

# Computational models for quantum computation

Pascal Steger

Proseminar in theoretical physics, 2008

- 1 Introduction
  - overview
  - literature
  - two basic models
- 2 Quantum Gates
  - definitions
  - Toffoli- and Q-gate
  - universality
- 3 Quantum Turing Machine
  - Church-Turing
  - step operator
  - dynamics
- 4 Complexity
  - theorems
  - Everett's interpretation; stock market



P. Benioff.

Models of quantum turing machines.

*Fortsch. Phys.*, 46:423–442, 2007.



D. Deutsch.

Quantum theory, the church-turing principle and the universal quantum computer.

*Proc. R. Soc. Lond. A*, 400:97–117, 1985.



D. Deutsch.

Quantum computation networks.

*Proc. R. Soc. Lond. A*, 425:73–90, 1989.



A. C. Yao.

Quantum circuit complexity.

*Proc. of the 34th Ann. Symp. on Found. of Comp. Sc. (FOCS)*, pages 352–361, 1993.

# two models

## two basic models for quantum computation

- quantum computational network, built of quantum gates
- Quantum Turing Machine

## connections between models

- quantum mechanical description: step operator
- complexity theory

- 1 Introduction
  - overview
  - literature
  - two basic models
- 2 Quantum Gates
  - definitions
  - Toffoli- and Q-gate
  - universality
- 3 Quantum Turing Machine
  - Church-Turing
  - step operator
  - dynamics
- 4 Complexity
  - theorems
  - Everett's interpretation; stock market

# general definitions

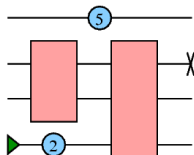
**computation:** process that produces output depending on input

**in-,output:** abstract symbols

**bit,quantum:** smallest possible quantity of non-probabilistic information

**carrier:** physical representation of a bit, e.g. spin  $1/2$ -particle

# logic circuits



**logic circuit:** computing machine consisting of logic gates;  
computational steps synchronized;  
 $\text{outputs}(i) = \text{inputs}(i + 1)$ ; can use sources and sinks

**source:** gate with only one output that emits 0 or 1 in each step; reversible

**sink:** gate with only one input that deletes information; irreversible

**unit wire:** computes identity function with fixed time dilation

## physical processes in quantum computer

- 1 preparation of input states in carriers
- 2 as a black box:
- 3 QM elastic scattering (errorless)
- 4 measurement of output carriers after fixed step



## gates: definitions

**logic gate:** computing machine; input and output consist of fixed number of bits; fixed computation is done in fixed time.

**quantum gate:** states of input and output can be quantum mixtures of eigenstates of input observable  $\hat{I}$  and output observable  $\hat{O}$ .

**reversible gate:** inputs and outputs are related by invertible function (ideal case, no errors)

# mathematical descriptions of gates

computational basis:

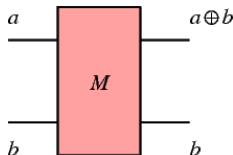
eigenstates of  $\hat{I}$  and  $\hat{O}$  in Schrödinger picture, if they coincide.

- by table
- by permutation: let  $\{|a, b\rangle\}$ ,  $a, b \in \{0, 1\}$  be the four computational basis states. A gate transforms inputs into outputs, e.g.

$$\begin{array}{ll} |0, 0\rangle & \rightarrow |0, 0\rangle \\ |0, 1\rangle & \rightarrow |1, 1\rangle \\ |1, 0\rangle & \rightarrow |1, 0\rangle \\ |1, 1\rangle & \rightarrow |0, 1\rangle \end{array}$$

- by  $S$ -Matrix, more suitable for quantum gates

# example: C-NOT, measurement gate



$a$	$b$	$a \oplus b$	$b$	$(a \oplus b) \oplus b$	$b$
0	0	0	0	0	0
0	1	1	1	0	1
1	0	1	0	1	0
1	1	0	1	1	1

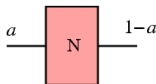
# S-matrix

- $S_{a'b'...}^{ab...}$  has clumped indices  $ab\dots, a'b'\dots$  denoting the states of the input and output carriers
- operation of gate corresponds to matrix multiplication with  $S_{a'b'...}^{ab...}$

$$|a, b, \dots\rangle \rightarrow \sum_{a', b', \dots \in \{0,1\}} S_{a'b'...}^{ab...} |a', b', \dots\rangle \equiv S|a, b, \dots\rangle. \quad (1)$$

