Quantum Computing

Proseminar in Theoretical Physics
Institut für theoretische Physik
ETH Zürich

Prof. Dr. Helmut G. Katzgraber
Prof. Dr. Renato Renner

SS07

typeset, compilation & editing by H. G. Katzgraber

Table of Contents

TABLE OF CONTENTS

Chapter 1

Computational Models for Quantum Computation

Pascal Stephan Philipp Steger
supervisor: Dr. Stefan Hohenegger

The quantum Turing machine and quantum networks are described as the two basic models of quantum computation. The quantum mechanical descriptions using S-matrices and Hamiltonians for the quantum gates as well as the step operator T for both gates and the quantum Turing machine are summarized. Finally, connections between the two models are established through theorems from complexity theory.

1.1 Introduction

I will concentrate on the articles by Deutsch ([1], [2]) for quantum networks, Benioff ([3]) for quantum Turing machines and Yao ([4]) for complexity theory. There exist two basic models for quantum computation: The quantum computational network, built of quantum gates and the Quantum Turing Machine (hereafter QTM). Connections between these models will be established through complexity theory and the step operator, which is a quantum mechanical description.

1.2 Quantum Gates

1.2.1 Logic Circuits

A *computation* is a process that produces output depending on input. *Input* and *output* denote abstract symbols. A *bit* or *quantum* is the smallest possible quantity of non-probabilistic information. The information is physically represented in a carrier, e.g. spin 1/2-particle. A *logic circuit* is a computing machine consisting of logic gates. The computational steps are synchronized. The outputs of step (i) can be used as inputs for step $(i+1)$. Sources (triangles) and sinks (crosses) can be used: A *source* is a gate with only one output that emits 0 or 1 in each step, it is reversible. A sink on the other hand has only one input and deletes information; it is irreversible. A *unit wire* computes the identity function, a fixed time dilation is indicated as number in a circle. Physical processes in a quantum computer follow three steps:

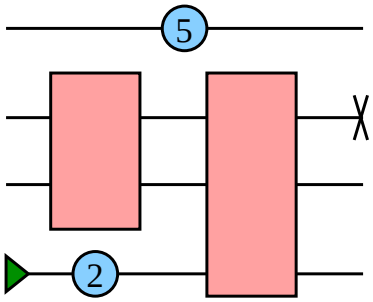

Figure 1.1: Example for a logic circuit showing different pieces.

1. preparation of the input states in carriers
2. QM elastic scattering (errorless)
3. measurement of output carriers after fixed step

The last two steps can be seen as happening in a black box. The actual scattering and projection of the state are implementation-specific and do not inferere with the theoretical model. What is a *logic gate*? It is a computing machine, where input and output consist of fixed number of bits. A fixed computation is done in fixed time. A *quantum gate* can have states of input and output to be quantum mixtures of eigenstates of the input observable $\hat{I}$ and output observable $\hat{O}$. These are called qubits. A *reversible gate* has the property that inputs and outputs are related by an invertible function (in the ideal case, if no errors occur).

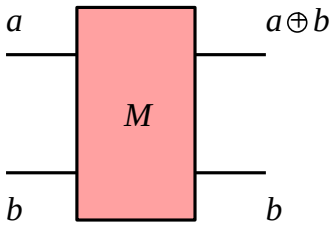

Figure 1.2: measurement gate - XOR - CNOT

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

1.2.2 Mathematical Descriptions

Several mathematical descriptions of gates are possible. We choose a *computational basis* by the eigenstates of $\hat{I}$ and $\hat{O}$ in the Schrödinger picture. They both have to be the same. In this basis one can write down the action of a gate using a table. As an example look at the gate in figure 1.2. This gate is called XOR since it computes the (logical) XOR function from inputs a and b, copying a as a second output to guarantee reversiblity. Its action can also be understood as inverting the b input if a is set and returning b unchanged otherwise. Therefore it is also referred to as CNOT (controlled NOT) or measurement gate. Another way of description uses permutation: let $\{|a,b\rangle\}, \quad a,b \in \{0,1\}$ be the four computational basis states for a system with two inputs and outputs. A gate transforms inputs into outputs, e.g. A third way is given by using a S-Matrix, this is most

