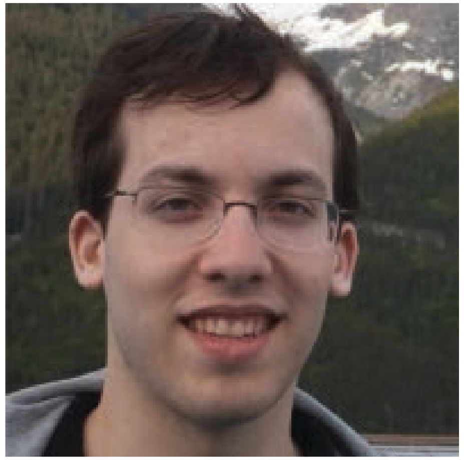
Separating Quantum Communication and Approximate Rank

Anurag Anshu Shalev Ben-David Ankit Garg

Rahul Jain Robin Kothari Troy Lee

Anurag Anshu



Shalev Ben-David

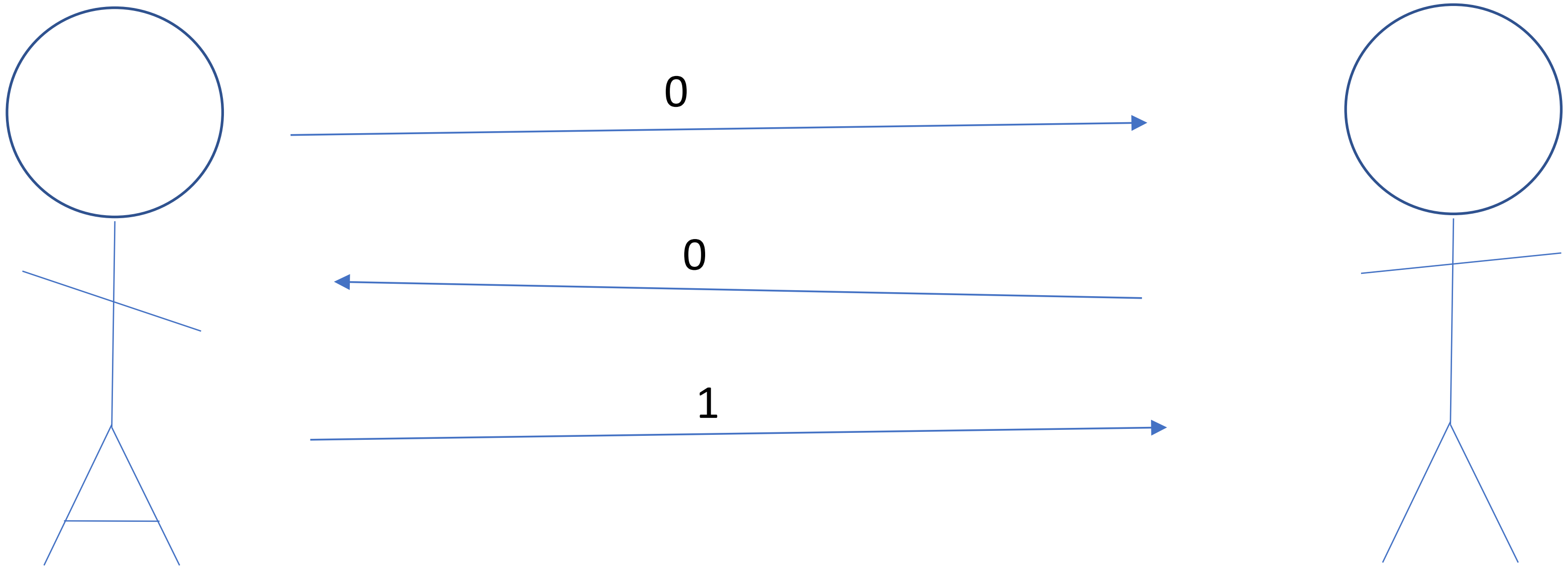
Ankit Garg

Rahul Jain

Robin Kothari

Troy Lee

Communication complexity



$x \in \{0,1\}^n$

$y \in \{0,1\}^n$

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

Quantum communication complexity

- Alice and Bob can exchange qubits
- They can start with shared entanglement
- They can err with bounded probability (say, 1/3)

- $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is known in advance
- $Q^{cc}(F)$ = minimum number of qubits exchanged in the best protocol
- Note: for all F, $Q^{cc}(F) \leq n$

Query vs. Communication

Query Complexity

- Studies queries

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

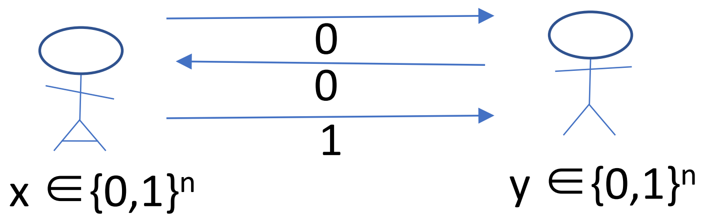
	0		1	0			

- Is easy

Communication Complexity

- Studies communication

$$F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$$



- Is hard

(Recommendation: work on query complexity!)

Query vs. Communication

- Q: How many different deterministic 1-query algorithms?
- A: n (where n is the input size)

- Q: How many different deterministic 1-bit communication protocols?
- A: 2^{2^n} (where n is the input size)
- (Because the bit Alice sends to Bob can be any function of her input, and there are 2^{2^n} different functions on n bits)

- How on Earth do we lower bound communication complexity?

