Simulating quantum computation with magic states
How many "bits" for "it"

Michael Zurel[1,2], Cihan Okay[3], Robert Raussendorf[1,2]

[1]Department of Physics & Astronomy, University of British Columbia, Vancouver, Canada
[2]Stewart Blusson Quantum Matter Institute, Vancouver, Canada
[3]Department of Mathematics, Bilkent University, Ankara, Turkey

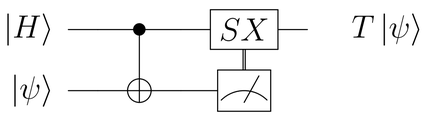
Abstract: A recently introduced classical simulation method for universal quantum computation with magic states operates by repeated sampling from probability functions [1]. This description of quantum computation is closely related to sampling algorithms based on Wigner functions, with the important distinction 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, it turns out that once sufficiently general (quasi)probability functions are admitted, there is no need for any negativity at all. Universal quantum computation can be described by repeated sampling from a generalized phase space whose points are labeled by the vertices of the Λ polytopes. This process essentially resembles a random walk, with the complication that the transition function changes from one time step to the next and can depend on the prior sampling history. 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?* For example, if it turned out that those bit strings were very long, say exponentially long in the number n of magic states, this would provide a convenient explanation for the hardness of classical simulation of universal quantum computation using Λ polytopes. If the information storage itself is inefficient, so is the processing. However, this is not what we find. 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.

Magic state quantum computation (QCM)

QCM is a universal model of quantum computation in which:

- The allowed operations are restricted to stabilizer operations (Clifford gates and Pauli measurements). These operations 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 T gate is implemented by the following circuit



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

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 $\mathcal{C}\ell_n$ is the group of unitary gates that map Pauli operators to Pauli operators under conjugation.
- Let $\mathrm{Herm}_1(\mathbb{C}^{2^n})$ denote the Hermitian operators on $\mathbb{C}^{2^n}$ with $\mathrm{Tr} = 1$, and $\mathcal{S}_n$ the set of n-qubit stabilizer states.

The Λ polytope model

For each number n of qubits, we define a polytope

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

Denote by $\{A_\alpha \mid \alpha \in \mathcal{V}_n\}$ the (finite) set of vertices of Λ_n.

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

1. *Any n-qubit 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_α, $\alpha \in \mathcal{V}_n$, and any Clifford gate $g \in \mathcal{C}\ell_n$, $gA_\alpha g^\dagger$ is a vertex of Λ_n. This defines an action of the Clifford group on $\mathcal{V}_n$ as $gA_\alpha g^\dagger =: A_{g\cdot\alpha}$ where $g\cdot\alpha \in \mathcal{V}_n$.*
3. *For any A_α, $\alpha \in \mathcal{V}_n$, 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 (HVM) 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 $g \cdot \alpha$ and $q_{\alpha,a}$.

Λ simulation method for 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** the end of the circuit has not been reached **do**
4: **if** a Clifford gate $g \in \mathcal{C}\ell_n$ is encountered **then**
5: update the phase space point according to $\alpha \rightarrowtail g \cdot \alpha$
6: **if** a Pauli measurement $a \in \mathbb{Z}_2^{2n}$ 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 outcome of the measurement
9: update the phase space point according to $\alpha \rightarrowtail \beta$

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

Main result

Naively, the number of bits required to specify a phase space point $\alpha \in \mathcal{V}_n$ 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 $|M\rangle^{\otimes n}$?".

In fact, for universal quantum computation, it suffices to consider adaptive sequences of commuting Pauli measurements of length n acting on a fixed magic state $|M\rangle^{\otimes n}$ [2]. 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, pairwise 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.*

