Methods in quantum computing

Mária Kieferová

August 5, 2022

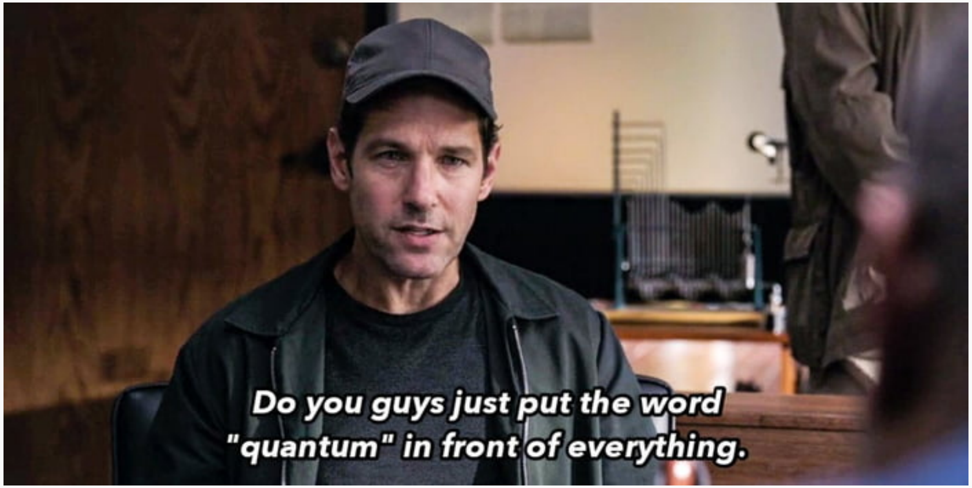
University of Technology Sydney

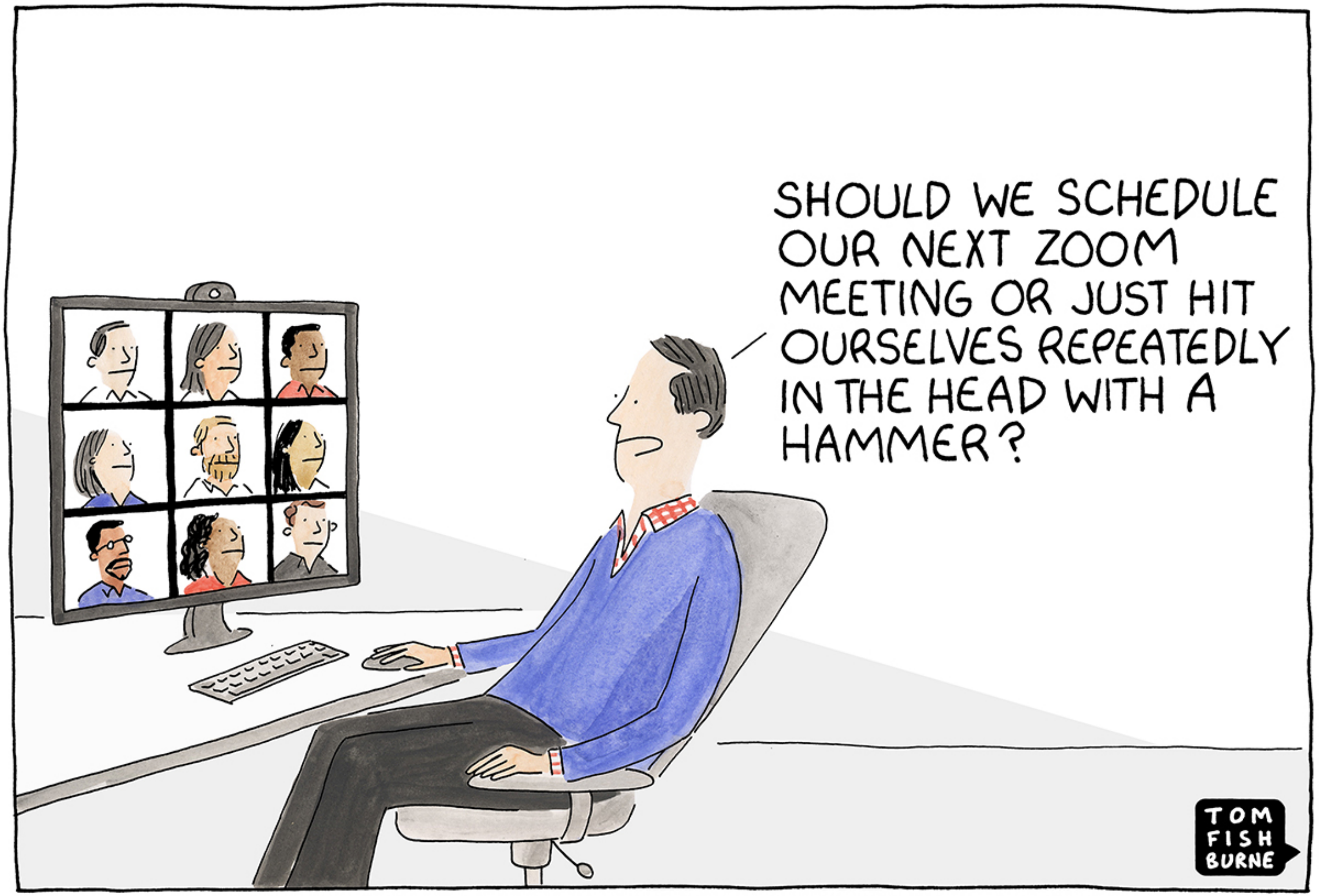
Class overview

- UTS undergraduates + SQA grads
- assumes familiarity with quantum computing and mathematical maturity (linear algebra, theorems and proofs)
- 12 weeks, 3 months, 3hour lecture + tutorial per week
- 3 types of assessments: problem sets, group video, final project
- 50% required to pass, attendance not required (but recommended)
- info on Canvas and `www.mariakieferova.com/methods-in-quantum-computing`
- office hours immediately after class or by appointment

