ darab}}=0, \tag{3.1}$$

$$\underbrace{q_1v_1+\ldots+q_jv_j}_{j \text{ darab}}+\underbrace{q'_{j+1}v_{j+1}+\ldots+q'_{e+1}v_{e+1}}_{e+1-j \text{ darab}}+\underbrace{q^*_{e+2}v^*_{e+2}+\ldots+q^*_{2e+1}v^*_{2e+1}}_{e \text{ darab}}=0, \tag{3.2}$$

ahol $q_i\neq q'_i$ $(i=j+1,\ldots,e+1)$. Ha a két kódszónak megegyezne a tartója, azaz $\{v_{e+2},\ldots,v_{2e+1}\}=\{v^*_{e+2},\ldots,v^*_{2e+1}\}$ lenne, akkor a c_3-c_1 kódszó legalább $(e+1-j)$ súlyú, de legfeljebb $e+(e+1-j)$ súlyú lenne, ami lehetetlen. Tehát c_1 tartója különbözik c_3-étól, és mivel $x_2\sim x_3$, ezért c_2-étől is.

Azaz x_1 és x_2 szavakhoz tartozó kódszavak tartói pontosan akkor egyeznek meg, ha $x_1\sim x_2$. Rögzítsünk $e+1$ koordinátapozíciót, és tekintsük azokat a szavakat, melyeknek ez a tartója. Ezeket a $\sim$ szerint

osztályozhatjuk, minden osztályban $(q-1)$ elem lesz, tehát $\frac{(q-1)^{e+1}}{q-1}$ osztályt kapunk, amelyekhez tartozó kódszavak mind különböző tartójúak. Így meghatároztunk egy $(e+1)-(n, 2e+1, (q-1)^e)$ rendszert. □

A bizonyításban nem zártuk ki, hogy a minimális súlyú kódszavak tartói több pontban is metszhessék egymást, így eseteleg egy $(e+1)$-nél nagyobb rendszert alkotva. Ehhez a következőt kéne belátnunk:

3.1.2. Állítás. *Ha x_1 és x_2 két olyan $e+1$ súlyú szó, amiknek ugyanaz a tartója, de nem egymás skalárszorosai, akkor a hozzájuk tartozó kódszavak tartói, csak az adott $e+1$ helyen metszik egymást.*

3.1.1. Lemma. *Azonos tartójú, $e+1$ súlyú, pontosan egy helyen eltérő szavakhoz tartozó kódszavak tartói csak a vizsgált szavak tartóiban egyeznek meg.*

Bizonyítás. Legyen x_1 és x_2 két ilyen szó. A korábbi bizonyításban elmondottakhoz hasonlóan legyen a c_1 és c_2 kódszóhoz tartozó lineáris kombináció

$$(3.3)\ q_1v_1 + \ldots + q_ev_e + q_{e+1}v_{e+1} + \underbrace{q_{e+2}v_{e+2} + \ldots + q_{2e+1}v_{2e+1}}_{e \text{ darab}} = 0,$$

$$(3.4)\ q_1v_1 + \ldots + q_ev_e + q'_{e+1}v_{e+1} + \underbrace{q^*_{e+2}v^*_{e+2} + \ldots + q^*_{2e+1}v^*_{2e+1}}_{e \text{ darab}} = 0,$$

ahol $q_{e+1} \neq q'_{e+1}$. Ekkor a $c_2 - c_1$ kódszóhoz tartozó lineáris kombináció

$$(q'_{e+1}-q_{e+1})v_{e+1}+\underbrace{q^*_{e+2}v^*_{e+2} + \ldots + q^*_{2e+1}v^*_{2e+1}}_{e \text{ darab}} - \underbrace{q_{e+2}v_{e+2} - \ldots - q_{2e+1}v_{2e+1}}_{e \text{ darab}} = 0.$$

Ennek tehát a v_{e+1} vektorhoz tartozó koordinátája nem 0, azaz súlya $\geq 2e+1$. Így a v_i vektorok mind különbözőek, hiszen különben egy minimális súlynál kisebb súlyú kódszót kapnék.

