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)

Today

1. Finish connections between NOF CC and additive combinatorics

2. Discrepancy LB method for NOF:
   - → BNS method generalizes to NOF
   - → Discussion of DISJ_k LB (high level only)

3. Introduction to Lifting

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)

Today

1. Finish connections between NOF CC and additive combinatorics

2. Discrepancy LB method for NOF:
   - → BNS method generalizes to NOF
   - → Discussion of DISJ_k LB (high level only)

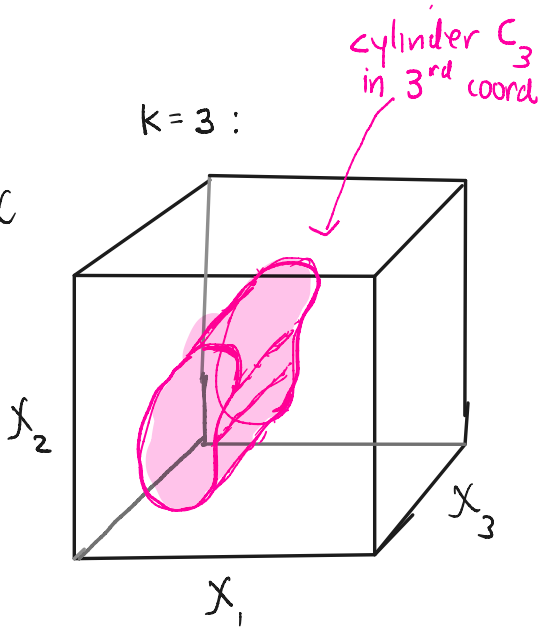
3. Introduction to Lifting

NOF Protocols

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

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

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



(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. $C = C_1 \cap C_2 \cap \cdots \cap C_k$, 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)

Analog of 2-party partition into rectangles

NOF Communication Complexity

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, Meka FOCS '23]
↖ gives $\Omega(n^2)$ LB on NIH PromiseEQ $k=3$

(ii) "Explicit separations between randomized & deterministic NOF Comm."
[Kelley, Lovett, Meka STOC '24]

(iii) "Quasipoly LBs for the corners theorem"
[Jaber, Liu, Lovett, Ostuni, Sawhney '25]

↖ gives $\Omega(n^2)$ deterministic NOF LB for ExactlyN $k=3$

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 ?

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 ?

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

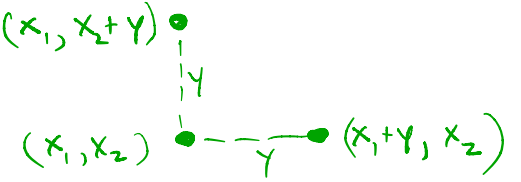
* It is known that ① $\cong$ ① $\left(c_3(N) \approx \frac{N}{r_3(N)} \right)$

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

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

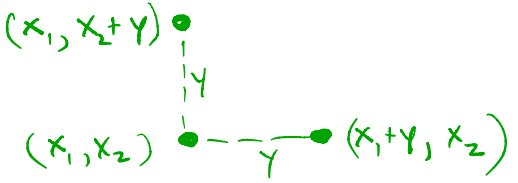
(2) **Corners Problem**: What is max size $r_2^<(N^2)$ of $S \subseteq [N]^2$ s.t. S does not contain a 3D corner?

3D corner:



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

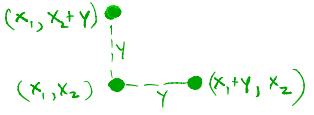
3D corner:



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

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
(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 $x=y=z$
(2) Corners Problem (Coloring) 	(2') NOF ExactlyN $k=3$ Player 1 : y, z Player 2 : x, z Player 3 : x, y Decide if $x+y+z=N$

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 $r_3(N) \geq N/\exp(2.25\sqrt{\log N})$

$\therefore\ c_3(N) \leq \exp(2.25\sqrt{\log N})$

↖ equivalently $\exists$ deterministic NIH protocol for Promise EQ $k=3$ of cost $\log(c_3(N)) = O(\sqrt{\log N}) = O(n^{1/2})$

Kelley, Meka 2023 (Huge exponential improvement over previous results)

$$r_3(N) \leq \frac{N}{\exp(c \log N^{1/12})}$$

$$\therefore\ c_3(N) \geq \exp(c \log N^{1/12})$$

↖ equivalently any det. NIH protocol for Promise EQ $k=3$ requires cost $\Omega(n^{1/12})$

State of the Art: Corner Free sets

Behrend : 1946

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

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 ExactlyN, $k=3$ of cost $O(n^{1/2})$

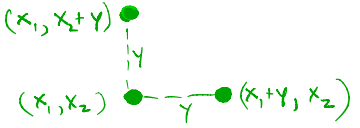
Best improvement to constant c : $c \sim 1.8$ [Linial, Shraibman '21] [Green '21]

Jaber, Liu, Lovett, Ostuni, Sawhney 2025

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

$\therefore\ c_2^<(N^2) \geq \Omega(n^{1/200})$ ← equivalently any NOF protocol for ExactlyN $k=3$ has cost $\Omega(n^{1/200})$

(2) Corners Problem (Coloring) $\approx\approx$ (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 $c_2^<(N)$ 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)

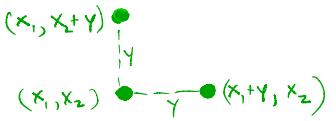
Player 2 (sees x, z): sends 1 iff color (x, y) = color $(x, y+d)$ ($N-x-z$)

Player 1 (sees y, z): sends 1 iff color (x, y) = color $(x+d, y)$ ($N-y-z$)

output 1 iff Players 2, 3 both send 1.

Complexity of protocol $= \log(c_2^<(N)) + 2$

(2) Corners Problem (Coloring) $\approx$ (2') NOF ExactlyN $k=3$



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

Color(x, y) := Transcript of Π on $(x, y, N-x-y)$ ← # colors $= 2^c$

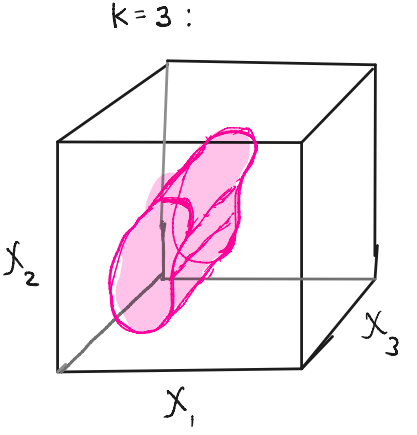
Claim: Each color class is corner free.

