Quantum Computation
(Lecture 5)

Luís Soares Barbosa

MSc Physics Engineering

Universidade do Minho, 2021-22

Simon's problem

The problem

Let $f : 2^n \longrightarrow 2^n$ be such that for some $s \in 2^n$,

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

Find s.

Equivalent formulation as a period-finding problem

Determine the period s of a function f periodic under $\oplus$:

$$f(x \oplus s) = f(x)$$

Note that f is bijective if $s = 0$ (because $x \oplus y = 0$ iff $x = y$), and two-to-one otherwise (because, for a given s there is only a pair of values x, y such that $x \oplus y = s$).

Simon's problem

Example

Let $f : 2^3 \longrightarrow 2^3$ be defined as

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

Cleary $s = 110$. Indeed, every output of f occurs twice, and the bitwise XOR of the corresponding inputs gives s.

Simon's problem, classically

Compute f for sequence of values until finding a value x_j such that $f(x_j) = f(x_i)$ for a previous x_i. Then

$$s = x_j \oplus x_i$$

- At any previous stage, if this procedure has picked m different values of x, then one concludes that $s \neq x_j \oplus x_i$ for all such values.
- Thus, at most
$$\frac{1}{2} m(m-1)$$
possible values for s have been discarded, out of $2^n - 1$ possible ones.
- The procedure is unlike to succeed until m becomes of the order of $\sqrt{2^n}$ — the execution time grows exponentially with the number of bits n.

Simon's problem relevance

Other examples of problems for which there is a quantum exponential advantage, admit classical probabilisitic interesting solutions, e.g.

Deutsch-Joza

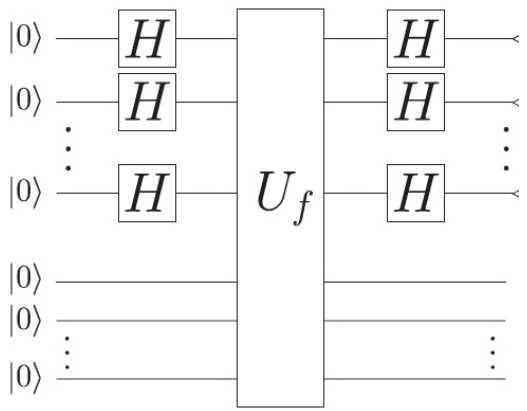
- Classical deterministic: requires $2^{n-1}+1$ queries in the worst case,
- Classical probabilisitic: requires 2 queries with a probability of error at most $\frac{1}{3}$,
- Quantum: requires 1 query.

However, for the Simon's problem an exponential number of queries to the oracle accessing f are required by any classical probabilisitic algorithm.

Going quantum

Reuse the circuit from the Deutsch-Joza algorithm but expand both registers to n qubits

The circuit



where

$$U_f = |x\rangle|c\rangle \mapsto |x\rangle|c \oplus f(x)\rangle$$

Going quantum

The oracle maps

$$\frac{1}{\sqrt{2^n}} \sum_{x \in 2^n} |x\rangle|0\rangle \quad \text{to} \quad \frac{1}{\sqrt{2^n}} \sum_{x \in 2^n} |x\rangle|f(x)\rangle$$

because $0 \oplus x = x$.

A measurement of the target register choose randomly one of the 2^{n-1} possible outcomes of f as f gives the same output for x and $x \oplus s$, to 2^n possible inputs correspond 2^{n-1} possible outcomes

This measurement is not very useful (why?).

Going quantum

If the result of measuring the target register is $f(k)$, then the control register will contain superposition

$$\frac{1}{\sqrt{2}}(|k\rangle + |k \oplus s\rangle)$$

as they are the unique values yielding $f(k)$.
Thus, the state after the oracle

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

can be rewritten as

$$\frac{1}{\sqrt{2^{n-1}}} \sum_{x \in P} \frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)|f(x)\rangle \tag{1}$$

Set P is composed of one representative of each of the 2^{n-1} sets of strings $\{x, x \oplus s\}$, into which 2^n can be partitioned.

Basic insight: the effect of $H^{\otimes n}$

Recall

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z \in 2} (-1)^{xz} |z\rangle$$

which extends to a n-qubit as follows

$$\begin{aligned}
H^{\otimes n}|x\rangle &= H|x_1\rangle H|x_2\rangle \cdots H|x_n\rangle \\
&= \frac{1}{\sqrt{2}} \sum_{z_1 \in 2^n} (-1)^{x_1 z_1} |z_1\rangle + \frac{1}{\sqrt{2}} \sum_{z_2 \in 2^n} (-1)^{x_2 z_2} |z\rangle \cdots \frac{1}{\sqrt{2}} \sum_{z_n \in 2^n} (-1)^{x_n z_n} |z_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{z_1, z_2, \cdots, z_n \in 2^n} (-1)^{x_1 z_1 + x_2 z_2 + \cdots + x_n z_n} |z_1 z_2 \cdots z_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} (-1)^{x \cdot z} |z\rangle
\end{aligned}$$