A long time ago, in the previous talk….

- Approximate degree was a useful lower bound technique for quantum query complexity
- It was thought to be defeated after Ambainis's adversary method (and its generalization to negative weights) was introduced
- But it can still strike back

- In communication complexity: approx degree is approx logrank
- It has never been defeated – no adversary methods
- Until now (a new hope?)

"logrank"?

- Consider a communication task in terms of the communication matrix
- For example, consider EQUALITY

Bob

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

- What does a (deterministic) protocol look like?

“logrank”?

- Consider a communication task in terms of the communication matrix
- For example, consider EQUALITY

Bob

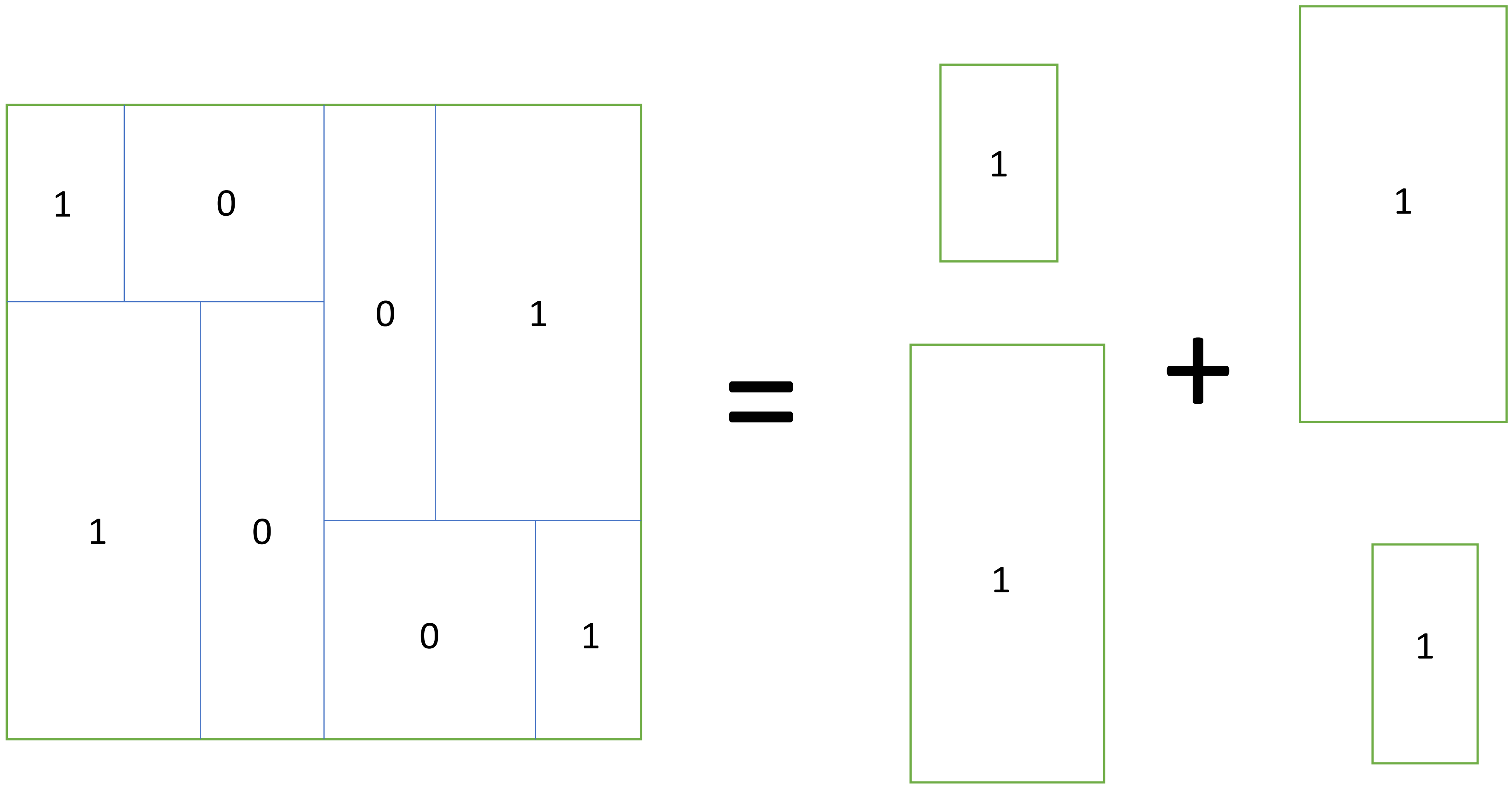
- If Alice said “1”: say “my input is/isn’t 00”
- If Alice said “0”: say “first bit is/isn’t 1”

“my input is (or isn’t) 00”

Alice

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

- What does a (deterministic) protocol look like?


