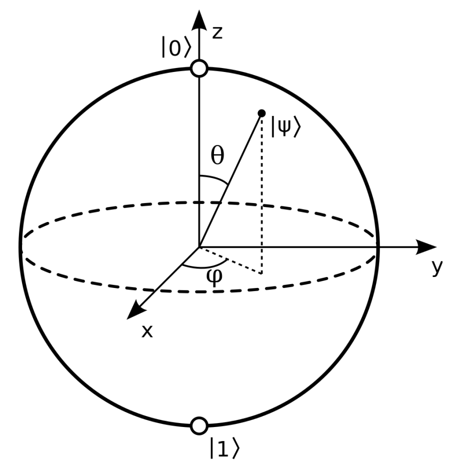
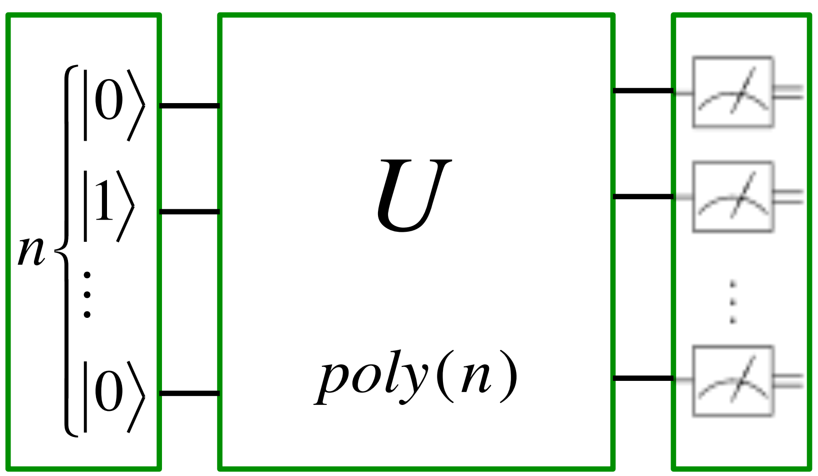
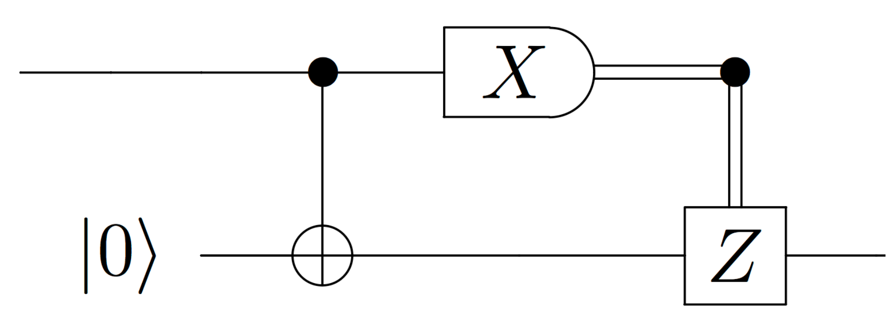


Introduction to quantum computation and simulability

Daniel J. Brod (UFF)
Leandro Aolita (UFRJ/ICTP-SAIFR)
<u>Ernesto F. Galvão (UFF)</u>

Instituto de Física
Universidade Federal Fluminense





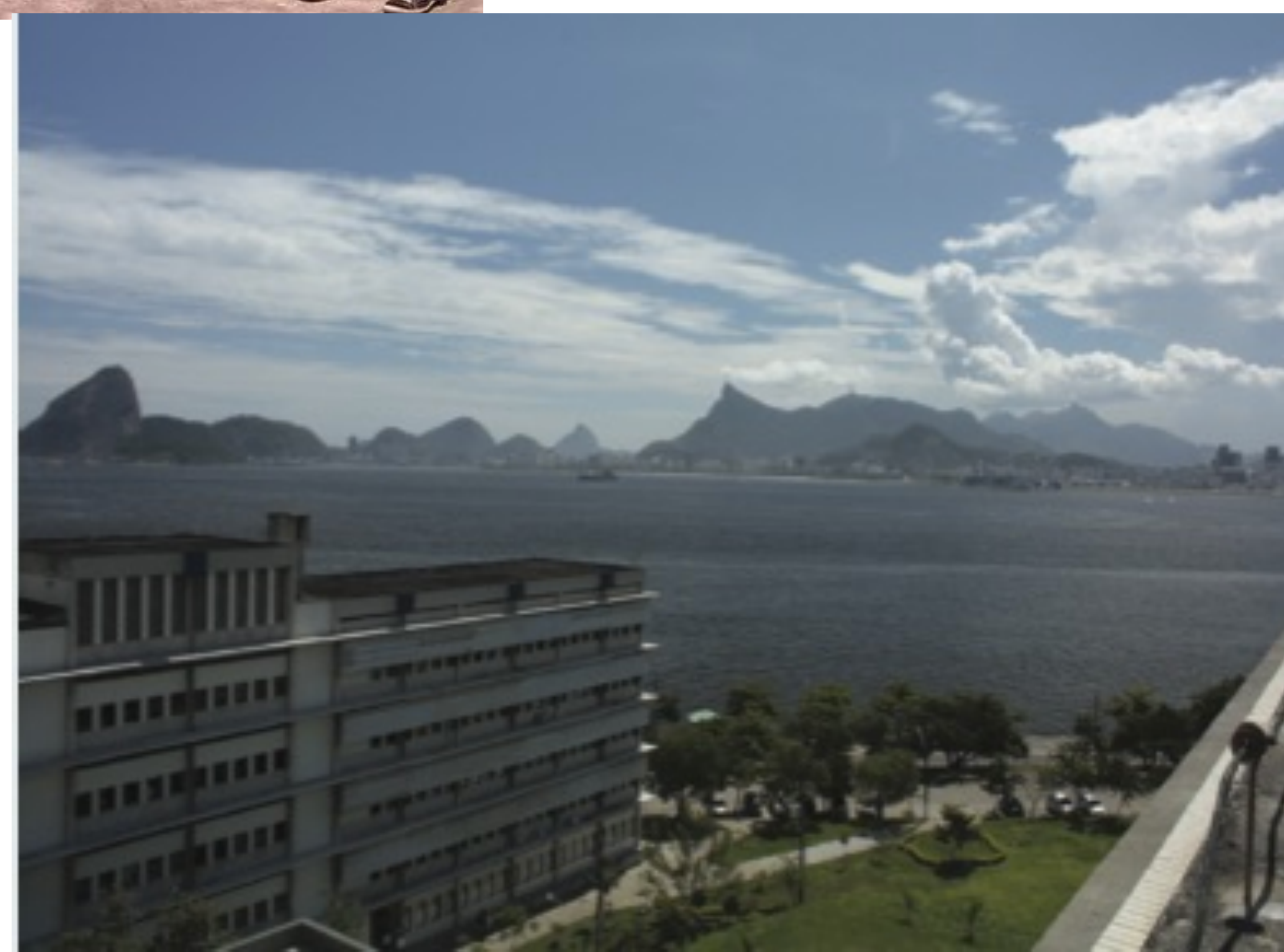
ICTP/SAIFR-IFT/UNESP, October 15th-19th, 2018

