Can Universal Quantum Computing Scale Up?

(And glimpses into my other work)

Kenneth W. Regan[1]
University at Buffalo (SUNY)

CSE501, 3 Sept., 2024

[1]With grateful acknowledgment to co-authors—including Tamal Biswas now of RKMVERI—and UB's Center for Computational Research (CCR)

Computational Complexity

- The study of the time *needed* to solve computational problems, and how much memory and other resources computers require.
- Largely independent of the computer model, beyond a fundamental divide into **serial**, **parallel**, and **quantum**.
- Main technical achievement: the relation of computational problems by **reducibility**.
- Main scientific surprise:

> The **many thousands** of computational problems that have been studied in many disciplines, some for centuries, cluster into **barely over a dozen** equivalence classes under reducibility.

- The biggest cluster is the class of **NP-complete** problems.

P=?NP and Worse

- **P**: problems with algorithms that **solve** them in **polynomial time**:

  As the size of the data doubles, the time needed goes up by at most a **linear** factor: $t(n) = n^k \implies t(2n) \leq Kt(n)$, $K = 2^k$.

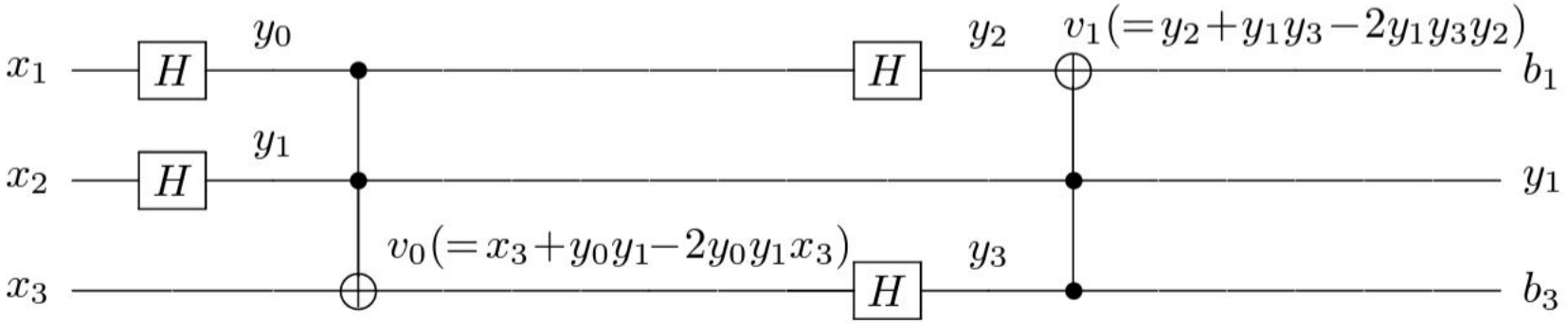
- **NP**: "Nondeterministic" Polynomial Time: If you know a secret fact or guess a good answer, you can verify and **teach** it to someone in polynomial time.
- Example: Given a Boolean formula f like

$$f = (x_1 \vee (\neg x_2)) \wedge ((\neg x_1) \vee x_2 \vee x_3) \wedge ((\neg x_2) \vee (\neg x_3)),$$

  is there a way to make f true?
- Called *Satisfiability* (SAT).
- Equivalent to $\neg f$ *not* being a **tautology**.
- Is NP-complete, so NP = P $\iff$ SAT belongs to P.
- We don't even know whether SAT can be solved in **linear** time!

