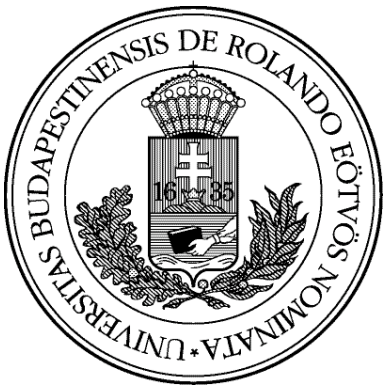
Eötvös Loránd Tudományegyetem
Természettudományi Kar

Dankovics Attila
Matematika BSc
Matematikus szakirány

Csoportot alkotó halmazrendszerekre vonatkozó extremális problémák

Szakdolgozat

Témavezető: Katona Gyula, egyetemi tanár
Számítógéptudományi tanszék



Budapest, 2015.

Tartalomjegyzék

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Katona Gyulának a téma ajánlását, segítségét a konzultációk során és a dolgozat alapos átnézését.

Bevezető

A klasszikus Sperner tétel a következő kérdésre ad választ:

Legyen X egy véges halmaz, $|X| = n$, és $\mathcal{F} \subset \mathcal{P}(X)$ olyan, hogy $\mathcal{F}$-nek nincs két különböző F_1, F_2 eleme, amelyre $F_1 \subset F_2$, mennyi ekkor $|\mathcal{F}|$ lehetséges legnagyobb elemszáma? A válasz pontosan $\binom{n}{\frac{n}{2}}$.

A kódelmélet motiválja a következő kapcsolódó kérdést:

Legyen X egy véges halmaz, $|X| = n$, és $\mathcal{F} \subset \mathcal{P}(X)$ olyan, hogy bármely két F_1, F_2 elemére $F_1 \oplus F_2$ is eleme $\mathcal{F}$-nek (ahol $\oplus$ a szimmetrikus differenciát jelöli) és $\mathcal{F}$-nek nincs két különböző $F_1 \neq \emptyset, F_2$ eleme, amelyre $F_1 \subset F_2$. Mennyi ekkor $|\mathcal{F}|$ lehetséges legnagyobb elemszáma?

Szakdolgozatom témája ezen kérdés, és hozzá kapcsolódó általánosítások, ekvivalens megfogalmazások, alkalmazások.

Katona és Srivistava eredménye a legjobb ismert felső becslés [1]: nagy n-re, ha $\mathcal{F}$ k dimenziós altere $\mathcal{P}(X)$-nek, akkor $k \leq 0{,}2835n$. A legjobb alsó becslés Komlós eredménye [3]: Minden n-re van k dimenziós megfelelő $\mathcal{F}$, hogy $k \geq 0{,}2075n$. Az első részben ezeket az alapvető eredményeket és a szükséges fogalmakat, definíciókat mutatom be.

A második részben különböző, de egymással szoros kapcsolatban álló véges affin és projektív geometriai fedési feladatokról mutatom meg, hogy a vizsgált kérdéssel ekvivalensek. A vizsgált problémákra vonatkozó alapvető állításokat is kimondok. A lehetséges geometriai megfogalmazások egyike szerepel Katona és Srivistava cikkében is [1].

Brassard, Crépeau és Sántha az Oblivious Transferekre vonatkozó tételükben [4] használták a kérdéses tulajdonságú halmazrendszereket. A harmadik részben ezért az Oblivious Transferekről írok, ami információ megosztási protokollok egy csoportja.

A negyedik részben a kérdés két lehetséges általánosítását mutatom be. Az egyik esetben nem csak diszjunkt halmaz párok előfordulását tiltjuk meg $\mathcal{F}$-ben, hanem olyanokat is, melyek metszete alacsony elemszámú. Ebben a kérdésben többnyire Miklós Dezső cikkét követem [3]. A másik esetben tartalmazó halmaz párok helyett l hosszú tartalmazó halmazláncok előfordulását tiltom meg $\mathcal{F}$-ben és erre az esetre általánosítom Katona és Srivistava eredményét.

1. Becslések metsző kódokra

1.1. Alapvető definíciók és állítások

A szakdolgozat témája főként a következő probléma.

1.1.1. Definíció. *Lineáris Sperner probléma: Legyen X egy véges halmaz, $|X| = n$, és $\mathcal{F} \subset \mathcal{P}(X)$ olyan, hogy bármely két F_1, F_2 elemére $F_1 \oplus F_2$ is eleme $\mathcal{F}$-nek (ahol $\oplus$ a szimmetrikus differenciát jelöli) és $\mathcal{F}$-nek nincs két különböző $F_1 \neq \emptyset, F_2$ eleme, amelyre $F_1 \subset F_2$. Mennyi ekkor $|\mathcal{F}|$ lehetséges legnagyobb elemszáma.*

A 1.1.1 problémában az általánosság rovása nélkül feltehetjük, hogy az alaphalmaz $[n] = \{1, ..., n\}$. Ezt kényelmi okokból meg is fogjuk tenni.

A 1.1.1 megfogalmazható lineáris kódok segítségével is. Az alaphalmaz részhalmazai megfeleltethetők $\mathbb{F}_2$ feletti vektoroknak: Egy $A \subset [n]$-nek megfelel egy x_A vektor (A karakterisztikus vektora), aminek k. koordinátája pont akkor 1, ha $k \in A$. Ekkor a szimmetrikus differenciának a vektor összeadás felel meg ($\mathbb{F}_2$ feletti azaz mod 2).

Továbbá az hogy a halmazrendszer nem tartalmaz egymást tartalmazó halmazokat ekvivalens azzal hogy nem tartalmaz diszjunkt halmazokat, mert ha A, B diszjunkt, akkor $A, A \oplus B$ tartalmazó, továbbá ha A, B tartalmazó, akkor $A, A \oplus B$ diszjunkt. Ezek következménye a következő alapvető állítás. Az állítás megfogalmazásához először két definíció következik.

1.1.2. Definíció. *Egy $\mathbb{F}_2$ feletti n dimenziós lineáris tér k dimenziós alterét (n, k) kódnak nevezzük. Ha egy K (n, k) kódra teljesül, hogy $\forall x_1, x_2 \in A, x_1, x_2 \neq 0$-ra teljesül, hogy $x_1 \odot x_2 \neq 0$ ($\odot$ a koordinátánkénti szorzást jelöli), azaz bármely két nem nulla vektorban van közös egyes, akkor azt mondjuk hogy K egy metsző (n, k) kód.*

1.1.3. Definíció. *Metsző lineáris kód probléma: Adott n-re mi a legnagyobb k, hogy létezik metsző (n, k) kód.*

1.1.4. Állítás. *A 1.1.1 és 1.1.3 probléma ekvivalens. Adott n-re, ha 1.1.3 megoldása k, akkor 1.1.1 megoldása 2^k.*

A bizonyítás a fenti meggondolásokból következik.

Általában a két ekvivalens megfogalmazás közül a lineáris kódokra vonatkozó lesz a hasznosabb, mivel lineáris kódokra sok ismeret áll rendelkezésünkre a kódelméleti alkalmazások miatt.

A továbbiakban feltesszük, hogy $n \geq 3$, hogy az esetleges érdektelen speciális eseteket kizárjuk. A következőkben bevezetünk néhány jelölést lineáris kódokhoz.

1.1.5. Definíció. *Legyen K egy (n, k) kód. Ekkor jelöljük A_K-val a K egy bázisából mint oszlopvektorokból alkotott mátrixot, ez egy $\mathbb{F}_2^{n\times k}$-beli mátrix. Ha egyértelmű milyen K-ról van szó, akkor egyszerűen csak A-val jelöljük.*

Az A mátrix segítségével szeretnénk kifejezni, hogy K metsző-e. Erre ekvivalens feltételt ad a következő állítás.

1.1.6. Állítás. *A következő állítások ekvivalensek:*

a) K metsző.

b) Minden $a, b \in \mathbb{F}_2^k$ $a, b \neq 0$ vektorra létezik olyan index $j \in [n]$, hogy $(Aa)_j = 1$ és $(Ab)_j = 1$.

c) Minden $a, b \in \mathbb{F}_2^k$ $a, b \neq 0, a \neq b$ vektorra létezik olyan index $j \in [n]$, hogy $(Aa)_j = 1$ és $(Ab)_j = 0$.

Bizonyítás. 1.) a) és b) ekvivalens:

Az A mátrix képtere éppen a K lineáris kód. Az hogy minden nem 0 vektorpár a képtérben tartalmaz közös egyest éppen azt jelenti, hogy K metsző.

2.) b) és c) ekvivalens:

Az $a = b$ eset triviális b) esetben. Különben, ha a, b-hez megfelelő j b)-hez, akkor $a, a + b$-hez megfelelő j c)-hez és fordítva is: ha a, b-hez megfelelő j c)-hez, akkor $a, a + b$-hez megfelelő j b)-hez. Tehát pontosan akkor lesz minden a, b-re megfelelő j b)-ben mint c)-ben. □

A 1.1.3 problémában adott n-hez keressük a lehető legnagyobb k-t. Mivel n függvényében k monoton növekvően változik, ezzel ekvivalens kérdés adott k-hoz keresni a lehető legkisebb n-et. Ezekhez bevezetünk egy jelölést.

