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 $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$. 
Wait... 

- Hasn’t this problem been solved before?

- Boolean logic gates, i.e., \( f : \{0, 1\}^n \rightarrow \{0, 1\} \)
  - Completely classified [Post 1941]
  - AND, OR, NOT are universal
  - XOR - generates all linear functions

- 1980’s - Research by Bennett, Toffoli, Fredkin, Landauer, ...

| Toffoli Gate | Fredkin Gate |
|--------------|--------------|
| \( c_1 \) | \( c \) |
| \( c_1 \) | \( c \) |
| \( c_2 \) | \( x \) |
| \( c_2 \) | \( c(x \oplus y) \oplus x \) |
| \( t \otimes c_1 c_2 \oplus t \) | \( y \) |
| \( c_1 c_2 \oplus t \) | \( c(x \oplus y) \oplus y \) |

- 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 $F : \{0, 1\}^n \rightarrow \{0, 1\}^n$

$$
G \left( \sum_x \alpha_x |x\rangle |0\rangle \right) = \sum_x \alpha_x |F(x)\rangle |\text{gar}(x)\rangle \rightarrow \text{BAD}
$$
Garbage is bad for quantum computation

Suppose trying to construct $F : \{0, 1\}^n \rightarrow \{0, 1\}^n$
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** $\text{SWAP} \in \langle S \rangle$.
- **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

\[ c_1 \leftarrow c_2 \leadsto x \leftarrow y \leftarrow 0 \]

\[ c_1 \leftarrow c_2 \leftarrow c_1c_2(x \oplus y) \oplus x \]

\[ c_1 \leftarrow c_2 \leftarrow c_1c_2(x \oplus y) \oplus y \]
Main Theorem

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

\[ F(x) = Ax + b \]

\( A \) is a permutation
Orthogonal:

\[ F(x) = Ax + b \]

\[ AA^T = I \]
Affine:
\[ F(x) = Ax + b \]
\[ A \text{ is invertible} \]
Hamming Weight Mod 4:

\[ |F(x)| \equiv |x| \pmod{4} \]
Proof Techniques: Uncomputing

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

![Diagram]

Observation

$Last \ bit \ is \ \text{NAND}(c_1, c_2).$

$x \rightarrow x, \text{gar}(x), F(x)$
Proof Techniques: Uncomputing

\[ F : \{0, 1\}^n \rightarrow \{0, 1\}^n \]

\[ x \]
\[ \rightarrow x, \text{gar}_1(x), F(x) \]
\[ \rightarrow x, \text{gar}_1(x), F(x), F(x) \]
\[ \rightarrow x, F(x) \]
\[ \rightarrow x, F(x), \text{gar}_2(F(x)), x \]
\[ \rightarrow F(x), \text{gar}_2(F(x)), x \]
\[ \rightarrow F(x) \]

**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?