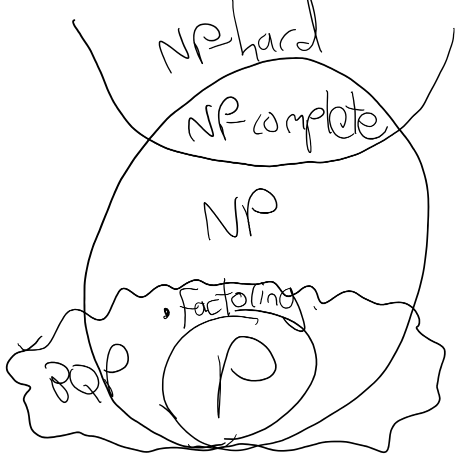
BQP After 28 Years

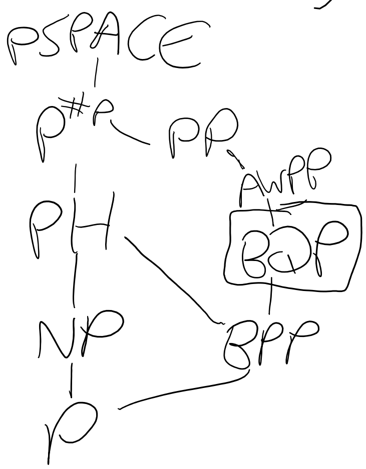
An unapologetically retro topic!

Scott Aaronson (UT Austin)

FSTTCS, December 16, 2021

BQP: Bounded-Error Quantum Polynomial-Time (Bernstein & Vazirani, 1993)





BBBV'94: $BQP^{BQP} = BQP$

Fortnow-Rogers '98: $PP^{BQP} = PP$

Profound Questions That Have Remained Open:

(1) $BPP = BQP$?

(2) $NP \subseteq BQP$?

(3) $BQP \subseteq NP$? AM? PH?

And many more arcane ones, e.g.

$$NP^{BQP} \subseteq BQP^{NP} ?$$

(Fortnow 2005)

Formally, we can do little better than point out some "obvious" relationships among these questions.

E.g., $NP \subseteq BQP$ AND $BQP \subseteq AM$

$\Longrightarrow$ PH collapses

(since then $coNP \subseteq AM$)

For BPP, we can say much more than for BQP. E.g.,

- $BPP \subseteq PH$ (Sipser-Gács-Lautemann)

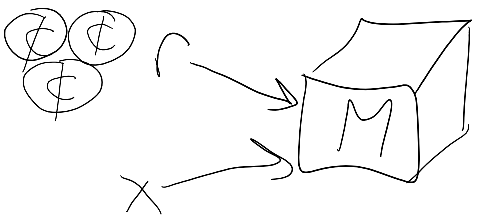
  So, $P = NP \Longrightarrow P = BPP$

- $BPP \subset P/poly$ (Adleman)

- $NP \subseteq BPP \Rightarrow PH \subseteq BPP$ & PH collapses

All these results depend on "pulling out the randomness" of a classical randomized algorithm

$p = |\alpha|^2$



$\Pr_r[M(x,r) \text{ accepts}]$

Nothing analogous seems to be possible for quantum algorithms!

This difference is crucial in, e.g., the analysis of sampling-based quantum supremacy experiments (A.-Arkhipov, Bremner-Jozsa-Shepherd...)

~

$P^{\#P} = BPP^{NP}$
$\Rightarrow PH$ collapse

But how could we ever prove these differences between BPP and BQP?

Like perturbation theory for physicists, relativization is complexity theorists' way to prove things even when it's too hard to prove things.

---

it's too hard to prove things.

Bernstein-Vazirani '93, Simon '94, Shor '94:
There exists an oracle A relative to which $BPP^A \neq BQP^A$.

BBBV '94: There's an oracle A such that $NP^A \not\subset BQP^A$
(I.e., Grover is optimal; any poly-time quantum algorithm for NP-complete problems must be non-black-box)

Fortnow-Rogers '98: There's an oracle relative to which $P = BQP$ yet PH is infinite
(A.-Chen 2017: Even relative to which quantum and classical polytime approximate sampling coincide, yet PH is infinite)

Bernstein-Vazirani '93, Watrous 2000:
There are oracles relative to which $BQP \not\subset NP$ and even $BQP \not\subset MA$

But what about $BQP \not\subset AM$?

$BQP \not\subset PH$?

These oracle separations were huge open problems for 25 years!