1.1.7. Definíció. *Jelölje $M(n)$ adott n-re a 1.1.3 probléma k megoldását. Jelölje $m(k)$ adott k-ra a legkisebb n-et, hogy $M(n) \geq k$.*

Most nevet adunk az általunk keresett tulajdonságú mátrixoknak, illetve egy hasonló tulajdonságú mátrix csoportnak.

1.1.8. Definíció. *Legyen $B \in \mathbb{F}_2^{n\times k}$. Azt mondjuk, hogy B metsző, ha teljesíti a 1.1.6-beli b) és c) feltételeket. Azt mondjuk, hogy B erősen metsző, ha ezen felül még minden $a, b \in \mathbb{F}_2^k$ $a, b \neq 0$ vektorra létezik olyan index $j \in [n]$, hogy $(Aa)_j = 0$ és $(Ab)_j = 0$.*

1.1.9. Definíció. *Jelölje $m_2(k)$ a legkisebb olyan n-et, amire van $\mathbb{F}_2^{n\times k}$-beli erősen metsző mátrix.*

1.1.10. Állítás. *A következő összefüggés áll fenn $m(k)$ és $m_2(k)$ között:*

$$m_2(k) = m(k) + 1.$$

A bizonyításra majd a geometriai részben térek vissza, egyelőre fogadjuk el ezt az állítást (2.1.4 állítás).

Már minden elő van készítve Komlós véletlen konstrukciójához, ami egy felső becslést ad $m(k)$-ra (és ekkor persze alsót $M(n)$-re). Komlós nem publikálta ezt az eredményét, de az eredmény megjelent Miklós Dezső [3] cikkében.

1.1.11. Tétel. *Fennáll a következő egyenlőtlenség:*

$$m(k) \leq 1 + k\frac{\log 4}{\log \frac{4}{3}} \simeq 1 + 4{,}82\ldots k.$$

Bizonyítás. Konstruálunk egy metsző A mátrixot. Ehhez rekurzívan definiálunk egy A_i mátrix sorozatot úgy, hogy $A_i \in \mathbb{F}_2^{i\times k}$ és az olyan $a, b \neq 0$ vektorpárok száma (feltehetjük hogy $a \neq b$ és ezt fel is tesszük a továbbiakban, az egyenlő párokra automatikusan teljesül a feltétel, ha $k \geq 2$), amire nincs $j \leq i$, hogy $(A_i a)_j = = 1$ és $(A_i b)_j = 1$ (nevezzük ezeket lefogatlan pároknak) legfeljebb $\lfloor 4^k(\frac{3}{4})^i \rfloor$. Ekkor $A = A_{1+\lfloor k\frac{\log 4}{\log \frac{4}{3}}\rfloor}$ jó lesz, mert

$$\lfloor 4^k(\frac{3}{4})^{1+\lfloor k\frac{\log 4}{\log \frac{4}{3}}\rfloor} \rfloor = 0.$$

Tehát már csak a megfelelő mátrixsorozat megkonstruálása van hátra. Kezdőlépésnek az üres mátrix jó, mivel a, b vektor párból kevesebb mint 4^k van.

$i \geq 1$-re A_i A_{i-1}-ből úgy áll elő, hogy hozzáveszünk még egy v sort, ami az lefogatlan a, b pároknak, legalább az $1/4$ részére

$$< v, a >= 1$$

és

$$< v, b >= 1$$

azaz v lefogja őket.

Ezzel megfelelő A_i-t kapunk, már csak megfelelő v létezését kell belátni. Ehhez számoljuk meg az olyan $v, a, b \in \mathbb{F}_2^k$ hármasokat, amire a, b egy lefogatlan pár és $< v, a >= 1$ és $< v, b >= 1$, azaz v lefogja őket, hívjuk ezt a mennyiséget h-nak. Legyen továbbá az eddig lefogatlan párok száma f és a lehetséges v vektorok száma $2^k = g$. Jelölje a lefogatlan párok halmazát F.

Először is kiszámolhatjuk h-t úgy, hogy minden lefogatlan a, b-hez megszámoljuk a megfelelő v-ket:

$$h = \sum_{(a,b)\in F} |\{v| < v, a >= 1 \wedge < v, b >= 1\}|.$$

Viszont

$$|\{v| < v, a >= 1 \wedge < v, b >= 1\}| = \frac{g}{4},$$

mivel ez egy 2 kodimenziós affin altér. Következésképpen

$$h = \frac{fg}{4}$$

Hasonlóan

$$h = \sum_{v} |\{(a, b) \in F| < v, a >= 1 \wedge < v, b >= 1\}|,$$

ami egy g tagú összeg, melynek már tudjuk hogy értéke legalább $\frac{fg}{4}$, tehát valamelyik összeadandó legalább $\frac{f}{4}$, azaz van olyan v ami $\frac{f}{4}$ lefedetlen párt lefed és éppen ilyen v-t kerestünk.

Ezzel az állítást beláttuk. □

1.2. Felső becslés $M(n)$-re

Ebben az alfejezetben Katona és Srivastava eredményét mutatom be, akik kódelméleti módszerekkel adtak felső becslést $M(n)$-re.

Alapvető kódelméleti definíciók és jelölések következnek.

1.2.1. Definíció. *Jelölje $e(v)$ a v vektorban előforduló egyesek számát.*

1.2.2. Definíció. *u, v vektorok esetén Hamming távolságnak nevezzük és $H(u, v)$-vel jelöljük azon i indexek számát, amire $u_i \neq v_i$.*

1.2.3. Állítás. *Az $e(v)$ és $H(u, v)$ függvények a következő kapcsolatban állnak:*

$$H(u, v) = e(u + v).$$

A bizonyítás triviális, hiszen $u+v$ pont azokon az indexeken 1, ahol u, v különböző volt.

1.2.4. Definíció. *Egy K vektor halmaz Hamming távolsága a benne szereplő különböző kódszó párok Hamming-távolságának a minimuma, jelölése $H(K)$. Azaz*

$$H(K) = \min\{H(u, v) | u \neq v \wedge u, v \in K\}.$$

1.2.5. Definíció. *Jelölje (n, k, d) az olyan (n, k) kódokat, melyek Hamming távolsága legalább d.*

A becslés alapját a következő lemma adja.

1.2.6. Lemma. *Minden metsző (n, k) kód egyben (n, k, k) kód.*

Bizonyítás. Legyen adott egy K metsző (n, k) kód.

Mivel K lineáris, ezért az 1.2.3 állítás alapján

$$H(K) = \min\{e(u) | 0 \neq u \in K\}.$$

Tehát azt kell belátni, hogy 0-n kívül minden K-beli vektorban legalább k egyes van.

Vegyünk egy rögzített $0 \neq v \in K$ vektort. Tegyük fel hogy vannak $u \neq w \in K$ vektorok, hogy $v \odot u = v \odot w$. Ekkor

$$v \odot (u + w) = 0,$$

ami lehetetlen, tehát nem lehet ilyen u, w különböző. Tehát K minden u elemére $v \odot u$ különböző, de ekkor K-nak legfeljebb $2^{e(v)}$ eleme lehet. Másfelől K-nak 2^k eleme van, tehát $e(v) \geq k$.

Mivel ez bármelyik $0 \neq v \in K$ vektorra elmondható, az állítást beláttuk. □

A következőben egy bizonyítás nélküli tételt közlünk, melynek bizonyítása megtalálható McEliece, Rodemich, Rumsey és Welch cikkében [5]. Először pár szükséges definíció:

1.2.7. Definíció. *Jelölje $\psi_1(n,d)$ a maximális elemszámát egy n hosszú bináris kódszavakból álló d Hamming távolságú vektor halmaznak.*

1.2.8. Definíció. *Vezessük be a következő jelölést is*

$$\psi(\delta) = \limsup_{n\to\inf} \frac{1}{n} \log_2 \psi_1(n, \lfloor \delta n \rfloor).$$

1.2.9. Definíció. *Jelölje H az entrópia függvényt, azaz $x \in$ [0,1]-re:*

$$H(x) = -x \log x - (1-x)\log(1-x).$$

Jelölje ϕ a következő függvény $x \in$ [0,1]-re:

$$\phi(x) = H(\frac{1}{2} - \sqrt{x(1-x)}).$$

És akkor a bizonyítás nélküli tétel:

1.2.10. Tétel. *Minden $x \in [0, \frac{1}{2}]$-re*

$$\psi(x) \leq \phi(x).$$

Továbbá ϕ monoton csökkenő $[0, \frac{1}{2}]$-en.

A felső becslés kimondásához szükségünk van még a felső korlát definíciójára.

