

Presentations

Schedule of presentation dates is posted
(see course webpage)

SIGNUP to discuss your presentation with
me and your group by Mar 1
(see google doc)

Last Class

Randomised CC LB of $\Omega(n)$ for Inner Product

Today

- Slicker randomised CC LB for IP (BNS)
- NOF communication:
 - Defn, cylinder intersections
 - Important Functions
 - Applications of NOF CC in addition combinatorics

Slightly slicker proof of lower Bound for randomized cc via discrepancy (that generalizes to NOF)

Called "BNS" method after seminal paper by Babai, Nisan, Szegedy introducing NOF cc and this method

Theorem [BNS bound]

Let $f: X \times Y \rightarrow \{-1, 1\}$, μ = unif distrib over $X \times Y$

Then $\forall R = S \times T \quad \text{Disc}_{\mu}(R, f)^2 \leq \mathbb{E}_{Y, Y'} \left| \mathbb{E}_X M_f(x, y) \cdot M_f(x', y') \right|$

Theorem [BNS bound] $R = S \times T$

$$\text{Disc}_\mu(R, f)^2 \leq \mathbb{E}_{Y, Y'} \left| \mathbb{E}_X M_f(x, Y) M_f(x, Y') \right|, \quad \mu = \text{uniform distrib over } X \times Y$$

Proof ($\mu = \text{unif. distrib}$)

$$\text{Disc}_\mu(f, S \times T) = \left| \mathbb{E}_{X, Y} 1_S(x) 1_T(y) M_f(x, y) \right|$$

$$\text{so } \text{Disc}_\mu(f, S \times T)^2 = \left(\mathbb{E}_{X, Y} 1_S(x) 1_T(y) M_f(x, y) \right)^2$$

$$= \left(\mathbb{E}_X 1_S(x) \mathbb{E}_Y 1_T(y) M_f(x, y) \right)^2$$

$$\leq \mathbb{E}_X \left(1_S(x) \mathbb{E}_Y 1_T(y) M_f(x, y) \right)^2$$

$$= \mathbb{E}_X \left(\mathbb{E}_Y 1_B(y) M_f(x, y) \right)^2$$

$$= \mathbb{E}_X \left(\mathbb{E}_{Y, Y'} 1_B(y) 1_B(y') M_f(x, y) M_f(x, y') \right)$$

$$= \mathbb{E}_{Y, Y'} 1_B(y) 1_B(y') \left(\mathbb{E}_X M_f(x, y) M_f(x, y') \right)$$

$$\leq \mathbb{E}_{Y, Y'} \left| \mathbb{E}_X M_f(x, Y) M_f(x, Y') \right|$$

Cauchy Schwartz
 $(\mathbb{E}[Z])^2 \leq \mathbb{E}[Z^2]$

replace S by $S = \{0, 1\}^n$

□

Theorem [BNS bound] $R = S \times T$

$$\text{Disc}_\mu(R, f)^2 \leq \mathbb{E}_{y, y'} \left| \mathbb{E}_x M_f(x, y) M_f(x, y') \right|, \quad \mu = \text{uniform distrib over } X \times Y$$

Theorem 2 $\text{Disc}_\mu(\text{IP}_n, S \times T) \leq 2^{-n/2}$ [and thus by Theorem 1, $D_\mu^{1/3}(\text{IP}_n) = \Omega(n)$]

PE:

$$\text{Disc}_\mu(\text{IP}_n, S \times T)^2 \leq \mathbb{E}_{y, y'} \left| \mathbb{E}_x M_{\text{IP}}(x, y) M_{\text{IP}}(x, y') \right| \quad [\text{By BNS Bound}]$$

$$= \Pr(y = y') = 2^{-n}$$

$$\left[\begin{array}{l} \text{orthogonality of rows of } H_n: \\ \mathbb{E}_x M_{\text{IP}}(x, y) M_{\text{IP}}(x, y') = \begin{cases} 0 & \text{if } y \neq y' \\ 1 & \text{if } y = y' \end{cases} \end{array} \right]$$

$$\therefore \text{Disc}_\mu(\text{IP}_n) = 2^{-n/2}$$

□

The BNS Bound $\text{Disc}_\mu(R_1 f)^2 \leq \mathbb{E}_{Y, Y'} \left| \mathbb{E}_X M_f(x, Y) M_f(x, Y') \right|$ holds

for any product distribution μ

($\mu = \mu_1 \times \mu_2$ where μ_1 is distrib on X , μ_2 on Y)

with same prob.

