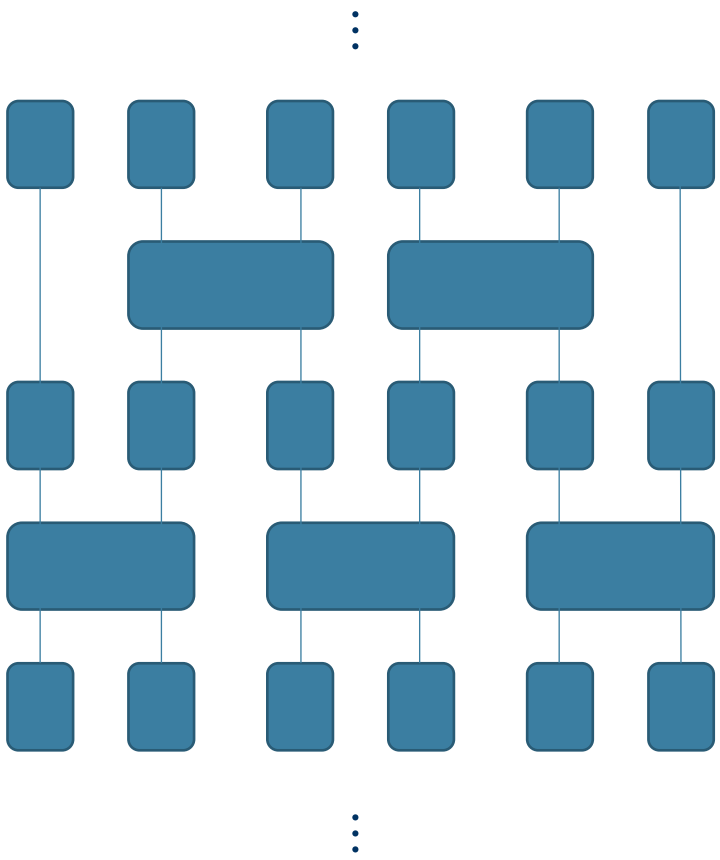
The parametrized complexity of quantum verification

Srinivasan Arunachalam (IBM)
Sergey Bravyi (IBM)
Chinmay Nirkhe (UC Berkeley → IBM)
Bryan O'Gorman (IBM)

The toggle between P and BQP



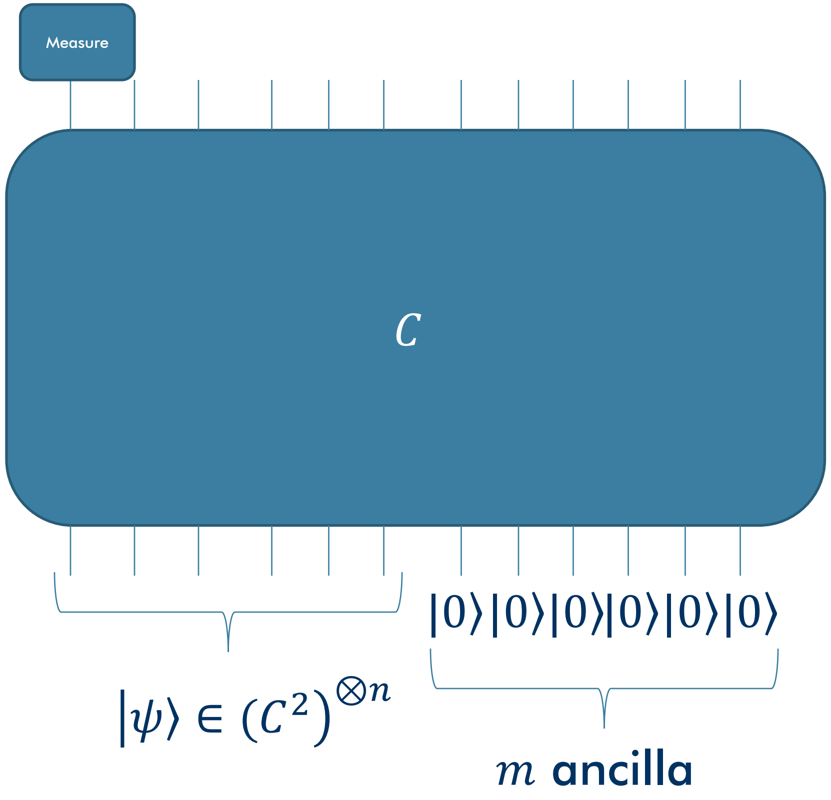
Counting the number of non-Clifford gates in a circuit is a measure of how "non-classical" a given circuit is

Gottesman & Knill showed that there is a P algorithm for deciding a quantum circuit decision problem if the circuit only has Clifford gates

A series of works has extended this famous theorem to Clifford gates of low non-Clifford gate count (most often counting the number of T gates) in both the decision and sampling regime

This gives parametrized (in # of T gates = t) algorithms for quantum circuit problems.

