Hidden variable model for quantum computation and Wheeler's "It from Bit"

Michael Zurel
Department of Mathematics, Simon Fraser University, Vancouver, Canada

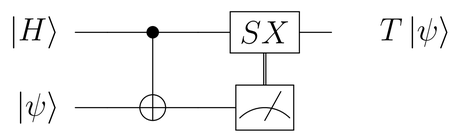
Abstract: Every quantum computation can be described by a probabilistic update of a probability distribution over a finite set of hidden variables. This description is closely related to classical simulation algorithms for quantum computations based on sampling from Wigner functions, except that Wigner functions can take negative values obstructing the sampling. Indeed, negativity in Wigner functions has been identified as a precondition for a quantum speed-up. However, if sufficiently general (quasi)probability functions are admitted, there is no need for any negativity at all. The question of interest for the present work is how much classical information the simulation of quantum computations must track, i.e., *What is the length of the bit strings returned by the sampling?* If it turned out that those bit strings were very long, say exponentially long in the number n of qubits, this would provide a convenient explanation for the hardness of classical simulation of universal quantum computation. However, we find that the bit strings are short: $O(n^2)$. Thus, the presumed hardness of this simulation must come from the computational hardness of the sampling processes involved. These results are consistent with Gleason's theorem and the Pusey-Barrett-Rudolph theorem, and have a connection to Wheeler's "It from Bit".

Quantum computation with magic

Quantum computation with magic states (QCM) [1] is a universal model of quantum computation in which:

- The operations are restricted to stabilizer operations (Clifford gates and Pauli measurements). These alone are not universal for quantum computation and can be efficiently simulated classically.
- Universality is restored by additional nonstabilizer quantum states at the input of the circuit.

For example, a (non-Clifford) $T := \mathrm{diag}(1, \exp(i\pi/4))$ gate is implemented as



where $|H\rangle = (|0\rangle + e^{i\pi/4}|1\rangle)/\sqrt{2}$ is a *magic* state.

Definitions

- Measurements in QCM are n-qubit Pauli observables which can be labelled by elements of $\mathbb{Z}_2^{2n}$. For any Pauli observable $T_a,\ a \in \mathbb{Z}_2^{2n}$, the projector corresponding to measurement outcome $s \in \mathbb{Z}_2$ is $\Pi_a^s := (1 + (-1)^s T_a)/2$.
- The Clifford group $\mathcal{C}\ell_n$ consists of all unitary gates that map Pauli operators to Pauli operators under conjugation.
- Let $\mathrm{Herm}_1(\mathbb{C}^{2^n})$ be the $\mathrm{Tr} = 1$ Hermitian operators on $\mathbb{C}^{2^n}$, and $\mathcal{S}_n$ the set of n-qubit stabilizer states.

The Λ polytope model

For any number n of qubits, we define a polytope

$$\Lambda_n = \left\{ X \in \mathrm{Herm}_1\left(\mathbb{C}^{2^n}\right) \mid \mathrm{Tr}(|\sigma\rangle\langle\sigma| X) \geq 0 \ \forall\, |\sigma\rangle \in \mathcal{S}_n \right\}.$$

Denote by $\{A_\alpha \mid \alpha \in \mathcal{V}_n\}$ the (finite) set of vertices of Λ_n. The Λ polytope mode is defined by the following theorem.

