Simon's Problem

An oracle computes a function

$$f : \{0,1\}^n \to \{0,1\}^n$$

It is known that

$$f(x) = f(y) \text{ iff } y = x \oplus a$$

where the *period* a is an n-bit string.

- f is a 2-to-1 function; nothing else is known.

- a is random over 2^n possible values.

Simon's problem: Determine a with probability of success $\geq 3/4$ and with as few calls to the oracle as possible.

Classical Complexity

At the ith oracle call: input x_i, output $f(x_i)$.

If $f(x_i) \neq f(x_j)$, then $a \neq x_i \oplus x_j$.

After m calls, $f(x_1), \ldots, f(x_m)$ known.

There are $\binom{m}{2}$ distinct pairs (x_i, x_j).

The probability of hitting a in $\leq m$ oracle calls is

$$\frac{\binom{m}{2}}{2^n} \approx \frac{m^2}{2^{n+1}}$$

Thus, $m \approx 2^{n/2}$ is needed for a probability 1/2 of determining a.

Classical complexity: Problem not in BPP.

Simon's Algorithm

1. Initialize registers:

$$\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0^n\rangle$$

2. Call oracle $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$$\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

3. Measure the second register to obtain

$$\rightarrow \frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)|f(x_0)\rangle$$

   with probability $2/2^n$.

4. Apply Hadamard transform to the first register

$$\begin{aligned} \rightarrow\ & \frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} \left[(-1)^{x_0\cdot y} + (-1)^{(x_0\oplus a)\cdot y}\right] |y\rangle \\ =\ & \frac{1}{2^{(n-1)/2}} \sum_{y:a\cdot y=0} (-1)^{x_0\cdot y}|y\rangle \end{aligned}$$

5. Measure the first register to obtain a y_1 such that $a \cdot y_1 = 0$. Each such y_1 has probability $1/2^{n-1}$ of being observed.

6. Repeat the above procedure until n linearly independent $y_1, \ldots, y_n$ are obtained. Solve the equations $y_i \cdot a = 0$, $i = 1, \ldots, n$ to determine a.

Complexity Analysis

Given $y_1, \ldots, y_m$ linearly independent, the next run of Simon's algorithm produces a linearly independent y_{m+1} with probability

$$\alpha_m = 1 - \frac{2^m}{2^{n-1}}.$$

No of trials until the next lineraly independent vector y_{m+1} is found is geometric with probability of success α_m.

Mean number of trials

$$\begin{aligned}\sum_{k=1}^{\infty} k(1-\alpha_m)^{k-1}\alpha_m &= \frac{1}{\alpha_m} = \frac{1}{1 - 2^m/2^{n-1}} \\ &\approx 1 + 2^m/2^{n-1} \approx 1.\end{aligned}$$

So, it takes close to n repetitions to obtain n linearly independent y_i's with high probability.

Conclusion: Simon's problem is in BQP.

BPP vs. BQP

Simon's problem shows that

$$\mathrm{BPP} \neq \mathrm{BQP}$$

relative to an oracle.

We do not know if BQP $\neq$ BPP for non-oracle problems.