NYILATKOZAT

Név: Kovács Benedek

ELTE Természettudományi Kar, szak: matematikus MSc

NEPTUN azonosító: ZVZ4F8

Szakdolgozat címe:
Páronként diszjunkt vektorpárok keresése F_2^n-ben előírt különbségsorozattal

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2022.05.28.

Kovács Benedek

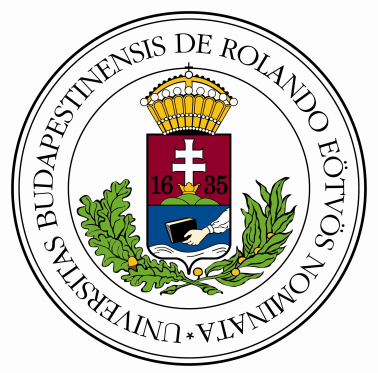
a hallgató aláírása

Páronként diszjunkt vektorpárok keresése $\mathbb{F}_2^n$-ben előírt különbségsorozattal

MSc szakdolgozat

írta: **Kovács Benedek**

témavezető: Nagy Zoltán Lóránt



Eötvös Loránd Tudományegyetem
Természettudományi Kar

Budapest, 2022

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Nagy Zoltán Lórántnak a rengeteg segítségét a kutatásban és a szakdolgozat elkészítésében, illetve hogy a sok hasznos tanácsával segít a kutatói pályán való elindulásomban. Szintén köszönetet szeretnék mondani az előző témavezetőmnek, Csikvári Péternek a kutatásban való sok segítségéért, és azért, hogy megismertette velem ezt az érdekes problémát. Továbbá köszönöm szépen a családom és a barátaim minden támogatását.

Tartalomjegyzék

1. Bevezetés **4**
1.1. Jelölések és elnevezések 5

2. A probléma története és korábbi eredmények **6**

3. Kezdeti észrevételek a fősejtéssel kapcsolatban **8**

4. A háromrészes mohó módszer bemutatása **10**

5. Kezdetek arányának szabályozása lineáris transzformációval **14**

6. A főprobléma megoldása $M \leq \frac{9}{32}N$ élre **17**

7. Csupa különböző különbségek **19**
7.1. Megfelelő transzformáció létezése 19
7.2. Az általánosított mohó módszer 21

8. Teljes párosítás kevés különbségosztály esetén **27**

9. Teljes párosítás sok azonos vektor esetén **34**

1. Bevezetés

Jelen szakdolgozat Balister, Győri és Schelp alábbi 2008-as sejtésével foglalkozik:

1.1. Sejtés. Legyen $n \geq 2$ egész és $m = 2^{n-1}$. Ha adottak $\mathbb{F}_2^n$-ben a $\mathbf{d_1}$, $\mathbf{d_2}$, ..., $\mathbf{d_m}$ nemnulla különbségvektorok (nem feltétlenül különbözők) úgy, hogy $\sum_{i=1}^{m} \mathbf{d_i} = \mathbf{0}$, akkor $\mathbb{F}_2^n$ felosztható diszjunkt $\{\mathbf{a_i}, \mathbf{b_i}\}$ párokra ($1 \leq i \leq m$) úgy, hogy minden i-re $\mathbf{a_i} - \mathbf{b_i} = \mathbf{d_i}$ legyen.

Ugyanebben az évben, a fenti sejtéstől függetlenül Bacher vetette fel a kérdésnek egy másik változatát [1], melyben $\mathbb{F}_2^n$ helyett $\mathbb{F}_p \setminus \{0\}$ elemeit osztjuk fel párokba, ahol p páratlan prím, és a megadott különbségek összegére nincs megszorítás. Ebben az esetben Preissmann és Mischler [10] bizonyítást adott az állítás igazságára. Ugyanez a kérdés $\mathbb{F}_p^n \setminus \{0\}$ elemeire is feltehető, ahol $n \geq 1$ egész. Karasev és Petrov [6] megmutatta, hogy ekkor az állítás ugyanilyen formában nem igaz, hanem csak egy relaxált verzióban, amit később bemutatunk.

Balister, Győri és Schelp [2] belátták az 1.1 sejtésnek azt az esetét, amikor a különbségvektorok fele mind azonos, és a többi pedig párokba sorolható úgy, hogy minden párban a két érték azonos.

A sejtésnek vizsgálható az alábbi relaxált változata is, melyben az $\mathbb{F}_2^n$ vektortérben nem teljes, hanem csak részleges párosítást keresünk megadott különbségek szerint:

1.2. Probléma. Legyenek $n \geq 2$, $N = 2^n$ és $M \leq \frac{1}{2}N - 2$ előre megadott egészek. Igaz-e, hogy tetszőleges $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_M} \in \mathbb{F}_2^n$ nemnulla különbségértékek esetén léteznek olyan csupa különböző $\mathbf{a_1}, \ldots, \mathbf{a_M}, \mathbf{b_1}, \ldots, \mathbf{b_M} \in \mathbb{F}_2^n$ vektorok, melyekre teljesül, hogy minden $1 \leq i \leq M$-re $\mathbf{a_i} - \mathbf{b_i} = \mathbf{d_i}$?

Dolgozatom fő eredményei a következők:

- A 4-6. fejezetben az 1.2 probléma állítását igazolom abban az esetben, amikor a megadott különbségek száma $M \leq \frac{9}{32}N$. Itt bemutatom a "háromrészes mohó módszert": ez egy olyan módszer, melyben a különbségvektorokat az első koordinátájuk alapján alkalmas sorrendbe teszem, majd sorban minden i-re olyan módon választom ki mohón az $\mathbf{a_i}$ és $\mathbf{b_i}$ vektorokat, hogy azoknak az első koordinátáját alkalmas módon rögzítem. Ez a módszer csak akkor működik, ha a különbségvektorok között a 0-val kezdődőek részaránya egy bizonyos intervallumon belülre esik; ellenkező esetben $\mathbb{F}_2^n$-nek egy megfelelő vektortér-automorfizmusát használva orvosolom a problémát.

- A 7. fejezetben az 1.2 problémát abban a speciális esetben vizsgálom, amikor minden $\mathbf{d_i}$ különbségérték legfeljebb $f(n)$-szer fordul elő, ahol $f(n) = o(2^n)$ egy rögzített függvény. Ebben az esetben beláttam, hogy a probléma megoldható $\frac{1}{2}N - o(N)$ különbség esetére. (A 7.1 tételben szerepel a konkrét felső korlát. Abban az esetben, amikor minden különbségvektor csupa különböző, vagyis $f(n) = 1$, akkor kellően nagy n-re és megfelelő $C > 0$ konstansra a feladat megoldható $\frac{1}{2}N - CN^{\frac{7}{8}}$ különbségre.) Ehhez a háromrészes mohó módszernek egy olyan általánosítását használom, ahol az egyes lépéseknél a kiválasztandó $\mathbf{a_i}$ és $\mathbf{b_i}$ vektoroknak nem csak az első, hanem alkalmas k-ra az első k koordinátáját adom meg.

- A 8. fejezetben az eredeti 1.1 sejtés igazságát mutatom meg abban az esetben, ha az $\frac{1}{2}N$ különbségvektor között csak legfeljebb $n-2\log n-1$ különböző érték fordul elő. Ennek belátásához a különbségértékek között úgynevezett *köröket* keresek, azaz tartalmazásra minimális, modulo $\mathbf{u}$ lineárisan összefüggő halmazokat, ahol $\mathbf{u}$ a leggyakrabban előforduló különbséget jelöli. Ezeknek megfelelően részleges párosításokat hozok létre úgy, hogy minden különbségértékből páros sok maradjon meg. Ezután pedig a feladat már egy sokkal egyszerűbb esetre visszavezethető, melyben csak 2-féle különbségérték van.

- A 9. fejezetben egy hasonló körkeresési módszer használatával belátom az 1.1 sejtést abban az esetben is, ha n elég nagy és a különbségvektorok legalább $\frac{28}{29}$ része mind azonos.

1.1. Jelölések és elnevezések

A továbbiakban az 1.1 sejtést fősejtésnek, az 1.2 problémát főproblémának fogjuk nevezni.

A dolgozat során $\mathbb{F}_p^k$ jelöli a p elemű test feletti k dimenziós vektorteret, $[n]$ pedig az $\{1,2,\ldots,n\}$ halmazt (ahol n pozitív egész).

Továbbá használni fogjuk az alábbi definíciót (jelölést) is:

1.3. Definíció. Legyen $B=\{B_1,B_2,\ldots,B_t\}$ egy multihalmaz, ahol $B_1,B_2,\ldots,B_t$ tetszőleges halmazok, és $t\in\mathbb{N}$. Ekkor B *szimmetrikus differenciája*:

$$\triangle B=\left\{x\in\bigcup_{i=1}^{t}B_i : |\{i:\ x\in B_i\}|\equiv 1 \pmod 2\right\}.$$

Speciálisan ha $t=2$, akkor $\triangle\{B_1,B_2\}$ helyett a $B_1\triangle B_2$ jelölést is használhatjuk.

2. A probléma története és korábbi eredmények

A fősejtésnek a bevezetőben említett, Bachertől származó változatára (melyben $\mathbb{F}_2^n$ helyett $\mathbb{F}_p \setminus \{0\}$ elemeit osztjuk fel párokba, ahol p páratlan prím, és a különbségértékek összegére nincs megszorítás) Preissmann és Mischler igenlő választ adott [10]; módszerük egy alkalmas $\mathbb{F}_p$ feletti többváltozós polinom értékeinek összegzésén alapul.

2.1. Tétel (Preissmann, Mischler)**.** *Legyen p páratlan prím és $M = \frac{p-1}{2}$. Ha adottak $\mathbb{F}_p$-ben a $d_1, d_2, \ldots, d_M$ nemnulla különbségek, akkor $\mathbb{F}_p \setminus \{0\}$ felosztható diszjunkt $\{a_i, b_i\}$ párokra ($1 \leq i \leq M$) úgy, hogy minden i-re $a_i - b_i = d_i$ legyen.*

Később Kohen és Sadofschi [7] ugyanerre az állításra új bizonyítást adtak a Kombinatorikus Nullstellensatz használatával.

Az állítás vizsgálható más ciklikus csoportokra is. A mod n maradékosztályok $\mathbb{Z}/(n)$ gyűrűjében jelölje $\mathbb{Z}/(n)^*$ az egységek, vagyis az n-hez relatív prím elemek halmazát. Adamaszek alábbi, páros rendű ciklikus csoportokra vonatkozó sejtését Kohen és Sadofschi [8] bizonyították:

2.2. Tétel (Kohen, Sadofschi)**.** *Legyen $n = 2M$ pozitív páros szám. Ha adottak tetszőlegesen a $d_1, d_2, \ldots, d_M \in \mathbb{Z}/(n)^*$ elemek, akkor $\mathbb{Z}/(n)$ felosztható diszjunkt $\{a_i, b_i\}$ párokra úgy, hogy minden i-re $a_i - b_i = d_i$ legyen.*

Karasev és Petrov [6] alábbi sejtése ezen állításnak a páratlan rendű ciklikus csoportokra vonatkozó változata:

2.3. Sejtés (Karasev, Petrov)**.** Legyen $n = 2M + 1$ pozitív páratlan szám. Ha adottak tetszőlegesen a $d_1, d_2, \ldots, d_M \in \mathbb{Z}/(n)^*$ elemek, akkor $\mathbb{Z}/(n) \setminus \{0\}$ felosztható diszjunkt $\{a_i, b_i\}$ párokra úgy, hogy minden i-re $a_i - b_i = d_i$ legyen.

A 2.1 tételnek egy másik lehetséges általánosítási módja, hogy $\mathbb{F}_p \setminus \{0\}$ helyett $\mathbb{F}_p^n \setminus \{0\}$-ra vizsgáljuk a problémát. Karasev és Petrov megmutatta, hogy ekkor az állítás ugyanilyen formában nem igaz: például ha minden $\mathbf{d_i}$ különbség értéke ugyanaz a nemnulla $\mathbf{d}$ vektor, akkor minden vektorpárban a két tagnak azonos $\langle \mathbf{d} \rangle$ szerinti mellékosztályba kell esnie, de a nemnulla mellékosztályok páratlan elemszámúak, így ilyen párokra nem oszthatók. Azonban belátták az alábbi állítást [6, Theorem 3]:

2.4. Tétel (Karasev, Petrov)**.** *Legyen p páratlan prím és $M = \frac{p^n-1}{2}$. Ha adottak $\mathbb{F}_p^n$-ben a $\{\mathbf{d_{1,1}}, \ldots, \mathbf{d_{1,n}}\}, \{\mathbf{d_{2,1}}, \ldots, \mathbf{d_{2,n}}\}, \ldots, \{\mathbf{d_{M,1}}, \ldots, \mathbf{d_{M,n}}\}$ halmazok úgy, hogy mindegyik halmaz egy bázisa $\mathbb{F}_p^n$-nek, akkor létezik olyan $g : [M] \to [n]$ függvény, hogy $\mathbb{F}_p^k \setminus \{\mathbf{0}\}$ felosztható diszjunkt $\{\mathbf{a_i}, \mathbf{b_i}\}$ párokra ($1 \leq i \leq M$) olyan módon, hogy minden i-re $\mathbf{a_i} - \mathbf{b_i} = \mathbf{d_{i,g(i)}}$ legyen.*

Ha $\mathbb{F}_p^n$ helyett $\mathbb{F}_2^n$-ben vizsgáljuk az állítást, akkor a teljes párosításhoz a nullvektort is be kell venni a párosítandó elemek közé. Ekkor sem igaz megszorítás nélkül az állítás tetszőleges nemnulla különbségvektorokra, mivel (mint ezt a 3. fejezetben is látni fogjuk) a különbségek összegének a vektortér összes elemének összegével, azaz nullával kell megegyeznie. Balister, Győri és Schelp sejtése (az 1.1 fősejtés) szerint a megfelelő teljes párosítás létezéséhez ez a feltétel elégséges is.

A [2] cikkben azt is leírják a szerzők, hogy $n \leq 5$ esetére igazolták a sejtést, illetve belátták a fősejtés állítását az alábbi speciális esetben [2, Theorem 4]:

2.5. Tétel (Balister, Győri, Schelp)**.** *A fősejtés megoldható abban az esetben, ha a* $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_{\frac{m}{2}}}$ *vektorok mind azonos értékűek, és minden* $1 \leq i \leq \frac{m}{2}$ *egészre* $\mathbf{d_{2i-1}} = \mathbf{d_{2i}}$.

Bizonyításuk fő ötlete az, hogy először mohó módon kijelöli a $\mathbf{d_1}$-től eltérő különbségekhez rendelt $\mathbf{a_i}$ és $\mathbf{b_i}$ értékeket úgy, hogy ha egy lépésben az $(\mathbf{a_i}, \mathbf{b_i})$ párt választottuk, akkor a következő lépésben az azonos különbséggel rendelkező $(\mathbf{a_i} + \mathbf{d_1}, \mathbf{b_i} + \mathbf{d_1})$ párt válasszuk, és így a végül megmaradó elemek $\mathbf{d_1}$ különbségű párokat fognak alkotni.

Jelen témában való kutatásom folyamán (azt követően, hogy a háromrészes mohó módszerrel beláttam egy $\mu > \frac{1}{4}$ értékre a főprobléma megoldhatóságát legfeljebb μN különbség esetére) 2021 szeptemberében Correia, Pokrovskiy és Sudakov egy általánosabb eredményüket publikálták [4, Thm 1.5], melyből következik az 1.2 probléma megoldhatósága $M \leq \frac{1}{2}N - o(N)$ esetére is:

2.6. Tétel. *Legyen* G *egy multigráf, melynek az élei* t *színnel vannak megszínezve úgy, hogy minden színosztály egy legalább* $t + 20t^{15/16}$ *élből álló párosítás. Ekkor létezik olyan* t *élből álló párosítás, melynek minden éle csupa különböző színű.*

2.7. Következmény. *Az 1.2 probléma állítása igaz* $M \leq \frac{1}{2}N - CN^{15/16}$ *esetén, ahol* $C = \frac{20}{2^{15/16}}$.

Bizonyítás. Az 1.2 problémára tekinthetünk úgy, hogy felveszünk egy gráfot, melynek csúcsai az $\mathbb{F}_2^n$ vektortér elemei, és minden megadott $\mathbf{d_i}$ különbségérték esetén behúzunk egy i színű élt az összes $\mathbf{d_i}$ különbségű pontpár közé. (Két pont között több színben is lehetnek élek, hiszen a $\mathbf{d_i}$ értékek között lehetnek egyenlőek.) Ekkor a feladat az lesz, hogy találjunk egy M élű párosítást, melynek minden éle különböző színű. Ha Correia, Pokrovskiy és Sudakov tételét alkalmazzuk az így kapott M db 2^{n-1} élből álló színosztályra, akkor megkapjuk a szükséges párosítást. □

Ha pedig Gao, Ramadurai, Wanless és Wormald alábbi sejtése [5] is igaz, akkor abból hasonló módon következne az 1.2 probléma megoldhatósága $M \leq \frac{1}{2}N - 2$ esetére is.

2.8. Sejtés. Legyen G egy multigráf, melynek az élei t színnel vannak megszínezve úgy, hogy minden színosztály egy legalább $t + 2$ élből álló párosítás. Ekkor létezik egy olyan t élből álló párosítás, melynek minden éle csupa különböző színű.

3. Kezdeti észrevételek a fősejtéssel kapcsolatban

A fősejtésről és a főproblémáról gyakran a gráfok nyelvén fogok beszélni. Ha M db különbségérték ($\mathbf{d_1}$, $\mathbf{d_2}$, …, $\mathbf{d_M}$) adott, akkor tekintsünk egy $2M$ csúcsú gráfot, mely M diszjunkt élből áll, és legyen minden élre ráírva egy $\mathbb{F}_2^n$-beli nemnulla címke (az i. élre $\mathbf{d_i}$). Úgy szeretnénk a gráf minden csúcsába csupa különböző $\mathbb{F}_2^n$-beli értékeket írni, hogy bármely két éllel összekötött csúcs értékének különbsége az őket összekötő él címkéjével egyezzen meg.

3.1. Lemma. *Az $\mathbb{F}_2^n$ vektortér összes elemének összege $\mathbf{0}$, ha $n \geq 2$.*

Bizonyítás. Adott $1 \leq i \leq n$-re 2^{n-1} vektor van $\mathbb{F}_2^n$-ben, melynek i. koordinátája 0 és 2^{n-1}, aminek 1. Így modulo 2 az összes vektor összegében az i. koordináta $2^{n-1} = 0$, mivel $n \geq 2$. □

3.2. Állítás. *A fősejtés nem lenne igaz, ha nem kötnénk ki, hogy a $\mathbf{d_i}$ címkék összege $\mathbf{0}$.*

Bizonyítás. Tegyük fel, hogy mégis igaz, és vegyük egy olyan megadását a $\mathbf{d_i}$ ($1 \leq i \leq M$) címkéknek, melyekre $\sum_{i=1}^{M} \mathbf{d_i} \neq 0$. Ekkor az $\mathbf{a_i}$, $\mathbf{b_i}$ vektorok egy helyes megadására $\sum_{i=1}^{M} \mathbf{d_i} = \sum_{i=1}^{M} (\mathbf{a_i} - \mathbf{b_i}) = \sum_{i=1}^{M} (\mathbf{a_i} + \mathbf{b_i}) = \sum_{i=1}^{M} \mathbf{a_i} + \sum_{i=1}^{M} \mathbf{b_i} = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \mathbf{x} = \mathbf{0}$, használva a 3.1 lemmát (azt is kihasználva, hogy 2 karakterisztikájú test fölötti vektortérben az összeadás ugyanaz, mint a kivonás). Ellentmondás. □

3.3. Megjegyzés. A főprobléma $M = \frac{1}{2}N - 1$ esetén sem mindig oldható meg, ugyanis ha a megadott M különbség összege $\mathbf{0}$, akkor nincs a csúcsoknak helyes kitöltése: ha ki tudnánk tölteni helyesen a $2M$ csúcsot az $N = 2M+2$ elemű vektortér $2M$ különböző elemével, akkor ezen elemek összege $\mathbf{0}$ lenne, így a 3.1 lemma miatt a kimaradó két elem összege is $\mathbf{0}$, de ez azt jelenti, hogy a kimaradó két elem azonos, ami ellentmondás.

