Quantum Algorithms

Topics in Complexity-Theory

Jesko Hüttenhain Lars Wallenborn

May 6th, 2011

Contents

Abstract

This handout was created in the context of a talk we gave at the "Graduate Seminar on Topics in Quantum Computation" by Prof. Nitin Saxena at the University of Bonn in the Summer Semester 2011. It is heavily based on the lecture notes [AAR] and the book [NC].

1 The Quantum Fourier Transform

Definition 1.1. *We denote by* $\omega_N := \exp\left(\frac{2\pi\hat{\imath}}{N}\right) \in \mathbb{C}$ *the canonical primitive* N*-th root of unity in the complex plane.*

Fact/Definition 1.2. *Let* $N = 2^n$ *be a power of two. We define the gate* QFT_n *on* n *q-bits to be the unitary* $N \times N$ *- matrix*

$$\mathrm{QFT}_n := \left(\frac{\omega_N^{jk}}{\sqrt{N}}\right)_{0\leq j,k<N} = \frac{1}{\sqrt{N}} \cdot \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N^1 & \omega_N^2 & \cdots & \omega_N^{(N-1)\cdot 1} \\ 1 & \omega_N^2 & \omega_N^4 & \cdots & \omega_N^{(N-1)\cdot 2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)^2} \end{pmatrix}.$$

Proof. To show that QFT_n is unitary, we only need to verify that its columns are orthonormal. To do so, we will show that

$$\sum_{k=0}^{N-1} \omega_N^{kj}\omega_N^{-hk} = \begin{cases} N & ; \quad j = h \\ 0 & ; \quad \text{otherwise} \end{cases} \tag{1.1}$$

It is noteworthy that $\overline{\omega_N^x} = \omega_N^{-x}$, so the above is actually the scalar product in $\mathbb{C}^N$. Now, ω_N^{j-h} is a root of the polynomial $F(X) := X^N - 1$. We know that $F(1) = 0$ and set $G := F/(X-1) = \sum_{k=0}^{N-1} X^k$.

Hence, we are either in the trivial case $j = h \Leftrightarrow \omega_N^{j-h} = 1$ or, otherwise, $G(\omega_N^{j-h}) = 0$ and this is precisely (1.1). □

1.1 Circuit Implementation

Notation 1.3. *We will associate the states* $|x\rangle = |x_1, \ldots x_n\rangle$*, where the* $x_i \in \{0,1\}$ *are the binary digits in the representation* $x = \sum_{j=1}^n x_j 2^{n-j}$*. Furthermore, we use the notation* $[0.x_1 \ldots x_n]$ *to denote the* ***binary fraction*** $\sum_{j=1}^n x_j 2^{-j}$*. For ease of notation, let*

$$\lambda_j(x) := \exp\left(2\pi\hat{\imath} \cdot [0.x_j \cdots x_n]\right).$$

Proposition 1.4. *The map*

$$|x\rangle \longmapsto \frac{1}{\sqrt{N}} \cdot \bigotimes_{j=0}^{n-1}\Big(|0\rangle + \lambda_{n-j}(x)\,|1\rangle\Big)$$

is the quantum fourier transform.

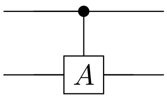
Proof. We calculate

$$\begin{aligned}
\sqrt{N}\cdot|x_1,\dots,x_n\rangle &\mapsto \sum_{k=0}^{N-1}\exp\left(\frac{2\pi\hat{\imath}xk}{N}\right)|k\rangle \\
&= \sum_{k_1\in\{0,1\}}\cdots\sum_{k_n\in\{0,1\}}\exp\left(2\pi\hat{\imath}x\frac{\sum_{j=1}^{n}k_j2^{n-j}}{2^n}\right)|k_1,\dots,k_n\rangle \\
&= \sum_{k_1\in\{0,1\}}\cdots\sum_{k_n\in\{0,1\}}\exp\left(2\pi\hat{\imath}x\textstyle\sum_{j=1}^{n}k_j2^{-j}\right)|k_1,\dots,k_n\rangle \\
&= \sum_{k_1\in\{0,1\}}\cdots\sum_{k_n\in\{0,1\}}\textstyle\bigotimes_{j=1}^{n}\exp\left(2\pi\hat{\imath}xk_j2^{-j}\right)|k_j\rangle \\
&= \bigotimes_{j=1}^{n}\left[\sum_{k_j\in\{0,1\}}\exp\left(2\pi\hat{\imath}xk_j2^{-j}\right)|k_j\rangle\right] \\
&= \bigotimes_{j=1}^{n}\left[|0\rangle+\exp\left(2\pi\hat{\imath}x2^{-j}\right)|1\rangle\right] \\
&= \bigotimes_{j=0}^{n-1}\left[|0\rangle+\exp\left(\pi\hat{\imath}\cdot\frac{x}{2^j}\right)|1\rangle\right] \\
&= \bigotimes_{j=0}^{n-1}\left(|0\rangle+\exp(2\pi\hat{\imath}[0.x_{n-j}\cdots x_n])\,|1\rangle\right) \qquad \square
\end{aligned}$$

