

On Beating the Hybrid Argument

Bill Fefferman (Caltech)

Joint with Ronen Shaltiel (Haifa),
Chris Umans (Caltech), and
Emanuele Viola (Northeastern)

Hybrid Argument

- U uniform distribution over binary strings
- $G: \{0,1\}^N \rightarrow \{0,1\}^M$
- [Yao '82] Suppose we have a circuit C that ϵ -distinguishes U_M from $G(U_N)$, then there is a similar size “predictor circuit” P


$$| \Pr[C(U_M) = 1] - \Pr[C(G(U_N)) = 1] | > \epsilon$$

$$\Rightarrow \Pr_{x \sim U}[P(G(x)_{1 \dots i-1}) = G(x)_i] > \frac{1}{2} + \epsilon/M$$

- Contrapositive: Unpredictability \Rightarrow Indistinguishability
 - Hybrid loss becomes hurdle when $M \gg 1/\epsilon$

Our results

We show the following consequences can be achieved if the loss of the hybrid argument can be avoided:

1. Oracle relative to which **BQP** $\not\subseteq$ **PH**  Today's focus
2. Better pseudorandom generators for small space
 - E.g., prove output of INW generator with seed length $O(\log n \log \log n)$ is unpredictable with advantage $1/\log n$ against polylog width read-once branching programs

Prove that such a beating is possible in restricted cases:

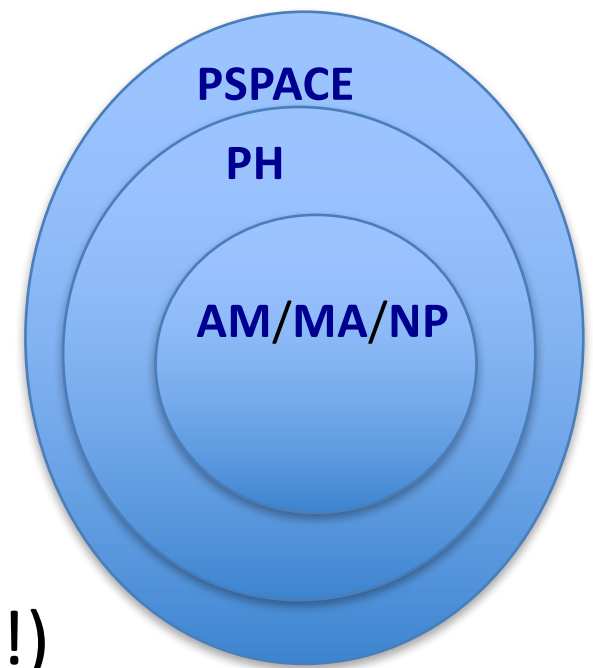
- Results in improved pseudorandom generators against classes related to **AC⁰**

How (classically) powerful are quantum computers?

- **BQP** – Class of languages that can be decided efficiently by a quantum computer
- Where is **BQP** relative to **NP**?
 - Is there a problem that can be solved with a quantum computer that can't be verified classically (**BQP** $\not\subseteq$ **NP**?)
 - Can we give evidence?
 - Oracle separations