3.4. Állítás. *A főprobléma megoldhatósága $M = \frac{1}{2}N - 1$-re a $\sum_{i=1}^{M} \mathbf{d_i} \neq \mathbf{0}$ esetre ekvivalens a fősejtéssel.*

Bizonyítás. Ha a fősejtés igaz, akkor tetszőleges adott $\mathbf{d_1}$, $\mathbf{d_2}$, …, $\mathbf{d_M}$ nemnulla vektorokra (ahol $\sum_{i=1}^{M} \mathbf{d_i} \neq \mathbf{0}$) legyen $\mathbf{d_{M+1}} = \sum_{i=1}^{M} \mathbf{d_i}$, így $\sum_{i=1}^{M+1} \mathbf{d_i} = \mathbf{0}$. Ekkor a sejtés alapján léteznek csupa különböző $\mathbf{a_i}, \mathbf{b_i}$ vektorok úgy, hogy $\mathbf{a_i} - \mathbf{b_i} = \mathbf{d_i}$ minden $1 \leq i \leq M+1$-re, speciálisan így az első M élt is helyesen töltöttük ki páronként diszjunkt vektorpárokkal.

A másik irányhoz tegyük fel, hogy a főprobléma megoldható $M = \frac{1}{2}N - 1$-re, ha a különbségek összege nemnulla. Most vegyünk tetszőleges $\mathbf{d_1}$, $\mathbf{d_2}$, …, $\mathbf{d_{M+1}}$ nemnulla különbségeket, melyek összege $\mathbf{0}$. Ekkor $\sum_{i=1}^{M} \mathbf{d_i} = \mathbf{d_{M+1}} \neq \mathbf{0}$, így az első M él végpontjai kitölthetők megfelelően $2M$ különböző vektorral. A vektortér maradék két elemének összege megegyezik az eddigi $2M$ elem összegével (a 3.1 lemma miatt), ami éppen $\sum_{i=1}^{M} \mathbf{d_i} = \mathbf{d_{M+1}}$. □

Az alábbiakban mutatunk egy egyszerű mohó algoritmust (ami a Balister, Győri és Schelp cikkében [2, Theorem 4] bemutatott módszerhez hasonlóan jár el), mellyel a főprobléma megoldható a fősejtésbeli $\frac{1}{2}N$ db él felére.

3.5. Tétel. *A főprobléma megoldható $M \leq \frac{1}{4}N$ élre.*

Bizonyítás. Válasszuk ki az M db párt sorban egymás után. Ha már ki van választva $\mathbf{a_1}, \ldots, \mathbf{a_{i-1}}$ és $\mathbf{b_1}, \ldots, \mathbf{b_{i-1}}$, ahol $1 \leq i \leq M$, akkor próbáljunk meg keresni olyan $\mathbf{a_i}$-t és $\mathbf{b_i}$-t, hogy $\mathbf{a_i} - \mathbf{b_i} = \mathbf{d_i}$. Mivel $\mathbf{d_i} \neq \mathbf{0}$, $\mathbb{F}_2^n$ felbomlik $\frac{1}{2}N$ olyan párra, melyek mindegyikében a két tag különbsége $\mathbf{d_i}$: ezek a párok pontosan a $\langle \mathbf{d_i} \rangle$ egydimenziós altér szerinti mellékosztályai $\mathbb{F}_2^n$-nek. Ezen párok közül tudunk olyat találni, melynek egyik tagját sem választottuk még ki, mert az eddig kiválasztott legfeljebb $2(M-1)$ elem a párok közül összesen legfeljebb $2(M-1) < 2M \leq \frac{1}{2}N$-ben helyezkedik el. Így $\{\mathbf{a_i}, \mathbf{b_i}\}$-nek megválaszthatunk egy ilyen párt. □

A főprobléma hasonlóan megoldható, ha ugyan a megadott élek száma $\frac{1}{4}N$-nél nagyobb, de közülük elég soknak mind ugyanaz a címkéje.

3.6. Tétel. *Ha $\frac{1}{4} < \mu < \frac{1}{2}$ és $\alpha \geq 2\mu - \frac{1}{2}$, akkor megoldható a főprobléma, ha $M \leq \mu N$ és az élek közül legalább αN-nek mind azonos a címkéje.*

Bizonyítás. Legyenek a megadott különbségek $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_A}, \ldots, \mathbf{d_M}$, ahol $\mathbf{d_1} = \mathbf{d_2} = \cdots = \mathbf{d_A} = \mathbf{d}$ és $A \geq \alpha N$. Először válasszuk ki megfelelően a $\mathbf{d_{A+1}}, \ldots, \mathbf{d_M}$ élek végpontjait. Ezt meg tudjuk tenni a 3.5 tétel alapján, mert ezen élek száma $M - A \leq (\mu - \alpha)N \leq \frac{1}{4}N$. (Ez azért teljesül, mert $m \geq \frac{1}{4}$ miatt $\mu - \frac{1}{4} \leq 2\mu - \frac{1}{2} \leq \alpha$, így $\mu - \alpha \leq \frac{1}{4}$.)

Ezután már csak az kell, hogy a maradék A db $\mathbf{d}$ címkéjű élre találjunk megfelelő vektorokat, azaz találjunk az eddig fel nem használt vektorok között A db páronként diszjunkt vektorpárt úgy, hogy minden párban $\mathbf{d}$ legyen a vektorok különbsége.

Megint tekintsük az $\frac{1}{2}N$ db $\langle \mathbf{d} \rangle$ szerinti mellékosztályát $\mathbb{F}_2^n$-nek. Ezek mind $\mathbf{d}$ különbségű párok, melyek közül eddig legfeljebb $2(M-A)$-ban van lefoglalva legalább egy elem. Így a maradék párok száma legalább $\frac{1}{2}N - 2(M-A)$. És mivel $\alpha \geq 2\mu - \frac{1}{2}$, ezért $A \geq \alpha N \geq \left(2\mu - \frac{1}{2}\right) N \geq 2M - \frac{1}{2}N$, így $\frac{1}{2}N + 2A \geq 2M + A$, tehát $\frac{1}{2}N - 2(M-A) \geq A$. Tehát legalább A pár maradt. □

4. A háromrészes mohó módszer bemutatása

A 4-6. fejezetekben bemutatunk egy módszert, amellyel a 3.5 tételt meghaladó eredmény érhető el: ezzel a módszerrel belátható a főprobléma megoldhatósága $M \leq \frac{9}{32}N$ élre.

Fel fogjuk tenni, hogy van már egy olyan módszerünk, mellyel a főproblémát mindig megoldhatjuk $M \leq \lambda N$ él esetén (minden $n \geq 2$-re). Erre a módszerre λ-*algoritmusként* fogunk hivatkozni. A 3.5 tétel miatt például vehetjük λ értékét $\frac{1}{4}$-nek.

4.1. Megfigyelés. (i) Ha $\mathbf{v} \in \mathbb{F}_2^n$ egy 0-val kezdődő nemnulla vektor, akkor $\mathbb{F}_2^n$-nek a $\langle \mathbf{v} \rangle$ szerinti mellékosztályai között 2^{n-2} olyan van, amiben mindkét vektor 0-val kezdődik (továbbiakban: *0-0 párok*) és 2^{n-2} olyan, amiben mindkét vektor 1-gyel kezdődik (*1-1 párok*).

(ii) Ha $\mathbf{v} \in \mathbb{F}_2^n$ egy 1-gyel kezdődő vektor, akkor $\mathbb{F}_2^n$-nek a $\langle \mathbf{v} \rangle$ szerinti mellékosztályai mind olyan párok, melyek egy 0-val és egy 1-gyel kezdődő vektort tartalmaznak (továbbiakban: *0-1 párok*).

Ebben a fejezetben feltesszük, hogy a megadott M db különbség közül B db-nak 0 az első koordinátája és C db-nak 1. Legyen $B = \beta N$ és $C = \gamma N$, így ha az $M = \mu N$ jelölést használjuk, akkor $\mu = \beta + \gamma$.

A célunk az, hogy az élek kitöltésének sorrendjét a rajtuk lévő címkék első koordinátái alapján szabályozva, és az egyes élekre írható vektorok első koordinátáira megfelelő megkötéseket téve egy olyan mohó algoritmust kapjunk, mely nemcsak $\mu \leq \frac{1}{4}$ esetén működik, hanem β és γ bizonyos értékei esetén kicsivel nagyobb μ értékekre is.

Az alábbi módszert használjuk:

4.2. Algoritmus. *A B és C értékek függvényében választunk B_1 és B_2 egész számokat úgy, hogy $B_1, B_2 \geq 0$ és $B_1 + B_2 = B$. (A későbbiekben részletezzük, hogy B_1-et és B_2-t hogyan kell megfelelően megválasztani, hogy a módszer működjön.) Ezután a B db 0-val kezdődő különbséget tetszőlegesen felosztjuk egy B_1 és egy B_2 különbségből álló részre: az előbbit nevezzük "induló" csoportnak, az utóbbit "befejező" csoportnak. Így az éleknek három csoportja keletkezik:*

1. *az induló élek B_1 elemből álló csoportja,*
2. *az 1-gyel kezdődő élek C elemből álló csoportja,*
3. *a befejező élek B_2 elemből álló csoportja.*

A módszerünk az alábbi három lépésből áll:

1. *Az induló éleket töltsük ki 0-0 párokkal úgy, hogy a kezdő nullák elhagyásával kapott $n-1$ dimenziós vektorokra a λ-algoritmust használjuk.*
2. *Vegyük sorra egyesével az 1-gyel kezdődő éleket, és töltsük ki őket 0-1 párokkal tetszőlegesen.*

3. Végül vegyük sorra egyesével a befejező éleket, és töltsük ki őket 1-1 párokkal tetszőlegesen.

Az alábbiakban megvizsgáljuk, hogy mely B és C értékekre lehet olyan B_1-et és B_2-t találni, hogy ez a módszer garantáltan működjön, azaz mindhárom lépés teljesíthető legyen.

4.3. Állítás. *Tegyük fel, hogy van egy λ-algoritmusunk (ahol $\frac{1}{4} \leq \lambda < \frac{1}{2}$). Legyen $n \geq 3$ egész és $N = 2^n$. Ha a $B, C \geq 0$, $B_1, B_2 \geq 0$, $B_1 + B_2 = B$ egészekre teljesül $B_1 \leq \frac{1}{2}\lambda N$, $B_1 + C \leq \frac{1}{4}N$ és $C + 2B_2 \leq \frac{1}{4}N + 1$, akkor a 4.2 algoritmus mindig helyesen működik B db 0-val és C db 1-gyel kezdődő $\mathbb{F}_2^n$-beli különbségre, a B_1, B_2 értékeket választva.*

Bizonyítás. Megvizsgáljuk sorra, hogy a három lépés ebben az esetben működni fog.

1. Az algoritmus 1. lépésében az induló élek első koordinátáját elhagyva kapunk B_1 db $n-1$ hosszú nemnulla különbséget, melyekre a λ-algoritmust használva ráírhatjuk $\mathbb{F}_2^{n-1}$-nek $2B_1$ különböző elemét, mert $B_1 \leq \lambda \cdot 2^{n-1} = \frac{1}{2}\lambda N$. Ha a csúcsokba írt értékek elé írunk egy 0-s koordinátát, akkor $\mathbb{F}_2^n$-nek kapjuk $2B_1$ különböző vektorát, melyeknek a páronkénti különbsége mindenhol a megfelelő induló él címkéje.

2. A 2. lépésben azt kell belátnunk, hogy sosem akadunk el, azaz mind a C db 1-gyel kezdődő élnél találni fogunk legalább egy megfelelő 0-1 párt (melynek még egyik tagját sem választottuk ki). Legyen a C db él közül a J-ediknek a címkéje $\mathbf{d}$. Ekkor mivel $\mathbf{d}$ 1-gyel kezdődik, $\mathbb{F}_2^n$ felosztható $2^{n-1} = \frac{1}{2}N$ db $\mathbf{d}$ különbségű 0-1 párra. Vizsgáljuk meg, hogy ezek közül legfeljebb hány foglalt. Az $\mathbb{F}_2^n$-ben eddig foglalt vektorok száma $2B_1 + 2(J-1)$ (mivel az 1. lépésben $2B_1$ vektort választottunk ki, a 2.-ban pedig az előző $J-1$ lépésben $2(J-1)$ vektort). A lehetséges 0-1 párok közül így legfeljebb $2B_1 + 2(J-1)$-ben van foglalt vektor. Azt kell belátnunk, hogy a foglalt 0-1 párok száma $\frac{1}{2}N$-nél kisebb. Ez pedig teljesül: $2B_1 + 2(J-1) \leq 2B_1 + 2(C-1) = 2(B_1 + C) - 2 \leq 2 \cdot \frac{1}{4}N - 2 < \frac{1}{2}N$.

3. A 3. lépésben megint azt kell belátnunk, hogy a J-edik befejező élnél ($1 \leq J \leq B_2$, legyen az él címkéje $\mathbf{d}$) mindig találni fogunk megfelelő 1-1 párt, amit az él csúcsaiba írhatunk. Van 2^{n-2} db $\mathbf{d}$ különbségű 1-1 pár $\mathbb{F}_2^n$-ben, és ezek közül legfeljebb annyi foglalt, ahány 1-gyel kezdődő vektort eddig összesen kiválasztottunk az algoritmus során. A 2. lépésben kiválasztottunk C db-ot, a 3.-ban pedig eddig $2(J-1)$ db-ot. Így elég belátni, hogy $C + 2(J-1) < 2^{n-2}$ (és ebből következik, hogy nem lehet foglalt mind a 2^{n-2} db 1-1 pár). Ez pedig teljesül, mert $C + 2(J-1) \leq C + 2(B_2 - 1) = C + 2B_2 - 2 \leq (\frac{1}{4}N + 1) - 2 < \frac{1}{4}N = 2^{n-2}$.

□

4.4. Állítás. *Tegyük fel, hogy van egy λ-algoritmusunk (ahol $\frac{1}{4} \leq \lambda < \frac{1}{2}$). Legyen $n \geq 3$ tetszőleges egész, $N = 2^n$ és $0 \leq B, C \leq \frac{1}{4}N$ olyan egész értékek, melyekre ha $\beta = B/N$ és $\gamma = C/N$, akkor $\beta \leq \min\left(\frac{1}{4} - \gamma, \frac{1}{2}\lambda\right) + \left(\frac{1}{8} - \frac{1}{2}\gamma\right)$. Ekkor B db 0-val kezdődő és C db 1-gyel kezdődő $\mathbb{F}_2^n$-beli nemnulla különbségre mindig működik a 4.2 algoritmus (B_1 és B_2 alkalmas választásával).*

Bizonyítás. Legyen $B_2 = \min(\lceil \frac{1}{8}N - \frac{1}{2}C \rceil, B)$ és $B_1 = B - B_2$. Ekkor a 4.3 állítás alkalmazásához a következő feltételeket kell leellenőriznünk:

1. $B_1 \geq 0$
2. $B_2 \geq 0$
3. $B_1 \leq \frac{1}{2}\lambda N$ és $B_1 + C \leq \frac{1}{4}N$
4. $C + 2B_2 \leq \frac{1}{4}N + 1$

Ellenőrizzük ezeket rendre:

1. B_2 definíciója alapján világos, hogy $B_2 \leq B$, és így $B_1 = B - B_2 \geq 0$.
2. Annak belátásához, hogy $B_2 \geq 0$, elég azt látnunk, hogy $\frac{1}{8}N - \frac{1}{2}C \geq 0$. Ez azzal ekvivalens, hogy $C \leq \frac{1}{4}N$, amit kikötöttünk feltételként.
3. Ha $B_2 = B$, akkor $B_1 = 0$, így a $B_1 \leq \frac{1}{2}\lambda N$ állítás triviális, továbbá a $C \leq \frac{1}{4}N$ feltétel miatt a $B_1 + C \leq \frac{1}{4}N$ is. Máskülönben $B_2 = \lceil \frac{1}{8}N - \frac{1}{2}C \rceil \geq \frac{1}{8}N - \frac{1}{2}C$. Mivel $\beta \leq \min\left(\frac{1}{4} - \gamma, \frac{1}{2}\lambda\right) + \left(\frac{1}{8} - \frac{1}{2}\gamma\right)$, ezért ($N$-nel beszorozva):

$$B \leq \min\left(\frac{1}{4}N - C, \frac{1}{2}\lambda N\right) + \frac{1}{8}N - \frac{1}{2}C$$

Tehát

$$B \leq \min\left(\frac{1}{4}N - C, \frac{1}{2}\lambda N\right) + B_2$$

vagyis $B_1 \leq \frac{1}{4}N - C$ és $B_1 \leq \frac{1}{2}\lambda N$.

4. Végezetül az utolsó pont teljesül, mert $B_2 \leq \lceil \frac{1}{8}N - \frac{1}{2}C \rceil < \frac{1}{8}N - \frac{1}{2}C + 1$, így $2B_2 + C < \frac{1}{4}N - C + 2 + C = \frac{1}{4}N + 2$, és mivel mindkét oldal egész, $2B_2 + C \leq \frac{1}{4}N + 1$.

□

4.5. Következmény. *Tegyük fel, hogy van egy λ-algoritmusunk (ahol $\frac{1}{4} \leq \lambda < \frac{1}{2}$). Legyenek $0 \leq \beta, \gamma \leq \frac{1}{4}$ olyan értékek, melyekre $\beta \leq \min\left(\frac{1}{4} - \gamma, \frac{1}{2}\lambda\right) + \left(\frac{1}{8} - \frac{1}{2}\gamma\right)$. Ekkor a főprobléma mindig megoldható, ha a 0-val kezdődő különbségek száma legfeljebb βN és az 1-gyel kezdődőeké legfeljebb γN.*

Bizonyítás. Először foglalkozzunk az $n = 2$ triviális esettel. Ekkor mivel $\beta, \gamma \leq \frac{1}{4}$, a 0-val kezdődő és az 1-gyel kezdődő élek száma is legfeljebb 1, és nem lehet mindkettő 1, mivel a feltételből könnyen látszik, hogy β és γ nem lehet egyszerre $\frac{1}{4}$. Így csak egyetlen élünk lehet, legyen ez $\mathbf{d_1}$. Ekkor $\mathbf{a_1} = \mathbf{d_1}$ és $\mathbf{b_1} = \mathbf{0}$ választással $\mathbf{a_1} - \mathbf{b_1} = \mathbf{d_1}$.

