

# Quantum Computation

Lectures by Richard Jozsa

## Contents

<b>1</b>	<b>Review of Shor's Algorithm</b>	<b>2</b>
1.1	Factoring Problem . . . . .	2
1.2	Quantum Factoring Algorithm Summary . . . . .	2
1.3	Quantum Algorithm for Periodicity Determination . . . . .	3

# 1 Review of Shor's Algorithm

This result is powered by the **quantum period finding algorithm**, and will lead us to the **hidden subgroup problem** (henceforce HSP).

## 1.1 Factoring Problem

Given an integer  $N$ , with  $n = O(\log N)$  digits, we want to find a non-trivial factor in time complexity  $O(\text{poly}(n))$ .

The important concept here is that of **polynomial time complexity**: any computation has an input, from which we obtain an input *size*  $n$ . Then by polynomial time complexity, we mean that the number of steps/gates (either classical or quantum) grows only polynomially with  $n$  (*i.e.* is  $O(\text{poly}(n))$ ).

When we refer to **efficient** computation, we are always referring to polynomial time complexity.

The best known *classical* factoring algorithm has complexity  $e^{O(n^{\frac{1}{3}}(\log n)^{\frac{2}{3}})}$ . However, the best known quantum algorithm (due to Shor) runs in  $O(n^3)$ , a considerable improvement.

## 1.2 Quantum Factoring Algorithm Summary

First, we convert factoring into period determination:

Given  $N$ , choose  $a < N$  with  $(a, N) = 1$  and consider  $f : \mathbb{Z} \rightarrow \mathbb{Z}_N, x \mapsto a^x \bmod N$ . Euler's Theorem tells us that  $f$  is periodic, and the period  $r$  is the order of  $a$  modulo  $N$ , *i.e.* the least  $m > 1$  such that  $a^m \equiv 1 \bmod N$  - this exists if and only if  $a, N$  are coprime. Through knowledge of  $r$  we are able to compute a factor of  $N$ .

While the process of determining  $r$  is *mathematically* very simple, it is in fact as difficult to compute from a classical perspective as factoring  $N$  itself. Instead we use the **Quantum algorithm for periodicity determination**.

**The task:** Given an oracle/black box for  $f : \mathbb{Z}_M \rightarrow \mathbb{Z}_N$  with promises:

- $f$  is periodic, with (unknown) period  $r \in \mathbb{Z}_M$ , *i.e.*  $f(x+r) = f(x)$  for all  $x \in \mathbb{Z}_M$ .
- $f$  is 1-1 in each period, *i.e.*  $f(x_1) \neq f(x_2)$  for any  $0 \leq x_1 < x_2 < r$ .

We want to find  $r$  in time  $O(\text{poly}(m))$ ,  $m = \log M$  (with any prescribed success probability  $1 - \varepsilon$ ,  $\varepsilon > 0$ ).

**Remark:** Queries to the oracle count as 1 step. In the quantum context we assume the oracle is a unitary gate  $U_f$  on  $\mathcal{U}_M \otimes \mathcal{U}_N$ , where  $\mathcal{U}_M$  is the state space with dimension  $M$ , basis  $\{|i\rangle\}_{i \in \mathbb{Z}_M}$ .  $U_f$  acts on basis states as

$$U_f \underbrace{|i\rangle}_{\text{input}} \underbrace{|j\rangle}_{\text{output}} = |i\rangle |j + f(i)\rangle, \quad i \in \mathbb{Z}_M, j \in \mathbb{Z}_M$$

The **Query complexity** of an algorithm is the number of times the oracle is queried, which is also required to be  $O(\text{poly}(m))$ .

To solve the periodicity problem classically, it can be shown that it is both necessary and sufficient to query the oracle  $O(\sqrt{N})$  times, so there is no polynomial algorithm. However, there *is* a quantum algorithm.

### 1.3 Quantum Algorithm for Periodicity Determination

For further details *c.f.* Part II notes pp.60-64.

Write  $A = M/r = \# \text{periods}$ . We work in the state space  $\mathcal{U}_M \otimes \mathcal{U}_N$  with basis  $\{|i\rangle|k\rangle : i \in \mathbb{Z}_M, k \in \mathbb{Z}_N\}$ .