1
0
0
1
1
0
0
1
=
1
1
+
1
1

Logrank as a lower bound on communication

- If there is a T-round protocol for F…
- Then the matrix of F can be decomposed into 2^T rectangles…
- Which means the rank of the matrix is at most 2^T

- Hence $D^{cc}(F) \geq \log \text{rank}(F)$
- Logrank is a measure that lower bounds communication complexity!
- It is also easy to compute (polynomial in 2^n, the size of the matrix)
- However, logrank(F) is not equal to $D^{cc}(F)$
- Conjecture: logrank(F) is polynomially related to $D^{cc}(F)$

logrank ≈ polynomial degree

Query Complexity

- Partial assignments

  ≈

- Monomials

- Linear combination of few monomials

  ≈

- Low-degree polynomial

Communication Complexity

- Rectangles

  ≈

- Rank-1 matrices

- Linear combination of few rectangles

  ≈

- Low-rank matrix

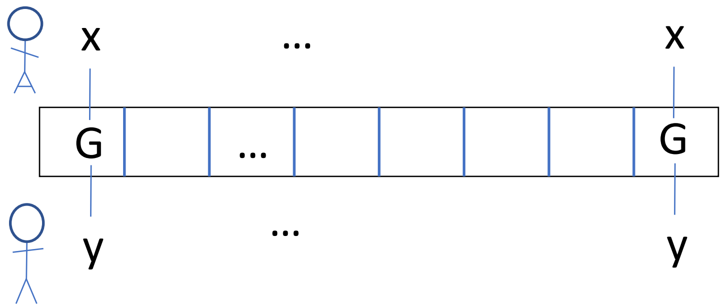
Approximate logrank

- Logrank of an approximating matrix
- The min, out of all matrices M that are pointwise 1/3 close to F, of logrank(M)
- Lower bounds quantum communication complexity
- Communication analogue of approximate degree (polynomial method)

- Our result here: exists F for which $Q(F) \geq \text{alogrank}(F)^{4-o(1)}$
- “polynomial method in communication complexity is far from tight”
- No separation previously known

Lifting Theorems

- Let $f:\{0,1\}^n \rightarrow \{0,1\}$ be any query function
- Fix a small communication task G, usually inner product on 2x2 bits (or log n bits)
- Define f∘G by replacing each input bit of f with G
  - Alice gets all the x's, Bob gets all the y's



- Compare: query complexity of f vs. communication complexity of f∘G
- "Lifting theorem": complexity of f (in some query model) is the same as that of f∘G (in a similar communication model)

Lifting Theorems

- GPW15, RM99: $D(f) \approx D^{cc}(f \circ G)$ (G is log n size)
- GPW17, ~~AGJKM17~~: $R(f) \approx R^{cc}(f \circ G)$ (G is log n complexity)
- folklore: $\deg(f) \approx \mathrm{logrank}(f \circ G)$ (G is constant size)
- Sherstov09: $\mathrm{adeg}(f) \approx \mathrm{alogrank}(f \circ G)$ (G is constant size)
- Conjecture: $Q(f) \approx Q^{cc}(f \circ G)$
- If you can prove this conjecture, our work here is obsolete!
  - Because we already have query function f with $Q(f) \geq \mathrm{adeg}(f)^{4-o(1)}$…
  - So a lifting theorem would imply $f \circ G$ has $Q^{cc}(f \circ G) \geq \mathrm{alogrank}(f \circ G)^{4-o(1)}$
- This happened to our QIP talk last year!

