Representation of Quantum Circuits with Clifford and $\pi/8$ Gates

Ken Matsumoto[1] * Kazuyuki Amano[1] †

[1] *Department of Computer Science, Graduate School of Engineering, Gunma University*
Tenjin 1-5-1, Kiryu, Gunma 376-8515 Japan

Abstract. In this paper, we introduce the notion of a normal form of one qubit quantum circuits over the basis $\{H, P, T\}$, where H, P and T denote the Hadamard, Phase and $\pi/8$ gates, respectively. This basis is known as the *standard set* and its universality has been shown by Boykin et al. [FOCS '99]. Our normal form has several nice properties: (i) Every circuit over this basis can easily be transformed into a normal form, and (ii) two normal form circuits perform same computation if and only if both circuits are identical. We also show that the number of unitary operations that can be represented by a circuit over this basis that contains at most n T-gates is exactly $192 \cdot (3 \cdot 2^n - 2)$.

Keywords: clifford group, representation of universal set, normal form

1 Introduction

Quantum computing is a very active area of research because of its ability to efficiently solve problems for which no efficient classical algorithms are known. For example, it is possible for a quantum computer to solve integer factorization in polynomial time with Shor's algorithms [7]. However, it is not yet known whether quantum computers are strictly more powerful than classical computers.

Quantum algorithms are realized by a quantum circuit consisting of basic gates corresponding to unitary matrices. In other words, the design of quantum algorithms can be seen as a decomposition of a unitary matrix into a product of matrices chosen from a basic set. A discrete set of quantum gates is called *universal* if any unitary transformation can be approximated with an arbitrary precision by a circuit involving those gates only. For example, Boykin et al. [2] proved that the basis $\{H, T, CNOT\}$ is universal, where H, T and $CNOT$ are called the Hadamard gate, the $\pi/8$ gate, and the controlled-NOT gate, respectively, and given by

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The basis $\{H, T, CNOT\}$ is called the *standard set* [6, pp. 195] and plays a fundamental role in the theory of quantum computing as the classical universal set $\{AND, NOT\}$ plays in the theory of classical computing. Note that any 2×2 unitary matrix can be decomposed with given precision as a product of H and T.

The Solovey-Kitaev theorem (see [4] or [6, Appendix 3]) says that polynomial size quantum circuits over this standard set can solve all the problems in **BQP**, where **BQP** is the class of problems that can be solved efficiently by quantum computers.

The situation is dramatically changed if we replace the T-gate by the T^2-gate in this basis. The gate that performs the unitary operation $P = T^2$ is known as the Phase gate. Quantum circuits over the basis $\{H, P, CNOT\}$ is usually called *stabilizer circuits* or *clifford circuits*. The Gottesman-Knill theorem says that circuits over this basis $\{H, P, CNOT\}$ are not more powerful than classical computers (see e.g., [6, Chap. 10.5.4]). A stronger limitation of clifford circuits has also been derived [1, 3]. Recently, Buhrman et al. [3] showed that every Boolean function that can be computed by a clifford circuit is written as the parity of a subset of input variables or its negation.

These give an insight that the T-gate is the root of the power of quantum computing. It may be natural to expect that the research on the effect of the T-gate may lead to better understanding of why a quantum computer can efficiently compute some hard problems.

Throughout this paper, we concentrate on *one qubit* circuits over the standard set, i.e., $\{H, T\}$ and analyze the properties of them. It seems difficult to give an efficient representation for a given unitary matrix with elements of such a discrete universal set, because a relation between a quantum circuit and the corresponding unitary matrix is not clear. However, if a good representation is found, it will be useful for designing an efficient quantum circuit. In this paper, we give such a representation named *normal form*. We also show that the number of unitary operations that can be represented by a circuit over this basis that contains at most n T-gates is exactly $192 \cdot (3 \cdot 2^n - 2)$.

2 The normal form

In this section, We introduce a representation named *normal form* for one qubit circuits over the universal basis $\{H, T\}$.

Let $\mathcal{C}_1$ be the set of 2×2 unitary matrices that can be represented by a circuit over the basis $\{H, P\}$. The set $\mathcal{C}_1$ forms a group known as *Clifford group* and has order 192. As usual, a circuit is represented by a string

