Quantum Logic

Marek Perkowskki
Sources

Origin of slides: John Hayes, Peter Shor, Martin Lukac, Mikhail Pivtoraiko, Alan Mishchenko, Pawel Kerntopf, Mosca, Ekert

Lee Spector
in collaboration with
Herbert J. Bernstein, Howard Barnum, Nikhil Swamy
{lSpector, hbernstein, hBarnum, nikhil_swamy}@hampshire.edu

School of Cognitive Science, School of Natural Science
Institute for Science and Interdisciplinary Studies (ISIS)
Hampshire College
Introduction

• Short-Term Objectives

Introduce Quantum Computing Basics to interested students at KAIST. Especially non-physics students

• Long-Term Objectives

Engage into AI/CS/Math Research projects benefiting from Quantum Computing. Continue our previous projects in quantum computing

• Prerequisite

- No linear algebra or quantum mechanics assumed
- A ECE, math, physics or CS background would be beneficial, practically-oriented class.
Introduction

• Main Textbook

Quantum Computation & Quantum Information

Michael A. Nielsen
Isaac L. Chuang

ISBN: 0 521 63503 9
Paperback
ISBN: 0 521 63235 8 Hardback

Cost: $48.00 New Paperback
$35.45 Used Paperback

(http://www.amazon.com)
also in KAIST bookstore
Presentation Overview

Qubits
1 Qubit -> Bloch Sphere,
2 Qubits -> Bell States,
 n Qubits

Quantum Computation
Gates: Single Qubit, Arbitrary Single Qubit -> Universal Quantum Gates, Multiple Qubit Gates -> CNOT
Other Computational Bases

Quantum Circuits
Qubit Swap Circuit
Qubit Copying Circuit
Bell State Circuit -> Quantum Teleportation

Quantum Algorithms
Toffoli Gate -> Quantum Parallelism -> Hadamard Transform
Deutsch's Algorithm, Deutsch-Josa Algorithm
Other Algorithms
- Fourier Transform, Quantum Search, Quantum Simulation

Quantum Information Processing
Stern-Gerlach, Optical Techniques, Traps, NMR, Quantum Dots
Historical Background and Links

Quantum Computation & Quantum Information

Study of information processing tasks that can be accomplished using quantum mechanical systems

- Quantum Mechanics
- Computer Science
- Cryptography
- Information Theory
- Digital Design
- Computer Science
- Information Theory
- Digital Design
What will be discussed?

- Background
- Quantum circuits synthesis and algorithms
- Quantum circuits simulation
- Quantum Computation
- AI for quantum computation
- Quantum computation for AI
- Quantum logic emulation and evolvable hardware
- Quantum circuits verification
- Quantum-based robot control
What is quantum computation?

- Computation with **coherent atomic-scale dynamics**.
- The behavior of a quantum computer is governed by the laws of quantum mechanics.
Why bother with quantum computation?

- **Moore’s Law**: We hit the quantum level 2010~2020.
- Quantum computation is more powerful than classical computation.
- More can be computed in less time—the complexity classes are different!
The power of quantum computation

- In quantum systems possibilities count, even if they never happen!
- Each of exponentially many possibilities can be used to perform a part of a computation at the same time.
“No, you’re not going to be able to understand it. . . . You see, my physics students don’t understand it either. That is because I don’t understand it. Nobody does. ... The theory of quantum electrodynamics describes Nature as absurd from the point of view of common sense. And it agrees fully with an experiment. So I hope that you can accept Nature as She is -- absurd.

Richard Feynman
Absurd but taken seriously (not just quantum mechanics but also quantum computation)

- Under active investigation by many of the top physics labs around the world (including CalTech, MIT, AT&T, Stanford, Los Alamos, UCLA, Oxford, l’Université de Montréal, University of Innsbruck, IBM Research . . .)
- In the mass media (including The New York Times, The Economist, American Scientist, Scientific American, . . .)
- Here.
Quantum Logic Circuits
Half of the photons leaving the light source arrive at detector A; the other half arrive at detector B.
The simplest explanation is that the beam-splitter acts as a classical coin-flip, randomly sending each photon one way or the other.
An interferometer

