A quantum circuit for Shor’s factoring algorithm using $2n+2$ qubits

Yasuhiro Takahashi$^\dagger$ and Noboru Kunihiro$^\ddagger$

$^\dagger$NTT Communication Science Labs., NTT Corp.
$^\ddagger$The University of Electro-Communications

Quantum Information and Computation, Vol. 6 No. 2, pp. 184-192, 2006
Abstract

• We construct a quantum circuit for Shor’s factoring algorithm using $2n+2$ qubits
  – [Qubit-efficient] The number of qubits is less than that in any other circuit ever constructed for the algorithm
  – [Size-efficient] The size of the circuit is about half that of Beauregard’s circuit, which uses $2n+3$ qubits
Background

• Shor proposed an efficient quantum algorithm for factoring for which no efficient classical algorithm is known
• Efficient circuits for Shor’s algorithm are useful for performing the algorithm on a quantum computer

There is great interest in constructing efficient circuits for the algorithm
Circuits for Shor’s algorithm

• It suffices to construct a circuit for order-finding

\[
\begin{align*}
N & : \text{an } n \text{-bit number to be factored} \\
a & : \text{a randomly chosen number less than } N \\
U_a & : \text{a modular multiplication that maps } |x\rangle \text{ to } |ax \mod N\rangle
\end{align*}
\]
## Previous circuits for order-finding

<table>
<thead>
<tr>
<th></th>
<th>Size</th>
<th>Depth</th>
<th>Number of qubits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vedral et al. 1996</td>
<td>$O(n^3)$</td>
<td>$O(n^3)$</td>
<td>$3n+2$</td>
</tr>
<tr>
<td>Beauregard 2003</td>
<td>$O(n^3 \log n)$</td>
<td>$O(n^3)$</td>
<td>$2n+3$</td>
</tr>
<tr>
<td><strong>Our circuit</strong></td>
<td>$O(n^3 \log n)$</td>
<td>$O(n^3)$</td>
<td>$2n+2$</td>
</tr>
</tbody>
</table>
The problem

• The problem is to reduce the number of qubits used for modular multiplication.

\[ 2n+2 \text{ qubits} = 1 \text{ qubit} + 2n+1 \text{ qubits} \]
Decomposition of modular multiplication

Modular multiplication

\[ |x\rangle \xrightarrow{U_a} |ax \mod N\rangle \]

Modular product-sum

\[ |x\rangle \xrightarrow{MPS_a} |x\rangle \]
\[ |b\rangle \xrightarrow{} |ax+b \mod N\rangle \]

There are useful qubits for constructing the new circuit

Modular addition

\[ |b\rangle \xrightarrow{MA_a} |a+b \mod N\rangle \]

New circuit!
Many “idle” qubits

• There are \( n-1 \) “idle” qubits while we perform a modular addition

\[
ax + b \mod N
\]

We use these “idle” qubits as “uninitialized” ancillary qubits
Our circuit for modular addition

- For a classical number $a$, we construct a quantum circuit for modular addition that maps $|b\rangle$ to $|a + b \mod N\rangle$

\[
\begin{align*}
\begin{array}{c}
n \left\{ \begin{array}{c}
|b\rangle & \rightarrow \text{COMP}_{N-a} \rightarrow |b\rangle & \rightarrow \text{ADD}_a \rightarrow |a+b\mod N\rangle \\
|0\rangle & \rightarrow \text{SUB}_{N-a} \rightarrow |y\rangle
\end{array} \right.
\end{array}
\end{align*}
\]

\[
\begin{align*}
N \rightarrow \text{COMP}_a \rightarrow |\text{z} \oplus 1\rangle = |0\rangle
\end{align*}
\]

