Quantum Computation

(Lecture 6)

Luís Soares Barbosa

Quantum Computing Course Unit

Universidade do Minho, 2020

The problem

Finding the period of a function

Let f be a periodic function with period $0 < r < 2^n$:

$$f(x+r) = f(x) \quad \text{with } x, r \in \{0, 1, 2, \cdots\}$$

Given a circuit for an operator $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, obtain r (with a single query to oracle U).

The algorithm follows the usual pattern

- Start with $|0\rangle|0\rangle$ creates a uniform superposition with $t = \mathcal{O}(n + \log \frac{1}{\epsilon})$ qubits;
- apply the oracle;
- estimate the relavant value with QFT^{-1} and measure the first register;
- (classical) post-processing to retrieve the period.

The algorithm

1. $|0\rangle|0\rangle$
2. Uniform superposition: $\longrightarrow$ $\frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}|x\rangle|0\rangle$
3. Oracle: $\longrightarrow$

$$\frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}|x\rangle|f(x)\rangle \approx \frac{1}{\sqrt{r2^t}}\sum_{l=0}^{r-1}\sum_{x=0}^{2^t-1} e^{\frac{2\pi i l x}{r}}|x\rangle|\overline{f}(l)\rangle$$

4. QFT^{-1}: $\longrightarrow$ $\frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}|\widetilde{\frac{l}{r}}\rangle|\overline{f}(l)\rangle$
5. Measure first register: $\longrightarrow$ $\widetilde{\frac{l}{r}}$
6. Post-processing: continued fractions: $\longrightarrow$ r

Details: Step 3

Step 3 is based on the equality

$$|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{\frac{2\pi i l x}{r}} |\overline{f}(l)\rangle$$

where state $|\overline{f}(l)\rangle$ is defined as

$$\frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-\frac{2\pi i l x}{r}} |f(x)\rangle$$

The equality holds because $\sum_{l=0}^{r-1} e^{\frac{2\pi i l x}{r}} = r$ whenever x is a multiple of r, i.e. $x = mr$, for m integer, reducing

$$e^{\frac{2\pi i l m r}{r}} = e^{2\pi i l m} = 1$$

Otherwise it sums 0 as parcels alternate with positive/negative non integer multiples of 2π

Details: Steps 3 and 6

Step 3

The equality in Step 3 is only an approximation because, in the general case, 2^t may not be an integer multiple of r.

Step 6

The value approximated by $\widetilde{\frac{l}{r}}$ is a rational number, the ratio of two bounded integers. The continued fractions method computes the nearest fraction $\frac{l'}{r'}$ to $\widetilde{\frac{l}{r}}$ making highly probable that r' is indeed r.

Analysis

To justify why the algorithm works, note that the definition of $|\overline{f}(l)\rangle$ is almost the Fourier transform over $\{0, 1, 2, \cdots, 2^n - 1\}$.

In general, for $0 \leq x \leq N$ and N an integer multiple of r, e.g. $N = mr$, the Fourier transform of f is

$$\overline{f}(l) = \frac{1}{N} \sum_{x=0}^{N-1} e^{-\frac{2\pi i l x}{N}} f(x)$$

Function f being cyclic and $N = mr$ entails

$$\overline{f}(l) = \frac{1}{N} \sum_{k=0}^{m-1} \sum_{x=0}^{r-1} e^{-\frac{2\pi i l(kr+x)}{mr}} f(x)$$

Analysis

Note that the term

$$\sum_{k=0}^{m-1} e^{-\frac{2\pi i l k r}{mr}} = m\,\delta_{l,mp} \quad \text{for } p \in \mathbb{Z}$$

i.e. it returns m if l is a multiple of m (i.e. of $\frac{N}{r}$), and 0 otherwise. Actually, if $l = mp$, for na integer p, then

$$\sum_{k=0}^{m-1} e^{-\frac{2\pi i m p k r}{mr}} = \sum_{k=0}^{m-1} e^{-2\pi i p k} = \sum_{k=0}^{m-1} 1 = m$$

Otherwise the parcels in the sum will take the form

$$e^{\frac{0}{m}},\ e^{\frac{-2l\pi i}{m}},\ e^{\frac{-4l\pi i}{m}} \ldots,\ e^{\frac{-2(m-1)l\pi i}{m}}$$

corresponding to angles regularly spanning the whole circle which cancel two by two.

