DISZJUNKT VEKTORPÁROK KERESÉSE $\mathbb{F}_2^n$-BEN ELŐÍRT KÜLÖNBSÉGSOROZATTAL

KOVÁCS BENEDEK

KIVONAT. A cikkben belátom, hogy ha az $\mathbb{F}_2^n$ vektortérben adottak a d_1, d_2, d_3, ..., d_M nemnulla elemek, ahol $M < \frac{5}{18} \cdot 2^n$, akkor ki lehet a vektortérben választani csupa különböző a_1, a_2, ..., a_M és b_1, b_2, ..., b_M vektorokat úgy, hogy minden i-re $a_i - b_i = d_i$ legyen. Módszerem alapötlete épít a Balister, Győri és Schelp cikkében ([4]) szereplő mohó algoritmusra, de ezen felül az említett eredmény teljes egészében új.

1. BEVEZETÉS, CIKK FELÉPÍTÉSE

R. Bacher vetette fel 2008-ban az alábbi problémát ([1]): legyen p páratlan prím és $M = \frac{p-1}{2}$. Igaz-e, hogy akárhogyan is adottak a d_1, d_2, d_3, ..., d_M nemnulla elemek az $\mathbb{F}_p$ testben, a test $2M$ db nemnulla eleme felosztható diszjunkt (a_i, b_i) párokba $(1 \leq i \leq M)$ úgy, hogy minden i-re $a_i - b_i = d_i$ legyen? Erre először Preissmann és Mischler adott választ ([2]), mégpedig igenlőt.

A feladat értelemszerűen kiterjeszthető a p elemű véges test helyett a p^k eleműre: ahogy azt Karasev és Petrov ([3]) megmutatta, ennek a nemnulla elemeire és $M = \frac{p^k-1}{2}$-re az állítás ugyanebben a formában nem igaz, viszont ha minden i-re adva van egy k elemű, csupa $\mathbb{F}_p$ felett lineárisan független elemet tartalmazó lista, melyből d_i értékét választhatjuk, akkor mindig tudunk a listákból olyan értékeket választani, melyekre a feladat megoldható.

Ha $p = 2$-t vesszük, akkor a 2^k elemű véges testre ugyanez a probléma értelemszerűen nem terjeszthető ki ugyanígy, hiszen a testben páratlan sok nemnulla elem van. Viszont a kérdés feltehető úgy, hogy a párosítandó elemek közé a nullvektort is bevesszük. Balister, Győri és Schelp 2008-as cikkükben ([4]) felvetették az alábbi sejtést:

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

Számítógépes programmal ellenőriztem, hogy a sejtés $n \leq 4$ esetén mindig igaz. A [4] cikkben a szerzők azt is belátták egy mohó eljárás segítségével, hogy ha az $\frac{1}{2}N$ különbségvektor közül $\frac{1}{4}N$ mind azonos, és a többi pedig olyan párokba sorolható, hogy minden páron belül a két érték megegyezik, akkor is kiválaszthatók a vektorok a feltételeknek megfelelően.

Jelen cikkben az ezen sejtés irányába történő haladás érdekében az alábbi gyengébb problémát vizsgálom:

1.2. Probléma. Legyenek $n \geq 2$, $N = 2^n$ és $M \leq \frac{1}{2}N - 1$ előre megadott egészek. Igaz-e, hogy tetszőleges d_1, d_2, ..., $d_M \in \mathbb{F}_2^n$ nemnulla különbségértékek esetén léteznek

olyan csupa különböző $a_1, \ldots, a_M, b_1 \ldots, b_M \in \mathbb{F}_2^n$ vektorok, melyekre teljesül, hogy minden $1 \leq i \leq M$-re $a_i - b_i = d_i$?

Mint azt a cikk 2. szakaszában látni fogjuk, az 1.2 probléma (egy kisebb kikötéssel) $M = \frac{1}{2}N - 1$-re ekvivalens az 1.1 sejtéssel. Kutatásom célja, hogy minél nagyobb M értékekre belássam az 1.2 probléma megoldhatóságát. Ez remélhetőleg olyan módszereket tud eredményezni, melyek az 1.1 sejtés bizonyítását segíthetik.

Cikkem 2-5. szakaszában belátom az 1.2 probléma állítását $M \leq \frac{5}{18}N$-re. Az alábbi módon épül fel a bizonyítás:

- A 2. fejezetben az 1.2 probléma és az 1.1 sejtés közötti összefüggés bemutatásán kívül bemutatok egy egyszerű mohó algoritmust, mellyel megoldható a feladat $M \leq \frac{1}{4}N$ élre, valamint $\frac{1}{4}N < M \leq \frac{1}{2}N$ esetén abban a speciális esetben, amikor a különbségek közül elég sok mind megegyezik.
- A 3. fejezetben bemutatom a fő módszeremet (a "háromrészes mohó módszert"): ez egy olyan mohó módszer, melyben a vektortér vektorpárjait három kategóriába osztom az alapján, hogy a benne lévő két vektor közül hánynak 1 az első koordinátája. Ezután a megadott különbségekhez egy alkalmas sorrendben rendelek vektorpárokat egymás után mohó módon, olyan megszorítással, hogy minden különbséghez előre lerögzítem, hogy milyen kategóriájú vektorpárt fogok hozzárendelni.

  Az derül ki, hogy ez a módszer $\frac{1}{4}N$-nél kicsivel nagyobb M értékek esetén is működik, de csak akkor, ha nem túl kicsi és nem túl nagy az 1-gyel kezdődő vektorok számának részaránya a megadott különbségek között.
- A 4. fejezetben az előbb említett korlátját orvosolom a háromrészes mohó módszernek: ha az élek száma egy bizonyos értéket nem halad meg, akkor belátom, hogy a problémát át tudom alakítani az $\mathbb{F}_2^n$ vektortérnek egy megfelelő automorfizmusával úgy, hogy az 1-gyel kezdődő vektorok számának részaránya a kívánt tartományba essen (attól a kivételes esettől eltekintve, ha a vektorok közül elég sok mind megegyezik, de ekkor a 2. fejezetben említett egyszerű mohó algoritmus alkalmazható).
- Az 5. fejezetben elvégzem a szükséges számításokat, melyekkel kiderül, hogy a 3-4. fejezetekben említett módszer minden $M \leq \frac{3}{11}N$-re közvetlenül működik. A háromrészes mohó módszer egyik része olyan, hogy annak az egyik részében az egyszerű mohó algoritmus helyett használhatunk tetszőleges jobb módszert is. Ilyen módon a módszer javítani tudja saját magát rekurzív módon: ha az $M \leq \frac{3}{11}N$-re működő módszert helyettesítjük bele, akkor egy jobb változatot kapunk, ami már $M \leq \frac{67}{242}N$-re is működik. Ha belehelyettesítjük a $\frac{67}{242}N$-es változatot, akkor megint jobbat kapunk. És így tovább, a limeszben megkapjuk azt, hogy a feladat minden $M \leq \frac{5}{18}N$-re megoldható.

