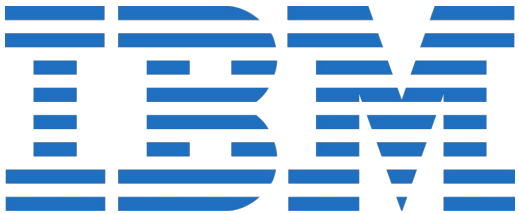
Improving Quantum Circuits of Toffoli Gates

RIPS IBM Team



Drew Gao, Xinjie He, James Woodcock

Muye “Willers” Yang (Project Manager)

Academic Mentors: Dmitri Maslov (IBM)

Jens Palsberg (UCLA)

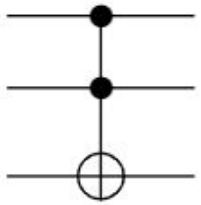
Micky Abir (UCLA)

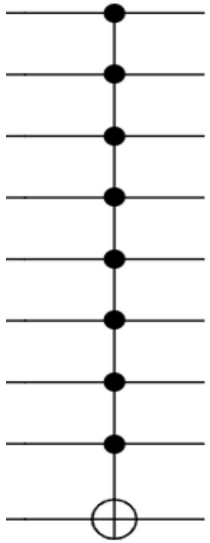
Introduction

Classical vs. Quantum Computing

Classical Computing	Quantum Computing
● Information stored as bits with a binary value ● Information manipulated by logic gates (which implement boolean functions) ● Larger functions broken down into 2, or 3 bit logic gates for implementation	● Information stored as qubits in superposition (unit vectors in C^2) ● Information manipulated by primitive quantum logic gates (which implement unitary matrices ie $U^\dagger U = UU^\dagger = I.$) ● Larger unitary operations broken down into 1 or 2 qubit quantum logic gates

Toffoli Gate(s)



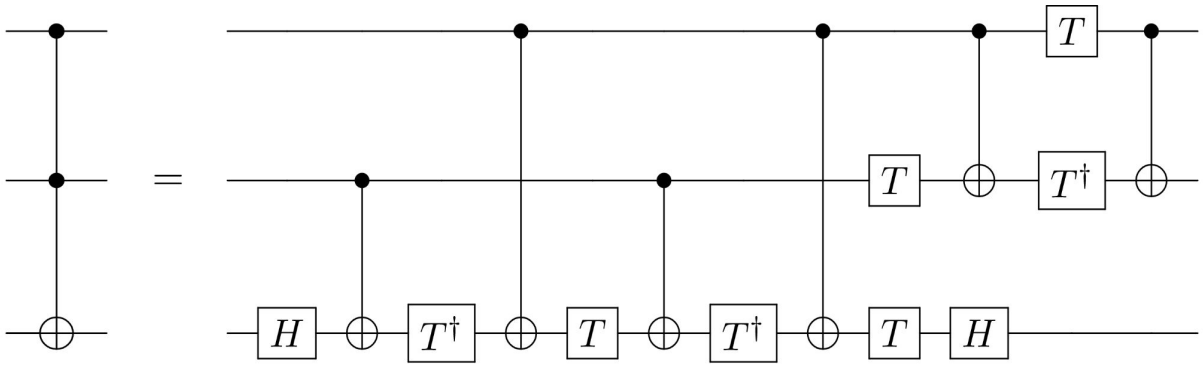


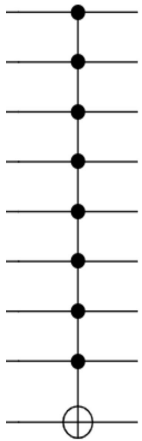
$$\begin{pmatrix} I_n & 0 \\ 0 & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix}$$

- Analogous to reversible multiple input AND gates
- Commonly used to construct other circuits

Decomposing a Toffoli Gate

- Want to minimize the amount of multiple qubit interactions and small rotations such as T gates which are hard to implement precisely





=

Current Construction: Relative Phase

- Relative phase toffoli gates have entries with *magnitude* 1

$$\begin{pmatrix} z_1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & z_2 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & z_3 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & z_4 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & z_5 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & z_n \\ 0 & 0 & 0 & 0 & 0 & 0 & z_{n-1} & 0 \end{pmatrix} \text{ s.t. } |z_i| = 1$$