Analysis

This entails

$$\overline{f}(l) = \begin{cases} \frac{\sqrt{N}}{r}\sum_{x=0}^{r-1} e^{-\frac{2\pi i l x}{N}} f(x) & \Leftarrow \ l \text{ is a multiple of } m \\ 0 & \Leftarrow \ \text{otherwise} \end{cases}$$

Making $N = r$ we retrieve, for $l \in \{0, 1, 2, \cdots, r-1\}$
the integer multiples of 1 ...,

$$\overline{f}(l) = \frac{1}{\sqrt{r}}\sum_{x=0}^{r-1} e^{-\frac{2\pi i l x}{r}} f(x)$$

Shift invariance

The crucial argument is that the Fourier transform verifies a shift invariance property, which, in a broader sense, is stated as follows:

Shift invariance

Given a group G and a subgroup S of G, if a function f defined in G is constant on the cosets of S, then its Fourier transform is invariant over cosets of S.

Recall: coset

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

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

Shift invariance

Proof

Let $S \subseteq G$, the latter indexing the states in a orthonormal basis, and consider the general expression of the QFT

$$\sum_{s \in S} \alpha_s |s\rangle \mapsto \sum_{g \in G} \beta_g |g\rangle$$

where

$$\beta_g = \sum_{s \in S} \alpha_s e^{\frac{2\pi i g s}{|G|}}$$

Applying operator $U_k|x\rangle = |x + r\rangle$ yields

$$U_k \sum_{s \in S} \alpha_s |s\rangle = \sum_{s \in S} \alpha_s |s + r\rangle$$

whose Fourier transform is

$$\sum_{g \in G} \sum_{s \in S} e^{\frac{2\pi i g (s+r)}{|G|}} |g\rangle = \sum_{g \in G} e^{\frac{2\pi i g r}{|G|}} \sum_{s \in S} e^{\frac{2\pi i g s}{|G|}} |g\rangle = \sum_{g \in G} e^{\frac{2\pi i g r}{|G|}} \beta_g |g\rangle$$

Shift invariance

Proof

Clearly, if we are representing the Fourier transform of a function f is constant in each coset, i.e.

$$f(s+r) = f(r) \text{ for all } s \in \{s' + r \mid s \in S\}$$

the (absolute values) of amplitudes

$$e^{\frac{2\pi igr}{|G|}}\beta_g \text{ and } \beta_g$$

coincide.

Thus, the Fourier transform of f is invariant in cosets

Order-finding

Order-finding as period estimation

The kernel of the algorithm for order-finding can be seen is an instance of period estimation for function

$$f_a(k) = a^k (\bmod n)$$

as the period is exactly the order:

$$a^{k+r} (\bmod n) = a^k a^r (\bmod n) = a^k (\bmod n)$$

(cf, the original approach in Shor's algorithm)

Discrete logarithm

The discrete logarithm problem

Determine t, given a and $b = a^t$.

This problem can be solved as an instance of period estimation for a much more complex function:

$$f_a(x, y) \;=\; a^{tx+y} \pmod n$$

through the observation that f is periodic

$$f(x + k, y - kt) = f(x, y)$$

with period $(k, -kt)$, for each integer k.

Afterthoughts

In the next lecture, we'll show that both the period estimation and discrete logarithm problems, and many others indeed, are instances of more general one:

the hidden subgroup problem

But first, we shall exercise our skills to deal with *QFT* based algorithms with a simple, but illustrative example.