Köszönöm szépen Zsigri Bálintnak a módszer ellenőrzésében és a számításokban való segítséget, valamint azt az észrevételt, hogy a 4.3 tételben ha k és l értékét nem feltétlenül vesszük egyenlőnek, azzal lényegesen javítható a módszerrel elért konstans. Köszönöm szépen témavezetőmnek, Csikvári Péternek, hogy megismertette velem ezt az érdekes problémát, lektorálta cikkemet és segítséget nyújtott a strukturálásában.

2. Észrevételek a fősejtéssel kapcsolatban

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

2.1. Megjegyzés. Az 1.1 és 1.2 állításokról gyakran a gráfok nyelvén fogok beszélni: adott egy $2M$ csúcsú gráf, mely M diszjunkt élből áll, és minden élre rá van írva egy $\mathbb{F}_2^n$-beli nemnulla címke. Úgy szeretnénk a gráf minden csúcsába csupa különböző $\mathbb{F}_2^n$-beli értékeket írni, hogy bármely két szomszédos csúcs értékének különbsége az őket összekötő él címkéjével egyezzen meg.

2.2. Lemma. *Az $\mathbb{F}_2^n$ vektortér összes elemének összege 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 $n \geq 2$. □

2.3. Állítás. *Az 1.1 sejtés nem lenne igaz, ha nem kötnénk ki, hogy a d_i címkék összege 0.*

Bizonyítás. Tegyük fel, hogy mégis igaz, és vegyük egy olyan megadását a d_i ($1 \leq i \leq M$) címkéknek, melyekre $\sum_{i=1}^{M} d_i \neq 0$. Ekkor az a_i, b_i vektorok egy helyes megadására $\sum_{i=1}^{M} d_i = \sum_{i=1}^{M}(a_i - b_i) = \sum_{i=1}^{M}(a_i + b_i) = \sum_{i=1}^{M} a_i + \sum_{i=1}^{M} b_i = \sum_{x \in \mathbb{F}_2^n} x = 0$, használva a 2.2 lemmát (azt is kihasználva, hogy 2 karakterisztikájú test fölötti vektortérben az összeadás ugyanaz, mint a kivonás). Ellentmondás. □

2.4. Megjegyzés. A főprobléma nem mindig oldható meg $M = \frac{1}{2}N - 1$ esetén, ugyanis ha a a megadott M különbség összege 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 0 lenne, így a 2.2 lemma miatt a kimaradó két elem összege is 0, de ez azt jelenti, hogy a kimaradó két elem azonos, ami ellentmondás.

2.5. Állítás. *A főprobléma megoldhatósága $M = \frac{1}{2}N - 1$-re a $\sum_{i=1}^{M} d_i \neq 0$ esetre ekvivalens az 1.1 sejtéssel.*

Bizonyítás. Ha az 1.1 sejtés igaz, akkor tetszőleges adott d_1, d_2, ..., d_M nemnulla vektorokra (ahol $\sum_{i=1}^{M} d_i \neq 0$) legyen $d_{M+1} = \sum_{i=1}^{M} d_i$, így $\sum_{i=1}^{M+1} d_i = 0$. Ekkor a sejtés alapján léteznek csupa különböző a_i, b_i vektorok úgy, hogy $a_i - b_i = d_i$ 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 d_1, d_2, ..., d_{M+1} nemnulla különbségeket, melyek összege 0. Ekkor $\sum_{i=1}^{M} d_i = d_{M+1} \neq 0$, így az első M él végpontjai kitölthetők megfelelően $2M$ különböző vektorral. A vektortér maradék két elemének összege megegyezik az eddigi $2M$ elem összegével (a 2.2 lemma miatt), ami éppen $\sum_{i=1}^{M} d_i = d_{M+1}$. □

Az alábbiakban mutatunk egy egyszerű mohó algoritmust, mellyel a főprobléma megoldható a fősejtésbeli $\frac{1}{2}N$ élszám felére.

2.6. 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 $a_1, \ldots, a_{i-1}$ és $b_1, \ldots, b_{i-1}$, ahol $1 \leq i \leq M$, akkor próbáljunk meg keresni olyan a_i-t és b_i-t, hogy $a_i - b_i = d_i$. Mivel $d_i \neq 0$, $\mathbb{F}_2^n$ felbomlik $\frac{1}{2}N$ olyan párra, melyek

mindegyikében a két tag különbsége d_i. (Ezek a párok pontosan a $\langle d_i \rangle$ 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 $\{a_i, b_i\}$-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.

2.7. Tétel. *Ha $\frac{1}{4} < m < \frac{1}{2}$ és $a \geq 2m - \frac{1}{2}$, akkor megoldható a főprobléma, ha $M \leq mN$ és az élek közül legalább aN-nek mind azonos a címkéje.*

Bizonyítás. Legyenek a megadott különbségek $d_1, d_2, ..., d_A, ..., d_M$, ahol $d_1 = d_2 = ... = d_A = d$ és $A \geq aN$. Először válasszuk ki megfelelően a $d_{A+1}, ..., d_M$ él végpontjait. Ezt meg tudjuk tenni a 2.6 tétel alapján, mert ezen élek száma $M - A \leq (m-a)N \leq \frac{1}{4}N$. (Ez azért teljesül, mert $m \geq \frac{1}{4}$ miatt $m - \frac{1}{4} \leq 2m - \frac{1}{2} \leq a$, így $m - a \leq \frac{1}{4}$.)

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

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

3. A háromrészes mohó módszer

A 3-5. fejezetekben bemutatunk egy módszert, amellyel a 2.6 tételt meghaladó eredmény érhető el: ezzel a módszerrel belátható a főprobléma megoldhatósága $M \leq \frac{5}{18}N$ élre.

Feltesszük, 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 2.6 tétel miatt például vehetjük λ értékét $\frac{1}{4}$-nek.

