Learning stabilizer states by Bell sampling

Ashley Montanaro[1]

[1]*School of Mathematics, University of Bristol, UK*[*]

We show that measuring pairs of qubits in the Bell basis can be used to obtain a simple quantum algorithm for efficiently identifying an unknown stabilizer state of n qubits. The algorithm uses $O(n)$ copies of the input state and fails with exponentially small probability.

It is well-known and follows from Holevo's theorem [7] that approximately determining an arbitrary quantum state $|\psi\rangle$ of n qubits requires exponentially many (in n) copies of $|\psi\rangle$. One way of circumventing this problem is to relax the notion of what it means to determine $|\psi\rangle$ (e.g. by requiring only that we are able to predict the result of "most" measurements on $|\psi\rangle$, according to some probability distribution [1]); another way is to restrict the class of states to be determined to some class which can be described efficiently. In this setting, we are given a quantum system that is promised to be in a state picked from some family of quantum states, and are asked to determine its state, exactly or approximately.

One example where efficient identification can be achieved is the class of states well approximated by a matrix product state [4]. Another example, on which we will focus here, is the class of stabilizer states. Aaronson and Gottesman described an efficient procedure for identifying an unknown stabilizer state $|\psi\rangle$ of n qubits [3]. One variant of their algorithm uses $O(n^2)$ copies of $|\psi\rangle$. In this variant, all measurements are performed on single copies of $|\psi\rangle$. Another variant uses only $O(n)$ copies of $|\psi\rangle$, but is based on collective measurements across all these copies. This second algorithm is information-theoretically optimal: as there are $2^{\Theta(n^2)}$ stabilizer states on n qubits [2], identifying $|\psi\rangle$ requires $\Omega(n)$ copies of $|\psi\rangle$ by Holevo's theorem [7].

In related work, Low has shown that an unknown element U of the Clifford group on n qubits can be identified with $O(n^2)$ uses of U, or even only $O(n)$ if $U^\dagger$ is also available [8]. Rocchetto has shown that an unknown stabilizer state can be learned efficiently in the PAC model [9].

Here we will prove the following result:

Theorem 1. *There is a quantum algorithm which identifies an unknown stabilizer state $|\psi\rangle$ of n qubits given access to $O(n)$ copies of $|\psi\rangle$. The algorithm makes collective measurements across at most two copies of $|\psi\rangle$ at a time, runs in time $O(n^3)$ and fails with probability exponentially small in n.*

The number of copies of $|\psi\rangle$ used by this algorithm thus matches that of Aaronson and Gottesman's collective-measurement algorithm [3], but the algorithm acts on a smaller number of copies at a time. In addition, the measurements made by the algorithm across pairs of copies of $|\psi\rangle$ are simple to implement: they are based on measuring pairs of corresponding qubits of $|\psi\rangle^{\otimes 2}$ in the Bell basis. This is reminiscent of the algorithm of [6] for testing product states, where the measurement performed across pairs of qubits was the swap test.

An alternative algorithm for identifying an unknown graph state (a subclass of stabilizer states) on n qubits using $O(n)$ copies has been presented in independent work of Zhao, Pérez-Delgado and Fitzsimons [12]. Their algorithm has some structural similarities to the algorithm of the present paper.

Preliminaries

We will use the matrices

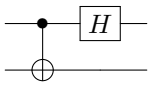
$$\sigma_{00} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_{01} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_{10} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$\sigma_{11} := \sigma_{10}\sigma_{01} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

which are the Pauli matrices up to applying $-i$ to σ_{11}, and the Bell basis, i.e. the ordered basis of $\mathbb{C}^4$ which we define by

$$|\sigma_{00}\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |\sigma_{01}\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\sigma_{10}\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), |\sigma_{11}\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

The notation is supposed to highlight the fact that $|\sigma_i\rangle = \mathrm{vec}(\sigma_i)/\sqrt{2}$, where vec is the linear map defined by $\mathrm{vec}(|x\rangle\langle y|) = |x\rangle|y\rangle$ for computational basis states x, y. The vec operator preserves inner products: $\langle \mathrm{vec}(A)| \mathrm{vec}(B)\rangle = \mathrm{tr}\, A^\dagger B$. For $s \in \{0,1\}^{2n}$, we write $\sigma_s := \sigma_{s_1 s_2} \otimes \cdots \otimes \sigma_{s_{2n-1} s_{2n}}$, $|\sigma_s\rangle := |\sigma_{s_1 s_2}\rangle \ldots |\sigma_{s_{2n-1} s_{2n}}\rangle$. Up to multiplying by -1, $\sigma_s \sigma_t = \sigma_{s \oplus t}$.