Theorem 1 (Ref. [2]) *For any number of qubits n,*

1. *Any quantum state ρ can be decomposed as*
$$\rho = \sum_{\alpha \in \mathcal{V}_n} p_\rho(\alpha) A_\alpha,$$
with $p_\rho(\alpha) \geq 0$ for all $\alpha \in \mathcal{V}_n$, and $\sum_\alpha p_\rho(\alpha) = 1$.
2. *For any $A_\alpha,\ \alpha \in \mathcal{V}_n$, and any Clifford gate g, $gA_\alpha g^\dagger =: A_{g\cdot\alpha}$ is a vertex of Λ_n with $g \cdot \alpha \in \mathcal{V}_n$.*
3. *For any $A_\alpha,\ \alpha \in \mathcal{V}_n$, and any Pauli projector Π_a^s,*
$$\Pi_a^s A_\alpha \Pi_a^s = \sum_{\beta \in \mathcal{V}_n} q_{\alpha,a}(\beta, s) A_\beta,$$
with $q_{\alpha,a}(\beta, s) \geq 0\ \forall \beta, s$, and $\sum_{\beta,s} q_{\alpha,a}(\beta, s) = 1$.

This theorem describes a hidden variable model for QCM in which (1) states are represented by probability distributions p_ρ over $\mathcal{V}_n$, (2) Clifford gates and Pauli measurements are represented by stochastic maps, $g \cdot - : \mathcal{V}_n \to \mathcal{V}_n$ and $q_{\alpha,a} : \mathcal{V}_n \times \mathbb{Z}_2^{2n} \to \mathcal{V}_n \times \mathbb{Z}_2$.

Classical simulation of QCM

A classical simulation algorithm for QCM based on the Λ polytope model is given below.

1: sample $\alpha \in \mathcal{V}_n$ according to $p_\rho : \mathcal{V}_n \to \mathbb{R}_{\geq 0}$
2: propagate α through the circuit
3: **while** end of circuit has not been reached **do**
4: **if** Clifford gate $g \in \mathcal{C}\ell_n$ is encountered **then**
5: update the phase space point $\alpha \hookleftarrow g \cdot \alpha$
6: **if** Pauli measurement a is encountered **then**
7: sample $(\beta, s) \in \mathcal{V}_n \times \mathbb{Z}_2$ according to $q_{\alpha,a}$
8: **return** $s \in \mathbb{Z}_2$ as the measurement outcome
9: update the phase space point $\alpha \hookleftarrow \beta$

This algorithm returns samples from the distribution of measurement outcomes for the quantum circuit being simulated which agree with the predictions of quantum theory.

"Its" to "Bits"

Naively, the number of bits required to specify a sample $\alpha \in \mathcal{V}_n$ in the simulation of a quantum computation is $\log_2(|\mathcal{V}_n|)$. However, this can be reduced using the following simple insight: in the QCM model, for any fixed value n, all quantum computations start in the *same* magic state $|M\rangle^{\otimes n}$. Thus, the question of interest for classical simulation of QCM using Λ polytopes is not "What is the size of the phase space $\mathcal{V}_n$?", but rather "What is the size of the region of $\mathcal{V}_n$ that can be reached from the initial state $|M\rangle^{\otimes n}$?".

For universal quantum computation, it suffices to consider adaptive sequences of commuting Pauli measurements of length n acting on a fixed magic state $|M\rangle^{\otimes n}$ [3]. For this restricted (but still universal) model of QCM, we have the following result.

Theorem 2 (Ref. 4, Main result) *Any quantum computation consisting of a sequence of n independent, pair-wise commuting Pauli measurements on a fixed magic state $|M\rangle^{\otimes n}$ can be simulated using a memory of $2n^2 + 3n$ bits to specify the phase space points reached.*

For a QCM computation on state ρ, and the corresponding simulation based on the Λ polytopes, the memory requirements are summarized by the following diagram:

$$\begin{array}{ccccccccc}
\rho & \xrightarrow{a_1} & s_1 & \xrightarrow{a_2} & s_2 & \xrightarrow{a_3} & s_3 & \cdots \\
p_\rho & \xrightarrow{q_{\alpha_0,a_1}} & (\alpha_1, s_1) & \xrightarrow{a_{\alpha_1,a_2}} & (\alpha_2, s_2) & \xrightarrow{q_{\alpha_2,a_3}} & (\alpha_3, s_3) & \cdots \\
\alpha_0 & \xrightarrow{a_1} & (\alpha_1, s_1) & \xrightarrow{a_2} & (\alpha_2, s_2) & \xrightarrow{a_3} & (\alpha_3, s_3) & \cdots \\
2n & +2n & +2n+1 & +2n & +2n+1 & +2n & 2n+1 & \cdots
\end{array}$$

If we admit arbitrarily long sequences of (potentially non-commuting) Pauli measurements and Clifford gates, we find that the memory requirement merely doubles (see Corollary 1 of Ref. [4]).

