Part III — Quantum Computation

Theorems

Based on lectures by R. Jozsa

Notes taken by Dexter Chua

Michaelmas 2016

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

Quantum mechanical processes can be exploited to provide new modes of information processing that are beyond the capabilities of any classical computer. This leads to remarkable new kinds of algorithms (so-called quantum algorithms) that can offer a dramatically increased efficiency for the execution of some computational tasks. Notable examples include integer factorisation (and consequent efficient breaking of commonly used public key crypto systems) and database searching. In addition to such potential practical benefits, the study of quantum computation has great theoretical interest, combining concepts from computational complexity theory and quantum physics to provide striking fundamental insights into the nature of both disciplines.

The course will cover the following topics:

Notion of qubits, quantum logic gates, circuit model of quantum computation. Basic notions of quantum computational complexity, oracles, query complexity.

The quantum Fourier transform. Exposition of fundamental quantum algorithms including the Deutsch-Jozsa algorithm, Shor's factoring algorithm, Grovers searching algorithm.

A selection from the following further topics (and possibly others):

(i) Quantum teleportation and the measurement-based model of quantum computation;
(ii) Lower bounds on quantum query complexity;
(iii) Phase estimation and applications in quantum algorithms;
(iv) Quantum simulation for local hamiltonians.

Pre-requisites

It is desirable to have familiarity with the basic formalism of quantum mechanics especially in the simple context of finite dimensional state spaces (state vectors, Dirac notation, composite systems, unitary matrices, Born rule for quantum measurements). Prerequisite notes will be provided on the course webpage giving an account of the necessary material including exercises on the use of notations and relevant calculational techniques of linear algebra. It would be desirable for you to look through this material at (or slightly before) the start of the course. Any encounter with basic ideas of classical theoretical computer science (complexity theory) would be helpful but is not essential.

Contents

0 Introduction

1 Classical computation theory

2 Quantum computation

Lemma. For any boolean function $f : B_m \to B_n$, the function

$$\begin{aligned} \tilde{f} : B_{m+n} &\to B_{m+n} \\ (x, y) &\mapsto (x, y \oplus f(x)), \end{aligned}$$

is invertible, and in fact an involution, i.e. is its own inverse.

Lemma. Let $g : B_k \to B_k$ be a reversible permutation of k-bit strings. Then the linear map on $\mathbb{C}^k$ defined by

$$A : |x\rangle \mapsto |g(x)\rangle$$

on k qubits is unitary.

3 Some quantum algorithms

3.1 Balanced vs constant problem

3.2 Quantum Fourier transform and periodicities

Proposition. QFT is unitary.

3.3 Shor's algorithm

Lemma. For $a_1, a_2, \cdots, a_\ell$ any positive reals, we set

$$\begin{aligned} p_0 &= 0 & q_0 &= 1 \\ p_1 &= 1 & q_1 &= a_1 \end{aligned}$$

We then define

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k q_{k-1} + q_{k-2} \end{aligned}$$

Then we have

(i) We have

$$[a_1, \cdots, a_k] = \frac{p_k}{q_k}.$$

(ii) We also have

$$q_k p_{k-1} - p_k q_{k-1} = (-1)^k.$$

In particular, p_k and q_k are coprime.

3.4 Search problems and Grover's algorithm

Theorem. Let A be any quantum algorithm that solves the unique search problem with probability $1 - \varepsilon$ (for any constant ε), with T queries. Then T is at least $O(\sqrt{N})$. In fact, we have

$$T \geq \frac{\pi}{4}(1 - \varepsilon)\sqrt{N}.$$

3.5 Amplitude amplification

Theorem (Amplitude amplification thoerem)**.** In the 2-dimensional subspace spanned by $|\psi_g\rangle$ and $|\psi\rangle$ (or equivalently by $|\psi_g\rangle$ and $|\psi_b\rangle$), where

$$|\psi\rangle = \sin\theta\,|\psi_g\rangle + \cos\theta\,|\psi_b\rangle\,,$$

we have that $\mathcal{Q}$ is rotation by 2θ.

4 Measurement-based quantum computing

Theorem. Let C be any quantum circuit on n qubits with a sequence of gates $U_1, \cdots, U_K$ (in order). We have an input state $|\psi_{\text{in}}\rangle$, and we perform Z-measurements on the output states on specified qubits $j = i_1, \cdots, i_k$ to obtain a k-bit string.