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

suitable for quantum gates. $S^{ab\ldots}_{a'b'\ldots}$ has clumped indices $ab\ldots$, $a'b'\ldots$ denoting the states of the input and output carriers. The operation of a gate corresponds to a matrix multiplication with $S^{ab\ldots}_{a'b'\ldots}$

$$|a,b,\ldots\rangle \rightarrow \sum_{a',b',\ldots\in\{0,1\}} S^{ab\ldots}_{a'b'\ldots}|a',b',\ldots\rangle \equiv S|a,b,\ldots\rangle. \tag{1.1}$$

In this picture repeated gates are represented by powers of S. If no basis chosen explicitly, S can also denote a linear operator. For an example, consider the NOT gate in fig. 1.3.

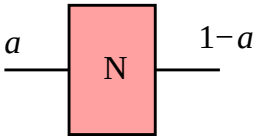

Figure 1.3: NOT gate

$$S_N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1.2}$$

$$S_{N^\alpha} = S_N^\alpha = \frac{1}{2}\begin{pmatrix} 1+e^{i\pi\alpha} & 1-e^{i\pi\alpha} \\ 1-e^{i\pi\alpha} & 1+e^{i\pi\alpha} \end{pmatrix} \tag{1.3}$$

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

1.2.3 Toffoli and Q

An analogon to the Toffoli gate in quantum computation is depicted in fig. 1.4. Its classical version can be described by the S-matrix

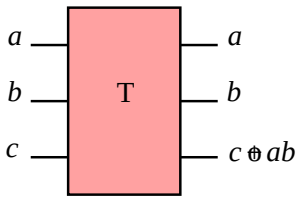

Figure 1.4: Toffoli gate

$$S^{abc}_{Ta'b'c'} = \delta^a_{a'}\delta^b_{b'}[(1-ab)\delta^c_{c'} + ab(S_N)^c_{c'}] \tag{1.4}$$

Analogously, the quantum gate Q reads as

$$S^{abc}_{Qa'b'c'} = \delta^a_{a'}\delta^b_{b'}\left[(1-ab)\delta^c_{c'} + iabe^{-i\pi\alpha/2}(S^\alpha_N)^c_{c'}\right] \tag{1.5}$$

Explicitly writing them out, we have to use a certain basis, e.g. $0 = |000\rangle$, $1 = |001\rangle$, ..., $6 = |110\rangle$, $7 = |111\rangle$. The S-matrix is given by

$$\begin{aligned} S_T &= \begin{pmatrix} \mathbb{1} & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix} \\ S_Q &= \begin{pmatrix} \mathbb{1} & & \\ & i\cos\pi\alpha/2 & \sin\pi\alpha/2 \\ & \sin\pi\alpha/2 & i\cos\pi\alpha/2 \end{pmatrix} \end{aligned}$$

Example NOT

$$S_{N^2} = S_N^2 = \mathbb{1}, \tag{1.6}$$

$$(S_{N^\alpha})^m = S_N^{m\alpha} = S_N^{m\alpha - 2\lfloor m\alpha/2 \rfloor}. \tag{1.7}$$

The exponent $1+\varepsilon$ is arbitrarily close to 1, but never exact for an irrational α, $m \in \mathbb{N}$. The time before non-classical behaviour can be expressed as the reciprocal of the expectation value for the wrong result:

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

Two circuits are called *computationally equivalent*, if they yield the same output given the same input. Exact equivalence is not possible in QM, see for example the repeated NOT gate. F and G are *adequate sets*, if there exists a series $\{g_n \in G\}$ for all $f \in F$ and a sequence $\{\phi_n\}$ of phase angles such that

$$\lim_{n\to\infty} S_{g_n} e^{i\phi_n} = S_f \tag{1.8}$$

$F = \{N\}$ and $G = \{N^\alpha, \mathbb{1}\}$ are adequate for example. A *universal gate* is a quantum gate such that the set of unit wire, source and this gate is adequate to set of other gates