Most legyen $n \geq 3$. Legyen $B = \beta N$ és $C = \gamma N$, valamint jelöljük a megadott 0-val kezdődő különbségek számát B'-vel és az 1-gyel kezdődőekét C'-vel. Továbbá legyen $B' = \beta' N$ és $C' = \gamma' N$. Ekkor $B' \leq B$ és $C' \leq C$, és így $\beta' \leq \beta$ és $\gamma' \leq \gamma$.

Ekkor nyilván teljesül $0 \leq \beta' \leq \beta \leq \frac{1}{4}$ és $0 \leq \gamma' \leq \gamma \leq \frac{1}{4}$, tehát $0 \leq B', C' \leq \frac{1}{4}N$.

Továbbá $\beta' \leq \beta \leq \min\left(\frac{1}{4} - \gamma, \frac{1}{2}\lambda\right) + \left(\frac{1}{8} - \frac{1}{2}\gamma\right) \leq \min\left(\frac{1}{4} - \gamma', \frac{1}{2}\lambda\right) + \left(\frac{1}{8} - \frac{1}{2}\gamma'\right)$, ezért a 4.4 állítás miatt a B' db 0-val kezdődő és C' db 1-gyel kezdődő különbségre működik a 4.2 algoritmus. □

Az alábbiakban bevezetünk néhány jelölést, amivel az eddig elért eredményeinket tömören megfogalmazhatjuk.

4.6. Definíció. Jelölje $U(\mu)$ azt az állítást, hogy a főprobléma $M \leq \mu N$ él esetén megoldható (tetszőleges $n \geq 2$ és $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_M} \in \mathbb{F}_2^n$ nemnulla különbségek esetén).

4.7. Definíció. Jelölje $U_{az}(\mu, \alpha)$ azt az állítást, hogy a főprobléma megoldható tetszőleges $n \geq 2$ esetén abban az esetben, ha a különbségek száma legfeljebb μN, és van legalább αN olyan különbség, ami mind azonos.

4.8. Definíció. Jelölje $U_{01}(\beta, \gamma)$ azt az állítást, hogy a főprobléma megoldható tetszőleges $n \geq 2$ esetén abban az esetben, ha a 0-val kezdődő különbségek száma legfeljebb βN és az 1-gyel kezdődőeké legfeljebb γN.

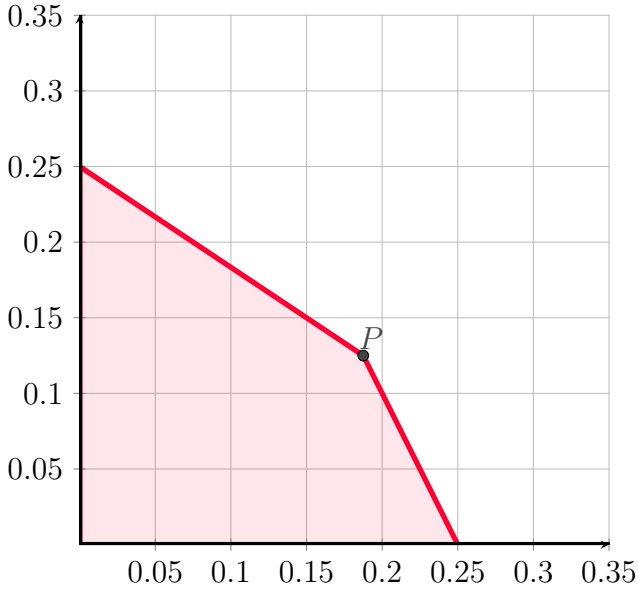
4.9. Megjegyzés. Ezen definíciók nyelvén a korábbi állításaink így szólnak:

- 3.5 tétel: $U\left(\frac{1}{4}\right)$
- 3.6 tétel: $\left(\frac{1}{4} < \mu < \frac{1}{2}\right)$ és $\left(\alpha \geq 2\mu - \frac{1}{2}\right) \implies U_{az}(\mu, \alpha)$
- 4.5 következmény: $\left(\frac{1}{4} \leq \lambda < \frac{1}{2}\right)$ és $(0 \leq \beta, \gamma \leq \frac{1}{4})$ és $U(\lambda)$ és $(\beta \leq \min(\frac{1}{4} - \gamma, \frac{1}{2}\lambda) + \left(\frac{1}{8} - \frac{1}{2}\gamma\right)) \implies U_{01}(\beta, \gamma)$.

5. Kezdetek arányának szabályozása lineáris transzformációval

Nézzük meg, mit mond a 4.5 következmény állítása $\lambda = \frac{1}{4}$ esetén: ha $0 \leq \beta, \gamma \leq \frac{1}{4}$ és $\beta \leq \min\left(\frac{1}{4} - \gamma, \frac{1}{8}\right) + \left(\frac{1}{8} - \frac{1}{2}\gamma\right)$, akkor $U_{01}(\beta, \gamma)$.

Ez akkor igazolja az $U_{01}(\beta, \gamma)$ állítást, ha a (β, γ) pont az alábbi ábrán a piros tartományba esik (ez az $x + \frac{3}{2}y = \frac{3}{8}$ és $x + \frac{1}{2}y = \frac{1}{4}$ egyenesek, valamint a két tengely által határolt zárt négyszög):



Ha az élek száma $M = \mu N$, ahol $\mu = \beta + \gamma$, akkor látható, hogy ha a 4.5 következmény segítségével szeretnénk belátni valamilyen adott $\mu > \frac{1}{4}$-re az állítást, akkor ez csak úgy tehető meg, ha a 0-val kezdődő élek $r = \frac{\beta}{\mu}$ részaránya egy $[r_{min}(\mu), r_{max}(\mu)]$ intervallumon belülre esik, ahol $0 < r_{min}(\mu)$ és $r_{max}(\mu) < 1$.

Az ábra P pontja a $\left(\frac{3}{16}, \frac{1}{8}\right)$ pont, amire $\mu = \frac{5}{16}$ és $r = \frac{3}{5}$. Így $\frac{1}{4} \leq \mu \leq \frac{5}{16}$ esetén az $[r_{min}(\mu), r_{max}(\mu)]$ intervallum mindig tartalmazza a $\frac{3}{5}$ pontot, és μ-t növelve egyre szűkebb. Mindkét végpont $\frac{3}{5}$-höz tart, ahogy $\mu \to \frac{5}{16}$. Ez azt jelenti, hogy ha ismert, hogy r beleesik egy $\frac{3}{5}$ körüli kicsi $I = [k, 1 - \ell]$ intervallumba, akkor minél szűkebb I, annál nagyobb μ értékekre látható be a főprobléma megoldhatósága.

Azonban ha a különbségek nagy része 0-val vagy nagy része 1-gyel kezdődik, akkor r nem fog ebbe az intervallumba beleesni, így egy ilyen megoldás nem működik. Ilyenkor a következő lemma fog segíteni:

5.1. Lemma. *Legyen $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ egy $\mathbb{F}_2$-vektortér-automorfizmus. Ekkor a $\mathbf{d_1}$, $\mathbf{d_2}$, …, $\mathbf{d_M} \in \mathbb{F}_2^n$ különbségekre pontosan akkor oldható meg a főprobléma, ha a $\phi(\mathbf{d_1})$, $\phi(\mathbf{d_2})$, …, $\phi(\mathbf{d_M})$ különbségekre megoldható.*

Bizonyítás. Tegyük fel, hogy a $\mathbf{d_1}$, …, $\mathbf{d_M}$ különbségekre az $\mathbf{a_1}$, …, $\mathbf{a_M}$, $\mathbf{b_1}$, …, $\mathbf{b_M}$ értékek megoldják a problémát. Ekkor minden i-re $\mathbf{d_i} = \mathbf{a_i} - \mathbf{b_i}$.

Ekkor az $\mathbf{a_i'} = \phi(\mathbf{a_i})$, $\mathbf{b_i'} = \phi(\mathbf{b_i})$ értékek megoldják a problémát a $\mathbf{d_i'} = \phi(\mathbf{d_i})$ különbségekre: az automorfizmus csupa különböző vektorokat csupa különbözőkbe visz, és minden i-re $\phi(\mathbf{d_i}) = \phi(\mathbf{a_i}) - \phi(\mathbf{b_i})$.

Ha ϕ automorfizmus, akkor ϕ^{-1} is az, így az odafelé irányt ϕ helyett ϕ^{-1}-re használva az állítás fordított iránya is megkapható. □

Így ha adottak a $\mathbf{d_1}, \ldots, \mathbf{d_M}$ különbségek, melyeknek a nagy része azonos számjeggyel kezdődik, de találunk egy olyan $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ automorfizmust, melyre $\phi(\mathbf{d_1})$, $\ldots$, $\phi(\mathbf{d_M})$ között a 0-val kezdődőek részaránya már beleesik $[r_{min}(\mu), r_{max}(\mu)]$-be, akkor az 5.1 lemma miatt dolgozhatunk az eredeti különbségek helyett a transzformáltakkal, melyekre a korábbiak alapján már meg tudjuk oldani a problémát.

Azonban ha a $\mathbf{d_i}$ értékek között sok azonos van, akkor azok bármilyen lineáris transzformációt követően azonosak maradnak, így ebben az esetben nem feltétlenül fogunk tudni olyan transzformációt találni, ami mindkét fajta kezdetű értékből létrehoz elég sokat. A fejezet további részében így azt fogjuk vizsgálni, hogy mely (k, ℓ, d) hármasokra teljesül az alábbi állítás:

5.2. Definíció. Legyen $0 \leq k, \ell, d \leq 1$ úgy, hogy $k+\ell \leq 1$. Ekkor jelölje $T(k, \ell, d)$ azt az állítást, hogy tetszőleges $n \geq 2$-re, $M \in \mathbb{N}^+$-ra és $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_M} \in \mathbb{F}_2^n$ nemnulla vektorokra teljesül, hogy vagy legalább dM azonos van a vektorok között, vagy létezik egy olyan $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ automorfizmus, melyekre a $\phi(\mathbf{d_1}), \ldots, \phi(\mathbf{d_M})$ vektorok között legalább kM 0-val és legalább ℓM 1-gyel kezdődik.

Ezen fejezet fő eredménye az alábbi tétel lesz:

5.3. Tétel. *Ha $0 < k \leq \frac{1}{3}$, akkor $T(k, k, 1-2k)$ teljesül.*

A bizonyításhoz szükségünk lesz az alábbi definíciókra és lemmára. Legyen $0 < k \leq \frac{1}{3}$ rögzített, és legyenek adottak a $\mathbf{d_1}, \ldots, \mathbf{d_M} \in \mathbb{F}_2^n$ nemnulla vektorok. A $\mathbf{d_i}$ vektor j-edik koordinátáját $\mathbf{d_i}(j)$-vel fogjuk jelölni ($1 \leq i \leq M$, $1 \leq j \leq n$, $\mathbf{d_i}(j) \in \{0, 1\}$).

5.4. Definíció. Ha $K \subseteq [n]$ egy nemüres halmaz, akkor legyen $A_K = \{\mathbf{x} \in \mathbb{F}_2^n : \sum_{i \in K} \mathbf{x}(i) = 0\}$. (Itt $\mathbf{x}(i)$ az $\mathbf{x}$ vektor i-edik koordinátáját jelöli.) Könnyen látható, hogy A_K egy $n-1$ dimenziós altere $\mathbb{F}_2^n$-nek.)

5.5. Definíció. Egy $K \subseteq [n]$ halmazt *szegénynek* nevezünk, ha a $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_M}$ vektorok közül kevesebb mint kM db esik bele az A_K altérbe, és *gazdagnak*, ha több mint $(1-k)M$ db. Egy $1 \leq j \leq n$ indexet *szegénynek*, illetve *gazdagnak* nevezünk, ha a $\{j\}$ halmaz szegény, illetve gazdag.

5.6. Lemma. *Legyen $n \in \mathbb{N}^+$ és $c \in \mathbb{R}^+$. Ha a $B_1, B_2, \ldots, B_n$ halmazokra teljesül, hogy minden $S \subseteq \{1, 2, \ldots, n\}$-re $|\triangle\{B_i : i \in S\}| < c$, akkor $\left|\bigcup_{i=1}^{n} B_i\right| < 2c$.*

Bizonyítás. Ha egy x elem a B_1, B_2, $\ldots$, B_n halmazok közül u darabban van benne, ahol $1 \leq u \leq n$, akkor azon $H \subseteq [n]$ részhalmazok száma, melyekre $\triangle\{B_i : i \in H\}$ tartalmazza x-et, $2^{u-1}2^{n-u} = 2^{n-1}$. (Mivel H-nak az x-et tartalmazó halmazok indexei közül páratlan sokat kell tartalmaznia, a többi index közül pedig tetszőleges számút.)

Számoljuk össze azon (H, x) párokat, ahol $H \subseteq [n]$ nemüres részhalmaz, és $x \in \triangle\{B_i : i \in H\}$. Az előző bekezdés alapján ezen párok száma $2^{n-1}\left|\bigcup_{i=1}^{n} B_i\right|$. Másrészt viszont minden nemüres $H \subseteq [n]$-re tudjuk, hogy a hozzá tartozó szimmetrikus differencia mérete kisebb c-nél, ezért a keresett párok száma összesen kisebb $c(2^n - 1)$-nél. Tehát

$$2^{n-1}\left|\bigcup_{i=1}^{n} B_i\right| < c(2^n-1),$$

$$\left|\bigcup_{i=1}^{n} B_i\right| < c\left(2-\frac{1}{2^{n-1}}\right) < 2c.$$

□

A 5.3 tétel bizonyítása. Tegyük fel, hogy van egy olyan $K \subseteq [n]$ nemüres halmaz, ami nem szegény és nem is gazdag. Ekkor a $\mathbf{d_1}$, $\mathbf{d_2}$, …, $\mathbf{d_M}$ vektorok közül az A_K-ba esők száma legalább kM és legfeljebb $(1-k)M$. Egy véges dimenziós vektortérnek bármely két azonos dimenziójú altere átvihető egymásba egy automorfizmussal. Azaz A_K átvihető valamilyen ϕ automorfizmussal $A_{\{1\}}$-be, mert mindkettő $n-1$ dimenziós altér $\mathbb{F}_2^n$-ben. Ekkor minden i-re $\mathbf{d_i} \in A_K$ pontosan akkor, ha $\phi(\mathbf{d_i}) \in A_{\{1\}}$, azaz $\phi(\mathbf{d_i})$ 0-val kezdődik. Azaz $\phi(\mathbf{d_1}), \ldots, \phi(\mathbf{d_M})$ közül legalább kM db 0-val kezdődik és legalább kM db 1-gyel.

Így már csak az az eset maradt, amikor minden $K \subseteq [n]$ nemüres halmaz szegény vagy gazdag. Speciálisan minden $1 \le j \le n$ index vagy szegény, vagy gazdag: legyen $\{s_1, s_2, \ldots, s_a\}$ a szegény, $\{g_1, g_2, \ldots, g_b\}$ pedig a gazdag indexek halmaza.

Minden $1 \le j \le a$-ra legyen $S_j = \{1 \le i \le M : \mathbf{d_i}(s_j) = 0\}$, és minden $1 \le j \le b$-re legyen $G_j = \{1 \le i \le M : \mathbf{d_i}(g_j) = 1\}$. Be fogjuk látni, hogy az így kapott $S_1, \ldots, S_a, G_1, \ldots, G_b$ halmazok uniója $2kM$-nél kevesebb elemet tartalmaz. Ehhez a 5.6 lemmát fogjuk használni, ennek használatához pedig az szükséges, hogy a halmazok közül akárhogyan is választunk ki néhányat, a kiválasztottak szimmetrikus differenciájának elemszáma kisebb kM-nél.

Ez utóbbi állítást a kiválasztott halmazok száma szerinti indukcióval látjuk be. Ha csak 0 vagy 1 halmazt választunk ki, akkor az állítás triviális, mert a gazdag, illetve szegény indexek definíciója alapján minden S_j és minden G_j elemszáma kisebb kM-nél. Most válasszuk ki WLOG az S_1, S_2, …, S_e, G_1, …, G_f halmazokat, ahol $0 \le e \le a$, $0 \le f \le b$ és $e+f \ge 2$. Ha az $e+f$ db halmaz közül egyet elhagyunk, akkor az indukciós feltevés miatt a megmaradó halmazok szimmetrikus differenciája kM-nél kevesebb elemet tartalmaz. Maga a kimaradó halmaz is kM-nél kevesebb elemet tartalmaz. Mivel tetszőleges A, B halmazokra $|A \triangle B| \le |A| + |B|$, ezt használva az $e+f$ db halmazunk szimmetrikus differenciájának elemszáma $2kM$-nél kisebb.

Másrészt pedig ha $K = \{s_1, \ldots, s_e, g_1, \ldots, g_f\}$, akkor $S_1 \triangle \cdots \triangle S_e \triangle G_1 \triangle \cdots \triangle G_f$ vagy megegyezik az $\{1 \le i \le M : \mathbf{d_i} \in A_K\}$ halmazzal, vagy pedig annak komplementerével. (Hogy a két lehetőség közül melyik áll fenn, az e paritásától függ.) Mivel a $K = \{s_1, \ldots, s_e, g_1, \ldots, g_f\}$ halmaz vagy szegény, vagy gazdag, ezért $|S_1 \triangle \cdots \triangle S_e \triangle G_1 \triangle \cdots \triangle G_f|$ vagy kM-nél kisebb, vagy $(1-k)M$-nél nagyobb. Azt már láttuk, hogy $2kM$-nél kisebb, tehát nem lehet $(1-k)M$-nél nagyobb (mert $k \le \frac{1}{3}$). Tehát kM-nél kisebb, azaz a kívánt állítást beláttuk.

Tehát a 5.6 lemma miatt $|S_1 \cup \cdots \cup S_a \cup G_1 \cup \cdots \cup G_b| < 2kM$. Tehát az unión kívül eső i indexekre $\mathbf{d_i}(s_j) = 1$ és $\mathbf{d_i}(g_j) = 0$ minden j-re, vagyis ezekre az i-kre a $\mathbf{d_i}$ vektorok mind megegyeznek. Vagyis a vektorok közül több mint $(1-2k)M$ mind azonos. □

6. A főprobléma megoldása $M \leq \frac{9}{32}N$ élre

Ebben a fejezetben összerakjuk az eddigi eredményeinket, hogy belássuk a főprobléma $M \leq \frac{9}{32}N$ él esetén.

6.1. Tétel. *Ha adottak a k, ℓ, d, α valós számok, melyekre teljesül az alábbi feltételek mindegyike:*

1. $0 \leq k, \ell, d \leq 1$,
2. $k + \ell \leq 1$,
3. $\frac{1}{4} \leq \alpha < \frac{1}{2}$,
4. $T(k, \ell, d)$,
5. *minden $0 \leq \mu \leq \alpha$-ra teljesül $U_{az}(\mu, d\mu)$,*
6. *minden $k \leq r \leq 1 - \ell$-re teljesül $U_{01}(r\alpha, (1-r)\alpha)$,*

akkor $U(\alpha)$ is teljesül.

Bizonyítás. Legyenek adottak a $\mathbf{d_1}, \ldots, \mathbf{d_M}$ nemnulla különbségek $\mathbb{F}_2^n$-ben, ahol $M \leq \alpha N$. Legyen $M = \mu N$ (ahol $0 \leq \mu \leq \alpha$). Ekkor $T(k, \ell, d)$ miatt vagy van legalább dM azonos a vektorok között, vagy van olyan α automorfizmusa $\mathbb{F}_2^n$-nek, melyre $\alpha(\mathbf{d_1})$, $\ldots$, $\alpha(\mathbf{d_M})$ közül legalább kM 0-val és legalább ℓM 1-gyel kezdődik.

