Quantum Fourier transform beyond Shor's algorithm: Exercise Sheet 1

July 17, 2023

András Gilyén (Alfréd Rényi Institute of Mathematics)

The first 5 exercises are from Ronald de Wolf's lecture notes [dW19, Chapter 4 Exercises 1, 2, 3, 4, 6]. Feel free to skip exercises that you find too easy or hard. On the last page you can find some hints where indicated by (**H**).

Exercises

1.) For $\omega = e^{-2\pi i/3}$ and $F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$, calculate $F_3 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $F_3 \begin{pmatrix} 1 \\ \omega^2 \\ \omega \end{pmatrix}$.

2.) (**H**) The *total variation distance* between two probability distributions P and Q on the same set, is defined as $d_{TVD}(P,Q) = \frac{1}{2}\sum_i |P(i) - Q(i)|$. An equivalent alternative way to define this: $d_{TVD}(P,Q)$ is the maximum, over all events E, of $|P(E) - Q(E)|$. Hence $d_{TVD}(P,Q)$ is small iff all events have roughly the same probability under P and under Q.

The *Euclidean distance* between two states $|\phi\rangle = \sum_i \alpha_i |i\rangle$ and $|\psi\rangle = \sum_i \beta_i |i\rangle$ is defined as $\||\phi\rangle - |\psi\rangle\| = \sqrt{\sum_i |\alpha_i - \beta_i|^2}$. Assume the two states are unit vectors. Suppose the Euclidean distance is small: $\||\phi\rangle - |\psi\rangle\| = \epsilon$. If we measure $|\phi\rangle$ in the computational basis then the probability distribution over the outcomes is given by the $|\alpha_i|^2$, and if we measure $|\psi\rangle$ then the probabilities are $|\beta_i|^2$. Show that these distributions are close: the total variation distance $\frac{1}{2}\sum_i \big||\alpha_i|^2 - |\beta_i|^2\big|$ is $\leq \epsilon$.

3.) (**H**) The *operator norm* of a matrix A is defined as $\|A\| = \max_{v:\|v\|=1} \|Av\|$.

An equivalent definition is that $\|A\|$ is the largest singular value of A.

The *distance* between two matrices A and B is defined as $\|A - B\|$.

a.) What is the distance between the 2×2 identity matrix and the phase-gate $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$?

b.) What is the distance between the 4×4 identity matrix and the *controlled* version of the phase gate of (a)?

c.) What is the distance between the $2^n \times 2^n$ identity matrix I_{2^n} and the controlled phase gate of (b) tensored with $I_{2^{n-2}}$?

d.) Suppose we have a product of n-qubit unitaries $U = U_T U_{T-1} \cdots U_1$ (for instance, each U_i could be an elementary gate on a few qubits, tensored with identity on the other qubits). Suppose we drop the j-th gate from this sequence: $U' = U_T U_{T-1} \cdots U_{j+1} U_{j-1} \cdots U_1$. Show that $\|U' - U\| = \|I - U_j\|$.

e.) Now we also drop the k-th unitary: $U'' = U_T U_{T-1} \cdots U_{j+1} U_{j-1} \cdots\cdots U_{k+1} U_{k-1} \cdots U_1$. Show that $\|U'' - U\| \leq \|I - U_j\| + \|I - U_k\|$.

f.) Give a quantum circuit with $O(n \log n)$ elementary gates that has distance less than $1/n$ from the Fourier transform F_{2^n}.

Comment: The above exercise shows the important fact that if we have a quantum circuit C that has various subparts ("subroutines"), then a circuit $\tilde{C}$ where those subroutines are implemented with small operator-norm error, rather than perfectly, still works well: if $\left\|C - \tilde{C}\right\|$ is small then (by definition of operator norm) for all initial states $|\phi\rangle$ the states $C|\phi\rangle$ and $\tilde{C}|\phi\rangle$ are close in Euclidean distance. By Exercise 2 then also the final output distributions are close (in total variation distance).

4.) Prove that the Fourier coefficients of the convolution of vectors a and b are the product of the Fourier coefficients of a and b. In other words, prove that for every $a, b \in \mathbb{R}^N$ and every $\ell \in \{0, \ldots, N-1\}$ we have $\left(\widehat{a * b}\right)_\ell = \widehat{a}_\ell \cdot \widehat{b}_\ell$. Here the Fourier transform $\widehat{a}$ is defined as the vector $F_N a$, and the ℓ-entry of the convolution-vector $a * b$ is $(a*b)_\ell = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j b_{(\ell-j) \bmod N}$.

5.) **a**.) The squared Fourier transform, F_N^2, turns out to map computational basis states to computational basis states. Describe this map, i.e., determine to which basis state a basis state $|k\rangle$ gets mapped for each $k \in \{0,1\}^n$.

b.) Show that $F_N^4 = I$. What can you conclude about the eigenvalues of F_N?

6.) Show that the quantum circuit for F_N implies the famous fast Fourier transform result:* when $N = 2^n$, one can compute the Fourier transform of a vector in time $\mathcal{O}(N \log(N))$ (which is much better than naïve matrix-vector multiplication that would result in running time $\mathcal{O}(N^2)$.)

7.) (**H**) Show that the following are special cases of the hidden subgroup problem:

a.) Simon's problem: given $f\colon \{0,1\}^n \to \{0,1\}^n$ such that $f(x) = f(y)$ iff $x = y$ of $x = y \oplus s$ for some fixed $s \in \{0,1\}^n$, find s with a few queries to f.

b.) Period finding: given $f\colon \mathbb{Z} \to \{0,1\}^n$ such that $f(a) = f(b)$ iff $a \equiv b \mod r$, for some fixed $r \in \mathbb{N}$, find r with a few queries to f.

c.) (**H**) Discrete logarithm: given a generator γ of a cyclic multiplicative group C of size N (i.e., $C = \{\gamma^a \mid a \in \{0, 1, \ldots, N-1\}\}$), and $A \in C$, find the unique $a \in \{0, 1, \ldots, N-1\}$ such that $\gamma^a = A$.

d.) Generalized discrete logarithm: given generators $\gamma_1, \gamma_2, \ldots, \gamma_t$ of the Abelian group $G = \langle\gamma_1\rangle \oplus \langle\gamma_2\rangle \oplus \cdots \oplus \langle\gamma_t\rangle$, where we use additive notation and $\oplus$ denotes the (internal) direct sum, and $A \in G$, find the unique $a_i \in \{0, 1, \ldots, |\langle\gamma_i\rangle| - 1\}$ such that $\sum_{i=1}^t a_i \gamma_i = A$.

Optional difficult exercises, assuming familiarity with phase estimation, amplitude amplification and Shor's algorithm:

8.) (**H**) Give an efficient exact algorithm for quantum Fourier transform overt $\mathbb{Z}_N$ for arbitrary $N \in \mathbb{N}$.†

9.) (**H**) Suppose we have a generating set of a finite Abelian group, and we can perform group operations (inversion and addition), and every element of G has a unique encoding (binary representation).

a.) Give an efficient quantum algorithm‡ that decomposes the group as

$$G = \langle\gamma_1\rangle \oplus \langle\gamma_2\rangle \oplus \cdots \oplus \langle\gamma_t\rangle$$

in terms of generators $\gamma_1, \gamma_2, \ldots, \gamma_t$ and determines the order of each element γ_i. This means that the $G \simeq \mathbb{Z}_{|\langle\gamma_1\rangle|} \times \mathbb{Z}_{|\langle\gamma_2\rangle|} \times \cdots \times \mathbb{Z}_{|\langle\gamma_t\rangle|}$.

b.) Show that if you could efficiently solve the above problem using a classical algorithm, then you could break the RSA encryption.

c.) Give an efficient quantum algorithm for quantum Fourier transform over the group G.

*FFT works for more general N, but here we only study the case $N = 2^n$ for simplicity.

†This problem was first solved by Mosca and Zalka.

‡This problem was first solved by Cheung and Mosca.

Hints

Exercise 2: Use $\big||\alpha_i|^2 - |\beta_i|^2\big| = \big||\alpha_i| - |\beta_i|\big| \cdot \big||\alpha_i| + |\beta_i|\big|$ and the Cauchy-Schwarz inequality.

Exercise 3.e: Use triangle inequality.

Exercise 3.f: Drop all phase-gates with small angles $\phi < 1/n^3$ from the $\mathcal{O}\big(n^2\big)$-gate circuit for F_{2^n}. Calculate how many gates are left in the circuit, and analyze the distance between the unitaries corresponding to the new circuit and the original circuit.

Exercise 7: You can find the solution to parts **a.)-c.)** in [dW19, Chapter 6].

Exercise 7.c: Use $G = \mathbb{Z}_N \times \mathbb{Z}_N$ and define $f(x, y) := \gamma^x A^{-y}$.

Exercise 8: First prepare the state $|j\rangle \to |j\rangle \otimes QFT_N|j\rangle$, then uncompute the first state using phase estimation approximately. Use amplitude amplification to make the operation exact. If still stuck follow the strategy outlined in the paper of Mosca and Zalka `https://arxiv.org/abs/quant-ph/0301093`.

Exercise 9: First find a generating set each having prime order using period finding and Shor's algorithm. The subgroups of elements generated by different primes are distinct (apart from the unit element), so it suffices to decompose these further – this last part is challenging and provides a proof of the "Basis Theorem" of finite Abelian groups – if still stuck follow the strategy outlined in Andrew Child's lecture notes (Chapter 6 of `https://www.cs.umd.edu/~amchilds/qa/`).

References

[dW19] Ronald de Wolf. Quantum computing: Lecture notes (version 5), 2019. arXiv: `1907.09415v5`