Quantum Computation and Algorithms Dr. Toby Cubitt

Problem Sheet

Computation and Complexity

1. (a) Prove that the (classical) gate set $\{AND, NOT, FANOUT\}$ is universal.

   (b) Prove that the $TOFFOLI$ gate can be used to reversibly-compute AND, NOT, and $FANOUT$.

   (c) Prove that, without loss of generality, all measurements in a quantum circuit can be postponed until the very end.

First Algorithms

2. (a) **(Euclid's algorithm)** Prove Euclid's algorithm for computing $gcd(a, b)$ works, and performs $O(logb)$ divisions for $b \geq a$. Use this to argue that $GCD \in P$.

   (b) **(Exponentiation by squaring)** Prove that a^n can be computed using $O(\log n)$ multiplications.

   Hint: Try calculating 13^9 *by hand. (Pen and paper only, no calculators!) Do any shortcuts occur to you?*

3. **(Deutsch-Jozsa)** Construct a classical probabilistic algorithm that solves the Deutsch-Jozsa problem with probability $\geq 1 - \epsilon$ using $O(\log 1/\epsilon)$ queries to the black-box oracle.

QFT and Phase Estimation

4. **(QFT)** Show that for any δ, there is a circuit $\widetilde{QFT}$ on n qubits such that:

   (i). The circuit contains only $O(\operatorname{poly} n)$ gates from the standard gate set.

   (ii). $\|QFT_{2^n} - \widetilde{QFT}\| \leq \delta$.

   Hint: Consider the circuit obtained by dropping all controlled-phase gates with exponentially small phase rotations from the original QFT circuit.

5. **(Phase Estimation)** Prove that running the phase estimation circuit for black-box unitary U on an arbitrary input state φ, produces an estimate $\tilde{\theta}_i$ to the phase θ_i of the eigenvalue associated with eigenvector $|\varphi_i\rangle$ of U, chosen at random according to probability distribution $|\langle\varphi|\varphi_i\rangle|^2$.

Shor's algorithm

6. (a) Prove that U_a defined by $U_a\,|x\rangle = |ax \pmod N\rangle$ is unitary if $gcd(a, N) = 1$.

   (b) Using exponentiation by squaring and properties of modular arithmetic, or otherwise, show that $U_a^{2^n}$ can be implemented in time $O(\operatorname{poly} n)$.

7. Prove that there is a quantum algorithm that solves order-finding with success probability $\geq 1 - \delta$ in total run-time $O(n^3 \log n \log 1/\delta)$.

Grover's algorithm

8. **(Exact Grover search)** Let $f : \{0,1\}^n \to 0,1$ be a black-box boolean function. Let $\Pi_G = \sum_{x:f(x)=1} |x\rangle\langle x|$ where $x \in \{0,1\}^n$ and $\Pi_G^\perp$ be the projector onto the "good" subspace. Assume that the state $|\psi\rangle = s\,|\varphi\rangle + c\,|\varphi^\perp\rangle$ can be constructed efficiently, and that the value s is known.

   By adjoining an extra qubit (suitably extending the notion of goodness/badness from x to $x0$ and $x1$) and using at most one extra (quantum) query to f, show that the Amplitude Amplification algorithm for unstructured search can be made exact. I.e. the final measurement of the modified process will yield an x such that $f(x) = 1$ with certainty.

   Hint: Recall Grover search for "1 in 4".

Part B-style exam questions

9. **Bernstein-Vazirani** Let $s \in \{0,1\}^n$ be an n-bit string. Let $f : \{0,1\}^n \to \{0,1\}$ be the boolean function defined by $f(x) = x \cdot s = x_1 s_1 \oplus x_2 s_2 \oplus \cdots \oplus x_n s_n$. Let $U_f\,|x\rangle\,|b\rangle = |x\rangle\,|b \oplus f(x)\rangle$ be the corresponding quantum oracle for f, where $b \in \{0,1\}$ is a single bit. ($\oplus$ denotes addition modulo 2.) Using a construction similar to the Deutsch-Jozsa algorithm, or otherwise, prove that there is a quantum algorithm that determines s using only one query to U_f.

10. **Period finding**

    (a) Let $f : \mathbb{Z}_n \to \mathbb{Z}_m$ be a periodic boolean function with period r. I.e. $f(x + r \pmod{n}) = f(x) \pmod{m}$. Let $U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle$ be the corresponding quantum oracle for f. By using the inverse-QFT, or otherwise, show how a single query to U_f suffices to obtain a value kn/r, with $k \in \{0,\dots,r-1\}$ chosen uniformly at random.

    (b) Briefly explain how this could be applied to solve the Order-Finding problem.