

Nielsen and Chuang Solutions

Jacob Watkins

May 2021

Chapter 1

Plan and Progress

1.1 Goals of this project

There exist other partial solution manuals to N&C, most of them on github. It appears, taken together, they have covered chapters 2,3,4 and 9 almost completely, with scattered solutions for other chapters. Here, we wish to help fill in the gaps, and perhaps ultimately create the most comprehensive solution manual to date. The strategy here is as follows:

- Create solution manuals for appendices
- Create solution manuals for chapters 5-8
- Create solutions for chapters 10-12
- (If motivated) Fill in remaining problems in chapters already covered by others (in chapters 2-4 for example.)
- (If REALLY motivated) Compile together solutions already created, and bring them into a common format, so that we may come closer to a universal solutions manual!

I would enjoy collaboration from the community, if anyone wants to help contribute to this project.

To-do

- Fix QFT circuit, recreate it in Qiskit and set barrier option to True
- Double check circuit shown in problem 5.4

1.2 Progress so far

This progress was last updated February 1st, 2021.

- Chapter 2: Exercises 2.1-2.4 complete. Many exercises remain

- Chapter 5: Exercises 5.1-5.14 complete. Exercises 5.15-5.29 remain, along with 6 practice problems
- Chapter 6: Only first few problems completed
- Appendix 1: All exercises complete!
- Appendix 4: All exercises complete except A4.17 and part 2 of problem 1
- Appendix 5: Almost done. Problem 1 needs to be cleaned up.
- Appendix 6: All exercises complete!

Chapter 2

Introduction to quantum mechanics

Exercise 2.1: (Linear dependence: example)

Show that $(1, -1)$, $(1, 2)$ and $(2, 1)$ are linearly dependent.

Solution: By inspection, one might be able to see that $(2, 1) = (1, -1) + (1, 2)$, hence,

$$(1, -1) + (1, 2) - (2, 1) = 0. \quad (2.1)$$

This demonstrates linear dependence. A more systematic approach would be to cast this problem as a system of linear equations. A desired set of coefficients can be found by solving

$$\begin{pmatrix} 1 & 1 & 2 \\ -2 & 2 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = 0 \quad (2.2)$$

using standard techniques of linear algebra (such as row reduction).

Exercise 2.2: (Matrix representations: example)

Suppose V is a vector space with basis vectors $|0\rangle$ and $|1\rangle$, and A is a linear operator from V to V such that $A|0\rangle = |1\rangle$ and $A|1\rangle = |0\rangle$. Give a matrix representation for A , with respect to the input basis $|0\rangle, |1\rangle$, and the output basis $|0\rangle, |1\rangle$. Find input and output bases which give rise to a different matrix representation of A .

Solution: Making the identification

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (2.3)$$

it is easy to see that the matrix representation M of A must be

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (2.4)$$

On the other hand, say we choose the output basis to be $|1\rangle, |0\rangle$ instead of $|0\rangle, |1\rangle$ (note that order matters). In this case, M would take the form of the identity matrix.

Exercise 2.3: (Matrix representation for operator products)

Suppose A is a linear operator from vector space V to vector space W , and B is a linear operator from vector space W to vector space X . Let $|v_i\rangle$, $|w_j\rangle$, and $|x_k\rangle$ be bases for the vector spaces V , W , and X respectively. Show that the matrix representation for the linear transformation BA is the matrix product of the matrix representations for B and A , with respect to the appropriate bases.

Solution: Let us compute the action of BA on a basis vector $|v_i\rangle$.

$$\begin{aligned}
 BA|v_i\rangle &= B(A|v_i\rangle) \\
 &= B\left(\sum_j A_{ji}|w_j\rangle\right) \\
 &= \sum_j A_{ji}B|w_j\rangle \\
 &= \sum_j \sum_k A_{ji}B_{kj}|x_k\rangle \\
 &= \sum_k \left(\sum_j B_{kj}A_{ji}\right)|x_k\rangle \\
 &= \sum_k (BA)_{ki}|x_k\rangle.
 \end{aligned} \tag{2.5}$$

In the last step, we identified the coefficient as the product of the two matrix representations of A and B . This gives the result.

Exercise 2.4: (Matrix representation for the identity)

Show that the identity operator on a vector space V has a matrix representation which is one along the diagonal and zero everywhere else, if the matrix representation is taken with respect to the same input and output bases. This matrix is known as the *identity matrix*.

Solution: Let $\mathbb{1}$ be the matrix representation of the identity operator I with respect to some basis $\{|v_i\rangle\}$. Then,

$$I|v_i\rangle = |v_i\rangle = \sum_j \delta_{ji}|v_j\rangle, \tag{2.6}$$

where δ_{ji} is the Kronecker delta. The coefficients δ_{ji} are exactly those of the identity matrix $\mathbb{1}$, hence the identity matrix is the matrix representation of I .

Exercise 2.5

Verify that (\cdot, \cdot) just defined is an inner product on \mathbb{C}^n .

Solution:

Chapter 3

Introduction to computer science

Exercise 3.1

Chapter 4

Quantum circuits

Exercise 4.1

Chapter 5

The Quantum Fourier Transform and its applications

Exercise 5.1

Give a direct proof that the linear transformation defined by Equation (5.2) is unitary.

Solution: It suffices to show that, for any two computational basis states $|j\rangle, |k\rangle$,

$$\langle j | (QFT)^\dagger (QFT) | k \rangle = \langle j | k \rangle = \delta_{ij}. \quad (5.1)$$

To do this, we substitute the definition into the above equation.

$$\begin{aligned} \langle k | (QFT)^\dagger (QFT) | j \rangle &= \left(\frac{1}{\sqrt{N}} \sum_{p=0}^{N-1} e^{-2\pi i k p / N} \langle p | \right) \left(\frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} e^{2\pi i j q / N} | q \rangle \right) \\ &= \frac{1}{N} \sum_{p=0}^{N-1} \sum_{q=0}^{N-1} e^{2\pi i (j q - k p) / N} \langle p | q \rangle \\ &= \frac{1}{N} \sum_{p=0}^{N-1} e^{2\pi i (j - k) p / N} \end{aligned} \quad (5.2)$$

where in the last step we used the orthonormality of the p, q states to eliminate one of the sums. Clearly, if $j = k$, the result is exactly one, as desired. Otherwise, $j - k$ is a nonzero integer, say n , such that $|n| < N$. We will show that in this case the sum above is zero.

The basic idea is that we are taking a sum over phases which are symmetrically distributed around the unit circle, so the result must be zero. To make this argument rigorous, multiply the sum by $e^{2\pi i n / N}$.

$$e^{2\pi i n / N} \sum_{p=0}^{N-1} (e^{2\pi i n / N})^p = \sum_{p=0}^{N-1} (e^{2\pi i n / N})^{p+1} = \sum_{p=1}^N (e^{2\pi i n / N})^p \quad (5.3)$$

In the last equation we simply reindexed. Because of the N -periodicity, $(e^{2\pi i n / N})^N = 1 = (e^{2\pi i n / N})^0$. Hence, we see that the sum is left unchanged by the multiplication. Since $e^{2\pi i n / N} \neq 1$, the sum must in fact be zero. This completes the proof.

Exercise 5.2

Explicitly compute the Fourier transform of the n qubit state $|00\dots 0\rangle$.

Solution: Suppose there are n qubits, so that $N = 2^n$. Using the definition given directly above in the textbook,

$$|00\dots 0\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{i0} |k\rangle \quad (5.4)$$

$$= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle, \quad (5.5)$$

which is simply a uniform superposition over the computational basis states. Evidently, the QFT on the zero state simply acts the same as Hadamards on all the qubits!

We remark that this result is consistent with the interpretation that the Fourier transform decomposes a “signal” into its frequency components. Here, the signal was a sharp spike, which requires a large spread in frequency to construct. Conversely, a uniform superposition without phases is like a constant function signal, which has a frequency of zero.

Exercise 5.3 (Classical fast Fourier transform)

Suppose we wish to perform a Fourier transform of a vector containing 2^n complex numbers on a classical computer. Verify that the straightforward method for performing the Fourier transform, based upon direct evaluation of Equation (5.1) requires $\Theta(2^{2n})$ elementary arithmetic operations. Find a method for reducing this to $\Theta(n2^n)$ operations, based upon Equation (5.4). There are 2^n complex numbers we need to compute, which are the output amplitudes of the Fourier transform. If we compute each one using (5.1), each such amplitude involves a sum which contains 2^n terms. Thus, there will be $2^n \times 2^n = 2^{2n}$ summations and therefore at least as many arithmetic operations.

Solution: Let’s now consider a computation based on the factored form of the QFT, Equation (5.4). As before, this involves a computation of 2^n amplitudes, one for each bitstring $k = k_1 k_2 \dots k_n$. Using (5.4) the amplitude a_k corresponding to the state $|k\rangle$ is given by

$$\langle k | QFT | j \rangle = \frac{1}{2^{n/2}} (\delta_{k_1 0} + e^{2\pi i 0 \cdot j_n} \delta_{k_1 2}) (\delta_{k_2 0} + e^{2\pi i 0 \cdot j_{n-1} j_n} \delta_{k_2 2}) \dots (\delta_{k_n 0} + e^{2\pi i 0 \cdot j_1 \dots j_n} \delta_{k_n 2}). \quad (5.6)$$

where $|j\rangle$ is our input state. This involves a multiplication of n terms, hence there are $n \times 2^n$ total multiplications. This is a lower bound for the number of operations.

Exercise 5.4

Give a decomposition of the controlled- R_k gate into single qubit and CNOT gates.

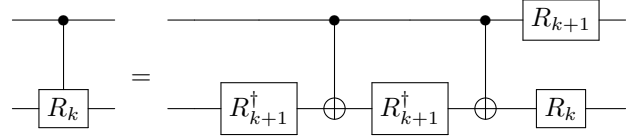
Solution: We use the *ABC* construction of Corollary 4.2 to make our controlled R_k according to Figure 4.6. First, note that

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix} = e^{2\pi i/2^{k+1}} \begin{pmatrix} e^{-2\pi i/2^{k+1}} & 0 \\ 0 & e^{2\pi i/2^{k+1}} \end{pmatrix} = e^{i\alpha} R_z(\beta) \quad (5.7)$$

where $\alpha = 2\pi/2^{k+1}$ and $\beta = 2\pi/2^k$. Comparing this to the Euler decomposition formula of Theorem 4.1, we set $\gamma = \delta = 0$. Following through the steps, this implies,

$$\begin{aligned} A &= R_z(\beta) \\ B &= R_z(-\beta/2) \\ C &= R_z(-\beta/2) \end{aligned} \tag{5.8}$$

can be used in the ABC construction of R_k . As a final step, primarily one of cosmetics, we notice these gates are related to the R_k through global phases which cancel each other out. Thus, the following circuit implements the controlled- R_k , as is easy to verify.

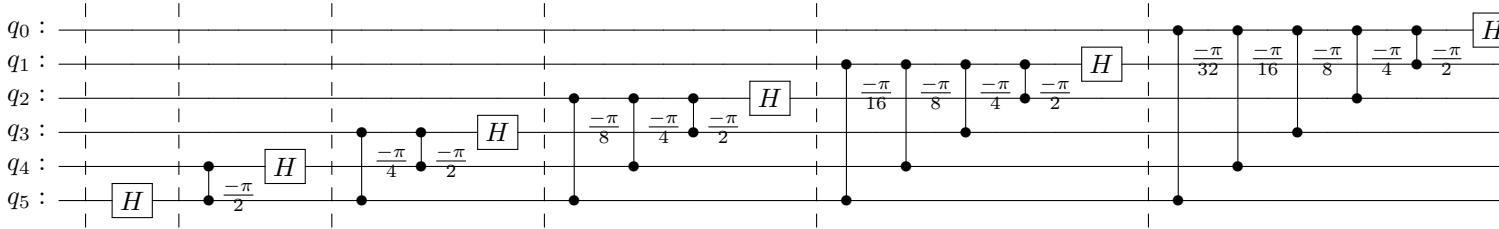


$$\tag{5.9}$$

Exercise 5.5

Give a quantum circuit to perform the inverse quantum Fourier transform.

Solution: Here is the circuit for six qubits (generated using qiskit).



Here, the vertical line segments are the R_k gates, where the number alongside indicate angle of phase rotated. Like the inverse to any quantum circuit, can be obtained by reversing the order of the gates and taking the inverse of each gate. Note the Hadamard H is self-inverse.

Exercise 5.6 (Approximate quantum Fourier transform)

The quantum circuit construction of the quantum Fourier transform apparently requires gates of exponential precision in the number of qubits used. However, such precision is never required in any quantum circuit of polynomial size. For example, let U be the ideal quantum Fourier transform on n qubits, and V be the transform which results if the controlled- R_k gates are performed to a precision $\Delta = 1/p(n)$ for some polynomial $p(n)$. Show that the error $E(U, V) \equiv \max_{|\psi\rangle} \|(U - V)|\psi\rangle\|$ scales as $\Theta(n^2/p(n))$, and thus polynomial precision in each gate is sufficient to guarantee polynomial accuracy in the output state.

