Hidden Variable Model for Universal Quantum Computation with Magic States on Qubits

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

1: *Department of Physics and Astronomy, University of British Columbia, Vancouver, Canada,*

2: *Stewart Blusson Quantum Matter Institute, University of British Columbia, Vancouver, Canada*

3: *Department of Mathematics, Bilkent University, Ankara, Turkey*

Abstract: We show that every quantum computation can be described by a probabilistic update of a probability distribution on a finite phase space. Negativity in a quasiprobability function is not required in states or operations. Our result is consistent with Gleason's theorem and the Pusey-Barrett-Rudolph theorem. This result was recently published in Phys. Rev. Lett. [6]

Introduction

It is often pointed out that the fundamental objects in quantum mechanics are amplitudes, not probabilities. This fact notwithstanding, here we construct a description of universal quantum computation—and hence of all quantum mechanics in finite-dimensional Hilbert spaces—in terms of probabilistic update of a probability distribution. In this formulation, quantum algorithms look structurally akin to classical diffusion problems.

While this seems implausible, there exists a well-known special instance of it: quantum computation with magic states (QCM) on a single qubit. Compounding two standard one-qubit Wigner functions, a hidden variable model can be constructed in which every one-qubit quantum state is positively represented [2]. This representation is furthermore covariant under all one-qubit Clifford unitaries and positivity-preserving under all one-qubit Pauli measurements. The update under such operations preserves the probabilistic character of the model, and hence QCM on one qubit can be classically simulated by probabilistic update of a probability function on eight elements.

The prevailing view on the one-qubit example is that it is an exception, and for multiple qubits negativity will inevitably creep into any quasiprobability function of any computationally useful quantum state, rendering classical simulation inefficient. This hypothesis is informed by the study of Wigner functions in finite-dimensional state spaces, which establishes Wigner function negativity as a necessary computational resource, i.e., there can be no quantum speedup without negativity. A quantum optics notion of quantumness—negativity of Wigner functions—and a computational notion—hardness of classical simulation—thus align.

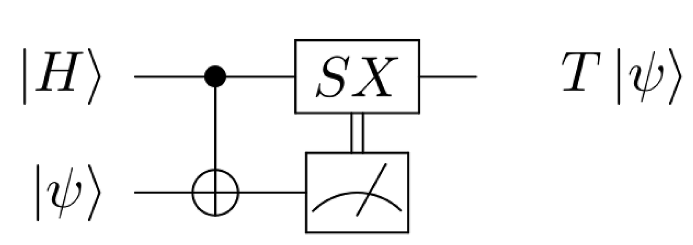
The viewpoint just summarized requires correction. As we show, the one-qubit case is not an exception; rather it is an example illustrating the general case. *Every* quantum state on any number of qubits can be represented by a probability function, and the update of this probability function under Pauli measurement is also probabilistic. We emphasize that *both* the states and operations are represented positively, not just one or the other.

We apply this to quantum computation with magic states, showing that universal quantum computation can be classically simulated by the probabilistic update of a probability distribution.

Quantum computation with magic states (QCM)

In quantum computation by injection of magic states [1],

- The unitaries, measurements and state preparations are non-universal, and are considered "free". The free unitaries are chosen from a subgroup of the Clifford group, and the free measurements are of Pauli observables.
- The computational power resides with the *magic states*, which can be injected into the computation.



Setting and definitions

We denote the n-qubit Pauli operators by

$$T_a = i^{\phi(a)} \bigotimes_{k=1}^{n} X^{a_X[k]} Z^{a_Z[k]}, \quad \forall a = (a_X, a_Z) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n =: E_n.$$

The projectors onto the eigenspaces of Pauli observables are

$$\Pi_{a,s} := \frac{I + (-1)^s T_a}{2}, \quad \forall a \in E_n, s \in \mathbb{Z}_2.$$

The state space Λ_n of our model is defined as follows. Denote by $\text{Herm}_1(2^n)$ the set of Hermitian operators on n-qubit Hilbert space $H = \mathbb{C}^{2^n}$ with the property that $\text{Tr}(X) = 1$ for all $X \in \text{Herm}_1(2^n)$, and by $\mathcal{S}_n$ the set of all n-qubit pure stabilizer states. Then we define the polytope Λ_n as

$$\Lambda_n := \{X \in \text{Herm}_1(2^n) | \text{Tr}(|\sigma\rangle\langle\sigma|\, X) \geq 0, \forall\, |\sigma\rangle \in \mathcal{S}_n\}.$$

Denote by $\mathcal{A}_n$ the set of vertices of Λ_n, and the vertices by $A_\alpha \in \mathcal{A}_n$. These are our generalized phase point operators, and the corresponding index set $\{\alpha\} =: \mathcal{V}_n$ is the generalized phase space.