Equal path lengths, rigid mirrors.
Only one photon in the apparatus at a time.
All photons leaving the source arrive at B.
WHY?
Possibilities count

- There is a quantity that we’ll call the “amplitude” for each possible path that a photon can take.
- The amplitudes can interfere constructively and destructively, even though each photon takes only one path.
- The amplitudes at detector A interfere destructively; those at detector B interfere constructively.
Calculating interference

- Arrows for each possibility.
- Arrows rotate; speed depends on frequency.
- Arrows flip 180° at mirrors, rotate 90° counter-clockwise when reflected from beam splitters.
- Add arrows and square the length of the result to determine the probability for any possibility.
Double slit interference
Quantum Interference: Amplitudes are added and not intensities!

Figure 1: Two-slit experiment.
Interference in the interferometer
Quantum Interference

The simplest explanation must be wrong, since it would predict a 50-50 distribution.
More experimental data

\[ \sin^2\left(\frac{\varphi}{2}\right) \]

\[ \cos^2\left(\frac{\varphi}{2}\right) \]
A new theory

The particle can exist in a linear combination or superposition of the two paths

\[ \frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \]
\[ \frac{i}{\sqrt{2}}|0\rangle + \frac{e^{i\phi}}{\sqrt{2}}|1\rangle \]
\[ \frac{e^{i\phi} - 1}{2}|0\rangle + \frac{i(e^{i\phi} + 1)}{\sqrt{2}}|1\rangle \]
If the photon is measured when it is in the state \( \alpha_0 |0\rangle + \alpha_1 |1\rangle \) then we get \( |0\rangle \) with probability \( |\alpha_0|^2 \) and \( |1\rangle \) with probability of \( |\alpha_1|^2 \)

\[ |\alpha_0|^2 + |\alpha_1|^2 = 1 \]
Quantum Operations

The operations are induced by the apparatus *linearly*, that is, if

\[ |0\rangle \rightarrow \frac{i}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \]

and

\[ |1\rangle \rightarrow \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} |1\rangle \]

then

\[ \alpha_0 |0\rangle + \alpha_1 |1\rangle \rightarrow \alpha_0 \left( \frac{i}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) + \alpha_1 \left( \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} |1\rangle \right) \]

\[ = \left( \alpha_0 \frac{i}{\sqrt{2}} + \alpha_1 \frac{1}{\sqrt{2}} \right) |0\rangle + \left( \alpha_0 \frac{1}{\sqrt{2}} + \alpha_1 \frac{i}{\sqrt{2}} \right) |1\rangle \]
Any linear operation that takes states
\[ \alpha_0 |0\rangle + \alpha_1 |1\rangle \] satisfying
\[ |\alpha_0|^2 + |\alpha_1|^2 = 1 \]
and maps them to states
\[ \alpha_0' |0\rangle + \alpha_1' |1\rangle \] satisfying
\[ |\alpha_0'|^2 + |\alpha_1'|^2 = 1 \]
must be **UNITARY**
Linear Algebra

\[ U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \]

is unitary if and only if

\[ UU^\dagger = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} u^*_{00} & u^*_{10} \\ u^*_{01} & u^*_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \]
\[ |0\rangle \text{ corresponds to } \begin{pmatrix} 1 \\ 0 \end{pmatrix} \]

\[ |1\rangle \text{ corresponds to } \begin{pmatrix} 0 \\ 1 \end{pmatrix} \]

\[ \alpha_0|0\rangle + \alpha_1|1\rangle \text{ corresponds to } \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \]
corresponds to \[
\begin{pmatrix}
i & 1 \\
\sqrt{2} & \sqrt{2} \\
1 & i \\
\sqrt{2} & \sqrt{2}
\end{pmatrix}
\]

\[
\begin{pmatrix}1 & 0 \\
0 & e^{i\varphi}
\end{pmatrix}
\]
corresponds to

$$\begin{pmatrix} i & 1 \\ \sqrt{2} & \sqrt{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{pmatrix} i & 1 \\ \sqrt{2} & \sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
Abstraction

The two position states of a photon in a Mach-Zehnder apparatus is just one example of a quantum bit or qubit.

