A 2D Nearest-Neighbor Quantum Architecture for Factoring

Paul Pham
University of Washington
Quantum Theory Group
Box 352350, Seattle, WA 98195, USA,
ppham@cs.washington.edu,
`http://www.cs.washington.edu/homes/ppham/`

Krysta M. Svore
Microsoft Research
Quantum Architectures and Computation Group
One Microsoft Way, Redmond, WA 98052, USA
ksvore@microsoft.com,
`http://research.microsoft.com/en-us/people/ksvore/`

December 13, 2012

This document responds to comments by Referee 2, which were received on November 30, 2012. These comments are quoted and responded to below.

1 General Comments

> The paper "A 2D Nearest-Neighbor Quantum Architecture for Factoring", by Pham and Svore, contains new ideas and represents a step forward in our understanding of how to implement arithmetic on a quantum computer. The authors do two things that separate their paper from previous analyses of Shor's algorithm: they consider a 2D network, and they choose to optimize depth rather than width. While it is still too early to say which physical constraints on quantum computers will be most restrictive, the authors explore an important new part of the space of algorithms. This paper is appropriate for publication in QIC.
>
> There are a few issues that should be addressed before publication.

1.1 The introduction does not state the main result

The introduction does not state the main result. At the very least, there should be a statement of the asymptotic behavior of the circuit. It is even possible that most (or all) of Section 8 should be moved earlier, including figure 11. The reader should not have to read to the end to find out the punch line.

1.2 The introduction to Section 4 is confusing.

The introduction to Section 4 is confusing. Is the pair (u, v) a CSE number only when it arises from this construction? Is $u_{n-1} = 0$ a convention within the paper or part of the definition? The example in Figure 2 might suggest that $u_i = v_i = 1$ is not permitted, when in fact it is. The authors need to clarify standard definitions versus their conventions. A reference to pre-quantum literature on carry-save addition would help.

1.3 Non-unique representations of the answer

The authors imply that the final output of their exponentiation circuit is left in CSE form, which is not a unique representation of the answer. This could mess up the next step of Shor's algorithm, in which states with the same answer collapse. The authors need to either (a) explain why this is not a problem, or (b) explicitly say that they convert the answer to standard form. (Note that, at worst, this conversion can be done in log depth, so the asymptotic analysis of the algorithm is be affected.)

2 Minor comments

Some other minor comments, to be addressed at the authors' discretion:

- Page 1: "best-known" should be "best known". ("best-known" means "most famous", which is not what is intended.)

KRYSTA TODO

- Top of Section 2.1: Should be "following Van Meter and Itoh [Van Meter and Itoh (2005)]" or "following [Van Meter and Itoh (2005)]".

KRYSTA TODO

- Page 2: “where each qubit has four neighbors” is misleading since it implies a torus rather than a bounded planar region, and since the authors are about to change four to six. Simply “where there is an extra...” would suffice.

KRYSTA TODO

- Last sentence of Section 2: ”there is no known way”. Do the authors mean (a) no one has found a way, (b) there is provably no way, or (c) there is provably no way for a particular family of circuits? The at-large citation to Rosenbaum is unhelpful. One way to clarify would be to cite a specific result from Rosenbaum.

- Bottom of page 6: ”The circuit operations out-of-place and produces two garbage qubits”. No. An out-of-place circuit leaves its input intact; this circuit overwrites a_i, so it operates in place. Calling b_i and c_i ”garbage” seems not quite right, since if they were not present the circuit would not be reversible. One could design an out-of-place version, but in this case cleaning up b_i and c_i would be straightforward and there would be no garbage.

- Page 7: The phrase ”n-bit” appears twice in one sentence, once as a an adjective and once as a noun, meaning two different things. This is not technically ambiguous, but it is awkward.

KRYSTA TODO

- Page 7, before (6): The term ”signficance” has not been defined and seems not be to used elsewhere. The sentence could be rewritten.

KRYSTA TODO: I defined the term significance in Section 4, on the Carry-Save technique, but this appears to be removed in the submitted version.

- Page 7, proof of lemma 1: extraneous ”.” in ”Our”.

KRYSTA TODO

- Pages 8 and 9: The argument that $v'''_{n+2} = 0$ is convoluted, working backward from the conclusion to a true statement (and misusing the word ”implies” in the process), and contains at least one mistake. It would be cleaner to work forward. For example: since $u'_{(n)} + v'_{(n+1)} = u_{(n)} + v_{(n)} <= 2^{n+1}$, the bits $u'_n and v'_{n+1}$ cannot both be 1. But $u''_{n+1} = v'_{n+1}$ and $v''_{n+1} = u'_n v'_n$, so u''_{n+1} and v''_{n+1} cannot both be 1, and hence $v'''_{n+2} = 0$.