3.1. Definíció. Egy $v \in \mathbb{F}_2^n$ vektor *0-val* (vagy rendre *1-gyel*) *kezdődik*, ha az első koordinátája 0 (vagy 1).

3.2. Megfigyelés. Ha $v \in \mathbb{F}_2^n$ egy 0-val kezdődő nemnulla vektor, akkor $\mathbb{F}_2^n$-nek a $\langle v \rangle$ szerinti mellékosztályai között 2^{n-2} olyan van, ami két 0-val kezdődő vektort tartalmaz (továbbiakban: *0-0 párok*) és 2^{n-2} olyan, ami két 1-gyel kezdődőt (*1-1 párok*).

3.3. Megfigyelés. Ha $v \in \mathbb{F}_2^n$ egy 1-gyel kezdődő vektor, akkor $\mathbb{F}_2^n$-nek a $\langle v \rangle$ 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 $M = mN$ jelölést használjuk, akkor $m = \beta + \gamma$.

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 $m \leq \frac{1}{4}$ esetén működik, hanem β és γ bizonyos értékei esetén kicsivel nagyobb m-ekre is.

Az alábbi módszert használjuk:

3.4. 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 őket 0-0 párokkal tetszőlegesen 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.

3.5. 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 3.4 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 d. Ekkor mivel d 1-gyel kezdődik, $\mathbb{F}_2^n$ felosztható $2^{n-1} = \frac{1}{2}N$ db 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 d) mindig találni fogunk megfelelő 1-1 párt, amit az él csúcsaiba írhatunk. Van 2^{n-2} db 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 $C + 2(J-1) \leq C + 2(B_2 - 1) = C + 2B_2 - 2 \leq (\frac{1}{4}N + 1) - 2 < \frac{1}{4}N = 2^{n-2}$.

□

3.6. 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 3.4 algoritmus (B_1 és B_2 alkalmas választásával).*

Bizonyítás. Legyen $B_2 = \min(\left\lceil \frac{1}{8}N - \frac{1}{2}C \right\rceil, B)$ és $B_1 = B - B_2$. Ekkor a 3.5 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 $B_2 \geq B$, 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 $B_2 = \left\lceil \frac{1}{8}N - \frac{1}{2}C \right\rceil \geq \frac{1}{8}N - \frac{1}{2}C$.
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 $B_2 \leq \left\lceil \frac{1}{8}N - \frac{1}{2}C \right\rceil \leq \frac{1}{8}N - \frac{1}{2}C + 1$, így $2B_2 + C \leq \frac{1}{4}N - C + 1 + C = \frac{1}{4}N + 1$.

□

3.7. 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 feltételekből könnyen látszik, hogy β és γ nem lehet egyszerre $\frac{1}{4}$. Így csak egyetlen élünk lehet, legyen ez d_1. Ekkor $a_1 = d_1$ és $b_1 = 0$ választással $a_1 - b_1 = d_1$.

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 3.6 állítás miatt a B' db 0-val kezdődő és C' db 1-gyel kezdődő különbségre működik a 3.4 algoritmus. □

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

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

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

3.10. 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.

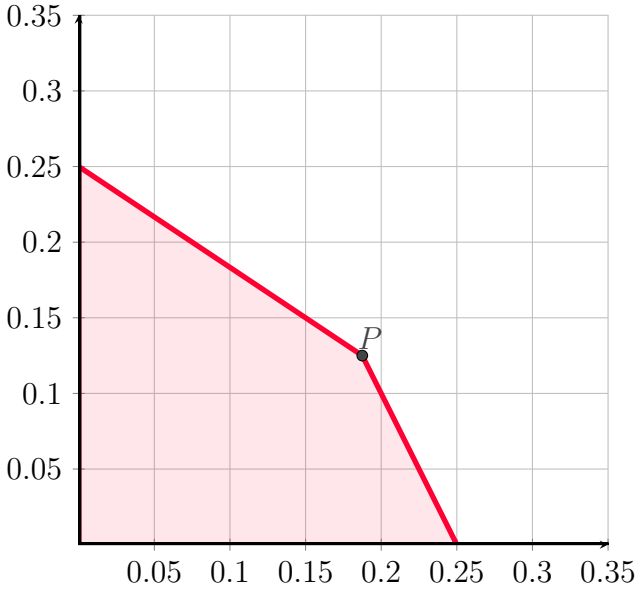
3.11. Megjegyzés. Ezen definíciók nyelvén a korábbi állításaink így szólnak:

- 2.6 tétel: $U\left(\frac{1}{4}\right)$
- 2.7 tétel: $\left(\frac{1}{4} < m < \frac{1}{2}\right)$ és $\left(a \geq 2m - \frac{1}{2}\right) \implies U_{az}(m, a)$
- 3.7 következmény: $\left(\frac{1}{4} \leq \lambda < \frac{1}{2}\right)$ és $(0 \leq \beta, \gamma \leq \frac{1}{4})$ és $U(\lambda)$ és $(\beta \leq \min(\frac{1}{4} - \gamma, \frac{1}{2}\lambda) + \left(\frac{1}{8} - \frac{1}{2}\gamma\right)) \implies U_{01}(\beta, \gamma)$.

4. Kezdetek arányának szabályozása lineáris transzformációval

Nézzük meg, mit mond a 3.7 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 $M = mN$, ahol $m = \beta + \gamma$, akkor látható, hogy ha a 3.7 következmény segítségével szeretnénk belátni valamilyen adott $m > \frac{1}{4}$-re az állítást, akkor ez csak úgy tehető meg, ha a 0-val kezdődő élek $r = \frac{\beta}{m}$ részaránya egy $[r_{min}(m), r_{max}(m)]$ intervallumon belülre esik, ahol $0 < r_{min}(m)$ és $r_{max}(m) < 1$.

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

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 a főprobléma megoldásában:

4.1. Lemma. *Legyen $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2^n$ egy $\mathbb{F}_2$-vektortér-automorfizmus. Ekkor a d_1, d_2, ..., $d_M \in \mathbb{F}_2^n$ élekre pontosan akkor oldható meg a főprobléma, ha az $\alpha(d_1)$, $\alpha(d_2)$, ..., $\alpha(d_M)$ élekre megoldható.*

Bizonyítás. Tegyük fel, hogy a d_1, ..., d_M élekre az a_1, ..., a_M, b_1, ..., b_M értékek megoldják a problémát. Ekkor minden i-re $d_i = a_i - b_i$.

