Solutions to exercises and problems in "Quantum Computation and Quantum Information: 10th Anniversary Edition"

H. Li (hengyueli@gmail.com)

Version: May 24, 2024

Notation

- C number + matrix $c + \boldsymbol{A}$ is short for $c\boldsymbol{I} + \boldsymbol{A}$.
- $\boldsymbol{A} = c$ is short for $\boldsymbol{A} = c\boldsymbol{I}$.
- $x \overset{N}{=} y$ is short for $x = y (\text{mod } N)$, where $x, y \in$ integers.
- Residue Class $R_x^N = \{x + iN | i \in \text{ integers}\}$

Resource

- Useful online-calculator for matrix calculation
- Online Videos(12 all in Chinese) for introduction to *Number theory*
- Simulator of 1-tape Turing machine

1 Introduction and overview

Exercise: 1.1

(Probabilistic classical algorithm) Suppose that the problem is not to distinguish between the constant and balanced functions with certainty, but rather, with some probability of error $\epsilon < 1/2$. What is the performance of the best classical algorithm for this problem?

At worst, we still need$2^n/2 + 1$ samples. It successfully detects the result with a probability of $P = (1 - \epsilon)^{2^{1-1}+1}$.

Exercise: 1.2

Explain how a device which, upon input of one of two non-orthogonal quantum states $|\psi\rangle$ or

$|\varphi\rangle$ correctly identified the state, could be used to build a device which cloned the states $|\phi\rangle$ and $|\varphi\rangle$, in violation of the no-cloning theorem. Conversely, explain how a device for cloning could be used to distinguish non-orthogonal quantum states.

1. If we can identify the states, say

Problem: 1.1

(Feynman-Gates conversation) Construct a friendly imaginary discussion of about 2000 words between Bill Gates and Richard Feynman, set in the present, on the future of computation. (Comment: You might like to try waiting until you've read the rest of the book before attempting this question. See the 'History and further reading' below for pointers to one possible answer for this question.)

...

Problem: 1.2

What is the most significant discovery yet made in quantum computation and quantum information? Write an essay of about 2000 words for an educated lay audience about the discovery. (Comment: As for the previous problem, you might like to try waiting until you've read the rest of the book before attempting this question.)

...

2 Introduction to quantum mechanic

Short summary of some concepts

- Normal matrix A: $AA^\dagger = A^\dagger A$.
- Positive operators A: $\langle\psi|A|\psi\rangle \geq 0$ (A is automatically Hermitian)
- Positive definted A: $\langle\psi|A|\psi\rangle > 0$
- Spectral Theorem: Normal matrix $A \iff A = \sum a_i |i\rangle\langle i|$.

Exercise: 2.1

(Linear dependence: example) Show that $(1, -1)$, $(1, 2)$ and $(2, 1)$ are linearly dependent.

$$(1, -1) + (1, 2) = (2, 1)$$

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 out put basis $|0\rangle$, $|1\rangle$. Find input and output bases which give rise to a different matrix representation of A.

Short answer For basis $\{|v_i\rangle\} = \{|0\rangle, |1\rangle\}$, the matrix representation of A is $\bar{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. For basis $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$, $\bar{A} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Long answer The matrix representation of an operator is defined by (Eq. (2.12)) $A|v_j\rangle = \sum_i A_{ij}|w_i\rangle$. According to the definition, $A|0\rangle = |1\rangle = \begin{pmatrix} 0 & 1 \end{pmatrix}\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix}$ and $A|1\rangle = |0\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix}$. The matrix representation is directly given by

$$\bar{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

To have a different representation, we expand V by another basis $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$. Following the same procedure we can derive $\bar{A}' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Until now, the "inner products" is not defined. But we will have a more clear view if we use some "future notation" as follows. An equivalent (but more vivid) definition of Eq. (2.12) is given by

$$A = \sum_{ij} A_{ij}|w_i\rangle\langle v_j|,$$

which gives

$$A_{ij} = \langle w_i|A|v_j\rangle = \langle v_i|A|v_j\rangle.$$

Therefore for basis vectors $\{|0\rangle, |1\rangle\}$, we directly write down $\bar{A} = (A_{ij}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

To obtain a different representation of A, according to a unitary transform S, we can chose a new basis $\{v_i'\}$, where$|v_i\rangle = \sum_j S_{ij}^T|v_j\rangle$. The matrix element of A in the new basis is given as

$$A'_{ij} = \langle v_i'|A|v_j'\rangle = \sum_{kl} S_{ik}^\dagger\langle v_k|A|v_l\rangle S_{lj} = \left(S^\dagger AS\right)_{ij}$$

For example, we chose $S = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, the new basis vectors are $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$, correspondingly the matrix representation of A is $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

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.

According to the definition $A|v_j\rangle = \sum_i A_{ij}|w_i\rangle$, and $B|w_j\rangle = \sum_i B_{ij}|x_i\rangle$, we have

$$\begin{aligned} BA|v_j\rangle &= B\sum_i A_{ij}|w_i\rangle = \sum_i A_{ij}\left(B|w_i\rangle\right) = \sum_i A_{ij}\sum_k B_{ki}|x_k\rangle \\ &= \sum_{ik} B_{ki}A_{ij}|x_k\rangle = \sum_k \left(\sum_i B_{ki}A_{ij}\right)|x_k\rangle = \sum_k \left(\bar{B}\bar{A}\right)_{kj}|x_k\rangle, \end{aligned}$$

where $\bar{*}$ represents the matrix representation. We see that the rule BA is the same as the matrix product $\bar{B}\bar{A}$.

Exercise: 2.4

(Matrix representation for 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*.

The element I_{ij} represent the transformation between $|i\rangle$ and $|j\rangle$. According to the definition, it is 0 for $i \neq j$. Therefore $I_{ij} = \delta_{ij}$.

Exercise: 2.5

Verify that $(\cdot,\cdot)$ just defined is an inner production C^n.

For $|y\rangle = \begin{pmatrix} y_1 \\ ... \\ y_n \end{pmatrix}$ and $|z\rangle = \begin{pmatrix} z_1 \\ ... \\ z_n \end{pmatrix}$, the product defined by $(|y\rangle, |z\rangle) = \sum_i y_i^* z_i$

- requirement 1: $\left(|y\rangle, \sum_i \lambda_i|z_i\rangle\right) = ... \sum_i \lambda_i \left(|v\rangle, |z_i\rangle\right)$
- requirement 2: $(|y\rangle, |z\rangle) = (|z\rangle, |y\rangle)^*$
- requirement 3: $(|y\rangle, |y\rangle) \geq 0$.

Exercise: 2.6

Show that any inner product $(\cdot,\cdot)$ is conjugate-linear in the first argument,

$$\left(\sum_i \lambda_i |w_i\rangle, |v\rangle\right) = \sum_i \lambda_i^* \left(|w_i\rangle, |v\rangle\right).$$

$$\left(\sum_i \lambda_i |w_i\rangle, |v\rangle\right) \xrightarrow{\text{req. 2}} \left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right)^* \xrightarrow{\text{req. 1}} \left(\sum_i \lambda_i \left(|v\rangle, |w_i\rangle\right)\right)^*$$
$$= \sum_i \lambda_i^* \left(|v\rangle, |w_i\rangle\right)^* = \sum_i \lambda_i^* \left(|w_i\rangle, |v\rangle\right)$$

Exercise: 2.7

Verify that $|w\rangle \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $|v\rangle \equiv \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ are orthogonal. What are the normalized forms of these vectors?

- $\frac{|w\rangle}{\sqrt{\langle w|w\rangle}} = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$
- $\frac{|v\rangle}{\sqrt{\langle v|v\rangle}} = (\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$

Exercise: 2.8

Prove that the Gram–Schmidt procedure produces an orthonormal basis for V.

Basis set $\{|w_i\rangle\}$ expand V. Gram-Schmidt procedure:

$$|v_k\rangle = \frac{|x_k\rangle}{\sqrt{\langle x_k|x_k\rangle}},$$

where $|x_k\rangle = |w_k\rangle - \sum_{i=1}^{k-1} \langle v_i|w_k\rangle |v_i\rangle$. Apparently, if $\alpha = \beta$, we have$\langle v_\alpha|v_\beta\rangle = 1$ (since $|v_k\rangle$ is normalized from $|x_k\rangle$). We use induction method to prove the remaining part. Apparently, $\langle v_1|v_2\rangle = \langle v_2|v_1\rangle = 0$. Assume that for any $i, j \leq d$ we have $\langle v_i|v_j\rangle = \delta_{ij}$. Then for any $j \leq d$, we have

$$\langle v_j|v_{d+1}\rangle = \frac{1}{\sqrt{\langle x_{d+1}|x_{d+1}\rangle}} \left(\langle v_j|w_{d+1}\rangle - \sum_{i=1}^{d} \langle v_i|w_{d+1}\rangle \langle v_j|v_i\rangle\right)$$
$$\xrightarrow{\langle v_i|v_j\rangle = \delta_{ij}} \frac{1}{\sqrt{\langle x_{d+1}|x_{d+1}\rangle}} \left(\langle v_j|w_{d+1}\rangle - \langle v_j|w_{d+1}\rangle\right) = 0.$$

therefore we have proved that for any $i, j \leq d+1$, we have $\langle v_i|v_j\rangle = \delta_{ij}$. Done!

Exercise: 2.9

(Pauli operators and the outer product) The Pauli matrices (Figure 2.2 on page 65) can be considered as operators with respect to an orthonormal basis $|0\rangle$, $|1\rangle$ for a two-dimensional Hilbert space. Express each of the Pauli operators in the outer product notation.

- $X = |1\rangle\langle 0| + |0\rangle\langle 1|$
- $Y = i|1\rangle\langle 0| - i|0\rangle\langle 1|$
- $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$

Exercise: 2.10

Suppose $|v_i\rangle$ is an orthonormal basis for an inner product space V . What is the matrix representation for the operator $|v_j\rangle\langle v_k|$, with respect to the $|v_i\rangle$ basis?

The matrix element of $|v_j\rangle\langle v_k|$ is $A_{\alpha\beta} = \langle v_\alpha|v_j\rangle\langle v_k|v_\beta\rangle = \delta_{\alpha j}\delta_{\beta k}$. Therefore A has matrix element 1 at (row,column)=(j,k) and 0 at all other positions.

Exercise: 2.11

(Eigendecomposition of the Pauli matrices) Find the eigenvectors, eigenvalues, and diagonal representations of the Pauli matrices X, Y ,and Z.

Method 1 Solving eigen-equation $P|v_\lambda\rangle = \lambda|v_\lambda\rangle$ with $P = X, Y, Z$ respectively to obtain

$$|x = \pm 1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix}$$
$$|y = \pm 1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm i \end{pmatrix}$$
$$|z = \pm 1\rangle = \begin{pmatrix} \delta_{z1} \\ 1 - \delta_{z1} \end{pmatrix}.$$

The diagonal representation is $P = |p = 1\rangle\langle p = 1| - |p = -1\rangle\langle p = -1|$.

Method 2 For a general operator P with its eigensystem $\{|\psi_i\rangle, p_i\}$, its diagonal representation is $P = S^\dagger \tilde{P} S$, where $\tilde{P}$ is diagonal. According to the eigen-equation

$$P|\psi_i\rangle = S^\dagger \tilde{P} S|\psi_i\rangle = p_i|\psi_i\rangle,$$

we have $\tilde{P}S|\psi\rangle = p_i S|\psi\rangle$, according to which we can write down the matrix of S is

$$S = \begin{pmatrix} \langle\psi_0| \\ ... \\ \langle\psi_{d-1}| \end{pmatrix}$$

For Pauli matrices $P(= X, Y, Z)$, since $P^2 = 1$ we know that the eigenvalues are $\{\pm 1\}$. Therefore we have $P = S^\dagger \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} S$. The diagonal representation is written as $P = |p = 1\rangle\langle p = 1| - |p = -1\rangle\langle p = -1|$

- For $P = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $|x = \pm 1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix}$, $S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.
- For $P = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $|y = \pm 1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm i \end{pmatrix}$, $S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}$.
- For $P = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $|z = \pm 1\rangle = \begin{pmatrix} \delta_{z1} \\ 1 - \delta_{z1} \end{pmatrix}$, $S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{1}$.

Exercise: 2.12

Prove that the matrix $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$is not diagonalizable.

Assume that the matrix can be diagonalized by $U = e^{i\theta} \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix}$,where $|\alpha|^2 + |\beta|^2 = 1$. We have

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} \alpha^* & -\beta \\ \beta^* & \alpha \end{pmatrix} = \begin{pmatrix} \alpha\lambda_1 & \beta\lambda_2 \\ -\beta^*\lambda_1 & \alpha^*\lambda_2 \end{pmatrix} \begin{pmatrix} \alpha^* & -\beta \\ \beta^* & \alpha \end{pmatrix} \\ &= \begin{pmatrix} |\alpha|^2\lambda_1 + |\beta|^2\lambda_2 & -\alpha\beta\lambda_1 + \alpha\beta\lambda_2 \\ -\beta^*\alpha^*\lambda_1 + \alpha^*\beta^*\lambda_2 & |\beta|^2\lambda_1 + |\alpha|\lambda_2 \end{pmatrix}. \end{aligned}$$

We can see that there is no solution of U.

Exercise: 2.13

If $|w\rangle$ and $|v\rangle$ are any two vectors, show that $(|w\rangle\langle v|)^\dagger = |v\rangle\langle w|$.

Let $A = |w\rangle\langle v|$, we have

$$\begin{aligned} (|x\rangle, A|y\rangle) &= \delta_{xw}\delta_{yv} \\ (A^\dagger|x\rangle, |y\rangle) &= (|y\rangle, A^\dagger|x\rangle)^* = (\langle y|A^\dagger|x\rangle)^*. \end{aligned}$$

Since the definition of $A^\dagger$ is by $(|x\rangle, A|y\rangle) = (A^\dagger|x\rangle, |w\rangle)$, we obtain that $\langle y|A^\dagger|x\rangle = \delta_{xw}\delta_{yv}$. That is $A^\dagger = |v\rangle\langle w|$.

Exercise: 2.14

(Anti-linearity of the adjoint) Show that the adjoint operation is anti-linear,

$$\left(\sum_i a_i A_i\right)^\dagger = \sum_i a_i^* A_i^\dagger.$$

$$\begin{aligned}
&\left(\left(\sum_i a_i A_i\right)^\dagger |v\rangle, |w\rangle\right) \\
&\xrightarrow{\text{by definition}} \left(|v\rangle, \sum_i a_i A_i |w\rangle\right) \\
&\xrightarrow{\text{requirement 1 of inner product}} \sum_i a_i \left(|v\rangle, A_i|w\rangle\right) \\
&\xrightarrow{\text{by definition}} \sum_i a_i \left(A_i^\dagger |v\rangle, |w\rangle\right) \\
&\xrightarrow[\text{(Exercise 2.6)}]{\text{conjugate-linear}} \left(\sum_i a_i^* A_i^\dagger |v\rangle, |w\rangle\right)
\end{aligned}$$

Therefore $(\sum_i a_i A_i)^\dagger = \sum_i a_i^* A_i^\dagger$.

Exercise: 2.15

Show that $\left(A^\dagger\right)^\dagger = A$.

$$\left(|v\rangle, \left(A^\dagger\right)^\dagger |w\rangle\right) = \left(\left(A^\dagger\right)^\dagger |w\rangle, |v\rangle\right)^* = \left(|w\rangle, A^\dagger|v\rangle\right)^* = \left(A^\dagger|v\rangle, |w\rangle\right) = \left(|v\rangle, A|w\rangle\right)$$

Therefore $\left(A^\dagger\right)^\dagger = A$.

Exercise: 2.16

Show that any projector P satisfies the equation $P^2 = P$.

$$P^2 = \sum_i |i\rangle\langle i| \sum_j |j\rangle\langle j| = \sum_{ij} \delta_{ij} |i\rangle\langle j| = P$$

Exercise: 2.17

Show that a normal matrix is Hermitian if and only if it has real eigenvalues.

For a given normal matrix N, we have $NN^\dagger = N^\dagger N$. According to the spectra decomposition, $N = \sum_i n_i |i\rangle\langle i|$. If $N = N^\dagger$, $N - N^\dagger = \sum_i (n_i - n_i^*)|i\rangle\langle i| = 0$. Therefore $\{n_i\}$ are all real.

Exercise: 2.18

Show that all eigenvalues of a unitary matrix have modulus 1, that is, can be written in the form $e^{i\theta}$ for some real θ.

For U that $U|\psi\rangle = \rho e^{i\theta}|\psi\rangle$, we have $\langle\psi|U^\dagger U|\psi\rangle = \langle\psi|U^\dagger U|\psi\rangle = 1 = \rho^2$. Therefore $\rho = 1$.

Exercise: 2.19

(Pauli matrices: Hermitian and unitary) Show that the Pauli matrices are Hermitian and unitary.

For $i = 1, 2, 3$, one can check that $\sigma_i^\dagger = \sigma_i$ and $\sigma_i^2 = 1$.

Exercise: 2.20

(Basis changes) Suppose $A\prime$ and $A\prime\prime$ are matrix representations of an operator A on a vector space V with respect to two different orthonormal bases, $|v_i\rangle$ and $|w_i\rangle$. Then the elements of $A\prime$ and $A\prime\prime$ are $A'_{ij} = \langle v_i|A|v_j\rangle$ and $A''_{ij} = \langle w_i|A|w_j\rangle$. Characterize the relationship between $A\prime$ and $A\prime\prime$.

$$\begin{aligned} A''_{ij} = \langle w_i|A|w_j\rangle &= \sum_{\alpha\beta} \langle w_i|v_\alpha\rangle\langle v_\alpha|A|v_\beta\rangle\langle v_\beta|w_j\rangle \\ &= \sum_{\alpha\beta} \langle w_i|v_\alpha\rangle A'_{\alpha\beta}\langle v_\beta|w_j\rangle \end{aligned}$$

Exercise: 2.21-2.22

Show that the eigenvalues of a projector P are all either 0 or 1.

A projector is represented as $P = |\psi\rangle\langle\psi|$, therefore $P^2 = P$. According to the eigen-equation of P ($P|\psi\rangle = p|\psi\rangle$), we have

$$P^2|\psi\rangle = p^2|\psi\rangle = p|\psi\rangle. \tag{1}$$

Therefore we have $p^2 = p$, whose solution is $p = 0/1$.

Exercise: 2.24

(Hermiticity of positive operators) Show that a positive operator is necessarily Hermitian. (Hint: Show that an arbitrary operator A can be written $A = B + iC$ where B and C are Hermitian.)

For any matrix A, we can write it as $A = B + iC$, where $B = \frac{1}{2}\left(A + A^\dagger\right)$ and $C = \frac{i}{2}\left(A^\dagger - A\right)$. One can check that B and C are Hermitian. If A is positive operator, $\langle\psi|A|\psi\rangle = \langle\psi|B|\psi\rangle + i\langle\psi|C|\psi\rangle \geq 0$. Therefore we immediately know that $C = 0$, therefore $A = A^\dagger$.

Exercise: 2.25

Show that for any operator A, $A^\dagger A$ is positive.

$$\langle\psi|A^\dagger A|\psi\rangle = \sum_i \langle\psi|A^\dagger|i\rangle\langle i|A|\psi\rangle = \sum_i |\langle i|A|\psi\rangle|^2 \geq 0.$$

Exercise: 2.26

Let $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Write out $|\psi\rangle^{\otimes 2}$ and $|\psi\rangle^{\otimes 3}$ explicitly, both in terms of tensor products like $|0\rangle\ |1\rangle$, and using the Kronecker product.

From $|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, we have

$$|\psi\rangle^{\otimes 2} = \frac{1}{\sqrt{2}}\begin{pmatrix} |\psi\rangle \\ |\psi\rangle \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

and

$$|\psi\rangle^{\otimes 3} = |\psi\rangle^{\otimes 2} \otimes |\psi\rangle = \frac{1}{2}\begin{pmatrix} |\psi\rangle \\ |\psi\rangle \\ |\psi\rangle \\ |\psi\rangle \end{pmatrix} = \frac{1}{2\sqrt{2}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}^T$$

Exercise: 2.27

Calculate the matrix representation of the tensor products of the Pauli operators (a) X and Z; (b) I and X; (c) X and I. Is the tensor product commutative?

$$X \otimes Z = \begin{pmatrix} 0 & Z \\ Z & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

$$I \otimes X = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$X \otimes I = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

The tensor product is not commutative.

Exercise: 2.28

Show that the transpose, complex conjugation, and adjoint operations distribute over the tensor product,

$$(A \otimes B)^* = A^* \otimes B^*; (A \otimes B)^T = A^T \otimes B^T; (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger.$$

$$(A \otimes B)^* = \begin{pmatrix} A_{11}B & A_{12}B & ... \\ A_{21}B & ... & \\ ... & & \end{pmatrix}^* = \begin{pmatrix} A_{11}^*B^* & A_{12}^*B^* & ... \\ A_{21}^*B^* & ... & \\ ... & & \end{pmatrix} = A^* \otimes B^*$$

$$(A \times B)^T = ... = A^T \otimes B^T$$

$$(A \otimes B)^\dagger = ... = A^\dagger \otimes B^\dagger$$

Exercise: 2.29

Show that the tensor product of two unitary operators is unitary.

For $AA^\dagger = BB^\dagger = 1$,

$$(A \otimes B)(A \otimes B)^\dagger = (A \otimes B)\left(A^\dagger \otimes B^\dagger\right) = \left(AA^\dagger \otimes BB^\dagger\right) = (I \otimes I)$$

Exercise: 2.30

Show that the tensor product of two Hermitian operators is Hermitian.

For $A = A^\dagger$ and $B = B^\dagger$

$$(A \otimes B)^\dagger = \left(A^\dagger \otimes B^\dagger\right) = (A \otimes B)$$

Exercise: 2.31

Show that the tensor product of two positive operators is positive.

For $\langle a|A|a\rangle \geq 0$ and $\langle b|B|b\rangle \geq 0$,

$$\langle a| \otimes \langle b| (A \otimes B) |a\rangle \otimes |b\rangle = \langle a|A|a\rangle\langle b|B|b\rangle \geq 0.$$

Exercise: 2.32

Show that the tensor product of two projectors is a projector.

For two given projectors $p_1 = |\psi\rangle\langle\psi|$ and $p_2 = |\phi\rangle\langle\phi|$in space V, the tensor product

$$P = p_1 \otimes p_2 = |\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|$$

is a projector in space $V \otimes V$.

Exercise: 2.33

The Hadamard operator on one qubit may be written as

$$H = \frac{1}{\sqrt{2}} \left[(|0\rangle + |1\rangle) \langle 0| + (|0\rangle - |1\rangle) \langle 1| \right].$$

Show explicitly that the Hadamard transform on n qubits, $H^{\otimes n}$, may be written as

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} |x\rangle\langle y|.$$

The H gate on the i-th qubit can be written as

$$H = \frac{1}{\sqrt{2}} \sum_{x_i=0}^{1} \sum_{y_i=0}^{1} (-1)^{\delta_{x_i 1}\delta_{y_i 1}} |x_i\rangle\langle y_i|.$$

Therefore we have

$$\begin{aligned} H^{\otimes n} &= \frac{1}{\sqrt{2^n}} \sum_{x_0} ... \sum_{x_{n-1}} \sum_{y_0} ... \sum_{y_{n-1}} (-1)^{\left(\delta_{x_0,1}\delta_{y_0,1}+...+\delta_{x_{n-1},1}\delta_{y_{n-1},1}\right)} |x_0...x_{n-1}\rangle\langle y_0...y_{n-1}| \\ &= \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{\left(\delta_{x_0,1}\delta_{y_0,1}+...+\delta_{x_{n-1},1}\delta_{y_{n-1},1}\right)} |x\rangle\langle y| \\ &= \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{\left(\delta_{x_0,y_0}\delta_{x_0,1}+...\delta_{x_{n-1},y_{n-1}}\delta_{x_{n-1},1}\right)} |x\rangle\langle y| \\ &= \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x\cdot y} |x\rangle\langle y|. \end{aligned}$$

Exercise: 2.34

Find the square root and logarithm of the matrix

$$A = \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}.$$

$A = \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} = S^\dagger \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix} S$, where $S = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$. Eigenstates are $|\psi_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}$ and $|\psi_7\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Therefore we have

$$f(A) = f(1)|\psi_1\rangle\langle\psi_1| + f(7)|\psi_7\rangle\langle\psi_7| = \frac{1}{2} \begin{pmatrix} f(7)+f(1) & f(7)-f(1) \\ f(7)-f(1) & f(7)+f(1) \end{pmatrix}.$$

By $f(A)$ we can calculate any function,

$$\sqrt{A} = \frac{1}{2} \begin{pmatrix} \sqrt{7}+1 & \sqrt{7}-1 \\ \sqrt{7}-1 & \sqrt{7}+1 \end{pmatrix}$$

$$\log(A) = \frac{\log 7}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Exercise: 2.35

(Exponential of the Pauli matrices) Let $\vec{v}$ be any real, three-dimensional unit vector and θ a real number. Prove that

$$\exp(i\theta\vec{v}\cdot\vec{\sigma}) = \cos(\theta) + i\sin(\theta)\,\vec{v}\cdot\vec{\sigma}$$

where $\vec{v}\cdot\vec{\sigma} \equiv \sum_{i=1}^{3} v_i\sigma_i$. This exercise is generalized in Problem 2.1 on page 117.

First we prove that $\sigma_v^2 = 1$, where $\sigma_v \equiv \boldsymbol{v} \cdot \boldsymbol{\sigma} = \sum_{i=1}^{3} v_i \sigma_i$. Since $\boldsymbol{v}$ is a unit vector, we can represent it as $\boldsymbol{v} = (\sin\vartheta\cos\phi, \sin\vartheta\sin\phi, \cos\vartheta)$. Therefore we have

$$\begin{aligned}
\sigma_v^2 &= (\sigma_x \sin\vartheta\cos\phi + \sigma_y \sin\vartheta\sin\phi + \sigma_z\cos\vartheta)^2 \\
&= \sin^2\vartheta\cos^2\phi + \sin^2\vartheta\sin^2\phi + \cos^2\vartheta \\
&+ \sin^2\vartheta\cos\phi\sin\phi(\sigma_x\sigma_y + \sigma_y\sigma_x) \\
&+ \sin\vartheta\cos\phi\cos\vartheta(\sigma_x\sigma_z + \sigma_z\sigma_x) \\
&+ \sin\vartheta\cos\vartheta\sin\phi(\sigma_y\sigma_z + \sigma_z\sigma_y) \\
&= 1.
\end{aligned}$$

Then we have

$$\begin{aligned}
e^{i\theta\sigma_v} &= \sum_n \frac{(i\theta\sigma_v)^2}{n!} = \sum_n \frac{(i\theta\sigma_v)^{2n}}{(2n)!} + \sum_n \frac{(i\theta\sigma_v)^{2n+1}}{(2n+1)!} \\
&= \sum_n \frac{(-1)^n\theta^{2n}}{(2n)!} + i\sigma_v \sum_n \frac{(-1)^2\theta^{2n+1}}{(2n+1)!} = \cos\theta + i\sigma_v\sin\theta
\end{aligned}$$

Exercise: 2.36

Show that the Pauli matrices except for I have trace zero.

tr(σ_i)=0 for $i = x, y, z$. tr$I$=2 .

Exercise: 2.37

(Cyclic property of the trace) If A and B are two linear operators show that

$$\mathrm{tr}\,(AB) = \mathrm{tr}\,(BA)\,.$$

$$tr(AB) = \sum_i \langle i|AB|i\rangle = \sum_{ij} \langle i|A|j\rangle\langle j|B|i\rangle = \sum_j \langle j|B\left(\sum_i |i\rangle\langle i|\right)A|j\rangle = tr(BA).$$

Exercise: 2.38

(Linearity of the trace) If A and B are two linear operators, show that

$$\mathrm{tr}\,(A+B) = \mathrm{tr}\,(A) + \mathrm{tr}\,(B)$$

and if z is an arbitrary complex number show that

$$\mathrm{tr}\left(zA\right) = z\mathrm{tr}\left(A\right).$$

$$\mathrm{tr}\left(A+B\right) = \sum_i \langle i|\left(A+B\right)|i\rangle = \sum_i \langle i|A|i\rangle + \sum_i \langle i|B|i\rangle = \mathrm{tr}\left(A\right) + \mathrm{tr}\left(B\right).$$

$$\mathrm{tr}\left(zA\right) \quad = \quad \sum_i \langle i|zA|i\rangle \quad = \quad z\sum_i \langle i|A|i\rangle \quad = \quad z\mathrm{tr}\left(A\right)$$

Exercise: 2.39

(The Hilbert–Schmidt inner product on operators) The set L_V of linear operators on a Hilbert space V is obviously a vector space – the sum of two linear operators is a linear operator, zA is a linear operator if A is a linear operator and z is a complex number, and there is a zero element 0. An important additional result is that the vector space L_V can be given a natural inner product structure, turning it into a Hilbert space.

(1) Show that the function $(\cdot,\,\cdot)$ on $L_V \times L_V$ defined by

$$(A,B) \quad \equiv \quad \mathrm{tr}\left(A^\dagger B\right)$$

is an inner product function. This inner product is known as the Hilbert–Schmidt or trace inner product.

(2) If V has d dimensions show that L_V has dimension d^2.

(3) Find an orthonormal basis of Hermitian matrices for the Hilbert space L_V.

(1)

- requirement 1 for inner product:

$$(A, \sum_i \lambda_i B_i) = tr(A^\dagger \sum_i \lambda_i B_i) = tr(\sum_i \lambda_i A^\dagger B_i) = \sum_i \lambda_i tr(A^\dagger B_i) = \sum_i (A, B_i)$$

- requirement 2 for inner product:

$$\begin{aligned}(A,B) = tr(A^\dagger B) = \sum_{ij} \langle i|A^\dagger|j\rangle\langle j|B|i\rangle = \left(\sum_{ij} \langle i|B^\dagger|j\rangle\langle j|A|i\rangle\right)^* \\ = \left(tr(B^\dagger A)\right)^* = (B,A)^*\end{aligned}$$

- requirement 3 for inner product:

$$\begin{aligned}(A,A) = tr(A^\dagger A) = \sum_{ij} \langle i|A^\dagger|j\rangle\langle j|A|i\rangle \\ = \sum_{ij} |\langle j|A|i\rangle|^2 \geq 0 \end{aligned} \tag{2}$$

(2) Chose a set of orthonormal basis $\{|i\rangle|i = 1, 2, ..., d\}$, we define a set of basis in $L_v \times L_v$ as $\{|i\rangle\langle j||i, j = 1, 2, ..., d\}$. We can prove that this set of basis is also orthonormal since $(|i\rangle\langle j|, |\alpha\rangle\langle\beta|) = \delta_{\alpha i}\delta_{j\beta}$ and $\sum_{ij} (|i\rangle\langle j|)^\dagger (|i\rangle\langle j|)^\dagger = 1$. Any element in this space can be expanded by this set of basis. The dimension is therefore d^2.

(3) For any Hermitian matrix H, we can find a diagonal decomposition as $H = \sum_i h_i|i\rangle\langle i|$. Then $\{|i\rangle\}$ is what we want.

Exercise: 2.40

(Commutation relations for the Pauli matrices) Verify the commutation relations

$$[X, Y] = 2iZ; [Y, Z] = 2iX; [Z, X] = 2iY.$$

There is an elegant way of writing this using ϵ_{jkl}, the antisymmetric tensor on three indices, for which $\epsilon_{jkl} = 0$ except for $\epsilon_{123} = \epsilon_{231} = \epsilon_{312} = 1$, and $\epsilon_{321} = \epsilon_{213} = \epsilon_{132} = -1$:

$$[\sigma_j, \sigma_k] = 2i \sum_{l=1}^{3} \epsilon_{jkl}\sigma_l.$$

...

Exercise: 2.41

(Anti-commutation relations for the Pauli matrices) Verify the anti-commutation relations

$$\{\sigma_i, \sigma_j\} = 0$$

where $i \neq j$ are both chosen from the set $1, 2, 3$. Also verify that $(i = 0, 1, 2, 3)$

$$\sigma_i^2 = 1.$$

...

Exercise: 2.42

Verify that

$$AB = \frac{[A, B] + \{A, B\}}{2}.$$

$$AB = \frac{2AB + BA - BA}{2} = \frac{(AB + BA) + (AB - BA)}{2} = \frac{[A, B] + \{A, B\}}{2}.$$

Exercise: 2.43

Show that for $j, k = 1, 2, 3$,

$$\sigma_j \sigma_k = \delta_{jk} + i \sum_{l=1}^{3} \epsilon_{jkl} \sigma_l.$$

$$\begin{aligned}
\sigma_j \sigma_k &= \left[\delta_{jk} + (1 - \delta_{jk})\right] \sigma_j \sigma_k \\
&= \delta_{jk} + (1 - \delta_{jk}) \frac{\sigma_j \sigma_k - \sigma_k \sigma_j}{2} \\
&= \delta_{jk} + (1 - \delta_{jk}) \frac{[\sigma_j, \sigma_k]}{2} \\
&\xrightarrow{Exercise 2.40} \delta_{jk} + i\,(1 - \delta_{jk}) \sum_{l=1}^{3} \epsilon_{jkl} \sigma_l \\
&= \delta_{jk} + i \sum_{l=1}^{3} \epsilon_{jkl} \sigma_l
\end{aligned}$$

Exercise: 2.44

Suppose $[A, B] = 0$, $\{A, B\} = 0$, and A is invertible. Show that B must be 0.

Since $[A, B] = AB - BA = 0$ we know that $AB = BA$. Because A is invertible, we have $B = ABA^{-1}$ (multiply A^{-1} at both side). Similarly, from $\{A, B\} = 0$ we can obtain $B = -ABA^{-1}$. Therefore $B = -B$ which means $B = 0$.

Exercise: 2.45

Show that $[A, B]^\dagger = [B^\dagger, A^\dagger]$.

$$[A, B]^\dagger = (AB - BA)^\dagger = (AB)^\dagger - (BA)^\dagger = B^\dagger A^\dagger - A^\dagger B^\dagger = [B^\dagger, A^\dagger].$$

Exercise: 2.46

Show that $[A, B] = -[B, A]$.

$$[A, B] = AB - BA = -(BA - AB) = -[B, A].$$

Exercise: 2.47

Suppose A and B are Hermitian. Show that $i[A, B]$ is Hermitian.

