Simon's Algorithm: The Quantum Part

Andreas Klappenecker

The Problem

Given: a Boolean function f: $\{0,1\}^n \rightarrow \{0,1\}^n$ such that there exists an s in $\{0,1\}^n$ so that for all x, y in $\{0,1\}^n$ the following property holds:

$$f(x)=f(y) \text{ if and only if } x=y \text{ or } x \oplus s=y$$

where $\oplus$ is the bitwise xor operator (=addition mod 2).

Goal: Find s

Example

Let n=3.

The function f(x) is a 2-to-1 function.

We have s=101

Notice: You might have to evaluate as many as $2^{n-1}+1$ different arguments to find s.

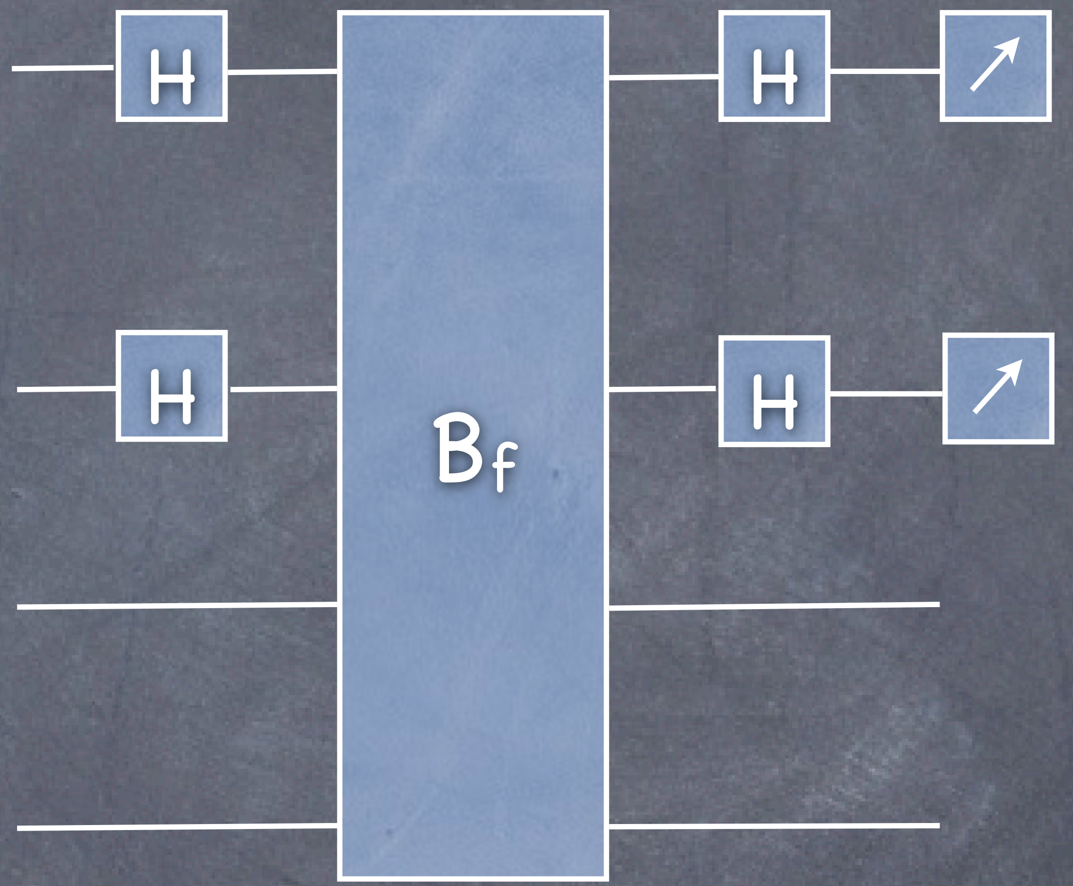
x	f(x)
000	111
001	000
010	110
011	101
100	000
101	111
110	101
111	110

Quantum Algorithm

The quantum part is particularly simple:

All 2n qubits are initialized to |0>. MSBs are input, and LSBs are output

Apply Hadamard gate, then B_f, followed by Hadamard gates and measurement.