Ekkor az $a'_i = \alpha(a_i)$, $b'_i = \alpha(b_i)$ különbségek megoldják a problémát a $d'_i = \alpha(d_i)$ különbségekre: az automorfizmus csupa különböző vektorokat csupa különbözőbe visz, és minden i-re $\alpha(d_i) = \alpha(a_i) - \alpha(b_i)$.

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

Így ha adottak a d_1, ..., d_M különbségek, melyeknek a nagy része azonos számjeggyel kezdődik, de találunk egy olyan $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2^n$ automorfizmust, melyre $\alpha(d_1)$, ...,

$\alpha(d_M)$ között a 0-val kezdődőek részaránya már beleesik $[r_{min}(m), r_{max}(m)]$-be, akkor a 4.1 lemma miatt dolgozhatunk az eredeti különbségek helyett a transzformáltakkal, melyekre a korábbiak alapján már meg tudjuk oldani a problémát.

Azonban ha a 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:

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

A fejezet fő eredménye az alábbi tétel lesz:

4.3. Tétel. *Legyen $0 < l \leq k \leq \frac{1}{3}$. Ekkor $T(k, l, 1 - 2k - 2l)$ teljesül.*

A 4.3 tétel bizonyítása

4.4. Definíció. Ha $K \subseteq \{1, 2, ..., n\}$ egy nemüres halmaz, akkor legyen $A_K = \{x \in \mathbb{F}_2^n : \sum_{i \in K} x_i = 0\}$. (Könnyen látható, hogy A_K egy $n - 1$ dimenziós altere $\mathbb{F}_2^n$-nek.)

A továbbiakban K mindig egy nemüres részhalmaza $[n]$-nek[1], és $0 < l \leq k \leq \frac{1}{3}$ rögzített valós számok. Továbbá feltételezzük, hogy adottak a d_1, ..., $d_M \in \mathbb{F}_2^n$ nemnulla vektorok. A d_i vektor j-edik koordinátáját $d_{i,j}$-vel fogjuk jelölni ($1 \leq i \leq M$, $1 \leq j \leq N$, $d_{i,j} \in \{0, 1\}$).

4.5. Definíció. Egy K halmazt *szegénynek* nevezünk, ha a $d_1, d_2, ..., d_M$ vektorok közül kevesebb mint kM db esik bele az A_K altérbe.

4.6. Definíció. Egy K halmazt *gazdagnak* nevezünk, ha a $d_1, d_2, ..., d_M$ vektorok közül több mint $(1 - l)M$ esik bele az A_K altérbe.

Jegyezzük meg, hogy egy halmaz nem lehet egyszerre szegény és gazdag, mert $k + l \leq 1$ miatt $k \leq 1 - l$.

4.7. Definíció. Egy $1 \leq j \leq n$ indexet *szegénynek*, illetve *gazdagnak* nevezünk, ha a $\{j\}$ halmaz szegény, illetve gazdag.

4.8. Definíció. Egy K halmaz *gyarmata*: $Gyar(K) = \{1 \leq i \leq M : (\exists j \in K) d_{i,j} = 0\}$, és *kommünje*: $Komm(K) = \{1 \leq i \leq M : (\exists j \in K) d_{i,j} = 1\}$.

4.9. Lemma. *Tegyük fel, hogy $[n]$ minden $K \neq \emptyset$ részhalmaza vagy szegény, vagy gazdag. Ekkor tetszőleges, csak szegény indexekből álló nemüres halmaz gyarmatának mérete $< 2kM$.*

Bizonyítás. Belátjuk a szerinti indukcióval, hogy egy a db szegény indexből álló halmaz gyarmatának mérete $< \left(2 - \frac{1}{2^{a-1}}\right) kM$. (Ebből a lemma állítása következik.)

Az $a = 1$ eset:

Egy egyelemű $\{j\}$ halmazra, ahol j szegény, $|Gyar(\{j\})| = |\{i : d_i \in A_{\{j\}}\}| < kM$, ahol az utóbbi egyenlőtlenségnél $\{j\}$ szegénységét használtuk.

[1] Az $[n] = \{1, 2, ..., n\}$ jelölést használjuk.

Indukciós lépés:

Tegyük fel, hogy $a \geq 2$, és az a-nál kisebb $1 \leq a' \leq a-1$ értékekre már beláttuk az állítást. Vegyünk egy a db szegény indexből álló K halmazt.

Segédlemma: K-nak minden páratlan méretű részhalmaza szegény, és minden páros méretű részhalmaza gazdag.

Segédlemma bizonyítása: Ha K-nak vesszük egy $L \subset K$ valódi részhalmazát, akkor mivel $|L| \leq a-1$, ezért az indukciós feltétel miatt $|Gyar(L)| < 2kM$. Ez azt jelenti, hogy a d_i vektorok közül több mint $(1-2k)M$-nek az összes L-beli koordinátája 1-es. Ezen vektorok tehát mind benne vannak A_L-ben, ha $|L|$ páros, és egyikük sincs benne A_L-ben, ha $|L|$ páratlan. Tehát ha $|L|$ páros, akkor az A_L-be eső d_i-k száma $> (1-2k)M \geq \frac{1}{3}M \geq kM$ (használva, hogy $k \leq \frac{1}{3}$), emiatt L nem lehet szegény, tehát gazdagnak kell lennie. Ha pedig $|L|$ páratlan, akkor az A_L-be eső d_i-k száma $< 2kM \leq (1-l)M$ (használva, hogy $2k+l \leq 2 \cdot \frac{1}{3} + \frac{1}{3} = 1$), emiatt L nem lehet gazdag, tehát szegénynek kell lennie.

A segédlemma bizonyításához még meg kell vizsgálnunk az $L = K$ esetet. Először tegyük fel, hogy $|K|$ páros. Ekkor vegyünk ki K-ból egy j indexet, és legyen $K' = K \setminus \{j\}$. Mivel $|K'|$ páratlan, ezért K' szegény. Továbbá maga $\{j\}$ is szegény. Így kevesebb mint kM db d_i esik bele $A_{K'}$-be, és kevesebb mint kM esik $A_{\{j\}}$-be. Tehát a d_i-k közül kevesebb mint $2kM$ esik az $A_{K'}$ és $A_{\{j\}}$ alterek legalább egyikébe. Így több mint $(1-2k)M$ db d_i-re teljesül, hogy a K'-beli koordinátáinak összege is 1 és a j. koordinátája is 1. Így ezekre a vektorokra a K-beli koordináták összege 0, vagyis benne vannak A_K-ban. Így az A_K-ban lévő d_i-k száma $> (1-2k)M \geq kM$ (mivel $k \leq \frac{1}{3}$), emiatt K nem lehet szegény, vagyis gazdag.