Topic overview

1. Quantum formalism, quantum mechanics and quantum information theory
2. Quantum stack - physical implementation, architecture and quantum error correction
3. Quantum algorithm and complexity
4. Quantum communication and entanglement



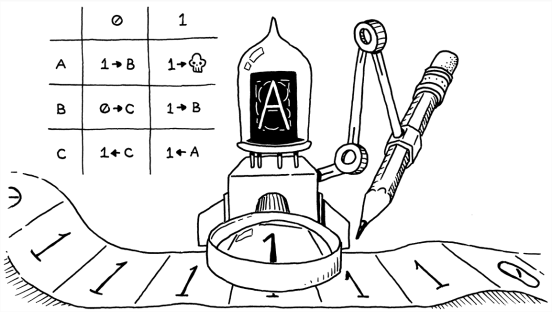

SHOULD WE SCHEDULE OUR NEXT ZOOM MEETING OR JUST HIT OURSELVES REPEATEDLY IN THE HEAD WITH A HAMMER?
TOM FISH BURNE

Introduce yourself to the class! Were are you from? What are your plans for this weekend?

Today

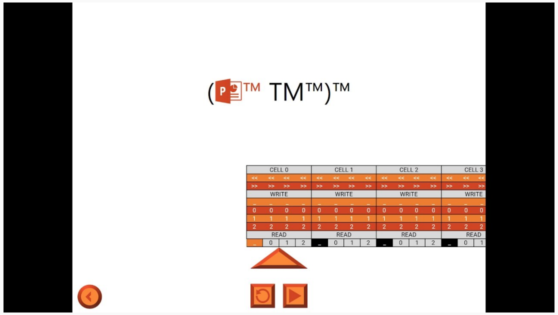
1. Motivation behind quantum computing
2. Models of computation
3. Quantum circuits

