- Schedule of presentation dates is posted (see course webpage)
- No class next week (spring break)

Last Time

1. Finish connections between NOF CC and additive combinatorics

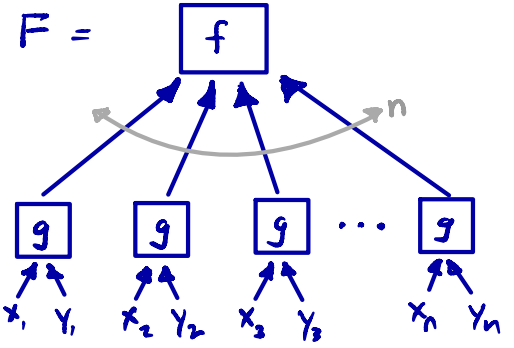
2. Introduction to Lifting, Zhang Lifting (for Boolean fxns only)

Today

Lifting via degree

QUERY TO COMMUNICATION LIFTING

$f : \{0,1\}^n \to \Theta$ ⇝



LIFTING THEOREM

Communication complexity of F ≈ Query complexity of F

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

Lifting Degree to Rank

Papers:

(1) Sherstov: Pattern Matrix Method:
degree → rk LBs for Boolean functions (Not search problems)
over R
methods: analytic (so restricted to Reals)

(2) Robert Robere PhD thesis
Pitassi-Robere '18 "Lifting Nullstellensatz to Monotone span programs over any field"

(3) Followup paper: de Rezende, Meir, Nordstrom, P, Robere, Vinyals
"Lifting with Simple Gadgets + Appl's to Circuit and Proof Complexity"

degree → rk for orb. search problems, and any Field

we'll mostly follow presentation from this paper

Lifting Degree to Rank

High Level (easiest for now to think of f as a Boolean function from $\{0,1\}^n$ to $\mathbb{R}$)

$\deg(f) \triangleq$ the degree of the unique multilinear polynomial $p(z_1 \dots z_n)$
s.t. $\forall \alpha \in \{0,1\}^n \quad p(\alpha) = f(\alpha)$

For search problems $S \subseteq \{0,1\}^n \times \Theta$, $\deg(S) =$ min degree over all f that compute S.

We want to start with a little gadget $g: X \times Y \to \{0,1\}$, $|X| = |Y| = O(1)$

and prove: $\text{rank}(f \circ g^n) \approx \text{rank}(g)^{\deg(f)}$

Since $\deg(f) \leq D^{dt}(f) \leq (\deg(f))^3$ and $CC(M) \geq \log \text{Rank}(M) \ \forall M$

this gives deterministic CC LBs on $f \circ g^n$
from lower bounds on $D^{dt}(f)$
decision tree complexity

Main Theorem Let f be any Boolean function or search problem, and Let $p \in \mathbb{F}[z_1, \ldots, z_n]$ be multilinear poly for f.

Let $g : X \times Y \to \mathbb{F}$ be any gadget of $\text{rank}(g) \geq 3$. Then

$$\sum_{S : \hat{p}(S) \neq 0} (\text{rank}(g) - 3)^{|S|} \leq \text{rank}(p \circ g^n) \leq \sum_{S : \hat{p}(S) \neq 0} \text{rank}(g)^{|S|}$$

← Lifts degree of p to rank of $p \circ g^n$

Notes gadget size is constant!

Works for any total search problem (not just Boolean functions)

Let p be any multilinear polynomial, $g = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ $g: X \times Y \to \{0,1\}$

Matrix for $p \circ g^n$:

$\forall \vec{x} = x_1 x_2 \ldots x_n \in X^n$, $\forall \vec{y} \in \in Y^n$:

$$M_{p \circ g^n}(x_1 \cdots x_n, y_1 \ldots y_n) = p(g(x_1 y_1), g(x_2 y_2), \ldots g(x_n y_n))$$

Kronecker Product $A \otimes B$ of 2 matrices

$A: r \times s$

$B: t \times v$

$$A \otimes B = \underbrace{\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1,s}B \\ \vdots & & & \\ a_{r1}B & a_{r2}B & \cdots & a_{r,s}B \end{bmatrix}}_{s \cdot v} \Bigg\} r \times t$$

Ex $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$

$$A \otimes B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Fact

$\text{Rank}(A \otimes B) = \text{Rank}(A) \cdot \text{Rank}(B)$

Let $f = z_1 \wedge \dots \wedge z_n$

so $P_f = z_1 \cdot \dots \cdot z_n$

Then matrix for $f \circ g^n$ is $\overbrace{g \otimes g \dots \otimes g}^{n}$

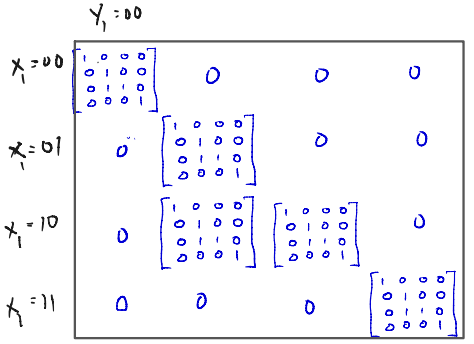
Let $g =$

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

$$p(x_1 x_2 y_1 y_2) = g(x_1 y_1) \cdot g(x_2 y_2)$$

$$x_i, y_i \in \{0,1\}^2$$

$n=2$:



← "g-patterned matrix" for f

rank $= 4^2 = rk(g)^{deg(f)}$

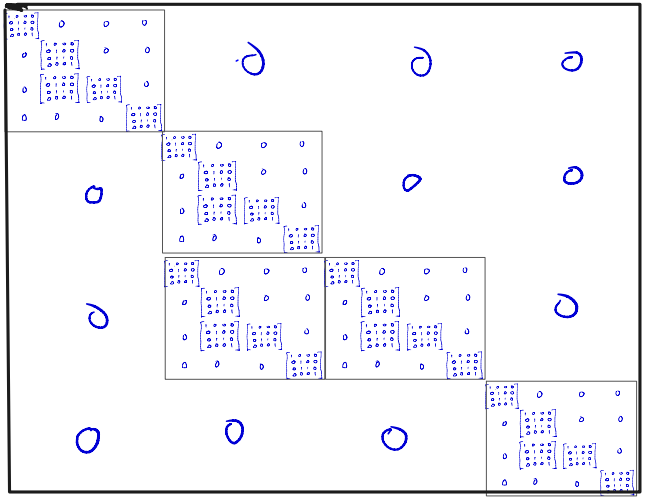
Let $f = z_1 \wedge \cdots \wedge z_n$

so $P_f = z_1 \cdots z_n$

Let $g = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Matrix for $f \circ g^n$ for $n = 3$:

$n = 3$:



$\text{rank} = 4^3 = \text{rk}(g)^{\deg(F)}$

Intuition For more general multivar. polys we could get cancellations But if we choose a "good" g that keeps row space / column space distinct we'll get above behavior

Defn. A gadget $g : X \times Y \to \mathbb{F}$ is good if $\forall A, B$ of same size

$$\operatorname{rank}(\underbrace{1_{X,Y}}_{\text{all 1's matrix}} \otimes A + g \otimes B) = \operatorname{rank}(A) + \operatorname{rank}(g) \cdot \operatorname{rank}(B)$$

Lemma $g : X \times Y \to \mathbb{F}$ is good iff the all 1's vector is not in $\underbrace{\text{row}(g)}_{\text{rowspace of } g}$ or $\underbrace{\text{col}(g)}_{\text{column space of } g}$

Defn. A gadget $g : X \times Y \to \mathbb{F}$ is *good* if $\forall A, B$ of same size

$$\text{rank}(\underbrace{1_{X,Y}}_{\text{all 1's matrix}} \otimes A + g \otimes B) = \text{rank}(A) + \text{rank}(g) \cdot \text{rank}(B)$$

Lemma 1 $g : X \times Y \to \mathbb{F}$ is *good* iff the all 1's vector is not in $\underbrace{\text{row}(g)}_{\text{row space of } g}$ or $\underbrace{\text{col}(g)}_{\text{column space of } g}$

Proof of Lemma 1 (sketch)

Theorem [characterization of when rank is additive, MS'72]
Let A', B' be 2 matrices of same size, over $\mathbb{F}$. Then

$$\text{rank}(A' + B') = \text{rank}(A') + \text{rank}(B') \text{ iff}$$

$$\text{row}(A') \cap \text{row}(B') = \text{col}(A') \cap \text{col}(B') = \{0\}$$

rank additive iff the corresponding linear operators act on disjoint parts of vector space

Using above theorem, we can prove the following claim:

(1) $\forall A B$ $\text{rank}(\underbrace{f \otimes A}_{A'} + \underbrace{g \otimes B}_{B'}) = \text{rank}(f)\,\text{rank}(A) + \text{rank}(g)\,\text{rank}(B)$ iff

(2) $\text{rank}(f + g) = \text{rank}(f) + \text{rank}(g)$

Main Theorem Let $p \in \mathbb{F}[z_1, \ldots, z_n]$ be any multilinear polynomial. Let $g : X \times Y \to \mathbb{F}$ be any gadget of $\text{rank}(g) \geq 3$. Then

$$\sum_{S : \hat{p}(S) \neq 0} (\text{rank}(g) - 3)^{|S|} \leq \text{rank}(p \circ g^n) \leq \sum_{S : \hat{p}(S) \neq 0} \text{rank}(g)^{|S|}$$

← Lifts degree of p to rank of $p \circ g^n$

Proof idea: By induction on n, using the following lemma

Lemma 2 Let $g : X \times Y \to \mathbb{F}$, where $\text{rank}(g) \geq 3$. Then for every A, B of the same size:

$$\text{rank}(1_{X \times Y} \otimes A + g \otimes B) \geq \text{rank}(A) + (\text{rank}(g) - 3)\,\text{rank}(B)$$

Main Theorem Let $p \in \mathbb{F}[z_1, \ldots, z_n]$ be any multilinear polynomial.
Let $g : X \times Y \to \mathbb{F}$ be any gadget of $\text{rank}(g) \geq 3$. Then

$$\sum_{S : \hat{p}(S) \neq 0} (\text{rank}(g) - 3)^{|S|} \leq \text{rank}(p \circ g^n) \leq \sum_{S : \hat{p}(S) \neq 0} \text{rank}(g)^{|S|}$$