Solution: First we will show a more general result (one which will be further generalized in part 3 of the book, when discussing quantum channels). Let \mathcal{X} and \mathcal{Y} be quantum gates, and let X and Y be gates which we will think of as approximating \mathcal{X} and \mathcal{Y} respectively. We will show that

$$E(\mathcal{X}\mathcal{Y}, XY) \leq E(\mathcal{X}, X) + E(\mathcal{Y}, Y). \tag{5.10}$$

To proceed, we set things up to make use of our friend: the triangle inequality. For any state $|\psi\rangle$ we have

$$\|(\mathcal{X}\mathcal{Y} - XY)|\psi\rangle\| = \|(\mathcal{X}\mathcal{Y} - X\mathcal{Y} + X\mathcal{Y} - XY)|\psi\rangle\| \quad (5.11)$$

$$= \|(\mathcal{X} - X)\mathcal{Y}|\psi\rangle + X(\mathcal{Y} - Y)|\psi\rangle\| \quad (5.12)$$

$$\leq \|(\mathcal{X} - X)\mathcal{Y}|\psi\rangle\| + \|X(\mathcal{Y} - Y)|\psi\rangle\| \quad (5.13)$$

Since this inequality holds for any $|\psi\rangle$, it certainly holds if we take the max of both sides. Hence,

$$E(\mathcal{X}\mathcal{Y}, XY) \leq \max_{|\psi\rangle} (\|(\mathcal{X} - X)\mathcal{Y}|\psi\rangle\| + \|X(\mathcal{Y} - Y)|\psi\rangle\|) \quad (5.14)$$

Certainly, the maximum of a sum $A + B$ is less than (or equal to) maximizing each individual piece A, B , so we may distribute the max function and maintain the inequality. Let's consider each term on the left hand side. Since \mathcal{Y} is unitary, it is a bijection on the space of valid states. Hence, we can maximize over $|\phi\rangle = \mathcal{Y}|\psi\rangle$ instead. Now consider the rightmost term. Since X is unitary, it preserves norm. Altogether,

$$E(\mathcal{X}\mathcal{Y}, XY) \leq \max_{|\phi\rangle} \|(\mathcal{X} - X)|\phi\rangle\| + \max_{|\psi\rangle} \|(\mathcal{Y} - Y)|\psi\rangle\| \quad (5.15)$$

$$= E(\mathcal{X}, X) + E(\mathcal{Y}, Y). \quad (5.16)$$

This places a bound on the error when composing imperfect gates. Moreover, this bound is tight, since if $X = \mathcal{X}$ and $Y = \mathcal{Y}$ we get strict equality. We can generalize this result, by simple induction, to arbitrary sequences of gates with corresponding approximations. Thus, in our present case, if each controlled R_k has precision Δ ,

$$E(U, V) \leq \frac{n(n+1)}{2} \Delta \in \Theta(n^2 \Delta). \quad (5.17)$$

Here, the use of Θ is appropriate rather than \mathcal{O} since our bound is tight.

Exercise 5.7

Additional insight into the circuit in Figure 5.2 may be obtained by showing, as you should now do, that the effect of the sequence of controlled- U operations like that in Figure 5.2 is to take the state $|j\rangle|u\rangle$ to $|j\rangle U^j |u\rangle$. (Note that this does not depend on $|u\rangle$ being an eigenstate of U .)

Solution: Suppose there are t qubits in the first register, so the integer j can be expressed in binary as $j_{t-1} \dots j_1 j_0$, with $j_k \in \{0, 1\}$ for every $0 \leq k < t$. By definition, this means $j = j_0 + 2j_1 + \dots + 2^{t-1}j_{t-1}$. The state $|j\rangle$ has tensor product form

$$|j\rangle = \bigotimes_{k=0}^{t-1} |j_k\rangle \equiv |j_{t-1}\rangle \dots |j_0\rangle. \quad (5.18)$$

The action of the controlled- U^{2^k} controlled on the k th qubit is given by

$$|j_k\rangle |u\rangle \longrightarrow |j_k\rangle U^{2^k j_k} |u\rangle \quad (5.19)$$

as can be readily verified. Thus, the full sequence of controlled gates acts as follows.

$$\begin{aligned} |j\rangle |u\rangle &= \bigotimes_{k=0}^{t-1} |j_k\rangle |u\rangle \longrightarrow |j\rangle U^{2^{t-1}j_{t-1}} \dots U^{2^0 j_0} |u\rangle \\ &= |j\rangle U^{2^0 j_0 + \dots + 2^{t-1} j_{t-1}} |u\rangle \\ &= |j\rangle U^j |u\rangle \end{aligned} \quad (5.20)$$

In the last step we reused the definition of j being expressed in binary. This gives the desired result, which, as we see, did not rely on particular knowledge of the state $|u\rangle$.

Exercise 5.8

Suppose the phase estimation algorithm takes the state $|0\rangle|u\rangle$ to the state $|\tilde{\varphi}_u\rangle|u\rangle$, so that the input $|0\rangle(\sum_u c_u|u\rangle)$, the algorithm outputs $\sum_u c_u|\tilde{\varphi}_u\rangle|u\rangle$. Show that if t is chosen according to (5.35), then the probability for measuring φ_u accurate to n bits at the conclusion of the phase estimation algorithm is at least $|c_u|^2(1 - \epsilon)$.

Solution: If t is chosen as such, then $\tilde{\varphi}_u$ is an n -bit approximation to φ_u with probability $p_{succ} \geq (1 - \epsilon)$. Meanwhile, the probability of measuring $\tilde{\varphi}_u$ on the first register is given by the Born rule: $p_u = |c_u|^2$. These two events are independent, hence, the probability of measuring $\tilde{\varphi}_u$ and having it be an n -bit approximation is

$$p_u p_{succ} \geq |c_u|^2(1 - \epsilon). \quad (5.21)$$

Moreover, any other eigenstate $|v\rangle$ of U such that $\varphi_v \neq \varphi_u$ might still result in an n -bit approximation to φ_u , provided they are sufficiently close (it may even be that $\tilde{\varphi}_v = \tilde{\varphi}_u$). This will only further increase the probability of success. In any case, the right side of (5.21) remains a lower bound.

Exercise 5.9

Let U be a unitary transform with eigenvalues ± 1 , which acts on a state $|\psi\rangle$. Using the phase estimation procedure, construct a quantum circuit to collapse $|\psi\rangle$ into one or the other of the two eigenspaces of U , giving also a classical indicator as to which space the final state is in. Compare your result with Exercise 4.34.

Solution: If the eigenvalues of U are 1 and -1 , the corresponding phases are 0.0 and 0.1 respectively. Because these phases are finite bitstrings, there is no possibility of error and, in fact, we can take $t = n$, which in our case is 1. The inverse-QFT on one qubit is simply the Hadamard, and our circuit reduces to the following.



If a 0 (1) is measured, the final state is known to be in the plus (minus) subspace. The probability of each outcome is simply related to the initial overlap with each subspace via the Born rule.

Exercise 5.10

Show that the order of $x = 5$ modulo $N = 21$ is 6.

Solution: We proceed by exhaustive calculation.

$$\begin{aligned} 5^1 \bmod 21 &= 5 \\ 5^2 \bmod 21 &= 4 \\ 5^3 \bmod 21 &= 20 \\ 5^4 \bmod 21 &= 16 \\ 5^5 \bmod 21 &= 17 \\ 5^6 \bmod 21 &= 1 \end{aligned} \quad (5.23)$$

Hence, 6 is the smallest positive integer r such that $5^r \bmod 21 = 1$. Thus, 6 is the order of 5 modulo 21.

Exercise 5.11

Show that the order of x satisfies $r \leq N$.

Solution: Consider the set $\{x^n \bmod N\}_{n=1}^N$. Because we assume x and N share no common factors, it is not possible for $x^n \bmod N = 0$. Hence, $0 < x^n \bmod N < N$. By the pigeonhole principle, not all the values for $x^n \bmod N$ can be unique. There must exist some $x^i = x^j \bmod N$ for some $1 \leq i, j \leq N$ and $j \neq i$. Assume $j > i$ without loss of generality. Then, we have

$$\begin{aligned} x^j - x^i &= 0 \bmod N \\ x^i(x^{j-i} - 1) &= 0 \bmod N. \end{aligned} \tag{5.24}$$

This implies $N | x^i(x^{j-i} - 1)$. But $N \nmid x^i$, again by assumption of no common factors. Hence, we must have $N | (x^{j-i} - 1)$, or $x^{j-i} = 1 \bmod N$. Since r is the smallest integer satisfying this condition, we must have $r \leq j - i < N$. Note this is a strict inequality, unlike what is given in the text.

Exercise 5.12

Show that U is unitary (Hint: x is co-prime to N , and therefore has an inverse modulo N).

Solution: Since U acts as a map on the computational basis states, it suffices to show this map is injective (one-to-one). If $y \geq N$, then $|y\rangle$ is mapped to itself. On the other hand, if $0 \leq y < N$, then $|y\rangle$ is certainly mapped to some $|z\rangle$ where $z < N$. Hence, U is injective on the subspace where $y \geq N$, and it suffices to focus on the case where $y < N$. To this end, suppose $U|y\rangle = U|z\rangle$ for $y, z < N$. Then,

$$\begin{aligned} xy \bmod N &= xz \bmod N \\ x(y - z) &= 0 \pmod{N} \end{aligned} \tag{5.25}$$

This implies N divides $x(y - z)$. However, since N and x are coprime, they share no common factors. This implies $N | (y - z)$. But $|y - z| < N$, so it must be that $y - z = 0$. Hence

$$|y\rangle = |z\rangle \tag{5.26}$$

which proves that U is injective on the basis, as desired.

Exercise 5.13

Prove (5.44). (Hint: $\sum_{s=0}^{r-1} \exp(-2\pi i s k / r) = r \delta_{k0}$). In fact, prove that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k / r} |u_s\rangle = |x^k \bmod N\rangle \tag{5.27}$$

Solution: Let us crank the wheel: putting in the definition of $|u_s\rangle$ to the left side of (5.44) and regrouping.

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k / r} |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k / r} \frac{1}{\sqrt{r}} \sum_{t=0}^{r-1} e^{-2\pi i s t / r} |x^t \bmod N\rangle \tag{5.28}$$

$$= \frac{1}{r} \sum_{s=0}^{r-1} \sum_{t=0}^{r-1} e^{2\pi i s (k-t) / r} |x^t \bmod N\rangle \tag{5.29}$$

$$= \frac{1}{r} \sum_{t=0}^{r-1} |x^t \bmod N\rangle \left(\sum_{s=0}^{r-1} e^{2\pi i s (k-t) / r} \right) \tag{5.30}$$

Making gracious use of the hint, we see the rightmost sum on the last line equals $r\delta_{kt}$. Hence,

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k / r} |u_s\rangle = \sum_{t=0}^{r-1} \delta_{tk} |x^t \bmod N\rangle \quad (5.31)$$

$$= |x^k \bmod N\rangle. \quad (5.32)$$

To obtain (5.44) from the text, simply set $k = 0$.

Exercise 5.14

The quantum state produced in the order-finding algorithm, before the inverse Fourier transform, is

$$|\psi\rangle = \sum_{j=0}^{2^t-1} |j\rangle U^j |1\rangle = \sum_{j=0}^{2^t-1} |j\rangle |x^j \bmod N\rangle \quad (5.33)$$

if we initialize the second register as $|1\rangle$. Show that the same state is obtained if we replace U^j with a *different* unitary transform V , which computes

$$V |j\rangle |k\rangle = |j\rangle |k + x^j \bmod N\rangle, \quad (5.34)$$

and start the second register in the state $|0\rangle$. Also show how to construct V using $O(L^3)$ gates.

Solution: It is obvious that, by setting $k = 0$, we obtain the same output using V as we would if $k = 1$ and we had acted with U . To construct V we can simply use the U^j as before and store the result in an ancillary register whose initial value was one, then *add* that result to the register initialized to 0. The addition step can be carried out bitwise, and only takes $O(L^2)$ gates naively. Hence, the algorithm remains $O(L^3)$ after this addition step.

Exercise 5.15

Show that the least common multiple of positive integers x and y is $xy / \gcd(x, y)$, and thus may be computed in $O(L^2)$ operations if x and y are L bit numbers.

Solution: Let $d = \gcd(x, y)$. Since $d|x$ and $d|y$, it divides the product, so $xy = dn$ for some integer $n > 0$. Our goal is to prove that $n = \text{lcm}(x, y)$.

By Bézout's lemma, there exists integers a, b such that $d = ax + by$. Let m be a common multiple of x and y . Then there exists integers s and t such that $m = sx = ty$. Consider the product md . Using the lemma,

$$\begin{aligned} md &= axm + bym \\ &= axty + bysx \\ &= xy(at + bs). \end{aligned} \quad (5.35)$$

This implies $xy|md$, or since $n = xy/d$, $n|m$. Therefore, n divides every common multiple of x and y . On the other hand, n is itself a common multiple, because

$$n = x \left(\frac{y}{d} \right) = \left(\frac{x}{d} \right) y, \quad (5.36)$$

where the terms in parenthesis are integers. Thus, n is the least common multiple, and the statement is proved.

Exercise 5.16

For all $x \geq 2$ prove that $\int_x^{x+1} 1/y^2 dy \geq 2/3x^2$. Show that

$$\sum_q \frac{1}{q^2} \leq \frac{3}{2} \int_2^\infty \frac{1}{y^2} dy = \frac{3}{4}, \quad (5.37)$$

and thus that (5.58) holds.

Solution: Performing the integral directly yields the solution

$$\int_x^{x+1} 1/y^2 dy = \frac{1}{x^2 + x}. \quad (5.38)$$

For all $x \geq 2$,

$$x \leq \frac{x^2}{2}. \quad (5.39)$$

Thus,

$$\int_x^{x+1} 1/y^2 dy = \frac{1}{x^2 + x} \geq \frac{1}{x^2 + x^2/2} = \frac{2}{3x^2} \quad (5.40)$$

To complete the exercise, note that the sum over prime numbers q is less than the same sum over all integers starting from 2. Thus,

$$\begin{aligned} \sum_q \frac{1}{q^2} &\leq \sum_{n \geq 2} 1/n^2 \\ &\leq \sum_{n \geq 2} \frac{3}{2} \int_n^{n+1} \frac{1}{y^2} dy \\ &= \frac{3}{2} \int_2^\infty \frac{1}{y^2} dy = \frac{3}{4} \end{aligned} \quad (5.41)$$

This proves our result.

Exercise 5.17

Suppose N is L bits long. The aim of this exercise is to find an efficient classical algorithm to determine whether $N = a^b$ for some integers $a \geq 1$, $b \geq 2$. This may be done as follows:

1. Show that b , if it exists, satisfies $b \leq L$.
2. Show that it takes at most $O(L^2)$ operations to compute $\log_2 N$, $x = y/b$ for $b \leq L$, and the two integers u_1 and u_2 nearest to 2^x .
3. Show that it takes at most $O(L^2)$ operations to compute u_1^b and u_2^b (use repeated squaring) and check to see if either is equal to N .
4. Combine the previous results to give an $O(L^3)$ operation algorithm to determine whether $N = a^b$ for integers a and b .

