13 Quantum Computing (ad260)

A Boolean formula $\phi$ with $n$ variables in it can be seen as defining a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, and we say that $\phi$ is satisfiable if there is some $x \in \{0, 1\}^n$ such that $f(x) = 1$.

(a) Explain how $f$ can be suitably represented as a unitary operation $U_f$ on a complex space of dimension $2^{n+1}$. [3 marks]

(b) Suppose that we are given a blackbox implementing $U_f$. Describe how this would be used to form the Grover iterate which can be repeated to find a value $x$ such that $f(x) = 1$. [5 marks]

(c) If there is exactly one value $x$ such that $f(x) = 1$, how many iterations of the Grover iterate would you use to find this value? What is the probability of finding it? [3 marks]

(d) If there are $M$ distinct values such that $f(x) = 1$, how many iterations of the Grover iterate would you use to find one of these values? What is the probability of finding one of them? [3 marks]

(e) If you are able to turn an arbitrary formula $\phi$ into an implementation of the corresponding unitary operator $U_f$, how would you use this to give an algorithm for determining whether $\phi$ is satisfiable or not? Give an estimate of the running time of your algorithm in terms of $n$. [6 marks]