Stabilizer States as a Basis for Density Matrices

Simon J. Gay
School of Computing Science, University of Glasgow, UK

December 9, 2011

Abstract

We show that the space of density matrices for n-qubit states, considered as a $(2^n)^2$-dimensional real vector space, has a basis consisting of density matrices of stabilizer states. We describe an application of this result to automated verification of quantum protocols.

1 Definitions and Results

We are working with the stabilizer formalism [5], in which certain quantum states on sets of qubits are represented by the intersection of their stabilizer groups with the group generated by the Pauli operators. The stabilizer formalism is defined, explained and illustrated in a substantial literature; good introductions are given by Aaronson and Gottesman [1] and Nielsen and Chuang [7, Sec. 10.5].

In this paper we only need to use the following facts about stabilizer states.

1. The standard basis states are stabilizer states.
2. The set of stabilizer states is closed under application of Hadamard (H), Pauli (X, Y, Z), controlled not (CNot), and phase ($\mathsf{P} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$) gates.
3. The set of stabilizer states is closed under tensor product.

Notation 1 *Write the standard basis for n-qubit states as $\{|x\rangle \mid 0 \leqslant x < 2^n\}$, considering numbers to stand for their binary representations. We omit normalization factors when writing quantum states.*

Definition 1 *Let $\mathsf{GHZ}_n = |0\rangle + |2^n - 1\rangle$ and $\mathsf{iGHZ}_n = |0\rangle + i|2^n - 1\rangle$, as n-qubit states.*

Lemma 1 *For all n, GHZ_n and iGHZ_n are stabilizer states.*

Proof: By induction on n. For the base case ($n = 1$), we have that $|0\rangle + |1\rangle$ and $|0\rangle + i|1\rangle$ are stabilizer states, by applying H and then P to $|0\rangle$.

For the inductive case, GHZ_n and iGHZ_n are obtained from $\mathsf{GHZ}_{n-1} \otimes |0\rangle$ and $\mathsf{iGHZ}_{n-1} \otimes |0\rangle$, respectively, by applying CNot to the two rightmost qubits. □

Lemma 2 *If $0 \leqslant x, y < 2^n$ and $x \neq y$ then $|x\rangle + |y\rangle$ and $|x\rangle + i|y\rangle$ are stabilizer states.*

Proof: By induction on n. For the base case ($n = 1$), the closure properties imply that $|0\rangle + |1\rangle$, $|0\rangle + i|1\rangle$ and $|1\rangle + i|0\rangle = |0\rangle - i|1\rangle$ are stabilizer states.

For the inductive case, consider the binary representations of x and y. If there is a bit position in which x and y have the same value b, then $|x\rangle + |y\rangle$ is the tensor product of $|b\rangle$ with an $(n-1)$-qubit state of the form $|x'\rangle + |y'\rangle$, where $x' \neq y'$. By the induction hypothesis, $|x'\rangle + |y'\rangle$ is a stabilizer state, and the conclusion follows from the closure properties. Similarly for $|x\rangle + i|y\rangle$.

Otherwise, the binary representations of x and y are complementary bit patterns. In this case, $|x\rangle + |y\rangle$ can be obtained from GHZ_n by applying X to certain qubits. The conclusion follows from Lemma 1 and the closure properties. The same argument applies to $|x\rangle + i|y\rangle$, using iGHZ_n. □

Theorem 1 *The space of density matrices for n-qubit states, considered as a $(2^n)^2$-dimensional real vector space, has a basis consisting of density matrices of n-qubit stabilizer states.*

Proof: This is the space of Hermitian matrices and its obvious basis is the union of

$$\{|x\rangle\langle x| \mid 0 \leqslant x < 2^n\} \tag{1}$$

$$\{|x\rangle\langle y| + |y\rangle\langle x| \mid 0 \leqslant x < y < 2^n\} \tag{2}$$

$$\{-i|x\rangle\langle y| + i|y\rangle\langle x| \mid 0 \leqslant x < y < 2^n\}. \tag{3}$$

