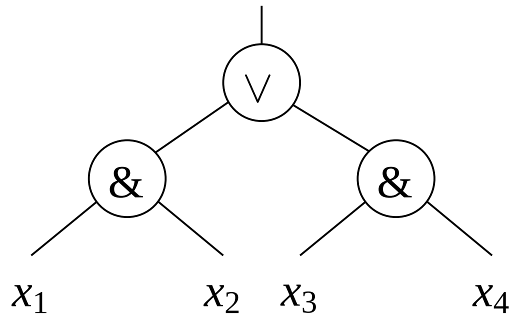
Quantum Computation and Quantum Circuits

Robert Špalek, CWI

September 18, 2003

Classical computation

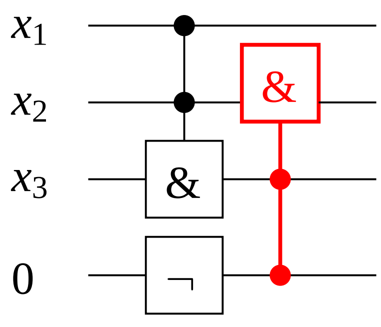
- *deterministic*
- computer in 1 state at each moment
- *parallel* computation modelled by circuits:



- elementary gates: Not, And, Or
- polynomial *size*, bounded *fan-in*, unbounded *fan-out*

Reversible circuits

- constant number of bits
- *ancilla* bits initialised to 0
- elementary *reversible* gates: Not, Toffoli



- can simulate classical comp. with small overhead

Probabilistic computation

- can flip random coins
- state is a *prob. distribution* on *classical states* e_i:

$$x = \sum_{i=0}^{2^n-1} p_i e_i, \; 0 \le p_i \le 1, \text{ and } \sum p_i = 1$$

- evolution is a *stochastic process*
- result is *sampled* from the prob. distribution
- allow small *error* (one-sided, two-sided) or *zero-error* comp. of small *expected* time

Quantum physics

Nature obeys quantum laws:

- quantum *superposition* $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
- *product* state $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ versus

  entangled state (EPR-pair) $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- *unitary* evolution (reversible and norm-preserving)

Irreversible processes possible due to interaction with environment, i.e. energy dissipation, we call them

- quantum *measurement*.

  They *collapse* the quantum state!

Quantum circuits

- are like reversible circuits, but with *quantum gates*:
  - Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
  - phase shift $R_z(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$
  - controlled-not maps cnot:$|x\rangle|y\rangle \to |x\rangle|x \oplus y\rangle$
- state is a *superposition* of classical states $|x\rangle$:

$$|\varphi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle, \ \alpha_x \in \mathbb{C}, \text{ and } \sum |\alpha_x|^2 = 1$$

- *measurement* at the end gives prob. $p_x = |\alpha_x|^2$

Elementary quantum gates

- are *universal* for quantum computation
  (every unitary operation can be efficiently approximated)

- Hadamard gate is **like** a random coin flip, but it is reversible:

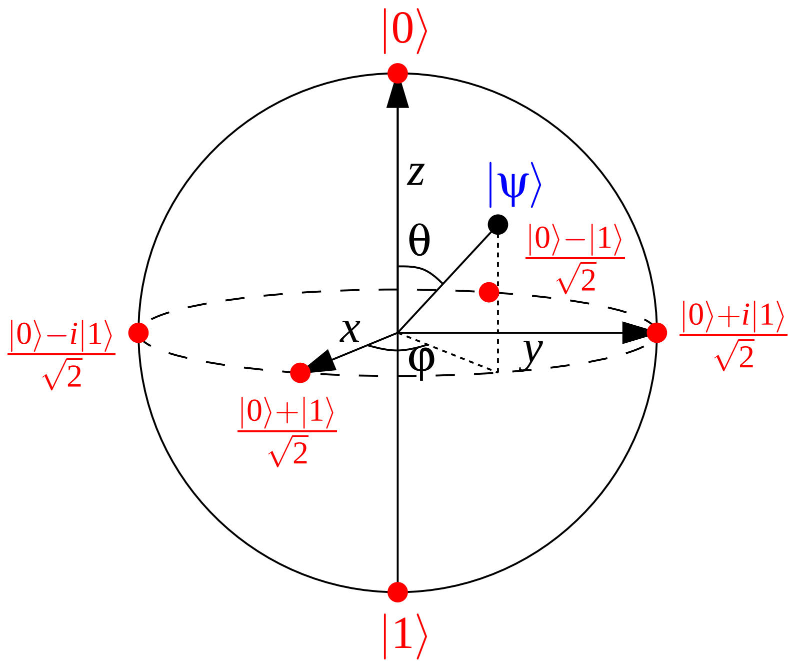
$$
\begin{aligned}
H|0\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
H^2 &= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^2 = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I \text{ (identity)}
\end{aligned}
$$