1.2.11. Definíció. *Jelölje a*

$$x = \phi(x)$$

egyenletnek a $x \in [0, \frac{1}{2}]$ feltétel melletti egyetlen megoldását

$$\varepsilon \simeq 0{,}2834.$$

1.2.12. Tétel. *Teljesül a következő felső korlát:*

$$\limsup_{n\to\inf} \frac{1}{n} M(n) \leq \varepsilon \leq 0{,}2835.$$

Bizonyítás. Tegyük fel indirekten, hogy

$$\limsup_{n\to\inf} \frac{1}{n} M(n) = \varepsilon^* > \varepsilon.$$

Tudjuk $M(n)$ definíciója alapján, hogy van $(n, M(n))$ metsző kód. Ennek elemszáma természetesen $2^{M(n)}$. Másfelől 1.2.6 alapján ez egy $(n, M(n), M(n))$ kód. Ekkor 1.2.10 alapján az elemszáma legfeljebb $\psi_1(n, M(n))$. Ebből kapjuk a

$$2^{M(n)} \leq \psi_1(n, M(n))$$

egyenlőtlenséget. Ezt átrendezve kapjuk, hogy

$$\frac{1}{n} M(n) \leq \frac{1}{n} \log_2 \psi_1(n, M(n)).$$

Az indirekt feltevés miatt a $\frac{1}{n}M(n)$ sorozatnak végtelen sok $\frac{\varepsilon+\varepsilon^*}{2}$-nál nagyobb eleme van. Ekkor az előző egyenlőtlenség alapján a

$$\frac{1}{n} \log_2 \psi_1(n, \lfloor \varepsilon n \rfloor)$$

sorozatnak is. Következésképpen

$$\frac{\varepsilon + \varepsilon^*}{2} \leq \psi(\varepsilon).$$

Felhasználva a 1.2.10 tételt

$$\frac{\varepsilon + \varepsilon^*}{2} \leq \psi(\varepsilon) \leq \phi(\varepsilon) \leq \varepsilon,$$

ami ellentmondás.

Ezzel a tételt beláttuk. □

1.2.13. Következmény. *Elég nagy n esetén*

$$0{,}207 < \frac{1}{n} M(n) < 0{,}284.$$

A következő sejtést Cohen fogalmazta meg [2] cikkében. Azon alapszik, hogy majdnem minden (n, k, d) teljesíti Varshamov-Gilbert korlátot mely szerint

$$H(d) \geq 1 - \frac{k}{n}.$$

Ezt a korlátot itt nem bizonyítjuk, de kimondjuk az ebből adódó sejtést.

1.2.14. Állítás. *Cohen sejtése: Minden elég nagy n esetén*

$$0{,}207 < \frac{1}{n}M(n) < 0{,}22.$$

2. Geometriai megfogalmazások

Ebben a fejezetben a 1.1.1 probléma illetve azzal ekvivalens 1.1.3 probléma véges geometriai megfogalmazásaival foglalkozunk. Belátjuk geometria állításokról, hogy ekvivalensek a fenti problémákkal. Kimondjuk ezek néhány következményét, illetve kimondunk állításokat ezekre a problémákra. Mindezt először affin, majd projektív geometriai problémákkal.

2.1. Véges affin geometriai megfogalmazások

Az első geometriai megfogalmazás Katona és Srivastava cikkében [1] szerepel.

Emlékeztetőül a metsző és erősen metsző mátrixok definíciója.

2.1.1. Definíció. *Legyen $B \in \mathbb{F}_2^{n\times k}$. Azt mondjuk, hogy B metsző, ha teljesíti, hogy minden $a, b \in \mathbb{F}_2^k$ $a, b \neq 0$ vektorra létezik olyan index $j \in L_n$, hogy $(Aa)_j = 1$ és $(Ab)_j = 1$ és olyan i index, hogy $(Aa)_i = 1$ és $(Ab)_i = 0$. Azt mondjuk, hogy B erősen metsző, ha ezen felül még minden $a, b \in \mathbb{F}_2^k$ $a, b \neq 0$ vektorra létezik olyan index $l \in L_n$, hogy $(Aa)_l = 0$ és $(Ab)_l = 0$.*

2.1.2. Állítás. *Egy $A \in \mathbb{F}_2^{n\times k}$ mátrix pontosan akkor erősen metsző, ha sorai mint a $\mathbb{F}_2^k$ tér pontja olyanok, hogy bármely 2 kodimenziós ($k-2$ dimenziós) affin altér tartalmaz legalább egy pontot a halmazból.*

Bizonyítás. Vegyük észre, hogy $(Aa)_j$ éppen az A j-edik sorának és a-nak a skalárszorzata. Továbbá egy nem nulla vektorral vett skaláris szorzat értékének rögzítése éppen egy hipersíkot ad. Két nem párhuzamos hipersík metszete éppen egy 2 kodimenziós affin altér. Ezzel az állítást beláttuk. □

Ennek az állításnak azonnali következménye a következő.

2.1.3. Következmény. *Ha egy dimenzió tartó affin transzformációt alkalmazunk egy $A \in \mathbb{F}_2^{n\times k}$ erősen metsző mátrix minden sorára, akkor az így kapott mátrix is erősen metsző. Ilyen transzformáció egy 1 determinánsú mátrixszal való jobb szorzás, illetve egy adott vektor minden sorhoz való hozzáadása.*

Bizonyítás. Egy ilyen transzformáció az előző állításban szereplő tulajdonságot megtartja. □

Ezzel beláttuk egy véges affin geometriai probléma és az erősen metsző mátrixok kapcsolatát, de az eredeti probléma, $m(n)$ vizsgálata a metsző mátrixokkal állt kapcsolatban, tehát jó lenne belátni egy $m(n)$ és $m_2(n)$ közötti összefüggést. Ilyen a következő állítás.

2.1.4. Állítás. *Teljesül a következő egyenlőség:*

$$m(k) + 1 = m_2(k)$$

Bizonyítás. Ha van egy metsző mátrixunk, akkor hozzávéve egy csupa 0-ból álló sort egy erősen metsző mátrixot kapunk, ezért

$$m(k) + 1 \geq m_2(k)$$

Ha van egy erősen metsző mátrixunk, akkor minden sorához hozzáadhatjuk az első sorát 2.1.3 következmény alapján és ugyanakkora, erősen metsző mátrixot kapunk. Ekkor az első sor csupa 0 lesz, ezért ez az index sosem lesz megfelelő j vagy i a metsző mátrixok definíciójában. Tehát a mátrix többi sora metsző mátrix kell hogy legyen. Következésképpen van eggyel kevesebb sorból álló metsző mátrix, így

$$m(k) + 1 \leq m_2(k)$$

teljesül. Ezzel az állítást beláttuk. □

Ennek következményeként most már kimondhatjuk az eredeti probléma és a geometriai probléma ekvivalenciáját. Ehhez először pontosan definiáljuk a problémát.

2.1.5. Definíció. *2 fedési probléma: Adott egy $\mathbb{F}_2$ feletti k dimenziós affin tér. Legalább hány pontját kell kiválasztani, hogy minden 2 kodimenziós altér tartalmazzon legalább egy pontot a kiválasztottak közül.*

És akkor az ekvivalenciát kimondó következmény.

2.1.6. Következmény. *A 1.1.3 és 2.1.5 problémák ekvivalensek. Míg 1.1.1 probléma megoldása adott n-re $M(n)$, addig 2.1.5 probléma megoldása adott k-ra $m(k)+1$.*

Most egy másik geometriai problémával való ekvivalenciát fogunk belátni, ami mint később kiderül szoros kapcsolatban áll ezzel a problémával.

2.1.7. Definíció. *Egy $0 \neq v \in \mathbb{F}_2^k$ vektorra jelölje $H(v)$ azt a hipersíkot, melyek b pontjait az $< v, b >= 1$ egyenlet határozza meg.*

A következő állítás egyszerű, de később szükség lesz rá.

2.1.8. Állítás. *$H(v)$ alakban éppen a 0-t nem tartalmazó affin hipersíkok állnak elő.*

Bizonyítás. A hipersík nem tartalmazhatja a 0-t, mert $< v,0 >= 0$. Másfelől a vele párhuzamos hipersík tartalmazza 0-t, így előáll $< v, b >= 0$ alakban, valamilyen v-re. Ekkor az eredeti hipersík $H(v)$. □

A következő állítás a metsző mátrixok és egy fedési probléma között teremt kapcsolatot.

2.1.9. Állítás. *Egy A mátrix pontosan akkor metsző, ha v soraira teljesül, hogy a $H(v)$ hipersíkok lefedik $\mathbb{F}_2^k$ minden 0-t nem tartalmazó egyenesét.*

Bizonyítás. $\mathbb{F}_2^k$ 0-t nem tartalmazó egyenesei éppen a nem 0 pontpárok. Ezen a, b-khez kell olyan hipersík, ami fedi őket, azaz olyan v sorvektor, amire $< v, a >= 1$ és $< v, b >= 1$. Ez pontosan a 1.1.6-beli b) feltétel. □

2.1.10. Definíció. *Egy pont kihagyott egyenes fedési probléma: Az $\mathbb{F}_2^k$ affin térből legalább hány 0-t nem tartalmazó hipersíkot kell kiválasztani, hogy minden 0-t nem tartalmazó egyenest lefedjen.*

2.1.11. Következmény. *A 2.1.10 és 2.1.5 problémák ekvivalensek, adott k-ra $m(k)+$ $+ 1$ és $m(k)$ a megoldásuk rendre.*

Ez a legutóbbi ekvivalense a problémának egy új megközelítési módot ad. Az affin alterek mérete, illetve hogy hány egyenest tartalmaznak nem lehet annyira sokféle (csak a dimenziótól függ). Továbbá ha a kiválasztott hipersíkok minden részhalmazára tudnánk, hogy hány dimenziós, akkor egy szitaformulával meg tudnánk mondani, hogy hány egyenest fednek le (speciálisan hogy lefedik-e mindet).

Ezzel a megközelítéssel eddig nem jutottam el felső vagy alsó becsléséig $m(k)$-nek, mindenesetre most az ebben az irányban belátott állítások következnek.

