Quantum Computation

(Lecture 10)

Luís Soares Barbosa

Universidade do Minho

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

UNITED NATIONS UNIVERSITY UNU-EGOV

Quantum Computing Course Unit

Universidade do Minho, 2021

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 relevant 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: $\longrightarrow \quad \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle$
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}: $\longrightarrow \quad \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |\widetilde{\frac{l}{r}}\rangle|\overline{f}(l)\rangle$
5. Measure first register: $\longrightarrow \quad \widetilde{\frac{l}{r}}$
6. Post-processing: continued fractions: $\longrightarrow \quad r$

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

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

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 an 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

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

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

Analysis

This entails

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

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

Example: 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

$$f_a(k) = a^k (\mathrm{mod}\, n)$$

as the period is exactly the order:

$$a^{k+r} (\mathrm{mod}\, n) = a^k a^r (\mathrm{mod}\, n) = a^k (\mathrm{mod}\, n)$$

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

Example: 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

Both the period estimation and discrete logarithm problems, and many others indeed, are instances of more general one:

the hidden subgroup problem

The discrete logarithm problem

The problem

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

This problem can be solved as an instance of period estimation for function:

$$f(x_1, x_2) \;=\; a^{sx_1 + x_2} (\mathrm{mod}\, n)$$

through the observation that f is periodic:

$$f(x_1 + k, x_2 - ks) \;=\; a^{s(x_1+k)+x_2-ks} (\mathrm{mod}\, n) \;=\; a^{sx_1+x_2} (\mathrm{mod}\, n) \;=\; f(x_1, x_2)$$

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

The ingredients

Although the expression for the period is less common, the algorithm follows step-by-step the one for period finding discussed in the previous lecture.

From the outset, one assumes

- An oracle
$$U|x_1\rangle|x_2\rangle|y\rangle \ = \ y \otimes f(x_1, x_2)$$
- Knowledge of the order of a, i.e. the minimum r positive such that $\mathrm{rem}\,(a^r, n) = 1$, computed by the order finding algorithm.
- A state to store the function evaluation and two other registers with a suitable number of qubits ($t = \mathcal{O}(\log r + \log \frac{1}{\epsilon})$), all of them prepared to hold 0.

The algorithm

1. $|0\rangle|0\rangle|0\rangle$
2. Uniform superposition: $\longrightarrow \quad \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|0\rangle$
3. Oracle: $\longrightarrow$

$$\frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1,x_2)\rangle$$

$$\approx \frac{1}{2^t\sqrt{r}}\sum_{k=0}^{r-1}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1} e^{\frac{2\pi i(skx_1+kx_2)}{r}}|x_1\rangle|x_2\rangle|\bar{f}(sk,k)\rangle$$

$$= \frac{1}{2^t\sqrt{r}}\sum_{k=0}^{r-1}\left(\sum_{x_1=0}^{2^t-1} e^{\frac{2\pi i skx_1}{r}}|x_1\rangle\right)\left(\sum_{x_2=0}^{2^t-1} e^{\frac{2\pi i kx_2}{r}}|x_2\rangle\right)|\bar{f}(sk,k)\rangle$$

The algorithm

4. QFT^{-1}: $\longrightarrow$ $\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\widetilde{\frac{sk}{r}}\rangle|\widetilde{\frac{k}{r}}\rangle|\bar{f}(sk,k)\rangle$
5. Measure the first two registers: $\longrightarrow$ $\left(\widetilde{\frac{sk}{r}},\widetilde{\frac{k}{r}}\right)$
6. Post-processing: continued fractions: $\longrightarrow$ s

Observing that $r \approx 2^t$, step 3 is the crucial step introducing state $|\bar{f}(k_1,k_2)\rangle$ as the Fourier transform of $|f(x_1,x_2)\rangle$ which can be written as

$$|\bar{f}(k_1,k_2)\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{\frac{-2\pi i k_2 j}{r}}|f(0,j)\rangle$$

whenever $k_1 - k_2 s$ is an integer multiple of r.

Proof

Making $k = -x_1$ in $f(x_1 + k, x_2 - sk)$, $f(x_1, x_2) = f(0, x_1 s + x_2)$. Thus,

$$
\begin{aligned}
|\overline{f}(k_1, k_2)\rangle &= \frac{1}{r\sqrt{r}} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{\frac{-2\pi i(k_1 x_1 + k_2 x_2)}{r}} |f(x_1, x_2)\rangle = \\
&= \frac{1}{r\sqrt{r}} \sum_{x_1=0}^{r-1} \sum_{j=x_1 s}^{x_1 s+(r-1)} e^{\frac{-2\pi i(k_1 x_1 + k_2 x_2 - k_2 x_1 s)}{r}} |f(0, j)\rangle \\
&= \frac{1}{r\sqrt{r}} \sum_{x_1=0}^{r-1} e^{\frac{-2\pi i(k_1 - k_2 s) x_1}{r}} \sum_{j=x_1 s}^{x_1 s+(r-1)} e^{\frac{-2\pi i k_2 j}{r}} |f(0, j)\rangle \\
&= \frac{1}{r\sqrt{r}}\, r\, \delta_{k_1 - k_2 s, r} \sum_{j=x_1 s}^{x_1 s+(r-1)} e^{\frac{-2\pi i k_2 j}{r}} |f(0, j)\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{\frac{-2\pi i k_2 j}{r}} |f(0, j)\rangle\, \delta_{k_1 - k_2 s, r}
\end{aligned}
$$

Going generic

The problem

Given a group $(G, +)$ and a function $f : G \longrightarrow S$ to a finite set S, such that there exists a nontrivial subgroup $H \leq G$ for which f is

constant and distinct in each of its cosets,

determine H, i.e. the set of its generators.

