1 Introduction

Quantum model of computation

We focus on quantum properties relevant to our algorithms. A quantum system operates on qubits. Single qubit can be either in a pure or a mixed state. A pure state is a vector in a 2-dimensional Hilbert space $\mathcal{H}$, while a mixed state is modelled as a probabilistic distribution over pure states. Similarly, a register consisting of $d$ qubits can also be in a pure or a mixed state. A pure quantum state, denoted $|x\rangle$, is a vector of $2^d$-dimensional Hilbert space $\mathcal{H}^{\otimes d} = \mathcal{H} \otimes \ldots \otimes \mathcal{H}$. Again, a mixed state of larger dimension is viewed a probabilistic distribution over pure states. In our paper, we will operate only on pure states, and we will use only the standard computational basis of the Hilbert space, which consists of vectors $\{|b_1 \ldots b_d\rangle : b_1, \ldots, b_d \in \{0, 1\}^d\}$, to describe the system. Therefore, any state $|x\rangle$ can be expressed as $|x\rangle = \sum_{i=0}^{2^d-1} \alpha_i |i\rangle$, with the condition that $\sum_{i=0}^{2^d-1} |\alpha_i|^2 = 1$, since quantum states can be only normalized vectors.

Transitions, or equivalently – changes of states of a quantum system, are given by unitary operators on the Hilbert space of $d$ qubits. These unitary transformations are called quantum gates. These operations are exhaustive in the sense that any quantum computation can be expressed as a unitary operator on some Hilbert space. There are small-size sets of quantum gates working on two-dimensional space that are universal – any unitary transformation on a $2^d$-dimensional quantum space can be approximated by a finite collection of these universal gates. In our applications, any quantum algorithm computation run by a process requires polynomial (in $n$) number of universal gates.

Finally, an important part of quantum computation is also a quantum measurement. Measurements are performed with respect to a basis of the Hilbert space – in our case this is always the computational basis. A complete measurement in the computational basis executed on a state $|x\rangle = \sum_{i=0}^{2^d-1} \alpha_i |i\rangle$ leaves the state in one of the basis vectors, $|i\rangle$, for $i \in \{0, 1\}^d$, with probability $\alpha_i^2$. The outcome of the measurement is a classic register of $d$ bits, informing to which vector the state has been transformed. It is also possible to measure only some qubits of the system, which is called a partial measurement. If $A$ describes the subset of qubits that we want to measure and $B$ is the remaining part of the system, then the partial measurement is defined by the set of projectors $\{\Pi_i = |i\rangle_A \langle i| \otimes I_B \mid i \in \{0, 1\}^d\}$. In the former, a subscript refers to the part of the system on which the object exists, $I$ denotes the identity function, while $\langle i|$ is a functional of the dual space to the original Hilbert space (its matrix representation is the conjugate transpose of the matrix representation of $|i\rangle$). If before the measurement the system was in a state $|x\rangle_{AB}$ then, after the measurement, it is in one of the states $\{\Pi_i |x\rangle_{AB} \mid i \in \{0, 1\}^d\}$, where state $\Pi_i |x\rangle_{AB}$ is achieved with probability $\langle x |_{AB} \Pi_i |x\rangle_{AB}$. The reader can find a comprehensive introduction to quantum computing in [?].

Graph notations.

Let $G = (V, E)$ denote an undirected graph. Let $W \subseteq V$ be a set of nodes of $G$. We say that an edge $(v, w)$ of $G$ is internal for $W$ if $v$ and $w$ are both in $W$. We say that an edge $(v, w)$ of $G$ connects the sets $W_1$ and $W_2$, or is between $W_1$ and $W_2$, for any disjoint subsets $W_1$ and $W_2$ of $V$, if one of its ends is in $W_1$ and the other in $W_2$. The subgraph of $G$ induced by $W$, denoted $G[W]$, is the subgraph of $G$ containing the nodes in $W$ and all the edges internal for $W$ in $G$. A node adjacent to a node $v$ is a neighbor of $v$ and the set of all the neighbors of a node $v$ is the neighborhood of $v$. $N_G(v)$ denotes the set of all the nodes in $V$ that are of distance at most $i$ from some node in $W$.

\footnote{Whenever it could be irrelevant, from the context, we may follow the standard notation in quantum computing and skip writing normalizing factors.}

\footnote{$\Pi_i |x\rangle_{AB}$ and $\langle x|_{AB} \Pi_i |x\rangle_{AB}$ are simply linear operations on matrices and vectors.}
in graph $G$. In particular, the (direct) neighborhood of $v$ is denoted $N_G(v) = N_G^1(v)$.

The following combinatorial properties are of utter importance in the analysis of our algorithms. Graph $G$ is said to be $\ell$-expanding, or to be an $\ell$-expander, if any two subsets of $\ell$ nodes each are connected by an edge. Graph $G$ is said to be $((\ell, \alpha, \beta)$-edge-dense if, for any set $X \subseteq V$ of at least $\ell$ nodes, there are at least $\alpha |X|$ edges internal for $X$, and for any set $Y \subseteq V$ of at most $\ell$ nodes, there are at most $\beta |Y|$ edges internal for $Y$. Graph $G$ is said to be $(\ell, \varepsilon, \delta)$-compact if, for any set $B \subseteq V$ of at least $\ell$ nodes, there is a subset $C \subseteq B$ of at least $\varepsilon \ell$ nodes such that each node’s degree in $G|_C$ is at least $\delta$. We call any such set $C$ a survival set for $B$. 