Implementations of Quantum Adders and Quantum Modular Adders

Hao-Chien Wang

Department of Physics, National Taiwan University

March 26, 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`

Eigenvalues and Eigenvectors of U_a

$$U\left|u_s\right\rangle = e^{\frac{2\pi i s}{r}}\left|u_s\right\rangle$$

$$\left|u_s\right\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{\frac{-2\pi i s k}{r}}\left|x^k \mod N\right\rangle$$

It can be proved that

$$\frac{1}{\sqrt{r}}\sum_{t=0}^{r-1}\left|u_t\right\rangle = \left|1\right\rangle$$

Therefore, we estimate the eigenvalues to obtain $\frac{s}{r}$.

Proof: Eigenvalues and Eigenvectors

$$
\begin{aligned}
U\left|u_s\right\rangle &= U\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{\frac{-2\pi isk}{r}}\left|x^k \mod N\right\rangle \\
&= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{\frac{-2\pi isk}{r}}\left|x^{k+1} \mod N\right\rangle \\
&= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{\frac{-2\pi is(k-1)}{r}}\left|x^k \mod N\right\rangle \\
&= e^{\frac{2\pi is}{r}}\left|u_s\right\rangle
\end{aligned}
$$

Proof: Sum of Eigenvectors is $|1\rangle$

$$
\begin{aligned}
\frac{1}{\sqrt{r}}\sum_{t=0}^{r-1}|u_t\rangle &= \frac{1}{\sqrt{r}}\sum_{t=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{\frac{-2\pi itk}{r}}\left|x^k \mod N\right\rangle \\
&= \frac{1}{r}\sum_{k=0}^{r-1}\left(\sum_{t=0}^{r-1}e^{\frac{-2\pi itk}{r}}\right)\left|x^k \mod N\right\rangle \\
&= \frac{1}{r}\sum_{k=0}^{r-1}\left(\delta_{k,0}\,r\right)\left|x^k \mod N\right\rangle \\
&= |1\rangle
\end{aligned}
$$

Review: Quantum Fourier Transform

Define:

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

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

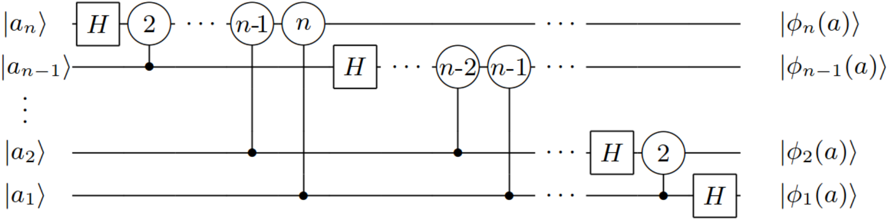
$$\frac{a}{2^k} = 0.a_k a_{k-1}\cdots a_2 a_1$$

$$R_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e\left(\frac{1}{2^k}\right) \end{pmatrix}$$

QFT:

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

QFT Circuit



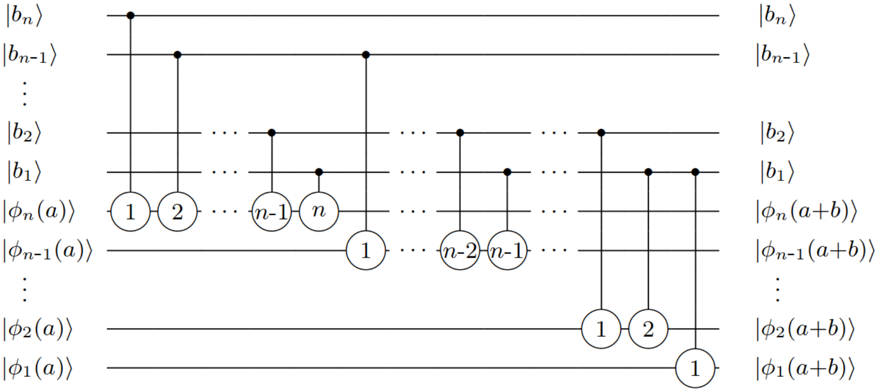
$|a_n\rangle$
$|a_{n-1}\rangle$
$|a_2\rangle$
$|a_1\rangle$
H
2
n-1
n
H
n-2
n-1
H
2
H
$|\phi_n(a)\rangle$
$|\phi_{n-1}(a)\rangle$
$|\phi_2(a)\rangle$
$|\phi_1(a)\rangle$

Tracing QFT

$$
\begin{aligned}
|a_n\rangle &\xrightarrow{Hadamard} \frac{1}{\sqrt{2}}\left(|0\rangle + e(0.a_n)\,|1\rangle\right) \\
&\xrightarrow{C_{n-1}-R_2} \frac{1}{\sqrt{2}}\left(|0\rangle + e(0.a_n a_{n-1})\,|1\rangle\right) \\
&\qquad\vdots \\
&\xrightarrow{C_1-R_n} \frac{1}{\sqrt{2}}\left(|0\rangle + e(0.a_n a_{n-1}\cdots a_1)\,|1\rangle\right) \\
&= |\phi_n(a)\rangle
\end{aligned}
$$

