Quantum Computation
(Lecture 8)

Luís Soares Barbosa

Universidade do Minho

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

UNITED NATIONS UNIVERSITY UNU-EGOV

MSc Physics Engineering

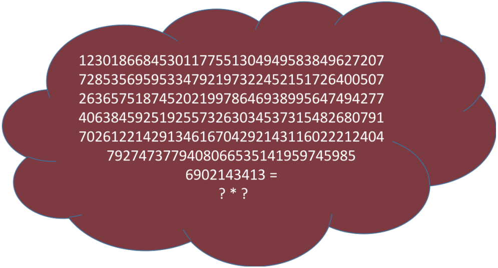
Universidade do Minho, 2021-22

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 a $\mathcal{O}(\log n)$ 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

Order of an element in a group

The order of an element a in a group $G = (A, \theta, e, {}^{-1})$ is the least positive integer r such that $a^r = e$, if any such r exists

Examples

- Every element of the permutation group of degree 4

$$(\text{bijections onto } \{1,2,3,4\}, \cdot, id, {}^{-1})$$

has order 4. For example, consider element $(1,2,3,4) = \{1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 1\}$

$$\begin{aligned}(1,2,3,4)^1 &= (1,2,3,4) \neq id\\(1,2,3,4)^2 &= (1,3)(2,4) \neq id\\(1,2,3,4)^3 &= (1,4,3,2) \neq id\\(1,2,3,4)^4 &= id\end{aligned}$$

Preliminaries

- In $\mathbb{Z} = (\mathbb{Z}, \times, 1, \ ^{-1})$ every element but 0 has order ∞.
- Consider the group of integers modulo n,

$$\mathbb{Z}_n = (\{0, 1, 2, \cdots, n-1\}, \times_n, 1, \ ^{-1})$$

Note then when defining the order of a as the smallest positive integer r such that $a^r = 1$, the exponentiation is taken modulo n, and therefore the equality can be written as

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

where $x = y \pmod{n}$ abbreviates $\text{rem}\,(x-y, n) = 0$, i.e. $\text{rem}\,(x, n) = \text{rem}\,(y, n)$, which is the equality in $\mathbb{Z}_n$

So, e.g. the order of 4 in $\mathbb{Z}_5$ is 2 because

$$\begin{aligned} 4^1 &= 4 \pmod{5} \\ 4^2 &= 1 \pmod{5} \end{aligned}$$

The problem

Note that any integer a st $\gcd(a, n) = 1$ the number 1 will appear somewhere in the sequence

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

after what the sequence repeats itself in a periodic way.

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, i.e. the smallest positive integer r such that

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

Strategy: The eigenvalue approach

Consider the following operator:

$$U_a(|q\rangle) = |\text{rem}(qa, n)\rangle \quad \text{for } 0 \leq q < n$$

Clearly, U_a is unitary: being a coprime with n, a has an inverse modulo n and, thus, is reversible.

Note that U_a can be extended reversibly to an implementation in a circuit over m qubits ($2^m > n$) making

$$U_a(|q\rangle) = |\text{rem}(qa, n)\rangle \quad \text{for } 0 \leq q < n$$
$$U_a(|q\rangle) = |q\rangle \quad \text{for } q \geq n$$

In any case, let us focus on the action of U_a restricted to the state space spanned by $\{|0\rangle, |1\rangle, \cdots, |n-1\rangle\}$.

Strategy: The eigenvalue approach

Since $a^r = 1(\text{mod } n)$,

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

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 the rth root of 1, which means they take the form $e^{2\pi i \frac{k}{r}}$, for some integer k.

Thus, suppose one is able to prepare the state

$$|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{q=0}^{r-1} e^{-2\pi i \frac{k}{r} q} |\text{rem}\,(a^q, n)\rangle$$

Strategy: The eigenvalue approach

$$\begin{aligned} U_a|u_k\rangle &= \frac{1}{\sqrt{r}}\sum_{q=0}^{r-1} e^{-2\pi i \frac{k}{r} q} U_a|\text{rem}\,(a^q, n)\rangle \\ &= \frac{1}{\sqrt{r}}\sum_{q=0}^{r-1} e^{-2\pi i \frac{k}{r} q}|\text{rem}\,(a^{q+1}, n)\rangle \\ &= e^{2\pi i \frac{k}{r}} \frac{1}{\sqrt{r}}\sum_{q=0}^{r-1} e^{-2\pi i \frac{k}{r}(q+1)}|\text{rem}\,(a^{q+1}, n)\rangle \\ &= e^{2\pi i \frac{k}{r}}|u_k\rangle \end{aligned}$$

Observing that, for the last step, we have

$$e^{2\pi i \frac{k}{r} r}|\text{rem}\,(a^{q+1}, n)\rangle = e^{2\pi i \frac{k}{r} 0}|\text{rem}\,(a^0, n)\rangle$$

Strategy: The eigenvalue approach

... concluding that

$|u_k\rangle$ is an eigenstate for U_a with eigenvalue $e^{2\pi i \frac{k}{r}}$

Thus, for any value $0 \leq k \leq r-1$, the eigenvalue estimation algorithm will compute an approximation $\widetilde{k/r}$ to $\frac{k}{r}$ mapping

$$|0\rangle|u_k\rangle \mapsto |\widetilde{k/r}\rangle|u_k\rangle$$

However ...