Solution: (1) Note that this statement does not actually hold in the special case $N = 1$, since $b \geq 2$ by assumption and $L = \log_2 1 = 0$. Now to the more interesting case of $N \geq 2$. Then it must be that $a \geq 2$. Assuming that b exists, it may be obtained by computing $\log_a N$. Meanwhile, $L = \lceil \log_2 N \rceil = \lceil b \log_2 a \rceil$. Since $\log_2 a \geq 1$, $L \geq b$.

(2)

Exercise 5.18 (Factoring 91)

Suppose we wish to factor $N = 91$. Confirm that steps **1** and **2** are passed. For step **3**, suppose we choose $x = 4$, which is co-prime to 91. Compute the order r of x with respect to N , and show that $x^{r/2} \bmod 91 = 64 \neq -1 \pmod{91}$, so the algorithm succeeds, giving $\gcd(64 - 1, 91) = 7$.

It is unlikely that this is the most efficient method you've seen for factoring 91. Indeed, if all computations had to be carried out on a classical computer, this reduction would not result in an efficient factoring algorithm, as no efficient method is known for solving the order-finding problem on a classical computer.

Solution: Step **1** is passed since 91 is odd.

Exercise 5.19

Show that $N = 15$ is the smallest number for which the order-finding subroutine is required, that is, it is the smallest composite number that is not even or a power of some smaller integer.

Solution: This can be checked by exhaustion. See the below list

1	Special case (N/A)
2	Prime
3	Prime
4	2^2
5	Prime
6	Even
7	Prime
8	2^3
9	3^2
10	Even
11	Prime
12	Even
13	Prime
14	Even
15	Composite, Odd, distinct prime factors ✓

Exercise 5.20

Suppose $f(x+r) = f(x)$, and $0 \leq x < N$ for N an integer multiple of r . Compute

$$\hat{f}(l) \equiv \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i l x / N} f(x), \quad (5.42)$$

and relate the result to (5.63). You will need to use the fact that

$$\sum_{\{0, r, 2r, \dots, N-r\}} e^{2\pi i k l / N} = \begin{cases} \sqrt{N/r} & \text{if } l \text{ is an integer multiple of } N/r \\ 0 & \text{otherwise.} \end{cases} \quad (5.43)$$

Solution:

Exercise 5.21 (Period finding a phase estimation)

Suppose you are given a unitary operator U_y which performs the transformation $U_y |f(x)\rangle = |f(x+y)\rangle$, for the periodic function described above.

1. Show that the eigenvectors of U_y are $|\hat{f}(l)\rangle$, and calculate their eigenvalues.
2. Show that given $|f(x_0)\rangle$ for some x_0 , U_y can be used to realize a black box which is as useful as U in solving the period-finding problem.

Solution:

Exercise 5.22

Show that

$$|\hat{f}(l_1, l_2)\rangle = \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{-2\pi i(l_1 x_1 + l_2 x_2)} = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i l_2 j / r} |f(0, j)\rangle \quad (5.44)$$

and we are constrained to have $l_1/s - l_2$ be an integer multiple of r for this expression to be non-zero.

Solution:

Exercise 5.23

Compute

$$\frac{1}{r} \sum_{l_1=0}^{r-1} \sum_{l_2=0}^{r-1} e^{2\pi i(l_1 x_1 + l_2 x_2)/r} |\hat{f}(l_1, l_2)\rangle \quad (5.45)$$

using (5.70), and show that the result is $f(x_1, x_2)$.

Solution:

Exercise 5.24

Construct the generalized continued fractions algorithm needed in step 6 of the discrete logarithm algorithm to determine s from estimates of sl_2/r and l_2/r .

Solution:

Exercise 5.25

Construct a quantum circuit for the black box U used in the quantum discrete logarithm algorithm, which takes a and b as parameters, and performs the unitary transform $|x_1\rangle |x_2\rangle |y\rangle \rightarrow |x_1\rangle |x_2\rangle |y \oplus b^{x_1} a^{x_2}\rangle$. How many elementary operations are required?

Solution:

Exercise 5.26

Since K is a subgroup of G , when we decompose G into a product of cyclic groups of prime power order, this also decomposes K . Re-express (5.77) to show that determining l'_i allows one to sample from the corresponding cyclic subgroup K_{p_i} of K .

Solution:

Exercise 5.27

Of course, the decomposition of a general finite Abelian group G into a product of cyclic groups of prime power order is usually a difficult problem (at least as hard as factoring integers, for example). Here, quantum algorithms come to the rescue again: explain how the algorithms in this chapter can be used to efficiently decompose G as desired.

Solution:

Exercise 5.28

Write out a detailed specification of the quantum algorithm to solve the hidden subgroup problem, complete with runtime and success probability estimates, for finite Abelian groups.

Solution:

Exercise 5.29

Give quantum algorithms to solve the Deutsch and Simon problems listed in Figure 5.5, using the framework of the hidden subgroup problem.

Solution:

Problem 5.5 (Non-Abelian hidden subgroups- Research)

Let f be a function on a finite group G to an arbitrary finite range X , which is promised to be constant and distinct on distinct left cosets of a subgroup K . Start with the state

$$\frac{1}{\sqrt{|G|^m}} \sum_{g_1, \dots, g_m} |g_1, \dots, g_m\rangle |f(g_1), \dots, f(g_m)\rangle \quad (5.48)$$

and prove that picking $m = 4 \log |G| + 2$ allows K to be identified with probability at least $1 - 1/|G|$. Note that G does not necessarily have to be Abelian, and being able to perform a Fourier transform over G is not required. This result shows that one can produce (using only $O(\log |G|)$ oracle calls) a final result in which the pure state outcomes corresponding to different possible hidden subgroups are nearly orthogonal. However, it is unknown whether a POVM exists or not which allows the hidden subgroup to be identified *efficiently* (i.e. using $\text{poly}(\log |G|)$ operations) from this final state.

Solution:

Problem 5.6 (Addition by Fourier transform)

Consider the task of constructing a quantum circuit to compute $|x\rangle \rightarrow |x + y \bmod 2^n\rangle$, where y is a fixed constant, and $0 \leq x < 2^n$. Show that one efficient way to do this, for values of y such as 1, is to first perform a quantum Fourier transform, then to apply single qubit phase shifts, then an inverse Fourier transform. What values of y can be added easily this way, and how many operations are required?

Solution:

Chapter 6

Quantum Search Algorithms

Exercise 6.1

Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.

Solution: For $|x\rangle = |0\rangle$,

$$(2|0\rangle\langle 0| - I)|0\rangle = 2|0\rangle - |0\rangle = |0\rangle \quad (6.1)$$

Meanwhile, for $|x\rangle \neq |0\rangle$,

$$(2|0\rangle\langle 0| - I)|x\rangle = 2|0\rangle\langle 0|x\rangle - |x\rangle = -|x\rangle \quad (6.2)$$

Altogether,

$$(2|0\rangle\langle 0| - I)|x\rangle = (-1)^{\delta_{0x}}|x\rangle \quad (6.3)$$

Exercise 6.2

Show that the operation $(2|\psi\rangle\langle\psi| - I)$ applied to a general state $\sum_k \alpha_k |k\rangle$ produces

$$\sum_k (-\alpha_k + 2\langle\alpha\rangle) |k\rangle \quad (6.4)$$

where $\langle\alpha\rangle \equiv \sum_k \alpha_k / N$ is the mean value of the α_k . For this reason, $(2|\psi\rangle\langle\psi| - I)$ is sometimes referred to as the *inversion about mean* operation.

Solution: By linearity,

$$\begin{aligned} (2|\psi\rangle\langle\psi| - I) \sum_k \alpha_k |k\rangle &= \sum_k 2\alpha_k (|\psi\rangle\langle\psi|) |k\rangle - \sum_k \alpha_k |k\rangle \\ &= 2|\psi\rangle \sum_k \alpha_k \langle\psi|k\rangle - \sum_k \alpha_k |k\rangle \end{aligned}$$

Because $|\psi\rangle$ is uniform superposition over the computational basis states, for all k we have $\langle\psi|k\rangle = 1/\sqrt{N}$.

Hence,

$$(2|\psi\rangle\langle\psi| - I) \sum_k \alpha_k |k\rangle = \frac{2}{\sqrt{N}} \left(\sum_k \alpha_k \right) |\psi\rangle - \sum_k \alpha_k |k\rangle \quad (6.5)$$

$$= 2\sqrt{N}\langle\alpha\rangle |\psi\rangle - \sum_k \alpha_k |k\rangle \quad (6.6)$$

Finally, we expand out the definition of $|\psi\rangle$ and cancel the factors of \sqrt{N} . This gives our result.

$$2\sqrt{N}\langle\alpha\rangle |\psi\rangle - \sum_k \alpha_k |k\rangle = \sum_k (2\langle\alpha\rangle - \alpha_k) |k\rangle \quad (6.7)$$

Exercise 6.3

Show that in the $|\alpha\rangle, |\beta\rangle$ basis, we may write the Grover iteration as

$$G = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \quad (6.8)$$

where θ is a real number in the range 0 to $\pi/2$ (assuming for simplicity that $M \leq N/2$; this limitation will be lifted shortly), chosen so that

$$\sin \theta = \frac{2\sqrt{M(N-M)}}{N} \quad (6.9)$$

Solution: As discussed in the text, both the oracle O and the reflection $2|\psi\rangle\langle\psi| - I$ leave the subspace $V = \text{span}(|\alpha\rangle, |\beta\rangle)$ invariant. Hence, so does the product G . Therefore, we will from here on speak of G only in terms of its action on the 2-dimensional subspace $V = \text{span}(|\alpha\rangle, |\beta\rangle)$, and consider the matrix representation in the orthonormal basis $\{|\alpha\rangle, |\beta\rangle\}$. This representation is unitary (since G itself is), and in fact it is orthogonal, since both O and $(2|\psi\rangle\langle\psi| - I)$ have real matrix elements. More specifically, G is *special* orthogonal, meaning it has determinant one, because it is the product of two reflections. All of this implies G is a proper rotation in the plane, and any such matrix may be parametrized as equation (6.8) for *some* angle θ . It remains to show θ satisfies relation (6.9). To do this, we simply compute the matrix element $\langle\beta|G|\alpha\rangle$.

$$\begin{aligned} \langle\beta|G|\alpha\rangle &= \langle\beta|(2|\psi\rangle\langle\psi| - I)O|\alpha\rangle \\ &= \langle\beta|(2|\psi\rangle\langle\psi| - I)|\alpha\rangle \\ &= \langle\beta|(2|\psi\rangle\langle\psi|\alpha\rangle - |\alpha\rangle) \\ &= 2\langle\beta|\psi\rangle\langle\psi|\alpha\rangle, \end{aligned} \quad (6.10)$$

where, along the way, we used the orthogonality of $|\alpha\rangle, |\beta\rangle$ and the fact that $O|\alpha\rangle = |\alpha\rangle$. Finally, using the expression given in the text for $|\psi\rangle$ expanded in the $|\alpha\rangle, |\beta\rangle$ basis, we arrive at our result.

$$\langle\beta|G|\alpha\rangle = \sin \theta = \frac{2\sqrt{M(N-M)}}{N} \quad (6.11)$$

Note that, in fact, we did not require the assumption that $M \leq N/2$ in our derivation.

Exercise 6.4

Give explicit steps for the quantum search algorithm, as above, but for the case of multiple solutions ($1 < M < N/2$).

Solution:

Algorithm: Quantum Search

Input: (1) a black box oracle O which performs the transformation $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$, where f is a boolean function on n bits in which exactly M inputs are known to return 1, with the rest 0. (2) $n+1$ qubits in the state $|0\rangle$.

Output: One of the M solutions to the search problem, where a solution x is a n -bit string such that $f(x) = 1$.

Procedure:

1. $|0\rangle^{\otimes n} |0\rangle$ (initial state)
2. $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$ (apply $H^{\otimes n}$ to the first n qubits and HX to the last).
3. $\rightarrow [(2|\psi\rangle\langle\psi| - I)O]^R \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$
 $\approx \frac{1}{\sqrt{2^M}} \sum_{s=1}^M |s\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$ (apply the Grover iterate $R \approx \lceil \frac{\pi}{4} \sqrt{\frac{2^n}{M}} \rceil$ times)
4. \rightarrow some s such that $f(s) = 1$ (measure the first n qubits)

Exercise 6.5

Show that the augmented oracle O' may be constructed using one application of O , and elementary quantum gates, using the extra qubit $|q\rangle$.

Solution: Notice that O' amounts to applying the oracle O to the first n qubits, conditioned on qubit q being in the 0 state. We can express this schematically as



Thus, we are making a single access to the oracle O .

Exercise 6.6

Verify that the gates in the dotted box in the second figure of Box 6.1 perform the conditional phase shift operation $2|00\rangle\langle 00| - I$, up to an unimportant global phase factor.

Solution: Because $HXH = Z$, the CNOT gate sandwiched between H gates is equivalent to a CZ gate. Moreover, $XZX = -Z$. Thus, the gates in the dotted box enact a controlled minus Z gate, where the control is taken to be the zero state. In bracket form, if R is this set of gates,

$$R = |0\rangle\langle 0| \otimes (-Z) + |1\rangle\langle 1| \otimes I. \tag{6.13}$$

Let's consider the action of R on the computational basis. For states with a 1 on the top qubit, the state is unaffected. Otherwise, the top qubit is in the state 0, in which case a minus sign is applied only if the

bottom qubit is also zero. Thus, R applies a minus sign to $|00\rangle$ and leaves the other basis states unchanged. Hence,

$$R = I - 2|00\rangle\langle 00| \quad (6.14)$$

which is the reflection operator up to an unimportant minus sign.

Exercise 6.7

Verify that the circuits shown in Figures 6.4 and 6.5 implement the operations $\exp(-i|x\rangle\langle x|\Delta t)$ and $\exp(-i|\psi\rangle\langle\psi|\Delta t)$, respectively, with $|\psi\rangle$ as in (6.24).

Solution:

Exercise 6.8

Suppose the simulation step is performed to an accuracy $O(\Delta t^r)$. Show that the number of oracle calls required to simulate H to reasonable accuracy is $O(N^{r/2(r-1)})$. Note that as r becomes large the exponent of N approaches $1/2$.

