A Measurement-Based Form of the Out-of-Place Quantum Carry Lookhead Adder

A. Trisetyarso1), R. Van Meter1), K. M. Itoh2)

1)Department of Applied Physics and Physico-Informatics, Keio University, Japan

2)Yagami Campus,3-14-1Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa-ken 223-8522, Japan

Abstract

We present the design of a quantum carry-lookahead adder using measurement-based quantum computation. The quantum carry-lookahead adder (QCLA) is faster than a quantum ripple-carry adder; QCLA has logarithmic depth while ripple adders have linear depth. Our design is evaluated in terms of number of time steps, number of measurements, the total number of qubits used and the number of successful clustering operations required.

Keyword : Quantum Carry-Lookahead Adder, Cluster-State Computation

Measurement-based quantum computation (MBQC) is a new paradigm for implementing quantum algorithms using a quantum cluster state [1][2][3]. MBQC is attractive because cluster states are considered to be easy to create on systems ranging from the polarization state of photons [4] to charge qubits. Quantum information propagation in a cluster is driven by the pattern of measurement bases, regardless of the measurement outcomes [1][2]. A cluster is in the form of

$$\left|\phi_N\right\rangle = \frac{1}{2^N} \otimes_{a=1}^{N} \left(\left|0\right\rangle_a \sigma_v^{a+1} + \left|1\right\rangle_a\right) \tag{1}$$

Where v can be x, y, or z depending on the choice of interaction Hamiltonian between neighbors [4] and with the convention $\sigma_{\upsilon}^{N+1} = 1$. In general, the cluster state should obey the quantum correlation equation

$$\sigma_i^a \otimes \sigma_j^b \left|\phi_{\{k\}}\right\rangle_c = \left(-1^{k_a}\right)\left|\phi_{\{k\}}\right\rangle_c \tag{2}$$

$i \neq j = 0, x, y, z$ and $k_a = \{0,1\}$ where the upper index (a) represents a cluster site in the lattice and (b) is its neighbor site. The binary parameters k_a are a set of binary parameters specifying the cluster state.

We consider a two-dimensional rectangular lattice with Manhattan geometry. Employing quantum correlations for quantum computation, as stated in Raussendorf's first theorem in [3], quantum gates can be simulated by measuring lattice qubits in a particular basis. All gates in the Clifford group, including CNOT, can be performed in one step time via a large number of concurrent measurements. Remarkably, because both wires and SWAP gates are in the Clifford group, MBQC supports long-distance gates in a single time step. The Toffoli Phase gate can be executed in two time steps, where the measurement basis for the second step is adapted depending on previous measurement outcomes. For many circuits, this adaptive measurement process results in circuit depths on MBQC that are the same as the abstract circuit definition. Those benefits can be seen as a potential resource to attack complex problems such as the quantum carry-lookahead adder.

Addition is a critical subroutine for algorithms such as Shor's algorithm for factoring large numbers [5]. Addition can be executed in many ways, with its performance being primarily dependent on carry propagation. The simplest method is ripple-carry addition, which has depth of $O_{(n)}$ [6]. In a ripple-carry adder, carry information is propagated from the low-order qubits to the high order qubits one step at a time.

Raussendorf et al. mapped the VBE ripple-carry adder to MBQC [3][6]. However, a ripple-carry adder does not take good advantage of the strengths of MBQC. By unifying the Quantum Carry-Lookahead Adder (QCLA) with MBQC, we have designed a much faster circuit.

The quantum carry-lookahead adder is potentially more efficient than a quantum ripple-carry adder since its depth is O (log $_n$) [7]. A carry lookahead adder uses three phases, the "Generate", "Propagate", and "Kill" networks, each of which progressively doubles the length of its span in each time step. In practice, the networks are somewhat redundant, and Draper et al. defined their circuit using only the P, C and G networks to calculate the final carry. Unfortunately, QCLA requires long-distance gates. The out-of-place form of the QCLA performs the unitary transformation :

$| a, b, 0\rangle \rightarrow | a, b, a+b\rangle \rightarrow$ where $| a\rangle \rightarrow | b\rangle \rightarrow$ and $| a+b\rangle$ are n - qubit registers.

Our design for a 10-bit form of out-of-place QCLA on MBQC is shown in Figure1. The input qubits are on the left (top in the rotated figure) and output states are on the right. The propagation of one qubits are spaced with a pitch of four lattice sites. Each large box outlines one round in the P,G, or C networks. The circuit is presented in unoptimized form for clarity.

In our circuit, the depth is reduced to $14\times(\lfloor \log_2(n)\rfloor + \lfloor \log_2(n/3)\rfloor + 5)$ compared to $\approx O(n)$ for the ripple-carry. However, this circuit costs more in physical resources, $\approx 395n + 237\times\lfloor \log(n)\rfloor$ compared to $\approx 304n$ for the ripple carry.