Definition 1.5. *We denote the k-**rotation gate** by*

$$R_k=\begin{pmatrix}1 & 0\\ 0 & \exp\left(\frac{2\pi\hat{\imath}}{2^k}\right)\end{pmatrix}.$$

Notation 1.6. *For any unitary matrix $A\in\mathbb{C}^{2\times2}$, we will use the diagram notation*



*to denote the **controlled A-gate**, which corresponds to the unitary matrix*

$$\begin{pmatrix}I & \mathbf{0}\\ \mathbf{0} & A\end{pmatrix},$$

where $I\in\mathbb{C}^{2\times2}$ is the unit matrix.

Theorem 1.7. *The circuit in Figure 1 computes the quantum fourier transform, up to reordering of the quantum bits.*

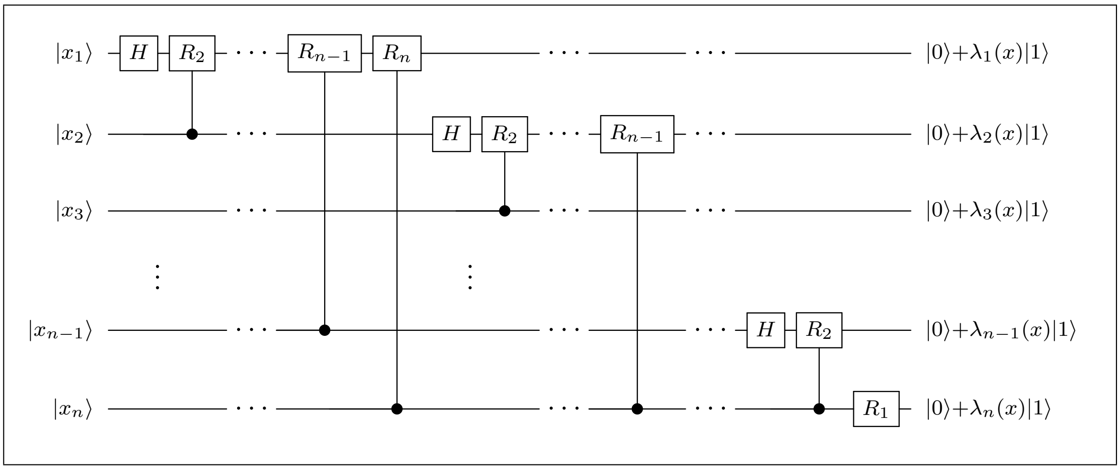

$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|x_{n-1}\rangle$
$|x_n\rangle$
H
R_2
R_{n-1}
R_n
R_1
$|0\rangle + \lambda_1(x)|1\rangle$
$|0\rangle + \lambda_2(x)|1\rangle$
$|0\rangle + \lambda_3(x)|1\rangle$
$|0\rangle + \lambda_{n-1}(x)|1\rangle$
$|0\rangle + \lambda_n(x)|1\rangle$

Figure 1: The Quantum Fourier Circuit Implementation

Proof. Let $|x_1 \dots x_n\rangle$ be the input of the circuit. Applying Hadamard to the first bit yields the state

$$\frac{1}{\sqrt{2}}\Big(|0\rangle + \exp\left(2\pi\hat{\imath} \cdot [0.x_1]\right)|1\rangle\Big)\,|x_2 \dots x_n\rangle$$

since $\exp\left(2\pi\hat{\imath} \cdot [0.x_1]\right) = (-1)^{x_1}$. Applying the controlled R_2-gate turns this into

$$\frac{1}{\sqrt{2}}\Big(|0\rangle + \exp\left(2\pi\hat{\imath} \cdot [0.x_1x_2]\right)|1\rangle\Big)\,|x_2 \dots x_n\rangle$$

and consequently, the controlled gates R_3, R_4, …, R_{n-1} and R_n leave us with

$$\frac{1}{\sqrt{2}}\Big(|0\rangle + \lambda_1(x)\,|1\rangle\Big)\,|x_2 \dots x_n\rangle\,.$$