Quantum Optics and Quantum Information group

INSTITUTO DE FÍSICA
Universidade Federal Fluminense

Niterói, across the bay from Rio de Janeiro

View from the Physics building:



Quantum Optics and Quantum Information group

Instituto de Física
Universidade Federal Fluminense

Research:

1- Quantum optics for quantum information
Antonio Zelaquett Khoury, Carlos Eduardo R. de Souza,
Kaled Dechoum, Daniel T. Schneider

2- Foundations of quantum computation
Daniel Brod, Daniel Jonathan, Ernesto F. Galvão

3- Interface between condensed matter physics and q. information
Marcelo Sarandy, Thiago R. de Oliveira, Mohammad Rajabpour

Lecture 2 : Introduction to the circuit model

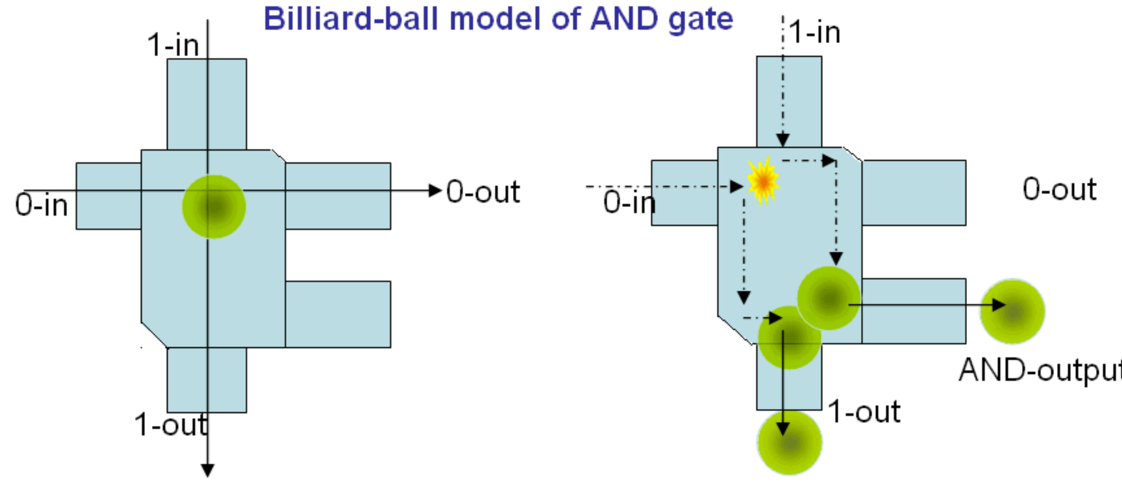
Outline:

- Introduction: computational models
- Circuit model
  - Bloch sphere and one-qubit gates
  - Two qubit gates
  - Computational basis preparation and measurement
  - Universal gate sets – approximating unitaries
- Clifford circuits
  - Groups of unitaries: Pauli and Clifford groups
  - Simulability of Clifford circuits
  - Upgrading Clifford circuits to universal QC
- Introduction to restricted models of QC
  - Weak and strong simulation

- For slides and links to related material, see https://sites.google.com/view/intro-qc-simulability/home

Models for quantum computation

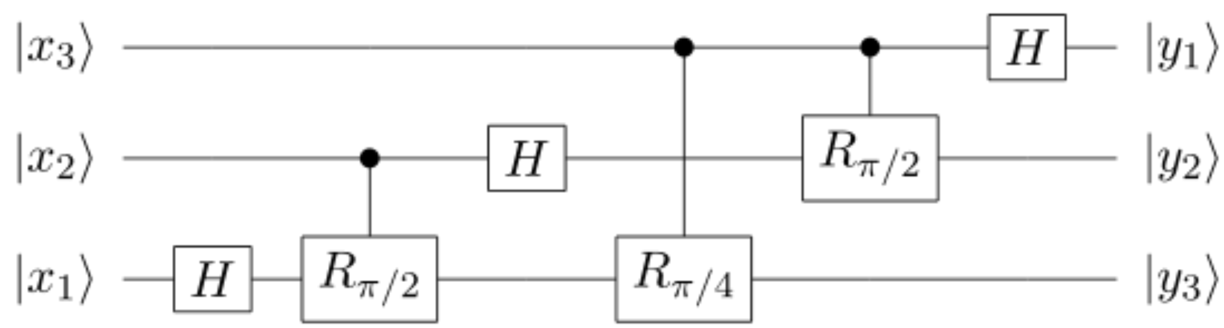
- A **computational model** is a mathematical model allowing for computation
  Examples: Turing machines, gate arrays (circuits), lambda calculus, billiard-ball computing, cellular automata



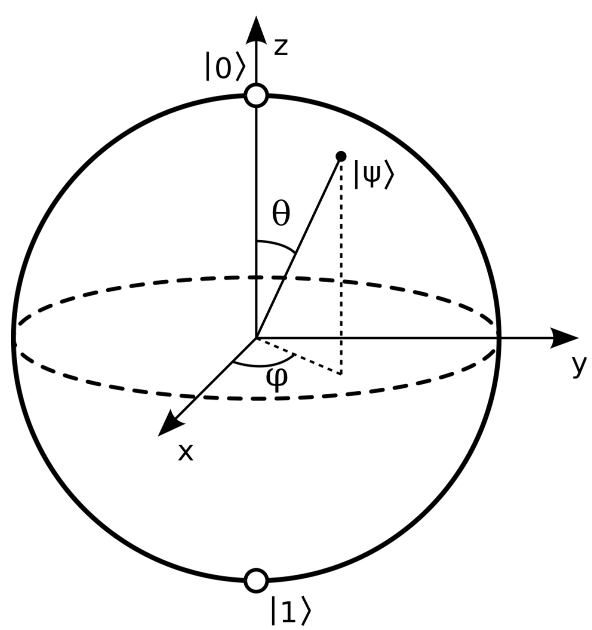
- There are many models for quantum computation
- Presumed to be equivalent (Church-Turing-Deutsch Principle)
- Differences result in
  - conceptual insights on QM
  - important practical differences in implementations

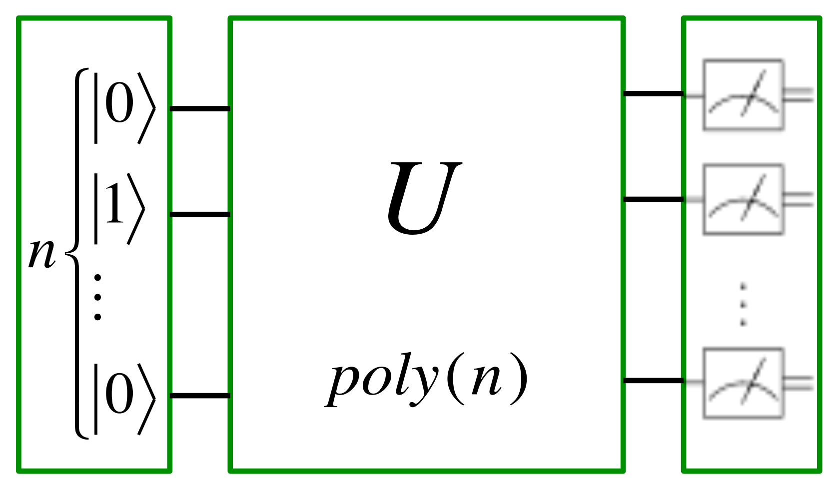
- Main models for universal quantum computation:

- Circuit model
- Measurement-based models
- Adiabatic quantum computation
- Topological quantum computation



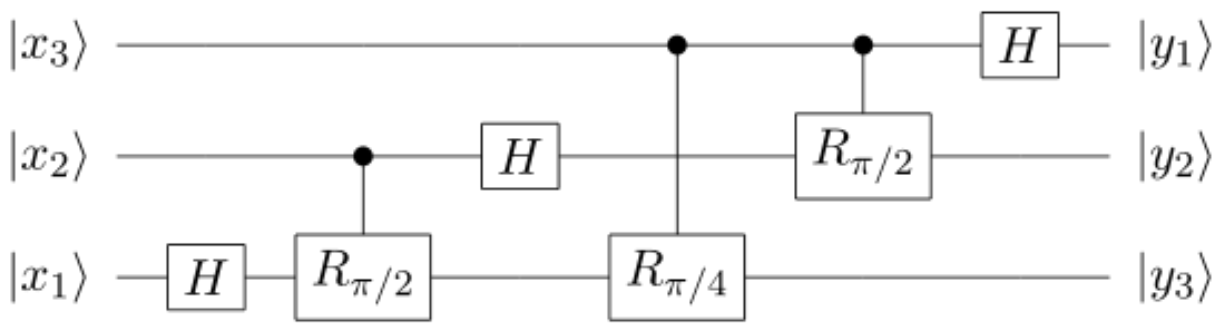
Basics of the circuit model



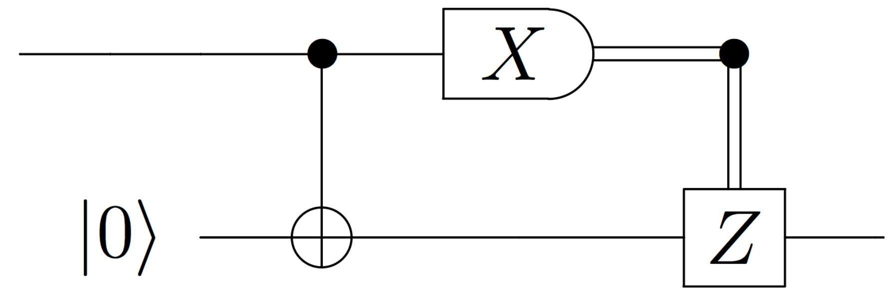


Basics of the circuit model

- The most well-known model for quantum computation is the circuit model, obtained in analogy with classical circuits

