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
• \( G : \{0,1\}^N \to \{0,1\}^M \)
• \([Yao \ '82]\) Suppose we have a circuit \( C \) that \( \epsilon \)-distinguishes \( U^M \) from \( G(U^N) \), then there is a similar size “predictor circuit” \( P \)

\[
| \Pr[C(U^M) = 1] - \Pr[C(G(U^N)) = 1] | > \epsilon \\
\implies \Pr_{x \sim U}[P(G(x)_{1 \ldots i-1}) = G(x)_i] > \frac{1}{2} + \frac{\epsilon}{M}
\]

• Contrapositive: Unpredictability \( \implies \) Indistinguishability
  • Hybrid loss becomes hurdle when \( M >> 1/\epsilon \)
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 $\text{BQP} \not\subset \text{PH}$
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 $\text{AC}^0$
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 $\text{BQP} \not\subseteq \text{PH}$?

- History: Towards stronger oracle separations
  - [Bernstein & Vazirani ‘93]
    - Recursive Fourier Sampling?
  - [Aaronson ‘09]
    - Conjecture: “Fourier Checking”
      - not in $\text{PH}$
        - Assuming GLN
  - [Aaronson ‘10] (counterexample!)
    - GLN false (depth 3)
What can’t $\text{PH}^0$ do?

- Essentially equivalent to: what can’t $\text{AC}^0$ do?
  - $\text{AC}^0$ 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

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

• Want a function $f: \{0,1\}^N \rightarrow \{0,1\}$
  – in $\text{BQLOGTIME}$
    • $O(\log N)$ quantum steps
    • random access to $N$-bit input: $|i\rangle|z\rangle \rightarrow |i\rangle|z \oplus f(i)\rangle$
    • accept with high probability iff $f(\text{input}) = 1$

– but not in $\text{AC}^0$
Equivalent Setup

• More general (and transformable to previous setting):
  – two distributions on N bit strings $D_1, D_2$
  – $\text{BQLOGTIME}$ algorithm that distinguishes them
  – proof that $\text{AC}^0$ cannot distinguish them
  – we will always take $D_2$ to be uniform
What can’t $\text{AC}^0$ do?

- PARITY and MAJORITY not in $\text{AC}^0$ [FSS ’84]
- $\text{AC}^0$ circuits can’t distinguish:
  1. Bits distributed uniformly
  2. Bits drawn from “Nisan-Wigderson” distribution derived from:
     1. function hard (on average) for $\text{AC}^0$ 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

• \( S_1, S_2, \ldots, S_M \subseteq [N] \) 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., \textsc{majority})
- \( S_1, \ldots, S_M \subset [N] \) is an \((N', p)\)-design

\[
G(x) = f(x|_{S_1}) \circ f(x|_{S_2}) \circ \ldots \circ f(x|_{S_M})
\]

truth table of \( f \):

```
010100101111101011001010
```

Seed \( x \in \{0,1\}^N \)
Distributions distinguishable from Uniform with a quantum computer

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

- 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)

\[
\begin{bmatrix}
  +1 \\
  -1 \\
  +1
\end{bmatrix}
= \text{design } S
\]

\[
\begin{bmatrix}
  A \\
  x
\end{bmatrix}
= (Ax)
\]

signs are output of \(NW_{S, \text{MAJORITY}}\)

---

January 2012

ITCS 2012
Quantum Algorithm

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

- We claim there is a quantum algorithm to distinguish \( D_A \) from \( U_{2N} \)
  1. enter uniform superposition over \( \log N \) qubits
  2. query \( x \) and multiply into phases: \( \sum_i x_i |i> \)
  3. apply \( A \): \( \sum_i (Ax)_i |i> \)
  4. query \( y \) and multiply into phases: \( \sum_i y_i(Ax)_i |i> \)
  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”

- 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)
Construction

• Each row will be supported on two parallel “paired-lines”

• Identify columns with affine plane

\[
\mathbb{F}_{\sqrt{N}} \times \mathbb{F}_{\sqrt{N}}
\]

| + + + | - - - | + + + | - - - |
| + | + - + | - - + | - + - |
| + | + - + | - - + | - + - |

• \( \sqrt{N} \) 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 $\mathbb{F}_{\sqrt{N}} \times \mathbb{F}_{\sqrt{N}}$

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
  – 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 $\text{AC}^0$ 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 $\mathsf{AC}^0$ can distinguish from uniform with constant gap $\varepsilon$
  
  – proof: distinguisher to predictor, and then circuit for majority w/ success $\frac{1}{2} + \varepsilon/(N/2)$
  
  – but already possible w/ success $\frac{1}{2} + \Omega(1/N^{1/4})$
  
  ... no contradiction

Nonetheless, we conjecture this distribution cannot be distinguished by $\mathsf{AC}^0$ with constant gap $\varepsilon$
Beating the Hybrid Argument?
“Resampling lemma”

• \( S \) is a **resampler** for function \( f(x) \) if
  \[
  S(x) \text{ is uniform on } \{x' : f(x') = f(x)\}
  \]

**Lemma (informal):** Suppose \( f \) has resampler, then distinguishing:
  \[
  M \text{ repetitions of } (U_n, f(U_n))
  \]
  from
  \[
  \text{uniform}
  \]
  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 $= n/2 - t$
  - Resampler: randomly permute bits!
- PRGs with improved stretch for
  - $\text{AC}^0[p]$ with prime $p > 2$ (via parity)
  - $\text{AC}^0$ with a not-too-large number of majority gates (via parity)
  - $\text{AC}^0[2]$ via the Connectivity Matrix Determinant problem [Ishai + Kushilevitz]
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 $\mathsf{AC}^0$
  – Proves “disjoint case” of quantum conjecture!

January 2012

ITCS 2012