Ha $L = K$ és $|K|$ páratlan, akkor $|K'|$ páros, így K' gazdag. Használva K' gazdagságát és j szegénységét, az $A_{K'}$ altér $A^c_{K'}$ komplementerébe kevesebb mint lM db d_i esik, és az $A_{\{j\}}$ altérbe pedig kevesebb mint kM db. Így több mint $(1-k-l)M$ esik $A_{K'} \cap A^c_{\{j\}}$-be. Ezekre a vektorokra a K'-koordináták összege 0, és a j. koordináta 1, így mindegyikben a K-koordináták összege 1, tehát ezek nem esnek A_K-ba. Így az A_K-ba eső d_i-k száma $< (k+l)M \leq (1-l)M$. (Használva, hogy $k+2l \leq \frac{1}{3} + 2 \cdot \frac{1}{3} \leq 1$.) Emiatt K nem lehet gazdag, így szegény. $\square$

Indukciós lépés befejezése: Legyen $e = (1, 1, ..., 1) \in \mathbb{F}_2^n$ a csupa 1-es vektor. Legyen $S = \{(i, L) : 1 \leq i \leq M, \emptyset \neq L \subseteq K, d_i + e \notin A_L\}$. Számoljuk le kétféleképpen S elemszámát.

Azon d_i vektoroknak, melyekre $i \notin Gyar(K)$, minden K-beli koordinátájuk 1, így ezekre $d_i + e$ minden K-beli koordinátája 0. Így az ilyen i-kre minden $L \subseteq K$-ra $d_i + e \in A_L$. Tehát minden $(i, L) \in S$-re $i \in Gyar(K)$.

Ha $i \in Gyar(K)$, akkor a $d_i + e$ vektor K-beli koordinátái nem mind nullák. Legyen közülük f db 1-es és g db 0. (Itt $f \geq 1$.) Ekkor egy $L \subseteq K$ részhalmazra akkor teljesül $d_i + e \notin A_L$, ha $d_i + e$-nek páratlan sok L-beli koordinátája 1-es. Így ha úgy szeretnénk megválasztani adott i-re az $L \subseteq K$ részhalmazt, hogy $d_i + e \notin A_L$ legyen, akkor $d_i + e$-nek az f db 1-es koordinátája közül páratlan sokat kell beleválasztanunk L-be, a g db 0-s koordináta közül pedig tetszőlegeseket beleválaszthatunk. Mivel $f \geq 1$, az 1-es koordinátáknak 2^{f-1} részhalmaza lesz páratlan elemszámú, a 0-s koordinátáknak pedig 2^g részhalmaza létezik, így összesen $2^{f-1}2^g = 2^{a-1}$-féleképpen választhatjuk meg L-et. Emiatt $|S| = |Gyar(K)|2^{a-1}$.

Másrészt pedig számoljuk meg adott $L \subseteq K$ nemüres részhalmazra, hogy hány $1 \leq i \leq M$-re lesz $(i, L) \in S$.

Ha $|L|$ páratlan, akkor L szegény, így kM-nél kevesebb i-re lesz $d_i \in A_L$. Így több mint $(1-k)M$ db i-re lesz $d_i \notin A_L$. Ezekre az i-kre d_i L-beli koordinátáinak összege 1, tehát mivel $|L|$ páratlan, ezért d_i+e L-beli koordinátáinak összege 0, tehát $d_i+e \in A_L$. Így kevesebb mint kM db i-re lesz $d_i+e \notin A_L$ (azaz $(i,L) \in S$).

Ha pedig $|L|$ páros, akkor L gazdag, így több mint $(1-l)M$ db i-re lesz $d_i \in A_L$. Ezekre az i-kre a d_i vektor L-beli koordinátáinak összege 0, így a d_i+e vektor L-beli koordinátáinak is 0 az összege, mert $|L|$ páros. Tehát ezekre az i-kre $d_i+e \in A_L$, így kevesebb mint lM olyan i van, melyre $d_i+e \notin A_L$ (azaz $(i,L) \in S$).

A K halmaz nemüres részhalmazai közül $2^{a-1}-1$ db páros elemszámú és 2^{a-1} db páratlan elemszámú. Ezek alapján, ha az előző két bekezdésben kapott becsléseket minden $L \subseteq K$-ra ($L \neq \emptyset$) összegezzük, azt kapjuk, hogy

$$|S| < 2^{a-1}kM + (2^{a-1}-1)lM$$

Így

$$|Gyar(K)|2^{a-1} < 2^{a-1}kM + (2^{a-1}-1)lM$$

$$|Gyar(K)| < kM + \left(1 - \frac{1}{2^{a-1}}\right) lM$$

Felhasználva, hogy $l \leq k$:

$$|Gyar(K)| < kM + \left(1 - \frac{1}{2^{a-1}}\right) kM = \left(2 - \frac{1}{2^{a-1}}\right) kM$$

Ezzel a 4.9 lemma bizonyítását befejeztük.

□

4.10. Lemma. *Tegyük fel, hogy $[n]$ minden $K \neq \emptyset$ részhalmaza vagy szegény, vagy gazdag. Ekkor tetszőleges, csak gazdag indexekből álló nemüres halmaz kommünjének mérete $< 2lM$.*

Bizonyítás. Az állítás, és így bizonyításunk is analóg lesz a 4.9 lemmáéval, de annál egyszerűbb, mert itt nem lesznek paritás miatti esetszétválasztások.

Belátjuk a szerinti indukcióval, hogy egy a db gazdag indexből álló halmaz kommünjének mérete $< \left(2 - \frac{1}{2^{a-1}}\right) lM$. (Ebből a lemma állítása következik.)

Az $a = 1$ eset:

Egy egyelemű $\{j\}$ halmazra, ahol j gazdag, $|Komm(\{j\})| = |\{i : d_i \notin A_{\{j\}}\}| < lM$, ahol az utóbbi egyenlőtlenségnél $\{j\}$ gazdagságát használtuk.

Indukciós lépés:

Tegyük fel, hogy $a \geq 2$, és az a-nál kisebb $1 \leq a' \leq a-1$ értékekre már beláttuk az állítást. Vegyünk egy a db gazdag indexből álló K halmazt.