Claim:

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

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

Step 1 and 2: Toffoli gate

Choose basis $0 = |000\rangle$, $1 = |001\rangle$, ..., $6 = |110\rangle$, $7 = |111\rangle$. One can compute the $4n+1$-th power of S_Q,

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

$S_Q^{4n+1} = S_T$ for arguments $\pi(2m+1/2)$, $m \in \mathbb{N}$; it is arbitrarily close to the Toffoli gate with $\pi\alpha(2n+1/2)$ for some $n \in \mathbb{N}$. The Toffoli gate is therefore in the repetoire, the proof goes similar to the one for the one that powers of QM NOT are adequate to the logical NOT. Moreover, the Toffoli gate is universal for all logic gates, meaning that all logic gates in repetoire.

Step 3: 3-bit quantum gates

Consider now powers of the form $4n$ with $n \in \mathbb{N}$:

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

These are in the repetoire, since there exists $m \in \mathbb{N}$ such that $|2\pi n\alpha - 2\pi m| < \varepsilon$ for ε arbitrarily small. Permutations are logic gates, and therefore in the repetoire; the limit of combinations of permutations and U does also:

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

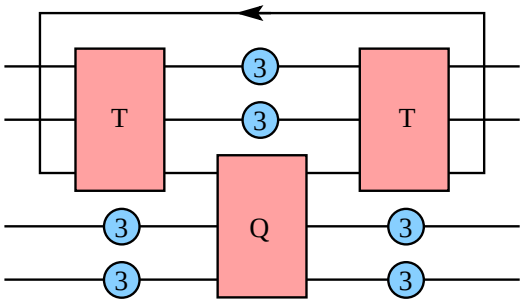

Figure 1.5: General gate with four qubits.

A change in global phase factor does not change the expectation value of an observable:

$$X_\lambda \equiv \mathrm{diag}(1, \ldots, 1, e^{i\lambda}) \tag{1.9}$$

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

$$\begin{aligned} |\Psi\rangle &= \sum_{n=0}^{7} c_n |n\rangle, \quad \sum_{n=0}^{7} |c_n|^2 = 1 \\ Z_6[|\Psi\rangle] &:= X_{-\arg(c_6 c_7)/2} V_{-\arctan|c_6/c_7|} W_{-\arg(c_7/c_6)/2} \\ |\Psi\rangle &\Rightarrow \sum_{n=0}^{5} c_n |n\rangle + 0 + \sqrt{|c_6|^2 + |c_7|^2}|7\rangle \end{aligned} \tag{1.10}$$

By analogy follows that the map $G: c_i \to 0, i < 7$ as a gate is in the repetoire. More generally:

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

Q is universal to all 3×3-matrices

STEP 4 & 5: n BIT GATES

Look at a possible general four-bit gate in fig. 1.5. The loopback is necessary to connect all inputs and outputs. It is initialized to 0. By plugging in all 2^4 inputs it can be verified that its output is always 0. This loopback makes the circuit reversible, the use of a source and a sink would yield irreversible gates.

$$S^{abcd}_{Q_4 a' b' c' d'} = \delta^a_{a'} \delta^b_{b'} \delta^c_{c'} [(1 - abc)\delta^d_{d'} + iabc e^{-i\pi\alpha/2} (S^\alpha_N)^d_{d'}]$$

One can use the same procedure to get n-bit gates. Therefore the n-bit gates are also in the repetoire. This closes the proof.