Is there a toggle between P and QMA?

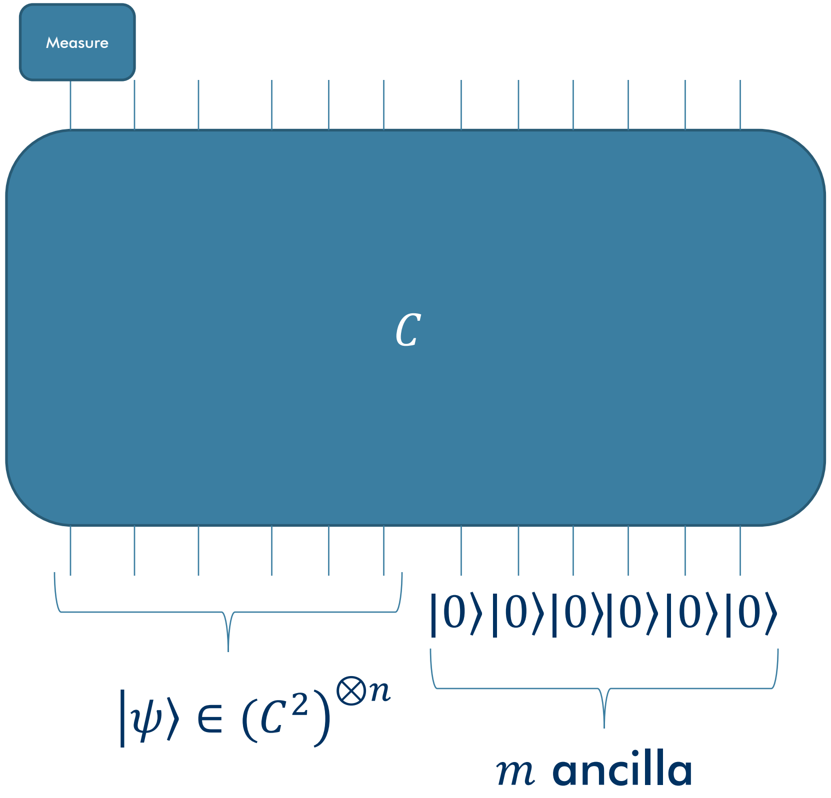


Canonical QMA: Does there exist a $|\psi\rangle$ such that the circuit accepts with probability $> 2/3$ or for all $|\psi\rangle$, is the acceptance probability bounded by $< 1/3$?

What is the complexity of the parametrized quantum circuit satisfiability problem when the circuit on

- n qubits,
- m ancilla,
- s gates,
- t non-Clifford gates (T gates)?

Is there a toggle between P and QMA?



Co ... ci ... the ac ...

What is the complexity of the parametrized quantum circuit satisfiability problem when the circuit on

- n qubits,
- m ancilla,
- s gates,
- t non-Clifford gates (T gates)?

Theorem: There exists a reduction to an equivalent QCSAT problem on

- $t$qubits,
- $m + n - t$ ancilla,
- $s + O((n+m)^2/\log(n+m))$ gates,
- t non-Clifford gates (T gates).

Non-determinism and quantum don't clash

- Yoganathan, Jozsa, and Strelchuk 2019 construct a reduction that reduces the computation (after classical processing) to a new t T-gate computation on n qubits witness but with no ancilla.
- In our result we maintain the ancilla but drastically reduces the witness to t size.
- Furthermore, we give an $2^{\max(2+\alpha),\omega)\cdot t} \cdot \mathrm{poly}(s) \approx 5.3^t$ runtime algorithm for solving parametrized QCSAT
  - α is stabilizer rank of magic states
  - ω is matrix multiplication constant

The Clifford perspective

- Clifford group = $\mathrm{span}(H, CNOT, S)$
- Classically simulable because $CPC^\dagger = P'$ for any Pauli P

Warmup: Clifford QCSAT is in P

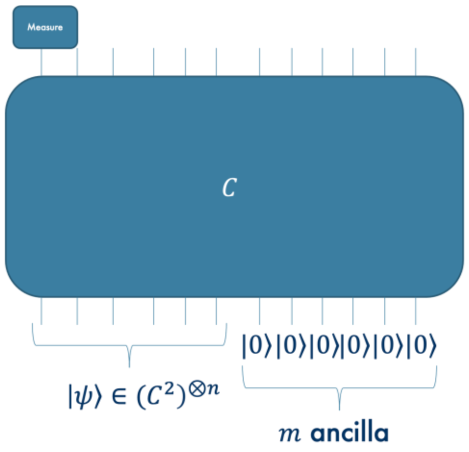
The measurement at the end $|0\rangle\langle 0| = \frac{I+Z}{2}$ so we are trying to optimize

$$\frac{1}{2} + \frac{1}{2}\left|\langle\psi| \otimes \langle 0^m|C^\dagger Z C\, |\psi\rangle \otimes |0^m\rangle\right|^2 = \frac{1}{2} + \frac{1}{2}|\langle\psi|P|\psi\rangle \otimes \langle 0^m|Q|0^m\rangle|^2$$

for Paulis P, Q.