Segédlemma: K-nak minden nemüres részhalmaza gazdag.

Segédlemma bizonyítása: Ha $L \subset K$ valódi részhalmaz, akkor az indukciós feltevés miatt $|Komm(L)| < 2lM$. Tehát a d_i-k közül több mint $(1-2l)M$-nek minden L-koordinátája 0, tehát ezekre a vektorokra biztosan teljesül $d_i \in A_L$. Így az A_L-be eső d_i-k száma $> (1-2l)M \geq kM$ (mivel $k + 2l \leq \frac{1}{3} + 2 \cdot \frac{1}{3} = 1$), így L nem lehet szegény. Tehát L gazdag.

Így már csak az $L = K$ eset maradt. Válasszunk egy $j \in K$ indexet, és legyen $K' = K \setminus \{j\}$. Ekkor az előzőek alapján K' gazdag, és tudjuk, hogy $\{j\}$ is gazdag. Így kevesebb mint lM db i van, melyre $d_i \notin A_{K'}$, és kevesebb mint lM db i, melyre

$d_i \notin A_{\{j\}}$. Így több mint $(1-2l)M$ db i-re teljesül $d_i \in A_{K'} \cap A_{\{j\}}$. Ezekre az d_i-kre a K'-beli koordináták összege is 0 és a j. koordináta is 0, így a K-beli koordináták összege is 0, azaz ezekre $d_i \in A_K$. Tehát az A_K-ba eső d_i-k száma $> (1-2l)M \geq kM$. Azaz K nem lehet szegény, így gazdag. □

Indukciós lépés befejezése: Legyen $S = \{(i, L) : 1 \leq i \leq M, \emptyset \neq L \subseteq K, d_i \notin A_L\}$. Számoljuk meg kétféleképp S elemeit.

Ha egy adott i-re ha $i \notin Komm(K)$, akkor d_i-nek minden K-koordinátája 0, így minden $L \subseteq K$-ra $d_i \in A_L$. Tehát minden $(i, L) \in S$-re $i \in Komm(K)$.

Ha $i \in Komm(K)$, akkor legyen a d_i 1-es koordinátáinak száma f, és a 0-sok száma g. Ekkor $f \geq 1$. Egy $L \subseteq K$ részhalmazra pontosan akkor teljesül $d_i \notin A_L$, ha d_i-nek páratlan sok L-beli koordinátája 1-es. Így (az előző lemma bizonyításához hasonlóan) $2^{f-1}2^g = 2^{a-1}$-féleképpen választhatjuk meg úgy L-et, hogy $d_i \notin A_L$ legyen. Tehát ezek alapján $|S| = |Komm(K)|2^{a-1}$.

Másrészt minden $L \subseteq K$ gazdag, így mindegyikre $< lM$ db i van, hogy $d_i \notin A_L$. Mivel K-nak összesen $2^a - 1$ nemüres részhalmaza van, ezért ebből az jön ki, hogy $|S| < (2^a - 1)lM$. Tehát

$$|Komm(K)|2^{a-1} < (2^a - 1)lM$$

$$|Komm(K)| < \frac{2^a - 1}{2^{a-1}} lM = \left(2 - \frac{1}{2^{a-1}}\right) lM$$

És ezt kellett belátnunk. □

A 4.3 tétel bizonyítása. Azt kell belátnunk, hogy ha $0 < l \leq k \leq \frac{1}{3}$, akkor tetszőleges $n \geq 2$-re, $M \in \mathbb{N}^+$-ra és $d_1, d_2, ..., d_M \in \mathbb{F}_2^n$ nemnulla vektorokra teljesül, hogy vagy legalább $(1-2k-2l)M$ azonos van a vektorok között, vagy pedig létezik egy $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2^n$ automorfizmus, hogy $\alpha(d_1), ..., \alpha(d_M)$ közül legalább kM db 0-val és legalább lM db 1-gyel kezdődik.

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

Ha pedig bármely $K \subseteq [n]$ nemüres halmaz szegény vagy gazdag, akkor a 4.9 és 4.10 lemmák miatt az összes szegény index alkotta halmaz gyarmatának mérete $< 2kM$, az összes gazdag index alkotta halmaz kommünjének mérete $< 2lM$, így a d_i-k közül több mint $(1-2k-2l)M$ db nincs benne sem a szegények gyarmatában, sem a gazdagok kommünjében. Azonban minden ilyen d_i megegyezik egymással, mert egy ilyen d_i-nek minden szegény indexnél a koordinátája 1, és minden gazdag indexnél a koordinátája 0. Tehát ebben az esetben a vektorok között legalább $(1-2k-2l)M$ azonos található. □

5. A főprobléma megoldása $M \leq \frac{5}{18}N$ élre

Ebben a fejezetben összerakjuk az eddigi eredményeinket, hogy belássuk a főproblémát $M \leq \frac{5}{18}N$ él esetén.

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

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

akkor $U(\alpha)$ is teljesül.

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

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

Az utóbbi esetben legyen rM azon i indexek száma, melyekre d_i 0-val kezdődik. Ekkor $k \leq r \leq 1 - l$. A nullával kezdődő d_i-k száma $rM = r\beta N \leq r\alpha N$ és az 1-gyel kezdődőeké $(1-r)M = (1-r)\beta N \leq (1-r)\alpha N$. Így $U_{01}(r\alpha, (1-r)\alpha)$ miatt megoldható a főprobléma az $\alpha(d_i)$ vektorokra, és így a 4.1 lemma miatt a d_i vektorokra is. □

5.2. Tétel. *Ha egy $\frac{1}{4} \leq \lambda < \frac{5}{18}$ értékre $U(\lambda)$ teljesül, akkor $U\left(\frac{4\lambda+5}{22}\right)$ is teljesül.*

Bizonyítás. Legyen $\alpha = \frac{4\lambda+5}{22}$. Továbbá legyen $k = 3 - \frac{3}{4\alpha}$ és $l = 2 - \frac{4\lambda+1}{4\alpha}$, illetve $d = 1 - 2k - 2l$. Leellenőrizzük, hogy az 5.1 tétel feltételei teljesülnek ezekre az értékekre.

Mivel $\frac{1}{4} \leq \lambda < \frac{5}{18}$, ezért $\frac{4\cdot\frac{1}{4}+5}{22} \leq \alpha = \frac{4\lambda+5}{22} < \frac{4\cdot\frac{5}{18}+5}{22}$, vagyis $\frac{3}{11} \leq \alpha < \frac{5}{18}$.