Az előbbi esetben, mivel a μN vektor közül legalább $d\mu N$ megegyezik, ezért $U_{az}(\mu, d\mu)$ miatt megoldható a főprobléma.

Az utóbbi esetben legyen rM azon i indexek száma, melyekre $\mathbf{d_i}$ 0-val kezdődik. Ekkor $k \leq r \leq 1 - \ell$. A nullával kezdődő $\mathbf{d_i}$-k száma $rM = r\mu N \leq r\alpha N$ és az 1-gyel kezdődőeké $(1-r)M = (1-r)\mu N \leq (1-r)\alpha N$. Így $U_{01}(r\alpha, (1-r)\alpha)$ miatt megoldható a főprobléma az $\alpha(\mathbf{d_i})$ különbségekre, és így az 5.1 lemma miatt a $\mathbf{d_i}$ különbségekre is. □

6.2. Tétel. *A főprobléma megoldható $M \leq \frac{9}{32}N$ élre.*

Bizonyítás. Alkalmazzuk a 6.1 tételt a $k = \ell = d = \frac{1}{3}$ és $\alpha = \frac{9}{32}$ értékekre. Ekkor az 1-3. feltételek nyilván teljesülnek. A 4. feltétel ellenőrzéséhez használjuk az 5.3 tételt $k = \frac{1}{3}$-ra.

Tekintsük most az 5. feltételt. Azt kell belátnunk, hogy minden $0 \leq \mu \leq \alpha$-ra teljesül $U_{az}(\mu, d\mu)$. Ha $\mu \leq \frac{1}{4}$, akkor a 3.5 tétel miatt $U(\mu)$, így $U_{az}(\mu, d\mu)$ is teljesül. Ha pedig $\frac{1}{4} < \mu \leq \frac{9}{32}$, akkor a 3.6 tétel miatt teljesülni fog $U_{az}(\mu, d\mu)$, ha $d\mu \geq 2\mu - \frac{1}{2}$. És $\frac{1}{3}\mu \geq 2\mu - \frac{1}{2} \Leftrightarrow \frac{1}{2} \geq \frac{5}{3}\mu \Leftrightarrow \mu \leq \frac{3}{10}$, ami teljesül.

A 6. feltétel belátásához a 4.5 következményt használjuk $\lambda = \frac{1}{4}$, $\beta = r\alpha$ és $\gamma = (1-r)\alpha$ választásával, ahol $\frac{1}{3} \leq r \leq \frac{2}{3}$ rögzített szám. Ekkor $\frac{1}{4} \leq \lambda < \frac{1}{2}$ és $U(\lambda)$ nyilván teljesül, így elegendő az alábbiakat belátnunk minden $\frac{1}{3} \leq r \leq \frac{2}{3}$-ra:

(6a) $0 \leq \beta, \gamma \leq \frac{1}{4}$,
(6b) $\beta \leq \frac{1}{4} - \gamma + \left(\frac{1}{8} - \frac{1}{2}\gamma\right) = \frac{3}{8} - \frac{3}{2}\gamma$,
(6c) $\beta \leq \frac{1}{2}\lambda + \left(\frac{1}{8} - \frac{1}{2}\gamma\right) = \frac{1}{4} - \frac{1}{2}\gamma$.

Ezek bizonyítása:

(6a) $r\alpha, (1-r)\alpha \geq 0$ triviális. Mivel $r, 1-r \leq \frac{2}{3}$, ezért $r\alpha, (1-r)\alpha \leq \frac{2}{3} \cdot \frac{9}{32} = \frac{18}{96} \leq \frac{1}{4}$.

(6b) $r\alpha \leq \frac{3}{8} - \frac{3}{2}(1-r)\alpha \Leftrightarrow \frac{9}{32}r \leq \frac{3}{8} - \frac{3}{2}(1-r)\frac{9}{32} \Leftrightarrow \frac{9}{32}r \leq -\frac{3}{64} + \frac{27}{64}r \Leftrightarrow \frac{1}{3} \leq r$, ami teljesül.

(6c) $r\alpha \leq \frac{1}{4} - \frac{1}{2}(1-r)\alpha \Leftrightarrow \frac{9}{32}r \leq \frac{1}{4} - \frac{1}{2}(1-r)\frac{9}{32} \Leftrightarrow \frac{9}{64}r \leq \frac{7}{64} \Leftrightarrow r \leq \frac{7}{9}$, ami szintén igaz.

A 6.1 tétel állítása alapján tehát $U\left(\frac{9}{32}\right)$ teljesül. □

7. Csupa különböző különbségek

Abban a speciális esetben, amikor minden megadott $\mathbf{d_i}$ különbség csupa különböző, be fogjuk látni, hogy a főprobléma megoldható $M \leq \frac{1}{2}N - o(N)$ esetén. Sőt, ugyanez igaz lesz abban az esetben is, ha a különbségek ugyan nem mind különbözők, de az egyes különbségek előfordulásainak számára létezik egy $f(n)$ felső korlát, ahol $f(n) = o(2^n)$ egy rögzített függvény:

7.1. Tétel. *Legyen $\varepsilon : \mathbb{N} \to \mathbb{R}$ olyan függvény, melyre $\varepsilon(n) \geq 2^{-n}$ teljesül minden n-re és $\varepsilon(n) \to 0$, ahogy $n \to \infty$. Ekkor létezik olyan $C > 0$ konstans és $n_0 \in \mathbb{N}$, melyre $M \leq \lambda \cdot \frac{1}{2} \cdot 2^n$ és $n \geq n_0$ esetén az 1.2 probléma állítása igaz, ha a $\mathbf{d_i}$-k között minden érték legfeljebb $f(n)$-szer fordul elő, ahol $f(n) = \varepsilon(n) \cdot 2^n$ és $\lambda = 1 - C\varepsilon(n)^{\frac{1}{8}}$.*

A tétel belátásához a 4. fejezetben ismertetett *háromrészes mohó módszer* általánosítását használjuk, melyben az $\mathbb{F}_2^n$ vektortér elemeit és a megadott $\mathbf{d_1}, \ldots, \mathbf{d_M} \in \mathbb{F}_2^n$ különbségeket az első k koordinátájuk alapján 2^k kupacra osztjuk. (Itt $1 \leq k \leq n$ értéke megválasztható; a korábbi módszerben $k = 1$ volt.) A módszer működéséhez szükséges lesz, hogy a megadott különbségek közül mind a 2^k kupacba nagyjából azonos számú kerüljön. A feladat eltranszformálható $\mathbb{F}_2^n$-nek egy tetszőleges ϕ vektortér-automorfizmusával (lásd az 5.1 lemmát): a $\mathbf{d_i}$ különbségvektorokra az $\{\mathbf{a_i}, \mathbf{b_i}\}$ párok pontosan akkor adnak megoldást, ha a $\phi(\mathbf{d_i})$ különbségvektorokra a $\{\phi(\mathbf{a_i}), \phi(\mathbf{b_i})\}$ párok megoldást adnak. Egy olyan automorfizmust szeretnénk találni, melynek az alkalmazása után a kupacok a lehető legegyenlőbbek lesznek.

7.1. Megfelelő transzformáció létezése

Adott $\mathbf{c} = (c_1, \ldots, c_k) \in \mathbb{F}_2^k$-ra jelölje $d_\mathbf{c}(\phi)$ a ϕ transzformáció után a $\mathbf{c}$-vel kezdődő különbségek számát. Ekkor a $d_\mathbf{c}$ értékek átlaga mindenképpen $\overline{d} = \frac{1}{2^k}M$. A ϕ transzformáció hibája legyen $h(\phi) = \max\{|d_\mathbf{c} - \overline{d}| : \mathbf{c} \in \mathbb{F}_2^k\}$. Az alábbi állítás, mely felső becslést ad a legkisebb elérhető hibára, a Charbit et al. cikkében [3] található 1. tételnek az általánosítása. A bizonyítás is az ott szereplőhöz hasonló módszert követ. Véletlenszerű automorfizmust választunk, majd az egyes kupacok méreteinek kiszámítjuk az átlagát és szórását, és a Csebisev-egyenlőtlenség segítségével felső becslést adunk annak a valószínűségére, hogy a kupac mérete az átlagtól a kívánt hibánál jobban eltér.

Legyen $\mathbb{F}_2^n$ standard bázisa $\mathbf{e_1}, \ldots, \mathbf{e_n}$. A teljes automorfizmus helyett elég csak az $\mathbf{a_1} := \phi^{-1}(\mathbf{e_1}), \ldots, \mathbf{a_k} := \phi^{-1}(\mathbf{e_k})$ vektorokat megadni, ennek megfelelően a $d_\mathbf{c}(\phi)$ és $h(\phi)$ helyett a $d_\mathbf{c}(\mathbf{a_1}, \ldots, \mathbf{a_k})$ és $h(\mathbf{a_1}, \ldots, \mathbf{a_k})$ jelölést használjuk. Az $\mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n$ vektorok pontosan akkor határoznak meg ilyen módon egy ϕ automorfizmust, ha lineárisan függetlenek.

7.2. Állítás. *Legyenek $\mathbf{u_1}, \ldots, \mathbf{u_M} \in \mathbb{F}_2^n$ nemnulla vektorok, és $1 \leq k \leq n$ egész. Legyen $A = \{(i,j) : 1 \leq i, j \leq M, \mathbf{u_i} = \mathbf{u_j}\}$, és tegyük fel, hogy $M \geq \sqrt{A} \cdot 2^k$. Ekkor léteznek olyan $\mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n$ lineárisan független vektorok, melyekre $h(\mathbf{a_1}, \ldots, \mathbf{a_k}) < \sqrt{A}$.*

Bizonyítás. Vezessük be az alábbi jelölést: $\mathbf{u}, \mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n$ és $\mathbf{c} \in \mathbb{F}_2^k$ vektorok esetén legyen

$$f_{\mathbf{c}}(\mathbf{u}, \mathbf{a_1}, \ldots, \mathbf{a_k}) = \begin{cases} 1 & \text{ha } \langle \mathbf{a_i}, \mathbf{u} \rangle = c_i \text{ minden } i\text{-re,} \\ 0 & \text{különben.} \end{cases}$$

Ekkor

$$d_{\mathbf{c}}(\mathbf{a_1}, \ldots, \mathbf{a_k}) = \sum_{i=1}^{M} f_{\mathbf{c}}(\mathbf{u_i}, \mathbf{a_1}, \ldots, \mathbf{a_k})$$

Most rögzítsük $\mathbf{c} \in \mathbb{F}_2^k$ értékét, és tekintsük az alábbi összegeket:

$$S := \sum_{\mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n} d_{\mathbf{c}}(\mathbf{a_1}, \ldots, \mathbf{a_k})$$

$$S_2 := \sum_{\mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n} d_{\mathbf{c}}(\mathbf{a_1}, \ldots, \mathbf{a_k})^2$$

Először is

$$S = \sum_{\mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n} \sum_{i=1}^{M} f_{\mathbf{c}}(\mathbf{u_i}, \mathbf{a_1}, \ldots, \mathbf{a_k})$$

A szummázás sorrendjét megcseréljük:

$$S = \sum_{i=1}^{M} \sum_{\mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n} f_{\mathbf{c}}(\mathbf{u_i}, \mathbf{a_1}, \ldots, \mathbf{a_k})$$

Kihasználva, hogy minden $\mathbf{u_i}$ nemnulla, tehát az $\mathbb{F}_2^n$-ben minden $\mathbf{u_i}$-re 2^{n-1} db merőleges és 2^{n-1} db nem merőleges vektor létezik:

$$S = \sum_{i=1}^{M} (2^{n-1})^k = \frac{1}{2^k} M N^k$$

Most számítsuk ki S_2 értékét:

$$S_2 = \sum_{\mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n} \sum_{i,j=1}^{M} f_{\mathbf{c}}(\mathbf{u_i}, \mathbf{a_1}, \ldots, \mathbf{a_k}) f_{\mathbf{c}}(\mathbf{u_j}, \mathbf{a_1}, \ldots, \mathbf{a_k})$$

$$S_2 = \sum_{i,j=1}^{M} \sum_{\mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n} f_{\mathbf{c}}(\mathbf{u_i}, \mathbf{a_1}, \ldots, \mathbf{a_k}) f_{\mathbf{c}}(\mathbf{u_j}, \mathbf{a_1}, \ldots, \mathbf{a_k})$$

Ha $\mathbf{u_i} = \mathbf{u_j}$, akkor az ezen esethez tartozó tag értéke az előbbiek alapján $\sum_{\mathbf{a_1}, \ldots, \mathbf{a_k} \in \mathbb{F}_2^n} f_{\mathbf{c}}(\mathbf{u_i}, \mathbf{a_1}, \ldots, \mathbf{a_k}) = (2^{n-1})^k$.

Ha pedig $\mathbf{u_i} \neq \mathbf{u_j}$, akkor tetszőleges $b, b' \in \mathbb{F}_2$ esetén $\mathbb{F}_2^n$-ben $\frac{1}{4}N$ db olyan vektor van, melynek $\mathbf{u_i}$-vel vett skaláris szorzata b, és az $\mathbf{u_j}$-vel vett skaláris szorzata pedig b'. Ezért minden $\mathbf{a}_\ell$-re $\frac{1}{4}N$-féle választási lehetőségünk van, vagyis

$$\sum_{\mathbf{a_1},\ldots,\mathbf{a_k}\in\mathbb{F}_2^n} f_{\mathbf{c}}(\mathbf{u_i},\mathbf{a_1},\ldots,\mathbf{a_k})f_{\mathbf{c}}(\mathbf{u_j},\mathbf{a_1},\ldots,\mathbf{a_k}) = \left(\frac{1}{4}N\right)^k$$

és így

$$S_2 = A\left(\frac{1}{2}N\right)^k + (M^2-A)\left(\frac{1}{4}N\right)^k = \left(\frac{A}{2^k} + \frac{M^2-A}{4^k}\right)N^k$$

Ezek alapján ha az $\mathbf{a_1},\ldots,\mathbf{a_k} \in \mathbb{F}_2^n$ vektorokat véletlenszerűen választjuk (egyenletes eloszlással, egymástól függetlenül), és $\mathbf{c} \in \mathbb{F}_2^k$ rögzített, akkor a $d_{\mathbf{c}} := d_{\mathbf{c}}(\mathbf{a_1},\ldots,\mathbf{a_k})$ valószínűségi változóra az alábbiak teljesülnek:

$$\mathbb{E}(d_{\mathbf{c}}) = \frac{S}{N^k} = \frac{1}{2^k}M$$

$$\mathbb{E}(d_{\mathbf{c}}^2) = \frac{S_2}{N^k} = \frac{A}{2^k} + \frac{M^2-A}{4^k}$$

Így

$$\mathrm{Var}(d_{\mathbf{c}}) = \mathbb{E}(d_{\mathbf{c}}^2) - \mathbb{E}(d_{\mathbf{c}})^2 = \left(\frac{1}{2^k} - \frac{1}{4^k}\right)A$$

A Csebisev-egyenlőtlenség alapján

$$\mathbb{P}\left(\left|d_{\mathbf{c}} - \frac{1}{2^k}M\right| \geq \sqrt{A}\right) \leq \frac{\mathrm{Var}(d_{\mathbf{c}})}{A} < \frac{1}{2^k}$$

azaz annak az esélye, hogy létezik $\mathbf{c} \in \mathbb{F}_2^k$, melyre $\left|d_{\mathbf{c}} - \frac{1}{2^k}M\right| \geq \sqrt{A}$, kisebb 1-nél. Tehát létezik olyan $\mathbf{a_1},\ldots,\mathbf{a_k} \in \mathbb{F}_2^n$, melyre $h(\mathbf{a_1},\ldots,\mathbf{a_k}) < \sqrt{A}$.

Annak a belátása maradt, hogy ekkor $\mathbf{a_1},\ldots,\mathbf{a_k} \in \mathbb{F}_2^n$ lineárisan függetlenek. Ha lenne közöttük lineáris összefüggés, akkor megadhatóak lennének olyan $c_1,\ldots,c_k$ értékek, hogy semmilyen $\mathbf{u} \in \mathbb{F}_2^n$-re ne teljesüljön $\langle \mathbf{u}, \mathbf{a_i}\rangle = c_i$ minden $1 \leq i \leq k$-ra. Ekkor $d_{\mathbf{c}}(\mathbf{a_1},\ldots,\mathbf{a_k}) = 0$, tehát $h(\mathbf{a_1},\ldots,\mathbf{a_k}) < \sqrt{A}$ miatt $\frac{1}{2^k}M < \sqrt{A}$, azaz $M < \sqrt{A}\cdot 2^k$, ez pedig ellentmond az állítás feltételének. □

7.2. Az általánosított mohó módszer

Az alkalmazandó mohó módszer felépítésének szemléltetéséhez tekintsük az alábbi feladatot, mely önmagában is érdekes:

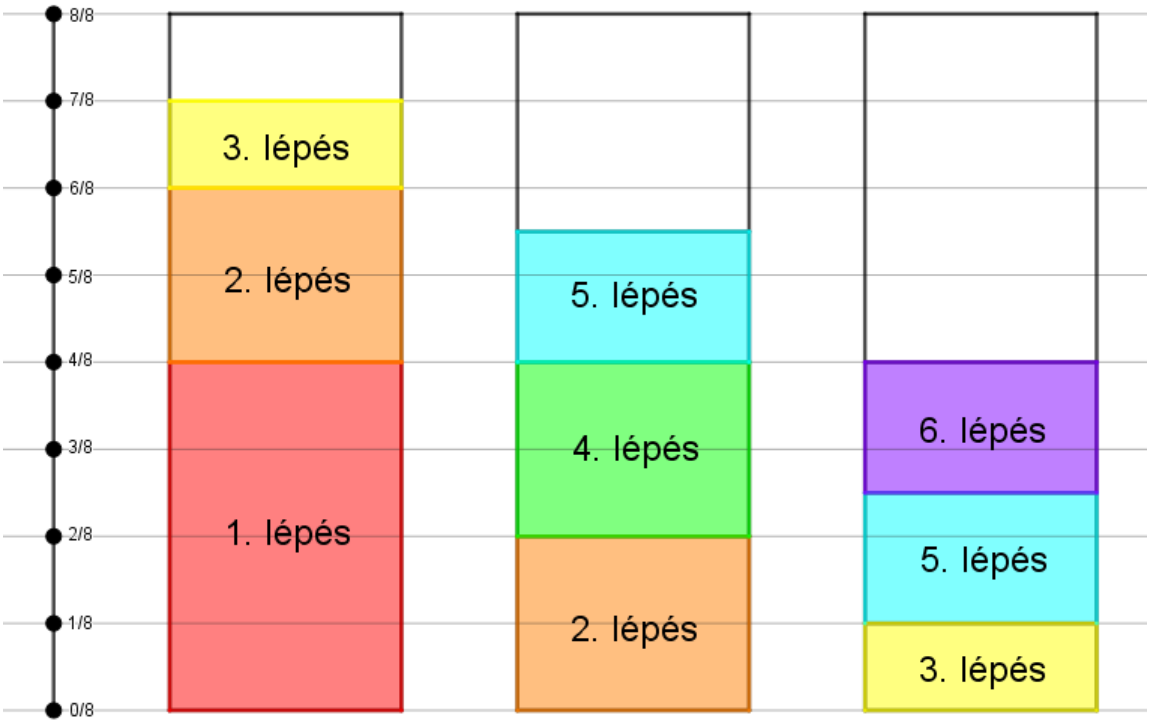
Feladat. Adott r db pohár, mindegyiknek az űrtartalma 1 egység. Kezdetben minden pohár üres. Az alábbi kétfajta lépés egyikét végezhetjük:

1. kiválasztunk egy olyan poharat, mely legfeljebb 1/2 részéig van tele, és töltünk bele valamilyen mennyiségű vizet úgy, hogy továbbra is legfeljebb 1/2 részéig legyen tele;

2. kiválasztunk két különböző poharat, melyben összesen legfeljebb 1 egység víz van. A két pohárba valamilyen mennyiségű vizet töltünk, mindkét pohárba ugyanannyit, mégpedig úgy, hogy ezután is legfeljebb 1 egység víz legyen összesen a két pohárban.