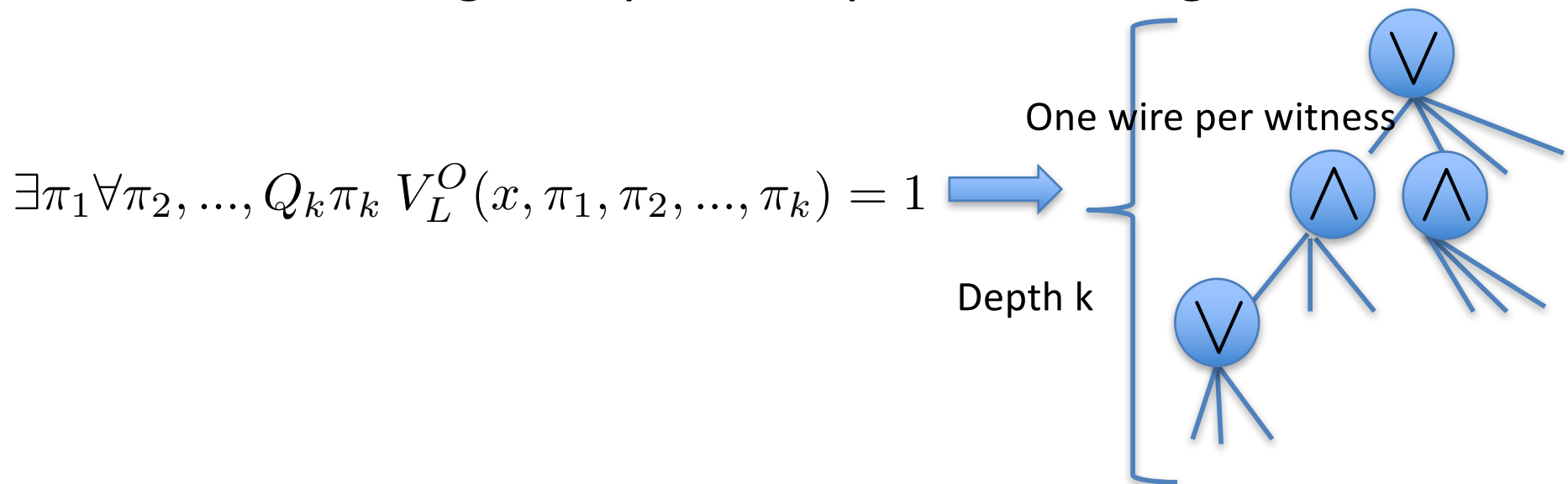
Is **BQP** $\not\subseteq$ **PH**?

- History: Towards stronger oracle separations
 - *[Bernstein & Vazirani '93]*
 - Recursive Fourier Sampling?
 - *[Aaronson '09]*
 - Conjecture: “Fourier Checking”
not in **PH**
 - Assuming GLN
 - *[Aaronson '10]* (counterexample!)
 - GLN false (depth 3)



What can't PH^0 do?

- Essentially equivalent to: what can't AC^0 do?
 - AC^0 is constant depth, AND-OR-NOT circuits of (polynomial size) and unbounded fanin
 - Idea: In circuit, \exists becomes OR, \forall becomes AND and oracle string an input of exponential length



Equivalent Setup

- Want a function $f:\{0,1\}^N \rightarrow \{0,1\}$
 - in **BQLOGTIME**
 - $O(\log N)$ quantum steps
 - random access to N -bit input: $|i\rangle \quad |z\rangle \rightarrow |i\rangle \quad |z \oplus f(i)\rangle$
 - accept with high probability iff $f(\text{input}) = 1$
 - but not in **AC⁰**

Equivalent Setup

- More general (and transformable to previous setting):
 - two distributions on N bit strings D_1, D_2
 - **BQLOGTIME** algorithm that distinguishes them
 - proof that **AC⁰** cannot distinguish them
 - we will always take D_2 to be uniform

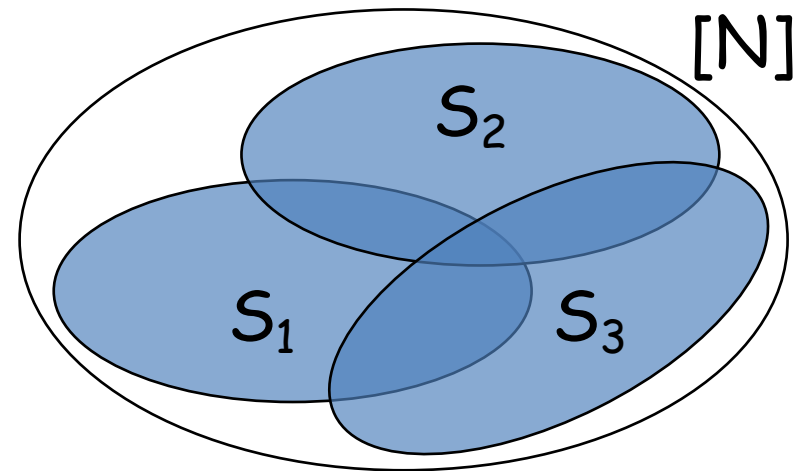
What can't AC^0 do?