Lemma Let $g : X \times Y \to \mathbb{F}$, where $\text{rank}(g) \geq 3$.
Then for every A, B of the same size:

$$\text{rank}(1_{X \times Y} \otimes A + g \otimes B) \geq \text{rank}(A) + (\text{rank}(g) - 3)\,\text{rank}(B)$$

Main theorem
Proof idea: By induction on n, using the above lemma
Write $p = q + z_1 r$ (recall p is multilinear). Then

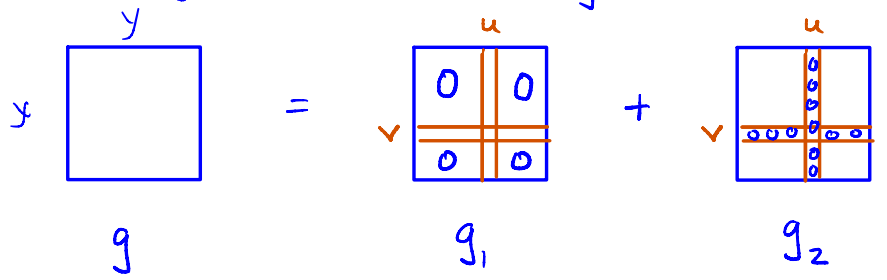
$$\begin{aligned}
\text{rank}(p \circ g^n) &= \text{rank}\left(1 \otimes (q \circ g^{n-1}) + g \otimes (r \circ g^{n-1})\right) \\
&\geq \text{rank}(q \circ g^{n-1}) + (\text{rank}(g) - 3)\,\text{rank}(r \circ g^{n-1}) && \text{By Lemma 2} \\
&\geq \sum_{S : \hat{q}(S) \neq 0} (\text{rank}(g) - 3)^{|S|} + (\text{rank}(g) - 3) \sum_{T : \hat{r}(T) \neq 0} (\text{rank}(g) - 3)^{|T|} && \text{By I.H} \\
&= \sum_{\substack{S : \hat{p}(S) \neq 0 \\ z_1 \notin S}} (\text{rank}(g) - 3)^{|S|} + (\text{rank}(g) - 3) \sum_{\substack{T : \hat{p}(T) \neq 0 \\ z_1 \in T}} (\text{rank}(g) - 3)^{|T|} \\
&= \sum_{S : \hat{p}(S) \neq 0} (\text{rank}(g) - 3)^{|S|}
\end{aligned}$$

∎

Lemma 2 Let $g : X \times Y \to \mathbb{F}$, where $\text{rank}(g) \geq 3$.
Then for every A, B of the same size:

$$\text{rank}(\mathbb{1}_{X\times Y} \otimes A + g \otimes B) \geq \text{rank}(A) + (\text{rank}(g)-3)\,\text{rank}(B)$$

Pf Assume $|X| = |Y|$ (general case very similar)



g_1 : zero out all but column u, row v

g_2 : zero out column u and row v

Note: g_2 is good

$$\text{rank}(\mathbb{1}\otimes A + g\otimes B) = \text{rank}(\mathbb{1}\otimes A + g_1\otimes B + g_2\otimes B)$$

$$\geq \text{rank}(\mathbb{1}\otimes A + g_2\otimes B) - \text{rank}(g_1\otimes B)$$ ← adding R can decrease rk by at most rank(R)

$$= \text{rank}(\mathbb{1}\otimes A + g_2\otimes B) - \text{rank}(g_1)\,\text{rank}(B)$$ ← Rank of Kronecker product is multiplicative

$$\geq \text{rank}(A) + \text{rank}(g_2)\,\text{rank}(B) - 2\,\text{rank}(B)$$ ← since g_2 is good

$$= \text{rank}(A) + \text{rank}(g-3)\,\text{rank}(B)$$

$\text{rank}(g_2) = \text{rank}(g) - 1$

How do we get degree LBs for search problems?

From proof complexity!

Recall our main search problems of interest are "TFNP" search problems.

Example: $C = C_1 \wedge C_2 \cdots \wedge C_m$ unsat k-CNF over $z_1 \ldots z_n$

Search_C: on input $\alpha \in \{0,1\}^n$ output some $j \in [m]$ s.t. $C_j(\alpha) = 0$

Search (Cog^n): Replace each clause $C_j(i_1\ i_2 \cdots i_k)$ by $C_j'(g(x_{i_1} y_{i_1}), g(x_{i_2} y_{i_2}) \cdots g(x_{i_k} y_{i_k}))$ to get a new CNF over vars $\vec{x}, \vec{y}$

↑

CC problem: Alice gets $\vec{x}$, Bob $\vec{y}$, output some C_j' that is falsified by $\vec{x}, \vec{y}$

Let $C = C_1 \wedge \cdots \wedge C_m$ unsat KCNF over $z_1 \ldots z_n$

Convert each clause C_i to poly eqn:

Example: $C_i = (z_1 \vee \bar{z}_2 \vee z_3) \Rightarrow P_i := (1-z_1)\, z_2\, (1-z_3) = 0$

plus we add n extra equations $(z_i^2 - z_i) = 0$ to force only 0/1 solns

A Nullstellensatz refutation of C (over a Field F):

$$\sum P_i(z)\, q_i(z) = 1$$

Theorem: For any unsat KCNF C, the min degree of Search(C) is $\Omega(\text{Nsatz-degree}(C))$

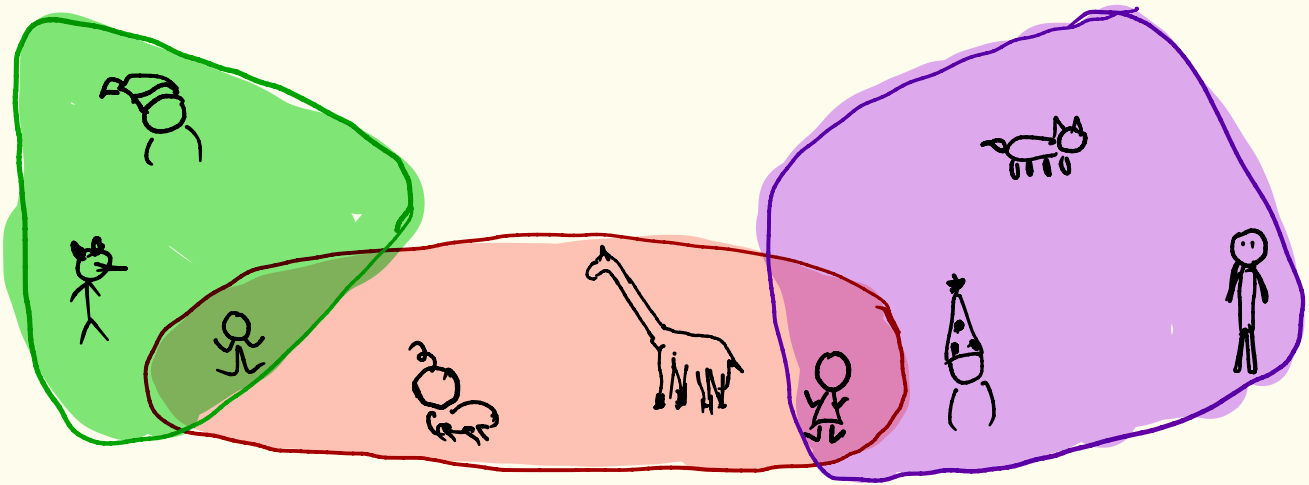
Applications of this result

1. Truly Exponential LBs for: Monotone formula size LBs
   Monotone Branching Program
   Monotone Span Programs

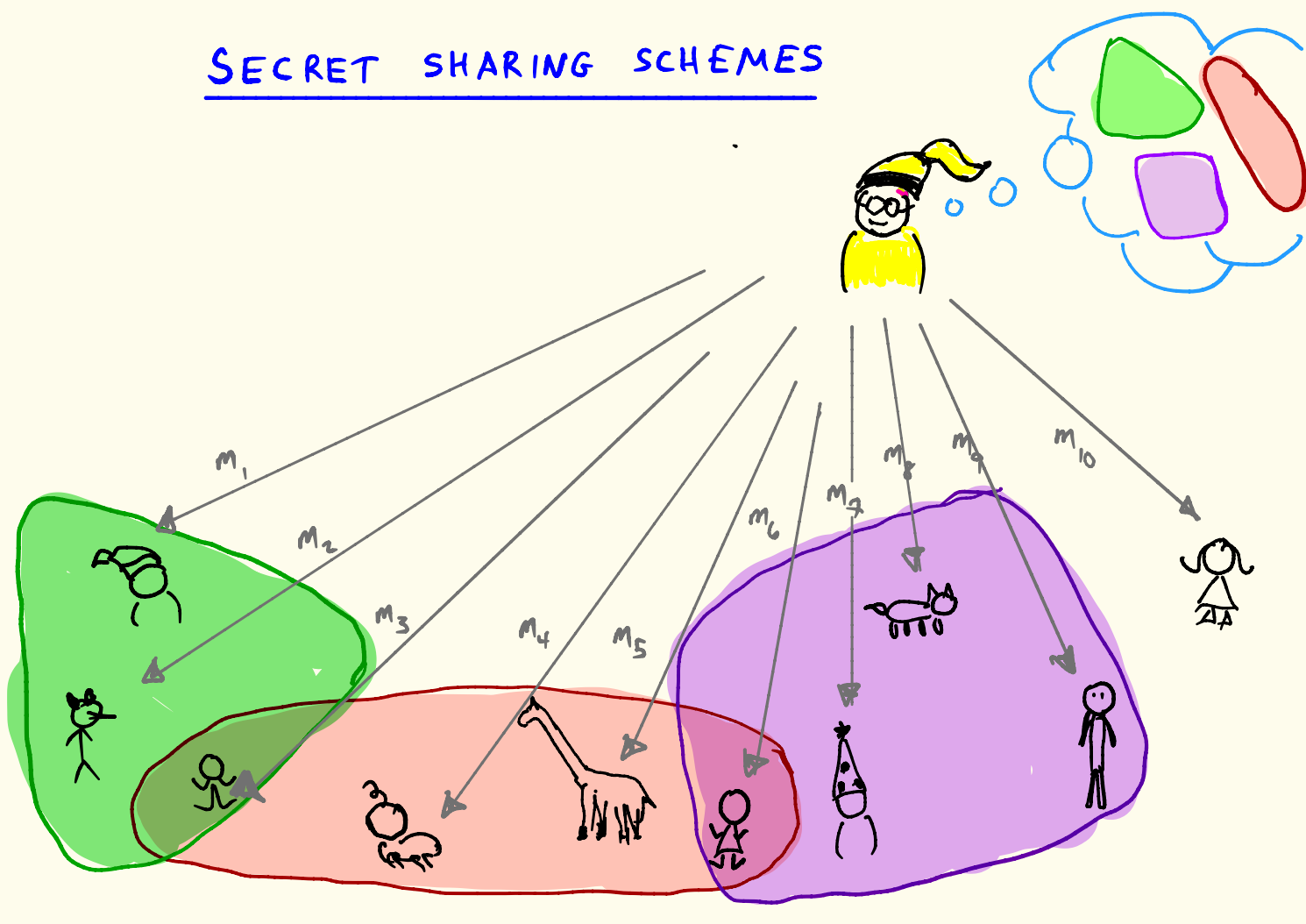
2. Secret sharing schemes (truly exponential on all fields)