Multiparty CC

There are 2 different models when k (# players) ≥ 3
(they coincide when $k=2$)

(1) NIH (Number IN Hand)

Player 1 gets	x_1	} Typically $ x_1 = x_2 = x_3 $
2	x_2	
3	x_3	

(2) NOF (Number on Forehead)

Player 1 sees	x_2, x_3
2 "	x_1, x_3
3 "	x_1, x_2

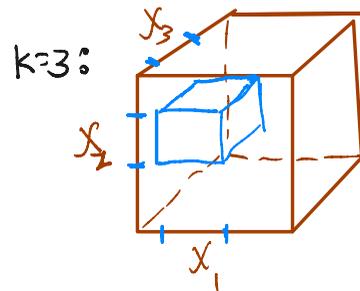
NIH Protocols $k \geq 2$

A k -party NIH protocol Π for $f(x_1, \dots, x_k)$, each $|x_i| = n$

- Player $i \in [k]$ sees x_i
- Just like 2-party case, a k -party Π specifies
 - which player's turn it is to speak (all msgs are broadcast to all players)
 - $F \times N$ at nd r (assuming Player i speaks) depends on transcript + x_i

• Deterministic k -party CC: $D_k^{\text{NIH}}(f)$

Deterministic Π for $f(x_1, \dots, x_k)$ partitions $x_1 \times \dots \times x_k$ into monochromatic k -dimensional rectangles (tensors)



- We can also define randomized NIH and Distributional complexity wrt. distrib μ over $x^1 \times \dots \times x^k$ (analogous to $k=2$)

We'll mostly focus on NMF CC due to its many applications, including:

* (1) Additive Combinatorics

(2) ACC Lower bounds

(3) Proof Complexity Lower Bounds

* (4) Matrix Multiplication

* : Presentation Topic

* Today

NOF Protocols

- A k -party NOF protocol Π for $f(x_1, \dots, x_k)$, each $|x_i| = n$
- Player $i \in [k]$ sees all x_j except for x_i
 - Just like 2-party case, a k -party Π specifies
 - which player's turn it is to speak (all msgs are broadcast to all players)
 - F_x^i at rnd r (assuming Player i speaks) depends on: transcript so far, and inputs $x^{-i} \stackrel{d}{=} \{x_1, \dots, x_{(i-1)}, x_{(i+1)}, \dots, x_k\}$

Deterministic k -party CC : $D_k(f)$

Distributional complexity wrt. distrib μ over x_1, x_2, \dots, x_k : $D_k^{\epsilon, \mu}(f)$

NOF Protocols

Defn. Let $X = X_1 \times X_2 \times \dots \times X_k$ (input space)

A cylinder C_i in i^{th} coordinate is a subset of X that doesn't depend on i^{th} coordinate

ie. $(x_1, \dots, x_i, \dots, x_k) \in C_i \Rightarrow \forall x'_i \in X_i: (x_1, \dots, x'_i, \dots, x_k) \in C_i$

(Easy) Proposition If C_i, C_i' are cylinders in i^{th} coord, then so is $C_i \cap C_i'$

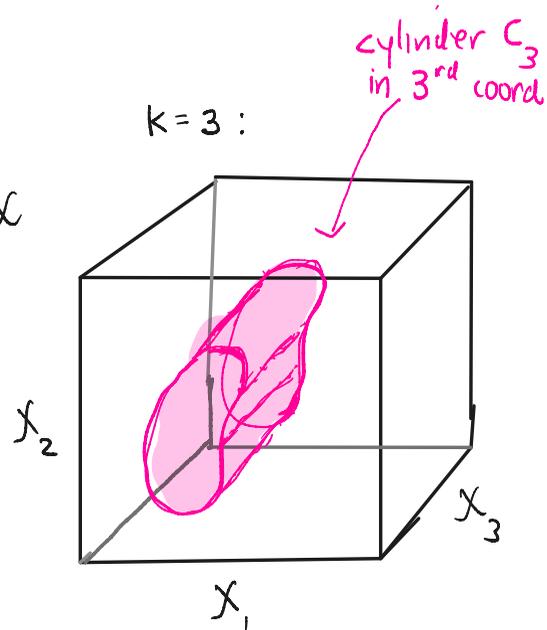
Defn A cylinder intersection is a subset

$C \subseteq X$ s.t. $C = C_1 \cap C_2 \cap \dots \cap C_k$, where $C_i =$ cylinder intersect in i^{th} coord.

