Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: **2** November 2021, 08:00 on Moodle

Tutorial 1 (Double-slit experiment)

With this tutorial we want to illustrate the counter-intuitiveness and strangeness of quantum mechanics. The content is not relevant for the final exam.

One of the most famous experiments that demonstrates the simultaneous particle-wave duality in quantum mechanics is Young's double-slit experiment. In the original experiment, the beam from a coherent light source (laser) illuminates a sheet with two thin parallel slits (Fig. 1).

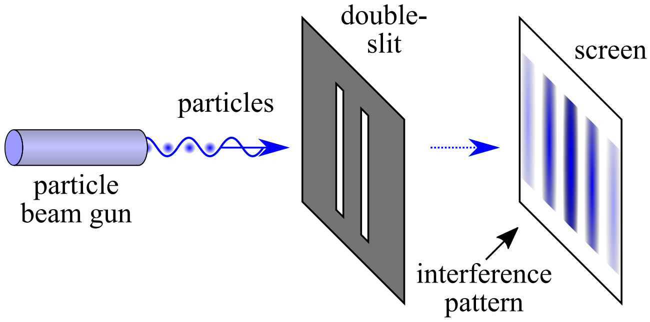


Figure 1: Double-slit experiment [1]

A screen is placed a distance away from the sheet and an interference pattern is observed on the screen. The pattern is attributed to the interference of the lightwave emitted from each slit, in which destructive and constructive interference result in a striped pattern. Surprisingly, interference is observed even when only a single particle (like a photon or electron) at a time is sent through.[2]

On the other hand, the interference pattern is destroyed when we determine which slit a particle traveled through.[3] This can be explained by the "wavefunction collapse" at the slit due to measurement.

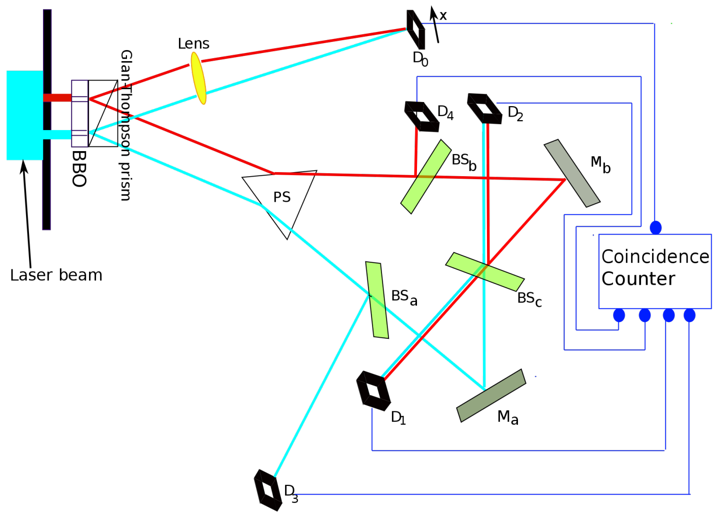


Figure 2: Experimental setup for the "delayed-choice quantum eraser" [4]

An even more counter-intuitive variant of the experiment is the "delayed-choice quantum eraser"[5], where the "which slit" information is obtained *after* the particle has already been detected on the screen (D_0 in Fig. 2).

[1]Image source: `https://en.wikipedia.org/wiki/Double-slit_experiment`

[2]R. Bach, D. Pope, S.-H. Liou, H. Batelaan: *Controlled double-slit electron diffraction*. New J. Phys. 15, 033018 (2013)

[3]S. Frabboni, G. C. Gazzadi, G. Pozzi: *Ion and electron beam nanofabrication of the which-way double-slit experiment in a transmission electron microscope*. Appl. Phys. Lett. 97, 263101 (2010)

[4]Image source: `https://en.wikipedia.org/wiki/Delayed-choice_quantum_eraser`

[5]Y.-H. Kim, R. Yu, S. P. Kulik, Y. Shih, M. O. Scully: *Delayed "Choice" Quantum Eraser*. Phys. Rev. Lett. 84, 1 (2000); see also `https://en.wikipedia.org/wiki/Delayed-choice_quantum_eraser`

Exercise 1.1 (Complex number arithmetic)
This exercise should refresh your knowledge and proficiency with complex numbers. Given $a = 3 + 4i$ and $b = 2 - i$:

(a) Compute

- $a + b$
- ab (product of a and b)
- $1/a$
- a^* (complex conjugate of a)
- $|a|$ and $\arg(a)$ (argument), such that $a = |a|\,\mathrm{e}^{i\arg(a)}$
- the Euclidean length of the vector $\psi = \begin{pmatrix} a \\ b \end{pmatrix}$, denoted $\|\psi\|$

(b) Draw a in the complex plane, and interpret a^*, $|a|$ and $\arg(a)$ geometrically.

(c) How can one construct $a + b$ and ab geometrically in the complex plane?

Exercise 1.2 (Linear algebra basics)

(a) Compute (with "pen and paper") the matrix-vector product

$$\begin{pmatrix} 2 & -i & 5 \\ 3 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ i \\ -3 \end{pmatrix},$$

and the matrix-matrix product

$$\begin{pmatrix} -2 & 7 \\ 3 & 1+2i \end{pmatrix} \cdot \begin{pmatrix} 5 & -4 \\ 6i & 0 \end{pmatrix}.$$

(b) Find a 2×2 matrix which is not normal.
Hint: you can restrict your search to real-valued matrices.

(c) Show that the following matrix is normal, and compute its characteristic polynomial, eigenvalues and an eigenvector corresponding to one of the eigenvalues:

$$A = \begin{pmatrix} 0 & \frac{3}{5} & \frac{4}{5} \\ -\frac{3}{5} & 0 & 0 \\ -\frac{4}{5} & 0 & 0 \end{pmatrix}.$$

(d) Show that the following matrix is unitary (with $\theta \in \mathbb{R}$ a real parameter):

$$\begin{pmatrix} \cos(\theta) & i\sin(\theta) \\ i\sin(\theta) & \cos(\theta) \end{pmatrix}.$$

(e) Let $U \in \mathbb{C}^{n \times n}$ be a unitary matrix. Show that

$$|\det(U)| = 1,$$

where $|\cdot|$ denotes the absolute value.
Hint: consider $\det(U^\dagger U)$.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 1.1 (Complex number arithmetic)
This exercise should refresh your knowledge and proficiency with complex numbers. Given $a = 3 + 4i$ and $b = 2 - i$:

(a) Compute

- $a + b$
- ab (product of a and b)
- $1/a$
- a^* (complex conjugate of a)
- $|a|$ and $\arg(a)$ (argument), such that $a = |a|\, \mathrm{e}^{i \arg(a)}$
- the Euclidean length of the vector $\psi = \begin{pmatrix} a \\ b \end{pmatrix}$, denoted $\|\psi\|$

(b) Draw a in the complex plane, and interpret a^*, $|a|$ and $\arg(a)$ geometrically.

(c) How can one construct $a + b$ and ab geometrically in the complex plane?

Solution

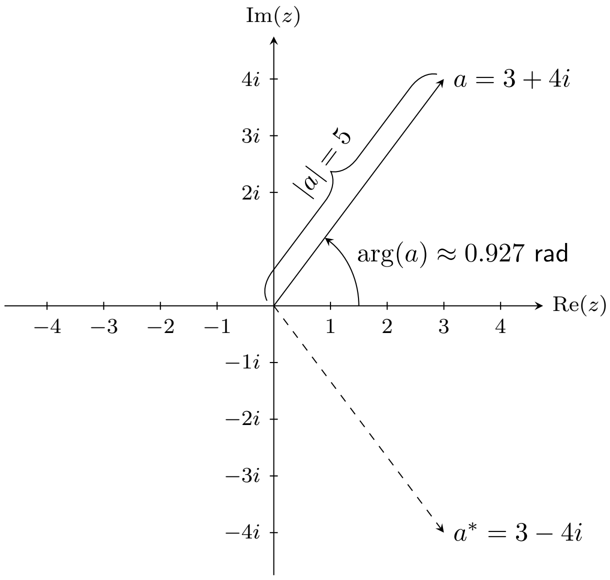
(a) Given $a = 3 + 4i$ and $b = 2 - i$, the following expressions are equal to

- $a + b = 5 + 3i$
- $ab = 10 + 5i$ $\quad 6 - 3i + 8i + 4$
- $1/a = \frac{a^*}{|a|^2} = \frac{3}{25} - \frac{4}{25} i$
- $a^* = 3 - 4i$
- $|a| = \sqrt{aa^*} = \sqrt{\mathrm{Re}(a)^2 + \mathrm{Im}(a)^2} = 5$, $\arg(a) = \arctan(4/3) \approx 0.927$ rad
- In general, the norm of a complex vector $\psi = (\psi_1, \psi_2, \ldots, \psi_n)$ is defined as

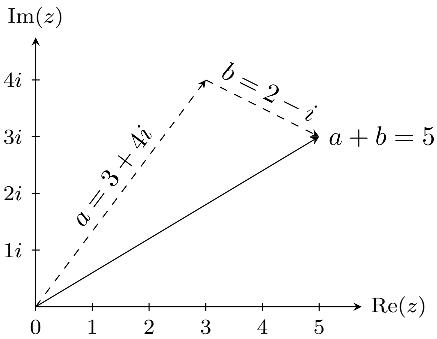
$$\|\psi\| = \sqrt{\sum_{i=1}^{n} |\psi_i|^2}.$$

Here $\|\psi\| = \sqrt{|a|^2 + |b|^2} = \sqrt{25 + 5} = \sqrt{30}$.

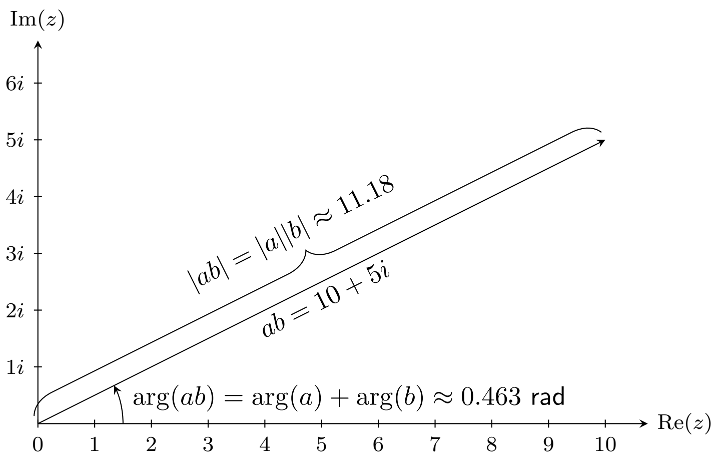
(b) Drawing a in the complex plane:



(c) Drawing $a + b$ in the complex plane:



Drawing ab in the complex plane:



Exercise 1.2

(a)

```
{{2, -i, 5}, {3, 0, 1}}.{4, i, -3} // MatrixForm
```

$$\begin{pmatrix} -6 \\ 9 \end{pmatrix}$$

```
{{-2, 7}, {3, 1 + 2 i}}.{{5, -4}, {6 i, 0}} // MatrixForm
```

$$\begin{pmatrix} -10+42\,i & 8 \\ 3+6\,i & -12 \end{pmatrix}$$

(b)

```
(* this matrix is not normal *)
Amat = {{0, 0}, {1, 0}};
% // MatrixForm
```

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

```
(* not the same *)
Amat.Transpose[Amat] // MatrixForm
Transpose[Amat].Amat // MatrixForm
```

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

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

(c)

$$A_{mat} = \left\{\left\{0, \frac{3}{5}, \frac{4}{5}\right\}, \left\{-\frac{3}{5}, 0, 0\right\}, \left\{-\frac{4}{5}, 0, 0\right\}\right\};$$

```
% // MatrixForm
```

$$\begin{pmatrix} 0 & \frac{3}{5} & \frac{4}{5} \\ -\frac{3}{5} & 0 & 0 \\ -\frac{4}{5} & 0 & 0 \end{pmatrix}$$

The matrix is normal since it is anti-symmetric, i.e., its adjoint is the same as -A, and A commutes with -A.

```
(* for the homework submission, you should compute this with "pen and paper" *)
(* minus sign to adhere to convention from the lecture *)
-CharacteristicPolynomial[Amat, λ]
Solve[% == 0, λ]
```

$\lambda + \lambda^3$

$\{\{\lambda \to 0\}, \{\lambda \to -i\}, \{\lambda \to i\}\}$

Thus the eigenvalues are 0 and $\pm i$.

```
(* eigenspace corresponding to eigenvalue 0 *)
NullSpace[A_mat]
(* normalized eigenvector *)
v_0 = FullSimplify[%[[1]] / Norm[%[[1]]]]
```

$$\left\{\left\{0, -\frac{4}{3}, 1\right\}\right\}$$

$$\left\{0, -\frac{4}{5}, \frac{3}{5}\right\}$$

```
(* eigenspace corresponding to eigenvalue i *)
NullSpace[i IdentityMatrix[3] - A_mat]
(* normalized eigenvector *)
v_i = FullSimplify[%[[1]] / Norm[%[[1]]]]
```

$$\left\{\left\{-\frac{5\,i}{4}, \frac{3}{4}, 1\right\}\right\}$$

$$\left\{-\frac{i}{\sqrt{2}}, \frac{3}{5\sqrt{2}}, \frac{2\sqrt{2}}{5}\right\}$$

```
(* eigenspace corresponding to eigenvalue -i *)
NullSpace[(-i) IdentityMatrix[3] - A_mat]
(* normalized eigenvector *)
v_-i = FullSimplify[%[[1]] / Norm[%[[1]]]]
```

$$\left\{\left\{\frac{5\,i}{4}, \frac{3}{4}, 1\right\}\right\}$$

$$\left\{\frac{i}{\sqrt{2}}, \frac{3}{5\sqrt{2}}, \frac{2\sqrt{2}}{5}\right\}$$

(d)

```
U[θ_] := {{Cos[θ], i Sin[θ]}, {i Sin[θ], Cos[θ]}}
```

```
FullSimplify[U[θ].ConjugateTranspose[U[θ]], Assumptions → {θ ∈ Reals}] // MatrixForm
```

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

(e)

$$1 = \mathrm{Det}[\mathrm{id}] = \mathrm{Det}[U^\dagger.U] = \mathrm{Det}[U^\dagger]\,\mathrm{Det}[U] = \mathrm{Det}[U]^*\,\mathrm{Det}[U] = |\mathrm{Det}[U]|^2$$

Introduction to Quantum Computing (IN2381) – WS021/2022 **Sheet 2**

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: 8 November 2021, 08:00 on Moodle

Tutorial 2 (Dirac notation and inner products)
The Dirac notation (also called bra-ket notation), which you have seen being used in the lecture, uses "kets", such as $|\psi\rangle$, to represent a quantum state. For our purposes, a ket is always a complex (column) vector.[1] ψ is usually the actual vector itself, or can be an identifier or index for the quantum state, as for $|0\rangle$ and $|1\rangle$.

The corresponding "bra" $\langle\psi|$ is then the conjugate-transposed $|\psi\rangle$, i.e., a row vector with complex-conjugated entries of $|\psi\rangle$. A motivation for this notation is that "bras" are linear maps from quantum states to complex numbers via the inner product. Namely, given $\phi \in \mathbb{C}^n$:

$$\langle\phi| : \mathbb{C}^n \to \mathbb{C}, \quad |\psi\rangle \mapsto \langle\phi|\psi\rangle = \sum_{j=1}^{n} \phi_j^* \, \psi_j .$$

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

(a) Write down the matrix representation of the following expressions:

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

(b) Express the Hadamard gate H using Dirac notation in the computational basis (i.e. $\{|0\rangle, |1\rangle\}$).

(c) Given the qubit state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, compute $H|\psi\rangle$ using only the bra-ket notation.

(d) For any $\psi, \phi \in \mathbb{C}^n$ and $A \in \mathbb{C}^{n\times n}$, verify that

$$\langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle,$$

with $A^\dagger = (A^*)^T$ denoting the conjugate transpose (adjoint) of A.

(e) Prove that unitary matrices are norm-preserving, i.e., $\|U\psi\| = \|\psi\|$ for all unitary $U \in \mathbb{C}^{n\times n}$ and $\psi \in \mathbb{C}^n$.
Hint: Use that $\|\psi\|^2 = \langle\psi|\psi\rangle$ and part (d).

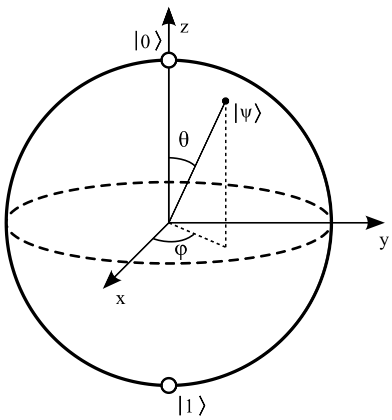
$\varphi = i$

Exercise 2.1 (Bloch sphere and single qubit rotation gates)
Recall from the lecture that an arbitrary single qubit quantum state can be parametrized as

$\theta = \frac{2\pi}{3}$

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$

where θ, φ and γ are real numbers, which can be chosen such that $0 \le \theta \le \pi$ and $0 \le \varphi \le 2\pi$. The angles θ and φ define the Bloch sphere representation of $|\psi\rangle$, as shown on the right.



https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg

(a) Find the Bloch angles θ and φ of $|\psi\rangle = \frac{i}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$, and the corresponding Bloch vector

$$\vec{r} = (\cos(\varphi)\sin(\theta), \sin(\varphi)\sin(\theta), \cos(\theta)).$$

For a real unit vector $\vec{v} \in \mathbb{R}^3$, the rotation by an angle ω about the $\vec{v}$ axis is defined as

$$R_{\vec{v}}(\omega) = \exp(-i\omega\,\vec{v}\cdot\vec{\sigma}/2) = \cos(\omega/2)I - i\sin(\omega/2)(\vec{v}\cdot\vec{\sigma}),$$

where $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ is the Pauli vector. The rotations R_x, R_y, R_z about the standard axes correspond to the special cases $\vec{v} = (1,0,0)$, $\vec{v} = (0,1,0)$ and $\vec{v} = (0,0,1)$, respectively.

(b) Compute $R_x(\frac{2\pi}{3})|\psi\rangle$ for the state $|\psi\rangle$ defined in (a), and visualize this operation on the Bloch sphere.
Hint: $\cos(\frac{\pi}{3}) = \frac{1}{2}$ and $\sin(\frac{\pi}{3}) = \frac{\sqrt{3}}{2}$.

[1] In general, quantum states can also be complex-valued functions (e.g., electronic orbitals of atoms), but these will not play a role in this course.

(c) The *Z-Y decomposition* theorem states the following: given any unitary 2×2 matrix U, there exist real numbers $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$U = \mathrm{e}^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Find the Z-Y decomposition of the Hadamard gate $H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$.

Hint: There exists a solution with $\beta = 0$.

Exercise 2.2 (Basic single qubit gates)
Imagine you are playing a game against an adversary. The game consists of multiple trials through which the adversary performs one of the following with equal probability:

1. They flip a coin and send you $|0\rangle$ or $|1\rangle$ depending on the outcome.

OR

2. They send you the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Your goal is to decide which of the two they performed, and you win if you can decide correctly for $\frac{3}{4}$ of the trials on average.

(a) Before you make your guess (based on a quantum measurement on the qubit), you are allowed to perform **one** of the gates X, Y, Z or H. Compute the outputs you would obtain in each situation with each of these gates.

(b) Which of the gates would allow you to win the game? Explain your strategy.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 2 (Dirac notation and inner products)
The Dirac notation (also called bra-ket notation), which you have seen being used in the lecture, uses "kets", such as $|\psi\rangle$, to represent a quantum state. For our purposes, a ket is always a complex (column) vector.[1] ψ is usually the actual vector itself, or can be an identifier or index for the quantum state, as for $|0\rangle$ and $|1\rangle$.

The corresponding "bra" $\langle\psi|$ is then the conjugate-transposed $|\psi\rangle$, i.e., a row vector with complex-conjugated entries of $|\psi\rangle$. A motivation for this notation is that "bras" are linear maps from quantum states to complex numbers via the inner product. Namely, given $\phi \in \mathbb{C}^n$:

$$\langle\phi| : \mathbb{C}^n \to \mathbb{C}, \quad |\psi\rangle \mapsto \langle\phi|\psi\rangle = \sum_{j=1}^{n} \phi_j^* \, \psi_j.$$

(a) Write down the matrix representation of the following expressions:

- $|0\rangle\langle 1|$
- $|0\rangle\langle 0| + |1\rangle\langle 1|$
- $|+\rangle\langle 0|$, with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

(b) Express the Hadamard gate H using Dirac notation in the computational basis (i.e. $\{|0\rangle, |1\rangle\}$).

(c) Given the qubit state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, compute $H|\psi\rangle$ using only the bra-ket notation.

(d) For any $\psi, \phi \in \mathbb{C}^n$ and $A \in \mathbb{C}^{n\times n}$, verify that

$$\langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle,$$

with $A^\dagger = (A^*)^T$ denoting the conjugate transpose (adjoint) of A.

(e) Prove that unitary matrices are norm-preserving, i.e., $\|U\psi\| = \|\psi\|$ for all unitary $U \in \mathbb{C}^{n\times n}$ and $\psi \in \mathbb{C}^n$.
Hint: Use that $\|\psi\|^2 = \langle\psi|\psi\rangle$ and part (d).

Solution

(a) Using the column and row vector forms leads to

$$\begin{aligned}
|0\rangle\langle 1| &= \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix},\\
|0\rangle\langle 0| + |1\rangle\langle 1| &= \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = I_2 \quad \text{(identity matrix)},\\
|+\rangle\langle 0| &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\1 & 0\end{pmatrix}.
\end{aligned}$$

(b) Recall that the Hadamard gate is defined as

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}.$$

We can re-write this in bra-ket notation as

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

(c) Here we can use the fact that $|0\rangle$ and $|1\rangle$ form an orthonormal basis, and therefore: $\langle a|b\rangle = \delta_{ab}$ for $a, b \in \{0, 1\}$. Thus

$$\begin{aligned}
H|\psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \cdot \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\\
&= \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle.
\end{aligned}$$

[1] In general, quantum states can also be complex-valued functions (e.g., electronic orbitals of atoms), but these will not play a role in this course.

For comparison, the equivalent vector notation for the same operation reads

$$H|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \cdot \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \begin{pmatrix}1\\ 0\end{pmatrix}.$$

(d) Using the definition of the inner product and the index notation for a matrix-vector product, we can write

$$\langle\phi|A\psi\rangle = \sum_{j=1}^{n}\phi_j^*\sum_{k=1}^{n}A_{jk}\psi_k = \sum_{j,k=1}^{n}\phi_j^*A_{jk}\psi_k.$$

Now, note that $A_{jk} = (A^\dagger)_{kj}^*$ which we can use to rewrite the above expression as

$$\langle\phi|A\psi\rangle = \sum_{j,k=1}^{n}(A^\dagger)_{kj}^*\phi_j^*\psi_k = \langle A^\dagger\phi|\psi\rangle.$$

(e) Using our result from part (d) and that $U^\dagger U = I$ by definition of a unitary matrix,

$$\|U\psi\|^2 = \langle U\psi|U\psi\rangle = \langle U^\dagger U\psi|\psi\rangle = \langle\psi|\psi\rangle = \|\psi\|^2.$$

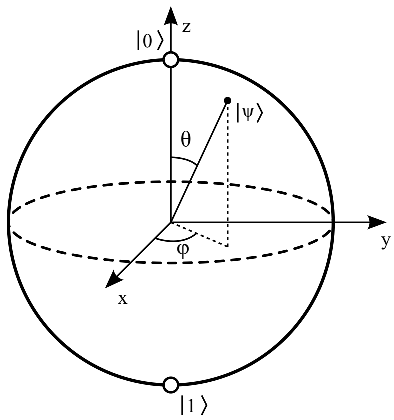
This means that $\|U\psi\| = \|\psi\|$.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 2.1 (Bloch sphere and single qubit rotation gates)
Recall from the lecture that an arbitrary single qubit quantum state can be parametrized as

$$|\psi\rangle = \mathrm{e}^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$

where θ, φ and γ are real numbers, which can be chosen such that $0 \leq \theta \leq \pi$ and $0 \leq \varphi \leq 2\pi$. The angles θ and φ define the Bloch sphere representation of $|\psi\rangle$, as shown on the right.



https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg

(a) Find the Bloch angles θ and φ of $|\psi\rangle = \frac{i}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$, and the corresponding Bloch vector

$$\vec{r} = (\cos(\varphi)\sin(\theta), \sin(\varphi)\sin(\theta), \cos(\theta)).$$

For a real unit vector $\vec{v} \in \mathbb{R}^3$, the rotation by an angle ω about the $\vec{v}$ axis is defined as

$$R_{\vec{v}}(\omega) = \exp(-i\omega\,\vec{v}\cdot\vec{\sigma}/2) = \cos(\omega/2)I - i\sin(\omega/2)(\vec{v}\cdot\vec{\sigma}),$$

where $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ is the Pauli vector. The rotations R_x, R_y, R_z about the standard axes correspond to the special cases $\vec{v} = (1,0,0)$, $\vec{v} = (0,1,0)$ and $\vec{v} = (0,0,1)$, respectively.

(b) Compute $R_x(\frac{2\pi}{3})|\psi\rangle$ for the state $|\psi\rangle$ defined in (a), and visualize this operation on the Bloch sphere.

Hint: $\cos(\frac{\pi}{3}) = \frac{1}{2}$ and $\sin(\frac{\pi}{3}) = \frac{\sqrt{3}}{2}$.

(c) The *Z-Y decomposition* theorem states the following: given any unitary 2×2 matrix U, there exist real numbers $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$U = \mathrm{e}^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta).$$

Find the Z-Y decomposition of the Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Hint: There exists a solution with $\beta = 0$.

Solution hints

(a) Absorb the prefactor i of $|\psi\rangle$ into $\mathrm{e}^{i\gamma}$ by setting $\gamma = \frac{\pi}{2}$. The last entry of the Bloch vector $\vec{r}$ is $-\frac{1}{2}$.

(b) You should obtain $R_x(\frac{2\pi}{3})|\psi\rangle = i|0\rangle$. R_x rotates $|\psi\rangle$ within the y-z-plane to the north pole. (The prefactor i in $i|0\rangle$ does not affect the Bloch vector representation.)

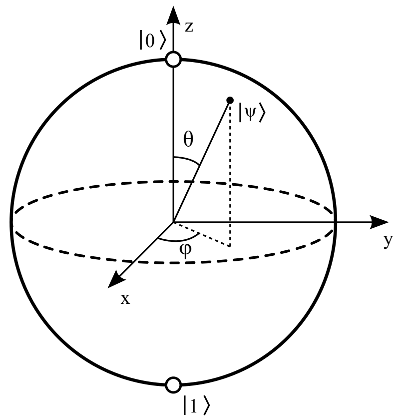
(c) Set $\gamma = \frac{\pi}{2}$ and $\delta = \pi$, and absorb an overall prefactor in $\mathrm{e}^{i\alpha}$.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 2.1 (Bloch sphere and single qubit rotation gates)
Recall from the lecture that an arbitrary single qubit quantum state can be parametrized as

$$|\psi\rangle = \mathrm{e}^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\right)$$

where θ, φ and γ are real numbers, which can be chosen such that $0 \le \theta \le \pi$ and $0 \le \varphi \le 2\pi$. The angles θ and φ define the Bloch sphere representation of $|\psi\rangle$, as shown on the right.



https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg

(a) Find the Bloch angles θ and φ of $|\psi\rangle = \frac{i}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$, and the corresponding Bloch vector

$$\vec{r} = (\cos(\varphi)\sin(\theta), \sin(\varphi)\sin(\theta), \cos(\theta)).$$

For a real unit vector $\vec{v} \in \mathbb{R}^3$, the rotation by an angle ω about the $\vec{v}$ axis is defined as

$$R_{\vec{v}}(\omega) = \exp(-i\omega\,\vec{v}\cdot\vec{\sigma}/2) = \cos(\omega/2)I - i\sin(\omega/2)(\vec{v}\cdot\vec{\sigma}),$$

where $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ is the Pauli vector. The rotations R_x, R_y, R_z about the standard axes correspond to the special cases $\vec{v} = (1,0,0)$, $\vec{v} = (0,1,0)$ and $\vec{v} = (0,0,1)$, respectively.

(b) Compute $R_x(\frac{2\pi}{3})\,|\psi\rangle$ for the state $|\psi\rangle$ defined in (a), and visualize this operation on the Bloch sphere.

Hint: $\cos(\frac{\pi}{3}) = \frac{1}{2}$ and $\sin(\frac{\pi}{3}) = \frac{\sqrt{3}}{2}$.

(c) The *Z-Y decomposition* theorem states the following: given any unitary 2×2 matrix U, there exist real numbers $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$U = \mathrm{e}^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta).$$

Find the Z-Y decomposition of the Hadamard gate $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$.

Hint: There exists a solution with $\beta = 0$.

Solution

(a)

$$|\psi\rangle = \frac{i}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle = i\left(\frac{1}{2}|0\rangle + i\frac{\sqrt{3}}{2}|1\rangle\right) \stackrel{!}{=} \mathrm{e}^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\right)$$

for $\theta = \frac{2\pi}{3}$, $\varphi = \frac{\pi}{2}$ and $\gamma = \frac{\pi}{2}$ (since $\mathrm{e}^{i\pi/2} = i$). Inserted into the Bloch vector results in

$$\vec{r} = (\cos(\varphi)\sin(\theta), \sin(\varphi)\sin(\theta), \cos(\theta)) = \left(0, \tfrac{\sqrt{3}}{2}, -\tfrac{1}{2}\right).$$

We observe that the Bloch vector lies in the y-z-plane.

(b) We first evaluate the rotation operator:

$$R_x(\tfrac{2\pi}{3}) = \cos(\tfrac{\pi}{3})I - i\sin(\tfrac{\pi}{3})X = \begin{pmatrix}\frac{1}{2} & -i\frac{\sqrt{3}}{2}\\ -i\frac{\sqrt{3}}{2} & \frac{1}{2}\end{pmatrix}.$$

Applying $R_x(\frac{2\pi}{3})$ to $|\psi\rangle$ gives

$$R_x(\tfrac{2\pi}{3})\,|\psi\rangle = \begin{pmatrix}\frac{1}{2} & -i\frac{\sqrt{3}}{2}\\ -i\frac{\sqrt{3}}{2} & \frac{1}{2}\end{pmatrix}\begin{pmatrix}\frac{i}{2}\\ -\frac{\sqrt{3}}{2}\end{pmatrix} = \begin{pmatrix}i\\ 0\end{pmatrix} = i\,|0\rangle.$$

On the Bloch sphere, R_x is a rotation about the x-axis; here $|\psi\rangle$ is rotated within the y-z-plane to the north pole. (The prefactor i in $i\,|0\rangle$ does not affect the Bloch vector representation.)

(c)

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \underbrace{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}}_{R_y(\frac{\pi}{2})}\underbrace{\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}}_{iR_z(\pi)} = \mathrm{e}^{i\pi/2}R_y(\tfrac{\pi}{2})R_z(\pi),$$

thus the parameters of the Z-Y decomposition are $\alpha = \frac{\pi}{2}$, $\beta = 0$, $\gamma = \frac{\pi}{2}$ and $\delta = \pi$.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 2.2 (Basic single qubit gates)
Imagine you are playing a game against an adversary. The game consists of multiple trials through which the adversary performs one of the following with equal probability:

1. They flip a coin and send you $|0\rangle$ or $|1\rangle$ depending on the outcome.

OR

2. They send you the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Your goal is to decide which of the two they performed, and you win if you can decide correctly for $\frac{3}{4}$ of the trials on average.

(a) Before you make your guess (based on a quantum measurement on the qubit), you are allowed to perform **one** of the gates X, Y, Z or H. Compute the outputs you would obtain in each situation with each of these gates.

(b) Which of the gates would allow you to win the game? Explain your strategy.

Solution hints

(a) Applying Hadamard for case 2 gives $|0\rangle$.

(b) Strategy consists of applying a Hadamard gate, performing a standard basis measurement, and voting for case 2 in case of measuring 0. Winning probability $\frac{3}{4}$ can be computed by enumerating all possible cases.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 2.2 (Basic single qubit gates)
Imagine you are playing a game against an adversary. The game consists of multiple trials through which the adversary performs one of the following with equal probability:

1. They flip a coin and send you $|0\rangle$ or $|1\rangle$ depending on the outcome.

OR

2. They send you the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Your goal is to decide which of the two they performed, and you win if you can decide correctly for $\frac{3}{4}$ of the trials on average.

(a) Before you make your guess (based on a quantum measurement on the qubit), you are allowed to perform **one** of the gates X, Y, Z or H. Compute the outputs you would obtain in each situation with each of these gates.

(b) Which of the gates would allow you to win the game? Explain your strategy.

Solution

(a) If we apply X then the outcome for each scenario will be:

1. $|1\rangle$ or $|0\rangle$.
2. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

$$\frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

If we apply Y:

1. $i\,|1\rangle$ or $-i\,|0\rangle$.
2. $\frac{i}{\sqrt{2}}(-|0\rangle + |1\rangle)$.

$$\frac{2|0\rangle}{2} = |0\rangle$$

If we apply Z:

1. $|0\rangle$ or $-|1\rangle$.
2. $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

If we apply H:

1. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
2. $|0\rangle$. $\Rightarrow \frac{1}{2}$

(b) Applying a Hadamard gate allows us to win the game. In the second scenario we would always measure 0, so if we measure 1 we know with certainty that we are in the first scenario. Therefore, our strategy would work as follows:

- Apply a Hadamard gate.
- Measure in the standard basis to obtain either 0 or 1.
- If we obtain 1 say we are in scenario 1.
- If we obtain 0 say we are in scenario 2.

Note that we will obtain 1 in $\frac{1}{4}$ of the trials, for which we will always be correct. For the remaining $\frac{3}{4}$ we will be correct in $\frac{2}{3}$ of the trials. Therefore, we will be correct $1 \cdot \frac{1}{4} + \frac{2}{3} \cdot \frac{3}{4} = \frac{3}{4}$ of the times, as required.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: 15 November 2021, 08:00 on Moodle

Tutorial 3 (Schrödinger equation for single qubits)
The Schrödinger equation

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t} |\psi(t)\rangle = H |\psi(t)\rangle \tag{1}$$

describes how a quantum state $|\psi(t)\rangle$ governed by a Hamiltonian operator H evolves in time $t \in \mathbb{R}$. In this tutorial, we assume that H is a time-independent Hermitian matrix (not to be confused with the Hadamard gate). The formal solution of Eq. (1) is then

$$|\psi(t)\rangle = U_t |\psi(0)\rangle \quad \text{with} \quad U_t = \mathrm{e}^{-iHt/\hbar}.$$

U_t is the unitary *time evolution operator*. In quantum computing, U_t is used as quantum gate. In the following, we absorb the reduced Planck constant $\hbar$ into H, effectively setting $\hbar = 1$.

(a) Show that U_t is indeed unitary.

(b) Consider the Hamiltonian operator

$$H = \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix}$$

acting on a single qubit, with the "frequency" parameters $\omega_1, \omega_2 \in \mathbb{R}$. Find U_t and $|\psi(t)\rangle$ for the initial state (i) $|\psi(0)\rangle = |0\rangle$ and (ii) $|\psi(0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

(c) We now add a small perturbation of strength ϵ to the Hamiltonian:

$$H = \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix} + \epsilon \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Compute U_t and the "overlap" $\langle 1|\psi(t)\rangle$ between $|1\rangle$ and $|\psi(t)\rangle$ for the initial state $|\psi(0)\rangle = |0\rangle$.

Hint: Represent H in terms of the identity and Pauli-X and Z matrices: $H = \bar{\omega} I + \sqrt{\Delta\omega^2 + \epsilon^2}\,(\vec{v} \cdot \vec{\sigma})$ with $\Delta\omega = (\omega_1 - \omega_2)/2$ and suitable $\bar{\omega} \in \mathbb{R}$, $\vec{v} \in \mathbb{R}^3$, and then use the definition of $R_{\vec{v}}(\theta)$ from the lecture.

Exercise 3.1 (Properties of Pauli matrices and matrix exponential)
As usual, $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) = (X, Y, Z)$ denotes the Pauli vector.

(a) Verify that the Pauli matrices anti-commute with each other, i.e.,

$$\{\sigma_1, \sigma_2\} = 0, \quad \{\sigma_2, \sigma_3\} = 0, \quad \{\sigma_3, \sigma_1\} = 0,$$

where $\{A, B\} = A\,B + B\,A$ denotes the *anti-commutator* of two matrices.

(b) Verify the following commutation relations (here $[A, B] = A\,B - B\,A$ denotes the *commutator* of two matrices):

$$[\sigma_1, \sigma_2] = 2i\sigma_3, \quad [\sigma_2, \sigma_3] = 2i\sigma_1, \quad [\sigma_3, \sigma_1] = 2i\sigma_2.$$

(c) Use the series expansion of the matrix exponential to derive that, for any $A \in \mathbb{C}^{n\times n}$ and unitary matrix $U \in \mathbb{C}^{n\times n}$,

$$\mathrm{e}^{U^\dagger A U} = U^\dagger\,\mathrm{e}^A\,U.$$

Remark: In case A is normal, one can combine this relation with the spectral decomposition to evaluate e^A, since the matrix exponential of a diagonal matrix is the pointwise exponential of the diagonal entries.

(d) Show that

$$HXH = Z \quad \text{and} \quad HZH = X,$$

where H denotes the Hadamard gate. (Since H is Hermitian and self-inverse, i.e., $H^2 = I$, H can thus be interpreted as base change matrix between the eigenvectors of X and Z.)

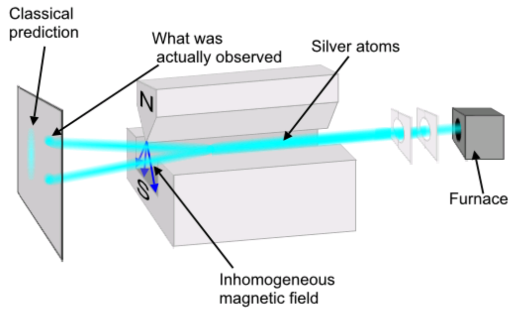
(e) Combine parts (c) and (d) to argue that

$$HR_x(\theta)H = R_z(\theta) \quad \text{for all } \theta \in \mathbb{R}.$$

Exercise 3.2 (The Stern-Gerlach experiment)

The Stern-Gerlach experiment is a fundamental experiment in the history of quantum mechanics, leading to the insight that electrons have an intrinsic, quantized spin degree of freedom. Otto Stern conceived the experiment in 1921, and conducted it together with Walther Gerlach in 1922.

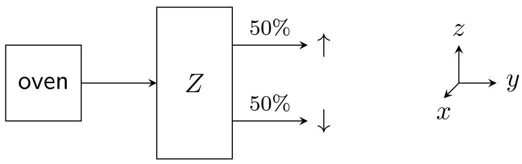
The setup is illustrated on the right. An oven (furnace) sends a beam of hot atoms through an inhomogeneous magnetic field, which causes the atoms to be deflected; the atoms are finally detected on a screen. The original experiment was conducted with silver atoms, but for our purpose it is simpler to discuss an analogous experiment with hydrogen atoms, which was performed in 1927.



https://commons.wikimedia.org/wiki/File:Stern-Gerlach_experiment.PNG

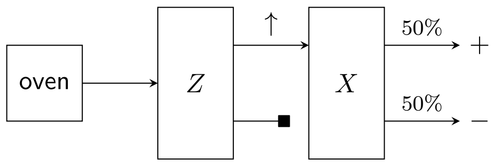
Based on classical physics, the electron orbiting around the proton in a hydrogen atom can be regarded as small magnetic dipole. One would then expect a continuous distribution of deflection angles, since the dipole axes are oriented randomly in space. Quantum mechanics predicts zero magnetic dipole moment for the hydrogen atom, and correspondingly the beam should not be deflected at all. Instead, a splitting into two beams was observed in the experiment.

We use the following schematic to summarize the Stern-Gerlach experiment:

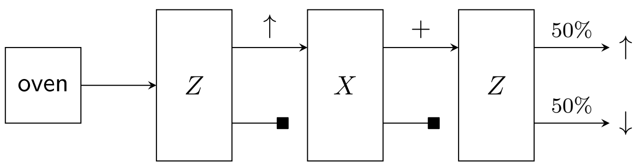


The coordinate system is chosen such that the beam propagates in y-direction. The inhomogeneous magnetic field (which we take to be oriented along the z-direction) splits the beam into two parts, one deflected up and the other down. Based on this description, one could hypothesize that each electron carries a classical bit of information, which specifies whether the atom goes up or down.

Now suppose we block the lower beam and send the upper beam through another inhomogeneous magnetic field, which is oriented along the x-direction. Classically, a dipole pointing in z-direction has zero moment in the x-direction, so one might expect that the final output is a single peak. Instead, experimentally one finds again two peaks, which we label $+$ and $-$:



Thus maybe each electron carries two classical bits of information, for selecting $\uparrow$ or $\downarrow$ and $+$ or $-$? If this was the case, and the electrons retained this information, then sending one beam of the previous output through another z-oriented field should result in a single beam deflected upwards. Instead, again two beams of equal intensity are observed:



Without any knowledge of quantum mechanics, it appears indeed challenging to invent a model explaining these observations.

Conversely, in the following we investigate the predictions of quantum mechanics when identifying the electronic spin as qubit, with $|0\rangle$ assigned to $\uparrow$ and $|1\rangle$ assigned to $\downarrow$. The inhomogeneous magnetic fields oriented along z- and x-direction measure the spin w.r.t. the eigenvectors of Pauli-Z (i.e., a standard measurement) and Pauli-X (equivalent to applying the Hadamard gate before the measurement and after the wavefunction collapse), respectively.

(a) Compute the eigenvalues and normalized eigenvectors of the Pauli-X, Y and Z matrices.

(b) Calculate the probabilities when measuring $|0\rangle$ with respect to the eigenvectors of X denoted $|+\rangle$, $|-\rangle$ (i.e., apply H before and after a standard measurement), and compare your results with the second schematic above.

(c) Explain the experimental observations of the third schematic setup. What would happen when orienting the last magnetic field along the x-direction instead of the z-direction?

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 3 (Schrödinger equation for single qubits)
The Schrödinger equation

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t} |\psi(t)\rangle = H |\psi(t)\rangle \tag{1}$$

describes how a quantum state $|\psi(t)\rangle$ governed by a Hamiltonian operator H evolves in time $t \in \mathbb{R}$. In this tutorial, we assume that H is a time-independent Hermitian matrix (not to be confused with the Hadamard gate). The formal solution of Eq. (1) is then

$$|\psi(t)\rangle = U_t |\psi(0)\rangle \quad \text{with} \quad U_t = \mathrm{e}^{-iHt/\hbar}.$$

U_t is the unitary *time evolution operator*. In quantum computing, U_t is used as quantum gate. In the following, we absorb the reduced Planck constant $\hbar$ into H, effectively setting $\hbar = 1$.