Measurement in the Bell basis can be implemented by applying the circuit



and measuring in the computational basis. Given a pure state of $2n$ qubits divided into systems $A_1, \ldots, A_n$, $B_1, \ldots, B_n$, we call the operation of measuring each pair $A_i B_i$ of qubits in the Bell basis *Bell sampling*. Each such measurement returns a $2n$-bit string.

For any state $|\psi\rangle$, let $|\psi^*\rangle$ denote the complex conjugate (taken in the computational basis).

Lemma 2. *Let $|\psi\rangle$ be a state of n qubits. Bell sampling on $|\psi\rangle^{\otimes 2}$ returns outcome r with probability*

$$\frac{|\langle\psi|\sigma_r|\psi^*\rangle|^2}{2^n}.$$

Proof. We have $|\psi\rangle|\psi\rangle = \mathrm{vec}(|\psi\rangle\langle\psi^*|)$, so $|\langle\sigma_r|\psi\rangle|\psi\rangle|^2 = 2^{-n}|\operatorname{tr}\sigma_r^\dagger|\psi\rangle\langle\psi^*||^2 = 2^{-n}|\langle\psi|\sigma_r|\psi^*\rangle|^2$. □

LEARNING STABILIZER STATES

We now show that Bell sampling can be used to learn stabilizer states efficiently. By a result of [5] (see [11] for an alternative proof), up to an overall phase every stabilizer state $|\psi\rangle$ can be written in the form

$$|\psi\rangle = \frac{1}{\sqrt{|A|}}\sum_{x\in A} i^{\ell(x)}(-1)^{q(x)}|x\rangle,$$

where A is an affine subspace of $\mathbb{F}_2^n$, and $\ell, q : \{0,1\}^n \to \{0,1\}$ are linear and quadratic (respectively) polynomials over $\mathbb{F}_2$. As ℓ is linear, $\ell(x) = s\cdot x$ for some $s \in \{0,1\}^n$, so we have $i^{\ell(x)} = \prod_{k\in S} i^{x_k}$ for some $S \subseteq [n]$. Hence

$$|\psi^*\rangle = \sigma_{10}^{\otimes S}|\psi\rangle.$$

If we perform Bell sampling on $|\psi\rangle^{\otimes 2}$, by Lemma 2 we receive outcome r with probability

$$\frac{|\langle\psi|\sigma_r|\psi^*\rangle|^2}{2^n} = \frac{|\langle\psi|\sigma_r\sigma_{10}^{\otimes S}|\psi\rangle|^2}{2^n}. \tag{1}$$

Any stabilizer state $|\psi\rangle$ is uniquely specified by a commuting subgroup G of Pauli matrices M (with potentially additional overall phases ± 1) such that $|G| = 2^n$, $M|\psi\rangle = |\psi\rangle$ for all $M \in G$, and $\langle\psi|M|\psi\rangle = 0$ for all Pauli matrices $M \notin G$. Let T denote the set of strings $t \in \{0,1\}^{2n}$ such that $\sigma_t \in G$, up to a phase. Then T is an n-dimensional linear subspace of $\mathbb{F}_2^{2n}$. Determining T suffices to uniquely determine $|\psi\rangle$: although T does not contain information about phases, once we have found a basis for T, we can measure $|\psi\rangle$ in the eigenbasis of each corresponding Pauli matrix M to decide whether $M|\psi\rangle = |\psi\rangle$ or $M|\psi\rangle = -|\psi\rangle$.

By eqn. (1), Bell sampling gives an outcome r which is uniformly distributed on the set $\{t \oplus s : t \in T\}$ for some $s \in \{0,1\}^{2n}$. Thus, for any two such outcomes r_1, r_2, the sum $r_1 \oplus r_2$ is uniformly distributed in T. In order to find a basis for T, we can therefore produce $k+1$ Bell samples $r_0, r_1, \ldots, r_k$, for some k, and consider the uniformly random elements of T given by $r_1 \oplus r_0, r_2 \oplus r_0, \ldots, r_k \oplus r_0$. If the dimension of the subspace of $\mathbb{F}_2^{2n}$ spanned by these vectors is n, any basis of this subspace is a basis for T.