Tehát ha egy $e+1$ súlyú x szóban csak 1 koordinátát változtatok meg, a két különböző kódszó tartója csak x tartójában lesz közös. □

3.1.3. Állítás. *Nem egyelemű, lineáris pefekt kódok esetén, azonos tartójú, $e+1$ súlyú x_1 és x_2 szavakra csak a következők valamelyike lehetséges:*

- $x_1 \sim x_2$, *vagy*
- $\exists x_3 \sim x_2$, *hogy* $d(x_1, x_3) = 1$.

Bizonyítás. Emlékezzünk a 2.3.1 Tietäväinen-van Lint tételre, mely szerint nem triviális, egynél több hibát javító perfekt kód csak Golay kód lehet, ha q prímhatvány. Ezért elég az alábbi eseteket vizsgálnunk:

|Q|=2 eset: Bináris esetben kölcsönösen egyértelmű kapcsolat van a szavak, és a tartóik közt, így minden azonos tartójú szó egyenlő is.

e=1 eset: Ugyanazt elmondhatjuk, mint a 3.1.1 állítás bizonyításásban. Ha $x_1 \nsim x_2$, akkor legyen x_1 első nem 0 koordinátája l_1, x_2-é pedig l_2. Mivel Q test, ezért $\exists l_2^{-1}$, $x_3 := l_1 l_2^{-1} x_2$. Így x_3 és x_1 leagalább 1 koordinátában megegyeznek, de nem az összesben. Azaz 2 súlyú szavak esetében az egyik koordinátában megegyeznek, a másikban nem.

|Q|=3, e=2 eset: Legyen $Q = \{0, 1, \alpha\}$, ahol 1 egységelem, $\alpha\alpha = 1$, $1 + \alpha = 0$. Vegyünk két, $e + 1 = 3$ súlyú x_1 és x_2 szót. x_1 és x_2 a tartóján semelyik koordinátában sem 0, valamint $0 \leq d(x_1, x_2) \leq 3$. Ha $d(x_1, x_2) = 0$, akkor x_1 és x_2 egyenlőek, tehát ugyanabban az osztályban vannak. Ha $d(x_1, x_2) = 1$, akkor x_1 és x_2 pontosan egy helyen térnek el. Ha $d(x_1, x_2) = 2$, akkor αx_2 koordinátái pontosan x_2 koordinátáinak ellentettjei, vagyis x_1 és αx_2 pontosan egy koordinátában térnek el. Ha $d(x_1, x_2) = 3$, akkor x_1 és αx_2 koordinátái megegyeznek, tehát x_1 és x_2 ugyanabban az osztályban vannak.

□

Tehát a 3.1.3 állításból a 3.1.1 lemma miatt lineáris perfekt kódokra igaz a 3.1.2 állítás.

3.1.1. Következmény. *Lineáris, e-hibajavító perfekt kódok esetén a minimális súlyú kódszavak tartói egy* $(e+1)-(n, 2e+1, (q-1)^e)$ *rendszer blokkjait határozzák meg, mely nem alkot* $t > e + 1$*-re* t*-rendszert.*

3.2. Golay kódok

Térjünk vissza a Golay kódok vizsgálatára.

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

Bizonyítás. Jelöljük s-sel azon koordináták számát, ahol x és y is egyes. Ekkor x és y pontosan akkor ortogonálisak, ha s páros. Mivel

$$\mathrm{w}(x + y) = \mathrm{w}(x) + \mathrm{w}(y) - 2s,$$

ezért $4 \mid \mathrm{w}(x)$ és $4 \mid \mathrm{w}(y)$ esetén az összegük súlya pontosan akkor osztható 4-gyel, ha s páros. □

3.2.1. Tétel. *A* $\mathbf{0}$*-t tartalmazó,* $(24, 2^{12}, 8)_2$ *kódok ekvivalencia erejéig egyértelműek.*

Bizonyítás. Ez a bizonyítás [6]-t követi. Legyen C ilyen kód. Egy koordináta törlésével $(23, 2^{12}, 7)_2$ paraméterű kódot kapok, mely a 2.6.1 szerint perfekt. Ekkor (2.2) alapján súlypolinomját meghatározzák a paraméterei, vagyis

$$A(z) = 1 + 253z^7 + 506z^8 + 1288z^{11} + 1288z^{12} + 506z^{15} + 253z^{16} + z^{23}.$$

