Pseudorandom Generators and the BQP vs PH Problem

Bill Fefferman (IQI, Caltech)

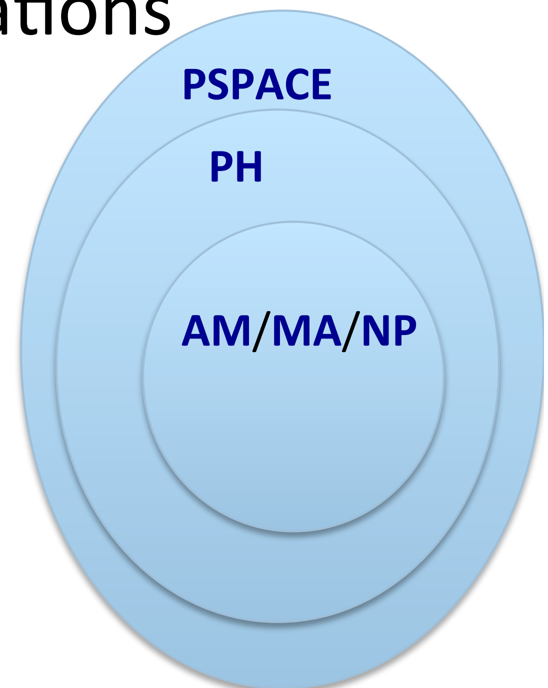
Joint with Chris Umans

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** $\not\subset$ **NP**?)
  – Can we give evidence?
    - Oracle separations

Is **BQP** $\not\subset$ **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)
- Why is it so hard?
  - Cannot rely on crude arguments about low degree approximating polynomials (both classes have such approximations… see [RS '87], [Beals et al '01])



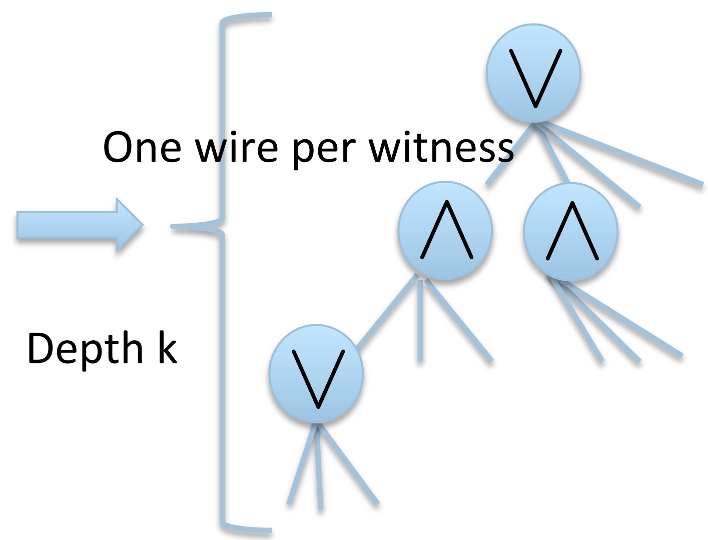
Today: A new approach

- Show oracle separation would follow from question studied in "pseudorandomness" literature [BSW '03]
- Under conjecture, quantum computers can break instantiation of the famous "Nisan-Wigderson" generator [NW '94]
- Unconditionally, gives another example of exponential quantum speedup over randomized classical computation

What can't $\mathbf{PH^O}$ do?

- Essentially equivalent to: what can't $\mathbf{AC_0}$ do?
  - $\mathbf{AC_0}$ is constant depth, AND-OR-NOT circuits of (polynomial size) and unbounded fanin
  - Idea: In circuit, ∃ becomes OR, ∀ becomes AND and oracle string an input of exponential length

$$\exists \pi_1 \forall \pi_2, ..., Q_k \pi_k \, V_L^O(x, \pi_1, \pi_2, ..., \pi_k) = 1$$



Equivalent Setup

- want a function $f:\{0,1\}^N \mapsto \{0,1\}$
  - in **BQLOGTIME**
    - O(log N) quantum steps
    - random access to N-bit input: $|i\rangle|z\rangle \mapsto |i\rangle|z \oplus f(i)\rangle$
    - accept with high probability iff f(input) = 1
  - but not in **AC_0**

