COMPUTER SCIENCE TRIPOS Part II – 2024 – Paper 8

11 Quantum Computing (sjh227)

(*a*) In which quantum and classical computational complexity classes is factoring? [2 marks]

(*b*) Shor's algorithm is used to factor $N = 21$. Shor's algorithm requires a positive integer x, which is greater than one and less than N, to be chosen at random.

(*i*) What property must x have for Shor's algorithm not to terminate early? If $x = 14$ is chosen, when does Shor's algorithm terminate? [3 marks]

(*ii*) Instead $x = 4$ is chosen. What is the order of 4 modulo 21? [3 marks]

(*iii*) If Shor's algorithm is run with $x = 4$ explain what happens. Is the correct answer returned? [3 marks]

(*c*) Consider a three-state quantum automaton with initial state $|0\rangle$ and a single accepting state $|2\rangle$. The input letters are c and d, with transition matrices respectively:

$$M_c = \frac{1}{2}\begin{bmatrix} 1+i & 1-i & 0 \\ 1-i & 1+i & 0 \\ 0 & 0 & 2 \end{bmatrix}; \qquad M_d = \frac{1}{2}\begin{bmatrix} 2 & 0 & 0 \\ 0 & 1+i & 1-i \\ 0 & 1-i & 1+i \end{bmatrix}$$

(*i*) For quantum automata what property must hold for the transition matrices of each letter of the alphabet? [1 mark]

(*ii*) Verify that this property holds for M_c and M_d. [4 marks]

(*iii*) Give a four-letter input string containing two occurrences of c and two occurrences of d that is accepted with 100% probability. [2 marks]

(*iv*) Give an eight-letter input string containing both c and d that returns to the initial state with 100% probability. [2 marks]