- Use $RTOF^{N-1}$ to construct TOF^N
  - Maslov 2016:

$$\text{Cost}(TOF^N) \leq 2 \times \text{Cost}(RTOF^{N-1}) + 6 \text{ with 1 clean ancilla}$$
$$\text{Cost}(TOF^N) \leq 2 \times \text{Cost}(RTOF^{N-1}) + 8 \text{ with 1 dirty ancilla}$$

Main Results

Lower Bounds

Previous Works

	TOF^N	$RTOF^N$
ROM	Not possible to implement	Not known
R-W	2N (2008, Shende & Markov)	Not known

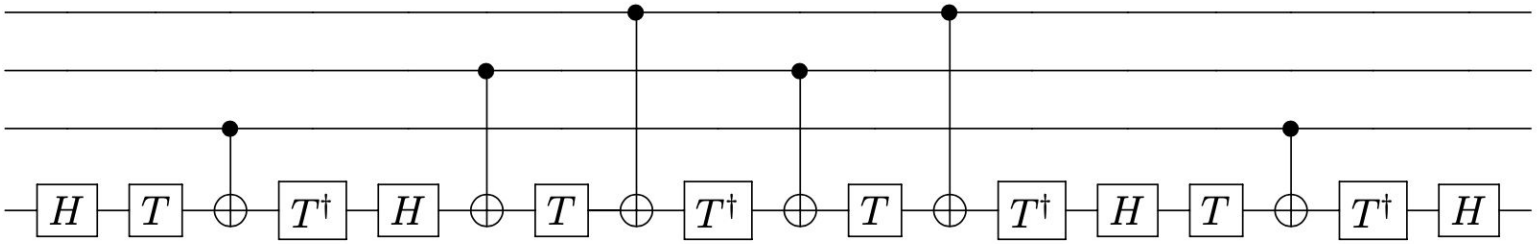
Our Results on Lower Bound of RTOF on CNOT Costs

	TOF^N	$RTOF^N$
ROM	Not possible to implement	2N - 2 (N > 3) 3N - 6 (N > 4, for special type RTOF)
R-W	2N (2008, Shende & Markov)	3/2N - 1 (N > 3)

More Results

Corollary 1: Optimality of RTOF^4 in ROM

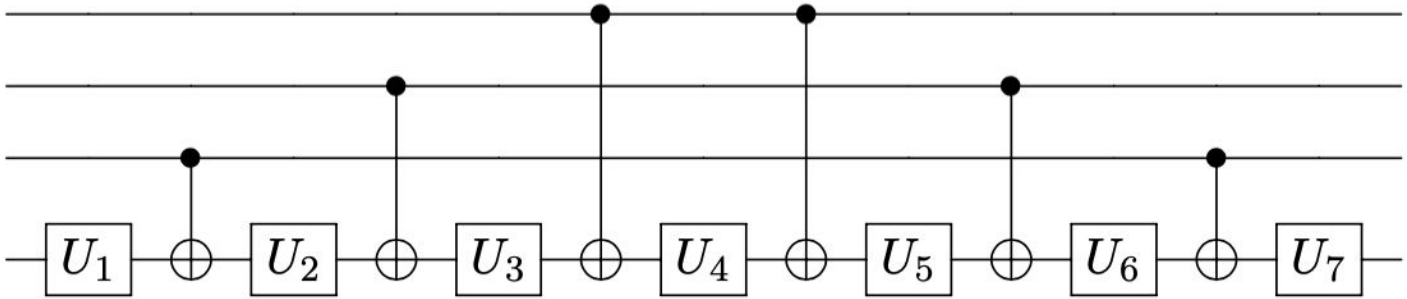
Theorem 4 (Our Result): Even in R-W, 6 CNOTs are required to implement RTOF^4 (Optimality of RTOF^4 in R-W)



Conjectures

Theorem 5: 3N - 6 CNOTs are required to implement a special type of $RTOF^N$ in ROM

Conjecture 1: 3N - 6 CNOTs are required to implement $RTOF^N$ in ROM



Why ROM when you have access to R-W?

1. Almost all current known implementations of $RTOF^N$ are in ROM
2. These implementations in ROM are also optimal in R-W in terms of CNOT costs by our following theorems:

Theorem 4 (G.Song, 2004): 3 CNOTs are required to implement $RTOF^3$ in R-W

Theorem 5 (Our Result): 6 CNOTs are required to implement $RTOF^4$ in R-W

Conjecture 1: In terms of CNOT costs of $RTOF^N$, ROM and R-W Model have the same computational power.