SECRET SHARING SCHEMES

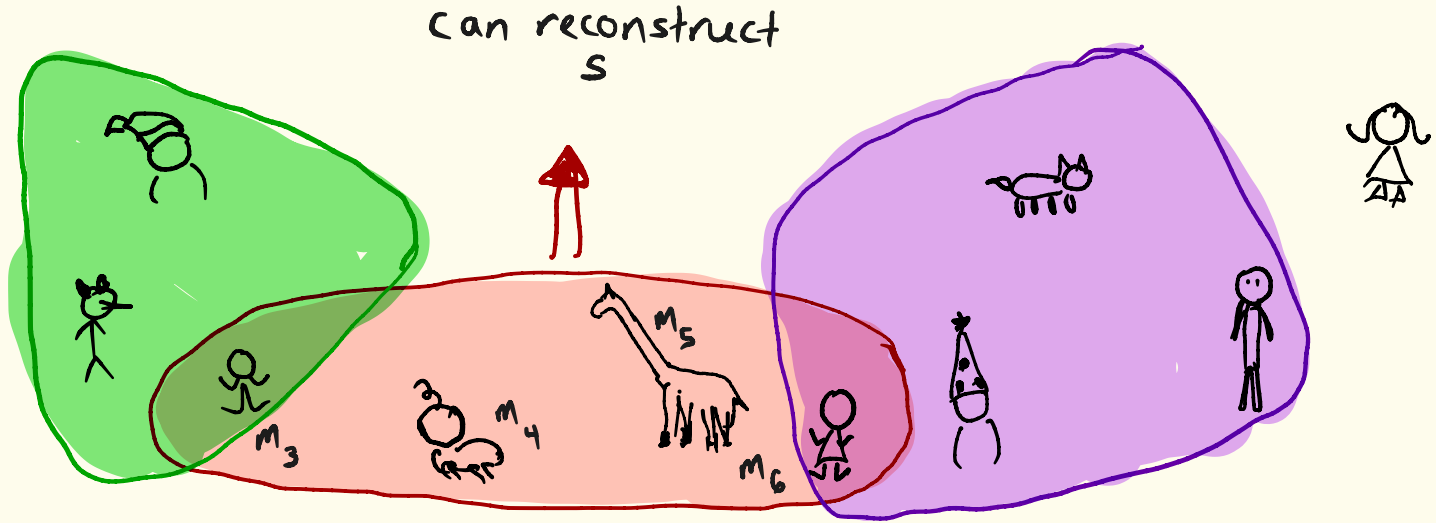
share secret s
with select groups



SECRET SHARING SCHEMES

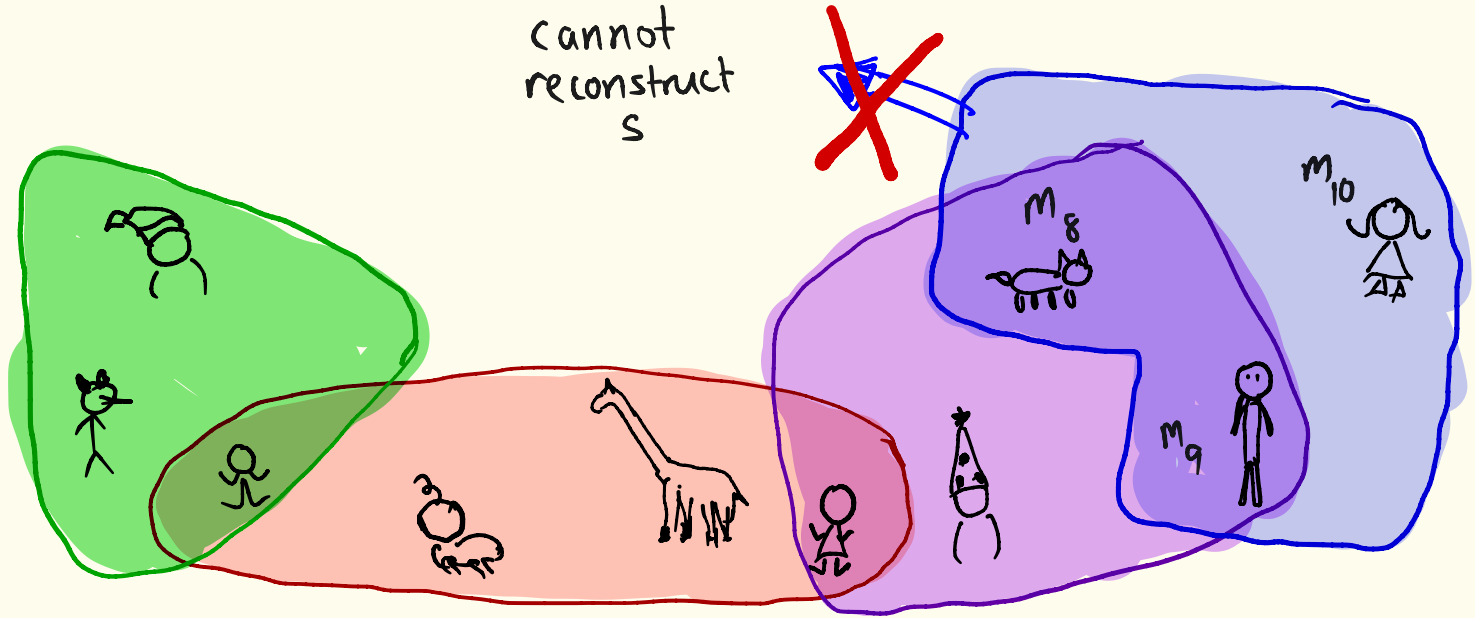


SECRET SHARING SCHEMES



SECRET SHARING SCHEMES

cannot reconstruct s



SECRET SHARING SCHEMES

Introduced by Shamir in 1979

OPEN QUESTION: n parties, and subsets of allowed groups $P_1, \ldots, P_m$, how long must the messages be?

Trivial: $2^{O(n)}$ bits

SECRET SHARING SCHEMES

Introduced by Shamir in 1979

OPEN QUESTION: n parties, and subsets of allowed groups $P_1, \ldots, P_m$, how long must the messages be?

Nearly all (known) schemes are LINEAR...
How long must messages be for LINEAR schemes?

SECRET SHARING SCHEMES