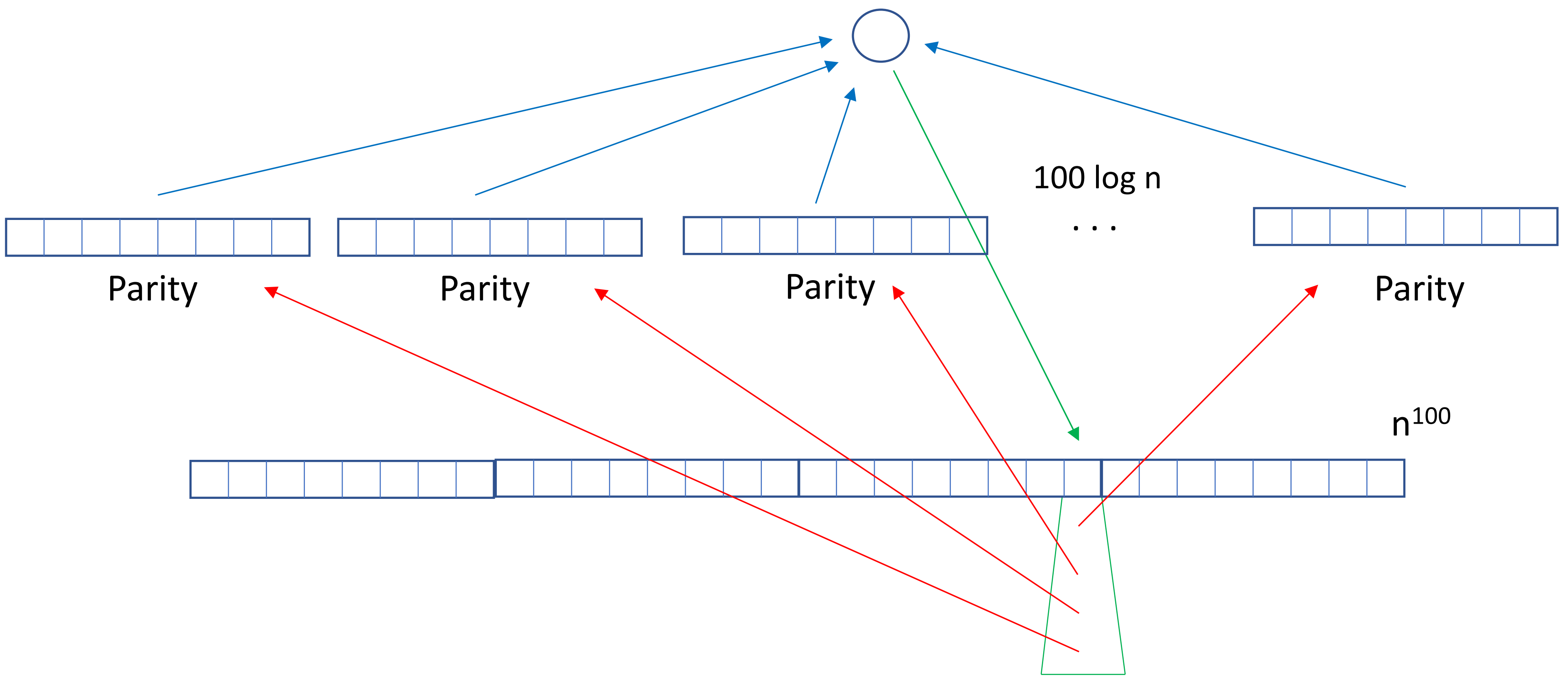
Proving the separation

- Approach 1: Ambainis's adversary method
  - Problem: no adversary method in communication complexity!

- Approach 2: cheat sheet method
- Cheat sheets do two things:
  - Turn partial functions into total functions (sort of)
  - They decrease the degree (sometimes)

- Our only hope: cheat sheets in communication complexity

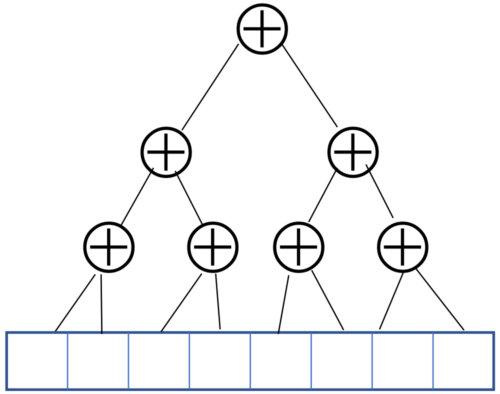
Cheat sheets in query complexity



- Cheat sheet tells us something about parity that makes it easier to certify

Making parity easy to certify

- Certificate complexity of parity is n
- To convince you the input string has parity 0, I have to show you all the bits
- But what if you're quantum?