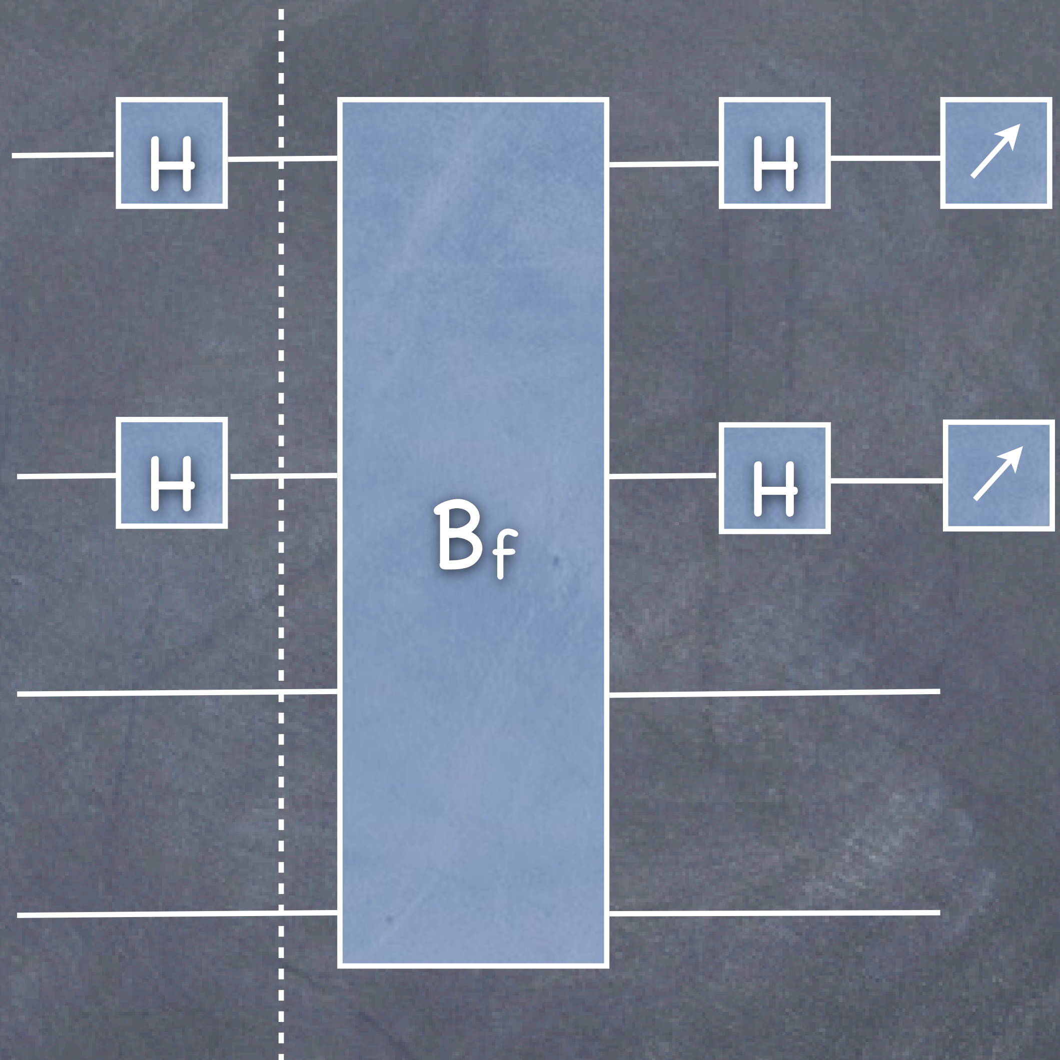


$$B_f = \begin{cases} \mathbf{C}^{2^n} \otimes \mathbf{C}^{2^n} & \rightarrow & \mathbf{C}^{2^n} \otimes \mathbf{C}^{2^n} \\ |x\rangle \otimes |y\rangle & \mapsto & |x\rangle \otimes |y \oplus f(x)\rangle \end{cases}$$

Quantum Algorithm

Initial state: $|0^n\rangle \otimes |0^n\rangle$
After Hadamard gates are applied to n most significant bits, we get