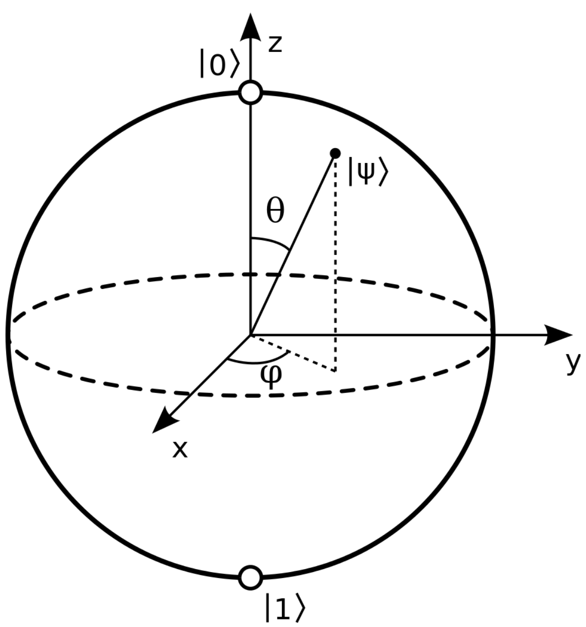


3-qubit QFT

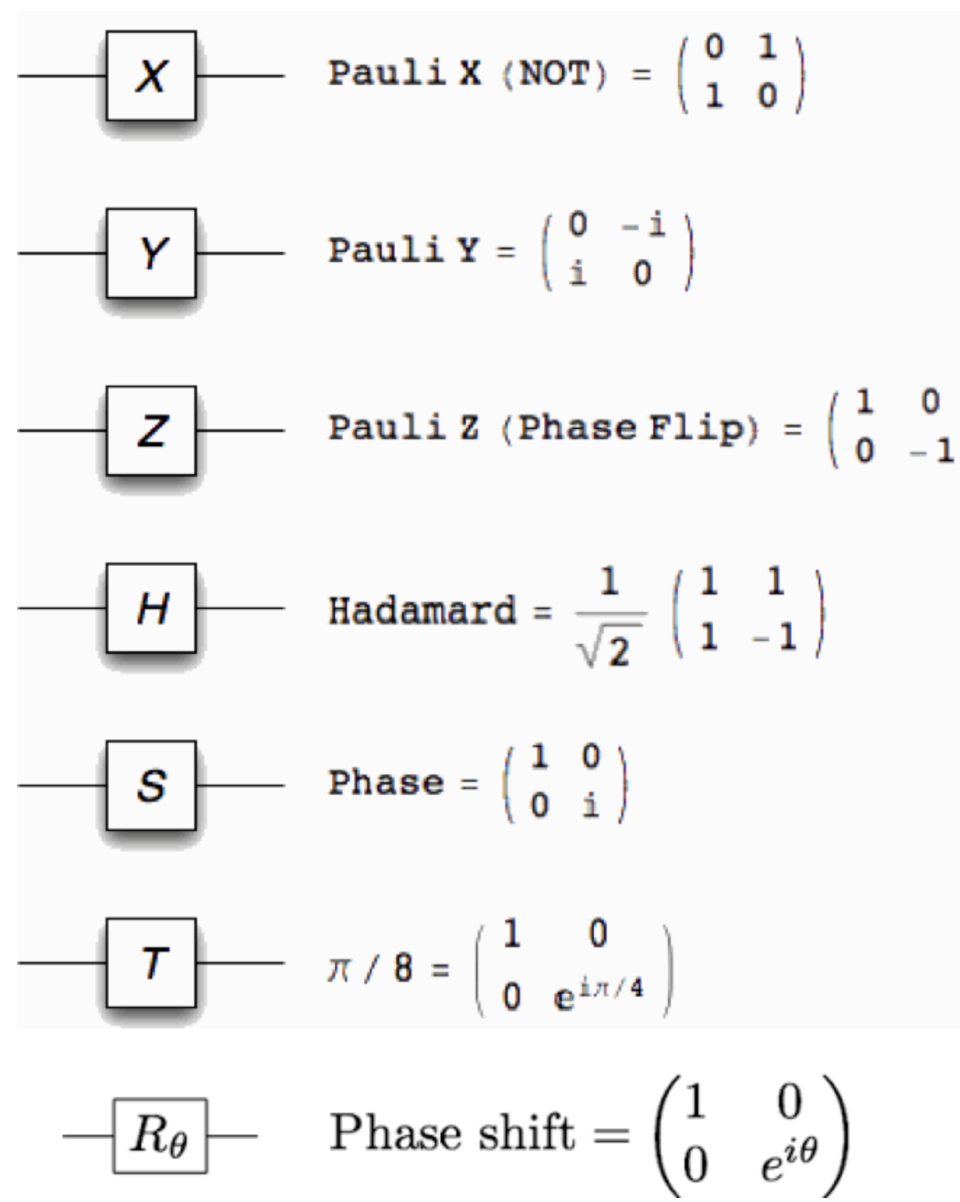


1-bit Z teleportation

- wires = qubits (i.e. 2-level systems)
- little boxes = single-qubit gates

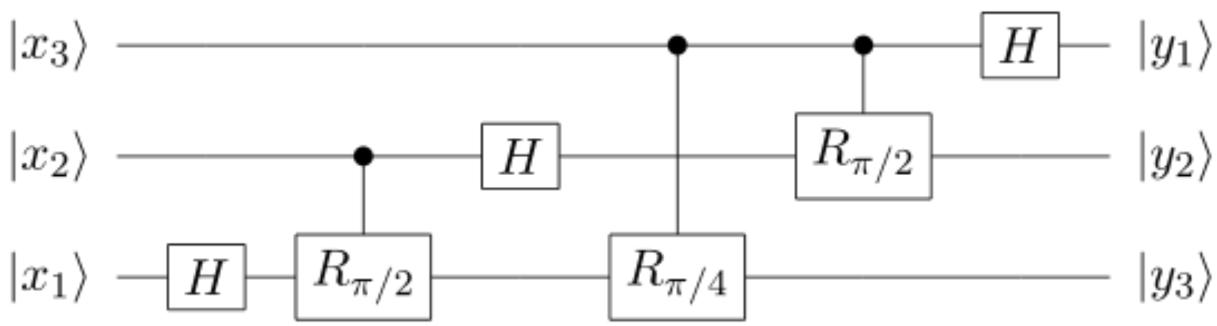


$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$

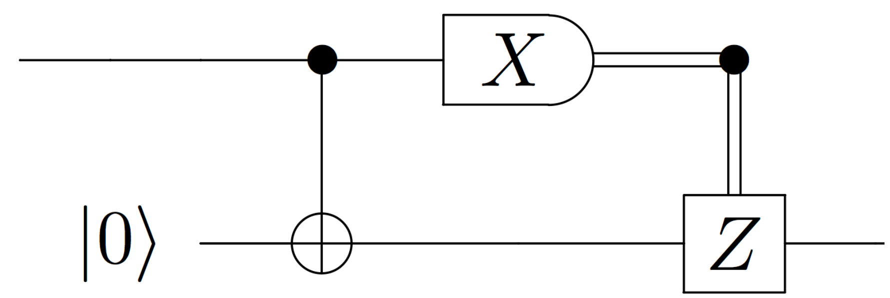


Basics of the circuit model

- The most well-known model for quantum computation is the circuit model, obtained in analogy with classical circuits

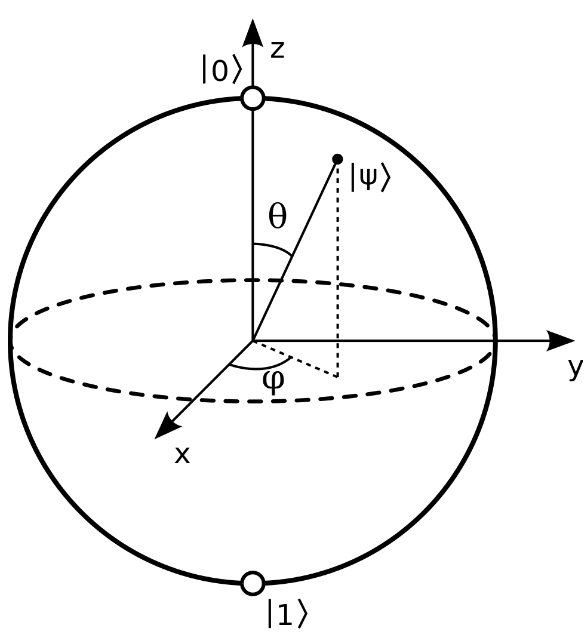


3-qubit QFT



1-bit Z teleportation

- wires = qubits (i.e. 2-level systems)
- little boxes = single-qubit gates



$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$

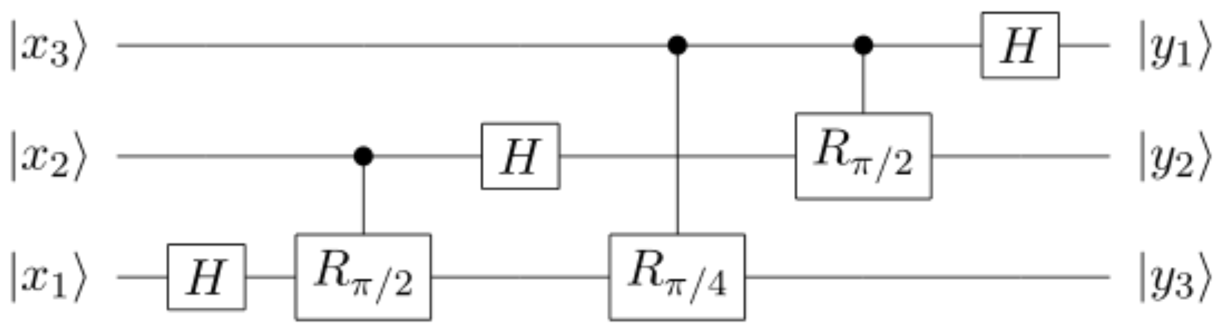
- Any single-qubit unitary is a rotation of the Bloch sphere

$$U = \exp(i\alpha) R_{\hat{n}}(\theta)$$

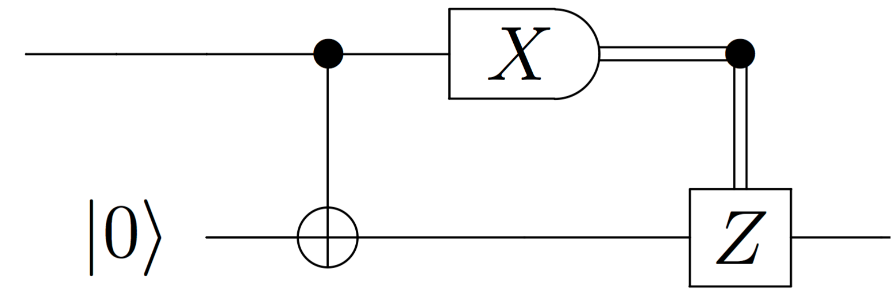
$$R_{\hat{n}}(\theta) \equiv \exp\left(\frac{-i\hat{n}\cdot\vec{\sigma}}{2}\right) = \cos(\theta/2)I - i\sin(\theta/2)(n_x X + n_y Y + n_z Z)$$