Claim Let Π be a cost c NOF protocol.

then Π induces a partition of X into 2^c cylinder intersections

(pf by induction on c , using Proposition above)



Analogy of
2-party
partition
into rectangles

Important NOF Functions

(1) gIP (generalized Inner Product)

Input $\vec{x}_1, \dots, \vec{x}_k$ (Player $j \in [k]$ sees all $x_{ji}, j \neq i$)

$$\text{gIP}(\vec{x}_1, \dots, \vec{x}_k) = 1 \text{ iff } \sum_{i=1}^n x_{1i} \wedge \dots \wedge x_{ki} = 1 \pmod{2}$$

(ie output is 1 iff size of intersection $x_1 \wedge \dots \wedge x_k = 1 \pmod{2}$)

(2) k-player Disjointness

$$\text{DISJ}(x_1, \dots, x_k) = 1 \text{ iff } \sum_{i=1}^n x_{1i} \wedge \dots \wedge x_{ki} \geq 1$$

← easy for nondet protocol

- For $k = \text{constant}$ both gIP, DISJ require randomized comm. $\Omega\left(\frac{n}{4^k}\right)$

Important NOF Functions

(3) Exactly-N function ($k=3$)

Each player $i \in \{1, 2, 3\}$ gets a number $x_i \in [N]$ $\left(\begin{array}{l} |x_i| = n \\ N = 2^n \end{array} \right)$
Output 1 iff $x_1 + x_2 + x_3 = N$



Has $O(1)$ -cost randomized NOF protocol!

Longstanding open problem: Best deterministic NOF protocol?

Deterministic NOF cc of Exactly-N ($k=3$) is
essentially equivalent to corners problem in additive
combinatorics

Important NOF Functions

(3) Exactly-N function ($k=3$)

Each player $i \in \{1, 2, 3\}$ gets a number $x_i \in [N]$

Output 1 iff $x_1 + x_2 + x_3 = N$

$$\left(\begin{array}{l} |x_i| = n \\ N = 2^n \end{array} \right)$$

Randomized protocol

Player 1 sees x_2, x_3 and computes $x_2 + x_3$

Player 2 sees x_1 and computes $N - x_1$

Players 1, 2 run 2-party randomized EQ protocol
to check if $N - x_1 = x_2 + x_3$

Cost = $o(1)$!

NOF model: some surprising UPPER BOUNDS

$$(1.) \text{EQ}(x_1, \dots, x_k) = 1 \text{ iff } x_1 = \dots = x_k$$

Note $k=2$: def CC is $\Omega(n)$

But easy for $k > 2$!

Player 1: check if $x_2 = \dots = x_k$
If not halt + output 0
or send 1

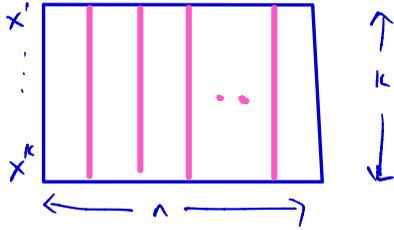
Player 2: check if $x_1 = x_3$
output 1 if equal + halt
or output 0 + halt

$$(2.) \underset{\uparrow}{D^k}(\text{GIP}_n^k) = O\left(\frac{kn}{2^k}\right) \quad [\text{Grolmusz '94}]$$

k Player
Determin. NOF

$$D^k(\text{gIP}_n^k) = O\left(\frac{kn}{2^k}\right)$$

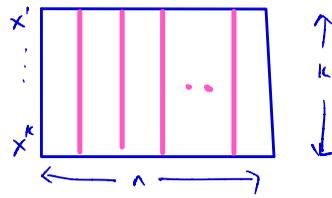
Protocol:



← Input to gIP_n^k

- Divide columns into blocks of size $2^{k-1} - 1$
- Compute gIP for every block + then sum results mod z to get answer
 $\text{cost} \approx \frac{n}{2^k} \cdot \text{cost-per-block}$

$$D^k(\text{gIP}_n^k) = O\left(\frac{kn}{2^k}\right)$$

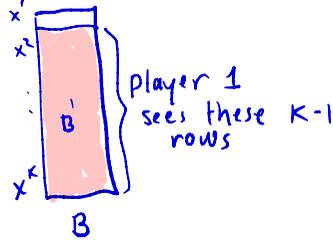


← Input to gIP_n^k

Protocol:

• Protocol for a block B :

1. P1 finds a vector $\alpha \in \{0,1\}^k$ that is not in $\text{columns}(B)$, + sends to other players



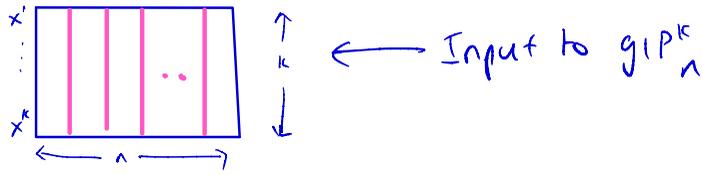
By PHP \exists vector α' not in $\text{columns}(B')$
 extend $\alpha' \rightarrow \underbrace{1 \alpha}_{\alpha}$

2. If $\alpha =$ all-1 vector \Rightarrow output \neg

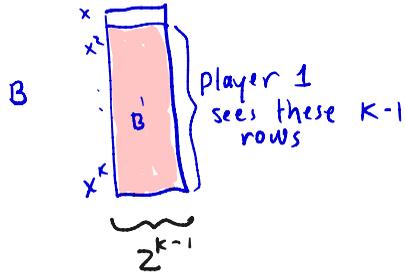
Else α contains at least one 0. Players want to compute # of all-1 column vectors in B
 assume α has l 0's and $k-l$ 1's (for some l)

Let $y_i =$ # column vectors in B with i 0's, $n-i$ 1's

$$D^k(\text{gIP}_n^k) = O\left(\frac{kn}{2^k}\right)$$



Protocol:



$$\text{gIP}(B) = \# \text{ all-1 columns in } B \pmod{2}$$

Suppose α has l 0's, $k-l$ 1's: $\underbrace{0000\dots 0}_l \underbrace{11\dots 1}_{k-l}$

permute rows so all 0's then all 1's

$\forall i \leq l: Y_i \stackrel{d}{=} \# \text{ column vectors of form } \underbrace{0\dots 0}_i \underbrace{11\dots 1}_{k-i}$

$Z_i \stackrel{d}{=} \# \text{ column vectors of form } \underbrace{000\dots 0}_{i-1} \times \underbrace{111\dots 1}_{k-i}$

Claim $Z_i = Y_{i-1} + Y_i \leftarrow \text{player } i \text{ can compute } Z_i!$

Π : • Players $i \in [1, \dots, l]$ compute + send Z_i } From Z_1, \dots, Z_l, Y_l they can compute Y_0
 • They all know $Y_l = 0$

Cost: $\frac{n}{2^k} \cdot k$

(Explicit) NOF Lower Bounds - What is known

1. GIP : LB $\Omega\left(\frac{n}{4^k}\right)$ randomized k -player NOF

breaks down when $k > \log n$

* No explicit LBs in NOF model for $k > \log n$

We'll prove slightly weaker LB due to RNS Babai, Nisan, Szegedy

2. k -player Disjointness : LB $\Omega\left(\frac{n}{4^k}\right)$ randomized k -player

3. What about functions that are "easy" for randomized NOF ?
Like Exactly N ?

↑ Many open questions here in NOF cc are actually equivalent to fundamental problems in additive combinatorics

(Explicit) NOF Lower Bounds - What is known

3. What about functions that are "easy" for randomized NOF?
Like Exactly N?

Recent breakthrough LBs for deterministic NOF $k=3$

- (i) "Strong Bounds for 3-progressions" [Kelley, Mehta FOCS'23]
↳ gives $\Omega(n^\epsilon)$ LB on NIH Promise $\epsilon > 0$ $k=3$
- (ii) "Explicit Separations between randomized + deterministic NOF Comm."
[Kelley, Lovett, Mehta STOC'24]
- (iii) "Quasipoly LBs for the corners theorem"
[Jaber, Liu, Lovett, Ostuni, Sawhney '25]