Let $H = i[A, B]$,we have

$$H^\dagger = -i[A,B]^\dagger \xrightarrow{Exercise 2.45} -i[B^\dagger, A^\dagger] \xrightarrow{Exercise 2.46} i[A^\dagger, B^\dagger] \xrightarrow{\text{A,B are Hermitian}} i[A,B] = H.$$

Exercise: 2.48

What is the polar decomposition of a positive matrix P? Of a unitary matrix U? Of a Hermitian matrix, H?

For any operator A, the polar decomposition gives $A = UJ = KU$.
If $A = P$, $P = IP = PI$. That is $U = K = I$ and $J = K = P$.
If $A = u$, $u = Iu = uI$. That is $U = K = u$ and $J = K = I$.
If $A = A^\dagger$, we use a diagonal representation of $A = \sum a_i |i\rangle\langle i|$, where the a_i is real. Therefore J is given by $J = \sum_i \lambda_i |i\rangle\langle i|$, where $\lambda_i = |a_i|$. Then we have $|e_i\rangle = \frac{1}{\lambda_i} A|i\rangle = \text{sign}(a_i)|i\rangle$, and correspondingly $U = \sum_i |e_i\rangle\langle i| = \sum_i \text{sign}(a_i)|i\rangle\langle i|$. And finally $K = UJU^\dagger = J$.

Exercise: 2.49

Express the polar decomposition of a normal matrix in the outer product representation.

For a given normal matrix N, according to the spectral theorem, we have $N = \sum_i^d n_i |i\rangle\langle i|$. We can write the eigen-values as $n_i = \rho_i e^{i\alpha_i}$. Therefore we can write down

$$J = \sum_i \sqrt{|n_i|^2} |i\rangle\langle i| = \sum_i \rho_i |i\rangle\langle i|,$$

We define that $|e_i\rangle = \frac{1}{\lambda_i} N|i\rangle = e^{i\alpha_i}|i\rangle$. For the case $d \leq D$, where D is the dimension of the inner product space, expand the set $\{e_i\}$ to the whole space. Therefore we have

$$U = \sum_i |e_i\rangle\langle i| = \sum_i e^{i\alpha_i} |i\rangle\langle i|,$$

and $K = UJU^\dagger = J$.

Exercise: 2.50

Find the left and right polar decompositions of the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

For $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$,

$$A^\dagger A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = a_+|+\rangle\langle+| + a_-|-\rangle\langle-|,$$

where $a_\pm = \frac{3\pm\sqrt{5}}{2}$, and $|+\rangle = \frac{\sqrt{2}}{\sqrt{5-\sqrt{5}}}\begin{pmatrix} 1 \\ \frac{\sqrt{5}-1}{2} \end{pmatrix}, |-\rangle = \sqrt{\frac{\sqrt{2}}{5+\sqrt{5}}}\begin{pmatrix} 1 \\ -\frac{\sqrt{5}+1}{2} \end{pmatrix}$. Then we have

$$J = \sqrt{A^\dagger A} = \lambda_+|+\rangle\langle+| + \lambda_-|-\rangle\langle-|,$$

where $\lambda_\pm = \sqrt{\frac{3\pm\sqrt{5}}{2}}$ and $|e_\pm\rangle = \frac{1}{\lambda_\pm}A|\pm\rangle = |\pm\rangle$. Therefore $U = |+\rangle\langle+| + |-\rangle\langle-|$, and $K = UJU^\dagger = J$.

Exercise: 2.51

Verify that the Hadamard gate H is unitary.

...

Exercise: 2.52

Verify that $H^2 = I$.

...

Exercise: 2.53

What are the eigenvalues and eigenvectors of H?

$$|+1\rangle = \frac{1}{\sqrt{4+2\sqrt{2}}}\begin{pmatrix} 1+\sqrt{2} \\ 1 \end{pmatrix}$$
$$|-1\rangle = \frac{1}{\sqrt{4-2\sqrt{2}}}\begin{pmatrix} 1-\sqrt{2} \\ 1 \end{pmatrix}$$

Exercise: 2.54

Suppose A and B are commuting Hermitian operators. Prove that $\exp(A)\exp(B) = \exp(A+B)$. (Hint: Use the results of Section 2.1.9.)

We expand $\exp(A+B)$ as

$$\exp(A+B) = \sum_m \frac{(A+B)^m}{m!} \xrightarrow{[A,B]=0} \sum_m \frac{1}{m!}\sum_{k=0}^{m}\begin{pmatrix} m \\ k \end{pmatrix} A^k B^{m-k} = \sum_m \sum_{k=0}^{m} \frac{1}{k!(m-k)!} A^k B^{m-k}$$

let $F_{AB}(k, m-k) \equiv \frac{1}{k!(m-k)!} A^k B^{m-k}$, then we have

$$\begin{aligned}
\exp(A+B) &= \sum_m \sum_{k=0}^{m} F_{AB}(k, m-k) \\
&= \underbrace{(F_{AB}(0,0))}_{m=0} + \underbrace{(F_{AB}(0,1) + F_{AB}(1,0))}_{m=1} + \underbrace{(F_{AB}(0,2) + F_{AB}(1,1) + F_{AB}(2,0))}_{m=2} + ... \\
&= \sum_k F_{AB}(0,k) + \sum_k F_{AB}(1,k) + \sum_k F_{AB}(2,k) ... \\
&= \sum_{km} F_{AB}(k,m) = \sum_{mk} \frac{1}{k!m!} A^k B^m = \exp(A)\exp(B).
\end{aligned}$$

Exercise: 2.55

Prove that $U(t_1, t_2) \equiv \exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]$ defined in Equation (2.91) is unitary.

We can calculate that $U^\dagger(t_1, t_2) = \exp\left[\frac{iH^\dagger(t_2-t_1)}{\hbar}\right] = U^{-1}(t_1, t_2) = U(t_2, t_1)$.

Exercise: 2.56

Use the spectral decomposition to show that $K \equiv -i \log(U)$ is Hermitian for any unitary U , and thus $U = \exp(iK)$ for some Hermitian K.

For any unitary matrix U, we can find a decomposition $U = \sum_i u_i |i\rangle\langle i|$ since U is also a normal matrix. From $UU^\dagger = 1$ we know that $u_i = e^{i\theta_i}$ for some real number θ_i. Therefore we have $K = -i \ln U = \sum_i \theta_i |i\rangle\langle i|$ and K is Hermitian. By the same spirit, we can prove the inverse relation.

Exercise: 2.57

(Cascaded measurements are single measurements) Suppose $\{L_l\}$ and $\{M_m\}$ are two sets of measurement operators. Show that a measurement defined by the measurement operators $\{L_l\}$ followed by a measurement defined by the measurement operators $\{M_m\}$ is physically equivalent to a single measurement defined by measurement operators $\{N_{lm}\}$ with the representation $N_{lm} \equiv M_m L_l$.

After the measurement of $\{L_l\}$ on an initial state $|\psi\rangle$, the probability of outcome l is $p(L=l) = \langle\psi|L_l^\dagger L_l|\psi\rangle$. The state after the measurement is $|\psi'\rangle = \frac{L_l|\psi\rangle}{\sqrt{\langle\psi|L_l^\dagger L_l|\psi\rangle}}$. Then we apply the measurement of $\{M_m\}$. The probability of outcome m is

$$p(M=m) = \langle\psi'|M_m^\dagger M_m|\psi'\rangle = \langle\psi|\left(M_m L_l\right)^\dagger \left(M_m L_l\right)|\psi\rangle.$$

The output state of the measurement of $\{M_m\}$ is

$$|\psi''\rangle = \frac{M_m|\psi'\rangle}{\sqrt{\langle\psi'|M_m^\dagger M_m|\psi'\rangle}} = \frac{M_m L_l|\psi\rangle}{\langle\psi|L_l^\dagger M_m^\dagger M_m L_l|\psi\rangle}$$
$$= \frac{(M_m L_l)\,|\psi\rangle}{\langle\psi|\,(M_m L_l)^\dagger\,(M_m L_l)\,|\psi\rangle}.$$

According to the definition of measurement, the state $|\psi''\rangle$ can be seen as an output of the measurement $\{M_m L_l\}$.

Exercise: 2.58

Suppose we prepare a quantum system in an eigenstate $|\psi\rangle$ of some observable M , with corresponding eigenvalue m. What is the average observed value of M , and the standard deviation?

$$\langle M\rangle = m$$
$$\Delta M = 0$$

Exercise: 2.59

Suppose we have qubit in the state $|0\rangle$, and we measure the observable X. What is the average value of X? What is the standard deviation of X?

$$\langle X\rangle = \langle 0|X|0\rangle = 0.$$

$$\Delta X = \sqrt{\langle X^2\rangle - \langle X\rangle^2} = 1.$$

Exercise: 2.60

Show that $\vec{v}\cdot\vec{\sigma}$ has eigenvalues ± 1, and that the projectors onto the corresponding eigenspaces are given by $P_\pm = (1 + \vec{v}\cdot\vec{\sigma})/2$.

Let $A = \boldsymbol{v}\cdot\boldsymbol{\sigma}$, the eigen-equation is given by $A|\psi\rangle = a|\psi\rangle$. One can check that $A^2 = 1$, therefore

$$|\psi\rangle = A^2|\psi\rangle = A\,(A|\psi\rangle) = aA|\psi\rangle = a^2|\psi\rangle,$$

which means $a^2 = 1$, so the eigenvalues are $\{+1, -1\}$. The corresponding eigenvectors can be represented as $\{|+\rangle, |-\rangle\}$. By the diagonal representation of $A = |+\rangle\langle+| - |-\rangle\langle-|$ and the completeness of the projector:

$$\begin{cases} |+\rangle\langle+| - |-\rangle\langle-| = P_+ - P_- \\ 1 = P_+ + P_- \end{cases},$$

we have

$$P_\pm = (1 \pm A)/2.$$

Exercise: 2.61

Calculate the probability of obtaining the result +1 for a measurement of $\vec{v}\cdot\vec{\sigma}$, given that the state prior to measurement is $|0\rangle$. What is the state of the system after the measurement if +1 is obtained?

$$\boldsymbol{v}\cdot\boldsymbol{\sigma} = \sigma_x \sin\theta\cos\phi + \sigma_y \sin\theta\sin\phi + \sigma_z\cos\theta = \begin{pmatrix} \cos\theta & \sin\theta e^{-i\phi} \\ \sin\theta e^{i\phi} & -\cos\theta \end{pmatrix} = |+\rangle\langle+| - |-\rangle\langle-|,$$

where

$$\begin{cases} |+\rangle = \begin{pmatrix} \cos\frac{\theta}{2}e^{-i\frac{\phi}{2}} \\ \sin\frac{\theta}{2}e^{i\frac{\phi}{2}} \end{pmatrix} \\ |-\rangle = \begin{pmatrix} \sin\frac{\theta}{2}e^{-i\frac{\phi}{2}} \\ -\cos\frac{\theta}{2}e^{i\frac{\phi}{2}} \end{pmatrix} \end{cases}.$$

Therefore we have

$$\text{Prob}(\boldsymbol{v}\cdot\boldsymbol{\sigma} \text{ on } —0\rangle \text{ is } 0) = |\langle+|0\rangle|^2 = \cos^2\frac{\theta}{2}$$

After measurement if +1 is obtained, the state must be $|+\rangle$.

Exercise: 2.62

Show that any measurement where the measurement operators and the POVM elements coincide is a projective measurement.

Assume now that there is a quantum measurement $\{M_m\}$. The corresponding POVM is $E_m = M_m^\dagger M_m$. If $E_m = M_m$, that is $M_m^\dagger M_m = M_m$, we have $\sum_m M_m = \sum_m E_m = 1$. On the other hand, if $M_m^\dagger M_n \neq \delta_{mn} M_n$, we have $M_m^\dagger M_m \neq \delta_{mm} M_m$. It can conclude that M_m is a projector.

Exercise: 2.63

Suppose a measurement is described by measurement operators M_m. Show that there exist unitary operators U_m such that $M_m = U_m\sqrt{E_m}$, where E_m is the POVM associated to the measurement.

According to the polar decomposition, $M_m = U_m J$, where $J = \sqrt{M_m^\dagger M_m} = \sum_i \lambda_i |i\rangle\langle i|$.

Exercise: 2.64

Suppose Bob is given a quantum state chosen from a set $|\psi_1\rangle$,..,$|\psi_m\rangle$ of linearly independent states. Construct a POVM $\{E_1, E_2, ..., E_{m+1}\}$ such that if outcome E_i occurs, $1 \leq i \leq m$, then Bob knows with certainty that he was given the state $|\psi_i\rangle$. (The POVM must be such

that $\langle\psi_i|E_i|\psi_i\rangle > 0$ for each i.)

For any state $|\psi_i\rangle$ and $|\psi_j\rangle$ in $\{|\psi_i\rangle\}$ with $i \neq j$, $\langle\psi_j|\psi_i\rangle = 0$. If not so, there is no solution (see 2.2.4). Then we define $E_i = \frac{|\psi_i\rangle\langle\psi_i|}{\langle\psi_i|\psi_i\rangle}$ for $i = 1, ..., m$. To make the POVM self-consistent$E_{m+1} = I - \sum_{i=1}^{m} E_i$.

Exercise: 2.65

Express the states $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$ in a basis in which they are not the same up to a relative phase shift.

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{i0}|1\rangle}{\sqrt{2}}$$
$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{i\pi}|1\rangle}{\sqrt{2}}$$

Exercise: 2.66

Show that the average value of the observable $X_1 Z_2$ for a two qubit system measured in the state $(|00\rangle + |11\rangle)/\sqrt{2}$ is zero.

Method 1

$$Z_2 \otimes X_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|0\rangle + |3\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

therefore

$$\langle\psi|Z_2 \otimes X_1|\psi\rangle = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 0.$$

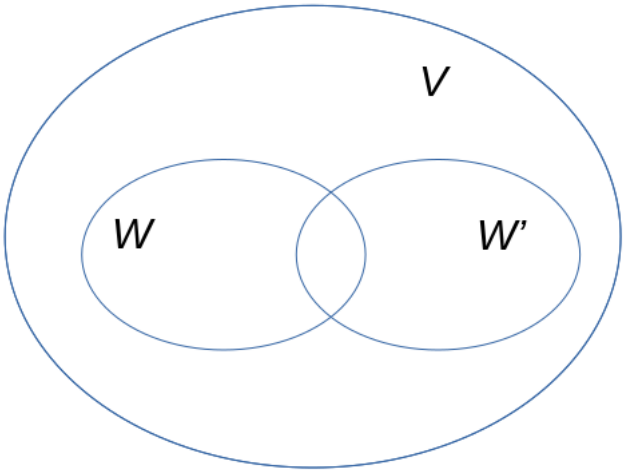


Figure 1:

Method 2

$$\begin{aligned}\langle\psi|X_1Z_2|\psi\rangle &= \frac{1}{2}\left(\langle 00| + \langle 11|\right)X_1Z_2\left(|00\rangle + |11\rangle\right)\\ &= \frac{1}{2}\left(\langle 0|\otimes\langle 0| + \langle 1|\otimes\langle 1|\right)\left(X_1|0\rangle\otimes Z_2|0\rangle + X_1|1\rangle\otimes Z_2|1\rangle\right)\\ &= \frac{1}{2}\left(\langle 0|\otimes\langle 0| + \langle 1|\otimes\langle 1|\right)\left(|1\rangle\otimes|0\rangle - |0\rangle\otimes|1\rangle\right)\\ &= 0.\end{aligned}$$

Exercise: 2.67

Suppose V is a Hilbert space with a subspace W. Suppose $U : W \to V$ is a linear operator which preserves inner products, that is, for any $|w_1\rangle$ and $|w_w\rangle$ in W,

$$\langle w_1|U^\dagger U|w_2\rangle = \langle w_1|w_2\rangle.$$

Prove that there exists a unitary operator $U\prime : V \to V$ which *extends* U . That is, $U'|w\rangle = U|w\rangle$ for all $|w\rangle$ in W, but $U\prime$ is defined on the entire space V. Usually we omit the prime symbol ´ and just write U to denote the extension.

The whole space V can be split as shown in Fig. 1. Under U, any vector in space W is transferred into W'. Assume that the space W can be expanded by a set of orthogonal basis $\{|\bar{w}_i\rangle|i = 1, ..., d\}$, where $d = \dim(W)$. Then W' can be expanded by $\{U|w_i\rangle\}$, since U preserves inner products. Let us define $X = W \cup W'$. Therefore X can be expanded by $\{|\bar{w}_i\rangle|i = 1, ..., d'\}$, where $d' = d + k$. If $W|\cap W' = \phi$, then we know that $k = d$. The basis $|\bar{w}_i\rangle$ for that $i > d$ is calculated by Gram–Schmidt

process. For example, we calculate $|w_{d+j}\rangle$as follows: First we calculate

$$|\bar{w_j}'\rangle = U|\bar{w_j}\rangle.$$

Then we calculate

$$|\bar{y}_{d+j}\rangle = |\bar{w_j}'\rangle - \sum_{\alpha=1}^{d+j-1} \langle \bar{w_\alpha}|\bar{w_j}'\rangle|\bar{w_\alpha}\rangle.$$

If $|\bar{y}_{d+j}\rangle = 0$, it means that $|\bar{y}_{d+j}\rangle \in W \cap W'$ (see in figure), then we ignore this one and to go find next one directly. If $|\bar{y}_{d+j}\rangle \neq 0$,we can append $|\bar{w}_{d+j}\rangle = \frac{|\bar{y}_{d+j}\rangle}{\sqrt{\langle \bar{y}_{d+j}|\bar{y}_{d+j}\rangle}}$. After we obtain $\{|\bar{w_i}\rangle|i = 1, ..., d'\}$, we continue appending basis to obtain a set to expand V so that we have $\{|\bar{w_i}\rangle|i = 1, ..., D\}$, where $D = \dim(V)$. Then the target operator can be represented by

$$U' = \sum_{i\leq d} |U\bar{w_i}\rangle\langle\bar{w_i}| + \sum_{d<i\leq d'} |U^{-1}\bar{w_i}\rangle\langle\bar{w_i}| + \sum_{i>d'} |\bar{w_i}\rangle\langle\bar{w_i}|.$$

Then U' is an operator defined in the space V.

Exercise: 2.68

Prove that $|\psi\rangle \neq |a\rangle|b\rangle$ for all single qubit states $|a\rangle$ and $|b\rangle$.

If $|\psi\rangle = |a\rangle|b\rangle$, $\langle\psi|\psi\rangle = \frac{\langle 00|+\langle 11|}{\sqrt{2}}|a\rangle|b\rangle = \frac{\delta_{a0}\delta_{b0}+\delta_{a1}\delta_{b1}}{\sqrt{2}} \neq 1$.

Exercise: 2.69

Verify that the Bell basis forms an orthonormal basis for the two qubit state space.

Bell basis can be represented as $\{|B_i\rangle\} = \{U|i\rangle\}$, where $\{|i\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and U represent a Hadamard gate followed by a CNOT gate (with control qubit at the same index as the Hadamard gate). Then for any two Bell state $|B_i\rangle$ and $|B_j\rangle$ we have

$$\langle B_i|B_j\rangle = \langle i|U^\dagger U|j\rangle = \langle i|j\rangle = \delta_{ij}.$$

Exercise: 2.70

Suppose E is any positive operator acting on Alice's qubit. Show that $\langle\psi|E \otimes I|\psi\rangle$ takes the same value when $|\psi\rangle$ is any of the four Bell states. Suppose some malevolent third party ('Eve') intercepts Alice's qubit on the way to Bob in the superdense coding protocol. Can Eve infer anything about which of the four possible bit strings 00, 01, 10, 11 Alice is trying to send? If so, how, or if not, why not?

For $E = E_1|e_1\rangle\langle e_1| + E_2|e_2\rangle\langle e_2|$, the constant value is $\frac{1}{2}(E_1 + E_2)$. (helped by 20230511_1.py)

Exercise: 2.71

(Criterion to decide if a state is mixed or pure) Let ρ be a density operator. Show that $tr(\rho^2) \leq 1$, with equality if and only if ρ is a pure state.

Let $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$,

$$tr(\rho^2) = tr(\sum_i p_i^2 |\psi_i\rangle\langle\psi_i|) = \sum_s \sum_i p_i^2 \langle s|\psi_i\rangle\langle\psi_i|s\rangle$$
$$= \sum_s \sum_i p_i^2 \langle\psi_i|s\rangle\langle s|\psi_i\rangle = \sum_i p_i^2$$

since $\sum_i p_i = 1$ and $p_i^2 < p_i$, we have $tr(\rho^2) = \sum_i p_i^2 \leq \sum_i p_i = 1$.

Exercise: 2.72

(Bloch sphere for mixed states) The Bloch sphere picture for pure states of a single qubit was introduced in Section 1.2. This description has an important generalization to mixed states as follows.

(1) Show that an arbitrary density matrix for a mixed state qubit may be written as

$$\rho = \frac{1 + \vec{r} \cdot \vec{\sigma}}{2},$$

where $\vec{r}$ is a real three-dimensional vector such that $|r| \leq 1$. This vector is known as the *Bloch vector* for the state ρ.

(2) What is the Bloch vector representation for the state $\rho = \frac{1}{2}$?

(3) Show that a state ρ is pure if and only if $|\vec{r}| = 1$.

(4) Show that for pure states the description of the Bloch vector we have given coincides with that in Section 1.2.

(1)

The general form of the density matrix of a single qubit is $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. According to the completeness of the Pauli matrix, any 2×2 matrix ($|\psi_i\rangle\langle\psi_i|$) can be decomposed by Pauli matrix as

$$|\psi_i\rangle\langle\psi_i| = c_{i0} + \frac{c_{ix}}{2}\sigma_x + \frac{c_{iy}}{2}\sigma_y + \frac{c_{iz}}{2}\sigma_z.$$

We have

$$tr(|\psi_i\rangle\langle\psi_i|) = 1 = tr(c_{i0} + \frac{c_{ix}}{2}\sigma_x + \frac{c_{iy}}{2}\sigma_y + \frac{c_{iz}}{2}\sigma_z).$$

Since $tr(\sigma_i) = 0$, we have $c_{i0} = \frac{1}{2}$. And according to

$$tr((|\psi_i\rangle\langle\psi_i|)^2) = 1 = tr\left(c_{i0}^2 + \frac{c_{ix}^2 + c_{iy}^2 + c_{iz}^2}{4} + ...\right)$$

we have $2(\frac{1}{4}+\frac{c_{ix}^2+c_{iy}^2+c_{iz}^2}{4})=1$, therefore $c_{ix}^2+c_{iy}^2+c_{iz}^2=1$. Therefore $\boldsymbol{r}_i=(c_{ix},c_{iy},c_{iz})$ is a unite vector in $O(3)$. Therefore we can represent the density matrix as

$$\rho=\sum_i p_i(\frac{1}{2}+\frac{1}{2}\boldsymbol{r}_i\cdot\boldsymbol{\sigma})=\frac{1+\boldsymbol{r}\cdot\boldsymbol{\sigma}}{2},$$

where $\boldsymbol{r}=\sum_i p_i\boldsymbol{r}_i$. One can check that $|\boldsymbol{r}|\leq 1$.

(2)

$\boldsymbol{r}=0$.

(3)

$|\boldsymbol{r}|=|\sum_i p_i\boldsymbol{r}_i|\leq\sum_i p_i|\boldsymbol{r}_i|=1$. (hint: for a triangle, $a+b>c$)

(4)

For $\boldsymbol{r}=(\sin\theta\cos\phi,\sin\theta\sin\phi,\cos\theta)$,

$$\begin{aligned}\rho&=\frac{1}{2}\begin{pmatrix}\cos\theta+1 & \sin\theta e^{-i\phi}\\ \sin\theta e^{i\phi} & -\cos\theta+1\end{pmatrix}=\begin{pmatrix}\cos^2\frac{\theta}{2} & \sin\frac{\theta}{2}\cos\frac{\theta}{2}e^{-i\phi}\\ \sin\frac{\theta}{2}\cos\frac{\theta}{2}e^{i\phi} & \sin^2\frac{\theta}{2}\end{pmatrix}\\&=|\psi\rangle\langle\psi|,\end{aligned}$$

where

$$|\psi\rangle=\begin{pmatrix}\cos\frac{\theta}{2}e^{i\frac{\phi}{2}}\\ \sin\frac{\theta}{2}e^{-i\frac{\phi}{2}}\end{pmatrix}.$$

Exercise: 2.73

Let ρ be a density operator. A *minimal ensemble* for ρ is an ensemble $\{p_i,|\psi_i\rangle\}$ containing a number of elements equal to the rank of ρ. Let $|\psi\rangle$ be any state in the support of ρ. (The support of a Hermitian operator A is the vector space spanned by the eigenvectors of A with non-zero eigenvalues.) Show that there is a minimal ensemble for ρ that contains $|\psi\rangle$, and more over that in any such ensemble $|\psi\rangle$ must appear with probability

$$p_i=\frac{1}{\langle\psi_i|\rho^{-1}|\psi_i\rangle},$$

where ρ^{-1} is defined to be the inverse of ρ, when ρ is considered as an operator acting only on the support of ρ. (This definition removes the problem that ρ may not have an inverse.)

Since $\rho^\dagger=\rho$, we can find the diagonal representation of

$$\rho=\sum_{i=1}^{d}p_i|\psi_i\rangle\langle\psi_i|+\sum_{j=1}^{k}\lambda_j|\phi_j\rangle\langle\phi_j|,$$

where all $p_i > 0$ and $\lambda_j \leq 0$. This is a minimal ensemble of ρ, and $d + k = R$, where R is the rank of ρ. The inverse of ρ is given by

$$\rho^{-1} = \sum_{i=1}^{d} p_i^{-1} |\psi_i\rangle\langle\psi_i| + \sum_{j=1}^{k} \lambda_j^{-1} |\phi_j\rangle\langle\phi_j|,$$

by which we can easily obtain that $p_i^{-1} = \langle\psi_i|\rho^{-1}|\psi_i\rangle$.

Exercise: 2.74

Suppose a composite of systems A and B is in the state $|a\rangle|b\rangle$, where $|a\rangle$ is a pure state of system A, and $|b\rangle$ is a pure state of system B. Show that the reduced density operator of system A alone is a pure state.

$\rho' = tr_B(|a\rangle|b\rangle\langle a|\langle b|) = |a\rangle\langle a|$, $\rho'^2 = 1$. done.

Exercise: 2.75

For each of the four Bell states, find the reduced density operator for each qubit.

For all state, $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ and $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, the reduced density matrix is (they are the same)

$$\mathrm{tr}_i \rho = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Exercise: 2.76

Extend the proof of the Schmidt decomposition to the case where A and B may have state spaces of different dimensionality.

Without loss of generality, assume that $\dim(A) > \dim(B)$. For any state $|\psi\rangle = \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} c_{ij} |i\rangle|j\rangle$, the matrix c (whose element is c_{ij}) is decomposed as $c = U^T D V$. Therefore by unitary transformation of A by U and B by V, we have

$$|i'_A\rangle = \sum_{j=1}^{d_A} U_{ij} |j_A\rangle$$

$$|i'_B\rangle = \sum_{j=1}^{d_B} V_{ij} |j_B\rangle.$$

Therefore

$$\begin{aligned} |\psi\rangle &= \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} \sum_{k=1}^{d_A} \sum_{l=1}^{d_B} U_{ik}^T D_{kk} \delta_{kl} V_{lj} |i\rangle|j\rangle \\ &= \sum_{k=1}^{d_A} \sum_{l=1}^{d_B} |k'_A\rangle D_{kk} \delta_{kl} |l'_B\rangle = \sum_{k=1}^{d_B} D_{kk} |k'_A\rangle|k'_B\rangle \end{aligned}$$

Exercise: 2.77

Suppose ABC is a three component quantum system. Show by example that there are quantum states $|\psi\rangle$ of such systems which can not be written in the form

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle |i_C\rangle,$$

where λ_i are real numbers, and $|i_A\rangle, |i_B\rangle, |i_C\rangle$ are orthonormal bases of the respective systems.

An example Consider the 3-qubit linear cluster state

$$\begin{aligned} |C_3\rangle &= CZ_{01}CZ_{12}H_0H_1H_2|000\rangle \\ &= \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle + |111\rangle\right). \end{aligned}$$

There is no way to write it in the form of $|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle |i_C\rangle$.

Exercise: 2.78

Prove that a state $|\psi\rangle$ of a composite system AB is a product state if and only if it has Schmidt number 1. Prove that $|\psi\rangle$ is a product state if and only if ρ^A (and thus ρ^B) are pure states.

For $|\psi\rangle = \sum_{i=1}^K \lambda_i |i\rangle |i\rangle$, we calculate the reduced density matrix of A as

$$\begin{aligned} \rho_A &= tr_B \left(\sum_{ij=1}^K \lambda_i \lambda_j^* |i\rangle\langle j| \otimes |i\rangle\langle j| \right) \\ &= \sum_{ij=1}^K \lambda_i \lambda_j^* |i\rangle\langle j| \delta_{ij} = \sum_{i=1}^K |\lambda_i|^2 |i\rangle\langle i|. \end{aligned}$$

If $K > 1$, we know that ρ_A is a mix state (similar to Exercise 2.71 we can prove that $tr(\rho_A^2) < 1$ if $K > 1$). Therefore $|\psi\rangle$ is an entanglement state (not a product state).

Exercise: 2.79

Consider a composite system consisting of two qubits. Find the Schmidt decompositions of the states

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}; \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{\sqrt{2}}; \text{ and} \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}}.$$

$\frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

For two qubit state $|\psi\rangle = \sum q_{ij}|i\rangle|j\rangle$, q is a 2×2 matrix. By SVD decomposition, we have $q = U^T D V$, therefore $|\psi\rangle = \sum_k D_{kk} \left(\sum_i U_{ki}|i\rangle\right) \left(\sum_j V_{kj}|j\rangle\right)$.

- For $q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.
- For $q = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$, $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$,$D = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$, $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}}$.
- For $q = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $U = ..., D =, ..., V =, ...$

$$|\psi\rangle = \sqrt{\frac{1}{6}(3+\sqrt{5})}\,(0.85...|0\rangle + 0.52...|1\rangle)\,(0.85...|0\rangle + 0.52...|1\rangle) + \sqrt{\frac{1}{6}(3-\sqrt{5})}\,(0.52...|0\rangle - 0.85...|1\rangle)\,(0.85...|0\rangle - 0.52...|1\rangle)$$

Exercise: 2.80

Suppose $|\psi\rangle$ and $|\varphi\rangle$ are two pure states of a composite quantum system with components A and B, with identical Schmidt coefficients. Show that there are unitary transformations U on system A and V on system B such that $|\psi\rangle = (U \otimes V)\,|\varphi\rangle$.

For $|\psi\rangle = \sum_{i=1}^{k} \lambda_i |\chi_A^i\rangle|\chi_B^i\rangle$, $|\varphi\rangle = \sum_{i=1}^{k} \lambda_i |\xi_A^i\rangle|\xi_B^i\rangle$. We define U such that $U\{|\xi_A^i\rangle\} = \{|\chi_A^i\rangle\}$. To be more specific:

$$\begin{pmatrix} |\xi_A^1\rangle \\ |\xi_A^2\rangle \\ ... \end{pmatrix} \xrightarrow{U} \begin{pmatrix} |\chi_A^1\rangle \\ |\chi_A^2\rangle \\ ... \end{pmatrix}.$$

This is possible, for example in the basis of $\{|\xi_A^i\rangle\}$ we have $|\chi_A^\alpha\rangle = \sum_j c_{\alpha j}|\xi_A^j\rangle$. Notice that $\{c_{\alpha j}\}$ are known values. Then, according to the definition, $U|\xi_A^l\rangle = |\chi_A^l\rangle$. Therefore the matrix element is given by

$$U_{kl} = \langle\xi_A^k|U|\xi_A^l\rangle = \langle\psi_A^k|\chi_A^l\rangle = \sum_j c_{lj}\langle\xi_A^k|\xi_A^j\rangle = c_{lk}.$$

Likewise, we can define V such that $V|\xi_B^k\rangle = |\chi_B^k\rangle$. Then we have

$$U \otimes V|\psi\rangle = \sum_{i=1}^{k} \lambda_i U|\xi_A^i\rangle V|\xi_B^i\rangle = \sum_{i=1}^{k} \lambda_i |\chi_A^i\rangle|\chi_B^i\rangle = |\psi\rangle.$$

Exercise: 2.81

(Freedom in purifications) Let $|AR_1\rangle$ and $|AR_2\rangle$ be two purifications of a state ρ_A to a composite system AR. Prove that there exists a unitary transformation U_R acting on system R such that $|AR_1\rangle = (I_A \otimes U_R)\,|AR_2\rangle$.

For an existed purification $|AR\rangle = \sum_i \sqrt{p_i}|i^A\rangle|i^R\rangle$, we chose an arbitrary unitary operator U in the space R. Then we have $|AR'\rangle = \sum_i \sqrt{p_i}|i^A\rangle U|i^R\rangle$. The reduced density matrix is

$$\begin{aligned}\rho &= tr_R(|AR'\rangle\langle AR'|) = tr_R(\sum_{ij}\sqrt{p_ip_j}|i^A\rangle\langle j^A|\otimes U|i^R\rangle\langle j^R|U^\dagger)\\ &= \sum_{ij}\sqrt{p_ip_j}|i^A\rangle\langle j^A|tr\left(U|i^R\rangle\langle j^R|U^\dagger\right)\\ &= \sum_{ij}\sqrt{p_ip_j}|i^A\rangle\langle j^A|tr\left(|i^R\rangle\langle j^R|U^\dagger U\right)\\ &= \sum_{ij}p_i|i^A\rangle\langle i^A| = \rho_A.\end{aligned}$$

Exercise: 2.82

Suppose $\{p_i, |\psi_i\rangle\}$ is an ensemble of states generating a density matrix $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ for a quantum system A. Introduce a system R with orthonormal basis $|i\rangle$.

(1) Show that $\sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle$ is a purification of ρ.

(2) Suppose we measure R in the basis $|i\rangle$, obtaining outcome i. With what probability do we obtain the result i, and what is the corresponding state of system A?