A következő pár állítás lineáris algebrai alapismeretek alkalmazása, definíciók bevezetése a konkrét esetre. Továbbá néhány jelölést vezetek be, amikre a későbbi tételhez lesz szükség.

2.1.12. Definíció. *Azt mondjuk, hogy $A = \{H(v_i)\}$ hipersíkok egy halmaza elemien összefüggő, ha $\sum v_i = 0$ (ilyen az üres halmaz is).*

2.1.13. Állítás. *Egy $H(v_i)$ hipersík halmaz metszete pontosan akkor üres, ha van páratlan elemszámú elemien összefüggő részhalmaza.*

Bizonyítás. Ez abból a lineáris algebrából ismert állításból következik, hogy egy egyenlet rendszer akkor megoldhatatlan, ha lineáris kombinációjaként előáll a $1 = 0$ egyenlet. □

2.1.14. Definíció. *Legyen $A = \{H(v_i)\}$ hipersík rendszer $\mathbb{F}_2^k$-ban. Jelölje $q(A)$ az A elemien metsző részhalmazainak számát és $d(A)$ a metszet dimenzióját (tekintsük az üres halmazt is 0 dimenziósnak most, hiszen a lefedett egyenesek érdekelnek csak minket és egy nulla dimenziós altérben nincs egyenes).*

Jelölje továbbá $e(A)$ az A által lefedett egyenesek számát.

2.1.15. Állítás. *Legyen $A = \{H(v_i)\}$ hipersík rendszer $\mathbb{F}_2^k$-ban, melynek metszete nem üres. Ekkor teljesül a következő egyenlőség*

$$d(A) = k - |A| + \log_2(q(A)).$$

Bizonyítás. Jelölje $B = \{v_i\}$ a meghatározó vektorok halmazát. Továbbá $dim(B)$ a vektorok által feszített altér dimenzióját. Ekkor lineáris algebrai ismeretek alapján

$$d(A) = k - dim(B),$$

azaz a megoldások éppen annyi kodimenziós alteret alkotnak, ahány dimenziós az egyenletrendszer (ha van megoldás, de azt feltettük). Továbbá ha vesszük B-nek egy bázisát, akkor a többi vektor tetszőleges részhalmaza előáll ezek lineáris kombinációjaként pontosan egyféleképpen. Tehát

$$q(A) = 2^{|A|-dim(B)},$$

azaz

$$-dim(B) = -|A| + \log_2(q(A)),$$

és ezt behelyettesítve az első egyenletünkbe kapjuk a bizonyítandó állítást. □

2.1.16. Definíció. *Jelölje $E(k)$ $\mathbb{F}_2^k$ egyeneseinek a számát. Ekkor persze*

$$E(k) = \binom{2^k}{2}.$$

Már minden elő van készítve a szitaformulából adódó tétel kimondásához.

2.1.17. Tétel. *Legyen $A = \{H(v_i)\}$ hipersík rendszer. Ekkor*

$$e(A) = \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} E(d(B)).$$

Bizonyítás. Ez lényegében a szitaformula alkalmazása ebben a speciális esetben. Jelölje $w(B)$ a B hipersík halmaz mindegyike által lefedett egyenesek számát. A szitaformula szerint

$$e(A) = \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} w(B),$$

de mivel

$$w(B) = E(d(B)),$$

az állítást beláttuk. □

A következő következmény az elemien összefüggő részhalmazok jelentőségét mutatja.

2.1.18. Következmény. *Ha adott egy $A = \{H(v_i)\}$ hipersík rendszerünk és tudjuk, hogy mely részhalmazai elemien összefüggőek, akkor meg tudjuk mondani, hogy hány egyenest fednek le (speciálisan, hogy lefedik-e mindet ami nem megy át 0-n).*

Bizonyítás. A 2.1.17 tételben szereplő $|B|$ természetesen ismert. 2.1.13 állítás megmondja, hogy a B-hez tartozó metszet üres-e. Ha nem akkor

$$d(B) = n - |B| + \log_2(q(B))$$

a 2.1.15 állítás alapján, ahol $q(B)$ ismert a feltétel szerint. Továbbá 2.1.16 alapján

$$E(k) = \binom{2^k}{2},$$

ezzel a következményt beláttuk. □

2.1.19. Megjegyzés. *Ezen a ponton a következő heurisztikus megfigyeléseket tehetjük:*

- *Az $e(A)$ mennyiséget növeli a páratlan elemszámúak metszete és csökkenti a páros elemszámúak metszete (legalább is közvetlenül a 2.1.17 képletben).*
- *Páratlan sok elemien összefüggő hipersík csökkenti azon részhalmazokhoz tartozó $E(d(B))$ értéket (2.1.13), amiben előfordul (így általában csökkenti $e(A)$-t)*

– *Páros sok elemien összefüggő hipersík növeli azon azon részhalmazokhoz tartozó $E(d(B))$ értéket (2.1.15), amiben előfordul (így általában csökkenti $e(A)$-t)*

Ezek alapján vizsgálhatjuk a azt az általánosított problémát, amikor a geometriai háttértől elvonatkoztatva A tetszőleges részhalmaz rendszerére azt mondhatjuk, hogy elemien összefüggő és így vizsgáljuk a képleteink alapján kiszámolt $e(A)$ értéket.

Itt is ugyanúgy megkérdezhető, hogy mi A legkisebb lehetséges elemszáma, amire $e(A)$ legalább az összes egyenes száma. Speciális esetként adódik amikor egyik részhalmaz sem elemien összefüggő, ugyanis heurisztikáink szerint az elemi összefüggőség csökkenti $e(A)$-t.

Sajnos kis n értékekre megvizsgálva nem tűnik valószínűnek, hogy ez a szélső helyzet: n paritásától függően $e(A_k)$ (A_k jelöli a k darab általános helyzetű hipersík halmazát) vagy viszonylag gyorsan a maximális egyenes szám fölé megy, vagy pedig sosem éri el azt.

2.2. Véges projektív geometriai megfogalmazások

Ebben az alfejezetben az előző részben leírt problémákat terjesztjük ki projektív geometriára. Ez szorosabb kapcsolatot teremt a két probléma között, megtartja az eddig felfedezett jó tulajdonságokat, sőt néhány állítást erősít.

Először definiáljuk a problémák projektív megfelelőjét. A következő kiterjesztés elsőre elég erőltetettnek tűnik, de segít jobban megérteni a korábbi két geometriai megfogalmazás közötti kapcsolatot.

2.2.1. Definíció. *Projektív 2 fedési probléma: Adott egy $\mathbb{F}_2$ feletti k dimenziós projektív tér. Legalább hány pontját kell kiválasztani, hogy minden 2 kodimenziós altér tartalmazzon legalább egy pontot a kiválasztottak közül, ha egy kitüntetett hipersíkjáról nem szabad pontokat választani és altereit nem is kell lefedni.*

Persze ez ekvivalens az affin megfelelőjével.

2.2.2. Állítás. *2.1.5 és 2.2.1 ekvivalens, mindkettőnek a megoldása $m_2(k)$.*

Bizonyítás. Bár kiegészítettük a problémát egy végtelen távoli hipersíkkal, valójában azt ki is zártuk a fedésből. □

2.2.3. Definíció. *Projektív egyenes fedési probléma: Az $\mathbb{F}_2$ feletti k dimenziós projektív térből legalább hány 0-t nem tartalmazó hipersíkot kell kiválasztani, hogy minden 0-t nem tartalmazó egyenest lefedjen.*

2.2.4. Állítás. *2.1.10 és 2.2.3 ekvivalens. Míg 2.1.10 megoldása $m(k)$, addig 2.2.3 megoldása eggyel több, de mivel*

$$m_2(k) = m(k) + 1,$$

ez éppen $m_2(k)$.

Bizonyítás. Jelöljük a bizonyításban $m_1(k)$-nak a 2.2.3 probléma megoldását.

Egy megfelelő affin fedéshez hozzávehető a végtelen távoli hipersík, így projektív fedés lesz, tehát

$$m_1(k) \leq m(k) + 1.$$

Másfelől ha van egy projektív fedésünk, akkor abból egy kiválasztott hipersíkot elhagyva éppen egy affin tér eggyel kevesebb elemű fedését kapjuk, tehát

$$m_1 \geq m(k) + 1.$$

Ezzel az állítást beláttuk, azaz $m_1(k) = m_2(k)$. □

Most már beláthatjuk a két probléma közötti kapcsolatot.

2.2.5. Állítás. *A 2.2.1 probléma és a 2.2.3 probléma egymás duálisa.*

Bizonyítás. Valóban, a pont megfelelője a hipersík, az egyenes megfelelője a 2 kodimenziós altér és ugyanezek fordítva is igazak. Továbbá a megfelelő tartalmazások pont megfordulnak. □

Most az előző alfejezet végén lévő definíciókat és állításokat fogom átírni projektívre, amik néhány módosítással fognak járni.

