### Quantum computation and quantum information

Chapter 4 Quantum circuits

#### Projects

- 1 Quantum simulators, *Andreas*
- 2 Free space communication, *Andreas*
- 3 Quantum computation with spins in quantum dots, *Peter*
- 4 Bell inequality: quantum non-locality vs local realism, Peter
- 5 Entanglement: concept, measures and open problems, *Peter*
- 6 Quantum computing in rare earth ion doped crystals, *Stefan*
- 7 Quantum repeaters, Stefan
- 8 Quantum memories, *Stefan*
- 9 Quantum computation with superconducting qubits, *Ville*
- 10 Majorana qubits & topological quantum computation, Martin
- 11 Beam up my quantum state, Scotty!, Peter

### Please sign up for a project Wednesday April 17th at the latest

- Choose project by sending a mail to Stefan.kroll@fysik.lth.se or by handing a note the lecturers
- You can sign up alone or in pairs
- If you sign up alone you will be grouped in pairs with an other person who also has signed up alone
- When you sign up, you specify your first, second and third choice for project
- We will try to give as many as possible their favourite choice under the constraint of not having more than two groups on each project
- Give your preferred presentation date, May 29th or June 3<sup>rd</sup>
- If one of the dates is impossible for you please write this.

#### Errata list, Nielsen & Chuang

• http://www.michaelnielsen.org/qcqi/errata/e rrata/errata.html

#### Part II, Nielsen & Chuang

- Quantum circuits (Ch 4) SK
- Quantum algorithms (Ch 5 & 6)
  - Göran Johansson
- Physical realisation of quantum computers (Ch 7)
  - Andreas Walther

#### Chapter 4

- Quantum circuits
  - Quantum circuits provide us with a language for describing quantum algorithms ⇒ We can quantify the resources needed for a quantum algorithm in terms of gates, operations etc. It also provides a toolbox for algorithm design.
- Simulation of quantum systems

#### Chapter 4, Quantum circuits

- 4.1 Quantum algorithms
- 4.2 Single qubit operations
- 4.3 Controlled operations
- 4.4 Measurement
- 4.5 Universal quantum gates
- 4.6 Circuit model summary
- 4.7 Simulation of quantum systems

#### Chapter 4, Quantum circuits

- 4.1 Quantum algorithms
- 4.2 Single qubit operations
- 4.3 Controlled operations
- 4.4 Measurement
- 4.5 Universal quantum gates
- 4.6 Circuit model summary
- 4.7 Simulation of quantum systems

## Why are there few quantum algorithms

- Algorithm design is difficult
- Quantum algorithms need to be better than classical algorithms to be interesting
- Our intuition works better for classical algorithms, making obtaining ideas about quantum algorithms still harder

#### Chapter 4, Quantum circuits

- 4.1 Quantum algorithms
- 4.2 Single qubit operations
- 4.3 Controlled operations
- 4.4 Measurement
- 4.5 Universal quantum gates
- 4.6 Circuit model summary
- 4.7 Simulation of quantum systems

#### Chapter 4, Quantum circuits

- 4.2 Single qubit operations
  - We will analyse arbitrary single qubit and controlled single qubit operations

In quantum information data is represented by quantum bits (qubits)

• A qubit is a quantum mechanical systems with two states |0> and |1> that can be in any arbitrary superposition

$$\Psi = \alpha |0\rangle + \beta |1\rangle$$

of those states

#### Qubit representation

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



Figure 1.3. Bloch sphere representation of a qubit.

#### Single qubit gates

• Single qubit gates, U, are unitary

#### 1.3.1 Single qubit gates



Figure 1.5. Single bit (left) and qubit (right) logic gates.

There are infinitely many two by two unitary matrices, and thus infinitely many single

Fig 4.2, page 177



Figure 4.2. Names, symbols, and unitary matrices for the common single qubit gates.

# Single qubit gates on Bloch sphere

- X-gate
  - 180° rotation around x-axis
- Y-gate
  - 180° rotation around y-axis
- Z-gate
  - 180° rotation around z-axis

#### The Bloch sphere



Figure 1.3. Bloch sphere representation of a qubit.