(3) Let $|AR\rangle$ be any purification of ρ to the system AR. Show that there exists an orthonormal basis $|i\rangle$ in which R can be measured such that the corresponding post-measurement state for system A is $|\psi_i\rangle$ with probability p_i.

(1) $tr_R(|AR\rangle\langle AR|) = ... = \rho$.

(2) Use the notation $|\Psi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle$. $M_i = |i\rangle\langle i|$

The corresponding probability $P = \langle\Psi|M_i^\dagger M_i|\Psi\rangle = p_i$. The corresponding state is

$$\frac{M_i|\Psi\rangle}{\sqrt{\langle\Psi|M_i^\dagger M_i|\Psi\rangle}} = |\psi_i\rangle|i\rangle.$$

(3) For any purification of ρ that $|\Phi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle|i'\rangle$, according to the result in Exercise 2.81, we can find a unitary transformation U so that $|i\rangle = \sum_j U_{ij}|j'\rangle$. Then the required measurement is

$$M_i' = |i'\rangle\langle i'| = \sum_j\sum_k U_{ij}^\dagger U_{ji}|j\rangle\langle k|.$$

Problem: 2.1

(Functions of the Pauli matrices) Let $f(\cdot)$ be any function from complex numbers to complex

numbers. Let $\vec{n}$ be a normalized vector in three dimensions, and let θ be real. Show that

$$f(\theta\vec{n}\cdot\vec{\sigma}) = \frac{f(\theta)+f(-\theta)}{2} + \frac{f(\theta)-f(-\theta)}{2}\vec{n}\cdot\vec{\sigma}.$$

Use notation $\sigma_n \equiv \vec{n}\cdot\vec{\sigma} = \sigma_x \sin\theta\cos\phi + \sigma_y \sin\theta\sin\phi + \sigma_z\cos\theta$, one can check that

$$\sigma_n^2 = (\sigma_x \sin\theta\cos\phi + \sigma_y \sin\theta\sin\phi + \sigma_z\cos\theta)^2 = ... = 1.$$

From relation

$$\begin{cases} f(\theta) = \sum_k \frac{f^{(k)}(0)}{k!}\theta^k = \sum_k \frac{f^{(2k)}(0)}{2k!}\theta^{2k} + \sum_k \frac{f^{(2k+1)}(0)}{(2k+1)!}\theta^{2k+1} \\ f(-\theta) = \sum_k \frac{f^{(k)}(0)}{k!}(-\theta)^k = \sum_k \frac{f^{(2k)}(0)}{2k!}\theta^{2k} - \sum_k \frac{f^{(2k+1)}(0)}{(2k+1)!}\theta^{2k+1} \end{cases}$$

we have $\frac{f(\theta)+f(-\theta)}{2} = \sum_k \frac{f^{(2k)}(0)}{2k!}\theta^{2k}$ and $\frac{f(\theta)-f(-\theta)}{2} = \sum_k \frac{f^{(2k+1)}(0)}{(2k+1)!}\theta^{2k+1}$. The original expression is rewritten as

$$\begin{aligned} f(\theta\vec{n}\cdot\vec{\sigma}) &= \sum_k \frac{f^{(k)}(0)}{k!}(\theta\sigma_n)^k \\ &= \sum_k \frac{f^{(2k)}(0)}{(2k)!}(\theta\sigma_n)^{2k} + \sum_k \frac{f^{(2k+1)}(0)}{(2k+1)!}(\theta\sigma_n)^{2k+1} \\ &\xrightarrow{\sigma_n^2=1} \sum_k \frac{f^{(2k)}(0)}{(2k)!}\theta^{2k} + \theta\sigma_n \sum_k \frac{f^{(2k+1)}(0)}{(2k+1)!}\theta^{2k} \\ &= \frac{f(\theta)+f(-\theta)}{2} + \theta\sigma_n \sum_k \frac{f(\theta)-f(-\theta)}{2} \end{aligned}$$

Problem: 2.2

(Properties of the Schmidt number) Suppose $|\psi\rangle$ is a pure state of a composite system with components A and B.

(1) Prove that the Schmidt number of $|\psi\rangle$ is equal to the rank of the reduced density matrix $\rho_A \equiv \mathrm{tr}_B(|\psi\rangle\langle\psi|)$. (Note that the rank of a Hermitian operator is equal to the dimension of its support.)

(2) Suppose $|\psi\rangle = \sum_j |\alpha_j\rangle|\beta_j\rangle$ is a representation for $|\psi\rangle$, where $|\alpha_j\rangle$ and $|\beta_j\rangle$ are (unnormalized) states for systems A and B, respectively. Prove that the number of terms in such a decomposition is greater than or equal to the Schmidt number of $|\psi\rangle$, $\mathrm{Sch}(\psi)$.

(3) Suppose $|\psi\rangle = \alpha|\varphi\rangle + \beta|\gamma\rangle$. Prove that

$$\mathrm{Sch}(\psi) \geq |\mathrm{Sch}(\varphi) - \mathrm{Sch}(\gamma)|.$$

(1)

The system state is expanded as$|\psi\rangle = \sum_{i=1}^{d_A}\sum_{j=1}^{d_B}\xi_{ij}|a_i\rangle|b_j\rangle$. The $d_A \times d_B$ matrix ξ_{ij} can be written as (SVD decomposition):

$$\boldsymbol{\xi} = U\boldsymbol{\Lambda}V^{\dagger},$$

where U $(d_A \times d_A)$ and $V(d_B \times d_B)$ are unitary. The diagonal matrix $\boldsymbol{\Lambda}(d_A \times d_B)$ has N_s non-zero values. $N_s = \mathrm{Sch}(\psi)$ is the Schmidt number of $|\psi\rangle$ since

$$\begin{aligned}
|\psi\rangle &= \sum_{ij}\sum_{\alpha\beta} U_{i\alpha}\Lambda_{\alpha\alpha}\delta_{\alpha\beta}V^{\dagger}_{\beta j}|a_i\rangle|b_j\rangle \\
&= \sum_{\alpha=1}^{N_s}\Lambda_{\alpha\alpha}\left(\sum_i U_{i\alpha}|a_i\rangle\right)\left(\sum_j V^{\dagger}_{\alpha j}|b_j\rangle\right) \\
&\equiv \sum_{\alpha=1}^{N_s}\Lambda_{\alpha\alpha}|A_\alpha\rangle|B_\alpha\rangle. \qquad (3)
\end{aligned}$$

The density matrix of the composed system is given by $\rho = |\psi\rangle\langle\psi| = \sum_{\alpha=1}^{N_s}\sum_{\beta=1}^{N_s}\Lambda_{\alpha\alpha}\Lambda_{\beta\beta}|A_\alpha\rangle\langle A_\beta|\otimes |B_\alpha\rangle\langle B_\beta|$. Therefore the reduced density matrix is given by

$$\begin{aligned}
\rho_A = tr_B(\rho) &= \sum_{x=1}^{d_B}\sum_{\alpha=1}^{N_s}\sum_{\beta=1}^{N_s}\Lambda_{\alpha\alpha}\Lambda_{\beta\beta}|A_\alpha\rangle\langle A_\beta|\langle x|B_\alpha\rangle\langle B_\beta|x\rangle \\
&= \sum_{\alpha=1}^{N_s}\sum_{\beta=1}^{N_s}\Lambda_{\alpha\alpha}\Lambda_{\beta\beta}|A_\alpha\rangle\langle A_\beta|\left(\langle B_\beta|\sum_{x=1}^{d_B}|x\rangle\langle x|B_\alpha\rangle\right) \\
&= \sum_{\alpha=1}^{N_s}\sum_{\beta=1}^{N_s}\Lambda_{\alpha\alpha}\Lambda_{\beta\beta}|A_\alpha\rangle\langle A_\beta|\left(\sum_k\sum_j V^{*}_{j\alpha}V_{k\beta}\langle b_k|b_j\rangle\right) \\
&= \sum_{\alpha=1}^{N_s}\sum_{\beta=1}^{N_s}\Lambda_{\alpha\alpha}\Lambda_{\beta\beta}|A_\alpha\rangle\langle A_\beta|\left(\sum_j V^{\dagger}_{\alpha j}V_{j\beta}\right) \\
&= \sum_{\alpha=1}^{N_s}\Lambda^2_{\alpha\alpha}|A_\alpha\rangle\langle A_\alpha|
\end{aligned}$$

It shows that $Rank(\rho_A) = N_s$ too.

(2)

(3)

not yet

Problem: 2.3

(Tsirelson's inequality) Suppose $Q = \vec{q}\cdot\vec{\sigma}$, $R = \vec{r}\cdot\vec{\sigma}$, $S = \vec{s}\cdot\vec{\sigma}$, $T = \vec{t}\cdot\vec{\sigma}$, where $\vec{q}, \vec{r}, \vec{s}$ and $\vec{t}$ are real unit vectors in three dimensions. Show that

$$(Q\otimes S + R\otimes S + R\otimes T - Q\otimes T)^2 = 4I + [Q,R]\otimes[S,T].$$

Use this result to prove that

$$\langle Q\otimes S\rangle + \langle R\otimes S\rangle + \langle R\otimes T\rangle - \langle Q\otimes T\rangle \leq 2\sqrt{2},$$

so the violation of the Bell inequality found in Equation (2.230) is the maximum possible in quantum mechanics.

3 Introduction to computer science

Exercise: 3.1

(Non-computable processes in Nature) How might we recognize that a process in Nature computes a function not computable by a Turing machine?

—-

Exercise: 3.2

(Turing numbers) Show that single-tape Turing machine scan each be given a number from the list $1, 2, 3, ...$ in such a way that the number uniquely specifies the corresponding machine. We call this number the Turing number of the corresponding Turing machine. (Hint: Every positive integer has a unique prime factorization $p_1^{a_1}p_2^{a_2}...p_k^{a_k}$, where p_i are distinct prime numbers, and $a_1, ..., a_k$ are non-negative integers.)

Several encoding methods exist. Here, we explore one such solution.

For a given Turing machine with $\Gamma = \{\gamma_1, ..., \gamma_m\}$, $Q = \{q_1, ..., q_n\}$, $R(\text{move direction}) = \{-1, +1, 0\}$ and program lines $\{t_i = \langle q_i^{\text{in}}, s_i^{\text{in}}, q_i^{\text{out}}, s_i^{\text{out}}, r_i\rangle\}$, we use $2m+2n+3$ prime numbers to encode it. The alphabet table is represented by $\Gamma^{\text{in}}_{\text{encode}} = \{p_1, ..., p_m\}$ and $\Gamma^{\text{out}}_{\text{encode}} = \{p_{m+1}, ..., p_{2m}\}$. The state list is represented by $Q^{\text{in}}_{\text{encode}} = \{p'_1, ..., p'_n\}$ and $Q^{\text{out}}_{\text{encode}} = \{p'_{n+1}, ..., p'_{2n}\}$. The move direction is represented by $R_{\text{encode}} = \{p''_1, p''_2, p''_3\}$. Now we discuss how to encode a program line. For example the program line $t = \langle q_i, s_j, q_k, s_l, +1\rangle$ is encoded by follows. $q_i \in \Gamma^{\text{in}}_{\text{encode}}$ is represented by p_i. $s_j \in Q^{\text{in}}_{\text{encode}}$ is represented by p'_j. $q_k \in \Gamma^{\text{out}}_{\text{encode}}$ is represented by p_{m+k}. $s_l \in Q^{\text{out}}_{\text{encode}}$ is represented by p'_{n+l}. And finally $+1 \in R_{\text{encode}}$ is represented by p''_2. The encoded integer for representing this program line is

$$t \to p_i p'_j p_{m+k} p'_{n+1} p''_2 \equiv n.$$

Therefore all program lines $\{t_i\}$ are encoded as $\{n_i\}$. Then we need to combine these numbers into one unique integer. We use Cantor pairing function $\pi(a,b) = \frac{1}{2}(a+b)(a+b+1)+b$ to

combine two number in each time. In 3-number combining case, we define $\pi_3(a,b,c) = \pi(\pi(a,b),c)$. In the same spirit, we can define $\pi_L(n_1,...,n_L)$. We further pack m, n and L into it to obtain $X = \pi_{L+3}(n_1,...,n_L,m,n,L)$. The number X is the Turing number we want.

We give an given example to encode the Turing machine in section 3.1.1 (the constant function $f(x) = 1$). The tape character $\Gamma = \{\triangleright, 0, 1, b\}$. Therefore we have $\Gamma^{\text{in}}_{\text{encode}} = \{2,3,5,7\}$ and $\Gamma^{\text{out}}_{\text{encode}} = \{11,13,17,19\}$. The internal state $Q = \{q_s, q_1, q_2, q_3, q_h\}$. Therefore we have $Q^{\text{in}}_{\text{encode}} = \{23,29,31,37,41\}$ and $Q^{\text{out}}_{\text{encode}} = \{43,47,53,59,61\}$. And finally $R_{\text{encode}} = \{67,71,73\}$. All program lines are encoded as follows:

$$
\begin{aligned}
l_1 &= \langle q_s, \triangleright, q_1, \triangleright, +1\rangle \to 23\times 2\times 47\times 11\times 71 = 1688522\\
l_2 &= \langle q_1, 0, q_1, b, +1\rangle \to 29\times 3\times 47\times 19\times 71 = 5516061\\
l_3 &= \langle q_1, 1, q_1, b, +1\rangle \to 29\times 5\times 47\times 19\times 71 = 9193435\\
l_4 &= \langle q_1, b, q_2, b, -1\rangle \to 29\times 7\times 53\times 19\times 67 = 13696207\\
l_5 &= \langle q_2, b, q_2, b, -1\rangle \to 31\times 7\times 53\times 19\times 67 = 14640773\\
l_6 &= \langle q_2, \triangleright, q_3, \triangleright, +1\rangle \to 31\times 2\times 59\times 11\times 71 = 2856898\\
l_7 &= \langle q_3, b, q_h, 1, 0\rangle \to 37\times 7\times 61\times 17\times 73 = 19606559.
\end{aligned}
$$

The Truing number is given by

$$X = \pi_{10}(l_1,...,l_7,4,5,7) = \underbrace{1859...385}_{\text{length:3358}}.$$

Now we see an example of decoding a number. Let

$X = 4863896654282922388473526966848622409226853627872654674695277046657116858034740536872537321127377700962626034044192812679101005881401297524667979407683784331818718031.$

Since $\pi^{-1}(X) = (986295...41589, 3)$, we know that there are 3 program lines. Then parameters are decoded by

$$\pi_6^{-1}(X) = (131054, 163618, 128535, 2, 3, 3).$$

Then we write down $\Gamma^{\text{in/out}}_{\text{encode}} = \{2,3\}/\{5,7\}$, $Q^{\text{in/out}}_{\text{encode}} = \{11,13,17\}/\{19,23,29\}$ and $R_{\text{encode}} = \{31,37,41\}$. Each program line, represented by large integers, can be parsed by factorization as follows:

$$
\begin{aligned}
131054 &= 2\times 11\times 7\times 23\times 37\\
163618 &= 2\times 13\times 7\times 29\times 31\\
128535 &= 3\times 11\times 5\times 19\times 41
\end{aligned}
$$

We then can write down the Turing machine: $\Gamma = \{\gamma_1, \gamma_2\}$, $Q = \{q_1, q_2, q_3\}$ with program lines:

$$
\begin{aligned}
l_1 &= \langle \gamma_1, q_1, \gamma_2, q_2, +1\rangle\\
l_2 &= \langle \gamma_1, q_2, \gamma_2, q_3, -1\rangle\\
l_3 &= \langle \gamma_2, q_1, \gamma_1, q_1, 0\rangle.
\end{aligned}
$$

We have demonstrated that each single-tape Turing machine can be uniquely identified by an integer, confirming the feasibility of tagging these machines with numbers. However, it remains to be determined whether a precise encoding method exists that can map each Turing machine to an integer in a one-to-one correspondence.

Exercise: 3.3

(Turing machine to reverse a bit string) Describe a Turing machine which takes a binary number x as input, and outputs the bits of x in reverse order. (Hint: In this exercise and the next it may help to use amulti-tape Turing machine and/or symbols other than $\triangleright$, 0, 1 and the blank.)

Method 1: use two-tape Turing machine

1. $\langle q_s, \triangleright, \triangleright, q_1, \triangleright, \triangleright, 1, 0\rangle$ # start: move tape A forward the end, while keep tape B in origin
2. $\langle q_1, 0, \triangleright, q_1, 0, \triangleright, 1, 0\rangle$ # treat $0 \in \Gamma$
3. $\langle q_1, 1, \triangleright, q_1, 1, \triangleright, 1, 0\rangle$ # treat $1 \in \Gamma$
4. $\langle q_1, b, \triangleright, q_2, b, \triangleright, -1, 1\rangle$ # already end of x. Move tape A back, write data into tape B
5. $\langle q_2, 0, b, q_2, 0, 0, -1, 1\rangle$ # treat $0 \in \Gamma$
6. $\langle q_2, 1, b, q_2, 1, 1, -1, 1\rangle$ # treat $1 \in \Gamma$
7. $\langle q_2, \triangleright, b, q_h, \triangleright, b, 0, 0\rangle$ # end

One tape for input and the other one is used for output. If the output must be on the first tape, we need an additional process to copy data from the second tape into the first one. (This code has NOT been tested on a simulator.)

Method 2: use 1-tape Turing machine Use $\Gamma = \{\triangleright, 0, 1, b, d\}$, and state $Q = \{q_s, q_h, q_1, q_{2*}, q_{3*}, q_{4*}, q_5\}$. The following code has been tested on a simulator.

1. $\langle q_s, \triangleright, q_1, \triangleright, 1\rangle$ # start
2. $\langle q_1, 0, q_1, 0, 1\rangle$ # (2-3): move right until end (b)
3. $\langle q_1, 1, q_1, 1, 1\rangle$
4. $\langle q_1, b, q_{21}, d, -1\rangle$ # make end as d
5. $\langle q_{21}, 0, q_{30}, b, 1\rangle$ # state q_{21}: move left and ready to carry data
6. $\langle q_{21}, 1, q_{31}, b, 1\rangle$# (5-6) carry data by state q_{3i} where $i = 0/1$ represent data
7. $\langle q_{21}, b, q_{21}, b, -1\rangle$ # skip b
8. $\langle q_{20}, d, q_{21}, d, -1\rangle$ # q_{20} : move left but not ready for carrying data
9. $\langle q_{20}, 0, q_{20}, 0, -1\rangle$ # at right hand side of d (past regime), do nothing
10. $\langle q_{20}, 1, q_{20}, 1, -1\rangle$
11. $\langle q_{21}, \triangleright, q_5, \triangleright, 1\rangle$ # q_5: no further data need handle, ready to stop

12. $\langle q_5, d, q_5, b, 1\rangle$
13. $\langle q_5, 0, q_h, 0, 0\rangle$ # (13-14): finished. position represent the state of output
14. $\langle q_5, 1, q_h, 1, 0\rangle$
15. $\langle q_5, b, q_5, b, 1\rangle$
16. $\langle q_{30}, b, q_{30}, b, 1\rangle$ # (16-17): carry data and move right
17. $\langle q_{31}, b, q_{31}, b, 1\rangle$
18. $\langle q_{30}, d, q_{40}, d, 1\rangle$ # (18-19): ready to past data
19. $\langle q_{31}, d, q_{41}, d, 1\rangle$
20. $\langle q_{40}, b, q_{20}, 0, -1\rangle$ # (20-21) past data
21. $\langle q_{41}, b, q_{20}, 1, -1\rangle$
22. $\langle q_{40}, 0, q_{40}, 0, 1\rangle$ # (22-25): keep moving while not b
23. $\langle q_{40}, 1, q_{40}, 1, 1\rangle$
24. $\langle q_{41}, 0, q_{41}, 0, 1\rangle$
25. $\langle q_{41}, 1, q_{41}, 1, 1\rangle$

Exercise: 3.4

(Turing machine to add modulo 2) Describe a Turing machine to add two binary numbers x and y modulo 2. The numbers are input on the Turing machine tape in binary, in the form x, followed by a single blank, followed by a y. If one number is not as long as the other then you may assume that it has been padded with leading 0s to make the two numbers the same length.

$\Gamma = \{\triangleright, 0, 1, b, Z, W, E, F\}$ and $Q = \{q_s, q_h, q_{1*}, q_{2*}, q_{3*}...\}$. The ideal is to carry each bit of y to add with x. The following code has been tested on a simulator.

1. $\langle q_s, \triangleright, q_{10}, \triangleright, 1\rangle$ # (1-7) use symbol E and F to split x and y: tape=$[\triangleright, x, E, y, F]$
2. $\langle q_{10}, 0, q_{10}, 0, 1\rangle$
3. $\langle q_{10}, 1, q_{10}, 1, 1\rangle$
4. $\langle q_{10}, b, q_{11}, E, 1\rangle$
5. $\langle q_{11}, 0, q_{11}, 0, 1\rangle$
6. $\langle q_{11}, 1, q_{11}, 1, 1\rangle$
7. $\langle q_{11}, b, q_{20}, F, -1\rangle$

8. $\langle q_{20}, 0, q_{20}, 0, -1\rangle$ (8-11): move cursor to E and start to carry bit in y.
9. $\langle q_{20}, 1, q_{20}, 1, -1\rangle$
10. $\langle q_{20}, b, q_{20}, b, -1\rangle$
11. $\langle q_{20}, E, q_{21}, E, 1\rangle$
12. $\langle q_{21}, b, q_{21}, b, 1\rangle$
13. $\langle q_{21}, 0, q_{30}, b, -1\rangle$ # carry bit(y)=0, move to x
14. $\langle q_{21}, 1, q_{31}, b, -1\rangle$ # carry bit(y)=1, move to x
15. $\langle q_{21}, F, q_7, b, -1\rangle$ # no more bit in y, ready to finish
16. $\langle q_{30}, b, q_{30}, b, -1\rangle$ # (16-28) process to calculate bit(y)=0
17. $\langle q_{31}, b, q_{31}, b, -1\rangle$
18. $\langle q_{30}, E, q_{40}, E, -1\rangle$
19. $\langle q_{31}, E, q_{41}, E, -1\rangle$
20. $\langle q_{40}, 0, q_{40}, 0, -1\rangle$
21. $\langle q_{40}, 1, q_{40}, 1, -1\rangle$
22. $\langle q_{40}, Z, q_{40}, Z, -1\rangle$
23. $\langle q_{40}, W, q_{40}, W, -1\rangle$
24. $\langle q_{40}, \triangleright, q_{50}, \triangleright, 1\rangle$
25. $\langle q_{50}, Z, q_{50}, Z, 1\rangle$
26. $\langle q_{50}, W, q_{50}, W, 1\rangle$
27. $\langle q_{50}, 0, q_6, Z, 1\rangle$ # (27-28) bit $0 \oplus 1$
28. $\langle q_{50}, 1, q_6, W, 1\rangle$
29. $\langle q_6, 0, q_6, 0, 1\rangle$
30. $\langle q_6, 1, q_6, 1, 1\rangle$
31. $\langle q_6, Z, q_6, Z, 1\rangle$
32. $\langle q_6, W, q_6, W, 1\rangle$
33. $\langle q_6, E, q_{21}, E, 1\rangle$
34. $\langle q_{31}, 0, q_{31}, 0, -1\rangle$ #(34-44) process to calculate bit(y)=1, similar to (16-28)
35. $\langle q_{41}, 0, q_{41}, 0, -1\rangle$

36. $\langle q_{41}, 1, q_{41}, 1, -1\rangle$
37. $\langle q_{41}, Z, q_{41}, Z, -1\rangle$
38. $\langle q_{41}, W, q_{41}, W, -1\rangle$
39. $\langle q_{41}, \triangleright, q_{51}, \triangleright, 1\rangle$
40. $\langle q_{51}, b, q_{51}, b, 1\rangle$
41. $\langle q_{51}, Z, q_{51}, Z, 1\rangle$
42. $\langle q_{51}, W, q_{51}, W, 1\rangle$
43. $\langle q_{51}, 0, q_6, W, 1\rangle$
44. $\langle q_{51}, 1, q_6, Z, 1\rangle$
45. $\langle q_7, b, q_7, b, -1\rangle$ # (45-48) clear temporary variables $W \to 1$ and $Z \to 0$.
46. $\langle q_7, E, q_7, b, -1\rangle$
47. $\langle q_7, Z, q_7, 0, -1\rangle$
48. $\langle q_7, W, q_7, 1, -1\rangle$
49. $\langle q_7, \triangleright, q_h, \triangleright, 1\rangle$ # done

Exercise: 3.5

(Halting problem with no inputs) Show that given a Turin machine M there is no algorithm to determine whether M halts when the input to the machine is a blank tape.

If there is a such kind of algorithm to determine whether a given M halts, we can define a Turin machine A such that:

1. The input of A is any Turin machine M
2. If M halts when the input is a blank tape, A set into a non-stop state (infinite loop). And if M does not halt, A halts.

That is

$$A(M) = \begin{cases} \text{halts, if } M \text{ dead loop} \\ \text{dead loop, if } M \text{ halts} \end{cases}.$$

Then we see that there is a contradiction. If we input A into A, then there is no result for $A(A)$. Because if A halts, then A must not halts. We conclude that there is no such kind of algorithm.

Exercise: 3.6

(Probabilistic halting problem) Suppose we number the probabilistic Turing machines using a scheme similar to that found in Exercise 3.2 and define the probabilistic halting function $h_p(x)$ to be 1 if machine x halts on input of x with probability at least $1/2$ and 0 if machine x halts on input of x with probability less than $1/2$. Show that there is no probabilistic Turing machine which can output $h_p(x)$ with probability of correctness strictly greater than $1/2$ for all x.

–

Exercise: 3.7

(Halting oracle) Suppose a black box is made available to us which takes a non-negative integer x as input, and then outputs the value of $h(x)$, where $h(\cdot)$ is the halting function defined in Box 3.2 on page130. This type of black box is sometimes known as an oracle for the halting problem. Suppose we have a regular Turing machine which is augmented by the power to call the oracle. One way of accomplishing this is to use a two-tape Turing machine, and add an extra program instruction to the Turing machine which results in the oracle being called, and the value of $h(x)$ being printed on the second tape, where x is the current contents of the second tape. It is clear that this model for computation is more powerful than the conventional Turing machine model, since it can be used to compute the halting function. Is the halting problem for this model of computation undecidable? That is, can a Turing machine aided by an oracle for the halting problem decide whether a program for the Turing machine with oracle will halt on a particular input?

–

Exercise: 3.8

(Universality of NAND) Show that the gate can be used to simulate the AND, XOR and NOT gates, provided wires, ancilla bits and FANOUT are available.

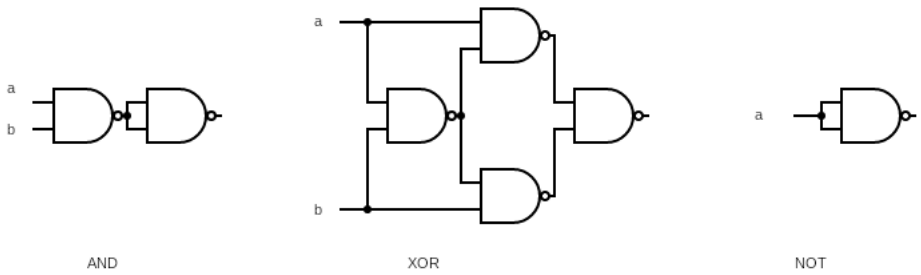


Figure 2: AND, XOR and NOT

Exercise: 3.9

Prove that $f(n)$ is $O(g(n))$ if and only if $g(n)$ is $\Omega(f(n))$. Deduce that $f(n)$ is $\Theta(g(n))$ if and only if $g(n)$ is $\Theta(f(n))$.

Prove that $f(n)$ is $O(g(n))$ if and only if $g(n)$ is $\Omega(f(n))$:

1. $f(n)$ is $O(g)(n) \iff f(n) \leq c_1 g(n)$ for $n \geq n_1 \Longrightarrow g(n)$ is $\Omega(f(n))$
2. $g(n)$ is $\Omega(f(n)) \iff f(n) \leq c_2 g(n)$ for $n \geq n_2 \Longrightarrow f(n)$ is $O(g)(n)$.

Deduce that $f(n)$ is $\Theta(g(n))$ if and only if $g(n)$ **is** $\Theta(f(n))$ $\quad f(n)$ is $\Theta(g(n)) \Longleftrightarrow f(n)$ is $O(g(n))$ and $f(n)$ is $\Omega(g(n)) \Longleftrightarrow g(n)$ is $\Omega(f(n))$ and $g(n)$ is $O(f(n)) \Longleftrightarrow g(n)$ is $\Theta(f(n))$

Exercise: 3.10

Suppose $g(n)$ is a polynomial of degree k. Show that $g(n)$ is $O(n^l)$ for any $l \geq k$.

$g(n) = \sum_{i=0}^{k} c_i n^i \leq a_0 + a_1 n + ... a_k n^k = a_0 + a_1 n + ... a_k n^k = n^l (a_0 n^{-l} + a_1 n^{-l+1} + ... + a_k n^{k-l})$

4 Quantum circuits

Exercise: 4.1

In Exercise 2.11, which you should do now if you haven't already done it, you computed the eigenvectors of the Pauli matrices. Find the points on the Bloch sphere which correspond to the normalized eigenvectors of the different Pauli matrices.

The representation of Bloch sphere: $\begin{pmatrix} \cos\theta/2 \\ e^{i\varphi}\sin\theta/2 \end{pmatrix} \rightarrow (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta) \rightarrow (\theta, \varphi)$. See Fig. 3

Exercise: 4.2

Let x be a real number and A a matrix such that $A^2 = I$. Show that

$$\exp(iAx) = \cos(x) + i\sin(x)\, A$$

Use this result to verify Equations (4.4) through (4.6).

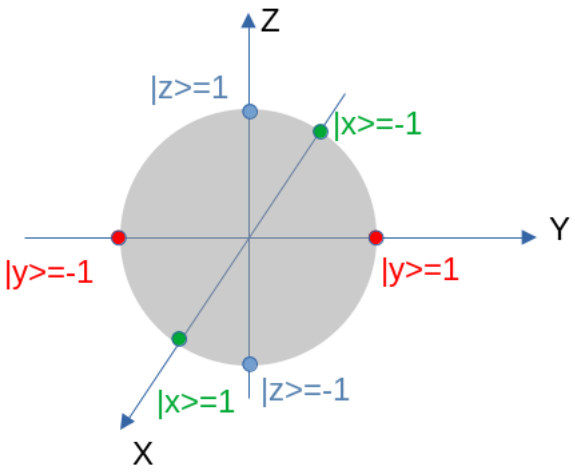


Figure 3: Eigen vectors of Pauli matrix on the Bloch sphere

$$
\begin{aligned}
e^{iAx} &= \sum_n \frac{(iAx)^n}{n!} = \sum_n \frac{(iAx)^{2n}}{(2n)!} + \sum_n \frac{(iAx)^{2n+1}}{(2n+1)!} \\
&= \sum_n \frac{(x)^{2n}}{(2n)!}(i^2A^2)^n + iA\sum_n \frac{(x)^{2n+1}}{(2n+1)!}(i^2A^2)^n \\
&= \cos x + iA\sin x
\end{aligned}
$$

Exercise: 4.3

Show that, up to a global phase, the $\pi/8$ gate satisfies $T = R_z(\pi/4)$.

$$
R_z(\pi/4) = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} = e^{-i\frac{\pi}{8}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = e^{-i\frac{\pi}{8}} T.
$$

Exercise: 4.4

Express the Hadamard gate H as a product of R_x and R_z rotations and $e^{i\varphi}$ for some φ.

$$
-iH = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = R_x(\pi) R_y(\frac{\pi}{2})
$$

Replace R_y by R_z with $R_y(\frac{\pi}{2}) = R_z(\frac{\pi}{2})R_x(\frac{\pi}{2})R_z^\dagger(\frac{\pi}{2})$. Finally we have

$$H = e^{i\pi/2}R_x(\pi)R_z(\frac{\pi}{2})R_x(\frac{\pi}{2})R_z(-\frac{\pi}{2}).$$

Exercise: 4.5

Prove that $(\hat{n}\cdot\vec{\sigma})^2 = 1$, and use this to verify Equation(4.8).

$\sigma_n^2 = 1$ see Problem 2.1

Exercise: 4.6

(Bloch sphere interpretation of rotations) One reason why the $R_{\hat{n}}(\theta)$ operators are referred to as rotation operators is the following fact, which you are to prove. Suppose a single qubit has a state represented by the Bloch vector $\vec{\lambda}$. Then the effect of the rotation $R_{\hat{n}}(\theta)$ on the state is to rotate it by an angle θ about the $\hat{n}$ axis of the Bloch sphere. This fact explains the rather mysterious looking factor of two in the definition of the rotation matrices.

Use the result in Exercise 4.2,

$$R_n(\theta) = e^{-i\sigma_n\frac{\theta}{2}} = \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}\sigma_n = \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}(n_xX + n_yY + n_zZ). \tag{4}$$

According to Eq. (4), for a given vector $n = \begin{pmatrix} \sin\theta_n\cos\phi_n \\ \sin\theta_n\sin\phi_n \\ \cos\theta_n \end{pmatrix}$, we have

$$R_n(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}\cos\theta_n & -i\sin\frac{\theta}{2}\sin\theta_n e^{-i\phi_n} \\ -i\sin\frac{\theta}{2}\sin\theta_n e^{i\phi_n} & \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\cos\theta_n \end{pmatrix}. \tag{5}$$

For any vector $\vec{\lambda} = \lambda(\alpha,\varphi) = \begin{pmatrix} \cos\alpha/2 \\ e^{i\varphi}\sin\alpha/2 \end{pmatrix}$, we have

$$R_n(\theta)\begin{pmatrix} \cos\alpha/2 \\ e^{i\varphi}\sin\alpha/2 \end{pmatrix} = ...\lambda(\alpha',\varphi')$$

One can check that in $SO(3)$ space, the vector $\begin{pmatrix} \sin\alpha'\cos\varphi' \\ \sin\alpha'\sin\varphi' \\ \cos\varphi' \end{pmatrix}$ can be obtained by a rotation on the axis n with angle θ.

Exercise: 4.7

Show that $XYX = -Y$ and use this to prove that $XR_y(\theta)X = R_y(-\theta)$.