↳ gives $\Omega(n^\epsilon)$ deterministic NOF LB for Exactly N $k=3$

Some Equivalences between Additive Comb's Problems + NOF CC Problems

[we will do case of $k=3$ but equivalences hold $\forall k \geq 3$]

① 3-AP Problem : What is max size $r_3(N)$ of a subset $S \subseteq [N]$ s.t. S does not contain a 3AP?

$$\text{3AP: } (x, x+y, x+2y) \in [N]^3$$



① 3-AP Coloring Problem : What is min $c_3(N)$ s.t. $[N]$ can be partitioned into $c_3(N)$ subsets s.t. no subset contains a 3AP?

$$\text{3AP: } (x, x+y, x+2y) \in [N]^3$$

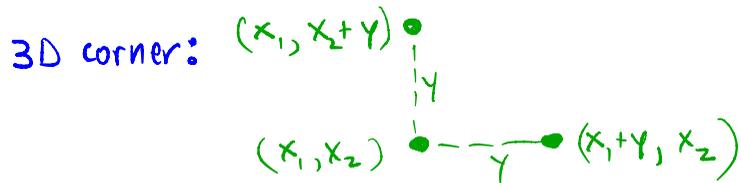


* It is known that ① \cong ① $\left(c_3(N) \approx \frac{N}{r_3(N)} \right)$

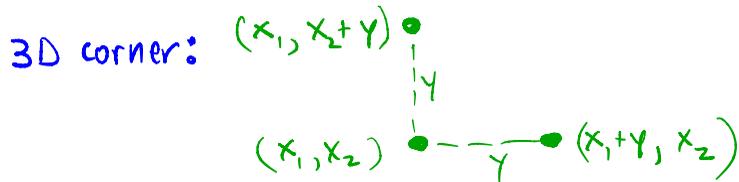
Some Equivalences between Additive Comb's Problems + NOF CC Problems

[we will do case of $k=3$ but equivalences hold $\forall k \geq 3$]

② Corners Problem: What is max size $r_2^{\leq}(N^2)$ of $S \subseteq [N]^2$ s.t. S does not contain a 3D corner?



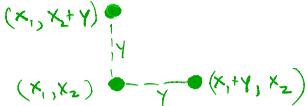
② Corners Problem ^{Coloring}: What is min $c_2^{\leq}(N)$ st $[N]^2$ can be partitioned into $c_2^{\leq}(N)$ subsets s.t. no subset contains a 3D corner?



Again it is known that $c_2^{\leq}(N^2) \approx N / r_2^{\leq}(N^2)$

Some Equivalences between Additive Comb's Problems + NOF CC Problems

[we will do case of $k=3$ but equivalences hold $\forall k \geq 3$]

Additive Combinatorics Problem	Equivalent Comm. Complexity Problem
<p>① <u>3-AP Coloring Problem</u></p> 	<p>①' <u>NIH Promise EQ, $k=3$</u></p> <p>Player 1: x Player 2: y Player 3: z</p> <p>} Promise: x, y, z is a 3AP</p> <p>Decide if $x=y=z$</p>
<p>② <u>Corners Coloring Problem</u></p> 	<p>②' <u>NOF Exactly N $k=3$</u></p> <p>Player 1: y, z Player 2: x, z Player 3: x, y</p> <p>Decide if $x+y+z = N$</p>

Also: $CC(2') \leq CC(1')$ (So LBs for ②' \Rightarrow LBs for ①')

So LBs for ② \Rightarrow LBs for ①

State of the Art: 3AP-Free sets

Behrend :
1946

\exists a 3AP free subset of $[N]$ of size $N/\exp(2.25\sqrt{\log N})$
ie $r_3(N) \geq N/\exp(2.25\sqrt{\log N})$

$\therefore C_3(N) \leq \exp(2.25\sqrt{\log N})$
 \swarrow equivalently \exists deterministic NIT protocol for
Promise $\in \mathbb{Q}$ $k=3$ of cost $\log(C_3(N)) = O(\sqrt{\log N}) = O(n^{1/2})$