Computational models

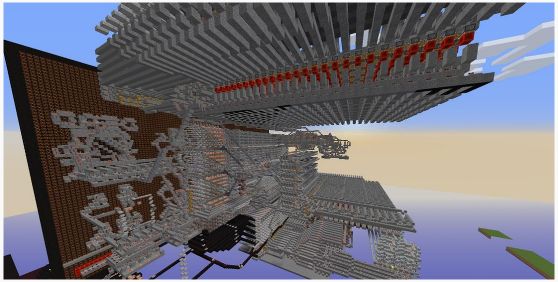


(a) Turing machine

(b) Conway's game of life

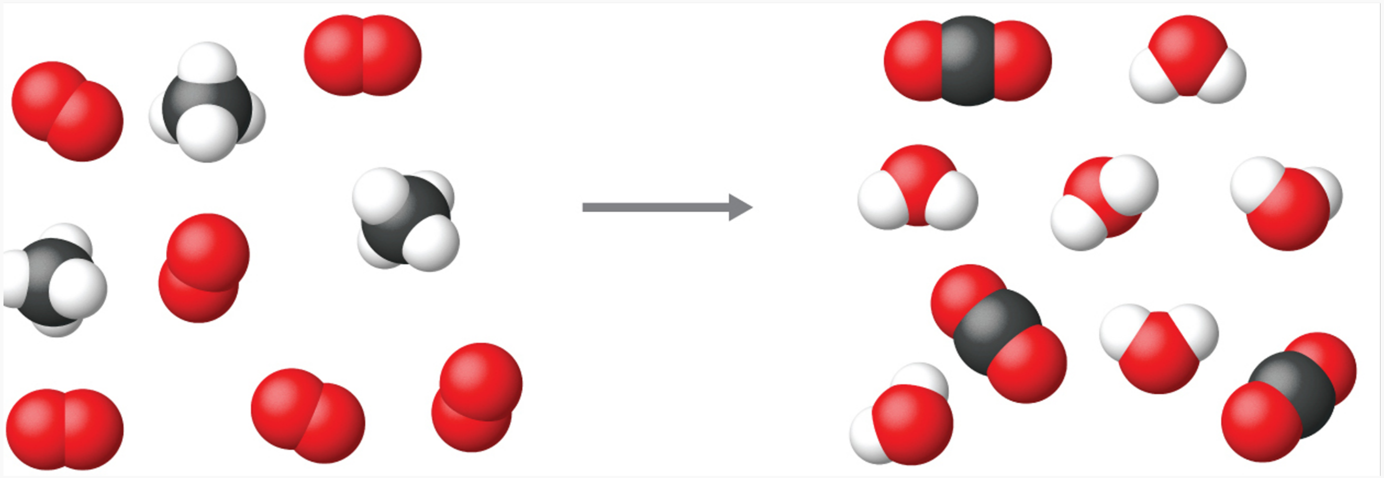


(c) Power Point



(d) Minecraft

Simulating nature

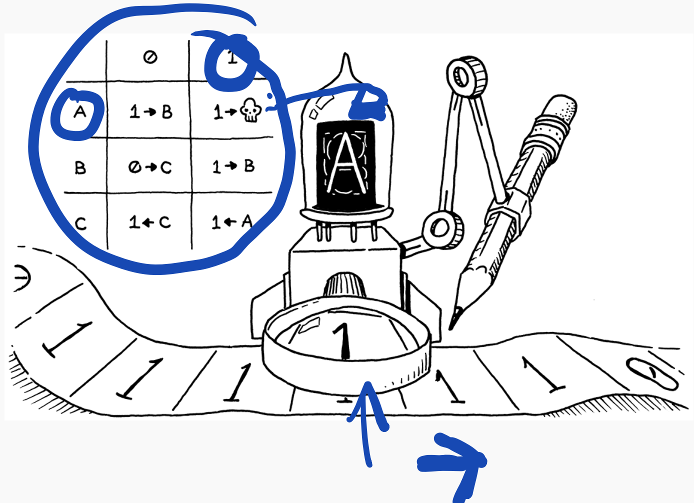


Physics of Computation

Why are you interested in quantum computing?

What topics are you working on and why did you choose them?

