The Classification of Reversible Bit Operations

Scott Aaronson
UT Austin

Daniel Grier
MIT

Luke Schaeffer
MIT

Motivation

- Problem: Given a set of quantum gates, which unitaries do they generate?
- Non-universal
  - 1-qubit gates
  - Classical reversible gates such as CNOT and Toffoli
  - Clifford gates [Gottesman-Knill 1998]
  - Toffoli + Hadamard
- Universal
  - Random 2-qubit gate
  - CNOT + all single-qubit gates
- This is hard…

Classical Gates!

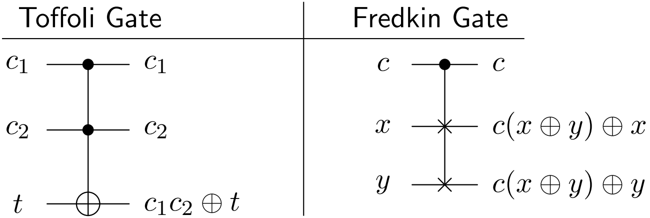
- New Problem: Given a set of *classical reversible* gates, are they universal? If not, what do they generate?

Definition

Reversible gate - bijective function $f : \{0,1\}^n \to \{0,1\}^n$.

Wait. . .

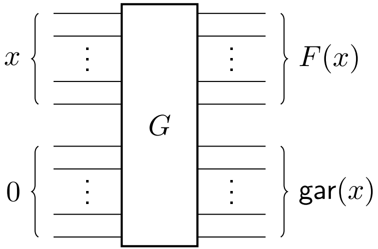
- Hasn't this problem been solved before?
- Boolean logic gates, i.e., $f : \{0,1\}^n \to \{0,1\}$
  - Completely classified [Post 1941]
  - AND, OR, NOT are universal
  - XOR - generates all linear functions
- 1980's - Research by Bennett, Toffoli, Fredkin, Landauer, . . .



- Lloyd (1992), De Vos & Storme (2004): Classify all reversible gate sets when leftover garbage bits are allowed.

Garbage is bad for quantum computation

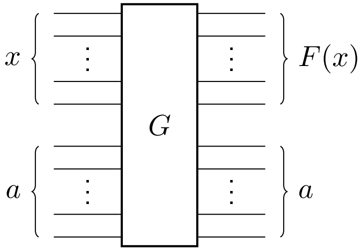
Suppose trying to construct $F : \{0,1\}^n \to \{0,1\}^n$



$$G\left(\sum_x \alpha_x |x\rangle|0\rangle\right) = \sum_x \alpha_x |F(x)\rangle|\mathsf{gar}(x)\rangle \rightarrow \text{BAD}$$

Garbage is bad for quantum computation

Suppose trying to construct $F : \{0,1\}^n \to \{0,1\}^n$



Model

Suppose we have a set of gates $S = \{G_1, G_2, \ldots\}$. The *class* $\langle S \rangle$ is its closure under the circuit building operations:

- **Composition Rule** If $G, F \in \langle S \rangle$, then $G \circ F \in \langle S \rangle$.
- **Extension Rule** If $G \in \langle S \rangle$, then $G \otimes I \in \langle S \rangle$.
- **Swap Rule** $\mathrm{SWAP} \in \langle S \rangle$.
- **Ancilla Rule** If $G \in \langle S \rangle$, then

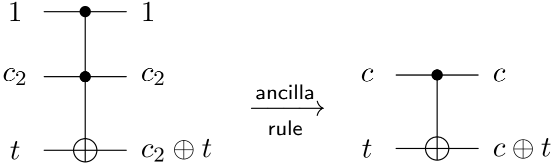
$$G(x, a) = F(x), a$$

for all x implies $F \in \langle S \rangle$.

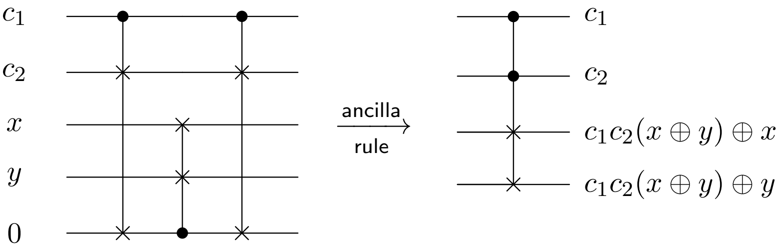
Corollary

If $G \in \langle S \rangle$, then $G^{-1} \in \langle S \rangle$.