Basics of the circuit model

- The most well-known model for quantum computation is the circuit model, obtained in analogy with classical circuits

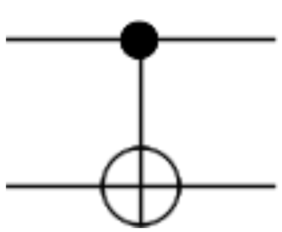


3-qubit QFT

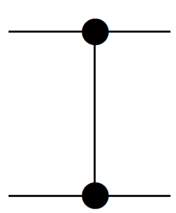


1-bit Z teleportation

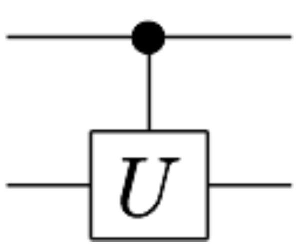
- Two-qubit gates:



$$= \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



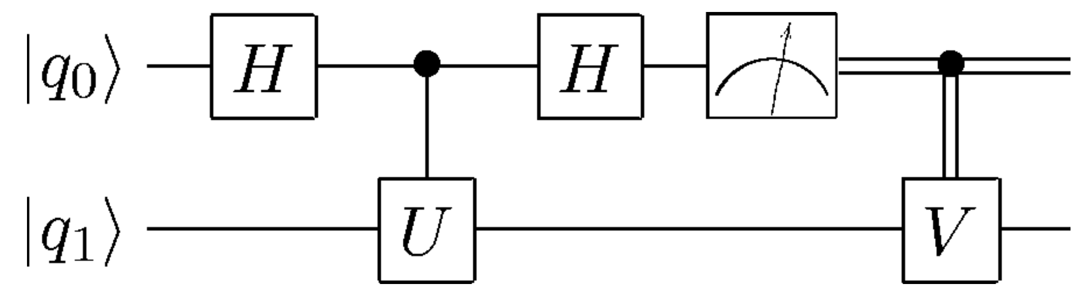
$$= \text{Controlled-}Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$



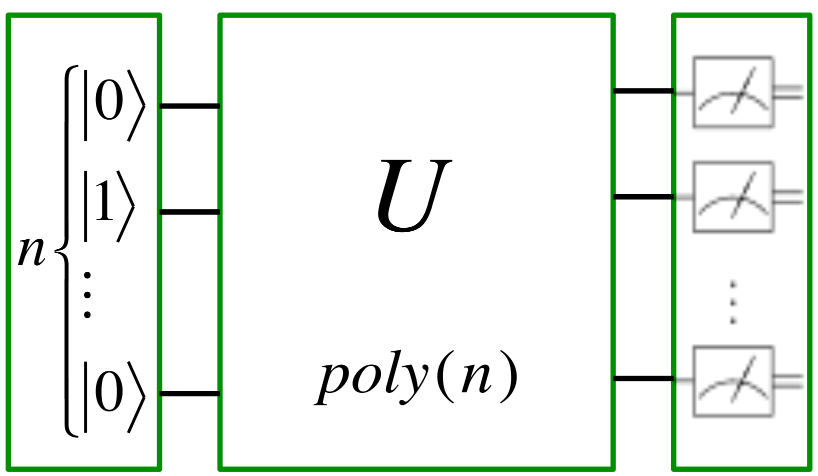
$$= \text{Controlled-U} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha & \beta \\ 0 & 0 & \gamma & \delta \end{pmatrix}$$

Measurement bases

- What about the final measurements?
  Convention: Z, or computational, basis
  $$\{|0\rangle, |1\rangle\}$$



- Sometimes we allow for unitaries being applied conditionally on the result of a measurement

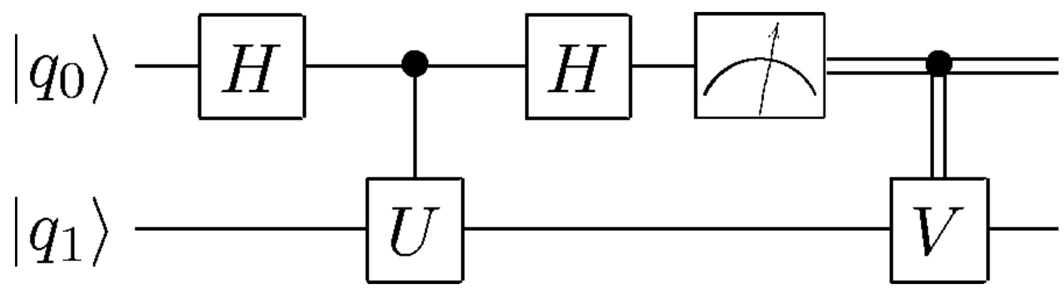


- What if we change the output measurement?

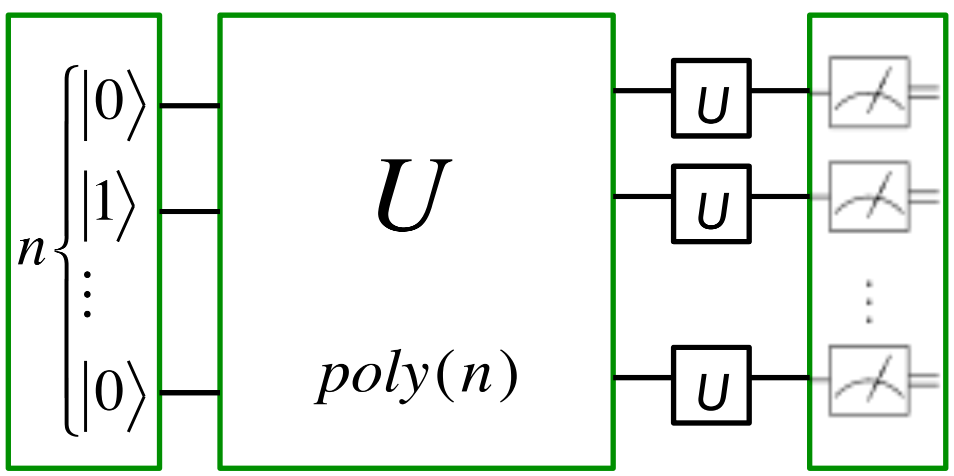
Measurement bases

- What about the final measurements?
  Convention: Z, or computational, basis

$$\{|0\rangle, |1\rangle\}$$



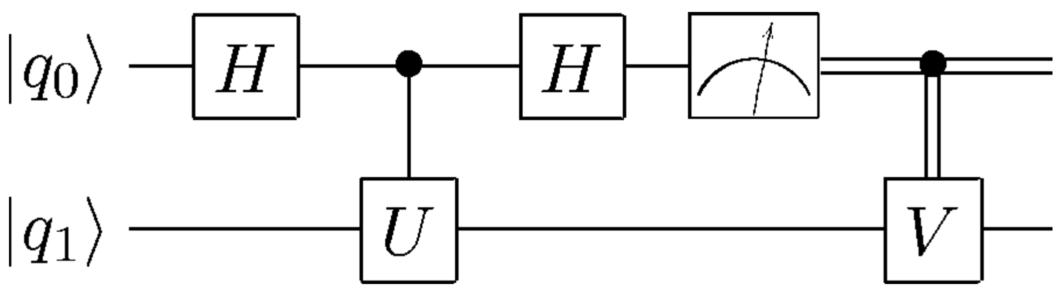
- Sometimes we allow for unitaries being applied conditionally on the result of a measurement



