Lecture 10:
Shor's algorithm

Luís Soares Barbosa

Universidade do Minho

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

INL
INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

UNU

Mestrado em Engenharia Física

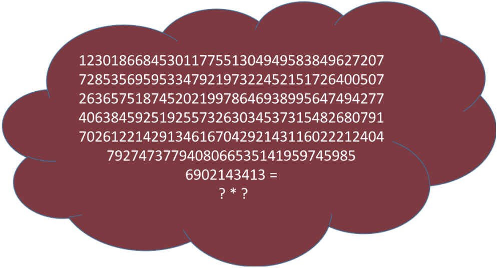
Universidade do Minho, 2025-26

Shor's algorithm

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer

Proc. 35th Annual Symp. on Foundations of Computer Science, IEEE Computer Society Press, pp. 124-134 (1994)

was a turning point in quantum computing for its spectacular decrease of the time complexity of factoring from $\mathcal{O}(e^{\sqrt[3]{n}})$ to $\mathcal{O}(n^3 \log n)$, with potential impact in cryptography.



Factorization

In this famous 1994 paper, Peter Shor proved that it is possible to factor a n-bit number in time that is polynomial to n.

The factorization problem

Given an integer n, find positive integers $p_1, p_2, \cdots, p_m, r_1, r_2, \cdots, r_m$ such that

- Integers $p_1, p_2, \cdots, p_m$ are distinct primes;
- and, $n = p_1^{r_1} \times p_2^{r_2} \times \cdots \times p_m^{r_m}$.

Note that one may assume n to be odd and contain at least two distinct odd prime factors (why?)

Factorization

Since the test for primality can be done classically in polynomial time, the factoring problem can be reduced to $\mathcal{O}(\log n)$ instances of the following problem:

The odd non-prime-power integer splitting problem

Given an odd integer n, with at least two distinct prime factors, compute two integers

$$1 < n_1 < n \quad \text{and} \quad 1 < n_2 < n$$

st $n = n_1 \times n_2$

Factorization

Miller proved in 1975 that this problem reduces probabilistically to another problem whose solution resorts to the eigenvalue estimation problem, already studied.

The order-finding problem

Given two coprime integers a and n, i.e. st $\gcd(a, n) = 1$, find the order of a modulo n.

Preliminaries: Modular arithmetic

Arithmetic within the set of integers modulo n

$$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$$

proceeds by dividing by n the result of the relevant operation and returning the corresponding reminder.
Indeed,

$$x \equiv y \pmod{n} \;\text{ iff }\; \mathrm{rem}\,(x, n) = y$$

or, equivalently, $\mathrm{rem}\,(x-y, n) = 0$, where $\mathrm{rem}\,(a, b)$ is the reminder of the integer division of a by b.

Examples

$5 \equiv 0 \pmod{5}$ and $6 \equiv 1 \pmod{5}$

Preliminaries: Modular arithmetic

Particularly important in what follows is the subset of coprimes with n, i.e.

$$\mathcal{Z}_n^\star = \{a \in \mathcal{Z}_n \mid \gcd(a, n) = 1\}$$

and the following observations:

- This set is the carrier of an Abelian group from multiplication modulo n.
- Repeatedly multiplying an arbitrary element of $\mathcal{Z}_n^\star$ by itself will eventually return 1, i.e., for $a \in \mathcal{Z}_n^\star$, the number 1 will appear somewhere in the sequence

$$\mathrm{rem}\,(a, n), \mathrm{rem}\,(a^2, n), \mathrm{rem}\,(a^3, n), \cdots$$

after what the sequence repeats itself in a periodic way.

Order of $a \pmod{n}$

Definition

For $a \in \mathbb{Z}_n^\star$ (or, in general, for two co-prime integers $a < n$) the order of $a \pmod{n}$ is the smallest integer $r > 0$ s.t.

$$a^r \equiv 1 \pmod{n}$$

Example

If $n = 5$ the sequence $3^0, 3^1, 3^2, 3^3, 3^4, 3^5, 3^6, \ldots$ leads to the sequence $1, 3, 4, 2, 1, 3, 4, \ldots$. Thus, the

$$\text{order of } 3 \pmod{5} \text{ is } 4$$

Exercise

What is the order of $2 \pmod{11}$?