We can always simulate the process as follows:

(i) The starting resource is a graph state $|\psi_G\rangle$, where G is chosen depending on the connectivity structure of C.

(ii) The computational steps are 1-qubit measurements of the form $\mathsf{M}_i(\alpha)$, i.e. measurement in the basis $\mathcal{B}(\alpha)$. This is adaptive — α may depend on the (random) outcomes $s_1, s_2, \cdots$ of previous measurements.

(iii) The computational process is a prescribed (adaptive) sequence $\mathsf{M}_{i_1}(\alpha_1)$, $\mathsf{M}_{i_2}(\alpha_2)$, $\cdots$, $\mathsf{M}_{i_N}(\alpha_N)$, where the qubit labels $i_1, i_2, \cdots, i_N$ all distinct.

(iv) To obtain the output of the process, we perform further measurements $\mathsf{M}(\mathsf{Z})$ on k specified qubits not previously measured, and we get results $s_{i_1}, \cdots, s_{i_k}$, and finally the output is obtained by further (simple) *classical* computations on $s_{i_1}, \cdots, s_{i_k}$ as well as the previous $\mathsf{M}_i(\alpha)$ outcomes.

Lemma (J-lemma)**.** Given any 1-qubit state $|\psi\rangle$, consider the state

$$\mathsf{E}_{12}(|\psi\rangle_1 |+\rangle_2).$$

Suppose we now measure $\mathsf{M}_1(\alpha)$, and suppose the outcome is $s_1 \in \{0, 1\}$. Then after measurement, the state of 2 is

$$\mathsf{X}^{s_1} \mathsf{J}(\alpha) |\psi\rangle .$$

Also, two outcomes $s = 0, 1$ always occurs with probability $\frac{1}{2}$, regardless of the values of $|\psi\rangle\, b, \alpha$.

Lemma. Suppose we start with a state

$$|\psi\rangle_{1\mathcal{S}} = |0\rangle_1 |a\rangle_{\mathcal{S}} + |1\rangle_1 |b\rangle_{\mathcal{S}} .$$

We then apply the J-lemma process by adding a new qubit $|+\rangle$ for $2 \notin \mathcal{S}$, and then query 1. Then the resulting state is

$$\mathsf{X}_2^{s_1} \mathsf{J}_2(\alpha) |\psi\rangle_{2\mathcal{S}} .$$

Lemma (Concatenation lemma)**.** If we concatenate the process of J-lemma on a row of qubits $1, 2, 3, \cdots$ to apply a sequence of $\mathsf{J}(\alpha)$ gates, then all the entangling operators $\mathsf{E}_{12}, \mathsf{E}_{23}, \cdots$ can be done *first* before any measurements are applied.

5 Phase estimation algorithm

Theorem. If the measurements in the above algorithm give $y_0, y_1, \cdots, y_n$ and we output

$$\theta = 0.y_0 y_1 \cdots y_{n-1},$$

then

(i) The probability that θ is φ to n digits is at least $\frac{4}{\pi^2}$.

(ii) The probability that $|\theta - \varphi| \geq \varepsilon$ is at most $O(1/(2^n \varepsilon))$.

6 Hamiltonian simulation

Proposition.

$$\|A + B\| \leq \|A\| + \|B\|$$
$$\|AB\| \leq \|A\| \|B\| .$$

Theorem (Solovay-Kitaev theorem)**.** Let U be a unitary operator on k qubits and S any universal set of quantum gates. Then U can be approximated to within ε using $O(\log^c \frac{1}{\varepsilon})$ from S, where $c < 4$.

Lemma. Let $\{U_i\}$ and $\{V_i\}$ be sets of unitary operators with

$$\|U_i - V_i\| \leq \varepsilon.$$

Then

$$\|U_m \cdots U_1 - V_m \cdots V_1\| \leq m\varepsilon.$$

Proposition. Let

$$H = \sum_{j=1}^m H_j$$

be any k-local Hamiltonian with commuting terms.

Then for any t, e^{-iHt} can be approximated to within ε by a circuit of

$$O\left(m \operatorname{poly}\left(\log\left(\frac{m}{\varepsilon}\right)\right)\right)$$

gates from any given universal set.

Lemma (Lie-Trotter product formula)**.** Let A, B be matrices with $\|A\|, \|B\| \leq K < 1$. Then we have

$$e^{-iA} e^{-iB} = e^{-i(A+B)} + O(K^2).$$