$y = \begin{cases} 
1 & a + b < N\\ 
0 & \text{otherwise}
\end{cases}$

$a + b \mod N = \begin{cases} 
1 & y = 1\\ 
0 & \text{otherwise}
\end{cases}$

$z = \begin{cases} 
1 & a + b \mod N < a\\ 
0 & \text{otherwise}
\end{cases}$

$a + b < N \iff a + b \mod N \geq a$

\[y = 1 \iff z = 0\]

\[y \oplus z \oplus 1 = 0\]
Our and Beauregard’s circuits

Draper’s QFT-based addition with no new ancillary qubits

\[
\begin{align*}
\text{Our circuit} & : \quad \NOT_{N-a}(b) \quad \text{ADD}_a \quad \text{or} \quad \text{SUB}_{N-a}(y) \\
& \quad \quad \quad \quad \quad a + b \mod N \\
\text{Beauregard’s circuit} & : \quad U \quad V \\
& \quad \quad \quad \quad \quad a + b - N \\
& \quad \quad \quad \quad \quad \quad \text{or} \quad a + b \mod N \\
& \quad \quad \quad \quad \quad n+1 \text{ qubits} \\
& \quad 1 \text{ qubit}
\end{align*}
\]

If we use no new ancillary qubits, the number of qubits is less than that in Beauregard’s by one
Comparison

• For a classical number $a$, we construct a quantum circuit for comparison that maps $|b\rangle|z\rangle$ to $|b\rangle|z \oplus y\rangle$, where

$$y = \begin{cases} 1 & a > b \\ 0 & \text{otherwise} \end{cases}$$

= the high bit of $a + b'$

We construct a circuit for computing only the high bit (the last carry bit) using the conventional adder.

But, the adder uses $n-1$ new ancillary qubits.
The use of “idle” qubits

• We use not \( n-1 \) new ancillary qubits but “uninitialized” ancillary qubits
• They are available in the other register!

The conventional adder

\[
\begin{align*}
|b\rangle & \rightarrow \text{HIGH BIT} \begin{array}{c} a \end{array} |b\rangle \\
|z\rangle & \rightarrow |z \oplus c_n\rangle \\
|0\rangle & \rightarrow 0 \\
\vdots & \vdots \\
|0\rangle & \rightarrow 0
\end{align*}
\]

“A modified adder

\[
\begin{align*}
|b\rangle & \rightarrow \text{HIGH BIT} \begin{array}{c} a \end{array} |b\rangle \\
|z\rangle & \rightarrow |z \oplus c_n\rangle \\
|0\rangle & \rightarrow 0 \\
\vdots & \vdots \\
|0\rangle & \rightarrow 0
\end{align*}
\]

“Idle” qubits

\[
\begin{align*}
|b\rangle & \rightarrow \text{HIGH BIT} \begin{array}{c} a \end{array} |b\rangle \\
|z\rangle & \rightarrow |z \oplus c_n\rangle \\
|0\rangle & \rightarrow 0 \\
\vdots & \vdots \\
|0\rangle & \rightarrow 0
\end{align*}
\]

Uninitialized qubits

\[
\begin{align*}
|b\rangle & \rightarrow \text{HIGH BIT} \begin{array}{c} a \end{array} |b\rangle \\
|z\rangle & \rightarrow |z \oplus c_n\rangle \\
|0\rangle & \rightarrow 0 \\
\vdots & \vdots \\
|0\rangle & \rightarrow 0
\end{align*}
\]
HIGHBIT gate

- We construct a circuit for the operation

$$|b\rangle|z\rangle|r_1 \cdots r_{n-1}\rangle \mapsto |b\rangle|z \oplus c_n\rangle|r_1 \cdots r_{n-1}\rangle$$

by modifying the conventional adder
Changes of the values

\[ |b\rangle|z\rangle|r_1r_2r_3r_4\rangle \]
\[ \rightarrow |b\rangle|z\oplus c_5\rangle|r_1r_2r_3r_4\rangle \]
Complexity analysis

- Our circuit uses $2n+2$ qubits
  - The sequential computation of the QFT uses 1 qubit
  - $|b\rangle, |z\rangle, |x\rangle$ in modular multiplication use $2n+1$ qubits

- The size of our circuit is about half that of Beauregard’s circuit
  - The number of QFT-based additions is about half that in Beauregard’s circuit
Conclusions

• We construct a quantum circuit for order-finding using $2n+2$ qubits
  – The number of qubits is less than that in any other circuit ever constructed for order-finding

• The key ingredient of the circuit is the HIGHBIT gate that uses “uninitialized” ancillary qubits