Egyéni kutatómunka 2.
Páronként diszjunkt vektorpárok keresése $\mathbb{F}_2^n$-ben előírt különbségsorozattal

Kovács Benedek

Témavezető: Csikvári Péter

2021.05.20.

Kérdésfelvetés, korábban elért eredmények

A 2020-as őszi félévi kutatómunkámban az alábbi sejtéssel foglalkoztam:

Sejtés (Balister, Győri, Schelp, 2008)

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 különbségek (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.

Kérdésfelvetés, korábban elért eredmények

Ezen sejtésnek az alábbi gyengített változatát vizsgáltam, melyre az igenlő választ igyekeztem minél nagyobb M értékekre belátni:

Főprobléma

Legyenek $n \geq 2$, $N = 2^n$ és $M \leq \frac{1}{2}N - 2$ előre megadott egészek. Igaz-e, hogy tetszőleges $d_1, d_2, \ldots, d_M \in \mathbb{F}_2^n$ 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 $a_i - b_i = d_i$?

Legfőbb eredményem az volt, hogy az "igen" választ beláttam $M \leq \frac{5}{18}N$ esetén egy továbbfejlesztett mohó módszer használatával.

Új eredmények összefoglalása

Az alábbi két fő eredményt értem el ebben a félévben a probléma kapcsán:

- A főproblémát $M \leq \frac{9}{32}N = 0{,}28125N$ esetén is megoldottam.
- Abban az esetben, amikor minden megadott különbség csupa különböző, $M \leq \frac{1}{2}N - O(N^{5/6})$ különbségre is megoldottam a feladatot.

A probléma megoldása $M \leq \frac{9}{32}N$ esetén

$T(k, l, d)$ definíciója

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

Tétel (az előző félévben beláttam)

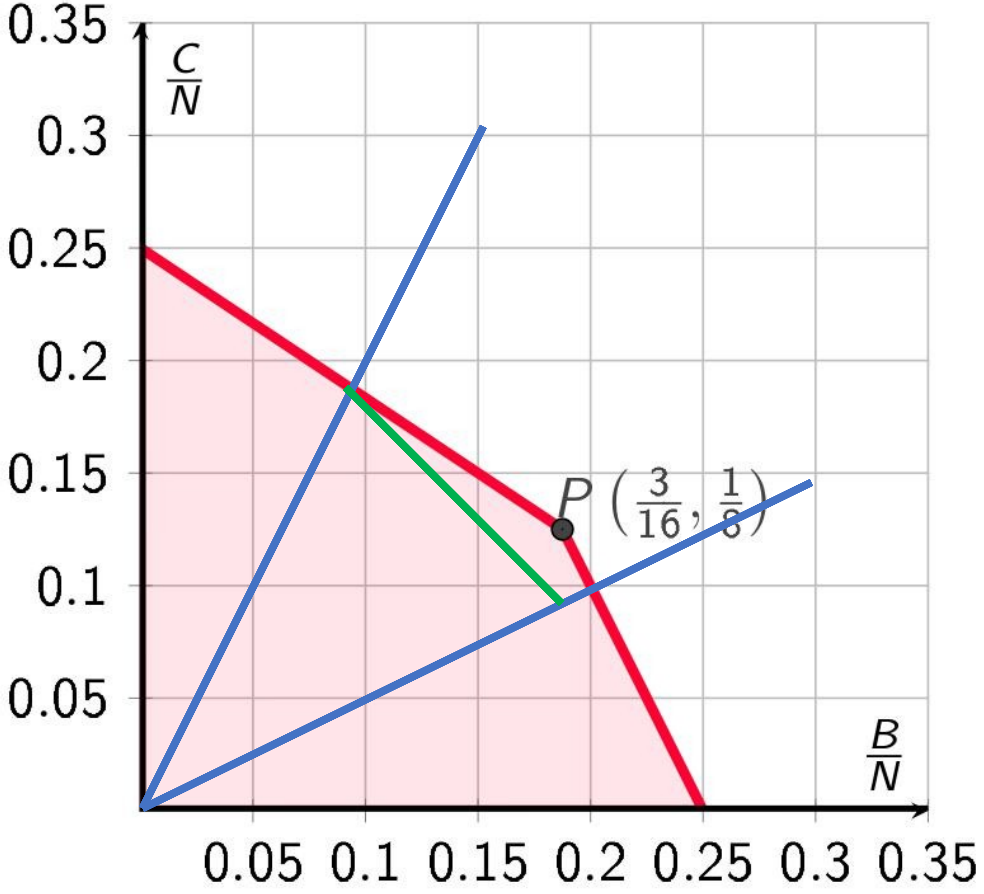
$0 < l \leq k \leq \frac{1}{3} \Rightarrow T(k, l, 1 - 2k - 2l)$