Use $R_y(\theta) = \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}Y$ we have

$$\begin{aligned} XR_y(\theta)X &= \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}XYX = \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}Y \\ &= \cos\frac{-\theta}{2} - i\sin\frac{-\theta}{2}Y = R_y(-\theta). \end{aligned}$$

Exercise: 4.8

An arbitrary single qubit unitary operator can be written in the form

$$U = \exp(i\alpha)\, R_{\hat{n}}(\theta)$$

for some real numbers α and θ, and are a real three-dimensional unit vector $\hat{n}$.

1. Prove this fact.
2. Find values for α, θ, and $\hat{n}$ giving the Hadamard gate H.
3. Find values for α, θ, and $\hat{n}$ giving the phase gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

(1)

According to Eq. (5),

$$e^{i\alpha}R_n(\theta) = e^{i\alpha}\begin{pmatrix} \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}\cos\theta_n & -i\sin\frac{\theta}{2}\sin\theta_n e^{-i\phi_n} \\ -i\sin\frac{\theta}{2}\sin\theta_n e^{i\phi_n} & \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\cos\theta_n \end{pmatrix}$$

A general $SU(2)$ matrix is represented as $\begin{pmatrix} z & -w \\ w^* & z^* \end{pmatrix}$ with $|z|^2 + |w|^2 = 1$. This is consistent with the expression of $R_n(\theta)$. Therefore $e^{i\alpha}R_n(\theta)$ can represents any $U(2)$ element.

(2) H gate

$$\begin{pmatrix} \alpha \\ \theta \\ \theta_n \\ \phi_n \end{pmatrix} = \begin{pmatrix} (k+\frac{1}{2})\pi \\ (4M-2k+1)\pi \\ \pi/4 \\ (2N-2M)\pi \end{pmatrix} or \begin{pmatrix} (k+\frac{1}{2})\pi \\ (4M-2k+3)\pi \\ 3\pi/4 \\ (2N-2M-1)\pi \end{pmatrix}$$

An example:

$$\begin{pmatrix} \alpha \\ \theta \\ \theta_n \\ \phi_n \end{pmatrix} = \begin{pmatrix} \pi/2 \\ \pi \\ \pi/4 \\ 0 \end{pmatrix}$$

(3) S gate

$$\begin{pmatrix} \alpha \\ \theta \\ \theta_n \\ \phi_n \end{pmatrix} = \begin{pmatrix} \pi/4 \\ \pi/2 \\ 0 \\ \phi_n \end{pmatrix}$$

Exercise: 4.9

Explain why any single qubit unitary operator may be written in the form (4.12).

($X - Y$ decomposition of rotations) Give a decomposition analogous to Theorem 4.1 but using R_x instead of R_z.

$$\begin{aligned} U &= e^{i\alpha} R_x(\rho) R_y(\sigma) R_x(\xi) \\ &= \begin{pmatrix} \left(-i \sin\frac{\sigma}{2} \sin\left(\frac{\rho}{2} - \frac{\xi}{2}\right) + \cos\frac{\sigma}{2} \cos\left(\frac{\rho}{2} + \frac{\xi}{2}\right)\right) e^{i\alpha} & \left(-\sin\frac{\sigma}{2} \cos\left(\frac{\rho}{2} - \frac{\xi}{2}\right) - i \sin\left(\frac{\rho}{2} + \frac{\xi}{2}\right) \cos\frac{\sigma}{2}\right) e^{i\alpha} \\ \left(\sin\frac{\sigma}{2} \cos\left(\frac{\rho}{2} - \frac{\xi}{2}\right) - i \sin\left(\frac{\rho}{2} + \frac{\xi}{2}\right) \cos\frac{\sigma}{2}\right) e^{i\alpha} & \left(i \sin\frac{\sigma}{2} \sin\left(\frac{\rho}{2} - \frac{\xi}{2}\right) + \cos\frac{\sigma}{2} \cos\left(\frac{\rho}{2} + \frac{\xi}{2}\right)\right) e^{i\alpha} \end{pmatrix} \end{aligned}$$

Exercise: 4.11

Suppose $\hat{m}$ and $\hat{n}$ are non-parallel real unit vectors in three dimensions. Use Theorem 4.1 to show that an arbitrary single qubit unitary U may be written

$$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta),$$

for appropriate choices of α, β, γ and δ.

Give A, B, C, and α for the Hadamard gate.

According to Eq. (4.12) (book),

$$\begin{cases} e^{i(\alpha - \beta/2 - \delta/2)} \cos\frac{\gamma}{2} = 1/\sqrt{2} \\ e^{i(\alpha + \beta/2 - \delta/2)} \sin\frac{\gamma}{2} = 1/\sqrt{2} \\ e^{i(\alpha + \beta/2 + \delta/2)} \cos\frac{\gamma}{2} = -1/\sqrt{2} \end{cases}$$

we have

$$\begin{cases} \alpha = \pi/2 \\ \beta = 0 \\ \gamma = \pi/2 \\ \delta = \pi \end{cases}$$

Exercise: 4.13

(Circuit identities) It is useful to be able to simplify circuits by inspection, using well-known identities. Prove the following three identities:

$$HXH = Z; HYH = -Y; HZH = X.$$

–

Exercise: 4.14

Use the previous exercise to show that $HTH = R_x(\pi/4)$, up to a global phase.

Since $T \sim R_z(\pi/4) = e^{-iZ(\pi/8)} = \cos\pi/8 - iZ\sin\pi/8$, we have

$$\begin{aligned} HTH &= \cos\pi/8 - iHZH\sin\pi/8 = \cos\pi/8 - iX\sin\pi/8 \\ &= e^{-i\frac{X}{2}(\frac{\pi}{4})} = R_x(\frac{\pi}{4}). \end{aligned}$$

Exercise: 4.15

(Composition of single qubit operations) The Bloch representation gives a nice way to visualize the effect of composing two rotations.

(1) Prove that if a rotation through an angle β_1 about the axis $\hat{n}_1$ is followed by a rotation through an angle β_2 about an axis $\hat{n}_2$, then the overall rotation is through an angle β_{12} about an axis $\hat{n}_{12}$ given by

$$\begin{aligned} c_{12} &= c_1c_2 - s_1s_2\hat{n}_1 \cdot \hat{n}_2 \\ s_{12}\hat{n}_{12} &= s_1c_2\hat{n}_1 + c_1s_2\hat{n}_2 - s_1s_2\hat{n}_2 \times \hat{n}_1, \end{aligned}$$

where $c_i = \cos(\beta_i/2), s_i = \sin(\beta_i/2), c_{12} = \cos(\beta_{12}/2), \text{and} s_{12} = \sin(\beta_{12}/2)$.

(2) Show that if $\beta_1 = \beta_2$ and $\hat{n}_1 = \hat{z}$ these equations simplify to

$$\begin{aligned} c_{12} &= c^2 - s^2\hat{z} \cdot \hat{n}_2 \\ s_{12}\hat{n}_{12} &= sc(\hat{z} + \hat{n}_2) - s^2\hat{n}_2 \times \hat{z}, \end{aligned}$$

where $c = c_1$ and $s = s_1$.

(1)

The math formula of the description is

$$R_{n_2}(\beta_2)R_{n_1}(\beta_1) = R_{n_{12}}(\beta_{12}). \tag{6}$$

By the formula $R_n(\theta) = e^{-i\frac{\theta}{2}\boldsymbol{\sigma}\cdot\boldsymbol{n}} = \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}\boldsymbol{\sigma}\cdot\boldsymbol{n}$ we can rewrite Eq. (6) as

$$\left(\cos\frac{\beta_2}{2} - i\sin\frac{\beta_2}{2}\boldsymbol{\sigma}\cdot\boldsymbol{n}_2\right)\left(\cos\frac{\beta_1}{2} - i\sin\frac{\beta_1}{2}\boldsymbol{\sigma}\cdot\boldsymbol{n}_1\right) = \left(\cos\frac{\beta_{12}}{2} - i\sin\frac{\beta_{12}}{2}\boldsymbol{\sigma}\cdot\boldsymbol{n}_{12}\right).$$

It is expanded as

$$c_2c_1 - ic_2s_1\boldsymbol{\sigma}\cdot\boldsymbol{n}_1 - \boldsymbol{\sigma}\cdot\boldsymbol{n}_2 is_2c_1 - s_1s_2\left(\boldsymbol{\sigma}\cdot\boldsymbol{n}_2\right)\left(\boldsymbol{\sigma}\cdot\boldsymbol{n}_1\right) = c_{12} - is_{12}\boldsymbol{\sigma}\cdot\boldsymbol{n}_{12}. \tag{7}$$

Consider a useful relation $\sigma_i\sigma_j = \delta_{ij} + i\sum_k \varepsilon_{ijk}\sigma_k$ (Exercise 2.43), we have

$$\begin{aligned}\left(\boldsymbol{\sigma}\cdot\boldsymbol{n}_2\right)\left(\boldsymbol{\sigma}\cdot\boldsymbol{n}_1\right) &= \sum_i \sigma_i n_2^i \sum_j \sigma_j n_1^j \\ &= \sum_{ij}(\delta_{ij} + i\sum_k \varepsilon_{ijk}\sigma_k)n_2^i n_1^j = \boldsymbol{n}_1\cdot\boldsymbol{n}_2 + i\boldsymbol{\sigma}\cdot(\boldsymbol{n}_2\times\boldsymbol{n}_1).\end{aligned}$$

Therefore Eq. (7) becomes

$$c_2c_1 - s_1s_2\boldsymbol{n}_1\cdot\boldsymbol{n}_2 + is_{12}\boldsymbol{\sigma}\cdot\boldsymbol{n}_{12} = c_{12} + i\boldsymbol{\sigma}\cdot\left(s_1s_2(\boldsymbol{n}_2\times\boldsymbol{n}_1) + \boldsymbol{n}_2s_2c_1 + c_2s_1\boldsymbol{n}_1\right).$$

Real and imaginary parts on both side should be equal, therefore we have

$$\begin{cases} c_{12} = c_2c_1 - s_1s_2\boldsymbol{n}_1\cdot\boldsymbol{n}_2 \\ s_{12}\boldsymbol{n}_{12} = s_1s_2(\boldsymbol{n}_2\times\boldsymbol{n}_1) + \boldsymbol{n}_2s_2c_1 + c_2s_1\boldsymbol{n}_1 \end{cases}$$

(2)

(Trivial)

Exercise: 4.16

(Matrix representation of multi-qubit gates) What is the 4×4 unitary matrix for the circuit

$$\begin{array}{r} x_2 - [H]- \\ x_1 - - - - \end{array}$$

in the computational basis? What is the unitary matrix for the circuit

$$\begin{array}{r} x_2 - -- \\ x_1 - [H]- \end{array}$$

in the computational basis?

$$H\otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix} I & I \\ I & -I \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

$$I\otimes H = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Exercise: 4.17

(Building from controlled-Z gates) Construct a gate from one controlled-Z gate, that is, the gate whose action in the computational basis is specified by the unitary matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

and two Hadamard gates, specifying the control and target qubits.

$$CNOT(c_1, t_2) = H_2 CZ H_2$$

Exercise: 4.18

Show that $CZ_{12} = CZ_{21}$

–

Exercise: 4.18

($CNOT$ action on density matrices) The gate is a simple permutation whose action on a density matrix ρ is to rearrange the elements in the matrix. Write out this action explicitly in the computational basis.

In the coupled representation, $|i\rangle \in \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. The operation of a CNOT gate is to exchange $|2\rangle$ and $|3\rangle$. For $\rho = \sum_{\alpha\beta\gamma\delta} c_{\alpha\beta\gamma\delta} |\alpha\beta\rangle\langle\gamma\delta| = \sum_{ij} C_{ij} |i\rangle\langle j|$, the output state of the operation of CNOT is

$$CNOT\rho CNOT^\dagger = \begin{pmatrix} |0\rangle & |1\rangle & |2\rangle & |3\rangle \end{pmatrix} \begin{pmatrix} c_{00} & c_{01} & c_{03} & c_{02} \\ c_{10} & c_{11} & c_{13} & c_{12} \\ c_{30} & c_{31} & c_{33} & c_{32} \\ c_{20} & c_{21} & c_{23} & c_{22} \end{pmatrix} \begin{pmatrix} \langle 0| \\ \langle 1| \\ \langle 2| \\ \langle 3| \end{pmatrix}$$

Exercise: 4.20

(basis transformations) Unlike ideal classical gates, ideal quantum gates do not have (as electrical engineers say) 'high-impedance' inputs. In fact, the role of 'control' and 'target' are arbitrary – they depend on what basis you think of a device as operating in. We have described how the behaves with respect to the computational basis, and in this description the state of the control qubit is not changed. However, if we work in a different basis then the control qubit does change: we will show that its phase is flipped depending on the state of the 'target' qubit! Show that

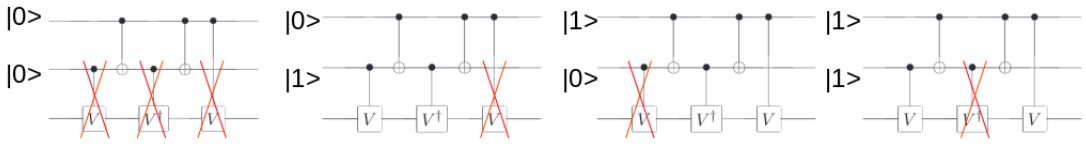
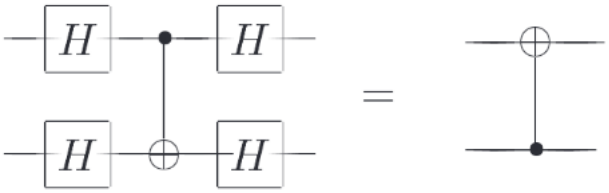


Figure 4: Exercise 4.21



Introducing basis states $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$, use this circuit identity to show that the effect of a with the first qubit as control and the second qubit as target is as follows:

$$|+\rangle|+\rangle \rightarrow |+\rangle|+\rangle$$
$$|-\rangle|+\rangle \rightarrow |-\rangle|+\rangle$$
$$|+\rangle|-\rangle \rightarrow |-\rangle|-\rangle$$
$$|-\rangle|-\rangle \rightarrow |+\rangle|-\rangle$$

Thus, with respect to this new basis, the state of the target qubit is not changed, while the state of the control qubit is flipped if the target starts as $|-\rangle$, otherwise it is left alone. That is, in this basis, the target and control have essentially interchanged roles!

–

Exercise: 4.21

Verify that Figure 4.8 implements the $C^2(U)$ operation.

For different configuration of control qubits as shown in Fig. 4

- For $|c_1\rangle|c_2\rangle = |0\rangle|0\rangle$, no operator is valid. The output is I.
- For $|c_1\rangle|c_2\rangle = |0\rangle|1\rangle$, the output is $VV^\dagger = I$
- For $|c_1\rangle|c_2\rangle = |1\rangle|0\rangle$, the output is $V^\dagger V = I$
- For $|c_1\rangle|c_2\rangle = |1\rangle|1\rangle$, the output is $V^2 = U$.

It concludes that the output is $C^2(U)$.

Exercise: 4.22

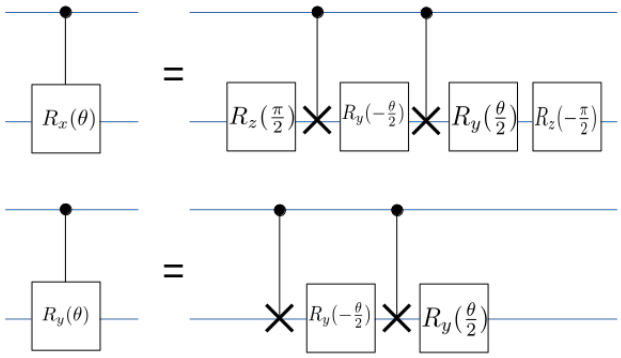


Figure 5: Exercise 4.23

Prove that a $C^2(U)$ gate (for any single qubit unitary U) can be constructed using at most eight one-qubit gates, and six controlled-NOTs.

Based on the conclusion of Exercise 4.21, the equivalent problem is that how to implement a controlled-V gate. Recall the relation $V = e^{i\alpha}AXBXC$, each controlled-V gate can be implemented by 2 CNOT and 3 single-qubit gate (A,B and C). Therefore totally we need $3 \times 2 + 2$ (2 for those in Fig. 4) CNOT gate and 6 single-qubit gate (A, $A^\dagger$, B, $B^\dagger$, C and $C^\dagger$).

Exercise: 4.23

Construct a $C^1(U)$ gate for $U = R_x(\theta)$ and $U = R_y(\theta)$, using only $CNOT$ and single qubit gates. Can you reduce the number of single qubit gates needed in the construction from three to two?

Consider the result in Exercise 4.11 that $U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$ and the Corollary 4.2 that $A = R_z(\beta)R_y(\gamma/2)$,$B = R_y(-\gamma/2)R_z(-\frac{\delta+\beta}{2}), C = R_z(\frac{\delta-\beta}{2})$ for $U = e^{i\alpha}AXBXC$,

- For $U = R_x(\theta) = R_z(-\frac{\pi}{2})R_y(\theta)R_z^\dagger(-\frac{\pi}{2})$, we have $\{\alpha = 0, \beta = -\frac{\pi}{2}, \gamma = \theta, \delta = \frac{\pi}{2}\}$, therefore

$$\begin{aligned} A &= R_z(-\frac{\pi}{2})R_y(\theta/2), \\ B &= R_y(-\theta/2) \\ C &= R_z(\pi/2) \end{aligned}$$

- For $U = R_y(\theta)$, we have $\{\alpha = 0, \beta = 0, \gamma = \theta, \delta = 0\}$,therefore

$$\begin{aligned} A &= R_y(\theta/2), \\ B &= R_y(-\theta/2) \\ C &= I \end{aligned}$$

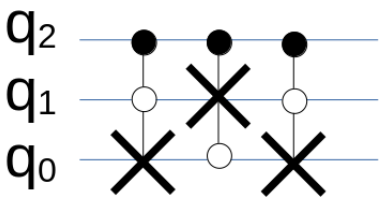


Figure 6: Exercise 4.25 (1)

Exercise: 4.24

Verify that Figure 4.9 implements the Toffoli gate.

–

Exercise: 4.25

(Fredkin gate construction) Recall that the Fredkin (controlled-swap) gate performs the transform

$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & \dots & \\ & & 1 & & & \dots & 0 & \dots \\ & & & 1 & & & \dots & \\ & & & & 1 & & & \\ & \dots & & & & & & \\ \dots & 0 & \dots & & & 0 & 1 & \\ & \dots & & & & 1 & 0 & \\ & & & & & & & 1 \end{pmatrix}$$

(1) Give a quantum circuit which uses three Toffoli gates to construct the Fredkin gate (Hint: think of the swap gate construction – you can control each gate, one at a time).

(2) Show that the first and last Toffoli gates can be replaced by gates.

(3) Now replace the middle Toffoli gate with the circuit in Figure 4.8 to obtain a Fredkin gate construction using only six two-qubit gates.

(4) Can you come up with an even simpler construction, with only five two-qubit gates?

(1)

Recall the major spirit of gray-code.

Exercise 4.26 - 4.30

Exercise 4.31

Exercise: 4.32

Suppose ρ is the density matrix describing a two qubit system. Suppose we perform a projective measurement in the computational basis of the second qubit. Let $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ be the projectors onto the $|0\rangle$ and $|1\rangle$ states of the second qubit, respectively. Let ρ' be the density matrix which would be assigned to the system after the measurement by an observer who did not learn the measurement result. Show that

$$\rho' = P_0\rho P_0 + P_1\rho P_1$$

Also show that the reduced density matrix for the first qubit is not affected by the measurement, that is, $\mathrm{tr}_2(\rho) = \mathrm{tr}_2(\rho')$.

For a general state $\rho = \sum_{ij\alpha\beta} c_{i\alpha j\beta}|i\alpha\rangle\langle j\beta|$, we have

$$\begin{aligned}\rho' &= P_0\rho P_0 + P_1\rho P_1 \\ &= \sum_{ij\alpha\beta} c_{i\alpha j\beta}|0\rangle\langle 0|i\alpha\rangle\langle j\beta|0\rangle\langle 0| + \sum_{ij\alpha\beta} c_{i\alpha j\beta}|1\rangle\langle 1|i\alpha\rangle\langle j\beta|1\rangle\langle 1| \\ &= \sum_{ij} c_{i0j0}|i\rangle\langle j| \otimes |0\rangle\langle 0| + \sum_{ij} c_{i1j1}|i\rangle\langle j| \otimes |1\rangle\langle 1|.\end{aligned}$$

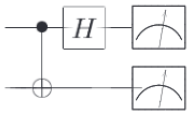
On one hand we have $tr_2(\rho') = \sum_{ij\alpha\beta} c_{i0j0}|i\rangle\langle j| + \sum_{ij} c_{i1j1}|i\rangle\langle j|$, on the other hand we have

$$tr_2(\rho) = \sum_{ij\alpha\beta s} c_{i\alpha j\beta}|i\rangle\langle j| \otimes \langle s|\alpha\rangle\langle\beta|s\rangle = \sum_{ij\alpha} c_{i\alpha j\alpha}|i\rangle\langle j|.$$

We have $tr_2(\rho) = tr_2(\rho')$.

Exercise: 4.33

(Measurement in the Bell basis) The measurement model we have specified for the quantum circuit model is that measurements are performed only in the computational basis. However, often we want to perform a measurement in some other basis, defined by a complete set of orthonormal states. To perform this measurement, simply unitarily transform from the basis we wish to perform the measurement in to the computational basis, then measure. For example, show that the circuit



performs a measurement in the basis of the Bell states. More precisely, show that this circuit results in a measurement being performed with corresponding POVM elements the four projectors onto the Bell states. What are the corresponding measurement operators?

We use notations of Bell states $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right), |\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right)$. The POVM is (in order) $\{E_m | m = 0, 1, 2, 3\} = \{|\Phi^+\rangle\langle\Phi^+|, |\Psi^+\rangle\langle\Psi^+|, |\Phi^-\rangle\langle\Phi^-|, |\Psi^-\rangle\langle\Psi^-|\}$. The reason is given as follows.

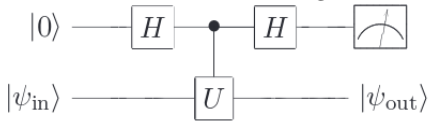
Due to the completeness of Bell state, any input state can be represented as

$$|\psi\rangle = \sum_{i=0}^{3} c_i |B_i\rangle,$$

where $\{|B_i\rangle\} = \{|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle\}$ (in order). The output state is $|\psi_{out}\rangle = C_0^1 H_1$, where C_0^1 represent a CNOT gate with a control at the qubit 1 and target at qubit 0. One can check that $p_m = \langle\psi_{out}|E_m|\psi_{out}\rangle = |c_m|^2$.

Exercise: 4.34

(Measuring an operator) Suppose we have a single qubit operator U with eigenvalues ± 1, so that U is both Hermitian and unitary, so it can be regarded both as an observable and a quantum gate. Suppose we wish to measure the observable U. That is, we desire to obtain a measurement result indicating one of the two eigenvalues, and leaving a post-measurement state which is the corresponding eigenvector. How can this be implemented by a quantum circuit? Show that the following circuit implements a measurement of U :



Assume that eigenvectors of U are $\{|+\rangle, |-\rangle\}$, due to the completeness of U (because of Hermitian), the input state is represented as $|\psi_{in}\rangle = c_+|+\rangle + c_-|-\rangle$. For the input $|0\rangle \otimes |\psi_{in}\rangle$, we call the output state (just before the final measurement) as $|\Psi_{out}\rangle$. The state after the first Hadamard gate is

$$|\Psi_{out}^1\rangle = c_+ \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |+\rangle + c_- \frac{|0\rangle - |1\rangle}{\sqrt{2}} CU|-\rangle.$$

The state after the CU gate is

$$|\Psi_{out}^2\rangle = c_+ \frac{|0\rangle|+\rangle + |1\rangle|+\rangle}{\sqrt{2}} + c_- \frac{|0\rangle|-\rangle + |1\rangle|-\rangle}{\sqrt{2}}.$$

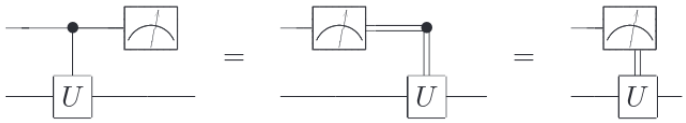
The state after the second Hadamard gate is

$$|\Psi_{out}\rangle = c_+|0\rangle|+\rangle + c_-|0\rangle|-\rangle.$$

So this circuit is working.

Exercise: 4.35

(Measurement commutes with controls) A consequence of the principle of deferred measurement is that measurements commute with quantum gates when the qubit being measured is a control qubit, that is:



Assume that the input state is $\rho_{in} = \sum_{ij\alpha\beta} c_{i\alpha j\beta}|i\rangle\langle j| \otimes |\alpha\rangle\langle\beta|$.
For the first circuit, the CU gate generate

$$\rho_1' = CU\rho_{in}CU^\dagger = \sum_{ij\alpha\beta} c_{i\alpha j\beta}|i\rangle\langle j| \otimes U^i|\alpha\rangle\langle\beta|U^{\dagger j}$$

then we consider the measurement, the output state is

$$\rho_1'' = P_0\rho_1'P_0 + P_1\rho_1'P_1 = |0\rangle\langle 0| \otimes \sum_{\alpha\beta} c_{0\alpha 0\beta}|\alpha\rangle\langle\beta| + |1\rangle\langle 1| \otimes \sum_{\alpha\beta} c_{1\alpha 1\beta}U|\alpha\rangle\langle\beta|U^\dagger$$

The reduced density matrix for the second qubit is

$$\rho_1 = tr_1(\rho_1'') = \sum_{\alpha\beta} c_{0\alpha 0\beta}|\alpha\rangle\langle\beta| + \sum_{\alpha\beta} c_{1\alpha 1\beta}U|\alpha\rangle\langle\beta|U^\dagger$$

For the second circuit, we first consider the measurement

$$\rho_2' = P_0\rho_{in}P_0 + P_1\rho_{in}P_1 = |0\rangle\langle 0| \otimes \sum_{\alpha\beta} c_{0\alpha 0\beta}|\alpha\rangle\langle\beta| + |1\rangle\langle 1| \otimes \sum_{\alpha\beta} c_{1\alpha 1\beta}|\alpha\rangle\langle\beta|$$

The case of $|q_1\rangle = |1\rangle$, we need to consider a U operation, the output state is

$$\begin{aligned}\rho_2'' &= P_0\rho_{in}P_0 + UP_1\rho_{in}P_1U^\dagger \\ &= |0\rangle\langle 0| \otimes \sum_{\alpha\beta} c_{0\alpha 0\beta}|\alpha\rangle\langle\beta| + |1\rangle\langle 1| \otimes \sum_{\alpha\beta} c_{1\alpha 1\beta}U|\alpha\rangle\langle\beta|U^\dagger\end{aligned}$$

The final output is $\rho_2 = tr_1(\rho_2'') = \sum_{\alpha\beta} c_{0\alpha 0\beta}|\alpha\rangle\langle\beta| + \sum_{\alpha\beta} c_{1\alpha 1\beta}U|\alpha\rangle\langle\beta|U^\dagger$. Therefore we have $\rho_1 = \rho_2$.

Exercise 4.36

Exercise: 4.37

Provide a decomposition of the transform

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

into a product of two-level unitaries. This is a special case of the quantum Fourier transform, which we study in more detail in the next chapter.

$U = U_1U_2U_3U_4U_5U_6U_7$, where

$$U_1 = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 & 0 \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$U_2 = \begin{pmatrix} \frac{\sqrt{6}}{3} & 0 & \frac{\sqrt{3}}{3} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{\sqrt{3}}{3} & 0 & -\frac{\sqrt{6}}{3} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$U_3 = \begin{pmatrix} \frac{\sqrt{3}}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} \end{pmatrix},$$

$$U_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{3}\cdot(1-i)}{4} & \frac{3}{4} - \frac{i}{4} & 0 \\ 0 & \frac{3}{4} + \frac{i}{4} & \frac{\sqrt{3}(-1-i)}{4} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$U_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{6}}{3} & 0 & -\frac{\sqrt{3}i}{3} \\ 0 & 0 & 1 & 0 \\ 0 & \frac{\sqrt{3}i}{3} & 0 & -\frac{\sqrt{6}}{3} \end{pmatrix},$$

$$U_6 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ 0 & 0 & -\frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix},$$

$$U_7 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}.$$

One can reproduced this by code 20230505_1.py

Exercise 4.38

Exercise: 4.39

Find a quantum circuit using single qubit operations and sto implement the transformation

$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & a & & & & c & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & b & & & & d & \end{pmatrix},$$

where $\tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is an arbitrary 2×2 unitary matrix.

The start and end state of the gray-code is $|s\rangle = |2\rangle$ and $|t\rangle = |7\rangle$. The Gray-code connection is given by the following table:

	q_2	q_1	q_0
g_1	0	1	0
g_2	0	1	1
g_3	1	1	1

guide by which we can implement the required circuit shown in Fig. 7.

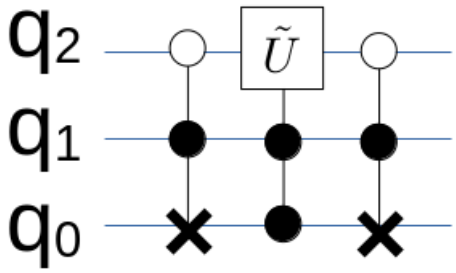


Figure 7: Exercise 4.39

Exercise 4.40

Exercise: 4.41

This and the next two exercises develop a construction showing that the Hadamard, phase, controlled- and Toffoli gates are universal. Show that he circuit in Figure 4.17 applies the operation $Rz(\theta)$ to the third (target) qubit if the measurement outcomes are both 0, where $\cos\theta = 3/5$, and otherwise applies Z to the target qubit. Show that the probability of both

measurement outcomes being 0 is 5/8, and explain how repeated use of this circuit and $Z = S^2$ gates may be used to apply a $Rz(\theta)$ gate with probability approaching 1.

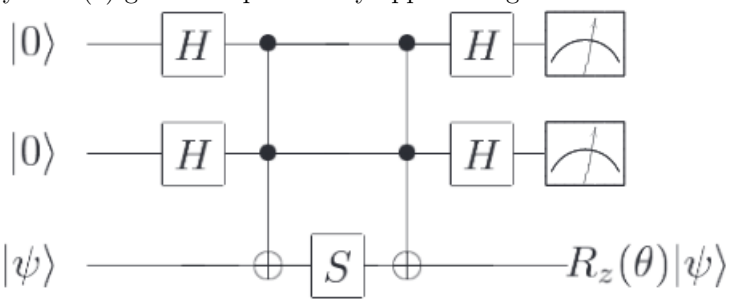


Figure 4.17. Provided both measurement outcomes are 0 this circuit applies $R_z(\theta)$ to the target, where $\cos\theta = 3/5$. If some other measurement outcome occurs then the circuit applies Z to the target.

Assume that $|\psi\rangle$ is in the low-bit index. For the input state $|\Psi_{in}\rangle = |0\rangle|0\rangle \otimes |\psi\rangle = (\psi_0|0\rangle|0\rangle|0\rangle + \psi_1|0\rangle|0\rangle|1\rangle)$, the output state (just before the measurement) is given as

$$\begin{aligned}|\Psi_{out}\rangle = &\frac{3+i}{4}\psi_a|000\rangle + \frac{1+3i}{4}\psi_b|001\rangle + \frac{1-i}{4}\psi_a|010\rangle + \frac{i-1}{4}\psi_b|011\rangle \\ &+ \frac{1-i}{4}\psi_a|100\rangle + \frac{i-1}{4}\psi_b|101\rangle + \frac{i-1}{4}\psi_a|110\rangle + \frac{1-i}{4}\psi_b|111\rangle\end{aligned}$$

It is rewritten as

$$\begin{aligned}|\Psi_{out}\rangle &= |00\rangle \otimes \left(\frac{3+i}{4}\psi_a|0\rangle + \frac{1+3i}{4}\psi_b|1\rangle\right) + \frac{1-i}{4}\left(|01\rangle + |10\rangle + |11\rangle\right)\left(\psi_a|0\rangle - \psi_b|1\rangle\right) \\ &= \sqrt{\frac{5}{8}}|00\rangle \otimes \begin{pmatrix} |0\rangle & |1\rangle \end{pmatrix} \begin{pmatrix} \sqrt{\frac{8}{5}}\frac{3+i}{4} & 0 \\ 0 & \sqrt{\frac{8}{5}}\frac{1+3i}{4} \end{pmatrix} \begin{pmatrix} \psi_a \\ \psi_b \end{pmatrix} + \frac{1-i}{4}\left(\sum_{x=1}^{3}|x\rangle\right) \otimes \begin{pmatrix} |0\rangle & |1\rangle \end{pmatrix} Z \begin{pmatrix} \psi_a \\ \psi_b \end{pmatrix}\end{aligned}$$

To specify it more clearly,

$$\begin{pmatrix} \sqrt{\frac{8}{5}}\frac{3+i}{4} & 0 \\ 0 & \sqrt{\frac{8}{5}}\frac{1+3i}{4} \end{pmatrix} = \sqrt{\frac{8}{5}}\frac{3+i}{4}\begin{pmatrix} 1 & 0 \\ 0 & \frac{3+4i}{5} \end{pmatrix} \equiv e^{i\alpha}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Now it is very clear that $\cos\theta = \frac{3}{5}$. The leading coefficient give rise to the probability of $\frac{5}{8}$. So this circuit gate is non-deterministic. The rotation angle of this gate is irrational. With S gate, it is possible to implement a general $R_z(\theta)$.

Details of the calculation can be found in 20230505_2.py.

Exercise 4.42 - Exercise 4.45

Exercise: 4.46

(Exponential complexity growth of quantum systems) Let ρ be a density matrix describing

the state of n qubits. Show that describing ρ requires $4n-1$ independent real numbers.

The dimension of the Hilbert space is $d = 2^n$. Therefore each density matrix must be stored in a $d \times d$ matrix with $M = \sum_{i=1}^{d}(d-i) = \frac{d(d+1)}{2}$ (ρ is Hermitian, only half size of the original matrix). Since the diagonal terms are all real, the number of independent real numbers is $2M - d = d^2 = 4^n$. Notice that the trace of the density matrix is a constant. So finally there are $4^n - 1$ independent real numbers.