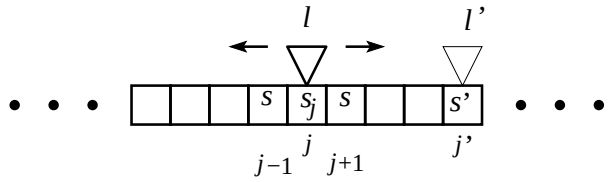

Figure 1.6: QTM

1.3 Quantum Turing Machine

1.3.1 Quantum Turing Machine (QTM)

As analogon to the classical a QTM consists of a finite processor and an infinite memory. Computation proceeds in steps of fixed duration T. During a step only the processor and a finite part of memory interact. It *halts*, if two subsequent states identical or if the halt flag set. The *halt flag* is an observable with spectrum $\{0, 1\}$, independent of $\hat{I}$. It's state is measurable without disturbing the state of the QTM. The QTM is universal, it can simulate any other quantum computer.

1.3.2 Church-Turing

The Church-Turing hypothesis states that every function which would naturally be regarded as computable can be computed by the universal Turing machine. Expressed in a more physical way, this reads as: Ëvery finitely realizible physical system can be perfectly simulated by a universal computing machine operating by finite means.¨
The QTM fulfills this principle. A Turing machine does not fulfill the second version, since it is finite, but continuous systems can be described with only a few parameters.

1.3.3 Step Operator

A step operator describes a single step of computation. The head of a QTM interacts with the tape only at one position in a fixed time. It can move to the left, to the right, or stay and interact. All this can be described with a unitary *step operator* T. It must be local and may describe a displacement in at most one direction. Moreover, the periodicity of the lattice sites must be taken into

account. Mathematically these three requirements are expressed with

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

1.3.4 Dynamics

The dynamics of a QTM can be described by its Hamiltonian. For gates this is, according Deutsch,

$$H \equiv \frac{i}{t}\ln S. \tag{1.11}$$

H is local; the description complexity is relatively small. Feynman proposed another form of H,

$$H \equiv K(2 - T - T^\dagger). \tag{1.12}$$

This gives the kinetic energy, if T is only a displacement. T by itself can be a sum of elementary unitary step operators for single gates and therefore describes the evolution of a whole circuit.

1.4 Complexity

The *size* of a circuit gives the number of elementary gates in a quantum circuit. The *depth* is the maximal length of a directed path from in- to output register. An *interacting pair of quantum circuits* describes a partition of the circuit with disjoint sets of inputs such that all outputs are on one side. The *communication cost* gives then the number of wires between interacting pairs. A quantum circuit (n, t)-*simulates* a QTM, 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. Any unitary operator $U \in \mathbb{C}^{2^n}$ can be simulated by a 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 $poly(n, t)$.
3. There exists a universal QTM that can simulate any other QTM with only polynomial slowdown

See Yao 1993 [4] for a proof of these theorems.

1.4.1 QTM vs. TM: computation speed

A QTM is not faster than a classical Turing machine on average if it is performing simple calculations. There is a huge speed-up, however, if specialized algorithms like the ones of Deutsch-Josza and Grover are considered. One could imagine these algorithms taking advantage of "parallel universes" to instantiate copies of the QTM and return the result in a shorter time $t = pt_0, p < 1$, but with a failure probability of $1 - p$.

1.5 Summary

Quantum gates can have superpositions of states as input, the qubits. The Q-gate is universal wrt the set of all quantum gates. The proof thereof constructs a repetoire of gates that Q is adequate to. The QTM is constructed as a quantum analogon to Turing machine. It fulfills the Church-Turing principle and can be described by step operators or a Hamiltonian. A QTM can be simulated by quantum circuit or other QTM with polynomial slowdown. A quantum computer "calculates in parallel universes", not faster in average.

Bibliography

[1] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proc. R. Soc. Lond. A **400**, 97 (1985).

[2] D. Deutsch, *Quantum computation networks*, Proc. R. Soc. Lond. A **425**, 73 (1989).

[3] P. Benioff, *Models of quantum turing machines*, Fortsch. Phys. **46**, 423 (2007).

[4] A. C. Yao, *Quantum Circuit Complexity*, Proc. of the 34th Ann. Symp. on Found. of Comp. Sc. (FOCS) p. 352 (1993).