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

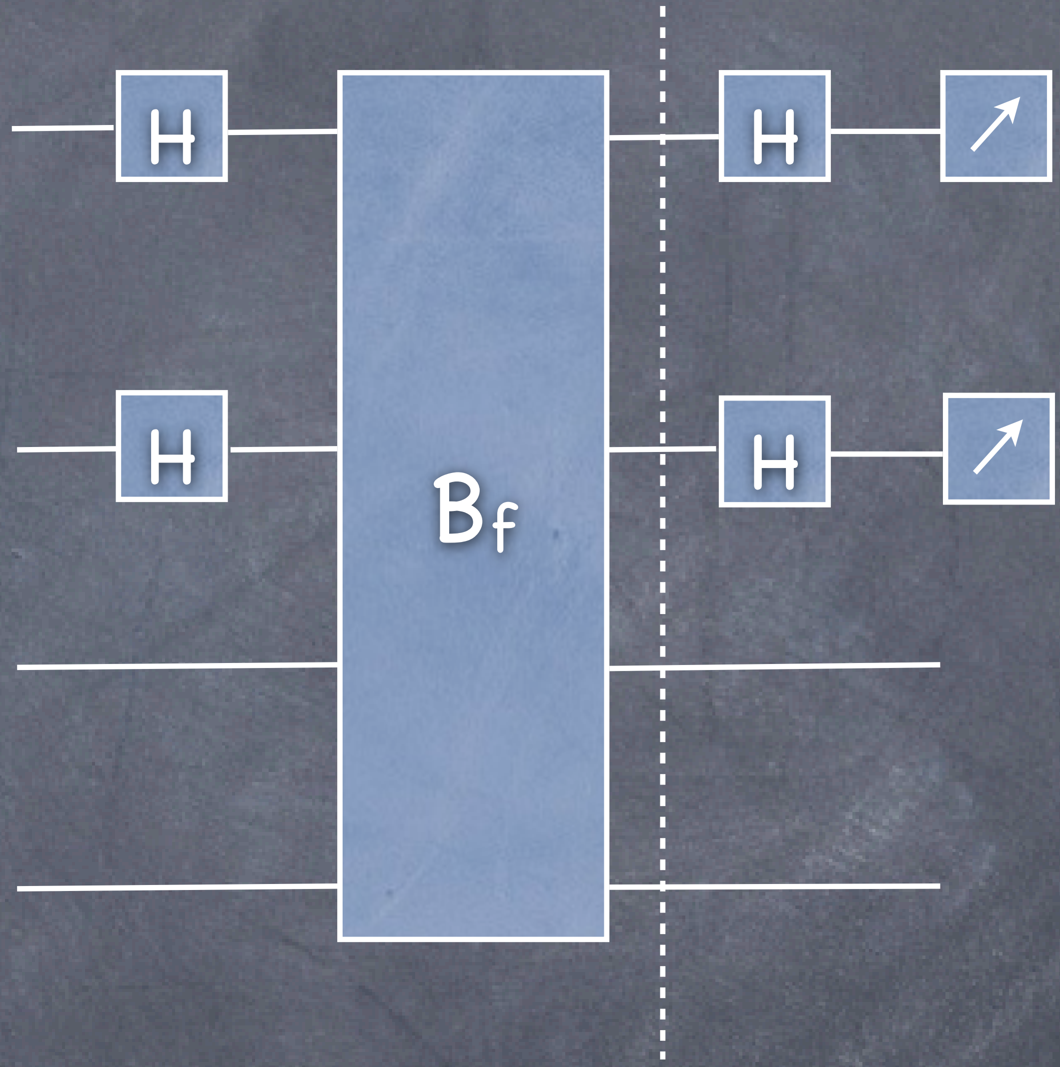


Quantum Algorithm

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

Applying B_f yields

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle$$

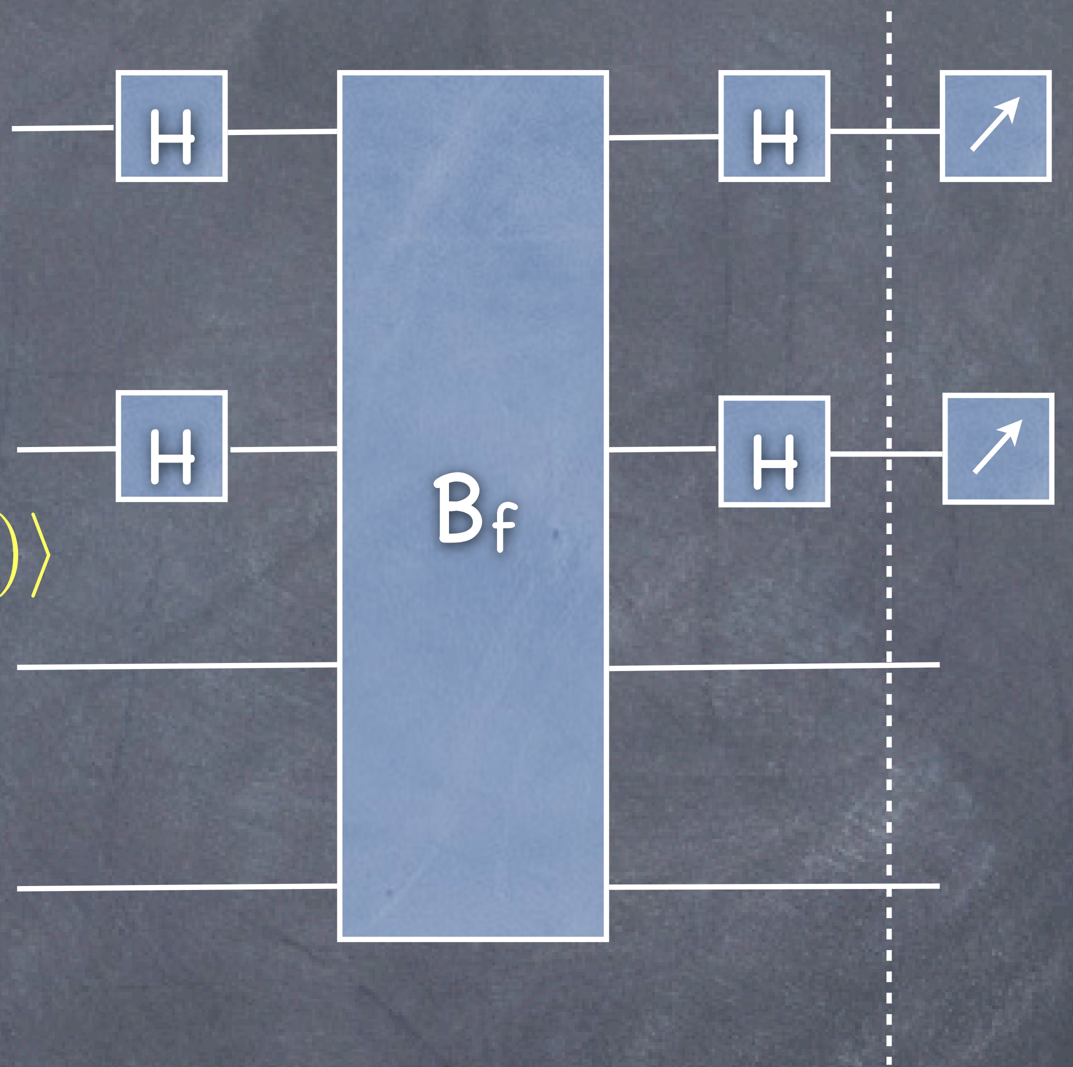


Quantum Algorithm

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle$$

Applying Hadamard gates yields

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \otimes |f(x)\rangle$$



Measurement

The state before measurement is given by

$$\frac{1}{2^n}\sum_x\sum_y(-1)^{x\cdot y}|y\rangle\otimes|f(x)\rangle = \sum_{y\in\{0,1\}^n}|y\rangle\otimes\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot y}|f(x)\rangle\right)$$

If $s=0$, then $f(x)$ is injective, hence bijective.

Then the probability to observe y is given by

$$\left\|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot y}|f(x)\rangle\right\|^2 = \left\|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot y}|x\rangle\right\|^2 = \frac{1}{2^n}$$