Exercise: 4.47

For $H = \sum_k^L H_k$, prove that $e^{-iHt} = e^{-iH_1 t}e^{-iH_2 t}...e^{-iH_L t}$ for all t if $[H_j, H_k] = 0$, for all j, k.

For operators A and B with $[A, B] = 0$, one can check that $e^{A+B} = ... = e^A e^B = e^B e^A$. More generally we have

$$e^{-iHt} = e^{-i\sum_k H_k t} = \prod_k e^{-iH_k t}$$

Exercise: 4.48

Show that the restriction of H_k to involve at most c particles implies that in the sum (4.97), L is upper bounded by a polynomial in n.

(Baker–Campbell–Hausdorf formula) Prove that $e^{(A+B)\Delta t} = e^{A\Delta t}e^{B\Delta t}e^{-\frac{1}{2}[A,B]\Delta t^2} + O(\Delta t^3)$ and also prove Equations (4.103) and (4.104).

$$e^{(A+B)\Delta t} = 1 + (A+B)\Delta t + \frac{1}{2}(A+B)^2\Delta t^2 + O(\Delta t^3)$$

$$e^{A\Delta t} = 1 + A\Delta t + \frac{1}{2}A^2\Delta t^2 + O(\Delta t^3)$$

$$e^{B\Delta t} = 1 + B\Delta t + \frac{1}{2}B^2\Delta t^2 + O(\Delta t^3)$$

$$e^{-\frac{1}{2}[A,B]\Delta t^2} = 1 - \frac{1}{2}[A,B]\Delta t^2 + O(\Delta t^4)$$

$$\begin{aligned} e^{A\Delta t}e^{B\Delta t}e^{-\frac{1}{2}[A,B]\Delta t^2} &= \left(1 + A\Delta t + \frac{1}{2}A^2\Delta t^2 + O(\Delta t^3)\right)\left(1 + B\Delta t + \frac{1}{2}B^2\Delta t^2 + O(\Delta t^3)\right)\left(1 - \frac{1}{2}[A,B]\Delta t^2 + O(\Delta t^4)\right) \\ &= 1 + (A+B)\,\Delta t + \frac{1}{2}\left(A^2 + B^2 + (AB + BA)\right)\Delta t^2 + O(\Delta t^3) \end{aligned}$$

Therefore $e^{(A+B)\Delta t} = e^{A\Delta t}e^{B\Delta t}e^{-\frac{1}{2}[A,B]\Delta t^2}$.

Exercise 4.50

Exercise: 4.51

Construct a quantum circuit to simulate the Hamiltonian

$$H = X_1 \otimes Y_2 \otimes Z_3,$$

performing the unitary transform $e^{-i\Delta t H}$ for any Δt.

For the term X, for instance, the trick is to change the computing bases to the eigen states of X. Use the notation $R \equiv R_y(-\pi/2)$ to represent the rotation for the first qubit, we first check that $RXR^\dagger = Z$. Therefore we have

$$e^{-iH\Delta t} = R^\dagger \left(Re^{-iH\Delta t}R^\dagger\right) R = e^{-iZ_1Y_2Z_3\Delta t}.$$

Likewise, the can transfer Y_2 to Z_2. The final circuit is implemented with the guide of following relation:

$$e^{-iH\Delta t} = R_y^1(\frac{\pi}{2})R_y^2(-\frac{\pi}{2})e^{-iZ_1Z_2Z_3\Delta t}R_y^1(-\frac{\pi}{2})R_y^2(\frac{\pi}{2}).$$

The circuit is shown in the figure.

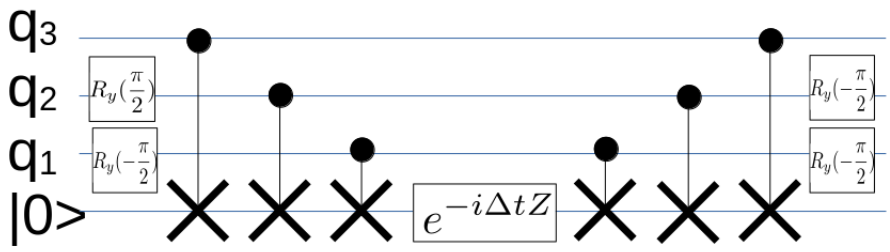


Figure 8: Exercise 4.51

Problem 4.1

Problem 4.2

Problem 4.3

(1)

According to Exercise 2.18, U is diagonalizable. We expand the inner product space by eigenvectors of U. Then

$$H = i \ln \begin{pmatrix} e^{i\theta_1} & & \\ & e^{i\theta_2} & \\ & & \dots \end{pmatrix} = - \begin{pmatrix} \theta_1 & & \\ & \theta_2 & \\ & & \dots \end{pmatrix}$$

So apparently H is Hermitian and the eigenvalues are in range 0 to 2π.

(2)

(3)

Problem 4.4

Problem 4.5

Problem 4.6

5 The quantum Fourier transform and its applications

Notation

We introduce the "k-space" whose basis are marked as $|k\rangle_p$ (with a subscript p). The basis in the real space is marked as $|j\rangle$ (without subscript p). The Fourier expansion of a basis in real space is given as $|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i\left(2\pi \frac{k}{N}\right)j} |k\rangle_p$. Or in the language of the book, we define a Fourier transform as $U|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i\left(2\pi \frac{k}{N}\right)j} |k\rangle$ (no subscript p).

Exercise 5.1

$|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i\left(2\pi \frac{k}{N}\right)j} |k\rangle_p \equiv \sum_k U_{jk} |k\rangle_p$, where $U_{jk} = \frac{1}{\sqrt{N}} e^{i\left(2\pi \frac{k}{N}\right)j}$.

$$\begin{aligned}\left(UU^\dagger\right)_{\alpha\beta} &= \sum_{k=0}^{N-1} U_{\alpha k} U^\dagger_{k\beta} = \frac{1}{N} \sum_{k=0}^{N-1} e^{i\left(2\pi \frac{k}{N}\right)\alpha} e^{-i\left(2\pi \frac{k}{N}\right)\beta} \\ &= \frac{1}{N} \sum_{k=0}^{N-1} e^{\frac{2\pi i k}{N}(\alpha-\beta)} = \delta_{\alpha\beta}\end{aligned}$$

Similarly we have $U^\dagger U = 1$ too.

Exercise 5.2

We expand $|0\rangle$ as

$$|0\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle_p,$$

where $N = 2^n$.

Exercise 5.3

Exercise 5.4

Since $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{2^k}} \end{pmatrix} = e^{i\frac{2\pi/2^k}{2}} R_z(2\pi/2^k)$, according to *Theorem 4.1*, we write it as $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$, where $\alpha = e^{i\frac{2\pi/2^k}{2}}, \beta = 0, \gamma = 0$ and $\delta = 2\pi/2^k$. Then according to *Corollary 4.2*, we rewrite it as $U = e^{i\alpha} AXBXC$, where $A = I, B = R_z(-\frac{2\pi}{2^{k+1}})$ and $C = R_z(\frac{2\pi}{2^{k+1}})$. And the corresponding circuit is shown in Figure 4.6.

Exercise 5.5

Replace R_k to $\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{2\pi}{2^k}} \end{pmatrix}$.

Exercise 5.6

Exercise 5.7

For $|j\rangle = |j_{t-1}j_{t-2}...j_0\rangle$, we can write down a set of index $\zeta = \{i\}$, whose element represent the index at which the bit is 1. For example $|2\rangle = |10\rangle$ has $\zeta_2 = \{1\}$ and $|4\rangle = |100\rangle$ has $\zeta_4 = \{2\}$.

$$|j\rangle|u\rangle = |j_{t-1}j_{t-2}...j_0\rangle|u\rangle = \otimes_{x=0}^{t-1}|j_x\rangle|u\rangle \rightarrow \prod_{i\in\zeta_j} U^{2^i} \otimes_{x=0}^{t-1} |j_x\rangle|u\rangle$$
$$= U^{\sum_{i\in\zeta_j} 2^i}|j\rangle|u\rangle = U^j|j\rangle|u\rangle.$$

Exercise 5.8

Exercise 5.9

Exercise 5.10

- $x^1 = 5 + 0N$
- $x^2 = 4 + N$
- $x^3 = 20 + 5N$
- $x^4 = 16 + 29N$
- $x^5 = 17 + 148N$
- $x^6 = 1 + 744N$

Exercise 5.11

As shown in Exercise A4.16, $r|\varphi(N)$, $r \leq \varphi(N) \leq N$.

Exercise 5.12

$I = \sum_{i=0}^{2^L-1} |i\rangle\langle i|$.

$$UU^\dagger = U \sum_{i=0}^{2^L-1} |i\rangle\langle i|U^\dagger = \sum_{i=0}^{N-1} |xi \bmod N\rangle\langle xi \bmod N| + \sum_{i\geq N} |i\rangle\langle i|$$

Since $\gcd(x, N) = 1$, the inverse (x^{-1}) exists. For any $i, j \in [0, N-1]$ and $i \neq j$, $xi \overset{n}{\neq} xj$. Therefore $x\{i \in N\}$ only rearrange $\{i \in N\}$. Therefore

$$UU^\dagger = \sum_{i=0}^{N-1} |i\rangle\langle i| + \sum_{i \geq N} |i\rangle\langle i| = 1.$$

Exercise 5.13

$$\begin{aligned}
\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i \frac{sk}{r}} |u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i \frac{sk}{r}} \left(\frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \exp\left(\frac{-2\pi i s l}{r}\right) |x^l \bmod N\rangle \right) \\
&= \frac{1}{r} \sum_{l=0}^{r-1} \left(\sum_{s=0}^{r-1} \exp\left(\frac{2\pi i s\,(k-l)}{r}\right) \right) |x^l \bmod N\rangle \\
&= \frac{1}{r} \sum_{l=0}^{r-1} r\delta_{kl} |x^l \bmod N\rangle = |x^k \bmod N\rangle
\end{aligned}$$

Exercise 5.14

In Eq. (5.20), we replace $|u\rangle$ with $|u_s\rangle$ to obtain

$$\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \frac{s}{r} k} |k\rangle |u_s\rangle.$$

Then what we want is

$$\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \frac{s}{r} k} |k\rangle \left(\frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \exp\left(\frac{-2\pi i s l}{r}\right) |x^l \bmod N\rangle \right) \\
&= \frac{1}{2^{t/2}} \sum_{l=0}^{r-1} \sum_{k=0}^{2^t-1} \left(\frac{1}{r} \sum_{s=0}^{r-1} \exp\left(2\pi i s \frac{k-l}{r}\right) \right) |k\rangle |x^l \bmod N\rangle \\
&= \frac{1}{2^{t/2}} \sum_{l=0}^{r-1} \sum_{k=0}^{2^t-1} \delta_{kl} |k\rangle |x^l \bmod N\rangle \\
&= \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} |k\rangle |x^k \bmod N\rangle
\end{aligned}$$

If we, additionally, apply $FT^\dagger$ to $|\psi\rangle$, we obtain

$$\begin{aligned} FT^\dagger|\psi\rangle &= \frac{1}{\sqrt{N}}\frac{1}{2^{t/2}}\sum_{k=0}^{N-1}\sum_{j=0}^{2^t-1} e^{-i\left(2\pi\frac{k}{N}\right)j}|k\rangle|x^j \bmod N\rangle \\ &\stackrel{?}{=} \frac{\sqrt{r}}{\sqrt{N}}\frac{1}{2^{t/2}}\sum_{k=0}^{N=2^t-1}|k\rangle\left(\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-i\left(2\pi\frac{k}{r}\right)j}|x^j \bmod N\rangle\right) \\ &= \frac{\sqrt{r}}{\sqrt{N}}\frac{1}{2^{t/2}}\sum_{s=0}^{N=2^t-1}|s\rangle|u_s\rangle \end{aligned}$$

6 Quantum search algorithms

Exercise 6.1

For $|\psi\rangle = \sum_x c_x|x\rangle$,

$$\begin{aligned} (2|0\rangle\langle 0| - 1)\,|\psi\rangle &= 2|0\rangle c_0 - \sum_{x\geq 1} c_x|x\rangle - c_0|0\rangle = |0\rangle c_0 - \sum_{x\geq 1} c_x|x\rangle \\ &= -\sum_x (-1)^{\delta_{x0}} c_x|x\rangle \end{aligned}$$

Exercise 6.2

$$\begin{aligned} &(2|\psi\rangle\langle\psi| - 1)\sum_k \alpha_k|k\rangle \\ &= 2\frac{1}{N}\sum_{xy}|x\rangle\langle y|\sum_k \alpha_k|k\rangle - \sum_k \alpha_k|k\rangle \\ &= 2\sum_x\left(\frac{1}{N}\sum_y \alpha_y\right)|x\rangle - \sum_k \alpha_k|k\rangle \\ &= \sum_k\left(-\alpha_k + 2\langle\alpha\rangle\right)|k\rangle \end{aligned}$$

Exercise 6.3

First we write O as

$$O = |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta| = \begin{pmatrix} |\alpha\rangle & |\beta\rangle \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \langle\alpha| \\ \langle\beta| \end{pmatrix}.$$

Similary we have

$$|\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha\rangle & |\beta\rangle \end{pmatrix}\begin{pmatrix} \cos^2\frac{\theta}{2} & \cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2}\sin\frac{\theta}{2} & \sin^2\frac{\theta}{2} \end{pmatrix}\begin{pmatrix} \langle\alpha| \\ \langle\beta| \end{pmatrix},$$

where $\cos\frac{\theta}{2} = \sqrt{(N-M)/N}$. Therefore we have

$$\begin{aligned} G &= (2|\psi\rangle\langle\psi| - 1)\, O \\ &= \begin{pmatrix} |\alpha\rangle & |\beta\rangle \end{pmatrix} \left(2 \begin{pmatrix} \cos^2\frac{\theta}{2} & \cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2}\sin\frac{\theta}{2} & \sin^2\frac{\theta}{2} \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \langle\alpha| \\ \langle\beta| \end{pmatrix} \\ &= \begin{pmatrix} |\alpha\rangle & |\beta\rangle \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \langle\alpha| \\ \langle\beta| \end{pmatrix}. \end{aligned}$$

Exercise 6.4

Exercise 6.5

Exercise 6.6

$$\begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix} \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= -2 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + 1 = -2\,(|0\rangle\langle 0| - 1)$$

7 Quantum computers: physical realization

8 Quantum noise and quantum operations

Exercise: 8.1

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

The output state ρ' can be represented by the wave-function $|\phi\rangle = U|\psi\rangle$ as

$$\rho' = |\phi\rangle\langle\phi| = U|\psi\rangle\langle\psi|U^\dagger = U\rho U^\dagger.$$

Exercise: 8.2

(Measurement as a quantum operation) Recall from Section2.2.3 (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

$$\frac{\mathcal{E}_m(\rho)}{\mathrm{tr}\left(\mathcal{E}_m(\rho)\right)}.$$

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

We assume that the state can be decomposed as $\rho = \sum_i p_i |\psi\rangle_i\langle\psi_i|$. For each component $|\psi_i\rangle$, the probability of measuring the outcome m is $p_{mi} = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle$ (with the corresponding output state $|\phi_{mi}\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{p_{mi}}}$). So the probability of final result of m is given by

$$\begin{aligned} p(m) &= \sum_i p_i \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \sum_i p_i \langle\psi_i|M_m^\dagger \left(\sum_x |x\rangle\langle x|\right) M_m|\psi_i\rangle \\ &= \sum_x \langle x|M_m \left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right) M_m^\dagger|x\rangle = tr\left(M_m\rho M_m^\dagger\right) = tr\left(\mathcal{E}_m(\rho)\right). \end{aligned}$$

$\rho_i' = M_m\rho_i M_m^\dagger$

$|\phi_{mi}\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{p_{mi}}}$

$$\begin{aligned} \rho' &= \sum_i p_i|\phi_{mi}\rangle\langle\phi_{mi}| = \sum_i p_i \frac{M_m|\psi_i\rangle}{\sqrt{p_{mi}}}\frac{\langle\psi_i|M_m^\dagger}{\sqrt{p_{mi}}} \\ &= \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{p_{mi}} = \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle} \\ &= \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger\left(\sum_x |x\rangle\langle x|\right)M_m|\psi_i\rangle} = \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{tr\left(M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger\right)} \end{aligned}$$

$tr(\rho') = \sum_i p_i \frac{p_{mi}}{tr\left(M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger\right)}$

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 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 system BC. Show that the map $\mathcal{E}(\rho) = \rho'$ satisfies

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

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

For input state $\rho \otimes |0_C\rangle\langle 0_c| \otimes |0_D\rangle\langle 0_D|$, the output state after U (U act on the composed space of A, B, C, D) is given as $U\rho|0_C\rangle\langle 0_c| \otimes |0_D\rangle\langle 0_D|U^\dagger$. The reduced density matrix in the space BC is given as

$$\begin{aligned}\rho' &= tr_{AD}\left(U\rho|0_C\rangle\langle 0_c| \otimes |0_D\rangle\langle 0_D|U^\dagger\right) \\ &= \sum_{ij}\langle i_A|\langle j_D|U\rho|0_C\rangle\langle 0_c| \otimes |0_D\rangle\langle 0_D|U^\dagger|i_A\rangle|j_D\rangle = \sum_{ij} F_{ij}\rho F_{ij}^\dagger\end{aligned}$$

where $F_{ij} = \langle i_A|\langle j_D|U|0_D\rangle|0_C\rangle$. One can also check that

$$\begin{aligned}\sum_{ij} F_{ij}^\dagger F_{ij} &= \langle 0_C|\langle 0_D|U^\dagger \left(\sum_i |i_A\rangle\langle i_A|\right)\left(\sum_j |j_D\rangle\langle j_D|\right) U|0_D\rangle|0_C\rangle \\ &= \langle 0_C|\langle 0_D|U^\dagger U|0_D\rangle|0_C\rangle = 1.\end{aligned}$$

Exercise: 8.4

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

$$U = P_0 \otimes I + P_1 \otimes X,$$

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 $|0\rangle$.

$\mathcal{E}(\rho) = \sum_{k=0}^{1} E_k \rho E_k$, where

$$\begin{aligned}E_0 &= \langle e_0|U|e_0\rangle = P_0 \\ E_1 &= \langle e_1|U|e_0\rangle = P_1\end{aligned}$$

Exercise: 8.5

(Spin flips) Just as in the previous exercise, but now let

$$U = \frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X,$$

Give the quantum operation for this process, in the operator-sum representation.

$$E_0 = \frac{X}{\sqrt{2}}$$
$$E_1 = \frac{Y}{\sqrt{2}}$$

Exercise: 8.6

(Composition of quantum operations)Suppose $\mathcal{E}$ and $\mathcal{F}$ are quantum operations on the same quantum system. Show that the composition $\mathcal{F} \circ \mathcal{E}$ is a quantum operation, in the sense that it has an operator-sum representation. State and prove an extension of this result to the case where $\mathcal{E}$ and $\mathcal{F}$ do not necessarily have the same input and output spaces.

For $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ and $\mathcal{F}(\rho) = \sum_l F_l \rho F_l^\dagger$, we have

$$(\mathcal{F} \circ \mathcal{E})(\rho) = \sum_l F_l \sum_k E_k \rho E_k^\dagger F_l^\dagger = \sum_{kl} (F_l E_k)\, \rho\, (F_l E_k)^\dagger .$$

Exercise: 8.7

Suppose that instead of doing a projective measurement on the combined principal system and environment we had performed a general measurement described by measurement operators $\{M_m\}$. Find operator-sum representations for the corresponding quantum operations $\mathcal{E}_m$ on the principal system, and show that the respective measurement probabilities are $tr[\mathcal{E}(\rho)]$.

Initial state is assumed to be $\rho \otimes \sigma = \rho \sum q_i |i\rangle\langle i|$. After the measurement of M_m,

$$\begin{aligned}
\mathcal{E}_m(\rho) &= tr_E \left(M_m U \rho \otimes \sigma U^\dagger M_m^\dagger \right) \\
&= \sum_i \sum_k q_i \langle e_k | M_m U \rho \otimes |i\rangle\langle i| U^\dagger M_m^\dagger | e_k \rangle \\
&= \sum_{ik} E_{ik} \rho E_{ik}^\dagger
\end{aligned}$$

where $E_{ik} = \sqrt{q_i} \langle e_k | M_m U | i \rangle$.

Exercise: 8.8

(Non-trace-preserving quantum operations) Explain how to construct a unitary operator for a system–environment model of a non-trace-preserving quantum operation, by introducing an extra operator, E_∞, into the set of operation elements E_k, chosen so that when summing over the complete set of k, including $k = \infty$, one obtains $\sum_k E_k^\dagger E_k = I$.

With including E_∞, we have $\sum_k E_k^\dagger E_k = 1$. Therefore U is defined by $U|\psi\rangle|e_0\rangle = \sum_k E_k |\psi\rangle |e_k\rangle$. The summation includes $k = \infty$.

Exercise: 8.9

(Measurement model) If we are given a set of quantum operations $\{\mathcal{E}_m\}$ such that $\sum_m \mathcal{E}_m$ is trace-preserving, then it is possible to construct a measurement model giving rise to this set of quantum operations. For each m, let E_{mk} be a set of operation elements for $\mathcal{E}_m$. Introduce an environmental system, E, with a northonormal basis $|m,k\rangle$ in one-to-one correspondence with the set of indices for the operation elements. Analogously to the earlier construction, define an operator U such that

$$U|\psi\rangle|e_0\rangle = \sum_{mk} E_{mk}|\psi\rangle|m,k\rangle.$$

Next, define projectors $P_m \equiv \sum_k |m,k\rangle\langle m,k|$ on the environmental system, E. Show that performing U on $\rho \otimes |e_0\rangle\langle e_0|$, then measuring P_m gives m with probability $\mathrm{tr}(\mathcal{E}_m(\rho))$, and the corresponding post-measurement state of the principal system is $\mathcal{E}_m(\rho)/\mathrm{tr}\left(\mathcal{E}_m(\rho)\right)$.

Assume that there are two degree of freedoms in the environment, by which we can study the partial trace (or say measurement) on the environment. Or in other words, part of the environment is under control. U is defined as

$$U|\psi\rangle|e_0\rangle = \sum_{mk} E_{mk}|\psi\rangle|mk\rangle.$$

For the input state $\rho \otimes |e_0\rangle\langle e_0| = \sum_i p_i|\psi_i\rangle|e_0\rangle\langle e_0|\langle\psi_i|$, U evolves the state as

$$\begin{aligned}
\rho' = U\rho \otimes |e_0\rangle\langle e_0|U^\dagger &= \sum_i p_i U|\psi_i\rangle|e_0\rangle\langle e_0|\langle\psi_i|U^\dagger \\
&= \sum_i p_i \sum_{nk}\sum_{n'k'} E_{nk}|\psi_i\rangle|nk\rangle\langle n'k'|\langle\psi_i|E^\dagger_{n'k'} \\
&= \sum_{nk}\sum_{n'k'} E_{nk}\rho E^\dagger_{n'k'} \otimes |nk\rangle\langle n'k'|
\end{aligned}$$

with projection P_m, the state collapses to $\rho'_m = \frac{\mathcal{E}_m}{tr(\mathcal{E}_m)}$, where $p(m) = 1/tr\left(\mathcal{E}_m\right)$ is the probability of observing m, and

$$\begin{aligned}
\mathcal{E}_m &= tr_E\left(P_m\rho' P_m\right) \\
&= \sum_k\sum_{k'} E_{mk}\rho E^\dagger_{mk'} tr_E\left(|mk\rangle\langle mk'|\right) = \sum_k E_{mk}\rho E^\dagger_{mk}.
\end{aligned}$$

One can check that

$$\sum_k E_{mk}E^\dagger_{mk} = 1 - \sum_{n\neq m}\sum_k E_{nk}E^\dagger_{nk} \leq 1.$$

Exercise: 8.10

Give a proof of Theorem 8.3 based on the freedom in the operator-sum representation, as follows. Let $\{E_j\}$ be a set of operation elements for $\mathcal{E}$. Define a matrix $W_{jk} \equiv \mathrm{tr}\left(E_j^\dagger E_k\right)$. Show that the matrix W is Hermitian and of rank at most d^2, and thus there is unitary matrix u such that $uWu^\dagger$ is diagonal with at most d^2 non-zero entries. Use u to define a new set of at most d^2 non-zero operation elements $\{F_j\}$ for $\mathcal{E}$.

As proved in Exercise 2.39, for space L_V with dimension d (where ρ stays), any operation in such space can at most has d^2 independent parameters. Therefore there can be (at most) $M = d^2$ independent $\{E_i\}$. W is Hermitian since $W_{jk}^* = \sum_x \langle x|E_j^\dagger E_k|x\rangle^* = \sum_x \langle x|E_k^\dagger E_j|x\rangle = W_{kj}$. We define a new set $\{F_j\}$ by

$$F_i = \sum_k u_{ik} E_k.$$

Therefore

$$\begin{aligned}\mathcal{E} &= \sum_k E_k \rho E_k^\dagger = \sum_k \left(\sum_i u_{kj} F_j\right) \rho \left(\sum_i u_{ki} F_i\right)^\dagger \\ &= \sum_{ij} \left(\sum_k u_{kj} u_{ki}^*\right) F_j \rho F_i^\dagger = \sum_i F_i \rho F_i^\dagger.\end{aligned}$$

Exercise 8.11-8.14

Exercise: 8.15

Suppose a projective measurement is performed on a single qubit in the basis $|+\rangle$, $|-\rangle$, where $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. In the event that we are ignorant of the result of the measurement, the density matrix evolves according to the equation

$$\rho \to \mathcal{E}(\rho) = |+\rangle\langle +|\rho|+\rangle\langle +| + |-\rangle\langle -|\rho|-\rangle\langle -|.$$

Illustrate this transformation on the Bloch sphere.

The measurement is given by $\{P_+, P_-\}$ where $P_\pm = |\pm\rangle\langle\pm|$. According to Eq. (2.152), the operation is given as

$$\mathcal{E}(\rho) = \sum_m P_m \rho P_m = |+\rangle\langle +|\rho|+\rangle\langle +| + |-\rangle\langle -|\rho|-\rangle\langle -|.$$

The operation element is given by

$$E_0 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \frac{1}{2} + \frac{1}{2}X,$$

and

$$E_1 = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1}{2} - \frac{1}{2}X,$$

from which we obtain that

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and $c = 0$.

Exercise 8.16

Exercise: 8.17

Verify (8.101) as follows. Define

$$\mathcal{E}(A) = \frac{A + XAX + YAY + ZAZ}{4},$$

and show that

$$\mathcal{E}(I) = I;\ \mathcal{E}(X) = \mathcal{E}(Y) = \mathcal{E}(Z) = 0.$$

Now use the Bloch sphere representation for single qubit density matrices to verify (8.101).

For $\mathcal{E}(A) = \frac{A+XAX+YAY+ZAZ}{4}$, we can easily have $\mathcal{E}(1) = 1$, $\mathcal{E}(X) = \mathcal{E}(Y) = \mathcal{E}(Z) = 0$. For a general state $\rho = \frac{1}{2}(1 + \boldsymbol{r}\cdot\boldsymbol{\sigma})$,we have

$$\mathcal{E}(\rho) = \mathcal{E}(\frac{1}{2} + \sum_i \frac{r_i}{2}\sigma_i) \xrightarrow{\text{Axiom 2}} \mathcal{E}(\frac{1}{2}) + \sum_i \frac{r_i}{2}\mathcal{E}(\sigma_i) = \frac{1}{2}.$$

Exercise: 8.18

For $k \geq 1$ show that $\mathrm{tr}(\rho_k)$ is never increased by the action of the depolarizing channel.

For the state $\rho = \frac{1}{2}(1 + \boldsymbol{r}\cdot\boldsymbol{\sigma})$, we have

$$\rho^k = \frac{1}{2^k}(1 + \boldsymbol{r}\cdot\boldsymbol{\sigma})^k = \frac{1}{2^k}\sum_{\xi=0}^{k}\begin{pmatrix} k \\ \xi \end{pmatrix}(\boldsymbol{r}\cdot\boldsymbol{\sigma})^\xi$$

It is easy to show the following relations:

$$\begin{aligned}
(\boldsymbol{r}\cdot\boldsymbol{\sigma})^2 &= r_1^2 + r_2^2 + r_3^2 = |r|^2 \\
(\boldsymbol{r}\cdot\boldsymbol{\sigma})^3 &= |r|^2(\boldsymbol{r}\cdot\boldsymbol{\sigma}) \\
&\cdots \\
(\boldsymbol{r}\cdot\boldsymbol{\sigma})^\xi &= |r|^{2[\xi/2]}(\boldsymbol{r}\cdot\boldsymbol{\sigma})^{\xi-2[\xi/2]},
\end{aligned}$$

where $[f]$ represent taking the integer part of f. Therefore

$$tr(\rho^k) = \frac{1}{2^k}\sum_{\xi=0}^{[k/2]} \begin{pmatrix} k \\ 2\xi \end{pmatrix} |r|^{2\xi} \cdot 2 = \frac{1}{2^{k-1}}\sum_{\xi=0}^{[k/2]} \frac{k!}{(2\xi)!(k-2\xi)!}|r|^{2\xi}.$$

For the depolarizing channel, $r \to (1-p)r < r$, therefore $tr(\rho^k)$ decreases with increasing k.

Exercise: 8.19

Find an operator-sum representation for a generalized depolarizing channel acting on a $d-$dimensional Hilbert space.

For d-dimensional case, $\mathcal{E}(\rho) = p\frac{1}{d} + (1-p)\rho$. First we select an orthonormal basis in such space $\{|i\rangle\}$. We can construct basis for any operator in the space as $\{X_\alpha\} = \{\frac{1}{\sqrt{d}}|i\rangle\langle j|\}$ for all $i \neq j$. Therefore $\alpha = 1, ..., d^2 - d$. The diagonal terms are $\{Y_i\} = \{\frac{1}{\sqrt{d}}|i\rangle\langle i|\}$ for all $i = 1, ..., d$. Therefore there are totally d^2 element in $\{X_\alpha, Y_i\}$ and any operator in this space can be decomposed by them.

However, we want to split the identical operator $\boldsymbol{I}$ from $\{Y_i\}$. According to the major spirit of Gram–Schmidt process, we replace $\{Y_i\}$ by $\{Z_i\}$, where $Z_1 = \frac{1}{\sqrt{d}}\boldsymbol{I}$ and all elements in $\{Z_i\}$ are orthonormal. We define Z_2 as follows. First we have

$$Z_2' = Y_2 - tr\left(Z_1^\dagger Y_2\right) Y_2.$$

and then we define

$$Z_2 = \frac{1}{\sqrt{tr\left(Z_2'\right)}} Z_2'.$$

For any $i \geq 2$, we define

$$Z_i' = Y_i - \sum_{j<i} tr\left(Z_j^\dagger Y_i\right) Y_i$$

and

$$Z_i = \frac{1}{\sqrt{tr\left(Z_i'\right)}} Z_i'.$$

We rearrange$\{X_\alpha, Z_i\}$ as $\{B_i | i = 1, ..., d^2\}$ and $B_1 = Z_1 = \frac{1}{\sqrt{d}}\boldsymbol{I}$. Therefore we can decomposed any operator A as $A = \sum_i a_i B_i$, where $a_i = tr\left(B_i^\dagger A\right)$.

Finally we define that $\mathcal{E}(A) = \sum_i B_i A B_i^\dagger$.

We first construct two kinds of operators: $\{X_\alpha\}$ and $\{Y_i\}$.

NOT WORK!!!

Exercise: 8.20

(Circuit model for amplitude damping) Show that the circuit in Figure 8.13 models the amplitude damping quantum operation, with $\sin^2(\theta/2) = \gamma$.

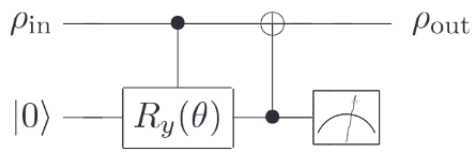


Figure 8.13. Circuit model for amplitude damping

The input state of the composed system is

$$\rho_{in} \otimes |0\rangle\langle 0| = \rho_{00}|00\rangle\langle 00| + \rho_{01}|00\rangle\langle 10| + \rho_{10}|10\rangle\langle 00| + \rho_{11}|10\rangle\langle 10|.$$

Use the formula $R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$, we calculate the output state of the control-R_y gate is

$$\begin{aligned}
\rho' &= C_{Ry}\left(\rho_{in} \otimes |0\rangle\langle 0|\right) C_{Ry}^{\dagger} \\
&= \rho_{00}|00\rangle\langle 00| + \rho_{01}\cos\frac{\theta}{2}|00\rangle\langle 10| + \sin\frac{\theta}{2}\rho_{01}|00\rangle\langle 11| + \rho_{10}\cos\frac{\theta}{2}|10\rangle\langle 00| + \rho_{10}\sin\frac{\theta}{2}|11\rangle\langle 00| \\
&+ \rho_{11}\cos\frac{\theta}{2}\cos\frac{\theta}{2}|10\rangle\langle 10| + \rho_{11}\cos\frac{\theta}{2}\sin\frac{\theta}{2}|10\rangle\langle 11| + \rho_{11}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|11\rangle\langle 10| + \rho_{11}\sin\frac{\theta}{2}\sin\frac{\theta}{2}|11\rangle\langle 11|.
\end{aligned}$$

Then we calculate the output state of the CNOT gate is

$$\begin{aligned}
\rho'' &= C_{not}\rho' C_{not}^{\dagger} \\
&= \rho_{00}|00\rangle\langle 00| + \rho_{01}\cos\frac{\theta}{2}|00\rangle\langle 10| + \sin\frac{\theta}{2}\rho_{01}|00\rangle\langle 01| + \rho_{10}\cos\frac{\theta}{2}|10\rangle\langle 00| + \rho_{10}\sin\frac{\theta}{2}|01\rangle\langle 00| \\
&+ \rho_{11}\cos\frac{\theta}{2}\cos\frac{\theta}{2}|10\rangle\langle 10| + \rho_{11}\cos\frac{\theta}{2}\sin\frac{\theta}{2}|10\rangle\langle 01| + \rho_{11}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|01\rangle\langle 10| + \rho_{11}\sin\frac{\theta}{2}\sin\frac{\theta}{2}|01\rangle\langle 01|.
\end{aligned}$$

Finally we measure the ancilla qubit and trace out the result to obtain

$$\mathcal{E}(\rho_{in}) = tr_R\left(\sum_m P_m \rho'' P_m\right) = \begin{pmatrix} |0\rangle & |1\rangle \end{pmatrix} \begin{pmatrix} \rho_{00} + \rho_{11}\sin\frac{\theta}{2}\sin\frac{\theta}{2} & \rho_{01}\cos\frac{\theta}{2} \\ \rho_{10}\cos\frac{\theta}{2} & \rho_{11}\cos\frac{\theta}{2}\cos\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} \langle 0| \\ \langle 1| \end{pmatrix} = \sum_{i=0}^{1} E_i \rho_{in} E_i^{\dagger}$$

where

$$E_0 = \begin{pmatrix} |0\rangle & |1\rangle \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} \begin{pmatrix} \langle 0| \\ \langle 1| \end{pmatrix},$$

and

$$E_1 = \begin{pmatrix} |0\rangle & |1\rangle \end{pmatrix} \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \langle 0| \\ \langle 1| \end{pmatrix},$$

with $\gamma \equiv \sin^2\theta$.