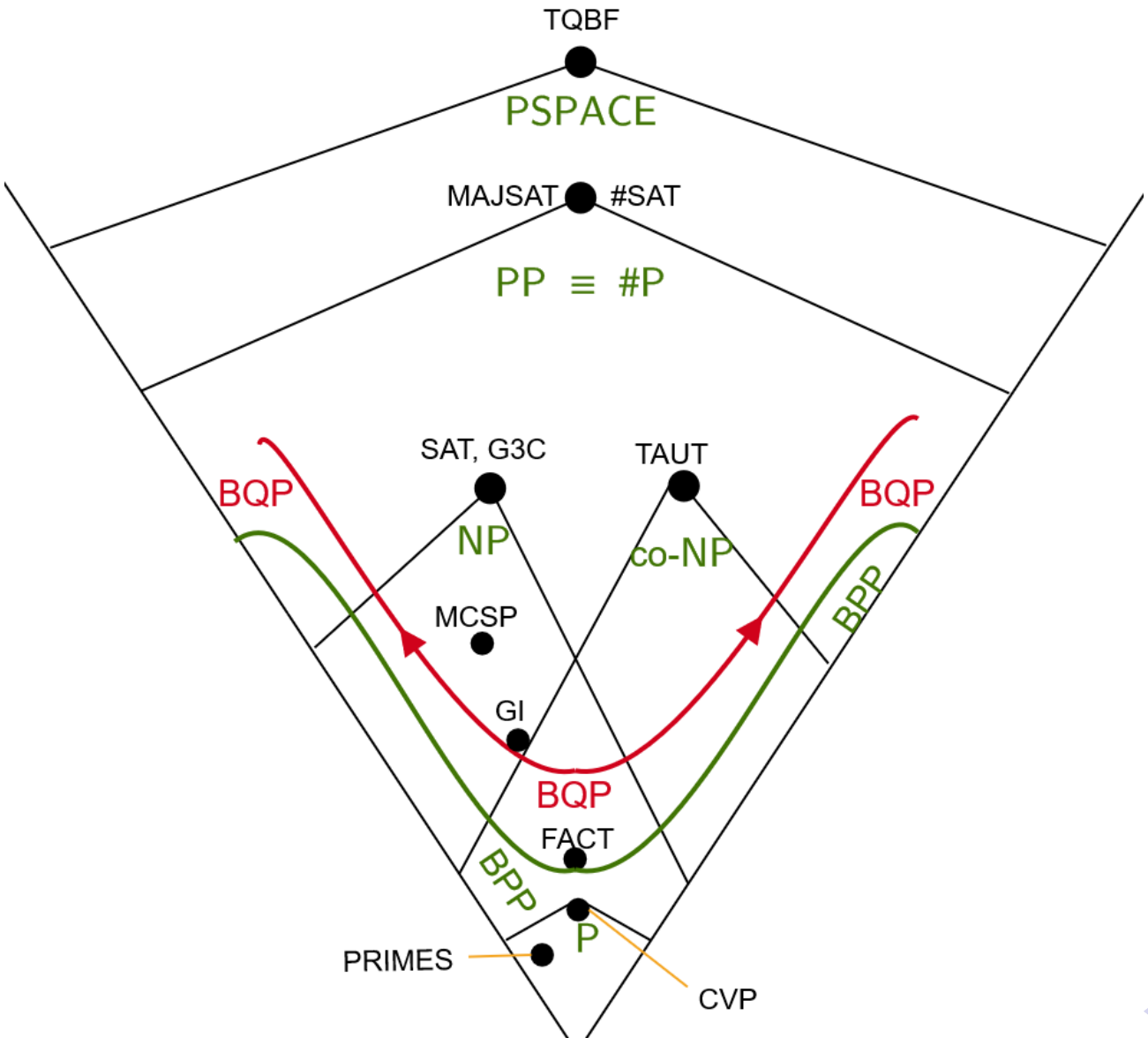
Application to Quantum Computing

- **Factoring** is among a handful of problems in NP not known to be complete or in P.
- RSA security depends on it, so many want it to be *hard*.
- But solvable in polynomial time by a **quantum computer**.
- Textbook on quantum algorithms; blog series: Can QCs be Built?
- Research on simulating **quantum circuits** by logic and algebra:




```
p1 = p0 XOR (y0 & x1)   p2 = p1 XOR (y1 & x2)   v0 = x3 XOR (y0 & y1)
p3 = p2 XOR (y2 & y0)   p4 = p3 XOR (y3 & v0)   v1 = y2 XOR (y3 & y1)
```

The Complexity Class Neighborhood...



...Might Not Have Room For BQP

Dichotomy = The phenomenon of *natural* computational problems and mathematical entities clumping into an "easy" level A and a "hard" level B with little or nothing *salient* in between.

1. "Almost all" problems in NP are either in P or NP-complete.
2. For "most" problems not known to be in P, the best known running time is strictly exponential.
3. Note: If $\mathsf{NP} \neq \mathsf{P}$ then there are languages in $\mathsf{NP} \setminus (\mathsf{NPC} \cup \mathsf{P})$. But they are expressly diagonal and thus "artificial."
4. Work by Jin-Yi Cai (begun in Buffalo) argues the squeeze between **#P** and **P** for natural **counting problems** is even tighter. And he now disbelieves Shor's Algorithm.

Other Universal QC Skepticism

- **Gil Kalai**: 2018 article in Quanta Magazine. His Blog
- IEEE Spectrum, Dec. 2023.
- Forbes, May 2022.
- Forum Roundup.
- In 2012, I moderated a debate on the *Gödel's Lost Letter* blog between Kalai and Aram Harrow.
- Harrow is the first 'H' in the famous HHL algorithm, which is propounded for *quantum machine learning*, but...
- Main engineering side is extreme difficulty maintaining **coherence** in systems of > 10 qubits.
- My Q: Is there an *intrinsic* reason for this difficulty?

A Whiff of Nonlinearity?

- Show article, "Grilling Quantum Circuits."
- Past and Ongoing Research with recent PhD graduate Chaowen Guan.
- The algebraic-geometric tools are being applied a different way with my current PhD student Chen Xu.
- Nothing major has been found (yet?).
- Regardless, quantum computing is a beautiful area.
- Currently teaching CSE439/501: Quantum Computing Via Linear Algebra from my joint textbook of that name.