*matsumoto@ja4.cs.gunma-u.ac.jp
†amano@cs.gunma-u.ac.jp

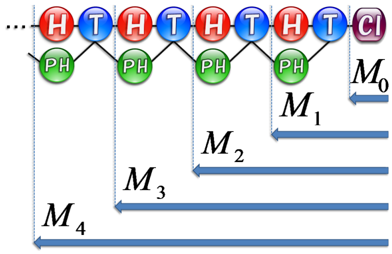

Figure 1: The normal form

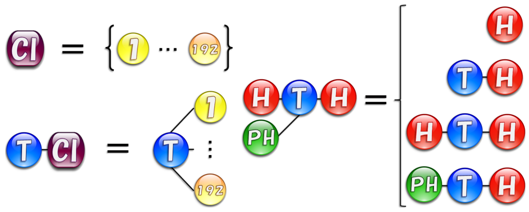

Figure 2: (Left) Cl in Figure 1 denotes the set of shortest circuits over $\{H, P\}$ for each matrix in $\mathcal{C}_1$, these are denoted by $1 \sim 192$ $(= |\mathcal{C}_1|)$. (Right) A normal form circuit is corresponding to a path from an arbitrary chosen gate to one of the rightmost gates in Figure 1.

consisting of symbols each of which represents a gate. Our normal form is defined recursively as follows (By convention, when we draw a circuit, the input is on the right side and the computation proceeds from right to left) .

(a) For each $D \in \mathcal{C}_1$, a shortest circuit over $\{H, P\}$ that represents D is a normal form (we break ties arbitrarily).

(b) If C is a normal form whose leftmost (closest to the output) gate is not T, then each of TC, HTC, and $PHTC$ is a normal form.

For example, if D is a shortest circuit over $\{H, P\}$ representing an element of $\mathcal{C}_1$, then D, TD and $PHTHTD$ are normal form whereas $THPHD$ and TTD are not. Equivalently, a normal form circuit is of the form $W_n T W_{n-1} T \cdots T W_1 T W_0$ for some $n \geq 0$ where $W_n \in \{I, H, PH\}$, $W_i \in \{H, PH\}$ for $i = 1, \ldots, n-1$, W_0 is a shortest circuit over $\{H, P\}$ that represents the corresponding element of $\mathcal{C}_1$, and I is the 2×2 identity matrix (see Figures 1 and 2). The set $\mathbf{M}_n$ in Figure 1 is defined as the set of all matrices that can be represented by a circuit over $\{H, P, T\}$ that contains at most n T-gates. Note that $\mathbf{M}_0 = \mathcal{C}_1$.

Our normal form representation is very powerful and appealing, because it has nice properties as follows:

(1) a normal form circuit has high regularity,

(2) every one qubit circuit over $\{H, P, T\}$ can easily be transformed into an equivalent normal form circuit,

(3) two normal form circuits represents same matrix if and only if both circuits are identical (comparison can be made as a string).

(3) is a surprising property. This enables us to decide whether two normal form circuits perform same computation without calculating the matrix product.

Remark 1 *In this paper, we concentrate on circuits over the basis $\{H, P, T\}$. However, we can also define a normal form for circuits over other bases. For example, for circuits over the basis $\{R, P, T\}$, where $R = P^2 H$, we can show that if we replace H with R in the definition of our normal form, then the modified normal form satisfies all the above properties.*

Our main result can be stated as follows.

Theorem 1 *Let f be the map from the set of all normal form circuits to the group generated by two matrices H and T defined by $f(C) = U$, where C is a normal form circuit and U is the corresponding matrix. Then f is a bijection.*

Theorem 1 can also be used to estimate the number of 2×2 unitary matrices represented by a circuit over $\{H, P, T\}$ with at most n T-gates.

Corollary 2 *For all nonnegative integers n, $|\mathbf{M_n}| = |\mathcal{C}_1| \cdot (3 \cdot 2^n - 2) = 192 \cdot (3 \cdot 2^n - 2)$.*

Note that the number becomes $24 \cdot (3 \cdot 2^n - 2)$ when we identify two operations that are the same up to a global phase.

The proofs are omitted in this version due to space limitations. The details appear in a full version of the paper [5].

References

[1] S. Aaronson, D. Gottesman. Improved Simulation of Stabilizer Circuits. Physical Review A, 70:052328, 2004.

[2] P. O. Boykin, T. Mor, M. Pulver, V. P. Roychowdhury, F. Vatan. On Universal and Fault-Tolerant Quantum Computing: A Novel Basis and a New Constructive Proof of Universality for Shor's Basis. *Proc. 40th FOCS*, pages 486–494, 1999.

[3] H. Buhrman, R. Cleve, M. Laurent, N. Linden, A. Schrijver and F. Unger. New Limits on Fault-Tolerant Quantum Computation. *Proc. 47th FOCS*, pages 411–419, 2006.

[4] C. M. Dawson, M. A. Nielsen, The Solovey-Kitaev Algorithm. *Quantum Inf. Comput.*, Vol. 6, pages 81–95, 2006. also quant-ph/0505030, 2005.

[5] K. Matsumoto, K. Amano, Representation of Quantum Circuits with Clifford and $\pi/8$ Gates. quant-ph/0806.3834, 2008.

[6] M. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge Univ. Press, 2000.

[7] P. Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proc. 35th FOCS*, pages 56–65, 1994.