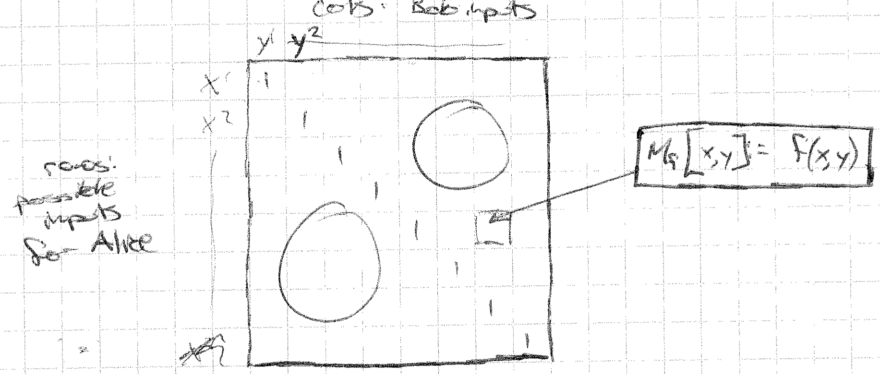
Open Problems

I log-rank Conjecture

$f: X \times Y \longrightarrow \{0,1\}$

Communication Matrix M_f



<u>Defn</u> $\text{rank}(f) :=$ rank of M_f over reals.

<u>Rank Lower Bound</u> $D(f) \geq \log_2(\text{rank}(M_f))$ [Mehlhorn–Schmidt '82]

<u>proof</u> A deterministic protocol partitions communication matrix into <u>monochromatic</u> rectangles

$R = A \times B \;:\; A \subseteq X,\ B \subseteq Y, \quad f(x,y) = f(x',y') \quad \forall\ x,x' \in A$ and $y,y' \in B$

Fix a protocol P, and look at leaves in protocol that give 1-outputs
look at 1-rectangles corresponding to leaves in protocol.

For each, define matrix M_ℓ: $M_\ell[x,y] = \begin{cases} 1 & \text{if } (x,y) \in R_\ell \\ 0 & \text{otherwise} \end{cases}$

Then $M_f = \sum_{\text{1-leaf}} M_\ell$

By rank properties (subadditivity) $\text{rank}(M_f) \leq \sum \text{rank}(M_\ell)$

$\Rightarrow \text{rank}(M_f) \leq \#\text{ 1-leaves} \leq 2^{D(f)}$

This allows us to use ~~da~~ linear algebraic techniques to prove lower bounds.

<u>Log-rank Conjecture:</u> $D(f) = (\log \text{rank}(f))^{O(1)}$ for all $f: X \times Y \to \{0,1\}$.

current state of the art: ~~$\log(\text{rank})^{1.631} \leq D(f) \leq$~~

[Kotlov 97]

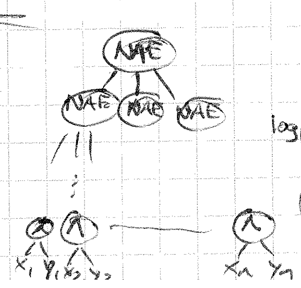
$\log(\text{rank}(f))^{1.631} \leq D(f) \leq 0.415\ \text{rank}(f)$

[Kushilevitz '16] for one function

NOT-ALL-EQ: 1 if 1 or 2 inputs = 1, 0 if 0 or 3 inputs = 1

~~$h(z_1, z_2, z_3) = z_1 + z_2 + z_3 - z_1 z_2 - z_1 z_3 - z_2 z_3$~~

h



$D(h) = \Omega(n)$

$\log(\text{rank}(M_h)) = O(n^{0.631\ldots})$

$(\log \text{rank}(M_h))^{1.58\ldots} = D(h)$

NOF CC and circuit complexity

ACC^0: constant depth, polynomial size circuits w/ AND, OR, NOT, MOD_m gates

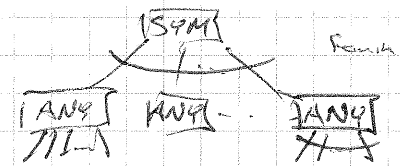
MOD_m: output 1 if # on inputs ≡ 0 mod m
0 oth

open problem: give explicit function $f \notin ACC^0$
$MAJ \notin ACC^0$?

recent: $NEXP \not\subseteq ACC^0$ ~~Ryan~~ [Williams 11]