Turing machine

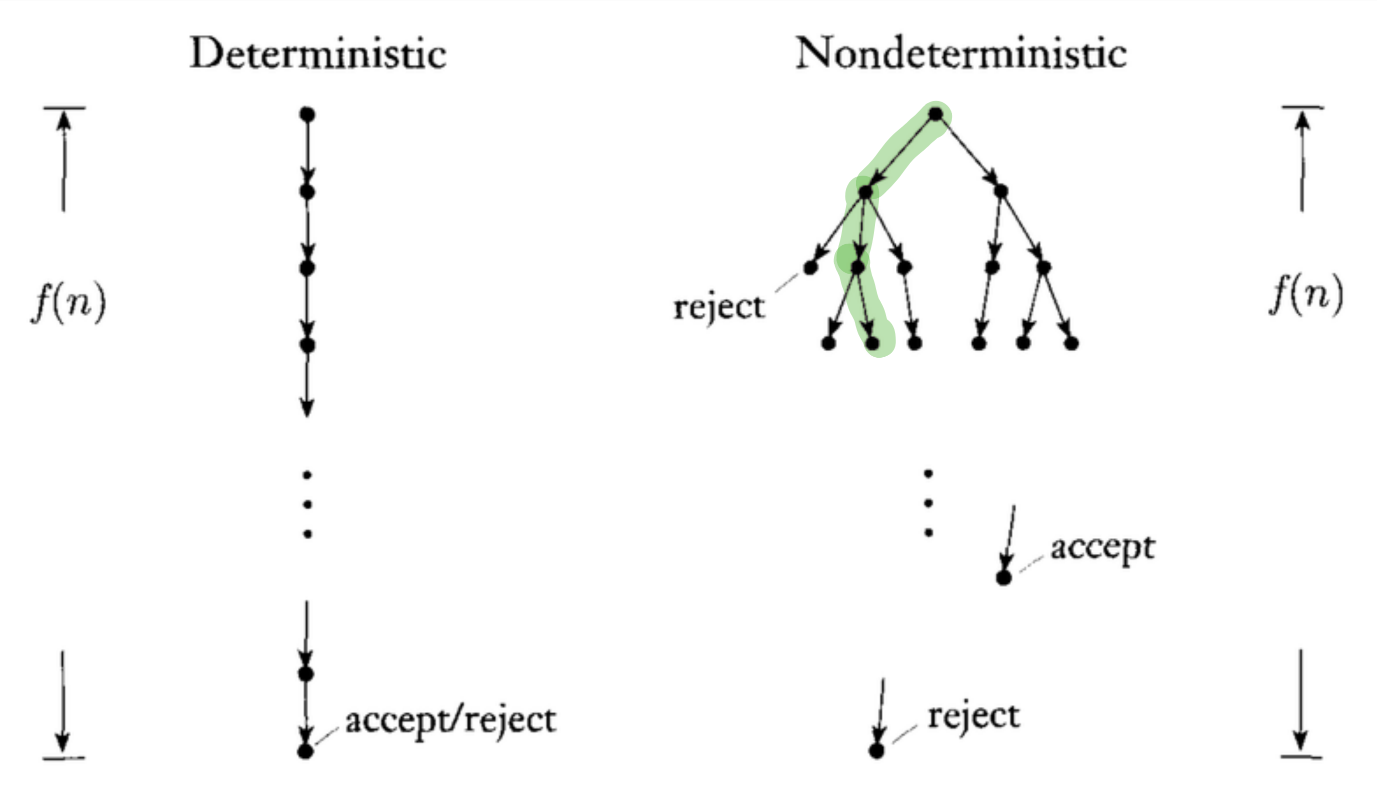


- Γ a non-empty alphabet, i.e. a set of allowed symbols
- $b \in \Gamma$ a blank symbol
- $\Sigma \subseteq \Gamma$ a set of symbols that initially appear on the tape
- Q a finite set of states of the machine
- $q_0 \in Q$ the initial state
- $F \subseteq Q$ set of accepting states. If the TM reaches one of these states, the computation finishes and the input is accepted ("yes").

- $\delta : Q \setminus F \times \Gamma \to Q \times \Gamma \times \{\text{left, right}\}$ is the transition function.

$\times \text{coin}\{0,1\}$

Turing machines



Church-Turing thesis

not a theorem

quantum computer can be simulated classically with exp overhead

A Turing machine can simulate any realistic model of computation.

computability

computational complexity

false!

polynomial

A probabilistic Turing machine can efficiently simulate any realistic model of computation.