The problem

The order-finding problem

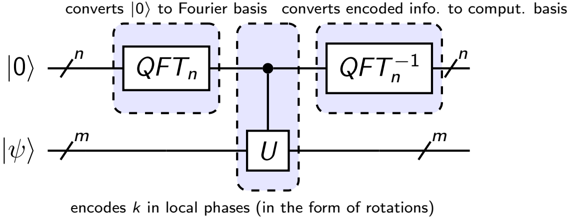
Given two coprime integers a and n, i.e. st $\gcd(a, n) = 1$, find the order of $a \pmod n$, i.e. the smallest positive integer r such that

$$a^r \equiv 1 \pmod n$$

- Classically, this problem can be difficult for large integers.
- In a quantum computer, however, it can be solved efficiently via the quantum eigenvalue estimation algorithm.

Strategy: The eigenvalue approach

Recall the eigenvalue estimation circuit:



Need to choose suitable U and $|\psi\rangle$ to disclose the order

Strategy: The eigenvalue approach

For $a \in \mathbb{Z}_n^\star$ define U_a in a system whose basis states are labelled by elements of $\mathbb{Z}_n$ (i.e., $\{|0\rangle, \cdots, |n-1\rangle\}$), by

$$U_a |q\rangle = |\mathrm{rem}\,(qa, n)\rangle$$

or, making clear the multiplication in $\mathbb{Z}_n$,

$$U_a |q\rangle = |qa\rangle$$

Exercise

Show U_a is unitary.

Exercise

Show that $U_a |\mathrm{rem}\,(a^n, n)\rangle = \left|\mathrm{rem}\,(a^{n+1}, n)\right\rangle$

Next step is to identify suitable eigenvectors.

A first attempt (starting with an axample)

For $n = 5$, sequence

$$3^0, 3^1, 3^2, 3^3, 3^4, 3^5, 3^6, \ldots$$

leads to $\underline{1, 3, 4, 2}, 1, 3, 4, \ldots$, thus the order r of $3 \pmod 5$ is 4.

Thus, compute

$$U_a\left(\frac{1}{\sqrt{r}}(|1\rangle + |3\rangle + |4\rangle + |2\rangle)\right)$$
$$= U_a\left(\frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}\left|\mathrm{rem}\,(3^i, 5)\right\rangle\right)$$
$$= \frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}\left|\mathrm{rem}\,(3^{i+1}, 5)\right\rangle$$
$$= \frac{1}{\sqrt{r}}\left(|3\rangle + |4\rangle + |2\rangle + |1\rangle\right)$$
$$= \frac{1}{\sqrt{r}}\left(|1\rangle + |3\rangle + |4\rangle + |2\rangle\right)$$

... to conclude that his state is an eigenvector of U_a

A first attempt

The previous example resorts to the equation

$$U_a\left(\frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}\left|\mathrm{rem}\,(a^i,n)\right\rangle\right)=\frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}\left|\mathrm{rem}\,(a^i,n)\right\rangle\right)$$

Unfortunately, the corresponding eigenvalue is 1 ...
... which does not disclose any information about r!

Need to find eigenvectors with more informative eigenvalues.

A second attempt

Since $a^r = 1 \pmod n$,

$$U_a^r(|q\rangle) = |\mathrm{rem}\,(qa^r, n)\rangle = |q\rangle$$

i.e. U_a is the rth-root of the identity operator I, i.e. $(U_a)^r = I$.