Except when addressing a particular physical implementation, we will simply talk about “basis” states $|0\rangle$ and $|1\rangle$ and unitary operations like

\[
\begin{align*}
\text{H} \quad \text{and} \quad \varphi
\end{align*}
\]
where $H$ corresponds to
\[
\begin{pmatrix}
1 & 1 \\
\sqrt{2} & \sqrt{2} \\
1 & -1 \\
\sqrt{2} & \sqrt{2}
\end{pmatrix}
\]
and $\varphi$ corresponds to
\[
\begin{pmatrix}
1 & 0 \\
0 & e^{i\varphi}
\end{pmatrix}
\]
An arrangement like

\[ 0 \]

is represented with a network like

\[ |0\rangle - H - \phi - H \]
More than one qubit

If we concatenate two qubits

$$(\alpha_0|0\rangle + \alpha_1|1\rangle) (\beta_0|0\rangle + \beta_1|1\rangle)$$

we have a 2-qubit system with 4 basis states

$|0\rangle|0\rangle = |00\rangle \quad |0\rangle|1\rangle = |01\rangle \quad |1\rangle|0\rangle = |10\rangle \quad |1\rangle|1\rangle = |11\rangle$

and we can also describe the state as

$$\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

or by the vector

$$\begin{pmatrix} 
\alpha_0\beta_0 \\
\alpha_0\beta \\
\alpha_1\beta_0 \\
\alpha_1\beta_1 
\end{pmatrix} = \begin{pmatrix} 
\alpha_0 \\
\alpha_1 \\
\beta_0 \\
\beta_1 
\end{pmatrix} \otimes \begin{pmatrix} 
\alpha_0 \\
\beta_0 \\
\alpha_1 \\
\beta_1 
\end{pmatrix}$$
More than one qubit

In general we can have arbitrary superpositions

\[ \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle \]

\[ |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \]

where there is no factorization into the tensor product of two independent qubits. These states are called entangled.
Entanglement

• Qubits in a multi-qubit system are not independent—they can become “entangled.”

• To represent the state of n qubits we use $2^n$ complex number amplitudes.
Measuring multi-qubit systems

If we measure both bits of

\[ \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle \]

we get \( |x\rangle|y\rangle \) with probability \( |\alpha_{xy}|^2 \)
Measurement

• $\sum |\alpha|^2$, for amplitudes of all states matching an output bit-pattern, gives the probability that it will be read.

• Example:

\[
0.316|00\rangle + 0.447|01\rangle + 0.548|10\rangle + 0.632|11\rangle
\]

– The probability to read the rightmost bit as 0 is $|0.316|^2 + |0.548|^2 = 0.4$

• Measurement during a computation changes the state of the system but can be used in some cases to increase efficiency (measure and halt or continue).
Classical Versus Quantum
**Classical vs. Quantum Circuits**

- **Goal:** Fast, low-cost implementation of useful algorithms using standard components (gates) and design techniques

- **Classical Logic Circuits**
  - Circuit behavior is governed implicitly by classical physics
  - Signal states are simple bit vectors, e.g. \( X = 01010111 \)
  - Operations are defined by Boolean Algebra
  - No restrictions exist on copying or measuring signals
  - Small well-defined sets of universal gate types, e.g. \{NAND\}, \{AND,OR,NOT\}, \{AND,NOT\}, etc.
  - Well developed CAD methodologies exist
  - Circuits are easily implemented in fast, scalable and macroscopic technologies such as CMOS
Quantum Logic Circuits

- Circuit behavior is governed explicitly by quantum mechanics
- Signal states are vectors interpreted as a superposition of binary “qubit” vectors with complex-number coefficients

\[ |\Psi\rangle = \sum_{i=0}^{2^n-1} c_i |i_{n-1}i_{n-2}…i_0\rangle \]

- Operations are defined by linear algebra over Hilbert Space and can be represented by unitary matrices with complex elements
- Severe restrictions exist on copying and measuring signals
- Many universal gate sets exist but the best types are not obvious
- Circuits must use microscopic technologies that are slow, fragile, and not yet scalable, e.g., NMR
Unitary Operations