- PARITY and MAJORITY not in AC^0 [FSS '84]
- AC^0 circuits can't *distinguish*:
 1. Bits distributed uniformly
 2. Bits drawn from “Nisan-Wigderson” distribution derived from:
 1. function hard (on average) for AC^0 to *compute*
 2. Nearly-disjoint “subset system”

Our work: There exists a specific choice of these subsets, for which the resulting distribution generated by the MAJORITY function can be distinguished (from uniform) quantumly!

Formal: Nisan-Wigderson PRG

- $S_1, S_2, \dots, S_M \subset [N]$ is an (N', p) -design if
 - for all i , $|S_i| = N'$
 - for all $i \neq j$, $|S_i \cap S_j| \leq p$



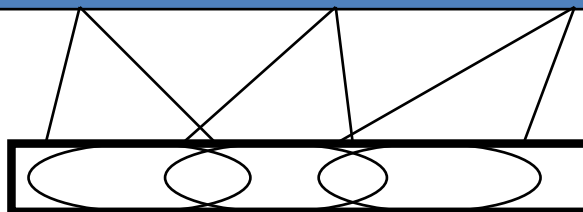
Nisan-Wigderson PRG

- $f:\{0,1\}^{N'} \rightarrow \{0,1\}$ is a hard function (e.g., MAJORITY)
- $S_1, \dots, S_M \subset [N]$ is an (N', p) -design

$$G(x) = f(x|_{S_1}) \circ f(x|_{S_2}) \circ \dots \circ f(x|_{S_M})$$

truth table of f :

01010010111101010111001010

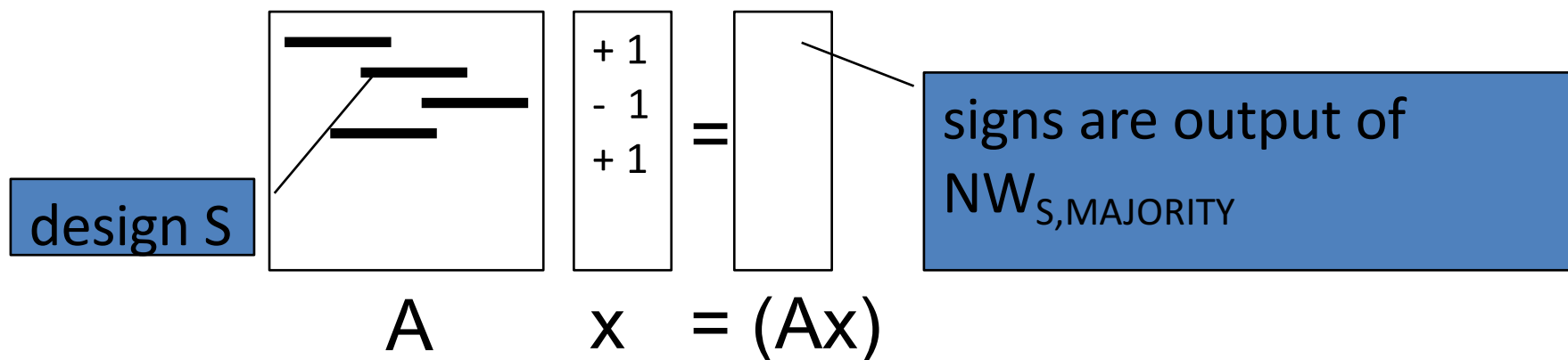


Seed $x \in \{0,1\}^N$

Distributions distinguishable from Uniform with a quantum computer

$D_A = (x, y)$: pick x uniformly from $\{1, -1\}^N$, set $y_i = \text{sgn}((Ax)_i)$

