Computational models for quantum computation

Pascal Steger

Proseminar in theoretical physics, 2008

ETH Zürich

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

two models

two basic models for quantum computation

- quantum computational network, built of quantum gates

two models

two basic models for quantum computation

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

two models

two basic models for quantum computation

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

connections between models

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

two models

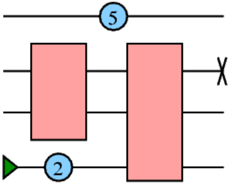
two basic models for quantum computation

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

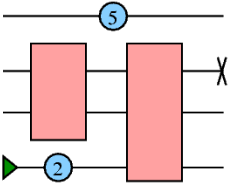
connections between models

- 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



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



logic circuit: computing machine consisting of logic gates; computational steps synchronized; outputs(i)=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

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

physical processes in gates

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

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 $\hat{O}$.

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:

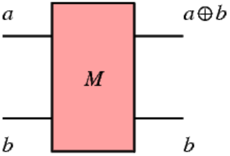
eigenstates of $\hat{I}$ and $\hat{O}$ in Schrödinger picture, if they coincide.

- by table
- by permutation: let $\{|a, b\rangle\}, \quad a, b \in \{0, 1\}$ be the four computational basis states, then:

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

- by S-Matrix, more suitable for quantum gates

example: 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

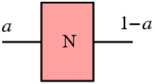
S-matrix

- $S^{ab\dots}_{a'b'\dots}$ 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 $S^{ab\dots}_{a'b'\dots}$

$$|a,b\rangle \to \sum_{a',b'\in\{0,1\}} S^{ab}_{a'b'}|a',b'\rangle \equiv S|a,b\rangle. \qquad (1)$$

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

example: NOT-gate

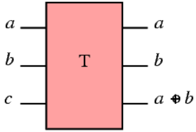


$$S_N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2}$$

$$S_{N^\alpha} = S_N^\alpha = \frac{1}{2}\begin{pmatrix} 1+e^{i\pi\alpha} & 1-e^{i\pi\alpha} \\ 1-e^{i\pi\alpha} & 1+e^{i\pi\alpha} \end{pmatrix} \tag{3}$$

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

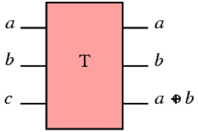
Toffoli gate in quantum computation



- classical gate: Toffoli

$$S^{abc}_{T a' b' c'} = \delta^a_{a'} \delta^b_{b'} [(1 - ab)\delta^c_{c'} + ab(S_N)^c_{c'}] \qquad (4)$$

Toffoli gate in quantum computation



- classical gate: Toffoli

$$S^{abc}_{Ta'b'c'} = \delta^a_{a'}\delta^b_{b'}[(1-ab)\delta^c_{c'} + ab(S_N)^c_{c'}] \tag{4}$$

- analogon: quantum gate Q

$$S^{abc}_{Qa'b'c'} = \delta^a_{a'}\delta^b_{b'}\left[(1-ab)\delta^c_{c'} + iabe^{-i\pi\alpha/2}(S^\alpha_N)^c_{c'}\right] \tag{5}$$

quantum gates: example NOT

$$S_{N^2} = S_N^2 = I, \tag{6}$$

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

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

time before non-classical behaviour:

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

definitions

computationally equivalent: same output for same input

problem: exact equivalence not possible, e.g. NOT

definitions

computationally equivalent: same output for same input

problem: exact equivalence 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

$$\lim_{n\to\infty} S_{g_n} e^{i\phi_n} = S_f \tag{8}$$

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

definitions

computationally equivalent: same output for same input

problem: exact equivalence 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

$$\lim_{n\to\infty} S_{g_n} e^{i\phi_n} = S_f \tag{8}$$

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

universal: set of quantum gates that is adequate to set of all gates

Claim:

The Q-gate is universal.

Claim:

The Q-gate is universal.

Proof:

create repetoire 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 $0 = |000\rangle$, $1 = |001\rangle$, ..., $6 = |110\rangle$, $7 = |111\rangle$

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

$S_Q^{4n+1} = S_T$ 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 repetoire, proof similar to that for NOT
Toffoli universal for all logic gates $\Rightarrow$ all logic gates in repetoire

proof: step 3: 3-bit quantum gates

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

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

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

$$\lim_{n\to\infty} [P_{56}(U_{\sqrt{\lambda/n}}P_{57})^2(U_{-\sqrt{\lambda/n}}P_{57})^2P_{56}]^n$$

$$= \begin{pmatrix} \mathbb{1} & & \\ & \cos\lambda & \sin\lambda \\ & -\sin\lambda & \cos\lambda \end{pmatrix} \equiv V_\lambda$$

$$\lim_{n\to\infty} [U_{\sqrt{\lambda/2n}}V_{\sqrt{\lambda/2n}}U_{-\sqrt{\lambda/2n}}V_{-\sqrt{\lambda/2n}}$$

$$= \mathrm{diag}(1,\dots,1,e^{-i\lambda},e^{i\lambda}) \equiv W_\lambda$$

change in global phase factor does not change observable:

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

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

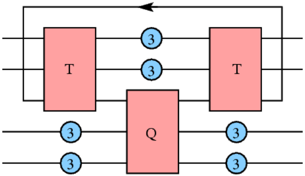
$$
\begin{aligned}
|\Psi\rangle &= \sum_{n=0}^{7} c_n|n\rangle, \quad \sum_{n=0}^{7}|c_n|^2 = 1 \\
Z_6[|\Psi\rangle] &:= X_{-\arg(c_6 c_7)/2} V_{-\arctan|c_6/c_7|} W_{-\arg(c_7/c_6)/2} \\
|\Psi\rangle &\Rightarrow \sum_{n=0}^{5} c_n|n\rangle + 0 + \sqrt{|c_6|^2 + |c_7|^2}|7\rangle
\end{aligned}
$$

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

$$
\begin{aligned}
S &= \sum_{n=0}^{7} e^{i\sigma_n}|\Psi_n\rangle\langle\Psi_n|; \\
S &= \prod_{n=0}^{7} S_{G^{-1}[|\Psi_n\rangle]} X_{\sigma_n} S_{G[|\Psi_n\rangle]}
\end{aligned}
$$

Q is universal to all 3×3-matrices

proof: 4,5: *n* bit gates, circuits



- 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

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

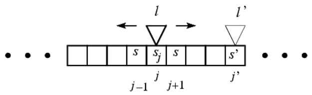
same procedure to get *n*-bit gates.

summary 1

Most important

- Q-gate is universal wrt the set of all quantum gates
- proof constructs repetoire of gates that are universal

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 realizible physical system can be perfectly simulated by a universal computing machine operating by finite means.

QTM fulfills principle, but not hypothesis

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
- requirements: locality, displacement in at most one direction, periodicity (lattice sites)

$$
\begin{aligned}
\langle l', j', s' | T | l, j, s \rangle &= \langle s'_{\neq j} | s_{\neq j} \rangle \langle l', j', s'_{j'} | \tilde{T} | l, j, s_j \rangle, \\
\tilde{T} &= \sum_{j=-\infty}^{\infty} \sum_{\Delta=-1}^{1} P_{j+\Delta} \tilde{T} P_j, \\
\langle l', j' + \Delta, s' | \tilde{T} | l, j', s' \rangle &= \langle l', j + \Delta, s' | \tilde{T} | l, j, s \rangle.
\end{aligned}
$$

Hamiltonian

according Feynman:

$$H \propto 2 - T - T^\dagger \tag{9}$$

for one gate (Deutsch):

$$H = \frac{i}{T} \ln S \tag{10}$$

- note: T can be a sum of elementary, unitary step operators for gates
- T not necessarily unitary for construction of Hamiltonian, time dependence $T \propto e^{-iHt}$
- H is local; description complexity keeps relatively small

summary 2

most important

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

complexity: definitions

size: number of elementary gates in a quantum circuit

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

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: own inputs, all outputs on one side

communication cost: no. wires between interacting pairs

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: own 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

majority function: logic function:

$$f(\vec{x}, \vec{y}) = 1 \text{ if at least } n \text{ 1s in input} \tag{11}$$

theorems by Yao

1. $U \in \mathbb{C}^{2n}$ can be simulated by quantum network using $\mathcal{O}^{2n}$ 3-gates, with $\mathcal{O}(n)$ wires
2. every QTM can be (n, t)-simulated by a quantum network of size $poly(n, t)$
3. $\exists$ universal QTM that can simulate any other QTM with only polynomial slowdown
4. quantum communication complexity (min cost) of f is $\geq \Omega(\log \log n)$.
5. majority function grows faster than linear

Everett's interpretation

computation takes place in parallel universes

Everett's interpretation

computation takes place in parallel universes

application

stock market:

- input: stocks of today
- calculate one day (time t)
- failure with 50%
- other 50% yield result of two days ($2t$) calculation time
- in average computation times are the same

summary 3

most important

- QTM can be simulated by quantum circuit or other QTM with polynomial slowdown

summary 3

most important

- QTM can be simulated by quantum circuit or other QTM with polynomial slowdown
- min. cost of f is $\geq \Omega(\log \log n)$.

summary 3

most important

- QTM can be simulated by quantum circuit or other QTM with polynomial slowdown
- min. cost of f is $\geq \Omega(\log \log n)$.
- computation takes place in parallel universes

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...