Introduced by Shamir in 1979

OPEN QUESTION: n parties, and subsets of allowed groups $P_1, \ldots, P_m$, how long must the messages be?

Nearly all schemes are LINEAR...
How long must messages be for LINEAR schemes?

A long line of work led to $n^{\Omega(\log n)}$ LOWER BOUNDS [Gál '01]

Progress stalled ...

SECRET SHARING SCHEMES

THEOREM [P, Robere '18]

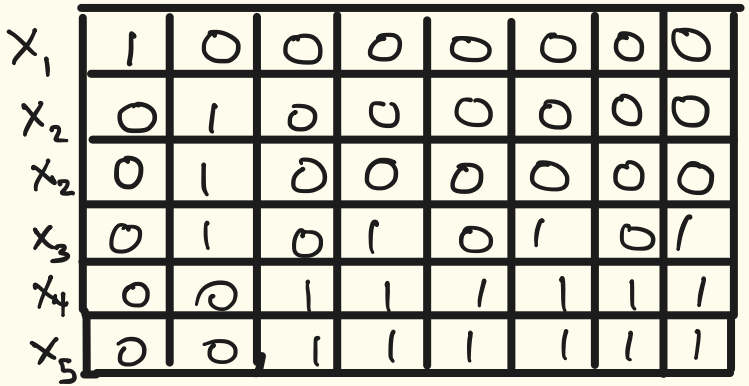
$\forall n$ there is a collection of allowed groups such that any linear sss for these groups requires $2^{\Omega(n)}$ message length.

COROLLARIES

$2^{\Omega(n)}$ LOWER BOUNDS FOR

- MONOTONE SPAN PROGRAMS
- MONOTONE BRANCHING PROGRAMS
- MONOTONE FORMULAS

(MONOTONE) SPAN PROGRAMS [Karchmer-Wigderson]