(a) Show that U_t is indeed unitary.

(b) Consider the Hamiltonian operator

$$H = \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix}$$

acting on a single qubit, with the "frequency" parameters $\omega_1, \omega_2 \in \mathbb{R}$. Find U_t and $|\psi(t)\rangle$ for the initial state (i) $|\psi(0)\rangle = |0\rangle$ and (ii) $|\psi(0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

(c) We now add a small perturbation of strength ϵ to the Hamiltonian:

$$H = \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix} + \epsilon \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Compute U_t and the "overlap" $\langle 1|\psi(t)\rangle$ between $|1\rangle$ and $|\psi(t)\rangle$ for the initial state $|\psi(0)\rangle = |0\rangle$.

Hint: Represent H in terms of the identity and Pauli-X and Z matrices: $H = \bar{\omega} I + \sqrt{\Delta\omega^2 + \epsilon^2}\,(\vec{v} \cdot \vec{\sigma})$ with $\Delta\omega = (\omega_1 - \omega_2)/2$ and suitable $\bar{\omega} \in \mathbb{R}$, $\vec{v} \in \mathbb{R}^3$, and then use the definition of $R_{\vec{v}}(\theta)$ from the lecture.

Solution

(a) First note that, for all $A \in \mathbb{C}^{n \times n}$,

$$\left(\mathrm{e}^{A}\right)^\dagger = \sum_{k=0}^{\infty} \frac{1}{k!} \left(A^k\right)^\dagger = \sum_{k=0}^{\infty} \frac{1}{k!} \left(A^\dagger\right)^k = \mathrm{e}^{(A^\dagger)}.$$

Together with the property that H is Hermitian, i.e., $H^\dagger = H$ and thus $(-iHt)^\dagger = iHt$, one obtains

$$U_t^\dagger U_t = \mathrm{e}^{iHt} \mathrm{e}^{-iHt} = \mathrm{e}^{i(H-H)t} = \mathrm{e}^0 = I.$$

(b) Since H is a diagonal matrix here, the matrix exponential e^{-iHt} can be computed by applying the exponential function to the diagonal entries:

$$U_t = \mathrm{e}^{-iHt} = \begin{pmatrix} \mathrm{e}^{-i\omega_1 t} & 0 \\ 0 & \mathrm{e}^{-i\omega_2 t} \end{pmatrix}.$$

We use vector notation to compute $|\psi(t)\rangle = U_t |\psi(0)\rangle$ for the two initial states:

$$U_t |0\rangle = \begin{pmatrix} \mathrm{e}^{-i\omega_1 t} & 0 \\ 0 & \mathrm{e}^{-i\omega_2 t} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathrm{e}^{-i\omega_1 t} \\ 0 \end{pmatrix} = \mathrm{e}^{-i\omega_1 t} |0\rangle$$

and

$$U_t \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{pmatrix} \mathrm{e}^{-i\omega_1 t} & 0 \\ 0 & \mathrm{e}^{-i\omega_2 t} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathrm{e}^{-i\omega_1 t} \\ \mathrm{e}^{-i\omega_2 t} \end{pmatrix} = \frac{1}{\sqrt{2}} \left(\mathrm{e}^{-i\omega_1 t} |0\rangle + \mathrm{e}^{-i\omega_2 t} |1\rangle\right).$$

(c) Following the hint, we represent

$$H = \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix} + \epsilon \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \bar{\omega} I + \Delta\omega Z + \epsilon X = \bar{\omega} I + \sqrt{\Delta\omega^2 + \epsilon^2}\,(\vec{v} \cdot \vec{\sigma})$$

with $\bar{\omega} = (\omega_1 + \omega_2)/2$, $\Delta\omega = (\omega_1 - \omega_2)/2$, the normalized vector

$$\vec{v} = \frac{1}{\sqrt{\Delta\omega^2 + \epsilon^2}} \begin{pmatrix} \epsilon \\ 0 \\ \Delta\omega \end{pmatrix}$$

and the Pauli vector $\vec{\sigma} = (X, Y, Z)$. Now using the properties of the generalized rotation operator (see lecture) leads to

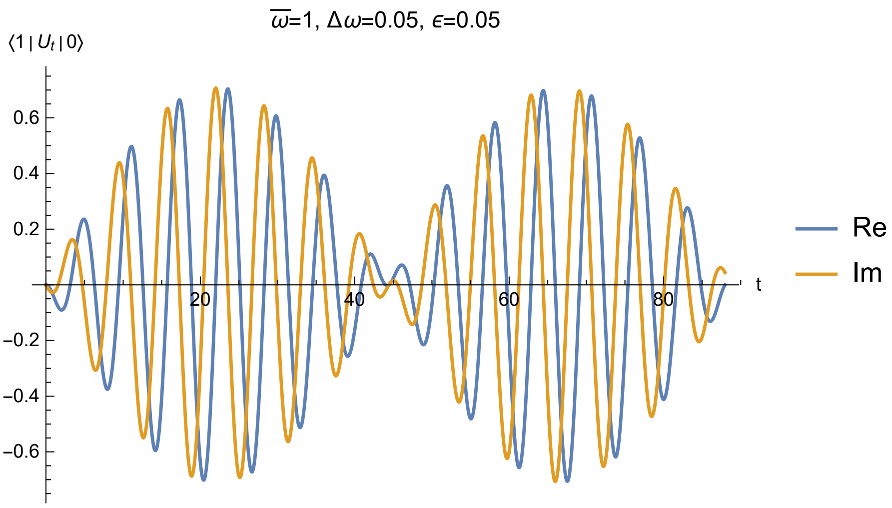
$$U_t = \mathrm{e}^{-iHt} = \mathrm{e}^{-i\bar{\omega}t}\,\mathrm{e}^{-i\sqrt{\Delta\omega^2+\epsilon^2}\,(\vec{v}\cdot\vec{\sigma})t} = \mathrm{e}^{-i\bar{\omega}t}\left(\cos\!\left(\sqrt{\Delta\omega^2 + \epsilon^2}\,t\right) I - i\sin\!\left(\sqrt{\Delta\omega^2 + \epsilon^2}\,t\right)(\vec{v}\cdot\vec{\sigma})\right).$$

The overlap is then

$$\begin{aligned} \langle 1 | \psi(t) \rangle = \langle 1 | U_t | 0 \rangle &= -i\,\mathrm{e}^{-i\bar{\omega}t} \sin\!\left(\sqrt{\Delta\omega^2 + \epsilon^2}\,t\right) \langle 1 | (\vec{v}\cdot\vec{\sigma}) | 0 \rangle \\ &= -i\,\mathrm{e}^{-i\bar{\omega}t} \sin\!\left(\sqrt{\Delta\omega^2 + \epsilon^2}\,t\right) \frac{\epsilon}{\sqrt{\Delta\omega^2 + \epsilon^2}}, \end{aligned}$$

where we have used that $\langle 1 | I | 0 \rangle = 0$, $\langle 1 | Z | 0 \rangle = 0$, $\langle 1 | X | 0 \rangle = 1$.

The following figure visualizes the real and imaginary parts of the overlap as function of time, for parameters $\omega_1 = 1.05$, $\omega_2 = 0.95$ and $\epsilon = 0.05$. One recognizes a fast oscillation with frequency $\bar{\omega}$, enveloped by a slow oscillation with frequency $\sqrt{\Delta\omega^2 + \epsilon^2}$.



Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 3.1 (Properties of Pauli matrices and matrix exponential)
As usual, $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) = (X, Y, Z)$ denotes the Pauli vector.

(a) Verify that the Pauli matrices anti-commute with each other, i.e.,

$$\{\sigma_1, \sigma_2\} = 0, \quad \{\sigma_2, \sigma_3\} = 0, \quad \{\sigma_3, \sigma_1\} = 0,$$

where $\{A, B\} = A\,B + B\,A$ denotes the *anti-commutator* of two matrices.

(b) Verify the following commutation relations (here $[A, B] = A\,B - B\,A$ denotes the *commutator* of two matrices):

$$[\sigma_1, \sigma_2] = 2i\sigma_3, \quad [\sigma_2, \sigma_3] = 2i\sigma_1, \quad [\sigma_3, \sigma_1] = 2i\sigma_2.$$

(c) Use the series expansion of the matrix exponential to derive that, for any $A \in \mathbb{C}^{n\times n}$ and unitary matrix $U \in \mathbb{C}^{n\times n}$,

$$\mathrm{e}^{U^\dagger A U} = U^\dagger\,\mathrm{e}^A\,U.$$

Remark: In case A is normal, one can combine this relation with the spectral decomposition to evaluate e^A, since the matrix exponential of a diagonal matrix is the pointwise exponential of the diagonal entries.

(d) Show that

$$HXH = Z \quad \text{and} \quad HZH = X,$$

where H denotes the Hadamard gate. (Since H is Hermitian and self-inverse, i.e., $H^2 = I$, H can thus be interpreted as base change matrix between the eigenvectors of X and Z.)

(e) Combine parts (c) and (d) to argue that

$$HR_x(\theta)H = R_z(\theta) \quad \text{for all } \theta \in \mathbb{R}.$$

Solution hints

(a) Explicit calculation to evaluate matrix products.

(b) Explicit calculation to evaluate matrix products.

(c) In the series expansion of $\mathrm{e}^{U^\dagger A U}$, the inner unitary terms cancel since $UU^\dagger = I$.

(d) Can show one of the relations by an explicit calculation, and the other by multiplying with H from both sides and using that $H^2 = I$.

(e) Insert the definition of $R_x(\theta)$ from the lecture, and use that $H^\dagger = H$.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 3.1 (Properties of Pauli matrices and matrix exponential)
As usual, $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) = (X, Y, Z)$ denotes the Pauli vector.

(a) Verify that the Pauli matrices anti-commute with each other, i.e.,

$$\{\sigma_1, \sigma_2\} = 0, \quad \{\sigma_2, \sigma_3\} = 0, \quad \{\sigma_3, \sigma_1\} = 0,$$

where $\{A, B\} = A\,B + B\,A$ denotes the *anti-commutator* of two matrices.

(b) Verify the following commutation relations (here $[A, B] = A\,B - B\,A$ denotes the *commutator* of two matrices):

$$[\sigma_1, \sigma_2] = 2i\sigma_3, \quad [\sigma_2, \sigma_3] = 2i\sigma_1, \quad [\sigma_3, \sigma_1] = 2i\sigma_2.$$

(c) Use the series expansion of the matrix exponential to derive that, for any $A \in \mathbb{C}^{n\times n}$ and unitary matrix $U \in \mathbb{C}^{n\times n}$,

$$\mathrm{e}^{U^\dagger A U} = U^\dagger\, \mathrm{e}^A\, U.$$

Remark: In case A is normal, one can combine this relation with the spectral decomposition to evaluate e^A, since the matrix exponential of a diagonal matrix is the pointwise exponential of the diagonal entries.

(d) Show that

$$HXH = Z \quad \text{and} \quad HZH = X,$$

where H denotes the Hadamard gate. (Since H is Hermitian and self-inverse, i.e., $H^2 = I$, H can thus be interpreted as base change matrix between the eigenvectors of X and Z.)

(e) Combine parts (c) and (d) to argue that

$$HR_x(\theta)H = R_z(\theta) \quad \text{for all } \theta \in \mathbb{R}.$$

Solution

(a) The anti-commutation relations can be verified by an explicit calculation:

$$\begin{aligned}\{\sigma_1, \sigma_2\} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = 0,\end{aligned}$$

and similarly for the other two.

(b) The commutation relations can likewise be verified by an explicit calculation:

$$\begin{aligned}[\sigma_1, \sigma_2] &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} - \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} - \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \\ &= \begin{pmatrix} 2i & 0 \\ 0 & -2i \end{pmatrix} \\ &= 2i\sigma_3,\end{aligned}$$

and similarly for the other two.

(c) We exploit that $UU^\dagger = I$:

$$\mathrm{e}^{U^\dagger A U} = \sum_{k=0}^{\infty} \frac{1}{k!} \underbrace{U^\dagger A U U^\dagger A U \cdots U^\dagger A U}_{k \text{ times}} = \sum_{k=0}^{\infty} \frac{1}{k!} U^\dagger A^k U = U^\dagger\, \mathrm{e}^A\, U.$$

(d) We can calculate explicitly

$$
\begin{aligned}
HZH &= \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\\
&= \frac{1}{2}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\\
&= \frac{1}{2}\begin{pmatrix}0 & 2\\ 2 & 0\end{pmatrix} = X.
\end{aligned}
$$

Multiplying this relation from left and right by H and using that $H^2 = I$ leads to

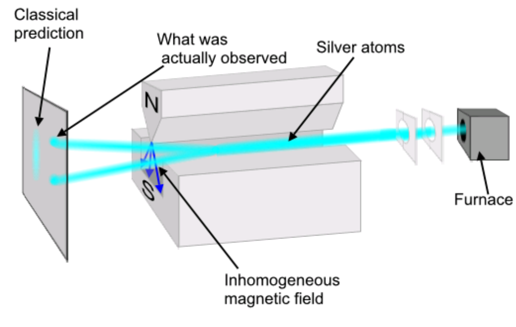
$$HXH = H(HZH)H = H^2ZH^2 = Z.$$

(e) We insert the definition of $R_x(\theta)$ from the lecture, and use that $H^\dagger = H$:

$$HR_x(\theta)H = H\mathrm{e}^{-i\theta X/2}H \overset{\text{(c)}}{=} \mathrm{e}^{-i\theta HXH/2} \overset{\text{(d)}}{=} \mathrm{e}^{-i\theta Z/2} = R_z(\theta).$$

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

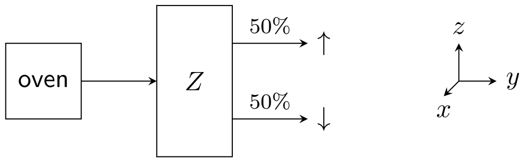
Exercise 3.2 (The Stern-Gerlach experiment)
The Stern-Gerlach experiment is a fundamental experiment in the history of quantum mechanics, leading to the insight that electrons have an intrinsic, quantized spin degree of freedom. Otto Stern conceived the experiment in 1921, and conducted it together with Walther Gerlach in 1922.
The setup is illustrated on the right. An oven (furnace) sends a beam of hot atoms through an inhomogeneous magnetic field, which causes the atoms to be deflected; the atoms are finally detected on a screen. The original experiment was conducted with silver atoms, but for our purpose it is simpler to discuss an analogous experiment with hydrogen atoms, which was performed in 1927.



https://commons.wikimedia.org/wiki/File:Stern-Gerlach_experiment.PNG

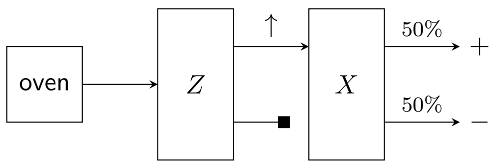
Based on classical physics, the electron orbiting around the proton in a hydrogen atom can be regarded as small magnetic dipole. One would then expect a continuous distribution of deflection angles, since the dipole axes are oriented randomly in space. Quantum mechanics predicts zero magnetic dipole moment for the hydrogen atom, and correspondingly the beam should not be deflected at all. Instead, a splitting into two beams was observed in the experiment.

We use the following schematic to summarize the Stern-Gerlach experiment:

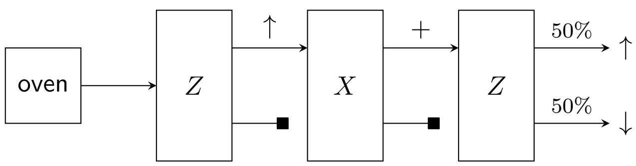


The coordinate system is chosen such that the beam propagates in y-direction. The inhomogeneous magnetic field (which we take to be oriented along the z-direction) splits the beam into two parts, one deflected up and the other down. Based on this description, one could hypothesize that each electron carries a classical bit of information, which specifies whether the atom goes up or down.

Now suppose we block the lower beam and send the upper beam through another inhomogeneous magnetic field, which is oriented along the x-direction. Classically, a dipole pointing in z-direction has zero moment in the x-direction, so one might expect that the final output is a single peak. Instead, experimentally one finds again two peaks, which we label $+$ and $-$:



Thus maybe each electron carries two classical bits of information, for selecting $\uparrow$ or $\downarrow$ and $+$ or $-$? If this was the case, and the electrons retained this information, then sending one beam of the previous output through another z-oriented field should result in a single beam deflected upwards. Instead, again two beams of equal intensity are observed:



Without any knowledge of quantum mechanics, it appears indeed challenging to invent a model explaining these observations.

Conversely, in the following we investigate the predictions of quantum mechanics when identifying the electronic spin as qubit, with $|0\rangle$ assigned to $\uparrow$ and $|1\rangle$ assigned to $\downarrow$. The inhomogeneous magnetic fields oriented along z- and x-direction measure the spin w.r.t. the eigenvectors of Pauli-Z (i.e., a standard measurement) and Pauli-X (equivalent to applying the Hadamard gate before the measurement and after the wavefunction collapse), respectively.

(a) Compute the eigenvalues and normalized eigenvectors of the Pauli-X, Y and Z matrices.

(b) Calculate the probabilities when measuring $|0\rangle$ with respect to the eigenvectors of X denoted $|+\rangle$, $|-\rangle$ (i.e., apply H before and after a standard measurement), and compare your results with the second schematic above.

(c) Explain the experimental observations of the third schematic setup. What would happen when orienting the last magnetic field along the x-direction instead of the z-direction?

Solution hints

(a) Each of the Pauli matrices has the eigenvalues $\lambda_{1,2} = \pm 1$. You can verify this using the characteristic polynomial, or noting that the Pauli matrices are Hermitian (hence their eigenvalues real), and that squaring them gives the identity matrix: $\sigma_j^2 = I$ for $j = 1, 2, 3$ (hence each eigenvalue λ satisfies $\lambda^2 = 1$). We can then identify the normalized eigenvectors by solving a series of linear equations and normalizing the results. For example, the eigenstates of X are:

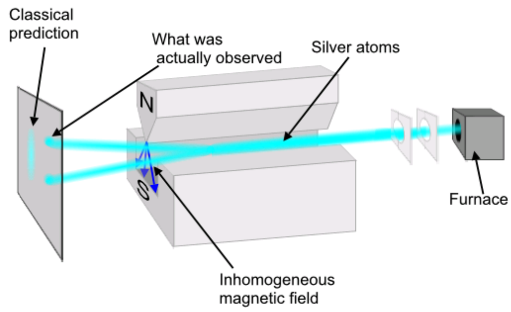
$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

(b) You should obtain $\frac{1}{2}$ for both probabilities.

(c) Orienting the last magnetic field along the x-direction means a repeated X-basis measurement. Since the quantum state is already the X eigenstate $|+\rangle$, the state will be unaffected by this repeated measurement, and the outcome will be "$+$" with probability 1.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

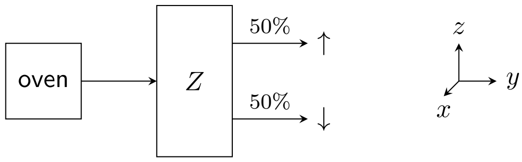
Exercise 3.2 (The Stern-Gerlach experiment)
The Stern-Gerlach experiment is a fundamental experiment in the history of quantum mechanics, leading to the insight that electrons have an intrinsic, quantized spin degree of freedom. Otto Stern conceived the experiment in 1921, and conducted it together with Walther Gerlach in 1922.
The setup is illustrated on the right. An oven (furnace) sends a beam of hot atoms through an inhomogeneous magnetic field, which causes the atoms to be deflected; the atoms are finally detected on a screen. The original experiment was conducted with silver atoms, but for our purpose it is simpler to discuss an analogous experiment with hydrogen atoms, which was performed in 1927.



https://commons.wikimedia.org/wiki/File:Stern-Gerlach_experiment.PNG

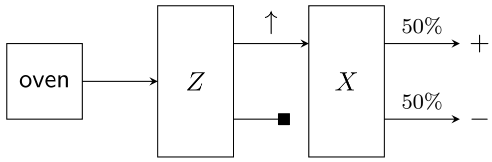
Based on classical physics, the electron orbiting around the proton in a hydrogen atom can be regarded as small magnetic dipole. One would then expect a continuous distribution of deflection angles, since the dipole axes are oriented randomly in space. Quantum mechanics predicts zero magnetic dipole moment for the hydrogen atom, and correspondingly the beam should not be deflected at all. Instead, a splitting into two beams was observed in the experiment.

We use the following schematic to summarize the Stern-Gerlach experiment:

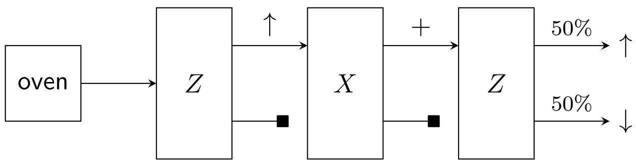


The coordinate system is chosen such that the beam propagates in y-direction. The inhomogeneous magnetic field (which we take to be oriented along the z-direction) splits the beam into two parts, one deflected up and the other down. Based on this description, one could hypothesize that each electron carries a classical bit of information, which specifies whether the atom goes up or down.

Now suppose we block the lower beam and send the upper beam through another inhomogeneous magnetic field, which is oriented along the x-direction. Classically, a dipole pointing in z-direction has zero moment in the x-direction, so one might expect that the final output is a single peak. Instead, experimentally one finds again two peaks, which we label $+$ and $-$:



Thus maybe each electron carries two classical bits of information, for selecting $\uparrow$ or $\downarrow$ and $+$ or $-$? If this was the case, and the electrons retained this information, then sending one beam of the previous output through another z-oriented field should result in a single beam deflected upwards. Instead, again two beams of equal intensity are observed:



Without any knowledge of quantum mechanics, it appears indeed challenging to invent a model explaining these observations.

Conversely, in the following we investigate the predictions of quantum mechanics when identifying the electronic spin as qubit, with $|0\rangle$ assigned to $\uparrow$ and $|1\rangle$ assigned to $\downarrow$. The inhomogeneous magnetic fields oriented along z- and x-direction measure the spin w.r.t. the eigenvectors of Pauli-Z (i.e., a standard measurement) and Pauli-X (equivalent to applying the Hadamard gate before the measurement and after the wavefunction collapse), respectively.

(a) Compute the eigenvalues and normalized eigenvectors of the Pauli-X, Y and Z matrices.

(b) Calculate the probabilities when measuring $|0\rangle$ with respect to the eigenvectors of X denoted $|+\rangle$, $|-\rangle$ (i.e., apply H before and after a standard measurement), and compare your results with the second schematic above.

(c) Explain the experimental observations of the third schematic setup. What would happen when orienting the last magnetic field along the x-direction instead of the z-direction?

Solution

(a) Each of the Pauli matrices has the eigenvalues $\lambda_{1,2} = \pm 1$. You can verify this using the characteristic polynomial, or noting that the Pauli matrices are Hermitian (hence their eigenvalues real), and that squaring them gives the identity matrix: $\sigma_j^2 = I$ for $j = 1, 2, 3$ (hence each eigenvalue λ satisfies $\lambda^2 = 1$). We can then identify the normalized eigenvectors by solving a series of linear equations and normalizing the results. For example:

$$\begin{aligned}
Xv &\overset{!}{=} v \\
v_2 &= v_1 \\
|\psi_{x,+}\rangle &= \frac{v}{\|v\|} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).
\end{aligned}$$

Similarly:

$$\begin{aligned}
|\psi_{x,+}\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad |\psi_{x,-}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \\
|\psi_{y,+}\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \quad |\psi_{y,-}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}i\\1\end{pmatrix} \\
|\psi_{z,+}\rangle &= \begin{pmatrix}1\\0\end{pmatrix}, \quad |\psi_{z,-}\rangle = \begin{pmatrix}0\\1\end{pmatrix}
\end{aligned}$$

(b) Following the description, we first apply a Hadamard gate before the measurement:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}.$$

The probabilities for the two possible measurement outcomes (labeled "+" and "−" here in reference to the eigenstates of X) are thus both equal to $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$, in agreement with the second schematic.

The quantum state immediately after the measurement is then

$$\begin{aligned}
H|0\rangle &= |\psi_{x,+}\rangle \quad \text{if measured } + \\
H|1\rangle &= |\psi_{x,-}\rangle \quad \text{if measured } -
\end{aligned}$$

(c) The quantum state immediately after a "+" outcome for the X-measurement is $|\psi_{x,+}\rangle$, and thus both measurement probabilities with respect to a subsequent standard Z-basis measurement equal to $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$.

Orienting the last magnetic field along the x-direction means a repeated X-basis measurement. Since the quantum state is already the X eigenstate $|\psi_{x,+}\rangle$, the state will be unaffected by this repeated measurement, and the outcome will be "+" with probability 1.

Tutorial 4 (Quantum circuit simulation)

In the lecture you learned about the tensor product of vector spaces to define multiple qubit spaces. Here we discuss how to compute and work with quantum gates applied to these qubits.

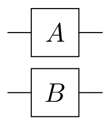
Given two vector spaces V and W and two operators A and B acting respectively on them, we define $A \otimes B$ implicitly via

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = (A\,|v\rangle) \otimes (B\,|w\rangle) \quad \text{for all } |v\rangle \in V \text{ and } |w\rangle \in W.$$

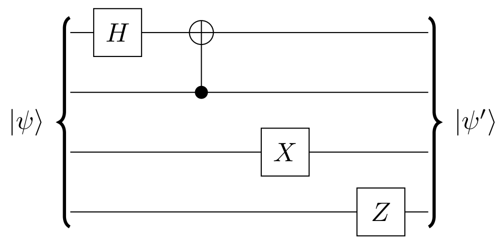
Using matrix notation, this leads to the *Kronecker product* of two matrices $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{p\times q}$:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \in \mathbb{C}^{mp\times nq},$$

with a_{ij} the entries of A, and the terms $a_{ij}B$ denoting $p \times q$ submatrices. The corresponding circuit diagram is

$A \otimes B =$ 

Now consider the following quantum circuit:

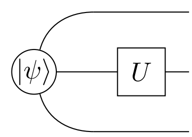


(a) What is the overall matrix representation of the first operation on $|\psi\rangle$?

(b) Assemble this matrix using Python/NumPy.

(c) If $|\psi\rangle$ was a 20 qubit state, what would be the dimension of the gates acting on it? Is it possible to store a *dense* matrix of such dimension on your laptop/PC? Discuss.

If a gate only acts non-trivially on a subset of the qubits, it can be implemented without forming the overall matrix. Specifically for a single-qubit gate U acting on the i-th qubit (counting from zero), we can first reshape the input state $|\psi\rangle$ into a $2^i \times 2 \times 2^{N-i-1}$ tensor and then apply U to the second dimension.

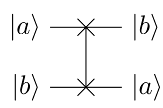


(d) Write a function that applies H to an arbitrary qubit of an input state $|\psi\rangle$ using a "matrix-free" approach.

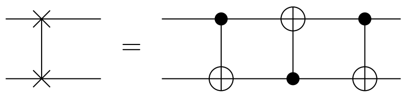
(e) Implement analogous functions for the X, Z and CNOT gates. Test your implementation via the above circuit with a random input state.

Exercise 4.1 (Basic quantum circuits)

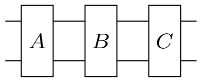
(a) Find the matrix representation (with respect to the computational basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$) of the *swap-gate* $|a,b\rangle \mapsto |b,a\rangle$, which is written in circuit form as



Also show that the swap operation is equivalent to the following sequence of three CNOT gates:

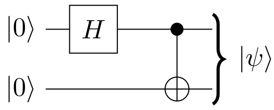


Hint: You can either work directly with basis states, e.g. $|a,b\rangle \overset{\text{CNOT}}{\mapsto} |a, a \oplus b\rangle$, or use matrix representations. In the latter case, note that a sequence of gates like



(with A, B, C unitary 4×4 matrices) corresponds to the matrix product CBA since the circuit is read from left to right, but the input vector in the matrix representation is multiplied from the right.

(b) Compute the output $|\psi\rangle$ of the following "entanglement circuit" applied to the input $|00\rangle$:



with $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ denoting the Hadamard gate.

(c) Build the CNOT gate from the controlled-Z gate and two Hadamard gates, and verify your construction.

Exercise 4.2 (IBM Q / Qiskit and Qaintum)
IBM Quantum (`https://quantum-computing.ibm.com/`) is a quantum cloud service and software platform, which allows users to run experiments even on real quantum computing hardware. For this exercise you should create a personal account and familiarize yourself with the service.

IBM Quantum offers a graphical *Circuit Composer* and *Qiskit Notebooks* as interface, which are Jupyter Python notebooks using the Qiskit open-source framework (`https://qiskit.org`). Both can be conveniently accessed online via a web browser; alternatively, you can also install Qiskit locally via `pip install qiskit`. An introduction to Qiskit is available at `https://qiskit.org/documentation/getting_started.html`.

(a) Use the Circuit Composer to construct the quantum circuit from exercise 4.1(b). You can view the corresponding `OPENQASM` code on the right side of the circuit interface. Compare the computed entries of the "Statevector" on the bottom left with the state $|\psi\rangle$ from exercise 4.1(b).

Please hand in a screenshot of the webpage.

(b) Construct the circuit again using Qiskit (including measurements), and execute the circuit via Aer's qasm_simulator (1024 shots).

Please hand in your code and the generated output.

(c) (Voluntary) Our group is working on a quantum computing software framework and circuit simulator written in Julia, see `https://github.com/Qaintum`. The main repository of the simulator is Qaintessent.jl, for which you will find the documentation under "docs". From your Julia command line you can install it via `using Pkg; Pkg.add("Qaintessent")`. Use this package to construct once again the circuit from 4.1(b) and measure both qubits with respect to the standard basis.

In the upcoming worksheets, programming assignments will be tested automatically by submitting your code through GitLab. Part (c) of this exercise is intended as test run for both you and us. Sign up and log in to your LRZ GitLab account (`https://gitlab.lrz.de/`) and follow these steps:

1. Edit Profile → Change Job Title to group number (set to an integer), i.e., for group 15, fill in '15'.
2. Go to "`https://gitlab.lrz.de/iqc`" and request access.
3. Wait until your request has been processed.
4. Follow the instructions in the ReadMe file.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 4 (Quantum circuit simulation)
In the lecture you learned about the tensor product of vector spaces to define multiple qubit spaces. Here we discuss how to compute and work with quantum gates applied to these qubits.

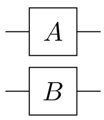
Given two vector spaces V and W and two operators A and B acting respectively on them, we define $A \otimes B$ implicitly via

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = (A\,|v\rangle) \otimes (B\,|w\rangle) \quad \text{for all } |v\rangle \in V \text{ and } |w\rangle \in W.$$

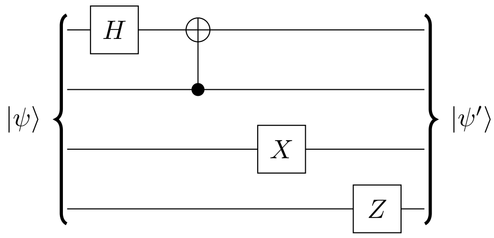
Using matrix notation, this leads to the *Kronecker product* of two matrices $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{p\times q}$:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \in \mathbb{C}^{mp\times nq},$$

with a_{ij} the entries of A, and the terms $a_{ij}B$ denoting $p \times q$ submatrices. The corresponding circuit diagram is

$A \otimes B =$ 

Now consider the following quantum circuit:

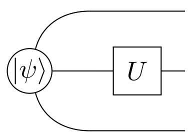


(a) What is the overall matrix representation of the first operation on $|\psi\rangle$?

(b) Assemble this matrix using Python/NumPy.

(c) If $|\psi\rangle$ was a 20 qubit state, what would be the dimension of the gates acting on it? Is it possible to store a *dense* matrix of such dimension on your laptop/PC? Discuss.

If a gate only acts non-trivially on a subset of the qubits, it can be implemented without forming the overall matrix. Specifically for a single-qubit gate U acting on the i-th qubit (counting from zero), we can first reshape the input state $|\psi\rangle$ into a $2^i \times 2 \times 2^{N-i-1}$ tensor and then apply U to the second dimension.



(d) Write a function that applies H to an arbitrary qubit of an input state $|\psi\rangle$ using a "matrix-free" approach.

(e) Implement analogous functions for the X, Z and CNOT gates. Test your implementation via the above circuit with a random input state.

Solution

(a) There is a Hadamard gate acting on the top qubit, and identities on the remaining three. Therefore the first operation is

$$H \otimes I_2 \otimes I_2 \otimes I_2 = H \otimes I_8 \in \mathbb{C}^{16\times 16},$$

with I_n denoting the $n \times n$ identity matrix.

(b) The NumPy function `kron` implements the Kronecker product:

```
import numpy as np
H = 1/np.sqrt(2) * np.array([[1, 1], [1,-1]])
H1 = np.kron(H, np.eye(8))
```

(c) It would be a $2^{20} \times 2^{20}$ matrix. Since a double precision floating-point value uses 8 bytes of memory, a matrix of this size would require $2^{20} \cdot 2^{20} \cdot 8$ bytes $= 2^{43}$ bytes $\approx 8.8 \times 10^{12}$ bytes $= 8.8$ TB of memory. No conventional PC or laptop has that much RAM. For a general gate with complex entries, even twice as much memory is needed.

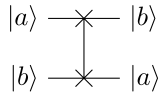
(d) See Jupyter notebook.

(e) See Jupyter notebook.

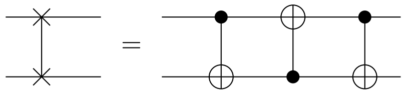
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 4.1 (Basic quantum circuits)

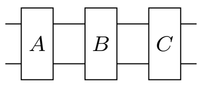
(a) Find the matrix representation (with respect to the computational basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$) of the *swap-gate* $|a, b\rangle \mapsto |b, a\rangle$, which is written in circuit form as



Also show that the swap operation is equivalent to the following sequence of three CNOT gates:

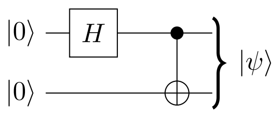


Hint: You can either work directly with basis states, e.g. $|a, b\rangle \overset{\text{CNOT}}{\mapsto} |a, a \oplus b\rangle$, or use matrix representations. In the latter case, note that a sequence of gates like



(with A, B, C unitary 4×4 matrices) corresponds to the matrix product CBA since the circuit is read from left to right, but the input vector in the matrix representation is multiplied from the right.

(b) Compute the output $|\psi\rangle$ of the following "entanglement circuit" applied to the input $|00\rangle$:



with $H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ denoting the Hadamard gate.

(c) Build the CNOT gate from the controlled-Z gate and two Hadamard gates, and verify your construction.

Solution hints

(a) The swap gate interchanges $|01\rangle \leftrightarrow |10\rangle$. Think about which elements are these in the two-qubit state vector. The swap matrix consists only of 0s and 1s. To prove the equivalency with the three CNOT gates using matrix representations, first convince yourself that the flipped CNOT gate reads

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

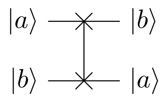
(b) The output is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

(c) Recall that H is self-inverse and note that $HZH = X$.

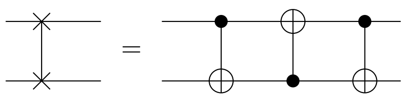
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 4.1 (Basic quantum circuits)

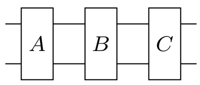
(a) Find the matrix representation (with respect to the computational basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$) of the *swap-gate* $|a, b\rangle \mapsto |b, a\rangle$, which is written in circuit form as



Also show that the swap operation is equivalent to the following sequence of three CNOT gates:

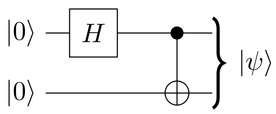


Hint: You can either work directly with basis states, e.g. $|a, b\rangle \overset{\text{CNOT}}{\mapsto} |a, a \oplus b\rangle$, or use matrix representations. In the latter case, note that a sequence of gates like



(with A, B, C unitary 4×4 matrices) corresponds to the matrix product CBA since the circuit is read from left to right, but the input vector in the matrix representation is multiplied from the right.

(b) Compute the output $|\psi\rangle$ of the following "entanglement circuit" applied to the input $|00\rangle$:



with $H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ denoting the Hadamard gate.

(c) Build the CNOT gate from the controlled-Z gate and two Hadamard gates, and verify your construction.

Solution

(a) The swap gate interchanges $|01\rangle \leftrightarrow |10\rangle$, thus

$$U_{\text{swap}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Concerning the sequence of three CNOT-gates:

$$|a, b\rangle \overset{\text{CNOT}}{\mapsto} |a, a \oplus b\rangle \overset{\text{flipped CNOT}}{\mapsto} |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \overset{\text{CNOT}}{\mapsto} |b, (a \oplus b) \oplus b\rangle = |b, a\rangle\,.$$

Here we have used that $a \oplus a = 0$ for $a \in \{0, 1\}$.

Alternative solution using matrix representations:

$$U_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad U_{\text{flipped CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

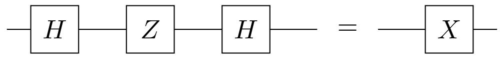
which gives as matrix representation of the three CNOT-gates:

$$U_{\mathsf{CNOT}} \cdot U_{\mathsf{flipped\ CNOT}} \cdot U_{\mathsf{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = U_{\mathsf{swap}}.$$

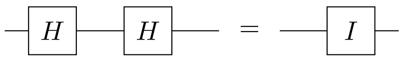
(b)

$$|00\rangle \overset{H\otimes I}{\mapsto} \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \overset{\mathsf{CNOT}}{\mapsto} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\psi\rangle$$

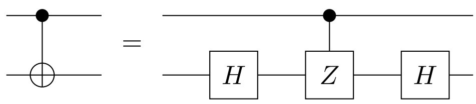
(c) Based on the matrix representation of the Hadamard gate and Pauli matrices, one directly verifies that $HZH = X$ and $H^2 = I$ (identity operation). Expressed in circuit form:



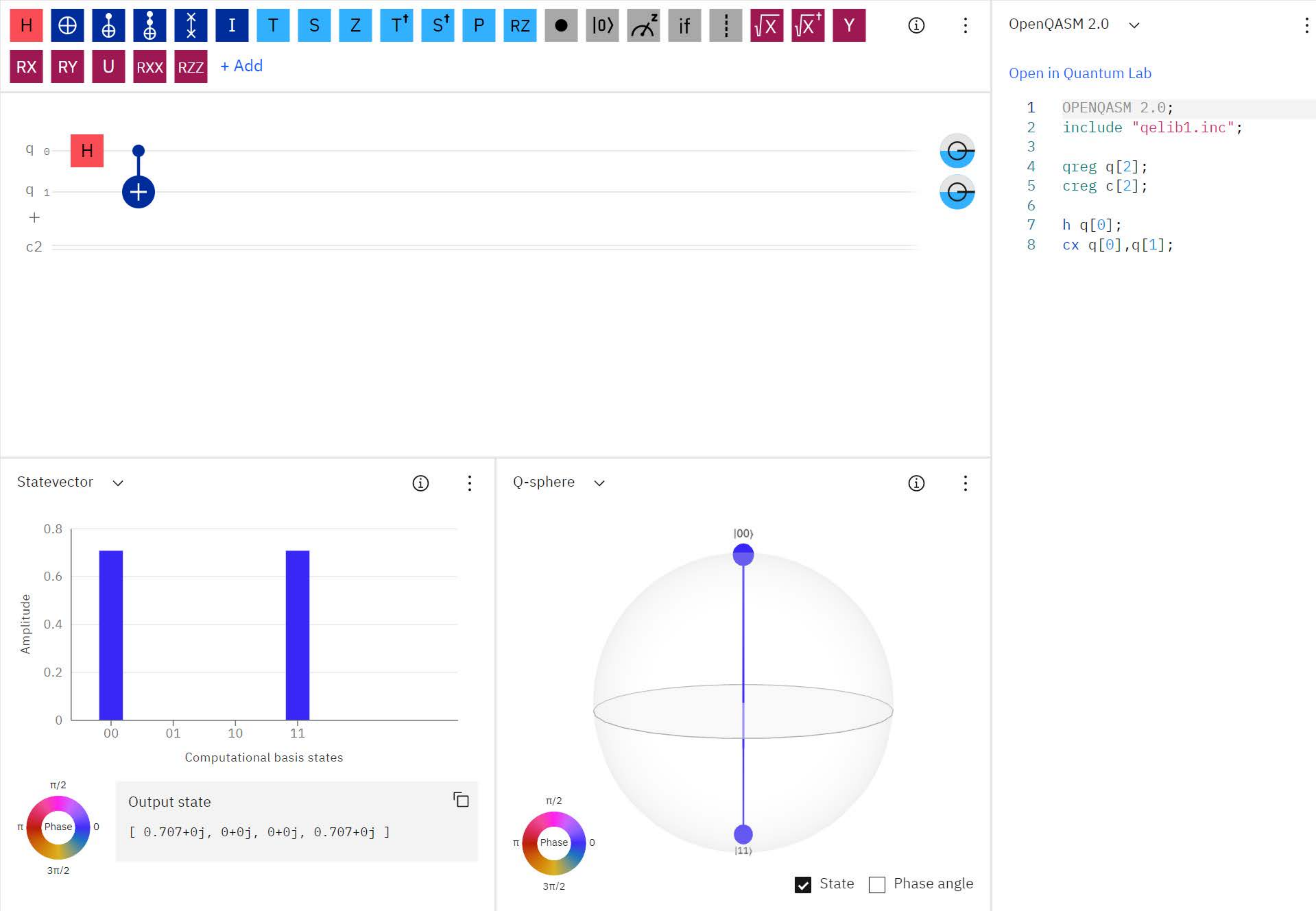
and



These properties lead to the following identity:



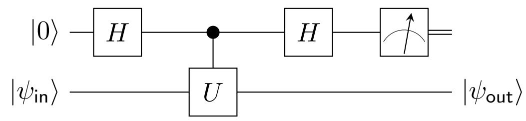
The circuit on the right is the requested construction.