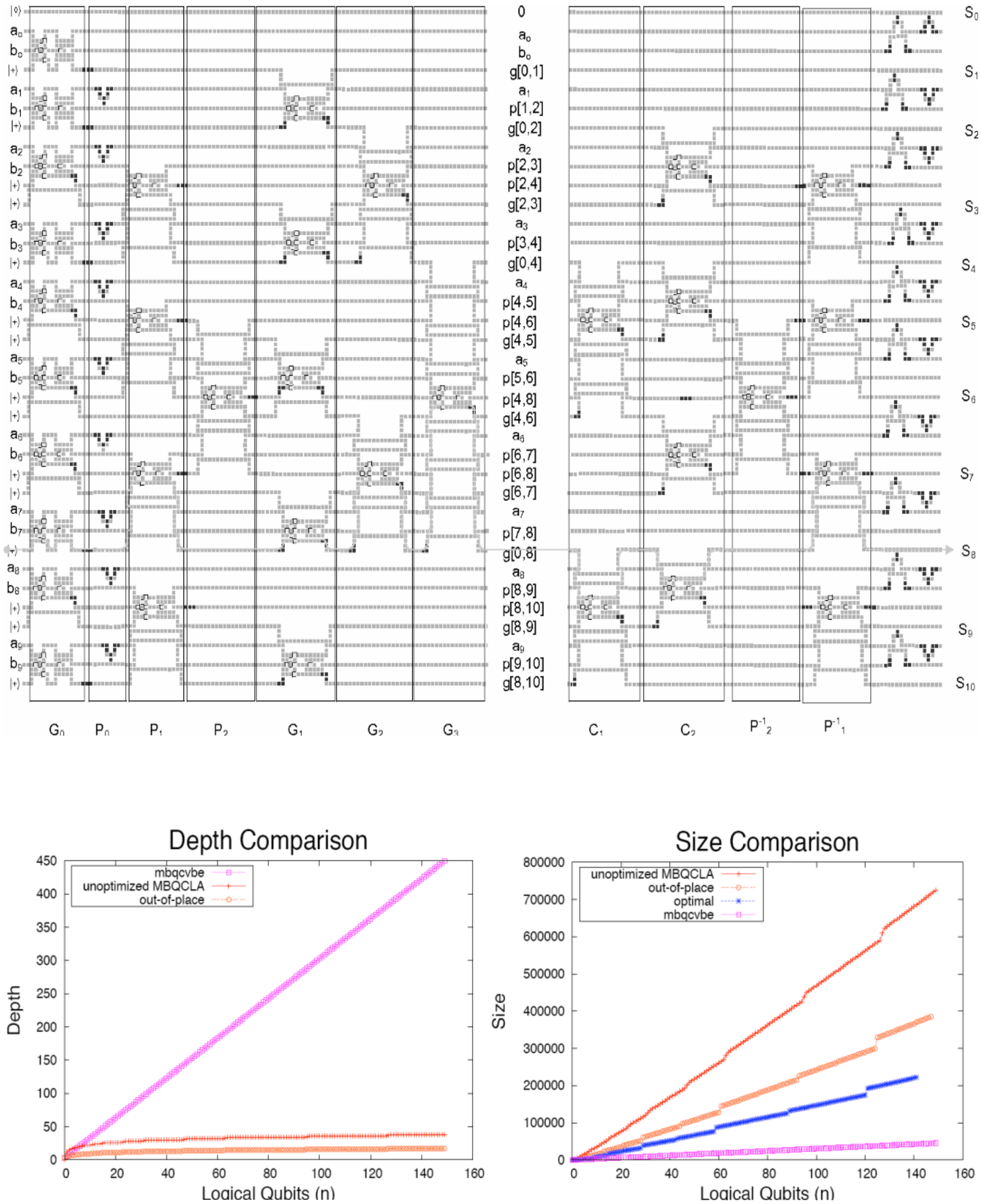

Figure 1 MBQC QCLA circuit

Preferences

[1] R.Raussendorf and H.J. Briegel. A One-Way Quantum Computer. *Phys. Rev. Lett*. 86, 5188 (2001).

[2] H.J. Briegel and R. Raussendorf. Persistent Entanglement in Arrays of Interacting Particles. *Phys. Rev. Lett*. 86, 910 (2001).

[3] Robert Raussendorf, aniel E. Browne, and Hans J. Briegel. Measurement-Based Quantum Computation on Cluster States. *Phys. Rev.* A68, 022312 (2003).

[4] P.Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger. *Nature (London) 434*,176 (2005).

[5] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Comp*, 26(5):1484-1509, 1997.

[6] Vlatko Vedral, Adriano Barenco, and Artur Ekert. Quantum networks for elementary arithmetic operations. *Phys. Rev.* A54, 147 (1996).

[7] T. Draper, S. Kutin, E. Rains, and K. Svore. A Logarithmic-Depth Quantum Carry-Lookahead Adder. *J. on. QIC* 6, 4-5, 351-369 (2006).