Solution: If the accuracy of a single step is $O(\Delta t^r)$, then the total error of the simulation is $O((t/\Delta t)\Delta t^r) = O(t\Delta t^{r-1})$, since $t/\Delta t$ is the number of steps in the simulation. For accurate results, we require this error to be $O(1)$, and from the previous section, we see that the time of simulation t is $O(\sqrt{N})$. Thus, we have $\Delta t \in O(1/N^{(r-1)/2})$.

Exercise 6.9

Verify Equation (6.25). (*Hint:* see Exercise 4.15.)

Solution:

Exercise 6.10

Show that by choosing Δt appropriately we can obtain a quantum search algorithm which uses $O(\sqrt{N})$ queries, and for which the final state is $|x\rangle$ *exactly*, that is, the algorithm works with probability 1, rather than with some smaller probability.

Solution:

Exercise 6.11 (Multiple solution continuous quantum search)

Guess a Hamiltonian with which one may solve the continuous time search problem in the case where the search problem has M solutions.

Solution:

Exercise 6.12 (Alternative Hamiltonian for quantum search)

Suppose

$$H = |x\rangle \langle \psi| + |\psi\rangle \langle x|. \quad (6.15)$$

(1) Show that it takes time $O(1)$ to rotate from the state $|\psi\rangle$ to the state $|x\rangle$, given an evolution according to the Hamiltonian H .

(2) Explain how a quantum simulation of the Hamiltonian H may be performed, and determine the number of oracle calls your simulation technique requires to obtain the solution with high probability.

Solution:

Exercise 6.13

Consider a classical algorithm for the counting problem which samples uniformly and independently k times from the search space, and let X_1, \dots, X_k be the results of the oracle calls, that is, $X_j = 1$ if the j th oracle call revealed a solution to the problem, and $X_j = 0$ if the j th oracle call did not reveal a solution to the problem. This algorithm returns the estimate $S = N \times \sum_j X_j / k$ for the number of solutions to the search problem. Show that the standard deviation in S is $\Delta S = \sqrt{M(N-M)/k}$. Prove that to obtain a probability at least $3/4$ of estimating M correctly to within an accuracy \sqrt{M} for all values of M we must have $k = \Omega(N)$.

Solution:

Exercise 6.14

Prove that *any* classical counting algorithm with a probability at least $3/4$ for estimating M correctly to within an accuracy $c\sqrt{M}$ for some constant c and for all values of M must make $\Omega(N)$ oracle calls.

Solution:

Exercise 6.15

Use the Cauchy–Schwarz inequality to show that for any normalized state vector $|\psi\rangle$ and set of N orthonormal basis vectors $|x\rangle$,

$$\sum_x \|\psi - x\|^2 \geq 2N - 2\sqrt{N}. \quad (6.16)$$

Solution:

Exercise 6.16

Suppose we merely require that the probability of an error being made is less than $1/2$ when averaged uniformly over the possible values for x , instead of for all values of x . Show that $O(\sqrt{N})$ oracle calls are still

required to solve the search problem.

Solution:

Exercise 6.17 (Optimality for multiple solutions)

Suppose the search problem has M solutions. Show that $O(\sqrt{N/M})$ oracle applications are required to find a solution.

Solution:

Exercise 6.18

Prove that the minimum degree polynomial representing a Boolean function $F(X)$ is unique.

Solution:

Exercise 6.19

Show that $P(X) = 1 - (1 - X_0)(1 - X_1)\dots(1 - X_{N-1})$ represents OR.

Solution:

Exercise 6.20

Show that $Q_0(OR) \geq N$ by constructing a polynomial which represents the OR function from the output of a quantum circuit which computes OR with zero error.

Solution:

Problem 6.1 (Finding the minimum)

Suppose x_1, \dots, x_N is a database of numbers held in memory, as in Section 6.5. Show that only $O(\log(N)\sqrt{N})$ accesses to the memory are required on a quantum computer, in order to find the smallest element on the list, with probability at least one-half.

Solution:

Problem 6.2 (Generalized quantum searching)

Let $|\psi\rangle$ be a quantum state, and define $U_{|\psi\rangle} \equiv I - 2|\psi\rangle\langle\psi|$. That is, $U_{|\psi\rangle}$ gives the state $|\psi\rangle$ a -1 phase, and leaves the states orthogonal to $|\psi\rangle$ invariant.

(1) Suppose we have a quantum circuit implementing a unitary operator U such that $U|0\rangle^{\otimes n} = |\psi\rangle$. Explain how to implement $U_{|\psi\rangle}$.

(2) Let $|\psi_1\rangle = |1\rangle$, $|\psi_2\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, $|\psi_3\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$. Suppose an unknown oracle O is selected from the set $U_{|\psi_1\rangle}, U_{|\psi_2\rangle}, U_{|\psi_3\rangle}$. Give a quantum algorithm which identifies the oracle with just *one* application of the oracle. (*Hint*: consider superdense coding.)

(3) **Research:** More generally, given k states $|\psi_1\rangle, \dots, |\psi_k\rangle$, and an unknown oracle selected from the set $U_{|\psi_1\rangle}, \dots, U_{|\psi_k\rangle}$, how many oracle applications are required to identify the oracle, with high probability?

Solution:

Problem 6.3 (Database retrieval)

Given a quantum oracle which returns $|k, y \oplus X_k\rangle$ given an n qubit query (and one scratchpad qubit) $|k, y\rangle$, show that with high probability, all $N = 2^n$ bits of X can be obtained using only $N/2 + \sqrt{N}$ queries. This implies the general upper bound $Q_2(F) \leq N/2 + \sqrt{N}$ for any F .

Solution:

Problem 6.4 (Quantum searching and cryptography)

Quantum searching can, potentially, be used to speed up the search for cryptographic keys. The idea is to search through the space of all possible keys for decryption, in each case trying the key, and checking to see whether the decrypted message makes ‘sense’. Explain why this idea doesn’t work for the Vernam cipher (Section 12.6). When might it work for cryptosystems such as DES? (For a description of DES see, for example, [MvOV96] or [Sch96a].)

Solution:

Chapter 7

Quantum computers: physical realization

Exercise 7.1

Using the fact that x and p do not commute, and that in fact $[x, p] = i\hbar$, explicitly show that $a^\dagger a = H/\hbar\omega - 1/2$.

Solution: Let us first apply the definition of a , which is given in the text.

$$\begin{aligned} a^\dagger a &= \frac{1}{2m\hbar\omega} (m\omega x - ip)(m\omega x + ip) \\ &= \frac{1}{2m\hbar\omega} ((m\omega x)^2 + p^2 + im\omega(xp - px)) \end{aligned} \tag{7.1}$$

Note that we cannot cancel the rightmost term since x and p do not commute. However, we can use the commutation relation between them. Regrouping and rearranging,

$$\begin{aligned} a^\dagger a &= \frac{p^2}{2m\hbar\omega} + \frac{1}{2\hbar\omega} m\omega^2 x^2 + \frac{i}{2\hbar} [x, p] \\ &= \frac{1}{\hbar\omega} \left(\frac{p^2}{2m} + \frac{1}{2} m\omega^2 x^2 \right) - \frac{1}{2} \\ &= \frac{H}{\hbar\omega} - \frac{1}{2}. \end{aligned} \tag{7.2}$$

In the last step, we identified the Hamiltonian of the harmonic oscillator. This completes the derivation.

Exercise 7.2

Chapter 8

Quantum noise and quantum operations

Exercise 8.1 (Unitary evolution as a quantum operation)

Pure states evolve under unitary transforms as $|\psi\rangle \rightarrow U|\psi\rangle$. Show that, equivalently, we may write $\rho \rightarrow \mathcal{E}(\rho) \equiv U\rho U^\dagger$, for $\rho = |\psi\rangle\langle\psi|$.

Solution: Consider the map f which identifies the ket representation of a pure quantum state, $|\psi\rangle$, with its representation as a rank one density operator.

$$f(|\psi\rangle) = |\psi\rangle\langle\psi| \quad (8.1)$$

Now suppose we have a unitary operation U on the quantum state, which in the ket representation acts as $|\psi\rangle \rightarrow U|\psi\rangle$. To arrive at a natural definition of the unitary transformation in the density operator formalism, we can consider what map \mathcal{E} satisfies the following commutative property.

$$f(U|\psi\rangle) = \mathcal{E}(f(|\psi\rangle)) = \mathcal{E}(|\psi\rangle\langle\psi|) \quad (8.2)$$

Let $|\psi'\rangle = U|\psi\rangle$, so that $f(U|\psi\rangle) = |\psi'\rangle\langle\psi'|$. I claim that

$$|\psi'\rangle\langle\psi'| = U|\psi\rangle\langle\psi|U^\dagger. \quad (8.3)$$

To see this, we can show that the right side of this equation sends $|\psi'\rangle$ to itself and anything orthogonal to $|\psi'\rangle$ to the zero vector. Indeed,

$$U|\psi\rangle\langle\psi|U^\dagger|\psi'\rangle = U|\psi\rangle\langle\psi|\psi\rangle = \langle\psi|\psi\rangle U|\psi\rangle = |\psi'\rangle. \quad (8.4)$$

Similarly, suppose $|\psi'_\perp\rangle$ is orthogonal to $|\psi'\rangle$. Then, $|\psi'_\perp\rangle = U|\psi_\perp\rangle$ for some $|\psi_\perp\rangle$ orthogonal to $|\psi\rangle$. Hence,

$$U|\psi\rangle\langle\psi|U^\dagger|\psi'_\perp\rangle = U|\psi\rangle\langle\psi|\psi_\perp\rangle = 0. \quad (8.5)$$

Thus, we see that $|\psi'\rangle\langle\psi'| = U|\psi\rangle\langle\psi|U^\dagger$. This demonstrates that the natural definition of a unitary U acting on the density matrix representation of a quantum state is given by

$$\mathcal{E}(|\psi\rangle\langle\psi|) = U|\psi\rangle\langle\psi|U^\dagger, \quad (8.6)$$

which is precisely what we sought to show.

Exercise 8.2

Recall from Section 2.2.3 (on page 84) that a quantum measurement with outcomes labeled by m is described by a set of measurement operators M_m such that $\sum_m M_m^\dagger M_m = I$. Let the state of the system immediately before the measurement be ρ . Show that for $\mathcal{E}_m(\rho) \equiv M_m \rho M_m^\dagger$, the state of the system immediately after the measurement is

$$\frac{\mathcal{E}_m(\rho)}{\text{tr}(\mathcal{E}_m(\rho))}. \quad (8.7)$$

Also show that the probability of obtaining this measurement result is $p(m) = \text{tr}(\mathcal{E}_m(\rho))$.

Solution: For reference, the axioms for pure state measurements as provided in the text are as follows. A measurement with outcome m (an event in the probability space) has corresponding probability $p(m)$ and final state $|\psi'\rangle$ given by

$$\begin{aligned} p(m) &= \langle \psi | M_m^\dagger M_m | \psi \rangle \\ |\psi'\rangle &= \frac{M_m | \psi \rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}, \end{aligned} \quad (8.8)$$

where $|\psi\rangle$ is the initial (pure) state of the system.

The results we are asked to “show” can be taken as axiomatic for open quantum systems. Unfortunately, because the map (8.7) is not convex linear, we cannot extend the axioms on pure states by linearity. The best we can do is show that (8.8) imply (8.7) in the case of pure states, then *assert* (i.e. define) the result to hold for any mixed state. This is what we do below.

First, consider the expression $p(m)$ in terms of ket $|\psi\rangle$. We have

$$\begin{aligned} p(m) &= \langle \psi | M_m^\dagger M_m | \psi \rangle \\ &= \text{tr}(M_m^\dagger M_m | \psi \rangle \langle \psi |) \\ &= \text{tr}(M_m | \psi \rangle \langle \psi | M_m^\dagger) \\ &= \text{tr}(\mathcal{E}_m(\rho)). \end{aligned} \quad (8.9)$$

where we used the property that the trace is cyclic and that, for any operator A and pure state,

$$\text{tr}(A | \psi \rangle \langle \psi |) = \langle \psi | A | \psi \rangle. \quad (8.10)$$

Now consider the pure state after measurement, which as a density operator is given by $|\psi'\rangle \langle \psi'|$. Using the transformation given by the second line of (8.8),

$$|\psi'\rangle \langle \psi'| = \frac{M_m | \psi \rangle \langle \psi | M_m^\dagger}{\langle \psi | M_m^\dagger M_m | \psi \rangle} = \frac{\mathcal{E}_m(| \psi \rangle \langle \psi |)}{\text{tr}(\mathcal{E}_m(| \psi \rangle \langle \psi |))}. \quad (8.11)$$

This shows the result for pure state density matrices that we desire. We can now extend this definition to all quantum states, mixed and pure.

Exercise 8.3

Our derivation of the operator-sum representation implicitly assumed that the input and output spaces for the operation were the same. Suppose a composite system AB initially in an unknown quantum state ρ initially in an unknown quantum state ρ is brought into contact with a composite system CD initially in some

standard state $|0\rangle$, and the two systems interact according to a unitary interaction U . After the interaction we discard systems A and D , leaving a state ρ' of the system BC . Show that the map $\mathcal{E}(\rho) = \rho'$ satisfies

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \quad (8.12)$$

for some set of linear operators E_k from the state space of the system AB to the state space of system BC , and such that $\sum_k E_k^\dagger E_k = I$.

Solution: The action of \mathcal{E} from AB to BC is summarized as follows: append a system CD with state $|0\rangle$, apply a unitary U which acts on the combined system $ABCD$, and trace out system AD . More explicitly,

$$\mathcal{E}(\rho) = \text{tr}_{AD}(U\rho \otimes |0\rangle \langle 0| U^\dagger). \quad (8.13)$$

Let $\{|u_k\rangle\}$ form an orthonormal basis for the space of system AD . Computing the trace with respect to this basis, we have

$$\begin{aligned} \mathcal{E}(\rho) &= \sum_k \langle u_k | U \rho \otimes |0\rangle \langle 0| U^\dagger | u_k \rangle \\ &= \sum_k \langle u_k | U | 0 \rangle \rho \langle 0 | U^\dagger | u_k \rangle \end{aligned} \quad (8.14)$$

Note that we can freely move the ket $|0\rangle$ across ρ to match with U since ρ and $|0\rangle$ live in different spaces. Consider the object E_k defined by

$$E_k \equiv \langle u_k | U | 0 \rangle. \quad (8.15)$$

This is, in fact, an operator from the space of AB to BC . From (8.14) we have

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \quad (8.16)$$

as desired. Moreover, we can check that the completeness relation is satisfied, as it must be for probability conservation.

$$\sum_k E_k^\dagger E_k = \sum_k \langle 0 | U^\dagger | u_k \rangle \langle u_k | U | 0 \rangle = \langle 0 | U^\dagger \left(\sum_k | u_k \rangle \langle u_k | \right) U | 0 \rangle = \langle 0 | U^\dagger U | 0 \rangle = I_{AB} \quad (8.17)$$

where the subscript emphasizes the space the identity is acting on.