H
I
T
S
Z
T†
S†
P
RZ
|0⟩
if
√X
√X†
Y
RX
RY
U
RXX
RZZ
+ Add
OpenQASM 2.0
Open in Quantum Lab
OPENQASM 2.0;
include "qelib1.inc";
qreg q[2];
creg c[2];
h q[0];
cx q[0],q[1];
q 0
q 1
c2
Statevector
0.8
0.6
0.4
0.2
0
Amplitude
00
01
10
11
Computational basis states
π/2
π
Phase
0
3π/2
Output state
[0.707+0j, 0+0j, 0+0j, 0.707+0j]
Q-sphere
|00⟩
|11⟩
π/2
π
Phase
0
3π/2
State
Phase angle

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: 29 November 2021, 08:00 on Moodle

Tutorial 5 (Measuring an operator[1])

Suppose U is a single qubit operator with eigenvalues ± 1, so that U is both Hermitian and unitary, i.e., 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. Show that this is implemented by the following quantum circuit:



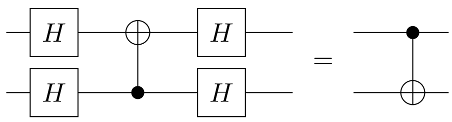
This tutorial requires the concept of an orthogonal projection (see also the linear algebra cheatsheet): a square matrix $P \in \mathbb{C}^{n\times n}$ is called an *orthogonal projection matrix* if P is Hermitian ($P^\dagger = P$) and $P^2 = P$, i.e., applying P a second time does not change the result any more. Note that a geometric projection is a special case of this abstract definition.

Exercise 5.1 (Basis transformation and measurement)

(a) Compute the probabilities when measuring $|\psi\rangle = \frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ with respect to the orthonormal basis $\{|u_1\rangle, |u_2\rangle\}$ given by $|u_1\rangle = \frac{3}{5}|0\rangle + i\frac{4}{5}|1\rangle$ and $|u_2\rangle = \frac{4}{5}|0\rangle - i\frac{3}{5}|1\rangle$.

Hint: You can obtain the coefficients of $|\psi\rangle$ with respect to these basis states by computing the inner products $\langle u_j|\psi\rangle$ for $j = 1, 2$.

(b) The role of the control and target qubit of a CNOT gate can be reversed by switching to a different basis! First show that



with H the Hadamard gate: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Use this identity to derive the following relations:

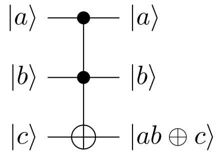
$$\begin{aligned}
|+\rangle|+\rangle &\overset{\text{CNOT}}{\mapsto} |+\rangle|+\rangle \\
|-\rangle|+\rangle &\overset{\text{CNOT}}{\mapsto} |-\rangle|+\rangle \\
|+\rangle|-\rangle &\overset{\text{CNOT}}{\mapsto} |-\rangle|-\rangle \\
|-\rangle|-\rangle &\overset{\text{CNOT}}{\mapsto} |+\rangle|-\rangle
\end{aligned}$$

with $|\pm\rangle$ defined as $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. In other words, with respect to the $|\pm\rangle$ basis, the second qubit assumes the role of the control and the first qubit the role of the target.

Hint: Use that $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$, and conversely $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$.

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Exercise 4.34

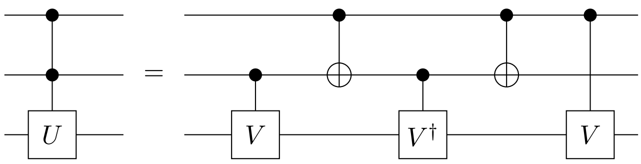
Exercise 5.2 (Toffoli gate and quantum logic)
The Toffoli gate is also known as CCNOT or "controlled-controlled-NOT" operation. In classical circuits, this gate inverts the target wire when the input of its two control wires is 1. Thus, defining the Toffoli gate in terms of computational basis states leads to (for any $a, b, c \in \{0, 1\}$):



The bottom (target) qubit gets flipped precisely if both control qubits are in the $|1\rangle$ state; equivalently, the flip occurs if the product ab equals 1, which leads to the expression $ab \oplus c$.

Physical quantum computers only implement a finite gate-set as hardware operations. Thus it is typically necessary to decompose such multi-control operations in terms of gates with at most one control wire. One such decomposition of a controlled-controlled-U operation, known as the Sleator and Weinfurter construction[2], is:

$|\psi\rangle = I$

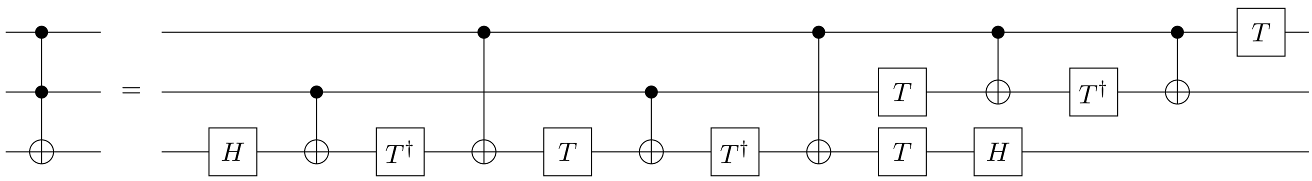


where V is a certain single-qubit gate depending on U. (The Toffoli gate corresponds to the special case $U = X$.)

(a) Which condition must V satisfy such that the equality holds? Verify your answer by inserting all four possible computational basis states for the control qubits.

(b) Find the V gate corresponding to $U = X$.
Hint: You can obtain a matrix power A^κ (with $\kappa \in \mathbb{R}$) of a normal matrix $A \in \mathbb{C}^{n \times n}$ by first computing its spectral decomposition: $A = U \operatorname{diag}(\lambda_1, \dots, \lambda_n) U^\dagger$ and U unitary; then exponentiate the eigenvalues, i.e., $A^\kappa = U \operatorname{diag}(\lambda_1^\kappa, \dots, \lambda_n^\kappa) U^\dagger$.

The so-called Clifford gates play an important role for quantum error correction and the Gottesman-Knill theorem.[3] Hence, most quantum computers support the "Clifford+T" gate set, which includes the Hadamard gate, the Pauli gates, the CNOT gate as well as the T gate, defined as $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$. It is possible to decompose the Toffoli gate in terms of these gates:



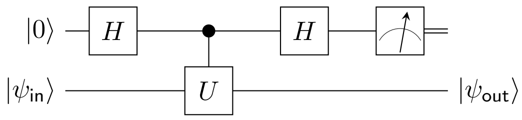
(c) Verify that the above circuit indeed implements the Toffoli gate.

[2] T. Sleator, H. Weinfurter: *Realizable Universal Quantum Logic Gates*. Phys. Rev. Lett. 74, 4087 (1995)
[3] Quantum error correction will be part of the follow-up course "Advanced Concepts of Quantum Computing" next semester.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

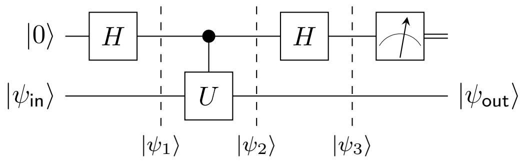
Tutorial 5 (Measuring an operator[1])

Suppose U is a single qubit operator with eigenvalues ± 1, so that U is both Hermitian and unitary, i.e., 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. Show that this is implemented by the following quantum circuit:



This tutorial requires the concept of an orthogonal projection (see also the linear algebra cheatsheet): a square matrix $P \in \mathbb{C}^{n\times n}$ is called an *orthogonal projection matrix* if P is Hermitian ($P^\dagger = P$) and $P^2 = P$, i.e., applying P a second time does not change the result any more. Note that a geometric projection is a special case of this abstract definition.

Solution We compute the intermediate two-qubit states $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$ shown below, which result from applying the circuit gates from left to right:



$$|\psi_1\rangle = (H|0\rangle) \otimes |\psi_{\text{in}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_{\text{in}}\rangle\,, \tag{1}$$

$$|\psi_2\rangle = (\text{controlled-}U)\,|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi_{\text{in}}\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes (U|\psi_{\text{in}}\rangle), \tag{2}$$

$$\begin{aligned}
|\psi_3\rangle &= \frac{1}{\sqrt{2}}(H|0\rangle) \otimes |\psi_{\text{in}}\rangle + \frac{1}{\sqrt{2}}(H|1\rangle) \otimes (U|\psi_{\text{in}}\rangle) \\
&= \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi_{\text{in}}\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes (U|\psi_{\text{in}}\rangle) \\
&= |0\rangle \otimes \frac{I+U}{2}|\psi_{\text{in}}\rangle + |1\rangle \otimes \frac{I-U}{2}|\psi_{\text{in}}\rangle \\
&= |0\rangle \otimes (P_+|\psi_{\text{in}}\rangle) + |1\rangle \otimes (P_-|\psi_{\text{in}}\rangle)
\end{aligned} \tag{3}$$

where we have defined $P_\pm = \frac{1}{2}(I \pm U)$. The $P_\pm$ are orthogonal projectors: they are Hermitian since U is Hermitian by assumption, and

$$P_\pm^2 = \frac{1}{4}(I \pm U)^2 = \frac{1}{4}\left(I \pm 2U + U^2\right) = \frac{1}{2}(I \pm U) = P_\pm.$$

In the last step we have used that $U^2 = U^\dagger U = I$. Moreover, the $P_\pm$ project onto orthogonal subspaces since

$$P_+ P_- = \frac{1}{4}(I + U)(I - U) = \frac{1}{4}\left(I - U^2\right) = 0.$$

Since $U = 1 \cdot P_+ + (-1) \cdot P_-$, we have found the spectral decomposition of U, i.e., the $P_\pm$ project onto the eigenspaces of U corresponding to the eigenvalues ± 1.

Now we show that the circuit can indeed be interpreted as measurement of $|\psi_{\text{in}}\rangle$ with measurement operators $P_\pm$: first, they satisfy the completeness relation since $P_+ + P_- = I$. Moreover, according to the last line of Eq. (3), $|\psi_3\rangle$ is a sum of two orthogonal states, and the probability that the measurement (in the circuit diagram) of the first qubit gives 0 or 1 is equal to the squared norm of the first and second state, respectively:

$$p(0) = \| |0\rangle \otimes (P_+|\psi_{\text{in}}\rangle) \|^2 = \|P_+|\psi_{\text{in}}\rangle\|^2 = \langle\psi_{\text{in}}|P_+^\dagger P_+|\psi_{\text{in}}\rangle = \langle\psi_{\text{in}}|P_+|\psi_{\text{in}}\rangle$$

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Exercise 4.34

and correspondingly $p(1) = \langle\psi_{\text{in}}| P_- |\psi_{\text{in}}\rangle$. Directly after the measurement, the second qubit will be in the state

$$|\psi_{\text{out}}\rangle = \frac{P_+ |\psi_{\text{in}}\rangle}{\|P_+ |\psi_{\text{in}}\rangle\|} \quad \text{if measured } 0,$$
$$|\psi_{\text{out}}\rangle = \frac{P_- |\psi_{\text{in}}\rangle}{\|P_- |\psi_{\text{in}}\rangle\|} \quad \text{if measured } 1$$

which agrees with the definition of a quantum measurement with operators $P_\pm$.

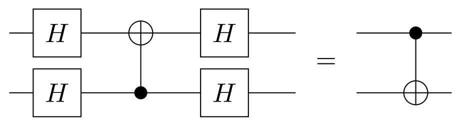
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 5.1 (Basis transformation and measurement)

(a) Compute the probabilities when measuring $|\psi\rangle = \frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ with respect to the orthonormal basis $\{|u_1\rangle, |u_2\rangle\}$ given by $|u_1\rangle = \frac{3}{5}|0\rangle + i\frac{4}{5}|1\rangle$ and $|u_2\rangle = \frac{4}{5}|0\rangle - i\frac{3}{5}|1\rangle$.

Hint: You can obtain the coefficients of $|\psi\rangle$ with respect to these basis states by computing the inner products $\langle u_j|\psi\rangle$ for $j = 1, 2$.

(b) The role of the control and target qubit of a CNOT gate can be reversed by switching to a different basis! First show that



with H the Hadamard gate: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Use this identity to derive the following relations:

$$
\begin{aligned}
|+\rangle|+\rangle &\overset{\text{CNOT}}{\mapsto} |+\rangle|+\rangle \\
|-\rangle|+\rangle &\overset{\text{CNOT}}{\mapsto} |-\rangle|+\rangle \\
|+\rangle|-\rangle &\overset{\text{CNOT}}{\mapsto} |-\rangle|-\rangle \\
|-\rangle|-\rangle &\overset{\text{CNOT}}{\mapsto} |+\rangle|-\rangle
\end{aligned}
$$

with $|\pm\rangle$ defined as $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. In other words, with respect to the $|\pm\rangle$ basis, the second qubit assumes the role of the control and the first qubit the role of the target.

Hint: Use that $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$, and conversely $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$.

Solution hints

(a) You should arrive at the following measurement probabilities:

$$
\begin{aligned}
p(u_1) &= |\alpha_1|^2 = \frac{1}{50}, \\
p(u_2) &= |\alpha_2|^2 = \frac{49}{50}.
\end{aligned}
$$

(b) To prove the first identity, you can use the relations $HXH = Z$ and $HZH = X$, see Exercise 3.1(d), and the fact that the controlled-Z gate is invariant when interchanging the roles of the control and target qubits.

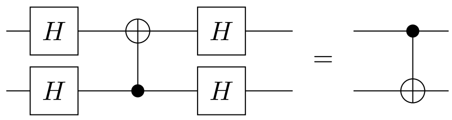
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 5.1 (Basis transformation and measurement)

(a) Compute the probabilities when measuring $|\psi\rangle = \frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ with respect to the orthonormal basis $\{|u_1\rangle, |u_2\rangle\}$ given by $|u_1\rangle = \frac{3}{5}|0\rangle + i\frac{4}{5}|1\rangle$ and $|u_2\rangle = \frac{4}{5}|0\rangle - i\frac{3}{5}|1\rangle$.

Hint: You can obtain the coefficients of $|\psi\rangle$ with respect to these basis states by computing the inner products $\langle u_j|\psi\rangle$ for $j = 1, 2$.

(b) The role of the control and target qubit of a CNOT gate can be reversed by switching to a different basis! First show that



with H the Hadamard gate: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Use this identity to derive the following relations:

$$|+\rangle|+\rangle \overset{\text{CNOT}}{\mapsto} |+\rangle|+\rangle$$
$$|-\rangle|+\rangle \overset{\text{CNOT}}{\mapsto} |-\rangle|+\rangle$$
$$|+\rangle|-\rangle \overset{\text{CNOT}}{\mapsto} |-\rangle|-\rangle$$
$$|-\rangle|-\rangle \overset{\text{CNOT}}{\mapsto} |+\rangle|-\rangle$$

with $|\pm\rangle$ defined as $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. In other words, with respect to the $|\pm\rangle$ basis, the second qubit assumes the role of the control and the first qubit the role of the target.

Hint: Use that $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$, and conversely $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$.

Solution

(a) We see that $\{|u_1\rangle, |u_2\rangle\}$ forms an orthonormal basis as $|u_1\rangle$ and $|u_2\rangle$ are normalized and $\langle u_1|u_2\rangle = 0$.

We then compute the inner products of $|\psi\rangle$ with $|u_1\rangle$ and $|u_2\rangle$:

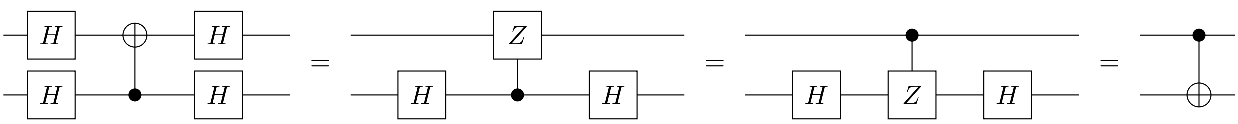
$$\alpha_1 = \langle u_1|\psi\rangle = -\frac{i}{5\sqrt{2}},$$
$$\alpha_2 = \langle u_2|\psi\rangle = \frac{7i}{5\sqrt{2}}.$$

Thus in terms of the new basis, $|\psi\rangle = \alpha_1|u_1\rangle + \alpha_2|u_2\rangle$.

The measurement probabilities are then the squared absolute values of the coefficients α_j:

$$p(u_1) = |\alpha_1|^2 = \frac{1}{50},$$
$$p(u_2) = |\alpha_2|^2 = \frac{49}{50}.$$

(b) Conjugating the Pauli-X gate with the Hadamard gate results in the Pauli-Z gate and other way around, i.e., $HXH = Z$ and $HZH = X$, see Exercise 3.1(d). Moreover, applying the Hadamard gate twice gives the identity, $H^2 = I$. This justifies the first and last step of the following identities:

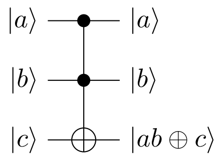


The second equal sign uses the fact that the controlled-Z operation is a diagonal matrix, with only a flipped sign on $|11\rangle$. Hence, this gate is invariant when interchanging the roles of the control and target qubits.

The relations then follow immediately by noting that the Hadamard gate switches between the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ bases.

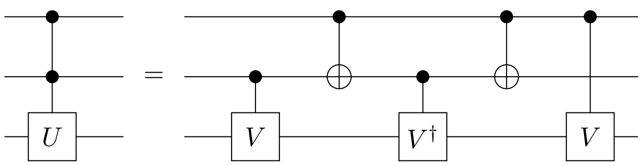
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 5.2 (Toffoli gate and quantum logic)
The Toffoli gate is also known as CCNOT or "controlled-controlled-NOT" operation. In classical circuits, this gate inverts the target wire when the input of its two control wires is 1. Thus, defining the Toffoli gate in terms of computational basis states leads to (for any $a, b, c \in \{0, 1\}$):



The bottom (target) qubit gets flipped precisely if both control qubits are in the $|1\rangle$ state; equivalently, the flip occurs if the product ab equals 1, which leads to the expression $ab \oplus c$.

Physical quantum computers only implement a finite gate-set as hardware operations. Thus it is typically necessary to decompose such multi-control operations in terms of gates with at most one control wire. One such decomposition of a controlled-controlled-U operation, known as the Sleator and Weinfurter construction[1], is:

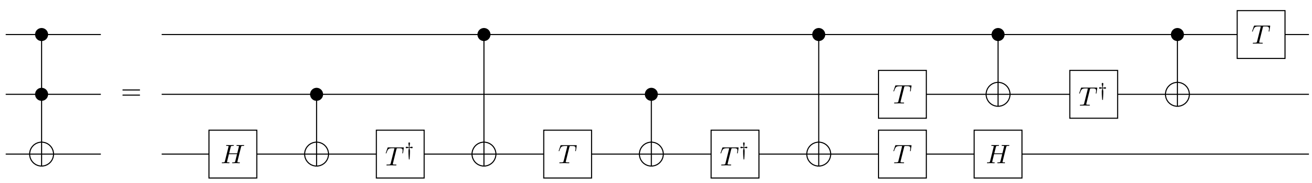


where V is a certain single-qubit gate depending on U. (The Toffoli gate corresponds to the special case $U = X$.)

(a) Which condition must V satisfy such that the equality holds? Verify your answer by inserting all four possible computational basis states for the control qubits.

(b) Find the V gate corresponding to $U = X$.
Hint: You can obtain a matrix power A^κ (with $\kappa \in \mathbb{R}$) of a normal matrix $A \in \mathbb{C}^{n\times n}$ by first computing its spectral decomposition: $A = U \operatorname{diag}(\lambda_1, \dots, \lambda_n)U^\dagger$ and U unitary; then exponentiate the eigenvalues, i.e., $A^\kappa = U \operatorname{diag}(\lambda_1^\kappa, \dots, \lambda_n^\kappa)U^\dagger$.

The so-called Clifford gates play an important role for quantum error correction and the Gottesman-Knill theorem.[2] Hence, most quantum computers support the "Clifford+T" gate set, which includes the Hadamard gate, the Pauli gates, the CNOT gate as well as the T gate, defined as $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{smallmatrix}\right)$. It is possible to decompose the Toffoli gate in terms of these gates:



(c) Verify that the above circuit indeed implements the Toffoli gate.

Solution hints

(a) The condition is $V^2 = U$.

(b) We need to find $V = \sqrt{X}$, i.e., $\kappa = \frac{1}{2}$ in the hint. The final result is

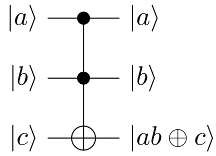
$$\sqrt{X} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \frac{1+i}{2} I + \frac{1-i}{2} X.$$

(c) Check the action of the circuit for the four possible inputs in the computational basis on the control qubits.

[1] T. Sleator, H. Weinfurter: *Realizable Universal Quantum Logic Gates*. Phys. Rev. Lett. 74, 4087 (1995)
[2] Quantum error correction will be part of the follow-up course "Advanced Concepts of Quantum Computing" next semester.

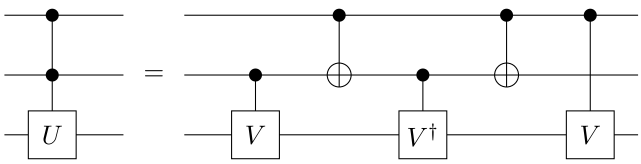
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 5.2 (Toffoli gate and quantum logic)
The Toffoli gate is also known as CCNOT or "controlled-controlled-NOT" operation. In classical circuits, this gate inverts the target wire when the input of its two control wires is 1. Thus, defining the Toffoli gate in terms of computational basis states leads to (for any $a, b, c \in \{0, 1\}$):



The bottom (target) qubit gets flipped precisely if both control qubits are in the $|1\rangle$ state; equivalently, the flip occurs if the product ab equals 1, which leads to the expression $ab \oplus c$.

Physical quantum computers only implement a finite gate-set as hardware operations. Thus it is typically necessary to decompose such multi-control operations in terms of gates with at most one control wire. One such decomposition of a controlled-controlled-U operation, known as the Sleator and Weinfurter construction[1], is:

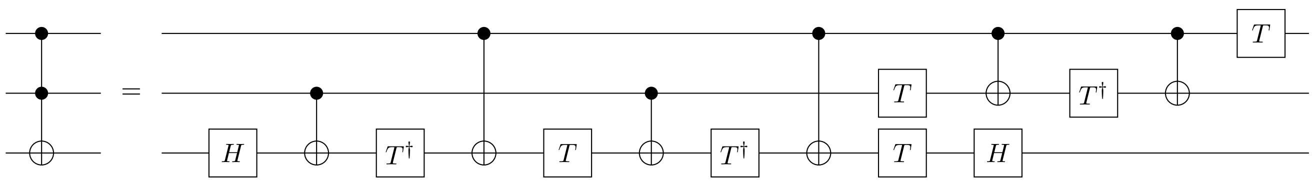


where V is a certain single-qubit gate depending on U. (The Toffoli gate corresponds to the special case $U = X$.)

(a) Which condition must V satisfy such that the equality holds? Verify your answer by inserting all four possible computational basis states for the control qubits.

(b) Find the V gate corresponding to $U = X$.
Hint: You can obtain a matrix power A^κ (with $\kappa \in \mathbb{R}$) of a normal matrix $A \in \mathbb{C}^{n\times n}$ by first computing its spectral decomposition: $A = U \operatorname{diag}(\lambda_1, \dots, \lambda_n)U^\dagger$ and U unitary; then exponentiate the eigenvalues, i.e., $A^\kappa = U \operatorname{diag}(\lambda_1^\kappa, \dots, \lambda_n^\kappa)U^\dagger$.

The so-called Clifford gates play an important role for quantum error correction and the Gottesman-Knill theorem.[2] Hence, most quantum computers support the "Clifford+T" gate set, which includes the Hadamard gate, the Pauli gates, the CNOT gate as well as the T gate, defined as $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$. It is possible to decompose the Toffoli gate in terms of these gates:



(c) Verify that the above circuit indeed implements the Toffoli gate.

Solution

(a) We first check the action of the circuit when the inputs on the control qubits are $|11\rangle$. We find that V^2 is applied to the target qubit. Hence, equality with the controlled-controlled-U operation requires that $V^2 = U$.

We can also verify the three other possible inputs on the control qubits, $|00\rangle, |01\rangle, |10\rangle$:

For $|00\rangle$, no gates are applied to the target qubit since all the controlled gates are inactive.

For $|01\rangle$, we see that $V^\dagger V = I$ is applied to the target qubit, and similarly for $|10\rangle$, $VV^\dagger = I$ is applied.

Hence, for the input states $|00\rangle, |01\rangle, |10\rangle$ on the control qubits, the circuit acts as identity, as required.

[1] T. Sleator, H. Weinfurter: *Realizable Universal Quantum Logic Gates*. Phys. Rev. Lett. 74, 4087 (1995)
[2] Quantum error correction will be part of the follow-up course "Advanced Concepts of Quantum Computing" next semester.

(b) We need to find $V = \sqrt{X}$, i.e., $\kappa = \frac{1}{2}$ in the hint. The spectral decomposition of the Pauli-X gate is

$$X = H \operatorname{diag}(1, -1) H,$$

with H the Hadamard gate (see previous exercises). Taking the square-root of the eigenvalues then leads to

$$\sqrt{X} = H \operatorname{diag}(1, i) H = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \frac{1+i}{2} I + \frac{1-i}{2} X.$$

(Multiplying the matrix on the right by itself indeed results in X, as expected.)

(c) Similar to part (a), we can simply check the action of the circuit for the four possible inputs in the computational basis on the control qubits. We first verify that no changes occur when the input to the control wires is not $|11\rangle$, noting that the T gate has no effect on qubits in the $|0\rangle$ state and $T^\dagger T = TT^\dagger = I$.

For $|00\rangle$, we see that $HTT^\dagger TT^\dagger H = I$ is applied to the target wire. (Note that the circuit diagram runs from left to right, while the order of applied matrices runs from right to left!) We then note that no changes occur in the control wires as they are both in the $|0\rangle$ state.

For $|01\rangle$, we see that $HTT^\dagger XTT^\dagger XH = I$ is applied to the target qubit. The output on the control wires is $(T|0\rangle) \otimes (T^\dagger T|1\rangle) = |01\rangle$.

For $|10\rangle$, we see that $HTXT^\dagger TXT^\dagger H = I$ is applied to the target wire. On the control wires, the action of the circuit is:

$$\begin{aligned}
&(T|1\rangle) \otimes (XT^\dagger XT|0\rangle) \\
&= (T|1\rangle) \otimes (XT^\dagger X|0\rangle) \\
&= e^{\frac{i\pi}{4}}|1\rangle \otimes (XT^\dagger|1\rangle) \\
&= e^{\frac{i\pi}{4}}|1\rangle \otimes (e^{\frac{-i\pi}{4}} X|1\rangle) \\
&= e^{\frac{i\pi}{4}}|1\rangle \otimes e^{\frac{-i\pi}{4}}|0\rangle = |10\rangle .
\end{aligned}$$

Finally, for $|11\rangle$, we see that $HT(XT^\dagger X)T(XT^\dagger X)H$ is applied to the target wire. We note the effect of conjugation by the Pauli-X gate is to flip the entries of a diagonal 2×2 matrix.

$$\begin{aligned}
XT^\dagger X &= \begin{pmatrix} \mathrm{e}^{-\frac{i\pi}{4}} & 0 \\ 0 & 1 \end{pmatrix}, \\
TXT^\dagger X &= \begin{pmatrix} \mathrm{e}^{-\frac{i\pi}{4}} & 0 \\ 0 & \mathrm{e}^{\frac{i\pi}{4}} \end{pmatrix}, \\
(TXT^\dagger X)^2 &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -iZ, \\
H(TXT^\dagger X)^2 H &= -iX.
\end{aligned}$$

We then note that the effect of the circuit on the control wires is effectively:

$$T|1\rangle \otimes T|1\rangle = i|11\rangle .$$

The final output of a circuit with input $|11x\rangle$, where $x \in \{0, 1\}$, is then

$$i|11\rangle \otimes (-iX|x\rangle) = |11\bar{x}\rangle ,$$

which realizes the Toffoli gate.

Tutorial 6 (The no-cloning theorem[1])

The *no-cloning theorem* states that, surprisingly, one cannot make a copy of an unknown quantum state. In more detail, we consider a system of two qubits (source and target): the first qubit is the source state $|\psi\rangle$, and the second qubit starts out in some standard state $|s\rangle$, for example $|s\rangle = |0\rangle$. Thus the initial state is $|\psi\rangle \otimes |s\rangle \equiv |\psi\rangle\,|s\rangle$. One would like to copy $|\psi\rangle$ into $|s\rangle$, that is, find some unitary transformation $U \in \mathbb{C}^{4\times 4}$ such that

$$|\psi\rangle \otimes |s\rangle \mapsto U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle\,.$$

Show that such a copying procedure is impossible: the equation cannot hold for arbitrary source qubits $|\psi\rangle$.

Exercise 6.1 (Heisenberg uncertainty principle for a single qubit)

Imagine we prepare multiple copies of an arbitrary single-qubit state $|\psi\rangle$, described by the Bloch vector (r_x, r_y, r_z). Some of these copies are measured using the observable Z, and the remaining copies using the observable X.

(a) Compute the expectation values of both measurements.
Hint: These two measurements are projective measurements and have a geometric interpretation on the Bloch sphere. You can use without proof the identities $\cos(\alpha/2)^2 - \sin(\alpha/2)^2 = \cos(\alpha)$ and $2\cos(\alpha/2)\sin(\alpha/2) = \sin(\alpha)$ for any $\alpha \in \mathbb{R}$.

(b) What will be their corresponding standard deviations? Recall from the lecture that the standard deviation of an observable M is defined as $\Delta M = \sqrt{\langle M^2\rangle - \langle M\rangle^2}$, with $\langle A\rangle \equiv \langle\psi|\,A\,|\psi\rangle$ for any observable A.

(c) Evaluate the commutator $[Z, X]$ and its expectation value $\langle\psi|\,[Z, X]\,|\psi\rangle$.

(d) Insert your results and explicitly verify that the Heisenberg uncertainty principle is satisfied.

Exercise 6.2 (Universal set of quantum gates[2])

A set of quantum gates is called *universal* if any unitary operation can be approximated to arbitrary accuracy by a quantum circuit composed of only gates in this set. An example is the set of single qubit gates and the CNOT gate. In particular, this set is able to represent any two-level unitary (that is, any unitary acting non-trivially only on at most two vector components). The set of two-level unitaries is universal, and consequently so is the set of single qubit gates and CNOT.

In this exercise, you will work on representing two-level unitaries as a combination of single qubit gates and the CNOT gate.

Consider a unitary U acting non-trivially only on two basis states: $|g_1\rangle$ and $|g_m\rangle$. Here, g_1 and g_m are two binary strings which differ in m bits. Flipping $m-1$ differing bits from g_1 results in g_{m-1}, which agrees with g_m except for a single bit. With this in mind, the circuit implementing U works as follows:

1. Apply controlled flips to swap the basis states $|g_1\rangle$ and $|g_{m-1}\rangle$.
2. Apply a controlled $\tilde{U}$ on the qubit in the position where $|g_m\rangle$ and $|g_{m-1}\rangle$ differ, conditional on the other qubits being in the state of the bits in both $|g_m\rangle$ and $|g_{m-1}\rangle$. Here $\tilde{U}$ is the non-trivial submatrix of U.
3. Swap back $|g_1\rangle$ and $|g_{m-1}\rangle$.

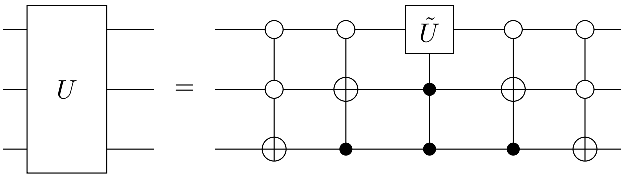
As an example, consider the following unitary operator U acting non-trivially only on $|000\rangle$ and $|111\rangle$:

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}, \quad \text{with} \quad \tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), page 532

[2] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), section 4.5.2

A circuit implementation of U is:



A white dot on the control qubit means that the gate only acts if the control is $|0\rangle$. Note that the first two controlled gates on the right realize the map $|000\rangle \mapsto |011\rangle$.

(a) Show that U and the above circuit are equivalent for an arbitrary input state.

(b) Without stating the full proof, explain why the controlled flips and the controlled $\tilde{U}$ can be replaced using only single qubit gates and the CNOT gate. Hint: Section 4.3 of the Nielsen and Chuang book may be helpful.

(c) Using the procedure above, find an implementation of the two-level operation

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{pmatrix}.$$

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 6 (The no-cloning theorem[1])

The *no-cloning theorem* states that, surprisingly, one cannot make a copy of an unknown quantum state. In more detail, we consider a system of two qubits (source and target): the first qubit is the source state $|\psi\rangle$, and the second qubit starts out in some standard state $|s\rangle$, for example $|s\rangle = |0\rangle$. Thus the initial state is $|\psi\rangle \otimes |s\rangle \equiv |\psi\rangle\,|s\rangle$. One would like to copy $|\psi\rangle$ into $|s\rangle$, that is, find some unitary transformation $U \in \mathbb{C}^{4\times 4}$ such that

$$|\psi\rangle \otimes |s\rangle \mapsto U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle\,.$$

Show that such a copying procedure is impossible: the equation cannot hold for arbitrary source qubits $|\psi\rangle$.

Solution Suppose the copying procedure works for two particular states $|\psi\rangle$ and $|\varphi\rangle$. Then

$$\begin{aligned} U(|\psi\rangle \otimes |s\rangle) &= |\psi\rangle \otimes |\psi\rangle\,, \\ U(|\varphi\rangle \otimes |s\rangle) &= |\varphi\rangle \otimes |\varphi\rangle\,. \end{aligned}$$

Taking inner products gives for the left sides

$$\Big\langle U(|\psi\rangle \otimes |s\rangle)\Big|U(|\varphi\rangle \otimes |s\rangle)\Big\rangle = (\langle\psi| \otimes \langle s|)U^\dagger U(|\varphi\rangle \otimes |s\rangle) = (\langle\psi| \otimes \langle s|)(|\varphi\rangle \otimes |s\rangle) = \langle\psi|\varphi\rangle\langle s|s\rangle = \langle\psi|\varphi\rangle$$

and for the right sides

$$\Big\langle\, |\psi\rangle \otimes |\psi\rangle \,\Big|\, |\varphi\rangle \otimes |\varphi\rangle \,\Big\rangle = \langle\psi|\varphi\rangle\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2,$$

leading to $\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2$. But this can only hold for $\langle\psi|\varphi\rangle = 1$ or $\langle\psi|\varphi\rangle = 0$, so either $|\psi\rangle = |\varphi\rangle$ or $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. In other words, general quantum cloning is impossible; for example, a potential quantum cloner cannot copy the qubit states $|\psi\rangle = |0\rangle$ and $|\varphi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

[1]M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), page 532

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 6.1 (Heisenberg uncertainty principle for a single qubit)
Imagine we prepare multiple copies of an arbitrary single-qubit state $|\psi\rangle$, described by the Bloch vector (r_x, r_y, r_z). Some of these copies are measured using the observable Z, and the remaining copies using the observable X.

(a) Compute the expectation values of both measurements.
Hint: These two measurements are projective measurements and have a geometric interpretation on the Bloch sphere. You can use without proof the identities $\cos(\alpha/2)^2 - \sin(\alpha/2)^2 = \cos(\alpha)$ and $2\cos(\alpha/2)\sin(\alpha/2) = \sin(\alpha)$.

(b) What will be their corresponding standard deviations? Recall from the lecture that the standard deviation of an observable M is defined as $\Delta M = \sqrt{\langle M^2\rangle - \langle M\rangle^2}$, with $\langle A\rangle \equiv \langle\psi| A |\psi\rangle$ for any observable A.

(c) Evaluate the commutator $[Z, X]$ and its expectation value $\langle\psi| [Z, X] |\psi\rangle$.

(d) Insert your results and explicitly verify that the Heisenberg uncertainty principle is satisfied.

Solution hints

(a) You should arrive at $\langle Z\rangle = r_z$ and $\langle X\rangle = r_x$.

(b) Note that $X^2 = Z^2 = I$.

(c) $[Z, X] = 2iY$.

(d) We already know the terms on the left-hand side of Heisenberg inequality, so we can focus on the right:

$$\langle\psi| [Z, X] |\psi\rangle = \langle\psi| 2iY |\psi\rangle = 2i\langle Y\rangle = 2ir_y$$

Plug this into the equation and check that the inequality is satisfied.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 6.1 (Heisenberg uncertainty principle for a single qubit)
Imagine we prepare multiple copies of an arbitrary single-qubit state $|\psi\rangle$, described by the Bloch vector (r_x, r_y, r_z). Some of these copies are measured using the observable Z, and the remaining copies using the observable X.

(a) Compute the expectation values of both measurements.
Hint: These two measurements are projective measurements and have a geometric interpretation on the Bloch sphere. You can use without proof the identities $\cos(\alpha/2)^2 - \sin(\alpha/2)^2 = \cos(\alpha)$ and $2\cos(\alpha/2)\sin(\alpha/2) = \sin(\alpha)$ for any $\alpha \in \mathbb{R}$.

(b) What will be their corresponding standard deviations? Recall from the lecture that the standard deviation of an observable M is defined as $\Delta M = \sqrt{\langle M^2\rangle - \langle M\rangle^2}$, with $\langle A\rangle \equiv \langle\psi| A |\psi\rangle$ for any observable A.

(c) Evaluate the commutator $[Z, X]$ and its expectation value $\langle\psi| [Z, X] |\psi\rangle$.

(d) Insert your results and explicitly verify that the Heisenberg uncertainty principle is satisfied.

Solution

(a) In the Bloch sphere, measuring Z corresponds to projecting onto the z-axis, and measuring X means projecting onto the x-axis. Therefore,

$$\langle Z\rangle = r_z \quad \text{and} \quad \langle X\rangle = r_x.$$

Alternatively, one can compute these expectation values starting from the Bloch angles θ and φ, which define the quantum state $|\psi\rangle$ via

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\varphi}\sin(\theta/2)\,|1\rangle\,,$$

and the Bloch vector via

$$\vec{r} = \begin{pmatrix} \cos(\varphi)\sin(\theta) \\ \sin(\varphi)\sin(\theta) \\ \cos(\theta) \end{pmatrix}.$$

(b) Note that $X^2 = Z^2 = I$. Thus, together with the normalization of the quantum state $|\psi\rangle$,

$$\Delta Z = \sqrt{1 - r_z^2}, \qquad \Delta X = \sqrt{1 - r_x^2}.$$

(c) Inserting the definitions of Z and X directly leads to

$$[Z, X] = ZX - XZ = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix} = 2iY.$$

Analogous to the expectation values of X and Z, one obtains $\langle Y\rangle = r_y$, and thus $\langle\psi| [Z, X] |\psi\rangle = 2ir_y$.

(d) The Heisenberg uncertainty principle states that

$$\Delta Z \Delta X \geq \frac{|\langle\psi| [Z, X] |\psi\rangle|}{2}.$$

In the present setting,

$$\sqrt{1 - r_z^2}\sqrt{1 - r_x^2} \overset{!}{\geq} |r_y|$$
$$(1 - r_z^2)(1 - r_x^2) \overset{!}{\geq} r_y^2$$
$$1 - r_z^2 - r_x^2 + r_z^2 r_x^2 \overset{!}{\geq} r_y^2$$

The Bloch vector must be normalized, i.e., $r_x^2 + r_y^2 + r_z^2 = 1$. Using this, the above inequality can be simplified to

$$r_z^2 r_x^2 \geq 0,$$

which is always true. The Heisenberg uncertainty principle is satisfied.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 6.2 (Universal set of quantum gates[2])
A set of quantum gates is called *universal* if any unitary operation can be approximated to arbitrary accuracy by a quantum circuit composed of only gates in this set. An example is the set of single qubit gates and the CNOT gate. In particular, this set is able to represent any two-level unitary (that is, any unitary acting non-trivially only on at most two vector components). The set of two-level unitaries is universal, and consequently so is the set of single qubit gates and CNOT.

In this exercise, you will work on representing two-level unitaries as a combination of single qubit gates and the CNOT gate.

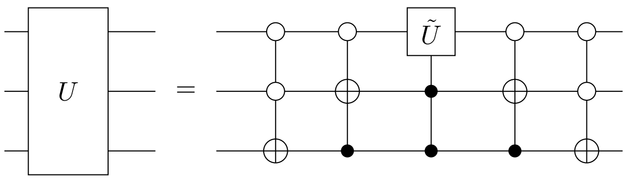
Consider a unitary U acting non-trivially only on two basis states: $|g_1\rangle$ and $|g_m\rangle$. Here, g_1 and g_m are two binary strings which differ in m bits. Flipping $m-1$ differing bits from g_1 results in g_{m-1}, which agrees with g_m except for a single bit. With this in mind, the circuit implementing U works as follows:

1. Apply controlled flips to swap the basis states $|g_1\rangle$ and $|g_{m-1}\rangle$.
2. Apply a controlled $\tilde{U}$ on the qubit in the position where $|g_m\rangle$ and $|g_{m-1}\rangle$ differ, conditional on the other qubits being in the state of the bits in both $|g_m\rangle$ and $|g_{m-1}\rangle$. Here $\tilde{U}$ is the non-trivial submatrix of U.
3. Swap back $|g_1\rangle$ and $|g_{m-1}\rangle$.

As an example, consider the following unitary operator U acting non-trivially only on $|000\rangle$ and $|111\rangle$:

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}, \quad \text{with} \quad \tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

A circuit implementation of U is:



A white dot on the control qubit means that the gate only acts if the control is $|0\rangle$. Note that the first two controlled gates on the right realize the map $|000\rangle \mapsto |011\rangle$.

(a) Show that U and the above circuit are equivalent for an arbitrary input state.

(b) Without stating the full proof, explain why the controlled flips and the controlled $\tilde{U}$ can be replaced using only single qubit gates and the CNOT gate. Hint: Section 4.3 of the Nielsen and Chuang book may be helpful.

(c) Using the procedure above, find an implementation of the two-level operation

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{pmatrix}.$$

[2] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), section 4.5.2

Solution hints

(a) Given an arbitrary input state

$$|\psi\rangle = x_0\,|000\rangle + x_1\,|001\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + x_7\,|111\rangle\,,$$

U only acts on $|000\rangle$ and $|111\rangle$. Explicitly applying the circuit gates to $|\psi\rangle$ gives the same result.

(b) The Toffoli gate can be decomposed into single-qubit and CNOT gates (see Exercise 5.2). Any unitary can be decomposed into $e^{i\alpha}AXBXC$, where $ABC = I$ (see Figure 4.6 in the Nielsen and Chuang book).

(c) U only acts non-trivially on $|010\rangle$ and $|111\rangle$. Swap $|010\rangle$ with $|011\rangle$ and apply controlled-$\tilde{U}$ on the first qubit.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 6.2 (Universal set of quantum gates[2])
A set of quantum gates is called *universal* if any unitary operation can be approximated to arbitrary accuracy by a quantum circuit composed of only gates in this set. An example is the set of single qubit gates and the CNOT gate. In particular, this set is able to represent any two-level unitary (that is, any unitary acting non-trivially only on at most two vector components). The set of two-level unitaries is universal, and consequently so is the set of single qubit gates and CNOT.