Early 90's Håstad-Goldmann, Beigel-Tarui, Yao: $ACC^0 \subseteq SYM^+$

SYM^+: depth 2 circuits



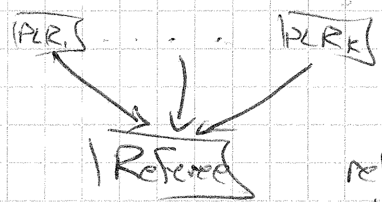
fan-in: quasipolynomial $= 2^{\Theta(\text{polylog}(n))}$

fan-in ~~k-1~~ $\text{polylog}(n) =: k-1$

Note: Williams uses this connection

~~Fact: If $f \in SYM^+$ then it has NOF protocol w/ k players and each send poly~~ ~~→ O(polylog(n)) SM~~

Fact if $f \in SYM^+$ then it has a $k = \text{polylog}(n)$ player, $O(\text{polylog}(n))$-bit simultaneous message (SM) protocol



each plr sends single message

Referee sees no input; outputs answer

proof ~~W~~ adversarily distribute inputs to players
each ANY gate has fan-in $k-1$ so some player can compute it

Protocol: Assign ANY gates to players
Each player counts # ANY gates evaluate to 1
Referee adds them up, computes SYM^+ function.

Corollary if $\exists$ f which requires $n^{0.001}$ communication in SM model for $k = \text{polylog}(n)$ players then $f \notin ACC^0$. ← Another big problem: find such a function

Candidate function Pointer Jumping MPJ_k

3 player version: Alice has $i \in [n]$ on forehead
Bob has $f: [n] \to [n]$
Carol has $x \in \{0,1\}^n$

$$MPJ_3(i, f, x) = x[f(i)]$$

k player version: $MPJ_k(i, f_2, \dots, f_{k-1}, x) = x\Big[f_{k-1}(f_{k-2}(\dots(f_2(i))\dots))\Big]$

known: $D(MPJ_3) = O\left(n\sqrt{\frac{\log\log n}{\log n}}\right)$ [Brody-Chakrabarti 08]
[Pudlak-Rödl-Sgall 97]

$R^{\rightarrow}(MPJ_k) \geq \frac{n^{1/k-1}}{k^{O(k)}}$ [Viola-Wigderson ~~10~~ 07]

$R(MPJ_3) = \Omega(\sqrt{n})$

log-rank is one of these embarrassing conjectures that ~~[illegible]~~ we haven't made much progress on, until very recently

An additive combinatorics approach ~~for~~ relating rank to communication complexity
Ben-Sasson, Lovett, Ron-Zewi FOCS 12

Polynomial Freiman-Ruzsa Conjecture

Thm PFR conjecture $\Longrightarrow$ $D(f) = O\left(\frac{\text{rank}(f)}{\log \text{rank}(f)}\right)$.

For $A \in \mathbb{F}_2^n$
$A+A = \{a+a' : a,a' \in A\}$

$\exists r$ s.t. if $|A+A| \le K|A|$
then $\exists A' \subseteq A$ of size
$|A'| \ge K^{-r}|A|$ s.t.
$|\text{span}(A')| \le |A|$

Note: Such a thm exists w/ K^{-r} replaced by $K^{O(-\lg^3 K)}$

Freiman Ruzsa Thm: $|A+A| \le K|A|$
$\Rightarrow |\text{span}(A)| \le K^2 2^{K^4}|A|$
exponential dependence on K is necessary

Numbers on the Forehead (NOF) complexity

k-players, goal: compute $f(x_1, \ldots, x_k)$ $\quad x_1, \ldots, x_k \in \{0,1\}^n$

Communication Models
- Number in hand: PLR$_i$ sees x_i
- Number on Forehead: PLR$_i$ sees all inputs except x_i

In NOF protocols, lots of information/input is shared
- This makes computing f easier
- This makes proving NOF lower bounds harder

Big Open Problem: Give an explicit function $f: \{0,1\}^{n \times k} \to \{0,1\}$ for $k = \text{polylog}(n)$ s.t. $R_{1/3}^{NOF}(f) = \omega(\log n)$

~~The BNS-Chung Criterion for Multiparty~~

State-of-the-art lower bounds: $\Omega(n/2^k)$
- based on discrepancy extensions:
- works for randomized CC

$C_{\frac{1}{2}-\delta}(f) = \Omega(\log(\delta/\text{Disc}(f)))$

Meta-question: How to bound $\text{Disc}(f)$?

