

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

Yasuhiro Takahashi[†] and Noboru Kunihiro[‡]

[†] NTT Communication Science Labs., NTT Corp.

[‡] The University of Electro-Communications

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

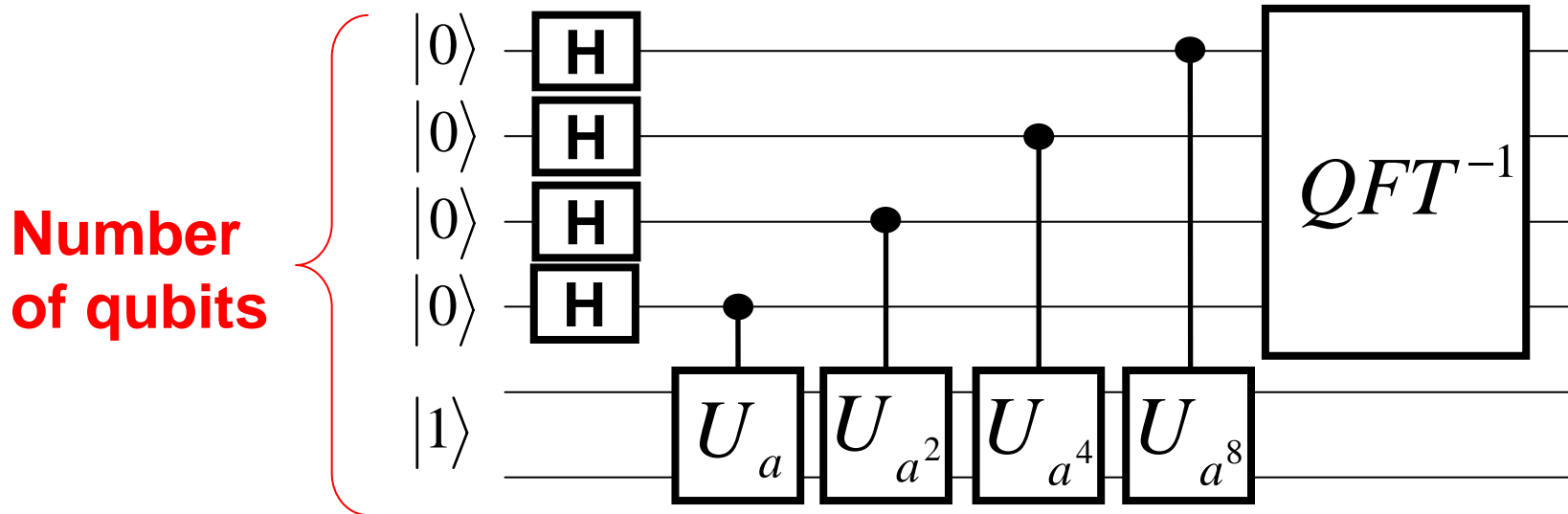
Background

- **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



N : an n -bit number to be factored

a : a randomly chosen number less than N

U_a : a modular multiplication that maps $|x\rangle$ to $|ax \bmod N\rangle$

Previous circuits for order-finding

	Size	Depth	Number of qubits
Vedral et al. 1996	$O(n^3)$	$O(n^3)$	$3n+2$
Beauregard 2003	$O(n^3 \log n)$	$O(n^3)$	$2n+3$