Proof sketch. Since Λ_n lives in $\mathrm{Herm}_1\left(\mathbb{C}^{2^n}\right)$, a space of dimension $4^n - 1$, by Carathéodory's theorem there exist choices for p_ρ, and for $q_{\alpha,a}(-, s)$ for each $s \in \mathbb{Z}_2$, such that $|\mathrm{supp}(p_\rho)| \leq 4^n$ and $|\mathrm{supp}(q_{\alpha,a}(-, s))| \leq 4^n$. To start we fix a canonical choice for the distributions p_ρ and $q_{\alpha,a}$ satisfying these properties. Then specifying a sample from p_ρ requires no more than $\log_2(4^n) = 2n$ bits.
There are $4^n - 1$ nontrivial n-qubit Pauli measurements, therefore, specifying each measurement requires no more than $2n$ bits. For the t^{th} measurement a_t, the distribution q_{α_{t-1},a_t} is uniquely specified by the sampling history consisting of states $\alpha_0, \alpha_1, \ldots, \alpha_{t-1}$, measurements $a_1, a_2, \ldots, a_{t-1}$, and measurement outcomes $s_1, s_2, \ldots, s_{t-1}$. Once the distribution is fixed, with the canonical choice above, specifying a sample from this distribution requires no more than $2n + 1$ bits (1 bit for s_t and $2n$ bits for α_t).
Since the length of the measurement sequence is no more than n, the number of classical bits required to specify the complete sampling history is no more than

$$\underbrace{2n}_{\alpha_0} + \sum_{t=1}^{n} \left[\underbrace{2n}_{a_t} + \underbrace{1}_{s_t} + \underbrace{2n}_{\alpha_t} \right] = 4n^2 + 3n.$$

With some slightly more careful accounting, this bound can be improved to the one stated. □.

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:

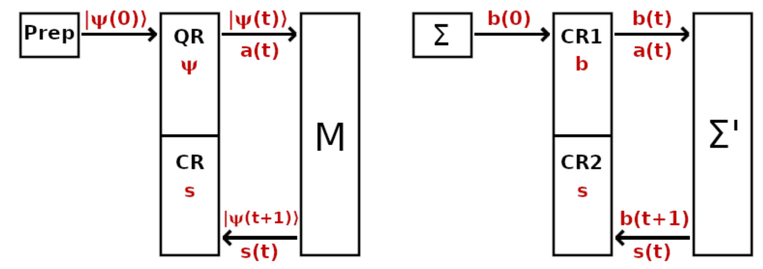
$$\begin{array}{ccccccccc}
\rho & \xrightarrow{a_1} & s_1 & \xrightarrow{a_2} & s_2 & \xrightarrow{a_3} & s_3 & \cdots \\
p_\rho & \xrightarrow{q_{\alpha_0,a_1}} & (\alpha_1, s_1) & \xrightarrow{a_{\alpha_1,a_2}} & (\alpha_2, s_2) & \xrightarrow{q_{\alpha_2,a_3}} & (\alpha_3, s_3) & \cdots \\
\alpha_0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

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).

References

[1] M Zurel, C Okay, R Raussendorf. Phys Rev Lett **125** 260404 (2020)
[2] F Peres, E Galvão. arXiv:2203.01789 (2022)
[3] JA Wheeler. "Information, Physics, Quantum: The Search for Links" (1989)
[4] M Zurel, C Okay, R Raussendorf. arXiv:2305.17287 (2023)

Illustration of the simulation method



(a) (b)

A QCM computation (a), and its simulation based on Λ polytopes (b). (a) QCM consists of preparing a quantum register in a magic state $|M\rangle^{\otimes n}$, followed by a sequence of Pauli measurements. This requires a device Prep to deliver the magic states to the quantum register QR, and a classical register CR to store the previous measurement record **s**, a classical side computation to identify the label $a(t)$ of the Pauli observable measured in step t, and a measurement device M to perform the measurements and to output the corresponding results $s(t)$. (b) The overall structure of the classical simulation is the same. Prep is replaced by a first sampler Σ that samples from the phase space distribution of the initial state $|M\rangle^{\otimes n}$. There are two classical registers, CR1 and CR2. The former stores the phase space samples $b(t)$, and the latter the prior measurement record, as in (a). The measurement device M is replaced by a second sampler Σ' that takes as input a phase space point $b(t)$ and a Pauli label $a(t)$, and outputs a new phase space point $b(t+1)$ as well as a measurement outcome $s(t)$.

"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 has been 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.
It should be noted that, in the end, what needs to be reproduced is the quantum mechanical prediction for the joint distribution of measurement outcomes. For it, the statistical distribution of the bit strings $\{b(t), \forall t\}$ matters, not individual values $b(t)$. However, this is the same for the quantum mechanical states $|\Psi(t)\rangle$. They too are conditioned on prior measurement outcomes, hence probabilistic.