Kelley, Mehta
2023

(Huge exponential improvement over previous results)

$$r_3(N) \leq \frac{N}{\exp(c \log N^{1/2})}$$

$$\therefore C_3(N) \geq \exp(c \log N^{1/2})$$

\swarrow equivalently any det. NIT protocol
for Promise $\in \mathbb{Q}$ $k=3$ requires cost $\Omega(n^{1/2})$

State of the Art: Corner Free sets

Behrend :
1946

\exists a corner-free subset of $[N^2]$ of size $N/\exp(c\sqrt{\log N})$

$$\text{ie } r_3(N) \geq N/\exp(c\sqrt{\log N})$$

$$\therefore C_3(N) \leq \exp(\sqrt{\log N})$$

← equivalently there is a deterministic NOF protocol for exactly N , $k=3$ of cost $O(n^{1/2})$

Best improvement : $c \sim 1.8$ [Linial, Shraibman '21] [Green '21]
to constant c

Jaber, Liu,
Lovett, Ostuni,
Sawhney
2025

$$r_2^<(N^2) \leq N^2/\exp(c(\log N)^{1/200})$$

$$\therefore C_2^<(N^2) \geq \Omega(n^{1/200})$$

← equivalently any NOF protocol for exactly N $k=3$ has cost $\Omega(n^{1/200})$

① 3-AP Problem ^{Coloring}



①' NIH Promise EQ, k=3



Player 1: x
Player 2: y
Player 3: z

} Promise: x, y, z
is a 3AP

Decide if $x=y=z$

\Rightarrow : Let $S_1, \dots, S_{c_3(N)}$ be a partition of $[N]$ into $c_3(N)$ subsets, all S_i 3AP free.

Protocol for NIH promise EQ (on input (x, y, z)):

P1 sends $i \in C_3(N)$ s.t. $x \in S_i$

P2: sends 1 iff $y \in S_i$

P3: send 1 iff $z \in S_i$

output 1 iff P2, P3 both send 1.

Since (x, y, z) is a 3AP, they are in same set S_i iff $x=y=z$
(because each S_i contains no nontrivial 3AP)

Complexity of protocol: $\log(c_3(N)) + 2$

① 3-AP Problem ^{Coloring}



①' NIH Promise $\in \mathbb{Q}$, $k=3$



Player 1: x
Player 2: y
Player 3: z } Promise: x, y, z
is a 3AP

Decide if $x=y=z$

\Leftarrow : Let Π be a NIH protocol for Promise $\in \mathbb{Q}$.

Using Π , we define a coloring (=partition) of $[N]$:

Color(x) $\stackrel{d}{=} \text{Transcript of } \Pi \text{ on } (x, x, x)$

We claim $\forall S \subseteq [N]$ st. all elements in S have same color (transcript),

S contains no 3AP:

Assume otherwise, so $x, \overbrace{x+\delta}^y, \overbrace{x+2\delta}^z$ have same transcript $S > 0$

Then since protocol is NIH, $\Pi(x, y, z) = \Pi(x, x, x) = \Pi(y, y, y) = \Pi(z, z, z)$
by rectangular prop of Π

But then protocol is incorrect since $(x, x, x), (y, y, y), (z, z, z)$
are 1-inputs but (x, y, z) is a 0-input

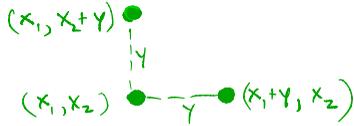
②

Coloring
Corners Problem



②'

NOF Exactly N k=3



Player 1: y, z

Player 2: x, z

Player 3: x, y

Decide if $x+y+z = N$

\Rightarrow : Assume $[N]^2$ has a partition (coloring) into $c_2^{\leq}(N)$ corner-free subsets.
 Consider the inputs: $\{(x, y), (x, y+d), (x+d, y)\}$, $d = N - x - y - z$
 They have same color iff $d=0$ iff $N = x+y+z$

Protocol For Exactly N on (x, y, z) :

Player 3 (sees x, y): sends color (x, y)

Player 2 (sees x, z): sends 1 iff color $(x, y) = \text{color}(x, y+d)$

Player 1 (sees y, z): sends 1 iff color $(x, y) = \text{color}(x+d, y)$

output 1 iff Players 2, 3 both send 1.