- Goal: Matrix A with rows that
 1. Have large support
 2. Have supports with small pairwise intersection (form some (N', p) -design)
 3. Are pairwise orthogonal
 4. Should be an efficient quantum circuit (product of $\text{polylog}(N)$ local unitaries)



Quantum Algorithm

$D_A = (x, y)$: pick x uniformly from $\{1, -1\}^N$, set $y_i = \text{sgn}((Ax)_i)$

- We claim there is a quantum algorithm to distinguish D_A from U_{2N}

- enter uniform superposition over $\log N$ qubits
- query x and multiply into phases: $\sum_i x_i |i\rangle$
- apply A : $\sum_i (Ax)_i |i\rangle$
- query y and multiply into phases: $\sum_i y_i (Ax)_i |i\rangle$
- measure in Hadamard basis, accept iff $(0,0,\dots,0)$

- Crucially, after step 4 we are back to all positive amplitudes in case oracle is D_A
- But in case oracle is U_{2N} with high prob. we have random mix of signs (low weight on $|0\dots 0\rangle$ after final Hadamard)

Constructing A using “Paired Lines”

- Goal: construct an $N \times N$ unitary matrix with supports of rows forming (N', p) -design
 - Identify with each row a pair of parallel “lines” in the affine plane $\mathbb{F}_{\sqrt{N}} \times \mathbb{F}_{\sqrt{N}}$
 - Identify points in the plane with columns
- For each row, as we go across columns:
 - +1 if point is on one of the lines
 - -1 if point is on other
 - 0 otherwise
- Use geometry of plane to argue orthogonality (and thus unitarity)

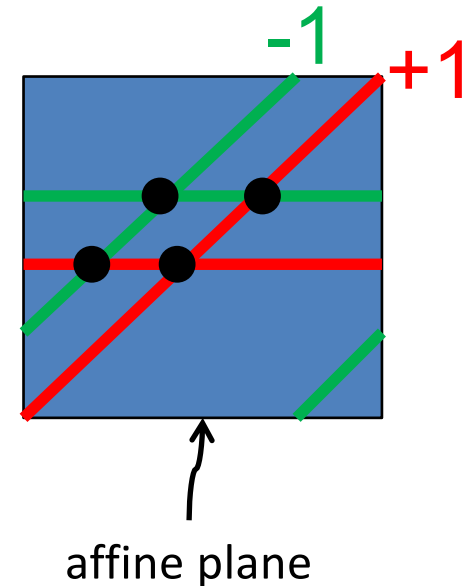
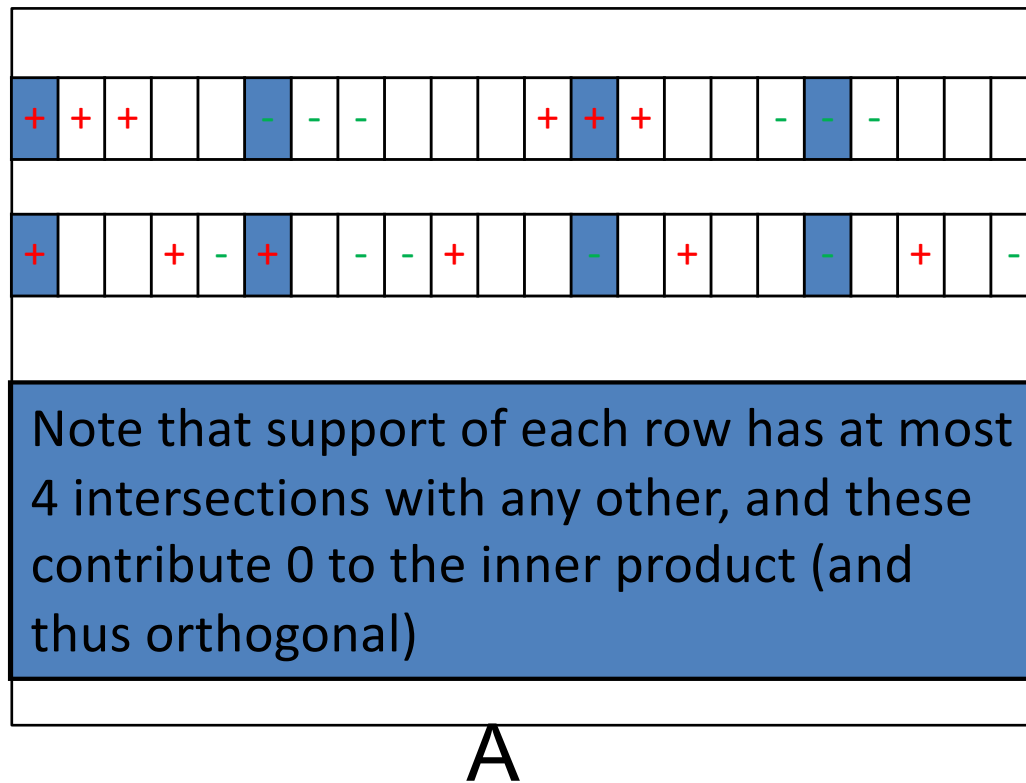
A