- phase shift changes the *relative phase* of $|0\rangle$ and $|1\rangle$

Visualisation of one qubit

Bloch sphere

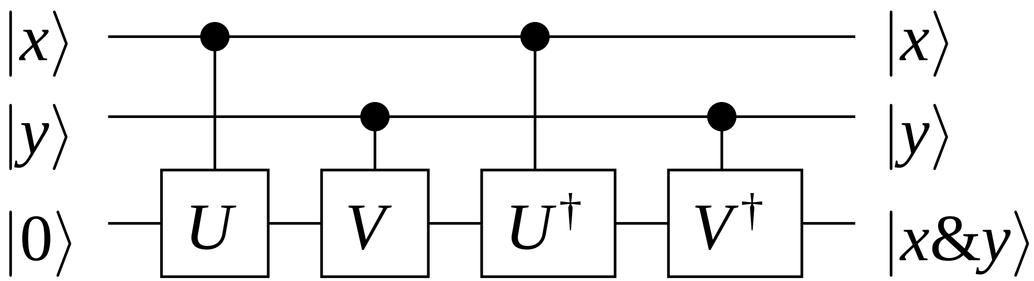
- is mapping between states of **one** qubit and points on a sphere.
- Let $\theta \in \langle 0, \pi \rangle$ and $\varphi \in \langle 0, 2\pi)$.
  Then $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$.
- 2 real parameters instead of 4, since
  - the norm must be 1,
  - *global phase* is unobservable.
- 1-qubit operations rotate the sphere.

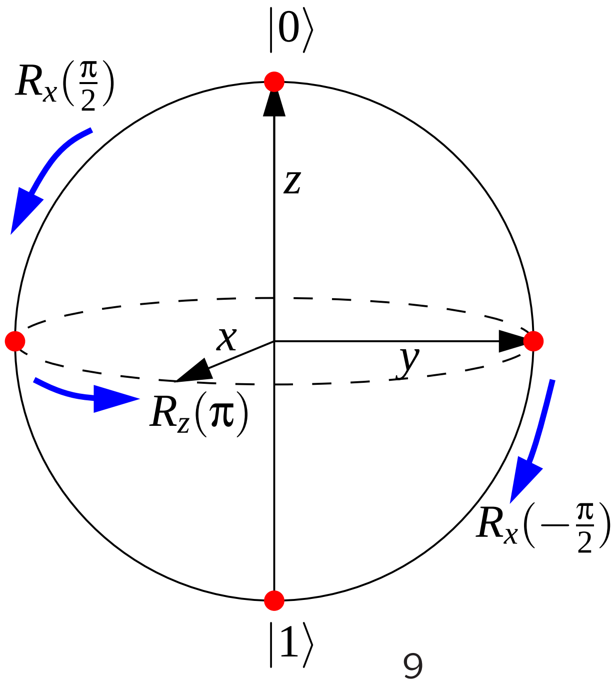


Toffoli (And) gate from elementary gates

1. Implement controlled one-qubit gate (skipped).

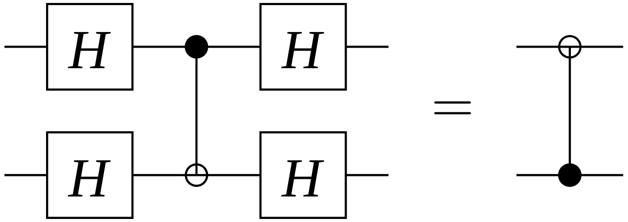
2. Take two *non-commuting* one-qubit operations U, V:
$U = R_x(\frac{\pi}{2})$, $V = R_z(\pi)$. Note: $UVU^\dagger V^\dagger = X$ (Not).





If $x = y = 1$, then X is applied.
If $x = 1$ & $y = 0$, then $UU^\dagger = I$ is applied.
Nothing happens if $x = y = 0$.