Applying $H^{\otimes n}$

$$H^{\otimes n} \otimes I \left(\frac{1}{\sqrt{2^{n-1}}} \sum_{x \in P} \frac{1}{\sqrt{2}} (|x\rangle + |x \oplus s\rangle) |f(x)\rangle \right)$$

$$= \frac{1}{\sqrt{2^{n-1}}} \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} \sum_{x \in P} \frac{1}{\sqrt{2}} ((-1)^{x \cdot z} + (-1)^{(x \oplus s) \cdot z}) |z\rangle |f(x)\rangle$$

$$= \frac{1}{2^n} \sum_{z \in 2^n} \sum_{x \in P} \underbrace{(-1)^{x \cdot z} (1 + (-1)^{s \cdot z})}_{(\star)} |z\rangle |f(x)\rangle$$

- $s \cdot z = 1 \Rightarrow (\star) = 0$ and the corresponding basis state $|z\rangle$ vanishes
- $s \cdot z = 0 \Rightarrow (\star) \neq 0$: and the corresponding basis state $|z\rangle$ is kept
  In this case the probability of geting z upon measurement is $\frac{1}{2^{n-1}}$ (why?)

Applying $H^{\otimes n}$

This state can be presented as a uniform superposition as follows

$$\begin{aligned} & \frac{1}{2^n} \sum_{z \in 2^n} \sum_{x \in P} (-1)^{x \cdot z} (1 + (-1)^{s \cdot z}) \, |z\rangle |f(x)\rangle \\ = \; & \frac{1}{2^n} \sum_{z \in S^{\perp}} \sum_{x \in P} 2(-1)^{x \cdot z} (1 + (-1)^{s \cdot z}) \, |z\rangle |f(x)\rangle \\ = \; & \frac{1}{2^{n-1}} \sum_{z \in S^{\perp}} \sum_{x \in P} (-1)^{x \cdot z} (1 + (-1)^{s \cdot z}) \, |z\rangle |f(x)\rangle \end{aligned}$$

where $S^{\perp}$, for $S = \{0, s\}$ is the orthogonal complement of subspace S, with $\dim(S^{\perp}) = n - 1$
(because $\dim(S) = 1$, as S is the subspace generated by s)

Notes

S and $S^{\perp}$

Both are subspaces of the vector space Z_2^n whose vectors are strings of length n over $Z_2 = \{0, 1\}$.

- The dimension of Z_2^n is n; a basis is provided by strings with exactly one 1 in the kth position (for $k = 1, 2, \cdots, n$).
- Two vectors v, u in Z_2^n are orthogonal iff $v \cdot u = 0$ (operation $\cdot$ acts as the internal product).
- Thus, for any subspace F of Z_2^n, $F^{\perp} = \{u \in Z_2^n \mid \forall_{v \in F}.\ \ u \cdot v = 0\}$

Warning: to not confuse with the Hilbert space in which the algorithm is executed and whose basis are labelled by elements of Z_2^n.

Notes

The triple $(Z_2^n, \oplus, 0)$ forms a group

Groups

A group (G, θ, u) is a set G with a binary operation θ which is associative, and equipped with an identity element u and an inverse:

$$a^{-1}\theta a = u = a\theta a^{-1}$$

Each set $\{x, x \oplus s\}$ in (1) is a coset of subgroup $S = (\{0, s\}, \oplus, 0)$

Coset

The coset of a subgroup S of a group (G, θ) wrt $g \in G$ is

$$gS = \{g\theta s \mid s \in S\}$$

In this case

$$xS = \{x \oplus 0, x \oplus s\} = \{0, x \oplus s\}$$

Putting everything together

Running this circuit and measuring the control register results in some z in $(Z_2)^n$ satisfying

$$s \cdot z = 0 \,,$$

the distribution being uniform over all the strings that satisfy this constraint.

Exercise

In the previous discussion we assumed that $s \neq 0$. Show that the conclusion above is still valid if $s = 0$.

Putting everything together

Thus, it is enough to repeat this procedure until $n-1$ linearly independent values $\{z_1, z_2 \cdots, z_{n-1}\}$ are found, and solve the following set of $n-1$ equations in n unknowns (corresponding to the bits of s):

$$\begin{aligned} z_1 \cdot s &= 0 \\ z_2 \cdot s &= 0 \\ &\vdots \\ z_{n-1} \cdot s &= 0 \end{aligned}$$

to determine s. Actually,

$\text{span}\{z_1, z_2, \cdots, z_{n-1}\} = S^{\perp}$ and $\{z_1, z_2, \cdots, z_{n-1}\}$ forms a base for $S^{\perp}$

Thus, s is the unique non-zero solution of

$$Z\, s = 0$$

where Z is the matrix whose line i corresponds to vector z_i.

Putting everything together

Finally, to determine s, one has to compute this system of linear equations t by Gaussian elimination modulo 2 (in time polynomial in n).

