2010 Paper 9 Question 11

Quantum Computing

(a) Which of the following are possible states of a qubit?

(i) $\frac{1}{\sqrt{2}}(|1\rangle + |0\rangle)$

(ii) $0.6|0\rangle + 0.4|1\rangle$

(iii) $0.8|0\rangle - 0.6e^{3i\pi/4}|1\rangle$

(iv) $\frac{\sqrt{3}}{2}i|0\rangle - \frac{1}{2}|1\rangle$

[1 mark each]

For each valid state among the above, give the probabilities of observing $|0\rangle$ and $|1\rangle$ when the system is measured in the standard computational basis. [4 marks]

(b) Suppose a two-qubit system is in the state $0.8|00\rangle + 0.6|11\rangle$. A Pauli X gate (i.e. a NOT gate) is applied to the second qubit, and a Hadamard gate is applied to the first qubit.

(i) What is the new state of the system? [2 marks]

(ii) What are the probabilities of the possible outcomes if both qubits are now measured? [2 marks]

(c) Suppose we have an algorithm which, given a blackbox computing a periodic function f with range $\{0, \ldots, N-1\}$, determines the period of f. Moreover, the algorithm runs in time $(\log N)^2$. Explain how this would enable us to have an efficient (i.e. polynomial-time) algorithm for factoring numbers. [8 marks]