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 $X = X_1 \times X_2 \times \cdots \times X_k$ (input space)

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

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

Defn A cylinder intersection is a subset

$C \subseteq X$ s.t. $C = C_1 \cap C_2 \cap \cdots \cap C_k$, 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 $f : X_1 \times X_2 \times \dots \times X_k \to \{0,1\}$ then Π induces a partition of X into 2^c f-monochromatic cylinder intersections

Defn (Discrepancy for cylinder Intersections)

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

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

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

same as Defn of Disc(f, R) but now over cylinder intersections

Lemma $D^{\varepsilon, \mu}_k(f) \geq \log\left(\frac{1-2\varepsilon}{\text{Disc}_\mu(f)}\right)$

Distrib. cc of k-player deterministic NOF of f

Proof same as for Disc over Rectangles

Theorem Let μ = unif distribution over X.

$$D_{1/3,\mu}^{k}(g|P_n) = \Omega\left(\frac{n}{4^k}\right)$$

Main Lemma $\mathrm{Disc}_{\mu}(g|P_n) \leq \exp(-n/4^k)$

↑

Proof is very similar to our "BNS" proof of 2-player lower bound for IP_n

But now we apply Cauchy Swartz (Jensen's INEQ) $k-1$ times. Each time we lose a factor of ~ 4 in the LB.

Introduction to Lifting in Comm. Complexity

Some motivation:

We already saw strong randomized LBs for DISJ, IP.
This already gives many applications

However for many important applications this isn't enough.

We want LBs for communication problems that are search problems -- problems where there can be more than one answer.

So a stronger LB is needed (against any function solving the search problem)

Introduction to Lifting in Comm. Complexity

Let $R \subseteq Z \times O$

R is <u>total</u> if $\forall z \in Z$ $\exists$ at least one $o \in O$ st $R(z,o)=1$

Total search problem associated with total R:

On input z output some o st $R(z,o)=1$

Two party total search problems: $R \subseteq X \times Y \times O$

$Search_R$: on input (x,y) output some $o \in O$ st $R(x,y,o)=1$

- Any Boolean function $f: Z \to \{0,1\}$ is a total search problem, but not all total search problems are Boolean functions

Some Applications of 2-player CC LBs

1. Streaming Algs
* 2. game Theory
3. Streaming LBs
* 4. Property testing
5. Time / space Tradeoffs (TMs)
6. Circuit complexity
7. Extension complexity
8. Proof complexity LBs
9. Learning Theory

} Need CC Lower Bounds for search problems

* Presentation topics

Examples : CC SEARCH PROBLEMS

$S \subseteq \{0,1\}^n \times \{0,1\}^n \times \Theta$

Example 1 (KW_f Search)

Alice: $x \in f^{-1}(1)$ Bob: $y \in f^{-1}(0)$

Output $i \in [n]$ such that $x_i \neq y_i$

Examples : CC SEARCH PROBLEMS

$S \subseteq \{0,1\}^* \times \{0,1\}^* \times \Theta$

Example 2 (CNF Search)

Fix an unsatisfiable CNF C over $x_1 \dots x_n$ $y_1 \dots y_n$

Alice: $x \in \{0,1\}^n$ Bob: $y \in \{0,1\}^n$

Output clause C_i falsified by (x,y)

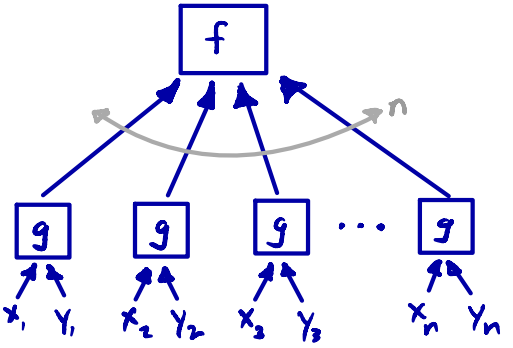
Lifting in CC

Main idea is to take a function f or total search problem that is hard in "query" model —
ex. requires large dec tree complexity

Then Form a hard 2-player function from f
by composing f with a "hard" 2-player function

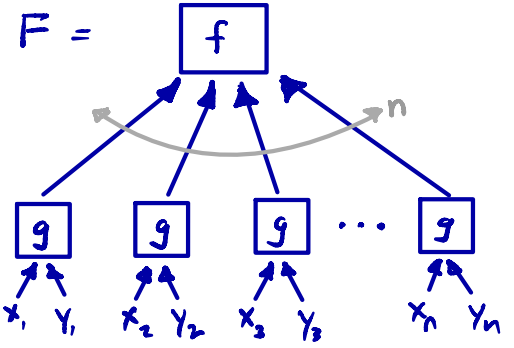
QUERY TO COMMUNICATION LIFTING

$f : \{0,1\}^n \to \Theta$ ⇝ $F :$



QUERY TO COMMUNICATION LIFTING

$f : \{0,1\}^n \to \Theta$ ⇝



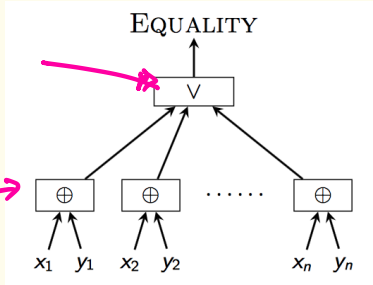
LIFTING THEOREM

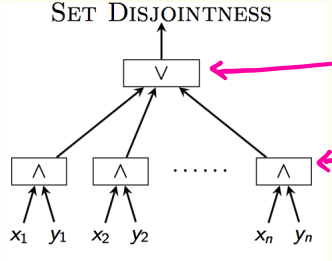
Communication complexity of F ≈ Query complexity of F

INTUITION: MOST HARD COMMUNICATION PROBLEMS ARE COMPOSED FUNCTIONS $f \circ g^n$

f : OR

g: =



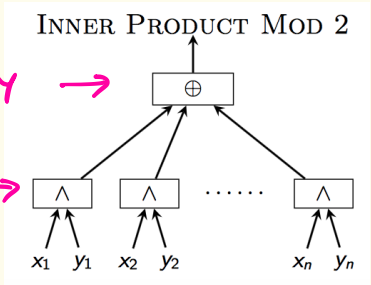


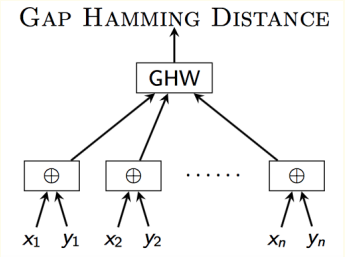
f : OR

g: AND

f: PARITY

g: AND





Lifting Theorems Makes Lower Bounds Easy!

2 step Recipe:

(1.) Prove problem specific query lower bound

(2) Apply Lifting theorem to obtain communication complexity lower bound

APPLICATIONS

- Streaming
- Property Testing
- game theory
- TIME/SPACE Turing Machine LBs
- Circuit complexity
- Proof complexity
- Extension Complexity
- Clique/Coclique, Graph Theory, Learning Partial Functions
- Secret Sharing Schemes (For Linear schemes)

(SOME) LIFTING THEOREMS

	Measure on $f \circ g^n$	Measure on f
Raz-Mckenzie '99	Deterministic CC	Decision tree
Razborov '03	Quantum CC	approx. degree
Sherstov '07	discrepancy, sign rank, unbded error	Threshold degree
Göös-P '14	Randomized CC	(critical) Block Sensitivity
GLMWZ '15	Nondeterministic CC, Partition	approx. Junta degree
Lee-Raghavendra Steurer '15	Semidefinite Rank	SOS degree
RPRC '16 PR '17, PR'17b	Razborov Rank / Algebraic Tiling	algebraic gap degree Nullsatz degree.
KMR '16	Nonnegative Rank	Junta degree
Göös-P-Watson '17	Randomized CC	Randomized dec. tree