Draper's Fourier Adder

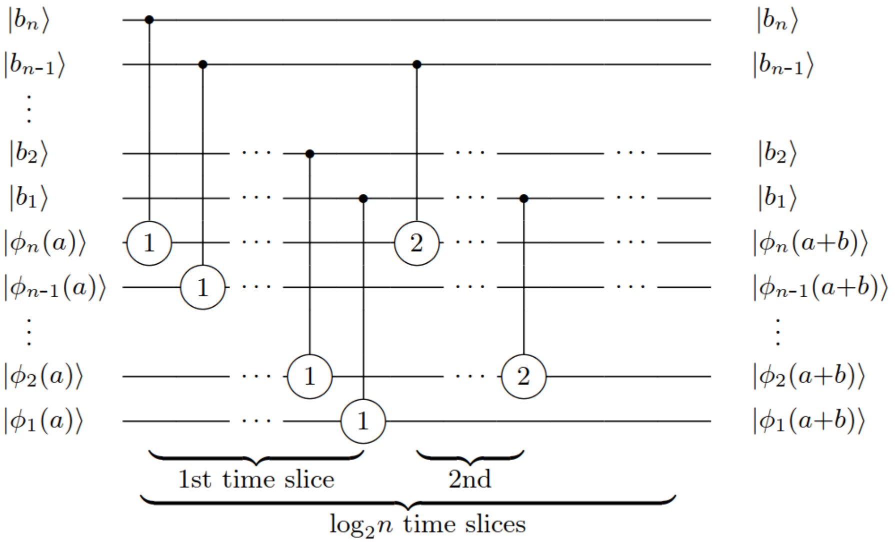
$$|\phi(a)\rangle \to |\phi(a+b)\rangle$$



Tracing Draper's Adder

$$
\begin{aligned}
|\phi_n(a)\rangle &\xrightarrow{C_{b_n}-R_1} \frac{1}{\sqrt{2}}\left(|0\rangle + \Big[e(0.a_n a_{n-1}\cdots a_1 + 0.b_n)\Big]|1\rangle\right) \\
&\xrightarrow{C_{b_{n-1}}-R_2} \frac{1}{\sqrt{2}}\left(|0\rangle + \Big[e(0.a_n a_{n-1}\cdots a_1 + 0.b_n b_{n-1})\Big]|1\rangle\right) \\
&\qquad\vdots \\
&\xrightarrow{C_{b_1}-R_n} \frac{1}{\sqrt{2}}\left(|0\rangle + \Big[e(0.a_n a_{n-1}\cdots a_1 + 0.b_n b_{n-1}\cdots b_1)\Big]|1\rangle\right) \\
&= |\phi_n(a+b)\rangle
\end{aligned}
$$

Parallel Adder



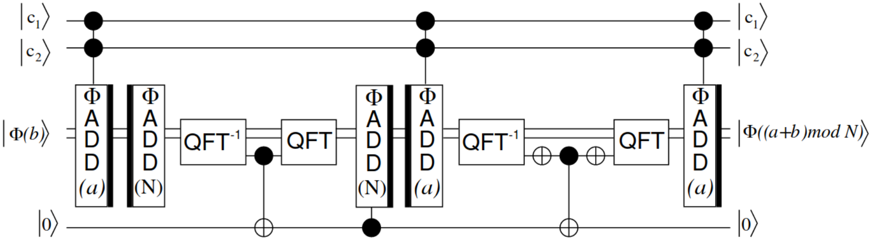
Beauregard's Modular Adder

$$\Phi ADD(a) MOD(N) |\phi(b \mod N)\rangle = |\phi(a + b \mod N)\rangle$$

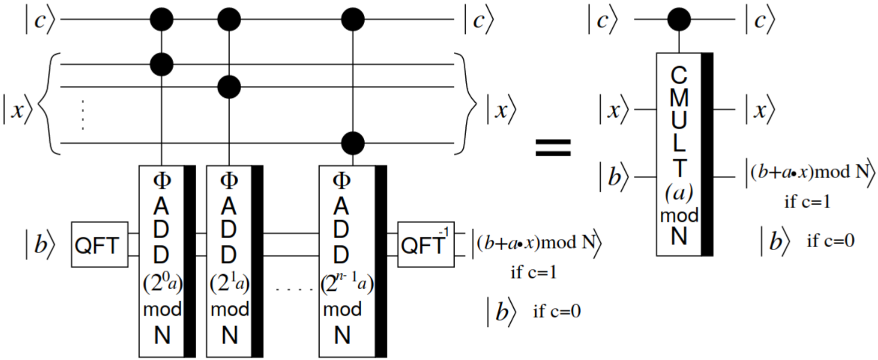
- Qubits
  - Use 2 controls (1 for $C - U_a$, 1 for building modular multipler).
  - 1 ancilla qubit (must be cleared).
  - Use one more qubit to store a to prevent overflow and detect sign (check MSB).
- Adding numbers larger than N can be reduced.
- Steps:
  1. Add a
  2. Subtract N
  3. Convert to Computational basis, check MSB. Add N back if MSB is 1.
  4. Clear the ancilla bit using

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

Beauregard's Modular Adder



Final Gate (for now)



Implementation

- Currently complete:
  - Adder
  - Modular adder
  - Modular Multiplier
- Obstacle: the circuit is too big to get the correct result using real device.

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).