Exercise 8.4: (Measurement)

Suppose we have a single qubit principal system, interacting with a single qubit environment through the transform

$$U = P_0 \otimes I + P_1 \otimes X \quad (8.18)$$

where X is the usual Pauli matrix (acting on the environment) and $P_0 \equiv |0\rangle \langle 0|$, $P_1 \equiv |1\rangle \langle 1|$ are projectors (acting on the system). Give the quantum operation for this process, in the operator-sum representation, assuming the environment starts in the state $|0\rangle$.

Solution: There will be two operation elements, E_0 and E_1 , since the dimension of the environment is two. Moreover, per the preceding discussion these will be given by

$$E_j = \langle u_j | U | 0 \rangle \quad (8.19)$$

where the $|u_j\rangle$ form an orthonormal basis for the environment. Let's take these to be the computational basis. We then have

$$\begin{aligned} E_0 &= \langle 0|U|0\rangle = P_0 \otimes \langle 0|I|0\rangle + P_1 \otimes \langle 0|X|0\rangle = P_0 \\ E_1 &= \langle 1|U|0\rangle = P_0 \otimes \langle 1|I|0\rangle + P_1 \otimes \langle 1|X|0\rangle = P_1. \end{aligned} \tag{8.20}$$

Thus, the quantum operation \mathcal{E} can be expressed as

$$\mathcal{E}(\rho) = P_0 \rho P_0 + P_1 \rho P_1 \tag{8.21}$$

Note that this is equivalent to a measurement in the computational basis. It is straightforward to show that these operators satisfy the completeness relation.

Appendix 1: Notes on basic probability theory

Exercise A1.1

Prove Bayes' rule.

Solution: From the definition of conditional probability, we have

$$p(x, y) = p(y|x)p(x) = p(x|y)p(y) \quad (8.22)$$

Rearranging the last of these equations gives the desired result.

Exercise A1.2

Prove the law of total probability.

Solution: We start with the notion that, in the joint probability distribution for (X, Y) , one sums over all outcomes of X to get a probability distribution on Y alone.

$$p(y) = \sum_x p(x, y) \quad (8.23)$$

We arrive at our result by noting that, from the definition of conditional probability, $p(x, y) = p(y|x)p(x)$.

Exercise A1.3

Prove there exists a value of $x \geq \mathbf{E}(X)$ such that $p(x) > 0$.

Solution: Suppose, for sake of contradiction, that every value x of X with nonzero probability has the property $x < \mathbf{E}(X)$. Intuitively, we'd expect that the expectation value would have to be less than $\mathbf{E}(X)$. Indeed, using the inequality in the definition of expectation value,

$$\mathbf{E}(X) = \sum_{x \in X} xp(x) < \mathbf{E}(X) \sum_{x \in X} p(x) = \mathbf{E}(X) \quad (8.24)$$

Hence, $\mathbf{E}(X) < \mathbf{E}(X)$, a clear contradiction. We conclude our premise was false, hence there does exist a value of $x \in X$ such that $x \geq \mathbf{E}(X)$ and $p(x) > 0$.

Exercise A1.4

Prove that $\mathbf{E}(X)$ is linear in X .

Solution: The following computation gives us the result.

$$\begin{aligned}
 \mathbf{E}(aX + bY) &= \sum_{(x,y) \in (X,Y)} (ax + by)p(x, y) \\
 &= \sum_{x \in X} \sum_{y \in Y} axp(x, y) + byp(x, y) \\
 &= \sum_{x \in X} ax \sum_{y \in Y} p(x, y) + \sum_{y \in Y} by \sum_{x \in X} p(x, y) \\
 &= a \sum_{x \in X} xp(x) + b \sum_{y \in Y} yp(y) \\
 &= a\mathbf{E}(X) + b\mathbf{E}(Y).
 \end{aligned} \tag{8.25}$$

Here, a, b are constants. Along the way, we used $p(x) = \sum_y p(x, y)$ and the definition of expectation value.

Exercise A1.5

Prove that for independent random variables X and Y , $\mathbf{E}(XY) = \mathbf{E}(X)\mathbf{E}(Y)$.

Solution: Recall that, for independent random variables, the joint probability distribution breaks into a product of individual probabilities. This yields the following computation.

$$\begin{aligned}
 \mathbf{E}(XY) &= \sum_x \sum_y xy p(x, y) \\
 &= \sum_x \sum_y xy p(x)p(y) \\
 &= \sum_x p(x) \sum_y p(y) \\
 &= \mathbf{E}(X)\mathbf{E}(Y)
 \end{aligned} \tag{8.26}$$

Exercise A1.6

Prove Chebyshev's inequality.

Solution: Our solution is taken from Kliesch and Roth, 2021. We start by proving a more fundamental result: *Markov's inequality*. Let Y be a nonnegative random variable, and $t > 0$. Then

$$p(Y \geq t) \leq \frac{\mathbf{E}(Y)}{t}. \tag{8.27}$$

To show this, let Ω be the set of outcomes over which our random variable Y is defined. Consider the indicator function $\mathbf{1}_A$ for some $A \subset \Omega$, defined as follows.

$$\mathbf{1}_A(\omega) = \begin{cases} 1 & \omega \in A \\ 0 & \omega \notin A \end{cases} \tag{8.28}$$

Take the particular choice $A = \{\omega \in \Omega | Y(\omega) \geq t\}$, one can observe that

$$t\mathbf{1}_A(\omega') \leq Y(\omega') \quad (8.29)$$

for any $\omega' \in \Omega$. Taking the expectation value of our results gives us Markov's inequality.

To obtain Chebyshev's inequality, let $Y = |X - \mathbf{E}(X)|^2$ for some probability distribution X , and let $\lambda^2 = t/\Delta(X)^2$. Note that $\mathbf{E}(Y) = \Delta(X)^2$. Making these substitutions for t and Y gives

$$p(|X - \mathbf{E}(X)|^2 \geq \lambda^2 \Delta(X)^2) \leq \frac{1}{\lambda^2} \quad (8.30)$$

$$p(|X - \mathbf{E}(X)| \geq \lambda \Delta(X)) \leq \frac{1}{\lambda^2} \quad (8.31)$$

This proves our result.

Appendix 2: Group theory

Exercise A2.1

Prove that for any element g of a finite group, there always exists a positive integer r such that $g^r = e$. That is, every element of such a group has an order.

Solution: The proof relies on the pigeonhole principle. If G is a finite group, and $g \in G$, then taking repeated powers of g must yield a repeated element. More formally, there exist distinct positive integers $i, j \in \mathbb{Z}^+$ such that $g^i = g^j$. Without loss of generality, assume $j > i$. Multiplying by g^{-i} on both sides gives $e = g^{j-i}$. Hence, there exists a positive integer $k = j - i$ such that $g^k = e$. Hence g has an order.

Exercise A2.2

Prove Lagrange's theorem.

Solution: To prove the theorem, we will introduce the notion of a coset, which is actually discussed later in the appendix. If $g \in G$, define the (left) coset $gH = \{gh | h \in H\}$. Consider the set of cosets $\{gH | g \in G\}$. I claim two things.

1. Each coset is the same size, and in particular the same size as H (which is itself a coset).
2. The collection of cosets is a *partition* of the group G . This means that
 - (a) Each distinct coset is disjoint, i.e. if $g_1H \neq g_2H$, then $g_1H \cap g_2H = \emptyset$
 - (b) Every element of G is in some coset.

Let us prove each of these claims one by one. Consider some coset gH , and define a bijection $g : H \rightarrow gH$ by left multiplication.

$$g(h) = gh \tag{8.32}$$

Clearly, this is a map to and from the appropriate sets. The map is surjective (onto) since any element $x \in gH$ is equal to gh for some h , and there for the image of h under the map induced by g . To prove the map is injective (one-to-one), suppose $gh_1 = gh_2$ for some $h_1, h_2 \in H$. Taking the inverse of both sides and using associativity, we have $h_1 = h_2$. This proves g is a bijection, and hence H and gH have the same number of elements.

Now for the second item, namely the set of cosets form a partition of G . It is easy to see that every element of $g \in G$ is in the coset gH , proving item (b). To show item (a), we prove the contrapositive: if

$g_1H \cap g_2H \neq \emptyset$, then $g_1H = g_2H$. Assuming the intersection is nonempty, there exists an element g such that both $g = g_1h_1$ and $g = g_2h_2$ for some $h_1, h_2 \in H$. Hence, $g_1 = g_2h_2(h_1)^{-1} \in g_2H$, since H is closed under multiplication. This implies $g_1H \subset g_2H$. But as we just showed, all cosets are the same size (for finite G). Thus, in fact, $g_1H = g_2H$.

Having established the claims above, it is straightforward to prove Lagrange's theorem. There are $|G|$ elements of G , partitioned into a finite number of cosets, each of size $|H|$. That is, $|G| = n|H|$, where n is the number of cosets. This proves the result.

Exercise A2.3

Show that the order of an element $g \in G$ divides $|G|$.

Solution: The order of an element g is the same as the size of the cyclic subgroup H generated by g . By Lagrange's theorem, the order must divide the size of the group.

Exercise A2.4

Show that if $y \in G_x$ then $G_y = G_x$.

Solution: Suppose $y \in G_x$. Then there exists some $g \in G$ such that $y = g^{-1}xg$. Hence, $gyg^{-1} = x$, which implies $x \in G_y$.

We will prove $G_y \subset G_x$. Let $z \in G_y$, so that $z = w^{-1}yw$ for some $w \in G$. Using the conjugacy relation between x and y ,

$$z = w^{-1}(g^{-1}xg)w = u^{-1}xu \quad (8.33)$$

where $u = gw \in G$. Thus, $z \in G_x$, so $G_y \subset G_x$.

We can prove $G_x \subset G_y$ by the argument of the previous paragraph, interchanging x with y and g with g^{-1} wherever they appear. This implies $G_x = G_y$.

Exercise A2.5

Show that if x is an element of an Abelian group G then $G_x = \{x\}$.

Solution: Since $x = exe$, x is in its own conjugacy class. Thus, G_x is nonempty. Let $y \in G_x$, so that $y = g^{-1}xg$ for some $g \in G$. Since the group is Abelian,

$$g^{-1}xg = g^{-1}gx \quad (8.34)$$

$$= ex \quad (8.35)$$

$$= x \quad (8.36)$$

Hence, $y = x$. This implies any element of G_x is x itself, so $G_x = \{x\}$.

Exercise A2.6

Show that any group of prime order is cyclic.

Solution: Let G be a group of prime order. Then, $|G| > 1$, and therefore $G \setminus \{e\}$ is nonempty. Let $g \in G \setminus \{e\}$ and consider the cyclic subgroup $H = \langle g \rangle$. By Lagrange's theorem, $|H|$ divides $|G|$. However, since $|G|$ is prime, it must be that $|H| = 1$ or $|H| = |G|$. It cannot be that $|H| = 1$, since H contains e and g . Hence, $|H| = |G|$. Since $H \subset G$ we have $H = G$. Thus, G is cyclic.

Exercise A2.7

Show that every subgroup of a cyclic group is cyclic.

Solution:

Exercise A2.8

Show that if $g \in G$ has finite order r , then $g^m = g^n$ if and only if $m = n \pmod{r}$.

Solution: If $m = n$, the statement is true automatically. Otherwise, $m < n$ or $m > n$. Assume the former without loss of generality. Then, multiplying both sides by g^{-m} ,

$$e = g^{n-m} \tag{8.37}$$

By Euclid's division lemma, there exist integers q, s such that

$$n - m = qr + s \tag{8.38}$$

where $0 \leq s < r$. Substituting this into equation (8.37),

$$e = g^{qr} g^s \tag{8.39}$$

$$e = (g^r)^q g^s \tag{8.40}$$

$$e = e^q g^s \tag{8.41}$$

$$e = g^s. \tag{8.42}$$

Since r is the order by assumption, and $s < r$ it cannot be that $s > 0$ or else s would be the order of g . This implies $s = 0$. Hence, $r|(n - m)$ and $m = n \pmod{r}$.

Exercise A2.9

Cosets define an equivalence relation between elements. Show that $g_1, g_2 \in G$ are in the same coset of H in G if and only if there exists some $h \in H$ such that $g_2 = g_1 h$.

Solution: Suppose $g_2 = g_1 h$ for some h . Then, by definition, $g_2 \in g_1 H$. Moreover, $g_1 = g_1 e \in g_1 H$. Thus, g_1 and g_2 are in the same coset.

Conversely, suppose g_1 and g_2 are in the same coset, so that there exists some $g \in G$ such that $g_1, g_2 \in gH$. This implies there exist $h_1, h_2 \in H$ such that $g_1 = gh_1$ and $g_2 = gh_2$. Inverting the second of these relations

gives $g = g_2 h_2^{-1}$, and substituting this into the relation for g_1 gives

$$g_1 = (g_2 h_2^{-1}) h_1 \quad (8.43)$$

$$g_1 = g_2 h^{-1}, \quad (8.44)$$

where $h = h_1^{-1} h_2 \in H$. Thus, $g_2 = g_1 h$.

Exercise A2.10

How many cosets of H are there in G ?

Solution: All cosets are the same size $|H|$ and form a partition of the total group G (see Exercise A2.2). Hence, the number of cosets n satisfies

$$n = \frac{|G|}{|H|}. \quad (8.45)$$

Exercise A2.11: (Characters)

Prove the properties of characters given above.

Solution: We will actually assume the result of the subsequent exercise: any (finite) matrix group is equivalent to a unitary matrix group. Hence, we can prove the statements for unitary matrix groups, and the result follows in general since the equivalence preserves character. Note that the proof of unitary equivalence does not rely on the results of this exercise, so there is no circular logic.

(1): The identity element of a matrix group must be the identity matrix itself. The trace of the identity matrix is just the dimension n .

$$\text{tr}(\mathbb{1}) = \sum_{i=1}^n \delta_{ii} = n. \quad (8.46)$$

(2): Let $g \in G$. By unitarity, g is diagonalizable, with eigenvalues $\lambda_k = e^{i\phi_k}$ for $\phi_k \in \mathbb{R}$ and $k = 1, \dots, n$. Since the trace is the sum of the eigenvalues,

$$|\chi(g)| = \left| \sum_{k=1}^n \lambda_k \right| \quad (8.47)$$

$$\leq \sum_{k=1}^n |e^{i\phi_k}| = n. \quad (8.48)$$

Above, we made use of the triangle inequality and the fact that the eigenvalues have unit norm. This proves this part.

(3): Using the notation of the previous part, suppose that $|\chi(g)| = n$. Then we may write $\chi(g) = ne^{i\theta}$ for some phase $\theta \in \mathbb{R}$. This implies $\chi(g') = n$, where $g' = e^{-i\theta} g$. Since g is unitary, so is g' , and by the previous relationship the eigenvalues λ'_k of g' are given by $e^{i\phi'_k}$, where $\phi'_k = \phi_k - \theta$.

We will show that $\phi'_k = 0$ for all $k = 1, \dots, n$, which implies that $\phi_k = \theta$. This, in turn, means that all the eigenvalues of g are the same value $e^{i\theta}$, so that $g = e^{i\theta} I$ as desired. To proceed, let's observe that, if

$\text{tr}(g') = n$, we have

$$\begin{aligned} \sum_{k=1}^n e^{i\phi'_k} &= \sum_{k=1}^n 1 \\ \implies \sum_{k=1}^n (1 - e^{i\phi'_k}) &= 0 \end{aligned} \tag{8.49}$$

The only way this equality can be satisfied is if $\phi'_k = 0$, as can be seen by considering, say, the real part of the above equation. This proves (3).

(4): Suppose $g_1, g_2 \in G$ are members of the same conjugacy class, so that they are related by some similarity transform

$$g_1 = x g_2 x^{-1} \tag{8.50}$$

for some element $x \in G$. The cyclic property of the trace implies it is invariant under a similarity transform. That is,

$$\chi(g_1) = \text{tr}(x g_2 x^{-1}) = \text{tr}(x^{-1} x g_2) = \text{tr}(e g_2) = \text{tr}(g_2) = \chi(g_2) \tag{8.51}$$

Thus, we see that the character is the same for any two members of the same conjugacy class.

(5): We make use of our equivalence to a unitary representation, to say $g^{-1} = g^\dagger$. Hence,

$$\chi(g^{-1}) = \text{tr}(g^\dagger) = \sum_{k=1}^n g_{kk}^* = \chi(g)^* \tag{8.52}$$

(6): What is an algebraic number? I don't really know how to do this one.

Exercise A2.12: (Unitary matrix groups)

A unitary matrix group is comprised solely of unitary matrices (those which satisfy $U^\dagger U = I$). Show that every matrix group is equivalent to a unitary matrix group. If a representation of a group consists entirely of unitary matrices, we may refer to it as being a *unitary representation*.

Solution: Let G be a finite matrix group. Given an inner product $\langle \cdot, \cdot \rangle$, we wish to construct a new inner product $\langle \cdot, \cdot \rangle'$ for which G is unitary. In general, we may relate $\langle \cdot, \cdot \rangle$ and $\langle \cdot, \cdot \rangle'$ via a positive definite matrix P .

$$\langle \cdot, \cdot \rangle' = \langle \cdot, P \cdot \rangle \tag{8.53}$$

The property we want from P is that, for any $g \in G$,

$$g^\dagger P g = P. \tag{8.54}$$

We imagine that, whatever P is, it must be expressed in terms of the group G itself. The simplest way to construct positive matrices from G is to take outer products of the form $g^\dagger g$. We know such constructions are strictly positive, since g is never the zero matrix. Moreover, positive linear combinations of positive matrices are themselves positive, so we might consider trying something of the form

$$P = \sum_{g \in G} c_g g^\dagger g, \quad c_g \geq 0. \tag{8.55}$$

To satisfy condition (8.54), we recall that each element $g \in G$ acts as a permutation on the group via the group multiplication. Because sums over a set are invariant under permutations of the set, we recognize that what we need is $c_g = 1$ for all g . Let's explicitly check that this works.

$$g^\dagger P g = \sum_{g' \in G} g^\dagger g'^\dagger g' g = \sum_{g' \in G} (g' g)^\dagger (g' g) = \sum_{g \in G} g^\dagger g = P. \quad (8.56)$$

Thus, we have proven our result. As a final note, if we wish to transform the group itself instead of the inner product of the space, we observe that we can think instead of acting on our vector space with the transformation \sqrt{P} , since $\langle \cdot, P \cdot \rangle = \langle \sqrt{P}^\dagger \cdot, \sqrt{P} \cdot \rangle$. The group therefore transforms as the corresponding similarity transform.

$$g' = \sqrt{P} g \sqrt{P}^{-1} \quad (8.57)$$

This new matrix group is isomorphic to the original, it has the same characters, and is unitary with respect to the original inner product. This proves our result.

Exercise A2.13

Show that every irreducible Abelian matrix group is one dimensional.

Solution: If A is an abelian matrix group, then by definition each element commutes with one another. This implies the collection A is simultaneously diagonalizable with the same unitary U . Thus there is an equivalent representation of A consisting of diagonal matrices. Diagonal is a special case of block diagonal, and we have multiple blocks unless the dimension is 1. Thus, the group is irreducible if and only if $\dim(A) = 1$.

Exercise A2.14

Prove that if ρ is an irreducible representation of G , then $|G|/d_{rho}$ is an integer.

Solution:

Exercise A2.15

Using the Fundamental Theorem, prove that characters are orthogonal, that is:

$$\sum_{i=1}^r r_i (\chi_i^p)^* (\chi_i^q) = |G| \delta_{pq} \quad \text{and} \quad \sum_{p=1}^r (\chi_i^p)^* (\chi_j^p) = \frac{|G|}{r_i} \delta_{ij}, \quad (8.58)$$

where p, q and δ_{pq} have the same meaning as in the theorem, and χ_i^p is the value the character of the p th irreducible representation takes on the i th conjugacy class of G , and r_i is the size of the i th conjugacy class.

Solution:

Exercise A2.16

S_3 is the group of permutations of three elements. Suppose we order these as mapping 123 to: 123; 231; 312; 213; 132, and 321, respectively. Show that there exist two one-dimensional irreducible representations

of S_3 , one of which is trivial, and the other of which is 1, 1, 1, -1, -1, -1, corresponding in order to the six permutations given earlier. Also show that there exists a two-dimensional irreducible representation, with the matrices

$$\begin{aligned} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}, \\ & \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}. \end{aligned} \quad (8.59)$$

Verify that the representations are orthogonal.

Solution:

Exercise A2.17

Prove that the regular representation is faithful.

Solution:

Exercise A2.18

Show that the character of the regular representation is zero except on the representation of the identity element, for which $\chi(I) = |G|$.

Solution:

Exercise A2.19

Use Theorem A2.5 to show that the regular representation contains d_{ρ^p} instances of each irreducible representation ρ^p . Thus, if R denotes the regular representation, and \hat{G} denotes the set of all inequivalent irreducible representations, then

$$\chi_i^R = \sum_{\rho \in \hat{G}} d_{\rho} \chi_i^{\rho} \quad (8.60)$$

Solution:

Exercise A2.20

The character of the regular representation is zero except for the conjugacy class i containing e , the identity element in G . Show, therefore, that

$$\sum_{\rho \in \hat{G}} d_{\rho} \chi^{\rho}(g) = N \delta_{ge} \quad (8.61)$$

Solution:

Exercise A2.21

Show that $\sum_{\rho \in \hat{G}} d_\rho^2 = |G|$.

Solution:

Exercise A2.22

Substitute (A2.10) into (A2.9) and prove that $\hat{f}(\rho)$ is obtained.

Solution:

Exercise A2.23

Let us represent an Abelian group G by $g \in [0, N - 1]$, with addition as the group operation, and define $\rho_h(g) = \exp[-2\pi i gh/N]$ as the h representation of g . This representation is one-dimensional, so $d_\rho = 1$. Show that the Fourier transform relations for G are

$$\hat{f}(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} f(g) e^{-2\pi i gh/N} \quad \text{and} \quad f(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} \hat{f}(g) e^{2\pi i hg/N}. \quad (8.62)$$

Solution:

Exercise A2.24

Using the results of Exercise A2.16, construct the Fourier transform over S_3 and express it as a 6×6 unitary matrix.

Solution:

Appendix 3: The Solovay–Kitaev theorem

Exercise A3.1:

In Chapter we made use of the distance measure $E(U, V) = \max_{|\psi\rangle} \|(U - V)|\psi\rangle\|$, where the maximum is over all pure states $|\psi\rangle$. Show that when U and V are single qubit rotations, $U = R_{\hat{m}}(\theta)$, $V = R_{\hat{n}}(\varphi)$, $D(U, V) = 2E(U, V)$, and thus it does not matter whether we use the trace distance or the measure $E(\cdot, \cdot)$ for the Solovay-Kitaev theorem.

Solution: First, let's consider $E(U, V)$. We have

$$E(U, V) = \max_{|\psi\rangle} \|(U - V)|\psi\rangle\| = \max_{|\psi\rangle} \|U(\mathbb{1} - U^\dagger V)|\psi\rangle\| = \max_{|\psi\rangle} \|(\mathbb{1} - W)|\psi\rangle\| \quad (8.63)$$

where $W = U^\dagger V \in SU(2)$. Hence, there exists a unit vector \hat{q} and angle $\alpha \in [0, 4\pi)$ such that $W = R_{\hat{q}}(\alpha)$. Let us proceed to calculate the norm in E for an arbitrary state $|\psi\rangle$.

$$\begin{aligned} \|(\mathbb{1} - W)|\psi\rangle\| &= \sqrt{\langle\psi|(\mathbb{1} - W)^\dagger(\mathbb{1} - W)|\psi\rangle} \\ &= \sqrt{1 + 1 - \langle\psi|W^\dagger|\psi\rangle - \langle\psi|W|\psi\rangle} \\ &= \sqrt{2 - 2\operatorname{Re}(\langle W \rangle)} \end{aligned} \quad (8.64)$$

Here, $\langle W \rangle \equiv \langle\psi|W|\psi\rangle$. Recall that, since W is a single qubit rotation,

$$W = R_{\hat{q}}(\alpha) = \cos(\alpha/2)\mathbb{1} + i\sin(\alpha/2)(\hat{q} \cdot \sigma). \quad (8.65)$$

Hence,

$$\operatorname{Re}(\langle W \rangle) = \operatorname{Re}(\cos(\alpha/2)) + \operatorname{Re}(i\sin(\alpha/2)\langle\hat{q} \cdot \sigma\rangle) = \cos(\alpha/2), \quad (8.66)$$

where we used the fact that $\langle\hat{q} \cdot \sigma\rangle$ is purely real. Note that this result is independent of the chosen state $|\psi\rangle$. To summarize our findings

$$E(U, V) = \sqrt{2 - 2\cos(\alpha/2)} = 2\sin(\alpha/4) \quad (8.67)$$

Now let's consider the trace distance $D(U, V)$. First, note that for any operator X and unitary U , $|X| = |UX|$. Hence,

$$|U - V| = |U(\mathbb{1} - U^\dagger V)| = |\mathbb{1} - W| \quad (8.68)$$

with W as before. Consider the eigenvalues of $|\mathbb{1} - W|$. For any operator X , if λ is an eigenvalue, then $|\lambda|$ is an eigenvalue of $|X|$. The eigenvalues of $\mathbb{1} - W$ are given by $1 - e^{\pm i\alpha/2}$, so the eigenvalues of $|\mathbb{1} - W|$ are

$$|1 - e^{\pm i\alpha/2}| = 2|\sin(\pm\alpha/4)| = 2\sin(\alpha/4). \quad (8.69)$$

Note that both eigenvalues are equal. Since the trace is the sum of the eigenvalues (weighted by multiplicity)

$$D(U, V) = \text{tr} |\mathbb{1} - W| = 4 \sin(\alpha/4). \quad (8.70)$$

Comparing with (8.67), we see that $D(U, V) = E(U, V)$, which is the desired result. Note that the arguments used depended crucially on the fact that we are in two dimensions (one qubit).

Exercise A3.2

Appendix 4: Number theory

Exercise A4.1 (Transitivity)

Show that if $a|b$ and $b|c$, then $a|c$.

Solution: The premises imply, by definition, that there exist integers j, k such that $b = aj$ and $c = bk$. Substituting the first of these two equations into the second, we see $c = ajk = al$, where $l = jk \in \mathbb{Z}$. Hence, there exists an integer, namely l , such that $c = al$, proving $a|c$.

Exercise A4.2

Show that if $d|a$ and $d|b$ then d also divides a linear combination of a and b , $ax + by$, where x and y are integers.

Solution: From the definition of $d|a$ and $d|b$, there exist integers j, k such that $a = dj$ and $b = dk$. Hence,

$$ax + by = djx + dky = d(jx + ky). \quad (8.71)$$

Define $m = jx + ky \in \mathbb{Z}$. Then we see $ax + by = dm$. From the definition of dividing, we have $d|(ax + by)$.

Exercise A4.3

Suppose a and b are positive integers. Show that if $a|b$ then $a \leq b$. Conclude that if $a|b$ and $b|a$ then $a = b$.

Solution: Suppose that $a|b$. Then there exists some $k \in \mathbb{Z}$ such that $b = ak$. By the hypothesis that a and b are positive, it must be that $k > 0$. Hence, $k - 1 \geq 0$. This, of course, implies

$$b(k - 1) \geq 0 \quad (8.72)$$

since, again, b is nonnegative (positive, in fact). The result we desire comes from basic manipulations of inequalities.

$$\begin{aligned} b(k - 1) \geq 0 &\implies bk \geq b \\ &\implies a \geq b \end{aligned} \quad (8.73)$$

As an immediate corollary, if $a|b$ and $b|a$ (both being positive integers), we have $a \geq b$ and $b \geq a$. Of course, this implies $a = b$. Note that the assumption of positivity was crucial for the proof to hold, and indeed, it is easy to see how it can be broken if negative numbers are included.

Exercise A4.4

Find the prime factorizations of 697 and 36 300.

Solution: I do not pretend to solve these in any mechanical fashion. Looking online, I notice 697 is a product of 41 and 17. Each of these numbers are themselves prime, so the prime factorization is

$$697 = 41^1 17^1 \quad (8.74)$$

Unlike the first, the second number is easier to do in your head. We can pull out two factors of 10 and easily prime factor those. Meanwhile, 363 is divisible by 3, and then if you cared to memorize some perfect squares, $121 = 11^2$. Altogether.

$$36300 = 2^2 3^1 5^2 11^2. \quad (8.75)$$

Exercise A4.5

For p a prime prove that all integers in the range 1 to $p - 1$ have multiplicative inverses modulo p . Which integers in the range 1 to $p^2 - 1$ do not have multiplicative inverses modulo p^2 ?

Solution: For any integer $a \in [1, p - 1]$, a is coprime with p . Hence, a has an inverse modulo p . In the case of p^2 , the only integer which is not coprime with p^2 in the range $[0, p^2 - 1]$ is p itself. Every other integer in the range has a multiplicative inverse.

Exercise A4.6

Find the multiplicative inverse of 17 modulo 24.

Solution: We seek an positive integer $n < 24$ such that $17 * n = 1 \pmod{24}$. Without yet an efficient method, we can perform an exhaustive check by hand or with a computer. It turns out the answer is $n = 17$ itself.

Exercise A4.7

Find the multiplicative inverse of $n + 1$ modulo n^2 , where n is any integer greater than 1.

Solution: The answer, which might be reasonably guessed (or not). Is $n - 1$.

$$(n + 1)(n - 1) = n^2 - 1 = 1 \pmod{n^2}. \quad (8.76)$$

Exercise A4.8 (Uniqueness of the inverse)

Suppose b and b' are multiplicative inverses of a , modulo n . Prove that $b = b' \pmod{n}$.

Solution: If b and b' are both inverses of a , then $ab = ab' \pmod{n}$. This implies

$$a(b - b') = 0 \pmod{n}. \quad (8.77)$$

From this, we conclude $n|a(b-b')$. But we also know, by Corollary A4.4, that n and a are coprime. Hence, $n|(b-b')$, so $b = b' \pmod{n}$.

Exercise A4.9

Explain how to find $\gcd(a, b)$ if the prime factorizations of a and b are known. Find the prime factorizations of 6825 and 1430, and use them to compute $\gcd(6825, 1430)$.

Solution: If the prime factorization of a and b are known, simply find the largest set (counting multiplicity) of shared prime factors.

The prime factorization of 6825 and 1430 are $3^1 5^1 15^1 419^1$ and $2^1 5^1 11^1 13^1$ respectively. The only shared prime factor is 5, hence this is also the gcd.

Exercise A4.10

What is $\varphi(187)$?

Solution: The prime factorization of 187 is 11×17 . Hence,

$$\varphi(187) = \varphi(17 \times 11) = \varphi(17)\varphi(11) = 16 \times 10 = 160 \quad (8.78)$$

Exercise A4.11

Problem: Prove that

$$n = \sum_{d|n} \varphi(d) \quad (8.79)$$

where the sum is over all positive divisors d of n , including 1 and n . (*Hint:* Prove the result for $n = p^\alpha$ first, then use the multiplicative property (A4.22) of φ to complete the proof.

Solution: Follow the advice of the hint, suppose $n = p^\alpha$ where p is prime. The divisors of n are p^j , where $0 \leq j \leq \alpha$. Hence, starting from the right hand side,

$$\begin{aligned} \sum_{d|n} \varphi(d) &= \sum_{j=0}^{\alpha} \varphi(p^j) = 1 + \sum_{j=1}^{\alpha} p^{j-1}(p-1) \\ &= 1 + (p-1) \sum_{j=1}^{\alpha} p^{j-1} \\ &= 1 + \sum_{j=0}^{\alpha} p^j - \sum_{j=0}^{\alpha} p^{j-1} \\ &= p^\alpha, \end{aligned} \quad (8.80)$$

where, in the last step, all but p^α cancel from subtractions. This proves the result when n is a power of a prime.

To generalize the argument, we use the fundamental theorem of arithmetic, which says any $n \in \mathbb{Z}$ has a prime factorization.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}. \quad (8.81)$$

Since all terms are powers of prime, they are coprime with each other, and we may use the multiplicative property of φ .

$$\begin{aligned} \varphi(n) &= \prod_{j=1}^m \varphi(p_j^{\alpha_j}) \\ &= \prod_{j=1}^m \sum_{k_j=0}^{\alpha_j} \varphi(p^{k_j}) \end{aligned} \quad (8.82)$$

In the second step we used the first result derived above for powers of primes. By repeated use of the distributive property, the sum and product in the second line of (8.82) can be reversed, and cast as a sum over m variables.

$$\begin{aligned} \prod_{j=1}^m \sum_{k_j=0}^{\alpha_j} \varphi(p^{k_j}) &= \sum_{k_1=0}^{\alpha_1} \sum_{k_2=0}^{\alpha_2} \dots \sum_{k_m=0}^{\alpha_m} \prod_{j=1}^m \varphi(p^{k_j}) \\ &= \sum_{k_1=0}^{\alpha_1} \sum_{k_2=0}^{\alpha_2} \dots \sum_{k_m=0}^{\alpha_m} \varphi(p^{k_1} p^{k_2} \dots p^{k_m}) \end{aligned} \quad (8.83)$$

A careful examination of this last equation reveals it is nothing more than a sum over all possible divisors d of n , expressed via the prime factorization. Hence,

$$\varphi(n) = \sum_{d|n} \varphi(d) \quad (8.84)$$

as desired.

Exercise A4.12

Verify that \mathbf{Z}_n^* forms a group of size $\varphi(n)$ under the operation of multiplication modulo n .

Solution: That \mathbf{Z}_n^* is a set of size $\varphi(n)$ follows directly from the definition of φ . Let $a, b \in \mathbf{Z}_n^*$, with inverses a^{-1}, b^{-1} . Then, the product ab has inverse $a^{-1}b^{-1}$, hence is in \mathbf{Z}_n^* (note the order doesn't matter since multiplication is commutative). Thus, the set is closed under the binary operator. Moreover, multiplication modulo n is associative. Finally, it is easy to see that $1 \in \mathbf{Z}_n^*$ (being its own inverse) and it acts as the identity operator. Of course inverses exist, by definition, therefore we have shown that \mathbf{Z}_n^* satisfies the properties of a group under multiplication modulo n .

Exercise A4.13

Let a be an arbitrary element of \mathbf{Z}_n^* . Show that $S \equiv \{1, a, a^2, \dots\}$ forms a subgroup of \mathbf{Z}_n^* , and that the size of S is the least value of r such that $a^r = 1 \pmod{n}$.

Solution: For any finite group G , if I take a single element $g \in G$ and generate a subset $S \subset G$ by repeatedly multiplying g by itself, the result will be a subgroup (when I include the induced binary operation).

More generally, I can have multiple generators g_1, g_2, \dots, g_m and the result will still be a subgroup. Note this does not hold for infinite groups such as \mathbb{Z} , unless we allow negative exponents.

If r is the smallest positive integer satisfying $a^r = 1 \pmod{n}$, it follows that each a^i is unique for $i = 0, 1, \dots, r-1$. Otherwise, $a^i = a^j$ for some $i, j < r$, which implies $a^{j-i} = 1$. This contradicts the assertion that r is the *least* such value. Hence, S has at least r values. In fact, it cannot have more than r unique values, since for any $k > r$ we have

$$k = qr + i \tag{8.85}$$

for some $q \in \mathbb{Z}^+$ and $i < r$. But this will give the same power of a as i does.

$$a^k = a^{qr+i} = (a^r)^q a^i = 1^q a^i = a^i \tag{8.86}$$

Here all powers are taken modulo n . Thus, S has r elements.

Exercise A4.14

Suppose g is a generator for \mathbf{Z}_n^* . Show that g must have order $\varphi(n)$.

Solution: If g generates \mathbf{Z}_n^* , then every $a \in \mathbf{Z}_n^*$ must be some power of g . Hence, \mathbf{Z}_n^* is cyclic. By the results from the previous exercise, the size of \mathbf{Z}_n^* , which is $\varphi(n)$ must equal the order of the generator g .

Exercise A4.15

Lagrange's theorem (Theorem A2.1 on page 610) is an elementary result of group theory stating that the size of a subgroup must divide the order of the group. Use Lagrange's theorem to provide an alternative proof of Theorem A4.9, that is, show that $a^{\varphi(n)} = 1 \pmod{n}$ for any $a \in \mathbf{Z}_n^*$.

Solution: Consider the subgroup $A \subset G$ generated by a . Then the size of A is the order of a , say, r . By Lagrange's theorem, r must divide $\varphi(n)$, the size of \mathbf{Z}_n^* . That is, $\varphi(n) = kr$ for some $k \in \mathbb{Z}^+$. Given this,

$$a^{\varphi(n)} = a^{kr} = (a^r)^k = 1^k = 1 \tag{8.87}$$

where all values are taken modulo n . This proves Euler's generalization of the little theorem.

Exercise A4.16

Use Theorem A4.9 to show that the order of x modulo N must divide $\varphi(N)$.

Solution: This follows directly from Lagrange's theorem (see the previous cluster of exercises). We've already shown that the size of a cyclic subgroup of \mathbf{Z}_n^* is the order of a generating element. Lagrange's theorem says this order r must divide the size of the larger group \mathbf{Z}_n^* , which is $\varphi(n)$.

Exercise A4.17 (Reduction of order-finding to factoring)

We have seen that an efficient order-finding algorithm allows us to factor efficiently. Show that an efficient factoring algorithm would allow us to efficiently find the order modulo N of any x co-prime to N .

Solution:

Exercise A4.18

Find the continued fraction expansion for $x = 19/17$ and $x = 77/65$

Solution: In both cases we apply the repeated fraction algorithm. The case $x = 19/17$ is only a few steps.

$$\frac{19}{17} = 1 + \frac{2}{17} = 1 + \frac{1}{\frac{17}{2}} = 1 + \frac{1}{8 + \frac{1}{2}} \quad (8.88)$$

For the case $x = 77/65$, we have to work a little harder. Here are the intermediate steps.

$$\begin{aligned} 77/65 &= 1 + 12/65 \\ 65/12 &= 5 + 5/12 \\ 12/5 &= 2 + 2/5 \\ 5/2 &= 2 + 1/2. \end{aligned} \quad (8.89)$$

Hence the result is

$$\frac{77}{65} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} \quad (8.90)$$

Exercise A4.19

Show that $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$ for $n \geq 1$. Use this fact to conclude that $\gcd(p_n, q_n) = 1$. (*Hint:* Induct on n .)

Solution: As the hint suggests, we proceed by induction on n . In the case $n = 1$, using the definitions provided in the text,

$$q_1 p_0 - p_1 q_0 = a_1 a_0 - (1 + a_0 a_1) 1 = -1 \quad (8.91)$$

as desired. By inductive hypothesis, assume the statement holds for $n = m$. Then, using the recursive definition for p and q ,

$$q_{m+1} p_m - p_{m+1} q_m = (a_{m+1} q_m + q_{m-1}) p_m - (a_{m+1} p_m + p_{m-1}) q_m \quad (8.92)$$

$$= \cancel{a_{m+1} q_m p_m} + q_{m-1} p_m - \cancel{a_{m+1} p_m q_m} - p_{m-1} q_m \quad (8.93)$$

$$= -(q_m p_{m-1} - p_m q_{m-1}) \quad (8.94)$$

$$= (-1)^m + 1, \quad (8.95)$$

where in the last step we invoked the inductive hypothesis. Hence, the statement also holds for $n = m + 1$. By induction, the statement holds for all $n \geq 1$.

Note that the result may be reexpressed as

$$(-1)^n (q_n p_{n-1} - p_n q_{n-1}) = 1. \quad (8.96)$$

By Theorem A4.2, we must have $\gcd(p_n, q_n) = 1$.

Problem 4.1 (Prime number estimate)

Let $\pi(n)$ be the number of prime numbers which are less than n . A difficult-to-prove result known as the *prime number theorem* asserts that $\lim_{n \rightarrow \infty} \pi(n) \log(n)/n = 1$ and thus $\pi(n) \approx n/\log(n)$. This problem gives a poor man's version of the prime number theorem which gives a pretty good lower bound on the distribution of prime numbers.

(1) Prove that $n \leq \log \binom{2n}{n}$.

Solution to (1): Note this is equivalent proving $2^n \geq \binom{2n}{n}$ (note the logarithm is base two). By definition,

$$\binom{2n}{n} = \frac{2n!}{n!n!} = \prod_{i=1}^n \frac{n+i}{i}. \quad (8.97)$$

Moreover, for each i in the product, $(n+i)/i = 1 + n/i \geq 2$. Hence,

$$\prod_{i=1}^n \frac{n+i}{i} \geq \prod_{i=1}^n 2 = 2^n. \quad (8.98)$$

This proves the result.

(2) Show that

$$\log \binom{2n}{n} \leq \sum_{p \leq 2n} \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \log p \quad (8.99)$$

where the sum is over all primes p less than or equal to $2n$.

Solution to (2): This one is hard! I could rewrite the problem as showing

$$\binom{2n}{n} \leq \prod_{p < 2n} e^{\log p \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor} \quad (8.100)$$

(3) Use the previous two results to show that

$$\pi(2n) \geq \frac{n}{\log(2n)} \quad (8.101)$$

Solution to (3): From the previous two parts, we have

$$n \leq \sum_{p \leq 2n} \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \log p. \quad (8.102)$$

Moreover, for any two positive real numbers x and y ,

$$\lfloor x \rfloor y \leq \lfloor xy \rfloor. \quad (8.103)$$

Hence,

$$\begin{aligned} \sum_{p \leq 2n} \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \log p &\leq \sum_{p \leq 2n} \left\lfloor \frac{\log(2n)}{\log p} \log p \right\rfloor \\ &\leq \sum_{p \leq 2n} \lfloor \log(2n) \rfloor \\ &\leq \log(2n) \pi(2n) \end{aligned} \quad (8.104)$$

From this, we have $n \leq \log(2n) \pi(2n)$, and we have our result from rearranging.