Fig 4.2, page 177



Figure 4.2. Names, symbols, and unitary matrices for the common single qubit gates.

# Single qubit gates on Bloch sphere

- S-gate
  - 90° rotation around z-axis
- T-gate
  - $-45^{\circ}$  rotation around z-axis
- H-gate
  - 90° rotation around the y-axis followed by 180° rotation around the x-axis

### Rotation an arbitrary angle around axes x, y and z

Exercise 4.2: Let x be a real number and A a matrix such that  $A^2 = I$ . Show that  $\exp(iAx) = \cos(x)I + i\sin(x)A$ . (4.7)

Use this result to verify Equations (4.4) through (4.6).

$$R_{x}(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$
(4.4)  

$$R_{y}(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$
(4.5)  

$$\vdots$$
  

$$R_{z}(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} .$$
(4.6)

#### Chapter 4, Quantum circuits

- 4.1 Quantum algorithms
- 4.2 Single qubit operations
- 4.3 Controlled operations
- 4.4 Measurement
- 4.5 Universal quantum gates
- 4.6 Circuit model summary
- 4.7 Simulation of quantum systems

### CNOT is a MODULO-2 addition of the control bit to the target bit



Figure 4.3. Circuit representation for the controlled-NOT gate. The top line represents the control qubit, the bottom line the target qubit.

#### Fig 4.4, control-U

 $|c\rangle|t\rangle \rightarrow |c\rangle U^{c}|t\rangle$ 



#### Controlled arbitrary rotation



Figure 4.6. Circuit implementing the controlled-U operation for single qubit U.  $\alpha$ , A, B and C satisfy  $U = \exp(i\alpha)AXBXC$ , ABC = I.

 $|c\rangle|t\rangle \rightarrow |c\rangle U^{c}|t\rangle$ 

Lets start with inputs  $|c\rangle = |0\rangle$ and  $|t\rangle = |\Psi\rangle$ , what is the output?

Now we choose  $|c\rangle = |1\rangle$  and  $|t\rangle = |\Psi\rangle$ , what is the output?

#### Controlled arbitrary rotation



Figure 4.6. Circuit implementing the controlled-U operation for single qubit U.  $\alpha$ , A, B and C satisfy  $U = \exp(i\alpha)AXBXC$ , ABC = I.



#### Arbitrary single qubit operation in terms of z and y rotations (theorem 4.1 page 175)



Figure 1.3. Bloch sphere representation of a qubit.

#### Preparing for logical gates Page 176

Corollary 4.2: Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that ABC = I and  $U = e^{i\alpha}AXBXC$ , where  $\alpha$  is some overall phase factor.

#### Proof

In the notation of Theorem 4.1, set  $A \equiv R_z(\beta)R_y(\gamma/2)$ ,  $B \equiv R_y(-\gamma/2)R_z(-(\delta + \beta)/2)$ and  $C \equiv R_z((\delta - \beta)/2)$ . Note that

$$ABC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) = I. \quad (4.14)$$

Since  $X^2 = I$ , and using Exercise 4.7, we see that

$$XBX = XR_y\left(-\frac{\gamma}{2}\right)XXR_z\left(-\frac{\delta+\beta}{2}\right)X_z = R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right).$$
(4.15)

#### Controlled arbitrary rotation



Figure 4.6. Circuit implementing the controlled-U operation for single qubit U.  $\alpha$ , A, B and C satisfy  $U = \exp(i\alpha)AXBXC$ , ABC = I.