- repeated gates are represented by powers of  $S$
- $S$  can also denote linear operator if no basis chosen

## example: NOT-gate

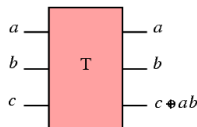


$$S_N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (2)$$

$$S_{N^\alpha} = S_N^\alpha = \frac{1}{2} \begin{pmatrix} 1 + e^{j\pi\alpha} & 1 - e^{j\pi\alpha} \\ 1 - e^{j\pi\alpha} & 1 + e^{j\pi\alpha} \end{pmatrix} \quad (3)$$

- $\alpha \notin \mathbb{N}$ :  $N^\alpha$  is a power of NOT
- $\alpha \in \mathbb{N}$ :  $N^\alpha$  is a logic gate: identity or NOT

# Toffoli gate in quantum computation



- classical gate: Toffoli

$$S_{Ta'b'c'}^{abc} = \delta_{a'}^a \delta_{b'}^b [(1 - ab)\delta_{c'}^c + ab(S_N)_{c'}^c] \quad (4)$$

- analogon: quantum gate  $Q$

$$S_{Qa'b'c'}^{abc} = \delta_{a'}^a \delta_{b'}^b \left[ (1 - ab)\delta_{c'}^c + iabe^{-i\pi\alpha/2}(S_N^\alpha)_{c'}^c \right] \quad (5)$$

# S-matrix of Toffoli and Q-gate

basis  $0 = |000\rangle$ ,  $1 = |001\rangle$ ,  $\dots$ ,  $6 = |110\rangle$ ,  $7 = |111\rangle$

$$S_T = \begin{pmatrix} \mathbb{1} & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix}$$

$$S_Q = \begin{pmatrix} \mathbb{1} & & \\ & i \cos \pi\alpha/2 & \sin \pi\alpha/2 \\ & \sin \pi\alpha/2 & i \cos \pi\alpha/2 \end{pmatrix}$$

## example NOT

$$S_{N^2} = S_N^2 = \mathbb{1}, \quad (6)$$

$$(S_{N^\alpha})^m = S_N^{m\alpha} = S_N^{m\alpha - 2\lfloor m\alpha/2 \rfloor}. \quad (7)$$

exponent  $1 + \varepsilon$  arbitrarily close to 1, but never exact for  $\alpha$  irrational,  $m \in \mathbb{N}$ .

time before non-classical behaviour:

$$t = \frac{1}{\max_{|\Psi\rangle} (1 - |\langle \Psi | S_N^\dagger S_N^m | \Psi \rangle|^2)} = \frac{1}{\sin^2 \pi \varepsilon / 2} \sim \varepsilon^{-2} \xrightarrow{(\varepsilon \rightarrow 0)} \infty$$



# universality: definitions

**computationally equivalent:** same output for same input

**problem:** exact equivalence in QM not possible, e.g. NOT

**adequate sets:**  $F$  and  $G$ , if  $\forall f \in F \exists \{g_n \in G\}$  and sequence  $\{\phi_n\}$  of phase angles such that

$$\lim_{n \rightarrow \infty} S_{g_n} e^{i\phi_n} = S_f \quad (8)$$

**example:**  $F = \{N\}$  and  $G = \{N^\alpha, \mathbb{1}\}$  are adequate

**universal gate:** quantum gate such that set of unit wire, source and this gate is adequate to set of other gates

### Claim:

The  $Q$ -gate is universal to set of all quantum gates.

### Proof:

create repertoire of gates that  $Q$  is adequate to:

- 1 Toffoli gate
- 2 all logic gates
- 3 all 3-bit quantum gates
- 4 all  $n$ -bit quantum gates
- 5 all quantum gates

## proof: step 1,2: Toffoli gate

choose basis  $0 = |000\rangle, 1 = |001\rangle, \dots, 6 = |110\rangle, 7 = |111\rangle$

$$S_Q^{4n+1} = \begin{pmatrix} \mathbb{1} & & & \\ & i \cos \pi\alpha(2n+1/2) & \sin \pi\alpha(2n+1/2) & \\ & \sin \pi\alpha(2n+1/2) & i \cos \pi\alpha(2n+1/2) & \\ & & & \end{pmatrix}$$

$S_Q^{4n+1} = S_T$  for arguments  $\pi(2m+1/2)$ ,  $m \in \mathbb{N}$ ;  
arbitrarily close to Toffoli with  $\pi\alpha(2n+1/2)$  for some  $n \in \mathbb{N}$ .