Without knowing r we do not know how to prepare $|u_k\rangle$.

Fortunately, it is not necessary!

Strategy: The eigenvalue approach

Instead of preparing an eigenstate corresponding to an eigenvalue $e^{2\pi i \frac{k}{r}}$ for a randomly selected $k \in \{0, 1, \cdots, r-1\}$, it suffices to prepare a uniform superposition of the eigenstates

Then the eigenvalue estimation algorithm will compute a superposition of these eigenstates entangled 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?

Strategy: The eigenvalue approach

The uniform superposition is

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|u_k\rangle \;=\; \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{q=0}^{r-1} e^{-2\pi i\frac{k}{r}q}|\text{rem}\,(a^q,n)\rangle$$

Note that

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

Thus, the amplitude of $|1\rangle$ in the above state is the sum over the terms for which $q=0$
(because q takes values in $[0,r-1]$ and must be a multiple of r)

$$\frac{1}{\sqrt{r}}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi i\frac{k}{r}0} \;=\; \frac{1}{r}\sum_{k=0}^{r-1} 1 \;=\; 1$$

Strategy: The eigenvalue approach

If the amplitude of $|1\rangle$ is 1, this means that 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, the eigenvalue estimation algorithm maps

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

Strategy: The eigenvalue approach

Thus, after executing the eigenvalue estimation algorithm the first register contains a uniform superposition of states $|\widetilde{k/r}\rangle$ for $k \in \{0, 1, \cdots, r-1\}$.

Measuring this register yields an integer x st $\frac{x}{2^n}$ is an estimate of $\frac{k}{r}$ for some k selected uniformly at random.

Finally, to estimate r one resorts to the following result in number theory:

Estimating r

Theorem: Let r be a positive integer, and take integers k_1 to k_2 selected independently and uniformly at random from $\{0, 1, \cdots, r-1\}$. Let c_1, c_2, r_1, r_2 be integers st $\gcd(r1, c1) = \gcd(r2, c2) = 1$ and

$$\frac{k_1}{r} = \frac{c_1}{r_1} \quad \text{and} \quad \frac{k_2}{r} = \frac{c_2}{r_2}$$

Then, $r = \operatorname{lcm}(r_1, r_2)$ with probability at least $\frac{6}{\pi^2}$.

Thus

- To obtain $\frac{c_1}{r_1}$ from $\widetilde{k/r}$, i.e. the nearest fraction approximating $\frac{k}{r}$ up to some precision dependent on the number of qubits used, one resorts to the continued fractions method.
- As a second pair (c_2, r_2) is needed, the whole algorithm is repeated.

The order-finding algorithm

1. Prepare a n-qubit register, identified as the control register, for an integer n st $2^n > 2r^2$, with $|0\rangle$ over n qubits.
2. Prepare a n-qubit register, identified as the target register, with $|1\rangle$.
3. Apply QFT to the control register, followed by cU_a^x to the target and control registers, and then QFT^{-1} to the control register.
4. Measure the control register to retrieve an estimate $\frac{x_1}{2^n}$ of a random integer multiple of $\frac{1}{r}$.
5. With the continued fractions method obtain integers c_1, r_1 such that

$$\left|\frac{x_1}{2^n} - \frac{c_1}{r_1}\right| \leq \frac{1}{2^{\frac{n-1}{2}}}$$

   Fail otherwise.

6. Repeat steps 1. to 6. to find another integer x_2, and a second pair (c_2, r_2) st $\left|\frac{x_2}{2^n} - \frac{c_2}{r_2}\right| \leq \frac{1}{2^{\frac{n-1}{2}}}$. Fail otherwise.
7. Compute $r = \text{lcm}(r_1, r_2)$. If $\text{rem}\,(a^r, n) = 1$ output r; fail otherwise.

Afterthoughts

How can the algorithm fail?

- The eigenvalue estimation algorithm produces a bad estimate of $\frac{k}{r}$. This occurs with a bounded probability that can be made smaller by an increase in the size of the circuit.
- The value found is not r itself, but a factor of r, which will be the case if the computed c_1, c_2 have common factors, eventually requiring additional repetitions of the algorithm

Recall

Like all quantum algorithms, this one is probabilistic: it gives the correct answer with high probability, and the probability of failure can be decreased by repeating the algorithm.

Afterthoughts

Cost

$\mathcal{O}((\log n)^3)$, the major cost coming from the modular exponentiation:

- The critical computation is the $cU_a^{2^j}$ operations, for $j \in \{0, 1, 2, \cdots, 2^{n-1}\}$, which constitutes cU_a^x and requires 2^j applications of operator U_a.
- However, $cU_a^{2^j} = cU_{a^{2^j}}$ — multiplying by $\text{rem}(a, n)$ for 2^j times is equivalent to multiplying by $\text{rem}(a^{2^j}, n)$ only once.
- $\text{rem}(a^{2^j}, n)$ can be computed with j multiplications modulo n (exponential improvement over multiplying $\text{rem}(a, n)$ for 2^j times).
- QFT requires $\mathcal{O}(\log n)^2)$ gates.