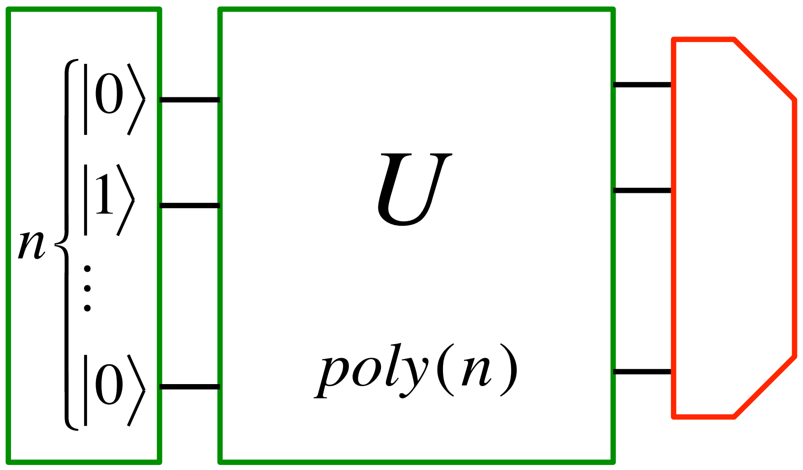
- What if we change the output measurement? Single-qubit measurements are OK…

Measurement bases

- What about the final measurements?
  Convention: Z, or computational, basis
  $$\{|0\rangle, |1\rangle\}$$



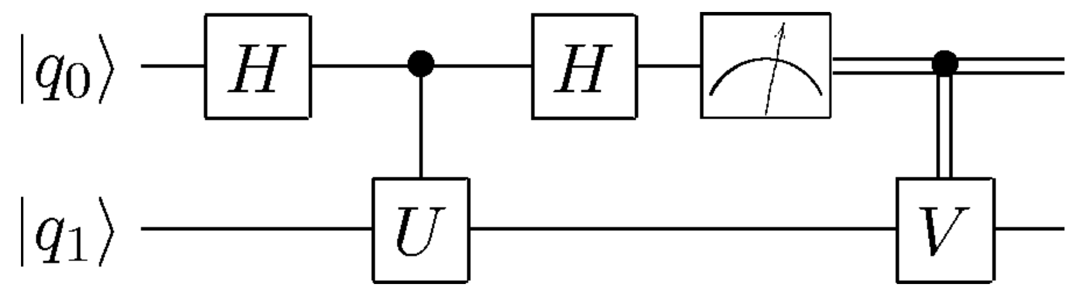
- Sometimes we allow for unitaries being applied conditionally on the result of a measurement



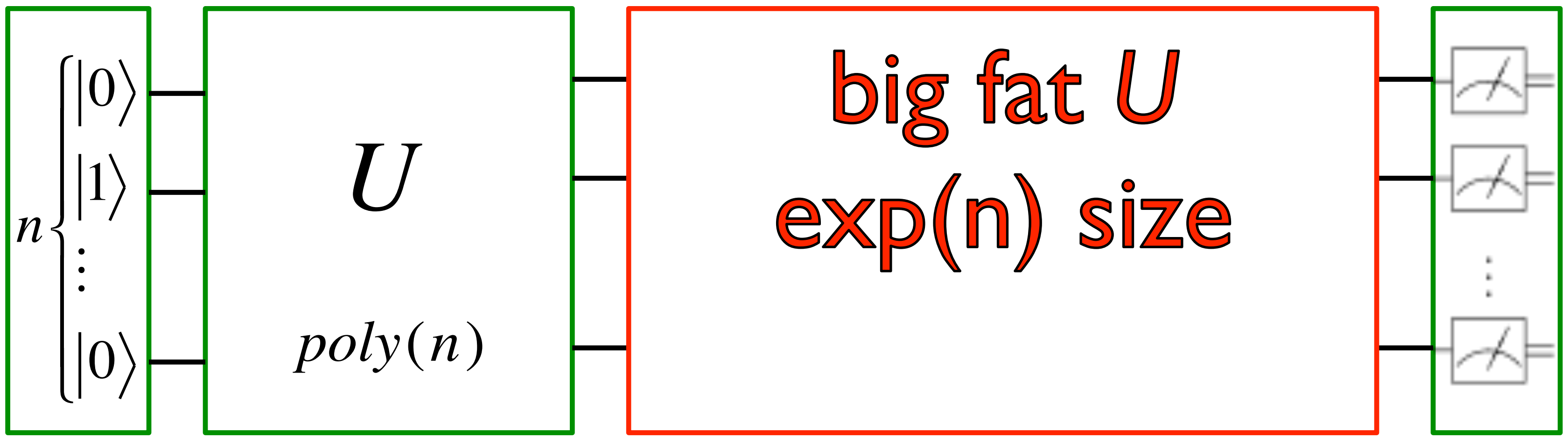
- What if we change the output measurement? Single-qubit measurements are OK…
  …but arbitrary global measurements are not OK.

Measurement bases

- What about the final measurements?
  Convention: Z, or computational, basis
  $$\{|0\rangle, |1\rangle\}$$



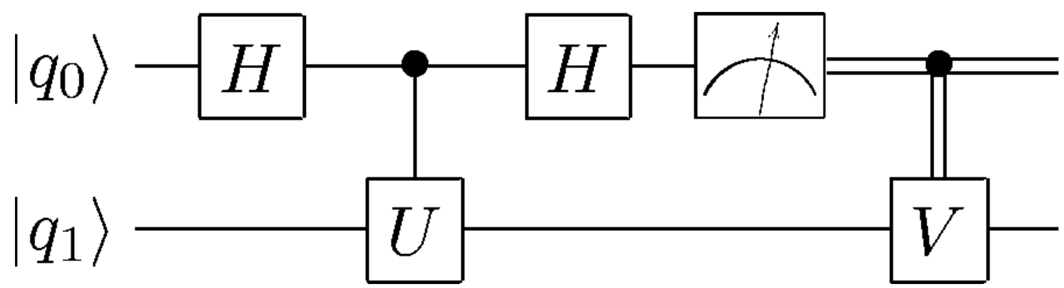
- Sometimes we allow for unitaries being applied conditionally on the result of a measurement