Note that the condition of being constant and distinct in each of its cosets is equivalent to

$$f_H : G|H \longrightarrow S \text{ is injective, and } \forall_{g \in G} \forall_{x,y \in g+H} \,.\; f(x) = f(y) \qquad (1)$$

Recall

- Recall that a coset of H for an element $g \in G$ is the set $g + H = \{g + h \mid h \in H\}$, intuitively a translation of H through g.
- The set of cosets of H forms a partition of G whose parts have identical cardinality (that of H itself).
- Give $T \subset G$, (T) is the subset of elements of G that can be formed from T by composition and inverses. Clearly, $H = (T)$ is a subgroup of G and T is called the set of generators of H.

Instances

Several problemas previously discussed are instances of the hidden subgroup problem.

Period finding

Let $G = (\mathbb{Z}, +)$, S any finite set, $H = (r)$, i.e. the set of all multiples of r: $\{0, r, 2r, 3r, \cdots\}$, and $f(x) = f(x + r)$.

Simon

Let $G = (\{0, 1\}^*, \oplus)$, S any finite set, $H = \{0, s\}$, for $s \in \{0, 1\}^*$, and $f(x) = f(x \oplus s)$.

Instances

Order-finding

Let $G = (\mathbb{Z}, +)$, $S = \{a^i \mid i \in \mathbb{Z}_r \text{ for } a^r = 1\}$, $H = (r)$, i.e. the set of all multiples of r: $\{0, r, 2r, 3r, \cdots\}$, and $f(x) = a^x$, with $f(x) = f(x + r)$.

Discrete logarithm

Let $G = (\mathbb{Z}_r \times \mathbb{Z}_r, + \times + (\text{mod } r))$, $S = \{a^i \mid i \in \mathbb{Z}_r \text{ for } a^r = 1\}$, $H = ((1, -s))$, where s is the discrete logarithm, and $f(x_1, x_2) = a^{sx_1 + x_2}$, with $f(x_1 + k, x_2 - ks) = f(x_1, x_2)$.

Deutsch

Let $G = (\{0, 1\}, \oplus)$, $S = \{0, 1\}$, $H = \{0\}$ if f balanced, or $\{0, 1\}$ if f constant.

The algorithm

... is a generalization of ones given to the specific problems discussed.

The basic observation is to replace group elements by matrices, so that linear algebra can be used as a tool in group theory.

1. Create a uniform superposition over the elements of G
2. Apply the oracle $U|g\rangle|h\rangle = |g\rangle|h \odot f(g)\rangle$ for a suitable operation $\odot$:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle$$

3. Choose

$$e^{\frac{2\pi ikg}{|G|}}$$

   as a representation of $g \in G$

The algorithm

1. Express $|f(g)\rangle$ as
$$\frac{1}{\sqrt{|G|}} \sum_{k=0}^{|G|-1} e^{\frac{2\pi ikg}{|G|}} |\bar{f}(k)\rangle$$
2. Because f is constant and distinct on cosets of H, this expression can be re-written st
$$|\bar{f}(k)\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} e^{\frac{-2\pi ikg}{|G|}} |f(g)\rangle$$
whose amplitude is very close to 0 but for the values of k st
$$\sum_{h \in H} e^{\frac{-2\pi ikh}{|G|}} = |H|$$
3. Determine k and then the elements of H using the linear constraint above.

The algorithm

In general, this last step this involves a decomposition of G into a product of cyclic groups $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_n}$, for each p_i prime, in order to rewrite the phase

$$e^{\frac{2\pi ikg}{|G|}}$$

as

$$\prod_{i=1}^{n} e^{\frac{2\pi ik_i g_i}{p_i}}$$

for $g_i \in \mathbb{Z}_{p_i}$. Then use the phase estimation algorithm to find each k_i and k from them.

Quantum algorithms

Recall the overall idea:

engineering quantum effects as computational resources

Classes of algorithms

- Algorithms with superpolynomial speed-up, typically based on the quantum Fourier transform, include Shor's algorithm for prime factorization. The level of resources (qubits) required is not yet currently available.
- Algorithms with quadratic speed-up, typically based on amplitude amplification, as in the variants of Grover's algorithm for unstructured search. Easier to implement in current NISQ technology, typical component of other algorithms.
- Quantum simulation

... and we are done!

Where to look further

- Quantum computation is an extremely young and challenging area, looking for young people either with a theoretical or experimental profile.
  Get in touch if you are interested in pursuing studies/research in the area at UMinho, INESC TEC and INL.
- A follow-up course on Quantum Logic next year, covering quantum programming languages, calculi and logics.

Universidade do Minho

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

… and we are done!

Where to look further

Two Research Groups at INL (dissertation themes coming next week!):

- Quantum Software Engineering Group: oriented towards the development of foundations and mathematical methods for Quantum Computer Science and Software Engineering and its application to strategic problem-areas.
- Quantum and Linear-Optical Computation Group: to explore the features of quantum theory that enable advantage in quantum information processing tasks, in particular those present in photonic implementations of quantum computers.

Universidade do Minho   HASLab HIGH-ASSURANCE SOFTWARE LABORATORY   INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY