Boolean Functions

Andreas Klappenecker

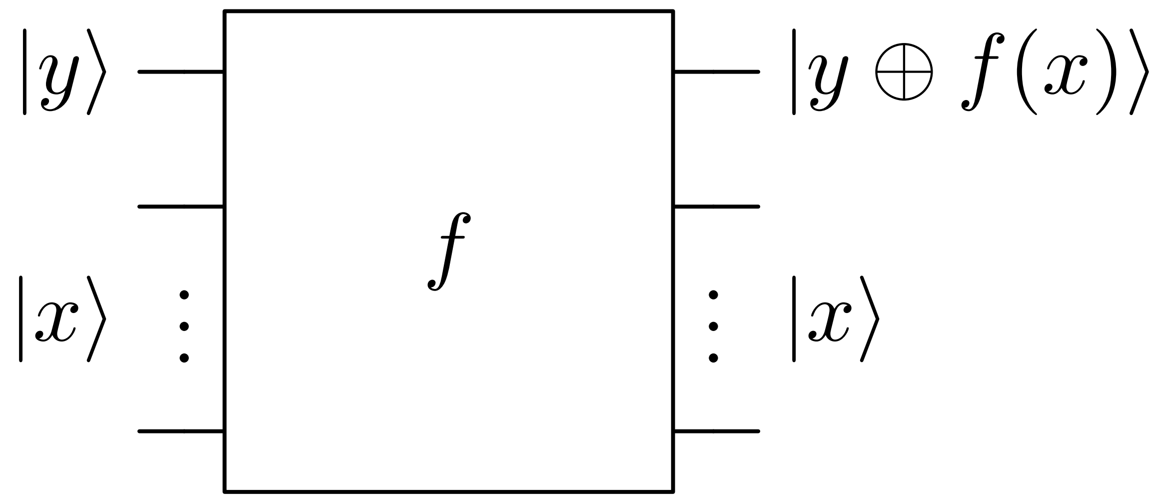
Implementing Boolean Functions

Suppose that we have a boolean function $f\colon \mathbf{F}_2^n \to \mathbf{F}_2$. A quantum circuit implementing f has to be realized by a unitary map. This can be accomplished, for instance, by implementing the map

$$|y\rangle \otimes |x\rangle \mapsto |y \oplus f(x)\rangle \otimes |x\rangle$$

on $n+1$ qubits, where $x \in \mathbf{F}_2^n$, and $y \in \mathbf{F}_2$. The most significant bit is the output bit, and the n lowest significant bits are the input bits. The result of $f(x)$ is added modulo 2 to the output bit.

Quantum Circuit



Typical Application

The linearity of the circuit allows to evaluate f for any linear combination of the basis states. Assume that all $n+1$ quantum bits are initialized with state $|0\rangle$. We apply the Hadamard gate to all n input bits. The resulting state is

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |0\rangle \otimes |x\rangle$$

a superposition of all possible inputs. If we apply the circuit implementing the function f, then we obtain as a result

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |f(x)\rangle \otimes |x\rangle$$