Constant-Depth Quantum Circuits with Gates for Addition

Yasuhiro Takahashi[1] * Yasuhito Kawano[1] † Masahiro Kitagawa[2] ‡

[1] *NTT Communication Science Laboratories, NTT Corporation.*
3-1 Morinosato-wakamiya, Atsugi, Kanagawa 243-0198, Japan.
[2] *Graduate School of Engineering Science, Osaka University.*
1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan.

Abstract. We investigate a class $\mathrm{QNC}^0(\mathrm{ADD})$ that is QNC^0 with gates for addition of two binary numbers, where QNC^0 is a class consisting of quantum operations computed by constant-depth quantum circuits. We show that $\mathrm{QNC}^0(\mathrm{ADD}) = \mathrm{QAC}^0(\mathrm{PAR}) = \mathrm{QAC}^0(\mathrm{MUL})$, where $\mathrm{QAC}^0(\mathrm{PAR})$ and $\mathrm{QAC}^0(\mathrm{MUL})$ are QAC^0 with gates for parity and multiplication respectively, and where QAC^0 is QNC^0 with Toffoli gates of arbitrary fan-in. In the classical setting, similar relationships do not hold. These relationships suggest that $\mathrm{QNC}^0 \subsetneq \mathrm{QNC}^0(\mathrm{ADD})$; that is, the use of gates for addition increases the computational power of constant-depth quantum circuits. To prove $\mathrm{QNC}^0 \subsetneq \mathrm{QNC}^0(\mathrm{ADD})$, we characterize it by the one-wayness of a permutation that is constructed explicitly. We conjecture that the permutation is one-way, which implies $\mathrm{QNC}^0 \subsetneq \mathrm{QNC}^0(\mathrm{ADD})$.

Keywords: constant-depth quantum circuit, elementary arithmetic operation, one-way permutation

1 Introduction

There are many studies of classical circuits for elementary arithmetic operations [8]. Regarding addition, parity, and multiplication, it can be shown that $\mathrm{AC}^0(\mathrm{ADD}) \subsetneq \mathrm{AC}^0(\mathrm{PAR}) \subsetneq \mathrm{AC}^0(\mathrm{MUL})$, where $\mathrm{AC}^0(\mathrm{ADD})$, $\mathrm{AC}^0(\mathrm{PAR})$, and $\mathrm{AC}^0(\mathrm{MUL})$ are AC^0 with gates for addition, parity, and multiplication respectively, and where AC^0 is a class consisting of functions computed by constant-depth circuits with AND and OR gates of arbitrary fan-in [2, 5, 8]. In particular, $\mathrm{NC}^0(\mathrm{ADD}) \subsetneq \mathrm{AC}^0(\mathrm{PAR}) \subsetneq \mathrm{AC}^0(\mathrm{MUL})$, where $\mathrm{NC}^0(\mathrm{ADD})$ is $\mathrm{AC}^0(\mathrm{ADD})$ excluding gates of arbitrary fan-in. These relationships suggest that the use of gates for addition does not increase the computational power of constant-depth classical circuits so much.

There are some studies of quantum circuits for elementary arithmetic operations [1, 3, 6, 7]. However, we do not know whether the relationships corresponding to the above classical ones hold; that is, the use of gates for addition increases the computational power of constant-depth quantum circuits. We investigate a class $\mathrm{QNC}^0(\mathrm{ADD})$ consisting of quantum operations computed by constant-depth quantum circuits having gates for addition of two binary numbers. We show that $\mathrm{QNC}^0(\mathrm{ADD}) = \mathrm{QAC}^0(\mathrm{PAR}) = \mathrm{QAC}^0(\mathrm{MUL})$, where $\mathrm{QAC}^0(\mathrm{PAR})$ and $\mathrm{QAC}^0(\mathrm{MUL})$ are QAC^0 with gates for parity and multiplication respectively, and where QAC^0 is QNC^0 with Toffoli gates of arbitrary fan-in. The relationships we show suggest that $\mathrm{QNC}^0 \subsetneq \mathrm{QNC}^0(\mathrm{ADD})$; that is, the use of gates for addition increases the computational power of constant-depth quantum circuts. To prove $\mathrm{QNC}^0 \subsetneq \mathrm{QNC}^0(\mathrm{ADD})$, we provide an explicit construction of a permutation that can be computed in QNC^0, whose inverse is as hard to compute as addition. And, we show the equivalence between the one-wayness of the permutation and $\mathrm{QNC}^0 \subsetneq \mathrm{QNC}^0(\mathrm{ADD})$. We conjecture that the permutation is one-way, which implies $\mathrm{QNC}^0 \subsetneq \mathrm{QNC}^0(\mathrm{ADD})$.