The classical algorithm is exponential on n: the best known one uses $e^{\mathcal{O}(\sqrt{\log n}\sqrt{(\log\log(n))}}$ classical gates.

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 sampling estimates problem is quantum.

Reduction to order-finding

- To split n, choose randomly, with uniform probability, an integer a and compute its order r such that a and n are coprime (test a from $\{2, 3, \cdots, n-2\}$). If they are not coprime, their greates comon divisor is already a non trivial factor of n.
- If r is even (it will be with at least a probability of 0.5), $a^r - 1$ can be factorized as

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

- As r is the order of a, n divides $a^r - 1$, which means n must share a factor with $(a^{\frac{r}{2}} - 1)$, or $(a^{\frac{r}{2}} + 1)$, or both.

  This factor can be extracted by the Euclides algorithm which efficiently returns $\gcd(a^r - 1, n)$.

Question

But how can be sure such a factor in non trivial?

Reduction to order-finding

- Clearly n does not divide $(a^{\frac{r}{2}} - 1)$.

  Actually, if rem $(a^{\frac{r}{2}} - 1, n) = 0$, $\frac{r}{2}$, rather than r, would be the order of a.

- However, n may divide $(a^{\frac{r}{2}} + 1)$, i.e. $a^{\frac{r}{2}} = 1 (\mathrm{mod}\, n)$ and not share any factor with $(a^{\frac{r}{2}} - 1)$.

Thus, the reduction is probabilistic according to the following

Theorem: Let $n = p_1^{r_1} \times p_2^{r_2} \times \cdots \times p_m^{r_m}$ be the prime factorization of an odd number with $m \geq 2$. Then for a random a, chosen uniformely as before, the probability that its order is even and $a^{\frac{r}{2}} \neq -1 (\mathrm{mod}\, n)$ is at least $(1 - \frac{1}{2^m}) \geq \frac{9}{16}$.

For number theoretic results see N. Koblitz. *A Course in Number Theory and Cryptography*, Springer, 1994.

Shor's algorithm

1. Choose $1 \leq a \leq n-1$ randomly.
2. If $\gcd(a, n) > 1$, then return $\gcd(a, n)$.
3. If $\gcd(a, n) = 1$, then use the order-finding algorithm to compute r — the order of a wrt n.
4. If r is odd or $a^{\frac{r}{2}} = -1 (\bmod n)$
   then return to 1.
   else return $\gcd(a^{\frac{r}{2}} - 1, n)$ and $\gcd(a^{\frac{r}{2}} + 1, n)$.

Shor's algorithm

Shor's approach to estimate a random integer multiple of $\frac{1}{r}$ in his original paper was different from the one discussed in this lecture, as an application of the eigenvalue estimation algorithm.

Shor's approach (based on period finding)

- Create a state

$$\sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}} |x\rangle |\mathrm{rem}\,(a^x, n)\rangle$$

which is shown to be re-written as

$$\sum_{b=0}^{r-1} \left(\frac{1}{\sqrt{2^n}} \sum_{z=0}^{m_b-1} |zr+b\rangle \right) |\mathrm{rem}\,(a^x, n)\rangle$$

where m_b is the largest integer st $(m_b-1)r + b \leq 2^n - 1$.

Shor's algorithm

Shor's approach (based on period finding)

- Measuring the target register yields $\text{rem}\left(a^b, n\right)$ for b chosen uniformly at random from $\{0, 1, 2, \cdots, r-1\}$, and leaves the control register in

$$\frac{1}{\sqrt{m_b}} \sum_{z=0}^{m_b-1} |zr+b\rangle$$

- Apply $QFT_{2^n}^{-1}$ to the control register

  Note that, if r, m_b were known (!), applying $QFT_{m_b r}^{-1}$ would lead to

$$\sum_{j=0}^{r-1} e^{-2\pi i \frac{b}{r} j} |m_b j\rangle$$

  i.e. only values x such that $\frac{x}{r m_b} = \frac{j}{r}$ would be measured.

- Measure x and output $\frac{x}{2^n}$.

Shor's algorithm

Note that in both approaches the circuit is the same.
The only difference is the basis in which the state of the system is analysed:

- the eigenvector basis
- the computational basis in Shor's original algorithm.

Shor's original algorithm is based on the period finding algorithm, which is another application of phase estimation
(see [Nielsen & Chuang, 2010] for a complete account)

In all cases, the underlying quantum component is, of course, the *QFT*.

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

... and we are done!

Where to look further

Two research directions at INL
(dissertation themes coming around May)

- Quantum Software Engineering (INESC TEC & INL): 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 (INL): 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

Continued Fractions

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

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

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

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

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.