- Gates and circuits must be reversible (information-lossless)
  - Number of output signal lines = Number of input signal lines
  - The circuit function must be a bijection, implying that output vectors are a permutation of the input vectors
- Classical logic behavior can be represented by permutation matrices
- Non-classical logic behavior can be represented including state sign (phase) and entanglement
• Quantum Measurement
  – Measurement yields only one state $X$ of the superposed states
  – Measurement also makes $X$ the new state and so interferes with computational processes
  – $X$ is determined with some probability, implying uncertainty in the result
  – States cannot be copied (“cloned”), implying that signal fanout is not permitted
  – Environmental interference can cause a measurement-like state collapse (decoherence)
Classical vs. Quantum Circuits

Classical adder

\[ \begin{align*}
   c_{n-1} & \quad a_0 \\
   b_0 & \\
   a_1 & \quad b_1 \\
   a_2 & \quad b_2 \\
   a_3 & \quad b_3 \\
\end{align*} \]

...
Classical vs. Quantum Circuits

Quantum adder

- Here we use Pauli rotations notation.
- Controlled $\sigma_x$ is the same as controlled NOT.

Controlled-controlled $\sigma_x$ is the same as Toffoli.

Controlled $\sigma_x$ is the same as Feynman.
Reversible Circuits
Reversible Circuits

- Reversibility was studied around 1980 motivated by power minimization considerations.
- Bennett, Toffoli et al. showed that any classical logic circuit $C$ can be made reversible with modest overhead.
Reversible Circuits

• How to make a given $f$ reversible
  – Suppose $f : i \rightarrow f(i)$ has $n$ inputs $m$ outputs
  – Introduce $n$ extra outputs and $m$ extra inputs
  – Replace $f$ by $f_{\text{rev}} : i, j \rightarrow i, f(i) \oplus j$ where $\oplus$ is XOR

• Example 1: $f(a, b) = \text{AND}(a,b)$

  \[
  \begin{array}{ccc|ccc}
  a & b & c & a & b & f \\
  \hline
  0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 1 & 0 & 0 & 1 \\
  0 & 1 & 0 & 0 & 1 & 0 \\
  0 & 1 & 1 & 0 & 1 & 1 \\
  1 & 0 & 0 & 1 & 0 & 0 \\
  1 & 0 & 1 & 1 & 0 & 1 \\
  1 & 1 & 0 & 1 & 1 & 1 \\
  1 & 1 & 1 & 1 & 1 & 0 \\
  \end{array}
  \]

  \[
  \begin{array}{cc}
  \text{Reversible AND gate} \\
  a & a \\
  b & b \\
  c & f = ab \oplus c \\
  \end{array}
  \]

• This is the well-known Toffoli gate, which realizes AND when $c = 0$, and NAND when $c = 1$. 
Reversible Ciruits

- Reversible gate family [Toffoli 1980]

- Every Boolean function has a reversible implementation using Toffoli gates.

- There is no universal reversible gate with fewer than three inputs.
Quantum Gates
Quantum Gates

- **One-Input gate: NOT**
  - Input state: $c_0|0\rangle + c_1|1\rangle$
  - Output state: $c_1|0\rangle + c_0|1\rangle$
  - Pure states are mapped thus: $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$
  - Gate operator (matrix) is 
    \[
    \begin{pmatrix}
    0 & 1 \\
    1 & 0 \\
    \end{pmatrix}
    \]
  - As expected:
    \[
    \begin{pmatrix}
    0 & 1 \\
    1 & 0 \\
    \end{pmatrix}\begin{pmatrix}
    0 & 1 \\
    1 & 0 \\
    \end{pmatrix} = \begin{pmatrix}
    1 & 0 \\
    0 & 1 \\
    \end{pmatrix}
    \]
Quantum Gates

• **One-Input gate:** “Square root of NOT”
  
  – Some matrix elements are imaginary
  
  – Gate operator (matrix):

    \[
    \begin{pmatrix}
    i/\sqrt{1/2} & 1/\sqrt{1/2} \\
    1/\sqrt{1/2} & i/\sqrt{1/2}
    \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\
    1 & i \end{pmatrix}
    \]