Végezzünk el néhány ilyen lépést; a poharakba összesen töltött víz mennyisége legyen v. Mekkora lehet legfeljebb $\frac{v}{r}$?

Az alábbi ábrán látható egy olyan 6 lépésből álló sorozat $r = 3$ esetén, mely $\frac{33}{48}$-os töltöttségi arányt ér el.



A 7.1 tétel alábbi bizonyításának alapja egy olyan töltögetési eljárás, mely $r \to \infty$ esetén 1-hez tartó töltöttségi arányt ér el. A poharak a 2^k db vektorkupacnak fognak megfelelni; a $\mathbf{c} \in \mathbb{F}_2^k$ címkéjű pohár tartozzon a $\mathbf{c}$-vel kezdődő $\mathbb{F}_2^n$-beli vektorok kupacához. Legyen most egyféle helyett 2^k féle folyadékunk, a folyadéktípusok szintén legyenek $\mathbb{F}_2^k$ elemeivel címkézve. Az 1. típusú lépéseknél mindig $\mathbf{0}$ címkéjű folyadékot töltsünk a pohárba, a 2. típusúaknál pedig ha az $\mathbf{a}$ és $\mathbf{b}$ címkéjű poharakba töltünk folyadékot, akkor $\mathbf{b} - \mathbf{a}$ címkéjűt töltsünk. A használt eljárás azzal az erősebb tulajdonsággal is rendelkezni fog, hogy minden típusú folyadékból pontosan ugyanannyit használunk. Egy pohár aktuális töltöttségi szintje annak fog megfelelni, hogy az adott kupacból hány vektort használtunk már fel, azaz rendeltünk eddig hozzá a megadott különbségvektorokhoz. A $\mathbf{c}$ címkéjű folyadék töltése az $\mathbf{a}$ és $\mathbf{b}$ poharakba pedig annak, hogy $\mathbf{c}$-vel kezdődő különbségvektorokhoz rendelünk hozzá egy-egy $\mathbf{a}$-val és $\mathbf{b}$-vel kezdődő vektort.

A 7.1 tétel bizonyítása. Az alábbi jelöléseket fogjuk használni: $\varepsilon_2(n) = \frac{1}{\sqrt{2}}\sqrt{\varepsilon(n)}$, valamint $B(n) = \frac{1}{\varepsilon_2(n)}$. (Ekkor $B(n) = \sqrt{2} \cdot \varepsilon(n)^{-\frac{1}{2}}$.) A bizonyításban szereplő logaritmusok 2-es alappal értendők.

Adva vannak a $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_M} \in \mathbb{F}_2^n$ nemnulla különbségvektoraink. Legyen $A = \{(i,j) : 1 \le i, j \le M,\ \mathbf{d_i} = \mathbf{d_j}\}$. Minden azonos értékű különbségekből álló csoport mérete $\le f(n)$, így $A \le Mf(n)$. A 7.2 állítást szeretnénk alkalmazni az M db vektorra; ehhez egy olyan k egészt kell kijelölnünk, melyre $M \ge \sqrt{A} \cdot 2^k$.

Legyen $k = \lceil \frac{1}{2} \log B(n) \rceil$.

Ekkor elég nagy n-re $2^k\sqrt{A} \leq 2^k\sqrt{Mf(n)} \leq M$, mert $2^k\sqrt{f(n)} = 2^k\sqrt{\varepsilon(n)}\cdot 2^{\frac{1}{2}n} \leq 2B(n)^{\frac{1}{2}}\varepsilon(n)^{\frac{1}{2}}\cdot 2^{\frac{1}{2}n} = 2^{\frac{5}{4}}\varepsilon(n)^{\frac{1}{4}}\cdot 2^{\frac{1}{2}n} \leq \frac{1}{2}\cdot 2^{\frac{1}{2}n} \leq \sqrt{M}$ (hiszen $M \geq \frac{1}{2}\cdot 2^{n-1}$ feltehető a 3.5 tétel miatt). És $k \leq n$, mert $\frac{1}{2}\log B(n) + 1 \leq n \Leftrightarrow 2\sqrt{B(n)} \leq 2^n$, ahol $\varepsilon(n) \geq 2^{-n} \geq 2^5\cdot 2^{-4n}$ miatt $\varepsilon(n)^{-\frac{1}{4}} \leq 2^{-\frac{5}{4}}\cdot 2^n$, tehát $2\sqrt{B(n)} = 2^{\frac{5}{4}}\varepsilon(n)^{-\frac{1}{4}} \leq 2^n$.

Tehát erre a k-ra a 7.2 állítás miatt létezik olyan $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ vektortér-automorfizmus, amelyre minden $\mathbf{s} \in \mathbb{F}_2^k$ esetén $\phi(\mathbf{d_1}), \ldots, \phi(\mathbf{d_M})$ közül legfeljebb $\frac{1}{2^k}M + \sqrt{A}$ db vektornak egyezik meg $\mathbf{s}$-sel az első k koordinátája.

Elegendő az automorfizmussal áttranszformált változatot megoldanunk, így mostantól feltesszük, hogy minden $\mathbf{s} \in \mathbb{F}_2^k$-ra a $\mathbf{d_i}$ vektorok közül legfeljebb $\frac{1}{2^k}M + \sqrt{A}$ db kezdődik $\mathbf{s}$-sel.

A korábban említett módon az $\mathbb{F}_2^n$ vektorteret osszuk a vektorok első k koordinátája alapján 2^k kupacba (így minden kupacba 2^{n-k} vektor kerül; minden kupac címkéje legyen a benne lévő vektorok első k koordinátája). Ha $\mathbf{r} \in \mathbb{F}_2^n$, és $\mathbf{r}$ első k koordinátája $\mathbf{s} \in \mathbb{F}_2^k$, és $\mathbf{s} \neq \mathbf{0}$, és $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^k$-ra teljesül $\mathbf{a} - \mathbf{b} = \mathbf{s}$, akkor az $\mathbf{a}$ és $\mathbf{b}$ indexű kupacok között van egy teljes párosítás, melyben minden él két végpontja közti különbség $\mathbf{r}$.

Ha pedig $\mathbf{r} \in \mathbb{F}_2^n$, és $\mathbf{r}$ első k koordinátája $\mathbf{0}$ (de $\mathbf{r} \neq \mathbf{0}$), akkor tetszőleges $\mathbf{a} \in \mathbb{F}_2^k$-ra az $\mathbf{a}$ indexű kupac feloszthatóa 2^{n-k-1} db párba úgy, hogy minden párban a két elem különbsége $\mathbf{r}$ legyen.

Ha $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^k$ és $c \in \mathbb{N}$, akkor nevezzük $(\mathbf{a}, \mathbf{b}, c)$ típusú lépésnek az alábbi folyamatot: a megadott $\mathbf{d_i}$ különbségeink közül c darab olyanhoz, amelyhez még nem rendeltünk $\mathbf{a_i}$ és $\mathbf{b_i}$ vektorokat, és amelynek kezdete $\mathbf{a} - \mathbf{b} \in \mathbb{F}_2^k$, sorban egyesével hozzárendelünk ilyen $\mathbf{a_i}$-t és $\mathbf{b_i}$-t tetszőleges módon úgy, hogy $\mathbf{a_i}$ kezdete $\mathbf{a}$, $\mathbf{b_i}$ kezdete pedig $\mathbf{b}$ legyen. Ez a mohó folyamat minden esetben elvégezhető, ha teljesül az alábbi feltétel:

- $\mathbf{a} \neq \mathbf{b}$ esetén $f_{\mathbf{a}} + f_{\mathbf{b}} + 2c \leq 2^{n-k}$,
- $\mathbf{a} = \mathbf{b}$ esetén pedig $f_{\mathbf{a}} + 2c \leq 2^{n-k-1}$,

ahol az $(\mathbf{a}, \mathbf{b}, c)$ típusú lépés megkezdése előtt már felhasznált $\mathbf{a}$ kezdetű vektorok számát $f_{\mathbf{a}}$, a $\mathbf{b}$ kezdetűekét $f_{\mathbf{b}}$ jelöli. (Ez a fenti párosítások használatával látható mind $\mathbf{a} = \mathbf{b}$, mind pedig $\mathbf{a} \neq \mathbf{b}$ esetén.)

Vegyük észre, hogy ez a két feltétel megfelel a töltögetős feladat két lehetséges lépésének feltételeinek.

Az $\mathbb{F}_2^k$ vektorteret azonosítsuk a 2^k elemű testtel, és ilyen módon definiáljuk az elemein a szorzást. Legyen g generátora a 2^k elemű test multiplikatív csoportjának. Ekkor $\mathbb{F}_2^k = \{1, g, g^2, \ldots, g^{2^k-2}, 0\}$. Legyen $1 \leq d \leq 2^k - 2$ egy konstans, melynek értékét később rögzítjük le.

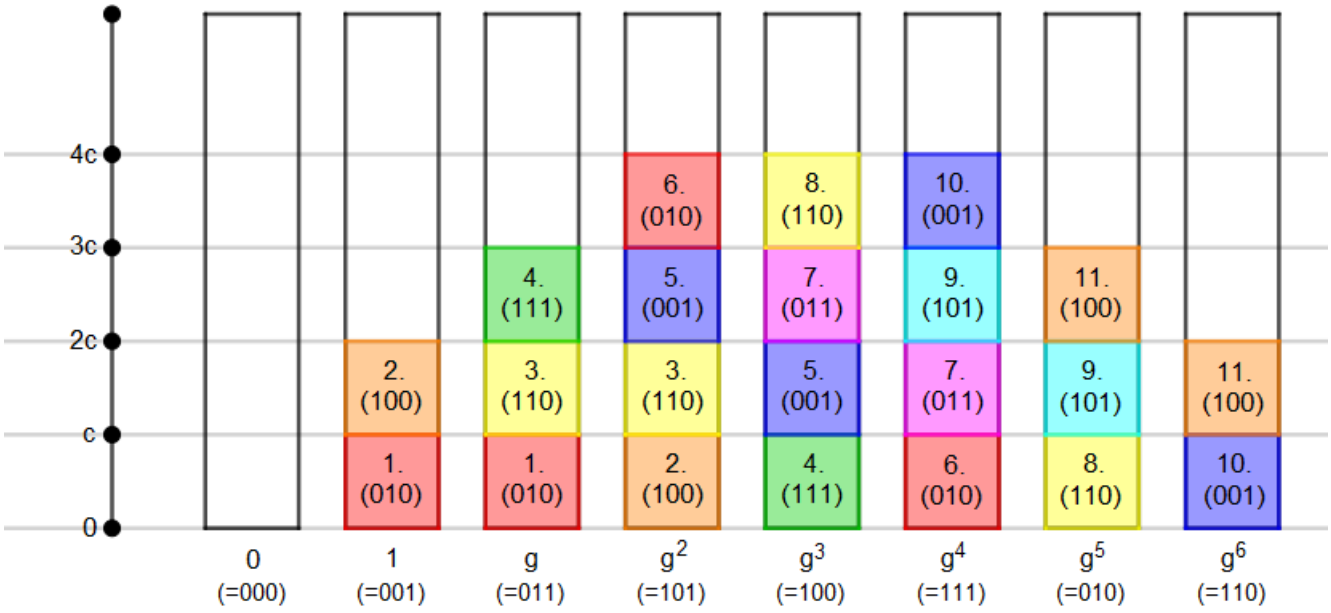
Tegyük meg az alábbi lépéseket, felsorolásuk sorrendjében, ahol c szintén később kiválasztandó konstans:

- $(g^0, g^1, c), (g^0, g^2, c), \ldots, (g^0, g^d, c)$,
- $(g^1, g^2, c), (g^1, g^3, c), \ldots, (g^1, g^{d+1}, c)$,
- $(g^2, g^3, c), (g^2, g^4, c), \ldots, (g^2, g^{d+2}, c)$,

- $\dots$
- $(g^{2^k-d-2}, g^{2^k-d-1}, c), (g^{2^k-d-2}, g^{2^k-d}, c), \dots, (g^{2^k-d-2}, g^{2^k-2}, c),$
- $(g^{2^k-d-1}, g^{2^k-d}, c), (g^{2^k-d-1}, g^{2^k-d+1}, c), \dots (g^{2^k-d-1}, g^{2^k-2}, c),$
- $\dots$
- $(g^{2^k-3}, g^{2^k-2}, c).$

(Ebben a felsorolásban ha valamelyik lépésnél az adott kezdetű különbségekből már csak c-nél kevesebb maradt, akkor csak a megmaradó különbségekhez keressünk vektorpárt.)

Például $k = 3$ és $d = 2$ esetén az alábbi pohártöltögetési ábra szemlélteti az elvégzett lépéseket, ahol az $\mathbb{F}_8 = \frac{\mathbb{F}_2[X]}{(X^3+X+1)}$ megfeleltetést használjuk a $g = X + 1$ generátorelemet választva, és az elemek koordinátázása az $(X^2, X, 1)$ bázis szerint történik. A sorszámok azt jelzik, hogy az adott adag folyadék hányadik lépésben került a pohárba, az alatta zárójelben lévő vektor pedig a folyadék címkéjét jelöli. A különböző színek szintén a poharakba töltött folyadék címkéjét (típusát) jelölik.



Minden $\mathbf{s} \in \mathbb{F}_2^k$-ra az $\mathbf{s}$-sel kezdődő különbségeket dc-szer szeretnénk az eljárás során összesen felhasználni. Ha $d \ll 2^k$, akkor ez már teljesül is, kivéve néhány kimaradó különbséget: mivel minden $1 \leq i \leq d$-re $g^i - g^0$, $g^{i+1} - g^1$, $g^{i+2} - g^2$, $\dots$, $g^{2^k-2} - g^{2^k-i-2}$ csupa különböző elemei $\mathbb{F}_2^k$-nak, ezért egy adott i-re $2^k - i - 1$ különféle különbségkezdetet használunk fel (mindegyiket c-szer), így lesz i-szer c db kimaradó különbség. Összesen ha minden $1 \leq i \leq d$-re tekintjük a dolgot, akkor $\frac{d(d+1)}{2}$ db c elemből álló kimaradó azonos kezdetű különbségcsoport van (melyeket még pluszban fel kell használnunk ahhoz, hogy minden nemnulla különbségkezdetet pontosan dc-szer használjunk).

Továbbá $\mathbf{0}$-val kezdődő különbséget sosem használtunk az eljárás során, így abból dc különbség kimaradt.

A most kimaradónak tekintett különbségeket használjuk fel a fenti lépések előtt az alábbi módon:

- A **0**-val kezdődő különbségeket mohó módon használjuk el úgy, hogy a lehető legegyenlőbben osszuk szét őket a 2^k db kupac között. Ekkor minden kupacban legfeljebb $\left\lceil \frac{dc}{2^k} \right\rceil < \frac{dc}{2^k} + 1$ db különbséget használunk, melyek kupaconként legfeljebb $\frac{dc}{2^{k-1}} + 2$ vektort fognak érinteni.

- A többi $\frac{d(d+1)}{2}$ db c elemből álló különbségcsoportot (minden csoport elemei ugyanazzal a vektorral kezdődnek) csoportonként használjuk fel mohó módon úgy, hogy minden csoport elemeit szétosztjuk a 2^{k-1} db lehetséges vektorkezdetpár között a lehető legegyenlőbben. Minden csoportnál így legfeljebb $\frac{c}{2^{k-1}} + 1$ db vektort használunk fel kupaconként, tehát az összes csoportot tekintve legfeljebb $\frac{d(d+1)}{2}\left(\frac{c}{2^{k-1}} + 1\right)$ darabot.

A fenti plusz párosítások tehát összesen legfeljebb $H := \frac{dc}{2^{k-1}} + 2 + \frac{d(d+1)}{2}\left(\frac{c}{2^{k-1}} + 1\right)$ vektort használnak el minden kupacból. Nézzük most meg, hogy mi szükséges ahhoz, hogy a most leírt előkészítő lépések, és a fenti általános lépések is működjenek.

Az előkészítő mohó lépések működéséhez elégséges, ha minden vektorkupacnak legfeljebb a felét használjuk el ezek alatt, tehát ha $H \leq 2^{n-k-1}$.

Egy általános lépésnél pedig – mint láttuk – ha az éppen **a** és **b** kezdetű kupacok között történik, elégséges a lépés működéséhez, ha $f_{\mathbf{a}} + f_{\mathbf{b}} + 2c \leq 2^{n-k}$.

Könnyen látható, hogy az eljárásunk során minden lépésben teljesül, hogy $f_{\mathbf{a}} + f_{\mathbf{b}} + 2c \leq 2H + (2d+1)c$.

Ezek alapján tehát elégséges feltétel az egész eljárás működésére, hogy $2H + (2d+1)c \leq 2^{n-k}$ teljesüljön.

Válasszuk meg a c és d értékeket a következőképpen:

$$c = \left\lceil \frac{1}{2}\lambda \cdot 2^{n-\frac{3}{2}k} + \varepsilon_2(n) \cdot 2^{n-\frac{1}{2}k} \right\rceil$$

$$d = \left\lceil 2^{\frac{1}{2}k} \right\rceil$$

Lássuk be, hogy az említett elégséges feltétel valóban teljesül (megfelelő $C > 0$ és elég nagy n esetén).

Láthatjuk, hogy $2^{\frac{1}{4}}\varepsilon(n)^{-\frac{1}{4}} = B(n)^{\frac{1}{2}} = 2^{\frac{1}{2}\log B(n)} \leq 2^k \leq 2^{\frac{1}{2}\log B(n)+1} = 2B(n)^{\frac{1}{2}} = 2^{\frac{5}{4}}\varepsilon(n)^{-\frac{1}{4}}$, tehát $2^k = \Theta(\varepsilon(n)^{-\frac{1}{4}})$.

Valamint $\varepsilon_2(n) \cdot 2^{n-\frac{1}{2}k} \leq \frac{1}{\sqrt{2}}\varepsilon(n)^{\frac{1}{2}} \cdot 2^n \cdot B(n)^{-\frac{1}{4}} = 2^{-\frac{5}{8}} \cdot 2^n\varepsilon(n)^{\frac{5}{8}}$.