Toffoli generates CNOT

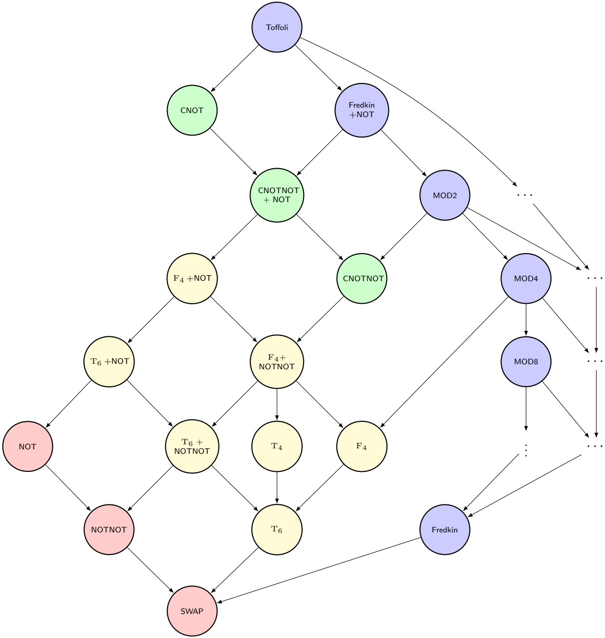


Fredkin generates controlled-controlled-SWAP



Main Theorem

Any set of reversible gates generates one of the classes in the following lattice:

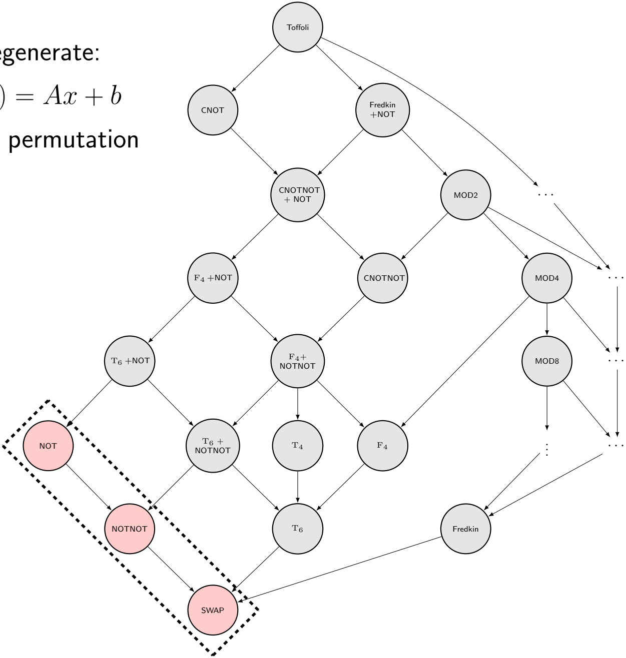


Toffoli
CNOT
Fredkin +NOT
CNOTNOT + NOT
MOD2
· · ·
F_4 +NOT
CNOTNOT
MOD4
· · ·
T_6 +NOT
F_4+ NOTNOT
MOD8
· · ·
NOT
T_6 + NOTNOT
T_4
F_4
⋮
· · ·
NOTNOT
T_6
Fredkin
SWAP

Degenerate:

$$F(x) = Ax + b$$

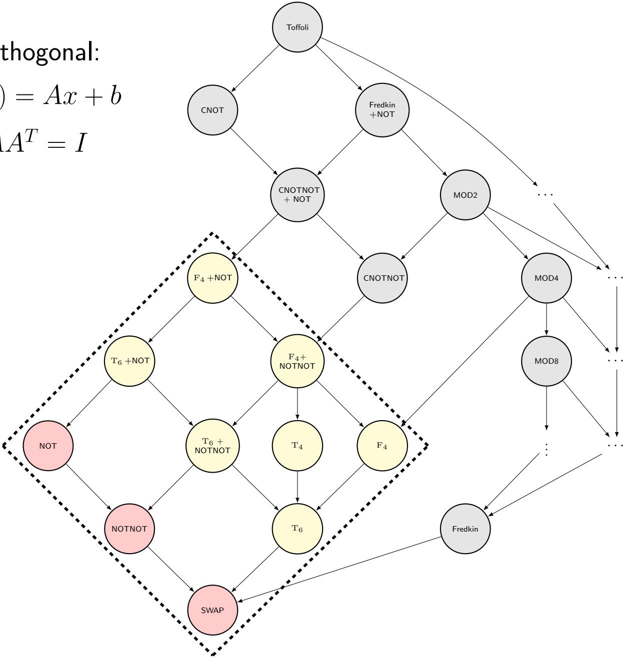
A is a permutation



Orthogonal:

$$F(x) = Ax + b$$

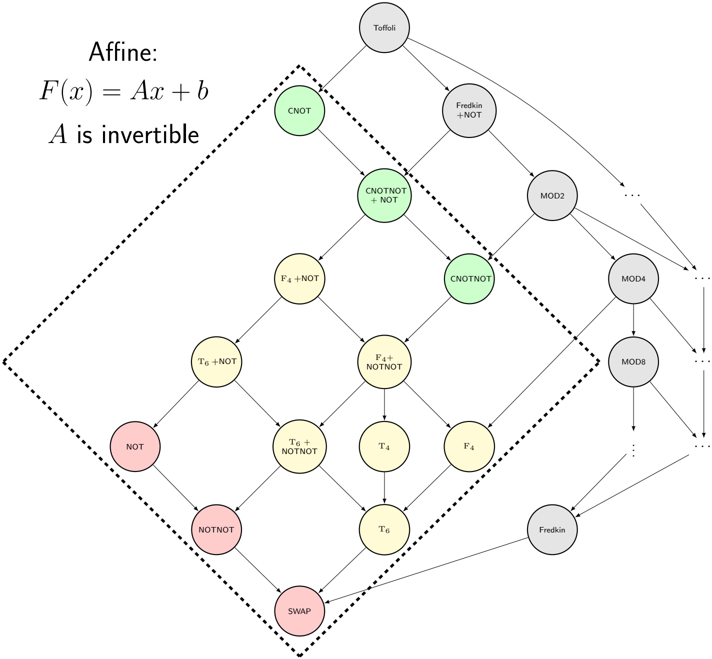
$$AA^T = I$$



Affine:

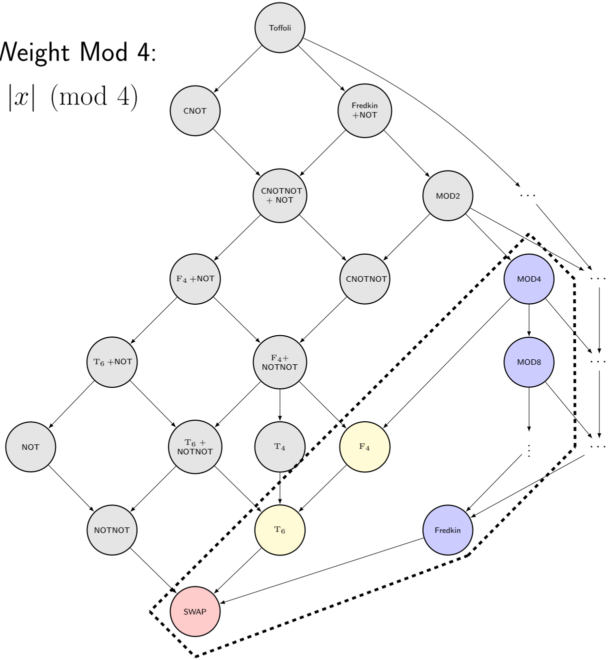
$$F(x) = Ax + b$$

A is invertible



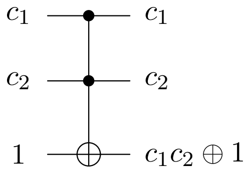
Hamming Weight Mod 4:

$$|F(x)| \equiv |x| \pmod 4$$



Proof Techniques: Uncomputing

Suppose we want to generate $F : \{0,1\}^n \to \{0,1\}^n$ using Toffoli



Observation

Last bit is NAND(c_1, c_2).

$$x \to x, \mathsf{gar}(x), F(x)$$

Proof Techniques: Uncomputing

$F : \{0,1\}^n \to \{0,1\}^n$

$$
\begin{aligned}
& x \\
\to\ & x, \mathsf{gar}_1(x), F(x) \\
\to\ & x, \mathsf{gar}_1(x), F(x), F(x) \\
\to\ & x, F(x) \\
\to\ & x, F(x), \mathsf{gar}_2(F(x)), x \\
\to\ & F(x), \mathsf{gar}_2(F(x)), x \\
\to\ & F(x)
\end{aligned}
$$

Theorem (AGS)

Given a set of reversible gates S. Any function $F \in \langle S \rangle$ can be constructed from gates in S using only $O(1)$ ancilla bits.

Open Questions

- What other gate sets can we classify?
  - Clifford gates [GS 2015]
  - 1 and 2-qubit gates
  - Hamiltonians
- Different ancilla rules?
- Different arity?