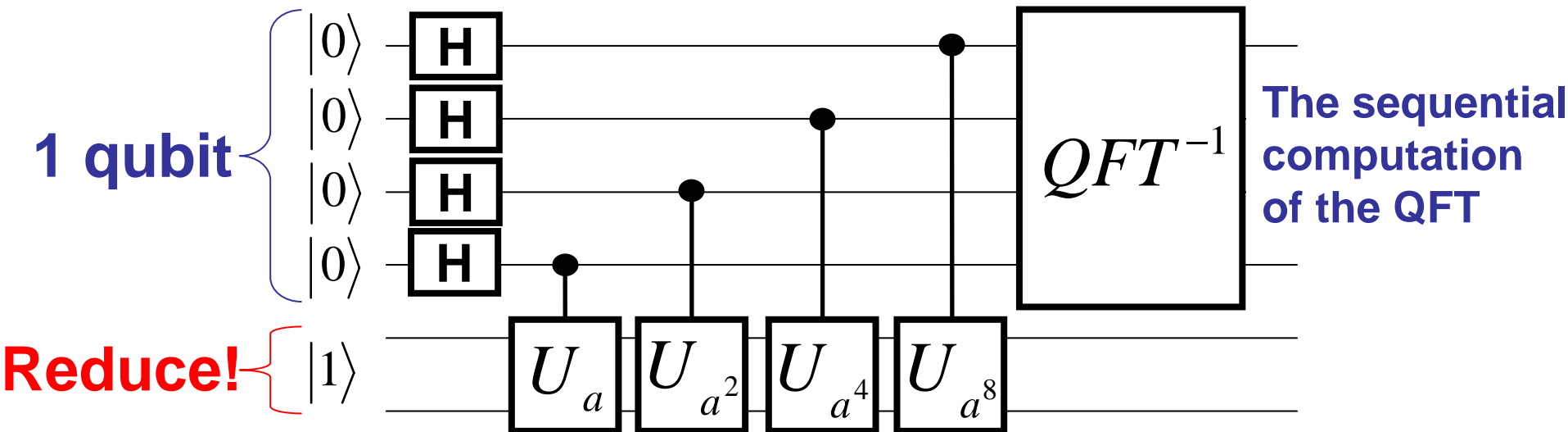
Half

1 qubit

Our circuit	$O(n^3 \log n)$	$O(n^3)$	$2n+2$
--------------------	-----------------	----------	--------

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

$$|x\rangle \text{---} \boxed{U_a} \text{---} |ax \bmod N\rangle$$



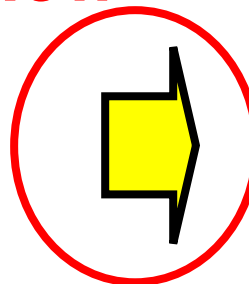
Modular product-sum

$$\begin{array}{c} |x\rangle \\ |b\rangle \end{array} \text{---} \boxed{MPS_a} \text{---} \begin{array}{c} |x\rangle \\ |ax+b \bmod N\rangle \end{array}$$

There are useful qubits
for constructing the new
circuit

Modular addition

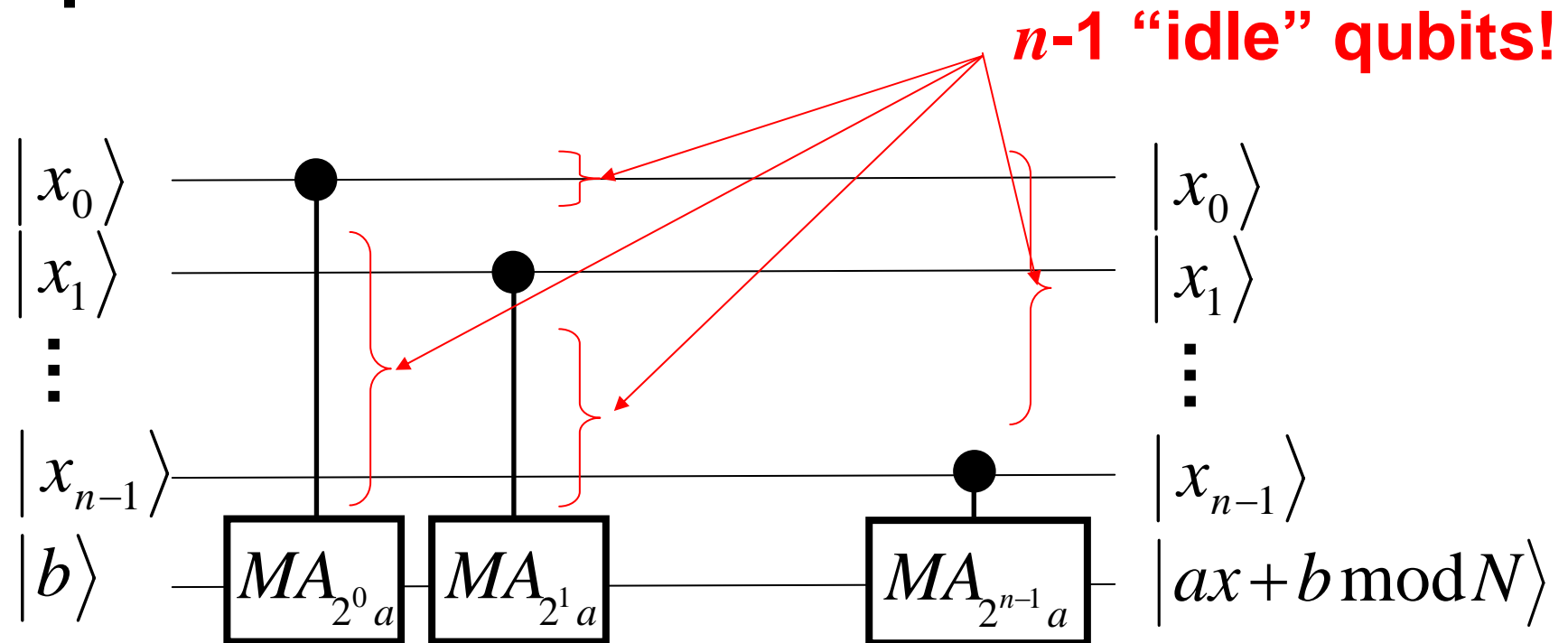
New circuit!