  – We find:

    \[
    \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \end{pmatrix} \begin{pmatrix} 1 \\
    0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\
    1 \end{pmatrix}
    \]

    so \( |0\rangle \rightarrow |0\rangle \) with probability \( |i/\sqrt{2}|^2 = 1/2 \)

    \[
    \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \end{pmatrix} \begin{pmatrix} 1 \\
    i \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\
    i \end{pmatrix}
    \]

    and \( |0\rangle \rightarrow |1\rangle \) with probability \( |1/\sqrt{2}|^2 = 1/2 \)

    Similarly, this gate randomizes input \( |1\rangle \)

  – But concatenation of two gates eliminates the randomness!

    \[
    \frac{1}{2} \begin{pmatrix} i & 1 \\
    1 & i \end{pmatrix} \begin{pmatrix} i & 1 \\
    1 & i \end{pmatrix} = \begin{pmatrix} 0 & i \\
    i & 0 \end{pmatrix}
    \]

    \[
    \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\
    1 & i \end{pmatrix} \begin{pmatrix} i & 1 \\
    1 & i \end{pmatrix} = \begin{pmatrix} 0 & i \\
    i & 0 \end{pmatrix}
    \]
Other variant of square root of not - we do not use complex numbers - only real numbers

A square-root-of-NOT (SRN) gate

\[
\begin{bmatrix}
1 & 1 \\
\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\
1 & 1 \\
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}
\end{bmatrix}
\]

- Applied once to a classical state, this \(~\)randomizes the value of the qubit.
- Applied twice in a row, this is \(~\)equivalent to NOT:

\[
\begin{bmatrix}
1 & 1 \\
\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\
1 & 1 \\
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}
\end{bmatrix} \times \begin{bmatrix}
1 & -1 \\
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\
1 & 1 \\
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}
\end{bmatrix} = \begin{bmatrix}
0 & -1 \\
1 & 0
\end{bmatrix}
\]
Quantum Gates

- **One-Input gate: Hadamard**
  \[
  \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}
  \]

  Maps \(|0\rangle \rightarrow \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle\) and \(|1\rangle \rightarrow \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\).

  Ignoring the normalization factor \(\frac{1}{\sqrt{2}}\), we can write
  \(|x\rangle \rightarrow (-1)^x |x\rangle - |1 - x\rangle\)

- **One-Input gate: Phase shift**
  \[
  \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}
  \]
Universal One-Input Gate Sets

- **Requirement:**

  \[ |0\rangle \rightarrow U \rightarrow \text{Any state } |\psi\rangle \]

- **Hadamard** and **phase-shift** gates form a universal gate set of 1-qubit gates, every 1-qubit gate can be built from them.

- **Example:** The following circuit generates

  \[ |\psi\rangle = \cos \theta |0\rangle + e^{i\phi} \sin \theta |1\rangle \]

  up to a global factor
Other Quantum Gates

Rotation ($U\theta$):
\[
\begin{bmatrix}
\cos(\theta) & \sin(\theta) \\
-sin(\theta) & \cos(\theta)
\end{bmatrix}
\]

Hadamard ($H$):
\[
\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}
\]

CNOT:
\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]

CPHASE:
\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & e^{i\alpha} \\
0 & 0 & 0 & e^{i\alpha}
\end{bmatrix}
\]

There are many small “universal” sets of gates.

Gates must be unitary: $U^\dagger U = UU^\dagger$, where $U^\dagger$ is the Hermitean adjoint of $U$. 
Quantum Gates

- **Two-Input Gate: Controlled NOT (CNOT)**

\[ |x\rangle \quad |y\rangle \quad \text{CNOT} \quad |x\oplus y\rangle \]

\[ \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0
\end{pmatrix} \]

- CNOT maps \(|x\rangle|0\rangle \rightarrow |x\rangle||x\rangle \) and \(|x\rangle|1\rangle \rightarrow |x\rangle||\text{NOT } x\rangle \)

\(|x\rangle|0\rangle \rightarrow |x\rangle||x\rangle \) *looks like cloning, but it’s not.* These mappings are **valid only for the pure states** \(|0\rangle\) and \(|1\rangle\)