A. 2009: FORRELATION, a candidate problem for these separations.

Given black-box functions

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

Promised that either

(i) They're uniformly random & independent, or

(ii) They're uniformly random individually, but g is correlated with $\hat{f}$ (f's Boolean Fourier transform).

Decide which. "forrelated"

I showed how to solve FORRELATION with only 1 (!) quantum query to f, g.

I conjectured it was not in $PH^{f,g}$.

Raz-Tal 2018 finally proved my

Raz-Tal 2018 finally proved my conjecture, with a breakthrough analysis of the Fourier spectra of AC^0 circuits.

$\Rightarrow$ $\boxed{\exists \text{ oracle relative to which } BQP \not\subset PH}$

Indeed, they proved something stronger: a PH machine can guess whether f, g are uniform or forrelated with bias at most $\frac{1}{\exp(n)}$.

Now I'd like to share some recent work with William Kretschmer & DeVon Ingram

"The Acrobatics of BQP"
arXiv: 2111.10409

Our first question was which <u>other</u> longstanding open problems about

BQP relative to oracles could be knocked off using Raz & Tal's breakthrough

Easy: There exist oracles relative to which

- $BQP \not\subset NP/poly$
- $P = NP \neq BQP$

Idea: First use FORRELATION to make $P \neq BQP$. Then, $\forall k \geq 1$, recursively encode into the oracle A the answers to all possible NP^A queries, using strings of length $\sim n^k$. This makes $P^A = NP^A = PH^A$, without re-collapsing P and BQP (by Raz-Tal).

More interesting:

There exists an oracle relative to which

$$P = NP \neq BQP = P^{\#P}.$$

(BQP: "I will not let my aspirations be constrained by NP's, unlike my weaker cousin BPP!")

Idea: First use, e.g., exp(n)-sized

MAJORITY instances to make $PH \neq P^{\#P}$. Then, $\forall k \geq 1$, and using strings of size $\sim n^k$, recursively:

- Encode into the oracle A the answers to all possible NP^A queries
- Encode into A the answers to all possible $\#P^A$ queries, <u>but</u> hide them in FORRELATION instances.

This way, we make $P^A = NP^A$ and $BQP^A = P^{\#P^A}$ but by Raz-Tal + a hybrid argument, we don't recollapse PH^A & $P^{\#P^A}$.

<u>Another new result:</u>
There exists an oracle relative to which $NP \subseteq BQP$ but PH is infinite.
(& even $BQP = P^{\#P}$)

("If a fast quantum algorithm for NP-complete problems collapses PH, it can only be for a non-relativizing reason.")

<u>Idea:</u> First, use a random oracle — this makes PH infinite with probability 1, by

Håstad Rossman-Servedio-Tan 2015:

Then, encode into the oracle A the answers to all possible NP^A queries, but hidden in FORRELATION instances. This makes $NP^A \subseteq BQP^A$. But by Raz-Tal + hybrid argument, it still looks uniformly random to PH^A, so by Rossman-Servedio-Tan it doesn't recollapse PH.

To go further, we needed more than Raz-Tal. Since the 80s, a central tool for oracle separations (e.g. $PH \neq PSPACE$) has been random restrictions.

Our Random Restriction Lemma for BQP

Suppose quantum alg. Q makes T queries to $X \in \{0,1\}^N$. Let $0 \le k \le 2pN$. If we sample $S \subseteq [N]$ s.t. each $i \in [N]$ is in S w.p. p, then w.p. $\geq 1 - e^{-k/6}$ over S, $\exists L \subseteq S$ with $|L| \le k$ s.t. for every $y \in \{0,1\}^N$ that differs from x only on $S \setminus L$,

$$|\Pr[Q(x) \text{ accepts}] - \Pr[Q(y) \text{ accepts}]| \leq 16Tp\sqrt{\frac{N}{k}}.$$

Proof Idea: Just careful BBBV!

Example Application: (though not yet using its full power)

$\forall k$, there's an oracle relative to which

$$\Sigma_{k+1}^{P} \not\subset BQP^{\Sigma_k^{P}}$$

(Indeed a random oracle!)

Proof Idea: Just plug our random restriction lemma into Rossman-Servedio-Tan's proof that PH is infinite relative to a random oracle.