computation that takes n steps

pTM – use poly(n)

n^2 ✓

$\exp(n)$ ✗

$n!$ ✗

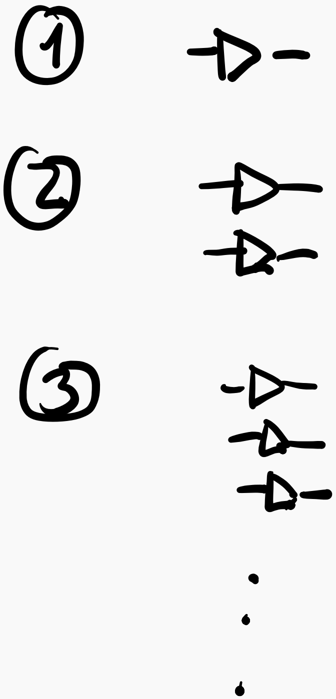
Logical circuits

Denote $\mathbb{B}^n := \mathbb{Z}_2^n$. Let $f : \mathbb{B}^n \to \mathbb{B}^m$ be a Boolean function that takes an n-bit string as input and outputs an m-bit string. Let $\mathcal{G}$ be a collection of basic logic gates. A Boolean circuit for f is a sequence of gates $\{g_1, \cdots, g_L\} \in \mathcal{G}$ which converts an input $\boldsymbol{x} \in \mathbb{B}^n$ to the output $\boldsymbol{y} \in \mathbb{B}^m$ with a fixed size of K auxiliary bits.

AND, OR, NOT

Logical gates

Uniform circuit families



For each length of the input n, there is a logical circuit.

Exercise

15 minutes

a → a a

Show that the NAND and FANOUT (copy) are universal for computation, i.e. they can be used to express all possible truth tables.

(a) Show that the NOT gate can be simulated using a single NAND gate.

0 → 00

1 → 11

(b) Show that the AND gate can be simulated with a constant number of NAND gates.

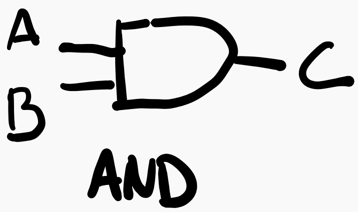
(c) Show that the OR gate can be simulated with a constant number of NAND gates. Hint: in the footnote [1]. How many NANDs is required for this construction?

You might use additional bits initialized to 0 or 1.

[1] Use De Morgan's Law: A OR B = NOT (NOT A AND NOT B).

Reversible circuits

Logical circuits that can be inverted are known as reversible circuits.



input $\to$ output

~~output $\to$ input~~

$a \wedge b = 1$

$a = 1$

$b = 1$

$a \wedge b = 0$

not is reversible

and isn't reversible

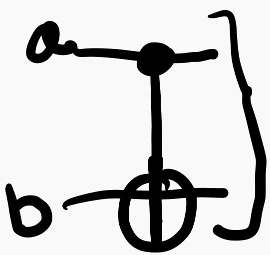
Exercise

What operations in Table 1 are reversible? What are the inverse operations to the reversible gates in Tables 1 and 2?

not

CNOT

\# inputs = # outputs



a	b	CNOT(a,b)
0	0	0 0
0	1	0 1
1	0	1 1
1	1	1 0

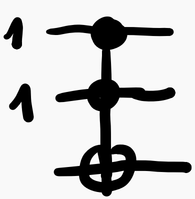
$$0_L = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$1_L = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\mathrm{NOT}\, 0_L = 1_L$$

$$\mathrm{NOT}\, 1_L = 0_L$$



activate NOT

Qubits

$|\cdot\rangle$ ket

$\langle\cdot|$ bra

$$0_L \to |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$1_L \to |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

valid quantum state

where $|\alpha|^2 + |\beta|^2 = 1$

Hello

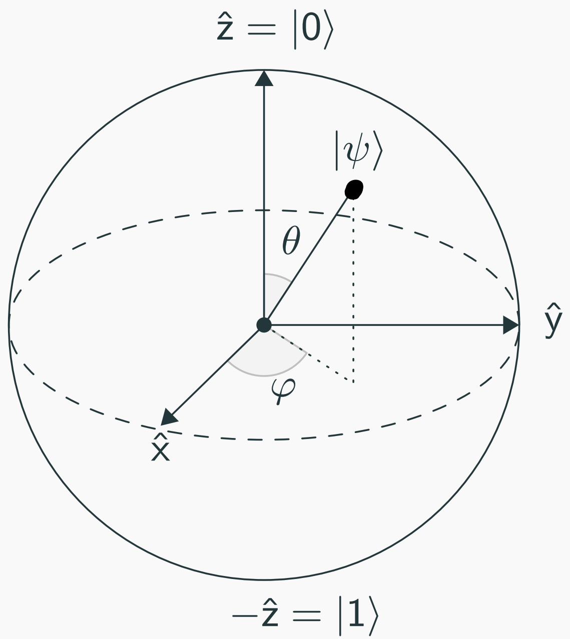
Qubits

$\sin^2\theta + \cos^2\theta = 1$

$$|\psi\rangle = \left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle .\right) i$$