**Step 1:** obtain the state

$$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle|0\rangle$$

**Step 2:** apply  $U_f$  to obtain

$$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle|f(i)\rangle$$

**Step 3:** measure the output register, obtaining result  $y$ . By the **Born rule**, the input register collapses to all those  $i$  such that  $f(i) = y$ , *i.e.*  $i = x_0, x_0 + r, \dots, x_0 + (A-1)r$  where  $0 \leq x_0 < r$  in the first period has  $f(x_0) = y$ .

We discard the output register to obtain

$$|\text{per}\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle$$

Note that each  $0 \leq x_0 < r$  occurs with probability  $1/r$ .

If we naively measure  $|\text{per}\rangle$ , the Born rule implies we get  $x_0 + jr$  with  $j = 0, \dots, A-1$  chosen uniformly with probability  $1/A$ , *i.e.* a random element of a random period; this is a uniformly random integer in  $\mathbb{Z}_M$ . This is useless to us. Instead...

**Step 4:** apply **Quantum Fourier Transform** (QFT). Recall that

Lecture 2

$$\text{QFT}|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \omega^{xy} |y\rangle$$

**Fact:** QFT modulo  $M$  is unitary, and can be implemented in  $O(m^2)$  time,  $m = \log M$ . See Part II QIC notes for circuit details of implementation.

Then

$$\begin{aligned} \text{QFT}|\text{per}\rangle &= \frac{1}{\sqrt{MA}} \sum_{j=0}^{A-1} \left( \sum_{y=0}^{M-1} \omega^{(x_0+jr)y} |y\rangle \right) \\ &= \frac{1}{\sqrt{MA}} \sum_{y=0}^{M-1} \omega^{x_0 y} \left[ \sum_{j=0}^{A-1} \omega^{jry} \right] |y\rangle \end{aligned}$$

Note that  $[\dots]$  is a geometric series, with ratio  $\omega^{ry} = e^{2\pi i r y / M} = (e^{e\pi i / A})^y$ . So the sum equals zero unless  $y$  is a multiple of  $A = M/r$ , in which case every term in the sum is 1 so the sum equals  $A$ . So the non-multiples of  $A$  get sifted out by QFT.

Hence, we have

$$\text{QFT}|\text{per}\rangle = \sqrt{\frac{A}{M}} \sum_{k=0}^{r-1} \omega^{x_0 k M/r} |k \frac{M}{r}\rangle$$

Then measuring  $\text{QFT}|\text{per}\rangle$  we get a value  $c = k_0 M/r$ , with  $0 \leq k_0 \leq r-1$  chosen uniformly at random. Thus we have  $k_0/r = c/M$ , where the values  $c, M$  are known and  $k_0$  has been chosen at random; we want  $r$ . Note that if we are fortunate enough to have  $(k_0, r) = 1$ , then we can (efficiently) cancel  $c/M$  down to its lowest terms, and read off  $r$  as the denominator. But in general this will not be the case:

**Theorem: (Coprimalty Theorem)** *The number of positive integers  $< r$  that are coprime to  $r$  grows as  $O(r/\log \log r)$  for large  $r$ .*

Hence the above  $\mathbb{P}(k_0 \text{ coprime to } r) = O(1/\log \log r)$ . So if we do it enough times, we will almost surely be successful:

**Probability Lemma:** If a single trial has success probability  $p$ , then we repeat  $k$  times, and for any  $0 < 1 - \varepsilon < 1$ , we have that

$$\begin{aligned} \text{if } k &= -\frac{\log \varepsilon}{p} \\ \text{then } \mathbb{P}(\geq 1 \text{ success in } k \text{ trials}) &> 1 - \varepsilon \end{aligned}$$

So after finding  $c$ , cancel  $c/M$  down to its lowest terms  $a/b$  (classically, in polynomial time using Euclid's algorithm). We get  $r$  as denominator  $b$  if  $(k_0, r) = 1$ , which happens with probability  $O(1/\log \log r)$ , otherwise  $c, M$  have more common factors, so  $b < r$ .

We don't know immediately whether that has happened or not, but we can check the  $b$  value by making two more queries to the oracle,  $f(0)$  and  $f(b)$ ; these are equal iff  $b = r$ .

So if we repeat this  $K = O(\log \log r)$  times, then we will obtain  $r$  with any high probability we desire - and this runs in polynomial time.