2 Preliminaries

A quantum circuit consists of arbitrary single-qubit unitary gates and CNOT gates. The size of the circuit is defined as the total number of gates. The depth of the circuit is defined as follows. Input qubits are considered to have depth 0. For each gate G, the depth of G is equal to 1 plus the maximal depth of a gate that G depends on. The depth of the circuit is equal to the maximal depth of a gate.

The following classes are dealt with in this paper.

- NC^0 consists of functions computed by families of classical circuits of AND, OR, and NOT gates with constant-depth and size polynomial in n, where n is the size of the input, and where the AND and OR gates have just two inputs.
- AC^0 is like NC^0, where we allow AND and OR gates of arbitrary fan-in.
- QNC^0 consists of quantum operations computed by families of quantum circuits of single-qubit unitary gates and CNOT gates with constant-depth and size polynomial in n, where n is the size of the input.
- QAC^0 is like QNC^0, where we allow Toffoli gates of arbitrary fan-in.

As usual, we do not allow fanout operation in QNC^0 and QAC^0, though we allow it in NC^0 and AC^0. Note that theorems in the following does not depend on whether we allow fanout operation in NC^0 and AC^0. For

*takahasi@theory.brl.ntt.co.jp
†kawano@theory.brl.ntt.co.jp
‡kitagawa@ee.es.osaka-u.ac.jp

a class C and a family of operations X, C(X) represents a class C with gates for X.

In the following, tensor products of quantum states are represented as $\bigotimes_{k=0}^{n-1} |x_k\rangle$ or $|x_0\rangle \cdots |x_{n-1}\rangle$. $\oplus$ denotes addition modulo 2, and $\bigoplus_{k=0}^{n-1} x_k$ denotes $(\sum_{k=0}^{n-1} x_k)$ mod 2. $\mathbb{N}$ denotes the set of natural numbers.

We define the quantum parity operation as follows.

Definition 1 *An* n-ary quantum parity operation par_n *on* n *source qubits* $|s_k\rangle$ *and target bit* $|t\rangle$ *performs*

$$|t\rangle \bigotimes_{k=0}^{n-1} |s_k\rangle \to |t \oplus \bigoplus_{k=0}^{n-1} s_k\rangle \bigotimes_{k=0}^{n-1} |s_k\rangle,$$

for computational basis states and the behavior for superposition states is defined by linearity. We define the family of quantum operations PAR *as* $\{\mathrm{par}_n\}_{n\in\mathbb{N}}$.

3 Addition, Parity, and Multiplication

Definition 2 *A* $2n{+}1$-ary quantum addition operation add_n *performs*

$$\bigotimes_{k=0}^{n-1} |a_k\rangle \bigotimes_{k=0}^{n-1} |b_k\rangle |0\rangle \to \bigotimes_{k=0}^{n-1} |a_k\rangle \bigotimes_{k=0}^{n} |s_k\rangle,$$

for computational basis states $a = a_{n-1} \cdots a_0$ *and* $b = b_{n-1} \cdots b_0$, *where* $s_n \cdots s_0$ *is the binary representation of* $a + b$. *The behavior for superposition states is defined by linearity. We define the family of quantum operations* ADD *as* $\{\mathrm{add}_n\}_{n\in\mathbb{N}}$.

Definition 3 *A* $4n$-ary quantum multiplication operation mul_n *performs*

$$\bigotimes_{k=0}^{n-1} |a_k\rangle \bigotimes_{k=0}^{n-1} |b_k\rangle \bigotimes_{k=0}^{2n-1} |0\rangle \to \bigotimes_{k=0}^{n-1} |a_k\rangle \bigotimes_{k=0}^{n-1} |b_k\rangle \bigotimes_{k=0}^{2n-1} |s_k\rangle,$$

for computational basis states $a = a_{n-1} \cdots a_0$ *and* $b = b_{n-1} \cdots b_0$, *where* $s_{2n-1} \cdots s_0$ *is the binary representation of* $a \times b$. *The behavior for superposition states is defined by linearity. We define the family of quantum operations* MUL *as* $\{\mathrm{mul}_n\}_{n\in\mathbb{N}}$.