If $s \neq 0$, then for each z in $\mathrm{ran}(f)$, there exist two distinct arguments x_z and x'_z such that $f(x_z) = z = f(x'_z)$, and $x_z \oplus s = x'_z$. The probability to observe y is given by

$$\left\| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} |f(x)\rangle \right\|^2 = \left\| \frac{1}{2^n} \sum_{z \in \mathrm{ran}(f)} ((-1)^{x_z \cdot y} + (-1)^{x'_z \cdot y}) |z\rangle \right\|^2$$

$$= \left\| \frac{1}{2^n} \sum_{z \in \mathrm{ran}(f)} ((-1)^{x_z \cdot y} + (-1)^{(x_z \oplus s) \cdot y}) |z\rangle \right\|^2$$

$$= \left\| \frac{1}{2^n} \sum_{z \in \mathrm{ran}(f)} (-1)^{x_z \cdot y} (1 + (-1)^{s \cdot y}) |z\rangle \right\|^2 = \begin{cases} 2^{-(n-1)} & \text{if } s \cdot y = 0 \\ 0 & \text{if } s \cdot y = 1 \end{cases}$$

Conclusions

For all s in $\{0,1\}^n$, the observed strings y are uniformly distributed among $\{ y \mid s \cdot y = 0 \}$.

Strategy: Repeat the quantum algorithm n-1 times to obtain elements $Y = \{ y_1, \ldots, y_{n-1} \}$.

If the vectors in Y are linearly independent, then there exists precisely one nonzero s′ in $\{0,1\}^n$ such that $s' \cdot y_k = 0$ for all k.

If $f(s')=f(0)$, then $s=s'$; otherwise $s=0$.