### **Origin and utility of QFT here**

Write  $R = \{0, r, 2r, \dots, (A-1)r\} \subset \mathbb{Z}_M$ , and

$$\begin{aligned} |R\rangle &= \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle \\ |\text{per}\rangle &= |x_0 + R\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |x_0 + kr\rangle \end{aligned}$$

The problem is that the  $|x_0 + kr\rangle$  terms are distributed randomly.

For each  $x_0 \in \mathbb{Z}_M$ , consider the map  $k \mapsto k + x_0$  on  $\mathbb{Z}_M$ ; this is the 1-1 reversible map "shift by  $x_0$ ".

This gives rise to a linear map  $U(x_0)$  on  $\mathcal{U}_M$ , and  $U(x_0) : |k\rangle \rightarrow |k + x_0\rangle$  is unitary, and  $|x_0 + R\rangle = U(x_0)|R\rangle$ .

Since  $(\mathbb{Z}_M, +)$  is an *abelian* group, these shift operators all commute, *i.e.*  $U(x_0)U(x_1) = U(x_0 + x_1) = U(x_1)U(x_0)$ . So they have an orthonormal basis of common eigenvectors  $\{|\chi_k\rangle\}_{k \in \mathbb{Z}_M}$ , called the *shift-invariant* states. Note that they are not left entirely unchanged by the  $U(x_0)$  operators, but they

are shifted only by a constant phase factor, i.e.  $U(x_0)|\chi_k\rangle = \omega(x_0, k)|\chi_k\rangle$  for all  $x_0, k \in \mathbb{Z}_M$ , and  $|\omega(x_0, k)| = 1$ .

Now consider  $|R\rangle$  written in the  $\chi$ -basis

$$|R\rangle = \sum_{k=0}^{M-1} a_k |\chi_k\rangle$$

where the amplitudes  $a_k$  depend only on  $r$ , and not on  $x_0$  (obviously). Then  $|\text{per}\rangle = U(x_0)|R\rangle = \sum a_k \omega(x_0, k) |\chi_k\rangle$ , and measurement in the  $\chi$ -basis has  $\mathbb{P}(k) = |a_k \omega(x_0, k)|^2 = |a_k|^2$ , independent of  $x_0$ , depending only on  $r$ . So we want to measure in this basis, but aren't allowed to do that (computationally) since the basis is too complicated.

So we introduce QFT as the unitary mapping that rotates the  $\chi_k$ -basis onto the standard basis  $|k\rangle$ , and follow this up by a standard basis measurement.

But what does this mapping look like, and where does it come from? We need the explicit form of the shift-invariant eigenstates:

$$\begin{aligned} |\chi_k\rangle &= \frac{1}{\sqrt{M}} \sum_{\ell=0}^{M-1} e^{-2\pi i k \ell / M} |\ell\rangle \\ \Rightarrow \mathcal{U}(x_0) |\chi_k\rangle &= \frac{1}{\sqrt{M}} \sum_{\ell=0}^{M-1} e^{-2\pi i k \ell / M} |\ell + x_0\rangle \\ &= \frac{1}{\sqrt{M}} \sum_{\tilde{\ell}=0}^{M-1} e^{-2\pi i k (\tilde{\ell} - x_0)} |\tilde{\ell}\rangle \\ &= e^{2\pi i k x_0 / M} |\chi_k\rangle \end{aligned}$$

So  $\omega(x_0, k) = e^{2\pi i k x_0 / M}$ .

The matrix of  $\text{QFT}^{-1}$  (mapping  $|k\rangle$  to  $|\chi_k\rangle$ ) has components of  $|\chi_k\rangle$  as the  $k^{\text{th}}$  column, so  $[\text{QFT}^{-1}]_{\ell k} = \frac{1}{\sqrt{M}} e^{-2\pi i \ell k / M}$ . Since QFT is unitary, to find the inverse we need only take the conjugate transpose.

Hence  $[\text{QFT}]_{k\ell} = \frac{1}{\sqrt{M}} e^{2\pi i k \ell / M}$ , as previously defined.

This notion of QFT in fact occurs very naturally in group theory as the *discrete Fourier transform*. The fact that this QFT is unitary means that all the group theoretic results it relies on slot in perfectly, allowing us to make as much use of this want in a way that we are not able classically.