It can be shown that the eigenvalues λ of such an operator satisfy

$$\lambda^r = 1$$

i.e. they are rth-roots of 1, which means they take the form

$$e^{i2\pi\frac{k}{r}}$$

for some integer k. In the previous example,

$$1 = e^{i2\pi\frac{0}{r}}$$

A second attempt

Let us consider a different state:

$$|\psi_1\rangle \;=\; \frac{1}{\sqrt{r}} \sum_{i=0}^{r-1} \omega^{-i} \left|\mathrm{rem}\left(a^i, n\right)\right\rangle$$

where $\omega = e^{i2\pi\cdot\frac{1}{r}}$ $\underbrace{\text{(division of the unit circle in } r \text{ slices)}}_{\text{a.k.a. the } r\text{th-roots of unity}}$

$$U_a\left(\tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1} \omega^{-i} \left|\mathrm{rem}\left(a^i, n\right)\right\rangle\right)$$
$$= \tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1} \omega^{-i} \left|\mathrm{rem}\left(a^{i+1}, n\right)\right\rangle$$
$$= \tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1} \omega\omega^{-(i+1)} \left|\mathrm{rem}\left(a^{i+1}, n\right))\right\rangle$$
$$= \omega\left(\tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1} \omega^{-(i+1)} \left|\mathrm{rem}\left(a^{i+1}, n\right)\right\rangle\right)$$
$$= \omega\left(\tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1} \omega^{-i} \left|\mathrm{rem}\left(a^{i}, n\right)\right\rangle\right)$$

A second attempt

The calculation in the previous slide shows that

$$U_a |\psi_1\rangle = \omega |\psi_1\rangle$$

So if we feed the quantum eigenvalue estimation circuit with U_a and $|\psi_1\rangle$ we obtain an approximation of

$$\frac{1}{r}$$

with a good success probability.

Exercise

Formally justify all the steps in that calculation.

Exercise

Would a similar conclusion pop out if our starting state was

$$|\psi_k\rangle \; = \; \frac{1}{\sqrt{r}} \sum_{i=0}^{r-1} \omega^{-ik} \left|\mathrm{rem}\left(a^i, n\right)\right\rangle$$

How good is this approximation?

The answer depends on the number m of control qubits available.

Typically, the algorithm provides a number $\frac{y}{2^m}$, for $y \in \{0, \cdots, 2^{m-1}\}$, as an approximation for $\frac{1}{r}$. Order r is computed by inverting and rounding to the nearest integer, i.e.

$$\left\lceil \frac{y}{2^m} + \frac{1}{2} \right\rceil$$

Exercise

Suppose $r = 6$. Which is the best approximation to this value one can expect to obtain with 5 and 4 control qubits?

How to estimate m?

The number m of control qubits should be enough to distinguish between $\frac{1}{r}$ and $\frac{1}{r+1}$ and $\frac{1}{r-1}$. In particular, the distance between $\frac{1}{r}$ and $\frac{1}{r+1}$ is

$$\frac{1}{r} - \frac{1}{r+1} \;=\; \frac{1}{r(r+1)}$$

Thus, one must choose m such that

$$\left| \frac{y}{2^m} - \frac{1}{r} \right| \;<\; \frac{1}{2r(r+1)}$$

i.e. the induced error is less than half the distance between $\frac{1}{r}$ and $\frac{1}{r+1}$. In practice, we ignore the value of r (of course!). As $r < n$, we may take instead

$$\left| \frac{y}{2^m} - \frac{1}{r} \right| \;<\; \frac{1}{2n^2}$$

Fine tunning U_a

Choosing m as $2\,\mathrm{rb}(n)+1$, where $\mathrm{rb}(n)$ is the number of bits needed to express the non-negative integer n in binary, given by:

$$\begin{aligned} 1 &\Longleftarrow n = 0 \\ 1 + \lfloor \log_2(n) \rfloor &\Longleftarrow n > 0 \end{aligned}$$

maximizes the probability of obtaining a good approximation to $\frac{1}{r}$.

Once m is fixed, U_a has to be extended to a circuit over m qubits, i.e., over a Hilbert space of dimension 2^m. Thus,

$$\begin{aligned} U_a\,|q\rangle &= |\mathrm{rem}\,(qa, n)\rangle \qquad \text{for } 0 \leq q < n \\ U_a\,|q\rangle &= |q\rangle \qquad \text{for } n \leq q \leq 2^m \end{aligned}$$

Exercise

Show that with this definition of U_a remains unitary.