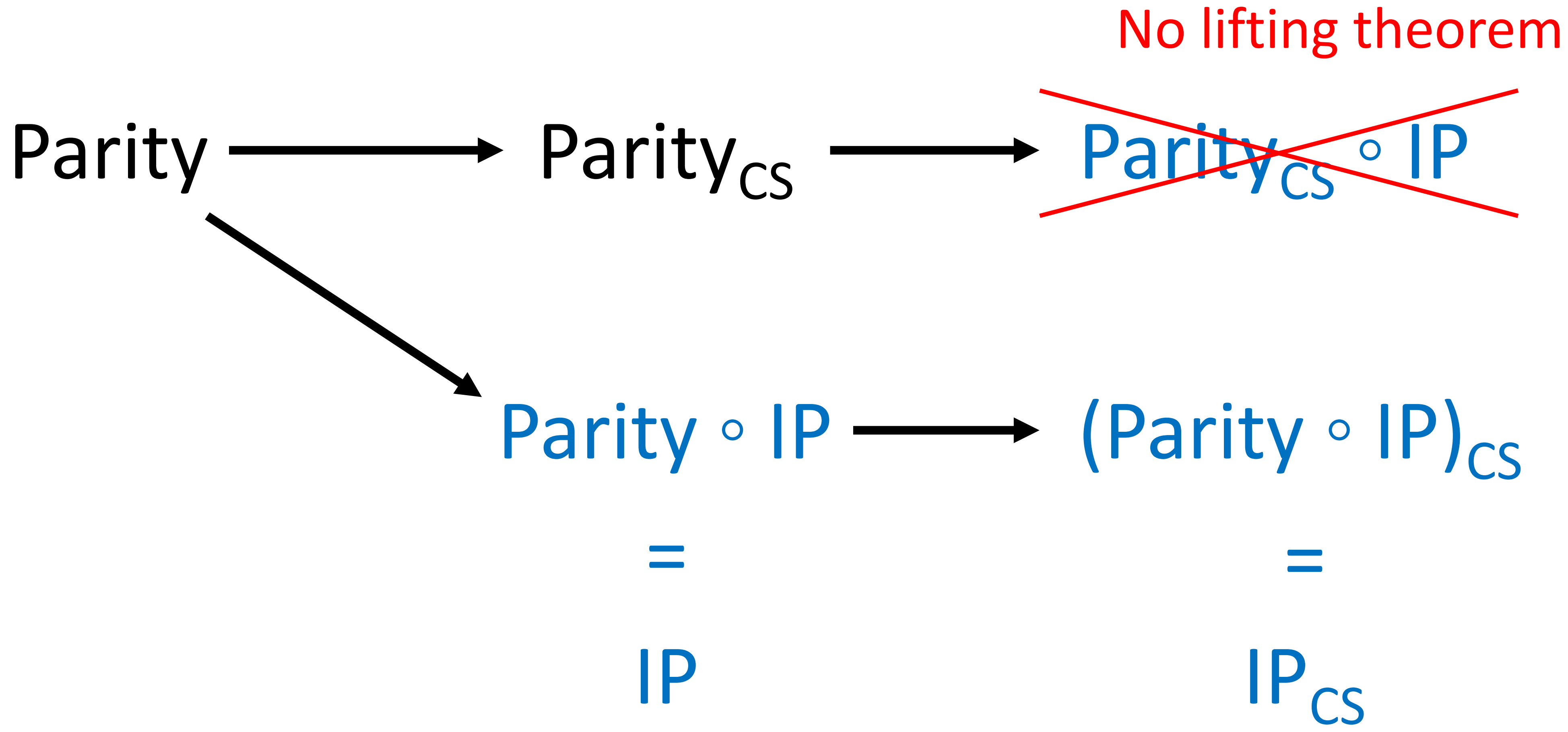


- Trick: parity has a circuit of size O(n)
- I will give you the output of each gate
- You Grover search for a wrongly-computed gate!
- <u>Upshot</u>: if f has circuit size n, then $adeg(f_{CS})=O(\sqrt{n})$
  - If you can find f with $adeg(f_{CS}) \gg \sqrt{n}$, you get circuit lower bounds

Lifting to communication complexity

- $\text{adeg}(\text{Parity}_{CS}) \approx \sqrt{n}$
- $Q(\text{Parity}_{CS}) \approx n$
- Take gadget $G = IP_{\log n}$
- Consider $\text{Parity}_{CS} \circ G$
- Have $\text{alogrank}(\text{Parity}_{CS} \circ G) \approx \sqrt{n}$
- Conjecture $Q^{cc}(\text{Parity}_{CS} \circ G) \approx n$

- Too hard to prove the quantum lower bound



No lifting theorem
Parity
Parity_{CS}
$\text{Parity}_{CS} \circ \text{IP}$
$\text{Parity} \circ \text{IP}$
$(\text{Parity} \circ \text{IP})_{CS}$
=
=
IP
IP_{CS}

Cheat sheets in communication complexity

- Step 1: define IP_{CS}
  - 100 log n copies of IP
  - Alice and Bob get an additional part of the input, consisting of n^{100} cells, but they must XOR their inputs to read a cell
- Step 2: prove alogrank(IP_{CS}) ≤ $O(\sqrt{n})$
  - Not hard
- Step 3: Prove $Q^{cc}(IP_{CS}) \geq \Omega(n)$
  - Idea: add coauthors until the problem is solved

