Lecture 12

Comment: HW1 graded, grade to be released today. HW2 to be released by this Friday.

Cont'd from last time. Three ways of thinking of the partial measurement:

1. direct from definition
2. expand first
3. use lemma from last time (will be useful in generalization to Deutsch-Jozsa).

Justification for the problem setup The setup is often referred to as the quantum query model. So we would say, for example, the "Deutsch's problem can be solved using one quantum query but two classical queries."

First do three-gate $f\colon \{0,1\} \to \{0,1\}$, $x \mapsto \bar{x} \wedge x$ as an example. The three gates are FANOUT, NOT, AND.

Definition 12. Let $f\colon \{0,1\}^m \to \{0,1\}^n$, the quantum oracle of f is the unitary (in fact, permutation) matrix $O_f \in \mathbb{C}^{2^{n+m}\times 2^{n+m}}$ defined by

$$O_f\colon \ |x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus f(x)\rangle\,. \tag{73}$$

Fact 4. Any $f\colon \{0,1\}^m \to \{0,1\}^n$ can be implemented as a classical circuit involving FANOUT, NOT, AND, OR gates (with ancilla bits).

Proof by example. Consider $f\colon \{0,1\}^2 \to \{0,1\}$. Suppose $f(00) = f(11) = 1$, then $f = (x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$. Comment: Can also make it interactive. □

Fact 5. Suppose we have the description of a classical circuit implementing the function $f\colon \{0,1\}^n \to \{0,1\}^m$ in terms of FANOUT, NOT, AND, OR gates. Then we can efficiently implement the quantum oracle for f. More precisely, the implementation takes linear time in the size of the classical circuit.

Proof sketch. The example we did above is essentially the proof. As in that example, we see FANOUT can be simulated using CNOT, NOT using X, AND using Toffoli. Note that OR can be simulated using X and Toffoli (think de Morgan's laws). For more details, see Section 6.3 of Watrous notes and accompanying video (in particular, starting at `45:37`). □

Deutsch-Jozsa problem. Given $f\colon \{0,1\}^n \to \{0,1\}$, ask balanced or constant. Classically, need $2^{n-1}+1$ queries f to solve with certainty. Quantumly, it turns out that only 1 (quantum) query to f suffices.

Remark 1. This problem is essentially the same as the all-zeros vs half-zeros problem: can view f as a length-2^n string $f(0^n), \ldots, f(1^n)$.