Reading:
- BNS-Chung Criterion for Multiparty CC [Raz 00]
- The Pattern Matrix Method [Sherstov 08]
- Multiparty CC of DISJ [Sherstov 12]

One example: Generalized Inner Product $\quad GIP(x_1, \ldots, x_k) = \text{PARITY}(\# i \text{ s.t. } x_j[i] = 1\ \forall j)$

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

$R(GIP) = \Omega\left(\frac{n}{4^k}\right)$

NOF CC and Dynamic Data Structures [Patrascu 10]

Dynamic Data Structures: store data, support queries in t_q time
updates in t_u time

by "time" we mean # memory references

Goal: minimize $\max\{t_q, t_u\}$
Best known
$$t_u + t_q = \Omega\left(\left(\frac{\log n}{\log\log n}\right)^2\right) \quad \text{[Larsen 12]}$$

Suspected $\quad t_u + t_q = \Omega(n) \quad$ for many problems

Multiphase Problem I Given k sets $S_1, \dots, S_k \subseteq [n]$
Preprocess in $O(nk\tau)$ time

II Given set $T \subseteq [n]$, update DS in $O(n \cdot \tau)$ time

III Given $i \in [k]$ answer $S_i \cap T = \emptyset$? in $O(\tau)$ time

Conjecture $\exists\ \gamma > 1, \delta > 0$ s.t. for $k = \Theta(n^{1+\delta})$ solving Multiphase requires $\tau = \Omega(n^{\delta})$.

Note: Multiphase reduces to all sorts of dynamic DS problems.
~~NOF version of Multiphase~~ $\Rightarrow$ thus lower bound implies polynomial l.b.s for lots of other problems

NOF version of Multiphase

Alice gets $i \in [n]$ (on forehead)

Bob gets $S_1, \dots, S_k$

Carol gets T

Goal: Decide if $S_i \cap T = \emptyset$?

Communication: Alice sends single message of $n \cdot M$ bits to Bob
Bob-Carol ~~speak~~ talk to each other, using M bits total

Conjecture: for $k = \Theta(n^{\delta})$ must have $M = \Omega(n^{\delta})$

This l.b. implies lower bound on multiphase.

[Chattopadhyay + SODA 12] can solve NOF problem in $\tilde{O}(\sqrt{n})$ communication

This is surprising and goes against intuition that this should be directsum.

Direct Sum Does computing m copies of a function cost m-times the communication?

[Barak Braverman Chen Rao 10]

① For all $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, for all $\alpha > 0$

$$R_\rho(f^m) = \tilde{\Omega}\left(R_{\rho+\alpha}(f) \cdot \alpha \cdot \sqrt{m}\right)$$

② If μ is a product distribution $\quad D_\rho^{\mu^m}(f^m) = \tilde{\Omega}\left(D^\mu_{\rho+\alpha}(f)\,\alpha^2 m\right)$

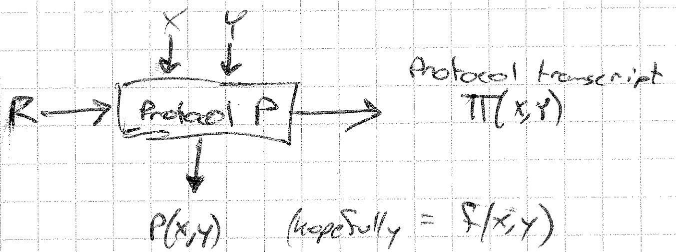
[Jain Pereszlényi Yao FOCS 12]

Achieves direct sum for t-round protocols $\quad \cancel{R^t_{1-(1-\varepsilon/2)^{\Omega(k\varepsilon^2/t^2)}}}$

$$R^t_{\varepsilon'}(f^m) = \Omega\left(\frac{\varepsilon m}{t}\left(R^t_\varepsilon(f) - \frac{kt^2}{\varepsilon}\right)\right)$$

where $\varepsilon' = 1 - (1-\varepsilon/2)^{\Omega(k\varepsilon^2/t^2)}$

method: Information complexity



External IC

$$I(XY;\Pi(X,Y)\mid R)$$

Internal IC

$$I(X;\Pi(X,Y)\mid R,Y) + I(Y;\Pi(X,Y)\mid R,X)$$

Techniques: protocol compression: if P has high CC but low IC
replace w/ P' that has CC ~~—~~ in terms of IC