Tehát az eredeti C-ben csak 0, 8, 12, 16 és 24 súlyú kódszavak lehettek (másképp, például egy 11 súlyú kódszóból „ügyetlenül" lyukasztva 10 súlyút kapnék). Ugyanígy, $u \in C$ esetén $u + C$-ben is csak ilyen súlyú kódszavak lesznek, tehát C elemeire igaz a 3.2.1 lemma, azaz C bármely két szava ortogonális. Ekkor a 2.2.1 lemma miatt $\dim(\langle C \rangle) \leq 12$. Mivel $|C| = 2^{12}$, ezért $\dim(\langle C \rangle) = 12$, vagyis $C = \langle C \rangle$, azaz lineáris (sőt önduális).

Vegyük egy 12 súlyú szavára vonatkozó reziduális kódját. A 2.5.1 állítás miatt ennek paraméterei: $[12, 11, d']_2$, ahol $d' \geq d - \frac{w_0}{2} = 8 - \frac{12}{2} = 2$. A Singleton korlát miatt viszont $d' \leq 12 - 11 + 1 = 2$, tehát a reziduális kód $[12, 11, 2]_2$ paraméterű MDS kód. Ez csak úgy lehet, ha az ellenőrzőmátrixa $(1, \ldots, 1)$, ekkor a kód éppen a páros súlyú kódszavakból áll, melynek generátormátrixa

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

tehát az eredeti C generátormátrixa

$$\begin{bmatrix} 1 & 1 \ldots 1 & 0 \ldots 0 & 0 \\ 0 & & & 1 \\ \vdots & A & I_{11} & \vdots \\ 0 & & & 1 \end{bmatrix} \text{ alakú.}$$

Itt az első oszlopban lévő nullákat úgy értük el, hogy ha valahol nem 0 volt, ahhoz a sorhoz hozzáadtuk c_0-t. Így minden sorban van legalább 11 darab 0. A súlyeloszlás miatt az egy sorban lévő egyesek száma ezért már csak 8 vagy 12 lehetne, ha azonban az első soron kívül is lenne egy 12 egyest tartalmazó sor (amiben tehát az A megfelelő sorában 10 darab egyes van), akkor ehhez hozzáadva az elsőt, egy 4 súlyú kódszót kapnék. Tehát C első

során kívül minden sorban pontosan 8 darab egyes van, azaz A minden sorában pontosan 6. Ugyanígy bármely 2 sor összege nem tartalmazhat az A részen, csak 6 darab egyest. Tehát A olyan 11×11-es mátrix, melynek minden sorában pontosan 6 darab egyes van, és bármely két sor összege is 6 darab egyest tartalmaz, vagyis bármely két sorban pontosan 3 darab közös egyes lesz. Azaz A egy 2-(11,6,3) négyzetes blokkrendszer illeszkedési mátrixa. A bizonyítás befejezéséhez be kell látni, hogy ez (illetve ennek komplementere) izomorfia erejéig egyértelmű, ez megtalálható [6]-ban. □

3.2.1. Állítás. *$\mathcal{G}_{24}$-ben a 8 súlyú kódszavak száma 759.*

Bizonyítás. (1.) Láttuk, hogy a minimális súly 8, és láttuk, hogy minden kódszó súlya osztható 4-gyel. Továbbá a lyukasztott kód súlypolinomjában z^{23} együtthatója nem 0 volt, tehát a csupa 1-esből álló vektor eleme a kódnak. Ebből az következik, hogy bármely kódszó komplementere is kódszó, vagyis ugyanannyi 8 és 16 súlyú szó lesz a kódban. A súlypolinom tehát $A(z) = 1 + az^8 + bz^{12} + az^{16} + z^{24}$ alakú lesz. A kódszavak száma $2 + 2a + b = 2^{12}$.