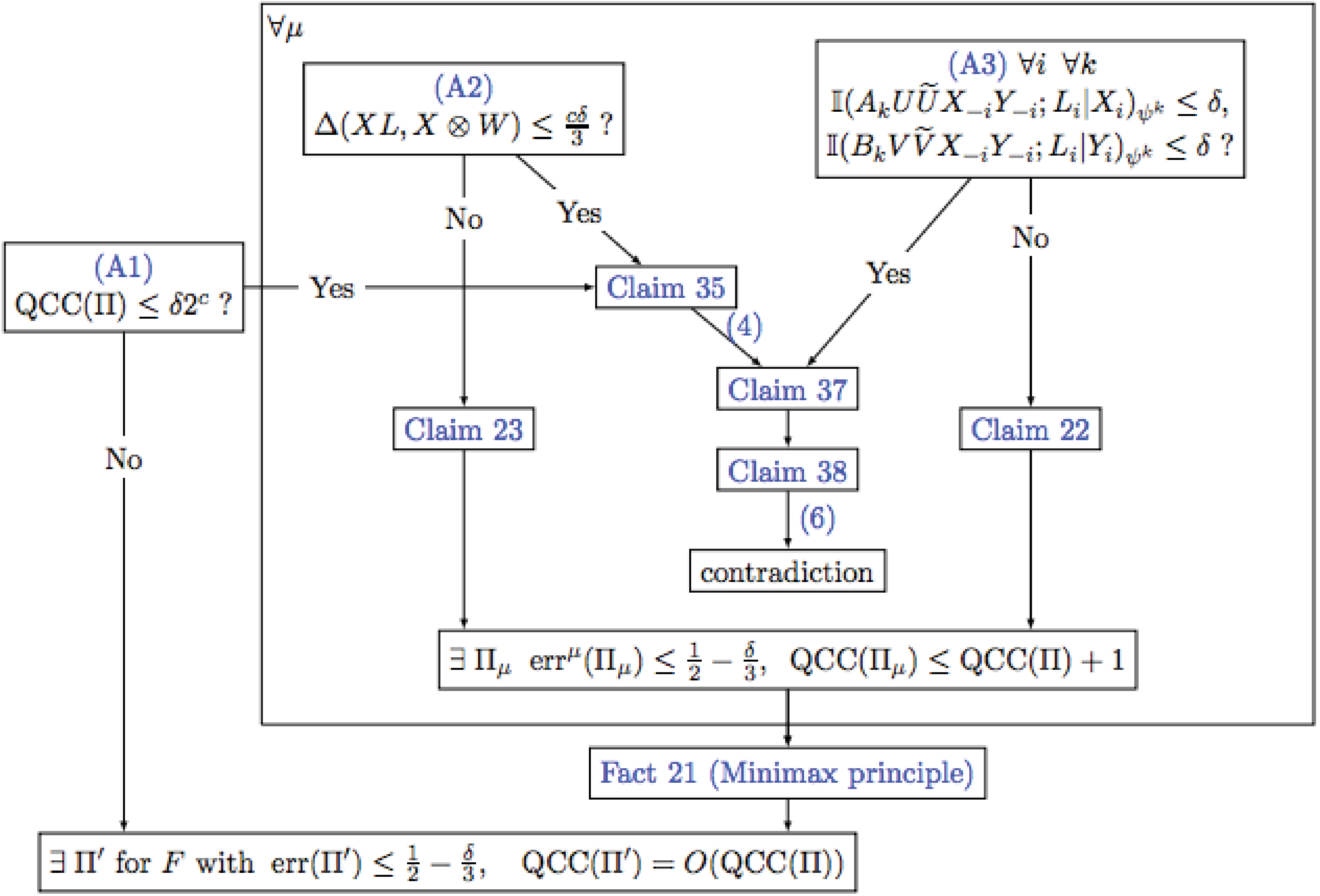


Figure 2: The structure of the proof of Theorem 33. Note that Claim 35 and Claim 37 only follow if both of their incoming arcs hold.

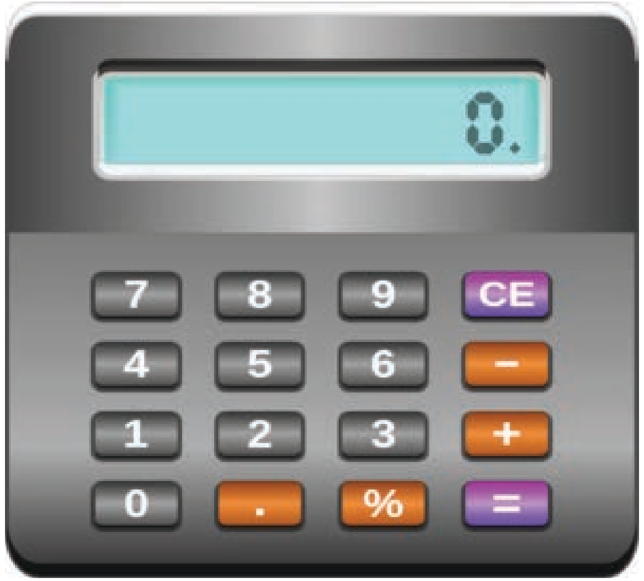
Cheat sheets in communication complexity

- We prove a general cheat sheet theorem for Q^{cc} (sort of): $Q^{cc}(f_{CS}) = \Omega(Q^{cc}_{1/poly(n)}(f))$
- Get a lower bound on f_{CS} from a lower bound on small-bias quantum communication for f
- This is fine when f=IP (discrepancy method)

- Conclusion: $Q^{cc}(f_{CS}) \geq \text{alogrank}(f_{CS})^2$

- What about the power 4 separation?
- First, recall the query version of the separation

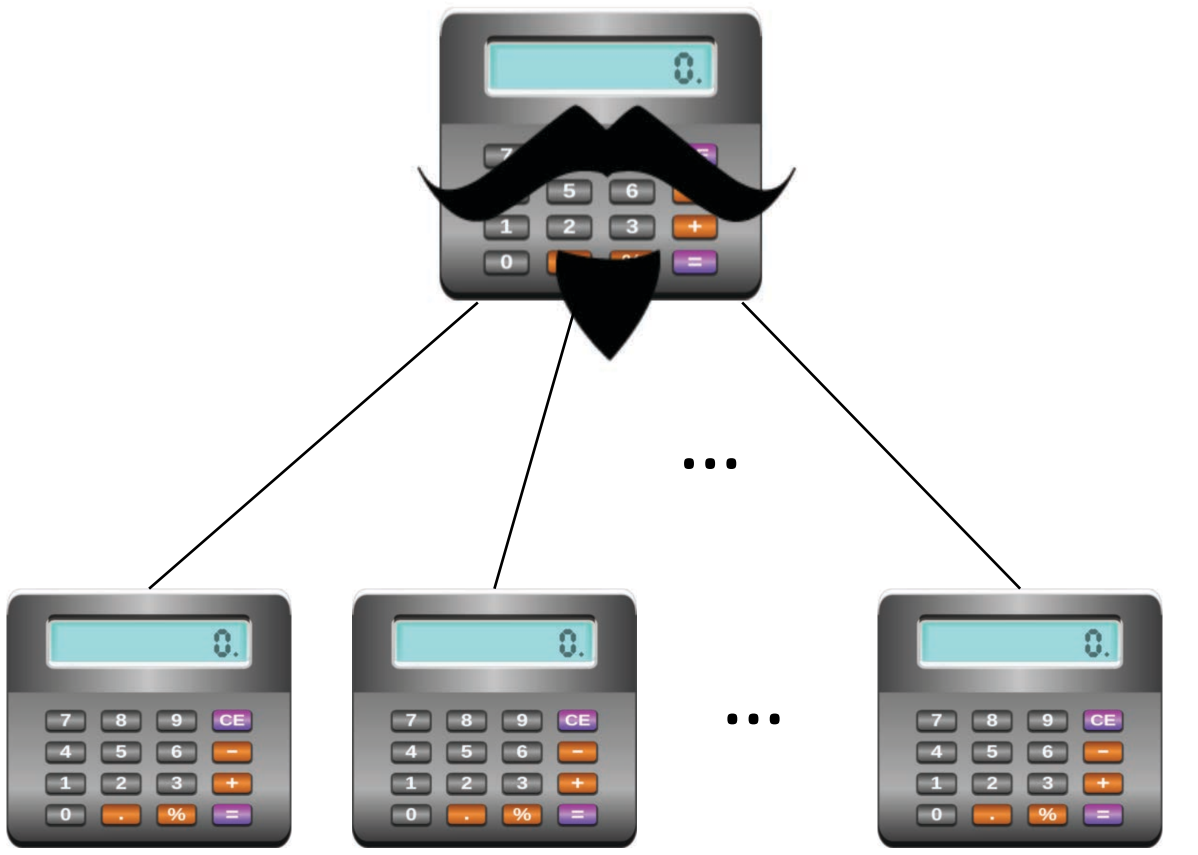
k-Sum (Belovs-Spalek 2012)