2.2.6. Definíció. *2.1.7 definíciót kiterjesztjük projektívvé azzal, hogy $H(0)$ jelöli a végtelen távoli hipersíkot.*

2.2.7. Definíció. *Az elemi összefüggőség 2.1.12 definíciója úgy módosul, hogy csak páros elemszámú részhalmazokra értjük. (az eddigi páratlan elemszámú elemi metsző halmazok, most a végtelen távoli hipersíkkal együtt alkotnak elemien metsző halmazt)*

2.2.8. Definíció. *A 2.1.14 definícióbeli $q(A)$, $d(A)$ és $e(A)$ jelölések módosítatlanul érvényben maradnak.*

2.2.9. Definíció. *Jelölje $E(k)$ egy $\mathbb{F}_2$ feletti k dimenziós projektív tér egyeneseinek számát.*

Ezzel minden jelölést bevezettünk (és esetleg módosítottunk), amire szükségünk lesz. Most a megfelelő állítások és sejtések módosítása következik projektív térre.

2.2.10. Állítás. *Teljesül, hogy*

$$E(k) = \frac{\binom{2^{k+1}-1}{2}}{3}.$$

Bizonyítás. Jelölje $p(k)$ a k dimenziós projektív tér pontjainak számát. Ekkor

$$p(k) = 2^{k+1} - 1.$$

Másfelől bármely két ponton át megy egyenes és minden egyenesen 3 pont van, így ha veszünk minden pontpárt, akkor minden egyenest 3-szor számolunk. Tehát

$$E(k) = \frac{\binom{p(k)}{2}}{3}$$

teljesül. A két képletünkből következik az állítás. □

2.2.11. Állítás. *Legyen $A = \{H(v_i)\}$ hipersík rendszer egy $\mathbb{F}_2$ feletti k dimenziós projektív térben. Ekkor minden további feltétel nélkül*

$$d(A) = k - |A| + \log_2(q(A)).$$

Bizonyítás. Az állítást indukcióval bizonyítjuk. Kezdetben

$$d(\emptyset) = k - |\emptyset| + \log_2(q(\emptyset)).$$

Hasonlóan egy elemű halmazra.

A továbbiakban feltehetjük az általánosság rovása nélkül, hogy $H(0) \in A$. Ezt fel is tesszük. Amikor A-hoz egy új $H(v)$ hipersíkot veszünk (így kapjuk A'-t), akkor vizsgáljuk meg, hogy $H(v)$ tartalmazza-e az eddigi metszetet.

Ha nem, akkor $H(v)$ nem függ össze elemien az eddigi hipersíkok semmilyen

részhalmazával, mert akkor azok metszetét tartalmazná, tehát

$$q(A') = q(A).$$

Továbbá a dimenzió tétel miatt

$$d(A') + k = d(A) + k - 1,$$

azaz

$$d(A') = d(A) - 1.$$

Ekkor

$$d(A') = d(A) - 1 = k - |A| - 1 + \log_2(q(A)) = k - |A'| + \log_2(q(A')).$$

Ha tartalmazza a metszetet, akkor

$$d(A') = d(A),$$

szintén a dimenzió tétel miatt. Viszont ekkor a v vektor előáll a v_i vektorok lineáris kombinációjaként, azaz hozzájuk véve nem növeli a rangjukat. Ez viszont a köztük lévő lineáris összefüggések számát kétszerezi. Mivel minden lineáris összefüggéshez éppen egy elemi összefüggés tartozik (vagy $H(0)$-val vagy anélkül), így

$$q(A') = 2q(A).$$

Ekkor

$$d(A') = d(A) = k - |A'| + 1 + \log_2(q(A)) = k - |A'| + \log_2(q(A')).$$

Ezzel az állítást beláttuk. □

2.2.12. Tétel. *Legyen $A = \{H(v_i)\}$ hipersík rendszer. Ekkor*

$$e(A) = \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} E(d(B)).$$

Bizonyítás. A bizonyítás megegyezik 2.1.17 bizonyításával, hiszen

$$e(A) = \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} w(B)$$

és

$$w(B) = E(d(B))$$

egyaránt fennáll itt is. □

A lényeges különbség tehát az affin és projektív eset között, hogy 2.1.15 és 2.1.13 állítások lényegében a 2.2.11 állításban egyesülnek, a hipersíkok metszeteinek speciális viselkedésének már csak egyféléje van.

2.2.13. Következmény. *Ha adott egy $A = \{H(v_i)\}$ hipersík rendszerünk egy $\mathbb{F}_2$ feletti k dimenziós projektív térben és tudjuk, hogy mely részhalmazai elemien összefüggőek, akkor meg tudjuk mondani, hogy hány egyenest fednek le (speciálisan, hogy lefedik-e mindet ami nem megy át 0-n).*

Sőt, rendelkezésünkre áll a következő összefüggés a kettő között:

$$e(A) = \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} \frac{\binom{q(B)2^{k-|B|}-1}{2}}{3}.$$

Bizonyítás. A 2.2.12 állításban belátott

$$e(A) = \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} E(d(B))$$

egyenletbe behelyettesítve $E(A)$ 2.2.10 állításban belátott

$$E(k) = \frac{\binom{2^{k+1}-1}{2}}{3}$$

értékét és a 2.2.11 állításban belátott

$$d(A) = k - |A| + \log_2(q(A))$$

egyenletet éppen a bizonyítandó állítást kapjuk. □

2.2.14. Megjegyzés. *A 2.1.19 pontban tett heurisztikus megfigyelések így a következőképpen módosulnak.*

- *Az $e(A)$ mennyiséget növeli a páratlan elemszámúak metszete és csökkenti a páros elemszámúak metszete (legalább is közvetlenül a 2.2.12 képletben).*
- *Páros sok elemien összefüggő hipersík növeli azon azon részhalmazokhoz tartozó $E(d(B))$ értéket (2.2.11), amiben előfordul (így általában csökkenti $e(A)$-t)*

Továbbra is vizsgálható a 2.1.19 pontban felvetett absztrakt verziója a problémának, amikor elvonatkoztatva a geometriai háttértől csak a képleteket használva próbálunk becslést adni. És bár a probléma megoldásához közelebb kerültünk, hiszen kevesebb nehezen kezelhető speciális eset van, ez nem oldja meg a problémát, hogy valószínűleg az általánosított problémának nem az általános helyzet a szélső esete.

A projektív geometriai átfogalmazással bár sok mindent megértettünk, de a kérdés kicsit mesterségesen hangzik ebben a megfogalmazásban. Sokkal természetesebb a következő kérdés.

2.2.15. Definíció. *Projektív egyenes fedési probléma: Egy $\mathbb{F}_2$ feletti k dimenziós projektív térből legalább hány hipersíkot kell kiválasztani, hogy minden egyenest lefedjen.*

Ennek a kérdésnek a megoldása segíthet a mi feladatunk megoldásában is, de ezzel a kérdéssel most nem foglalkozunk részletesebben.

3. Oblivious Transferek

Ebben a fejezetben az Oblivious Transferekről lesz szó, ami információ megosztási protokollok egy csoportja.

A fejezetben többnyire Brassard, Crépeau és Sántha cikkét fogjuk követni [4], de nem fogjuk teljes egészében feldolgozni, így akit érdekelnek a részletek, annak az eredeti cikket ajánlom. Jelölésekben viszont néhol eltérünk az eredeti cikktől.

Jelen dolgozatban néhány protokoll kerül ismertetésre, melyek egyike használja a metsző kódokat. A protokollok ismertetése mellett megmutatjuk miért jók a protokollok, de inkább csak intuitívan, nem fognak formális információelméleti bizonyítások szerepelni.

3.1. OT_2^k megvalósítása

Az információ megosztás egyirányú és két fél közötti. Jelölje a protokollokban az információ megosztót $\mathcal{A}$ és az információ fogadót $\mathcal{B}$. Az Oblivious Transfer legalapvetőbb verziója a következő helyzetre ad megoldást: $\mathcal{A}$ rendelkezik két bit információval és csak az egyiket szeretné megosztani $\mathcal{B}$-vel. Másfelől $\mathcal{B}$ nem szeretné, hogy $\mathcal{A}$ megtudja melyiket választotta.

A pontosabb definíció:

3.1.1. Definíció. *Kettőből egy bit Oblivious Transfernek nevezzük és OT_2^1-gyel jelöljük az olyan protokollokat, amik megvalósítják a következőt:*

$\mathcal{A}$ rendelkezik két bit információval: x_0 és x_1. A protokoll célja, hogy $\mathcal{B}$ megtudhassa x_0 és x_1 pontosan egyikét, de ne szerezhessen információt mindkettőről (még valószínűségi jellegűt sem). Ezenkívül $\mathcal{A}$ ne szerezhessen semmilyen információt, hogy $\mathcal{B}$ melyiket választotta.

Nem fogunk OT_2^1 megvalósításával foglalkozni, a cél hogy általánosabb protokollokat erre visszavezessünk.

A következő általánosabb protokoll, amikor $\mathcal{A}$ két k bites szóval rendelkezik és azok közül szeretne egyet megosztani. A formális definíció:

3.1.2. Definíció. *Kettőből egy szó Oblivious Transfernek nevezzük és OT_2^k-gyel jelöljük az olyan protokollokat, amik megvalósítják a következőt:*

$\mathcal{A}$ rendelkezik két szó ($\mathbb{F}_2^k$-beli vektor) információval: x_0 és x_1. A protokoll célja, hogy $\mathcal{B}$ megtudhassa x_0 és x_1 pontosan egyikét, de ne szerezhessen információt mindkettőről (még valószínűségi jellegűt sem). Ezenkívül $\mathcal{A}$ ne szerezhessen semmilyen információt, hogy $\mathcal{B}$ melyiket választotta.