In this exercise, you will work on representing two-level unitaries as a combination of single qubit gates and the CNOT gate.

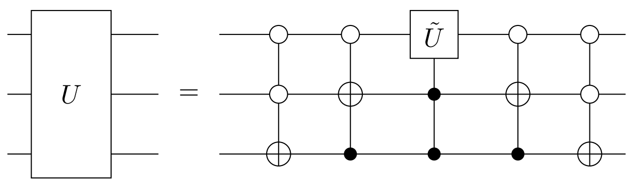
Consider a unitary U acting non-trivially only on two basis states: $|g_1\rangle$ and $|g_m\rangle$. Here, g_1 and g_m are two binary strings which differ in m bits. Flipping $m-1$ differing bits from g_1 results in g_{m-1}, which agrees with g_m except for a single bit. With this in mind, the circuit implementing U works as follows:

1. Apply controlled flips to swap the basis states $|g_1\rangle$ and $|g_{m-1}\rangle$.
2. Apply a controlled $\tilde{U}$ on the qubit in the position where $|g_m\rangle$ and $|g_{m-1}\rangle$ differ, conditional on the other qubits being in the state of the bits in both $|g_m\rangle$ and $|g_{m-1}\rangle$. Here $\tilde{U}$ is the non-trivial submatrix of U.
3. Swap back $|g_1\rangle$ and $|g_{m-1}\rangle$.

As an example, consider the following unitary operator U acting non-trivially only on $|000\rangle$ and $|111\rangle$:

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}, \quad \text{with} \quad \tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

A circuit implementation of U is:



A white dot on the control qubit means that the gate only acts if the control is $|0\rangle$. Note that the first two controlled gates on the right realize the map $|000\rangle \mapsto |011\rangle$.

(a) Show that U and the above circuit are equivalent for an arbitrary input state.

(b) Without stating the full proof, explain why the controlled flips and the controlled $\tilde{U}$ can be replaced using only single qubit gates and the CNOT gate. Hint: Section 4.3 of the Nielsen and Chuang book may be helpful.

(c) Using the procedure above, find an implementation of the two-level operation

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{pmatrix}.$$

[2]M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), section 4.5.2

Solution

(a) Given an arbitrary input state

$$|\psi\rangle = x_0\,|000\rangle + x_1\,|001\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + x_7\,|111\rangle\,,$$

then

$$U\,|\psi\rangle = (ax_0 + cx_7)\,|000\rangle + x_1\,|001\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + (bx_0 + dx_7)\,|111\rangle\,.$$

Applying each gate of the circuit:

$$|\psi\rangle \mapsto |\psi_1\rangle = x_0\,|001\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + x_7\,|111\rangle\,,$$

$$|\psi_1\rangle \mapsto |\psi_2\rangle = x_0\,|011\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|001\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + x_7\,|111\rangle\,,$$

$$\begin{aligned}
|\psi_2\rangle \mapsto |\psi_3\rangle &= x_0(\tilde{U}\,|0\rangle)\,|11\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|001\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + x_7(\tilde{U}\,|1\rangle)\,|11\rangle \\
&= ax_0\,|011\rangle + bx_0\,|111\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|001\rangle \\
&\quad + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + cx_7\,|011\rangle + dx_7\,|111\rangle \\
&= (ax_0 + cx_7)\,|011\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|001\rangle \\
&\quad + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + (bx_0 + dx_7)\,|111\rangle\,,
\end{aligned}$$

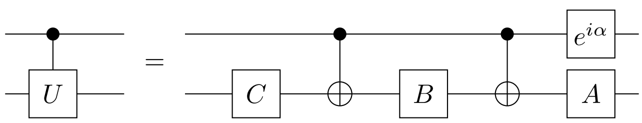
$$|\psi_3\rangle \mapsto |\psi_4\rangle = (x_0a + x_7c)\,|001\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + (x_0b + x_7d)\,|111\rangle\,,$$

$$|\psi_4\rangle \mapsto |\psi_5\rangle = (x_0a + x_7c)\,|000\rangle + x_1\,|001\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + (x_0b + x_7d)\,|111\rangle\,,$$

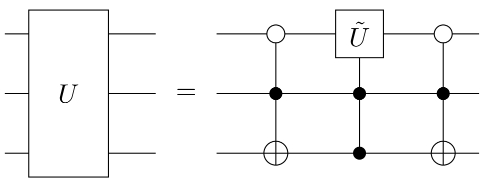
which agrees with $U\,|\psi\rangle$.

(b) All controlled flips can be written as a combination of Toffoli gates and X-Pauli gates (by simply including X gates before and after the white dots of the controlled flips). The Toffoli gate can be decomposed into single-qubit and CNOT gates, as shown in Exercise 5.2.

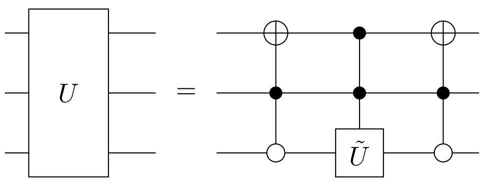
Any unitary can be decomposed into $e^{i\alpha}AXBXC$, where $ABC = I$. Therefore, the any controlled unitary can be decomposed into:



(c) U acts non-trivially only on $|010\rangle$ and $|111\rangle$. We first need to map $|010\rangle \mapsto |011\rangle$, and then apply a controlled-$\tilde{U}$ on the first qubit before swapping $|010\rangle$ and $|011\rangle$ again. This is realized by the circuit:



Alternatively, one can swap $|010\rangle \leftrightarrow |110\rangle$ and then apply the controlled-$\tilde{U}$ on the third qubit:



Tutorial 7 (Experimental quantum teleportation)
In this tutorial, we will discuss one of the first lab experiments[1] for quantum teleportation, which uses the polarization and "spatial path information" of photons as logical qubits. Quantum teleportation requires the following ingredients, which are challenging to realize experimentally:

1. the creation and distribution of entangled qubits,
2. measurement in the Bell basis.

The experimental setup is illustrated in the following Figure 1. It uses non-linear crystal excitations and beam splitters to generate entanglement.

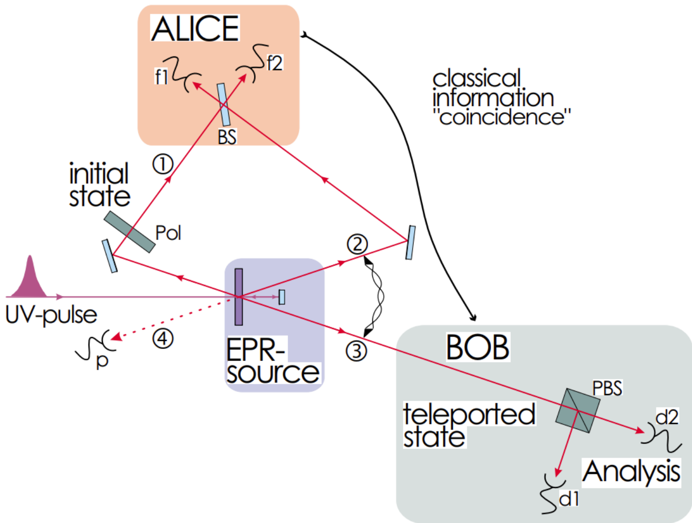


Figure 1: Quantum teleportation setup [1]

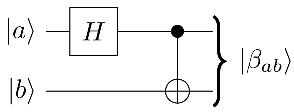
Discuss the various steps of the quantum teleportation process.

Exercise 7.1 (Bell states and superdense coding)
Recall that the *Bell states* are defined as

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

which can be summarized as $|\beta_{ab}\rangle = \frac{1}{\sqrt{2}}(|0,b\rangle + (-1)^a |1,1-b\rangle)$ for $a, b \in \{0,1\}$.

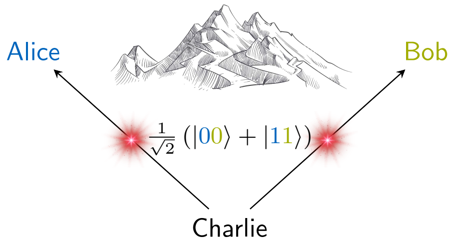
(a) Verify that the following quantum circuit creates the Bell states for inputs $|a,b\rangle$:

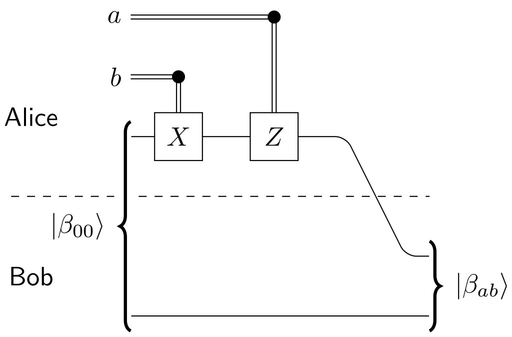


Note: this generalizes exercise 4.1(b). Since the circuit implements a unitary transformation of the standard basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, the Bell states form an orthonormal basis of the two qubit state space as well.

[1] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger: *Experimental quantum teleportation*. Nature 390, 575 (1997); see also: T. Jennewein, G. Weihs, A. Zeilinger: *Photon statistics and quantum teleportation experiments*. J. Phys. Soc. Jpn. 72, 168–173 (2003)

Superdense coding is a surprising use of entanglement to transmit two bits of classical information by sending just a single qubit! The setup agrees with quantum teleportation: two parties, usually referred to as Alice and Bob, live far from each other but share a pair of qubits in the entangled Bell state $|\beta_{00}\rangle$. They could have generated the pair during a visit in the past, or a common friend Charlie prepared it and sent one qubit to Alice and the other to Bob, as shown on the right.





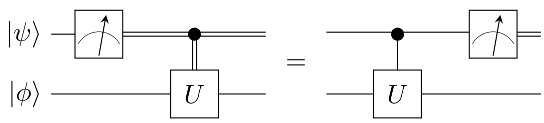
Now Alice's task is to communicate two bits 'ab' of classical information to Bob. Alice can achieve that by applying X and/or Z gates to her qubit before sending it to Bob, depending on the information she wants to transmit: for '00', she does nothing to her qubit, for '01' she applies X, for '10' she applies Z, and for '11' she applies first X and then Z, i.e., $ZX = iY$. It turns out that the resulting states are precisely the Bell states, which Bob can distinguish by performing a measurement with respect to this basis. The diagram on the left summarizes the protocol.

(b) Verify for all combinations of $a, b \in \{0, 1\}$ that the output of the circuit is indeed the Bell state $|\beta_{ab}\rangle$.

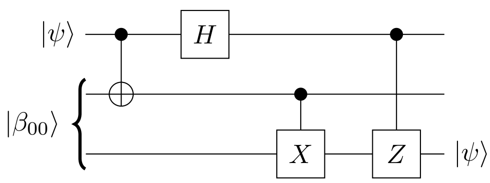
(c) Suppose E is an operator on Alice's qubit (e.g., $E = M_m^\dagger M_m$ in the general measurement framework, with M_m a measurement operator). Show that $\langle\beta_{ab}|E \otimes I\,|\beta_{ab}\rangle$ takes the same value for all four Bell states. Assuming an adversarial "Eve" intercepts Alice's qubit on the way to Bob, can Eve infer anything about the classical information which Alice tries to send?

Exercise 7.2 (Quantum teleportation circuit using IBM Q and Qiskit)

(a) By the *principle of deferred measurement*, measurement operations can always be moved to the end of the circuit, and classically controlled operations by conditional quantum operations. Verify this statement for the following controlled-U circuit, by inserting $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and computing the intermediate states:



(b) For the purpose of simulating the quantum teleportation circuit, we can exploit the principle of deferred measurement to omit the measurements altogether and rewrite the circuit in the following modified form:[2]



Construct this circuit in the IBM Q Circuit Composer. Insert a rotation operation at the beginning to prepare the initial qubit as $|\psi\rangle = R_y(\frac{\pi}{3})\,|0\rangle$. To check that the circuit works as intended, first compute the amplitudes α and β of the representation $R_y(\frac{\pi}{3})\,|0\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. Now insert a measurement operation at the end of the bottom qubit line, run 1024 "shots" your of circuit and compare the resulting measurement histogram with the expected probabilities $|\alpha|^2$ and $|\beta|^2$.

Also print a picture of your circuit and the corresponding `OPENQASM` code (shown in the Circuit Editor).

Hint: You can use the gates from exercise 3.1(b) to prepare the initial entangled pair $|\beta_{00}\rangle$.

(c) Construct the circuit in (b) using Qiskit, and execute the circuit via Aer's statevector_simulator. Print your code together with the final state vector.

Hint: See also https://github.com/Qiskit/qiskit-tutorials/blob/master/tutorials/simulators/1_aer_provider.ipynb.

[2] Note that the usual quantum teleportation protocol assumes that Alice and Bob are far from each other, such that conditional quantum operations between their qubits would be impractical.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 7 (Experimental quantum teleportation)
In this tutorial, we will discuss one of the first lab experiments[1] for quantum teleportation, which uses the polarization and "spatial path information" of photons as logical qubits. Quantum teleportation requires the following ingredients, which are challenging to realize experimentally:

1. the creation and distribution of entangled qubits,

2. measurement in the Bell basis.

The experimental setup is illustrated in the following Figure 1. It uses non-linear crystal excitations and beam splitters to generate entanglement.

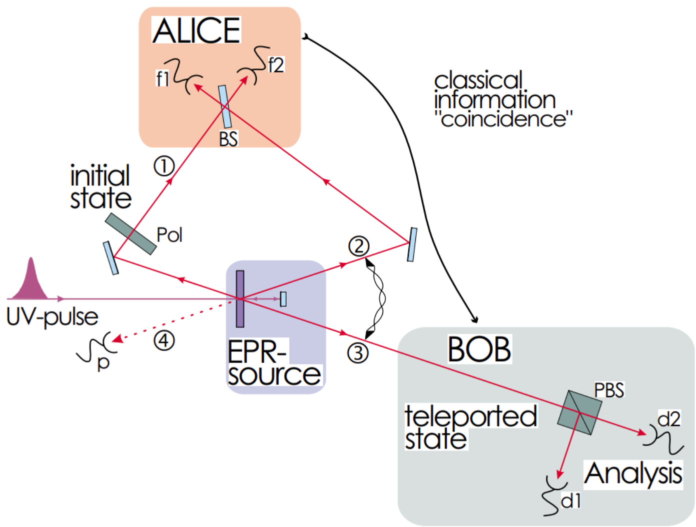


Figure 1: Quantum teleportation setup [1]

Discuss the various steps of the quantum teleportation process.

Solution The process can be divided into 4 steps:

1. An entangled pair is generated by exciting a non-linear crystal (like barium-borate) to produce an *polarity*-entangled pair of photons (labeled (2) and (3)) in the Bell state

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).$$

2. These photons are distributed to Alice and Bob.

3. The retroflection of the laser is used to generate a secondary entangled pair, one of which is discarded (4). The other (1) is initialized to an arbitrary polarization ($u, v \in \mathbb{C}$):

$$|\psi\rangle = u\,|0\rangle + v\,|1\rangle\,.$$

This is the state which Alice tries to teleport to Bob.

[1] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger: *Experimental quantum teleportation*. Nature 390, 575 (1997); see also: T. Jennewein, G. Weihs, A. Zeilinger: *Photon statistics and quantum teleportation experiments*. J. Phys. Soc. Jpn. 72, 168–173 (2003)

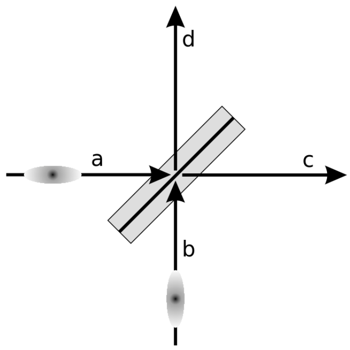
We can now represent the overall three-qubit state as follows:

$$\begin{aligned}
|\psi\rangle\,|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(u\,|0\rangle + v\,|1\rangle)(|01\rangle - |10\rangle) \\
&= -\frac{1}{2\sqrt{2}}\Big(-2u\,|001\rangle + 2u\,|010\rangle - 2v\,|101\rangle + 2v\,|110\rangle \Big) \\
&= -\frac{1}{2\sqrt{2}}\Big((|00\rangle + |11\rangle)\,(v\,|0\rangle - u\,|1\rangle) \\
&\qquad\quad (|00\rangle - |11\rangle)\,(-v\,|0\rangle - u\,|1\rangle) \\
&\qquad\quad (|01\rangle + |10\rangle)\,(u\,|0\rangle - v\,|1\rangle) \\
&\qquad\quad (|01\rangle - |10\rangle)\,(u\,|0\rangle + v\,|1\rangle) \Big) \\
&= -\frac{1}{2}\Big(|\beta_{00}\rangle\, iY\,|\psi\rangle - |\beta_{10}\rangle\, X\,|\psi\rangle + |\beta_{01}\rangle\, Z\,|\psi\rangle + |\beta_{11}\rangle\,|\psi\rangle \Big).
\end{aligned}$$

(Note that the gates which Alice applies in the quantum teleportation circuit perform a base change between the Bell basis and standard basis, and hence Alice's overall operation can be interpreted as measurement with respect to the Bell basis.)

4. In the experimental realization, only the Bell state $|\beta_{11}\rangle$ of Alice's photons (1) and (2) is probed for. Note that $|\beta_{11}\rangle$ is distinct from the other Bell states in the sense that it is antisymmetric, i.e., it flips its sign when swapping both particles, while the other three Bell states are symmetric. According to the above representation, detecting $|\beta_{11}\rangle$ for (1) and (2) will collapse Bob's qubit into $|\psi\rangle$.

   This measurement step is performed by combining the photons via a 50-50 beam splitter. This means that there is an equal possibility that incoming photons either pass through or are reflected by the beam splitter.



The action of a beam splitter on a single photon is:

$$|a\rangle \overset{\text{BS}}{\mapsto} \frac{1}{\sqrt{2}}(|c\rangle + i\,|d\rangle), \qquad |b\rangle \overset{\text{BS}}{\mapsto} \frac{1}{\sqrt{2}}(|d\rangle + i\,|c\rangle),$$

introducing a phase of i in the case of reflection.

Here, we examine the *spatial* coupling of two indistinguishable photons, a and b, along the outgoing paths c and d. The trick consists of differentiating (e.g., using photodetectors) between the case that

(i) both photons emerge along path c or both along d, or

(ii) the photons emerge at different paths, i.e., one photon travels along c and the other along d.

We can use this experimental protocol to determine whether the incident photons are in a symmetric or antisymmetric superposition. Namely for a symmetric input:

$$\begin{aligned}
\frac{1}{\sqrt{2}}(|ab\rangle + |ba\rangle) &\overset{\text{BS}}{\mapsto} \frac{1}{2\sqrt{2}}\Big((|c\rangle + i\,|d\rangle)(|d\rangle + i\,|c\rangle) + (|d\rangle + i\,|c\rangle)(|c\rangle + i\,|d\rangle)\Big) \\
&= \frac{1}{2\sqrt{2}}\Big(|cd\rangle + i\,|cc\rangle + i\,|dd\rangle - |dc\rangle + |dc\rangle + i\,|dd\rangle + i\,|cc\rangle - |cd\rangle \Big) \\
&= \frac{i}{\sqrt{2}}(|cc\rangle + |dd\rangle),
\end{aligned}$$

that is, either both photons emerge in c or both in d (case (i)).

Analogously for an antisymmetric input state:

$$\frac{1}{\sqrt{2}}(|ab\rangle - |ba\rangle) \overset{\text{BS}}{\mapsto} \cdots = \frac{1}{\sqrt{2}}(|cd\rangle - |dc\rangle),$$

which is a superposition of $|cd\rangle$ and $|dc\rangle$ and means that the photons travel along different paths (case (ii)).

Verification of the teleportation information is performed with a *polarizing beam splitter* (PBS) that only reflects a particular polarization and allows the rest to pass through. This is done by tuning qubit (1) to a particular polarity and adjusting the PBS to reflect that particular polarity. Note that Alice still has to classically transmit the information whether case (ii) occurred to Bob.

Remark: The experimental details of this tutorial are not relevant for the final exam.

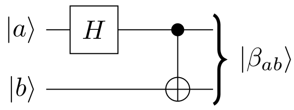
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 7.1 (Bell states and superdense coding)
Recall that the *Bell states* are defined as

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

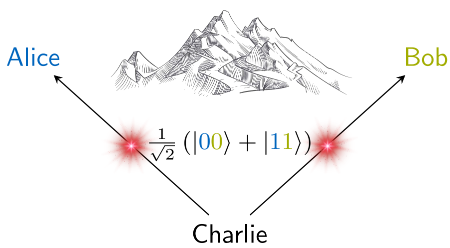
which can be summarized as $|\beta_{ab}\rangle = \frac{1}{\sqrt{2}}(|0,b\rangle + (-1)^a |1,1-b\rangle)$ for $a, b \in \{0,1\}$.

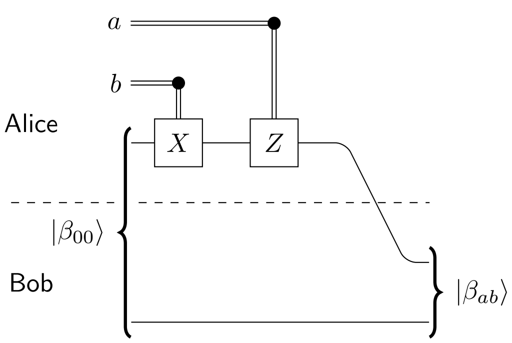
(a) Verify that the following quantum circuit creates the Bell states for inputs $|a,b\rangle$:



Note: this generalizes exercise 4.1(b). Since the circuit implements a unitary transformation of the standard basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, the Bell states form an orthonormal basis of the two qubit state space as well.

Superdense coding is a surprising use of entanglement to transmit two bits of classical information by sending just a single qubit! The setup agrees with quantum teleportation: two parties, usually referred to as Alice and Bob, live far from each other but share a pair of qubits in the entangled Bell state $|\beta_{00}\rangle$. They could have generated the pair during a visit in the past, or a common friend Charlie prepared it and sent one qubit to Alice and the other to Bob, as shown on the right.





Now Alice's task is to communicate two bits 'ab' of classical information to Bob. Alice can achieve that by applying X and/or Z gates to her qubit before sending it to Bob, depending on the information she wants to transmit: for '00', she does nothing to her qubit, for '01' she applies X, for '10' she applies Z, and for '11' she applies first X and then Z, i.e., $ZX = iY$. It turns out that the resulting states are precisely the Bell states, which Bob can distinguish by performing a measurement with respect to this basis. The diagram on the left summarizes the protocol.

(b) Verify for all combinations of $a, b \in \{0,1\}$ that the output of the circuit is indeed the Bell state $|\beta_{ab}\rangle$.

(c) Suppose E is an operator on Alice's qubit (e.g., $E = M_m^\dagger M_m$ in the general measurement framework, with M_m a measurement operator). Show that $\langle\beta_{ab}| E \otimes I |\beta_{ab}\rangle$ takes the same value for all four Bell states. Assuming an adversarial "Eve" intercepts Alice's qubit on the way to Bob, can Eve infer anything about the classical information which Alice tries to send?

Solution hints

(a) Explicitly apply the two gates to the input state $|a,b\rangle$ (with $a, b \in \{0,1\}$). The action of the Hadamard gate on $|a\rangle$ can be written as

$$|a\rangle \overset{H}{\mapsto} \frac{|0\rangle + (-1)^a |1\rangle}{\sqrt{2}}.$$

(b) Either enumerate all four cases explicitly, or note that the operation of the classically-controlled gates can be summarized as $Z^a X^b$ for $a, b \in \{0,1\}$ (with the convention that a matrix to the power of zero is the identity) and then evaluate $(Z^a X^b \otimes I)|\beta_{00}\rangle$.

(c) Evaluate $\langle\beta_{ab}| E\otimes I |\beta_{ab}\rangle$ symbolically. You should arrive at

$$\langle\beta_{ab}| E\otimes I |\beta_{ab}\rangle = \frac{1}{2}\big(\langle 0| E |0\rangle + \langle 1| E |1\rangle\big),$$

Thus, whichever measurement Eve performs, the outcome probabilities $p(m) = \langle\beta_{ab}| M_m^\dagger M_m |\beta_{ab}\rangle$ are independent of $a, b \rightsquigarrow$ Eve cannot infer anything about the classical information.

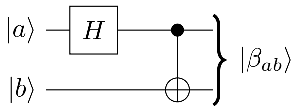
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 7.1 (Bell states and superdense coding)
Recall that the *Bell states* are defined as

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

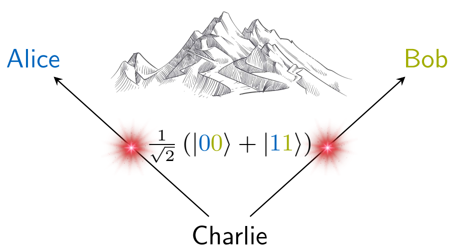
which can be summarized as $|\beta_{ab}\rangle = \frac{1}{\sqrt{2}}(|0,b\rangle + (-1)^a |1,1-b\rangle)$ for $a,b \in \{0,1\}$.

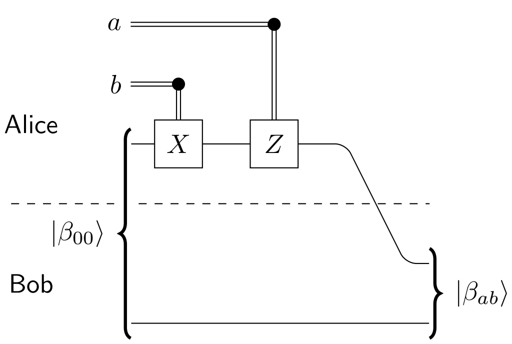
(a) Verify that the following quantum circuit creates the Bell states for inputs $|a,b\rangle$:



Note: this generalizes exercise 4.1(b). Since the circuit implements a unitary transformation of the standard basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, the Bell states form an orthonormal basis of the two qubit state space as well.

Superdense coding is a surprising use of entanglement to transmit two bits of classical information by sending just a single qubit! The setup agrees with quantum teleportation: two parties, usually referred to as Alice and Bob, live far from each other but share a pair of qubits in the entangled Bell state $|\beta_{00}\rangle$. They could have generated the pair during a visit in the past, or a common friend Charlie prepared it and sent one qubit to Alice and the other to Bob, as shown on the right.





Now Alice's task is to communicate two bits 'ab' of classical information to Bob. Alice can achieve that by applying X and/or Z gates to her qubit before sending it to Bob, depending on the information she wants to transmit: for '00', she does nothing to her qubit, for '01' she applies X, for '10' she applies Z, and for '11' she applies first X and then Z, i.e., $ZX = iY$. It turns out that the resulting states are precisely the Bell states, which Bob can distinguish by performing a measurement with respect to this basis. The diagram on the left summarizes the protocol.

(b) Verify for all combinations of $a,b \in \{0,1\}$ that the output of the circuit is indeed the Bell state $|\beta_{ab}\rangle$.

(c) Suppose E is an operator on Alice's qubit (e.g., $E = M_m^\dagger M_m$ in the general measurement framework, with M_m a measurement operator). Show that $\langle\beta_{ab}|E \otimes I\,|\beta_{ab}\rangle$ takes the same value for all four Bell states. Assuming an adversarial "Eve" intercepts Alice's qubit on the way to Bob, can Eve infer anything about the classical information which Alice tries to send?

Solution

(a) For all $a,b \in \{0,1\}$:

$$|a,b\rangle \overset{H\otimes I}{\mapsto} \frac{|0\rangle + (-1)^a |1\rangle}{\sqrt{2}}\,|b\rangle = \frac{1}{\sqrt{2}}\big(\,|0,b\rangle + (-1)^a |1,b\rangle\,\big) \overset{\text{CNOT}}{\mapsto} \frac{1}{\sqrt{2}}\big(\,|0,b\rangle + (-1)^a |1,1-b\rangle\,\big) = |\beta_{ab}\rangle\,.$$

(b) We enumerate all four cases explicitly:

$$
\begin{aligned}
ab = 00: &\quad |\beta_{00}\rangle \text{ remains unchanged} \\
ab = 01: &\quad (X \otimes I)\,|\beta_{00}\rangle = (X \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}((X\,|0\rangle)\,|0\rangle + (X\,|1\rangle)\,|1\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\beta_{01}\rangle \\
ab = 10: &\quad (Z \otimes I)\,|\beta_{00}\rangle = (Z \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}((Z\,|0\rangle)\,|0\rangle + (Z\,|1\rangle)\,|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\beta_{10}\rangle \\
ab = 11: &\quad (ZX \otimes I)\,|\beta_{00}\rangle = (ZX \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(-\,|10\rangle + |01\rangle) = |\beta_{11}\rangle
\end{aligned}
$$

Alternative solution: The operation of the classically-controlled gates can be summarized as $Z^a X^b$ for $a, b \in \{0, 1\}$. Note that X^b appears on the right since it is applied *first*. A matrix to the power of zero is the identity matrix, thus for example

$$
X^b = \begin{cases} I & \text{if } b = 0 \\ X & \text{if } b = 1 \end{cases}.
$$

A little thought confirms the following relations, for all $a, b \in \{0, 1\}$:

$$
\begin{aligned}
X^b\,|0\rangle &= |b\rangle\,, \quad X^b\,|1\rangle = |1-b\rangle\,, \\
Z^a\,|0\rangle &= |0\rangle\,, \quad Z^a\,|1\rangle = (-1)^a\,|1\rangle\,.
\end{aligned}
$$

With that, we can compute the output of the circuit:

$$
\begin{aligned}
(Z^a X^b \otimes I)\,|\beta_{00}\rangle &= (Z^a X^b \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= (Z^a \otimes I)\frac{1}{\sqrt{2}}\big((X^b\,|0\rangle)\,|0\rangle + (X^b\,|1\rangle)\,|1\rangle\big) \\
&= (Z^a \otimes I)\frac{1}{\sqrt{2}}\big(\,|b, 0\rangle + |1-b, 1\rangle\big) \\
&= (Z^a \otimes I)\frac{1}{\sqrt{2}}\big(\,|0, b\rangle + |1, 1-b\rangle\big) \\
&= \frac{1}{\sqrt{2}}\big((Z^a\,|0\rangle)\,|b\rangle + (Z^a\,|1\rangle)\,|1-b\rangle\big) \\
&= \frac{1}{\sqrt{2}}\big(\,|0, b\rangle + (-1)^a\,|1, 1-b\rangle\big) = |\beta_{ab}\rangle\,.
\end{aligned}
$$

The fourth equal sign follows from considering the two cases $b = 0$ and $b = 1$.

(c) $\langle\beta_{ab}|\, E \otimes I\,|\beta_{ab}\rangle$ turns out to be independent of a and b:

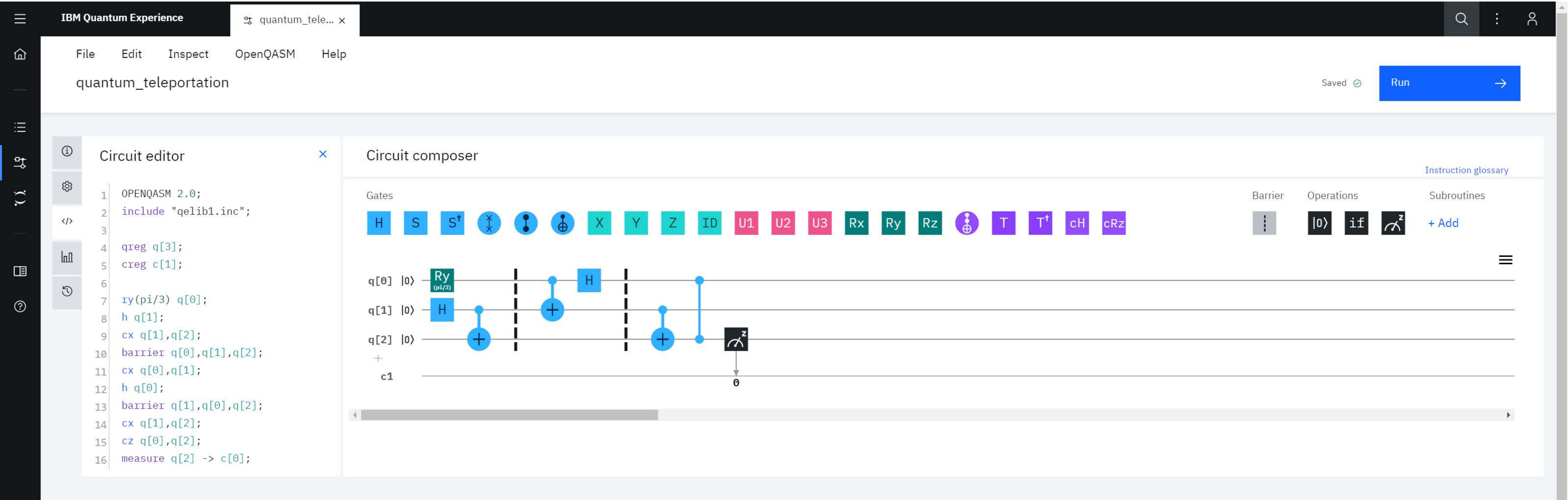
$$
\begin{aligned}
\langle\beta_{ab}|\, E \otimes I\,|\beta_{ab}\rangle &= \frac{1}{2}\Big(\,\langle 0, b| + (-1)^a\,\langle 1, 1-b|\,\Big)(E \otimes I)\Big(\,|0, b\rangle + (-1)^a\,|1, 1-b\rangle\,\Big) \\
&= \frac{1}{2}\Big(\,\langle 0, b|\, E \otimes I\,|0, b\rangle + (-1)^a\,\langle 0, b|\, E \otimes I\,|1, 1-b\rangle \\
&\qquad\qquad + (-1)^a\,\langle 1, 1-b|\, E \otimes I\,|0, b\rangle + \langle 1, 1-b|\, E \otimes I\,|1, 1-b\rangle\,\Big) \\
&= \frac{1}{2}\Big(\,\langle 0|\, E\,|0\rangle\,\underbrace{\langle b|b\rangle}_{=1} + (-1)^a\,\langle 0|\, E\,|1\rangle\,\underbrace{\langle b|1-b\rangle}_{=0} + (-1)^a\,\langle 1|\, E\,|0\rangle\,\underbrace{\langle 1-b|b\rangle}_{=0} + \langle 1|\, E\,|1\rangle\,\underbrace{\langle 1-b|1-b\rangle}_{=1}\Big) \\
&= \frac{1}{2}\big(\,\langle 0|\, E\,|0\rangle + \langle 1|\, E\,|1\rangle\,\big).
\end{aligned}
$$

Thus, whichever measurement (with operators $\{M_m\}$) Eve performs, the outcome probabilities $p(m) = \langle\beta_{ab}|\, M_m^\dagger M_m\,|\beta_{ab}\rangle$ are independent of $a, b \rightsquigarrow$ Eve cannot infer anything about the classical information.

$$R_y(\theta) = \mathrm{e}^{-i\theta Y/2} = \cos(\theta/2)I - i\sin(\theta/2)Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_y(\tfrac{\pi}{3}) = \begin{pmatrix} \cos\frac{\pi}{6} & -\sin\frac{\pi}{6} \\ \sin\frac{\pi}{6} & \cos\frac{\pi}{6} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

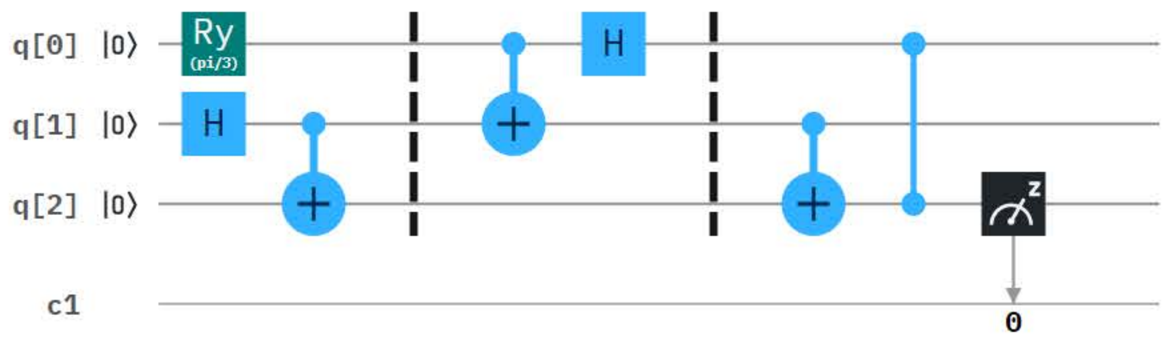
$$|\psi\rangle = R_y(\tfrac{\pi}{3})|0\rangle = \underbrace{\frac{\sqrt{3}}{2}}_{\alpha}|0\rangle + \underbrace{\frac{1}{2}}_{\beta}|1\rangle$$



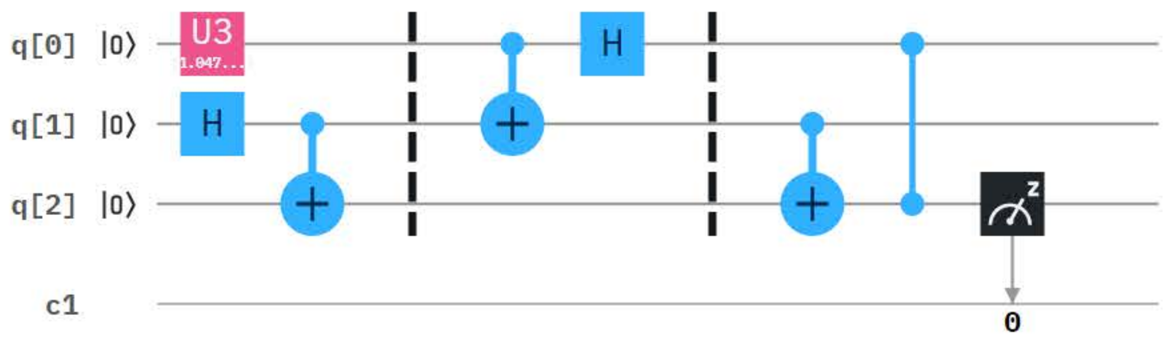
Circuit diagram

Diagram
OpenQasm

Original circuit

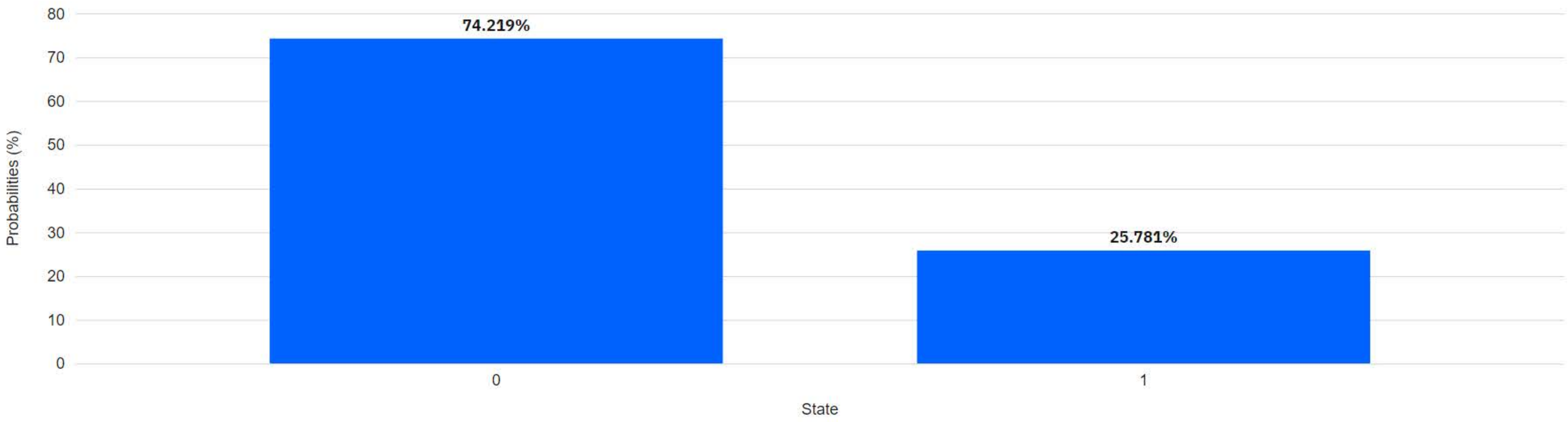


Transpiled circuit



Result

Histogram



$$R_y(\theta) = \mathrm{e}^{-i\theta Y/2} = \cos(\theta/2)I - i\sin(\theta/2)Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_y(\tfrac{\pi}{3}) = \begin{pmatrix} \cos\frac{\pi}{6} & -\sin\frac{\pi}{6} \\ \sin\frac{\pi}{6} & \cos\frac{\pi}{6} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

$$|\psi\rangle = R_y(\tfrac{\pi}{3})|0\rangle = \underbrace{\frac{\sqrt{3}}{2}}_{\alpha}|0\rangle + \underbrace{\frac{1}{2}}_{\beta}|1\rangle$$

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang, Lilly Palackal due: 20 December 2021, 08:00 on Moodle

Tutorial 8 (Experimental Bell inequality)

As mentioned in the lecture, the violation of Bell inequality has been experimentally verified. Many of these experiments make use of photons as the qubits.[1] Fig. 1 shows a schematic version of the most common setup used to test the Bell inequality with photons. The source generates a pair of entangled photons, one of which is sent to Alice, one of which is sent to Bob. The coincidence monitor counts the instances with simultaneous measurements on Alice's and Bob's side in order to discard detections of environment photons not created by the source.