Once a solution t is found test $f(0) = f(t)$:

- $f(0) = f(t) \Rightarrow$ s is t.
- $f(0) \neq f(t) \Rightarrow$ s is 0.
  (otherwise the unique non-zero solution to the system would be t.)

The algorithm

1. Prepare the initial state $\frac{1}{\sqrt{2^n}} \sum_{x \in 2^n} |x\rangle|0\rangle$ and make $i := 1$
2. Apply the oracle U_f to obtain the state

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

which can be re-written as

$$\frac{1}{\sqrt{2^{n-1}}} \sum_{x \in P} \frac{1}{\sqrt{2}} (|x\rangle + |x \oplus s\rangle)|f(x)\rangle$$

3. Apply $H^{\otimes n}$ to the control register yielding a uniform superposition of elements of $S^{\perp}$.

The algorithm

4. Measure the first register and record the value observed z_i, which is a randomly selected element of $S^{\perp}$.
5. If the dimension of the span of $\{z_1, z_2, \cdots, z_i\}$ is less than $n-1$, increment i and to go step 2; else proceed.
6. Compute s as the unique non-zero solution of

$$Z\,s \;=\; 0$$

The crucial observation is that the set of observed values must form a basis to $S^{\perp}$.

Analysis

- In each iteration i the probability of z_i being linearly independent of the values previously computed is at least 0.5.
- Thus, the probability that $\{z_1, z_2, \cdots, z_{n-1}\}$ are linearly independent is at least

$$\prod_{y=1}^{\infty}\left(1-\frac{1}{2^y}\right) = 0.288788\cdots > \frac{1}{4}$$

- It can be shown that if the entire process is repeated $4t$ times, the probability of not finding a basis during one of the iterations i less than

$$\left(1-\frac{1}{4}\right)^{4t} < \frac{1}{\mathrm{e}^t}$$

(i.e. about 20000^{-1} for $t = 10$.)

- The corresponding equations can be solved to find s in $O(n^2)$
- Thus, with high likelihood s is expected to be found with $O(n-1)$ calls to the oracle, followed by $O(n^2)$ steps to solve the equations.

The problem

The problem

Let $f : 2^n \longrightarrow X$, for some X finite, be such that,

$$f(x) = f(y) \text{ iff } x - y \in S$$

for some subspace S of Z_2^n with dimension m.

Find a basis $\{s_1, s_2, \cdots s_m\}$ for S.

In Simon's problem

- $x = y \oplus s$, i.e. $x - y = s$.
- s is a basis for the space S generated by $\{s\}$.

Generalised Simon's algorithm

If $S = \{0, y_1, \cdots, y_{2^m-1}\}$ is a subspace of dimension m of Z_2^n, 2^n can be decomposed into 2^{n-m} cosets of the form

$$\{x, x \oplus y_1, x \oplus y_2, \cdots, x \oplus y_{2^m-1}\}$$

Then Step 3 yields

$$\begin{aligned} & \sum_{x \in 2^n} |x\rangle |f(x)\rangle \\ = & \frac{1}{\sqrt{2^{n-m}}} \sum_{x \in P} \frac{1}{\sqrt{2^m}} (|x\rangle + |x \oplus y_1\rangle + |x \oplus y_2\rangle + \cdots + x \oplus y_{2^m-1}) |f(x)\rangle \\ = & \frac{1}{\sqrt{2^{n-m}}} \sum_{x \in P} |x + S\rangle |f(x)\rangle \end{aligned}$$

where P be a subset of 2^n consisting of one representative of each 2^{n-m} disjoint cosets, and

$$|x + S\rangle = \sum_{s \in S} \frac{1}{\sqrt{2^m}} |s\rangle$$

Generalised Simon's algorithm

- In step 4 the first register is left in a state of the form $|x + S\rangle$ for a random x.
- After applying the Hadamard transformation, the first register contains a uniform superposition of elements of $S^{\perp}$ and its measurement yields a value sampled uniformly at random from $S^{\perp}$.

This leads to the revised algorithm:

5. If the dimension of the span of $\{z_1, z_2, \cdots, z_i\}$ is less than $n - m$, increment i and to go step 2; else proceed.
6. Compute the system of linear equations

$$Z\, s \;=\; 0$$

and let $s_1, s_2, \cdots, s_m$ be the generators of the solution space. They form the envisaged basis.

The hidden subgroup problem

The group S is often called the hidden subgroup.
The (generalised) Simon's algorithm is an instance of a much general scheme, leading to exponential advantage, known as

The hidden subgroup problem

Let (G, θ, u) be a group and $f : G \longrightarrow X$ for some finite set X with the following property:

$$f \text{ is constant on cosets of } S \text{ and distinct on different cosets}$$

i.e.

$$\text{there is a subgroup } S \text{ of } G \text{ such that for any } x, y \in G,$$

$$f(x) = f(y) \text{ iff } x\theta S = y\theta S$$

Characterise S.