Toffoli gate in repertoire, proof similar to that for NOT

Toffoli universal for all logic gates  $\Rightarrow$  all logic gates in repertoire

## proof: step 3: 3-bit quantum gates

$$\begin{aligned}
 S_Q^{4n} &= \begin{pmatrix} 1 & & \\ & \cos 2n\pi\alpha & -i \sin 2n\pi\alpha \\ & -i \sin 2n\pi\alpha & \cos 2n\pi\alpha \end{pmatrix} \\
 &\equiv \begin{pmatrix} 1 & & \\ & \cos \lambda & i \sin \lambda \\ & i \sin \lambda & \cos \lambda \end{pmatrix} \equiv U_\lambda
 \end{aligned}$$

is in repertoire, since  $\exists m \in \mathbb{N} : |2\pi n\alpha - 2\pi m| < \varepsilon$  for  $\varepsilon$  arbitrarily small

permutations: logic gates, in repertoire;  
limit of combinations of permutations and  $U$  does also:

$$\begin{aligned} \lim_{n \rightarrow \infty} [P_{56}(U_{\sqrt{\lambda/n}} P_{57})^2 (U_{-\sqrt{\lambda/n}} P_{57})^2 P_{56}]^n \\ = \begin{pmatrix} \mathbb{1} & & \\ & \cos \lambda & \sin \lambda \\ & -\sin \lambda & \cos \lambda \end{pmatrix} \equiv V_\lambda \\ \lim_{n \rightarrow \infty} [U_{\sqrt{\lambda/2n}} V_{\sqrt{\lambda/2n}} U_{-\sqrt{\lambda/2n}} V_{-\sqrt{\lambda/2n}}]^n \\ = \text{diag}(1, \dots, 1, e^{-i\lambda}, e^{i\lambda}) \equiv W_\lambda \end{aligned}$$

change in global phase factor does not change observable:

$$X_\lambda \equiv \text{diag}(1, \dots, 1, e^{i\lambda})$$

$V_\lambda, W_\lambda, X_\lambda$  are in repertoire

$$|\psi\rangle = \sum_{n=0}^7 c_n |n\rangle, \quad \sum_{n=0}^7 |c_n|^2 = 1$$

$$Z_6[|\psi\rangle] := X_{-\arg(c_6 c_7)/2} V_{-\arctan |c_6/c_7|} W_{-\arg(c_7/c_6)/2}$$

$$|\psi\rangle \Rightarrow \sum_{n=0}^5 c_n |n\rangle + 0 + \sqrt{|c_6|^2 + |c_7|^2} |7\rangle$$

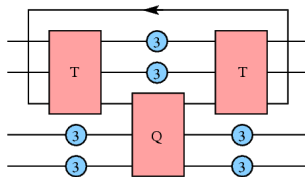
by analogy:  $G : c_i \rightarrow 0, i < 7$ , gate in repertoire. in general:

$$S = \sum_{n=0}^7 e^{i\sigma_n} |\psi_n\rangle \langle \psi_n|;$$

$$S = \prod_{n=0}^7 S_{G^{-1}[|\psi_n\rangle]} X_{\sigma_n} S_{G[|\psi_n\rangle]}$$

Q is universal to all  $3 \times 3$ -matrices

## proof: 4,5: $n$ bit gates



- loopback necessary to connect all inputs, outputs
- is initialized to 0, output is 0 again for all inputs
- makes circuit reversible, source and sink would yield irreversible gate

$$S_{Q_4 a' b' c' d'}^{abcd} = \delta_{a'}^a \delta_{b'}^b \delta_{c'}^c [(1 - abc) \delta_{d'}^d + iabce^{-i\pi\alpha/2} (S_N^\alpha)_{d'}^d]$$

same procedure to get  $n$ -bit gates.