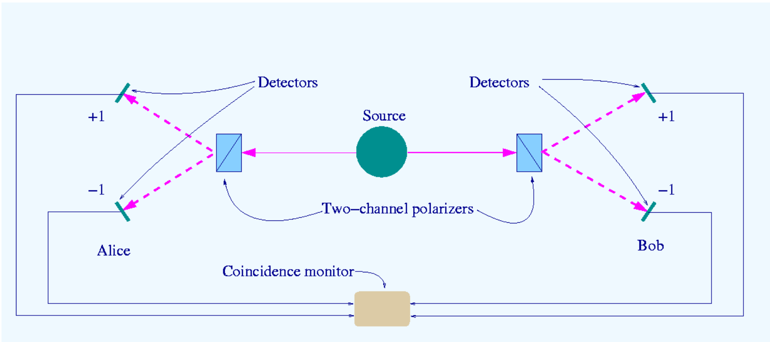


Figure 1: CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=641329

The actual setup, of course, contains many more elements, like in the experiment of M. Giustina et al.:

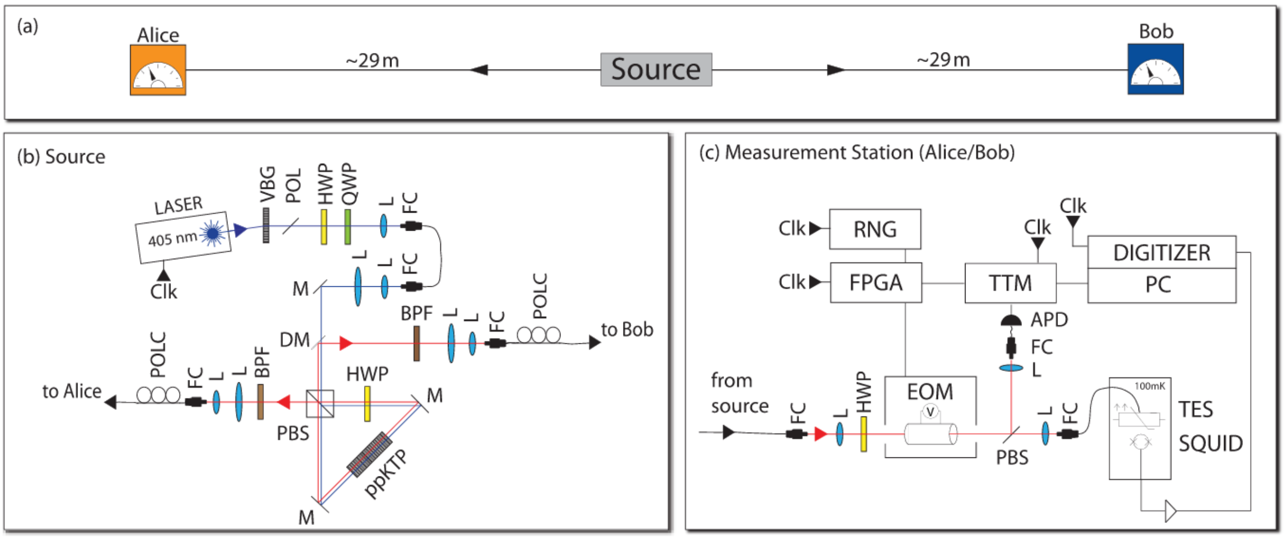


Figure 2: (a) Schematic setup. (b) Source of the entangled photons. (c) Detection station of one of the receivers.

(a) Discuss the role of the polarizers in these experiments. For simplicity, you can focus on the schematic representation from Fig. 1.

If we hypothesize that the experiment can be described by hidden variables, denoted λ, then the probability that Alice measures a and Bob measures b is given by:

$$P(a,b) = \sum_{x,y,\lambda} P(a|x,\lambda)P(b|y,\lambda)P(x,y)P(\lambda),$$

where x is the choice of the measurement basis used by Alice, and y is the one used by Bob. This expression is not able to reproduce all results from experiments according to Bell's inequality, so the consensus is that hidden variable theories are incorrect. However, there are *two* additional implicit assumptions leading to this expression:

[1] see, .e.g.,
M. Giustina et al.: *Significant-loophole-free test of Bell's theorem with entangled photons*. Phys. Rev. Lett. 115, 250401 (2015)
The BIG Bell Test Collaboration: *Challenging local realism with human choices*. Nature 557, 212-216 (2018)
D. Rauch et al.: *Cosmic Bell test using random measurement settings from high-redshift quasars*. Phys. Rev. Lett. 121, 080403 (2018)

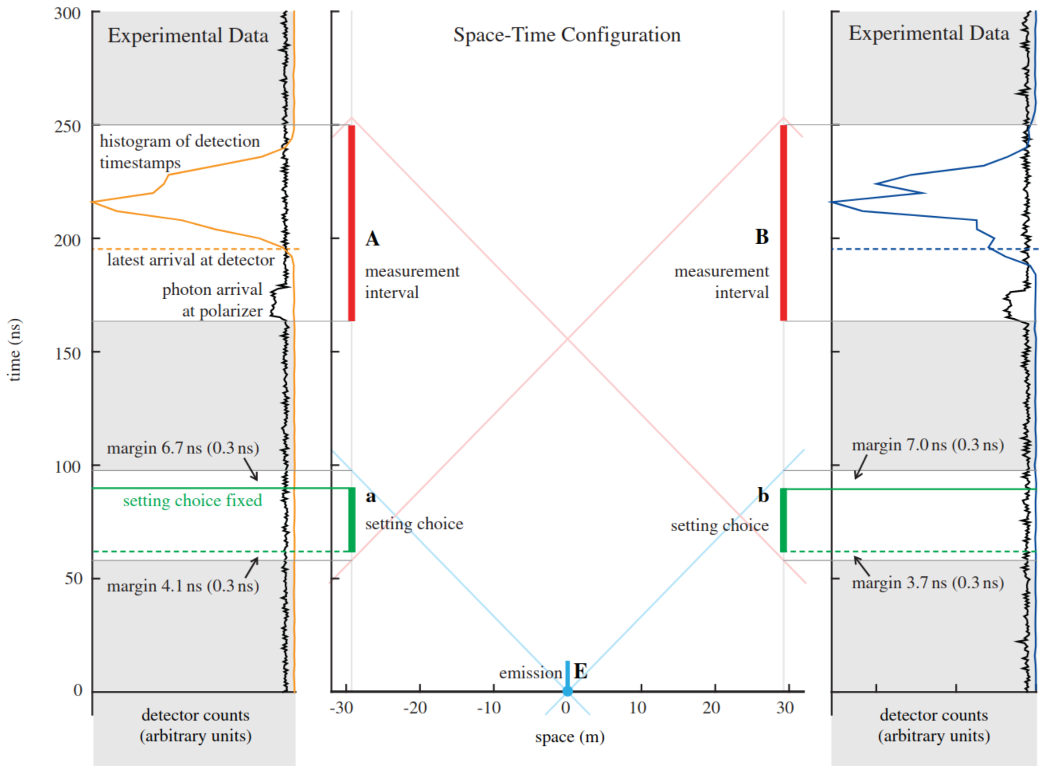


Figure 3: Space and time configuration of the experiment by M. Giustina et al. [Phys. Rev. Lett. 115, 250401 (2015)]

(b) One of these assumptions is locality. In a lab experiment the photon detection is not instantaneous. Why could this create a loophole, and what can be done to close this loophole? As an example, Fig. 3 shows the space-time configuration and specific times each experimental step takes.

(c) Identify the remaining assumption and discuss how one can make sure that it holds during the experiment.

Exercise 8.1 (Bell inequality violation by quantum mechanics)

(a) Let $\{|a\rangle, |b\rangle\}$ be an orthonormal basis of $\mathbb{C}^2$, and $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ chosen such that

$$|0\rangle = \alpha |a\rangle + \beta |b\rangle,$$
$$|1\rangle = \gamma |a\rangle + \delta |b\rangle.$$

Verify the relation

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = (\alpha\delta - \beta\gamma)\frac{|ab\rangle - |ba\rangle}{\sqrt{2}}.$$

(b) In the quantum experiment violating the Bell inequality, Charlie prepares the “spin singlet” quantum state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

and sends the first qubit to Alice and the second to Bob. Alice then measures the observable Q or R on her qubit and Bob the observable S or T on his qubit, defined as

$$Q = Z, \qquad S = \frac{-Z - X}{\sqrt{2}},$$
$$R = X, \qquad T = \frac{Z - X}{\sqrt{2}}.$$

Verify the following average values (which violate the Bell inequality):

$$\langle\psi| Q \otimes S |\psi\rangle = \frac{1}{\sqrt{2}}, \quad \langle\psi| R \otimes S |\psi\rangle = \frac{1}{\sqrt{2}}, \quad \langle\psi| R \otimes T |\psi\rangle = \frac{1}{\sqrt{2}}, \quad \langle\psi| Q \otimes T |\psi\rangle = -\frac{1}{\sqrt{2}}.$$

Exercise 8.2 (CHSH game)
The CHSH game demonstrates the power of quantum correlations and gives rise to a Bell inequality through a simple game in a real-world setting.

Alice and Bob play a game whose inputs and objective are described in the following. Alice and Bob each receive a completely random bit denoted by x resp. y (independently distributed, with equal probability for 0 or 1). After receiving their input they are not allowed to communicate until the end of the game. Alice and Bob each have to produce an output $a \in \{0,1\}$ resp. $b \in \{0,1\}$. They win the game whenever their inputs and outputs fulfill the condition

$$x \cdot y = a + b \mod 2.$$

As a resource Alice and Bob receive an EPR pair

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

shared between them.

(a) Draw a sketch of the setting described above.

(b) Before starting the game, Alice and Bob are allowed to agree on a strategy determining which outputs to generate for a given input. Note that Alice only has access to her input x and Bob only to his input y and they are not allowed to communicate once they received their input. In case Alice and Bob do not make use of their shared entanglement, the maximum winning probability they can achieve with a deterministic classical strategy is 75%. Give a deterministic classical strategy which Alice and Bob should follow in order to achieve the best possible classical winning probability.

We now give a strategy for Alice and Bob making use of their quantum resources. Define the unitary operator

$$U_\theta := \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \quad \text{for } \theta \in \mathbb{R}$$

and parameters

$$\theta_0 = 0, \quad \theta_1 = \frac{\pi}{4},$$
$$\tau_0 = \frac{\pi}{8}, \quad \tau_1 = -\frac{\pi}{8}.$$

Based on their inputs x, y Alice and Bob will apply operators U_{θ_x} and U_{τ_y} on their local system of the shared EPR pair. Afterwards, they measure their local register in the computational basis with outcomes a, b. The probability of receiving outcomes a, b dependent on inputs x, y is given by

$$P(a, b \mid x, y) = \langle (U_{\theta_x} \otimes U_{\tau_y})\beta_{00} \mid P_a \otimes P_b \mid (U_{\theta_x} \otimes U_{\tau_y})\beta_{00} \rangle,$$

where $P_a = |a\rangle\langle a|$ and $P_b = |b\rangle\langle b|$ are projections onto the computational basis states for $a, b \in \{0,1\}$. Alice and Bob use the outcome of their measurement a, b as output for the game.

(c) Show that Alice and Bob can win with probability roughly 85% when following the above quantum strategy.
Hint: The relation $(V \otimes W)|\beta_{00}\rangle = (V \cdot W^T \otimes \mathbb{1})|\beta_{00}\rangle$ for any $V, W \in \mathbb{C}^{2\times 2}$ might be helpful.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang, Lilly Palackal

Tutorial 8 (Experimental Bell inequality)
As mentioned in the lecture, the violation of Bell inequality has been experimentally verified. Many of these experiments make use of photons as the qubits.[1] Fig. 1 shows a schematic version of the most common setup used to test the Bell inequality with photons. The source generates a pair of entangled photons, one of which is sent to Alice, one of which is sent to Bob. The coincidence monitor counts the instances with simultaneous measurements on Alice's and Bob's side in order to discard detections of environment photons not created by the source.

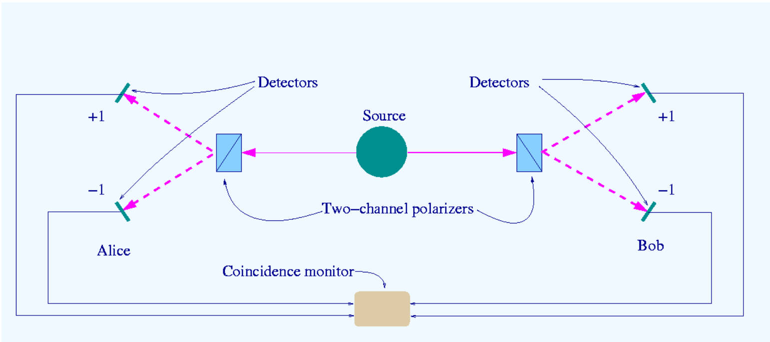


Figure 1: CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=641329

The actual setup, of course, contains many more elements, like in the experiment of M. Giustina et al.:

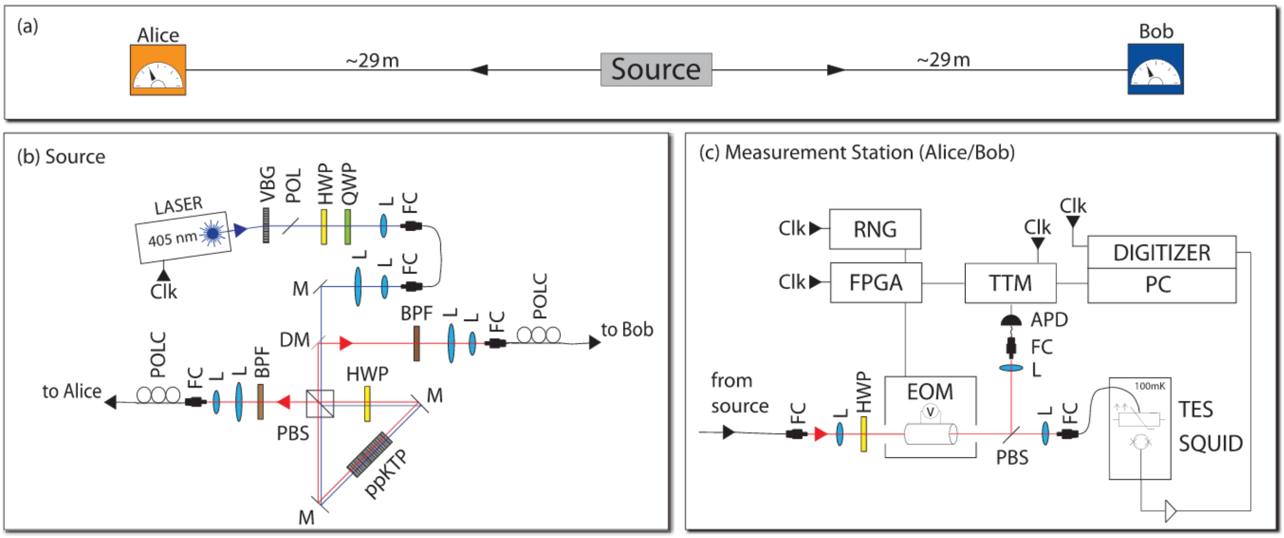


Figure 2: (a) Schematic setup. (b) Source of the entangled photons. (c) Detection station of one of the receivers.

(a) Discuss the role of the polarizers in these experiments. For simplicity, you can focus on the schematic representation from Fig. 1.

If we hypothesize that the experiment can be described by hidden variables, denoted λ, then the probability that Alice measures a and Bob measures b is given by:

$$P(a,b) = \sum_{x,y,\lambda} P(a|x,\lambda)P(b|y,\lambda)P(x,y)P(\lambda),$$

where x is the choice of the measurement basis used by Alice, and y is the one used by Bob. This expression is not able to reproduce all results from experiments according to Bell's inequality, so the consensus is that hidden variable theories are incorrect. However, there are *two* additional implicit assumptions leading to this expression:

[1] see, .e.g.,
M. Giustina et al.: *Significant-loophole-free test of Bell's theorem with entangled photons*. Phys. Rev. Lett. 115, 250401 (2015)
The BIG Bell Test Collaboration: *Challenging local realism with human choices*. Nature 557, 212-216 (2018)
D. Rauch et al.: *Cosmic Bell test using random measurement settings from high-redshift quasars*. Phys. Rev. Lett. 121, 080403 (2018)

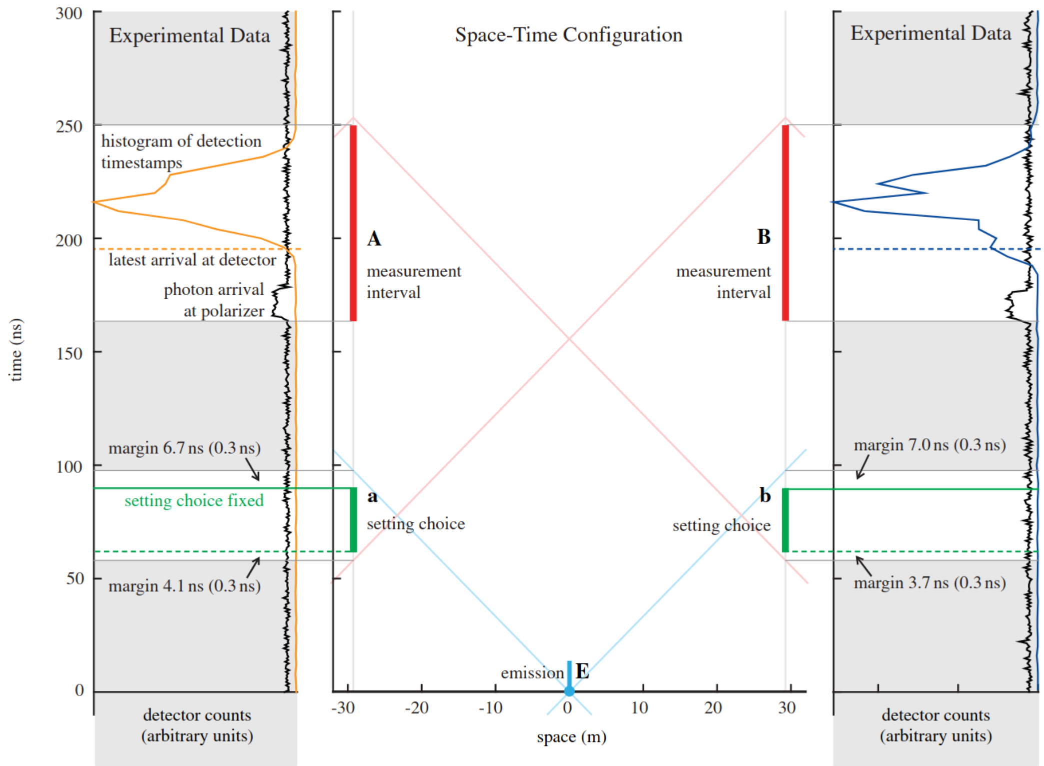


Figure 3: Space and time configuration of the experiment by M. Giustina et al. [Phys. Rev. Lett. 115, 250401 (2015)]

(b) One of these assumptions is locality. In a lab experiment the photon detection is not instantaneous. Why could this create a loophole, and what can be done to close this loophole? As an example, Fig. 3 shows the space-time configuration and specific times each experimental step takes.

(c) Identify the remaining assumption and discuss how one can make sure that it holds during the experiment.

Solution

(a) The role of the polarizers is to set the measurement basis. The two-channel polarizers only allow photons with a specific polarization to travel through them, and the orthogonal polarization is reflected. Consider a photon in state

$$|\psi\rangle = \alpha\,|\uparrow\rangle + \beta\,|\rightarrow\rangle\,,$$

where the arrows represent the polarization direction. If $|\psi\rangle$ encounters a vertical polarizer, the photon will be transmitted with probability $|\alpha|^2$ and reflected with probability $|\beta|^2$. A similar thing will happen, if

$$|\psi\rangle = \alpha\,|\nearrow\rangle + \beta\,|\searrow\rangle$$

encounters a diagonal polarizer. Furthermore, if $|\psi\rangle = |\uparrow\rangle$ encounters a diagonal polarizer, it will be transmitted or reflected with equal probability. At this point you can probably notice the equivalence with the qubit basis we usually use in the course. For example, we could represent the vertical and horizontal polarization as the $\{|0\rangle\,,|1\rangle\}$ basis, in which case the diagonal polarization would correspond to the $\{|+\rangle\,,|-\rangle\}$ basis.

(b) The locality assumption corresponds to the fact that the probability of measuring a is independent from b and y, and the probability of b is independent from a and x. However, if Alice's and Bob's measurements are not instantaneous, they could hypothetically influence each other. To ensure that this is not the case, Alice's and Bob's detectors are separated in the experiment by a distance large enough such that the time needed by light to travel from Alice to Bob is longer than the time to complete the detection.

In Fig. 3 we can see that ~ 200ns elapse between the choice of the measurement basis until the measurement is completed. 200 light nanoseconds correspond to ~ 59m, which is approximately the physical distance between Alice and Bob in the experiment.

(c) The other assumption is that the choice for measurement basis is independent of λ, i.e. the choice of measurements is not dependent on the hidden variables. The most common way to ensure that this assumption holds is to use random number generators to select the basis. However, random number generators are also affected by the underlying physics of the system that generates them, which is why strictly speaking one cannot rule out their dependence on λ. In the publication *Challenging local realism with human choices* [Nature 557, 212-216 (2018)], human choices (with no connection to the experiment) were used instead to select the measurement basis.

Superdeterminism is a (rather exotic) theory stating that all events in the universe are affected by the hidden variables λ. In this setting, even the choices from the participants in the above experiment would be influenced by λ. The study *Cosmic Bell test using random measurement settings from high-redshift quasars* [Phys. Rev. Lett. 121, 080403 (2018)] used the light from two quasars ~ 7.8 billion light years away to determine the basis for their measurements. They still found a Bell inequality violation. Therefore, if superdeterminism was correct, λ would have had to be fixed more that 7.8 billion years ago.

Exercise 8.1 solution

(a)

We insert the representation of $|0\rangle$ and $|1\rangle$ in terms of the new basis:

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} (\alpha\,|a\rangle + \beta\,|b\rangle) \otimes (\gamma\,|a\rangle + \delta\,|b\rangle) - \frac{1}{\sqrt{2}} (\gamma\,|a\rangle + \delta\,|b\rangle) \otimes (\alpha\,|a\rangle + \beta\,|b\rangle) =$$

$$\frac{1}{\sqrt{2}} (\alpha\,\gamma\,|aa\rangle + \alpha\,\delta\,|ab\rangle + \beta\,\gamma\,|ba\rangle + \beta\,\delta\,|bb\rangle) -$$

$$\frac{1}{\sqrt{2}} (\alpha\,\gamma\,|aa\rangle + \beta\,\gamma\,|ab\rangle + \alpha\,\delta\,|ba\rangle + \beta\,\delta\,|bb\rangle) =$$

$$\frac{1}{\sqrt{2}} (\alpha\,\delta\,|ab\rangle - \beta\,\gamma\,|ab\rangle + \beta\,\gamma\,|ba\rangle - \alpha\,\delta\,|ba\rangle) = (\alpha\,\delta - \beta\,\gamma)\,\frac{|ab\rangle - |ba\rangle}{\sqrt{2}}$$

(b)

```
Q = PauliMatrix[3];
% // MatrixForm
```

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

```
R = PauliMatrix[1];
% // MatrixForm
```

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

```
S = (-PauliMatrix[3] - PauliMatrix[1])/Sqrt[2];
% // MatrixForm
```

$$S = \frac{-\text{PauliMatrix}[3] - \text{PauliMatrix}[1]}{\sqrt{2}};$$

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

```
(* S is equal to the negative Hadamard matrix *)
Norm[S + HadamardMatrix[2]]
```

```
0
```

$$T = \frac{\text{PauliMatrix}[3] - \text{PauliMatrix}[1]}{\sqrt{2}};$$

```
% // MatrixForm
```

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

```
(* vector representation of spin singlet quantum state *)
ψ = 1/√2 {0, 1, -1, 0};
% // MatrixForm
```

$$\begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$

Now computing average values (for the homework you should compute this with “pen and paper”):

```
KroneckerProduct[Q, S] // MatrixForm
Conjugate[ψ].KroneckerProduct[Q, S].ψ
```

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

$$\frac{1}{\sqrt{2}}$$

```
KroneckerProduct[R, S] // MatrixForm
Conjugate[ψ].KroneckerProduct[R, S].ψ
```

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

$$\frac{1}{\sqrt{2}}$$

```
KroneckerProduct[R, T] // MatrixForm
Conjugate[ψ].KroneckerProduct[R, T].ψ
```

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

$$\frac{1}{\sqrt{2}}$$

```
KroneckerProduct[Q, T] // MatrixForm
Conjugate[ψ].KroneckerProduct[Q, T].ψ
```

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

$$-\frac{1}{\sqrt{2}}$$

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang, Lilly Palackal

Exercise 8.2 (CHSH game)
The CHSH game demonstrates the power of quantum correlations and gives rise to a Bell inequality through a simple game in a real-world setting.

Alice and Bob play a game whose inputs and objective are described in the following. Alice and Bob each receive a completely random bit denoted by x resp. y (independently distributed, with equal probability for 0 or 1). After receiving their input they are not allowed to communicate until the end of the game. Alice and Bob each have to produce an output $a \in \{0,1\}$ resp. $b \in \{0,1\}$. They win the game whenever their inputs and outputs fulfill the condition

$$x \cdot y = a + b \mod 2.$$

As a resource Alice and Bob receive an EPR pair

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

shared between them.

(a) Draw a sketch of the setting described above.

(b) Before starting the game, Alice and Bob are allowed to agree on a strategy determining which outputs to generate for a given input. Note that Alice only has access to her input x and Bob only to his input y and they are not allowed to communicate once they received their input. In case Alice and Bob do not make use of their shared entanglement, the maximum winning probability they can achieve with a deterministic classical strategy is 75%. Give a deterministic classical strategy which Alice and Bob should follow in order to achieve the best possible classical winning probability.

We now give a strategy for Alice and Bob making use of their quantum resources. Define the unitary operator

$$U_\theta := \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \quad \text{for } \theta \in \mathbb{R}$$

and parameters

$$\theta_0 = 0, \quad \theta_1 = \frac{\pi}{4},$$
$$\tau_0 = \frac{\pi}{8}, \quad \tau_1 = -\frac{\pi}{8}.$$

Based on their inputs x, y Alice and Bob will apply operators U_{θ_x} and U_{τ_y} on their local system of the shared EPR pair. Afterwards, they measure their local register in the computational basis with outcomes a, b. The probability of receiving outcomes a, b dependent on inputs x, y is given by

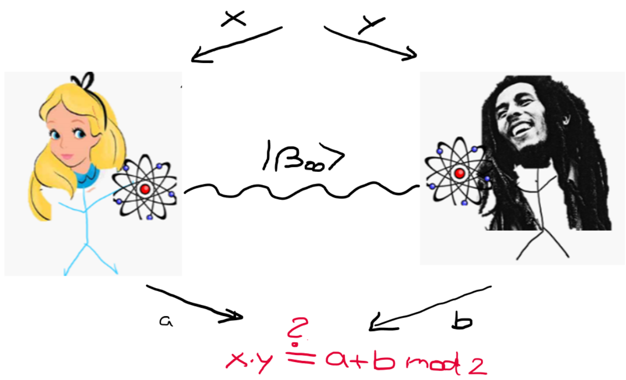
$$P(a, b \mid x, y) = \langle (U_{\theta_x} \otimes U_{\tau_y})\beta_{00} \mid P_a \otimes P_b \mid (U_{\theta_x} \otimes U_{\tau_y})\beta_{00} \rangle,$$

where $P_a = |a\rangle\langle a|$ and $P_b = |b\rangle\langle b|$ are projections onto the computational basis states for $a, b \in \{0,1\}$. Alice and Bob use the outcome of their measurement a, b as output for the game.

(c) Show that Alice and Bob can win with probability roughly 85% when following the above quantum strategy.
Hint: The relation $(V \otimes W)|\beta_{00}\rangle = (V \cdot W^T \otimes \mathbb{1})|\beta_{00}\rangle$ for any $V, W \in \mathbb{C}^{2\times 2}$ might be helpful.

Solution

(a)



(b) A deterministic classical strategy Alice and Bob can agree on in order to reach a winning probability of 75% is that both always output 0. For any pair of input bits except for $(x, y) = (1, 1)$ Alice and Bob will win, as inserting the different combinations of x and y with $a = b = 0$ into $x \cdot y = a + b \mod 2$ shows.

More formally, we can calculate the winning probability for this strategy by defining the set $A = \{(x, y, a, b) \in \{0,1\}^4 \mid x \cdot y = a + b \mod 2\}$ such that

$$\begin{aligned} P(\text{win}) &= \sum_{(x,y,a,b)\in A} P(x,y)P(a,b \mid x,y) \\ &= \frac{1}{4}\left(P(0,0 \mid 0,1) + P(0,0 \mid 1,0) + P(0,0 \mid 0,0)\right) \\ &= \frac{3}{4}, \end{aligned}$$

since for the chosen strategy $P(a, b \mid x, y) = 1$ for $a = b = 0$ and $P(a, b \mid x, y) = 0$ otherwise.

(c) Let again $A = \{(x, y, a, b) \in \{0,1\}^4 \mid x \cdot y = a + b \mod 2\}$. Then the winning probability for the quantum strategy is

$$\begin{aligned} P(\text{win}) &= \sum_{(x,y,a,b)\in A} P(x,y)P(a,b \mid x,y) \\ &= \frac{1}{4}\sum_{(x,y,a,b)\in A} P(a,b \mid x,y) \\ &= \frac{1}{4}\left(P(\{(0,1),(1,0)\} \mid 1,1) + \sum_{(x,y)\neq(1,1)} P(\{(0,0),(1,1)\} \mid x,y)\right) \\ &= \frac{1}{4}\left(P(0,1 \mid 1,1) + P(1,0 \mid 1,1) + \sum_{(x,y)\neq(1,1)} \left(P(0,0 \mid x,y) + P(1,1 \mid x,y)\right)\right) \\ &= \frac{1+\frac{1}{\sqrt{2}}}{2} \approx 85\%. \end{aligned}$$

The last equation is derived by computing the value of $P(a, b \mid x, y)$ for all $(x, y, a, b) \in A$ with the formula

$$P(a,b \mid x,y) = \langle (U_{\theta_x} \otimes U_{\tau_y})\beta_{00} \mid P_a \otimes P_b \mid (U_{\theta_x} \otimes U_{\tau_y})\beta_{00}\rangle. \tag{1}$$

Now this can be done by inserting the matrix representation of U_{θ_x}, U_{τ_y}, P_a, P_b and $|\beta_{00}\rangle$ and explicitly calculating the matrix-vector multiplications. Alternatively, we can first simplify equation (1):

$$\begin{aligned} P(a,b \mid x,y) &= \langle (U_{\theta_x} \otimes U_{\tau_y})\beta_{00} \mid P_a \otimes P_b \mid (U_{\theta_x} \otimes U_{\tau_y})\beta_{00}\rangle \\ &= \langle (U_{\theta_x} \cdot U_{-\tau_y} \otimes \mathbb{1})\beta_{00} \mid P_a \otimes P_b \mid (U_{\theta_x} \cdot U_{-\tau_y} \otimes \mathbb{1})\beta_{00}\rangle \\ &= \langle (U_{\theta_x} \cdot U_{-\tau_y} \otimes \mathbb{1})\beta_{00} \mid (P_a \otimes \mathbb{1})(\mathbb{1} \otimes P_b)(U_{\theta_x} \cdot U_{-\tau_y} \otimes \mathbb{1}) \mid \beta_{00}\rangle \\ &= \langle (U_{\theta_x} \cdot U_{-\tau_y} \otimes \mathbb{1})\beta_{00} \mid (P_a \otimes \mathbb{1})(U_{\theta_x} \cdot U_{-\tau_y} \otimes \mathbb{1})(\mathbb{1} \otimes P_b) \mid \beta_{00}\rangle \\ &= \langle (U_{\theta_x} \cdot U_{-\tau_y} \otimes \mathbb{1})\beta_{00} \mid (P_a \cdot U_{\theta_x} \cdot U_{-\tau_y} \otimes \mathbb{1})\frac{1}{\sqrt{2}}\,|bb\rangle \\ &= \frac{1}{2}\left(\langle 0|\,(U_{\theta_x} \cdot U_{-\tau_y})^\dagger \otimes \langle 0| + \langle 1|\,(U_{\theta_x} \cdot U_{-\tau_y})^\dagger \otimes \langle 1|\right)\left(P_a \cdot U_{\theta_x} \cdot U_{-\tau_y}\,|b\rangle \otimes |b\rangle\right) \\ &= \frac{1}{2}\langle (U_{\theta_x} \cdot U_{-\tau_y})b | (P_a \cdot U_{\theta_x} \cdot U_{-\tau_y})b\rangle \\ &= \frac{1}{2}\,\langle b|\,(U_{\theta_x} \cdot U_{-\tau_y})^\dagger (P_a \cdot U_{\theta_x} \cdot U_{-\tau_y})b\rangle \\ &= \frac{1}{2}\,\langle b|\,(U_{\theta_x} \cdot U_{-\tau_y})^\dagger\,|a\rangle\,\langle a|\,(U_{\theta_x} \cdot U_{-\tau_y})b\rangle \\ &= \frac{1}{2}\left|(U_{\theta_x} \cdot U_{-\tau_y})_{a,b}\right|^2. \end{aligned}$$

Here we have used the hint, and that $U_\theta^T = U_\theta^{-1} = U_{-\theta}$ since U_θ is an orthogonal rotation matrix.

Now computing (1) for a given (x, y, a, b) reduces to computing $\frac{1}{2}|(U_{\theta_x} \cdot U_{-\tau_y})_{a,b}|^2$. For example, we have

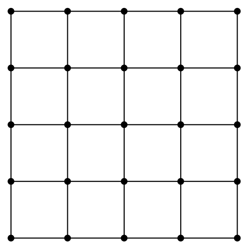
$$\begin{aligned}
P(0,0 \mid 0,1) &= \frac{1}{2}|(U_{\theta_0} \cdot U_{-\tau_1})_{0,0}|^2 \\
&= \frac{1}{2}\left|\left(\begin{pmatrix} \cos(0) & \sin(0) \\ -\sin(0) & \cos(0) \end{pmatrix} \cdot \begin{pmatrix} \cos\left(\frac{\pi}{8}\right) & \sin\left(\frac{\pi}{8}\right) \\ -\sin\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right) \end{pmatrix}\right)_{0,0}\right|^2 \\
&= \frac{1}{2}\cos\left(\frac{\pi}{8}\right)^2.
\end{aligned}$$

Tutorial 9 (Proving quantum advantage based on a Hidden Linear Function problem)
In a recent paper[1], the authors construct a variant of the standard Bernstein-Varizani Hidden Linear Function (HLF) problem, which can be solved by a constant depth quantum circuit. The authors then prove that an analogous classical circuit with constant depth cannot solve this problem in general. This provides a working example for a provable quantum advantage over classical methods.

The problem definition uses the concept of an *adjacency matrix* of a graph $G = (V, E)$ with vertices $V = \{v_1, \dots, v_n\}$ and edges E. The adjacency matrix $A \in \mathbb{R}^{n \times n}$ of G is defined by its entries

$$A_{i,j} = \begin{cases} 1, & \text{if } (v_i, v_j) \text{ is an edge in } E \\ 0, & \text{otherwise} \end{cases}$$

for $i, j \in \{1, \dots, n\}$. Note that A is a binary, symmetric matrix.
In the publication, the authors choose G as square grid with $N \times N$ vertices. The edges connect the nearest neighbors on the grid. The motivation for this setup are quantum computers with the same layout, i.e., each vertex a qubit. We will see that the quantum solution will only require two-qubit gates between neighbors of the graph, which could thus be directly realized by the quantum computer.



The problem statement is based on the function

$$q(x) = \sum_{i,j=1}^{n} A_{i,j} x_i x_j \mod 4, \quad x \in \{0,1\}^n,$$

and we will restrict x to the kernel of $A \bmod 2$: $\mathrm{Ker}(A) = \{x \in \{0,1\}^n : Ax = 0 \bmod 2\}$.

(a) Show that $q(x)$ is linear when its support is restricted to $\mathrm{Ker}(A)$.
Hint: Prove that $q(x \oplus y) = q(x) + q(y) \bmod 4$ for $x, y \in \mathrm{Ker}(A)$.

By the derivation of part (a), one concludes that $q(x)$ can be written as

$$q(x) = 2 \sum_{i=1}^{n} y_i x_i \mod 4, \quad x \in \mathrm{Ker}(A)$$

for some (non unique) binary string y, i.e., $q(x)$ effectively "hides" a binary string. The HLF problem asks to find such a y.

(b) We introduce a gate U_q that performs the following action (with i the imaginary unit):

$$U_q \left| s \right\rangle = i^{q(s)} \left| s \right\rangle, \; s \in \{0,1\}^n.$$

Derive the relation

$$H^{\otimes n} U_q H^{\otimes n} \left| 0^{\otimes n} \right\rangle = \frac{1}{2^n} \sum_{x,z \in \{0,1\}^n} i^{q(x)} (-1)^{z^T x} \left| z \right\rangle.$$

One can prove (see appendix) that the coefficient of each computational basis state $|z\rangle$ in this sum is non-zero precisely if z is a solution of the HLF problem. Thus a single standard measurement will yield a solution.

(c) We now discuss how a constant depth quantum circuit can realize U_q. Show that

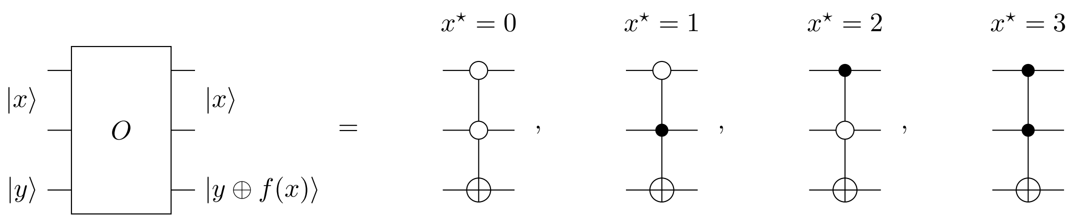
$$U_q = \prod_{(v_i, v_j) \in E} CZ_{i,j},$$

with $CZ_{i,j}$ the controlled-Z gate between qubits i and j, defined as $CZ_{i,j} \left| x \right\rangle = (-1)^{x_i x_j} \left| x \right\rangle$ for $x \in \{0,1\}^n$.

[1] S. Bravyi, D. Gosset, R. König: *Quantum advantage with shallow circuits.* Science 362, 308–311 (2018)

Exercise 9.1 (Two-bit quantum search)
We consider the quantum search (Grover's) algorithm for the special case $n = 2$, i.e., a search space with $N = 4$ elements, and $M = 1$ (exactly one solution). The solution is denoted $x^\star$, and correspondingly $f(x^\star) = 1$, $f(x) = 0$ for all $x \neq x^\star$.

The oracle, which is able to recognize the solution, can be realized as follows (depending on $x^\star$):

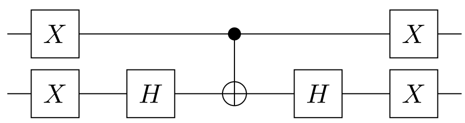


Note that the rightmost gate for $x^\star = 3$ is the Toffoli gate (cf. Exercise 5.2): the first and second qubits act as controls, and the third qubit as target, which is flipped precisely if both controls are set to 1. The empty circles in the gates for $x^\star = 0, 1, 2$ mean that the control is activated by 0 (instead of 1).

As derived in the lecture, the Grover operator G performs a rotation by angle θ in the plane spanned by the orthonormal states $|\alpha\rangle$ and $|\beta\rangle$; thus k applications to the initial equal superposition state $|\psi\rangle = \cos(\frac{\theta}{2})\,|\alpha\rangle + \sin(\frac{\theta}{2})\,|\beta\rangle$ results in

$$G^k\,|\psi\rangle = \cos\left((\tfrac{1}{2} + k)\theta\right)|\alpha\rangle + \sin\left((\tfrac{1}{2} + k)\theta\right)|\beta\rangle\,.$$

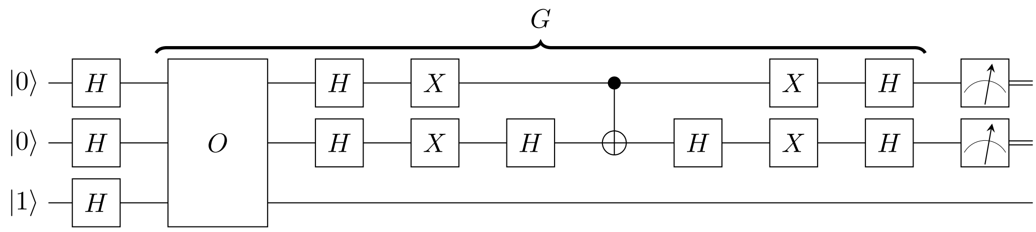
(a) Show that the following circuit implements the negated phase gate appearing in the Grover operator, that is, $-(2\,|00\rangle\langle 00| - I)$:



The global factor (-1) does not influence the final quantum measurement results and will be ignored from now on.

(b) Compute the angle θ defined via $\sin(\frac{\theta}{2}) = \sqrt{M/N}$. Why is a single application of G sufficient to reach the desired solution state $|\beta\rangle$ exactly, that is, $G\,|\psi\rangle = |\beta\rangle$?

In summary, the quantum search circuit with one use of G and the above realization of the phase gate is:



(c) Assemble this circuit in the IBM Q Circuit Composer for one of the four possible oracles of your choice, and verify that the final measurement indeed yields the solution $x^\star$.

Hint: You can use the Pauli-X gate to initialize the oracle qubit to $|1\rangle$. The Toffoli gate is available in the Circuit Composer.

Exercise 9.2 (Quantum search as quantum simulation, part 1)
Interestingly, the quantum search algorithm can be derived from a Schrödinger time evolution governed by a certain Hamiltonian H (cf. Tutorial 3). For simplicity, we assume that there is a single solution $x \in \{0, \dots, N-1\}$ to the search problem with N elements, and we start from an arbitrary initial state $|\psi\rangle$. It turns out that the Hamiltonian

$$H = |x\rangle\langle x| + |\psi\rangle\langle\psi|$$

achieves a transition from $|\psi\rangle$ to $|x\rangle$, that is, $\mathrm{e}^{-iHt^*}\,|\psi\rangle = |x\rangle$ for a certain time t^* (up to a phase factor, which is not relevant here). In part 1 we analyze the time evolution theoretically, and part 2 (next exercise sheet) discusses the simulation of the Hamiltonian.

To understand the transition from $|\psi\rangle$ to $|x\rangle$, first note that the time dynamics under H never leaves the two-dimensional space spanned by $|x\rangle$ and $|\psi\rangle$. Let the vector $|y\rangle$ be chosen such that $\{|x\rangle, |y\rangle\}$ forms an orthonormal basis of this subspace, and represent $|\psi\rangle = \alpha\,|x\rangle + \beta\,|y\rangle$ for some coefficients $\alpha, \beta \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 = 1$. For simplicity, we can assume that the phases of $|x\rangle$, $|y\rangle$ and $|\psi\rangle$ are such that α and β are real.

(a) Show that the matrix representation of H within this subspace is given by

$$H = I + \alpha(\beta X + \alpha Z).$$

Hint: The matrix entries of H restricted to a subspace with orthonormal basis $\{|u_j\rangle\}_{j=1,\dots,n}$ are $(\langle u_j|\, H \,|u_k\rangle)_{j,k}$.