- \sqrt{N} parallel line classes
- \sqrt{N} lines in each class
- $N/2$ rows



Construction

- Each row will be supported on two parallel “paired-lines”
- Identify columns with affine plane $\mathbb{F}_{\sqrt{N}} \times \mathbb{F}_{\sqrt{N}}$



Putting it all together

- “Technical Core”: We construct an efficient quantum circuit realized by unitary whose (un-normalized) rows are vectors from a paired-lines construction
 - $N \times N$
 - Half of the rows will correspond to the paired-lines vectors
- Note that we have a quantum algorithm, as described before, that uses this unitary A to distinguish between D_A and U_{2N}
- But distinguishing should be hard for AC^0 since $(x, \text{sgn}(Ax))$ is instantiation of NW generator!

But why aren't we finished? (hybrid loss)

- Distribution on $(3/2)N$ bits that is the NW generator w.r.t. MAJORITY on $N^{1/2}$ bits, with output length $N/2$
 - Suppose AC^0 can distinguish from uniform with constant gap ϵ
 - proof: distinguisher to predictor, and then circuit for majority w/ success $\frac{1}{2} + \epsilon/(N/2)$
 - but already possible w/ success $\frac{1}{2} + \Omega(1/N^{1/4})$
- ... no contradiction

Nonetheless, we **conjecture** this distribution cannot be distinguished by AC^0 with constant gap ϵ

Beating the Hybrid Argument?

“Resampling lemma”

- (informal) S is a **resampler** for function $f(x)$ if
 $S(x)$ is uniform on $\{x' : f(x') = f(x)\}$

Lemma (informal): Suppose f has resampler, then distinguishing:
 M repetitions of $(U_n, f(U_n))$
from
uniform
is as hard as computing (on avg.) $f(x)$.

(Nontrivial for large M !)

recall: need $M < 1/\text{adv}(f)$ for hybrid argument

now: M can be as large as $\exp(n)$, for suitably hard functions f

Resampling lemma allows us to beat Hybrid Argument in restricted cases

- Proves the “disjoint case” of Conjecture:
 - Theorem: $M = \exp(n)$ copies of U_n , $\text{MAJ}(U_n)$ indistinguishable from uniform
 - Don't know of resampler for MAJORITY!
 - Do for **Hamming Weight** problem
 - YES: x has weight = $n/2 + t$
 - NO: x has weight = $n/2 - t$
- PRGs with improved stretch for
 - $\text{AC}^0[p]$ with prime $p > 2$ (via parity)
 - AC^0 with a not-too-large number of majority gates (via parity)
 - $\text{AC}^0[2]$ via the Connectivity Matrix Determinant problem [Ishai + Kushilevitz]

weighted
mixture



Resampler: randomly permute bits!

Conclusions

- Showed settings in which “beating the hybrid argument” proves new results in complexity
- Proved that in restricted cases, we can beat the hybrid argument
 - Enough to show improved PRGs against classes related to AC^0
 - Proves “disjoint case” of quantum conjecture!