Introduction to Quantum Computing

Elham Kashefi

Tutorial Sample

Question. Most unitary transforms are hard to approximate.

1. Show that there exist $O(2^{n^2})$ distinct boolean functions of $n$ bits.

2. Show that a (classical) circuit composed of $n$ NAND gates can implement at most $O(n^{2n})$ distinct boolean functions.

3. Show that an arbitrary unitary transform applied to $n$ qubits is described by $O(2^{2n})$ real degrees of freedom.

4. How many distinct unitary transforms can be produced by a quantum circuit composed of $n$ controlled-Not, Hadamard, and T gates?

Solution.

1. We are dealing with boolean functions that take $n$ bits as input and output $n$ bits. Each boolean function function has $2^n$ possible inputs, and its output for each of these is described by $n$ bits. Therefore, since it takes $n2^n$ bits to describe an arbitrary boolean function, meaning that there are $2^n2^n$ different boolean functions which take in $n$ bits and output $n$ bits.

2. Any circuit of $n$ NAND gates can take at most $2n$ bits, and can be described (redundantly) by a sequence of $n$ steps each involving a single NAND gate. At each step, there are $\binom{N}{2}$ possible ways to have a NAND gate (You choose each of the two inputs). Since there are $n$ such steps, there are at most $\left(\binom{N}{2}\right)^n$ possible circuits. $\left(\binom{N}{2}\right)^n < (n^2)^n = n^{2n}$, and thus a classical circuit composed of $n$ NAND gates can implement at most $O(n^{2n})$ boolean functions.

3. An arbitrary $NN$ matrix has $N^2$ complex degrees of freedom. For a matrix to be unitary there are $\binom{N}{2} + N$ complex constraints (Each pair
of columns is orthogonal + Normalization of each column). Therefore, an arbitrary unitary matrix has $O(N^2)$ degrees of freedom. For a system of $n$ qubits, $N = 2^n$, and therefore an arbitrary unitary transform has $O(N^2) = O((2^n)^2) = O(2^{2n})$ degrees of freedom.

4. We use a similar reasoning that we did in part 1. Any quantum circuit of $n$ CNOT, Hadamard, and T gates can affect at most $2n$ qubits and may be described (redundantly) by a sequence of $n$ steps, each involving a single CNOT, Hadamard, or T gate. At each step, there are $\binom{n}{2} + 2n$ possible gates to apply, and thus there are at most $O((n^2)^n) = O(n^{2^n})$ possible unitary transforms.