Azt is láttuk, hogy a kód önduális, így a MacWilliams azonossággal

$$A(z) = 2^{-12}(1+z)^{24} A\left(\frac{1-z}{1+z}\right),$$

$$1 + az^8 + bz^{12} + az^{16} + z^{24} =$$

$$= 2^{-12}(1+z)^{24}\Big(1 + a\frac{(1-z)^8}{(1+z)^8} + b\frac{(1-z)^{12}}{(1+z)^{12}} + a\frac{(1-z)^{16}}{(1+z)^{16}} + \frac{(1-z)^{24}}{(1+z)^{24}}\Big) =$$

$$\begin{aligned} &= 2^{-12}\Big((1+z)^{24} + a(1-z)^8(1+z)^{16} + \\ &\quad + b(1-z)^{12}(1+z)^{12} + \\ &\quad + a(1-z)^{16}(1+z)^8 + (1-z)^{24}\Big). \end{aligned}$$

$A(z)$-ben a z^2 együtthatója 0, míg az egyenlet másik végén a binomiális tétel miatt ez

$$2^{-12}\left(2\binom{24}{2} + 2a\Big(\binom{8}{2} + \binom{16}{2} - 8\cdot 16\Big) + b\Big(\binom{12}{2} + \binom{12}{2} - 12\cdot 12\Big)\right),$$

ami $2^{-12}(552 + 40a - 12b)$. Mivel $b = 2^{12} - 2a - 2$, így

$$\begin{aligned} 0 &= 2^{-12}(552 + 40a - 12(2^{12} - 2a - 2)), \\ 0 &= 552 - 49152 + 24 + (40 + 24)a. \end{aligned}$$

Vagyis a=759. □
Bizonyítás. (2.) A lyukasztott perfekt kód súlypolinomja:

$$1 + 253z^7 + 506z^8 + 1288z^{11} + 1288z^{12} + 506z^{15} + 253z^{16} + z^{23}.$$

Láttuk, hogy az eredetiben minden kódszó súlya osztható 4-gyel, vagyis a lyukasztás során például a 7, és 8 súlyú szavak csak a 8 súlyúakból keletkezhettek. Így az eredeti kód súlypolinomja:

$$1 + (253 + 506)z^8 + (2 \cdot 1288)z^{12} + (506 + 253)z^{16} + z^{24}.$$

Azaz a 8 súlyú kódszavak száma 759. □

3.2.2. Tétel. *A $\mathcal{G}_{24}$ kibővített bináris Golay kód 8 súlyú szavai egy 5-(24,8,1) Steiner rendszer blokkjai.*

Bizonyítás. Legyen c_1 és c_2 két, minimális súlyú kódszó. Jelölje s azon koordináták számát, ahol mindkettő egyes.

$$8 \leq \mathrm{w}(c_1 + c_2) = \mathrm{w}(c_1) + \mathrm{w}(c_2) - 2s = 16 - 2s,$$

vagyis $s \leq 4$, azaz legfeljebb 4 helyen tartalmazhatnak közö egyest. Tehát 5 koordinátát megadva, már csak legfeljebb 1 olyan kódszó lehet, ami ezeken a pontokon egyes. Egy ilyen ötöst $\binom{24}{5}$ féleképpen választhatok, de ekkor minden 8 súlyú kódszót $\binom{8}{5}$-ször számoltam. Tehát legfeljebb $\binom{24}{5}/\binom{8}{5} = 759$ darab 8 súlyú kódszó lehet. Az előbb láttuk, hogy van is ennyi, tehát minden koordináta-ötöshöz lesz olyan 8 súlyú kódszó, ami ezeken a helyeken egyes, méghozzá pontosan 1. □

Fordított esetben, vizsgáljuk meg, milyen kódot lehet készíteni adott t-rendszerből.

3.2.1. Definíció. Legyen $\mathbf{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ illeszkedési struktúra, melynek illeszkedési mátrixa $M \in \mathrm{GF}(2)^{|\mathcal{P}|\times|\mathcal{B}|}$. Legyen C az $M^\top$ sorai által generált altér $\mathrm{GF}(2)^{|\mathcal{P}|}$-ben. Ekkor C-t a $\mathbf{D}$ *által generált kódnak* nevezzük. Egy B blokknak az $M^\top$-ban megfelelő sorvektort a blokk *karakterisztikus vektorának* hívjuk.