Equivalent Setup

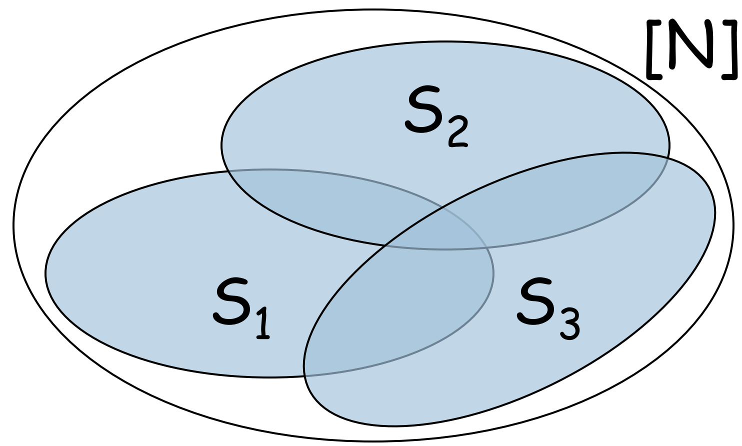
- More general (and transformable to previous setting):
  - two distributions on N bit strings D_1, D_2
  - **BQLOGTIME** algorithm that distinguishes them
  - proof that $\mathbf{AC_0}$ cannot distinguish them
  - we will always take D_2 to be uniform

What can't $\mathbf{AC_0}$ do?

- PARITY and MAJORITY not in $\mathbf{AC_0}$ [FSS '84]
- $\mathbf{AC_0}$ circuits can't *distinguish*:
  1. Bits distributed uniformly
  2. Bits drawn from "Nisan-Wigderson" distribution derived from:
     1. function hard (on average) for $\mathbf{AC_0}$ to *compute*
     2. Nearly-disjoint "subset system"
  – Our result: 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

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

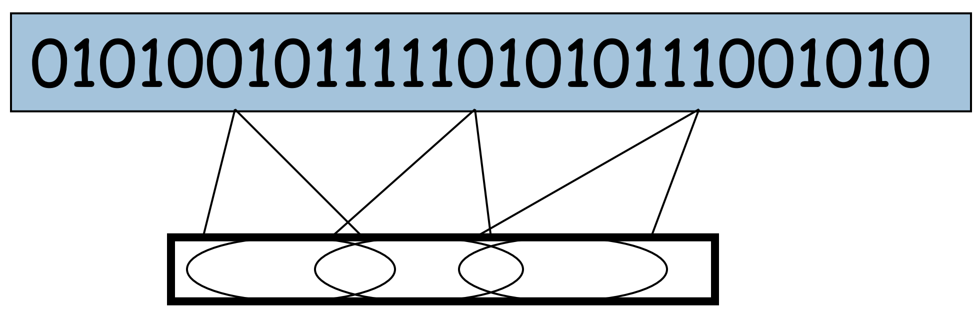


Nisan-Wigderson PRG

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

$$G(x)=x\circ f(x_{|S_1})\circ f(x_{|S_2})\circ\ldots\circ f(x_{|S_M})$$

truth table of f:



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

Proof of Classical Hardness: *Indistinguishability*

- Proof by contradiction:
  - assume circuit C *distinguishes* from uniform:

    $$|\Pr[C(U_{N+M}) = 1] - \Pr[C(G(U_N)) = 1]| > \varepsilon$$

    loss from hybrid argument!

  - transform C into a *predictor* circuit P

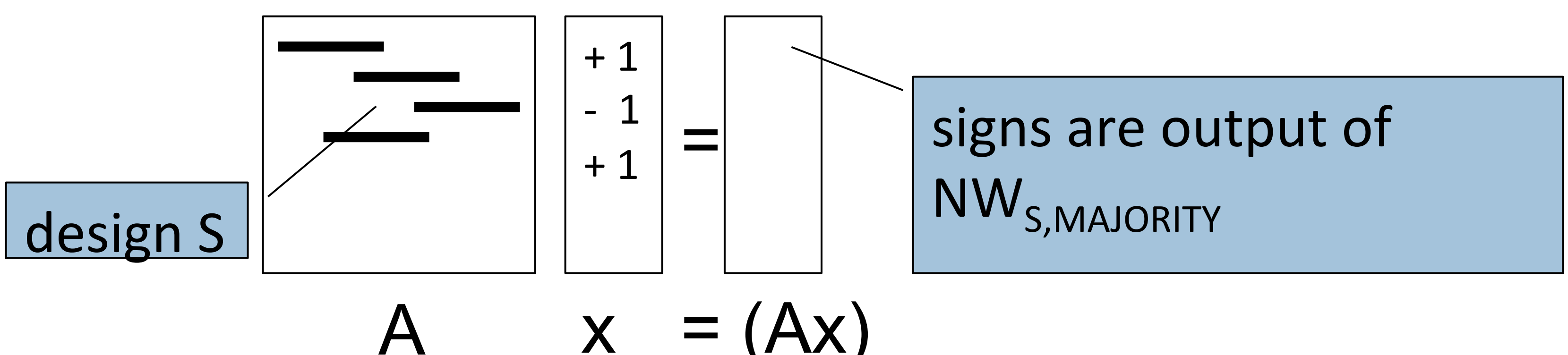
    $$\Pr_{x \sim U}[P(G(x)_{1 \ldots i-1}) = G(x)_i] > ½ + \varepsilon/\mathbf{M}$$