Így tehát d-re és c-re az alábbi felső becslések adhatók (elég nagy n-re):

$$d \leq 2 \cdot 2^{\frac{1}{2}k} \leq 2^{\frac{13}{8}} \cdot \varepsilon(n)^{-\frac{1}{8}}$$

$$c \leq \frac{1}{2} \cdot 2^{n-\frac{3}{2}k} + \varepsilon_2(n) \cdot 2^{n-\frac{1}{2}k} + 1 = O(2^n\varepsilon(n)^{\frac{3}{8}}) + O(2^n\varepsilon(n)^{\frac{5}{8}}) + 1$$

Így

$$dc = O(2^n\varepsilon(n)^{\frac{1}{4}}) + O(\varepsilon(n)^{-\frac{1}{8}}) \tag{1}$$

Illetve pontosabb becslés alapján

$$dc \leq (2^{\frac{1}{2}k}+1)\left(\frac{1}{2}\lambda\cdot 2^{n-\frac{3}{2}k}+\varepsilon_2(n)\cdot 2^{n-\frac{1}{2}k}+1\right)=$$

$$=\frac{1}{2}\lambda\cdot 2^{n-k}+\varepsilon_2(n)\cdot 2^n+2^{\frac{1}{2}k}+\frac{1}{2}\lambda\cdot 2^{n-\frac{3}{2}k}+\varepsilon_2(n)\cdot 2^{n-\frac{1}{2}k}+1$$

$$2dc \leq \lambda\cdot 2^{n-k}+2\varepsilon_2(n)\cdot 2^n+2^{\frac{1}{2}k+1}+\lambda\cdot 2^{n-\frac{3}{2}k}+2\varepsilon_2(n)\cdot 2^{n-\frac{1}{2}k}+2$$

Így $2H+(2d+1)c \leq \lambda\cdot 2^{n-k}+2\varepsilon_2(n)\cdot 2^n+2^{\frac{1}{2}k+1}+\lambda\cdot 2^{n-\frac{3}{2}k}+2\varepsilon_2(n)\cdot 2^{n-\frac{1}{2}k}+2+c+\frac{dc}{2^{k-2}}+4+d(d+1)\left(\frac{c}{2^{k-1}}+1\right)$.

Vagyis elég belátni, hogy

$$2\varepsilon_2(n)\cdot 2^n+2^{\frac{1}{2}k+1}+\lambda\cdot 2^{n-\frac{3}{2}k}+2\varepsilon_2(n)\cdot 2^{n-\frac{1}{2}k}+6+c+\frac{dc}{2^{k-2}}+$$

$$+d(d+1)\left(\frac{c}{2^{k-1}}+1\right)\leq C\varepsilon(n)^{\frac{1}{8}}\cdot 2^{n-k} \qquad (2)$$

A (2) egyenlőtlenség bal oldalán a $2^k=\Theta(\varepsilon(n)^{-\frac{1}{4}})$ és $\varepsilon(n)\geq 2^{-n}$ összefüggések használatával a tagokat felülről becsülve azt kapjuk, hogy minden tagnak a nagyságrendje $O(\varepsilon(n)^{\frac{1}{8}}\cdot 2^{n-k})$.

Az egyenlőtlenség így igaz, tehát a $2H+(2d+1)c\leq 2^{n-k}$ feltétel valóban teljesül.

A módszerünk tehát képes minden olyan felállás megoldására, ahol a $\mathbf{d_i}$ különbségek között mind a 2^k db kezdet (emlékeztetőül: egy vektor kezdete az első k koordinátát jelenti) legfeljebb dc-szer fordul elő. Nekünk arra kell felkészülnünk, hogy minden kezdetből akár $\frac{1}{2^k}M+\sqrt{A}$ db is lehet, tehát a módszer akkor működik, ha

$$\frac{1}{2^k}M+\sqrt{A}\leq dc \qquad (*)$$

Ekkor belátjuk, hogy $(*)$ valóban teljesülni fog elég nagy n esetén:

$$\frac{1}{2^k}M+\sqrt{A}\leq \frac{1}{2^k}M+\sqrt{Mf(n)}\leq \frac{1}{2^k}\cdot\lambda\cdot\frac{1}{2}\cdot 2^n+\sqrt{\lambda}\cdot\frac{1}{\sqrt{2}}\cdot 2^{\frac{1}{2}n}\cdot\sqrt{\varepsilon(n)}\cdot 2^{\frac{1}{2}n}=$$

$$=\frac{1}{2}\lambda\cdot 2^{n-k}+\sqrt{\lambda}\cdot\varepsilon_2(n)\cdot 2^n\leq\left(\frac{1}{2}\lambda\cdot 2^{n-\frac{3}{2}k}+\varepsilon_2(n)\cdot 2^{n-\frac{1}{2}k}\right)\left(2^{\frac{1}{2}k}\right)\leq dc$$

ahol használtuk, hogy $\lambda\leq 1$. □

8. Teljes párosítás kevés különbségosztály esetén

Most a fősejtést fogjuk megoldani egy speciális esetben. Legyenek adottak a $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_m}$ nemnulla különbségvektorok úgy, hogy $\sum_{i=1}^{m} \mathbf{d_i} = 0$, ahol $m = \frac{1}{2}N$. Nevezzük egy *különbségosztálynak* egy fix $\mathbf{d}$-re a $\mathbf{d}$ értékű különbségvektorok összességét. Egy adott $\{\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_m}\}$ konfigurációra a nemüres különbségosztályok számát jelöljük t-vel. Adott n esetén minél nagyobb $T(n)$-et szeretnénk megadni, melyre $t \leq T(n)$ esetén garantálni tudjuk egy megfelelő teljes párosítás létezését $\mathbb{F}_2^n$-ben.

A $t = 1$ esetben a feladat triviális, hiszen ekkor valamely $\mathbf{d} \neq \mathbf{0}$-ra 2^{n-1} db $\mathbf{d}$ különbségű párra kell felosztanunk a vektorteret; ehhez vegyük az $\mathbb{F}_2^n$ vektortér $\langle \mathbf{d} \rangle$ szerinti mellékosztályait.

Ha $t = 2$, akkor a 2.5 tétel segítségével könnyen megoldható a feladat. Ekkor ugyanis a $\sum \mathbf{d_i} = 0$ feltétel miatt mindkét különbségosztály mérete páros, és legalább az egyik osztály tartalmazza a különbségek felét. Így tehát fennáll az a struktúra, hogy a különbségek fele mind azonos, a többi különbség pedig azonos értékű párokba sorolható.

8.1. Tétel. *Az 1.1 sejtés igaz abban az esetben, ha a különbségosztályok száma* $t \leq n - 2\log n - 1$.

8.2. Definíció. Jelölje P_n az $[n]$ hatványhalmazát, mint tartalmazás szerint részbenrendezett halmazt.

8.3. Lemma. *Legyen* $n \geq 4$. *A* P_n *posetnek legyen* H *egy legfeljebb* $n+1$ *elemű részhalmaza, melyre* $\emptyset \notin H$ *és* $[n] \notin H$. *Továbbá tegyük fel, hogy* H *nem tartalmazza az összes egyelemű halmazt, és nem tartalmazza az összes* $n-1$ *elemű halmazt sem. Ekkor* $P_n \setminus H$ *tartalmaz* $n+1$ *elemű láncot.*

Bizonyítás. P_n-ben nevezzünk *szimmetrikus láncnak* egy olyan $X_k \subseteq X_{k+1} \subseteq \cdots \subseteq X_{n-k}$ sorozatot, melyre $|X_i| = i$ minden $k \leq i \leq n-k$-ra. (Itt $0 \leq k \leq \frac{n}{2}$.) Felhasználjuk azt a tényt, hogy P_n felbontható szimmetrikus láncok diszjunkt uniójára. Ennek bizonyítása megtalálható például a [9] jegyzetben (Proposition 2).

Ebből a tényből speciálisan az is következik, hogy P_n-ben találhatunk olyan, páronként diszjunkt C_1, C_2, …, $C_{\binom{n}{2}}$ szimmetrikus láncokat, melyek egy 2 elemű halmaztól egy $n-2$ eleműig tartanak. Egy ilyen, $\{a,b\}$-től $[n] \setminus \{c,d\}$-ig tartó lánc pontosan akkor egészíthető ki $n+1$ elemű lánccá $P_n \setminus H$-ban, ha maga a lánc nem tartalmaz H-beli elemet, továbbá ha $\{a\}$ és $\{b\}$ közül legfeljebb az egyik, továbbá $[n] \setminus \{c\}$ és $[n] \setminus \{d\}$ közül is legfeljebb az egyik van benne H-ban.

Lássuk be, hogy a C_i-k között mindig lesz olyan, ami kiegészíthető $n+1$ elemű lánccá $P_n \setminus H$-ban. Adjunk felső becslést a "rossz" C_i-k számára, azaz azokéra, melyekre ez nem tehető meg.

Legyen a H-beli egyelemű halmazok száma k, az $n-1$ eleműek száma ℓ, és H további elemeinek száma t. Ekkor $k+\ell+t \leq n+1$, és a feltevéseink miatt $k, \ell \leq n-1$. Ekkor legfeljebb $\binom{k}{2}$ db C_i lesz, melynek a kételemű végpontjából nem juthatunk el $\emptyset$-ig, illetve $\binom{\ell}{2}$ db olyan, melynek az $n-2$ elemű végpontjából nem juthatunk el $[n]$-ig. Valamint a t db további H-beli pont legfeljebb t db C_i-t fog le. A "rossz" láncok említett három kategóriája között lehetnek átfedések, de számuk (melyet jelöljünk R-rel) így legfeljebb $\binom{k}{2} + \binom{\ell}{2} + t$. Belátjuk, hogy ez $\binom{n}{2}$-nél kisebb.

$$R \le \binom{k}{2} + \binom{\ell}{2} + t \le \binom{k}{2} + \binom{\ell}{2} + n + 1 - k - \ell = \frac{k^2}{2} + \frac{\ell^2}{2} - \frac{3}{2}k - \frac{3}{2}\ell + n + 1$$

Azt fogjuk belátni, hogy

$$\frac{k^2}{2} + \frac{\ell^2}{2} - \frac{3}{2}k - \frac{3}{2}\ell + n + 1 < \binom{n}{2} = \frac{n^2}{2} - \frac{n}{2}$$

azaz

$$k^2 + \ell^2 - 3k - 3\ell + 2n + 2 < n^2 - n, \quad \text{vagyis}$$

$$\left(k - \frac{3}{2}\right)^2 + \left(\ell - \frac{3}{2}\right)^2 < n^2 - 3n + \frac{5}{2} \qquad (*)$$

Öt esetet különböztetünk meg:

1. eset: $\ell = 0$. Ekkor az kell, hogy

$$\left(k - \frac{3}{2}\right)^2 + \frac{9}{4} < n^2 - 3n + \frac{5}{2}$$

Tudjuk, hogy $0 \le k \le n-1$, és mivel $n - 1 \ge 3$, ezért teljesülni fog $\left(k - \frac{3}{2}\right)^2 \le \left(n - 1 - \frac{3}{2}\right)^2$. Így

$$\left(k - \frac{3}{2}\right)^2 + \frac{9}{4} \le \left(n - 1 - \frac{3}{2}\right)^2 + \frac{9}{4} = \left(n - \frac{5}{2}\right)^2 + \frac{9}{4} = n^2 - 5n + 9$$

Itt $n^2 - 5n + 9 < n^2 - 3n + \frac{5}{2} \Leftrightarrow n > \frac{13}{4}$, ami teljesül (hiszen $n \ge 4$).

2. eset: $\ell = 1$. Ekkor az kell, hogy

$$\left(k - \frac{3}{2}\right)^2 + \frac{1}{4} < n^2 - 3n + \frac{5}{2}$$

Ez az előző esetből triviálisan következik, hiszen az egyenlőtlenség bal oldala csökkent.

3. eset: $k = 0$. Ez k és ℓ szimmetriája miatt kijön az 1. esetből.

4. eset: $k = 1$. Ez is kijön a 2. esetből.

5. eset: $2 \le k, \ell \le n - 1$.

Ekkor $k + \ell \le n + 1$ (és $\ell > 0$ miatt $\left|\ell - \frac{3}{2}\right| \le \left|n + 1 - k - \frac{3}{2}\right|$), így $\left(\ell - \frac{3}{2}\right)^2 \le \left(n - k - \frac{1}{2}\right)^2$. Tehát

$$\left(k - \frac{3}{2}\right)^2 + \left(\ell - \frac{3}{2}\right)^2 \le \left(k - \frac{3}{2}\right)^2 + \left(n - k - \frac{1}{2}\right)^2 = 2k^2 - (2n+2)k + \left(n^2 - n + \frac{5}{2}\right)$$

Itt $k^2 - (n+1)k = \left(k - \frac{n+1}{2}\right)^2 - \frac{(n+1)^2}{4}$, ahol $2 \le k \le n-1$ miatt $\left|k - \frac{n+1}{2}\right| \le \frac{n-3}{2}$, tehát $k^2 - (n+1)k \le \frac{(n-3)^2}{4} - \frac{(n+1)^2}{4} = -2n + 2$. Vagyis

$$\left(k-\frac{3}{2}\right)^2+\left(\ell-\frac{3}{2}\right)^2 \le 2(-2n+2)+n^2-n+\frac{5}{2}=n^2-5n+\frac{13}{2}$$

és itt $n^2-5n+\frac{13}{2} < n^2-3n+\frac{5}{2} \Leftrightarrow 4<2n$, ami $n\ge 4$ miatt teljesül.
A "rossz" láncok száma így valóban kisebb $\binom{n}{2}$-nél, így létezik jó lánc. □

A 8.1 tétel bizonyítása. Legyenek a megadott különbségvektorok: n_1 darab $\mathbf{u_1}$, n_2 darab $\mathbf{u_2}$, …, n_t darab $\mathbf{u_t}$, ahol $n_1 \ge n_2 \ge \cdots \ge n_t$. Itt $\sum_{i=1}^{t} n_i = m$. Ekkor $n_1 \ge \frac{m}{t}$.

A $V=\mathbb{F}_2^n$-ben, mint $\mathbb{F}_2$-vektortérben legyen $U=\langle \mathbf{u_1},\dots,\mathbf{u_t}\rangle$, ekkor $\dim U = k \le t$. (Feltehető $k\ge 2$, különben $t=1$, és ezt az esetet már láttuk.) Nevezzük V-nek az U szerinti mellékosztályait *rétegeknek*. Ekkor a kész megoldásban minden vektorpárnak egy rétegen belül kell lennie. Az egyes rétegeken belül a párosításokat külön-külön fogjuk elkészíteni, és az elkészülő rétegeket később már nem módosítjuk. Összesen 2^{n-k} réteg van.

A módszernek három fázisa lesz.

1. fázis: Néhány (t-nél kevesebb) réteg elkészítésével elérjük, hogy minden különbségosztályból páros sok vektor maradjon meg.

2. fázis: Néhány (t-nél kevesebb) réteg elkészítésével elérjük, hogy minden különbségosztályban a megmaradó vektorok száma osztható legyen 2^{k-1}-gyel.

3. fázis: Az összes megmaradt különbségből homogén (azaz csak egy osztálybeli különbségeket használó) rétegeket készítünk.

Az első fázis. Legyen $H=\{\mathbf{u_i} : 2\le i\le t, n_i \equiv 1 \pmod 2\}$, továbbá használjuk az $\mathbf{u}=\mathbf{u_1}$ jelölést.

H-nak egy S részhalmazát nevezzük *körnek*, ha elemei mod $\mathbf{u}$ lineárisan összefüggőek, és S-nek semmilyen valódi részhalmaza nem rendelkezik ezzel a tulajdonsággal. (Tehát S kör, ha elemeinek összege $\mathbf{0}$ vagy $\mathbf{u}$, és ez S-nek semmilyen valódi részhalmazára nem teljesül.)

Egy S kört nevezzünk *jó paritásúnak*, ha S elemeinek összege $|S|\mathbf{u}$. Ha egy S körre ez nem teljesül (tehát ha az elemeinek összege $(|S|+1)\mathbf{u}$), akkor S-et *rossz paritásúnak* nevezzük.

Mivel $\sum n_i\mathbf{u_i}=\mathbf{0}$, ezért a H-beli elemek összege megegyezik $n_1\mathbf{u_1}$-gyel, tehát $\mathbf{0}$ mod $\mathbf{u}$. Az alábbi lépést fogjuk ismételni: ameddig H-ban még van elem, kiválasztunk belőle néhány (legalább három) vektort, és egy réteget elkészítünk ezen vektorok egy-egy példányát, illetve $\mathbf{u}$-ból kellő számú példányt használva. Az elhasznált H-beli vektorokat ezután töröljük H-ból. Amikor pedig a H-beli vektorok elfogynak, továbblépünk a második fázisra.

Most részletezni fogjuk a vektorok kiválasztásának és a rétegek elkészítésének módját. Egy olyan U-beli, nemnulla vektorokból álló $(\mathbf{v_1},\mathbf{v_2},\dots,\mathbf{v_i})$ sorozatot, melyre $\mathbf{0}$, $\mathbf{v_1}$, $\mathbf{v_1}+\mathbf{v_2}$, …, $\mathbf{v_1}+\mathbf{v_2}+\cdots+\mathbf{v_{i-1}}$ mind különbözők mod $\mathbf{u}$, nevezzünk *változatosnak*.

Tekintsünk egy olyan változatos $(\mathbf{v_1},\mathbf{v_2},\dots,\mathbf{v_i})$ sorozatot ($i\ge 1$), melyre teljesül $\mathbf{v_1}+\mathbf{v_2}+\cdots+\mathbf{v_i}=i\mathbf{u}$. Ekkor készíthető egy olyan réteg, melyben a $\mathbf{v_1}$, …, $\mathbf{v_i}$ különbségvektorokból egy-egy példányt használunk, és az összes többi felhasznált különbségvektor értéke $\mathbf{u}$: vegyük a $\{\mathbf{0},\mathbf{v_1}\}$, $\{\mathbf{v_1}+\mathbf{u},\mathbf{v_1}+\mathbf{v_2}+\mathbf{u}\}$, $\{\mathbf{v_1}+\mathbf{v_2},\mathbf{v_1}+$

$\mathbf{v_2}+\mathbf{v_3}\}$, $\{\mathbf{v_1}+\mathbf{v_2}+\mathbf{v_3}+\mathbf{u}, \mathbf{v_1}+\mathbf{v_2}+\mathbf{v_3}+\mathbf{v_4}+\mathbf{u}\}$, $\ldots$, $\{\mathbf{v_1}+\mathbf{v_2}+\cdots+\mathbf{v_{i-1}}+(i-1)\mathbf{u}, \mathbf{v_1}+\mathbf{v_2}+\cdots+\mathbf{v_i}+(i-1)\mathbf{u}=\mathbf{u}\}$ vektorpárokat. Vegyük észre, hogy ezek teljes U-beli $\mathbf{u}$ szerinti mellékosztályokat fednek le, és a kimaradó mellékosztályok lefedhetők néhány $\mathbf{u}$ értékű különbségvektorral.

Most legyen $A=\{\mathbf{a_1},\ldots,\mathbf{a_i}\}$ egy olyan minimális elemszámú részhalmaza H-nak, melyben az elemek összege $\mathbf{0}$ mod $\mathbf{u}$. (Ilyen létezik, mivel H elemeinek összege $\mathbf{0}$ mod $\mathbf{u}$.) Ekkor A kör. Két eset van:

1. eset: A jó paritású. Ekkor A tetszőleges sorrendje változatos, mert ha $\sum_{c=1}^{\alpha}\mathbf{a_c}\equiv\sum_{c=1}^{\beta}\mathbf{a_c}\pmod{\mathbf{u}}$ lenne, ahol $0\le\alpha<\beta\le i-1$, akkor $\sum_{c=\alpha+1}^{\beta}\mathbf{a_c}\equiv\mathbf{0}\pmod{\mathbf{u}}$, tehát létezne lineárisan összefüggő valódi részhalmaz. Mivel A elemeinek összege $|A|\mathbf{u}$, a fent leírt módon elkészíthető egy megfelelő réteg.

