11 Quantum Computing (sjh227)

(a) What problem does Grover’s search algorithm tackle, and what is its advantage over the best classical algorithm for this task? [2 marks]

(b) Let there be a database containing 32 elements, indexed by the binary numbers 00000 to 11111. A single element 00110 is marked.

(i) Give an oracle circuit that identifies the marked element. [1 mark]

(ii) If Grover’s search algorithm is applied to find the marked element, what should the initial state be set to, and what is the state after a single Grover iterate has been applied? [4 marks]

(iii) To find the marked element with maximum probability requires \( N \) iterates in total. What is the value of \( N \), and what is the probability of correctly finding the marked element? [4 marks]

(iv) If the algorithm is instead run with \( 3N \) iterates in total, what is the probability of correctly finding the marked element? Comment on your answer. [2 marks]

(c) Let \( V \) be an oracle circuit that marks one or more elements, acting as follows:

\[
V(|x\rangle|a\rangle) = |x\rangle|a \oplus f(x)\rangle
\]

Here \( a \) takes the values 0 or 1, and we have \( f(x) = 1 \) when \( x \) is the index of a marked element, and \( f(x) = 0 \) otherwise. How could \( V \) be altered to allow Grover’s search to find an unmarked element? [2 marks]

(d) A Grover iterate consists of the oracle circuit, typically denoted \( V \), followed by a circuit \( W \):

(i) What is the function of \( W \)? [1 mark]

(ii) What would happen if the order of \( V \) and \( W \) were swapped, such that Grover’s algorithm is run with \( V \) following \( W \) as the Grover iterate? [4 marks]