3 Main "Types" of Lifting

(1) Reduction from $\overset{cc}{UB}$ for fog^n $\longrightarrow$ cc upper bound for $DISJ_n$

[e.g., Zhang, göös-P]

(2) Linear algebraic

Reduce some measure of polynomial degree $\longrightarrow$ cc lower bound

[e.g. Sherstov, P-Robere]

(3) Direct simulation of cc protocol to extract query UB

(via measures of pseudorandomness, Fourier analysis, sunflower lemma)

[e.g., Raz-McKenzie, göös-P-Watson]

Quick Primer on Query Complexity of Boolean Functions

(1) $D^{dt}(f)$: dec. tree complexity of f

(2) $R^{dt}(f)$: randomized dec. tree compl of f

(3) Block-sensitivity (f, α) : max B s.t. there are B disjoint blocks $I_1, \ldots, I_B \subseteq [n]$
s.t. $\forall I_j \quad f(\alpha) \neq f(\alpha^{I_j})$

(4) Polynomial degree $\deg(f)$: degree of the unique multilinear polynomial over R that represents f

(5) Approx degree $\deg^{\varepsilon}(f)$: $\min$ degree of poly p s.t. $\forall \alpha \in \{0,1\}^n$
$f(\alpha) = p(\alpha) \pm \varepsilon$

Theorem [Nisan, Szegedy]

All of the above measures are polynomially related —

i.e. $R^{dt}(f) = \deg(f)^{O(1)}$, $\deg(f) = \left(R^{dt}(f)\right)^{O(1)}$

Zhang / göös-P Lifting (for Boolean functions only)

Boolean fxns: [Shengyu Zhang, "On the tightness of Buhrman-Cleve-Wigderson simulation"]

general search [göös-Pitassi, "Critical Block Sensitivity"]

Theorem [Zhang] $\exists g: \{0,1\}^2 \times \{0,1\}^2 \to \{0,1\}$ s.t. For any Boolean function $f: \{0,1\}^n \to \{0,1\}$

$$R^{cc}(f(g^n)) = \Omega\left(D^{dt}(f)^{1/3}\right)$$

$R^{cc}(f(g^n))$:

Alice gets $x_1 \dots x_n$

Bob gets $y_1 \dots y_n$

output: $f(g(x_1,y_1), g(x_2,y_2) \dots g(x_n,y_n)) \in \{0,1\}$

Block Sensitivity

$bs(f,x) \triangleq \max B \in \{0,..,n\}$ s.t. $\exists$ disjoint sets $I_1,..,I_B \subseteq [n]$ such that $f(x) \neq f(x^{I_j})$ $\forall j \in [B]$

x^{I_j}: x with assignment to I_j flipped

$bs(f) \triangleq \max_x$ Blocksensitivity(f,x)

Example: $f = x_1 \vee x_2 \vee .. x_n$ $\quad x = 00000\cdots0$

$bs(f,x) = n$

Theorem $bs(f) \leq D^{dt}(f) \leq bs(f)^3$ (open: $D^{dt}(f) \overset{?}{\leq} bs(f)^2$)

Proof of Zhang's Lifting Thm for Boolean functions:

The proof is a reduction showing:

$$\forall f : \{0,1\}^n \to \{0,1\} \text{ with } bs(f) = B$$

$$R^{cc}(UDISJ(x_1 \ldots x_B, y_1 \ldots y_B)) \leq R^{cc}(f \circ g^n)$$

Says a cc protocol for $f \circ g^n$ implies a cc protocol for $UDISJ_{n=B}$

UDISJ: "unique disjointness" restriction of DISJ where we are promised either $|x \cap y| = 0$ or $|x \cap y| = 1$

Theorem $R^{cc}(UDISJ_n) = \Omega(n)$ ← proof of $\Omega(n)$ LB for $DISJ_n$ actually shows LB even under "unique" promise

Proof of Zhang's Lifting Thm for Boolean functions:

Let $f : \{0,1\}^n \to \{0,1\}$, $bs(f) = B$ and let z be an input s.t. $bs(f,z) = B$.

Example z : 0 | 1 0 | 1 0 | 1 0 | 1 1 1 $\quad B = 3$

I_1 I_2 I_3

Reduction: Let x, y be input to UDISJ, $x = x_1, \ldots, x_B$ $y = y_1, \ldots, y_B$

Alice on x computes x', $|x'| = n$

Bob on y computes y', $|y'| = n$

Then they run protocol Π for fog^n on (x', y')

We want to show
$\exists$ mappings $M_A : x \to x'$
$M_B : y \to y'$

such that $UDISJ(x,y) \equiv fog^n(x', y')$

"Versatile" gadget : $g(x,y) = 1 \iff x + y \bmod 4 \in \{2,3\}$

g:

	00	01	10	11
00	0	0	1	1
01	0	1	1	0
10	1	1	0	0
11	1	0	0	0

g is a 2-bit gadget!

Defn Let $g_1 : X_1 \times Y_1 \to \{0,1\}$ $g_2 : X_2 \times Y_2 \to \{0,1\}$

$g_1 \leq g_2$ if $\exists$ 1-1 mappings π_A, π_B s.t. $\forall (x,y) \in X_1 \times Y_1$ $g_1(x,y) = g_2(\pi_A(x), \pi_B(y))$

Properties our gadget has:

1. $\neg g \leq g$:

$\pi_A^{\neg}(x) \to x + 2$
$\pi_B^{\neg}(y) \to y$

$(x + y \in \{2,3\}$ iff $\{x+2, y\} \in \{0,1\})$

2. AND $\leq g$:

	00	01	10	11
00	0	0	1	1
01	0	1	1	0
10	1	1	0	0
11	1	0	0	0

π_A^{AND} : $0 \to 00$, $1 \to 01$

π_B^{AND} : $0 \to 00$, $1 \to 01$

Example $bs(f,\alpha) = 3$ $\quad \alpha = 1\underbrace{011}_{I_1}\underbrace{0}\underbrace{10}_{I_2}\underbrace{1}_{I_3}$ $\quad f(\alpha) = b$, $f(\alpha^{B_i}) = \bar{b}$

$x = 011$

$y = 101$

WANT:

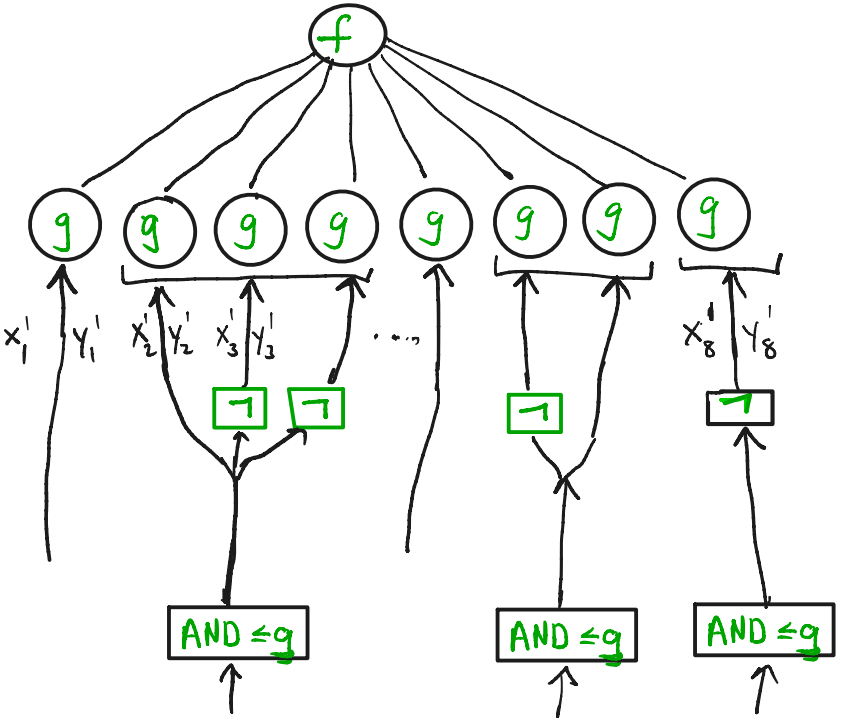
Alice: $M_A(x) \rightsquigarrow x'$

Bob: $M_B(y) \rightsquigarrow y'$

such that:

$UDISJ(x,y) = 0 \Rightarrow g^n(x',y') = \alpha$

$UDISJ(x,y) = 1$ with $x_i = y_i = 1 \Rightarrow g^n(x',y') = \alpha^{B_i}$

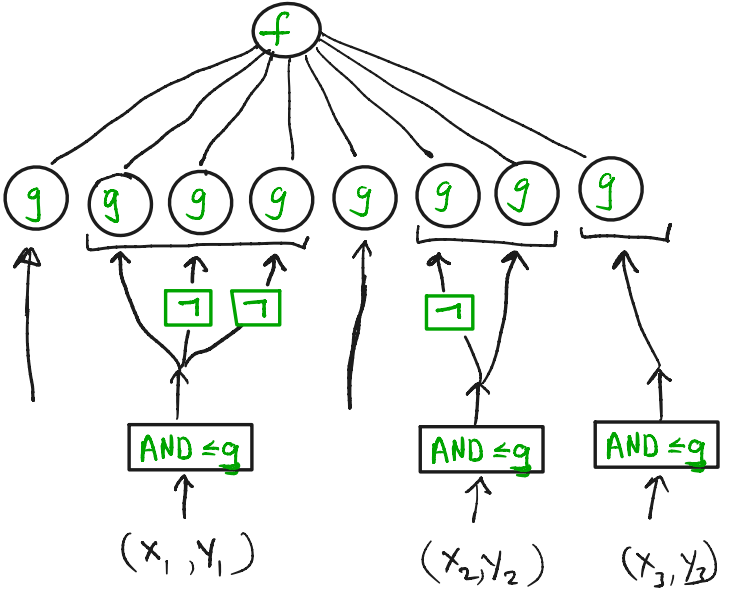


Example $bs(f) = 3$ and let $\alpha = 1\underbrace{011}_{I_1}\underbrace{0}\underbrace{10}_{I_2}\underbrace{1}_{I_3}$ be sensitive input

so $f(\alpha) = b$, $f(\alpha^{I_i}) = \bar{b}$

WANT: $UDISJ(x,y) = 0 \Rightarrow g^n(x,y) = \alpha$

$UDISJ(x,y) = 1$ with $x_i = y_i = 1 \Rightarrow g^n(x,y) = \alpha^{B_i}$



$M_A : x \to x'$:

x'_i: If $i \notin \{B_1, B_2, B_3\}$: if $\alpha_i = 0$ $x'_i = 00$; if $\alpha_i = 1$ $x'_i = 01$

If $i \in B_j$: if $\alpha_i = 0$ $x'_i = \pi_A^{AND}(x_i)$; if $\alpha_i = 1$ $x'_i = \pi_A^{\neg}(\pi_A^{AND}(x_i))$

$M_B : y \to y'$: same but use π_B^{AND}, $\pi_B^{\neg}$

Example $bs(f,\alpha) = 2$ $\alpha = \underbrace{1011}_{B_1}\underbrace{0}\underbrace{10}_{B_2}\underbrace{1}_{B_3}$ $f(\alpha) = b$ $f(\alpha^{B_i}) = \bar{b}$ $x = 011$ $y = 101$

WANT: $UDISJ(x,y) = 0 \Rightarrow g^n(x,y) = \alpha$

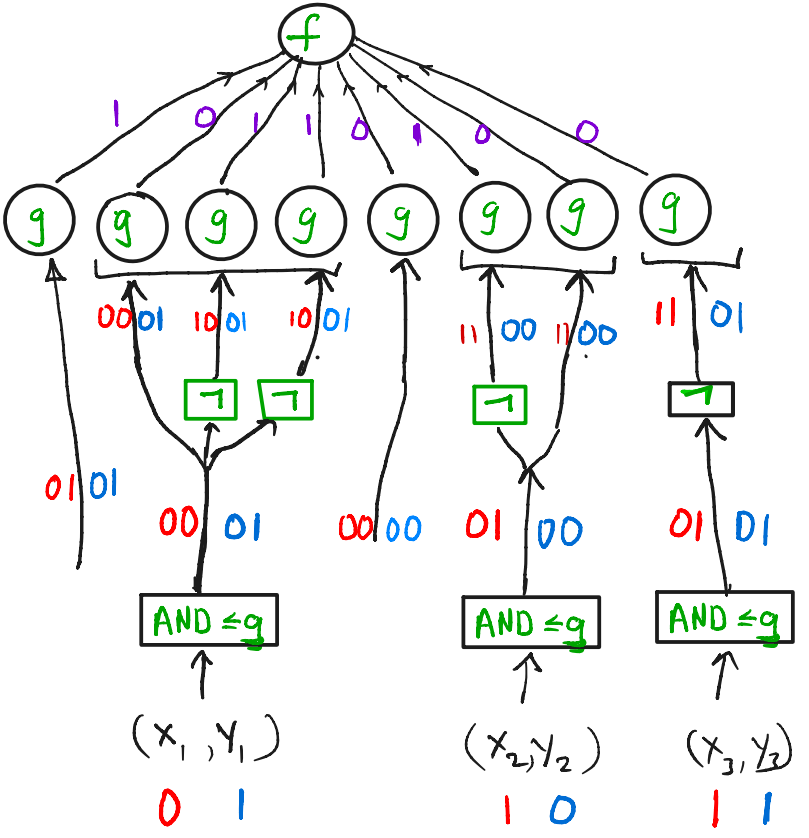
$UDISJ(x,y) = 1$ with $x_i = y_i = 1 \Rightarrow g^n(x,y) = \alpha^{B_i}$

$M_A : x \to x'$:

x'_i: If $i \notin \{B_1, B_2, B_3\}$: if $\alpha_i = 0$ $x'_i = 00$; if $\alpha_i = 1$ $x'_i = 01$

If $i \in B_j$: if $\alpha_i = 0$ $x'_i = \pi_A^{AND}(x_i)$; if $\alpha_i = 1$ $x'_i = \pi_A^{\neg}(\pi_A^{AND}(x_i))$

$M_B : y \to y'$: same but use π_B^{AND}, $\pi_B^{\neg}$



generalizing Zhang to general search Problems

PROs

- Use randomized reduction.
  Need an extra property of gadget (which versatile gadget satisfies)
- gadget g has constant size!
- generalizes to multiparty NIH + NOF !