Most belátjuk, hogy $0 < l \leq k \leq \frac{1}{3}$.

- $0 < l \Leftrightarrow 0 < 2 - \frac{4\lambda+1}{4\alpha} \Leftrightarrow 0 < 8\alpha - 4\lambda - 1 \Leftrightarrow 0 < \frac{32\lambda+40}{22} - 4\lambda - 1 = \frac{18}{22} - \frac{56}{22}\lambda$. Mivel $\lambda < \frac{5}{18}$, ezért $\frac{56}{22}\lambda < \frac{70}{99}$, így $\frac{18}{22} - \frac{56}{22}\lambda \geq \frac{18}{22} - \frac{70}{99} = \frac{1}{9} > 0$. Így teljesül $l > 0$ is.
- $l \leq k \Leftrightarrow 2 - \frac{4\lambda+1}{4\alpha} \leq 3 - \frac{3}{4\alpha} \Leftrightarrow 8\alpha - (4\lambda+1) \leq 12\alpha - 3 \Leftrightarrow 3 - (4\lambda+1) \leq 4\alpha$ $\Leftrightarrow 2 - 4\lambda \leq 4\alpha \Leftrightarrow 1 - 2\lambda \leq \frac{4\lambda+5}{11} \Leftrightarrow 11 - 22\lambda \leq 4\lambda + 5 \Leftrightarrow 6 \leq 26\lambda \Leftrightarrow \frac{3}{13} \leq \lambda$. Ez pedig teljesül, mert $\lambda \geq \frac{1}{4} \geq \frac{3}{13}$, így $l \leq k$ is fennáll.
- $k \leq \frac{1}{3} \Leftrightarrow 3 - \frac{3}{4\alpha} \leq \frac{1}{3} \Leftrightarrow \frac{8}{3} \leq \frac{3}{4\alpha} \Leftrightarrow 4\alpha \leq \frac{9}{8} \Leftrightarrow \alpha \leq \frac{9}{32}$. Mivel $\alpha < \frac{5}{18} < \frac{9}{32}$, ezért ez teljesül és így $k \leq \frac{1}{3}$ is.

Belátjuk most azt is, hogy $d \geq 0$:

$1 - 2k - 2l \geq 0 \Leftrightarrow 2k + 2l \leq 1 \Leftrightarrow 6 - \frac{3}{2\alpha} + 4 - \frac{4\lambda+1}{2\alpha} \leq 1 \Leftrightarrow 9 - \frac{4\lambda+4}{2\alpha} \leq 0 \Leftrightarrow$ $18\alpha - (4\lambda+4) \leq 0 \Leftrightarrow 4\lambda + 4 \geq 18\alpha \Leftrightarrow 4\lambda + 4 \geq \frac{18}{22}(4\lambda+5) \Leftrightarrow \lambda \geq \frac{1}{8}$, ami teljesül, mert tudjuk, hogy $\lambda \geq \frac{1}{4}$.

Az eddigiek alapján az (1) feltétel teljesül (például $d \leq 1$, mert $k, l \geq 0$).

A (2) feltétel is teljesül, mert $k + l \leq \frac{1}{3} + \frac{1}{3} < 1$.

A (3) feltétel következik abból, hogy $\frac{3}{11} \leq \alpha < \frac{5}{18}$.

A (4) feltétel következik a 4.3 tételből és abból, hogy $0 < l \leq k \leq \frac{1}{3}$.

Az (5) feltételhez először belátjuk, hogy $(2-d)\alpha \leq \frac{1}{2}$:

$(2-d)\alpha \le \frac{1}{2} \Leftrightarrow d\alpha \ge 2\alpha - \frac{1}{2} \Leftrightarrow (1-2k-2l)\alpha \ge 2\alpha - \frac{1}{2} \Leftrightarrow \frac{1}{2} \ge (1+2k+2l)\alpha \Leftrightarrow \alpha(1+2k+2l) = \alpha\left(1+6-\frac{3}{2\alpha}+4-\frac{4\lambda+1}{2\alpha}\right) \le \frac{1}{2} \Leftrightarrow \alpha\left(11-\frac{2\lambda+2}{\alpha}\right) \le \frac{1}{2} \Leftrightarrow 11\alpha - (2\lambda+2) \le \frac{1}{2} \Leftrightarrow \frac{4\lambda+5}{2} - (2\lambda+2) \le \frac{1}{2}$. (Ez utóbbi pedig egyenlőséggel teljesül.)

Ebből következik, hogy minden $0 \le \beta \le \alpha$-ra teljesül $d\beta \ge 2\beta - \frac{1}{2}$: ez azért van, mert $d\beta \ge 2\beta - \frac{1}{2} \Leftrightarrow \frac{1}{2} \ge (2-d)\beta$, és tudjuk, hogy mivel $d \le 1$, így $2-d > 0$, ezért $(2-d)\beta \le (2-d)\alpha \le \frac{1}{2}$.

Az (5) feltételben ha $0 \le \beta \le \frac{1}{4}$, akkor $U_{az}(\beta, d\beta)$ nyilván igaz, mert a 2.6 tétel miatt $\le \frac{1}{4}N$ él esetén a főprobléma mindig megoldható. Ha pedig $\frac{1}{4} < \beta \le \alpha$, akkor $U_{az}(\beta, d\beta)$ belátásához használjuk a 2.7 tételt: ez alapján elegendő, hogy $\frac{1}{4} < \beta < \frac{1}{2}$ és $d\beta \ge 2\beta - \frac{1}{2}$. Mivel $\alpha < \frac{1}{2}$, az előbbi nyilván teljesül, az utóbbit pedig most láttuk be. Ezzel az (5) feltételt minden β-ra beláttuk.

A (6) feltétel belátásához a 3.7 következmény miatt elegendő az alábbiakat belátnunk minden $k \le r \le 1-l$-re (használva, hogy $\frac{1}{4} \le \lambda < \frac{1}{2}$ és $U(\lambda)$):

(6a) $0 \le r\alpha, (1-r)\alpha \le \frac{1}{4}$,

(6b) $r\alpha \le \frac{1}{4} - (1-r)\alpha + \frac{1}{8} - \frac{1}{2}(1-r)\alpha = \frac{3}{8} - \frac{3}{2}(1-r)\alpha$,

(6c) $r\alpha \le \frac{1}{2}\lambda + \frac{1}{8} - \frac{1}{2}(1-r)\alpha$.