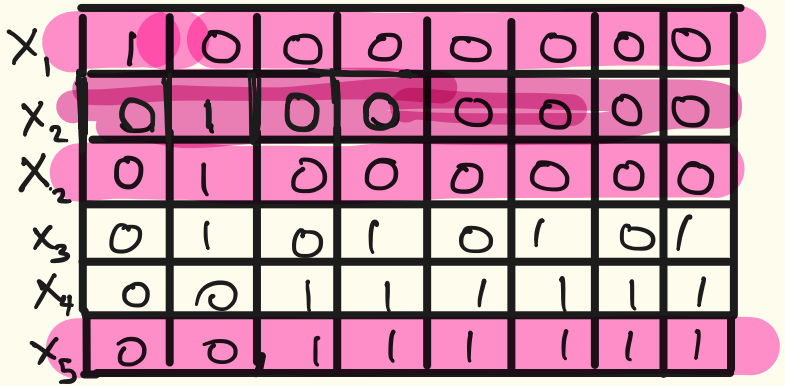


x_1	1	0	0	0	0	0	0	0
x_2	0	1	0	0	0	0	0	0
x_2	0	1	0	0	0	0	0	0
x_3	0	1	0	1	0	1	0	1
x_4	0	0	1	1	1	1	1	1
x_5	0	0	1	1	1	1	1	1

M

accept input α iff $\vec{1}$ in span$(M|_\alpha)$

(MONOTONE) SPAN PROGRAMS



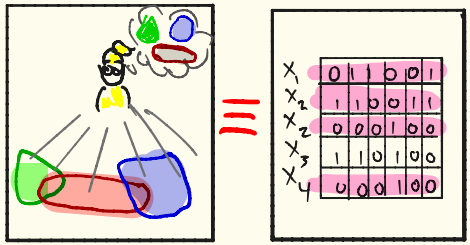
M

Example: $\alpha = 11001$

is accepted !

LINEAR SECRET SHARING LOWER BOUNDS

ALGORITHMS ⇔ COMMUNICATION → PROOFS



Linear SSS

Monotone SPAN

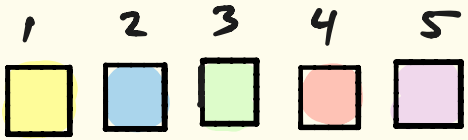
Algebraic Tiling

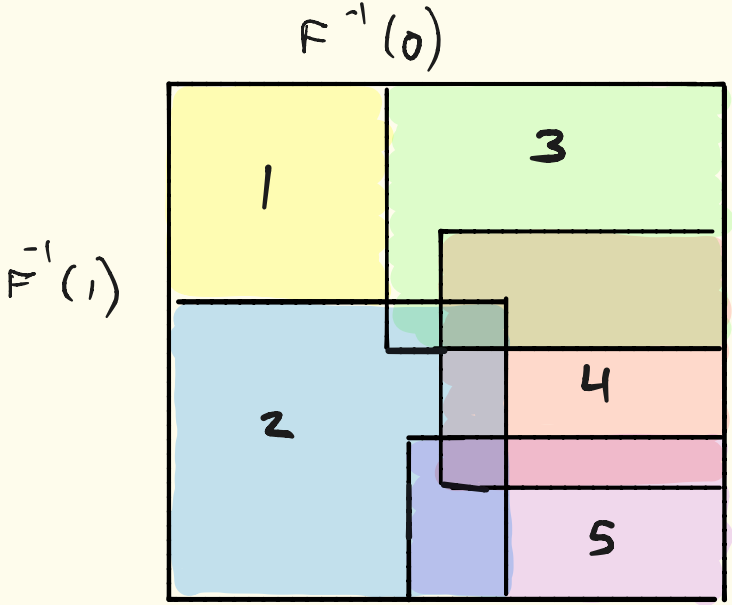
↑

cc-like measure similar to rank for search problems

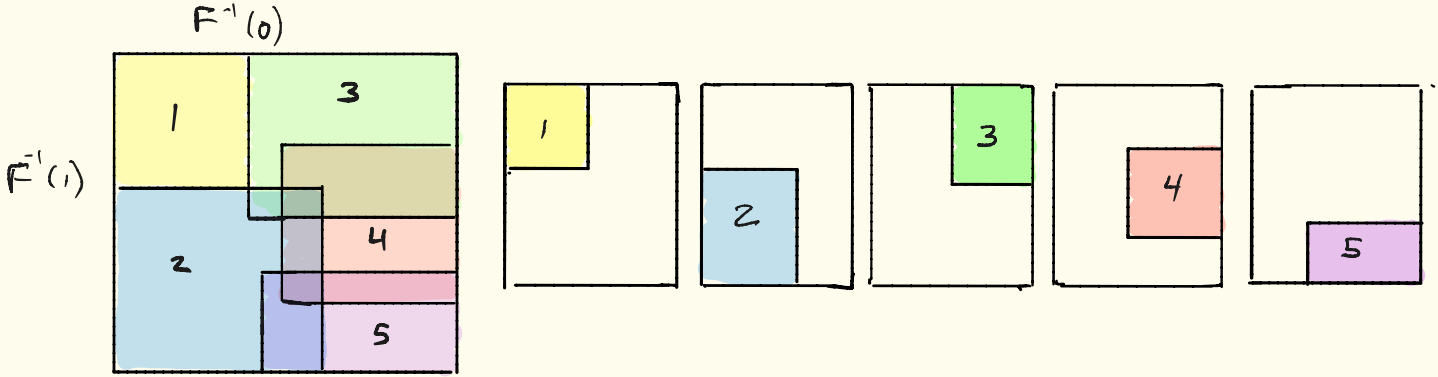
Nullstellensatz Proofs

ALGEBRAIC TILING [gál]