$$|b\rangle \text{---} \boxed{MA_a} \text{---} |a+b \bmod N\rangle$$

Many “idle” qubits

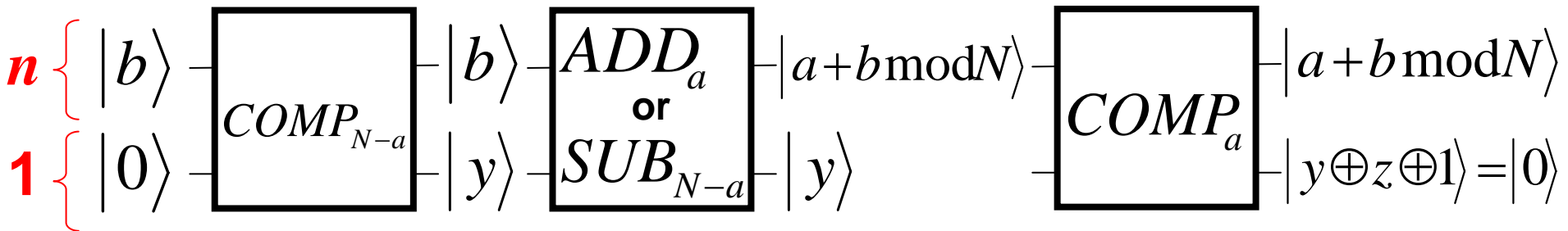
- There are $n-1$ “idle” qubits while we perform a modular addition



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 $|a + b \bmod N\rangle$



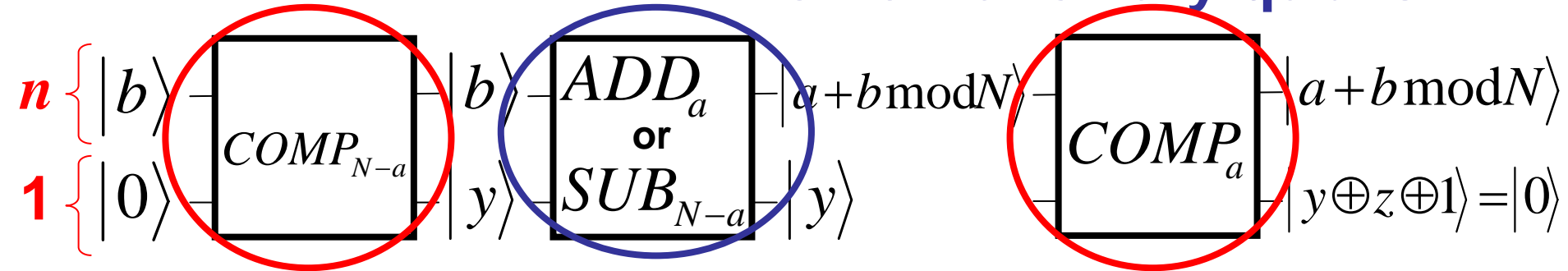
$$y = \begin{cases} 1 & a + b < N \\ 0 & \text{otherwise} \end{cases} \quad a + b \bmod N = \begin{cases} a + b & y = 1 \\ a + b - N & \text{otherwise} \end{cases} \quad z = \begin{cases} 1 & a + b \bmod N < a \\ 0 & \text{otherwise} \end{cases}$$

