Lecture 8: Quantum Computing (18 July - End)

Lecturer: Valentine Kabanets *Scribe: Lily Li*

8.1 Quantum Computing

8.1.1 Qubit

Let $|0\rangle$ measures 0 and $|1\rangle$ measures 1. You should think of each state as an energy level of the electron. However, in reality these states are continuous —rather than discrete. Consider a superposition of $|0\rangle$ and $|1\rangle$. We model quantum mechanics as $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ where $\alpha, \beta \in \mathcal{C}$ such that $|\alpha|^2 + |\beta|^2$. When we measure the qubit, the duality collapses and we just get classical bits with probability:

$$\begin{cases} 0 & \text{with probability } |\alpha|^2 \\ 1 & \text{with probability } |\beta|^2. \end{cases}$$

Observe that α, β are *not* the probabilities, but their squares *are*. Thus even though the probabilities are non-negative, the actual values α and β are complex (and can be negative).

8.1.2 Quantum Registers

For m qubits, we can describe a quantum register as

$$\sum_{x \in \{0,1\}^m} \alpha_x \cdot x$$

S where α_x is the amplitude of bit string x and $\sum |\alpha_x|^2$. Observe that for m qubits, the quantum system can be described by a vector in $\mathcal{C}^{2^m}$ (since the coefficient of each α_x is one variable). This gets exceedingly big exceedingly fast.

8.1.3 Quantum Operations

First let us describe the operation F on the quantum system equivalent to negation on the classical bits. As it turns out that these operations F are exactly unary matrices. Generally, it is too much to define F for a quantum system with m qubits even if m is modest. Thus we must restrict the number of qubits we operate upon at one time. For us, each operation will be applied to at most three qubits. Thus F will be a $2^3 \times 2^3$ or 8×8 matrix. It is unclear if each operator F is realizable.

For bits $|0\rangle$ and $|1\rangle$ observe that

8.1.4 Complexity BQP

Definition 8.1 *Let* $f : \{0,1\}^n \to \{0,1\}^n$

Consider next the $\wedge$ operation. Classically, we have $x, y \in \{0, 1\}$ such that $\mathsf{AND}(x, y) = x \wedge y$. In quantum computation we need the Trefoli gate which takes in three qubits x, y, z and outputs $\mathsf{QAND}(x, y, z) = (x, y, z \oplus (x \wedge y)$.