We show the following relationships.

Theorem 4 $\mathrm{QNC}^0(\mathrm{ADD})$=$\mathrm{QAC}^0(\mathrm{PAR})$=$\mathrm{QAC}^0(\mathrm{MUL})$.

In the classical setting, the theorem corresponding to Theorem 4 does not hold, where we regard quantum operations as the classical counterparts of them.

Theorem 5 $\mathrm{NC}^0(\mathrm{ADD}) \subsetneq \mathrm{AC}^0(\mathrm{PAR}) \subsetneq \mathrm{AC}^0(\mathrm{MUL})$.

4 Separability and One-Way Permutations

We define a permutation and its one-wayness as follows. We regard a function as a quantum operation by considering its reversible version.

Definition 6 *Let* f_n *be a function such that* $f_n : \{0,1\}^n \to \{0,1\}^n$. *A family of functions* $\{f_n\}_{n\in\mathbb{N}}$ *is called a* permutation *if* f_n *is one-to-one and for some strictly increasing function* $a : \mathbb{N} \to \mathbb{N}$, $\bigcup_{n\in\mathbb{N}} \mathrm{dom}(f_n) = \bigcup_{n\in\mathbb{N}} \{0,1\}^{a(n)}$, *where* $\mathrm{dom}(f_n)$ *is the domain of* f_n.

Definition 7 *A permutation* $\{f_n\}_{n\in\mathbb{N}}$ *is called* one-way in QNC^0 *if* $\{f_n\}_{n\in\mathbb{N}}$ *is in* QNC^0 *and* $\{f_n^{-1}\}_{n\in\mathbb{N}}$ *is not in* QNC^0.

We define a strictly increasing function $a(n) = 2n + 2$ and a family of functions $\{f_n\}_{n\in\mathbb{N}}$ such that $f_n : \{0,1\}^n \to \{0,1\}^n$ as follows. This construction is based on the construction of the one-way permutation in [4].

- $f_{2n+2}(x_0, \ldots, x_{2n+1}) = (y_0, \ldots, y_{2n+1})$, where
  - · $y_i = x_i$ for $0 \le i \le n$,
  - · $y_{n+1} = x_{n+1} \oplus x_1 \oplus x_0$,
  - · $y_i = x_i \oplus x_{i-n} \oplus (x_{i-1} \oplus x_{i-n-1}) x_{i-n-1}$ for $n + 2 \le i \le 2n$,
  - · $y_{2n+1} = x_{2n+1} \oplus (x_{2n} \oplus x_n) x_n$.

We show the following equivalence.

Theorem 8 *The following statements are equivalent.*

- $\{f_n\}_{n\in\mathbb{N}}$ *is one-way in* QNC^0.
- $\mathrm{QNC}^0 \subsetneq \mathrm{QNC}^0(\mathrm{ADD})$.

Conjecture 9 $\{f_n\}_{n\in\mathbb{N}}$ *is one-way in* QNC^0.

References

[1] T. Draper. Addition on a quantum computer. quant-ph/0008033, 2000.

[2] M. Furst, J. B. Saxe, and M. Sipser. Parity, circuits, and the polynomial hierarchy. *Mathematical Systems Theory* 17, pp.13–27, 1984.

[3] F. Green, S. Homer, C. Moore, and C. Polett. Counting, fanout, and the complexity of quantum ACC. *Quantum Information and Computation* 2, pp.35–65, 2002.

[4] J. Håstad. One-Way Permutations in NC^0. *Information Processing Letters* 26, pp.153–155, 1987.

[5] R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. of the 19th ACM STOC*, pp. 77–82, 1987.

[6] R. Špalek. Quantum circuits with unbounded fan-out. quant-ph/0208043, 2002.

[7] V. Vedral, A. Barenco, and A. Ekert. Quantum Networks for Elementary Arithmetic Operations. *Physical Review* A 54, pp. 147–153, 1996.

[8] H. Vollmer. *Introduction to Circuit Complexity.* Springer, 1999.