#### Notation

- Computational basis states (page 202)
  - A quantum circuit operating on n qubits acts in a  $2^n$ -dimensional complex Hilbert space. The computational basis state are product states  $|x_1, \dots, x_n\rangle$  where  $x_i=0,1$ .
  - For example a two qubit state  $|x_1\rangle|x_2\rangle$  in the computational basis is expressed as
  - $|\Psi > = \alpha |00 > + \beta |01 > + \gamma |10 > + \delta |11 >$ 
    - Where we have the basis states for the tensor product of the  $|x_1\rangle|x_2\rangle$  basis states

#### Hadamard gates, exercise 4.16

Exercise 4.16: (Matrix representation of multi-qubit gates) What is the 4×4 unitary matrix for the circuit



in the computational basis? What is the unitary matrix for the circuit

 $x_1$ 

$$x_2 - H -$$

#### Exercise 4.16, page

• Matrix for H-gate on x<sub>2</sub>

• Matrix for H-gate on x<sub>1</sub>

#### H-gate is unitary

• Matrix multiplication H<sup>†</sup>H=I

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

#### Exercise 4.20



Discuss with your neighbour. How would you solve this?

#### Multiplying the Hadamard gates

• We can just extend exercise 4.16 by multiplying the two Hadamard gates
## Exercise 4.20

• Multiplying Hadamard and CNOT gates give

• Answer: a CNOT gate where the lower bit is the control bit

### Two control bits



Figure 4.8. Circuit for the  $C^2(U)$  gate. V is any unitary operator satisfying  $V^2 = U$ . The special case  $V \equiv (1 - i)(I + iX)/2$  corresponds to the Toffoli gate.

## Many control bits



## Chapter 4, Quantum circuits

- 4.1 Quantum algorithms
- 4.2 Single qubit operations
- 4.3 Controlled operations
- 4.4 Measurement
- 4.5 Universal quantum gates
- 4.6 Circuit model summary
- 4.7 Simulation of quantum systems

## Principle of deferred measurement



Measurements followed by classically controlled operations can always be replaced by conditional quantum operations



Figure 1.13. Quantum circuit for teleporting a qubit. The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits (recall that single lines denote qubits).

$$\begin{split} |\psi_{2}\rangle &= \frac{1}{2} \left[ |00\rangle \left( \alpha |0\rangle + \beta |1\rangle \right) + |01\rangle \left( \alpha |1\rangle + \beta |0\rangle \right) \\ &+ |10\rangle \left( \alpha |0\rangle - \beta |1\rangle \right) + |11\rangle \left( \alpha |1\rangle - \beta |0\rangle \right] \,. \end{split}$$
(1.32)  
$$\begin{aligned} 00 &\longmapsto |\psi_{3}(00)\rangle &\equiv \left[ \alpha |0\rangle + \beta |1\rangle \right] &(1.33) \quad \begin{array}{l} \mathbf{Quantum} \\ \mathbf{01} &\longmapsto |\psi_{3}(01)\rangle &\equiv \left[ \alpha |1\rangle + \beta |0\rangle \right] \\ 10 &\longmapsto |\psi_{3}(10)\rangle &\equiv \left[ \alpha |0\rangle - \beta |1\rangle \right] &(1.35) \\ 11 &\longmapsto |\psi_{3}(11)\rangle &\equiv \left[ \alpha |1\rangle - \beta |0\rangle \right] \,. \end{aligned}$$
(1.36)

## Chapter 4, Quantum circuits

- 4.1 Quantum algorithms
- 4.2 Single qubit operations
- 4.3 Controlled operations
- 4.4 Measurement
- 4.5 Universal quantum gates
- 4.6 Circuit model summary
- 4.7 Simulation of quantum systems

## Universal quantum gates (4.5)

 A set of gates is universal if any unitary operation can be approximated to arbitrary accuracy by quantum circuits only involving these gates

## CNOT, Hadamard and T-gates form a universal set

- 1. An arbitrary unitary operator can be expressed as a product of unitary operators acting on two computational basis states (subsection 4.5.1).
- 2. An arbitrary unitary operator acting on two computational basis states can be expressed as a product of single qubit operations and CNOT gates. (page 192-193) (subsection 4.5.2, exercise 4.39)

## Exercise 4.93, Page 193

Exercise 4.39: Find a quantum circuit using single qubit operations and ONOTS to implement the transformation

1	1	0	0	0	0	0	0	0	1	
	0	1	0	0	0	0	0	0		
	0	0	a	0	0	0	0	c		(4.60)
	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	b	0	0	0	0	d		
	-								ō.	