2. eset: A rossz paritású. Ekkor mivel H és A elemeinek összege is $\mathbf{0}$ mod $\mathbf{u}$, ezért a $H\setminus A$-belieké is. Feltehető, hogy $H\setminus A$ már nem tartalmaz jó paritású kört (mert ha igen, akkor az 1. eset ismételt alkalmazásával ezek elhasználhatóak). A 3.1 lemma miatt minden rétegben a vektorok összege, így a benne használt különbségek összege is $\mathbf{0}$. Mivel kezdetben $\mathbf{0}$ volt az összes megmaradó különbségvektor összege, ezért most (néhány réteg elkészítése után) is. A maradó különbségvektorok számának természetesen párosnak kell lennie. Ezért $H\setminus A\neq\emptyset$, mert különben H elemeinek összege $(|H|+1)\mathbf{u}$ lenne (hiszen néhány jó paritású és egy rossz paritású körből tevődne össze H), de ekkor kezdetben az elemek összege $\mathbf{0}=n_1\mathbf{u}+(|H|+1)\mathbf{u}$, amiből $n_1+|H|+1$ páros, de a kezdeti vektorok száma $n_1+n_2+\cdots+n_t\equiv n_1+|H|\pmod 2$, azaz páratlan, ami ellentmondás. Így $H\setminus A$-ból is kiválaszthatunk egy minimális elemszámú, mod $\mathbf{u}$ lineárisan összefüggő halmazt, ez legyen $B=\{\mathbf{b_1},\ldots,\mathbf{b_j}\}$. Ekkor B rossz paritású kör.

Azt fogjuk csinálni, hogy $A\cup B$ elemeit változatos sorrendbe tesszük. (Ha ezt sikerül megtenni, készen vagyunk, mert két diszjunkt rossz paritású kör uniójára teljesül, hogy $\mathbf{u}$ szorozva az elemek számával megegyezik az elemek összegével; így a kívánt réteg elkészíthető.) Vegyük észre, hogy $A\cup B=\{\mathbf{a_1},\ldots,\mathbf{a_i},\mathbf{b_1},\ldots,\mathbf{b_j}\}$ elemei különböznek $\mathbf{0}$-tól mod $\mathbf{u}$. (A különbségek között $\mathbf{0}$ nem szerepelhet, és $\mathbf{u}$ sem, mert $\mathbf{u}\notin H$.) Mostantól ha nem jelzünk mást, akkor a $\equiv$ jelölés mod $\mathbf{u}$ kongruenciát fog jelölni.

Mivel A-t hamarabb választottuk ki, mint B-t, ezért $i\le j$. Továbbá nyilván $2\le i$, mert egy egyelemű kör csak $\{\mathbf{u}\}$ lehetne, de $\mathbf{u}$ nem szerepel H-ban. A változatos sorrendet $(\mathbf{a_{r_1}},\mathbf{b_{s_1}},\mathbf{a_{r_2}},\mathbf{a_{r_3}},\ldots,\mathbf{a_{r_i}},\mathbf{b_{s_2}},\mathbf{b_{s_3}},\ldots,\mathbf{b_{s_j}})$ alakban fogjuk keresni az indexeknek egy jól megválasztott sorrendjére.

Kezdjük azzal a legáltalánosabb esettel, amikor $i\ge 4$ és $j\ge 5$. Ekkor $A\cup B$ elemei nem csak $\mathbf{0}$-tól, hanem egymástól is különböznek mod $\mathbf{u}$. (Ugyanis ha $\mathbf{v}$ és $\mathbf{v}+\mathbf{u}$ szerepelne benne, akkor ezek egy kisebb kört alkotnának A-nál.)

A sorrendet kezdjük az $\mathbf{a_1}$, majd $\mathbf{b_1}$ vektorokkal, idáig nyilván változatos a sorrend ($\mathbf{a_1}\not\equiv\mathbf{b_1}$, így $\mathbf{a_1}+\mathbf{b_1}\not\equiv 0$). Ezután az $\mathbf{a_2},\ldots,\mathbf{a_i}$ vektorokkal szeretnénk a sorrendet folytatni. Ez $i-1$ lineárisan független vektor mod $\mathbf{u}$, melyek összege $\mathbf{a_1}$ mod $\mathbf{u}$. Ilyen módon a sorrend folytatása elképzelhető a P_{i-1} poset egy maximális láncaként, ahol a poset minden $L\subseteq\{2,\ldots,i\}$ elemének az $\mathbf{a_1}+\mathbf{b_1}+\sum_{c\in L}\mathbf{a_c}\pmod{\mathbf{u}}$ vektort feleltetjük meg. Ekkor a poset minden eleméhez csupa különböző vektort rendeltünk

mod $\mathbf{u}$ (a lineáris függetlenség miatt), és ha a 8.3 lemma miatt ha a $\mathbf{0}$ és $\mathbf{a_1}$ (mod $\mathbf{u}$) vektorokhoz tartozó elemeket kivesszük a posetből (ha léteznek), akkor (mivel $i-1>2$, így nem vehettük ki az összes 1 vagy $i-2$ elemű halmazt) még mindig marad benne i elemű lánc. A sorrendet ha ezen láncnak megfelelő módon folytatjuk, akkor továbbra is változatos marad.

Végül a sorozat végére a $\mathbf{b_2},\dots,\mathbf{b_j}$ vektorokat kell odaírnunk valamilyen sorrendben. Ez is $j-1$ lineárisan független vektor, és az előző posetes okoskodás alapján itt a részösszegekkel a korábbi $i+1$ részösszeget kell elkerülnünk. Azonban a $\mathbf{0}$ (mod $\mathbf{u}$) elkerülésére nem kell ügyelnünk, hiszen (a körtulajdonság miatt) akármilyen sorrendnek a végpontja ennek fog megfelelni, és a poset összes eleméhez itt is csupa különböző vektorokat rendeltünk. Tehát a P_{j-1} posetből itt legfeljebb i elemet veszünk el, és így kell benne továbbra is találnunk egy j elemű láncot.

- Ha $i\le j-2$, akkor lehetetlen, hogy mind a $j-1$ db egyelemű, vagy mind a $j-1$ db $j-2$ elemű halmazt elvegyük a posetből, ezért a 8.3 lemma alapján létezik megfelelő sorrend, ez pedig befejezi az $A\cup B$ halmaz elemeinek változatos felsorolását.

- Ha $i=j-1$ vagy $i=j$, akkor ügyelnünk kell arra az esetre, amikor minden egyelemű, vagy minden $j-2$ elemű halmazt elvettünk a posetből. De ezek nem lehetségesek. Ha ezek bármelyike bekövetkezik, akkor az $\mathbf{a_1}$, $\mathbf{a_1}+\mathbf{b_1}$, $\mathbf{a_1}+\mathbf{b_1}+\mathbf{a_{r_2}}$, $\dots$, $\mathbf{a_1}+\mathbf{b_1}+\mathbf{a_{r_2}}+\dots+\mathbf{a_{r_{i-1}}}$ (mod $\mathbf{u}$ mind különböző) elemek közül legalább $j-1$ felel meg az elvett elemeknek. Ezen elemek száma $i\le j$, és így közülük legalább $i-1$ megfelel egy elvett elemnek. Tehát vagy $\mathbf{a_1}$, vagy pedig $\mathbf{a_1}+\mathbf{b_1}$ megegyezik mod $\mathbf{u}$ egy $\mathbf{b_1}+\mathbf{b_c}$ ($2\le c\le j$) vagy egy $\mathbf{b_c}$ ($2\le c\le j$) alakú elemmel (az előbbi egy egyelemű, az utóbbi egy $j-2$ elemű halmaznak felel meg a posetben). Azonban könnyen látható, hogy ezekben az esetekben $A\cup B$ tartalmaz egy legfeljebb háromelemű, mod $\mathbf{u}$ lineárisan összefüggő halmazt, tehát ($i\ge 4$ miatt) A mégsem minimálisra lett választva, ami ellentmondás. Tehát itt is létezik megfelelő lánc, és így sorrend.

Most pedig oldjuk meg a kimaradó eseteket is, amelyekben i vagy j kicsi.

Ha $i=j=2$, akkor $A\cup B=\{\mathbf{x},\mathbf{x}+\mathbf{u},\mathbf{y},\mathbf{y}+\mathbf{u}\}$ valamely $\mathbf{x}\not\equiv\mathbf{y}$-ra. Ekkor az $(\mathbf{x},\mathbf{y},\mathbf{x}+\mathbf{u},\mathbf{y}+\mathbf{u})$ sorrend megfelelő lesz (ennek a részösszegei rendre $\mathbf{0}$, $\mathbf{x}$, $\mathbf{x}+\mathbf{y}$ és $\mathbf{y}+\mathbf{u}$, melyek egymástól mind különböznek mod $\mathbf{u}$).

Ha $i=2$ és $j=3$, akkor $A=\{\mathbf{x},\mathbf{x}+\mathbf{u}\}$ valamely $\mathbf{x}$-re, és $B=\{\mathbf{b_1},\mathbf{b_2},\mathbf{b_3}\}$, ahol $\mathbf{b_1},\mathbf{b_2},\mathbf{b_3}$ páronként inkongruensek mod $\mathbf{u}$ (különben B nem minimális lineárisan függő halmaz). Itt $\mathbf{b_1}+\mathbf{b_2}+\mathbf{b_3}=\mathbf{0}$. Az $(\mathbf{x},\mathbf{b_1},\mathbf{x}+\mathbf{u},\mathbf{b_2},\mathbf{b_3})$ sorrend jó lesz, mert a mod $\mathbf{u}$ tekintett részösszegek: $\mathbf{0},\mathbf{x},\mathbf{x}+\mathbf{b_1},\mathbf{b_1},\mathbf{b_3}$ páronként inkongruensek. (Ennek belátásához a $\mathbf{b_1}+\mathbf{b_2}+\mathbf{b_3}=\mathbf{0}$ feltételt használjuk, valamint a megadott vektorok nemnullaságát mod $\mathbf{u}$.)

Ha $i=2$ és $j\ge 4$, akkor $A=\{\mathbf{x},\mathbf{x}+\mathbf{u}\}$ valamely $\mathbf{x}$-re, és $B=\{\mathbf{b_1},\mathbf{b_2},\dots,\mathbf{b_j}\}$. Kezdjük a sorrendet $(\mathbf{x},\mathbf{b_1})$-gyel. Ezután $\mathbf{x}+\mathbf{u}$ jó folytatás, mert a $\mathbf{0},\mathbf{x},\mathbf{x}+\mathbf{b_1},\mathbf{b_1}$ részösszegek inkongruensek mod $\mathbf{u}$. Ezután a sorozat befejezéséhez a P_{j-1} posetben kell maximális láncot találnunk úgy, hogy legfeljebb 2 pontot ($\mathbf{x}$ és $\mathbf{x}+\mathbf{b_1}$ mod $\mathbf{u}$) kell elkerülnünk. Ha $j\ge 5$, akkor a 8.3 lemmából következik, hogy ez lehetséges. És $j=4$ esetén pedig triviális, hogy P_3-ban nem fedhető minden 4 hosszú lánc két ponttal.

Ha $i = 3$ és $j = 3$, akkor $A = \{\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}\}$ és $B = \{\mathbf{b_1}, \mathbf{b_2}, \mathbf{b_3}\}$, ahol $\mathbf{a_1}+\mathbf{a_2}+\mathbf{a_3} = \mathbf{b_1}+\mathbf{b_2}+\mathbf{b_3} = \mathbf{0}$ és $\{\mathbf{0}, \mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{b_1}, \mathbf{b_2}, \mathbf{b_3}\}$ mind inkongruensek mod $\mathbf{u}$. (Ha kettő kongruens lenne közülük, akkor nem A lett volna az elején a legkisebb összefüggő halmaz.) Ekkor könnyen látható, hogy az $(\mathbf{a_1}, \mathbf{b_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{b_2}, \mathbf{b_3})$ sorrend működik.

Ha $i = 3$ és $j = 4$, akkor $A = \{\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}\}$ és $B = \{\mathbf{b_1}, \mathbf{b_2}, \mathbf{b_3}, \mathbf{b_4}\}$, ahol $\mathbf{a_1} + \mathbf{a_2} + \mathbf{a_3} = \mathbf{0}$ és $\mathbf{b_1} + \mathbf{b_2} + \mathbf{b_3} + \mathbf{b_4} = \mathbf{u}$. Itt is $A \cup B$ elemei egymással és $\mathbf{0}$-val is inkongruensek mod $\mathbf{u}$. A sorrend mindenképp elkezdhető az $(\mathbf{a_1}, \mathbf{b_1}, \mathbf{a_2}, \mathbf{a_3})$ vektorokkal, ezután pedig olyan sorrendben kell a $\mathbf{b_2}, \mathbf{b_3}, \mathbf{b_4}$ vektorokkal befejeznünk, hogy az ezután érintett két pont mod $\mathbf{u}$ ne egyezzen meg az eddigi $\mathbf{a_1}$, $\mathbf{a_1} + \mathbf{b_1}$ és $\mathbf{a_3} + \mathbf{b_1}$ részösszegekkel. Itt P_3-ban keresünk utat úgy, hogy legfeljebb három pont tiltott. Ez csak akkor nem lehetséges, ha a három pont a három egyelemű vagy a három kételemű halmaznak felel meg. Előbbi esetben $\mathbf{a_1}+\mathbf{b_1}$ is megegyezik a $\mathbf{b_1}+\mathbf{b_2}$, $\mathbf{b_1} + \mathbf{b_3}$ és $\mathbf{b_1} + \mathbf{b_4}$ (egyelemű halmazoknak megfelelő) vektorok valamelyikével mod $\mathbf{u}$, azonban ez egy kételemű lineárisan függő halmazt eredményezne, ami kisebb A-nál. Utóbbi esetben $\mathbf{a_1}$ megegyezik a $\mathbf{b_2}$, $\mathbf{b_3}$ és $\mathbf{b_4}$ (kételemű halmazoknak megfelelő) vektorok valamelyikével mod $\mathbf{u}$, ami ugyanígy ellentmondást okoz. Tehát a sorrend mindig befejezhető megfelelően.

Ha $i = 3$ és $j \geq 5$, akkor is elkezdhető a sorrend az $(\mathbf{a_1}, \mathbf{b_1}, \mathbf{a_2}, \mathbf{a_3})$ vektorokkal, ezután pedig a P_{j-1} posetben legfeljebb 3 pont lesz tiltott $(3 < j-1)$, így mindenképpen találunk megfelelő utat.

Ha $i = 4$ és $j = 4$, akkor pedig $A = \{\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{a_4}\}$ és $B = \{\mathbf{b_1}, \mathbf{b_2}, \mathbf{b_3}, \mathbf{b_4}\}$, ahol $\mathbf{a_1} + \mathbf{a_2} + \mathbf{a_3} + \mathbf{a_4} = \mathbf{b_1} + \mathbf{b_2} + \mathbf{b_3} + \mathbf{b_4} = \mathbf{u}$. Itt is $A \cup B$ elemei egymással és $\mathbf{0}$-val is inkongruensek mod $\mathbf{u}$. A sorrend mindenképp elkezdhető az $(\mathbf{a_1}, \mathbf{b_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{a_4})$ vektorokkal, használva, hogy 4-nél kevesebb elemű összefüggés nincs. A befejezéshez a P_3 posetben kell keresnünk olyan utat, ami blokkolt pontot nem tartalmaz. A poset 1, illetve 2 elemű részhalmazainak a $\mathbf{b_1} + \mathbf{b_2}$, $\mathbf{b_1} + \mathbf{b_3}$ és $\mathbf{b_1} + \mathbf{b_4}$, illetve a $\mathbf{b_2}$, $\mathbf{b_3}$, $\mathbf{b_4}$ vektorok (mod $\mathbf{u}$) felelnek meg. A blokkoló elemek pedig az $\mathbf{a_1}$, $\mathbf{a_1} + \mathbf{b_1}$, $\mathbf{a_1} + \mathbf{b_1} + \mathbf{a_2}$ és $\mathbf{a_4} + \mathbf{b_1}$ részösszegek. Vegyük észre, hogy $\mathbf{a_1}$ nem blokkolhatja egyik pontot sem, különben egy legfeljebb 3 vektorból álló lineáris összefüggés jönne létre $A \cup B$-ben. Ugyanez áll $\mathbf{a_1}+\mathbf{b_1}$-re is. Így valójában legfeljebb 2 pont van blokkolva, és így mindig lesz 4 elemű lánc a posetben.

Ilyen módon a kívánt változatos sorrendet, és így a réteget is minden esetben elkészítettük.

Mindig, amikor egy réteget elkészítünk, akkor a rétegben felhasznált különbségvektorok összege $\mathbf{0}$, így a használt H-beli vektorok összege $\mathbf{0}$ mod $\mathbf{u}$ (mivel azokon kívül csak $\mathbf{u}$-ból használtunk példányokat). Így megmarad az a tulajdonság az elhasznált elemek törlése után is, hogy H elemeinek összege $\mathbf{0}$ mod $\mathbf{u}$.

A második fázis. Minden $2 \leq i \leq n$-re egymás után hajtsuk végre az alábbi lépést.

Ha az $\mathbf{u_i}$-ből megmaradó vektorok száma m_i maradékot ad 2^{k-1}-gyel osztva (ahol $2 \leq m_i \leq 2^{k-1} - 2$ páros), akkor m_i db $\mathbf{u_i}$ különbségből és $2^{k-1} - m_i$ db $\mathbf{u_1}$ különbségből készítsünk el egy réteget. Ez megtehető, mivel ez a fősejtésbeli feladat $\mathbb{F}_2^k$-ra (valójában annak egy eltoltjára, de ez nem változtat a helyzeten), és mivel m_i és $2^{k-1} - m_i$ páros, ezért itt a használandó különbségvektorok összege $\mathbf{0}$, és két különbségosztály esetére pedig már megoldottuk korábban a feladatot.

(Ha $m_i = 0$, akkor nincs teendőnk az i. osztállyal.)

A harmadik fázis. Mivel minden osztályban a megmaradó vektorok száma osztható 2^{k-1}-gyel, és tetszőleges $\mathbf{0} \neq \mathbf{v} \in U$ esetén U (illetve annak tetszőleges eltoltja) felosztható 2^{k-1} db $\mathbf{v}$ különbségű párra, ezért ennek a lépésnek a végrehajtása triviális, ezzel az $\mathbb{F}_2^n$-beli teljes párosítást elkészítettük a kívánt módon.