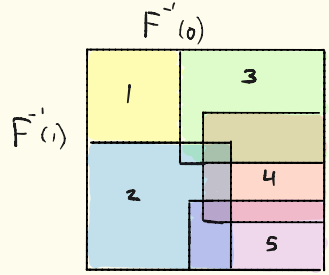


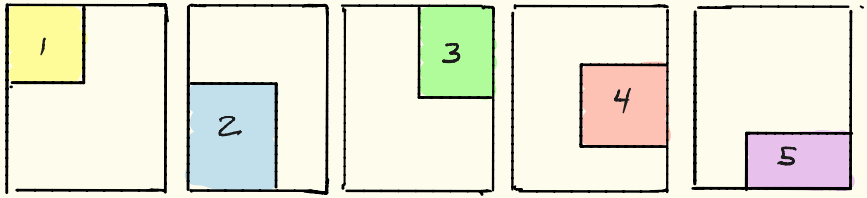


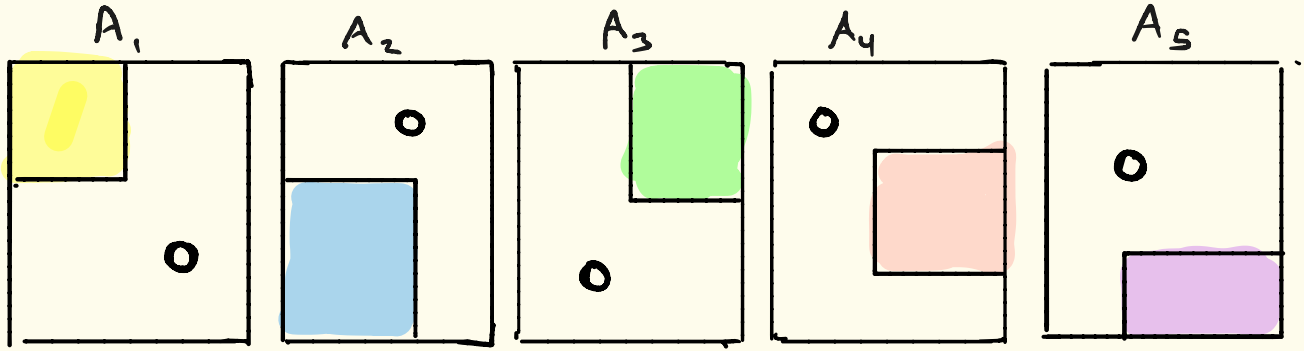
ALGEBRAIC TILING [gá!]



ALGEBRAIC TILING [gál]





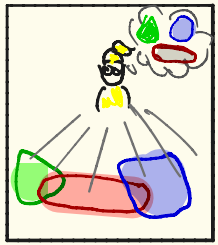


$$A_1 + A_2 + A_3 + A_4 + A_5 = 1$$

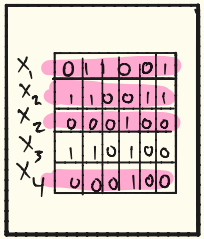
$$\text{Complexity of Tiling} = \sum_i \text{rank}(A_i)$$

II. LINEAR SECRET SHARING LOWER BOUNDS

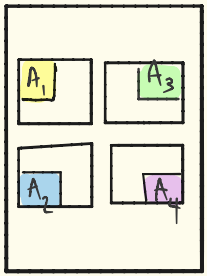
ALGORITHMS ⇔ COMMUNICATION → PROOFS



Linear SSs



monotone SPAN



Algebraic Tiling

Nullstellensatz Proofs

Nullstellensatz Proofs

Let $P = \{p_1 = 0, p_2 = 0, \ldots, p_m = 0\}$ be an unsat system of poly equations over $\mathbb{F}$

A Nullstellensatz Refutation of P is $Q = \{q_1, \ldots, q_m\}$ such that $\sum_{i=1}^{m} p_i q_i = 1$

$NS_{\mathbb{F}}(P)$ = min degree of Nullstellensatz refutation

Nullstellensatz Proofs

Let $P = \{p_1 = 0, p_2 = 0, \ldots, p_m = 0\}$ be an unsat system of poly equations over $\mathbb{F}$

A **Nullstellensatz Refutation** of P is $Q = \{q_1, \ldots, q_m\}$ such that $\sum_{i=1}^{m} p_i q_i = 1$

$NS_{\mathbb{F}}(P)$ = min degree of Nullstellensatz refutation

Lemma $NS_{\mathbb{F}}(P) \approx$ min degree of polynomial that solves search problem for P

LIFTING THEOREM (degree / algebraic tiling)

Theorem 4 [Robere, P]

$$2^{NS(f)} \approx \text{monotone-span}(f \circ g^n)$$

↑ constant-sized gadget

$$2^{NS(\mathcal{C})} \approx \text{algebraic-tiling}(\mathcal{C} \circ g^n)$$

$$= \text{monotone-span}(F_{\mathcal{C}})$$