A következő néhány definíció szükséges a protokollhoz, ami megvalósítja OT_2^k-et, OT_2^1 felhasználásával.

3.1.3. Definíció. *Legyen I egy index halmaza egy x vektornak. Ekkor x^I jelöli az I indexű helyen álló bitekből képzett vektort. Hasonlóan egy M mátrix esetén M^I jelölje az I indexű soraiból képzett mátrixot.*

3.1.4. Definíció. *Legyen $f : \mathbb{F}_2^n \to \mathbb{F}_2^k$ függvény. Azt mondjuk, hogy I informál f-ről, ha*

$$\exists a_0, a_1 \in \mathbb{F}_2^k, x \in \mathbb{F}_2^n : |\{z \in \mathbb{F}_2^n | z^I = x^I \wedge f(z) = a_0\}| \neq$$

$$\neq |\{z \in \mathbb{F}_2^n | z^I = x^I \wedge f(z) = a_1\}|.$$

Azaz intuitívan, ha ismerjük x^I-t, akkor lehet információnk $f(x)$-re. Ha I nem informál f-ről, akkor pusztán x^I ismerete alapján nem tudunk semmit (még valószínűségi alapon sem) $f(x)$-ről.

3.1.5. Definíció. *Legyen $f : \mathbb{F}_2^n \to \mathbb{F}_2^k$ függvény. Azt mondjuk, hogy f cikcakk függvény, ha minden I indexhalmazra I és $\overline{I}$ egyike nem informál f-ről. ($\overline{I}$ az I komplementere)*

A cikcakk függvények létén alapszik a következő protokoll.

3.1.6. Definíció. *OT_2^k protokoll: Legyen adott egy $f : \mathbb{F}_2^n \to \mathbb{F}_2^k$ cikcakk függvény.*

$\mathcal{A}$ kiválaszt véletlen szerűen $y_0, y_1 \in \mathbb{F}_2^n$ vektorokat, hogy $f(y_0) = x_0$ és $f(y_1) = x_1$. Ezek után OT_2^1 segítségével átküldi sorba a $OT_2^1(y_0^1, y_1^1)$, ..., $OT_2^1(y_0^n, y_1^n)$ üzeneteket.

3.1.7. Állítás. *A 3.1.6 protokoll valóban megvalósítja OT_2^k-t.*

Bizonyítás. Mivel minden információ átvitel OT_2^1 segítségével történt, ezért $\mathcal{A}$ nem tud semmit $\mathcal{B}$ választásáról.

$\mathcal{B}$ valóban megtudhatja az egyik teljes szót, például ha x_0 érdekli, akkor sorban y_0 bitjeit választja és végül behelyettesítve megtudja $x_0 = f(y_0)$ értékét. Másfelől $\mathcal{B}$ nem tud mindkét szóról információt szerezni, mert valamilyen I-re y_0^I és $y_1^{\overline{I}}$ lesz az összes információja és így mivel f cikcakk függvény, nem lehet információja x_0-ról is és x_1-ről is. □

A továbbiakban a cikcakk függvényeket vizsgáljuk, egész pontosan megnézzük, hogy egy lineáris leképzés mikor cikcakk függvény.

3.1.8. Definíció. *Egy M mátrixra jelölje f_M a hozzátartozó $x \to xM$ lineáris leképzést.*

A célunk belátni, hogy pontosan a metsző mátrixokhoz tartozó lineáris leképzések cikcakk függvények.

3.1.9. Állítás. *Legyen $M \in \mathbb{F}_2^{n\times k}$ mátrix.*

Egy I index halmaz pontosan akkor informál f_M-ről, ha $M^{\bar{I}}$ kisebb mint k rangú.

Bizonyítás. Ha fixáljuk x^I-t, akkor $x^{\bar{I}} \to xM$ egy affin leképzés, tehát minden felvett értéket ugyanannyiszor vesz fel. Az hogy felvesz-e minden értéket éppen $M^{\bar{I}}$ rangjától függ, mert ez lesz a képtér dimenziója. □

3.1.10. Következmény. *Legyen $M \in \mathbb{F}_2^{n\times k}$ mátrix. Az f_M függvény pontosan akkor cikcakk, ha bármely I indexhalmazra M^I és $M^{\bar{I}}$ legalább egyike k rangú.*

Most már kimondhatjuk a cél állítást.

3.1.11. Tétel. *Legyen $M \in \mathbb{F}_2^{n\times k}$ mátrix. f_M pontosan akkor cikcakk, ha M metsző.*

Bizonyítás. Azt fogjuk belátni, hogy a 1.1.6 állításbeli b) feltétel tagadása éppen a 3.1.10 következménybeli feltétel tagadása.

A b) feltétel tagadása:

$$\exists a, b \neq 0 \nexists j((Ma)_j = 1 \wedge (Mb)_j = 1),$$

azaz megfelelő a, b-re a képben nincs közös egyes, azaz a nullásaik mindent lefednek, tehát:

$$\exists a, b \neq 0 \exists I(M^I a = 0 \wedge M^{\bar{I}} b = 0).$$

A két létezés kvantort nyugodtan megcserélhetjük, azaz

$$\exists I \exists a, b \neq 0(M^I a = 0 \wedge M^{\bar{I}} b = 0).$$

Azaz létezik olyan I, amire sem M^I sem $M^{\bar{I}}$ nem teljes rangú.

Ezzel az állítást beláttuk. □

A következő következmény $m(k)$ ismeretének egyik lehetséges alkalmazását, illetve következményét mutatja.

3.1.12. Következmény. *A 3.1.6 protokollban a lehető legjobb lineáris f választása esetén $m(k)$-szor kell alkalmazni a OT_2^1 protokollt, hogy megvalósítsuk OT_2^k-t.*

3.2. OT_n^k megvalósítása

Ebben az alfejezetben tovább általánosítjuk a protokollt, és ismét visszavezetjük a korábbiakra.

Egy OT_2^k-nál általánosabb helyzet (protokoll), amikor $\mathcal{A}$ n darab k hosszúságú bitsorozattal rendelkezik és azok egyikét szeretné megosztani $\mathcal{B}$-vel az eddigiekhez hasonló módon.

A pontos definíció a következő:

3.2.1. Definíció. *n-ből egy szó Oblivious Transfernek nevezzük és OT_n^k-nel jelöljük az olyan protokollokat, amik megvalósítják a következőt:*

$\mathcal{A}$ rendelkezik n szó ($\mathbb{F}_2^k$-beli vektor) információval: $x_0, x_1, \ldots, x_{n-1}$. A protokoll célja, hogy $\mathcal{B}$ megtudhassa $x_0, x_1, \ldots, x_{n-1}$ pontosan egyikét, de ne szerezhessen információt legalább kettőről (még valószínűségi jellegűt sem). Ezenkívül $\mathcal{A}$ ne szerezhessen semmilyen információt, hogy $\mathcal{B}$ melyiket választotta.

Az előbb definiált OT_n^k-t szokták $ANDOS$nak is nevezni (All-or-Nothing Disclosure of Secrets). Ennek a protokollnak ismert alkalmazásai vannak különböző más protokollokban, például szavazásban, null-információs bizonyításokban, titok cserében, azonosításban. Ezekről többet Brassard, Crépeau és Sántha cikkéből [4] lehet megtudni.

Minden további előkészítés nélkül következhet a protokoll, ami megvalósítja OT_n^k-t.

3.2.2. Definíció. *OT_n^k protokoll: $\mathcal{A}$ kiválaszt véletlenszerűen $y_0, \ldots, y_{n-1} \in \mathbb{F}_2^k$ vektorokat. Először elárulja $\mathcal{B}$-nek y_0-t és $x_{n-1} + y_{n-1}$-et. Ezek után $i \in \{0, \ldots, n-2\}$-re elküldi OT_2^k segítségével $x_i + y_i$ és $y_i + y_{i+1}$ egyikét.*

3.2.3. Állítás. *A 3.2.2 protokoll valóban megvalósítja OT_n^k-t.*

Bizonyítás. Mivel minden információ átvitel OT_2^k segítségével történt, ezért $\mathcal{A}$ nem tud semmit $\mathcal{B}$ választásáról.

$\mathcal{B}$ valóban megtudhatja bármelyik szót, hiszen ha x_i érdekli, akkor először megtudja y_i-t (kezdetben tudja y_0-t és $j \in 0, \ldots, i-1$-re a $y_j + y_{j+1}$-et választja), majd $x_i + y_i$-t választja (vagy alapból tudja $i = n-1$ esetén) és így megtudja x_i-t.

Továbbá $\mathcal{B}$ nem szerezhet több szóról is információt, hiszen amint $x_i + y_i$-t választja egyszer, minden információja elveszik y_{i+1}-ről és így a további információk haszontalanok számára. □

A fejezetet a következő észrevételekkel zárjuk.

