C&O 781 Topics in Quantum Information
Ideas from Quantum in Classical Computation
University of Waterloo
Spring 2002

Instructor: Ashwin Nayak
Assignment 1, May 22, 2009
Due: June 4, 2009, before the lecture

Question 1. [5 marks] In the Kerenidis-de Wolf lower bound for two-query LDCs, you saw a method for learning two bits with one quantum query by viewing the bits in the Hadamard basis. Generalize this method to learning n bits with as few quantum queries as possible. How many queries do you use to achieve non-zero constant success probability?

Question 2. [5 marks] Show that you cannot compute the XOR of *three* bits with one quantum query with probability greater than $1/2$. Therefore, the Kerenidis-de Wolf lower bound method does not directly extend to three-query LDCs.

Question 3. [5 marks] Given a basis $B = \{b_1, \ldots, b_n\}$ for $\mathbb{R}^n$, the set

$$\mathcal{L}(B)^* \quad = \quad \{x \in \mathbb{R}^n \ : \ \langle x, v \rangle \in \mathbb{Z}, \forall v \in \mathcal{L}(B)\},$$

the dual of the lattice $\mathcal{L}(B)$ is also a lattice. In other words, show that there is a basis $Y = \{y_1, \ldots, y_n\}$ such that $\mathcal{L}(B)^* = \mathcal{L}(Y)$.

Question 4. [5 marks] Show that the Shortest Vector Problem is well-defined. In other words, given a basis B for $\mathbb{R}^n$, show that there exists a vector $v \in \mathcal{L}(B), v \neq 0$, that achieves the minimum length among all non-zero vectors in the lattice. In particular, this minimum length is non-zero.

[Note: in the lectures, we assumed that the basis elements had rational coordinates. In that case, the above fact is straightforward.]