Tétel (új eredmény)

$0 < k \leq \frac{1}{3} \Rightarrow T(k, k, 1 - 2k)$

A probléma megoldása $M \leq \frac{9}{32}N$ esetén

Az új tétel alapján $T\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$ teljesül. Idézzük fel az alábbi ábrát (B a 0-val kezdődő különbségek száma, C az 1-gyel kezdődőeké, és a piros tartományt oldja meg a korábbi háromrészes mohó algoritmusunk):



Csupa különböző különbségek esete

Tétel

Létezik olyan $a > 0$ konstans és $n_0 \in \mathbb{N}$, melyre $M \leq \frac{1}{2}N - aN^{5/6}$ és $n \geq n_0$ esetén a főprobléma megoldható, ha minden d_i páronként különböző.

A megoldás vázlatos menete:

- Feltehetjük, hogy az első k koordinátájuk szerint nézve a megadott M db különbség közel egyenlően oszlik el a 2^k lehetőség között.
- Használjunk egy, az előző félévi háromrészes mohó módszert általánosító eljárást, melyben minden különbséghez a hozzá tartozó vektorpárt úgy választjuk ki mohón, hogy mindkét vektornak megmondjuk, hogy mi legyen az első k koordinátája.

Csupa különböző különbségek - automorfizmus létezése

Állítás

Ha $k \geq 1$ és $M \geq 2^{2k}$ egészek, és $u_1, \ldots, u_M \in \mathbb{F}_2^n \setminus \{0\}$ páronként különbözők, akkor léteznek $a_1, \ldots, a_n \in \mathbb{F}_2^n$ lineárisan független vektorok, melyekre minden $c_1, \ldots, c_k \in \mathbb{F}_2$ esetén
$\left| d_{c_1,\ldots,c_k}(a_1, \ldots, a_k) - \frac{1}{2^k} M \right| \leq \sqrt{M}\sqrt{1 - \frac{1}{2^k}}$, ahol
$d_{c_1,\ldots,c_k}(a_1, \ldots, a_k) := |\{i : 1 \leq i \leq M, \langle u_i, a_j \rangle = c_j \ \forall 1 \leq j \leq k\}|$.

Bizonyítás

Charbit et al. (2007) $k = 1$-re való bizonyításához hasonlóan.
$$|d_{c_1,\ldots,c_k}(a_1, \ldots, a_k) - \frac{1}{2^k} M|^2 \leq \sum_{c_1,\ldots,c_k \in \mathbb{F}_2} |d_{c_1,\ldots,c_k}(a_1, \ldots, a_k) - \frac{1}{2^k} M|^2,$$
és a jobb oldali kifejezésnek kiszámítjuk a várható értékét, ami éppen $M \left(1 - \frac{1}{2^k}\right)$-nak adódik.

Csupa különböző különbségek - a mohó eljárás

Legyen $(\mathbb{F}_{2^k})^* = \langle g \rangle$. Ekkor $\mathbb{F}_{2^k} = \{1, g, g^2, ..., g^{2^k-2}, 0\}$.
Ha $a, b \in \mathbb{F}_2^k$ és $c \in \mathbb{N}$, akkor nevezzük (a, b, c) típusú lépésnek az alábbi folyamatot: a megadott d_i különbségeink közül c darab olyanhoz, amelyhez még nem rendeltünk a_i és b_i vektorokat, és amelynek kezdete $a - b \in \mathbb{F}_2^k$, sorban egyesével hozzárendelünk ilyen a_i-t és b_i-t tetszőleges módon úgy, hogy a_i kezdete a, b_i kezdete pedig b legyen. Ez a mohó folyamat minden esetben elvégezhető, ha teljesül az alábbi feltétel:

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

ahol a lépés megkezdése előtt felhasznált a kezdetű vektorok számát f_a, a b kezdetűekét f_b jelöli.

Csupa különböző különbségek - a mohó eljárás

Legyen $d = \left[2^{n/6}\right]$ és $k = \left[\frac{1}{3}n\right]$, és végezzük el az alábbi lépéseket:

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