Exercise: 8.21

(Amplitude damping of a harmonic oscillator) Suppose that our principal system, a harmonic oscillator, interacts with an environment, modeled as another harmonic oscillator, through the Hamiltonian

$$H = \chi(a^\dagger b + b^\dagger a)$$

where a and b are the annihilation operators for the respective harmonic oscillators, as defined in Section 7.3.

(1) Using $U = \exp(-iH\Delta t)$, denoting the eigenstates of $b^\dagger b$ as $|k_b\rangle$, and selecting the vacuum state $|0_b\rangle$ as the initial state of the environment, show that the operation elements $E_k = \langle k_b|U|0_b\rangle$ are found to be

$$E_k = \sum_n \sqrt{\binom{n}{k}}\sqrt{(1-\gamma)^{n-k}\gamma^k}|n-k\rangle\langle n|,$$

where $\gamma = 1 - \cos^2(\chi\Delta t)$ is the probability of loosing a single quantum of energy, and states such as $|n\rangle$ are eigenstates of $a^\dagger a$.

(2) Show that the operation elements E_k define a trace-preserving quantum operation.

(1)

Let $X \equiv i\chi\Delta t(a^\dagger b + b^\dagger a)$, $Y \equiv b$, by the following useful expression

$$e^X Y e^{-X} = Y + [X,Y] + \frac{1}{2!}[X,[X,Y]] + \frac{1}{3!}[X,[X,[X,Y]]] + ...$$

we have

$$\begin{aligned}
U^\dagger bU &= e^X Y e^{-X} \\
&= \left(1 + \frac{-1}{2!}(\chi\Delta t)^2 + \frac{1}{4!}\left(\chi^4\Delta t^4\right) + ...\right) b - i\left((\chi\Delta t) + \frac{-1}{3!}(\chi\Delta t)^3 + \frac{1}{5!}(\chi\Delta t)^5 ...\right) a \\
&= b\sum_n \frac{(-1)^n(\chi\Delta t)^{2n}}{(2n)!} - ia\sum_n \frac{(-1)^n(\chi\Delta t)^{2n+1}}{(2n+1)!} \\
&= b\cos(\chi\Delta t) - ia\sin(\chi\Delta t).
\end{aligned}$$

Therefore $bU = UG_{\Delta t}$ where $G_{\Delta t} = b\cos(\chi\Delta t) - ia\sin(\chi\Delta t)$. Therefore we can obtain a useful expression that

$$\begin{aligned}
b^n U &= b^{n-1}(bU) = b^{n-1}UG_{\Delta t} = b^{n-2}(bU)G_{\Delta t} = b^{n-2}UG_{\Delta t}^2 \\
&= ... = U(b\cos(\chi\Delta t) - ia\sin(\chi\Delta t))^n.
\end{aligned}$$

Likewise we can also obtain $a^n U = U\left(a\cos\left(\chi\Delta t\right) - ib\sin\left(\chi\Delta t\right)\right)^n$. The operator element can be rewritten as

$$\begin{aligned}
E_k = \langle k_b|U|0_b\rangle &= \frac{1}{\sqrt{k!}}\langle 0_b|b^k U|0_b\rangle \\
&= \frac{1}{\sqrt{k!}}\langle 0_b|U\left(b\cos\left(\chi\Delta t\right) - ia\sin\left(\chi\Delta t\right)\right)^k|0_b\rangle \\
&= \frac{1}{\sqrt{k!}}\langle 0_b|U|0_b\rangle\left(-ia\sin\left(\chi\Delta t\right)\right)^k \\
&\xrightarrow{\gamma=1-\cos^2(\chi\Delta t)} \frac{1}{\sqrt{k!}}(-i)^k\gamma^{k/2}\langle 0_b|Ua^k|0_b\rangle.
\end{aligned}$$

We then need to calculate $\langle 0_b|Ua^k|0_b\rangle$. By $\sum_n |n_a\rangle\langle n_a| = 1$ we have

$$\begin{aligned}
\langle 0_b|U|0_b\rangle a^k &= \sum_{mn}\langle 0_b|\otimes|n_a\rangle\langle n_a|Ua^k|m_a\rangle\langle m_a|\otimes|0_b\rangle \\
&= \sum_{mn}\langle 0_b|\otimes|n_a\rangle\frac{1}{\sqrt{n!}}\langle 0_a|a^n Ua^k|m_a\rangle\langle m_a|\otimes|0_b\rangle \\
&= \sum_{mn}|n_a\rangle\frac{1}{\sqrt{n!}}\langle 0_a 0_b|U\left(a\cos\left(\chi\Delta t\right) - ib\sin\left(\chi\Delta t\right)\right)^n a^k|m_a 0_b\rangle\langle m_a| \\
&= \sum_{mn}|n_a\rangle\cos^n\left(\chi\Delta t\right)\frac{1}{\sqrt{n!}}\langle 0_a 0_b|Ua^{n+k}|m_a 0_b\rangle\langle m_a|.
\end{aligned}$$

We notice that $[a^\dagger a + b^\dagger b, H] = 0$. Therefore U do not change the total particle number $n_a + n_b$. For the product $0_a 0_b|Ua^{n+k}|m_a 0_b\rangle$, we know it must be $n + k = m$. Therefore

$$\begin{aligned}
\langle 0_b|U|0_b\rangle a^k &= \sum_{mn}|n_a\rangle\cos^n\left(\chi\Delta t\right)\frac{1}{\sqrt{n!}}\langle 0_a 0_b|\delta_{m=n+k}Ua^{n+k}|m_a 0_b\rangle\langle m_a| \\
&= \sum_{n}|n_a\rangle(1-\gamma)^{n/2}\sqrt{\frac{(n+k)!}{n!}}\langle 0_a 0_b|U|0_a 0_b\rangle\langle n+k_a| \\
&= \sum_{n}(1-\gamma)^{n/2}\sqrt{k!}\sqrt{\begin{pmatrix} n+k \\ k \end{pmatrix}}|n_a\rangle\langle n+k_a|.
\end{aligned}$$

And finally we have $E_k = (-i)^k\sum_n\sqrt{\begin{pmatrix} n+k \\ k \end{pmatrix}}\sqrt{(1-\gamma)^n\gamma^k}|n\rangle\langle n+k|$.

(2)

$$\begin{aligned}
\sum_k E_k^\dagger E_k &= \sum_k\sum_n\sum_m\sqrt{\begin{pmatrix} m \\ k \end{pmatrix}\begin{pmatrix} n \\ k \end{pmatrix}}\sqrt{(1-\gamma)^{m+n-2k}\gamma^{2k}}\delta_{mn}|n\rangle\langle m| \\
&= \sum_n\left(\sum_k\begin{pmatrix} n \\ k \end{pmatrix}(1-\gamma)^{n-k}\gamma^k\right)|n\rangle\langle n| = \sum_n\left(1-\gamma+\gamma\right)^{n+k}|n\rangle\langle n| = 1.
\end{aligned}$$

Exercise: 8.22

(Amplitude damping of single qubit density matrix) For the general single qubit state

$$\rho = \begin{pmatrix} a & b \\ b^* & c \end{pmatrix}$$

show that amplitude damping leads to

$$\mathcal{E}_{AD}(\rho) = \begin{pmatrix} 1-(1-\gamma)(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c(1-\gamma) \end{pmatrix}.$$

$$\begin{aligned}
&E_0\rho E_0^\dagger + E_1\rho E_1^\dagger \\
&= \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}\begin{pmatrix} a & b \\ b^* & c \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} + \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ b^* & c \end{pmatrix}\begin{pmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{pmatrix} \\
&= \begin{pmatrix} a & \sqrt{1-\gamma}b \\ \sqrt{1-\gamma}b^* & (1-\gamma)c \end{pmatrix} + \begin{pmatrix} \gamma c & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+\gamma c & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c(1-\gamma) \end{pmatrix} \\
&\xrightarrow{tr(\rho)=1\to a+c=1} \begin{pmatrix} a+\gamma(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c(1-\gamma) \end{pmatrix} = \begin{pmatrix} 1-(1-\gamma)(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c(1-\gamma) \end{pmatrix}
\end{aligned}$$

Exercise: 8.23

(Amplitude damping of dual-rail qubits) Suppose that a single qubit state is represented by using two qubits, as

$$|\psi\rangle = a|01\rangle + b|10\rangle.$$

Show that $\mathcal{E}_{AD} \otimes \mathcal{E}_{AD}$ applied to this state gives a process which can be described by the operation elements

$$\begin{aligned}
E_0^{dr} &= \sqrt{1-\gamma}I \\
E_1^{dr} &= \sqrt{\gamma}\left[|00\rangle\langle 01| + |00\rangle\langle 10|\right],
\end{aligned}$$

that is, either nothing (E_0^{dr}) happens to the qubit, or the qubit is transformed (E_1^{dr}) into the state $|00\rangle$, which is orthogonal to $|\psi\rangle$. This is a simple error-detection code, and is also the basis for the robustness of the 'dual-rail' qubit discussed in Section 7.4.

Assume the initial state is $\rho = \begin{pmatrix} |01\rangle & |10\rangle \end{pmatrix}\begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix}\begin{pmatrix} \langle 01| \\ \langle 10| \end{pmatrix}$, though the noisy channel

we have

$$\begin{aligned}\mathcal{E}_{AD}\otimes\mathcal{E}_{AD}(\rho) &= \rho_{00}\mathcal{E}_{AD}\otimes\mathcal{E}_{AD}(|01\rangle\langle 01|)+\rho_{01}\mathcal{E}_{AD}\otimes\mathcal{E}_{AD}(|01\rangle\langle 10|)\\ &+\rho_{10}\mathcal{E}_{AD}\otimes\mathcal{E}_{AD}(|10\rangle\langle 01|)+\rho_{11}\mathcal{E}_{AD}\otimes\mathcal{E}_{AD}(|10\rangle\langle 10|)\\ &=\rho_{00}\mathcal{E}_{AD}(|0\rangle\langle 0|)\otimes\mathcal{E}_{AD}(|1\rangle\langle 1|)+\rho_{01}\mathcal{E}_{AD}(|0\rangle\langle 1|)\otimes\mathcal{E}_{AD}(|1\rangle\langle 0|)\\ &+\rho_{10}\mathcal{E}_{AD}(|1\rangle\langle 0|)\otimes\mathcal{E}_{AD}(|0\rangle\langle 1|)+\rho_{11}\mathcal{E}_{AD}(|1\rangle\langle 1|)\otimes\mathcal{E}_{AD}(|0\rangle\langle 0|).\end{aligned}$$

According to the result of Exercise 8.22, we have the following relations:

$$\begin{aligned}\mathcal{E}_{AD}(|0\rangle\langle 0|) &= |0\rangle\langle 0|\\ \mathcal{E}_{AD}(|0\rangle\langle 1|) &= \sqrt{1-\gamma}|0\rangle\langle 1|\\ \mathcal{E}_{AD}(|1\rangle\langle 0|) &= \sqrt{1-\gamma}|1\rangle\langle 0|\\ \mathcal{E}_{AD}(|1\rangle\langle 1|) &= (1-\gamma)|1\rangle\langle 1|+\gamma|0\rangle\langle 0|.\end{aligned}$$

Therefore we have

$$\begin{aligned}\mathcal{E}_{AD}\otimes\mathcal{E}_{AD}(\rho) &= \rho_{00}(|0\rangle\langle 0|)\otimes(\gamma|0\rangle\langle 0|+(1-\gamma)|1\rangle\langle 1|)+\rho_{01}(1-\gamma)(|0\rangle\langle 1|)\otimes(|1\rangle\langle 0|)\\ &+\rho_{10}(1-\gamma)(|1\rangle\langle 0|)\otimes(|0\rangle\langle 1|)+\rho_{11}(\gamma|0\rangle\langle 0|+(1-\gamma)|1\rangle\langle 1|)\otimes(|0\rangle\langle 0|)\\ &=(\gamma\rho_{00}+\rho_{11}\gamma)|00\rangle\langle 00|\\ &+(1-\gamma)(\rho_{00}|01\rangle\langle 01|+\rho_{01}|01\rangle\langle 10|+\rho_{11}|10\rangle\langle 10|+\rho_{10}|10\rangle\langle 01|)\\ &.\end{aligned}$$

We can verify that

$$\mathcal{E}_{AD}\otimes\mathcal{E}_{AD}(\rho)=E_0^{dr}\rho E_0^{dr\dagger}+E_1^{dr}\rho E_1^{dr\dagger}?.$$

$$\rho = \rho_{00}|01\rangle\langle 01| + \rho_{01}|01\rangle\langle 10| + \rho_{10}|10\rangle\langle 01| + \rho_{11}|10\rangle\langle 10|$$

$$E_0^{dr}\rho E_0^{dr\dagger}=(1-\gamma)\rho$$

$$\begin{aligned}E_1^{dr}\rho E_1^{dr\dagger} &= \gamma(|00\rangle\langle 01|+|00\rangle\langle 10|)(\rho_{00}|01\rangle\langle 01|+\rho_{01}|01\rangle\langle 10|+\rho_{10}|10\rangle\langle 01|+\rho_{11}|10\rangle\langle 10|)(|01\rangle\langle 00|+|10\rangle\langle 00|)\\ &=\gamma(\rho_{00}+\rho_{01}+\rho_{10}+\rho_{11})|00\rangle\langle 00|\end{aligned}$$

Warning: Is there any problem with the problem?

Exercise: 8.24

(Spontaneous emission is amplitude damping) A single atom coupled to a single mode of electromagnetic radiation undergoes spontaneous emission, as was described in Section 7.6.1. To see that this process is just amplitude damping, take the unitary operation resulting from the Jaynes-Cummings interaction, Equation (7.77), with detuning $\delta = 0$, and give the quantum operation resulting from tracing over the field.

$U \xrightarrow{\delta=0} |00\rangle\langle 00| + \cos\Omega t|01\rangle\langle 01| + \cos\Omega t|10\rangle\langle 10| - i\sin\Omega t(|01\rangle\langle 10| + |10\rangle\langle 01|)$ where the left "bit" represents the optical field and the right bit represents the atom. Let us assume that the initial state of the atom is

$$\rho = \begin{pmatrix} |0\rangle & |1\rangle \end{pmatrix} \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \begin{pmatrix} \langle 0| \\ \langle 1| \end{pmatrix}.$$

Therefore U evolves the state to

$$\begin{aligned}
&U\left(|0\rangle\langle 0| \otimes \rho\right) U^\dagger \\
&= U\left(\rho_{00}|00\rangle\langle 00| + \rho_{01}|00\rangle\langle 01| + \rho_{10}|01\rangle\langle 00| + \rho_{11}|01\rangle\langle 01|\right) U^\dagger \\
&= \rho_{10}\cos\Omega t|01\rangle\langle 00| + \rho_{11}\cos^2\Omega t|01\rangle\langle 01| + i\rho_{11}\cos\Omega t\sin\Omega t|01\rangle\langle 10| - \rho_{10} i\sin\Omega t|10\rangle\langle 00| \\
&- \rho_{11} i\sin\Omega t\cos\Omega t|10\rangle\langle 01| + \rho_{11}\sin^2\Omega t|10\rangle\langle 10| + \rho_{00}|00\rangle\langle 00| + \rho_{01}\cos\Omega t|00\rangle\langle 01| + \rho_{01} i\sin\Omega t|00\rangle\langle 10|.
\end{aligned}$$

Then we trace out the filed to obtain

$$\begin{aligned}
&tr_{field}\left(U\left(|0\rangle\langle 0| \otimes \rho\right) U^\dagger\right) \\
&= \left(\rho_{00} + \rho_{11}\sin^2\Omega t\right)|0\rangle\langle 0| + \rho_{01}\cos\Omega t|0\rangle\langle 1| + \rho_{10}\cos\Omega t|1\rangle\langle 0| + \rho_{11}\cos^2\Omega t|1\rangle\langle 1| \\
&= E_0\rho E_0^\dagger + E_1\rho E_1^\dagger,
\end{aligned}$$

where

$$E_0 = \begin{pmatrix} |0\rangle & |1\rangle \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} \begin{pmatrix} \langle 0| \\ \langle 1| \end{pmatrix},$$

and

$$E_1 = \begin{pmatrix} |0\rangle & |1\rangle \end{pmatrix} \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \langle 0| \\ \langle 1| \end{pmatrix},$$

with $\gamma \equiv \sin^2\Omega t$.

Exercise: 8.25

If we define the temperature T of a qubit by assuming that in equilibrium the probabilities of being in the $|0\rangle$ and $|1\rangle$ states satisfy a Boltzmann distribution, that is $p_0 = e^{-E_0/k_BT}/\mathcal{Z}$ and $p_1 = e^{-E_1/k_BT}/\mathcal{Z}$, where E_0 is the energy of the state $|0\rangle$, E_1 the energy of the state $|1\rangle$, and $\mathcal{Z} = e^{-E_0/k_BT} + e^{-E_1/k_BT}$, what temperature describes the state ρ_∞?

For a given p, we can calculate $T(p)$. According to

$$\frac{1-p}{p} = \frac{p_1}{p_0} = e^{-\frac{E_1-E_0}{k_BT}},$$

we have $T = \frac{E_1-E_0}{k_B \ln\frac{p}{1-p}}$. For finite temperature case $p < 1-p$ which gives $p < \frac{1}{2}$. When $T \to 0$, $p \to 1$. And when $T \to \infty$, $p \to \frac{1}{2}$.

Exercise: 8.26

(Circuit model for phase damping) Show that the circuit in Figure 8.15 can be used to model the phase damping quantum operation, provided θ is chosen appropriately.

Assume the input state is $\rho = \rho_{in} \otimes |0\rangle\langle 0| = \rho_{00}|00\rangle\langle 00| + \rho_{01}|00\rangle\langle 10| + \rho_{10}|10\rangle\langle 00| + \rho_{11}|10\rangle\langle 10|$, we have the output state

$$\begin{aligned}\rho' &= C_{Ry}\rho C_{Ry}^\dagger \\ &= \rho_{00}|00\rangle\langle 00| + \cos\frac{\theta}{2}\rho_{01}|00\rangle\langle 10| - \sin\frac{\theta}{2}\rho_{01}|00\rangle\langle 11| + \cos\frac{\theta}{2}\rho_{10}|10\rangle\langle 00| - \sin\frac{\theta}{2}\rho_{10}|11\rangle\langle 00| \\ &+ \rho_{11}\cos^2\frac{\theta}{2}|10\rangle\langle 10| - \rho_{11}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|10\rangle\langle 11| - \rho_{11}\cos\frac{\theta}{2}\sin\frac{\theta}{2}|11\rangle\langle 10| + \rho_{11}\sin^2\frac{\theta}{2}|11\rangle\langle 11|.\end{aligned}$$

Then we calculate the reduced density matrix for the principle system to obtain

$$\begin{aligned}\mathcal{E}(\rho) = tr_E(\rho') &= \begin{pmatrix} |0\rangle & |1\rangle \end{pmatrix} \begin{pmatrix} \rho_{00} & \cos\frac{\theta}{2}\rho_{01} \\ \cos\frac{\theta}{2}\rho_{10} & \rho_{11} \end{pmatrix} \begin{pmatrix} \langle 0| \\ \langle 1| \end{pmatrix} \\ &= E_0\rho E_0^\dagger + E_1\rho E_1^\dagger\end{aligned}$$

where $\lambda = 1 - \cos^2\frac{\theta}{2}$.

Exercise: 8.27

(Phase damping = phase flip channel) Give the unitary transformation which relates the operation elements of (8.127)–(8.128) to those of (8.129)–(8.130); that is, find u such that $\tilde{E}_k = \sum_j u_{kj}E_j$.

Assume that $u = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}$ with $|a|^2 + |b|^2 = 1$, according to

$$\tilde{E}_0 = u_{00}E_0 + u_{01}E_1 = \begin{pmatrix} a & 0 \\ 0 & a\sqrt{1-\lambda} + b\sqrt{\lambda} \end{pmatrix} = \sqrt{\alpha}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\tilde{E}_1 = u_{10}E_0 + u_{11}E_1 = \begin{pmatrix} -b^* & 0 \\ 0 & -b^*\sqrt{1-\lambda} + a^*\sqrt{\lambda} \end{pmatrix} = \sqrt{1-\alpha}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

where $E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}$ and $E_0 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix}$, we can obtain

$$\begin{aligned} a &= \sqrt{\alpha} \\ b &= -\sqrt{1-\alpha} \end{aligned}$$

with $\alpha = \frac{1+\sqrt{1-\lambda}}{2}$.

Exercise: 8.28

(One CNOT phase damping model circuit) Show that a single controlled-NOT gate can be used as a model for phase damping, if we let the initial state of the environment be a mixed state, where the amount of damping is determined by the probability of the states in the mixture.

Consider two qubits with each state is $\rho \otimes e = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \otimes \begin{pmatrix} e_{00} & e_{01} \\ e_{10} & e_{11} \end{pmatrix}$, under the operation of CNOT gate (with control on ρ), we have

$$\begin{aligned}(\rho \otimes e)' &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \rho_{00}e_{00} & \rho_{00}e_{01} & \rho_{01}e_{00} & \rho_{01}e_{01} \\ \rho_{00}e_{10} & \rho_{00}e_{11} & \rho_{01}e_{10} & \rho_{01}e_{11} \\ \rho_{10}e_{00} & \rho_{10}e_{01} & \rho_{11}e_{00} & \rho_{11}e_{01} \\ \rho_{10}e_{10} & \rho_{10}e_{11} & \rho_{11}e_{10} & \rho_{11}e_{11} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \rho_{00}e_{00} & \rho_{00}e_{01} & \rho_{01}e_{01} & \rho_{01}e_{00} \\ \rho_{00}e_{10} & \rho_{00}e_{11} & \rho_{01}e_{11} & \rho_{01}e_{10} \\ \rho_{10}e_{10} & \rho_{10}e_{11} & \rho_{11}e_{11} & \rho_{11}e_{10} \\ \rho_{10}e_{00} & \rho_{10}e_{01} & \rho_{11}e_{01} & \rho_{11}e_{00} \end{pmatrix}.\end{aligned}$$

Then we calculate the reduced density matrix of the principle system as

$$\mathcal{E}(\rho) = tr_E \left(\sum_{ijkl} \xi_{ij,kl} |ij\rangle\langle kl| \right) = \sum_{ij} \varsigma_{ij} |i\rangle\langle j|,$$

where $\varsigma_{ij} = \sum_l \xi_{il,jl}$ is given by

$$\begin{aligned}\varsigma &= \begin{pmatrix} \xi_{00,00} + \xi_{01,01} & \xi_{00,10} + \xi_{01,11} \\ \xi_{10,00} + \xi_{11,01} & \xi_{10,10} + \xi_{11,11} \end{pmatrix} = \begin{pmatrix} \rho_{00}e_{00} + \rho_{00}e_{11} & \rho_{01}e_{01} + \rho_{01}e_{10} \\ \rho_{10}e_{10} + \rho_{10}e_{01} & \rho_{11}e_{11} + \rho_{11}e_{00} \end{pmatrix} \\ &\xrightarrow{e_{00}+e_{11}=1} \begin{pmatrix} \rho_{00} & \rho_{01}(e_{01} + e_{10}) \\ \rho_{10}(e_{01} + e_{10}) & \rho_{11} \end{pmatrix}\end{aligned}$$

let $\lambda = 1 - (e_{01} + e_{10})^2$, we have

$$\varsigma = \begin{pmatrix} \rho_{00} & \sqrt{1-\lambda}\rho_{01} \\ \sqrt{1-\lambda}\rho_{10} & (1-\lambda)\rho_{11} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & \lambda\rho_{11} \end{pmatrix} = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger.$$

where $E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}$ and $E_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix}$.

Exercise: 8.29

(Unitality) A quantum process $\mathcal{E}$ is unital if $\mathcal{E}(I) = I$. Show that the depolarizing and phase damping channels are unital, while amplitude damping is not.

For $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$, we have $\mathcal{E}(1) = \sum_i E_i E_i^\dagger$. For amplitude damping case where $E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}$ and $E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$, we have $\mathcal{E}(1) = \begin{pmatrix} 1+\gamma & 0 \\ 0 & 1-\gamma \end{pmatrix}$.

Warning: When we check the depolarizing channel, we cannot use the expression of $\mathcal{E} = \frac{p}{2} + (1-p)\rho$. The invalidation is coming from the fact that Eq. (8.101) is not true for $\rho = I$. One should also notice that for any physical system we have $tr(\rho) = 1$, but $tr(I) = 2$. Therefore $\rho = I$ is NOT a physical system.

Exercise: 8.30

($T_2 \leq T_1/2$) The T_2 phase coherence relaxation rate is just the exponential decay rate of the off-diagonal elements in the qubit density matrix, while T_1 is the decay rate of the diagonal elements (see Equation (7.144)). Amplitude damping has both nonzero T_1 and T_2 rates; show that for amplitude damping $T_2 = T_1/2$. Also show that if amplitude and phase damping are both applied then $T_2 \leq T_1/2$.

Consider a qubit of a initial state $\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix}$. Under the noisy channel we have

According to Exercise 8.22, $\mathcal{E}_{AD}(\rho) = \begin{pmatrix} \rho_{00} + \gamma\rho_{11} & \rho_{01}\sqrt{1-\gamma} \\ \rho_{10}\sqrt{1-\gamma} & \rho_{11}(1-\gamma) \end{pmatrix}$

$\mathcal{E}(\rho)$

$$\mathcal{E}_{AD}(\rho) = \begin{pmatrix} 1-(1-\gamma)(1-\rho_{00}) & \rho_{01}\sqrt{1-\gamma} \\ \rho_{10}\sqrt{1-\gamma} & \rho_{11}(1-\gamma) \end{pmatrix} = \begin{pmatrix} 1-(1-\gamma)(1-\rho_{00}) & \rho_{01}\sqrt{1-\gamma} \\ \rho_{10}\sqrt{1-\gamma} & \rho_{11} - \rho_{11}\sin^2\Delta t \end{pmatrix}$$

$$\begin{pmatrix} \rho_{00} + \gamma\rho_{11} & \rho_{01}\sqrt{1-\gamma} \\ \rho_{10}\sqrt{1-\gamma} & \rho_{11}(1-\gamma) \end{pmatrix} \quad = \quad \begin{pmatrix} \rho_{00}\cos^2\theta + \sin^2\theta & \rho_{01}\cos\theta \\ \rho_{10}\cos\theta & \rho_{11}\cos^2\theta \end{pmatrix}$$

$\rho_{00}(t) = \rho_{00} e^{-\frac{t}{T_1}}$

$\rho_{00}\cos^2\theta_1 + \sin^2\theta_1 = \frac{1}{e}\rho_{00}$

$\rho_{01}\cos\theta_2 = \frac{1}{-}$

$\rho_{00}(\infty) = \left(\theta = \frac{\pi}{2}\right) =$

$\rho_{00}\cos^2\theta_1 \quad + \quad \sin^2\theta_1 \quad = \quad \frac{1}{e}\rho_{00}$

Exercise: 8.31

(Exponential sensitivity to phased amping) Using (8.126), show that the element $\rho_{nm} = \langle n|\rho|m\rangle$ in the density matrix of a harmonic oscillator decays exponentially as $e^{-\lambda(n-m)^2}$ under the effect of phase damping, for some constant λ.

Consider a harmonic oscillator in the state $\rho = \sum_{mn} \rho_{mn}|m\rangle\langle n|$. The noisy channel transfer it to

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger = \sum_{mn} \rho_{mn} \left(\sum_k E_k |m\rangle\langle n| E_k^\dagger \right),$$

where $E_k = \langle k_b|U|0_b\rangle = \langle k_b|e^{-i\chi\Delta t a^\dagger a(b+b^\dagger)}|0_b\rangle = \langle k_b|e^{T(X+Y)}|0_b\rangle$, and $X = a^\dagger a b^\dagger$, $Y = a^\dagger a b$ and $T = -i\chi\Delta t$. According to a easy calculation, we know that $[X,Y] = -\left(a^\dagger a\right)^2$ and $[X,[X,Y]] = [Y,[X,Y]] = 0$. Therefore we have

$$\begin{aligned} U = e^{T(X+Y)} &= e^{TX} e^{TY} e^{-\frac{T^2}{2}[X,Y]} \\ &= e^{-i\chi\Delta t a^\dagger a b^\dagger} e^{-i\chi\Delta t a^\dagger a b} e^{\frac{-\chi^2\Delta t^2}{2}\left(a^\dagger a\right)^2} \\ &= e^{\frac{-\chi^2\Delta t^2}{2}\left(a^\dagger a\right)^2} e^{-i\chi\Delta t a^\dagger a b^\dagger} e^{-i\chi\Delta t a^\dagger a b} \end{aligned}$$

Then we have

$$\begin{aligned} E_k &= \langle k_b| e^{\frac{-\chi^2\Delta t^2}{2}\left(a^\dagger a\right)^2} e^{-i\chi\Delta t a^\dagger a b^\dagger} e^{-i\chi\Delta t a^\dagger a b} |0_b\rangle \\ &= \langle k_b| e^{\frac{-\chi^2\Delta t^2}{2}\left(a^\dagger a\right)^2} \sum_m \frac{\left(-i\chi\Delta t a^\dagger a\right)^m}{m!} b^{\dagger m} |0_b\rangle \\ &\xrightarrow{\text{only } m=k} e^{\frac{-\chi^2\Delta t^2}{2}\left(a^\dagger a\right)^2} \frac{\left(-i\chi\Delta t a^\dagger a\right)^k}{\sqrt{k!}} \end{aligned}$$

And then we have

$$\begin{aligned} &\sum_k E_k |m\rangle\langle n| E_k^\dagger \\ &= e^{\frac{-\chi^2\Delta t^2}{2}\left(m^2+n^2\right)} \sum_k \frac{1}{k!} \frac{\left(\chi^2\Delta t^2 mn\right)^k}{\sqrt{k!}} |m\rangle\langle n| \\ &= e^{-\frac{\chi^2\Delta t^2}{2}\left(m^2+n^2-2mn\right)} |m\rangle\langle n| = e^{-\frac{\chi^2\Delta t^2}{2}(n-m)^2} |m\rangle\langle n|. \end{aligned}$$

And finally we have

$$\mathcal{E}(\rho) = \sum_{mn} \left(\rho_{mn} e^{-\frac{\chi^2\Delta t^2}{2}(n-m)^2} \right) |m\rangle\langle n|,$$

from which we see that $\lambda = \frac{\chi^2\Delta t^2}{2}$.

Exercise 8.32

Exercise 8.33

Use two different $\mathcal{E}$ to show that the output of $\{r_k\}$ are the same if $k \leq 3$.

Exercise 8.34

Exercise: 8.35

(Process tomography example) Consider a one qubit black box of unknown dynamics $\mathcal{E}_1$. Suppose that the following four density matrices are obtained from experimental measurements, performed according to Equations (8.173)–(8.176):

$$\rho_1' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\rho_2' = \begin{pmatrix} 0 & \sqrt{1-\gamma} \\ 0 & 0 \end{pmatrix}$$
$$\rho_3' = \begin{pmatrix} 0 & 0 \\ \sqrt{1-\gamma} & 0 \end{pmatrix}$$
$$\rho_4' = \begin{pmatrix} \gamma & 0 \\ 0 & 1-\gamma \end{pmatrix}$$

where γ is a numerical parameter. From an independent study of each of these input–output relations, one could make several important observations: the ground state $|0\rangle$ is left invariant by $\mathcal{E}_1$,the excited state $|1\rangle$ partially decays to the ground state, and superposition states are damped. Determine the χ matrix for this process.

According to Eq. (8.179), we have

$$\begin{aligned}
\chi &= \frac{1}{4}\begin{pmatrix} I & X \\ X & -I \end{pmatrix}\begin{pmatrix} \rho_1' & \rho_2' \\ \rho_3' & \rho_4' \end{pmatrix}\begin{pmatrix} I & X \\ X & -I \end{pmatrix} \\
&= \frac{1}{4}\begin{pmatrix} (\rho_1'+\rho_4') + X(\rho_2'+\rho_3') & X(\rho_1'-\rho_4') - (\rho_2'-\rho_3') \\ X(\rho_1'-\rho_4') + (\rho_2'-\rho_3') & (\rho_1'+\rho_4') - X(\rho_2'+\rho_3') \end{pmatrix} \\
&= \frac{1}{4}\begin{pmatrix} 1+\gamma+\sqrt{1-\gamma} & 0 & 0 & \gamma-1-\sqrt{1-\gamma} \\ 0 & 1-\gamma+\sqrt{1-\gamma} & 1-\gamma+\sqrt{1-\gamma} & 0 \\ 0 & \gamma-1+\sqrt{1-\gamma} & 1+\gamma-\sqrt{1-\gamma} & 0 \\ 1-\gamma-\sqrt{1-\gamma} & 0 & 0 & 1-\gamma-\sqrt{1-\gamma} \end{pmatrix}
\end{aligned}$$

Problem: 8.1

(Lindblad form to quantum operation) In the notation of Section 8.4.1, explicitly work through

the steps to solve the differential equation

$$\dot{\rho} = -\frac{\lambda}{2}\left(\sigma_+\sigma_-\rho + \rho\sigma_+\sigma_- - 2\sigma_-\rho\sigma_+\right)$$

for $\rho(t)$. Express the map $\rho(0) \to \rho(t)$ as $\rho(t) = \sum_k E_k(t)\rho(0)E_k^\dagger(t)$.