(b) From the representation in (a), we thus obtain $\mathrm{e}^{-iHt} = \mathrm{e}^{-it}\,\mathrm{e}^{-i\alpha t(\beta X + \alpha Z)}$, where the phase factor e^{-it} stems from the identity matrix in the representation. Use the definition of the single-qubit rotation operators (see lecture) to verify that

$$\mathrm{e}^{-iHt} = \mathrm{e}^{-it}\left(\cos(\alpha t) I - i\sin(\alpha t)(\beta X + \alpha Z)\right).$$

(c) Show that $(\beta X + \alpha Z)\,|\psi\rangle = |x\rangle$. Together with (b), we thus arrive at

$$\mathrm{e}^{-iHt}\,|\psi\rangle = \mathrm{e}^{-it}\left(\cos(\alpha t)\,|\psi\rangle - i\sin(\alpha t)\,|x\rangle\right).$$

(d) Specify a time t^* such that $\mathrm{e}^{-iHt^*}\,|\psi\rangle = |x\rangle$ up to a phase factor.

(e) Since the required time t^* depends on $\alpha = \langle x|\psi\rangle$ and thus seemingly on the (a priori unknown) solution x, a natural question is how to determine t^*. To resolve this question, one can choose $|\psi\rangle$ to be the equal superposition state. Compute α in this case, assuming that $|\psi\rangle$ is normalized.

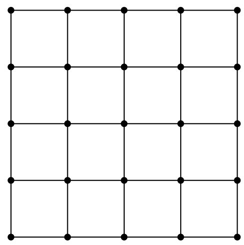
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 9 (Proving quantum advantage based on a Hidden Linear Function problem)
In a recent paper[1], the authors construct a variant of the standard Bernstein-Varizani Hidden Linear Function (HLF) problem, which can be solved by a constant depth quantum circuit. The authors then prove that an analogous classical circuit with constant depth cannot solve this problem in general. This provides a working example for a provable quantum advantage over classical methods.

The problem definition uses the concept of an *adjacency matrix* of a graph $G = (V, E)$ with vertices $V = \{v_1, \dots, v_n\}$ and edges E. The adjacency matrix $A \in \mathbb{R}^{n\times n}$ of G is defined by its entries

$$A_{i,j} = \begin{cases} 1, & \text{if } (v_i, v_j) \text{ is an edge in } E \\ 0, & \text{otherwise} \end{cases}$$

for $i, j \in \{1, \dots, n\}$. Note that A is a binary, symmetric matrix.
In the publication, the authors choose G as square grid with $N \times N$ vertices. The edges connect the nearest neighbors on the grid. The motivation for this setup are quantum computers with the same layout, i.e., each vertex a qubit. We will see that the quantum solution will only require two-qubit gates between neighbors of the graph, which could thus be directly realized by the quantum computer.



The problem statement is based on the function

$$q(x) = \sum_{i,j=1}^{n} A_{i,j} x_i x_j \bmod 4, \quad x \in \{0, 1\}^n,$$

and we will restrict x to the kernel of $A \bmod 2$: $\mathrm{Ker}(A) = \{x \in \{0, 1\}^n : Ax = 0 \bmod 2\}$.

(a) Show that $q(x)$ is linear when its support is restricted to $\mathrm{Ker}(A)$.
Hint: Prove that $q(x \oplus y) = q(x) + q(y) \bmod 4$ for $x, y \in \mathrm{Ker}(A)$.

By the derivation of part (a), one concludes that $q(x)$ can be written as

$$q(x) = 2\sum_{i=1}^{n} y_i x_i \bmod 4, \quad x \in \mathrm{Ker}(A)$$

for some (non unique) binary string y, i.e., $q(x)$ effectively "hides" a binary string. The HLF problem asks to find such a y.

(b) We introduce a gate U_q that performs the following action (with i the imaginary unit):

$$U_q |s\rangle = i^{q(s)} |s\rangle, \ s \in \{0, 1\}^n.$$

Derive the relation

$$H^{\otimes n} U_q H^{\otimes n} |0^{\otimes n}\rangle = \frac{1}{2^n} \sum_{x,z\in\{0,1\}^n} i^{q(x)} (-1)^{z^T x} |z\rangle .$$

One can prove (see appendix) that the coefficient of each computational basis state $|z\rangle$ in this sum is non-zero precisely if z is a solution of the HLF problem. Thus a single standard measurement will yield a solution.

(c) We now discuss how a constant depth quantum circuit can realize U_q. Show that

$$U_q = \prod_{(v_i,v_j)\in E} CZ_{i,j},$$

with $CZ_{i,j}$ the controlled-Z gate between qubits i and j, defined as $CZ_{i,j} |x\rangle = (-1)^{x_i x_j} |x\rangle$ for $x \in \{0, 1\}^n$.

[1] S. Bravyi, D. Gosset, R. König: *Quantum advantage with shallow circuits.* Science 362, 308–311 (2018)

Solution

(a) We first expand the expression algebraically, for $x, y \in \mathrm{Ker}(A)$:

$$\begin{aligned}
q(x \oplus y) &= \sum_{i,j=1}^{n} A_{i,j}(x_i \oplus y_i)(x_j \oplus y_j) \bmod 4 \\
&= \sum_{i,j=1}^{n} A_{i,j}(x_i x_j + y_i y_j + x_i y_j + x_j y_i) \bmod 4 \\
&= q(x) + q(y) + 2y^T A x \bmod 4 \\
&= q(x) + q(y) \bmod 4.
\end{aligned}$$

For the last step we have used that $x \in \mathrm{Ker}(A)$, such that $2Ax \bmod 4 = 0$. Using the linearity of q, we note that $0 = q(0) = q(x \oplus x) = 2q(x)$. Thus, $q(x) \in \{0, 2\}$. We now define the function l by

$$l(x) = \begin{cases} 0 & \text{if } q(x) = 0 \\ 1 & \text{if } q(x) = 2 \end{cases}$$

The function l inherits linearity under addition modulo 2 from q, and can thus be represented by

$$l(x) = \sum_{i=1}^{n} y_i x_i \bmod 2$$

for some binary string $y \in \{0,1\}^n$. Consequently, $q(x)$ can be written as

$$q(x) = 2\sum_{i=1}^{n} y_i x_i \bmod 4.$$

(b) We first note that the application of the Hadamard gate to a qubit $|x\rangle$, $x \in \{0,1\}$, can be represented as

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}} (-1)^{zx} |z\rangle .$$

Thus

$$\begin{aligned}
H^{\otimes n} U_q H^{\otimes n} |0^{\otimes n}\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} H^{\otimes n} U_q |x\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} i^{q(x)} H^{\otimes n} |x\rangle \\
&= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} i^{q(x)} (-1)^{z_1 x_1} \cdots (-1)^{z_n x_n} |z\rangle \\
&= \frac{1}{2^n} \sum_{x,z \in \{0,1\}^n} i^{q(x)} (-1)^{x^T z} |z\rangle .
\end{aligned}$$

(c) We can verify this via inspection of the terms $A_{i,j} x_i x_j$ defining q. The only non-trivial situation is $A_{i,j} = 1$ and $i \neq j$. The term $A_{i,j} x_i x_j$ will be non-zero precisely if both $x_i = 1$ and $x_j = 1$, and it actually appears twice in the definition of $q(x)$ $(i \leftrightarrow j)$. Thus it contributes a factor of $i^2 = -1$ to $i^{q(x)}$ in this case, and $i^0 = 1$ otherwise. This matches the action of the controlled-Z gate $CZ_{i,j}$.

Thus, the circuit solely consisting of CZ gates realizes U_q. Since each vertex of the graph has at most 4 neighbors and gates on disjoint pairs of qubits can be executed in parallel, the circuit has constant depth irrespective of problem size.

Appendix (Mathematical derivations for the quantum algorithm)
This section contains parts of the proof why the quantum algorithm provides a solution for the 2D HLF problem. For the full details, refer to section B in the supplementary information of the publication.

We first read off the probability (squared coefficient) of any computational basis state $|z\rangle$ in the summation expansion shown in (b):

$$p(z) = \frac{1}{4^n} \left| \sum_{x \in \{0,1\}^n} \left| i^{q(x)} (-1)^{z^T x} \right| \right|^2 .$$

Given a linear subspace $\mathcal{L} \subseteq \{0,1\}^n$ and $z \in \{0,1\}^n$, we define the so-called *partial Fourier transform* Γ by

$$\Gamma(\mathcal{L}, z) = \sum_{x \in \mathcal{L}} (-1)^{z^T x} \cdot i^{q(x)}.$$

Thus

$$p(z) = \frac{1}{4^n} \left| \Gamma(\{0,1\}^n, z) \right|^2 .$$

Now partition $\{0,1\}^n = \mathrm{Ker}(A) + \mathcal{K}$, where $\mathcal{K} \subseteq \{0,1\}^n$ is a linear subspace and $\mathrm{Ker}(A) \cap \mathcal{K} = \{0\}$. Then, by the linearity of q,

$$\begin{aligned}
\Gamma(\{0,1\}^n, z) &= \sum_{x \in \mathrm{Ker}(A), x' \in \mathcal{K}} (-1)^{z^T (x + x')} \cdot i^{q(x \oplus x')} \\
&= \sum_{x \in \mathrm{Ker}(A)} (-1)^{z^T x} \cdot i^{q(x)} \sum_{x' \in \mathcal{K}} (-1)^{z^T x'} \cdot i^{q(x')} = \Gamma(\mathrm{Ker}(A), z) \cdot \Gamma(\mathcal{K}, z).
\end{aligned}$$

It can be shown that (see supplementary information of the publication) that

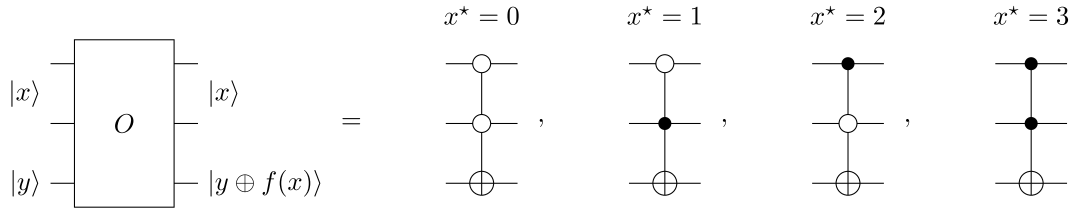
$$\Gamma(\mathrm{Ker}(A), z) = \begin{cases} \left|\mathrm{Ker}(A)\right| & \text{if } z \text{ is a solution to the 2D HLF problem} \\ 0 & \text{otherwise} \end{cases}$$

A required argumentation is the following: Let y be a hidden bit string such that $q(x) = 2 \sum_{i=1}^n y_i x_i$. Then $z \in \{0,1\}^n$ is another bit string with this property precisely if $z^T x = y^T x \bmod 2$ for all $x \in \mathrm{Ker}(A)$, which is equivalent to $(z \oplus y)^T x = 0 \bmod 2$ for all $x \in \mathrm{Ker}(A)$. This means that $z \oplus y \in \mathrm{Ker}(A)^\perp$ (orthogonal complement).

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 9.1 (Two-bit quantum search)
We consider the quantum search (Grover's) algorithm for the special case $n = 2$, i.e., a search space with $N = 4$ elements, and $M = 1$ (exactly one solution). The solution is denoted $x^\star$, and correspondingly $f(x^\star) = 1$, $f(x) = 0$ for all $x \neq x^\star$.

The oracle, which is able to recognize the solution, can be realized as follows (depending on $x^\star$):

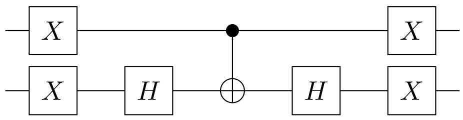


Note that the rightmost gate for $x^\star = 3$ is the Toffoli gate (cf. Exercise 5.2): the first and second qubits act as controls, and the third qubit as target, which is flipped precisely if both controls are set to 1. The empty circles in the gates for $x^\star = 0, 1, 2$ mean that the control is activated by 0 (instead of 1).

As derived in the lecture, the Grover operator G performs a rotation by angle θ in the plane spanned by the orthonormal states $|\alpha\rangle$ and $|\beta\rangle$; thus k applications to the initial equal superposition state $|\psi\rangle = \cos(\frac{\theta}{2})\,|\alpha\rangle + \sin(\frac{\theta}{2})\,|\beta\rangle$ results in

$$G^k\,|\psi\rangle = \cos\left((\tfrac{1}{2} + k)\theta\right)|\alpha\rangle + \sin\left((\tfrac{1}{2} + k)\theta\right)|\beta\rangle\,.$$

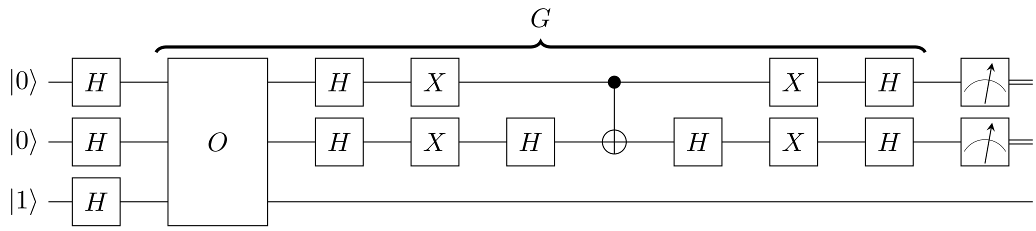
(a) Show that the following circuit implements the negated phase gate appearing in the Grover operator, that is, $-(2\,|00\rangle\langle 00| - I)$:



The global factor (-1) does not influence the final quantum measurement results and will be ignored from now on.

(b) Compute the angle θ defined via $\sin(\frac{\theta}{2}) = \sqrt{M/N}$. Why is a single application of G sufficient to reach the desired solution state $|\beta\rangle$ exactly, that is, $G\,|\psi\rangle = |\beta\rangle$?

In summary, the quantum search circuit with one use of G and the above realization of the phase gate is:

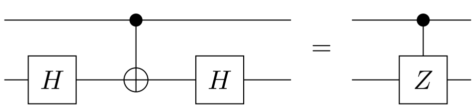


(c) Assemble this circuit in the IBM Q Circuit Composer for one of the four possible oracles of your choice, and verify that the final measurement indeed yields the solution $x^\star$.

Hint: You can use the Pauli-X gate to initialize the oracle qubit to $|1\rangle$. The Toffoli gate is available in the Circuit Composer.

Solution

(a) We have identified the controlled-NOT gate with the controlled-X gate in the lecture. Furthermore, since $HXH = Z$ and $H^2 = I$, the following identity holds:



The controlled-Z gate acts on computational basis states as

$$|00\rangle \mapsto |00\rangle\,, \quad |01\rangle \mapsto |01\rangle\,, \quad |10\rangle \mapsto |10\rangle\,, \quad |11\rangle \mapsto -|11\rangle\,,$$

which we can compactly represent as $I - 2\,|11\rangle\,\langle 11|$, or written in matrix form:

$$\text{controlled-}Z = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}.$$

Now the overall circuit operation (including the leading and trailing $X \otimes X$ gates) expressed in bra-ket notation reads

$$\begin{aligned} &(X \otimes X)(I - 2\,|11\rangle\,\langle 11|)(X \otimes X) \\ &= I - 2(X \otimes X)\,|11\rangle\,\langle 11|\,(X \otimes X) \\ &= I - 2(X\,|1\rangle \otimes X\,|1\rangle)(\langle 1|\,X \otimes \langle 1|\,X) \\ &= I - 2(|0\rangle \otimes |0\rangle)(\langle 0| \otimes \langle 0|) \\ &= I - 2\,|00\rangle\,\langle 00|\,. \end{aligned}$$

For the first equal sign we have used that $(X \otimes X)^2 = X^2 \otimes X^2 = I_2 \otimes I_2 = I_4$, where I_2 is the 2×2 identity matrix and likewise I_4 the 4×4 identity matrix.

Alternatively, we can use the matrix representation of $X \otimes X$:

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

Combined with the above matrix representation of controlled-Z leads to

$$(X \otimes X)(\text{controlled-}Z)(X \otimes X) = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix} = \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix},$$

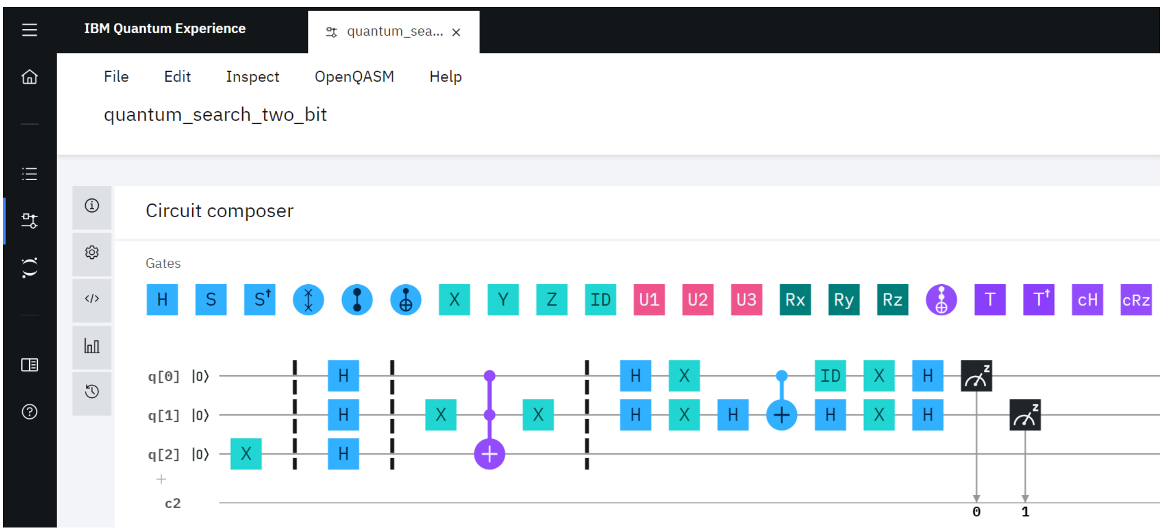
which is the matrix form of $I - 2\,|00\rangle\,\langle 00|$, as required.

(b) Here $M = 1$, $N = 4$, and $\sin(\frac{\theta}{2}) \stackrel{!}{=} \sqrt{M/N} = \frac{1}{2}$ for $\theta = \frac{\pi}{3}$. A single application of G yields

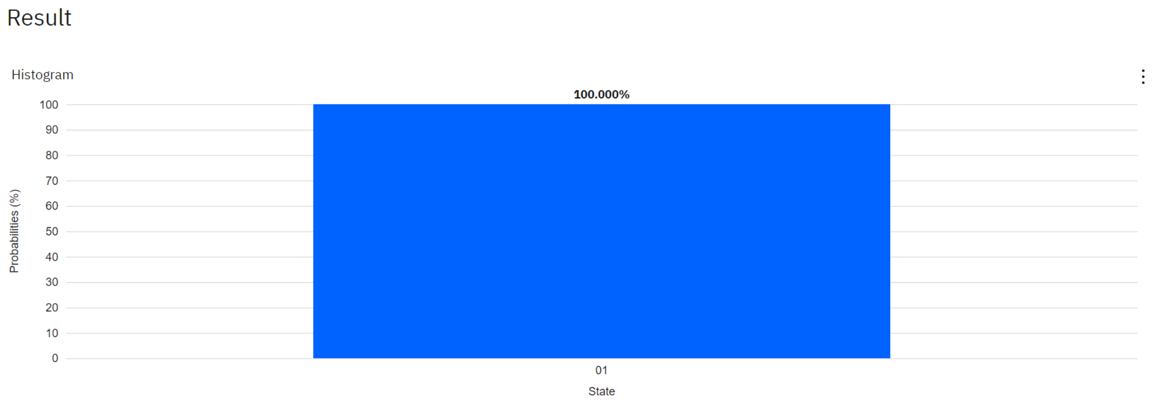
$$G\,|\psi\rangle = \cos\left(\tfrac{3}{2}\theta\right)|\alpha\rangle + \sin\left(\tfrac{3}{2}\theta\right)|\beta\rangle\,,$$

and inserting $\theta = \frac{\pi}{3}$ confirms that $G\,|\psi\rangle = |\beta\rangle$.

(c) A realization of the circuit (for $x^\star = 2$) in IBM Q is:



Simulating this circuit (using the `ibmq_qasm_simulator`) leads to the following result:



IBM Q uses the convention that the “first” (topmost) qubit corresponds to the least significant bit in the basis state enumeration, such that the reported state “01” actually corresponds to $|10\rangle$ following the convention of this exercise sheet. Thus we have indeed found the solution $x^{\star} = 2$, as expected.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 9.2 (Quantum search as quantum simulation, part 1)
Interestingly, the quantum search algorithm can be derived from a Schrödinger time evolution governed by a certain Hamiltonian H (cf. Tutorial 3). For simplicity, we assume that there is a single solution $x \in \{0, \dots, N-1\}$ to the search problem with N elements, and we start from an arbitrary initial state $|\psi\rangle$. It turns out that the Hamiltonian

$$H = |x\rangle\langle x| + |\psi\rangle\langle\psi|$$

achieves a transition from $|\psi\rangle$ to $|x\rangle$, that is, $\mathrm{e}^{-iHt^*}|\psi\rangle = |x\rangle$ for a certain time t^* (up to a phase factor, which is not relevant here). In part 1 we analyze the time evolution theoretically, and part 2 (next exercise sheet) discusses the simulation of the Hamiltonian.

To understand the transition from $|\psi\rangle$ to $|x\rangle$, first note that the time dynamics under H never leaves the two-dimensional space spanned by $|x\rangle$ and $|\psi\rangle$. Let the vector $|y\rangle$ be chosen such that $\{|x\rangle, |y\rangle\}$ forms an orthonormal basis of this subspace, and represent $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$ for some coefficients $\alpha, \beta \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 = 1$. For simplicity, we can assume that the phases of $|x\rangle$, $|y\rangle$ and $|\psi\rangle$ are such that α and β are real.

(a) Show that the matrix representation of H within this subspace is given by

$$H = I + \alpha(\beta X + \alpha Z).$$

Hint: The matrix entries of H restricted to a subspace with orthonormal basis $\{|u_j\rangle\}_{j=1,\dots,n}$ are $(\langle u_j| H |u_k\rangle)_{j,k}$.

(b) From the representation in (a), we thus obtain $\mathrm{e}^{-iHt} = \mathrm{e}^{-it}\,\mathrm{e}^{-i\alpha t(\beta X + \alpha Z)}$, where the phase factor e^{-it} stems from the identity matrix in the representation. Use the definition of the single-qubit rotation operators (see lecture) to verify that

$$\mathrm{e}^{-iHt} = \mathrm{e}^{-it}\left(\cos(\alpha t) I - i\sin(\alpha t)(\beta X + \alpha Z)\right).$$

(c) Show that $(\beta X + \alpha Z)|\psi\rangle = |x\rangle$. Together with (b), we thus arrive at

$$\mathrm{e}^{-iHt}|\psi\rangle = \mathrm{e}^{-it}\left(\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)|x\rangle\right).$$

(d) Specify a time t^* such that $\mathrm{e}^{-iHt^*}|\psi\rangle = |x\rangle$ up to a phase factor.

(e) Since the required time t^* depends on $\alpha = \langle x|\psi\rangle$ and thus seemingly on the (a priori unknown) solution x, a natural question is how to determine t^*. To resolve this question, one can choose $|\psi\rangle$ to be the equal superposition state. Compute α in this case, assuming that $|\psi\rangle$ is normalized.

Solution

(a) We insert $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$ into the definition of H:

$$\begin{aligned} H &= |x\rangle\langle x| + \big(\alpha|x\rangle + \beta|y\rangle\big)\big(\alpha\langle x| + \beta\langle y|\big) \\ &= |x\rangle\langle x| + \alpha^2|x\rangle\langle x| + \alpha\beta|x\rangle\langle y| + \alpha\beta|y\rangle\langle x| + \underbrace{\beta^2}_{1-\alpha^2}|y\rangle\langle y| \\ &= \big(|x\rangle\langle x| + |y\rangle\langle y|\big) + \alpha\big(\beta(|x\rangle\langle y| + |y\rangle\langle x|) + \alpha(|x\rangle\langle x| - |y\rangle\langle y|)\big). \end{aligned}$$

From this expression we can read off the matrix representation of H within the subspace:

$$\begin{pmatrix} \langle x| H |x\rangle & \langle x| H |y\rangle \\ \langle y| H |x\rangle & \langle y| H |y\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \alpha\left(\beta\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \alpha\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) = I + \alpha(\beta X + \alpha Z),$$

as required.

(b) We recall from the lecture the following formula for the rotation operator around an axis $\vec{v} \in \mathbb{R}^3$ with angle θ:

$$R_{\vec{v}}(\theta) = \mathrm{e}^{-i\theta(\vec{v}\cdot\vec{\sigma})/2} = \cos(\theta/2) I - i\sin(\theta/2)(\vec{v}\cdot\vec{\sigma}).$$

Here $\frac{\theta}{2} = \alpha t$ and $\vec{v} = (\beta, 0, \alpha)$, which has norm 1 since $\alpha^2 + \beta^2 = 1$. Inserted into the formula for the rotation operator directly leads to

$$\mathrm{e}^{-i\alpha t(\beta X + \alpha Z)} = \cos(\alpha t) I - i\sin(\alpha t)(\beta X + \alpha Z),$$

as required.

(c) The vector representation of $|\psi\rangle$ with respect to the $\{|x\rangle, |y\rangle\}$ basis is (α, β). Thus

$$(\beta X + \alpha Z)\,|\psi\rangle = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha^2 + \beta^2 \\ \beta\alpha - \alpha\beta \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |x\rangle\,.$$

(d) Setting $t^* = \frac{\pi}{2\alpha}$ satisfies $\cos(\alpha t^*) = 0$ and $\sin(\alpha t^*) = 1$, and thus

$$\mathrm{e}^{-iHt^*}\,|\psi\rangle = \mathrm{e}^{-it^*}\left(\cos(\alpha t^*)\,|\psi\rangle - i\sin(\alpha t^*)\,|x\rangle\right) = -i\,\mathrm{e}^{-i\pi/(2\alpha)}\,|x\rangle\,.$$

(e) The normalized equal superposition state is defined as

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} |z\rangle\,.$$

All computational basis states are equally likely, and $\alpha = \langle x|\psi\rangle = \frac{1}{\sqrt{N}}$, independent of x.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: 17 January 2022, 08:00 on Moodle

Tutorial 10 (Grover as a database search algorithm[1])
Grover's algorithm is sometimes referred to as a *database search algorithm*. In this tutorial we will examine how the algorithm could in principle be used to search in an unstructured database, and discuss the feasibility of this approach.

Assume we have a database containing $N = 2^n$ items, each of length l bits: $\{d_1, d_2, \ldots, d_N\}$. We want to determine where a particular item, s, is in this database.

(a) Discuss how a classical computer (with a CPU and a memory) would approach this problem. How many queries to the memory are required on average? What is the worst-case scenario?

Now imagine we are given a "quantum processing unit" (QPU) containing four registers:

- An n qubit register for the database index.
- An l qubit register for our query $|s\rangle$.
- An l qubit register for items loaded from the database, initialized as $|0\rangle$.
- A 1 qubit register initialized as $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

With this QPU, we can perform the following load operation: for an index x

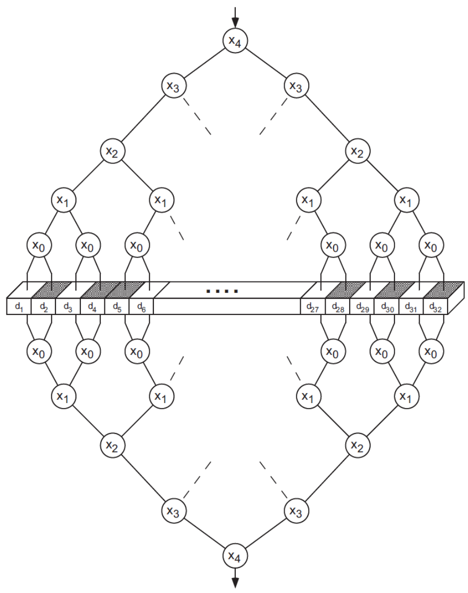
$$|x\rangle\,|s\rangle\,|t\rangle\,|-\rangle \overset{\text{LOAD}}{\mapsto} |x\rangle\,|s\rangle\,|t \oplus d_x\rangle\,|-\rangle\,.$$

In particular, for $|t\rangle = |0\rangle$ the third register will contain $|d_x\rangle$. Then, the second and the third register are compared and, if they are the same, a bit flip is applied to the forth register.

(b) What is the effect of this operation? What is its connection to Grover's algorithm?

Recall, however, that in Grover's algorithm we make use of superposition states. Thus, it may seem that in order to implement this we need a quantum memory besides our QPU. But in fact, we only need a classical memory which can be addressed by a quantum scheme.

The figure to the right shows a conceptual diagram of a 32 cell memory with a five qubit addressing scheme. The tree diagram represents the possible paths taken by an input qubit. At each node, the input qubit is sent left or right depending on the value of the qubit inside the circle. A superposition of paths is possible.



(c) What is the advantage of this scheme as opposed to a fully quantum memory?

(d) Discuss in general the practicality of this algorithm. Is the unstructured database problem common? Is the required hardware achievable?

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), section 6.5

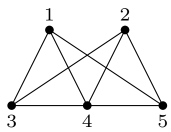
Exercise 10.1 (Hidden Linear Function problem on a specific graph)
Recall from tutorial 9 the following function q, given a square matrix A with binary entries:

$$q(x) = \sum_{i,j=1}^{n} A_{i,j} x_i x_j \bmod 4, \quad x \in \{0,1\}^n.$$

The Hidden Linear Function (HLF) problem asks to find a binary string y such that

$$q(x) = 2 \sum_{i=1}^{n} y_i x_i \bmod 4, \quad x \in \mathrm{Ker}(A).$$

A is chosen as adjacency matrix of a graph. Instead of a general square grid, here we consider the following graph as specific realization:



(a) Write down the corresponding adjacency matrix A.

(b) Compute the kernel $\mathrm{Ker}(A) \bmod 2$. (You are allowed to use a computer algebra system for this task.)

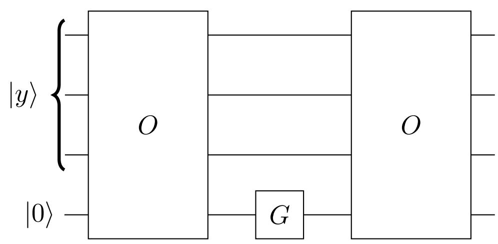
(c) Implement the quantum algorithm from part (b) and (c) of tutorial 9 using the circuit composer of IBM Q (`https://quantum-computing.ibm.com/`). Verify that one of the computational basis states appearing in the output with non-zero probability is indeed a solution to the HLF problem. Submit a screenshot showing the circuit as well as the output amplitudes or measurement probabilities.
Hint: You can create a controlled-Z gate by adding a control modifier to the Z gate in the circuit composer.

Exercise 10.2 (Quantum search as quantum simulation, part 2)
Continuing from exercise 9.2, the goal here is to *simulate* the time evolution governed by the Hamiltonian $H = |x\rangle\langle x| + |\psi\rangle\langle\psi|$ on a quantum computer. For that purpose, we can decompose $H = H_1 + H_2$ with $H_1 = |x\rangle\langle x|$ and $H_2 = |\psi\rangle\langle\psi|$, and approximate its effect via the Trotter formula, based on the identity:

$$\lim_{n\to\infty} \left(e^{-iH_1 t/n} e^{-iH_2 t/n}\right)^n = e^{-i(H_1+H_2)t}.$$

In our case, we can apply H_1 and H_2 in an alternating fashion using a small time step $\Delta t = t/n$ for some large n.

(a) Show that the following circuit implements $e^{-iH_1\Delta t}$, where $G = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{-i\Delta t} \end{smallmatrix}\right)$ and the oracle O is defined as in exercise 9.1, i.e., O maps $|y\rangle|0\rangle \mapsto |y\rangle|1\rangle$ precisely if $y = x$, and leaves $|y\rangle|0\rangle$ invariant otherwise.



Hint: Represent the input as

$$|y\rangle \otimes |0\rangle = (I - |x\rangle\langle x|)\,|y\rangle \otimes |0\rangle + |x\rangle\langle x\,|\,y\rangle \otimes |0\rangle,$$

and use the series expansion of the exponential to derive that $e^{-i|x\rangle\langle x|\Delta t} = I - |x\rangle\langle x| + e^{-i\Delta t}|x\rangle\langle x|$.

(b) Modify the oracle to design a circuit analogous to part (a) that implements the time evolution with respect to $H_2 = |\psi\rangle\langle\psi|$ for the cases

(i) $|\psi\rangle = |+\rangle^{\otimes 3}$, i.e., $|\psi\rangle$ the equal superposition state

(ii) $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|1\rangle$

(c) Identify the circuits from (a) and (b) for a time step $\Delta t = \pi$ with the building blocks of the circuit diagram of Grover's algorithm.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 10 (Grover as a database search algorithm[1])
Grover's algorithm is sometimes referred to as a *database search algorithm*. In this tutorial we will examine how the algorithm could in principle be used to search in an unstructured database, and discuss the feasibility of this approach.

Assume we have a database containing $N = 2^n$ items, each of length l bits: $\{d_1, d_2, \dots, d_N\}$. We want to determine where a particular item, s, is in this database.

(a) Discuss how a classical computer (with a CPU and a memory) would approach this problem. How many queries to the memory are required on average? What is the worst-case scenario?

Now imagine we are given a "quantum processing unit" (QPU) containing four registers:

- An n qubit register for the database index.
- An l qubit register for our query $|s\rangle$.
- An l qubit register for items loaded from the database, initialized as $|0\rangle$.
- A 1 qubit register initialized as $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

With this QPU, we can perform the following load operation: for an index x

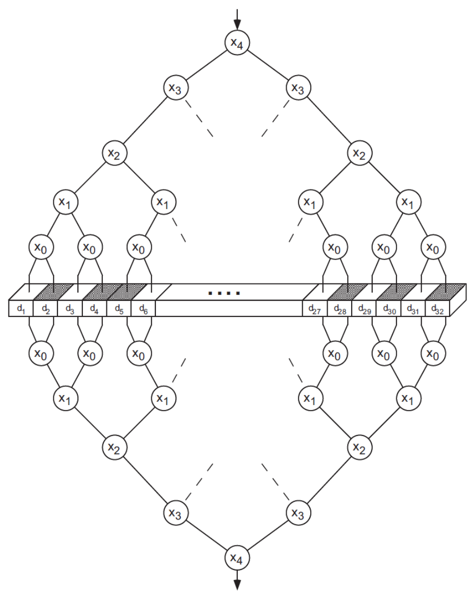
$$|x\rangle\,|s\rangle\,|t\rangle\,|-\rangle \overset{\text{LOAD}}{\mapsto} |x\rangle\,|s\rangle\,|t \oplus d_x\rangle\,|-\rangle\,.$$

In particular, for $|t\rangle = |0\rangle$ the third register will contain $|d_x\rangle$. Then, the second and the third register are compared and, if they are the same, a bit flip is applied to the forth register.

(b) What is the effect of this operation? What is its connection to Grover's algorithm?

Recall, however, that in Grover's algorithm we make use of superposition states. Thus, it may seem that in order to implement this we need a quantum memory besides our QPU. But in fact, we only need a classical memory which can be addressed by a quantum scheme.

The figure to the right shows a conceptual diagram of a 32 cell memory with a five qubit addressing scheme. The tree diagram represents the possible paths taken by an input qubit. At each node, the input qubit is sent left or right depending on the value of the qubit inside the circle. A superposition of paths is possible.



(c) What is the advantage of this scheme as opposed to a fully quantum memory?

(d) Discuss in general the practicality of this algorithm. Is the unstructured database problem common? Is the required hardware achievable?

Solution

(a) The CPU must have enough memory to store a bit string of length n. One can then iterate through the indexes of the database entries. Each entry, d_x, is loaded from the memory into the CPU and the condition $d_x = s$ is checked until satisfied. On average, this would require $N/2$ queries to the memory. The worst case scenario is when s is the very last item checked, i.e., one performs N queries.

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), section 6.5

(b) A conditional bit flip on the forth register results in

$$|x\rangle\,|s\rangle\,|d_x\rangle\,|-\rangle \mapsto \begin{cases} |x\rangle\,|s\rangle\,|d_x\rangle\,\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -\,|x\rangle\,|s\rangle\,|d_x\rangle\,|-\rangle\,, & \text{if } s = d_x \\ |x\rangle\,|s\rangle\,|d_x\rangle\,|-\rangle & \text{otherwise} \end{cases}$$

One can then perform the load operation again to reset the third qubit to zero, since $|d_x \oplus d_x\rangle = |0\rangle$. In summary, when the second and third register are the same, a phase of -1 is introduced. This is precisely the oracle in Grover's algorithm. Grover's algorithm will then only need $\mathcal{O}(\sqrt{N})$ such load and flip operations.

(c) Given that quantum states are very sensitive to noise, for long term storage it is preferable to use classical hardware.

(d) Unstructured databases are not common. Typically, the database is designed with some kind of structure to optimize the number of queries to memory needed (e.g., by storing items in alphabetical order). In terms of hardware, the quantum addressing scheme depicted above uses $\mathcal{O}(N\log(N))$ "switches" to send the input qubit left or right. At this point in time, such a setup would be too expensive, and not advantageous compared to distributed classical computing approaches.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

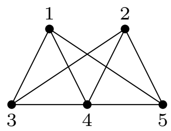
Exercise 10.1 (Hidden Linear Function problem on a specific graph)
Recall from tutorial 9 the following function q, given a square matrix A with binary entries:

$$q(x) = \sum_{i,j=1}^{n} A_{i,j} x_i x_j \bmod 4, \quad x \in \{0,1\}^n.$$

The Hidden Linear Function (HLF) problem asks to find a binary string y such that

$$q(x) = 2 \sum_{i=1}^{n} y_i x_i \bmod 4, \quad x \in \mathrm{Ker}(A).$$

A is chosen as adjacency matrix of a graph. Instead of a general square grid, here we consider the following graph as specific realization:



(a) Write down the corresponding adjacency matrix A.

(b) Compute the kernel $\mathrm{Ker}(A) \bmod 2$. (You are allowed to use a computer algebra system for this task.)

(c) Implement the quantum algorithm from part (b) and (c) of tutorial 9 using the circuit composer of IBM Q (`https://quantum-computing.ibm.com/`). Verify that one of the computational basis states appearing in the output with non-zero probability is indeed a solution to the HLF problem. Submit a screenshot showing the circuit as well as the output amplitudes or measurement probabilities.
Hint: You can create a controlled-Z gate by adding a control modifier to the Z gate in the circuit composer.

Solution

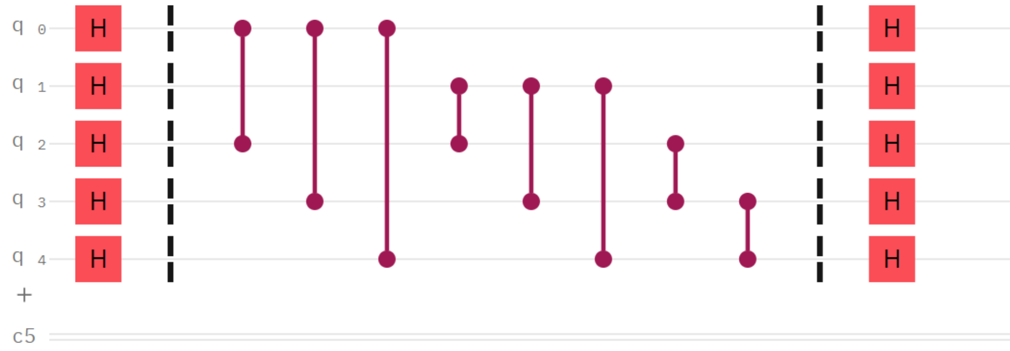
(a) The adjacency matrix of the graph is

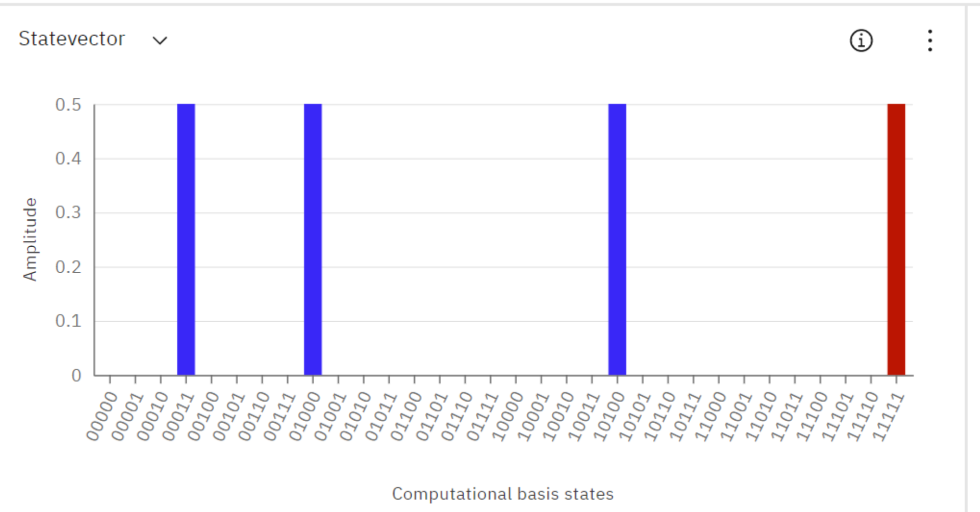
$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

(b) We want to find the vectors x such that $Ax = 0 \bmod 2$. They can be computed "by hand" for example by Gaussian elimination modulo 2. The space of solutions is spanned by the following three vectors:

$$\mathrm{Ker}(A) = \mathrm{span}\left(x^1, x^2, x^3\right) \quad \text{with} \quad x^1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad x^2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad x^3 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

(c) The corresponding quantum circuit and output statevector computed by the IBM circuit composer is





The output is a superposition of four computational basis states, one of which is

$$y = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Inserting the vectors from (b) into q results in

$$q(x_1) = 0, \quad q(x_2) = 0, \quad q(x_3) = 6 \bmod 4 = 2 \bmod 4.$$

This indeed agrees with $2\sum_{i=1}^{5} y_i x_i \bmod 4$, as required.

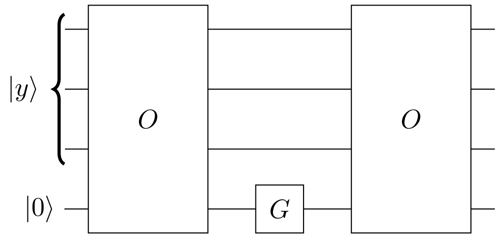
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 10.2 (Quantum search as quantum simulation, part 2)
Continuing from exercise 9.2, the goal here is to *simulate* the time evolution governed by the Hamiltonian $H = |x\rangle\langle x| + |\psi\rangle\langle\psi|$ on a quantum computer. For that purpose, we can decompose $H = H_1 + H_2$ with $H_1 = |x\rangle\langle x|$ and $H_2 = |\psi\rangle\langle\psi|$, and approximate its effect via the Trotter formula, based on the identity:

$$\lim_{n\to\infty}\left(e^{-iH_1 t/n}e^{-iH_2 t/n}\right)^n = e^{-i(H_1+H_2)t}.$$

In our case, we can apply H_1 and H_2 in an alternating fashion using a small time step $\Delta t = t/n$ for some large n.

(a) Show that the following circuit implements $e^{-iH_1\Delta t}$, where $G = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{-i\Delta t}\end{smallmatrix}\right)$ and the oracle O is defined as in exercise 9.1, i.e., O maps $|y\rangle|0\rangle \mapsto |y\rangle|1\rangle$ precisely if $y = x$, and leaves $|y\rangle|0\rangle$ invariant otherwise.



Hint: Represent the input as

$$|y\rangle\otimes|0\rangle = (I - |x\rangle\langle x|)\,|y\rangle\otimes|0\rangle + |x\rangle\langle x\,|\,y\rangle\otimes|0\rangle\,,$$

and use the series expansion of the exponential to derive that $e^{-i|x\rangle\langle x|\Delta t} = I - |x\rangle\langle x| + e^{-i\Delta t}|x\rangle\langle x|$.

(b) Modify the oracle to design a circuit analogous to part (a) that implements the time evolution with respect to $H_2 = |\psi\rangle\langle\psi|$ for the cases

(i) $|\psi\rangle = |+\rangle^{\otimes 3}$, i.e., $|\psi\rangle$ the equal superposition state

(ii) $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|1\rangle$

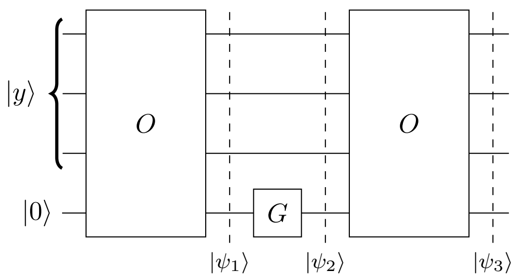
(c) Identify the circuits from (a) and (b) for a time step $\Delta t = \pi$ with the building blocks of the circuit diagram of Grover's algorithm.

Solution

(a) We first expand the term $e^{-i|x\rangle\langle x|\Delta t}$ via the matrix exponential series:

$$\begin{aligned}
e^{-i|x\rangle\langle x|\Delta t} &= \sum_{k=0}^{\infty}\frac{(-i\,|x\rangle\langle x|\,\Delta t)^k}{k!}\\
&= I + \sum_{k=1}^{\infty}\frac{(-i\Delta t)^k}{k!}\,|x\rangle\langle x|\\
&= I - |x\rangle\langle x| + \underbrace{\sum_{k=0}^{\infty}\frac{(-i\Delta t)^k}{k!}}_{e^{-i\Delta t}}\,|x\rangle\langle x|\\
&= I - |x\rangle\langle x| + e^{-i\Delta t}\,|x\rangle\langle x|\,.
\end{aligned}$$

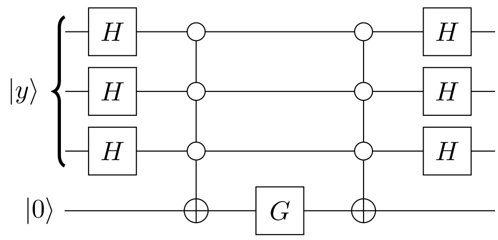
We then break down the circuit into individual steps:



$$
\begin{aligned}
|\psi_1\rangle &= (I - |x\rangle\langle x|)\,|y\rangle\,|0\rangle + |x\rangle\langle x\,|\,y\rangle\,|1\rangle \\
|\psi_2\rangle &= (I - |x\rangle\langle x|)\,|y\rangle\,|0\rangle + e^{-i\Delta t}\,|x\rangle\langle x\,|\,y\rangle\,|1\rangle \\
|\psi_3\rangle &= (I - |x\rangle\langle x|)\,|y\rangle\,|0\rangle + e^{-i\Delta t}\,|x\rangle\langle x\,|\,y\rangle\,|0\rangle \\
&= (I - |x\rangle\langle x| + \mathrm{e}^{-i\Delta t}\,|x\rangle\langle x|)\,|y\rangle\,|0\rangle \\
&= e^{-i|x\rangle\langle x|\Delta t}\,|y\rangle\,|0\rangle\,.
\end{aligned}
$$

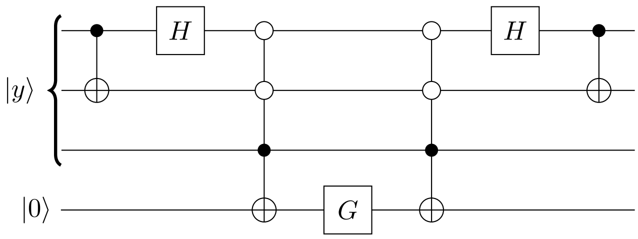
(b) Analogous to part (a), we note that the required effect of the to-be modified oracle is to flip the last qubit if the input $|y\rangle$ is equal to $|\psi\rangle$, and leave the last qubit invariant for any state orthogonal to $|\psi\rangle$. Different from (a), $|\psi\rangle$ is not a computational basis state here, but we can use Hadamard gates to perform as base change and then proceed as for computational basis states.

(i) Since $(H \otimes H \otimes H)\,|\psi\rangle = |000\rangle$, after the base change we need to recognize the state $|000\rangle$. This results in the overall circuit



The right half is a mirrored version of the left half to "uncompute" its action. The overall effect is to apply the phase factor $e^{-i\Delta t}$ precisely for input $|\psi\rangle$, as required.

(ii) We need an oracle which recognizes a Bell state in the leading two qubits:



(c) Note that $\mathrm{e}^{-i\pi} = -1$ corresponds to a sign flip. The circuit from part (b), case (i) (equal superposition state) can be identified with the Hadamard-phase-Hadamard block from Grover's algorithm, since it sends $|\psi\rangle \mapsto -|\psi\rangle$. The circuit from part (a) corresponds to the oracle application with the "oracle qubit" initialized to $|-\rangle$, since this likewise effects a sign flip precisely if the input is the sought solution $|x\rangle$.

Tutorial 11 (Bloch sphere interpretation of rotations[1])

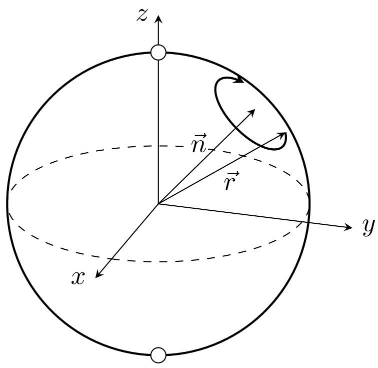
In this tutorial, we show that the Bloch sphere representation of a general single-qubit rotation operator

$$R_{\vec{n}}(\theta) = \mathrm{e}^{-i\theta(\vec{n}\cdot\vec{\sigma})/2} = \cos(\theta/2)I - i\sin(\theta/2)(\vec{n}\cdot\vec{\sigma})$$

is a conventional rotation (in three dimensions) by angle θ about axis $\vec{n} \in \mathbb{R}^3$. Let $\vec{r}$ denote the Bloch vector of the quantum state. It will be convenient to work with the following relation between $\vec{r}$ and the density matrix ρ of the quantum state:

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2}.$$

(By exercise 11.2 below, this coincides with the hitherto definition of the Bloch vector in case $\rho = |\psi\rangle\langle\psi|$ corresponds to a pure quantum state $|\psi\rangle$.)



(a) First verify the following commutation relation of the Pauli matrices: for any $j, k \in \{1, 2, 3\}$,

$$[\sigma_j, \sigma_k] = 2i \sum_{\ell=1}^{3} \epsilon_{jk\ell}\, \sigma_\ell,$$

where $[A, B] = AB - BA$ is the *commutator* of A and B, and the *Levi-Civita symbol* $\epsilon_{jk\ell}$ is defined by

$$\epsilon_{jk\ell} = \begin{cases} 1 & (j,k,\ell) \text{ is an even (cyclic) permutation of } (1,2,3) \\ -1 & (j,k,\ell) \text{ is an odd permutation of } (1,2,3) \\ 0 & \text{otherwise} \end{cases}$$

Conclude that, for any $\vec{a}, \vec{b} \in \mathbb{R}^3$,

$$\left[\vec{a}\cdot\vec{\sigma}, \vec{b}\cdot\vec{\sigma}\right] = 2i(\vec{a}\times\vec{b})\cdot\vec{\sigma}.$$

(b) Derive the relation

$$\left\{\vec{a}\cdot\vec{\sigma}, \vec{b}\cdot\vec{\sigma}\right\} = 2(\vec{a}\cdot\vec{b})I$$

for any $\vec{a}, \vec{b} \in \mathbb{R}^3$, where $\{A, B\} = AB + BA$ is the *anti-commutator* of A and B.

(c) Show that the Bloch vector of the rotated quantum state is obtained by applying Rodrigues' rotation formula:

$$\vec{r}' = \cos(\theta)\vec{r} + \sin(\theta)(\vec{n}\times\vec{r}) + (1 - \cos(\theta))\,(\vec{n}\cdot\vec{r})\vec{n}.$$

Remark: The interpretation as rotation applies to an arbitrary single-qubit gate U (when ignoring global phases), since it can always be represented as $U = \mathrm{e}^{i\alpha}R_{\vec{n}}(\theta)$ with $\alpha \in \mathbb{R}$ and a suitable rotation operator $R_{\vec{n}}(\theta)$.

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Exercise 4.6

Exercise 11.1 (von Neumann equation and time evolution with density operators)

(a) Based on the Schrödinger equation (cf. tutorial 3), derive the following *von Neumann equation* for a density matrix $\rho(t) = \sum_j p_j \, |\psi_j(t)\rangle \langle\psi_j(t)|$:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t}\rho(t) = [H, \rho(t)].$$

Here $[\cdot, \cdot]$ is the matrix commutator.

Hint: Use the product rule for computing the time derivative of each term $|\psi_j(t)\rangle \langle\psi_j(t)|$.

(b) What is the formal solution for $\rho(t)$ expressed in terms of the time evolution operator $U(t) = \mathrm{e}^{-iHt/\hbar}$?

(c) We consider the specific single-qubit Hamiltonian operator

$$H = JX$$

with parameter $J \in \mathbb{R}$. Compute the time-dependent density matrix $\rho(t)$ starting from the initial state $\rho_0 = \begin{pmatrix} 2/3 & 0 \\ 0 & 1/3 \end{pmatrix}$ at $t = 0$. For simplicity, you can set $\hbar = 1$.

(d) Since the map $\rho \mapsto [H, \rho]$ is linear, we can represent it as matrix-vector multiplication after "vectorizing" ρ, i.e., collecting its entries in a vector, denoted $\vec{\rho}$ in the following. For the commutator, this leads to

$$\vec{\rho} \mapsto \mathrm{vec}([H, \rho]) = \left(H \otimes I - I \otimes H^T\right) \vec{\rho},$$

where the identity matrix has the same dimension as H. Thus we can represent the von Neumann equation equivalently in the "superoperator" form

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t}\vec{\rho}(t) = \mathcal{H}\vec{\rho}(t), \quad \mathcal{H} = H \otimes I - I \otimes H^T.$$

Write down the formal solution of this differential equation, and determine $\mathcal{H}$ for the Hamiltonian from (c).

Exercise 11.2 (Bloch sphere for mixed state qubits[2])

(a) Show that an arbitrary density operator ρ for a qubit may be written as

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

where $\vec{r} \in \mathbb{R}^3$ is a real vector such that $\|\vec{r}\| \leq 1$. ($\vec{r}$ is called the *Bloch vector* of ρ.)

Hint: Note that $\{I, \sigma_1, \sigma_2, \sigma_3\}$ forms a basis of 2×2 matrices. Argue that the corresponding coefficients to represent a density matrix are real. Why is the coefficient of I equal to $\frac{1}{2}$? Finally, compute the eigenvalues of the above representation and use the positivity of ρ to derive the condition $\|\vec{r}\| \leq 1$.

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

(c) Verify that for pure states $\rho = |\psi\rangle \langle\psi|$, the above definition of the Bloch vector $\vec{r}$ coincides with the Bloch vector of $|\psi\rangle$ (cf. exercise 2.1).

Hint: Insert $|\psi\rangle = \mathrm{e}^{i\gamma}(\cos\frac{\theta}{2}\,|0\rangle + \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle)$ into $|\psi\rangle\langle\psi|$, read off the entries of $\vec{r}$ based on $|\psi\rangle\langle\psi| = (I + \vec{r}\cdot\vec{\sigma})/2$, and verify that $\vec{r} = (\cos(\varphi)\sin(\theta), \sin(\varphi)\sin(\theta), \cos(\theta))$.

[2] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Exercise 2.72

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 11 (Bloch sphere interpretation of rotations[1])

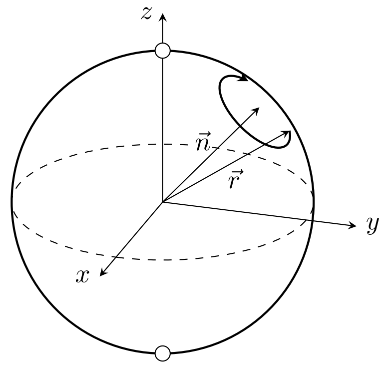
In this tutorial, we show that the Bloch sphere representation of a general single-qubit rotation operator

$$R_{\vec{n}}(\theta) = \mathrm{e}^{-i\theta(\vec{n}\cdot\vec{\sigma})/2} = \cos(\theta/2)I - i\sin(\theta/2)(\vec{n}\cdot\vec{\sigma})$$

is a conventional rotation (in three dimensions) by angle θ about axis $\vec{n} \in \mathbb{R}^3$. Let $\vec{r}$ denote the Bloch vector of the quantum state. It will be convenient to work with the following relation between $\vec{r}$ and the density matrix ρ of the quantum state:

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2}.$$

(By exercise 11.2 below, this coincides with the hitherto definition of the Bloch vector in case $\rho = |\psi\rangle\langle\psi|$ corresponds to a pure quantum state $|\psi\rangle$.)



(a) First verify the following commutation relation of the Pauli matrices: for any $j, k \in \{1,2,3\}$,

$$[\sigma_j, \sigma_k] = 2i \sum_{\ell=1}^{3} \epsilon_{jk\ell}\, \sigma_\ell,$$

where $[A,B] = AB - BA$ is the *commutator* of A and B, and the *Levi-Civita symbol* $\epsilon_{jk\ell}$ is defined by

$$\epsilon_{jk\ell} = \begin{cases} 1 & (j,k,\ell) \text{ is an even (cyclic) permutation of } (1,2,3) \\ -1 & (j,k,\ell) \text{ is an odd permutation of } (1,2,3) \\ 0 & \text{otherwise} \end{cases}$$

Conclude that, for any $\vec{a}, \vec{b} \in \mathbb{R}^3$,

$$\left[\vec{a}\cdot\vec{\sigma}, \vec{b}\cdot\vec{\sigma}\right] = 2i(\vec{a}\times\vec{b})\cdot\vec{\sigma}.$$

(b) Derive the relation

$$\left\{\vec{a}\cdot\vec{\sigma}, \vec{b}\cdot\vec{\sigma}\right\} = 2(\vec{a}\cdot\vec{b})I$$

for any $\vec{a}, \vec{b} \in \mathbb{R}^3$, where $\{A,B\} = AB + BA$ is the *anti-commutator* of A and B.

(c) Show that the Bloch vector of the rotated quantum state is obtained by applying Rodrigues' rotation formula:

$$\vec{r}' = \cos(\theta)\vec{r} + \sin(\theta)(\vec{n}\times\vec{r}) + (1-\cos(\theta))\,(\vec{n}\cdot\vec{r})\vec{n}.$$

Remark: The interpretation as rotation applies to an arbitrary single-qubit gate U (when ignoring global phases), since it can always be represented as $U = \mathrm{e}^{i\alpha}R_{\vec{n}}(\theta)$ with $\alpha \in \mathbb{R}$ and a suitable rotation operator $R_{\vec{n}}(\theta)$.

Solution

(a) We first note that for $j = k$, the commutator is clearly zero, as is the Levi-Civita symbol.

For $j = 1$ and $k = 2$, by an explicit calculation,

$$\begin{aligned}[\sigma_1, \sigma_2] &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} - \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} - \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 2i & 0 \\ 0 & -2i \end{pmatrix} \\ &= 2i\sigma_3 = 2i\sum_{\ell=1}^{3}\epsilon_{12\ell}\,\sigma_\ell,\end{aligned}$$

and similarly $[\sigma_2, \sigma_3] = 2i\sigma_1$ and $[\sigma_3, \sigma_1] = 2i\sigma_2$ (see also exercise 3.1). Finally, we note that an interchange $j \leftrightarrow k$ flips the sign of the commutator, $[\sigma_j, \sigma_k] = -[\sigma_k, \sigma_j]$, and likewise the sign of $\epsilon_{jk\ell}$ by definition. In summary, we have verified the relation for all possible cases of $j, k \in \{1,2,3\}$.

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Exercise 4.6

Expanding in terms of individual Pauli matrices leads to:

$$\left[\vec{a}\cdot\vec{\sigma},\vec{b}\cdot\vec{\sigma}\right] = \sum_{j,k=1}^{3} a_j b_k\,[\sigma_j,\sigma_k] = 2i \sum_{j,k,\ell=1}^{3} a_j b_k\,\epsilon_{jk\ell}\,\sigma_\ell = 2i \begin{pmatrix} a_2b_3 - a_3b_2 \\ a_3b_1 - a_1b_3 \\ a_1b_2 - a_2b_1 \end{pmatrix} \cdot \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix} = 2i(\vec{a}\times\vec{b})\cdot\vec{\sigma}.$$

(b) The statement follows from the fact that different Pauli matrices anti-commute, i.e., $\sigma_j\sigma_k = -\sigma_k\sigma_j$ for $j \neq k$ (see exercise 3.1), and that squaring a Pauli matrix gives the identity:

$$\left\{\vec{a}\cdot\vec{\sigma},\vec{b}\cdot\vec{\sigma}\right\} = \sum_{j,k=1}^{3} a_j b_k\,\{\sigma_j,\sigma_k\} = \sum_{j,k=1}^{3} a_j b_k\,\delta_{jk} 2I = 2(\vec{a}\cdot\vec{b})I.$$

(c) In general, applying a unitary matrix U to a quantum state $|\psi\rangle$ corresponds to a conjugation of the density matrix by U:

$$\rho \mapsto U\rho U^\dagger.$$

In our case, $U = R_{\vec{n}}(\theta)$, and $U^\dagger = R_{\vec{n}}(-\theta)$ (inverse rotation).

Inserting the Bloch representation of the density matrix leads to

$$\begin{aligned}
R_{\vec{n}}(\theta)\rho R_{\vec{n}}(-\theta) &= \frac{I}{2} + \frac{1}{2} R_{\vec{n}}(\theta)(\vec{r}\cdot\vec{\sigma})R_{\vec{n}}(-\theta) \\
&= \frac{I}{2} + \frac{1}{2}\cos(\theta/2)^2\,(\vec{r}\cdot\vec{\sigma}) + \frac{i}{2}\cos(\theta/2)\sin(\theta/2)\,(\vec{r}\cdot\vec{\sigma})(\vec{n}\cdot\vec{\sigma}) - \frac{i}{2}\cos(\theta/2)\sin(\theta/2)\,(\vec{n}\cdot\vec{\sigma})(\vec{r}\cdot\vec{\sigma}) \\
&\quad + \frac{1}{2}\sin(\theta/2)^2\,(\vec{n}\cdot\vec{\sigma})(\vec{r}\cdot\vec{\sigma})(\vec{n}\cdot\vec{\sigma}) \\
&= \frac{I}{2} + \underbrace{\frac{1}{2}\cos(\theta/2)^2\,(\vec{r}\cdot\vec{\sigma})}_{①} + \underbrace{\frac{i}{2}\cos(\theta/2)\sin(\theta/2)\,[\vec{r}\cdot\vec{\sigma},\vec{n}\cdot\vec{\sigma}]}_{②} + \underbrace{\frac{1}{2}\sin(\theta/2)^2\,(\vec{n}\cdot\vec{\sigma})(\vec{r}\cdot\vec{\sigma})(\vec{n}\cdot\vec{\sigma})}_{③}.
\end{aligned}$$

To further simplify ②, we use part (a) together with the identity $2\cos(\alpha)\sin(\alpha) = \sin(2\alpha)$ for any $\alpha \in \mathbb{R}$:

$$② = \frac{i}{2}\cos(\theta/2)\sin(\theta/2)\,2i(\vec{r}\times\vec{n})\cdot\vec{\sigma} = -\frac{1}{2}\sin(\theta)\,(\vec{r}\times\vec{n})\cdot\vec{\sigma} = \frac{1}{2}\sin(\theta)\,(\vec{n}\times\vec{r})\cdot\vec{\sigma}.$$

To simplify ③, we first note that, according to (b),

$$(\vec{n}\cdot\vec{\sigma})(\vec{r}\cdot\vec{\sigma}) = -(\vec{r}\cdot\vec{\sigma})(\vec{n}\cdot\vec{\sigma}) + 2(\vec{n}\cdot\vec{r})I.$$

Also, since $\vec{n}$ is a unit vector, $(\vec{n}\cdot\vec{\sigma})^2 = I$ (see lecture). Inserted into ③ leads to

$$\begin{aligned}
③ &= \sin(\theta/2)^2\,(\vec{n}\cdot\vec{r})(\vec{n}\cdot\vec{\sigma}) - \frac{1}{2}\sin(\theta/2)^2\,(\vec{r}\cdot\vec{\sigma}) \\
&= \frac{1}{2}\,(1-\cos(\theta))\,(\vec{n}\cdot\vec{r})(\vec{n}\cdot\vec{\sigma}) - \frac{1}{2}\sin(\theta/2)^2\,(\vec{r}\cdot\vec{\sigma}).
\end{aligned}$$

Combining parts ①, ②, ③, and using the identity $\cos(\alpha)^2 - \sin(\alpha)^2 = \cos(2\alpha)$, we obtain:

$$R_{\vec{n}}(\theta)\rho R_{\vec{n}}(-\theta) = \frac{I}{2} + \frac{1}{2}\underbrace{\Big(\cos(\theta)\vec{r} + \sin(\theta)(\vec{n}\times\vec{r}) + (1-\cos(\theta))\,(\vec{n}\cdot\vec{r})\vec{n}\Big)}_{\vec{r}'}\cdot\vec{\sigma}$$

The expression for the new Bloch vector $\vec{r}'$ is exactly Rodrigues' rotation formula, as required.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 11.1 (von Neumann equation and time evolution with density operators)

(a) Based on the Schrödinger equation (cf. tutorial 3), derive the following *von Neumann equation* for a density matrix $\rho(t) = \sum_j p_j \, |\psi_j(t)\rangle \langle \psi_j(t)|$:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t}\rho(t) = [H, \rho(t)].$$

Here $[\cdot,\cdot]$ is the matrix commutator.

Hint: Use the product rule for computing the time derivative of each term $|\psi_j(t)\rangle \langle \psi_j(t)|$.

(b) What is the formal solution for $\rho(t)$ expressed in terms of the time evolution operator $U(t) = \mathrm{e}^{-iHt/\hbar}$?

(c) We consider the specific single-qubit Hamiltonian operator

$$H = JX$$

with parameter $J \in \mathbb{R}$. Compute the time-dependent density matrix $\rho(t)$ starting from the initial state $\rho_0 = \left(\begin{smallmatrix} 2/3 & 0 \\ 0 & 1/3 \end{smallmatrix}\right)$ at $t = 0$. For simplicity, you can set $\hbar = 1$.

(d) Since the map $\rho \mapsto [H, \rho]$ is linear, we can represent it as matrix-vector multiplication after "vectorizing" ρ, i.e., collecting its entries in a vector, denoted $\vec{\rho}$ in the following. For the commutator, this leads to

$$\vec{\rho} \mapsto \mathrm{vec}([H, \rho]) = \left(H \otimes I - I \otimes H^T\right) \vec{\rho},$$

where the identity matrix has the same dimension as H. Thus we can represent the von Neumann equation equivalently in the "superoperator" form

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t}\vec{\rho}(t) = \mathcal{H}\vec{\rho}(t), \quad \mathcal{H} = H \otimes I - I \otimes H^T.$$

Write down the formal solution of this differential equation, and determine $\mathcal{H}$ for the Hamiltonian from (c).

Solution

(a) By the product rule,

$$\begin{aligned} i\hbar \frac{\mathrm{d}}{\mathrm{d}t}\rho(t) &= i\hbar \frac{\mathrm{d}}{\mathrm{d}t} \sum_j p_j \, |\psi_j(t)\rangle \langle \psi_j(t)| = \sum_j p_j \left(\frac{i\hbar \, \mathrm{d}\, |\psi_j(t)\rangle}{\mathrm{d}t} \langle \psi_j(t)| + |\psi_j(t)\rangle \frac{i\hbar \, \mathrm{d} \langle \psi_j(t)|}{\mathrm{d}t} \right) \\ &= \sum_j p_j \Big(\big(H\, |\psi_j(t)\rangle\big) \langle \psi_j(t)| - |\psi_j(t)\rangle \big(\langle \psi_j(t)| \, H^\dagger\big) \Big) = H\rho(t) - \rho(t)H = [H, \rho(t)]. \end{aligned}$$

Here we have used that the Hamiltonian H is Hermitian, that is, $H^\dagger = H$. The minus sign stems from taking the conjugate-transpose of the Schrödinger equation.

(b) The formal solution for a pure state is $|\psi(t)\rangle = U(t)\, |\psi(0)\rangle$, and thus

$$\rho(t) = U(t)\rho_0 U(t)^\dagger = U(t)\rho_0 U(-t).$$

This $\rho(t)$ indeed solves the von Neumann equation, since $\frac{\mathrm{d}}{\mathrm{d}t}U(t) = -\frac{i}{\hbar}H$.

(c) We first determine the unitary time evolution operator $U(t)$, using the formula for the R_x rotation operator:

$$U(t) = \mathrm{e}^{-iHt} = \mathrm{e}^{-iJXt} = \cos(Jt)I - i\sin(Jt)X = \begin{pmatrix} \cos(Jt) & -i\sin(Jt) \\ -i\sin(Jt) & \cos(Jt) \end{pmatrix}.$$

Inserted into the equation from (b) leads to

$$\begin{aligned} \rho(t) = U(t)\rho_0 U(-t) &= \begin{pmatrix} \cos(Jt) & -i\sin(Jt) \\ -i\sin(Jt) & \cos(Jt) \end{pmatrix} \begin{pmatrix} \frac{2}{3} & 0 \\ 0 & \frac{1}{3} \end{pmatrix} \begin{pmatrix} \cos(Jt) & i\sin(Jt) \\ i\sin(Jt) & \cos(Jt) \end{pmatrix} \\ &= \begin{pmatrix} \frac{2}{3}\cos^2(Jt) + \frac{1}{3}\sin^2(Jt) & \frac{i}{3}\cos(Jt)\sin(Jt) \\ -\frac{i}{3}\cos(Jt)\sin(Jt) & \frac{1}{3}\cos^2(Jt) + \frac{2}{3}\sin^2(Jt) \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{3} + \frac{1}{3}\cos^2(Jt) & \frac{i}{6}\sin(2Jt) \\ -\frac{i}{6}\sin(2Jt) & \frac{1}{3} + \frac{1}{3}\sin^2(Jt) \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{2} + \frac{1}{6}\cos(2Jt) & \frac{i}{6}\sin(2Jt) \\ -\frac{i}{6}\sin(2Jt) & \frac{1}{2} - \frac{1}{6}\cos(2Jt) \end{pmatrix} = \frac{1}{2}\left(I - \frac{1}{3}\sin(2Jt)Y + \frac{1}{3}\cos(2Jt)Z\right). \end{aligned}$$

(d) The superoperator differential equation can be identified with a Schrödinger equation, with analogous formal solution

$$\vec{\rho}(t) = \mathrm{e}^{-i\mathcal{H}t/\hbar}\,\vec{\rho}_0.$$

For the Hamiltonian from (c), we note that $X^T = X$, and obtain

$$\mathcal{H} = J(X \otimes I - I \otimes X) = J \begin{pmatrix} 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix}.$$

Exercise 11.2

(a)

Recall that σ_j are the Pauli matrices: $\sigma_1 = X$, $\sigma_2 = Y$, $\sigma_3 = Z$. Since $\{I, \sigma_1, \sigma_2, \sigma_3\}$ forms a basis of 2×2 matrices, we can represent any density matrix ρ as

$$\rho = \alpha I + \frac{1}{2} (r_1 \sigma_1 + r_2 \sigma_2 + r_3 \sigma_3)$$

using suitable coefficients α, r_1, r_2, r_3. These coefficients are real since any density matrix ρ and the Pauli matrices are Hermitian.

The Pauli matrices are traceless: $\mathrm{Tr}[\sigma_j] = 0$, thus

$\mathrm{Tr}[\rho] = \alpha\, \mathrm{Tr}[I] = 2\alpha.$

Density matrices have trace 1, and therefore $\alpha = \frac{1}{2}$.

In summary, we arrive at the representation

$$\rho = \frac{I + \vec{r}.\vec{\sigma}}{2} \tag{1}$$

```
BlochDensity[r_] := 1/2 (IdentityMatrix[2] + Sum[r[[i]] PauliMatrix[i], {i, 3}])
```

Explicit matrix form:

```
BlochDensity[{r1, r2, r3}] // MatrixForm
```

$$\begin{pmatrix} \frac{1}{2}(1 + r_3) & \frac{1}{2}(r_1 - i\, r_2) \\ \frac{1}{2}(r_1 + i\, r_2) & \frac{1}{2}(1 - r_3) \end{pmatrix}$$

Eigenvalues:

```
Eigenvalues[BlochDensity[{r1, r2, r3}]]
```

$$\left\{\frac{1}{2}\left(1 - \sqrt{r_1^2 + r_2^2 + r_3^2}\right), \frac{1}{2}\left(1 + \sqrt{r_1^2 + r_2^2 + r_3^2}\right)\right\}$$

Density matrices are positive operators, i.e., their eigenvalues are non-negative. In particular,

$$\frac{1}{2}\left(1 - \sqrt{r_1^2 + r_2^2 + r_3^2}\right) \geq 0,$$

which is equivalent to $\|\vec{r}\| \leq 1$.

(b)

Recall that a density matrix ρ describes a pure state if and only if it can be written as $\rho = |\psi\rangle\langle\psi|$, equivalently if one eigenvalue of ρ is 1 and the others are all 0. Based on the two eigenvalues computed above, this is equivalent to $\|\vec{r}\| = 1$.

Alternative solution: in the lecture we have derived the criterion $\mathrm{Tr}[\rho^2] = 1$ to characterize pure states. Inserting the representation in Eq. (1) leads to

$$\mathrm{Tr}\left[\rho^2\right] = \frac{1}{4}\mathrm{Tr}\left[\left(\mathrm{I}+\vec{r}.\vec{\sigma}\right)^2\right] = \frac{1}{4}\mathrm{Tr}\left[\mathrm{I}+2\,\vec{r}.\vec{\sigma}+\left(\vec{r}.\vec{\sigma}\right)^2\right] = \frac{1}{4}\left(\mathrm{Tr}[\mathrm{I}]+\mathrm{Tr}\left[\left(r_1^2+r_2^2+r_3^2\right)\mathrm{I}\right]\right) = \frac{1}{2}\left(1+\|\vec{r}\|^2\right) \tag{2}$$

where we have used that the Pauli matrices are traceless and $\left(\vec{r}.\vec{\sigma}\right)^2 = \left(r_1^2+r_2^2+r_3^2\right)\mathrm{I}$ (which one can check by direct computation). Directly from Eq. (2) one concludes that $\mathrm{Tr}[\rho^2] = 1$ is equivalent to $\|\vec{r}\| = 1$.

(c)

```
ψ = e^(ⅈ γ) {Cos[θ/2], e^(ⅈ ϕ) Sin[θ/2]};
```

Compute $|\psi\rangle\langle\psi|$:

```
FullSimplify[KroneckerProduct[ψ, Conjugate[ψ]],
  Assumptions → {γ ∈ Reals, θ ∈ Reals, ϕ ∈ Reals}] // MatrixForm
```

$$\begin{pmatrix} \mathrm{Cos}\left[\frac{\theta}{2}\right]^2 & \frac{1}{2}e^{-i\phi}\,\mathrm{Sin}[\theta] \\ \frac{1}{2}e^{i\phi}\,\mathrm{Sin}[\theta] & \mathrm{Sin}\left[\frac{\theta}{2}\right]^2 \end{pmatrix}$$

We now compute the vector $\vec{r}$ implicitly defined via $|\psi\rangle\langle\psi| = \left(\mathrm{I}+\vec{r}.\vec{\sigma}\right)/2$. First recall the definition of the Pauli matrices:

$$\sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\quad \sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\quad \sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Based on the diagonal entries, one concludes that

$$\mathrm{Cos}\left[\frac{\theta}{2}\right]^2 = \frac{1+r_3}{2},\quad \mathrm{Sin}\left[\frac{\theta}{2}\right]^2 = \frac{1-r_3}{2},$$

which has the solution $r_3 = \mathrm{Cos}[\theta]$. Check:

```
FullSimplify[Cos[θ/2]^2 - (1 + Cos[θ])/2]
FullSimplify[Sin[θ/2]^2 - (1 - Cos[θ])/2]
```

```
0
```

```
0
```

From the off-diagonal entries, it follows that

$$\frac{1}{2}e^{-i\phi}\,\mathrm{Sin}[\theta] = \frac{1}{2}(r_1 - i\,r_2),\quad \frac{1}{2}e^{i\phi}\,\mathrm{Sin}[\theta] = \frac{1}{2}(r_1 + i\,r_2)$$

with solution (see Euler's formula)

$$r_1 = \mathrm{Cos}[\phi]\,\mathrm{Sin}[\theta],\quad r_2 = \mathrm{Sin}[\phi]\,\mathrm{Sin}[\theta].$$

Tutorial 12 (Schmidt decomposition and purifications[1])

(a) Prove the following theorem:

Theorem (**Schmidt decomposition**) Suppose $|\psi\rangle$ is a pure state of a composite system, AB. Then there exist orthonormal states $|i_\mathsf{A}\rangle_{i=1,\dots,k}$ for system A, and orthonormal states $|i_\mathsf{B}\rangle_{i=1,\dots,k}$ for system B such that

$$|\psi\rangle = \sum_{i=1}^{k} \lambda_i \, |i_\mathsf{A}\rangle \, |i_\mathsf{B}\rangle \, ,$$

where λ_i are non-negative real numbers satisfying $\sum_{i=1}^{k} \lambda_i^2 = 1$ known as *Schmidt coefficients*.

(b) Show that, as consequence of the Schmidt decomposition, the deduced density matrices for subsystems A and B have the same eigenvalues if the composite system is in a pure state $|\psi\rangle$.

(c) Given a density operator ρ^A on a quantum system A, construct a pure state $|\psi\rangle$ on an extended quantum system AR such that $\rho^\mathsf{A} = \mathrm{tr}_\mathsf{R}[|\psi\rangle\langle\psi|]$. This procedure is known as *purification*.

Exercise 12.1 (Schmidt decomposition and entanglement entropy)
As in tutorial 12, let $|\psi\rangle$ be a pure state of a composite system, AB. The Schmidt decomposition of this state is denoted by $|\psi\rangle = \sum_{i=1}^{k} \sigma_i \, |i_\mathsf{A}\rangle \, |i_\mathsf{B}\rangle$.

(a) Verify that

$$\langle\psi|\psi\rangle = \sum_{i=1}^{k} \sigma_i^2.$$

In general, the *von Neumann entropy* of a density matrix ρ is defined as

$$\mathcal{S}(\rho) = -\,\mathrm{tr}[\rho \log(\rho)],$$

with the logarithm interpreted as matrix function, and the convention $0 \log(0) = \lim_{x\to 0} x \log(x) = 0$.

In tutorial 12 we found the reduced density matrices of the subsystems, defined as $\rho_1 = \mathrm{tr}_2[|\psi\rangle\langle\psi|]$ and $\rho_2 = \mathrm{tr}_1[|\psi\rangle\langle\psi|]$. We observed that ρ_1 and ρ_2 have the same eigenvalues $(\sigma_i^2)_{i=1,\dots,k}$. The *entanglement entropy* between the two subsystems is then given by

$$\mathcal{S}_\mathsf{ent} = \mathcal{S}(\rho_1) = \mathcal{S}(\rho_2) = -\sum_{i=1}^{k} \sigma_i^2 \log\bigl(\sigma_i^2\bigr).$$

(You should convince yourself that $\mathcal{S}(\rho_1)$ and $\mathcal{S}(\rho_2)$ are indeed equal to the sum on the right.) Intuitively, the entanglement entropy measures how strongly the subsystems are intertwined.

(b) Which sets of singular values $(\sigma_i)_{i=1,\dots,k}$ minimize and maximize the entanglement entropy, respectively, under the normalization condition $\sum_{i=1}^{k} \sigma_i^2 = 1$? ($k$ should be regarded as fixed.)
Hints: The smallest possible entanglement entropy is zero. Regarding maximization, you can take the normalization condition via a Lagrange multiplier into account.

(c) Show that $\mathcal{S}_\mathsf{ent} = 0$ (completely unentangled case) implies that $|\psi\rangle$ can be written as tensor product of a state from subsystem A and one from subsystem B.

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Section 2.5

Exercise 12.2 (Python/NumPy implementation of the partial trace)

(a) Implement the partial trace operation for arbitrary dimensions using Python/NumPy. Specifically, you should write a function with signature `partial_trace(rho, dimA, dimB)`, where `rho` is the density matrix of the composite quantum system, and `dimA`, `dimB` specify the dimensions of subsystems A and B, respectively. (Thus `rho` is a `dimA`$\cdot$`dimB` $\times$ `dimA`$\cdot$`dimB` matrix.) The function should return a tuple $(\rho^{\mathsf{A}}, \rho^{\mathsf{B}})$ containing the reduced density matrices $\rho^{\mathsf{A}} = \mathrm{tr}_{\mathsf{B}}[\mathtt{rho}]$ and $\rho^{\mathsf{B}} = \mathrm{tr}_{\mathsf{A}}[\mathtt{rho}]$.

Hint: First reshape `rho` into a `dimA` $\times$ `dimB` $\times$ `dimA` $\times$ `dimB` tensor using `numpy.reshape`. Then apply `numpy.trace` to trace out certain dimensions.

(b) Apply your function to $\rho = |\psi\rangle\langle\psi|$ with the Bell state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The reduced density matrices should both be equal to $\frac{I}{2}$.

Hint: Represent $|\psi\rangle$ as vector (NumPy array) of length 4. `numpy.outer(psi, psi.conj())` computes the outer product $|\psi\rangle\langle\psi|$.

(c) Test your implementation by constructing a random density matrix ρ on the composite system and a random observable M on subsystem A, and then numerically verifying that $\mathrm{tr}[M\rho^{\mathsf{A}}] = \mathrm{tr}[(M \otimes I)\rho]$ (up to numerical rounding errors).

You can use the following functions to obtain ρ and M:

```
import numpy as np


def construct_random_density_matrix(d):
    """
    Construct a complex random density matrix of dimension d x d.
    """
    # ensure that rho is positive semidefinite
    A = (np.random.randn(d, d) + 1j*np.random.randn(d, d))/np.sqrt(2)
    rho = A @ A.conj().T
    # normalization
    rho /= np.trace(rho)
    return rho


def construct_random_operator(d):
    """
    Construct a complex random Hermitian matrix of dimension d x d.
    """
    # ensure that M is Hermitian
    A = (np.random.randn(d, d) + 1j*np.random.randn(d, d))/np.sqrt(2)
    M = 0.5*(A + A.conj().T)
    return M
```

Hint: In Python $\geq$ 3.5, the `@` operator performs the matrix product.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 12 (Schmidt decomposition and purifications[1])

(a) Prove the following theorem:

Theorem (**Schmidt decomposition**) Suppose $|\psi\rangle$ is a pure state of a composite system, AB. Then there exist orthonormal states $|i_{\mathsf{A}}\rangle_{i=1,\dots,k}$ for system A, and orthonormal states $|i_{\mathsf{B}}\rangle_{i=1,\dots,k}$ for system B such that

$$|\psi\rangle = \sum_{i=1}^{k} \lambda_i \, |i_{\mathsf{A}}\rangle \, |i_{\mathsf{B}}\rangle \,,$$

where λ_i are non-negative real numbers satisfying $\sum_{i=1}^{k} \lambda_i^2 = 1$ known as *Schmidt coefficients*.

(b) Show that, as consequence of the Schmidt decomposition, the deduced density matrices for subsystems A and B have the same eigenvalues if the composite system is in a pure state $|\psi\rangle$.

(c) Given a density operator ρ^{A} on a quantum system A, construct a pure state $|\psi\rangle$ on an extended quantum system AR such that $\rho^{\mathsf{A}} = \mathrm{tr}_{\mathsf{R}}[|\psi\rangle\langle\psi|]$. This procedure is known as *purification*.

Solution

(a) The Schmidt decomposition is basically an application of the *singular value decomposition* of matrices (see also the linear algebra cheat sheet):

Theorem (**Singular value decomposition**) Let $A \in \mathbb{C}^{m\times n}$ be a complex matrix, then there exist unitary matrices $U \in \mathbb{C}^{m\times m}$ and $V \in \mathbb{C}^{n\times n}$ as well as non-negative real numbers $\sigma_1, \dots, \sigma_k$, $k = \min(m,n)$, with $\sigma_1 \geq \dots \geq \sigma_k \geq 0$ (denoted singular values) such that

$$A = USV^\dagger,$$

where S is the $m \times n$ "diagonal" matrix with diagonal entries $(\sigma_i)_{i=1,\dots,k}$ and zeros otherwise.