  - derive similar sized circuit approximating hard function (using properties of subset system)
  - Contradiction (assuming hard function cannot be approximated this well)

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 polylog(N) local unitaries)



Quantum Algorithm

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

1. enter uniform superposition over log N qubits
2. query x and multiply into phases: $\sum_i x_i \, |i\rangle$
3. apply A: $\sum_i (Ax)_i \, |i\rangle$
4. query y and multiply into phases: $\sum_i y_i (Ax)_i \, |i\rangle$
5. measure in Hadamard basis, accept iff (0,0,…,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….0> after final Hadamard)

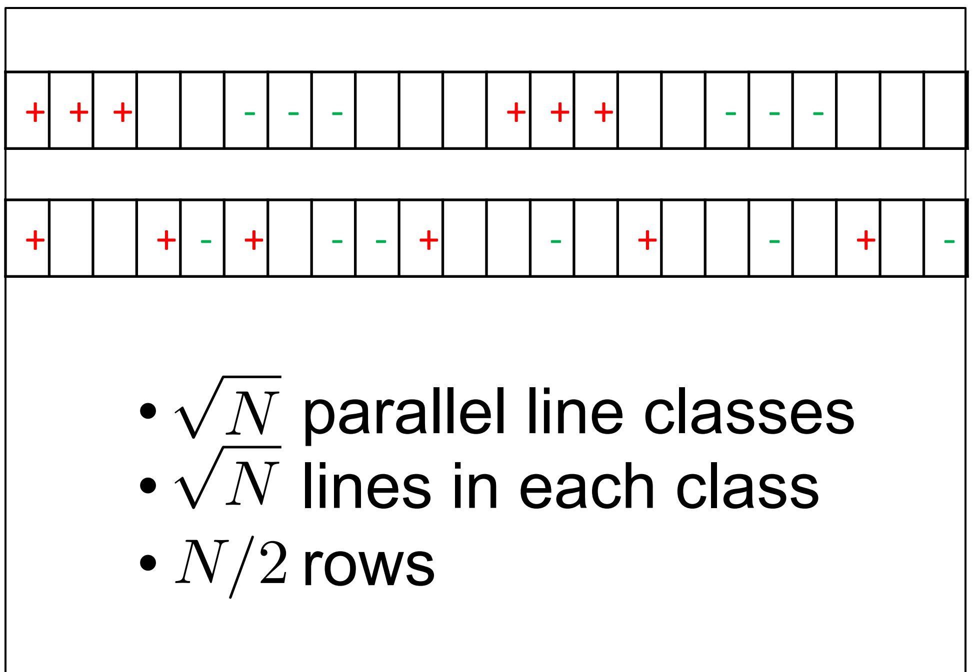
Constructing A using "Paired-Lines"

- Will describe $N/2$ pairwise-orthogonal vectors in $\{0, \pm 1\}^N$
- Identify N with the affine plane $\mathbb{F}_{\sqrt{N}} \times \mathbb{F}_{\sqrt{N}}$
- Let B_1, B_2 be an equipartition of $\mathbb{F}_{\sqrt{N}}$
- Take some $\phi : B_1 \to B_2$ (an arbitrary bijection). Then the vectors are:

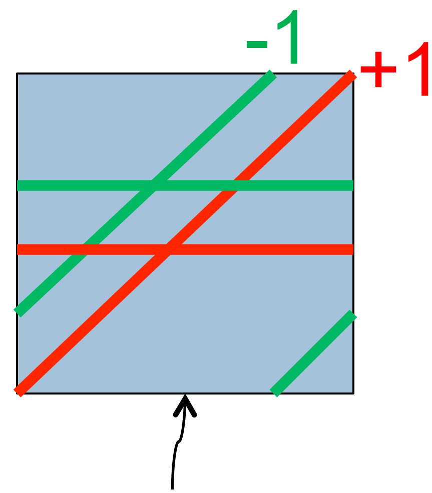
$$v_{a,b}[x,y] = \begin{cases} -1 & y = ax + b \\ +1 & y = ax + \phi(b) \\ 0 & otherwise \end{cases}$$