The exercise

The problem

Build a quantum circuit to compute

$$|x\rangle \mapsto |x + y \pmod{2^n}\rangle$$

where y is a constant and $0 \leq x \leq 2^n$

The strategy

Build a quantum circuit to compute

$$|x\rangle \mapsto \underbrace{\frac{1}{\sqrt{2^n}} \sum_k e^{\frac{2\pi i k x}{2^n}}}_{QFT} \mapsto \underbrace{\frac{1}{\sqrt{2^n}} \sum_k e^{\frac{2\pi i k (x+y)}{2^n}} |k\rangle}_{\text{phase shifts}} \mapsto \underbrace{|x + y \pmod{2^n}\rangle}_{QTF^{-1}}$$

The circuit

The phase shifts requires the application of

$$|k\rangle \mapsto e^{\frac{2\pi i k y}{2^n}} |k\rangle$$

Writing $k = \sum_{i=0}^{n-1} k_i \, 2^i$ and $y = \sum_{j=0}^{n-1} y_j \, 2^j$, the product boils down to

$$k\,y = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} k_i y_j \, 2^{i+j}$$

which, written in terms of the qubits used to represent $|k\rangle$, corresponds to the unitary operator

$$U = \bigotimes_i |k_i\rangle \mapsto \bigotimes_i \left(\prod_j e^{\frac{2\pi i y_j k_i}{2^{n-i-j}}} |k_i\rangle \right)$$

The circuit

Operator

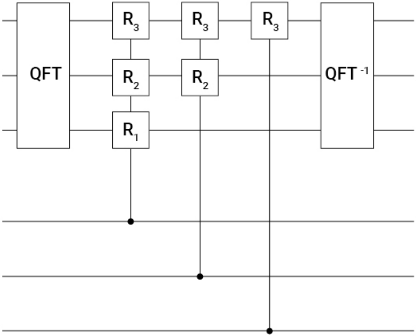
$$U = \bigotimes_i |k_i\rangle \mapsto \bigotimes_i \left(\prod_j e^{\frac{2\pi i y_j k_i}{2^{n-i-j}}} |k_i\rangle \right)$$

can be decomposed in phase shifts over state $|k\rangle$ controlled by y: i.e. for each qubit $|k_i\rangle$ and bit y_j, apply a gate R_{n-i-j} controlled by y_j, where

$$R_l = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^l}} \end{bmatrix}$$

The circuit

Clearly, $R_l = I$ for all $l \leq 0$ and therefore the rotation is not applied for every pair (i, j) such that $i + j \geq n$, yielding the following circuit for $n = 3$:



The circuit

If y is a power of 2 less phase shift gates will be necessary.

In particular, if $y = 2^n$ a single shift is required because only $y_{n-1} \neq 0$, e.g. for $n = 3$,

$$
\begin{aligned}
U(\bigotimes_i |k_i\rangle) &= \bigotimes_i \left(\prod_j e^{\frac{2\pi i y_j k_i}{2^{3-i-j}}} |k_i\rangle \right) \\
&= \left(e^{\frac{2\pi i y_0 k_0}{2^2}} \times e^{\frac{2\pi i y_1 k_0}{2^2}} \times e^{\frac{2\pi i y_2 k_0}{2^1}} \right) |k_0\rangle \\
&\otimes \left(e^{\frac{2\pi i y_0 k_1}{2^2}} \times e^{\frac{2\pi i y_1 k_1}{2^1}} \times e^{\frac{2\pi i y_2 k_1}{2^0}} \right) |k_1\rangle \\
&\otimes \left(e^{\frac{2\pi i y_0 k_2}{2^1}} \times e^{\frac{2\pi i y_1 k_2}{2^0}} \times e^{\frac{2\pi i y_2 k_2}{2^{-1}}} \right) |k_2\rangle
\end{aligned}
$$