We perform an equivalent method on the second qubit: After the Hadamard gate, the state is equal to

$$\frac{1}{\sqrt{2}^2}\Big(|0\rangle + \lambda_1(x)\,|1\rangle\Big)\Big(|0\rangle + \exp\left(2\pi\hat{\imath} \cdot [0.x_2]\right)|1\rangle\Big)\,|x_3 \dots x_n\rangle\,.$$

Then the controlled gates R_2 to R_{n-1} yield the state

$$\frac{1}{\sqrt{2}^2}\Big(|0\rangle + \lambda_1(x)\,|1\rangle\Big)\Big(|0\rangle + \lambda_2(x)\,|1\rangle\Big)\,|x_3 \dots x_n\rangle\,.$$

This procedure for every qubit produces the final state

$$\frac{1}{\sqrt{2}^n}\Big(|0\rangle + \lambda_1(x)\,|1\rangle\Big)\Big(|0\rangle + \lambda_2(x)\,|1\rangle\Big)\cdots\Big(|0\rangle + \lambda_n(x)\,|1\rangle\Big).$$

By 1.4, this is the quantum fourier transform with all qubits in reverse order. □

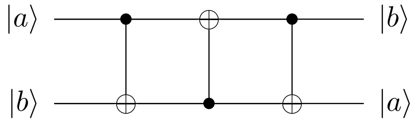
Corollary 1.8. *The quantum fourier transform can be implemented by using only polynomially many circuits.*

Proof. In Figure 1 we apply exactly one Hadamard and $n-i-1$ conditional rotation gates to the i-th qubit. So the total number of gates is

$$\sum_{i=1}^{n}\Big(1+(n-i-1)\Big)=\frac{n(n+1)}{2}.$$

□

Fact 1.9. *To swap two qubits, one may apply the quantum circuit*



Proof. We compute the composition of the three CNOT gates:

$$\begin{aligned} |ab\rangle &\longmapsto |a\rangle\otimes|a\oplus b\rangle \\ &\longmapsto |a\oplus(a\oplus b)\rangle\otimes|a\oplus b\rangle=|b\rangle\otimes|a\oplus b\rangle \\ &\longmapsto |b\rangle\otimes|(a\oplus b)\oplus b\rangle=|ba\rangle\,. \end{aligned}$$

□

1.2 Quantum Integer Factoring

We now plan to solve the following well-known problem efficiently on a quantum computer. Note that there is no classical algorithm known that factors large integers in polynomial time.

Integer Factoring Problem	
Instance:	An integer number $N\in\mathbb{Z}$.
Task:	Find a nontrivial factor of N.

Definition 1.10. *For any positive integer number $N\in\mathbb{Z}_+$, we define the* ***residue class ring*** $\mathbb{Z}_N:=\mathbb{Z}/(N)$*. Its multiplicative subgroup $\mathbb{Z}_N^\times$ can be written as*

$$\mathbb{Z}_N^\times=\{\,k\le N\mid\gcd(k,N)=1\,\}\,.$$

The ***Euler phi function*** *is defined as $\phi(N):=\#\mathbb{Z}_N^\times$. We write $\operatorname{ord}(x)$ for the* ***order of*** *$x\in\mathbb{Z}_N^\times$, i.e. the smallest positive integer number such that $x^{\operatorname{ord}(x)}=1$. For $k\in\mathbb{Z}$, we define*

$$\operatorname{ord}_N(k):=\begin{cases}\operatorname{ord}(k\bmod N) & ;\ \gcd(k,N)=1\\ 0 & ;\ \text{otherwise}\end{cases}$$

Note that when N is a prime, $\mathbb{Z}_N=:\mathbb{F}_N$ is a field and $\mathbb{F}_N^\times=\mathbb{F}_N\setminus\{0\}$.

Fact 1.11. *For any odd prime p,*

$$\Pr_{x \in_R \mathbb{F}_p^\times} (\mathrm{ord}_p(x) \in 2\mathbb{Z}) \geq \frac{1}{2}.$$

Proof. It is well-known that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$. Hence, $x^{p-1} = 1$ for all $x \in \mathbb{F}_p^\times$. Let now g be a generator. This means that for every $x \in \mathbb{F}_p^\times$, there exists some $k \in \mathbb{N}$ such that $x = g^k$. For $x \in_R \mathbb{F}_p^\times$, the probability of k being odd is precisely one half. We therefore assume that k is odd and prove that x has even order. Write

$$1 = x^{\mathrm{ord}(x)} = g^{k \cdot \mathrm{ord}(x)}$$

so we know that $p - 1 \,|\, k \cdot \mathrm{ord}(x)$. Since k is odd and $p-1$ is even, we are done. □