A third attempt

However ...

How $|\psi_1\rangle$, or, in general, $|\psi_k\rangle$. can be prepared, without knowing r?

Fortunately, it is not necessary!

Instead of preparing an eigenstate corresponding to an eigenvalue $e^{i2\pi \frac{k}{r}}$ for a randomly selected $k \in \{0, 1, \cdots, r-1\}$, it suffices to prepare a uniform superposition of these eigenstates

Then the eigenvalue estimation algorithm will compute a superposition of these eigenstates with estimates of their eigenvalues.

Thus, when a measurement is performed, the result is an estimate of a random eigenvalue.

Question

How to prepare such a superposition without knowing r?

A third attempt

Define

$$|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\psi_k\rangle$$

with $|\psi_k\rangle = \frac{1}{\sqrt{r}} \sum_{i=0}^{r-1} \omega^{-ik} \left|\mathrm{rem}\left(a^i, n\right)\right\rangle$.

Exercise

Show that $U_a |\psi_k\rangle = \omega^k |\psi_k\rangle$.

Now observe that

$$\left|\mathrm{rem}\left(a^i, n\right)\right\rangle \;=\; |1\rangle \;\text{ iff }\; \mathrm{rem}\left(i, r\right) = 0$$

Thus, the amplitude of $|1\rangle$ in the above state is the sum over the terms for which $i = 0$

$$\frac{1}{\sqrt{r}} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i2\pi \frac{k}{r} 0} \;=\; \frac{1}{r} \sum_{k=0}^{r-1} 1 \;=\; 1$$

A third attempt

Thus, if the amplitude of $|1\rangle$ is 1, the amplitudes of all other basis states are 0, yielding

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|u_k\rangle \;=\; |1\rangle$$

Thus, we defined a superposition of eigenvectors that is equal to $|1\rangle$.

Summing up

Thus, the eigenvalue estimation algorithm starting from

$$|0\rangle|1\rangle \;=\; |0\rangle\left(\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|u_k\rangle\right) \;=\; \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|0\rangle|u_k\rangle$$

gives an approximation $\frac{y}{2^m}$ of $\frac{k}{r}$, for $k \in \{0, \cdots, r-1\}$.

$\boxed{\text{But how to extract } r \text{ from this approximation?}}$

To estimate r, one resorts to another result in number theory ...

Estimating r

Theorem: Given an integer $n \geq 2$ and a real number $\rho \in [0, 1]$, there is at most one choice of integers $u, v \in \{0, \cdots, n-1\}$, with $v \neq 0$ and $\gcd(u, v) = 1$ such that

$$\left|\rho - \frac{u}{v}\right| < \frac{1}{2n^2}$$

Integers u, v are computed by the continued fraction algorithm

Taking $\rho = \frac{k}{2^m}$, for a close approximation of $\frac{k}{r}$, the continued fraction algorithm computes $\frac{u}{v}$. The theorem enforces

$$\frac{u}{v} = \frac{k}{r}$$

But how to recover r?

Another result in number theory claims that if u, v are learnt this way for a few different values of k chosen uniformly at random, a good guess for r is computed as the leastcommonmultiplier of all the observed values for v.

Reducing to order-finding

The odd non-prime-power integer splitting problem

Given an odd integer n, with at least two distinct prime factors, compute two integers

$$1 < n_1 < n \quad \text{and} \quad 1 < n_2 < n$$

st $n = n_1 \times n_2$

Miller proved in 1975 that this problem reduces probabilistically to the order-finding problem, all reductions being classical: only the estimation problem is quantum.

Eliminating the easy cases

- Spliting even numbers is trival: return 2 and $\frac{n}{2}$.
- Splitting perfect powers, i.e. $n = e^d$ for integers $e, d \geq 2$ is also easy: compute successive roots and check the nearby integers for e. Notice that quickly the root becomes less than 2, and no more candidates are in order to check.

