Modular Multiplier Implementation

Hao-Chien Wang

Department of Physics, National Taiwan University

March 22, 2020

Outline

Introduction

- Starting point: Paper by Archimeds Pavlidis and Dimitris Gizopoulos [1].
- Building block 1: Adder on Fourier basis by T. Draper[2].
- Building block 2: Modular adder by S. Beauregard[3].
- Building block 3: Modular multiplier by S. Beauregard[3] (will be covered by 宥頡).
- Current result: U_a using $2n+3$ qubits

All scripts are on my Github repo:
`https://github.com/fhcwcsy/qc_practice/tree/master/shor_s_algorithm`

Review: Quantum Fourier Transform

Define:

$$e(t) \equiv e^{2\pi i t}$$

$$|\phi_k(a)\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle + e\left(\frac{a}{2^k}\right)|1\rangle\right)$$

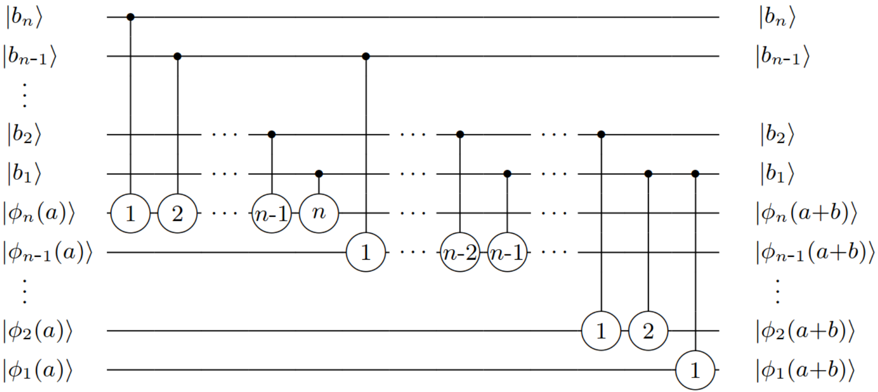
$$\frac{a}{2^k} = 0.a_k a_{k-1}\cdots a_2 a_1$$

QFT:

$$|a\rangle \xrightarrow{F_{2^n}} \frac{1}{2^{\frac{n}{2}}}\sum_{k=0}^{2^n-1} e\left(\frac{ak}{2^n}\right)|k\rangle = |\phi_n(a)\rangle \otimes \cdots \otimes |\phi_2(a)\rangle \otimes |\phi_1(a)\rangle$$

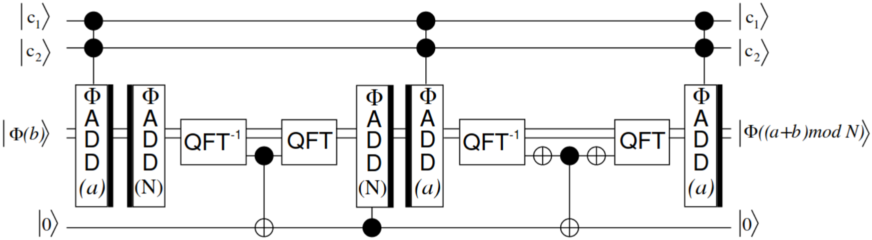
Tracing QFT

$$|\phi_n(a)\rangle \xrightarrow{Hadamard} \frac{1}{\sqrt{2}}(|0\rangle + e(0.a_0)\,|1\rangle) \tag{1}$$

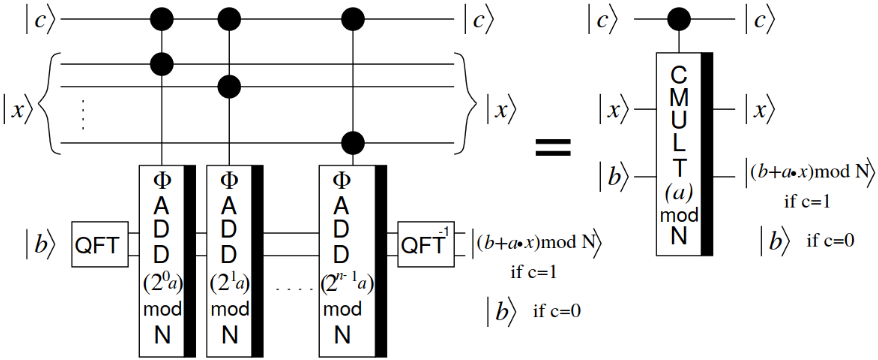

$|b_n\rangle$
$|b_{n-1}\rangle$
$|b_2\rangle$
$|b_1\rangle$
$|\phi_n(a)\rangle$
$|\phi_{n-1}(a)\rangle$
$|\phi_2(a)\rangle$
$|\phi_1(a)\rangle$
1
2
n-1
n
1
n-2
n-1
1
2
1
$|b_n\rangle$
$|b_{n-1}\rangle$
$|b_2\rangle$
$|b_1\rangle$
$|\phi_n(a+b)\rangle$
$|\phi_{n-1}(a+b)\rangle$
$|\phi_2(a+b)\rangle$
$|\phi_1(a+b)\rangle$

Draper's Adder

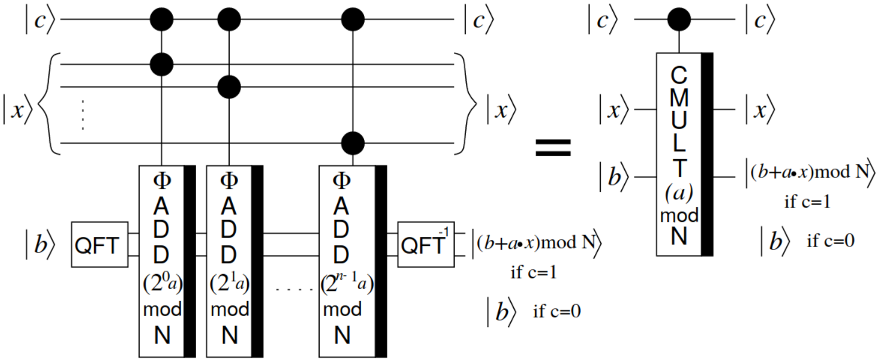
Beauregard's Modular Adder



Beauregard's Modular Multiplier



Final Gate (for now)



References

[1] Pavlidis, Archimedes, and Dimitris Gizopoulos. "Fast Quantum Modular Exponentiation Architecture for Shor's Factorization Algorithm." *arXiv preprint* arXiv:1207.0511 (2012).

[2] Draper, Thomas G. "Addition on a quantum computer." *arXiv preprint* quant-ph/0008033 (2000).

[3] Beauregard, Stephane. "Circuit for Shor's algorithm using 2n+ 3 qubits." *arXiv preprint* quant-ph/0205095 (2002).