Our Most Interesting (?) Result:

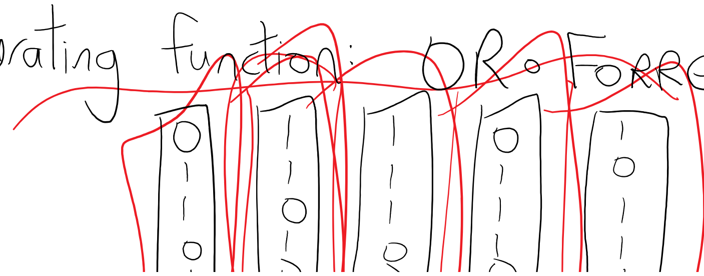
There exists an oracle relative to which

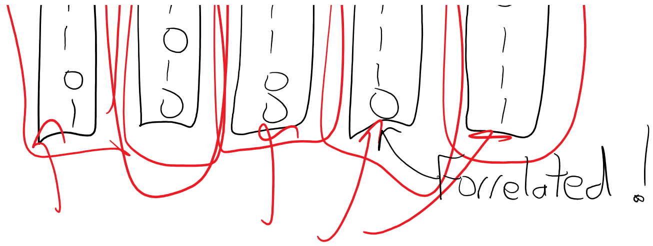
$$NP^{BQP} \not\subset BQP^{NP}$$

(& even $NP^{BQP} \not\subset BQP^{PH}$)

Solves Fortnow's problem from 2005!

Separating function: OR ∘ FORRELATION





BQP^{PH} has the "composition in the wrong order" to solve this—but how to formalize?

Need to rule out that AC^0 can "compute OR in homomorphically encrypted fashion," with FORRELATION as the encryption!

To do so, we use a concentration theorem for the block sensitivity of AC^0 functions, building on Gopalan-Servedio-Tal-Wigderson 2016 + the fact that FORRELATION is about distinguishing from the uniform distribution.

NOTE: All these oracle results are only possible in a post-Raz-Tal world—for if $BQP \subseteq AM$, then the statements would all be false, via relativizing proofs!

We also did the converse direction!

Theorem: There exists an oracle relative to which

Theorem: There exists an oracle relative to which

$$BQP^{NP} \not\subset PH^{BQP}$$

Separating example is now FORRELATION ∘ OR.

$$\left.\begin{array}{ccccc} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right\} N \quad \begin{array}{c} \to 1 \\ \to 1 \\ \to 0 \\ \to 1 \end{array} \quad \text{FORRELATION instance}$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{N}$$

Lemma: Any quantum algorithm that makes T queries to such an oracle & accepts or rejects can be simulated, on a $\geq 1-\delta$ fraction of oracles, by an $O(T^5 \log \frac{T}{\delta})$-query classical algorithm

"Aaronson-Ambainis Conjecture for sparse oracles"

Means that PH^{BQP} is no more powerful than PH for FORRELATION ∘ OR!

Result now follows by combining with Raz-Tal.

Another application of our random restriction lemma

There's an oracle relative to which

$PP \not\subset BQP^{NP}$

.... & even $BQP^{NP^{BQP^{NP^{\cdots}}}}$

.... & even $QMA^{QMA^{QMA^{\cdots}}}$

.... & even $(MIP^*)^{(MIP^*)^{(MIP^*)^{\cdots}}}$

(yes, even though in the "real world," $MIP^* = RE$!!

shows just how radically nonrelativizing $MIP^* = RE$ is)

Contrast $PostBQP = PP$ with $PostBPP$, which *is* relativizingly in BPP^{NP}!

Summary: Relative to suitable oracles, we can almost completely "unshackle" BQP from the complexity classes around it, by exploiting QCs' ability to solve FORRELATION combined with their inability to beat Grover. Even while BPP remains shackled!

Some Problems We Didn't Solve

- Oracle where $P = NP$, but $BQP = EXP = NEXP$?

- Oracle where $NP \subseteq BQP$ but $PH \not\subset BQP$?

Our personal favorite—we made a lot of progress but didn't resolve!

- Oracle where $P = QMA \neq PP$?
- Oracle where $QMA \not\subset BQP^{NP}$?
- Sharper random restriction lemma for BQP & QMA?

OK, but what about the unrelativized world???

My bets/speculations:

- $P = BPP \neq BQP$
- $NP \not\subset BQP$
- $BQP \subseteq NP$?? ← No idea on this one!
    - Under derandomization, $BQP \subseteq AM$ would suffice.
    - Is there an explicit instantiation of FORRELATION?
    - Is there a decision version of BOSONSAMPLING?

$M(x, r)$

$G(S)$

Thanks for listening!

Thanks for listening!

$$P \subseteq \boxed{EQP_G} \subset BQP$$

$$\exists A \quad P^A \neq EQP^A$$

$EQP \not\subset BPP$, $\not\subset NP$, $\not\subset MA$.

$RFS \notin PH$

$$\exists A \quad EQP^A \not\subset PH^A \; ?$$