S.KIMMEL

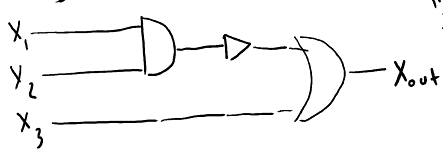
Classical Models of Computation (that helped inspire quantum model)

- Circuit (usual classical model)
- Reversible (b/c unitaries are reversible)
- Probabilistic (b/c measurements are probabilistic)

Circuit - way of describing functions on bits

bit: $x \in \{0,1\}$

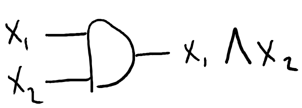
time →



implements the function $\approx f: \{0,1\}^3 \to \{0,1\}$

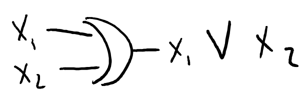
Set of all 3-bit strings
e.g. $\{0,1\}^2 = \{00, 01, 10, 11\}$
x_1 x_2

Gate ex:



AND

NOT



OR

FANOUT

universal universal

Not technically necessary for universality, but useful

Gate set is universal, can compute any $f: \{0,1\}^n \to \{0,1\}^m$

↑ Generalized Boolean function

Circuits provide way of determining how difficult it is to compute a function.

Measures of circuit complexity:

- Gate count = # gates used
- Depth = # time steps (depends on parallelization)
- Width/Size = max # wires present at a time

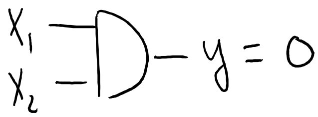
} want to minimize

Q

Ex: • find circuit that implements function $f: \{0,1\}^4 \to \{0,1\}$; $f(x_1 x_2) = \begin{cases} 1 & x_1 = x_2 = x_3 = x_4 = 0 \\ 0 & \text{otherwise} \end{cases}$
• What is gate count, depth, width?

S. KIMMEL

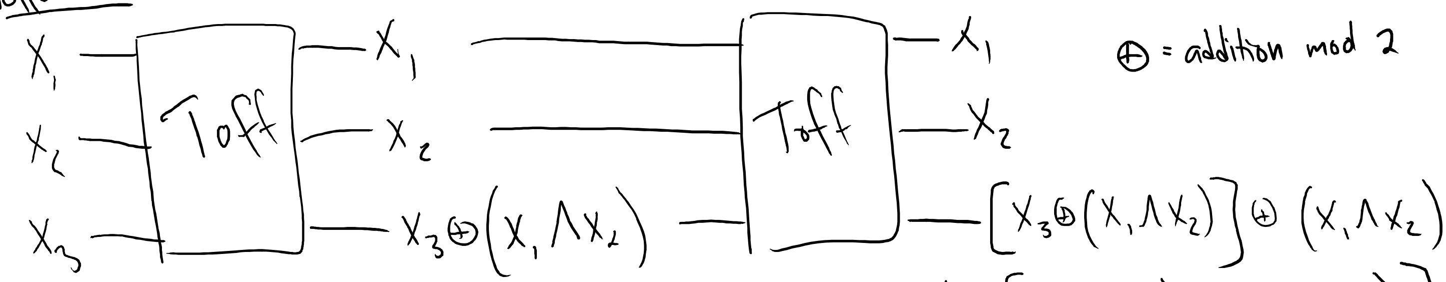
Reversible



$\Rightarrow x_1 x_2 = \{00, 01, 10\}$ NOT REVERSIBLE

(only 1 output bit for 2 input bits — information must have been destroyed)

Toffoli Gate



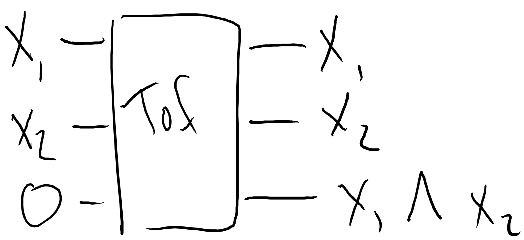
$\oplus$ = addition mod 2

$= x_3 \oplus [(x_1 \wedge x_2) \oplus (x_1 \wedge x_2)]$

$= x_3 \oplus 0 \quad = x_3$

Claim: Toffoli Gate is universal

ex: AND using Toffoli



* cost: extra input bit

A.L. Use Toffoli to create NOT, FANOUT, OR

Note: for reversible circuits, # wires in = # wires out

* Can make any classical circuit reversible using Toffoli.

Cost: increased # of wires

S.KIMMEL

Probabilistic Computation

Deterministic Bit: $X=0$ or $X=1$

Probabilistic Bit: $P(0) = .75$ $P(1) = .25$

↑ Probability of 0 ↑ Probability of 1

Store Info about probabilities in vectors

1-bit:

$$\begin{pmatrix} P(0) \\ P(1) \end{pmatrix}_A = \begin{pmatrix} .75 \\ .25 \end{pmatrix}$$

Another Bit

$$\begin{pmatrix} P(0) \\ P(1) \end{pmatrix}_B = \begin{pmatrix} .5 \\ .5 \end{pmatrix}$$

Together

$$\begin{pmatrix} .75 \\ .25 \end{pmatrix}_A \otimes \begin{pmatrix} .5 \\ .5 \end{pmatrix}_B = \begin{pmatrix} \frac{3}{8} \\ \frac{3}{8} \\ \frac{1}{8} \\ \frac{1}{8} \end{pmatrix} = \begin{pmatrix} P(00) \\ P(01) \\ P(10) \\ P(11) \end{pmatrix}$$

Quantum Correlation:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Classical Correlation:

$$\frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$ (Both bits have same value: $P(00) = P(11) = \frac{1}{2}$)

↑ can't be formed by combination of 2 independent bits

S.KIMMEL

Probabilistic n-bit State

$$\sum_{i \in \{0,1\}^n} a_i |i\rangle \qquad a_i \geq 0$$

not q. state, just vector

$$\sum a_i = 1$$

Probability of string i is a_i

Transform using left stochastic matrix

(preserves positivity & normalization)

Quantum n-bit State

$$\sum_{i \in \{0,1\}^n} a_i |i\rangle \qquad a_i \in \mathbb{C}$$

$$\sum |a_i|^2 = 1$$

If measure in standard basis, Probability of outcome i is $|a_i|^2$

Transform using unitary matrix U: $U^\dagger U = UU^\dagger = \underline{I}$

(preserves normalization)

S.KIMMEL

Probabilistic Gate

Left Stochastic Matrix (columns sum to 1, non-negative entries)

↑ These matrices

ex: $$\begin{pmatrix} 1/2 & 0 \\ 1/2 & 1 \end{pmatrix} \begin{pmatrix} p(0) \\ p(1) \end{pmatrix} = \begin{pmatrix} 1/2\, p(0) \\ 1/2\, p(0) + p(1) \end{pmatrix}$$