Tehát a $\mathbf{D}$ által generált kód, a blokkok karakterisztikus vektorai által generált bináris, lineáris kód. Minden blokknak megfelel egy kódszó. Ha $\mathbf{D}$ egyszerű, akkor a $\mathcal{B} \to C$ leképezés injektív.

3.2.3. Tétel. *Egy* $5-(24,8,1)$ *rendszer által generált kód a* $\mathcal{G}_{24}$*-gyel ekvivalens.*

Bizonyítás. Legyen a generált kód C. Nézzük meg, hogyan metszheti egymást két blokk. Azon blokkok számát, melyek egy B blokkot pontosan adott i pontban metszenek, jelöljük egyelőre $\mathrm{m}(i)$-vel. $\mathrm{m}(8)=1$. Mivel 5 pont egyértelműen meghatározza a B blokkot, ezért $i=5,6,7$ esetén $\mathrm{m}(i)=0$. 4 adott ponot tartalmazó blokkok száma λ_4, de ebből le kell vonnunk azt, ami több, mint 4 pontban metszi, ez viszont csak a B. Azaz $\mathrm{m}(4)=\lambda_4-1=4$. 3 ponton át λ_3 blokk megy, de ezek között olyan is van, ami 4 pontban is metszi a B-t. Ezt a negyedik pontot $8-3$ féleképpen választhatom, tehát

$$\mathrm{m}(3)=\lambda_3-5\mathrm{m}(4)-\mathrm{m}(8)=21-5\cdot 4-1=0.$$

Azaz két blokk metszete nem lehet 3 elemű. Látszik, hogy

$$\mathrm{m}(i)=\lambda_i-\binom{k-i}{1}\mathrm{m}(i+1)-\binom{k-i}{2}\mathrm{m}(i+2)-\ldots-\binom{k-i}{k-i}\mathrm{m}(k). \tag{3.5}$$

Így tehát

$$\begin{aligned}
\mathrm{m}(2) &= \lambda_2-6\mathrm{m}(3)-\binom{6}{2}\mathrm{m}(4)-\mathrm{m}(8)=77-0-60-1=16,\\
\mathrm{m}(1) &= \lambda_1-7\mathrm{m}(2)-\binom{7}{3}\mathrm{m}(4)-\mathrm{m}(8)=253-112-140-1=0,\\
\mathrm{m}(0) &= \lambda_0-\binom{8}{2}\mathrm{m}(2)-\binom{8}{4}\mathrm{m}(4)-\mathrm{m}(8)=759-448-280-1=30.
\end{aligned}$$

Ebből tehát az látszik, hogy bármely két 8 súlyú kódszó csak páros sok pontban tartalmazhat közös 1-est, így skaláris szorzatuk 0 lesz. Ekkor a 3.2.1 lemma miatt bármely két 8 súlyú kódszó összege osztható 4-gyel. Indukcióval belátható, hogy ugyanez igaz akárhány tagú összegükre is, azaz minden bináris lineáris kombinációjukra. Tehát C minden elemének súlya osztható 4-gyel. Mivel C lineáris, megint csak a 3.2.1 lemma miatt ez azt jelenti, hogy C bármely két eleme ortogonális, vagyis a 2.2.1 lemma miatt $\dim(C)\leq 12$.

Rögzítsünk most 4 pontot. Ezeken $\lambda_4=5$ darab blokk megy át, melyek ezeken kívül diszjunktak (hiszen 5 pont már egyértelműen meghatároz egy blokkot). Így tehát a maradék 20 pont mindegyikén ezekből pontosan egy blokk megy át. Tekintsük ezen 5 darab blokk karakterisztikus vektorának összegét. A rögzített 4 koordinátán 5 db egyest kell összeadnunk, ami 1. A többi 20 koordinátban 4 darab nullát, és 1 darab egyest, ami szintén 1. Azaz a csupa egyesből álló szó kódszó lesz.