We give an explicit description of this algorithm as Algorithm 1 (boxed). The algorithm uses $5n+2$ copies of $|\psi\rangle$. The time complexity of the algorithm is dominated by the basis-determination step, which can be achieved using Gaussian elimination in time $O(n^3)$; technically, this can be improved to $O(n^\omega)$, where $\omega < 2.373$ is the matrix multiplication exponent. Note that any algorithm for learning a stabilizer state requires time $\Omega(n^2)$ just to write the output.

Algorithm 1 (Learning stabilizer states).

1. Set $S = \emptyset$.
2. Create two copies of $|\psi\rangle$ and perform Bell sampling, obtaining outcome r_0.
3. Repeat the following $2n$ times:
   (a) Create two copies of $|\psi\rangle$ and perform Bell sampling, obtaining outcome r.
   (b) Add $r \oplus r_0$ to S.
4. Determine a basis for S; call this basis B.
5. For each element of B, measure a copy of $|\psi\rangle$ in the eigenbasis of the corresponding Pauli matrix M to determine whether $M|\psi\rangle = |\psi\rangle$ or $M|\psi\rangle = -|\psi\rangle$.

The algorithm fails (i.e. does not identify $|\psi\rangle$) if each of the $2n$ samples $r \oplus r_0$ lies in a subspace of T of dimension at most $n-1$. The probability that the samples are all contained in any one such subspace is 2^{-2n}; by a union bound over all subspaces of dimension $n-1$, the algorithm fails with probability at most 2^{-n}.

Algorithm 1 can be seen as a generalisation of a result of Rötteler [10] which gives an $O(n)$-query algorithm for learning functions $f : \{0,1\}^n \to \{0,1\}$ which are polynomials of degree 2 over $\mathbb{F}_2$. The algorithm of [10] works by producing states of the form

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle,$$

and then proceeds in a similar way to Algorithm 1 (although it is presented differently).

Acknowledgements. This work was largely carried out while the author was at the University of Cambridge, and was supported by the UK EPSRC (EP/G049416/2, EP/L021005/1). Thanks to Joe Fitzsimons for pointing out ref. [12].

* ashley.montanaro@bristol.ac.uk

[1] S. Aaronson. The learnability of quantum states. *Proceedings of the Royal Society A*, 463:2088, 2007. quant-ph/0608142.

[2] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328, 2004. quant-ph/0406196.

[3] S. Aaronson and D. Gottesman. Identifying stabilizer states, 2008. http://pirsa.org/08080052/.

[4] M. Cramer, M. Plenio, S. Flammia, R. Somma, D. Gross, S. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu. Efficient quantum state tomography. *Nature Communications*, 1(9):49, 2010. arXiv:1101.4366.

[5] J. Dehaene and B. De Moor. Clifford group, stabilizer states, and linear and quadratic operations over GF(2). *Phys. Rev. A*, 68:042318, 2003. quant-ph/0304125.

[6] A. Harrow and A. Montanaro. Testing product states, quantum Merlin-Arthur games and tensor optimization. *J. ACM*, 60(1), 2013. arXiv:1001.0017.

[7] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973. English translation *Problems of Information Transmission*, vol. 9, pp. 177-183, 1973.

[8] R. Low. Learning and testing algorithms for the Clifford group. *Phys. Rev. A*, 80:052314, 2009. arXiv:0907.2833.

[9] A. Rocchetto. Stabiliser states are efficiently PAC-learnable, 2017. arXiv:1705.00345.

[10] M. Rötteler. Quantum algorithms to solve the hidden shift problem for quadratics and for functions of large Gowers norm. In *Proc. MFCS'09, LNCS vol. 5734*, pages 663–674, 2009. arXiv:0911.4724.

[11] M. Van den Nest. Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond. *Quantum Inf. Comput.*, 10(3–4):0258–0271, 2010. arXiv:0811.0898.

[12] L. Zhao, C. Pérez-Delgado, and J. Fitzsimons. Fast graph operations in quantum computation. *Phys. Rev. A*, 93:032314, 2016. arXiv:1510.03742.