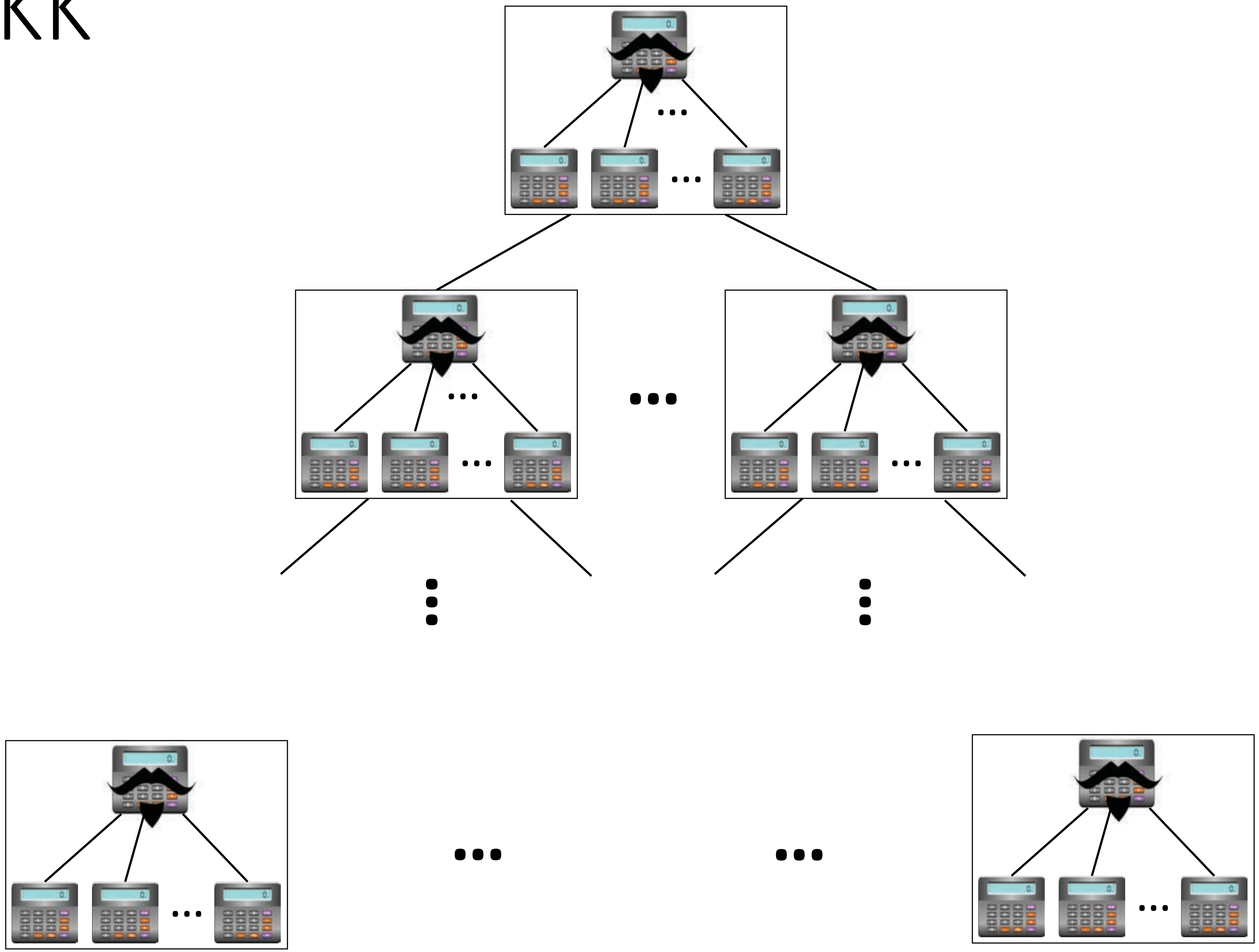
Block k-Sum

- A negated variant of k-sum

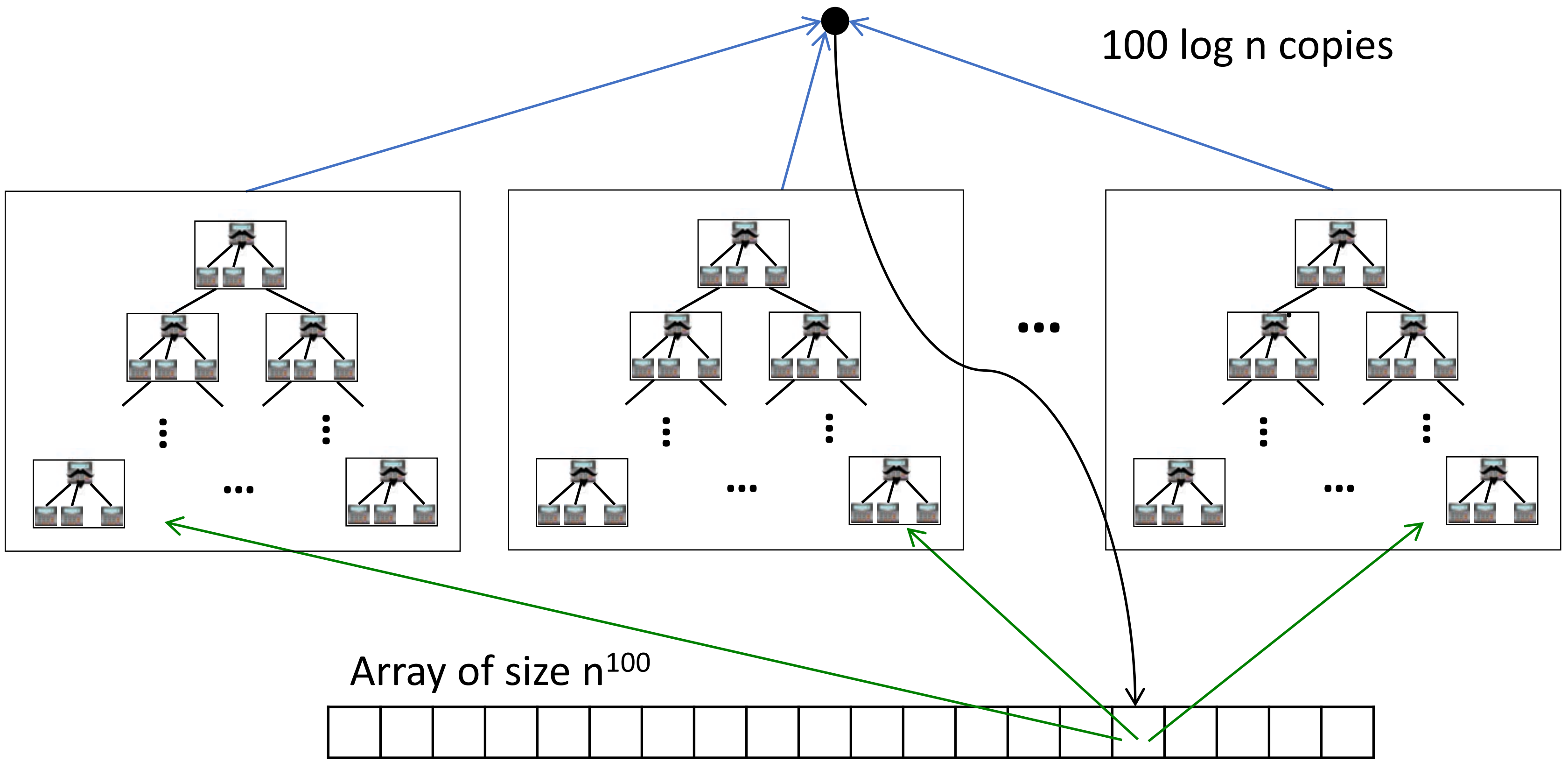
BKK



RecBKK



$RecBKK_{CS}$



$Q \approx adeg^{4-o(1)}$

Recipe for power 4 separation

- Ingredients:
  - A Boolean function g such that $\mathrm{adeg}(g) \geq C(g)^2$ (Bun, Thaler)
  - An XOR lemma for approximate degree (Sherstov)
  - A composition theorem for adeg-with-low-bias (folklore, Bun-Thaler)
  - A lifting theorem for alogrank (Sherstov)
  - Our quantum communication cheat sheet theorem
- Instructions:
  - Take g above, and write $h := \mathrm{Parity}_{\log n} \circ g$. Apply XOR lemma
  - Compose h with itself a bunch of times, get f. Apply composition theorem
  - Lift to communication task F by composing with IP_2. Apply lifting theorem
  - Add a cheat sheet. Apply cheat sheet theorem
  - Use the small C(f) and the self-composed nature of f to show certificates can be quantumly checked as fast as $\mathrm{adeg}(f)^{1/4}$
  - Conclude that $\mathrm{alogrank}(H_{CS}) \approx \mathrm{adeg}(f)^{1/4}$, $Q(H_{CS}) \approx \mathrm{adeg}(f)$. Serve fresh

Open problems

- Do you even lift?
  - Prove a lifting theorem for quantum communication complexity
- Separate quantum information complexity from alogrank
  - Our techniques don't quite do this
- Find better lower bound techniques for Q^{cc}
  - A communication version of the adversary bound?

Next talk: Adam Bouland

- Previous talk: polynomials lower bounding quantum algorithms
- This talk: polynomials and quantum algorithms are separate
- Next talk: quantum algorithms lower bounding polynomials

- The story of Darth Belovs the Wise?
- (Not a story the classical complexity theorists would tell you)

Thanks!