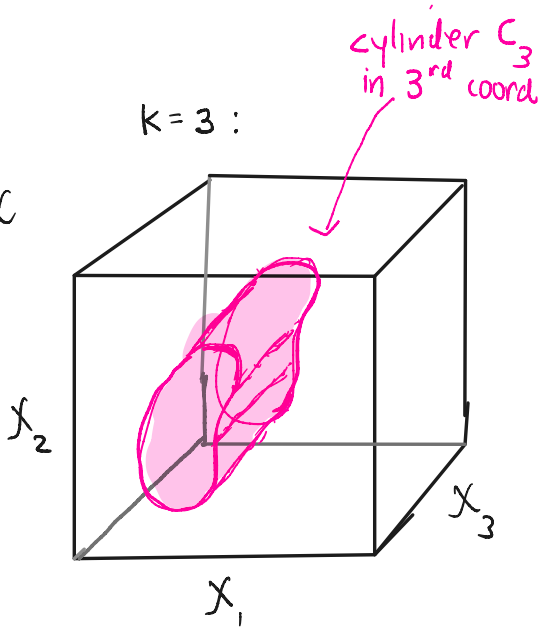
CONs generalize block sensitivity to critical block sensitivity
Limits applications

NOF Protocols

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

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

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



(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. $C = C_1 \cap C_2 \cap \cdots \cap C_k$, 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)

Analog of 2-party partition into rectangles

NOF Communication Complexity

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, Meka FOCS '23]
↖ gives $\Omega(n^2)$ LB on NIH PromiseEQ $k=3$

(ii) "Explicit separations between randomized & deterministic NOF Comm."
[Kelley, Lovett, Meka STOC '24]

(iii) "Quasipoly LBs for the corners theorem"
[Jaber, Liu, Lovett, Ostuni, Sawhney '25]

↖ gives $\Omega(n^2)$ deterministic NOF LB for ExactlyN $k=3$

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?

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?

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

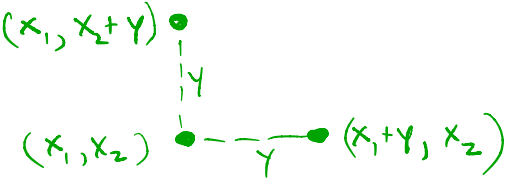
* It is known that ① $\cong$ ① $\left(c_3(N) \approx \frac{N}{r_3(N)} \right)$

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

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

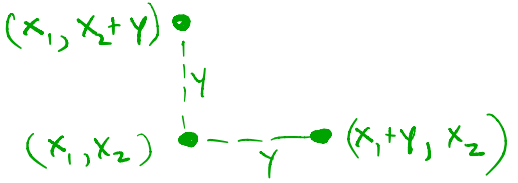
(2) **Corners Problem**: What is max size $r_2^<(N^2)$ of $S \subseteq [N]^2$ s.t. S does not contain a 3D corner?

3D corner:



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

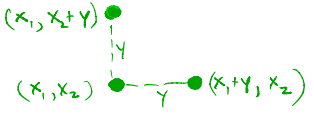
3D corner:



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

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
(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 $x=y=z$
(2) Corners Problem (Coloring) 	(2') NOF ExactlyN $k=3$ Player 1 : y, z Player 2 : x, z Player 3 : x, y Decide if $x+y+z=N$

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 $r_3(N) \geq N/\exp(2.25\sqrt{\log N})$

$\therefore\ c_3(N) \leq \exp(2.25\sqrt{\log N})$

↖ equivalently $\exists$ deterministic NIH protocol for Promise EQ $k=3$ of cost $\log(c_3(N)) = O(\sqrt{\log N}) = O(n^{1/2})$

Kelley, Meka 2023 (Huge exponential improvement over previous results)

$$r_3(N) \leq \frac{N}{\exp(c \log N^{1/12})}$$

$$\therefore\ c_3(N) \geq \exp(c \log N^{1/12})$$

↖ equivalently any det. NIH protocol for Promise EQ $k=3$ requires cost $\Omega(n^{1/12})$

State of the Art: Corner Free sets

Behrend : 1946

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

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 ExactlyN, $k=3$ of cost $O(n^{1/2})$

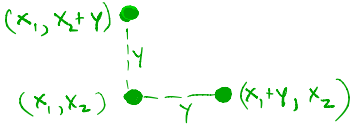
Best improvement to constant c : $c \sim 1.8$ [Linial, Shraibman '21] [Green '21]

Jaber, Liu, Lovett, Ostuni, Sawhney 2025

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

$\therefore\ c_2^<(N^2) \geq \Omega(n^{1/200})$ ← equivalently any NOF protocol for ExactlyN $k=3$ has cost $\Omega(n^{1/200})$

(2) Corners Problem (Coloring) $\approx\approx$ (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 $c_2^<(N)$ 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)

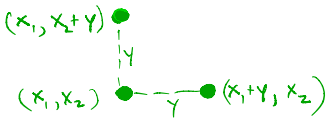
Player 2 (sees x, z): sends 1 iff color (x, y) = color $(x, y+d)$ ($N-x-z$)

Player 1 (sees y, z): sends 1 iff color (x, y) = color $(x+d, y)$ ($N-y-z$)

output 1 iff Players 2, 3 both send 1.

Complexity of protocol $= \log(c_2^<(N)) + 2$

(2) Corners Problem (Coloring) $\approx$ (2') NOF ExactlyN $k=3$



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

Color(x, y) := Transcript of Π on $(x, y, N-x-y)$ ← # colors $= 2^c$

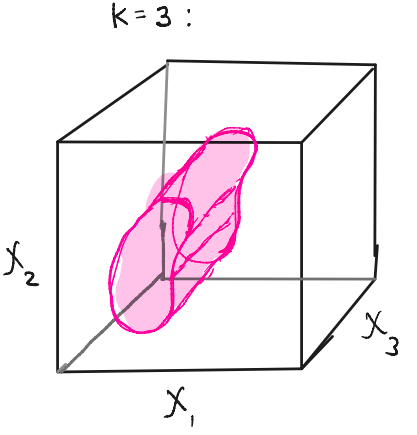
Claim: Each color class is corner free.

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 $X = X_1 \times X_2 \times \cdots \times X_k$ (input space)

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

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

Defn A cylinder intersection is a subset

$C \subseteq X$ s.t. $C = C_1 \cap C_2 \cap \cdots \cap C_k$, 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

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

Defn (Discrepancy for cylinder Intersections)

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

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

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

same as Defn of Disc(f, R) but now over cylinder intersections

Lemma $D^{\varepsilon, \mu}_k(f) \geq \log\left(\frac{1-2\varepsilon}{\text{Disc}_\mu(f)}\right)$

Distrib. cc of k-player deterministic NOF of f

Proof same as for Disc over Rectangles

Theorem Let μ = unif distribution over X.

$$D_{1/3,\mu}^{k}(g|P_n) = \Omega\left(\frac{n}{4^k}\right)$$

Main Lemma $\mathrm{Disc}_{\mu}(g|P_n) \leq \exp(-n/4^k)$

↑

Proof is very similar to our "BNS" proof of 2-player lower bound for IP_n

But now we apply Cauchy Swartz (Jensen's INEQ) $k-1$ times. Each time we lose a factor of ~ 4 in the LB.