complex

Bloch sphere



Quantum operations

Given an initial state $|\psi_0\rangle$, we can apply a gate U to obtain a new state $|\psi_1\rangle$

$$|\psi_1\rangle = U\,|\psi_0\rangle\,.$$

$n \to 2^n$

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} c & d \\ e & f \end{pmatrix} \begin{pmatrix} g \\ h \end{pmatrix}$$

$$\begin{pmatrix} \\ \end{pmatrix} = \begin{pmatrix} & \\ & \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix}$$

Exercise

Show that quantum operations must be unitary in order to preserve the norm of quantum states. An operation U is unitary if and only it satisfies $U^{-1} = U^{\dagger}$.

Exercise

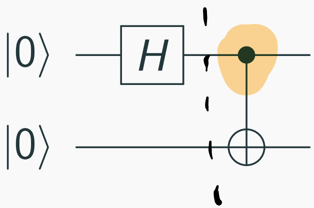
a Show that for a unitary matrix U, $|\det(U)| = 1$. Hint: in a footnote.

b A global phase of a quantum state is not detectable. In other words, states $|\psi\rangle$ and $e^{i\psi}|\psi\rangle$ represent the same physical state. What consequence will it have for single qubit gates?

c Write the most general single qubit gate U using the convention $\det(U) = 1$.

Exercise

What is the state state prepared by this circuit?



we can specify gates by defining how they act on basis states

H = Hadamard gate $\quad H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H_1|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

$$CNOT\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Solovay-Kitaev

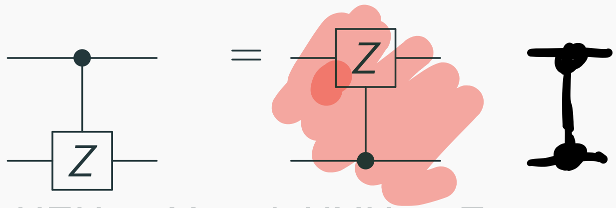
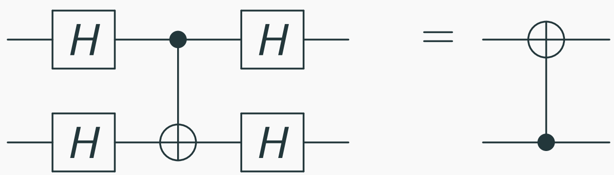
Given any universal set of gates $\mathcal{G}$ that is closed under inverse, any unitary operation $U \in SU(d)$ can be ε-approximated using $O(\log^c(\frac{1}{\varepsilon}))$ gates from $\mathcal{G}$ for some constant c.

good

$\{H, T, CNOT\}$

$\{H, Toff\}$ Barenco & co.

Exercise

1. Show that 
2. Show that $HZH = X$ and $HXH = Z$.
3. How would one construct CZ out of $CNOT$ and single qubit gates?
4. Show that 

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

$$H = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|\right)$$

$$CNOT = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$$

$$\mathbb{1} = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$\begin{aligned} C\text{-}Z &= |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes Z \\ &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 0| \otimes |1\rangle\langle 1| + \\ &\quad + |1\rangle\langle 1| \otimes |0\rangle\langle 0| - |1\rangle\langle 1| \otimes |1\rangle\langle 1| \\ &= \underbrace{\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)}_{\mathbb{1}} \otimes |0\rangle\langle 0| + \underbrace{\left(|0\rangle\langle 0| - |1\rangle\langle 1|\right)}_{Z} \otimes |1\rangle\langle 1| \\ &= \mathbb{1} \otimes |0\rangle\langle 0| + Z \otimes |1\rangle\langle 1| = Z\text{-}C \end{aligned}$$