Upper Bounds

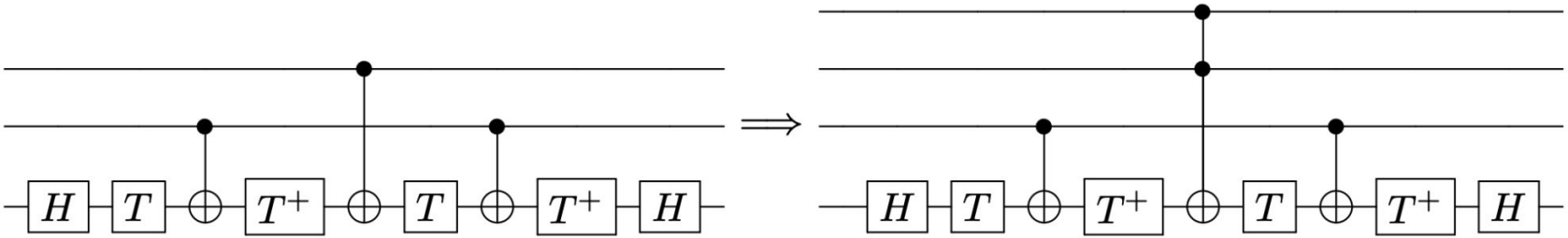
Previous Works on Upper Bound

	TOF^N	$RTOF^N$
No ancilla	Around 300N (Gidney, 2015)	Conjecture: 4N-10 in ROM (Maslov)
1 ancilla	12N (Maslov, 2016)	No good bound
~N/2 ancilla	6N (clean ancilla) 8N (dirty ancilla) (Maslov, 2016)	No good bound

Motivating Construction

Conjecture (Maslov): N-qubit relative phase Toffoli Gates can be implemented with 4N-10 CNOT gates

- Replace CNOTs with Margolus gates on a qubit to incorporate more controls
- Relative Phase introduced commute with unitary gates



Constructing ROTF^n with Clifford + T

Theorem 6: Let $n = 3^m + 1$ for some non-negative integer n, there exists a construction of RTOF^n with CNOT-cost $c(n)$ and T-cost $t(n)$, where

$$\begin{aligned} c(n) &= (n-1)^{\log_3 6} \\ t(n) &\leq \tfrac{8}{5}(n-1)^{\log_3 6} \end{aligned}$$

Improvement — Fewer Ancilla (04/06)

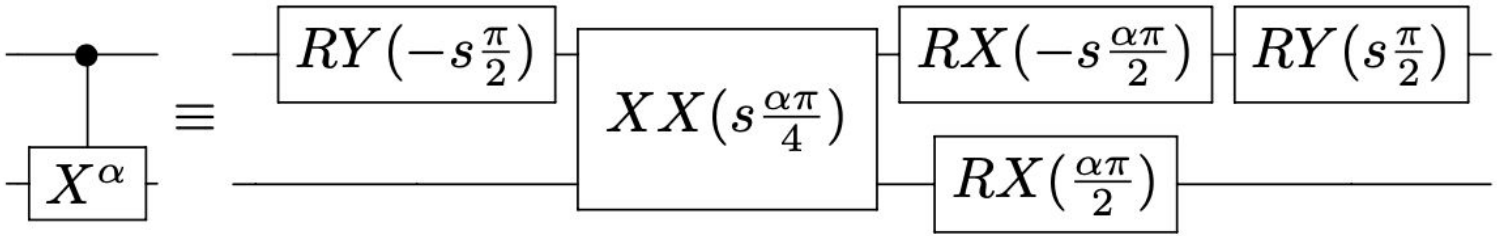
	# $CNOT$	# Ancilla	Ancilla Type
TOF^6	28	2	$\|xx\rangle$
	28	**1**	$\|x\rangle$
TOF^7	36	2	$\|xx\rangle$
	36	**1**	$\|x\rangle$
TOF^8	44	3	$\|xxx\rangle$
	44	**1**	$\|x\rangle$

Improvement — Less CNOT and T Cost with 1 ancilla

Ancilla	Clean Ancilla		Dirty Ancilla	
#Gates	$\#CNOT$	#T	$\#CNOT$	#T
TOF^{8}	66	72	88	96
	40	**48**	**44**	**66**
TOF^{9}	78	84	104	112
	48	**56**	**56**	**82**
TOF^{10}	90	96	120	128
	56	**68**	**68**	**98**
TOF^{11}	102	108	136	144
	64	**76**	**80**	**114**
TOF^{14}	138	144	184	192
	88	**108**	**128**	**186**