Shor's algorithm

1. Choose $1 < a \leq n - 1$ randomly.
2. Compute $d = \gcd(a, n)$.
3. If $d > 1$, set $n_1 = d$ and $n_2 = n/d$ and stop.
4. Compute r as the order of a modulo n.
5. If r is even compute: $x = a^{r/2} - 1 \pmod{n}$ and $d = \gcd(x, n)$ else fail
6. If $d > 1$, set $n_1 = d$ and $n_2 = n/d$ and stop, else fail.

Shor's algorithm: The essence

If r is even (it will be with at least a probability of 0.5), $\frac{r}{2}$ is an integer, and one may consider the numbers

$$a^{\frac{r}{2}} - 1 \pmod n \ \text{ and } \ a^{\frac{r}{2}} + 1 \pmod n$$

As $(z-1)(z+1) = z^2 - 1$, we may write

$$a^r - 1 \ = \ (a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)$$

n evenly divides $a^r - 1$ (because $a^r \pmod n = 1$ by definition of order). Thus n must share a prime factor with $(a^{\frac{r}{2}} - 1)$, or $(a^{\frac{r}{2}} + 1)$, or both.

The algorithm extracts this factor from the first term computing $\gcd(a^r - 1, n)$. This can be efficiently done with the the Euclides algorithm.

Shor's algorithm

This works well because it is unlikely that all prime factors of n will divide one of the terms and none will divide the other, in which case we may not find a factor.

A run of Shor's algorithm may fail to find a factor of n if

- r is odd
- r is even but $\gcd a^{r/2} - 1, n = 1$

It can be shown in number theory that, with a probability of at least 50%, neither of these situations occurs. More precisely, the probability that either of the situations occurs is at most $2^{-(p-1)}$, for p the number of distinct prime factors in n,

This also explains why, without the assumption that n is odd and contains at least two prime factors, the algorithm is not able to factorize.

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.
- Follow-up courses next semester on
  - Quantum Logic (calculi and logics for quantum programs)
  - Quantum Data Science (algorithms and exciting applications)

Universidade do Minho

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

Continued Fractions

Method to approximate any real number t with a sequence of rational numbers of the form

$$[a_0, a_1, \cdots, a_p] \text{ defined by } a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_p}}}}$$

computed inductively as follows

$$\begin{aligned} a_0 &= \lfloor t \rfloor & r_0 &= t - a_0 \\ a_j &= \left\lfloor \frac{1}{r_{j-1}} \right\rfloor & r_j &= \frac{1}{r_{j-1}} - \left\lfloor \frac{1}{r_{j-1}} \right\rfloor \end{aligned}$$

The sequence $[a_0, a_1, \cdots, a_p]$ is called the p-convergent of t.
If $r_p = 0$ the continued fraction terminates with a_p and
$t = [a_0, a_1, \cdots, a_p]$,

Continued Fractions

Example: $\frac{47}{13} = [3, 1, 1, 1, 1, 2]$

$$
\begin{aligned}
\frac{47}{13} &= 3 + \frac{8}{13} = 3 + \frac{1}{\frac{1}{\frac{13}{8}}} \\
&= 3 + \frac{1}{1 + \frac{5}{8}} = 3 + \frac{1}{1 + \frac{1}{\frac{8}{5}}} \\
&= 3 + \frac{1}{1 + \frac{1}{1 + \frac{3}{5}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{5}{3}}}} \\
&= 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{2}{3}}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}}
\end{aligned}
$$

Continued Fractions

Theorem: The expansion terminates iff t is a rational number.
[which makes continued fractions the *right*, finite expansion for rational numbers, differently form decimal expansion]

Theorem: $[a_0, a_1, \cdots, a_p] = \frac{p_j}{q_j}$ where

$$\begin{aligned} p_0 &= a_0, \ q_0 = 1 \\ p_1 &= 1 + a_0 a_1 \\ p_j &= a_j p_{j-1} + p_{j-2}, \ \ q_j = a_j q_{j-1} + q_{j-2} \end{aligned}$$

Theorem: Let x and $\frac{p}{q}$ be rationals st

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{2q^2}.$$

Then, $\frac{p}{q}$ is a convergent of the continued fraction for x.