Introduction to Lifting in Comm. Complexity

Some motivation:

We already saw strong randomized LBs for DISJ, IP.
This already gives many applications

However for many important applications this isn't enough.

We want LBs for communication problems that are search problems -- problems where there can be more than one answer.

So a stronger LB is needed (against any function solving the search problem)

Introduction to Lifting in Comm. Complexity

Let $R \subseteq Z \times O$

R is <u>total</u> if $\forall z \in Z$ $\exists$ at least one $o \in O$ st $R(z,o)=1$

Total search problem associated with total R:

On input z output some o st $R(z,o)=1$

Two party total search problems: $R \subseteq X \times Y \times O$

$Search_R$: on input (x,y) output some $o \in O$ st $R(x,y,o)=1$

- Any Boolean function $f: Z \to \{0,1\}$ is a total search problem, but not all total search problems are Boolean functions

Some Applications of 2-player CC LBs

1. Streaming Algs
* 2. game Theory
3. Streaming LBs
* 4. Property testing
5. Time / space Tradeoffs (TMs)
6. Circuit complexity
7. Extension complexity
8. Proof complexity LBs
9. Learning Theory

} Need CC Lower Bounds for search problems

* Presentation topics

Examples : CC SEARCH PROBLEMS

$S \subseteq \{0,1\}^n \times \{0,1\}^n \times \Theta$

Example 1 (KW_f Search)

Alice: $x \in f^{-1}(1)$ Bob: $y \in f^{-1}(0)$

Output $i \in [n]$ such that $x_i \neq y_i$

Examples : CC SEARCH PROBLEMS

$S \subseteq \{0,1\}^n \times \{0,1\}^n \times \Theta$

Example 2 (CNF Search)

Fix an unsatisfiable CNF C over $x_1 \dots x_n$ $y_1 \dots y_n$

Alice: $x \in \{0,1\}^n$ Bob: $y \in \{0,1\}^n$

Output clause C_i falsified by (x,y)

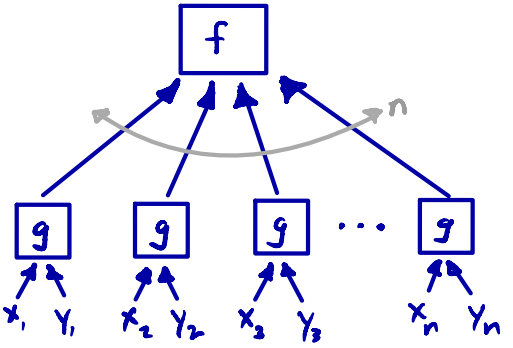
Lifting in CC

Main idea is to take a function f or total search problem that is hard in "query" model —
ex. requires large dec tree complexity

Then Form a hard 2-player function from f
by composing f with a "hard" 2-player function

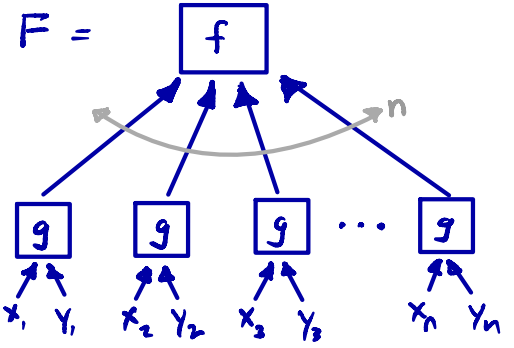
QUERY TO COMMUNICATION LIFTING

$f : \{0,1\}^n \to \Theta$ ⇝ $F :$



QUERY TO COMMUNICATION LIFTING

$f : \{0,1\}^n \to \Theta$ ⇝



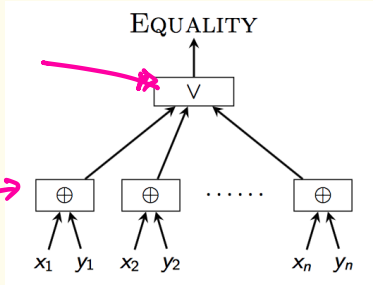
LIFTING THEOREM

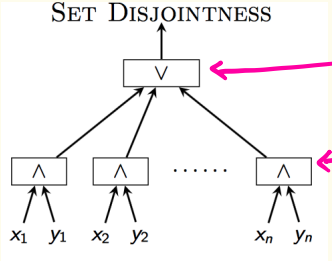
Communication complexity of F ≈ Query complexity of F

INTUITION: MOST HARD COMMUNICATION PROBLEMS ARE COMPOSED FUNCTIONS $f \circ g^n$

f : OR

g : =



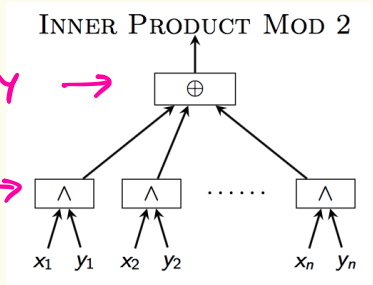


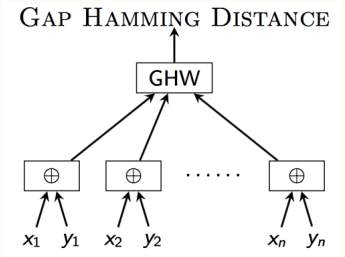
f : OR

g : AND

f : PARITY

g : AND





Lifting Theorems Makes Lower Bounds Easy!

2 step Recipe:

(1.) Prove problem specific query lower bound

(2) Apply Lifting theorem to obtain communication complexity lower bound

APPLICATIONS

- Streaming
- Property Testing
- game theory
- TIME/SPACE Turing Machine LBs
- Circuit complexity
- Proof complexity
- Extension Complexity
- Clique/Coclique, Graph Theory, Learning Partial Functions
- Secret Sharing Schemes (For Linear schemes)

(SOME) LIFTING THEOREMS

	Measure on $f \circ g^n$	Measure on f
Raz-Mckenzie '99	Deterministic CC	Decision tree
Razborov '03	Quantum CC	approx. degree
Sherstov '07	discrepancy, sign rank, unbded error	Threshold degree
Göös-P '14	Randomized CC	(critical) Block Sensitivity
GLMWZ '15	Nondeterministic CC, Partition	approx. Junta degree
Lee-Raghavendra Steurer '15	Semidefinite Rank	SOS degree
RPRC '16 PR '17, PR'17b	Razborov Rank / Algebraic Tiling	algebraic gap degree Nullsatz degree.
KMR '16	Nonnegative Rank	Junta degree
Göös-P-Watson '17	Randomized CC	Randomized dec. tree

3 Main "Types" of Lifting

(1) Reduction from $\overset{cc}{UB}$ for fog^n $\longrightarrow$ cc upper bound for $DISJ_n$

[e.g., Zhang, göös-P]