Main result

Theorem. For all numbers of qubits $n \in \mathbb{N}$, (i) each n-qubit quantum state ρ can be represented by a probability function $p_\rho : \mathcal{V}_n \longrightarrow \mathbb{R}_{\geq 0}$,

$$\rho = \sum_{\alpha \in \mathcal{V}_n} p_\rho(\alpha)\, A_\alpha. \tag{1}$$

(ii) For any Clifford unitary U, it holds that

$$U A_\alpha U^\dagger = A_{U\cdot\alpha} \in \mathcal{A}_n.$$

(iii) For the state update under Pauli measurements it holds that

$$\Pi_{a,s} A_\alpha \Pi_{a,s} = \sum_{\beta \in \mathcal{V}_n} q_{\alpha,a}(\beta, s)\, A_\beta. \tag{2}$$

For all $a \in E_n$, $\alpha \in \mathcal{V}_n$, the $q_{\alpha,a} : \mathcal{V}_n \times \mathbb{Z}_2 \longrightarrow \mathbb{R}_{\geq 0}$ are probability functions,

(iv) Denote by $P_{\rho,a}(s)$ the probability of obtaining outcome s for a measurement of T_a on the state ρ. Then, the Born rule $P_{\rho,a}(s) = Tr(\Pi_{a,s}\rho)$ takes the form

$$Tr(\Pi_{a,s}\rho) = \sum_{\alpha \in \mathcal{V}_n} p_\rho(\alpha) Q_a(s|\alpha), \tag{3}$$

where $Q_a(s|\alpha)$ is given by

$$Q_a(s|\alpha) := \sum_{\beta \in \mathcal{V}_n} q_{\alpha,a}(\beta, s). \tag{4}$$

Hence $0 \leq Q_a(s|\alpha) \leq 1$, for all a, s, α.

Classical simulation of universal quantum computation

The hidden variable model defined above can be used to simulate quantum computation with magic states.

Algorithm sketch.

1. Start with a decomposition of the input state ρ of the form Eq. (1). Sample from $p_\rho(\alpha)$ to obtain an initial phase space point α.
2. For each Clifford unitary U in the quantum circuit, update the phase space point $\alpha \longleftarrow U \cdot \alpha$.
3. For each Pauli measurement $a \in E_n$, sample from the distribution $q_{\alpha,a}$ to obtain $s \in \mathbb{Z}_2$ and $\beta \in \mathcal{V}_n$. Return s as the outcome of the measurement and update the phase space point $\alpha \longleftarrow \beta$.

Discussion

Negativity in quasiprobability representations has been identified as a cause for slowing down the classical simulation of quantum systems by sampling. A general result has been obtained in Ref. [4] stating that a quantum system described by a quasiprobability function W with negativity $\mathcal{M} = ||W||_1$ can be simulated by sampling at a cost that scales like $\mathcal{M}^2$. There are simulation schemes for QCM on qudits [3] and on qubits [5], where negativity is the only source for the computational hardness of classical simulation. Negativity is therefore singled out as a precondition for quantum speedup. We do not contradict these results but now find that they are an artifact of the particular quasiprobability functions chosen. Our result lies at the opposite end of the spectrum. There is no negativity but, presumably, still computational hardness.

For a more in depth discussion, including the relation of this model to the Pusey-Barrett-Rudolph theorem and Gleason's theorem, and a discussion of contextuality, see Ref. [6].

References

[1] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[2] J.J. Wallman and S.D. Bartlett, Phys. Rev. A **85**, 062121 (2012).

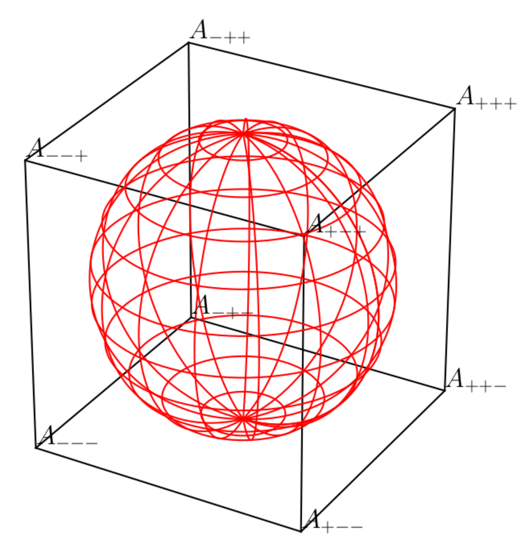
[3] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, New J. Phys. **15** 039502 (2012)

[4] H. Pashayan. J.J. Wallman and S.D. Bartlett, Phys. Rev. Lett. **115** 070501 (2015).

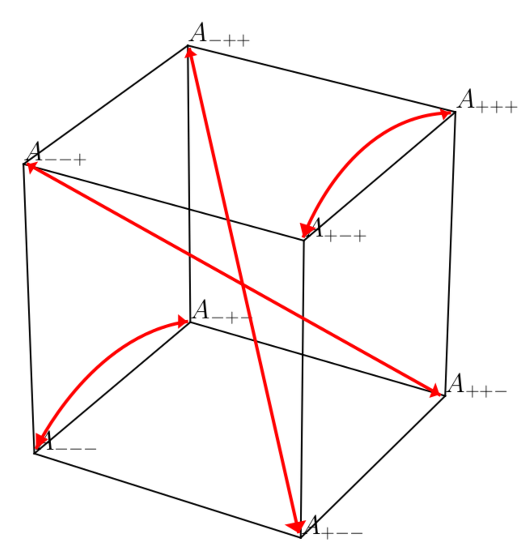
[5] Robert Raussendorf, Juani Bermejo-Vega, Emily Tyhurst, Cihan Okay, and Michael Zurel, Phys. Rev. A **101** 012350 (2020).