- Serves as a “non-demolition” measurement gate
Polarizing Beam-Splitter CNOT gate
from [Cerf, Adami, Kwiat]

- Two qubits encoded in one photon, one in momentum (direction) and one in polarization.
- Polarization controls change in momentum.
- Cannot be scaled up directly, but demonstrates an implementation of a 2-qubit gate.
Quantum Gates

- **3-Input gate:** Controlled CNOT (\(C^2\text{NOT or Toffoli gate}\))

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
\]

\[|a\rangle \quad |a\rangle\]

\[|b\rangle \quad |b\rangle\]

\[|c\rangle \quad |ab \oplus c\rangle\]
General controlled gates that control some 1-qubit unitary operation $U$ are useful.

$$
\begin{pmatrix}
  u_{00} & u_{01} \\
  u_{10} & u_{11}
\end{pmatrix}
$$

etc.
Universal Gate Sets

• To implement any unitary operation on \( n \) qubits exactly requires an infinite number of gate types

• The (infinite) set of all 2-input gates is universal
  – Any \( n \)-qubit unitary operation can be implemented using \( \Theta(n^{34^n}) \) gates [Reck et al. 1994]

• CNOT and the (infinite) set of all 1-qubit gates is universal
Discrete Universal Gate Sets

- The error on implementing $U$ by $V$ is defined as

$$E(U, V) = \max_{|\psi\rangle} \| (U - V) |\psi\rangle \|$$

- If $U$ can be implemented by $K$ gates, we can simulate $U$ with a total error less than $\epsilon$ with a gate overhead that is polynomial in $\log(K/\epsilon)$

- A discrete set of gate types $G$ is universal, if we can approximate any $U$ to within any $\epsilon > 0$ using a sequence of gates from $G$
Quantum Gates

Discrete Universal Gate Set

- **Example 1**: Four-member “standard” gate set

\[
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}
\]

CNOT          Hadamard      Phase      \(\pi/8\) (T) gate

- **Example 2**: \{CNOT, Hadamard, Phase, Toffoli\}
Quantum Circuits
A quantum (combinational) circuit is a sequence of quantum gates, linked by “wires”

The circuit has fixed “width” corresponding to the number of qubits being processed

Logic design (classical and quantum) attempts to find circuit structures for needed operations that are
  – Functionally correct
  – Independent of physical technology
  – Low-cost, e.g., use the minimum number of qubits or gates

Quantum logic design is not well developed!
Ad hoc designs known for many specific functions and gates

**Example 1** illustrating a theorem by [Barenco et al. 1995]: Any $C^2(U)$ gate can be built from CNOTs, $C(V)$, and $C(V^\dagger)$ gates, where $V^2 = U$

\[
\begin{align*}
V & \quad = \quad V^\dagger \\
U & \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quito
Example 1: Simulation

$|0\rangle |0\rangle$ $\Rightarrow$ $|0\rangle |0\rangle |0\rangle |0\rangle |0\rangle |0\rangle |0\rangle$

$|1\rangle |1\rangle$ $\Rightarrow$ $|1\rangle |1\rangle |1\rangle |1\rangle |1\rangle |1\rangle |1\rangle$

$|x\rangle U |x\rangle$ $\Rightarrow$ $|x\rangle V|x\rangle V^\dagger |x\rangle V |x\rangle$
Example 1: Simulation (contd.)

\[ |1\rangle |1\rangle = |1\rangle |1\rangle \]

\[ |1\rangle |1\rangle = |1\rangle |1\rangle \]

Exercise: Simulate the two remaining cases
Example 1: Algebraic analysis

\[ U_0(x_1, x_2, x_3) = U_5 U_4 U_3 U_2 U_1(x_1, x_2, x_3) \]
\[ = (x_1, x_2, x_1 x_2 \oplus U(x_3)) \]

We will verify unitary matrix of Toffoli gate

Observe that the order of matrices \( U_i \) is inverted.
Example 1 (contd);

We calculate the Unitary Matrix $U_1$ of the first block from left.