$$a + b < N \Leftrightarrow a + b \bmod N \geq a \quad \Rightarrow \quad y = 1 \Leftrightarrow z = 0 \quad \Rightarrow \quad y \oplus z \oplus 1 = 0$$

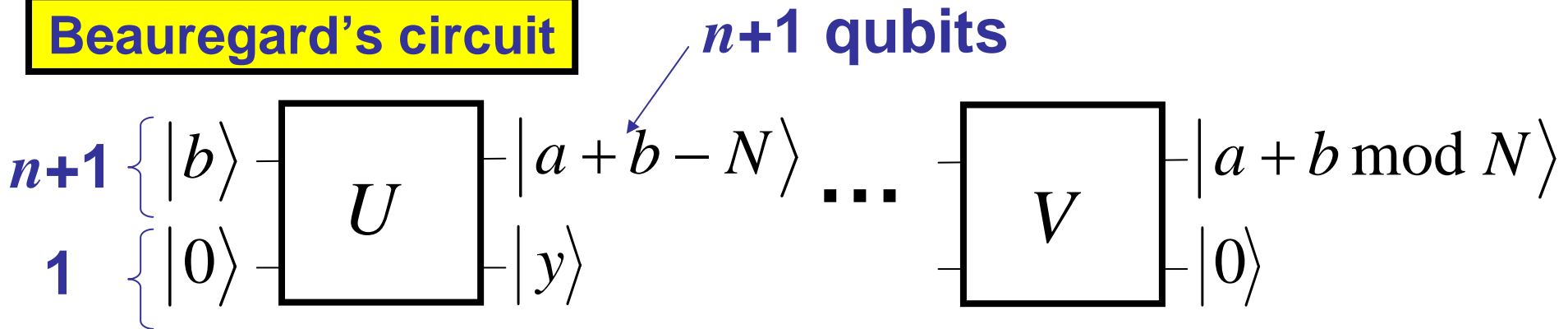
Our and Beauregard's circuits

Our circuit

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



Beauregard's circuit



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

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

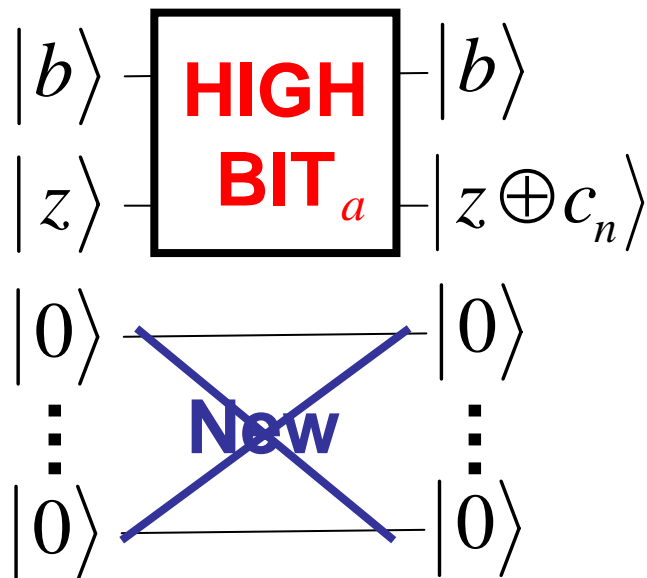
= the high bit of $a + b'$

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

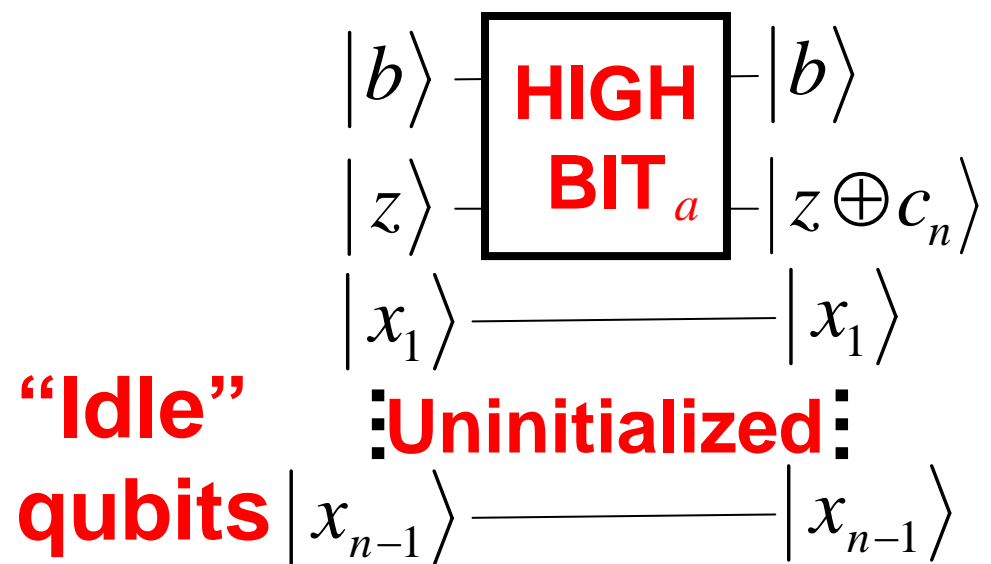
But, the adder uses $n-1$ new ancillary qubits