[6] Michael Zurel, Cihan Okay, and Robert Raussendorf, Phys. Rev. Lett. **125** 260404 (2020).

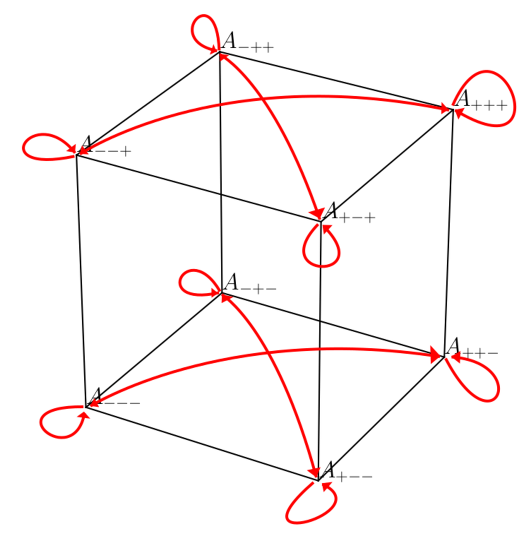
One-qubit example



The state space Λ_1 is a cube with eight vertices corresponding to the phase point operators $A_\alpha = [I + (-1)^{s_x}X + (-1)^{s_y}Y + (-1)^{s_z}Z]/2$, with $\alpha = (s_x, s_y, s_z) \in \mathbb{Z}_2^3$. The physical one-qubit states lie on or in the Bloch sphere that is contained in Λ_1. Any one-qubit state can be expressed as a convex combination of the vertices of the cube as in Eq. (1).



Under conjugation by a Clifford unitary, vertices of Λ_1 map deterministically to other vertices. For example, the action of a Hadamard gate H on the vertices is shown here. Each red arrow represents a deterministic transition.



Under a Pauli measurement, $a \in E_1$, outcome s is returned with probability $Q_a(s|\alpha)$ and the update of the vertices is probabilistic. For example, a Pauli Z measurement is shown here. Each red arrow represents a transition probability of 0.5.

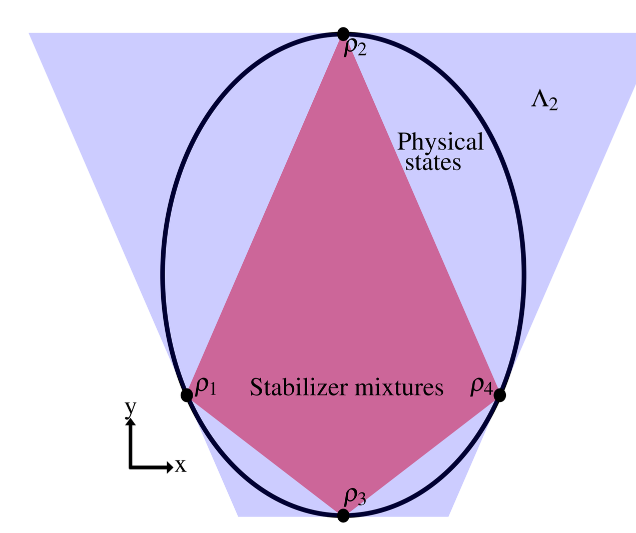
Structure of the polytope Λ

- In general, the polytope Λ_n is not a hypercube as in the case of one qubit. For example, on two qubits, Λ_2 is a polytope in a 15-dimensional space with 60 facets and 22320 vertices. A two-dimensional cross section of Λ_2 is shown in the figure below. The cross section is parametrized by

$$\rho(x, y) = \frac{1}{4} I_{12} + x(Z_1 + Z_2) + y(X_1X_2 + Z_1Z_2 - Y_1Y_2).$$

The four states labelled in the figure are

$$\begin{aligned}
\rho_1 &= \frac{1}{4} I_{12} - \frac{1}{8}(Z_1 + Z_2),\\
\rho_2 &= \frac{1}{4} I_{12} + \frac{1}{4}(X_1X_2 + Z_1Z_2 - Y_1Y_2),\\
\rho_3 &= \frac{1}{4} I_{12} - \frac{1}{12}(X_1X_2 + Z_1Z_2 - Y_1Y_2),\\
\rho_4 &= \frac{1}{4} I_{12} + \frac{1}{8}(Z_1 + Z_2).
\end{aligned}$$



- The phase point operators of the form

$$A_\Omega^\gamma = \frac{1}{2^n} \sum_{b \in \Omega} (-1)^{\gamma(b)} T_b$$

with $\Omega \subset E_n$ and $\gamma : \Omega \to \mathbb{Z}_2$ a noncontextual value assignment on Ω first defined in Ref. [5] are vertices of Λ_n. There are more vertices of Λ_n which do not have this form.