Construction

- Each row will be $v_{a,b}$ (supported on two parallel, "paired-lines" with slope a)
- Identify columns with affine plane $\mathbb{F}_{\sqrt{N}} \times \mathbb{F}_{\sqrt{N}}$



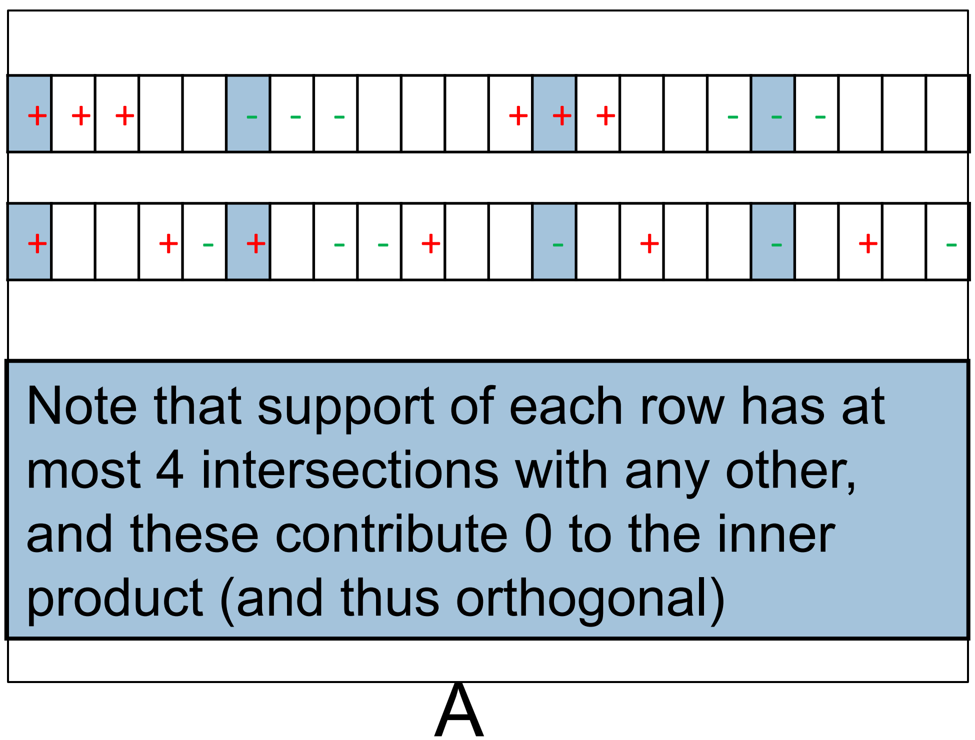
A



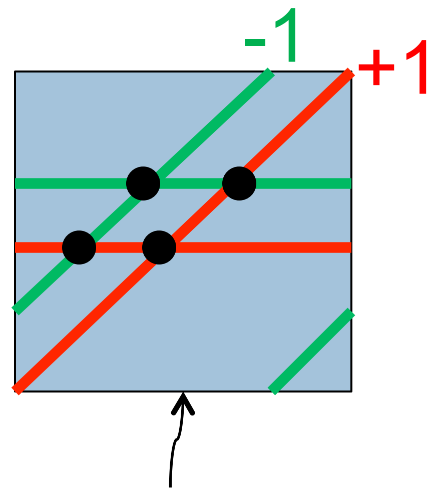
affine plane

Construction

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



Note that support of each row has at most 4 intersections with any other, and these contribute 0 to the inner product (and thus orthogonal)



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 wrt a specific bijection
  - N x 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 $\mathbf{AC_0}$ since Ax is instantiation of NW generator!

But why aren't we finished?

- 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 ½ + ε/(N/2)
  - but already possible w/ success ½ + $\Omega(1/N^{1/4})$

    … no contradiction

Our Conjecture

- 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
- Can **AC_0** can distinguish from uniform with constant gap ε?

Conjecture: No.

Recent new work [with Shaltiel, Umans & Viola]

- (Non-trivial) simplification of conjecture:
  - Take M *completely* disjoint subsets
  - Distinguish:
    1. All bits distributed uniformly
    2. First half bits are uniform, second are majorities over disjoint subsets of first half
  - This is indeed hard for **AC_0**!

Conclusions

- Assuming conjecture, gives a quantum algorithm that can “break” a PRG
- Unitaries used are novel and don’t seem to resemble those used in other quantum algorithms
- Conjecture implies oracle relative to which **BQP** is not in **PH**