Complexity of protocol = $\log(c_2^{\leq}(N)) + 2$

$N-x-z$

$N-y-z$

(2)

Coloring
Corners Problem



(2')

NOF Exactly N $k=3$

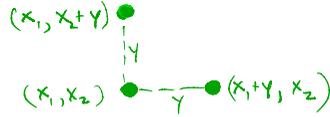
Player 1: y, z

Player 2: x, z

Player 3: x, y

Decide if $x+y+z = N$

$$|x| = |y| = |z| = n = \log N$$



\Leftarrow : Let Π be a c -bit protocol for Exactly N .

Using Π we give a coloring of $[N]^2$ s.t. each color class/partition is corner-free.

$\text{Color}(x, y) := \text{Transcript of } \Pi \text{ on } (x, y, N-x-y)$ \leftarrow # colors = 2^c

Claim: Each color class is corner free.

If not, then $\exists x, y, d > 0$ s.t. $(x, y), (x+d, y), (x, y+d)$ have same color

So $(x, y, N-x-y), (x+d, y, N-x-y-d), (x, y+d, N-x-y-d)$ have same transcript

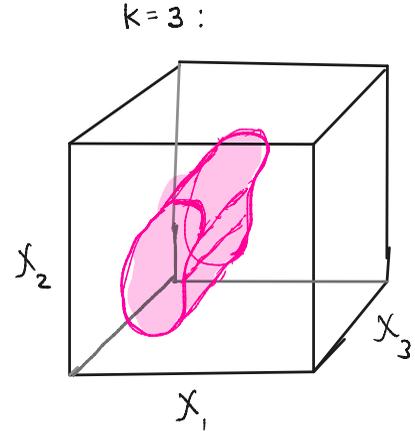
$\therefore (x, y, N-x-y-d)$ has same transcript also (By cylinder intersection property of Π)

NOF Lower Bounds via Discrepancy [BNS]

Defn. Let $X = X_1 \times X_2 \times \dots \times X_k$ (input space)

A cylinder C_i in i^{th} coordinate is a subset of X that doesn't depend on i^{th} coordinate

ie. $(x_1, \dots, x_i, \dots, x_k) \in C_i \Rightarrow \forall x'_i \in X_i: (x_1, \dots, x'_i, \dots, x_k) \in C_i$



Defn A cylinder intersection is a subset

$C \subseteq X$ s.t. $C = C_1 \cap C_2 \cap \dots \cap C_k$, where $C_i =$ cylinder intersect in i^{th} coord.

Claim Let Π be a cost c NOF protocol.

then Π induces a partition of X into 2^c cylinder intersections

Analog of
2-party
partition
into rectangles

\therefore If Π is a NOF protocol for $f: X_1 \times X_2 \times \dots \times X_k \rightarrow \{0,1\}$
 then Π induces a partition of X into 2^c f -monochromatic
 cylinder intersections

Defn (Discrepancy for cylinder intersections)

Let $f: X \rightarrow \{\pm 1\}$, and cylinder intersection $C: X \rightarrow \{0,1\}$

$$\text{Disc}_\mu(f, C) = \left| \mathbb{E}_{(x_1, \dots, x_k) \sim \mu} [f(x_1, \dots, x_k) C(x_1, \dots, x_k)] \right|$$

$$\text{Disc}_\mu(f) = \max_C \text{Disc}_\mu(f, C)$$

same as
 Defn of
 $\text{Disc}(f, R)$
 but now
 over cylinder
 intersections

Lemma $D_{\frac{\epsilon}{k}}^{\epsilon, \mu}(f) \geq \log \left(\frac{1 - 2\epsilon}{\text{Disc}_\mu(f)} \right)$

\nwarrow
 Distrib. cc of k -player
 deterministic NOF of f

Proof same
 as for
 Disc over
 Rectangles

Theorem Let $\mu =$ unif distribution on X .

$$D_{\frac{1}{k}}^{\frac{1}{3}, \mu}(g_{IP_n}) = \Omega\left(\frac{n}{4^k}\right)$$

Main Lemma $\text{Disc}_{\mu}(g_{IP_n}) \leq \exp(-n/4^k)$



Proof is very similar to our "BNS"

proof of 2-player lower bound for IP_n

But now we apply Cauchy Schwartz (Jensen's Ineq)

$k-1$ times. Each time we lose a factor of ~ 4
in the LB.