Turning around the controlled-not

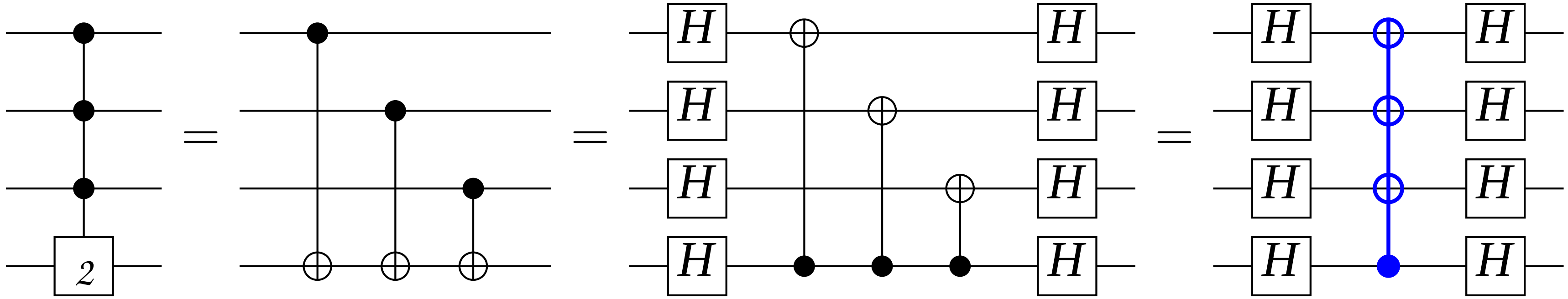


because

$$
\begin{aligned}
|a\rangle|b\rangle \quad &\rightarrow_{H^{\otimes 2}} \quad \frac{|0\rangle+(-1)^a|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+(-1)^b|1\rangle}{\sqrt{2}} = \\
&= \quad (|00\rangle+(-1)^a|10\rangle+(-1)^b|01\rangle+(-1)^{a+b}|11\rangle)/2 \\
&\rightarrow_{\text{cnot}} \quad (|00\rangle+(-1)^a|11\rangle+(-1)^b|01\rangle+(-1)^{a+b}|10\rangle)/2 \\
&= \quad (|00\rangle+(-1)^{a+b}|10\rangle+(-1)^b|01\rangle+(-1)^{(a+b)+b}|11\rangle)/2 \\
&= \quad H^{\otimes 2}|a+b\rangle|b\rangle \quad \rightarrow_{H^{\otimes 2}} \quad |a+b\rangle|b\rangle.
\end{aligned}
$$

Parity and fan-out

Def. *fan-out* is controlled-not-not-. . . -not.



Recall that:

- Hadamard gates change the direction of cnot.
- Two applications of H cancel each other, i.e. $H^2 = I$.

Classically, we need logarithmic depth!

Constant-depth circuits **with fan-out**

- any *commuting* gates can be applied *in parallel*,
  if we can efficiently change into their *diagonal basis*

- [Moore, 1999] mod[q] exactly in constant depth

- [Høyer & Špalek, 2003] constant-depth approximations
  with polynomially small error:
  - And, Or, exact[q], threshold[t], counting,
  - arithmetics, sorting,
  - quantum Fourier transform.

Classically, we need logarithmic depth even **with parity**, except for:
or and and can be approximated with error $\frac{1}{n}$ in depth $\mathrm{O}(\log\log n)$.

Exponential speedup

[Shor, 1994] *factoring* and *discrete-log* in polynomial time.
Uses modular exponentiation and quantum Fourier transform.

Further results:

- [Cleve & Watrous, 2000] quantum circuit of logarithmic depth + classical poly-time randomised algorithm
- [Høyer & Špalek, 2003] constant-depth quantum circuit **with fan-out** + classical poly-time randomised algorithm
- generalised to *hidden subgroup problem* for some groups

Quantum search

[Grover, 1996] searching n *unsorted records* in time $\mathrm{O}(\sqrt{n})$.

Further results:

- finding minimum in the same time
- *amplitude amplification* (compare with *probability amplification*):
  - assume a subroutine with success prob. ε
  - can amplify the prob. to $\Theta(1)$ in $\mathrm{O}(\sqrt{\frac{1}{\varepsilon}})$ iterations
  - classically we need $\mathrm{O}(\frac{1}{\varepsilon})$ iterations
- can do it exactly