Appendix 5: Public key cryptography and the RSA cryptosystem

Exercise A5.1

Written examples of the application of RSA tend to be rather opaque. It's better to work through an example yourself. Encode the word 'QUANTUM' (or at least the first few letters!), one letter at a time, using $p = 3$ and $q = 11$. Choose appropriate values for e and d , and use a representation of English text involving 5 bits per letter.

Solution: There is choice in how we represent the letters, but a natural one is to label from 1 to 26. In this representation, we have

$$\begin{aligned} Q &= 17 = 10001 \\ U &= 21 = 10101 \\ A &= 01 = 00001 \\ N &= 14 = 01110 \\ T &= 20 = 10100 \\ M &= 13 = 01101. \end{aligned} \tag{8.105}$$

In our encoding, the message is 35 bits in length, and given by

$$S = 10001101010000101110101001010101101 \tag{8.106}$$

$$= 18959782573 \tag{8.107}$$

where we converted to decimal in the last step. Next we choose an odd number e relatively prime to $\phi(n) = (p-1)(q-1) = 20$. We will choose $e = 9$. To compute the multiplicative inverse modulo 20, d , we employ Euler's algorithm. Following the steps outlined in appendix 4,

$$\begin{aligned} 20 &= 2 \times 9 + 2 \\ 9 &= 4 \times 2 + 1 \\ 2 &= 2 \times 1. \end{aligned} \tag{8.108}$$

Now we back substitute to find coefficients x, y such that $1 = 9x + 20y$.

$$\begin{aligned} 1 &= 9 - 4 \times 2 \\ &= 9 - 4 \times (20 - 2 \times 9) \\ &= 9 - 4 \times 20 + 8 \times 9 \\ &= 9 \times 9 - 4 \times 20. \end{aligned} \tag{8.109}$$

Reading off the coefficient, we can readily see that 9 is its own inverse modulo 20. Hence $d = e = 9$.

Alas, with such a small n we can only encode in 5 bit chunks. We'll therefore simply encode each letter separately. We have

$$E(Q) = 17^9 \pmod{33} = 02 = 00010 \quad (8.110)$$

$$E(U) = 21^9 \pmod{33} = 21 = 10101 \quad (8.111)$$

$$E(A) = 01^9 \pmod{33} = 01 = 00001 \quad (8.112)$$

$$E(N) = 14^9 \pmod{33} = 26 = 00010 \quad (8.113)$$

$$E(T) = 20^9 \pmod{33} = 05 = 00101 \quad (8.114)$$

$$E(M) = 13^9 \pmod{33} = 28 = 11100 \quad (8.115)$$

$$(8.116)$$

You can readily check, as expected, that taking the encoded message to the power of 9 (in 5 bit chunks) gets you back to the original message.

Exercise A5.2

Show that d is also an inverse of e modulo r , and thus $d = d' \pmod{r}$.

Solution: We will prove a somewhat more general result, namely if $ab = 1 \pmod{n}$ and $d|n$, then $ab = 1 \pmod{d}$. Indeed, the first statement implies $ab = qn + 1$ for some $q \in \mathbb{Z}$. On the other hand, since $d|n$, there is an integer k such that $n = dk$. Using these relations, we have $ab = q(dk) + 1 = (qk)d + 1$. Thus, $ab = 1 \pmod{d}$.

This solves the exercise when we recognize that $de = 1 \pmod{\phi(n)}$ and $r|\phi(n)$. A result from the previous appendix shows that the two inverses d and d' are equivalent modulo r .

Problem 5.1:

Write a computer program for performing encryption and decryption using the RSA algorithm. Find a pair of 20 bit prime numbers and use them to encrypt a 40 bit message.

Solution: I will first write pseudocode, then give an actual implementation in a common language such as python. Here is some pseudocode for the two major subroutines employed: RandomPrime and InverseMod.

Algorithm 1: RSA algorithm for public key cryptography

```

1 RSA algorithm ( $L, M$ );
   Input : An integer  $L$  specifying bit length of primes, and a  $2L$ -bit message  $M$ .
   Output: A public key  $P = (e, n)$  and private key  $M = (d, n)$ .
2  $p = \text{RandomPrime}(L)$ ;
3  $q = \text{RandomPrime}(L)$ ;
4  $n = pq$ ;
5  $\varphi = (p - 1)(q - 1)$ ;
6  $d = \text{InverseMod}(e, \varphi)$ ;
7  $P = (e, n)$ ;
8  $S = (d, n)$ ;
9 return  $P, S$ 
```

Algorithm 2: Algorithm for producing random prime p of given length.

```
1 RandomPrime ( $L$ );  
   Input : An integer  $L$  specifying the bit length of the desired prime  
   Output: A random prime  $p$  of that length  
2  $p = \text{RandomInt}(L)$ ;  
3 do  
4    $p = \text{RandomInt}(L)$ ;  
5 while not prime( $p$ );
```

Appendix 6: Proof of Lieb's theorem

Exercise A6.1 (\leq is preserved under conjugation)

If $A \leq B$, show that $XAX^\dagger \leq XBX^\dagger$ for all matrices X .

Solution: We will first prove that positivity is preserved under conjugation with X . That is, if P is positive, so is XPX^\dagger . Taking the adjoint shows that XPX^\dagger is hermitian.

$$(XPX^\dagger)^\dagger = (X^\dagger)^\dagger P^\dagger X^\dagger = XPX^\dagger \quad (8.117)$$

To prove positive-semidefiniteness, suppose λ is a (real) eigenvalue of XPX^\dagger , so that there is a normalized vector v such that.

$$XPX^\dagger v = \lambda v \quad (8.118)$$

Taking the inner product of both sides of this equation with v itself,

$$\begin{aligned} \langle v, XPX^\dagger v \rangle &= \langle v, \lambda v \rangle \\ \langle X^\dagger v, PX^\dagger v \rangle &= \lambda \langle v, v \rangle \\ \langle u, Pu \rangle &= \lambda, \end{aligned} \quad (8.119)$$

where $u = X^\dagger v$. Because P is positive semidefinite, we see that $\lambda \geq 0$. Hence, every eigenvalue of XPX^\dagger is nonnegative. This proves our result.

Exercise A6.2

Prove that $A \geq 0$ if and only if A is a positive operator.

Solution: If $A \geq 0$, then $A - 0$ is positive semidefinite, hence so is A . Conversely, if A is positive, so is $A - 0$, and thus $A \geq 0$.

Exercise A6.3 (\leq is a partial order)

Show that the relation \leq is a partial order on operators – that is, it is transitive ($A \leq B$ and $B \leq C$ implies $A \leq C$), asymmetric ($A \leq B$ and $B \leq A$ implies $A = B$), and reflexive ($A \leq A$).

Solution: Let's start by proving transitivity. If $A \leq B$ and $B \leq C$, then $B - A$ and $C - B$ are positive matrices. Hence so is their sum, $C - A$. This implies $A \leq C$ by definition.

To prove asymmetry, suppose $A \leq B$ and $B \leq A$. Let λ be an eigenvalue of $A - B$. It is then clear that $B - A$ must have eigenvalue $-\lambda$. By assumption of positive semidefiniteness of $A - B$ and $B - A$ we must have

$$\lambda \leq 0 \quad \lambda \geq 0. \quad (8.120)$$

Hence, $\lambda = 0$. Thus every eigenvalue of $A - B$ is zero, so $A - B = 0$. This proves asymmetry.

Finally, we note that $A - A = 0$ is positive semidefinite. Thus, $A \leq A$, proving the reflexive property.

Exercise A6.4

Suppose A has eigenvalues λ_i . Define λ to be the maximum of the set $|\lambda_i|$. Prove that

- (1) $\|A\| \geq \lambda$.
- (2) When A is Hermitian, $\|A\| = \lambda$.
- (3) When

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad (8.121)$$

$$\|A\| = 3/2 > 1 = \lambda$$

Solution: (1) Since A is a matrix, its set of eigenvalues is finite. Hence, there exists an eigenvalue λ_m such that $|\lambda_m| = \lambda$. Let $|u_m\rangle$ be the corresponding eigenvector, normalized. Then,

$$|\langle u_m | A | u_m \rangle| = |\lambda_m \langle u_m | u_m \rangle| = \lambda \quad (8.122)$$

Since $\|A\|$ is the maximum over all such inner products, it is certainly at least as big as the value set by $|u\rangle = |u_m\rangle$. Hence, $\|A\| \geq \lambda$.

(2) Using part (1), it suffices to show that $\|A\| \leq \lambda$ for hermitian A . If $|u\rangle$ is a normalized state, it can be expressed as a linear combination in an orthonormal basis defined by the eigenstates of A .

$$|u\rangle = \sum_i c_i |\lambda_i\rangle \quad (8.123)$$

Here, $|\lambda_i\rangle$ is an eigenstate of A with eigenvalue λ_i . Computing the inner product as in the definition of $\|A\|$,

$$|\langle u | A | u \rangle| = \left| \sum_i \lambda_i |c_i|^2 \right| \leq \sum_i |\lambda_i| |c_i|^2 \leq \lambda \sum_i |c_i|^2 = \lambda \quad (8.124)$$

Along the way, we used the triangle inequality, the fact that $|\lambda_i| \leq \lambda$, and the normalization of $|u\rangle$. Since λ is an upper bound for every $|u\rangle$, it is also an upper bound for the maximum, which is precisely $\|A\|$. Thus, $\|A\| \leq \lambda$, which combined with the previous result gives $\|A\| = \lambda$.

(3) A has a single eigenvalue $\lambda = 1$ with eigenvector $|\lambda\rangle = (0, 1)^T$. Hence, $\lambda = 1$. On the other hand, for some normalized $(a, b) \in \mathbb{C}^2$,

$$(a^* \quad b^*) \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2 + |b|^2 + ab^* \quad (8.125)$$

$$= 1 + ab^* \quad (8.126)$$

If $a = b = 1/\sqrt{2}$, then this value is $3/2$. On the other hand, for more arbitrary complex values of a and b , the triangle inequality puts $3/2$ as an upper bound on the magnitude.

$$|1 + ab^*| \leq 1 + |a||b| \leq 3/2. \quad (8.127)$$

Hence, $\|A\| = 3/2$, and we have our result.

Exercise 6.5: (AB and BA have the same eigenvalues)

Prove that AB and BA have the same eigenvalues. (*Hint:* For invertible A , show that $\det(xI - AB) = \det(xI - BA)$, and thus the eigenvalues of AB and BA are the same. By continuity this holds even when A is not invertible.

Solution: As the hint suggests, first suppose A is invertible. Because the eigenvalues of AB and BA are the zeros of the characteristic polynomial, showing these two polynomials are the same amounts to proving the statement. And these polynomials are precisely the determinants shown in the hint.

We will use the property that the determinant is indifferent to the permutation of matrices in a product.

$$\det(xI - AB) = \det(I(xI - AB)) \quad (8.128)$$

$$= \det(A^{-1}A(xI - AB)) \quad (8.129)$$

$$= \det(A^{-1}(xI - AB)A) \quad (8.130)$$

$$= \det(xI - BA) \quad (8.131)$$

This proves our result when A is invertible. If A is singular, then there exists an $\epsilon > 0$ such that

$$A' = A + \epsilon I \quad (8.132)$$

is invertible. Then the theorem carries over as before for A' , and to get the result for A we take $\epsilon \rightarrow 0$. This is valid since the determinant is only a polynomial in ϵ .

Exercise 6.6

Suppose A and B are such that AB is Hermitian. Using the previous two observations show that $\|AB\| \leq \|BA\|$.

Solution: Since AB is Hermitian, then $\|AB\| = |\lambda|$ for some eigenvalue of AB . By the previous exercise, λ is also an eigenvalue of BA , and by that same exercise we have $\lambda \leq \|BA\|$. Thus, $\|AB\| \leq \|BA\|$.

Exercise 6.7

Suppose A is positive. Show that $\|A\| \leq 1$ if and only if $A \leq I$.

Solution: (\implies) Suppose $\|A\| \leq 1$. Then every eigenvalue λ of A is such that $\lambda \in [0, 1]$. This implies the eigenvalues of $I - A$, which are given by $1 - \lambda$ are also in this range. In particular, $I - A$ is positive, so $A \leq I$.

(\impliedby) Suppose $A \leq I$, so that $I - A$ is positive. As above, the eigenvalues of $I - A$ are $1 - \lambda$, where λ is an eigenvalue of A . Since both A and $I - A$ are positive, we have

$$1 - \lambda \geq 0 \quad \lambda \geq 0. \quad (8.133)$$

This implies $\lambda \leq 1$ for each λ , so we have $\|A\| \leq 1$.

Exercise 6.8

Let A be a positive matrix. Define a superoperator (linear operator on matrices) by the equation $\mathcal{A}(X) \equiv AX$. Show that \mathcal{A} is positive with respect to the Hilbert-Schmidt inner product. That is, for all X , $\text{tr}(X^\dagger \mathcal{A}(X)) \geq 0$. Similarly, show that the superoperator defined by $\mathcal{A}(X) \equiv XA$ is positive with respect to the Hilbert-Schmidt inner product on matrices.

Solution: Suppose A is positive. Then for any matrix X , both XAX^\dagger and $X^\dagger AX$ are positive. Moreover, the trace of any positive matrix is itself positive. Therefore, the desired result comes from the simple fact that the condition for positivity of \mathcal{A} amounts to taking traces of the above matrices. For the first definition of \mathcal{A} ,

$$\text{tr}(X^\dagger \mathcal{A}(X)) = \text{tr}(X^\dagger AX). \quad (8.134)$$

For the second definition,

$$\text{tr}(X^\dagger \mathcal{A}(X)) = \text{tr}(X^\dagger XA) = \text{tr}(XAX^\dagger) \quad (8.135)$$