Ezt bármely 8 súlyú kódszóhoz hozzáadva 16 súlyú kódszót kapok, vagyis ezek száma is legalább annyi, mint a blokkok száma, vagyis 759.

Vegyünk egy blokkot, legyen a karakterisztikus vektora c. Olyan blokk, ami pontosan 2 pontban metszi ezt, a fentebb látottak alapján $\binom{8}{2}m(2) = 448$ darab van. Legyen c' egy ilyen blokk karakterisztikus vektora. Ekkor tehát c és c' pontosan 2 helyen tartalmaz közös egyest, tehát összegük súlya $8+8-2\cdot 2 = 12$. Így tehát előállíthatok 448 darab 12 súlyú kódszót. Egy ilyen szónak tehát 6 közös egyese lesz c-vel. Ehhez hozzáadva a csupa egyesből álló kódszót, olyan 12 súlyú szót kapok, aminek 2 közös egyese van c-vel, tehát újabb 448 darabot állíthatok így elő.

Azaz eddig $|C| \geq 2 \cdot 759 + 2 \cdot 448 + 2 = 2416 > 2^{11}$, és láttuk, hogy $\dim(C) \leq 12$, vagyis $|C| = 2^{12}$.

Láttuk, hogy minden kódszó súlya osztható 4-gyel. Tegyük fel, hogy van egy 4 súlyú c kódszavam, és tekintsük ennek tartóját. Mivel $\lambda_3 > \lambda_4$, ezért biztosan lesz olyan blokk, mely ezt pontotsan 3 pontban metszi, ami viszont páratlan. Tehát c és c' skaláris szorzata 1 lesz, ami ellentmond annak, hogy C bármely két eleme ortogonális. Tehát C minimális súlya 8.

Azaz C egy $[24, 12, 8]_2$ paraméterű lineáris kód, ami a 3.2.1 tétel miatt egyértelmű. □

3.2.4. Tétel. *Az* $5-(24, 8, 1)$ *rendszerek izomorfia erejéig egyértelműek.*

Bizonyítás. Az előző tétel alapján tehát ennek a rendszernek a blokkjai a $\mathcal{G}_{24}$-gyel ekvivalens kódot generálnak, és különböző blokkokhoz különböző 8 súlyú szavak tartoznak. Tudjuk, hogy $|\mathcal{B}| = \lambda_0 = 759$, és a 3.2.1 állításból, hogy $\mathcal{G}_{24}$-ben a 8 súlyú szavak száma is éppen ennyi. Tehát az eredeti blokkrendszer blokkjai (a koordináták permutációjától eltekintve) megegyeznek az egyértelmű Golay kód minimális súlyú szavaival. Ez tehát azt jelenti, hogy az eredeti rendszer izomorf a $\mathcal{G}_{24}$-ből 3.2.2 tétel szerint előállított rendszerrel. □

Az $5-(24,8,1)$ rendszert 24 pontú *Witt-féle* rendszernek nevezzük. Ennek metszési háromszöge:

$$759$$
$$253 \quad 506$$
$$77 \quad 176 \quad 330$$
$$21 \quad 56 \quad 120 \quad 210$$
$$5 \quad 16 \quad 40 \quad 80 \quad 130$$
$$1 \quad 4 \quad 12 \quad 28 \quad 52 \quad 78$$
$$1 \quad 0 \quad 4 \quad 8 \quad 20 \quad 32 \quad 46$$
$$1 \quad 0 \quad 0 \quad 4 \quad 4 \quad 16 \quad 16 \quad 30$$
$$1 \quad 0 \quad 0 \quad 0 \quad 4 \quad 0 \quad 16 \quad 0 \quad 30$$

A 3.2.3 tétel bizonyításában nem lett volna szükségünk az $\mathrm{m}(i)$-k bevezetésére. Vegyük ugyanis észre, hogy Steiner rendszer esetén $\mathrm{m}(i)$ éppen a kiterjesztett λ_i^{k-i} (továbbá kiszámolható, hogy a (3.5) rekurzióból épp az 1.5.2 állítás adódik). Azt tehát, hogy két blokk metszete mindig páros (amiből levezettük, hogy bármely két kódszó merőleges, és $\dim(C) \leq 12$), ránézésre megállapíthattuk volna a háromszög alsó sorából. Továbbá, a 4 súlyú kódszavak nem létezésére elmondottakat a következőképpen bővíthetjük:

Tegyük fel, hogy létezik i súlyú kódszó, tekintsük a tartóját. Ekkor $i \leq 5$ esetén az (1.5) alapján $\lambda_1^{i-1} > 0$, vagyis létezik olyan blokk, ami ezt az i pontot csak 1 pontban metszi, ami ellentmond annak, hogy bármely két kódszó merőleges. Tehát ha $C \subseteq C^{\perp}$, a minimális súly mindig legalább $\lambda + 1$ anélkül, hogy számolnunk kellett volna.

Utószó

Az 1.6 szakaszban láttuk, hogy milyen jól szemléltetik a metszési háromszögek a blokkrendszerek különböző konstrukcióit. Például ránézve egy adott (nem kiterjesztett) háromszögre, annak bármely részháromszöge egy megfelelő, kisebb rendszert határoz meg (az 1.6 szakasz konstrukcióival). Ha viszont növelni akarjuk a méretet, könnyen meghatározhatjuk, hogy meddig bővíthető egy ilyen háromszög ezekkel a módszerekkel, sőt ki is tudjuk számolni minden értékét annélkül, hogy a hozzá tartozó rendszer létezéséről tudnánk.

Mindemellett a 3.2.1 definícióban azt is láttuk, hogy hogyan lehet blokkrendszerekből bináris lineáris kódot előállítani. Szerencsés esetben a kiterjesztett háromszögből ránézésre meg tudjuk állapítani, hogy a kapott kódban bármely két kódszó merőleges, és ekkor szintén azonnal látható alsó határt adhatunk a minimális távolságra.

A. függelék

A.1. Programkód

```
Sub haromszog()
Dim t As Integer: Dim v As Integer: Dim k As Integer: Dim lambda As Integer
Dim i As Integer: Dim j As Integer: Dim li As Single: Dim max As Integer

t = InputBox("t"): v = InputBox("v"): k = InputBox("k")
lambda = InputBox("lambda")
If lambda = 1 Then
    max = k
    For i = t + 1 To k
        Cells(i + 1, 1) = 1
    Next
Else
    max = t
End If
Cells(t + 1, 1) = lambda
For i = t To 1 Step -1
    li = Cells(i + 1, 1) * (v - i + 1) / (k - i + 1)
    If Int(li) = li Then
        Cells(i, 1) = li
    Else
        Exit Sub
    End If
Next
For j = 1 To max: For i = 0 To max - j
    Cells(i + 1, j + 1) = Cells(i + 1, j) - Cells(i + 2, j)
Next: Next
End Sub
```

Irodalomjegyzék

[1] J. H. van Lint: *Introduction to Coding Theory*, Pringer (1999)

[2] E. F. Assmus Jr, J. D. Key: *Designs and their Codes*, Cambridge University Press (1992)

[3] F. de Clerck: *An Introduction to the Theory of the Designs*, ELTE (1992)

[4] M. J. de Resmini: *An Introduction to Steiner Systems*, ELTE (1992)

[5] C. C. Linder, A. Rosa: *Topics on Steiner Systems*, Elsevier (2011)

[6] Szőnyi Tamás: *Szimmetrikus kombinatorikus struktúrák*, ELTE jegyzet, Typotex (2013)

[7] T. Beth, d. Jungnickel, H. Lenz: *Design Theory*, Cambridge University Press, (1999)

[8] Hraskó András, Szőnyi Tamás: *Új matematikai mozaik: Hibajavító kódok*, Typotex (2002)

[9] Kiss Emil: *Bevezetés az algebrába*, Typotex (2007)

[10] Freud Róbert: *Lineáris algebra*, ELTE Eötvös (2006)

[11] Kiss György, Szőnyi Tamás: *Véges geometriák*, Typotex (2001)