# summary 1

## Most important

- quantum gates can have superpositions of states as input
- $Q$ -gate is universal wrt the set of all quantum gates
- proof constructs repertoire of gates that  $Q$  is adequate to



## 1 Introduction

- overview
- literature
- two basic models

## 2 Quantum Gates

- definitions
- Toffoli- and Q-gate
- universality

## 3 Quantum Turing Machine

- Church-Turing
- step operator
- dynamics

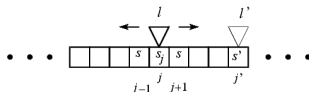
## 4 Complexity

- theorems
- Everett's interpretation; stock market

# Quantum Turing Machine (QTM)

## definition

- consists of a finite processor and an infinite memory
- computation proceeds in steps of fixed duration  $T$
- only processor and finite part of memory interact
- *halts*, if two subsequent states identical or halt flag set
- halt flag: observable, spectrum  $\{0, 1\}$ , independent of  $\hat{l}$ .
- universal, can simulate any other quantum computer



## Church-Turing hypothesis

Every function which would naturally be regarded as computable can be computed by the universal Turing machine.

## Church-Turing, physical principle

Every finitely realizable physical system can be perfectly simulated by a universal computing machine operating by finite means.

QTM fulfills this principle

Turing machine does not fulfill second version, since it is finite, but systems are continuous

## step operator: single step of computation

- head interacts with tape only at one position in fixed time
- head can move to the left, to the right, or stay and interact
- description: unitary *step* operator  $T$
- requirements: locality, displacement in at most one direction, periodicity (lattice sites)

$$\langle l', j', s' | T | l, j, s \rangle = \langle s'_{\neq j} | s_{\neq j} \rangle \langle l', j', s'_{\neq j} | \tilde{T} | l, j, s_j \rangle,$$

$$\tilde{T} = \sum_{j=-\infty}^{\infty} \sum_{\Delta=-1}^1 P_{j+\Delta} \tilde{T} P_j,$$

$$\langle l', j' + \Delta, s' | \tilde{T} | l, j', s' \rangle = \langle l', j + \Delta, s' | \tilde{T} | l, j, s \rangle.$$

# Hamiltonian

- ① for gates (Deutsch):

$$H \equiv \frac{i}{t} \ln S \quad (9)$$

- $H$  is local; description complexity is relatively small

- ② according Feynman:

$$H \equiv K(2 - T - T^\dagger) \quad (10)$$

- gives kinetic energy if  $T$  is only displacement
- note:  $T$  can be a sum of elementary, unitary step operators for single gates

## summary 2

### most important

- QTM is quantum analogon to Turing machine
- fulfills the Church-Turing principle
- can be described by step operators and Hamiltonian

- 1 Introduction
  - overview
  - literature
  - two basic models
- 2 Quantum Gates
  - definitions
  - Toffoli- and Q-gate
  - universality
- 3 Quantum Turing Machine
  - Church-Turing
  - step operator
  - dynamics
- 4 Complexity
  - theorems
  - Everett's interpretation; stock market

# complexity: definitions

**size:** number of elementary gates in a quantum circuit

**depth:** max. length of a directed path from in- to output

**interacting pair of quantum circuits:** partition of circuit with disjoint sets of inputs, all outputs on one side

**communication cost:** no. wires between interacting pairs

**$(n, t)$ -simulation:** of a QTM  $M$  by a quantum circuit  $C$ , if input  $\tilde{x} \in \{0, 1\}^n$  evolved by  $C$  is the same as the state of  $M$  after  $t$  steps



# theorems by Yao

- 1 unitary operator  $U \in \mathbb{C}^{2^n}$  can be simulated by quantum network using  $2^{\mathcal{O}(n)}$  3-gates, with  $\mathcal{O}(n)$  wires
- 2 every QTM can be  $(n, t)$ -simulated by a quantum network of size  $\text{poly}(n, t)$
- 3  $\exists$  universal QTM that can simulate any other QTM with only polynomial slowdown

## Everett's interpretation

computation takes place in parallel universes

### application

stock market:

- input: stocks of today
- calculate a time  $t$  to predict new stocks
- failure with 50%
- other 50% yield result of calculation time  $2t$
- in average computation times are the same

## summary 3

### most important

- QTM can be simulated by quantum circuit or other QTM with polynomial slowdown
- quantum computer "calculates in parallel universes", not faster in average

## 1 Introduction

- overview
- literature
- two basic models

## 2 Quantum Gates

- definitions
- Toffoli- and Q-gate
- universality

## 3 Quantum Turing Machine

- Church-Turing
- step operator
- dynamics

## 4 Complexity

- theorems
- Everett's interpretation; stock market

# discussion

questions...

answers...