Now consider the union of

$$\{|x\rangle\langle x| \mid 0 \leqslant x < 2^n\} \tag{4}$$

$$\{(|x\rangle + |y\rangle)(\langle x| + \langle y|) \mid 0 \leqslant x < y < 2^n\} \tag{5}$$

$$\{(|x\rangle + i|y\rangle)(\langle x| - i\langle y|) \mid 0 \leqslant x < y < 2^n\}. \tag{6}$$

This is also a set of $(2^n)^2$ states, and it spans the space because we can obtain states of forms (2) and (3) by subtracting states of form (4) from those of forms (5) and (6). Therefore it is a basis, and by Lemma 2 it consists of stabilizer states. □

2 Applications

The stabilizer formalism can be used to implement an efficient classical simulation of quantum computation, if quantum operations are restricted to those under which the set of stabilizer states is closed — i.e. the Clifford group operations. This result is the Gottesman-Knill Theorem [6]. Gay, Nagarajan and Papanikolaou [3, 4, 8] have applied it to formal verification of quantum systems, adapting model-checking techniques [2] from classical computer science. A simple example of model-checking is the following.

Consider a quantum teleportation protocol as a system with one qubit as input and one (different) qubit as output; call this system *Teleport*. Also consider the one-qubit identity operator I. Then the specification that teleportation should satisfy is that $\mathit{Teleport} = I$, where equality means the same transformation of a one-qubit state. The aim of model-checking in this context is to automatically verify that this specification is satisfied, by simulating the operation of the two systems on all possible inputs. For this to be possible, the teleportation protocol is first expressed in a formal modelling language analogous to a programming language.

The approach of Gay, Nagarajan and Papanikolaou reduces the problem to that of simulating teleportation on stabilizer states as inputs, which can be done efficiently because the teleportation protocol itself only uses Clifford group operations. Correctness of teleportation on stabilizer states is interpreted as evidence for, although not proof of, correctness on arbitrary states. Now, however, we can draw a stronger conclusion.

The teleportation protocol defines a superoperator; this can be proved, for example, by the techniques of Selinger [9], who uses superoperators to define the semantics of a programming language that can certainly express teleportation. Superoperators, among other properties, are linear operators on the space of density matrices. To check equivalence of two superoperators, it is therefore sufficient to check that they have the same effect on all elements of a particular basis. By taking a basis that consists of stabilizer states, this can be done efficiently.

Moreover, the number of stabilizer states on n qubits is approximately $2^{(n^2)/2}$, whereas the dimensionality of the space of n-qubit density matrices is only $(2^n)^2 = 2^{2n}$. It is therefore more efficient to model-check on a basis than on all stabilizer states.

3 Conclusion

We have proved that the space of n-qubit density matrices has a basis consisting of stabilizer states, and explained how this result can be used to improve the efficiency and strengthen the results of model-checking for quantum systems.

References

[1] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70:52328, 2004.

[2] E. M. Clarke, Jr., O. Grumberg, and D. A. Peled. *Model Checking.* MIT Press, 1999.

[3] S. J. Gay, N. Papanikolaou, and R. Nagarajan. QMC: a model checker for quantum systems. In *CAV 2008: Proceedings of the 20th International Conference on Computer Aided Verification*, number 5123 in Lecture Notes in Computer Science, pages 543–547. Springer, 2008.

[4] S. J. Gay, N. Papanikolaou, and R. Nagarajan. Specification and verification of quantum protocols. In *Semantic Techniques in Quantum Computation*, pages 414–472. Cambridge University Press, 2010.

[5] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A*, 54:1862, 1996.

[6] D. Gottesman. *Stabilizer Codes and Quantum Error Correction.* PhD thesis, California Institute of Technology, 1997.

[7] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[8] N. Papanikolaou. *Model Checking Quantum Protocols.* PhD thesis, University of Warwick, 2009.

[9] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.