## CNOT, Hadamard and T-gates form a universal set

- 1. An arbitrary unitary operator can be expressed as a product of unitary operators acting on two computational basis states (subsection 4.5.1).
- 2. An arbitrary unitary operator acting on two computational basis states can be expressed as a product of single qubit operations and CNOT gates. (page 192-193) (subsection 4.5.2, exercise 4.39)
- 3. Single qubit operations may be approximated to arbitrary accuracy using Hadamard and T gates (subsection 4.5.3)

### Single qubit operations may be approximated to arbitrary accuracy using H- and T-gates (subsection 4.5.3)

- From the corrected version of Eq. 4.13 page 176 we see that (exercise 4.11):
- If **m** and **n** are non parallel vectors in three dimensions any arbitrary single qubit unitary operation, U may be written as

 $U = e^{i\alpha} R_{\mathbf{n}}(\beta_1) R_{\mathbf{m}}(\gamma_1) R_{\mathbf{n}}(\beta_2) R_{\mathbf{m}}(\gamma_2) \dots$ 

• It is shown on page 196 that rotations of arbitrary angles can be carried out around two different axes using combinations of H- and T-gates

# Approximating arbitrary unitary gates (4.5.3 & 4.5.4)

- In order to approximate a quantum circuit consisting of m CNOT and single qubit gates with an accuracy ε, only about O[m\*log(m/ε)] gate operations are required (*Solovay-Kitaev theorem*).
- This does not sound too bad!
- The problem is that of the order 2<sup>2n</sup> gates are required to implement an arbitrary n-qubit unitary operation (see page 191-193), thus this is a computationally hard problem.

#### **Quantum Computational Complexity 4.5.5.**

**Relation to classical complexity classes** 



- BPP is thought to be subset of BQP, enabling QC to solve some problems more efficient than classical computers
- **BQP is a subset of PSPACE** Any problem consuming polynomial time can consume a maximal polynomial amount of space

## The power of quantum computation

- NP complete problems are a subgroup of NP
- If any NP-complete problem has a polynomial time solution then P=NP
- Factoring is not known to be NP-complete
- Quantum computers are known to solve all problems in P efficiently but cannot solve problems outside PSPACE efficiently
- If quantum computers are proved to be more efficient than classical computers P=/=PSPACE



# Quantum computing changes the landscape of computer science

- QC algorithms do not violate the Church-Turing thesis:
  - any algorithmic process can be simulated using a Turing machine
- QC algorithms challenge the strong version of the Church-Turing thesis
  - If an algorithm can be performed at any class of hardware, then there is an equivalent efficient algorithm for a Turing machine

## Chapter 4, Quantum circuits

- 4.1 Quantum algorithms
- 4.2 Single qubit operations
- 4.3 Controlled operations
- 4.4 Measurement
- 4.5 Universal quantum gates
- 4.6 Circuit model summary
- 4.7 Simulation of quantum systems

# The quantum circuit model of computation

### • Properties:

- Quantum computer may be a hybrid of quantum and classical resources to maximize efficiency
- A quantum circuit operates on n qubits spanning a  $2^n$  dimensional state space. The product states of the form  $|x_1,x_2,..,x_n\rangle$ ;  $x_i$ ={0,1} are the computational basis states

### • Basic steps:

- Preparation
- Computation
- Measurement

# The quantum circuit model of computation

- Maybe it would be better that the computational basis states are entangled
- Maybe the measurements should not be carried out in the computational basis
- It is not known whether the quantum circuit model constitute an optimum quantum computer language

## Chapter 4, Quantum circuits

- 4.1 Quantum algorithms
- 4.2 Single qubit operations
- 4.3 Controlled operations
- 4.4 Measurement
- 4.5 Universal quantum gates
- 4.6 Circuit model summary
- 4.7 Simulation of quantum systems

## Quantum simulation

- Feynman 1982
- Chemistry (large molecules, reactions)
- Biology (even larger molecules)
- Simulation of the properties of new synthesized molecules

# Simulation of quantum systems

$$i\hbar \frac{d}{dt} |\Psi\rangle = H |\Psi\rangle$$

- With n qubits there are 2<sup>n</sup> different differential equations that must be solved
- The equation above has the formal solution

$$|\Psi(t)\rangle = e^{-\frac{i}{\hbar}Ht}|\Psi(0)\rangle$$

#### Simulation of quantum systems

•While quantum computers are hoped to solve general calculations efficiently, another field in which they are hoped to succeed is the simulation of specific physical systems described by a Hamiltonian.