Since we are trying to maximize $|\psi\rangle$ then $\langle\psi|P|\psi\rangle = 1$ in best case.

3 cases: $\frac{1}{2} + \frac{1}{2}|\langle 0^m|Q|0^m\rangle|^2 \in \{0, 1, ½\}$. Can easily calculate given Q and Q is calculable using standard Clifford calculus.



What happens when there are T gates

While Clifford conjugation maintain Paulis …

$$T^\dagger I T = I$$
$$T^\dagger X T = (X + Y)/\sqrt{2}$$
$$T^\dagger Y T = (X - Y)/\sqrt{2}$$
$$T^\dagger Z T = Z$$

So, by induction on the gates of a circuit C, we see that $C^\dagger Z C$ can be expressed as the lin. combination of $\leq 2^t$ terms

Many terms but few linearly independent ones

Claim: There exists a basis of $t+1$ Pauli terms so that all 2^t terms can be expressed as products of basis terms.

Proof by induction: Base case: $I^\dagger ZI = Z = \mathrm{b}_1$.

Let $C = g_s g_{s-1} \dots g_1$. At step i, let basis be $b_1, \dots, b_j$.

- If g_i is Clifford then, new basis of $g_i^\dagger b_1 g_i, \dots, g_i^\dagger b_j g_i$.
- If $g_i = T$ acting on qubit q,
  - then first rewrite basis so that only b_1, b_2 act non-trivially on qubit q
  - at most one of $b_1(q)$ and $b_2(q)$ is $\in \{X, Y\}$ and the other is $\{I, X\}$.
  - wlog assume $b_1(q) = X$. Then add $b_{j+1} = b_1 \cdot (XY)_q$ to the basis.

Many terms but few linearly independent ones

Claim: Since the $\leq 2^t$ Paulis have a linearly independent basis of $t+1$ Pauli terms, then there exists a Clifford unitary W mapping these Pauli to a space of at most $t+1$ qubits.

Proof sketch: Each linearly independent Pauli defines a "qubit" and so W can be constructed by a sequence of Clifford SWAP gate-like gadgets.

A more sophisticated analysis produces W exactly with only $\text{poly}(s)$ pre-processing (not included in this talk).

Interesting lower bound from upper bounds

- A reduction to a witness of length t
- A $5.3^t \cdot \mathrm{poly}(s)$ algorithm for solving parametrized QCSAT

Classical Exponential Time Hypothesis: SAT formulas on n variables cannot be solved in time $2^{o(n)}$.

Corollary: There does **not** exist a generic reduction from SAT formulas on n variables to SAT formulas on $\mathrm{o}(n)$ variables.

Interesting lower bound from upper bounds

- A reduction to a witness of length t
- A $5.3^t \cdot \text{poly}(s)$ algorithm for solving parametrized QCSAT

ETH $\implies$ Quantum proof length optimality Conjecture: There does **not** exist a generic reduction from QCSAT formulas with witness length n to QCSAT formulas with witness length $o(n)$.

Corollary: Assuming conj., in the worst case for QMA-hard problems, $t = \Omega(n)$.

Lower bound for the complexity of $|W\rangle$

Any local Hamiltonian H with m terms can be expressed as the sum of $O(m)$ local Pauli terms.

Then there exists a Clifford operator C s.t. $H = \langle W_{O(m)}|C|W_{O(m)}\rangle$

So, the local Hamiltonian problem can be expressed as

$$\max_{\psi} \langle \psi, W|C|\psi, W\rangle$$

Assume $|W\rangle = V|0^k\rangle$ for V a circuit consisting of t T-gates.

Lower bound for the complexity of $|W\rangle$

Assume $|W_{O(m)}\rangle = V|0^k\rangle$ for V a circuit consisting of t T-gates. Then, the problem can be rewritten as

$$\max_{\psi} \langle \psi, W|C|\psi, W\rangle = \max_{\psi} \langle \psi, 0^k\left|V^\dagger C V\right|\psi, 0^k\rangle$$

which can be reduced to (by main result) to witness length t.

Assuming optimal proof length conjecture, $t = \Omega(m)$ proving a linear lower bound on T-gate complexity of $|W\rangle$ state. Proof is robust to $1/\mathrm{poly}(m)$ noise or $O(1)$ noise assuming QPCP.

What's next

- A computational method for "testing" avg-case QMA vs QCMA
- Many other QMA-complete problems are built from q. circuits
  - How many of them also have parametrized complexity solutions
  - Ex. Non-identity check problem is in P for Clifford unitaries
- Is there a parameter like non-Clifford gate count that parametrizes the complexity of the local Hamiltonian problem?
- Is there a parameter that scales the problem between NP and QMA?
  - What about between QCMA and QMA?