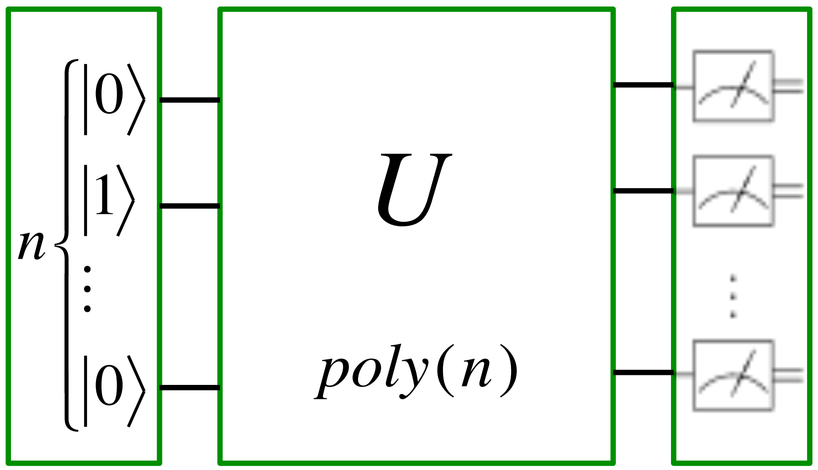
- What if we change the output measurement? Single-qubit measurements are OK… …but arbitrary global measurements are not OK.

Measurement bases

- What about the final measurements?
  Convention: Z, or computational, basis
  $$\{|0\rangle, |1\rangle\}$$



- Sometimes we allow for unitaries being applied conditionally on the result of a measurement

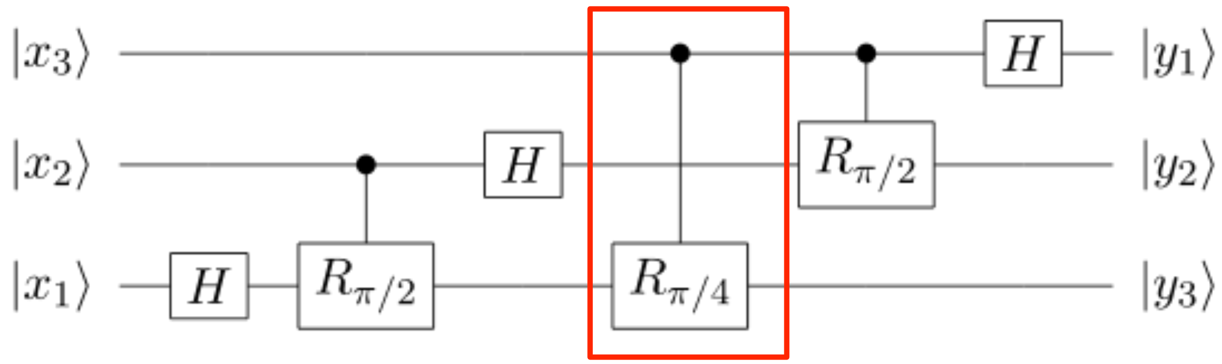


- What if we change the output measurement? Single-qubit measurements are OK…
  …but arbitrary global measurements are not OK.

- So let's stick to computational basis measurements

Approximating unitaries

- How can we approximate unitaries with a limited set of gates?



- Intuition: approximating a 2D rotation using multiple applications of a single rotation

- Many ways to approximate any U on n qubits. The standard set is:

$$\{H, T, S, CNOT\}$$

- Proof steps:
  1. Any unitary on n qubits can be decomposed exactly with single-qubit unitaries +CNOTs
  2. Any single-qubit unitary can be arbitrarily well-approximated using H, T gates only.

Approximating unitaries – Solovay-Kitaev theorem

- It's possible to approximate n-qubit unitaries with any universal set of gates, such as the standard set $\{H, T, S, CNOT\}$

- How efficient can the approximation be?

Solovay-Kitaev theorem:

Assume universal gate set G, in which each gate is accompanied by its inverse. I want an approximation (*n* fixed) with accuracy ε. This can be done with gate sequence of length $O\left(\log^c(1/\varepsilon)\right), c \approx 3.97$

Additionally: classical compilation time is $O\left(\log^{2.71}(1/\varepsilon)\right)$

- This is exponentially faster than naïve approximation

- Moreover, error of concatenation of *m* approximations increases linearly with *m* (benign scaling)

Other universal gate-sets

- Here are a few different sets of universal gates:

$$1.\{H, T, S, CNOT\}$$

$$2.\{\text{almost any two-qubit gate}\}$$

[Deutsch *et al.*, Proc. R. Soc. London A 449 (1937), 669 (1995)]
[Lloyd, PRL 75(2), 346 (1995)]

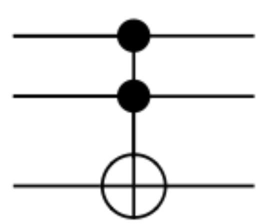
$$3.\{matchgates, SWAP\}$$

[Jozsa, Miyake Proc. R. Soc. London A 464, 3089 (2008)]

[Shi, quant-ph/0205115]

$$4.\{Toffoli, H\}$$

$Toffoli =$



$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

What's curious about this gate set?

- **Encoded universality**: all unitaries on logical qubits can be approximated (even if not on physical qubits). Example:

[DiVincenzo *et al.*, Nature 408, 339 (2000)]

5.{Exchange interaction}:

$$H = \sum_{i \neq j} J_{ij} (X_i \otimes X_j + Y_i \otimes Y_j + Z_i \otimes Z_j)$$

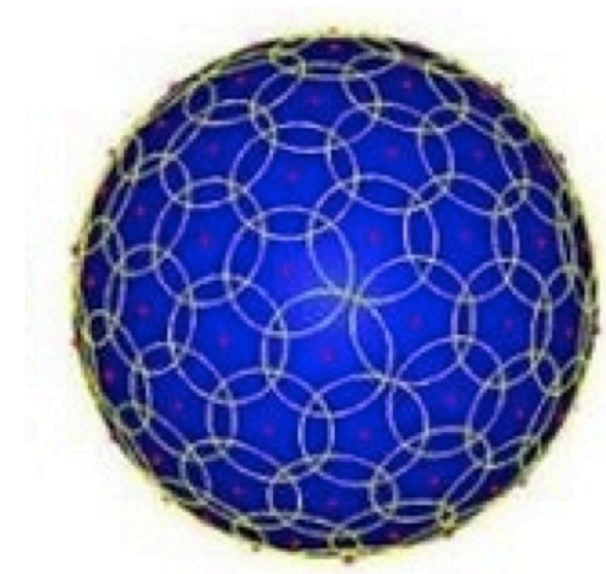
Logical qubits:

$$|0_L\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |100\rangle)$$

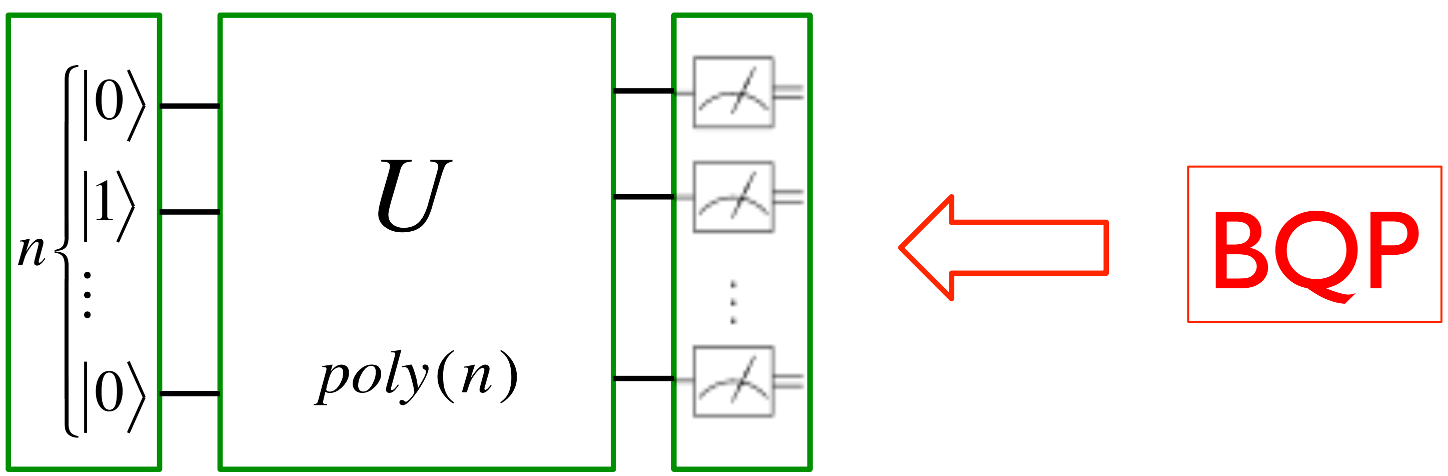
$$|1_L\rangle = \sqrt{2/3}\,|001\rangle - \sqrt{1/6}\,|010\rangle - \sqrt{1/6}\,|100\rangle$$

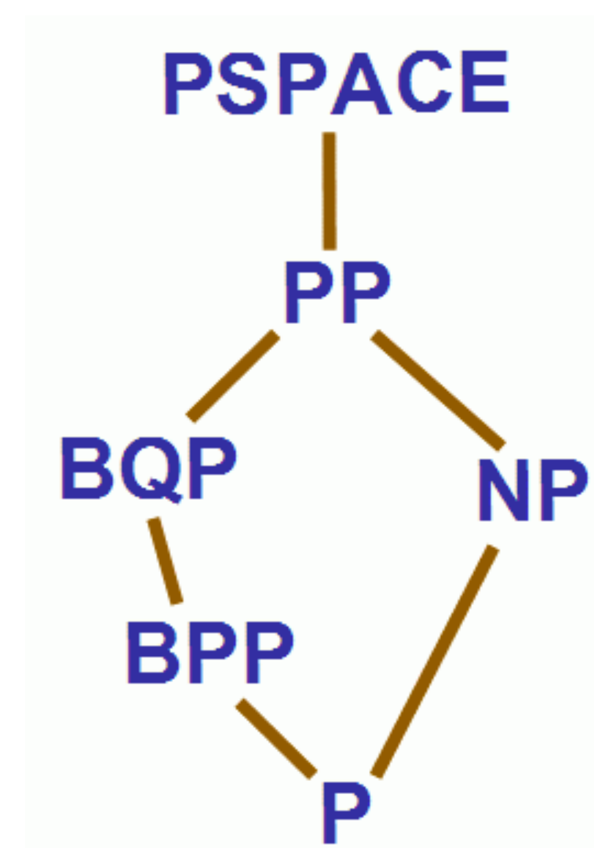
BQP

- It can be shown that generic unitaries require an **exponential number** of two-qubit gates to approximate
  - counting argument using epsilon-net of *n*-qubit states

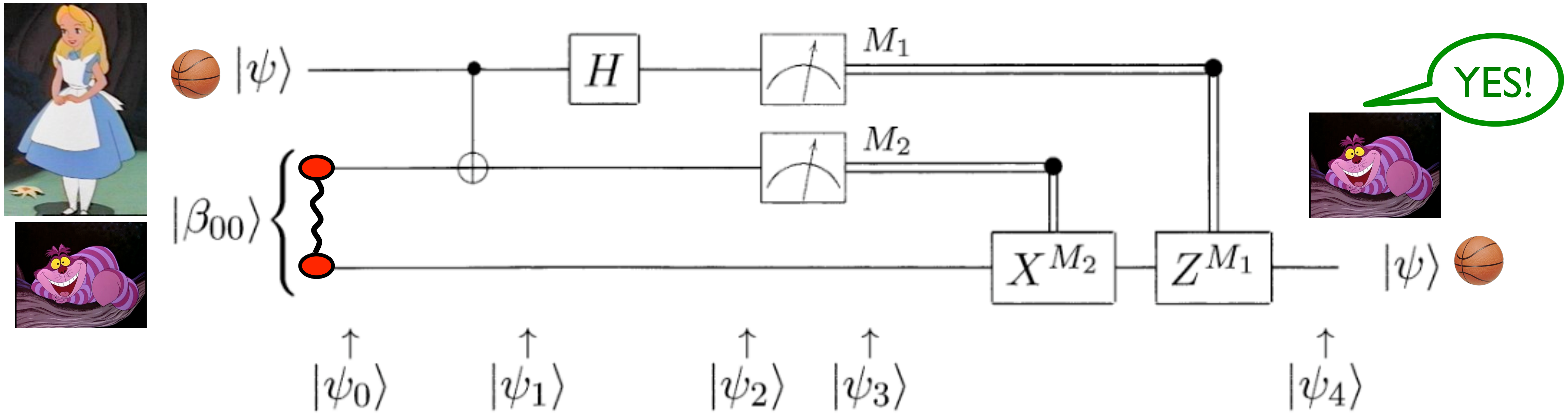


- Problems solvable with high probability by a polynomial-sized circuit (in *n*=input size) define complexity class **BQP**
  (bounded error, quantum polynomial time)





Quantum teleportation as a circuit



Quantum algorithms

Algorithms achieving **superpolinomial speed-up**:

- Factoring (Shor 1994)
  - Factor n-bit integer in $O(n^3)$ steps, against $O(e^{n^{1/3}\log(n)^{2/3}})$ on classical computer
  - used to break RSA cryptosystem
  - Mathematically: solving hidden Abelian subgroup problem

- Solution of linear system of equations (Harrow 2008)
  - Find approximate solution of Ax=b, with A being a n x n matrix. It takes O(log(n)) steps, against O(n) classically.

- Simulating quantum systems (Feynman 1982, Abrams/Lloyd 1997, etc.)
  - Simulation of physically reasonable Hamiltonians using n qubits in poly(n) steps.

- Calculating partition functions of classical systems (Lidar/Biham 1997, Aharonov et al. 2007)

- Various problems involving groups and rings.

Quantum algorithms

Algorithms with polynomial speed-up:

- Unstructured database search (Grover 1996)
    - Finds marked item in $O(\sqrt{n})$ queries, agains O(n) classically.
    - Conceptually important for other algorithms.

- Various graph properties

- Gradient search for minimum (Bulger 2005, Jordan 2008)