Fact 1.12. *Let $N = pq$ for two odd primes p and q. Then,*

$$\Pr_{x \in_R \mathbb{Z}_N^\times} \left(\mathrm{ord}(x) \in 2\mathbb{Z} \text{ and } x^{\frac{\mathrm{ord}(x)}{2}} \neq \pm 1\right) \geq \frac{3}{8}.$$

Proof. We will make use of the isomorphism $\mathbb{Z}_N^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$, which is essentially the Chinese remainder theorem. Choosing an element $x = (a, b)$ at random means independently choosing an element $a \in_R \mathbb{Z}_p^\times$ and an element $b \in_R \mathbb{Z}_q^\times$. Obviously

$$\mathrm{ord}(x) = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b)),$$

so by 1.11, the probability for x to be of even order is greater or equal than $\frac{3}{4}$.

Let us therefore assume that $x = y^2$ is of even order. We have to show that the probability of $y \neq \pm 1$ is at least $\frac{1}{2}$. Now, the equation $y^2 = 1$ has precisely two solutions (namely, 1 and -1) in both $\mathbb{F}_p$ and $\mathbb{F}_q$. Hence, it has the four solutions

$$(1,1) \qquad (-1,-1) \qquad (-1,1) \qquad (1,-1)$$

in $\mathbb{Z}_N \cong \mathbb{F}_p \times \mathbb{F}_q$, the latter two of which are not 1 or -1. □

Corollary 1.13. *Let $N = pq$ for two odd prime numbers p and q. With probability at least $\frac{3}{8}$, an element $x \in_R \mathbb{Z}_N^\times$ has even order $\mathrm{ord}(x) = 2r$ and both $\gcd(N, x^r + 1)$ and $\gcd(N, x^r - 1)$ are nontrivial factors of N.*

Proof. Choosing an element $x \in_R \mathbb{Z}_N^\times$ such that $\mathrm{ord}(x) = 2r$ and $x^r \neq \pm 1$ gives us the equality

$$0 = x^{2r} - 1 = (x^r - 1) \cdot (x^r + 1)$$

and since neither $(x^r - 1)$ nor $(x^r + 1)$ are equal to zero in $\mathbb{Z}_N$, this means that they represent nontrivial factors of N. □

Hence, we have reduced the Integer Factoring Problem to the

Period Finding Problem

Instance: A periodic function $f : \mathbb{Z} \to \Omega$.

Task: Find the period of f. This is the smallest $s \in \mathbb{Z}_+$ such that $f(x+s) = f(x)$ for all $x \in \mathbb{Z}$.

A quantum algorithm to solve this problem probabilistically is given below:

Algorithm 1 Period-Finding-Quantum-Subroutine

```
Input: 2 registers of $n$-qubits in state $|0\rangle\,|0\rangle$ and a black-box $B_f$ that computes a function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ with period $s$.
Output: A quantum state $|k\rangle\,|f(r)\rangle$
let $N := 2^n$ and $L := \lfloor \frac{N}{s} \rfloor$ where $s = \mathrm{ord}_M(x)$.
Apply Hadamard to register 1:
    $\frac{1}{\sqrt{N}} \cdot \sum_{j=0}^{N-1} |j\rangle\,|0\rangle$
Apply $B_f$:
    $\frac{1}{\sqrt{N}} \cdot \sum_{j=0}^{N-1} |j\rangle\,|f(j)\rangle$
Measure register 2. For the minimal $r$:
    $\frac{1}{\sqrt{L}} \cdot \sum_{j=0}^{L-1} |r+js\rangle\,|f(r)\rangle$
Apply $\mathrm{QFT}_n$ to register 1:
    $\frac{1}{\sqrt{NL}} \cdot \sum_{j=0}^{L-1} \sum_{k=0}^{N-1} \omega_N^{(r+js)k}\,|k\rangle\,|f(r)\rangle$
return $|k\rangle\,|f(r)\rangle$ by measuring register 1.
```

We make use of the following statement, which involves several tedious calculations:

Fact 1.14. *Let $M \in \mathbb{Z}$ be any number and n minimal such that $2^n \geq M^2$. Choose any $x \in \mathbb{Z}_M^\times$ and let $|k\rangle\,|x^r \bmod M\rangle$ be the quantum state returned by a call to the* Period-Finding-Quantum-Subroutine *with black-box $f(r) := x^r \bmod M$. Then, with high probability, $\omega_N^{ks} \approx 1$ where $s = \mathrm{ord}(x)$ is the period of f.*