Let $\rho(t) = \begin{pmatrix} r(t) & s(t) \\ s^*(t) & 1-r(t) \end{pmatrix}$, the differential equation becomes

$$\frac{d\rho(t)}{dt} = \begin{pmatrix} \dot{r}(t) & \dot{s}(t) \\ \dot{s}^*(t) & -\dot{r}(t) \end{pmatrix} = -\frac{\lambda}{2}\begin{pmatrix} -2\left(1-r(t)\right) & s(t) \\ s^*(t) & 2\left(1-r(t)\right) \end{pmatrix}.$$

Then we have

$$\begin{cases} \frac{d}{dt}r(t) = \lambda\left(1-r(t)\right) \\ \frac{d}{dt}s(t) = -\frac{\lambda}{2}s(t) \end{cases}.$$

The solution of the set of equations is $r(t) = 1 + \left(r(0)-1\right)e^{-\lambda t}$ and $s = s(0)e^{-\frac{\lambda}{2}t}$. Therefore we have

$$\rho(t) = \begin{pmatrix} 1 + \left(r(0)-1\right)e^{-\lambda t} & s(0)e^{-\frac{\lambda}{2}t} \\ s^*(0)e^{-\frac{\lambda}{2}t} & \left(1-r(0)\right)e^{-\lambda t} \end{pmatrix} = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger,$$

where $E_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}$ and $E_2 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$, with $\gamma = 1 - e^{-\lambda t}$.

Problem: 8.2

(Teleportation as a quantum operation) Suppose Alice is in possession of a single qubit, denoted as system 1, which she wishes to teleport to Bob. Unfortunately, she and Bob only share an imperfectly entangled pair of qubits. Alice's half of this pair is denoted system 2, and Bob's half is denoted system 3. Suppose Alice performs a measurement described by a set of quantum operations $\mathcal{E}_m$ with result m on systems 1 and 2. Show that this induces an operation $\tilde{\mathcal{E}}_m$ relating the initial state of system 1 to the final state of system 3, and that teleportation is accomplished if Bob can reverse this operation using a trace-preserving quantum operation $\mathcal{R}_m$, to obtain

$$\mathcal{R}_m\left(\frac{\tilde{\mathcal{E}}_m(\rho)}{\mathrm{tr}\left[\tilde{\mathcal{E}}_m(\rho)\right]}\right) = \rho,$$

where ρ is the initial state of system 1.

For a two-qubit system, any state can be decomposed by Bell basis $\{|\Phi^\pm\rangle, |\Psi^\pm\rangle\} \equiv \{|B_i\rangle | i = 1,2,3,4\}$. Suppose the imperfect pair is given by $\rho_{Bell} = \sum_{i,j=1}^4 \xi_{ij}|B_i\rangle\langle B_j|$. Also write the initial state as $\rho = \sum_{kl}\rho_{kl}|k\rangle\langle l|$. The composed system is represented by

$$\rho \otimes \rho_{Bell} = \sum_{kl}\sum_{ij}\rho_{kl}\xi_{ij}|kB_i\rangle\langle lB_j|.$$

$$\begin{pmatrix} \rho_{00}\xi & \rho_{01}\xi \\ \rho_{10}\xi & \rho_{11}\xi \end{pmatrix}$$

For the standard version of teleportation (follow section 1.3.7), the entangled state is $|B_1\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

$$\rho' \qquad = \qquad P_m \sum_{kl} \sum_{ij} \rho_{kl}\xi_{ij} |kB_i\rangle\langle lB_j| P_m$$

9 Distance measures for quantum information

Exercise: 9.1

What is the trace distance between the probability distribution (1, 0) and the probability distribution (1/2, 1/2)? Between (1/2, 1/3, 1/6) and (3/4, 1/8, 1/8)?

$$D\left(\{1,0\},\{\frac{1}{2},\frac{1}{2}\}\right) = \frac{1}{2}\left(|1-\frac{1}{2}| + |0-\frac{1}{2}|\right) = \frac{1}{2}.$$

$$D\left(\{\frac{1}{2},\frac{1}{3},\frac{1}{6}\},\{\frac{3}{4},\frac{1}{8},\frac{1}{8}\}\right) = \frac{1}{2}\left(|\frac{1}{2}-\frac{3}{4}| + |\frac{1}{3}-\frac{1}{8}| + |\frac{1}{6}-\frac{1}{8}|\right) = \frac{1}{4}.$$

Exercise: 9.2

Show that the trace distance between probability distributions (p, 1 − p) and (q, 1 − q) is |p − q|.

$$D\left(\{p,1-p\},\{q,1-q\}\right) = \frac{1}{2}\left(|p-q| + |\,(1-p)-(1-q)\,|\right) = |p-q|.$$

Exercise: 9.3

What is the fidelity of the probability distributions (1, 0) and (1/2, 1/2)? Of (1/2, 1/3, 1/6) and (3/4, 1/8, 1/8)?

$$F\left(\{1,0\},\{\frac{1}{2},\frac{1}{2}\}\right) = 1/\sqrt{2}$$

$$F\left(\{\frac{1}{2},\frac{1}{3},\frac{1}{6}\},\{\frac{3}{4},\frac{1}{8},\frac{1}{8}\}\right) = \frac{1+4\sqrt{2}}{4\sqrt{3}}.$$

Exercise: 9.4

Prove (9.3):

$$D(p_x, q_x) = \max_S \left| \sum_{x \in S} p_x - \sum_{x \in S} q_x \right|.$$

We can write

$$D(p_x, q_x) = \frac{1}{2} \sum_x |p_x - q_x| = \frac{1}{2} \left(\sum_{x \in X_1} + \sum_{x \in X_2} \right) |p_x - q_x| .$$

The original domain is split into two sets $\{x\} = Q + P$, where for $x \in Q$ all $p_x \geq q_x$, and for $x \in P$ all $p_x < q_x$. Therefore we have

$$\begin{aligned} D(p_x, q_x) &= \frac{1}{2} \sum_{x \in Q} (p_x - q_x) - \frac{1}{2} \sum_{x \in P} (p_x - q_x) \\ &= \frac{1}{2} \sum_{x \in Q} (p_x - q_x) - \frac{1}{2} \left(1 - \sum_{x \in Q} p_x \right) + \frac{1}{2} \left(1 - \sum_{x \in Q} q_x \right) \\ &= \sum_{x \in Q} p_x - \sum_{x \in Q} q_x = \max_S \left(\sum_{x \in S} p_x - \sum_{x \in S} q_x \right). \end{aligned}$$

When $S = Q$, the last expression reach its max value.

Exercise: 9.5

Show that the absolute value signs may be removed from Equation (9.3), that is,

$$D\left(p_x, q_x\right) = \max_S \left(p(S) - q(S)\right) = \max_S \left(\sum_{x \in S} p_x - \sum_{x \in S} q_x \right).$$

Done!

Exercise: 9.6

What is the trace distance between the density operators

$$\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|; \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|?$$

Between:

$$\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|; \frac{2}{3}|+\rangle\langle +| + \frac{1}{3}|-\rangle\langle -|?$$

(Recall that $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$.)

$$D\left(\begin{pmatrix} \frac{3}{4} & 0 \\ 0 & \frac{1}{4} \end{pmatrix}, \begin{pmatrix} \frac{2}{3} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}\right) = \frac{1}{24}\mathrm{tr}\left|\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right| = \frac{1}{12}.$$

$$\begin{aligned} D\left(\begin{pmatrix} \frac{3}{4} & 0 \\ 0 & \frac{1}{4} \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} \frac{2}{3} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\right) &= D\left(\begin{pmatrix} \frac{3}{4} & 0 \\ 0 & \frac{1}{4} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{2} \end{pmatrix}\right) \\ &= \frac{1}{2}\mathrm{tr}\left|\begin{pmatrix} \frac{1}{4} & -\frac{1}{6} \\ -\frac{1}{6} & -\frac{1}{4} \end{pmatrix}\right| = \frac{\sqrt{13}}{12}. \end{aligned}$$

Exercise: 9.7

Show that for any states ρ and σ, one may write $\rho - \sigma - Q - S$, where Q and S are positive operators with support on orthogonal vector spaces. (Hint: use the spectral decomposition $\rho - \sigma = UDU^\dagger$, and split the diagonal matrix D into positive and negative parts. This fact will continue to be useful later.)

Since $\rho - \sigma$ is hermitian, there exist a U such that $\rho - \sigma = UDU^\dagger$, with real and diagonal D. We can split the positive part and negative part as $D = D_+ - D_-$. Therefore both D_+ and D_- is positive, and $Q = UD_+U^\dagger$ and $S = UD_-U^\dagger$.

Alternatively, we can rewrite it in a block matrix form as $\rho - \sigma = \begin{pmatrix} u_+ & u_- \end{pmatrix}\begin{pmatrix} d_+ & 0 \\ 0 & -d_- \end{pmatrix}\begin{pmatrix} u_+^\dagger \\ u_-^\dagger \end{pmatrix}$.

Therefore $Q = u_+ d_+ u_+^\dagger \oplus \mathbf{0}$ and $S = \mathbf{0} \oplus u_- d_- u_-^\dagger$.

Exercise: 9.8

(Convexity of the trace distance) Show that the trace distance is convex in its first input,

$$D\left(\sum_i p_i\rho_i, \sigma\right) \leq \sum_i p_i D\left(\rho_i, \sigma\right).$$

By symmetry convexity in the second entry follows from convexity in the first.

Let $q_i = \delta_{i1}$, therefore we have $D\left(\sum_i p_i\rho_i, \sigma\right) = D\left(\sum_i p_i\rho_i, \sum_i q_i\sigma\right)$. Due to Theorem 9.3, we have $D\left(\sum_i p_i\rho_i, \sum_i q_i\sigma\right) \leq D\left(p_i, q_i\right) + \sum_i p_i D\left(\rho_i, \sigma\right)$. Therefore we have

$$D\left(\sum_i p_i\rho_i, \sigma\right) \leq \frac{1 - p_1}{2} + \frac{1}{2}\sum_{i>1}|p_i - q_i| + \sum_i p_i D\left(\rho_i, \sigma\right) \leq \sum_i p_i D\left(\rho_i, \sigma\right).$$

Exercise: 9.9

(Existence of fixed points) Schauder's fixed point theorem is a classic result from mathematics that implies that any continuous map on a convex, compact subset of a Hilbert space has a fixed point. Use Schauder's fixed point theorem to prove that any trace-preserving quantum operation $\mathcal{E}$ has a fixed point, that is, ρ such that $\mathcal{E}(\rho) = \rho$.

–

Exercise: 9.10

Suppose $\mathcal{E}$ is a strictly contractive trace-preserving quantum operation, that is, for any ρ and σ, $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$. Show that E has a unique fixed point.

Assume that $\mathcal{E}$ has two different fixed point ρ and σ. $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) = D(\rho, \sigma)$ which is contradicted to $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$.

Exercise: 9.11

Suppose $\mathcal{E}$ is a trace-preserving quantum operation for which there exists a density operator ρ_0 and a trace-preserving quantum operation $\mathcal{E}'$ such that

$$\mathcal{E}(\rho) = p\rho_0 + (1-p)\mathcal{E}'(\rho),$$

for some p, $0 < p < 1$. Physically, this means that with probability p the input state is thrown out and replaced with the fixed state ρ_0, while with probability $1-p$ the operation $\mathcal{E}'$ occurs. Use joint convexity to show that $\mathcal{E}$ is a strictly contractive quantum operation, and thus has a unique fixed point.

According to Exercise 9.9 we know that for any trace-preserving $\mathcal{E}$, there exist a fixed point ρ_0 so that $\mathcal{E}(\rho_0) = \rho_0$. The fixed point can be represented as $\rho_0 = \sum_{i=1}^{M} \lambda_i |\psi_i\rangle\langle\psi_i|$, where $\sum_i \lambda_i = 1$. We can use the standard Gram–Schmidt process to find a set of basis $S = \{|i\rangle | i = 1, ..., M\}$ by $\{|\psi_i\rangle | i = 1, ..., M\}$. Assume that the dimension of the whole space is N, therefore there are still $N - M$ degree of freedoms. We can further complement $P = \{|i\rangle | i = M+1, ..., N\}$. Thus $S + P$ can be used to expand any states. Let define a artificial density matrix given by

$$\sigma_0 = \frac{1}{N-M} \sum_{i=M+1}^{N} |\phi_i\rangle\langle\phi_i|.$$

Therefore any given ρ can be written as

$$\rho = \operatorname{tr}(\rho_0\rho)\,\rho_0 + \sum_{i=M+1}^{N} \operatorname{tr}(\sigma_i\rho)\,\sigma_i$$

where $\sigma_i \equiv |\phi_i\rangle\langle\phi_i|$. $\rho = \sum \rho_{ij} |\phi_i\rangle\langle\phi_i|$ Matrix basis$\{\rho_0, \sigma_2, ..., \sigma_{d^2}\}$

$$\rho = \operatorname{tr}(\rho_0\rho)\,\rho_0 + \sum_{i=2}^{d^2} \operatorname{tr}(\sigma_i\rho)\,\sigma_i$$

$$\rho_0 = \sum_{ij\in S} \rho_0^{ij}|i\rangle\langle j|$$

$$\rho = \sum_{ij} \rho_{ij}|i\rangle\langle j|$$

$$\mathrm{tr}\left(\rho_0\rho\right) =$$

Exercise: 9.12

Consider the depolarizing channel introduced in Section 8.3.4 on page 378, $\mathcal{E}(\rho) = pI/2 + (1-p)\rho$. For arbitrary ρ and σ find $D(\mathcal{E}(\rho), \mathcal{E}(\sigma))$ using the Bloch representation, and prove explicitly that the map $\mathcal{E}$ is strictly contractive, that is, $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$.

$$\begin{aligned} D\left(\mathcal{E}(\rho), \mathcal{E}(\sigma)\right) &= \frac{1-p}{2}\mathrm{tr}\left|\rho - \sigma\right| \\ &= \frac{1-p}{2}\mathrm{tr}\left|\frac{1+\boldsymbol{r}_\rho\cdot\boldsymbol{\sigma}}{2} - \frac{1+\boldsymbol{r}_\sigma\cdot\boldsymbol{\sigma}}{2}\right| = \frac{1-p}{4}\mathrm{tr}\left|(\boldsymbol{r}_\rho - \boldsymbol{r}_\sigma)\cdot\boldsymbol{\sigma}\right|, \end{aligned}$$

where $\boldsymbol{r}_\rho$ and $\boldsymbol{r}_\sigma$ are vectors in Block sphere. Let $\boldsymbol{r} = \frac{\boldsymbol{r}_\rho - \boldsymbol{r}_\sigma}{|\boldsymbol{r}_\rho - \boldsymbol{r}_\sigma|}$, then

$$\begin{aligned} D\left(\mathcal{E}(\rho), \mathcal{E}(\sigma)\right) &= \frac{1-p}{4}\left|\boldsymbol{r}_\rho - \boldsymbol{r}_\sigma\right|\mathrm{tr}\left|\boldsymbol{r}\cdot\boldsymbol{\sigma}\right| \\ &= \frac{1-p}{4}\left|\boldsymbol{r}_\rho - \boldsymbol{r}_\sigma\right|\mathrm{tr}\left|\sigma_r\right| = \frac{1-p}{4}\left|\boldsymbol{r}_\rho - \boldsymbol{r}_\sigma\right| \times 2 \\ &\xrightarrow{\text{Eq. (9.20) in book}} (1-p)\,D\left(\rho,\sigma\right) < D\left(\rho,\sigma\right). \end{aligned}$$

Exercise: 9.13

Show that the bit flip channel (Section 8.3.3) is contractive but not strictly contractive. Find the set of fixed points for the bit flip channel.

For bit flip case, $\mathcal{E}(\rho) = p\rho + (1-p)\,X\rho X$. With the Block representation $\rho = \frac{1+\boldsymbol{r}\cdot\boldsymbol{\sigma}}{2}$ we have

$$\mathcal{E}(\rho) = p\frac{1+\boldsymbol{r}\cdot\boldsymbol{\sigma}}{2} + (1-p)\,\frac{1+\boldsymbol{r}\cdot X\boldsymbol{\sigma}X}{2}.$$

We can further have

$$\begin{aligned} \boldsymbol{r}\cdot X\boldsymbol{\sigma}X &= \begin{pmatrix} r_x & r_y & r_z \end{pmatrix} X \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} X \\ &= \begin{pmatrix} r_x & r_y & r_z \end{pmatrix} \begin{pmatrix} X \\ -Y \\ -Z \end{pmatrix} = \begin{pmatrix} r_x & -r_y & -r_z \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \boldsymbol{r}'\cdot\boldsymbol{\sigma}, \end{aligned}$$

where $\boldsymbol{r}'$ represents the reflection about $y=0$ and $z=0$ from $\boldsymbol{r}$. Therefore we have

$$D\left(\mathcal{E}(\rho),\mathcal{E}(\sigma)\right)=\frac{1}{2}\mathrm{tr}\left|\frac{p}{2}\left(\boldsymbol{r}_\rho-\boldsymbol{r}_\sigma\right)\cdot\boldsymbol{\sigma}+\frac{1-p}{2}\left(\boldsymbol{r}'_\rho-\boldsymbol{r}'_\sigma\right)\cdot\boldsymbol{\sigma}\right|.$$

We see that if $\boldsymbol{r}'_\rho-\boldsymbol{r}'_\sigma=\boldsymbol{r}_\rho-\boldsymbol{r}_\sigma$, then we have $D\left(\mathcal{E}(\rho),\mathcal{E}(\sigma)\right)=D\left(\rho,\sigma\right)$ (not strictly contractive). In that case $r_{\rho i}=r_{\sigma i}$ for $i=y,z$.

Meanwhile, fixed points are those ρ_0 where $r_y=r_z=0$ in the Block representation. Therefore

$$\rho_0(x)=\frac{1+xX}{2}=\frac{1}{2}\begin{pmatrix}1&x\\x&1\end{pmatrix}.$$

Exercise: 9.14

(Invariance of fidelity under unitary transforms) Prove (9.61) by using the fact that for any positive operator A, $\sqrt{UAU^\dagger}=U\sqrt{A}U^\dagger$.

For any positive operator A with spectra decomposition, we have $A=\sum_i a_i|i\rangle\langle i|$. For any unitary transformation U, we have $U|i\rangle=|i'\rangle$. Therefore we can prove that

$$\sqrt{UAU^\dagger}=\sqrt{\sum_i a_i|i'\rangle\langle i'|}=\sum_i\sqrt{a_i}|i'\rangle\langle i'|=\sum_i\sqrt{a_i}U|i\rangle\langle i|U^\dagger=U\sqrt{A}U^\dagger.$$

Then we come back to our problem:

$$\begin{aligned}F\left(U\rho U^\dagger,U\sigma U^\dagger\right)&=\mathrm{tr}\sqrt{\left(U\rho U^\dagger\right)^{1/2}U\sigma U^\dagger\left(U\rho U^\dagger\right)^{1/2}}\\&=\mathrm{tr}\sqrt{U\sqrt{\rho}U^\dagger U\sigma U^\dagger U\sqrt{\rho}U^\dagger}=\mathrm{tr}\sqrt{U\sqrt{\rho}\sigma\sqrt{\rho}U^\dagger}\\&=\mathrm{tr}U\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}U^\dagger=\mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}=F\left(\rho,\sigma\right)\end{aligned}$$

Exercise: 9.15

Show that

$$F(\rho,\sigma)=\max_{|\varphi\rangle}|\langle\psi|\varphi\rangle|,$$

where $|\psi\rangle$is any fixed purification of ρ, and the maximization is over all purifications of σ.

Let "duplicate" Q, where ρ and σ are, to obtain R. Let $|m\rangle=\sum_i|i_R\rangle|i_Q\rangle$. $|\psi\rangle$ is given as

$$|\psi\rangle=U_R^0\otimes\sqrt{\rho}U_Q^0|m\rangle,$$

where U_R^0 and U_Q^0 are two constant (and unitary) operators. Let $|\varphi\rangle = V_R \otimes \sqrt{\sigma} V_Q |m\rangle$, where V_R and V_Q are variable operators. Then we have

$$\begin{aligned} |\langle\psi|\varphi\rangle| &= \left|\langle m| U_Q^{0\dagger} \sqrt{\rho} \otimes U_R^{0\dagger} V_R \otimes \sqrt{\sigma} V_Q |m\rangle\right| \\ &= \left|\langle m| \left(U_R^{0\dagger} V_R\right) \left(U_Q^{0\dagger} \sqrt{\rho}\sqrt{\sigma} V_Q\right) |m\rangle\right| \\ &\xrightarrow{\text{Exercise 9.16}} \left|\mathrm{tr}\left(V_R^\dagger U_R^0 U_Q^{0\dagger} \sqrt{\rho}\sqrt{\sigma} V_Q\right)\right|. \end{aligned}$$

In above expression, operators V_R, U_R^0, U_Q^0 and V_Q are all in one space. Set $U \equiv V_Q V_R^\dagger U_R^0 U_Q^{0\dagger}$, we have

$$|\langle\psi|\varphi\rangle| = \left|\mathrm{tr}\left(\sqrt{\rho}\sqrt{\sigma} U\right)\right| \leq \left|\mathrm{tr}\left(\sqrt{\rho}\sqrt{\sigma}\right)\right| = F(\rho, \sigma).$$

To attain the equality, let $\sqrt{\rho}\sqrt{\sigma} = \left|\sqrt{\rho}\sqrt{\sigma}\right| V$, therefore $U = V^\dagger = V_Q V_R^\dagger U_R^0 U_Q^{0\dagger}$. That is $V_Q = V^\dagger$ and $V_R = U_R^0 U_Q^{0\dagger}$.

Exercise: 9.16

(The Hilbert–Schmidt inner product and entanglement) Suppose R and Q are two quantum systems with the same Hilbert space. Let $|i_R\rangle$ and $|i_Q\rangle$ be orthonormal basis sets for R and Q. Let A be an operator on R and B an operator on Q. Define $|m\rangle \equiv \sum_i |i_R\rangle|i_Q\rangle$. Show that

$$\mathrm{tr}(A^\dagger B) = \langle m|(A \otimes B)|m\rangle,$$

where the multiplication on the left hand side is of matrices, and it is understood that the matrix elements of A are taken with respect to the basis $|i_R\rangle$ and those for B with respect to the basis $|i_Q\rangle$.

$$\begin{aligned} \langle m|A \otimes B|m\rangle &= \sum_{ij} \langle i_R|\langle i_Q|A \otimes B|j_R\rangle|j_Q\rangle \\ &= \sum_{ij} \langle i_R|A|j_R\rangle\langle i_Q|B|j_Q\rangle = \sum_{ij} \langle j_R|A^\dagger|i_R\rangle\langle i_Q|B|j_Q\rangle. \end{aligned}$$

To the end, we define a new operator β in R space such that for any i and j we have $\langle i_R|\beta|j_R\rangle = \langle i_Q|B|j_Q\rangle$. Therefore we know that the matrix form of operator B in Q space is the same as the matrix form of β in R. Then we have

$$\langle m|A \otimes B|m\rangle = \sum_{ij} \langle j_R|A^\dagger|i_R\rangle\langle i_R|\beta|j_R\rangle = \sum_j \langle j_R|A^\dagger\beta|j_R\rangle = \mathrm{tr}\left(A^\dagger\beta\right).$$

Exercise: 9.17

Show that $0 \leq A(\rho, \sigma) \leq \pi/2$, with equality in the first inequality if and only if $\rho = \sigma$.

According to Uhlmann's theorem, $F(\rho,\sigma) = \max|\langle\psi|\varphi\rangle| \in [0,1]$, therefore $A(\rho,\sigma) = \arccos F(\rho,\sigma) \in [0, \frac{\pi}{2}]$.

Exercise: 9.18

(Contractivity of the angle) Let $\mathcal{E}$ be a trace-preserving quantum operation. Show that

$$A(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \leq A(\rho,\sigma).$$

Since $F(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \geq F(\rho,\sigma)$, and $\arccos *$ is a monotonically decreasing function, we have $A(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \leq A(\rho,\sigma)$.

Exercise: 9.19

(Joint concavity of fidelity) Prove that the fidelity is jointly concave,

$$F\left(\sum_i p_i\rho_i, \sum_i p_i\sigma_i\right) \geq \sum_i p_i F(\rho_i,\sigma_i).$$

Assume that $|\psi_i\rangle$ and $|\varphi_i\rangle$ be purifications of ρ_i and σ_i such that $F(\rho_i,\sigma_i) = \langle\psi_i|\varphi_i\rangle$. Introduce an ancillary system which has orthonormal basis states $|i\rangle$ corresponding to the index set i for the probability distributions.

$$F\left(\sum_i \sqrt{p_i}\rho_i, \sum_i \sqrt{p_i}\sigma_i\right) \geq \left|\left(\sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle\right)^\dagger \left(\sum_i \sqrt{p_i}|\varphi_i\rangle|i\rangle\right)\right| = \sum_i p_i\langle\psi_i|\varphi_i\rangle = \sum_i p_i F\left(\rho_i,\sigma_i\right).$$

Exercise: 9.20

(Concavity of fidelity) Prove that the fidelity is concave in the first entry,

$$F\left(\sum_i p_i\rho_i, \sigma\right) \geq \sum_i p_i F(\rho_i,\sigma).$$

Let $q_i = p_i$, and $\sigma_i = \sigma$ for all i. According to Theorem 9.7,

$$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq \sum_i \sqrt{p_i q_i} F\left(\rho_i,\sigma_i\right) = \sum_i \sqrt{p_i p_i} F\left(\rho_i,\sigma\right) = \sum_i p_i F\left(\rho_i,\sigma\right).$$

Exercise: 9.21

When comparing pure states and mixed states it is possible to make a stronger statement than

(9.110) about the relationship between trace distance and fidelity. Prove that

$$1 - F(|\psi\rangle, \sigma)^2 \leq D\left(|\psi\rangle, \sigma\right).$$

$F\left(|\psi\rangle, \sigma\right) \xrightarrow{\text{Eq. (9.60)}} \sqrt{\langle\psi|\sigma|\psi\rangle}$

$$D\left(|\psi\rangle, \sigma\right) = \frac{1}{2}\mathrm{tr}\left||\psi\rangle\langle\psi| - \sigma\right| = \mathrm{tr}\left(P\left(|\psi\rangle\langle\psi| - \sigma\right)\right) \geq \mathrm{tr}\left(\left(|\psi\rangle\langle\psi| - \sigma\right)\right) = 1 - \sum_s \langle s|\sigma|s\rangle = 0$$

$$1 - F\left(|\psi\rangle, \sigma\right)^2 = 1 - \langle\psi|\sigma|\psi\rangle$$

$$\sum_{ij} \psi_j^* \psi_i \langle j|\sigma|i\rangle - \sum_s \langle s|\sigma|s\rangle = \sum_{ij} \psi_j^* \psi_i \langle j|\sigma|i\rangle - \sum_i p_i \sum_s \langle s|\phi_i\rangle\langle\phi_i|s\rangle$$

$$= \sum_{ij} \psi_j^* \psi_i \langle j|\sigma|i\rangle - 1$$

$$D\left(|\psi\rangle, \sigma\right) = \frac{1}{2}\mathrm{tr}\left||\psi\rangle\langle\psi| - \sigma\right|$$

Exercise: 9.22

(Chaining property for fidelity measures) Suppose U and V are unitary operators, and $\mathcal{E}$ and $\mathcal{F}$ are trace-preserving quantum operations meant to approximate U and V. Letting $d(\cdot, \cdot)$ be any metric on the space of density matrices satisfying $d(U\rho U^\dagger, U\sigma U^\dagger) = d(\rho, \sigma)$ for all density matrices ρ and σ and unitary U (such as the angle $\arccos(F(\rho, \sigma))$), define the corresponding $E(U, \mathcal{E})$ by

$$E(U, \mathcal{E}) \equiv \max_\rho d(U\rho U^\dagger, \mathcal{E}(\rho)),$$

and shown that $E(VU, \mathcal{F} \circ \mathcal{E}) \leq E(U, \mathcal{E}) + E(V, \mathcal{F})$. Thus, to perform a quantum computation with high fidelity it suffices to complete each step of the computation with high fidelity.

According to the definition, $E\left(VU, \mathcal{F} \circ \mathcal{E}\right) = \max_\rho d\left(VU\rho U^\dagger V^\dagger, \mathcal{F}\left(\mathcal{E}\left(\rho\right)\right)\right)$, we can find a state ρ_0 such that

$$E\left(VU, \mathcal{F} \circ \mathcal{E}\right) = d\left(VU\rho_0 U^\dagger V^\dagger, \mathcal{F}\left(\mathcal{E}(\rho_0)\right)\right) = d\left(U\rho_0 U^\dagger, V^\dagger \mathcal{F}\left(\rho'\right) V\right),$$

where $\rho' \equiv \mathcal{E}(\rho_0)$. Likewise we find σ_0 and τ_0 such that

$$E\left(U, \mathcal{E}\right) = d\left(U\sigma_0 U^\dagger, \mathcal{E}(\sigma_0)\right),$$
$$E\left(V, \mathcal{F}\right) = d\left(U\tau_0 U^\dagger, \mathcal{F}(\tau_0)\right).$$

Since $d(\cdot,\cdot)$ is a metric, we have

$$d(\rho,\sigma) \leq d(\rho,\tau) + d(\tau,\sigma)$$

for any ρ, σ and τ. Therefore we have

$$\begin{aligned} E\left(VU, \mathcal{F}\circ\mathcal{E}\right) &\leq d\left(U\rho_0 U^\dagger, \mathcal{E}(\rho_0)\right) + d\left(\mathcal{E}(\rho_0), V^\dagger \mathcal{F}\left(\rho'\right) V\right) \\ &\leq E\left(U,\mathcal{E}\right) + d\left(V\rho' V^\dagger, \mathcal{F}\left(\rho'\right)\right) \\ &\leq E\left(U,\mathcal{E}\right) + E\left(V,\mathcal{F}\right). \end{aligned}$$

Exercise: 9.23

Show that $\bar{F} = 1$ if and only if $\mathcal{E}(\rho_j) = \rho_j$ for all j such that $p_j > 0$.

We know that $F\left(\rho_j, \mathcal{E}(\rho_j)\right) \leq 1$. The equality attains when $\mathcal{E} = 1$. Therefore we have

$$\bar{F} = \sum_j p_j F\left(\rho_j, \mathcal{E}(\rho_j)\right) \leq \sum_j p_j = 1.$$

Problem: 9.1

(Alternate characterization of the fidelity) Show that

$$F(\rho,\sigma) = \inf_P \mathrm{tr}(\rho P)\mathrm{tr}(\sigma P^{-1}),$$

where the infimum is taken over all invertible positive matrices P.

Use the spectra decomposition to represent P as $P = \sum_i p_i |i\rangle\langle i|$, where $p_i > 0$ for all i. In the basis $\{|i\rangle\}$, we can expand ρ and σ as $\rho = \sum_{ij} \rho_{ij}|i\rangle\langle j|$ and $\sigma = \sum_{ij}\sigma_{ij}|i\rangle\langle j|$. Therefore we have

$$\begin{aligned} \mathrm{tr}(\rho P)\mathrm{tr}(\sigma P^{-1}) &= \mathrm{tr}(\sum_{ij}\rho_{ij}|i\rangle\langle j|\sum_k p_k|k\rangle\langle k|)\mathrm{tr}(\sum_{ij}\sigma_{ij}|i\rangle\langle j|\sum_k p_k^{-1}|k\rangle\langle k|) \\ &= \sum_{ij}\rho_{ii}\sigma_{jj}p_i p_j^{-1} \equiv f(p_1,p_2,...) = f(\boldsymbol{p}). \end{aligned}$$

We then study the minimum of the function $f(\boldsymbol{p})$. The derivative is give by

$$\frac{\partial f}{\partial p_k} = -\sum_i \rho_{ii}\sigma_{kk}p_i p_k^{-2} + \sum_j \rho_{kk}\sigma_{jj}p_j^{-1}.$$

Let $\frac{\partial f}{\partial p_k} = 0$ to obtain the optimized position $p_k^0 = \sqrt{\frac{\sigma_{kk}}{\rho_{kk}}G}$, where $G = \frac{\sum_i \rho_{ii}p_i}{\sum_j \sigma_{jj}/p_j}$. So the minimum is given by

$$f_m = f(\boldsymbol{p} = \boldsymbol{p}^0) = \sum_{ij}\rho_{ii}\sigma_{jj}\sqrt{\frac{\sigma_{ii}}{\rho_{ii}}G}\sqrt{\frac{\rho_{jj}}{\sigma_{jj}}G^{-1}} = \left(\sum_i \sqrt{\rho_{ii}\sigma_{ii}}\right)^2.$$

Then it is not so far to find the infimum of f_m. (How?)

Problem 9.2

Need to read the last section more carefully first.

10 Quantum error-correction

Exercise: 10.1

Verify that the encoding circuit in Figure 10.2 works as claimed.

Let $|\psi\rangle = a|0\rangle + b|1\rangle$,

$$U\left(|\psi\rangle|0\rangle|0\rangle\right) = a|0\rangle|0\rangle|0\rangle + b|1\rangle|1\rangle|1\rangle$$

Exercise: 10.2

The action of the bit flip channel can be described by the quantum operation $\mathcal{E}(\rho) = (1-p)\rho + pX\rho X$. Show that this may be given an alternate operator-sum representation, as $\mathcal{E}(\rho) = (1-2p)\,\rho + 2p\,(P_+\rho P_+ + P_-\rho P_-)$ where P_+ and P_- are projectors onto the $+1$ and -1 eigenstates of X, $(|0\rangle+|1\rangle)/\sqrt{2}$ and $(|0\rangle-|1\rangle)/\sqrt{2}$, respectively. This latter representation can be understood as a model in which the qubit is left alone with probability $1-2p$, and is 'measured' by the environment in the $|+\rangle$, $|-\rangle$ basis with probability $2p$.