$U_1 = I_1 \otimes C(V)$

$$
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & v_{00} & v_{01} \\
0 & 0 & v_{10} & v_{11}
\end{pmatrix}
$$

Unitary matrix of a wire
Kronecker since this is a parallel connection
Unitary matrix of a controlled $V$ gate (from definition)
Example 1 (contd);

We calculate the Unitary Matrix $U_2$ of the second block from left.

$$U_2 = U_4 = CNOT(x_1, x_2) \otimes I_1$$

$$\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix} \otimes \begin{pmatrix}
1 & 0 \\
0 & 1 \\
0 & 0 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}$$

Unitary matrix of CNOT or Feynman gate with EXOR down

As we can check in the schematics, the Unitary Matrices $U_2$ and $U_4$ are the same.
Quantum Circuits

Example 1 (contd);

\[ U_2 = U_4 = CNOT(x_1, x_2) \otimes I_1 \]

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\otimes
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
= \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}
\]
Example 1 (contd);

- $U_5$ is the same as $U_1$ but has $x_1$ and $x_2$ permuted (tricky!)
- It remains to evaluate the product of five 8 x 8 matrices $U_5 U_4 U_3 U_2 U_1$ using the fact that $VV^\dagger = I$ and $VV = U$
**Quantum Circuits**

Example 1 (contd);

- *We calculate matrix $U_3$*

<table>
<thead>
<tr>
<th>1 0</th>
<th>1 0 0 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1</td>
<td>0 1 0 0</td>
</tr>
<tr>
<td>0 0</td>
<td>0 0 $v_{00}$ $v_{10}$</td>
</tr>
<tr>
<td>0 0</td>
<td>0 0 $v_{01}$ $v_{11}$</td>
</tr>
</tbody>
</table>

This is a hermitian matrix, so we transpose and next calculate complex conjugates, we denote complex conjugates by bold symbols

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & v_{00} & v_{10} & 0 & 0 & 0 & 0 \\
0 & 0 & v_{01} & v_{11} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & v_{00} & v_{10} \\
0 & 0 & 0 & 0 & 0 & 0 & v_{01} & v_{11}
\end{pmatrix}
$$
Quantum Circuits

Example 1 (contd);

- $U_5$ is the same as $U_1$ but has $x_1$ and $x_2$ permuted because in $U_1$ black dot is in variable $x_2$ and in $U_5$ black dot is in variable $x_1$.
- This can be also checked by definition, see next slide.

$$U_5 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & v_{00} & v_{01} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & v_{10} & v_{11} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & v_{00} & v_{01} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & v_{10} & v_{11} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$
Quantum Circuits

**Example 1** (here we explain in detail how to calculate $U_5$)

$U_5$ is calculated as a Kronecker product of $U_7$ and $I_1$

$U_7$ is a unitary matrix of a swap gate

$U_5 = U_6 U_1 U_6$
Example 1 (contd);

- It remains to evaluate the product of five 8 x 8 matrices $U_5 U_4 U_3 U_2 U_1$ using the fact that $VV^\dagger = I$ and $VV = U$.
Implementing a Half Adder

- **Problem:** Implement the classical functions $\text{sum} = x_1 \oplus x_0$ and $\text{carry} = x_1 x_0$

- **Generic design:**

  \[
  \begin{align*}
  |x_1\rangle & \quad |y_1\rangle & \quad |y_0\rangle \\
  |x_0\rangle & \quad |x_0\rangle & \quad |y_0\rangle \\
  \end{align*}
  \]

  $U_{\text{add}}$

  \[
  \begin{align*}
  & |x_1\rangle \\
  & |x_0\rangle \\
  & |y_1\rangle \oplus \text{carry} \\
  & |y_0\rangle \oplus \text{sum} \\
  \end{align*}
  \]
• **Half Adder.** Generic design (contd.)

\[
U_{ADD} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]
Quantum Circuits

- **Half Adder**: Specific (reduced) design

$$
|x_0\rangle \quad \text{C}^2\text{NOT (Toffoli)} \quad \text{CNOT} \quad |x_1\rangle
$$

$$
|y\rangle \quad \text{sum} \quad |y\rangle \oplus \text{carry}
$$