Vegyük észre, hogy mindhárom fázis minden esetben végrehajtható: az első fázisban minden rétegben H elemeiből legalább 3-at felhasználunk, így legfeljebb $\frac{t-1}{3}$ réteget rakunk ki. A második fázisban pedig t-nél kevesebb réteget raktunk ki. Így az első két fázisban összesen $\leq \frac{4}{3}(t-1) \cdot 2^{k-1}$ példányát használtuk $\mathbf{u}$-nak. Ennyi rendelkezésre is állt, mert

$$\frac{4}{3}t(t-1)\cdot 2^{k-1} \leq \frac{4}{3}t(t-1)\cdot 2^{t-1} \leq \frac{4}{3}t(t-1)\cdot 2^{n-2\log n-2} = \frac{1}{3}\cdot t(t-1)\frac{2^n}{n^2} \leq \frac{1}{3}\cdot 2^n < 2^{n-1}$$

és így $\frac{4}{3}(t-1) \cdot 2^{k-1} < \frac{2^{n-1}}{t} = \frac{m}{t} \leq n_1$. □

9. Teljes párosítás sok azonos vektor esetén

Ebben a fejezetben a fősejtés megoldása szerepel abban a speciális esetben (elég nagy n-re), amikor a különbségvektorok legalább $\frac{28}{29}$ része mind azonos, a többi pedig tetszőleges. Tehát Balister, Győri és Schelp tételével (lásd 2.5 tétel) szemben itt most nem követeljük meg, hogy minden különbségvektor páros sokszor szerepeljen.

9.1. Lemma. *Legyen G egy véges Abel-csoport, és legyen adott egy $X \subseteq G$ részhalmaz. Az $\{a + x : x \in X\}$ alakú halmazokat (ahol $a \in G$ tetszőleges) nevezzük X-mintának. Ekkor G-ben kiválasztható legalább $\frac{|G|}{|X|(|X|-1)+1}$ darab páronként diszjunkt X-minta.*

Bizonyítás. Válasszunk mohón X-mintákat egymás után, mindig egy tetszőlegeset, ami az eddigiektől diszjunkt. Legyenek a kiválasztott minták $a_1 + X$, $a_2 + X$, $\ldots$, $a_\ell + X$, és tegyük fel, hogy újabb X-minta már nem választható ezek mellé.

Ekkor minden $a_{\ell+1} \in G$ elemre teljesül, hogy az $a_{\ell+1}+X$ minta ütközik valamelyik korábbival, azaz léteznek $x, x' \in X$ elemek és $1 \leq i \leq \ell$ úgy, hogy $a_{\ell+1} + x = a_i + x'$, tehát $a_{\ell+1} = a_i + x' - x$. Ilyen alakban azonban csak legfeljebb $\ell(1 + |X|(|X| - 1))$ elem írható fel (mivel $x' - x$ legfeljebb $|X|(|X| - 1)$ nemnulla értéket vehet fel), ezért $|G| \leq \ell(1 + |X|(|X| - 1))$, és így a lemmát beláttuk. □

9.2. Megjegyzés. Ha a G csoport exponense 2 (azaz minden $g \in G$-re $g + g = 0$), akkor $x' - x$ legfeljebb $\binom{|X|}{2}$ nemnulla értéket vehet fel, és így legalább $\frac{|G|}{\binom{|X|}{2}+1}$ darab páronként diszjunkt X-minta is kiválasztható.

9.3. Lemma. *Legyenek $n \geq 2$ valamint $a \geq t \geq 2$ egészek, melyekre $\sum_{i=0}^{\left\lfloor \frac{t}{2} \right\rfloor} \binom{a}{i} > 2^n$. Ekkor $\mathbb{F}_2^n$-ben tetszőleges a db vektor között található legfeljebb t darab, melyek lineárisan összefüggenek.*

Bizonyítás. Indirekten tegyük fel, hogy a $\mathbf{v_1}, \ldots, \mathbf{v_a} \in \mathbb{F}_2^n$ vektorok között minden legfeljebb t méretű halmaz független. Ekkor akárhogyan választunk ki $H, H' \subseteq \{1, 2, \ldots, a\}$ halmazokat, ahol $|H|, |H'| \leq \left\lfloor \frac{t}{2} \right\rfloor$ és $H \neq H'$, teljesülnie kell annak, hogy $\sum_{i \in H} \mathbf{v_i} \neq \sum_{i \in H'} \mathbf{v_i}$, hiszen különben $\sum_{i \in H \triangle H'} \mathbf{v_i} = \sum_{i \in H} \mathbf{v_i} + \sum_{i \in H'} \mathbf{v_i} = \mathbf{0}$, és így $1 \leq |H \triangle H'| \leq |H| + |H'| \leq t$ miatt egy legfeljebb t méretű nemtriviális lineáris összefüggés létezne.

Mivel tehát $\{1, 2, \ldots, a\}$-nak minden legfeljebb $\left\lfloor \frac{t}{2} \right\rfloor$ méretű H részhalmazára $\sum_{i \in H} \mathbf{v_i}$ értéke különböző, ezért az ilyen részhalmazok száma legfeljebb 2^n, ellentmondásban a lemma feltételével. □

9.4. Tétel. *Az 1.1 sejtés igaz abban az esetben, amikor a $\mathbf{d_i}$ különbségvektoroknak több mint $\frac{28}{29}$ része mind megegyezik, és n kellően nagy.*

Bizonyítás. A megadott különbségeink száma most $m = \frac{1}{2} \cdot 2^n$, és jelölje $\mathbf{u} \in \mathbb{F}_2^n$ azt a különbségértéket, ami $\frac{28}{29}m$-nél többször fordul elő a megadott $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_m}$ vektorok között.

Jelöljük H-val azon $\mathbf{d_i}$ vektorok multihalmazát, melyek nem egyenlők $\mathbf{u}$-val. Ekkor $|H| < \frac{1}{29}m$.

Az alábbi módon fogjuk megkonstruálni az $\mathbb{F}_2^n$ vektortérnek egy megfelelő partícióját. A vektorteret az $\langle \mathbf{u} \rangle$ altér szerinti (kételemű) mellékosztályokra bontjuk, majd minden lépésben a H multihalmaznak kijelöljük néhány elemét ($\mathbf{v_1}$, $\mathbf{v_2}$, …, $\mathbf{v_i}$), és ezeket felhasználjuk, azaz $\mathbb{F}_2^n$-ben az eddig felhasználatlan elemek között kijelölünk minden $1 \leq j \leq i$-re egy $\mathbf{v_j}$ különbségű elempárt (úgy, hogy azok diszjunktak legyenek egymástól). Egy adott lépésben mindig olyan elemhalmazt fogunk felhasználni, amely néhány $\langle \mathbf{u} \rangle$ szerinti mellékosztály uniója, így a folyamat végén, miután H elemeit mind felhasználtuk, már csak $\mathbf{u}$ értékű különbségek maradnak és ezekhez hozzárendelhető egy-egy mellékosztály.

Az egy lépésben elhasználandó különbséghalmazok kiválasztása a 8.1 tétel bizonyításának első fázisában használt módszerhez lesz hasonlatos, ezért az ott használtakhoz hasonlóan definiáljuk az alábbi fogalmakat:

- Egy $\mathbb{F}_2^n$-beli vektorokból álló $(\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_i})$ sorozatot nevezzünk *változatosnak*, ha a $\mathbf{0}$, $\mathbf{v_1}$, $\mathbf{v_1}+\mathbf{v_2}$, …, $\mathbf{v_1}+\mathbf{v_2}+\cdots+\mathbf{v_{i-1}}$ vektorok mind különböznek modulo $\mathbf{u}$.

- Egy $\mathbb{F}_2^n$-beli vektorokból álló multihalmazt nevezzünk *körnek*, ha elemei modulo $\mathbf{u}$ lineárisan összefüggenek, és a multihalmaz erre a tulajdonságra nézve tartalmazásra minimális.

- Egy S kört nevezzünk *jó paritásúnak*, ha elemeinek összege $|S|\mathbf{u}$. Ellenkező esetben (ha az összeg $(|S|+1)\mathbf{u}$) *rossz paritásúnak* nevezzük.

Ha a $(\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_i})$ nemnulla vektorok változatos sorozatot alkotnak, és $\mathbf{v_1}+\mathbf{v_2}+\cdots+\mathbf{v_i} = i\mathbf{u}$, akkor tetszőleges $\mathbf{c} \in \mathbb{F}_2^n$-re ha vesszük a $\{\mathbf{c}, \mathbf{c}+\mathbf{v_1}\}$, $\{\mathbf{c}+\mathbf{v_1}+\mathbf{u}, \mathbf{c}+\mathbf{v_1}+\mathbf{v_2}+\mathbf{u}\}$, $\{\mathbf{c}+\mathbf{v_1}+\mathbf{v_2}, \mathbf{c}+\mathbf{v_1}+\mathbf{v_2}+\mathbf{v_3}\}$, $\{\mathbf{c}+\mathbf{v_1}+\mathbf{v_2}+\mathbf{v_3}+\mathbf{u}, \mathbf{c}+\mathbf{v_1}+\mathbf{v_2}+\mathbf{v_3}+\mathbf{v_4}+\mathbf{u}\}$, …, $\{\mathbf{c}+\mathbf{v_1}+\mathbf{v_2}+\cdots+\mathbf{v_{i-1}}+(i-1)\mathbf{u}, \mathbf{c}+\mathbf{v_1}+\mathbf{v_2}+\cdots+\mathbf{v_i}+(i-1)\mathbf{u} = \mathbf{c}+\mathbf{u}\}$ vektorpárokat, akkor ez i darab páronként diszjunkt vektorpár, amelyek a megadott sorozat vektorai közül mindegyiket pontosan egyszer használják fel különbségként, és melyek uniója néhány $\langle \mathbf{u} \rangle$ szerinti mellékosztály uniója. Minden lépésben egy ilyen mintát fogunk felhasználni a vektortér particionálásánál.

Az eljárásunkban először H-t felosztjuk csoportokra az alábbi módon úgy, hogy minden csoport egy kör vagy két kör uniója legyen. Osszuk fel először H-t körökre úgy, hogy mindig a legkisebb méretű kört vesszük ki belőle (egy kör elemeinek összege mindig $\mathbf{0}$ mod $\mathbf{u}$, így minden kör kivétele után a maradék elemek összege $\mathbf{0}$ lesz mod $\mathbf{u}$, tehát lesz lineáris összefüggés és így kör közöttük). Tehát legyen $H = C_1 \cup C_2 \cup \cdots \cup C_\ell$, ahol minden i-re C_i a legkisebb kör $H \setminus \left(\bigcup_{j=1}^{i-1} C_j \right)$-ben, és minden $i < j$-re $C_i \cap C_j = \emptyset$. Ekkor $|C_1| \leq |C_2| \leq \cdots \leq |C_\ell|$ is teljesül. Ha a legkisebb méretű körből jó paritású és rossz paritású is van, akkor kezdjük mindig a jó paritásúakkal a kivételt.

Ekkor a C_i körök között páros sok rossz paritású van, ugyanis C_i elemeinek összegét $s(C_i)$-vel jelölve, $\sum_{i=1}^{\ell} s(C_i) = \sum_{i=1}^{m} \mathbf{d_i} - (2^{n-1} - \sum_{i=1}^{\ell} |C_i|)\mathbf{u} = 0 - 0 + \left(\sum_{i=1}^{\ell} |C_i| \right) \mathbf{u} = \left(\sum_{i=1}^{\ell} |C_i| \right) \mathbf{u}$. Ha a rossz paritású körök $C_{\alpha_1}, C_{\alpha_2}, \ldots, C_{\alpha_{2s}}$, ahol $\alpha_1 < \alpha_2 < \cdots < \alpha_{2s}$, akkor hozzuk létre belőlük a $\{C_{\alpha_1}, C_{\alpha_2}\}, \{C_{\alpha_3}, C_{\alpha_4}\}, \ldots, \{C_{\alpha_{2s-1}}, C_{\alpha_{2s}}\}$ csoportokat.

A jó paritású körök pedig önmagukban alkossanak egy-egy csoportot. Ilyen módon az ℓ kört $s + (\ell - 2s) = \ell - s$ db csoportba osztottuk; legyen $t = \ell - s$.

Rendezzük ezeket a csoportokat elemszámuk szerint csökkenő sorrendbe: legyenek $Y_1, Y_2, \ldots, Y_t$, ahol $|Y_1| \geq |Y_2| \geq \cdots \geq |Y_t|$. Ebben a sorrendben fogjuk a csoportokat felhasználni $\mathbb{F}_2^n$ elemeinek párosításához.

A 8.1 tétel bizonyításánál beláttuk (és így itt is igaz), hogy az ebből az eljárásból származó minden csoport elemei változatos sorrendbe tehetők. Ugyanis ott azt láttuk be, hogy egy jó paritású körnek minden sorrendje változatos, két rossz paritású kör (R_1 és R_2, ahol $|R_1| \leq |R_2|$) uniója pedig szintén változatos sorrendbe tehető, amennyiben $R_1 \cup R_2$ nem tartalmaz R_1-nél kisebb méretű kört, sem pedig két azonos vektort. Ezek a feltételek pedig itt teljesülnek, hiszen a körök növekvő sorrendben lettek kiválasztva, és a körök kivételét a 2 méretű jó paritású körökkel (azaz az azonos elempárokkal) kezdtük.

Tehát a fentiek alapján minden Y_i csoportnak megfeleltethető egy $X_i \subseteq \mathbb{F}_2^n$ részhalmaz, mely $\langle \mathbf{u} \rangle$ szerinti mellékosztályok uniója, és mely $|Y_i|$ db vektorpárra bontható olyan módon, hogy a párok különbségei éppen Y_i elemei legyenek. (Nyilván ekkor X_i tetszőleges eltoltja is felbontható Y_i elemeinek megfelelő módon.) Sorban minden $1 \leq i \leq t$ értéken végighaladva az X_i halmaznak vesszük egy olyan eltoltját, mely az összes korábbi X_j-től ($1 \leq j \leq i-1$) diszjunkt, és ezt felosztjuk az Y_i elemeinek megfelelően, ilyen módon "felhasználva" Y_i elemeit.

Már csak azt kell belátni, hogy ilyen eltolt minden X_i-re létezni fog. Nevezzünk egy Y_i csoportot nagynak, ha $|Y_i| > 8$, különben pedig nevezzük kicsinek. Amikor a C_i köröket kijelöltük H-ban (mindig a maradékok közül a legkisebbet), akkor a 9.3 lemma miatt ameddig a megmaradó vektorok száma (a) teljesítette az $\binom{a}{0}+\binom{a}{1}+\binom{a}{2} > 2^n$ összefüggést, addig találtunk legfeljebb 4 méretű kört.

Így $a > 2 \cdot 2^{\frac{1}{2}n}$ esetén $\binom{a}{0} + \binom{a}{1} + \binom{a}{2} = 1 + a + \frac{a(a-1)}{2} > \frac{1}{2}a^2 > 2 \cdot 2^n > 2^n$, emiatt pedig a legalább 5 méretű körök összmérete legfeljebb $2 \cdot 2^{\frac{1}{2}n}$. Minden nagy csoport tartalmaz egy legalább 5 méretű kört (és ez legalább a csoport méretének felét teszi ki), így a nagy csoportok összmérete legfeljebb $4 \cdot 2^{\frac{1}{2}n}$.

Lássuk be először, hogy a nagy csoportoknál lesz megfelelő eltolt. Minden i-re jelölje $\tilde{X}_i \subseteq \mathbb{F}_2^n/\langle \mathbf{u} \rangle$ az X_i halmaz vetületét. Tekintsük az X_i halmazt, ahol Y_i egy nagy csoport. A korábbi $\tilde{X}_j$ halmazok összmérete legfeljebb $4 \cdot 2^{\frac{1}{2}n}$, így ha $\mathbb{F}_2^n/\langle \mathbf{u} \rangle$-ban találunk $4 \cdot 2^{\frac{1}{2}n}$-nél több diszjunkt $\tilde{X}_i$-mintát, akkor lesz köztük olyan, aminek a metszete minden korábbi $\tilde{X}_j$-mal üres. A 9.2 megjegyzés alapján ez teljesülni fog, ha

$$\frac{2^{n-1}}{\binom{|\tilde{X}_i|}{2} + 1} > 4 \cdot 2^{\frac{1}{2}n} \qquad (*)$$

.

Itt Y_i legfeljebb két kör uniója, és minden kör legfeljebb $n+1$ elemű (mivel tartalmazásra minimális lineárisan összefüggő halmaz $\mathbb{F}_2^n$-ben), ezért $|Y_i| = |\tilde{X}_i| \leq 2n + 2$. Így $\binom{|\tilde{X}_i|}{2} + 1 \leq \frac{(2n+2)(2n+1)}{2} + 1 \leq (2n+2)^2$, és így $8\left(\binom{|\tilde{X}_i|}{2} + 1\right) \leq 8(2n+2)^2 < 2^{\frac{1}{2}n}$ kellően nagy n esetén, ebből pedig $(*)$ is következik.

Most pedig lássuk be, hogy a kicsi csoportoknál is lesz megfelelő eltolt. Ha Y_i egy kicsi csoport, akkor a korábbi $\tilde{X}_j$ ($j < i$) csoportok összmérete legfeljebb $|H| < \frac{1}{29}m = \frac{1}{58} \cdot 2^n$. Így ha $\mathbb{F}_2^n/\langle \mathbf{u} \rangle$-ban találunk legalább $\frac{1}{58} \cdot 2^n$ diszjunkt $\tilde{X}_i$-mintát, akkor Y_i elemeit megfelelően fel tudjuk használni. Ehhez elégséges, ha

$$\frac{2^{n-1}}{\binom{|\tilde{X}_i|}{2}+1} \geq \frac{1}{58} \cdot 2^n \qquad (**)$$

Itt a csoport kicsisége miatt $|\tilde{X}_i| \leq 8$, és így $\binom{|\tilde{X}_i|}{2}+1 \leq 29$, ami éppen a kívánt állítást adja.

Tehát a megadott módszerünk valóban működik és H összes elemét felhasználja, ezek után pedig az $\mathbb{F}_2^n$-ben megmaradó elemek $\mathbf{u}$ különbségű párokra oszthatók. Ezzel tehát megadtuk $\mathbb{F}_2^n$-nek egy megfelelő párokba osztását. □

Irodalomjegyzék

[1] A MathLinks-en R. Bacher által feltett kérdés 2008-ban, jelenleg itt érhető el: `https://artofproblemsolving.com/community/c6h183554`

[2] Balister, P. N., Győri, E., & Schelp, R. H. (2011). Coloring vertices and edges of a graph by nonempty subsets of a set. European Journal of Combinatorics, 32(4), 533-537.

[3] Charbit, P., Jeandel, E., Koiran, P., Perifel, S., & Thomassé, S. (2008). Finding a vector orthogonal to roughly half a collection of vectors. Journal of complexity, 24(1), 39-53.

[4] Correia, D. M., Pokrovskiy, A., & Sudakov, B. (2021). Short proofs of rainbow matching results. arXiv preprint arXiv:2108.07734.

[5] Gao, P., Ramadurai, R., Wanless, I. M., & Wormald, N. (2021). Full rainbow matchings in graphs and hypergraphs. Combinatorics, Probability and Computing, 1-19.

[6] Karasev, R. N., & Petrov, F. V. (2012). Partitions of nonzero elements of a finite field into pairs. Israel Journal of Mathematics, 192(1), 143-156.

[7] Kohen, D., & Sadofschi, I. (2010). A New Approach on the Seating Couples Problem. arXiv:1006.2571

[8] Kohen, D., & Sadofschi, I. (2016). On a generalization of the seating couples problem. Discrete Mathematics, 339(12), 3017-3019.

[9] Mička, O., Hypercube problems. `http://ktiml.mff.cuni.cz/~gregor/hypercube/lecture17.pdf`

[10] Preissmann, E., & Mischler, M. (2009). Seating Couples Around the King's Table and a New Characterization of Prime Numbers. The American Mathematical Monthly, 116(3), 268-272.