Handwaving. Note that the quantum state $|k\rangle\,|f(r)\rangle$ occurs with probability

$$\left|\sum_{j=0}^{L-1} \omega_N^{(r+js)k}\right|^2 = \left|\omega_N^{rk}\right|^2 \cdot \left|\sum_{j=0}^{L-1} \omega_N^{jsk}\right|^2$$

We claim that $\left|\sum_j \omega_N^{jsk}\right|^2$ is very large when $\omega_N^{sk} \approx 1$ and very small otherwise. This is morally correct because if ω_N^{sk} forms a large angle with the real axis, summing up over its periodic rotations will cancel out the amplitudes. If the angle is very small, on the other hand, they add up. □

Corollary 1.15. *There exists a polynomial time quantum algorithm to solve the* Period Finding Problem*.*

Proof. Since $\omega_N^{ks} \approx 1 = \omega_N^N$, we can estimate a multiple of the period s by N/k. Sampling a couple of more times and taking the greates common divisor of the multiples obtained will reveal the value of s. □

1.3 The Hidden Subgroup Problem

Definition 1.16. *Let G be a group and $f : G \to \Omega$ any map of sets. We say that f* ***conceals*** *H if $H \subset G$ is a subgroup of G and $f(x) = f(y)$ if and only if there exists a $h \in H$ with $x = hy$. In other words, f is constant on any left-coset of H.*

Hidden Subgroup Problem (HSP$_G$)

Parameters: A group G.
Instance: A map $f : G \to \Omega$ concealing $H \subset G$.
Task: Find a set of generators of H.

Example 1.17. *Note that the* Period Finding Problem *is a special case of the* Hidden Subgroup Problem *over $G = \mathbb{Z}$. Take $H = (s)$, the subgroup generated by the period of some function $f : \mathbb{Z} \to \Omega$. Then, f conceals precisely H and finding a set of generators of H is equivalent to finding s. Consequently,* Integer Factoring *reduces to* Hidden Subgroup*.*

In fact, the following result is known:

Theorem 1.18 (Shor,Kitaev). *For a finite abelian group G,* HSP$_G \in$ BQP*.* □

Remark 1.19. *For noncommutative groups G, it is still an open problem whether* HSP$_G$ *is in* BQP *or not.*

We end with the reduction of another well-known computational problem to HSP:

GRAPH ISOMORPHISM PROBLEM (GI)

Instance: Two undirected graphs G_1 and G_2.
Task: Decide whether $G_1 \cong G_2$.

Definition 1.20. *Recall that the automorphisms of a graph $G = (V, E)$ are given by all permutations of its vertices that induce a permutation of its edges, i.e.*

$$\mathrm{Aut}(G) = \{\, \pi : V \to V \mid \forall \{v, w\} \in E : \{\pi(v), \pi(w)\} \in E \,\}\,.$$

Furthermore, we denote by $\mathcal{G}_n := \{\, G \mid \#V(G) = n \,\}$ the set of all graphs on n vertices.

Theorem 1.21. $\mathrm{GI} \leq_T \mathrm{HSP}_{S_n}$.

Proof. We may assume without loss of generality that the instance (G_1, G_2) of GI is such that the G_i are both connected graphs. We set $G := G_1 \mathbin{\dot\cup} G_2$ and consider $\mathrm{Aut}(G)$ as a subgroup of S_n, where $n = \#V(G)$. For any $\pi \in S_n$ and $H \in \mathcal{G}_n$, we define

$$\pi(H) := (V, \{\, \{\pi(v), \pi(w)\} \mid \{v, w\} \in E(H) \,\}).$$

Note that $\pi(H) = H$ if and only if $\pi \in \mathrm{Aut}(H)$, but always $\pi(H) \cong H$. This is one of the rare cases where this subtle distinction needs to be sought through with great care.

Now, we define $f : S_n \to \mathcal{G}_n$ by $f(\pi) := \pi(G)$ and claim that f conceals $\mathrm{Aut}(G)$. Once we have shown this, we are done since $G_1 \ncong G_2$ if and only if each generator of $\mathrm{Aut}(G)$ operates independently on each of the G_i.

Hence, let $\pi, \sigma \in S_n$ and $\rho \in \mathrm{Aut}(G) \subseteq S_n$. Then, $\pi = \sigma\rho$ if and only if

$$f(\pi) = \pi(G) \overset{!}{=} \sigma(\rho(G)) = \sigma(G) = f(\sigma). \qquad \square$$

References

[AAR] Scott Aaronson, Lecture notes "Quantum Compexity Theory", Electronic Version[1] from 05/06/2011.

[NC] Michael A. Nielsen, Isaac L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, 2000

[1] http://stellar.mit.edu/S/course/6/fa08/6.896/materials.html