3.2.4. Megjegyzés.

- *A 3.2.2 protokoll $n-1$-szer használja OT_2^k-t OT_n^k megvalósításához.*
- *A 3.2.2 protokollban $y_0 = 0$ és $x_{n-1} = y_{n-1}$ feltehető, ez a megfogalmazás csak a jobb érthetőséget szolgálta.*
- *A 3.2.3 bizonyítás harmadik része nem túl precíz, inkább az intuícióra hagyatkozik, de mivel ez a protokoll csak igen lazán kapcsolódik az eredeti témához, precízebb bizonyításra itt nem kerül sor, de Brassard, Crépeau és Sántha cikkében [4] megtalálható.*

4. Néhány általánosítás

Két lehetséges általánosítását fogjuk vizsgálni a kérdésnek. Az egyikben a kódtól nem csak azt várjuk el, hogy metsző legyen, hanem hogy d-metsző legyen, azaz bármely két nem 0 kódszóban legyen d közös 1-es. A másik kérdésben diszjunkt kódszó párok megtiltása helyett páronként diszjunkt kódszó l-eseket tiltunk meg.

4.1. d-metsző kódok

Ebben a fejezetben Miklós Dezső [3] cikkét fogjuk követni. Két tétel fog szerepelni, az egyik bizonyítás nélkül, a másik bizonyítással.

Először alapvető definíciók és jelölések következnek.

4.1.1. Definíció. *Egy (n, k) kódra azt mondjuk, hogy d-metsző ($d \geq 1$), ha bármely két nem 0 kódszavának van legalább d közös egyese.*

4.1.2. Definíció. *d-metsző lineáris kód probléma: Adott n-re és d-re, mi a legnagyobb k, hogy létezik d-metsző (n, k) kód.*

Ennek a problémának a megoldását $M_d(n)$-nel jelöljük.

A fő kérdés, amit vizsgálni fogunk, hogy rögzített $\delta = \frac{d}{n}$ esetén és $n \to \inf$ mellett, mit tudunk mondani $\frac{M_d(n)}{n}$ határértékéről (speciálisan mikor lesz pozitív).

A következő lemma nagyon egyszerű, de igen hasznosnak fog bizonyulni a tétel bizonyításakor.

4.1.3. Lemma. *Adott k darab $\mathbb{F}_2^n$-beli vektor. Ezek pontosan akkor feszítenek egy d-metsző kódot, ha bármely két különböző nem üres részhalmazának x, y összege tartalmaz d közös egyest.*

Bizonyítás. A kód ekkor definíció szerint d-metsző lesz, csak azt kell ellenőrizni, hogy k dimenziós-e. Ehhez az kell, hogy lineárisan függetlenek legyenek a vektoraink, de az is teljesül, mert különben a 0 előállna nem üres összegként. □

4.1.4. Definíció. *Legyen $x, y \in \mathbb{F}_2^n$ vektorok és $I \in [n]$ ($d-1$ elemű) indexhalmaz. Azt mondjuk, hogy I lebuktatja x, y-t, ha x, y összes közös 1-ese I-ben van, azaz*

$$x^{\overline{I}} \odot y^{\overline{I}} = 0.$$

Ezt a tényt $L(I, x, y)$-nal jelöltjük.

4.1.5. Definíció. *Jelölje H az entrópia függvényt, azaz $0 \leq x \leq 1$-re*

$$H(x) = -x\log_2(x) - (1-x)\log_2(1-x).$$

Így már kimondhatjuk a fő tételt.

4.1.6. Tétel. *Minden $0 \leq \delta \leq 0.074$-re*

$$\liminf_{n\to\inf;\frac{d}{n}\to\delta} \frac{M_d(n)}{n} \geq \frac{\log_2 \frac{4}{3}}{2}(1-\delta) - \frac{1}{2}H(\delta).$$

Bizonyítás. Véletlen konstrukcióval fogjuk bizonyítani a tételt. Legyen először fix k, n, d.

Vegyünk k darab véletlen vektort $\mathbb{F}_2^n$-ből (mindegyik vektor mindegyik jegye egymástól függetlenül $\frac{1}{2}$ eséllyel 0 vagy 1). K az általuk generált kód. Legyen x, y ezeknek két nem üres részhalmazon vett összegük és $I \in \{1, \ldots, n\}$ $d-1$ elemű indexhalmaz. Ekkor

$$P(L(I,x,y)) \leq (\frac{3}{4})^{n-d+1}.$$

x, y választására $\leq 2^{2m}$ lehetőségünk van. I választására $\binom{n}{d-1}$ lehetőségünk van. Tehát

$$P(\exists x, y, I(L(I,x,y))) \leq (\frac{3}{4})^{n-d+1} 2^{2m} \binom{n}{d-1}.$$

Viszont

$$P(K : d-metsz, (n,k)) = P(\neg\exists x, y, I(L(I,x,y))).$$

Tehát

$$P(K : d-metsz, (n,k)) \geq 1 - (\frac{3}{4})^{n-d+1} 2^{2m} \binom{n}{d-1}.$$

Azaz biztosan létezik megfelelő K, ha

$$(\frac{3}{4})^{n-d+1} 2^{2m} \binom{n}{d-1} < 1.$$

Átrendezve kapjuk, hogy

$$M_d(n) \geq \frac{1}{2}\log_2(\frac{4}{3})(n-d+1) - \frac{1}{2}\log_2 \binom{n}{d-1} - 1,$$

amit leosztva n-nel és határértéket véve:

$$\liminf_{n\to\inf;\frac{d}{n}\to\delta} \frac{M_d(n)}{n} \geq \frac{\log_2 \frac{4}{3}}{2}(1-\delta) - \frac{1}{2}H(\delta).$$

□

4.1.7. Megjegyzés. *A tételben szereplő egyenlőtlenség bár fennáll $\delta \geq 0.075$ értékre is, de a jobb oldal nem pozitív, így az egyenlőtlenség ilyen δ értékekre semmitmondó.*

4.1.8. Következmény. *Fix d-re*

$$\liminf_{n\to\inf} \frac{M_d(n)}{n} \geq \frac{\log_2 \frac{4}{3}}{2}.$$

Bizonyítás. Az előző tételben $\delta \to 0$-t véve adódik a következmény. □

Miklós Dezső [3] cikkében szerepel egy felső becslés is $\frac{M_d(n)}{n}$-re, ezt bizonyítás nélkül megemlítjük, a bizonyítás megtalálható az eredeti cikkben.

4.1.9. Tétel. *Minden $0 \leq \delta \leq \frac{1}{4}$-re*

$$\limsup_{n\to\inf,\frac{d}{n}\searrow\delta} \frac{M_d(n)}{n} \leq H(\frac{1}{2} - \sqrt{\alpha(1-\alpha)}),$$

ahol $\alpha \in [2\delta, \frac{1}{2}]$ az egyetlen gyöke a következő egyenletnek

$$H(\frac{1}{2} - \sqrt{\frac{\delta}{x}(1-\frac{\delta}{x})})x = H(\frac{1}{2} - \sqrt{x(1-x)}).$$

4.2. l hosszú halmazláncok

Ebben a részben is az eredeti kérdést fogjuk általánosítani. A vizsgált feltétel itt az lesz, hogy a kód bármely l kódszavába legyen 2 olyan kódszó, aminek van közös 1-ese. Ez ekvivalens azzal a halmazelméleti feltétellel, hogy a halmazrendszerben nincs l hosszú tartalmazó lánc.

Mivel a definíciók, állítások, tételek és még a bizonyítások is igen hasonlóak az első fejezetben szereplőkhöz, így kevésbé részletezem őket.

4.2.1. Definíció. *Egy K (n,k) kódra azt mondjuk, hogy nem-l-diszjunkt, ha bármely l darab különböző, nem 0 kódszava közt van 2 olyan kódszó, amiknek van közös 1-ese.*

4.2.2. Definíció. *Nem-l-diszjunkt probléma: Jelölje $M(n,l)$, hogy n,l-re mi a legnagyobb k, hogy létezik nem-l-diszjunkt (n,k) kód.*

Jelölje $m(k,l)$, hogy adott k,l-re mi a legkisebb n, hogy létezik nem-l-diszjunkt (n,k) kód.

A probléma természetesen csak akkor érdekes, ha $l \geq 2$ ($M(n,1) = 0$). Továbbá $M(n,2) = M(n)$ és $m(k,2) = m(k)$. Ezenkívül $m(k,l)$ és $M(n,l)$ vizsgálata ekvivalens, egymásból kifejezhetők. Minél nagyobb l, annál gyengébb feltétel a nem-l-diszjunktság, tehát $M(n,l)$ l-ben monoton csökken, $m(k,l)$ l-ben monoton nő.

A következő tétel Komlós konstrukciójának általánosítása nem-l-diszjunktságra.