Gleason's theorem

Gleason's theorem says that in Hilbert spaces $\mathcal{H}$ of dimension 3 or greater, the only consistent way to assign probabilities to all measurement outcomes (subspaces $h \subset \mathcal{H}$) represented by projectors Π_h, is via the Born rule $\mathrm{Tr}(\rho\Pi_h)$ for some density matrix ρ. Gleason's theorem is sometimes interpreted as a mathematical proof that density operators are the fundamental notion of state in quantum theory. We show that every quantum state can be described by a probability distribution, and yet the Born rule is reproduced. This is possible because we restrict measurements to Pauli observables. This does not affect the universality of quantum computation!

The PBR theorem

The Λ polytope model is Ψ-epistemic. The PBR theorem [5] asserts that no Ψ-epistemic model can reproduce the predictions of quantum theory. Our result does not contradict the PBR theorem for two reasons. First, we consider only sequences of Pauli measurements rather than general measurements. Second, our model does not satisfy the assumption of preparation independence required for the theorem to hold. That is, in general, $p_{\rho_1} \otimes p_{\rho_2} \neq p_{\rho_1} \cdot p_{\rho_1}$. The assumption of preparation independence is less relevant for quantum computation with magic states, where, in the language of resource theories, the free sector is formed by stabilizer states and stabilizer operations, not local states and local operations. Further, the memory lower bound of Karanjai, Wallman, and Bartlett [7] shows that a classical simulation algorithm like that above is incompatible with this assumption.

Wheeler's "It from Bit"

In an article of 1989 [3], John Archibald Wheeler argued that quantum physics required a new perspective on reality based on information theoretic concepts. He wrote:

> No element in the description of physics shows itself as closer to primordial than the elementary quantum phenomenon, that is, the elementary device-intermediated act of posing a yes-no physical question and eliciting an answer or, in brief, the elementary act of observer-participancy. Otherwise stated, every physical quantity, every it, derives its ultimate significance from bits, binary yes-or-no indications, a conclusion we epitomize in the phrase, *it from bit*.

A prototypical realization of this view is provided in the description of QCM through the Λ polytopes. The "*It*" in this case is universal quantum computation, and hence all non-relativistic quantum mechanics in finite-dimensional Hilbert spaces. The "*Bits*" represent the binary outcomes of Pauli measurements and the labels of the vertices of the Λ polytopes. A crucial feature of the Λ polytope model is that the quantum state $|\Psi(t)\rangle$ of the system is replaced by a bit string $b(t)$ of bounded length. This description of the system's state does not invoke any approximation, $b(t)$ *is a valid and accurate representation of the quantum system,* and the distributions of measurement outcomes sampled from are the exact quantum-mechanical ones. The data representing the system is genuinely discrete, thus, we regard the Λ polytope model as a realization of Wheeler's proposal.

References

[1] Bravyi, Kitaev. Physical Review A **71**, 022316 (2005)
[2] Zurel, Okay, Raussendorf. Physical Review Letters **125** 260404 (2020)
[3] Peres, Galvão. Quantum **7** 1126 (2023)
[4] Zurel, Okay, Raussendorf. PRX Quantum **5** 030343 (2024)
[5] Pusey, Barrett, Rudolph. Nature Physics **8**, 475–478 (2012)
[6] Wheeler. "Information, Physics, Quantum: The Search for Links" (1989)
[7] Karanjai, Wallman, Bartlett. arXiv:1802.07744.