Ezek bizonyítása:

(6a)

$r\alpha, (1-r)\alpha \ge 0$ triviális.

Belátjuk, hogy $(1-l)\alpha \le \frac{1}{4}$:

$(1-l)\alpha \le \frac{1}{4} \Leftrightarrow \left(1-2+\frac{4\lambda+1}{4\alpha}\right)\alpha \le \frac{1}{4} \Leftrightarrow \left(\frac{4\lambda+1}{4\alpha}-1\right)\alpha \le \frac{1}{4} \Leftrightarrow \lambda + \frac{1}{4} - \alpha \le \frac{1}{4} \Leftrightarrow \lambda \le \alpha \Leftrightarrow \lambda \le \frac{4\lambda+5}{22} \Leftrightarrow \lambda \le \frac{5}{18}$, ami igaz.

Így minden $k \le r \le 1-l$ esetén $r\alpha \le (1-l)\alpha \le \frac{1}{4}$, és $(1-r)\alpha \le (1-k)\alpha \le (1-l)\alpha \le \frac{1}{4}$ (használva, hogy $l \le k$).

(6b)

$$r\alpha \le \frac{3}{8} - \frac{3}{2}\alpha + \frac{3}{2}r\alpha, \quad \forall k \le r \le 1-l$$

$$\Leftrightarrow \frac{3}{2}\alpha - \frac{3}{8} \le \frac{1}{2}r\alpha, \quad \forall k \le r \le 1-l$$

$$\Leftrightarrow \frac{3}{2}\alpha - \frac{3}{8} \le \frac{1}{2}k\alpha$$

$$\Leftrightarrow 12\alpha - 3 \le 4k\alpha$$

$$\Leftrightarrow \alpha(12-4k) \le 3$$

$$\Leftrightarrow \alpha\left(12 - 4\left(3 - \frac{3}{4\alpha}\right)\right) \le 3$$

$$\Leftrightarrow \alpha\left(12 - 12 + \frac{12}{4\alpha}\right) \le 3$$

$$\Leftrightarrow 3 \le 3$$

ami egyenlőséggel teljesül.

(6c)

$$r\alpha \le \frac{1}{2}\lambda + \frac{1}{8} - \frac{1}{2}\alpha + \frac{1}{2}r\alpha, \quad \forall k \le r \le 1-l$$

$$\Leftrightarrow \frac{1}{2}r\alpha \le \frac{1}{2}\lambda + \frac{1}{8} - \frac{1}{2}\alpha, \quad \forall k \le r \le 1-l$$

$$\Leftrightarrow \frac{1}{2}(1-l)\alpha \le \frac{1}{2}\lambda + \frac{1}{8} - \frac{1}{2}\alpha$$

$$\Leftrightarrow 4(1-l)\alpha \le 4\lambda + 1 - 4\alpha$$

$$\Leftrightarrow 4\left(1 - 2 + \frac{4\lambda+1}{4\alpha}\right)\alpha \le 4\lambda + 1 - 4\alpha$$

$$\Leftrightarrow \left(-4 + \frac{4\lambda+1}{\alpha}\right)\alpha \le 4\lambda + 1 - 4\alpha$$

$$\Leftrightarrow -4\alpha + 4\lambda + 1 \le 4\lambda + 1 - 4\alpha$$

ami egyenlőséggel teljesül.

Az 5.1 tétel miatt $U(\alpha) = U\left(\frac{4\lambda+5}{22}\right)$ teljesül. □

5.3. Tétel. *A főprobléma megoldható $M \le \frac{5}{18}N$ élre.*

Bizonyítás. Tekintsük a $(\lambda_n)_{n=0}^{\infty}$ sorozatot, melyet a következő rekurzió definiál: $\lambda_0 = \frac{1}{4}$, és minden $n \ge 1$-re $\lambda_n = \frac{4\lambda_{n-1}+5}{22}$.

Ekkor az alábbiakat vehetjük észre a (λ_n) sorozatról:

1. Minden tagja kisebb $\frac{5}{18}$-nál: az első tag $\frac{1}{4} < \frac{5}{18}$, és ha $\lambda_{n-1} < \frac{5}{18}$, akkor $\lambda_n = \frac{4\lambda_{n-1}+5}{22} < \frac{4\cdot\frac{5}{18}+5}{22} = \frac{5}{18}$.

2. A sorozat monoton nő és konvergál $\frac{5}{18}$-hoz: ennek belátásához elég azt látnunk, hogy a tagok $\frac{5}{18}$-tól vett távolsága minden lépésben legfeljebb a felére csökken, azaz minden $n \ge 1$-re $\frac{5}{18} - \lambda_n \le \frac{\frac{5}{18}-\lambda_{n-1}}{2}$. Ez pedig teljesül, mert $\lambda = \lambda_{n-1}$ és $\lambda' = \lambda_n$ esetén $\frac{5}{18} - \lambda' \le \frac{\frac{5}{18}-\lambda}{2} \Leftrightarrow 2\left(\frac{5}{18} - \frac{4\lambda+5}{22}\right) \le \frac{5}{18} - \lambda \Leftrightarrow \frac{5}{9} - \frac{4\lambda+5}{11} \le \frac{5}{18} - \lambda \Leftrightarrow \frac{7}{11}\lambda \le \frac{35}{198} \Leftrightarrow \lambda \le \frac{5}{18}$, ami teljesül.

Teljes indukcióval belátjuk, hogy minden $n \ge 0$-ra teljesül $U(\lambda_n)$. Nyilván $U(\lambda_0) = U(\frac{1}{4})$ teljesül a 2.6 tétel miatt, és ha $U(\lambda_{n-1})$ teljesül, akkor az 5.2 tétel miatt $U(\lambda_n)$ is (hiszen az előző állítások miatt $\frac{1}{4} \le \lambda_{n-1} < \frac{5}{18}$).

Ez mivel $\lambda_n \to \frac{5}{18}$, azt jelenti, hogy a főprobléma megoldható legfeljebb cN élre minden $c < \frac{5}{18}$ esetén. Mivel $\frac{5}{18}N$ nem lehet egész (hiszen N 2-hatvány), ezért ebből következik, hogy $U\left(\frac{5}{18}\right)$ is teljesül. □

Hivatkozások

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

[2] Preissmann, E. és Mischler, M., 2009. Seating couples around the King's table and a new characterization of prime numbers. The American Mathematical Monthly, 116(3), pp.268-272.

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

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