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



“Idle”
qubits

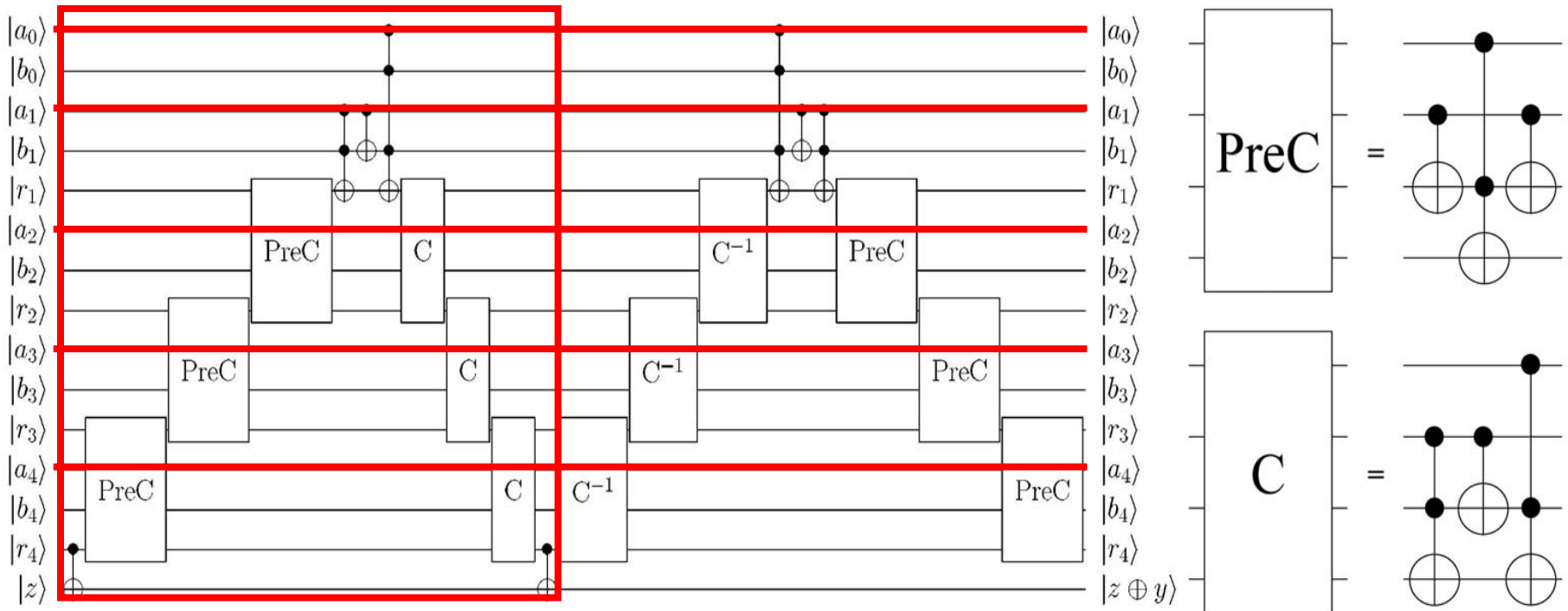
A modified adder

HIGHBIT gate

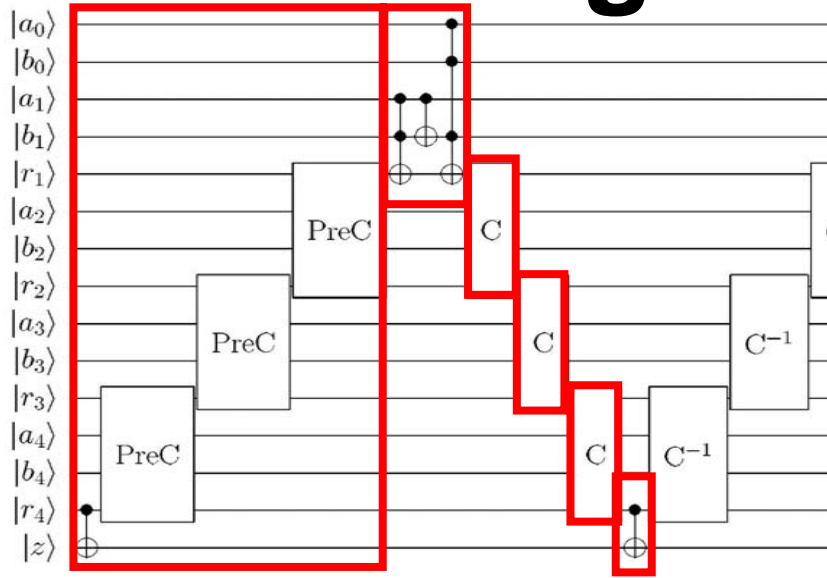
- We construct a circuit for the operation

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

by modifying the conventional adder



Changes of the values



$$|b\rangle|z\rangle|r_1r_2r_3r_4\rangle$$

$$\mapsto |b\rangle|z \oplus c_5\rangle|r_1r_2r_3r_4\rangle$$

	z	r_1	r_2	r_3	r_4
\longrightarrow	$z \oplus r_4$	r_1	$r_2 \oplus (a_2 \oplus b_2)r_1$	$r_3 \oplus (a_3 \oplus b_3)r_2$	$r_4 \oplus (a_4 \oplus b_4)r_3$
\longrightarrow	$z \oplus r_4$	$r_1 \oplus c_2$	$r_2 \oplus (a_2 \oplus b_2)r_1$	$r_3 \oplus (a_3 \oplus b_3)r_2$	$r_4 \oplus (a_4 \oplus b_4)r_3$
\longrightarrow	$z \oplus r_4$	$r_1 \oplus c_2$	$r_2 \oplus c_3$	$r_3 \oplus (a_3 \oplus b_3)r_2$	$r_4 \oplus (a_4 \oplus b_4)r_3$
\longrightarrow	$z \oplus r_4$	$r_1 \oplus c_2$	$r_2 \oplus c_3$	$r_3 \oplus c_4$	$r_4 \oplus (a_4 \oplus b_4)r_3$
\longrightarrow	$z \oplus r_4$	$r_1 \oplus c_2$	$r_2 \oplus c_3$	$r_3 \oplus c_4$	$r_4 \oplus c_5$
\longrightarrow	$z \oplus c_5$	$r_1 \oplus c_2$	$r_2 \oplus c_3$	$r_3 \oplus c_4$	$r_4 \oplus c_5$

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**