(2) Linear algebraic

Reduce some measure of polynomial degree $\longrightarrow$ cc lower bound

[e.g. Sherstov, P-Robere]

(3) Direct simulation of cc protocol to extract query UB

(via measures of pseudorandomness, Fourier analysis, sunflower lemma)

[e.g., Raz-McKenzie, göös-P-Watson]

Quick Primer on Query Complexity of Boolean Functions

(1) $D^{dt}(f)$: dec. tree complexity of f

(2) $R^{dt}(f)$: randomized dec. tree compl of f

(3) Block-sensitivity (f, α) : max B s.t. there are B disjoint blocks $I_1, \ldots, I_B \subseteq [n]$
s.t. $\forall I_j \quad f(\alpha) \neq f(\alpha^{I_j})$

(4) Polynomial degree $\deg(f)$: degree of the unique multilinear polynomial over R that represents f

(5) Approx degree $\deg^{\varepsilon}(f)$: $^{\min}$ degree of poly p s.t. $\forall \alpha \in \{0,1\}^n$
$f(\alpha) = p(\alpha) \pm \varepsilon$

Theorem [Nisan, Szegedy]

All of the above measures are polynomially related —

ie. $R^{dt}(f) = \deg(f)^{O(1)}$, $\deg(f) = \left(R^{dt}(f)\right)^{O(1)}$

Zhang / göös-P Lifting (for Boolean functions only)

Boolean fxns: [Shengyu Zhang, "On the tightness of Buhrman-Cleve-Wigderson simulation"]

general search [göös-Pitassi, "Critical Block Sensitivity"]

Theorem [Zhang] $\exists g: \{0,1\}^2 \times \{0,1\}^2 \to \{0,1\}$ s.t. For any Boolean function $f: \{0,1\}^n \to \{0,1\}$

$$R^{cc}(f(g^n)) = \Omega\left(D^{dt}(f)^{1/3}\right)$$

$R^{cc}(f(g^n))$:

Alice gets $x_1 \dots x_n$

Bob gets $y_1 \dots y_n$

output: $f(g(x_1,y_1), g(x_2,y_2) \dots g(x_n,y_n)) \in \{0,1\}$

Block Sensitivity

$bs(f,x) \triangleq \max B \in \{0,..,n\}$ s.t. $\exists$ disjoint sets $I_1,..,I_B \subseteq [n]$ such that $f(x) \neq f(x^{I_j})$ $\forall j \in [B]$

x^{I_j}: x with assignment to I_j flipped

$bs(f) \triangleq \max_x$ Blocksensitivity(f,x)

Example: $f = x_1 \vee x_2 \vee .. x_n$ $\quad x = 00000\cdots0$

$bs(f,x) = n$

Theorem $bs(f) \leq D^{dt}(f) \leq bs(f)^3$ (open: $D^{dt}(f) \overset{?}{\leq} bs(f)^2$)

Proof of Zhang's Lifting Thm for Boolean functions:

The proof is a reduction showing:

$$\forall f : \{0,1\}^n \to \{0,1\} \text{ with } bs(f) = B$$

$$R^{cc}(UDISJ(x_1 \ldots x_B, y_1 \ldots y_B)) \leq R^{cc}(f \circ g^n)$$

Says a cc protocol for $f \circ g^n$ implies a cc protocol for $UDISJ_{n=B}$

UDISJ: "unique disjointness" restriction of DISJ where we are promised either $|x \cap y| = 0$ or $|x \cap y| = 1$

Theorem $R^{cc}(UDISJ_n) = \Omega(n)$ ← proof of $\Omega(n)$ LB for $DISJ_n$ actually shows LB even under "unique" promise

Proof of Zhang's Lifting Thm for Boolean functions:

Let $f : \{0,1\}^n \to \{0,1\}$, $bs(f) = B$ and let z be an input s.t. $bs(f,z) = B$.

Example z : 0 | 1 0 | 1 0 | 1 0 | 1 1 1 $\quad B = 3$

I_1 I_2 I_3

Reduction: Let x, y be input to UDISJ, $x = x_1, \ldots, x_B$ $y = y_1, \ldots, y_B$

Alice on x computes x', $|x'| = n$

Bob on y computes y', $|y'| = n$

Then they run protocol Π for fog^n on (x', y')

We want to show
$\exists$ mappings $M_A : x \to x'$
$M_B : y \to y'$

such that $UDISJ(x,y) \equiv fog^n(x', y')$

"Versatile" gadget : $g(x,y) = 1 \iff x+y \bmod 4 \in \{2,3\}$

g:

	00	01	10	11
00	0	0	1	1
01	0	1	1	0
10	1	1	0	0
11	1	0	0	0

g is a 2-bit gadget!

Defn Let $g_1 : X_1 \times Y_1 \to \{0,1\}$ $g_2 : X_2 \times Y_2 \to \{0,1\}$

$g_1 \leq g_2$ if $\exists$ 1-1 mappings π_A, π_B s.t. $\forall (x,y) \in X_1 \times Y_1$ $g_1(x,y) = g_2(\pi_A(x), \pi_B(y))$

Properties our gadget has:

1. $\neg g \leq g$:

$\pi_A^{\neg}(x) \to x+2$
$\pi_B^{\neg}(y) \to y$

$(x+y \in \{2,3\}$ iff $\{x+2, y\} \in \{0,1\})$

2. AND $\leq g$:

	00	01	10	11
00	0	0	1	1
01	0	1	1	0
10	1	1	0	0
11	1	0	0	0

π_A^{AND} : $0 \to 00$, $1 \to 01$

π_B^{AND} : $0 \to 00$, $1 \to 01$

Example $bs(f,\alpha) = 3$ $\quad \alpha = \underbrace{1011}_{I_1}\underbrace{0}\underbrace{10}_{I_2}\underbrace{1}_{I_3}$ $\quad f(\alpha) = b$, $f(\alpha^{B_i}) = \bar{b}$

$x = 011$

$y = 101$

WANT:

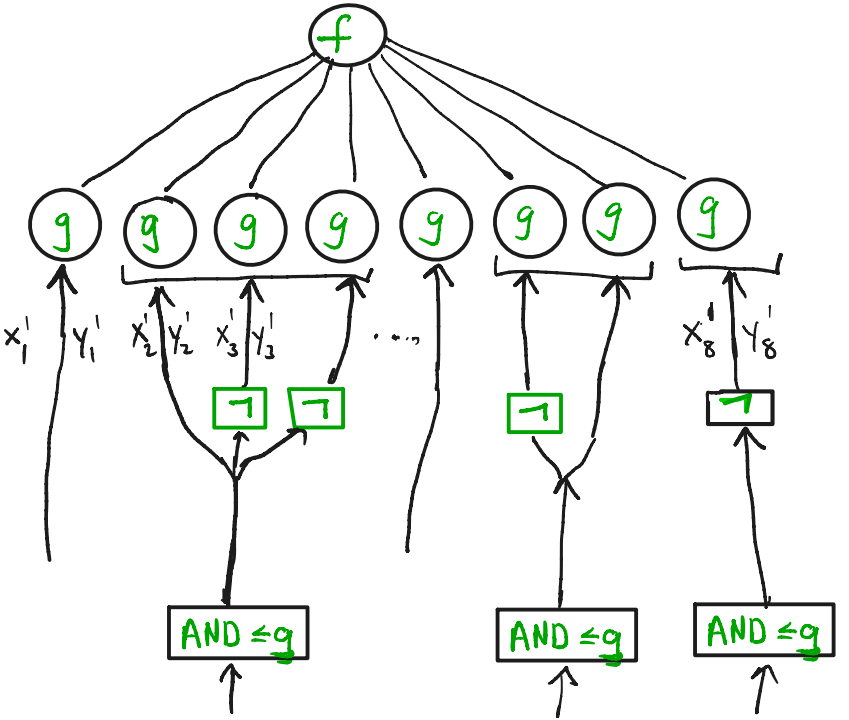
Alice: $M_A(x) \rightsquigarrow x'$

Bob: $M_B(y) \rightsquigarrow y'$

such that:

$UDISJ(x,y) = 0 \Rightarrow g^n(x',y') = \alpha$

$UDISJ(x,y) = 1$ with $x_i = y_i = 1 \Rightarrow g^n(x',y') = \alpha^{B_i}$

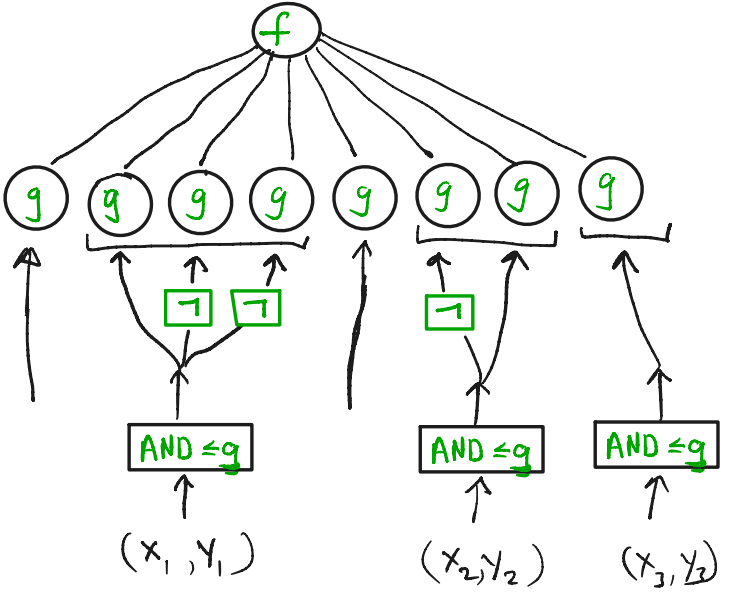


Example $bs(f) = 3$ and let $\alpha = 1\underbrace{011}_{I_1}\underbrace{0}_{}\underbrace{10}_{I_2}\underbrace{1}_{I_3}$ be sensitive input

so $f(\alpha) = b$, $f(\alpha^{I_i}) = \bar{b}$

WANT: $UDISJ(x,y) = 0 \Rightarrow g^n(x,y) = \alpha$

$UDISJ(x,y) = 1$ with $x_i = y_i = 1 \Rightarrow g^n(x,y) = \alpha^{B_i}$



$M_A : x \to x'$:

x'_i: If $i \notin \{B_1, B_2, B_3\}$: if $\alpha_i = 0$ $x'_i = 00$; if $\alpha_i = 1$ $x'_i = 01$

If $i \in B_j$: if $\alpha_i = 0$ $x'_i = \pi_A^{AND}(x_i)$; if $\alpha_i = 1$ $x'_i = \pi_A^{\neg}(\pi_A^{AND}(x_i))$

$M_B : y \to y'$: same but use π_B^{AND}, $\pi_B^{\neg}$

Example $bs(f,\alpha) = 2$ $\alpha = \underbrace{1011}_{B_1}\underbrace{0}\underbrace{10}_{B_2}\underbrace{1}_{B_3}$ $f(\alpha) = b$, $f(\alpha^{B_i}) = \bar{b}$ $x = 011$, $y = 101$

WANT: $UDISJ(x,y) = 0 \Rightarrow g^n(x,y) = \alpha$

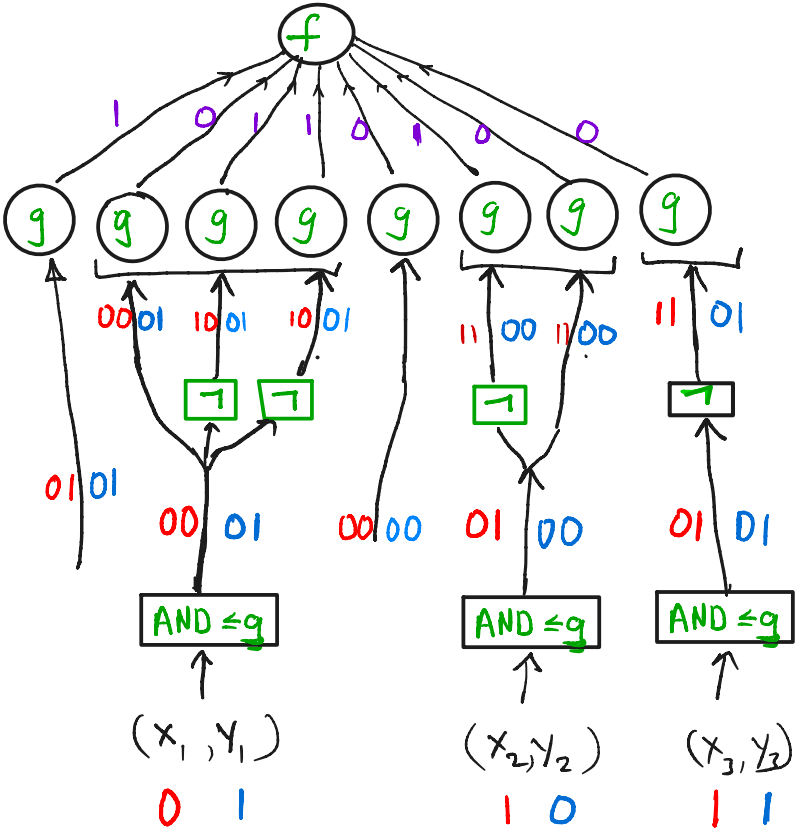
$UDISJ(x,y) = 1$ with $x_i = y_i = 1 \Rightarrow g^n(x,y) = \alpha^{B_i}$

$M_A : x \to x'$:

x'_i: If $i \notin \{B_1, B_2, B_3\}$: if $\alpha_i = 0$ $x'_i = 00$; if $\alpha_i = 1$ $x'_i = 01$

If $i \in B_j$: if $\alpha_i = 0$ $x'_i = \pi_A^{AND}(x_i)$; if $\alpha_i = 1$ $x'_i = \pi_A^{\neg}(\pi_A^{AND}(x_i))$

$M_B : y \to y'$: same but use π_B^{AND}, $\pi_B^{\neg}$



generalizing Zhang to general search Problems

PROs

- Use randomized reduction.
  Need an extra property of gadget (which versatile gadget satisfies)
- gadget g has constant size!
- generalizes to multiparty NIH + NOF !

CONs generalize block sensitivity to critical block sensitivity
Limits applications