11 Quantum Computing (AD)

Let a_0a_1 be the two-bit representation of $a \in \{0, 1, 2, 3\}$. We define the 2-bit Boolean function f_a by:

$$f_a(x_0, x_1) = (a_0 \cdot x_0) \oplus (a_1 \cdot x_1).$$

where $\cdot$ denotes Boolean *and* and $\oplus$ represents *exclusive or*.

For each such function f, let U_f denote the 3-qubit unitary operator that computes f in the sense that:

$$U_f|x_0x_1y\rangle = |x_0x_1\rangle|y \oplus f(x_0, x_1)\rangle.$$

In the following, $H^{\otimes n}$ denotes the n-bit Hadamard operator.

(*a*) Show how U_{f_2} can be implemented with the use of C-NOT gates. [3 marks]

(*b*) Show that:

$$(H^{\otimes 2}\textsf{C-NOT}H^{\otimes 2})|xy\rangle = \textsf{C-NOT}|yx\rangle.$$

[3 marks]

(*c*) Using (*b*) or otherwise, show that for each of the four possible values of a, the operator $(H^{\otimes 3}U_{f_a}H^{\otimes 3})$ can be implemented as a circuit using only C-NOT gates. [6 marks]

(*d*) Given a black box implementing U_{f_a} for an unknown value of a, show that we can construct a quantum circuit that determines the value of a with certainty, using the black box only once.

[*Hint:* Consider the circuit from (*c*) applied to a suitable computational basis state.]

[8 marks]