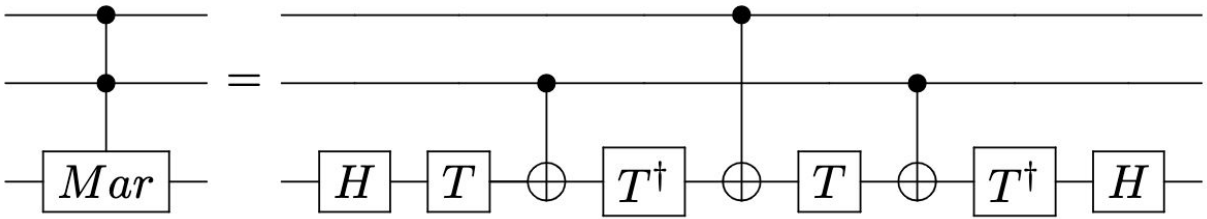
Replacing T with fractional CNOT gates

New cost metric: Counting the amount of coupling!

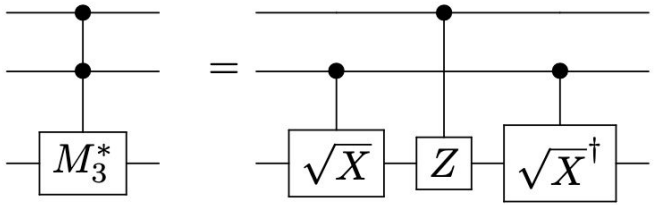


Replacing T with fractional CNOT gates

RTOF^3 with Clifford + T



RTOF^3 with Clifford + CrX



Constructing ROTF^n with Clifford + CX^r

Theorem 6: Let $n = 3^m + 1$ for some non-negative integer n, there exists a construction of RTOF^n with CNOT-cost $c(n)$ and T-cost $t(n)$, where

$$\begin{aligned} c(n) &= (n-1)^{\log_3 6} \\ t(n) &\leq \tfrac{8}{5}(n-1)^{\log_3 6} \end{aligned}$$

We can improve entangling cost by using square-root of CX and CZ, and *eliminate the need for single qubit gates* (including T gates!)

$$e(n) = \tfrac{2}{3}(n-1)^{\log_3 6} \qquad t(n) = 0$$

Improvements on RTOF construction

Gate Type	With Clifford $+C\sqrt{X}$		With Clifford$+T$	
	Ent. Cost	# Gates	Ent. Cost	T Cost
$RTOF^3$	2	4	3	4
$CCiX$	3	4	4	4
$RTOF^4$	4	6	6	8
C^3iX	5	6	DO NOT KNOW	
$RTOF^5$	6	10	10	14
$RTOF^7$	12	18	18	30
$RTOF^{10}$	24	36	36	56

Improvements on TOF construction

Type of Gate	With Clifford+CX^r			With Clifford+T		
	Ent. Cost	# Gates	Ancillae	Ent. Cost	T Cost	Ancillae
TOF^3	3.5	5	0	6	4	0
TOF^4	7.75	13	0	15	12	1
TOF^n	$4n - C$	$6.9n - C$	$\frac{n}{3} - C$			
TOF^n	$4.8n - C$	$7.2n - C$	$\frac{n}{5} - C$	$6n - C$	$8n - C$	$\frac{n}{2} - C$
TOF^n	$6n - C$	$9n - C$	$\frac{n}{8} - C$			

Conclusion

- First set of lower bounds on the CNOT cost of Relative Phase Toffoli Gates
  - 2n-2 for RTOF in ROM
  - 3n/2-1 for RTOF in R-W
  - 3n-6 for a special type RTOF in ROM
- First proof for the optimality of a $RTOF^4$
- New construction of $RTOF^N$ and TOF^N
  - Practical improvements for CNOT-count, T-count and Ancilla-count for small n (Clifford + T)
  - >30% reduction on entangling cost & ancillae needed, avoid single qubit gates (Clifford + CrX)
  - Currently working to demonstrate this advantage on a quantum device

Questions?

“Willers” Muye Yang - willers@mit.edu

Xinjie He - xinjieh@andrew.cmu.edu

Drew Gao - drewgao@stanford.edu