

# Course 2-11-2: Homework

Instructors: Iordanis Kerenidis, Julia Kempe, Miklos Santha

**Due on 26/01/2011**

1. Alice, Bob and Charlie share the following state:  $\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$ . They receive as input bits  $X_A, X_B, X_C$  respectively, which always satisfy  $X_A \oplus X_B \oplus X_C = 0$ . They wish to output  $a, b, c$  respectively such that  $X_A \vee X_B \vee X_C = a \oplus b \oplus c$ . Give a quantum protocol that achieves this with certainty.  
**Hint:** You will need the basis  $\{|+\rangle, |-\rangle\}$ .
2. i) Let  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  and  $U_f$  be the unitary operator that maps  $|x\rangle|b\rangle$  to  $|x\rangle|b \oplus f(x)\rangle$ , where  $x \in \{0, 1\}^n, b \in \{0, 1\}$ . Show that if we start with  $|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  then on input  $|x\rangle|b\rangle$ , the output is  $(-1)^{f(x)}|x\rangle|b\rangle$ , in other words, the transformation achieved is  $|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$ .  
  
ii) Let  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  a 4-to-1 function, i.e. there exist  $a, b \in \{0, 1\}^n$  with  $a \neq b$  and  $a, b \neq 0$  such that  $f(x) = f(x + a) = f(x + b) = f(x + a + b)$ . Give an efficient quantum algorithm to compute  $a$  and  $b$ .
3. **Variations on Grover's algorithm**
  - (a) *One faulty black-box:* Grover's algorithm, as we studied in class, applies a subroutine  $D \circ S_f$  a total of  $T$  times (assume  $T$  is odd here). Let's assume the following happens: At the  $(T + 1)/2$ -st run of the subroutine the black-box is subject to error, and instead of applying  $S_f = I_{2^n} - 2|w\rangle\langle w|$  it just applies the identity  $I_{2^n}$ . The subroutine is applied correctly in all the other runs. Analyse the behavior of this algorithm. Can it still find  $w$  with high probability? If yes, for which  $T$ ? If no, why?
  - (b)  *$r$  marked items:* We are given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  as a black box (let  $N = 2^n$ ), with the promise that there are exactly  $r$  of the inputs that evaluate to 1, all the other inputs evaluate to 0 (i.e.  $f(x) = 1$  iff  $x \in \{x_1, x_2, \dots, x_r\}$ ). (An input that evaluates to 1 is called a *marked item*). Give a quantum algorithm that finds (with a constant probability) one of the marked items using only  $O(\sqrt{\frac{N}{r}})$  queries. Analyze the algorithm and show that it does what it should. How many classical queries are needed for the same task (give a rough argument only).
  - (c) *Unknown number of marked items:* Assume we are given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  as a black-box (let  $N = 2^n$ ) and we do not know the number  $r$  of marked

items  $r = |\{x : f(x) = 1\}|$ . Design a quantum algorithm that finds a marked item with constant probability (say 1%) and uses  $O(\sqrt{N})$  queries. *Hint:*  $r$  lies between  $2^j$  and  $2^{j+1}$  for some  $j$ . Show that if you know  $j$  you would find the marked item with constant probability. Proceed to show what to do if  $j$  is not known.

4. **Collision finding:** We are given  $f : [N] \rightarrow [N]$  with the promise that  $f$  is two-to-one (i.e., for every  $i$  there is exactly one other element having the same value  $f(i)$ ). Our task is to find a collision, i.e. a pair  $\{i, j\}$  such that  $f(i) = f(j)$ .

- (a) Compare this problem with the problem for Simon's algorithm. Is it easier or harder?
- (b) Devise a quantum black-box algorithm that finds (with a constant probability) a collision using only  $O(N^{1/3})$  queries. (Hint: First make  $M$  classical queries  $x_1, \dots, x_M$  to  $f$ . Then look for a  $y$  such that  $f(x_i) = f(y)$  for one of the  $x_i \in \{x_1, \dots, x_M\}$ . Optimize  $M$ .)
- (c) Compare with classical algorithms (how well can a classical algorithm solve this problem?).

5. **Polynomial method:**

- (a) Let  $f : \{0, 1\}^N \rightarrow \{0, 1\}$  be a *symmetric* function. Prove that if there exists a degree  $k$  multi-variate polynomial  $p : \mathbb{R}^N \rightarrow \mathbb{R}$  that  $\epsilon$ -approximates  $f$ , then there exists a degree  $k$  *symmetric*, multi-variate polynomial  $p' : \mathbb{R}^N \rightarrow \mathbb{R}$  that  $\epsilon$ -approximates  $f$ .
- (b) Let  $p : \mathbb{R}^N \rightarrow \mathbb{R}$  be a degree  $k$  *symmetric* polynomial. Prove that there exists a degree  $k$  *univariate* polynomial  $q : \mathbb{R} \rightarrow \mathbb{R}$  such that for every  $x_1, \dots, x_N \in \{0, 1\}$ ,  $p(x_1, \dots, x_N) = q(\sum x_i)$ .
- (c) Prove that for any symmetric, non-trivial function  $f : \{0, 1\}^N \rightarrow \{0, 1\}$  we have  $\deg(f) \geq \frac{N}{2}$  and conclude that  $Q_E(f) \geq \frac{N}{4}$ . Here  $Q_E(f)$  denotes the *exact* query complexity of  $f$ , i.e. the number of queries to compute  $f$  exactly.