•However the physical system must be approximated efficiently, to do so:



#### Approximating the state

**|**ψ(0)>

 $|\psi'(0)>$ 

The continuous function is discretised to arbitrary precision using a finite set of basis vectors

$$|\Psi\rangle = \int c(x)\phi(x)dx \rightarrow |\Psi'\rangle = \sum_{k} c_{k}\phi_{k}$$

The set of basis vectors must be chosen such that for any given time, the approximated state has to be equal to the original state within a given error tolerance



#### Approximating the Operator

Discretizing of the differential equations begins with choosing an appropriate  $\Delta t$ . It has to fulfill the demands set by the maximum error.

The approximation of the differential operator is a three step process.

First, if possible separate H into a set of Hamiltonians,  $H_i$ , which act on a maximal constant number of particles. (next neighbor interaction, etc).

Secondly, write the effect of H on the system as time evolves as a product of the effect of the individual  $H_i$ .

Thirdly, the effect of  $H_i$  is written in terms of a quantum circuit.

# Separate H into Hamiltonians, H<sub>i</sub>, acting on subsets of particles.



#### Simulation of quantum systems

Approximating the Operator

The evolution operator is of the form

### Exp[-iHt]

If possible H is broken down into a sum of local interactions

 $H = \sum_{k} H_{k}$  If the sub Hamiltonians do not commute it follows that

 $\operatorname{Exp}[-i(H_1 + H_2 + \dots)t] \neq \operatorname{Exp}[-iH_1t]\operatorname{Exp}[-iH_2t]\dots$ 

We now introduce the Trotter formula

$$Exp[i(A+B)t] = \lim_{n \to \infty} \{ Exp[iAt / n] Exp[iBt / n] \}^n$$

**Simulation of quantum systems** Approximating the Operator

$$Exp[i(A+B)t] = \lim_{n \to \infty} \{ Exp[iAt / n] Exp[iBt / n] \}^n$$

(Trotter formula)

By varying n we can obtain a product representation of the evolution operator within any given error

$$Exp[i(H_1 + H_2)\Delta t] = Exp[iH_1\Delta t]Exp[iH_2\Delta t] + O(\Delta t^2)$$

Now that H is broken down into a product of local Hamiltonians which may be written on a quantum circuit form (Exercise 4.51). The product of the circuit corresponds to a unitary operator U.

$$U = Exp[iH_1\Delta t]Exp[iH_2\Delta t]...Exp[iH_n\Delta t]$$
$$|\Psi(t + \Delta t)\rangle = U|\Psi(t)\rangle$$
$$|\Psi(t_f)\rangle = U^j|\Psi(t_0)\rangle; t_f = j\Delta t$$

## Exercise 4.51, page 210

Exercise 4.51: Construct a quantum circuit to simulate the Hamiltonian

 $H = X_1 \otimes Y_2 \otimes Z_3, \tag{4.115}$ 

performing the unitary transform  $e^{-i\Delta tH}$  for any  $\Delta t$ .

## Chapter 4, Quantum circuits

- 4.1 Quantum algorithms
- 4.2 Single qubit operations
- 4.3 Controlled operations
- 4.4 Measurement

## Chapter 4, Quantum circuits

- 4.5 Universal quantum gates
  - Single qubit and CNOT gates are universal
  - A discrete set of universal operators
  - Approximating arbitrary unitary gates is hard
  - Quantum computational complexity
- 4.6 Circuit model summary
- 4.7 Simulation of quantum systems

## Chapter 4

End