According to $1 = P_+ + P_-$, we have

$$\rho = (P_+ + P_-)\,\rho\,(P_+ + P_-) = P_+\rho P_+ + P_+\rho P_- + P_-\rho P_+ + P_-\rho P_-,$$

which gives rise to $P_+\rho P_- + P_-\rho P_+ = \rho - P_+\rho P_+ - P_-\rho P_-$. According to the spectral decomposition $X = |+\rangle\langle+| - |-\rangle\langle-| = P_+ - P_-$, we have

$$\begin{aligned}
\mathcal{E}(\rho) &= (1-p)\rho + pX\rho X \\
&= (1-p)\,\rho + p\,(P_+ - P_-)\,\rho\,(P_+ - P_-) \\
&= (1-p)\,\rho + p\,(P_+\rho P_+ + P_-\rho P_-) - p\,(P_+\rho P_- + P_-\rho P_+) \\
&\xrightarrow{\text{above relation}} (1-p)\,\rho + p\,(P_+\rho P_+ + P_-\rho P_-) - p\,(\rho - P_+\rho P_+ - P_-\rho P_-) \\
&= (1-2p)\,\rho + 2p\,(P_+\rho P_+ + P_-\rho P_-)
\end{aligned}$$

Exercise: 10.3

Show by explicit calculation that measuring Z_1Z_2 followed by Z_2Z_3 is equivalent, up to labeling of the measurement outcomes, to measuring the four projectors defined by (10.5)–(10.8), in the sense that both procedures result in the same measurement statistics and post-measurement states.

Use the spectra decomposition, $Z_1Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I$. The measurement of Z_1Z_2 can be described by measurement operators $\{E_1, E_2\}$ where

$$E_1 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I = |000\rangle\langle 000| + |001\rangle\langle 001| + |110\rangle\langle 110| + |111\rangle\langle 111|$$
$$E_2 = (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I = |010\rangle\langle 010| + |100\rangle\langle 100| + |011\rangle\langle 011| + |101\rangle\langle 101|.$$

E_1 (E_2) represents the measuring Z_1Z_2 and obtain a measuring outcome of $+1$ (-1). Similarly, the measuring of Z_2Z_3 is described by $\{E_3, E_4\}$, where

$$E_3 = (+1\text{of } Z_2Z_3) = I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|) = |000\rangle\langle 000| + |100\rangle\langle 100| + |011\rangle\langle 011| + |111\rangle\langle 111|$$
$$E_4 = (\text{-}1\text{of } Z_2Z_3) = I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|) = |001\rangle\langle 001| + |010\rangle\langle 010| + |101\rangle\langle 101| + |110\rangle\langle 110|.$$

When a measurement E_m is operated on a state $|\psi\rangle$, the output state $\propto E_m|\psi\rangle$. If two measurement E_A and E_B are operated on the state, the output state $\propto E_BE_A|\psi\rangle$. So if $E_m = E_BE_A$, then these two measurements are equivalent. The measurement corresponding to which Z_1Z_2 gives $+1$ and Z_2Z_3 gives $+1$ is

$$M(+1,+1) = E_3E_1 = |000\rangle\langle 000| + |111\rangle\langle 111| = P_0.$$

So this measurement is equivalent to P_0 (Eq. (10.5)). Likewise we have

$$M(+1,-1) = E_4E_1 = |001\rangle\langle 001| - |110\rangle\langle 110| = P_3,$$
$$M(-1,+1) = E_3E_2 = |100\rangle\langle 100| + |011\rangle\langle 011| = P_1,$$
$$M(-1,-1) = E_4E_2 = |010\rangle\langle 010| + |101\rangle\langle 101| = P_2.$$

Therefore these two set of measurements are equivalent.

Exercise 10.4

(1)

$\{P_i = |i\rangle\langle i|\}, i = 0, ..., 7$. For example $P_5 = |5\rangle\langle 5| = |101\rangle\langle 101|$.

For $|\psi\rangle = a|0\rangle + b|1\rangle$, the encoded state is

$$|\Psi\rangle = \frac{1}{\sqrt{8}}((a+b)\,|0\rangle + (a-b)\,|1\rangle + (a-b)\,|2\rangle + (a+b)\,|3\rangle + (a-b)\,|4\rangle + (a+b)\,|5\rangle + (a+b)\,|6\rangle + (a-b)\,|7\rangle).$$

- $\langle P_0\rangle = 1$: no error
- $\langle P_1\rangle = 1$:

Exercise: 10.5

Show that the syndrome measurement for detecting phase flip errors in the Shor code corresponds to measuring the observables $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$.

For each bit flip code, we regard it as a logical qubit. We can prove that the logical X gate (denotes as $\bar{X}$) is implemented by$X^{\otimes 3}$, that is $\bar{X}|0_L\rangle = XXX|000\rangle = |111\rangle = |1_L\rangle$. We can treat the 9-qubit code as a simple phase flip code with each qubit is replaced by a logical qubit. Then we know that the syndrome measurement for the code is $\bar{X}_1\bar{X}_2 = X_1...X_6$ and $\bar{X}_2\bar{X}_3 = X_4...X_9$.

Exercise: 10.6

Show that recovery from a phase flip on any of the first three qubits may be accomplished by applying the operator $Z_1 Z_2 Z_3$.

Equivalently, we need to prove the logical Z operator ($\bar{Z}$) for the bit flip code is $\bar{Z} = Z^{\otimes 3}$. And this is easy to prove.

Exercise: 10.7

Consider the three qubit bit flip code of Section 10.1.1, with corresponding projector $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. The noise process this code protects against has operation elements $\left\{\sqrt{(1-p)^3}, \sqrt{p(1-p)^2}X_1, \sqrt{p(1-p)^2}X_2, \sqrt{p(1-p)^2}X_3\right\}$,where p is the probability that a bit flips. Note that this quantum operation is not trace-preserving, since we have omitted operation elements corresponding to bit flips on two and three qubits. Verify the quantum error-correction conditions for this code and noise process.

Since $E_i = \delta_{i0}\sqrt{(1-p)^3} + (1-\delta_{i0})\sqrt{p(1-p)^2}X_i$, we have

$$\begin{aligned}
E_i^\dagger E_j &= \delta_{i0}\delta_{j0}(1-p)^3 + \delta_{i0}\sqrt{(1-p)^5 p}X_j - \delta_{i0}\delta_{j0}\sqrt{(1-p)^5 p}X_j + \delta_{j0}\sqrt{p(1-p)^5}X_i - \delta_{i0}\delta_{j0}\sqrt{p(1-p)^5}X_i \\
&\quad + \left(p(1-p)^2\right)X_iX_j - \delta_{j0}\left(p(1-p)^2\right)X_iX_j - \delta_{i0}\left(p(1-p)^2\right)X_iX_j + \delta_{i0}\delta_{j0}\left(p(1-p)^2\right)X_iX_j \\
&= \delta_{i0}\delta_{j0}\left((1-p)^3 - 2\sqrt{(1-p)^5 p} + p(1-p)^2\right) + \left(\sqrt{p(1-p)^5} - p(1-p)^2\right)(\delta_{i0}X_j + \delta_{j0}X_i) + \left(p(1-p)^2\right)X_iX_j.
\end{aligned}$$

In principle we can define that X_0 to be anything. Here for simplification, we used $X_0 = 1$. Therefore we have

$$\begin{aligned}
PE_i^\dagger E_j P &= \delta_{i0}\delta_{j0}\left((1-p)^3 - 2\sqrt{(1-p)^5 p} + p(1-p)^2\right)P + \left(\sqrt{p(1-p)^5} - p(1-p)^2\right)P(\delta_{i0}X_j + \delta_{j0}X_i)P + \left(p(1-p)^2\right. \\
&= \delta_{i0}\delta_{j0}(1-2p)(1-p)^2 P + \delta_{ij}\left(p(1-p)^2\right)P \\
&= \alpha_{ij}P,
\end{aligned}$$

where $\alpha_{ij} = \delta_{i0}\delta_{j0}(1-2p)(1-p)^2 + \delta_{ij}\left(p(1-p)^2\right)$.

Exercise: 10.8

Verify that the three qubit phase flip code $|0_L\rangle = |+++\rangle$, $|1_L\rangle = |---\rangle$ satisfies the quantum error-correction conditions for the set of error operators $\{1, Z_1, Z_2, Z_3\}$.

Similarly, we use the formula $E_i = \delta_{i0} + (1-\delta_{i0})Z_i$ (without loss of generality, define $Z_0 = 1$), to derive that

$$E_i^\dagger E_j = \delta_{i0}\delta_{j0} + \delta_{i0}Z_j - \delta_{i0}\delta_{j0}Z_j - \delta_{i0}\delta_{j0}Z_i + Z_i\delta_{j0} + Z_iZ_j - \delta_{j0}Z_iZ_j - \delta_{i0}Z_iZ_j + \delta_{i0}\delta_{j0}Z_iZ_j.$$

Here the projector is $P = |+++\rangle\langle+++| + |---\rangle\langle---|$. We check that $PZ_iP = \delta_{i0}P$. Hence we have

$$PE_i^\dagger E_j P = \delta_{ij}P.$$

Exercise: 10.9

Again, consider the three qubit phase flip code. Let P_i and Q_i be the projectors onto the $|0\rangle$ and $|1\rangle$ states, respectively, of the ith qubit. Prove that the three qubit phase flip code protects against the error set $\{1, P_1, Q_2, P_2, Q_2, P_3, Q_3\}$.

Solution 1 For $\{E_i\} = \{1, P_1, Q_2, P_2, Q_2, P_3, Q_3\}$, calculate each $PE_i^\dagger E_j P$ to confirm that $PE_i^\dagger E_j P = \alpha_{ij} P$.

Solution 2 Rather than check $\{E_i\}$, we check its linear combination $\{F_j = \sum_i m_{ji} E_i\}$. If the error $\{F_j\}$ is protected then $\{E_i\}$ is protected. We replace P_1, Q_2 by $P_1 + Q_1 = 1$ and $P_1 - Q_1 = Z_1$. Therefore $\{F_j\} = \{1, Z_1, Z_2, Z_3\}$. Then it becomes Exercise 10.8.

Exercise 10.10

$$
\begin{aligned}
P &= |+_L +_L +_L\rangle\langle +_L +_L +_L| + |-_L -_L -_L\rangle\langle -_L -_L -_L| \\
&= \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{\langle 000| + \langle 111|}{\sqrt{2}} \frac{\langle 000| + \langle 111|}{\sqrt{2}} \frac{\langle 000| + \langle 111|}{\sqrt{2}} \\
&+ \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{\langle 000| - \langle 111|}{\sqrt{2}} \frac{\langle 000| - \langle 111|}{\sqrt{2}} \frac{\langle 000| - \langle 111|}{\sqrt{2}} \\
&= \sum_{ijk=0}^{1} \sum_{lmn} |7^i \cdot 2^6 + 7^j \cdot 2^3 + 7^k \cdot 2^0\rangle\langle 7^l \cdot 2^6 + 7^m \cdot 2^3 + 7^n \cdot 2^0| \\
&+ \sum_{ijk=0}^{1} \sum_{lmn} (-1)^{l+m+n} |7^i \cdot 2^6 + 7^j \cdot 2^3 + 7^k \cdot 2^0\rangle\langle 7^l \cdot 2^6 + 7^m \cdot 2^3 + 7^n \cdot 2^0| \\
&= \sum_{ijk=0}^{1} \sum_{lmn} \left(1 + (-1)^{l+m+n}\right) |7^i \cdot 2^6 + 7^j \cdot 2^3 + 7^k \cdot 2^0\rangle\langle 7^l \cdot 2^6 + 7^m \cdot 2^3 + 7^n \cdot 2^0|
\end{aligned}
$$

$$
X_1 = \sum_{i=0}^{2^8-1} |2x\rangle\langle 2x + 1| + h.c.
$$

$$
\begin{aligned}
X_i &= \sum_{\alpha=0}^{2^{9-i}-1} \sum_{\beta=0}^{2^{i-1}-1} |2\alpha 2^{i-1} + \beta\rangle\langle (2\alpha+1)\, 2^{i-1} + \beta| + h.c. \\
&= \sum_{\alpha=0}^{2^{9-i}-1} \sum_{\beta=0}^{2^{i-1}-1} |\alpha 2^i + \beta\rangle\langle 2^i\alpha + 2^{i-1} + \beta| + h.c.
\end{aligned}
$$

$$
Y_i = -i \sum_{\alpha=0}^{2^{9-i}-1} \sum_{\beta=0}^{2^{i-1}-1} |\alpha 2^i + \beta\rangle\langle 2^i\alpha + 2^{i-1} + \beta| + h.c.
$$

$$Z_i = \sum_{\alpha=0}^{2^{9-i}-1} \sum_{\beta=0}^{2^{i-1}-1} |2\alpha 2^{i-1}+\beta\rangle\langle 2\alpha 2^{i-1}+\beta| - \sum_{\alpha=0}^{2^{9-i}-1} \sum_{\beta=0}^{2^{i-1}-1} |\alpha 2^i + 2^{i-1}+\beta\rangle\langle \alpha 2^i + 2^{i-1}+\beta|$$

$$X_i X_j = \sum_{\alpha=0}^{2^{9-i}-1} \sum_{\beta=0}^{2^{i-1}-1} |\alpha 2^i+\beta\rangle\langle 2^i\alpha+2^{i-1}+\beta| \left(\sum_{\alpha=0}^{2^{9-j}-1} \sum_{\beta=0}^{2^{j-1}-1} |\alpha 2^j+\beta\rangle\langle 2^j\alpha+2^{j-1}+\beta| + \sum_{\alpha=0}^{2^{9-j}-1} \sum_{\beta=0}^{2^{j-1}-1} |\alpha 2^j+2^{j-1}+\beta\rangle \right.$$
$$+ \sum_{\alpha=0}^{2^{9-i}-1} \sum_{\beta=0}^{2^{i-1}-1} |\alpha 2^i+2^{i-1}+\beta\rangle\langle 2^i\alpha+\beta| \left(\sum_{\alpha=0}^{2^{9-j}-1} \sum_{\beta=0}^{2^{j-1}-1} |\alpha 2^j+\beta\rangle\langle 2^j\alpha+2^{j-1}+\beta| + \sum_{\alpha=0}^{2^{9-j}-1} \sum_{\beta=0}^{2^{j-1}-1} |\alpha 2^j+2^{j-1}+\beta\rangle\langle 2^j\alpha+\beta| \right.$$
$$= \sum_{\alpha=0}^{2^{9-i}-1} \sum_{\beta=0}^{2^{i-1}-1} \sum_{\alpha'=0}^{2^{9-j}-1} \sum_{\beta'=0}^{2^{j-1}-1} |\alpha 2^i+\beta\rangle\delta(2^i\alpha-\alpha' 2^j+2^{i-1}+\beta-\beta'=0)\langle 2^j\alpha'+2^{j-1}+\beta'| + \sum_{\alpha=0}^{2^{9-i}-1} \sum_{\beta=0}^{2^{i-1}-1} |\alpha 2^i+\beta\rangle\langle 2^i\alpha+2^{i-1}+\beta|$$

Exercise: 10.11

Construct operation elements for a single qubit quantum operation $\mathcal{E}$ that upon input of any state ρ replaces it with the completely randomized state $\frac{I}{2}$. It is amazing that even such noise models as this may be corrected by codes such as the Shor code!

Recall Eq. (8.102), we have $\mathcal{E}(\rho) = p\frac{1}{2} + (1-p)\rho = \left(1-\frac{3p}{4}\right)\rho + \frac{p}{4}\left(X\rho X + Y\rho Y + Z\rho Z\right)$. Therefore the operation elements are given by

$$\{E_i\} = \{\sqrt{1-\frac{3p}{4}}, \frac{\sqrt{p}}{2}X, \frac{\sqrt{p}}{2}Y, \frac{\sqrt{p}}{2}Z\}.$$

Exercise: 10.12

Show that the fidelity between the state $|0\rangle$ and $\mathcal{E}(|0\rangle\langle 0|)$ is $\sqrt{1-2p/3}$, and use this to argue that the minimum fidelity for the depolarizing channel is $\sqrt{1-2p/3}$.

For $\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$, $\mathcal{E}(|0\rangle\langle 0|) = (1-\frac{2}{3}p)|0\rangle\langle 0| + \frac{2p}{3}|1\rangle\langle 1|$. The fidelity is given by

$$F(|0\rangle, \mathcal{E}(|0\rangle\langle 0|)) = \sqrt{\langle 0|\mathcal{E}(|0\rangle\langle 0|)|0\rangle} = \sqrt{1-\frac{2}{3}p}.$$

Exercise: 10.13

Show that the minimum fidelity $F\left(|\psi\rangle, \mathcal{E}\left(|\psi\rangle\langle\psi|\right)\right)$ when $\mathcal{E}$ is the amplitude damping channel with parameter γ, is $\sqrt{1-\gamma}$.

Assume that $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, according Exercise 8.22, we have

$$\mathcal{E}\left(|\psi\rangle\langle\psi|\right) = \begin{pmatrix} 1-(1-\gamma)(1-|\alpha|^2) & \alpha\beta^*\sqrt{1-\gamma} \\ \alpha^*\beta\sqrt{1-\gamma} & |\beta|^2(1-\gamma) \end{pmatrix}.$$

Then the fidelity is given by

$$F\left(|\psi\rangle, \mathcal{E}\left(|\psi\rangle\langle\psi|\right)\right) = \sqrt{\langle\psi|\mathcal{E}(|\psi\rangle\langle\psi|)|\psi\rangle} = \sqrt{f(a)},$$

where $a \equiv |\alpha|^2 \in [0,1]$ ($|\beta|^2$ is replaced by $1-a$) , and

$$f(a) = -2\left(\sqrt{1-\gamma} - (1-\gamma)\right)a^2 + \left(2\sqrt{1-\gamma} - 2 + 3\gamma\right)a + (1-\gamma)$$

is a quadratic function. The function reaches its maximum at $a_{max} = \frac{\left(2\sqrt{1-\gamma}-2+3\gamma\right)}{2\left(\sqrt{1-\gamma}-(1-\gamma)\right)} > \frac{\left(2\sqrt{1-\gamma}-2+2\gamma\right)}{2\left(\sqrt{1-\gamma}-(1-\gamma)\right)} = 1$. Since $a_{max} > 1$, the function $f(a)$ is monotonic in $[0,1]$, and the minimum is given at $f(a=0)$. Therefore we have $F_{min} = \sqrt{f(0)} = \sqrt{1-\gamma}$.

Exercise: 10.14

Write an expression for a generator matrix encoding k bits using r repetitions for each bit. This is an $[rk, k]$ linear code, and should have an $rk \times k$ generator matrix.

To the end, we first write down an identity of $k \times k$ shape given by

$$I(1,0) = \begin{pmatrix} 1 & 0 & ... \\ 0 & 1 & 0 \\ ... & 0 & ... \end{pmatrix}.$$

Then we replace each diagonal term with $r \times 1$ block $\mathbf{1} = \begin{pmatrix} 1 \\ ... \\ 1 \end{pmatrix}$ and replace each non-diagonal term with $r \times 1$ block $\mathbf{0} = \begin{pmatrix} 0 \\ ... \\ 0 \end{pmatrix}$. The $rk \times k$ generator matrix is given by

$$G = I(\mathbf{1}, \mathbf{0}) = \begin{pmatrix} \mathbf{1} & \mathbf{0} & ... \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ ... & \mathbf{0} & ... \end{pmatrix}.$$

Exercise: 10.15

Show that adding one column of G to another results in a generator matrix generating the same code.

Similar to Exercise 10.14, we use symbols **0** and **1**. For a bit string $x = (b_0, ..., b_n)$, after the encoding by G, the output string is $y = Gx = (\boldsymbol{b}_0, ..., \boldsymbol{b}_n)^T$, where $\boldsymbol{b}_i$ is a $r \times 1$ matrix $b_i \cdot \mathbf{1}$. We obtain G' by adding the ith column of G to jth column: $G' = G + \Delta^{i\to j}$, where the matrix element of $\Delta^{i\to j}$ is $\Delta^{i\to j}_{\alpha\beta} = \delta_{\alpha i}\delta_{\beta j}\mathbf{1}$. Therefore we see the encoded string by G' is $y' = G'x$. The αth component (block) of y' is

$$y'_\alpha = \boldsymbol{b}_\alpha + \delta_{\alpha i}\boldsymbol{b}_j.$$

That is, y' is obtained by adding jth block of $y = (\boldsymbol{b}_0, ..., \boldsymbol{b}_n)^T$ to its ith block. We can check the difference of the encoded string by G and G':

	y	y'
$(b_i, b_j) = (0, 0)$	$(y_i, y_j) = (\mathbf{0}, \mathbf{0})$	$(y'_i, y'_j) = (\mathbf{0}, \mathbf{0})$
$(b_i, b_j) = (0, 1)$	$(y_i, y_j) = (\mathbf{0}, \mathbf{1})$	$(y'_i, y'_j) = (\mathbf{1}, \mathbf{1})$
$(b_i, b_j) = (1, 0)$	$(y_i, y_j) = (\mathbf{1}, \mathbf{0})$	$(y'_i, y'_j) = (\mathbf{1}, \mathbf{0})$
$(b_i, b_j) = (1, 1)$	$(y_i, y_j) = (\mathbf{1}, \mathbf{1})$	$(y'_i, y'_j) = (\mathbf{0}, \mathbf{1})$

So y and y' belong to the same code.

Exercise: 10.16

Show that adding one row of the parity check matrix to another does not change the code. Using Gaussian elimination and swapping of bits it is therefore possible to assume that the parity check matrix has the standard form $(A|I_{n-k})$, where A is an $(n-k) \times k$ matrix.

Assume that the ith row of H is represented by $\langle h_i| = \begin{pmatrix} H_{i1} & ... & H_{in} \end{pmatrix}$, then H is represented by

$$H = \begin{pmatrix} \langle h_1| \\ ... \\ \langle h_{n-k}| \end{pmatrix}.$$

For any $|x\rangle \in C$, we have $\langle h_i|x\rangle = 0$. If we add the ith row into the jth row to obtain H', we have $H' = H + \Delta H$ where ΔH contains only one non-zero row (with element $\langle h_i|$) at jth row. For any $|x\rangle \in C$, we have

$$H'|x\rangle = H|x\rangle + \begin{pmatrix} 0 \\ ... \\ \langle h_i|x\rangle \leftarrow j\text{th row} \\ ... \\ 0 \end{pmatrix} = 0.$$

Therefore H' also checks the same codewords C. By repeating this (add one row to another), we can diagonalized the right part of H to obtain $H' = (A|I_{n-k})$.

Exercise: 10.17

Find a parity check matrix for the $[6, 2]$ repetition code defined by the generator matrix in

(10.54).

The generator of $[n = 6, k = 2]$ code is given by

$$G = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

We first find $n - k = 4$ independent vectors $y_1$to y_4 which are orthogonal to columns of G.

$$\begin{aligned} y_1 &= \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}^T \\ y_2 &= \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}^T \\ y_3 &= \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}^T \\ y_4 &= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}^T. \end{aligned}$$

Then the parity check matrix is given by

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

The set of codewords C is given by

$$C = \left\{ \begin{array}{l} |00\rangle = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^T \\ |01\rangle = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}^T \\ |10\rangle = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}^T \\ |11\rangle = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}^T \end{array} \right\}.$$

One can check that for any x, if and only $x \in C$, we can have $Hx = 0$.

Exercise: 10.18

Show that the parity check matrix H and generator matrix G for the same linear code satisfy $HG = 0$.

Assume that G is a generator from $K = \{|k\rangle\}$ to $C = \{|n\rangle\}$. For any $|n\rangle \in C$, we have $H|n\rangle = 0$. And we also know that for this $|n\rangle$, there is a $|k\rangle$ in K so that $G|k\rangle = |n\rangle$. Therefore $0 = H|n\rangle = HG|k\rangle$.

Exercise: 10.19

Suppose an $[n, k]$ linear code C has a parity check matrix of the form $H = (A|I_{n-k})$, for some

$(n-k)\times k$ matrix A. Show that the corresponding generator matrix is

$$G = \begin{pmatrix} I_k \\ -A \end{pmatrix}.$$

(Note that $-A = A$ since we are working modulo 2; however, this equation also holds for linear codes over more general fields than Z_2.)

The $(n-k)\times k$ matrix H can be written as $H = \begin{pmatrix} A & 1_{n-k} \end{pmatrix}$,where A is a $(n-k)\times k$ matrix. Then we also write the corresponding generator in a form of

$$G = \begin{pmatrix} M \\ N \end{pmatrix},$$

where M is of the shape $k \times k$ and N is of the shape $(n-k)\times k$. According to Exercise 10.18 we know that

$$HG = AM + 1_{n-k}N = 0,$$

which gives $N = -AM$. We can simply set $M = I_k$, then we have $G = \begin{pmatrix} I_k \\ -A \end{pmatrix}$. Since $\pm 1 \in R_1^2$ (see notations), we have $-A = (-1)\times A \overset{2}{=} 1 \times A = A$.

Exercise 10.20: Let H be a parity check matrix such that any $d-1$ columns are linearly independent, but there exists a set of d linearly dependent columns. Show that the code defined by H has distance d.

Exercise 10.21: Show that an $[n,k,d]$ code must satisfy $n-k \geq d-1$.

Exercise 10.29

For any element $s \in S$, and any two vectors $|v_1\rangle$ and $|v_2\rangle$ in V_S, we have

$$s(a|v_1\rangle + b|v_2\rangle) = (as|v_1\rangle + bs|v_2\rangle) = (a|v_1\rangle + b|v_2\rangle).$$

Therefore we have $a|v_1\rangle + b|v_2\rangle \in V_S$.

$|x\rangle\langle d|$

Appendix 4: Number theory

Exercise A4.1

$$a|b \Rightarrow b = k_a a$$
$$b|c \Rightarrow c = k_b b$$

therefore we have $c = k_b k_a a$, that is $a|c$.

Exercise A4.2

$ax + by = (k_a d)\, x + (k_b d)\, y = (k_a x + k_b y)\, d$, therefore $d|\,(ax + by)$.

Exercise A4.3

For positive integer a and b, if $a|b$, we have $b = k_a a$, where $k_a \in Z$ and $k_a > 0$. Therefore $k_a \geq 1$. And $\frac{b}{a} = k_a \geq 1 \Rightarrow b \geq a$. Based on this we have

$$\begin{cases} a|b \\ b|a \end{cases} \Rightarrow a = b$$

Exercise A4.4

$$697 = 17 \times 41$$
$$36300 = 2^2 \times 3^1 \times 5^2 \times 11^2$$

Exercise A4.5

The element $p^2 - p$ has no multiplicative inverse.

First we prove that $p^2 - p \in [1, p^2 - 1]$. Since $p \geq 2$, we have $p^2 - p \leq p^2 - 2 < p^2 - 1$. Also $p^2 - p = p(p-1) \geq p(2-1)$. According to these, we know that $p^2 - p \in [1, p^2 - 1]$.

If $p^2 - p$ has a multiplicative inverse x, we have $x(p^2 - p) \overset{p}{=} 1$. However we know that $x(p^2 - p) \overset{p}{=} xp^2 - xp \overset{p}{=} 0$. Therefore $1 \overset{p}{=} 0$, wrong!

Exercise A4.6

It is itself, since $17 \times 17 \overset{24}{=} 1$.

Exercise A4.7

The solution is $x = 1 - n$, since $x(n+1) = 1 - n^2 \overset{n^2}{=} 1$

Exercise A4.8

if $b \overset{n^2}{\neq} b'$, we multiply a at both side to get $1 \overset{n^2}{=} ab \overset{n^2}{\neq} ab' \overset{n^2}{=} 1$. That is impossible.

Exercise A4.9

$\gcd(p_1^{\alpha_1} p_2^{\alpha_2} ..., p_1^{\beta_1} p_2^{\beta_2} ...) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} ...$

$$6825 = 2^0 \times 3 \times 5^2 \times 7 \times 11^0 \times 13$$
$$1430 = 2 \times 3^0 \times 5 \times 7^0 \times 11 \times 13$$

Therefore $\gcd(6825, 1430) = 5 \times 13 = 65$.

Exercise A4.10

$\varphi(187) = \varphi(7)\varphi(11) = (7-1)(11-1) = 60.$

Exercise A4.11

We first study the case of $n = p^\alpha$,where p is a prime number. Based on the relation $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, we write down the following set of equations:

$$\begin{cases} \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} \\ \varphi(p^{\alpha-1}) = p^{\alpha-1} - p^{\alpha-2} \\ \cdots \\ \varphi(p^1) = p^1 - p^0 \end{cases}.$$

When we plus all these, we obtain $\sum_{i=1}^{\alpha} \varphi(p^i) = p^\alpha - 1 = n - 1$. Since $\{d|n\} = \{1, p, ..., p^{\alpha-1}\}$, we obtain $n = \sum_{d|n} \varphi(d)$ (notice that $\varphi(1) \equiv 1$).

For the general case when $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_N^{\alpha_N}$, we have $\{d|n\} = \{p_1^{x_1} p_2^{x_2} ... p_N^{x_N} | \text{for all } x_i | p_i^{\alpha_i}\}$. We can write down the set of equations as follows:

$$\begin{cases} p_1^{\alpha_1} = \sum_{d|p_1^{\alpha_1}} \varphi(d) \\ p_2^{\alpha_2} = \sum_{d|p_2^{\alpha_2}} \varphi(d) \\ \cdots \\ p_1^{\alpha_1} = \sum_{d|p_N^{\alpha_N}} \varphi(d) \end{cases}.$$

Then we multiply all these to obtain

$$\begin{aligned} n &= \sum_{d_1|p_1^{\alpha_1}} \sum_{d_N|p_N^{\alpha_N}} \varphi(d_1)...\varphi(d_N) \\ &= \sum_{d_1|p_1^{\alpha_1}} \sum_{d_N|p_N^{\alpha_N}} \varphi(d_1...d_N) = \sum_{d|n} \varphi(d). \end{aligned}$$

Exercise A4.12

Exercise A4.13

$S = \{a^0, a^1, a^2, ...\} = \{a^i\}$. We first prove that for any i, a^i is in Z_n^*. For $i = 0$ and 1, it is apparent. Therefore we can define the inverse of a as a^{-1}. Assume that $a^k \in Z_n^*$. Then we know there is an element, denoted as a^{-k}, to be the inverse of a^k. Therefore we have $1 \overset{n}{=} \left(a^k a^{-k}\right)\left(aa^{-1}\right) \overset{n}{=} \left(a^k a\right)\left(a^{-k}a^{-1}\right) \overset{n}{=} a^{k+1}\left(a^{-k}a^{-1}\right)$. That is to say that we have found the inverse of a^{k+1} to be $a^{-k}a^{-1}$. Therefore a^{k+1} is also in Z_n^*.

Since each element in S is also in Z_n^*, then S must be a finite group. We can represent it as $\{1, a^1, ..., a^{r-1}\}$. Since S is a group, $aS = \{a^1, a^2, ..., a^r\} = S$. Then we assume all elements in both representation to obtain

$$a^1 a^2 ... a^r \overset{n}{=} a^0 a^1 ... a^{r-1},$$

which gives $a^r \overset{n}{=} 1$.

Exercise A4.14

The major spirit to prove this is similar to Exercise A4.13. Assume that $Z_n^* = \{z_1, z_2, ..., z_m\}$, where $m = \varphi(n)$. According to $gZ_n^* = Z_n^*$ we have

$$\{gz_1, gz_2, ..., gz_m\} \overset{n}{=} \{z_1, z_2, ..., z_m\},$$

therefore we multiply all elements in the group to obtain

$$g^m z_1 ... z_m \overset{n}{=} z_1 ... z_m.$$

Therefore we have $g^m = g^{\varphi(n)} \overset{n}{=} 1$.

Exercise A4.15

As we discussed in Exercise A4.13, S (with order r) is a subgroup of Z_n^* (with order $\varphi(n)$). Therefore, according to Langrange's theorem, we have $r|\varphi(n)$ or equivalently $\varphi(n) = kr$. Therefore $a^{\varphi(n)} = (a^r)^k \overset{n}{=} (1)^k \overset{n}{=} 1$.

Exercise A4.16

According to the definition,$x^r \overset{N}{=} 1$. Theorem A 4.9 tell us that $x^{\varphi(N)} = 1$. Since r is the smallest integer to satisfy this equation, then $r|\varphi(N)$.

The order of x modulo N is, according to $a^{\varphi(N)} \overset{N}{=} 1$, is $r = \varphi(N)$.

Exercise A4.17

If we have an efficient algorithm to decompose N, with obtaining a factor $x|N$. Then $x = nN$

$x^r = 1$

Exercise A4.18

$$\frac{19}{17} = 1 + \frac{2}{17} = 1 + \frac{1}{8 + \frac{1}{2}} = [1, 8, 2]$$

$$\begin{aligned}\frac{77}{65} &= 1 + \frac{12}{65} = 1 + \frac{1}{5 + \frac{5}{12}} = 1 + \frac{1}{5 + \frac{1}{\frac{12}{5}}} \\ &= 1 + \frac{1}{5 + \frac{1}{2 + \frac{2}{5}}} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = [1, 5, 2, 2, 2]\end{aligned}$$

NOTE

P442, for

$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} = \sum_i tr(\sigma_i^\dagger E_0)\sigma_i = \frac{1+\sqrt{1-\gamma}}{2} + \frac{1-\sqrt{1-\gamma}}{2} Z.$

$$E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix} = \frac{\sqrt{\gamma}}{2} X + \frac{i\sqrt{\gamma}}{2} Y$$

For any single-qubit error $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$, if we use $E_i = \sum_k c_{ik}\sigma_k^i$,

$$\mathcal{E}(\rho) = \sum_i \sum_{kl} c_{ik} c_{il}^* \sigma_k^i \rho \sigma_l^i$$

Prob. $\sqrt{AB} =? \sqrt{A}\sqrt{B}$

$$X = \sqrt{A}\sqrt{B} = \sum_{ij} \sqrt{a_i b_j} \langle a_i | b_j \rangle |a_i\rangle\langle b_j|$$

$$X^\dagger = \sum_{ij} \sqrt{a_i b_j} \langle a_i | b_j \rangle^* \left(|a_i\rangle\langle b_j|\right)^\dagger = \sum_{ij} \sqrt{a_i b_j} \langle b_j | a_i \rangle |b_j\rangle\langle a_i|$$

$$Y = AB = \sum_{ij} a_i b_j \langle a_i | b_j \rangle |a_i\rangle\langle b_j|$$

$$\sqrt{AB} = \sum_i \sqrt{a_i} |a_i\rangle\langle a_i|$$