Remarks:

- The singular value decomposition also works for real (instead of complex) matrices, in which case U and V are likewise real.
- The singular value decomposition exists for any matrix A, i.e., there are no requirements on A.
- When denoting the column vectors of U by $|u_i\rangle_{i=1,\dots,m}$ such that $U = \big(u_1|u_2|\cdots|u_m\big)$, and the column vectors of V by $|v_i\rangle_{i=1,\dots,n}$ such that $V = \big(v_1|v_2|\cdots|v_n\big)$, then $A = USV^\dagger$ can be written as

$$A = \sum_{i=1}^{k} \sigma_i \, |u_i\rangle \langle v_i| \,.$$

To derive the Schmidt decomposition, let $|a_j\rangle_{j=1,\dots,m}$ and $|b_\ell\rangle_{\ell=1,\dots,n}$ be orthonormal bases for systems A and B, respectively. Then $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{j=1}^{m}\sum_{\ell=1}^{n} c_{j\ell} \, |a_j\rangle \, |b_\ell\rangle$$

for some complex matrix $C = (c_{j\ell}) \in \mathbb{C}^{m\times n}$. By the singular value decomposition, $C = USV^\dagger$ with U, V, S as described above and the diagonal entries of S the singular values (σ_i). Thus

$$|\psi\rangle = \sum_{i,j,\ell} u_{ji} \, \sigma_i \, v_{\ell i}^* \, |a_j\rangle \, |b_\ell\rangle \,.$$

Defining $|i_{\mathsf{A}}\rangle = \sum_{j=1}^{m} u_{ji} \, |a_j\rangle$, $|i_{\mathsf{B}}\rangle = \sum_{\ell=1}^{n} v_{\ell i}^* \, |b_\ell\rangle$ and $\lambda_i = \sigma_i$ for $i = 1, \dots, k$ results in

$$|\psi\rangle = \sum_{i=1}^{k} \lambda_i \, |i_{\mathsf{A}}\rangle \, |i_{\mathsf{B}}\rangle \,.$$

Since U and V are unitary and $|a_j\rangle$, $|b_\ell\rangle$ orthonormal bases, the states $|i_{\mathsf{A}}\rangle$ and $|i_{\mathsf{B}}\rangle$ are likewise orthonormal. The property $\sum_{i=1}^{k} \lambda_i^2 = 1$ expresses the normalization of $|\psi\rangle$.

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Section 2.5

(b) Inserting the Schmidt decomposition into $\rho = |\psi\rangle\langle\psi|$ gives

$$\rho = \sum_{i,j=1}^{k} \lambda_i \, \lambda_j \, |i_{\mathsf{A}}\rangle \, |i_{\mathsf{B}}\rangle \, \langle j_{\mathsf{A}}| \, \langle j_{\mathsf{B}}| \, .$$

The reduced density matrices are then

$$\rho^{\mathsf{A}} = \mathrm{tr}_{\mathsf{B}}[\rho] = \sum_{i,j=1}^{k} \lambda_i \, \lambda_j \, |i_{\mathsf{A}}\rangle \, \langle j_{\mathsf{A}}| \underbrace{\langle j_{\mathsf{B}}|i_{\mathsf{B}}\rangle}_{\delta_{ij}} = \sum_{i=1}^{k} \lambda_i^2 \, |i_{\mathsf{A}}\rangle \, \langle i_{\mathsf{A}}| \, ,$$

and analogously

$$\rho^{\mathsf{B}} = \mathrm{tr}_{\mathsf{A}}[\rho] = \sum_{i=1}^{k} \lambda_i^2 \, |i_{\mathsf{B}}\rangle \, \langle i_{\mathsf{B}}| \, .$$

Since $|i_{\mathsf{A}}\rangle$ and $|i_{\mathsf{B}}\rangle$ are orthonormal, we have found the spectral decompositions of ρ^{A} and ρ^{B} with eigenvalues λ_i^2 in both cases.

(c) By the spectral decomposition of ρ^{A}, there exist orthonormal eigenvectors $|\varphi_i\rangle_{i=1,\dots,k}$ and corresponding non-negative eigenvalues p_i such that $\rho^{\mathsf{A}} = \sum_{i=1}^{k} p_i \, |\varphi_i\rangle \, \langle\varphi_i|$, where k denotes the dimension of A. Introduce a system R with the same dimension k and orthonormal basis states $|\chi_i\rangle_{i=1,\dots,k}$, and define the following state on the combined system:

$$|\psi\rangle = \sum_{i=1}^{k} \sqrt{p_i} \, |\varphi_i\rangle \, |\chi_i\rangle \, .$$

As in the calculation in part (b), one obtains

$$\mathrm{tr}_{\mathsf{R}}[|\psi\rangle \, \langle\psi|] = \sum_{i=1}^{k} p_i \, |\varphi_i\rangle \, \langle\varphi_i| = \rho^{\mathsf{A}},$$

as required.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 12.1 (Schmidt decomposition and entanglement entropy)
As in tutorial 12, let $|\psi\rangle$ be a pure state of a composite system, AB. The Schmidt decomposition of this state is denoted by $|\psi\rangle = \sum_{i=1}^{k} \sigma_i \, |i_\mathsf{A}\rangle \, |i_\mathsf{B}\rangle$.

(a) Verify that

$$\langle\psi|\psi\rangle = \sum_{i=1}^{k} \sigma_i^2.$$

In general, the *von Neumann entropy* of a density matrix ρ is defined as

$$\mathcal{S}(\rho) = -\operatorname{tr}[\rho \log(\rho)],$$

with the logarithm interpreted as matrix function, and the convention $0 \log(0) = \lim_{x\to 0} x \log(x) = 0$.

In tutorial 12 we found the reduced density matrices of the subsystems, defined as $\rho_1 = \operatorname{tr}_2[|\psi\rangle\langle\psi|]$ and $\rho_2 = \operatorname{tr}_1[|\psi\rangle\langle\psi|]$. We observed that ρ_1 and ρ_2 have the same eigenvalues $(\sigma_i^2)_{i=1,\dots,k}$. The *entanglement entropy* between the two subsystems is then given by

$$\mathcal{S}_\mathsf{ent} = \mathcal{S}(\rho_1) = \mathcal{S}(\rho_2) = -\sum_{i=1}^{k} \sigma_i^2 \log\big(\sigma_i^2\big).$$

(You should convince yourself that $\mathcal{S}(\rho_1)$ and $\mathcal{S}(\rho_2)$ are indeed equal to the sum on the right.) Intuitively, the entanglement entropy measures how strongly the subsystems are intertwined.

(b) Which sets of singular values $(\sigma_i)_{i=1,\dots,k}$ minimize and maximize the entanglement entropy, respectively, under the normalization condition $\sum_{i=1}^{k} \sigma_i^2 = 1$? ($k$ should be regarded as fixed.)
Hints: The smallest possible entanglement entropy is zero. Regarding maximization, you can take the normalization condition via a Lagrange multiplier into account.

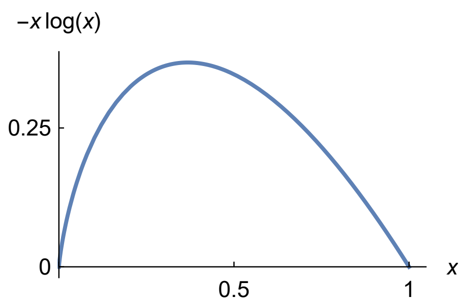
(c) Show that $\mathcal{S}_\mathsf{ent} = 0$ (completely unentangled case) implies that $|\psi\rangle$ can be written as tensor product of a state from subsystem A and one from subsystem B.

Solution

(a) Inserting the Schmidt decomposition of $|\psi\rangle$ directly leads to:

$$\langle\psi|\psi\rangle = \sum_{i,j=1}^{k} \sigma_i \sigma_j \underbrace{\langle i_A|j_A\rangle}_{\delta_{ij}} \underbrace{\langle i_B|j_B\rangle}_{\delta_{ij}} = \sum_i \sigma_i^2.$$

(b) We know that singular values are (in general) real and non-negative. Moreover, due to the normalization condition, $\sigma_i^2 \in [0,1]$ for all i. The following figure visualizes $-x\log(x)$, which is non-negative for any $x \in [0,1]$, and equal to 0 precisely if $x = 0$ or $x = 1$.



By identifying x with σ_i^2, one concludes that the entanglement entropy is non-negative. $\mathcal{S}_\mathsf{ent} = 0$ is reached by setting the first singular values to 1 and the others to 0 (which satisfies the normalization condition).

Regarding maximization of the entanglement entropy, we take the normalization constraint by a Lagrange multiplier $\lambda \in \mathbb{R}$ into account, and abbreviate $\sigma_i^2 = x_i$ for convenience:

$$\mathcal{L}(x_1, \dots, x_k, \lambda) = -\sum_{i=1}^{k} x_i \log(x_i) - \lambda \left(\sum_{i=1}^{k} x_i - 1 \right).$$

Finding an extremum of $\mathcal{L}$ by differentiation w.r.t. x_i, and using that $\log'(x) = \frac{1}{x}$ for $x > 0$, gives

$$0 \stackrel{!}{=} \frac{\partial \mathcal{L}}{\partial x_i} = -\log(x_i) - 1 - \lambda \quad \rightsquigarrow \quad x_i = e^{-1-\lambda}.$$

In particular, all x_i take the same value; combined with the normalization condition, one arrives at $x_i = \frac{1}{k}$ for all $i = 1, \dots, k$. This assignment indeed maximizes $\mathcal{L}$ since $-x\log(x)$ is concave. The corresponding singular values are $\sigma_i = \frac{1}{\sqrt{k}}$ for $i = 1, \dots, k$, and

$$\max_{\sigma_1, \dots, \sigma_k} \mathcal{S}_{\mathsf{ent}} = -\log(1/k) = \log(k).$$

(c) As already mentioned, $\mathcal{S}_{\mathsf{ent}} = 0$ is reached by setting the first singular values to 1 and the others to 0, and this is actually the only case in which $\mathcal{S}_{\mathsf{ent}} = 0$ since $-x\log(x) = 0$ implies $x = 0$ or $x = 1$. In terms of the Schmidt decomposition $|\psi\rangle = \sum_{i=1}^{k} \sigma_i |i_{\mathsf{A}}\rangle |i_{\mathsf{B}}\rangle$, only the first term remains, i.e.,

$$|\psi\rangle = |1_A\rangle |1_B\rangle$$

is a tensor product of two basis states.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: 7 February 2022, 08:00 on Moodle

Tutorial 13 (Experimentally resolving the quantum measurement process[1])

Recall from the lecture that a projective measurement is described by a Hermitian operator M. Writing its spectral decomposition as $M = \sum_m \lambda_m P_m$, where P_m is the projector onto the eigenspace of eigenvalue λ_m, the P_m's take the role of the measurement operators. If the measurement outcome is not recorded, then the overall process is represented by the quantum channel

$$\mathcal{E}_{\mathsf{proj}}(\rho) = \sum_m P_m \rho P_m.$$

In the history of quantum mechanics, the interpretation as mathematical projection onto subspaces traces back to an article by G. Lüders[2]. He concluded that the quantum superposition within an eigenspace of dimension 2 or larger "survives" the measurement process, and that two commuting observables M, $\tilde{M}$, $[M, \tilde{M}] = 0$, are "compatible" with each other, i.e., measuring M does not affect the outcome statistics of $\tilde{M}$. In this tutorial, we discuss an experimental realization [1] of such a "Lüders process" retaining the superposition. (The term "Lüders process" and "ideal measurement" refer to a projective measurement here.)

The principal quantum system is formed by three electronic states $|0\rangle$, $|1\rangle$ and $|2\rangle$ of a $^{88}Sr^+$ ion, as indicated in Fig. 1(a). Such a "qutrit" is a generalization of qubits to statevectors from $\mathbb{C}^3$. The ion has an additional short-lived excited state $|e\rangle$. In the experiment, a laser with variable power drives

$$|0\rangle \to g_0 |0\rangle + g_1 |e\rangle .$$

$|e\rangle$ quickly decays to $|0\rangle$, emitting a photon in the process: $|e\rangle |n = 0\rangle \to |0\rangle |n = 1\rangle$, where $|n\rangle$ is the quantum state of the photon environment. The (indirect) measurement process consists of the detection of the emitted photon, which indicates the occupancy of $|0\rangle$, but leaves a superposition between $|1\rangle$ and $|2\rangle$ intact. The coefficients g_0 and g_1 satisfy $|g_0|^2 + |g_1|^2 = 1$ and are used to demonstrate a transition from "no measurement" ($g_0 = 1$) to an ideal measurement ($g_0 = 0$). (In the experiment, fluorescence detection is actually only employed at the end for state tomography, but not during the measurement, i.e., one ignores the outcome.)

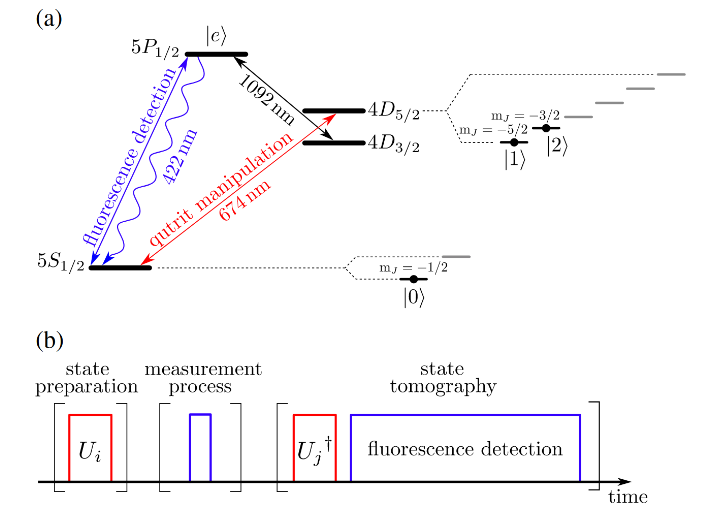


Figure 1: (a) Electronic states of the ion $^{88}Sr^+$. (b) Experimental sequence to characterize the process.

(a) The system is initialized to

$$|\psi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle) |n = 0\rangle .$$

What is the state of the system, $|\psi'\rangle$, after the excitation by the laser and $|e\rangle$ has decayed back into $|0\rangle$?

The Kraus operators which model this whole operation (i.e., the drive into $|e\rangle$ and the subsequent decay) are

$$E_0 = g_1 |0\rangle \langle 0| \quad \text{and} \quad E_1 = g_0 |0\rangle \langle 0| + |1\rangle \langle 1| + |2\rangle \langle 2| .$$

(b) Compute the reduced density matrix of the ion at the beginning of the experiment, $\rho_{\mathsf{ion}} = \mathrm{tr}_{\mathsf{env}}[|\psi\rangle \langle \psi|]$, and apply the quantum operation to ρ_{ion}.

(c) Verify that your result for (b) matches

$$\rho'_{\mathsf{ion}} = \mathrm{tr}_{\mathsf{env}}[|\psi'\rangle \langle \psi'|].$$

(d) Which measurement process corresponds to the case when $g_1 = 1$?

The experiment uses *process tomography* for characterization. A detailed explanation is beyond the scope of this tutorial; as brief summary: an additional laser (shown in red in Fig. 1) performs the initial state preparation, formally by applying a unitary matrix to $|0\rangle$. In the experiment, nine specific initial states $|\psi_i\rangle = U_i |0\rangle$ are used in different runs, corresponding to the unitaries $\{U_i\}$. Before the final fluorescence detection, the red laser realizes the action of one of the adjoint unitaries $U_j^\dagger$.

[1] F. Pokorny et al.: *Tracking the dynamics of an ideal quantum measurement*. Phys. Rev. Lett. 124, 080401 (2020)

[2] G. Lüders: *Über die Zustandsänderung durch den Meßprozeß*. Ann. Phys. 443, 322–328 (1950)

(e) Show that, in general, for a projective measurement with operators P_m, applying a unitary $U^\dagger$ beforehand changes the outcome probabilities as if using the operators $UP_mU^\dagger$.

The experiment represents the process in terms of the so-called Choi matrix, as shown in Fig. 2. As $g_0 \to 0$, the process becomes an ideal (projective) measurement.

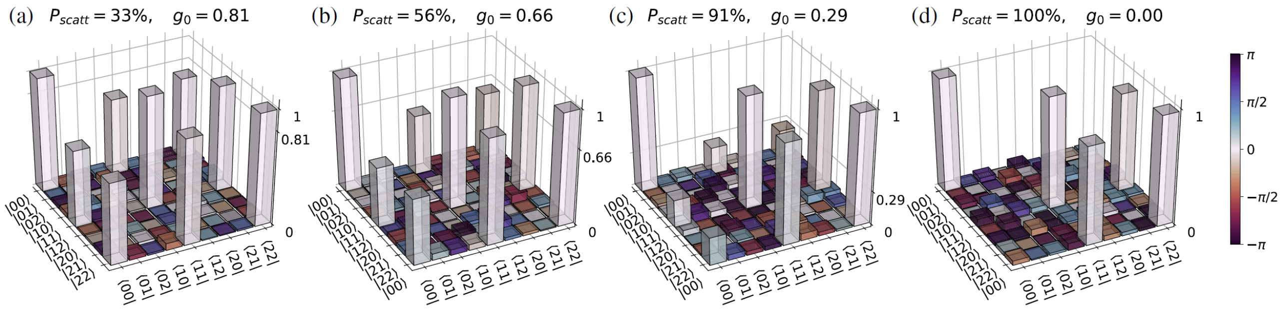
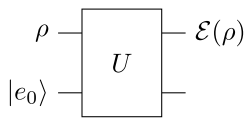


Figure 2: Choi matrices reconstructed from experimental data for different values of g_0, from [1].

(f) Which feature of the Choi matrix indicates that the superposition between $|1\rangle$ and $|2\rangle$ is preserved?

Exercise 13.1 (Quantum operations as coupling to an environment, and amplitude damping[3])
Any quantum operation can be represented by embedding the principal system into an environment, which we can assume (without loss of generality) to start in some state $|e_0\rangle$, and then applying a unitary transformation to the combined system, as illustrated in the following diagram:



From that, one obtains $\mathcal{E}(\rho)$ by "tracing out" the environment; for this purpose we first extend $|e_0\rangle$ to a basis $\{|e_k\rangle\}$ of the environment, and then compute the partial trace:

$$\mathcal{E}(\rho) = \mathrm{tr}_{\mathsf{env}}\left[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger\right] = \sum_k \langle e_k| U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger |e_k\rangle = \sum_k E_k \rho E_k^\dagger$$

with the matrix entries of E_k given by $(E_k)_{\ell,m} = \langle \ell, e_k| U |m, e_0\rangle$. The last term is the operator-sum representation of the quantum operation.

Amplitude damping models effects due to the loss of energy from a quantum system, for example by loosing a photon (elementary particle of light) from a cavity. In this case one can think of $|0\rangle$ and $|1\rangle$ as the physical system with zero or one photon, respectively. Specifically, the operator-sum representation of amplitude damping is given by

$$\mathcal{E}_{\mathsf{AD}}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger$$

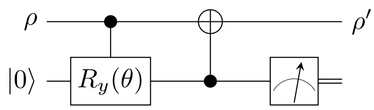
with

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}, \tag{1}$$

and a real parameter $\gamma \in [0,1]$, which one can interpret as the probability. Note that E_1 maps $|1\rangle \mapsto \sqrt{\gamma}\,|0\rangle$.

(a) Show that the operation elements $\{E_k\}$ in Eq. (1) satisfy $\sum_{k\in\{0,1\}} E_k^\dagger E_k = I$.

We now want to verify that the following circuit describes the amplitude damping operation, with $\gamma = \sin(\theta/2)^2$:



Recall that R_y is the rotation operator

$$R_y(\theta) = \mathrm{e}^{-i\theta Y/2} = \cos(\theta/2)I - i\sin(\theta/2)Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}.$$

[3] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Exercise 8.20

(b) Find the 4×4 matrix representation U_{AD} of the controlled-$R_y(\theta)$ gate followed by the flipped CNOT gate in the above circuit.

(c) Finally, read off the corresponding operation elements with entries $(E_0)_{\ell,m} = \langle \ell, 0 | U_{\mathsf{AD}} | m, 0 \rangle$ and $(E_1)_{\ell,m} = \langle \ell, 1 | U_{\mathsf{AD}} | m, 0 \rangle$, and confirm that they agree with Eq. (1).

Exercise 13.2 (Bloch sphere representation of the phase damping channel)
Phase damping models decoherence in realistic physical situations and is described by the quantum channel

$$\mathcal{E}_{\mathsf{PD}}(\rho) = \sum_{k=0}^{1} E_k \rho E_k^\dagger,$$

with operation elements

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix}$$

and "scattering" probability $\lambda \in [0, 1]$. We assume $0 < \lambda < 1$ in the following.

(a) A quantum channel $\mathcal{E}$ is called *unital* if $\mathcal{E}(I) = I$. Show that the phase damping channel is unital.

(b) Recall that an arbitrary density operator ρ for a mixed state qubit can be represented as

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

with $\vec{r} \in \mathbb{R}^3$ the *Bloch vector* of ρ and $\vec{\sigma}$ the vector of Pauli matrices. Compute the Bloch vector $\vec{r}'$ of the output state $\rho' = \mathcal{E}_{\mathsf{PD}}(\rho)$ of the phase damping channel in dependence of $\vec{r}$. Also provide a short geometric interpretation.

(c) In which case(s) does $\mathcal{E}_{\mathsf{PD}}(\rho)$ describe a pure quantum system?

(d) Compute the density matrix after n repeated applications of the phase damping operation, $\mathcal{E}_{\mathsf{PD}}(\dots\mathcal{E}_{\mathsf{PD}}(\mathcal{E}_{\mathsf{PD}}(\rho)))$, and take the limit $n \to \infty$. You may work with a symbolic 2×2 matrix representation of ρ, or its Bloch representation and part (b).

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 13 (Experimentally resolving the quantum measurement process[1])
Recall from the lecture that a projective measurement is described by a Hermitian operator M. Writing its spectral decomposition as $M = \sum_m \lambda_m P_m$, where P_m is the projector onto the eigenspace of eigenvalue λ_m, the P_m's take the role of the measurement operators. If the measurement outcome is not recorded, then the overall process is represented by the quantum channel

$$\mathcal{E}_{\mathsf{proj}}(\rho) = \sum_m P_m \rho P_m.$$

In the history of quantum mechanics, the interpretation as mathematical projection onto subspaces traces back to an article by G. Lüders[2]. He concluded that the quantum superposition within an eigenspace of dimension 2 or larger "survives" the measurement process, and that two commuting observables M, $\tilde{M}$, $[M, \tilde{M}] = 0$, are "compatible" with each other, i.e., measuring M does not affect the outcome statistics of $\tilde{M}$. In this tutorial, we discuss an experimental realization [1] of such a "Lüders process" retaining the superposition. (The term "Lüders process" and "ideal measurement" refer to a projective measurement here.)

The principal quantum system is formed by three electronic states $|0\rangle$, $|1\rangle$ and $|2\rangle$ of a $^{88}\mathsf{Sr}^+$ ion, as indicated in Fig. 1(a). Such a "qutrit" is a generalization of qubits to statevectors from $\mathbb{C}^3$. The ion has an additional short-lived excited state $|e\rangle$. In the experiment, a laser with variable power drives

$$|0\rangle \to g_0 |0\rangle + g_1 |e\rangle .$$

$|e\rangle$ quickly decays to $|0\rangle$, emitting a photon in the process: $|e\rangle |n = 0\rangle \to |0\rangle |n = 1\rangle$, where $|n\rangle$ is the quantum state of the photon environment. The (indirect) measurement process consists of the detection of the emitted photon, which indicates the occupancy of $|0\rangle$, but leaves a superposition between $|1\rangle$ and $|2\rangle$ intact. The coefficients g_0 and g_1 satisfy $|g_0|^2 + |g_1|^2 = 1$ and are used to demonstrate a transition from "no measurement" ($g_0 = 1$) to an ideal measurement ($g_0 = 0$). (In the experiment, fluorescence detection is actually only employed at the end for state tomography, but not during the measurement, i.e., one ignores the outcome.)

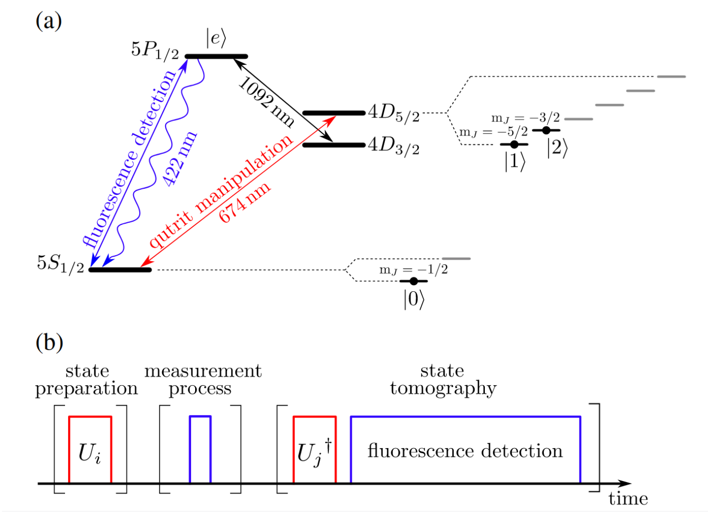


Figure 1: (a) Electronic states of the ion $^{88}\mathsf{Sr}^+$. (b) Experimental sequence to characterize the process.

(a) The system is initialized to

$$|\psi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle) |n = 0\rangle .$$

What is the state of the system, $|\psi'\rangle$, after the excitation by the laser and $|e\rangle$ has decayed back into $|0\rangle$?

The Kraus operators which model this whole operation (i.e., the drive into $|e\rangle$ and the subsequent decay) are

$$E_0 = g_1 |0\rangle \langle 0| \quad \text{and} \quad E_1 = g_0 |0\rangle \langle 0| + |1\rangle \langle 1| + |2\rangle \langle 2| .$$

(b) Compute the reduced density matrix of the ion at the beginning of the experiment, $\rho_{\mathsf{ion}} = \mathrm{tr}_{\mathsf{env}}[|\psi\rangle \langle\psi|]$, and apply the quantum operation to ρ_{ion}.

(c) Verify that your result for (b) matches

$$\rho'_{\mathsf{ion}} = \mathrm{tr}_{\mathsf{env}}[|\psi'\rangle \langle\psi'|].$$

(d) Which measurement process corresponds to the case when $g_1 = 1$?

The experiment uses *process tomography* for characterization. A detailed explanation is beyond the scope of this tutorial; as brief summary: an additional laser (shown in red in Fig. 1) performs the initial state preparation, formally by applying a unitary matrix to $|0\rangle$. In the experiment, nine specific initial states $|\psi_i\rangle = U_i |0\rangle$ are used in different runs, corresponding to the unitaries $\{U_i\}$. Before the final fluorescence detection, the red laser realizes the action of one of the adjoint unitaries $U_j^\dagger$.

[1]F. Pokorny et al.: *Tracking the dynamics of an ideal quantum measurement*. Phys. Rev. Lett. 124, 080401 (2020)
[2]G. Lüders: *Über die Zustandsänderung durch den Meßprozeß*. Ann. Phys. 443, 322–328 (1950)

(e) Show that, in general, for a projective measurement with operators P_m, applying a unitary $U^\dagger$ beforehand changes the outcome probabilities as if using the operators $UP_mU^\dagger$.

The experiment represents the process in terms of the so-called Choi matrix, as shown in Fig. 2. As $g_0 \to 0$, the process becomes an ideal (projective) measurement.

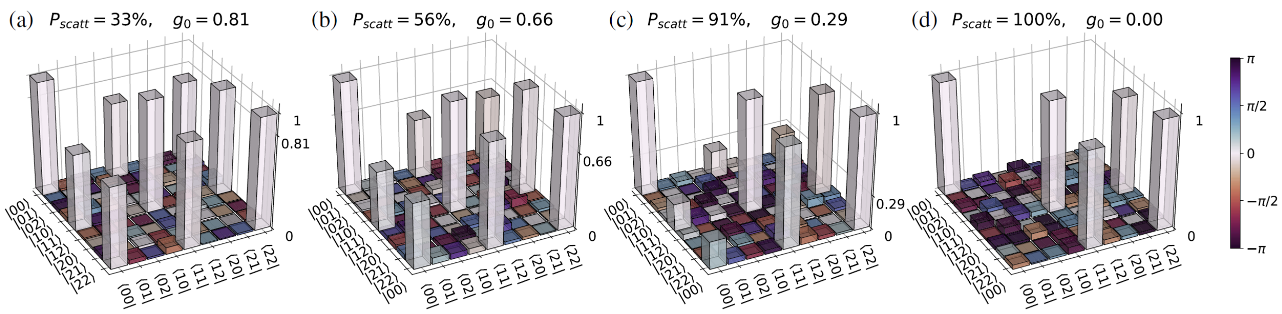


Figure 2: Choi matrices reconstructed from experimental data for different values of g_0, from [1].

(f) Which feature of the Choi matrix indicates that the superposition between $|1\rangle$ and $|2\rangle$ is preserved?

Solution

(a) Right after the excitation has happened, the state of the system is

$$(\alpha_0 g_0 |0\rangle + \alpha_0 g_1 |e\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle) |n = 0\rangle .$$

After the decay, this becomes

$$|\psi'\rangle = (\alpha_0 g_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle) |n = 0\rangle + \alpha_0 g_1 |0\rangle |n = 1\rangle .$$

(b) Initially the ion and the environment are unentangled, so we can directly read off the density matrix

$$\rho_{\text{ion}} = (\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle)(\alpha_0^* \langle 0| + \alpha_1^* \langle 1| + \alpha_2^* \langle 2|) = \begin{pmatrix} |\alpha_0|^2 & \alpha_0\alpha_1^* & \alpha_0\alpha_2^* \\ \alpha_1\alpha_0^* & |\alpha_1|^2 & \alpha_1\alpha_2^* \\ \alpha_2\alpha_0^* & \alpha_2\alpha_1^* & |\alpha_2|^2 \end{pmatrix} .$$

The overall quantum operation is

$$\mathcal{E}(\rho_{\text{ion}}) = \sum_k E_k \rho_{\text{ion}} E_k^\dagger .$$

Here

$$E_0\rho_{\text{ion}}E_0^\dagger = \begin{pmatrix} g_1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} |\alpha_0|^2 & \alpha_0\alpha_1^* & \alpha_0\alpha_2^* \\ \alpha_1\alpha_0^* & |\alpha_1|^2 & \alpha_1\alpha_2^* \\ \alpha_2\alpha_0^* & \alpha_2\alpha_1^* & |\alpha_2|^2 \end{pmatrix} \begin{pmatrix} g_1^* & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} |g_1|^2|\alpha_0|^2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

and

$$\begin{aligned} E_1\rho_{\text{ion}}E_1^\dagger &= \begin{pmatrix} g_0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} |\alpha_0|^2 & \alpha_0\alpha_1^* & \alpha_0\alpha_2^* \\ \alpha_1\alpha_0^* & |\alpha_1|^2 & \alpha_1\alpha_2^* \\ \alpha_2\alpha_0^* & \alpha_2\alpha_1^* & |\alpha_2|^2 \end{pmatrix} \begin{pmatrix} g_0^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} |g_0|^2|\alpha_0|^2 & g_0\alpha_0\alpha_1^* & g_0\alpha_0\alpha_2^* \\ g_0^*\alpha_1\alpha_0^* & |\alpha_1|^2 & \alpha_1\alpha_2^* \\ g_0^*\alpha_2\alpha_0^* & \alpha_2\alpha_1^* & |\alpha_2|^2 \end{pmatrix} . \end{aligned}$$

Adding both of these matrices, and using the fact that $|g_0|^2 + |g_1|^2 = 1$, we obtain

$$\mathcal{E}(\rho_{\text{ion}}) = \begin{pmatrix} |\alpha_0|^2 & g_0\alpha_0\alpha_1^* & g_0\alpha_0\alpha_2^* \\ g_0^*\alpha_1\alpha_0^* & |\alpha_1|^2 & \alpha_1\alpha_2^* \\ g_0^*\alpha_2\alpha_0^* & \alpha_2\alpha_1^* & |\alpha_2|^2 \end{pmatrix} .$$

(c) We trace out the environment by

$$\rho'_{\mathsf{ion}} = \sum_{i=0}^{1} \langle n = i|\psi'\rangle \langle\psi'|n = i\rangle .$$

Note that

$$\langle n = 0|\psi'\rangle = (\alpha_0 g_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle)$$

and

$$\langle n = 1|\psi'\rangle = \alpha_0 g_1 |0\rangle .$$

This leads us to

$$\rho'_{\mathsf{ion}} = \begin{pmatrix} |\alpha_0|^2 & g_0\alpha_0\alpha_1^* & g_0\alpha_0\alpha_2^* \\ g_0^*\alpha_1\alpha_0^* & |\alpha_1|^2 & \alpha_1\alpha_2^* \\ g_0^*\alpha_2\alpha_0^* & \alpha_2\alpha_1^* & |\alpha_2|^2 \end{pmatrix}$$

as in the previous section.

(d) When $g_1 = 1$, $g_0 = 0$ and therefore the Kraus operators are $E_0 = |0\rangle\langle 0|$ and $E_1 = I - |0\rangle\langle 0| = |1\rangle\langle 1| + |2\rangle\langle 2|$, i.e., this process is a projective measurement into the space spanned by $|0\rangle$ and its orthogonal complement.

(e) Denoting the quantum state before the measurement by $|\psi\rangle$, outcome m occurs with probability

$$p(m) = \langle\psi| P_m |\psi\rangle .$$

(Note that $P_m^2 = P_m$ by definition of a projection operator.) Applying $U^\dagger$ beforehand changes the probability to

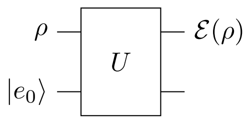
$$\tilde{p}(m) = \langle\psi| U P_m U^\dagger |\psi\rangle = \langle\psi| \tilde{P}_m |\psi\rangle$$

with $\tilde{P}_m = U P_m U^\dagger$.

(f) These are the four columns corresponding to $(|11\rangle + |22\rangle)(\langle 11| + \langle 22|)$.

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 13.1 (Quantum operations as coupling to an environment, and amplitude damping[1])
Any quantum operation can be represented by embedding the principal system into an environment, which we can assume (without loss of generality) to start in some state $|e_0\rangle$, and then applying a unitary transformation to the combined system, as illustrated in the following diagram:



From that, one obtains $\mathcal{E}(\rho)$ by "tracing out" the environment; for this purpose we first extend $|e_0\rangle$ to a basis $\{|e_k\rangle\}$ of the environment, and then compute the partial trace:

$$\mathcal{E}(\rho) = \mathrm{tr}_{\mathsf{env}}\left[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger\right] = \sum_k \langle e_k| U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger |e_k\rangle = \sum_k E_k \rho E_k^\dagger$$

with the matrix entries of E_k given by $(E_k)_{\ell,m} = \langle \ell, e_k| U |m, e_0\rangle$. The last term is the operator-sum representation of the quantum operation.

Amplitude damping models effects due to the loss of energy from a quantum system, for example by loosing a photon (elementary particle of light) from a cavity. In this case one can think of $|0\rangle$ and $|1\rangle$ as the physical system with zero or one photon, respectively. Specifically, the operator-sum representation of amplitude damping is given by

$$\mathcal{E}_{\mathsf{AD}}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger$$

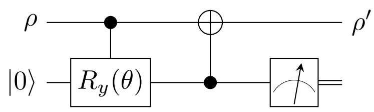
with

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}, \tag{1}$$

and a real parameter $\gamma \in [0,1]$, which one can interpret as the probability. Note that E_1 maps $|1\rangle \mapsto \sqrt{\gamma}\,|0\rangle$.

(a) Show that the operation elements $\{E_k\}$ in Eq. (1) satisfy $\sum_{k\in\{0,1\}} E_k^\dagger E_k = I$.

We now want to verify that the following circuit describes the amplitude damping operation, with $\gamma = \sin(\theta/2)^2$:



Recall that R_y is the rotation operator

$$R_y(\theta) = \mathrm{e}^{-i\theta Y/2} = \cos(\theta/2)I - i\sin(\theta/2)Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}.$$

(b) Find the 4×4 matrix representation U_{AD} of the controlled-$R_y(\theta)$ gate followed by the flipped CNOT gate in the above circuit.

(c) Finally, read off the corresponding operation elements with entries $(E_0)_{\ell,m} = \langle \ell, 0| U_{\mathsf{AD}} |m, 0\rangle$ and $(E_1)_{\ell,m} = \langle \ell, 1| U_{\mathsf{AD}} |m, 0\rangle$, and confirm that they agree with Eq. (1).

Solution

(a) Since γ is real, complex conjugation does not change γ, and thus

$$\sum_{k\in\{0,1\}} E_k^\dagger E_k = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{pmatrix}\begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1-\gamma \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix} = I.$$

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Exercise 8.20

(b) The controlled-$R_y(\theta)$ gate has the following matrix representation with respect to the standard computational basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$,

$$U_{\text{controlled-}R_y(\theta)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ 0 & 0 & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},$$

and the flipped-CNOT gate

$$U_{\text{flipped-CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Multiplying these two matrices (in the correct order!) gives U_{AD}:

$$U_{\text{AD}} = U_{\text{flipped-CNOT}} \cdot U_{\text{controlled-}R_y(\theta)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \\ 0 & 0 & \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

(c) E_0 and E_1 are submatrices of U_{AD}:

$$E_0 = \begin{pmatrix} \langle 00| U_{\text{AD}} |00\rangle & \langle 00| U_{\text{AD}} |10\rangle \\ \langle 10| U_{\text{AD}} |00\rangle & \langle 10| U_{\text{AD}} |10\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \cos\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix},$$
$$E_1 = \begin{pmatrix} \langle 01| U_{\text{AD}} |00\rangle & \langle 01| U_{\text{AD}} |10\rangle \\ \langle 11| U_{\text{AD}} |00\rangle & \langle 11| U_{\text{AD}} |10\rangle \end{pmatrix} = \begin{pmatrix} 0 & \sin\frac{\theta}{2} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix},$$

in agreement with Eq. (1).

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 13.2 (Bloch sphere representation of the phase damping channel)
Phase damping models decoherence in realistic physical situations and is described by the quantum channel

$$\mathcal{E}_{\mathsf{PD}}(\rho) = \sum_{k=0}^{1} E_k \rho E_k^\dagger,$$

with operation elements

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix}$$

and "scattering" probability $\lambda \in [0,1]$. We assume $0 < \lambda < 1$ in the following.

(a) A quantum channel $\mathcal{E}$ is called *unital* if $\mathcal{E}(I) = I$. Show that the phase damping channel is unital.

(b) Recall that an arbitrary density operator ρ for a mixed state qubit can be represented as

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

with $\vec{r} \in \mathbb{R}^3$ the *Bloch vector* of ρ and $\vec{\sigma}$ the vector of Pauli matrices. Compute the Bloch vector $\vec{r}'$ of the output state $\rho' = \mathcal{E}_{\mathsf{PD}}(\rho)$ of the phase damping channel in dependence of $\vec{r}$. Also provide a short geometric interpretation.

(c) In which case(s) does $\mathcal{E}_{\mathsf{PD}}(\rho)$ describe a pure quantum system?

(d) Compute the density matrix after n repeated applications of the phase damping operation, $\mathcal{E}_{\mathsf{PD}}(\dots\mathcal{E}_{\mathsf{PD}}(\mathcal{E}_{\mathsf{PD}}(\rho)))$, and take the limit $n \to \infty$. You may work with a symbolic 2×2 matrix representation of ρ, or its Bloch representation and part (b).

Solution

(a) Since $\lambda \in (0,1)$, $\sqrt{1-\lambda}$ and $\sqrt{\lambda}$ are both real numbers. Inserting the identity matrix leads directly to

$$\mathcal{E}_{\mathsf{PD}}(I) = E_0 E_0^\dagger + E_1 E_1^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & 1-\lambda \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

(b) We first note that

$$\begin{aligned} E_0 X E_0^\dagger &= \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix} = \sqrt{1-\lambda}\, X, \\ E_1 X E_1^\dagger &= \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix} = 0 \quad \text{(zero matrix)}, \end{aligned}$$

and similarly $E_0 Y E_0^\dagger = \sqrt{1-\lambda}\, Y$ and $E_1 Y E_1^\dagger = 0$. Analogous to (a), one computes that $\mathcal{E}(Z) = Z$. Now inserting the Bloch representation of ρ with $\vec{r} = (r_1, r_2, r_3)$ leads to

$$\mathcal{E}_{\mathsf{PD}}(\rho) = \frac{1}{2}\left(\mathcal{E}_{\mathsf{PD}}(I) + \sum_{\alpha=1}^{3} r_\alpha\, \mathcal{E}_{\mathsf{PD}}(\sigma_\alpha)\right) = \frac{1}{2}\left(I + \sqrt{1-\lambda}\, r_1\, X + \sqrt{1-\lambda}\, r_2\, Y + r_3\, Z\right) = \frac{I + \vec{r}' \cdot \vec{\sigma}}{2}$$

with $\vec{r}' = (\sqrt{1-\lambda}\, r_1, \sqrt{1-\lambda}\, r_2, r_3)$.

Thus the x- and y-components of $\vec{r}$ shrink by the factor $\sqrt{1-\lambda}$, while the z-component does not change. In other words, the Bloch vector approaches its projection onto the z-axis.

(c) The Bloch vector $\vec{r}$ of any density matrix ρ satisfies $\|\vec{r}\| \le 1$, with equality if and only if ρ describes a pure state (see exercise 11.2). According to (b), the quantum channel $\mathcal{E}_{\mathsf{PD}}$ scales the first and second entry of the input Bloch vector $\vec{r}$ by the factor $\sqrt{1-\lambda} < 1$. Thus the Bloch vector $\vec{r}'$ of $\mathcal{E}_{\mathsf{PD}}(\rho)$ has unit length, $\|\vec{r}'\| = 1$, precisely if $\vec{r}' = \vec{r} = (0, 0, \pm 1)$ (north or south pole of the Bloch sphere). The corresponding density matrices for these cases are $\rho = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $\rho = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, describing a quantum system in state $|0\rangle$ and $|1\rangle$, respectively.

(d) According to (b), the Bloch vector after n repeated applications of the channel is equal to

$$\left(\sqrt{1-\lambda}^{\,n} r_1, \sqrt{1-\lambda}^{\,n} r_2, r_3\right) \overset{n\to\infty}{\to} (0, 0, r_3)$$

since $\sqrt{1-\lambda} < 1$ by assumption. The matrix representation of the limiting density matrix is thus

$$\rho^{(\infty)} = \frac{1}{2}\begin{pmatrix} 1+r_3 & 0 \\ 0 & 1-r_3 \end{pmatrix},$$

that is, the phase damping channel "damps" the off-diagonal entries to zero.

Note: physically, $\rho^{(\infty)}$ represents a (classical) ensemble of the basis states $|0\rangle$ and $|1\rangle$, without any quantum superposition of these states.