4.2.3. Definíció. *Azt mondjuk, hogy egy $A \in \mathbb{F}_2^{n\times k}$ mátrix nem-l-diszjunkt, ha $\{Ax | x \in \mathbb{F}_2^k\}$ egy nem-l-diszjunkt (n,k) kód.*

4.2.4. Állítás. *Egy $A \in \mathbb{F}_2^{n\times k}$ mátrix pontosan akkor nem-l-diszjunkt, hogyha minden $v_1,\ldots,v_l$ nem 0, lineárisan független vektor l-esre létezik j, hogy legalább két v vektorra $v_1,\ldots,v_l$ közül $(Av)_j = 1$.*

Bizonyítás. A bizonyítás azonnal adódik a definíciókból. (Av) alakban éppen az értékkészlet elemei állnak elő és a feltétel éppen az, hogy bármely különböző l között legyen 2 aminek van közös 1-ese. A lineárisan összefüggő vektorrendszerekben automatikusan van metszés. □

4.2.5. Tétel. *Teljesül a következő felső becslés $m(k,l)$-re:*

$$m(k,l) \leq 1 + \frac{\log 2^{lk}}{\log \frac{2^l}{l+1}} = 1 + \frac{lk}{l - \log_2(l+1)}.$$

Bizonyítás. Konstruálunk egy nem-l-diszjunkt A mátrixot. Ehhez rekurzívan definiálunk egy A_i mátrix sorozatot úgy, hogy $A_i \in \mathbb{F}_2^{i\times k}$ és az olyan $v_1,\ldots,v_l$ nem 0, lineárisan független vektor l-esek száma, amire nincs $j \leq i$, hogy $(A_i v)_j = 1$ legalább két v vektorra $v_1,\ldots,v_l$ közül (nevezzük ezeket lefogatlan l-eseknek) legfeljebb $\lfloor 2^{lk}(\frac{1+l}{2^l})^i \rfloor$. Ekkor

$$A = A_{1+\lfloor \frac{\log 2^{lk}}{\log \frac{2^l}{l+1}} \rfloor}$$

jó lesz, mert

$$\lfloor 2^{lk}(\frac{1+l}{2^l})^{1+\lfloor \frac{\log 2^{lk}}{\log \frac{2^l}{l+1}} \rfloor} \rfloor = 0.$$

Tehát már csak a megfelelő mátrixsorozat megkonstruálása van hátra. Kezdőlépésnek az üres mátrix jó, mivel megfelelő vektor l-esekből kevesebb mint 2^{lk} van.

$i \geq 1$-re A_i A_{i-1}-ből úgy áll elő, hogy hozzáveszünk még egy v sort, ami az lefogatlan vektor l-eseknek, legalább az $\frac{2^l-l-1}{2^l}$ részét lefogja.

Ezzel megfelelő A_i-t kapunk, már csak megfelelő v létezését kell belátni. Ehhez számoljuk meg az olyan $v, v_1, \ldots, v_l \in \mathbb{F}_2^k$ $l+1$-eseket, amire $v_1, \ldots, v_l$ egy lefogatlan l-es és v lefogja őket, hívjuk ezt a mennyiséget h-nak. Legyen továbbá az eddig lefogatlan l-esek száma f és a lehetséges v vektorok száma $2^k = g$.

Először is kiszámolhatjuk h-t úgy, hogy minden lefogatlan $v_1, \ldots, v_l$-hez megszámoljuk a nem megfelelő v-ket: ezek azok amik $v_1, \ldots, v_l$ közül legfeljebb eggyel adnak 1 skalárszorzatot. Ez $l+1$ darab l kodimenziós altér diszjunkt uniója, így

$$h = fg\frac{2^l - l - 1}{2^l}.$$

Hasonlóan

$$h = \sum_v |\{(v_1, \ldots, v_l) \in F | Lefog(v, v_1, \ldots, v_l)\}|.$$

ami egy g tagú összeg, melynek már tudjuk hogy értéke legalább $fg\frac{2^l-l-1}{2^l}$, tehát valamelyik összeadandó legalább $f\frac{2^l-l-1}{2^l}$, azaz van olyan v ami $f\frac{2^l-l-1}{2^l}$ lefogatlan l-est lefog és éppen ilyen v-t kerestünk.

Ezzel az állítást beláttuk. □

Az utolsó tételünk Katona és Srivistava első fejezetben prezentált eredményének általánosítása, felső becslés $M(n, l)$-re.

Először 1.2.6 lemma általánosítása.

4.2.6. Lemma. *Adott egy K nem-l-diszjunkt (n, k)-kód. Ekkor K egy (n, k, d) kód valamilyen d-re, amire*

$$d + M(n - d, l - 1) \geq k.$$

Bizonyítás. Legyen d a legkevesebb egyest tartalmazó, nem 0 kódszó egyeseinek a száma és v maga a vektor. 1.2.3 alapján ekkor K (n, k, d) kód. Ekkor azok a kódszavak, amik v-től diszjunktak, nem-$(l-1)$-diszjunktak a többi koordinátán, tehát elemszámuk legfeljebb $2^{M(n-d,l-1)}$. Másfelől azon kódszavak, amiknek v-vel ugyanaz a metszésük (v-vel ugyanazok a közös egyeseik) is pontosan ugyanennyien

vannak (vagy egy sincs, hiszen annak az altérnek az eltoltjai). Tehát összesen

$$2^k \leq 2^d 2^{M(n-d,l-1)},$$

amiből következik a bizonyítandó állítás. □

Továbbá használni fogjuk a 1.2.7 és 1.2.8 definíciókat, illetve a 1.2.10 tételt.

4.2.7. Definíció. *Definiáljuk az a_l sorozatot rekurzívan. $a_1 = 0$. $i > 1$-re a_i az*

$$x = \phi(\frac{x - a_{i-1}}{1 - a_{i-1}})$$

egyenlet $a_{i-1} \leq x \leq \frac{1+a_{i-1}}{2}$ feltételt kielégítő egyetlen gyöke.

4.2.8. Tétel. *Teljesül a következő felső korlát:*

$$\limsup_{n\to\inf} \frac{1}{n} M(n,l) \leq a_l.$$

Bizonyítás. Indukcióval bizonyítunk. $l = 1$-re az állítás triviális, $l = 2$-re ez éppen 1.2.12 tétel, hiszen $\varepsilon = a_2$ (de indíthatjuk $l = 1$-ről is a bizonyítást).

Tegyük fel indirekten, hogy

$$\limsup_{n\to\inf} \frac{1}{n} M(n,l) = \varepsilon^* > a_l.$$

Vizsgáljunk csak olyan nagy n-et, amire

$$\frac{1}{n} M(n, l-1) \leq a_{l-1} + \delta.$$

Tudjuk $M(n,l)$ definíciója alapján, hogy van $(n, M(n))$ nem-l-diszjunkt kód, vegyünk egy ilyet, jelölje K. Ennek elemszáma természetesen $|K| = 2^{M(n,l)}$. Másfelől a 4.2.6 lemma alapján ez egy $(n, M(n,l), \frac{M(n,l)-na_{l-1}-n\delta}{1-a_{l-1}-\delta})$ kód. Ekkor 1.2.10 alapján az elemszáma legfeljebb

$$|K| \leq \psi_1(n, \frac{M(n,l) - na_{l-1} - n\delta}{1 - a_{l-1} - \delta}).$$

Ebből kapjuk az egyenlőséget, hogy

$$2^{M(n,l)} \leq \psi_1(n, \frac{M(n,l) - na_{l-1} - n\delta}{1 - a_{l-1} - \delta}).$$

Ezt átrendezve kapjuk, mely szerint

$$\frac{1}{n}M(n,l) \leq \frac{1}{n}\log_2 \psi_1(n, n\frac{\frac{M(n,l)}{n} - a_{l-1} - \delta}{1 - a_{l-1} - \delta}).$$

Az indirekt feltevés miatt a $\frac{1}{n}M(n,l)$ sorozatnak végtelen sok $\frac{a_l+\varepsilon^*}{2}$-nál nagyobb eleme van. Ekkor az előző egyenlőtlenség alapján a

$$\frac{1}{n}\log_2 \psi_1(n, \lfloor n\frac{a_l - a_{l-1}}{1 - a_{l-1}}\rfloor)$$

sorozatnak is (δ-t úgy választjuk ε^* függvényében). Következésképpen

$$\frac{a_l + \varepsilon^*}{2} \leq \psi(\frac{a_l - a_{l-1}}{1 - a_{l-1}}).$$

Felhasználva a 1.2.10 tételt

$$\frac{a_l + \varepsilon^*}{2} \leq \psi(\frac{a_l - a_{l-1}}{1 - a_{l-1}}) \leq \phi(\frac{a_l - a_{l-1}}{1 - a_{l-1}}) = a_l,$$

ami ellentmondás.

Ezzel a tételt beláttuk. □

Ez a tétel felső becslést ad $M(n,l)$-re, méghozzá nem triviális becslést, mert $a_l < 1$.

A 4.2.5 tétel és 4.2.8 tétel alsó és felső becslést ad $\frac{M(n,l)}{n}$ végtelenben való viselkedésére. Ezen becsléseknek kis l-re vett kerekített értékét mutatja a következő táblázat.

l	2	3	4	5	6	7	8	9	10
$\frac{l-\log_2(l+1)}{l}$	0.208	0.333	0.420	0.483	0.532	0.571	0.604	0.631	0.654
a_l	0.283	0.437	0.534	0.602	0.652	0.691	0.722	0.747	0.768

Hivatkozások

[1] G.O.H. Katona, J. Srivastava: Minimal 2-coverings of a finite affine space based on gf(2), Journal of Statistical Planning and Inference 8 (1983), 375-388.

[2] G. Cohen, A. Lempel: Linear intersecting codes, Discrete Mathematics 56 (1985), 35-43.

[3] D. Miklos: Linear binary codes with intersecting properties, Discrete Aplied Mathematics 9 (1984), 187-196.

[4] G. Brassard, C. Crépeau, M. Sántha: Oblivious Transfers and Intersecting Codes, Transaction on Information Theory 42(6) (1996), 1769-1780.

[5] R. J. McEliece, E. R. Rodemich, H. Rumsey, L. R. Welch: New Upper Bounds on the Rate of a Code via the Delsarte-MacWilliams Inequalities, Transctions on Information Theory 23(2) (1977), 157-166.