University of Oslo

FYS3415/FYS4415 — Quantum computing and quantum information

Problem set 1

This problem set will be discussed in the group exercise session on **Jan. 28**.

Problem 1: Trace and Pauli identities (J. Gulla, O. Leinonen)

Throughout this problem we work in the computational basis $\{|0\rangle, |1\rangle\}$ and use

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1}$$

You may use that the trace is cyclic, $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, as we proved in the lectures.

a) Trace of Pauli matrices. Compute $\mathrm{Tr}(\mathbb{1})$ and show that $\mathrm{Tr}(\sigma_x) = \mathrm{Tr}(\sigma_y) = \mathrm{Tr}(\sigma_z) = 0$.

Solution: The trace is the sum of diagonal entries:

$$\mathrm{Tr}(\mathbb{1}) = 1 + 1 = 2. \tag{2}$$

For the Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3}$$

we get

$$\mathrm{Tr}(\sigma_x) = 0, \qquad \mathrm{Tr}(\sigma_y) = 0, \qquad \mathrm{Tr}(\sigma_z) = 1 + (-1) = 0. \tag{4}$$

b) Linearity. Let A, B be arbitrary matrices and $a, b \in \mathbb{C}$. Show that

$$\mathrm{Tr}(aA + bB) = a\ \mathrm{Tr}(A) + b\ \mathrm{Tr}(B). \tag{5}$$

Solution: Using $\mathrm{Tr}(X) = \sum_i \langle i|X\,|i\rangle$,

$$\mathrm{Tr}(aA + bB) = \sum_i \langle i|(aA + bB)\,|i\rangle = a\sum_i \langle i|A\,|i\rangle + b\sum_i \langle i|B\,|i\rangle = a\ \mathrm{Tr}(A) + b\ \mathrm{Tr}(B). \tag{6}$$

c) Outer products in the trace. Let $|\phi\rangle, |\psi\rangle$ be vectors.

(i) Show that $\mathrm{Tr}(|\phi\rangle\langle\psi|) = \langle\psi|\phi\rangle$.

(ii) Show that for any matrix A, we have $\mathrm{Tr}(A\,|\phi\rangle\langle\psi|) = \langle\psi|A\,|\phi\rangle$.

Solution:
(i) Using $\mathrm{Tr}(X) = \sum_i \langle i|X\,|i\rangle$,

$$\mathrm{Tr}(|\phi\rangle\langle\psi|) = \sum_i \langle i|\big(|\phi\rangle\langle\psi|\big)\,|i\rangle = \sum_i \langle i|\phi\rangle\,\langle\psi|i\rangle = \langle\psi|\left(\sum_i |i\rangle\langle i|\right)|\phi\rangle = \langle\psi|\phi\rangle. \tag{7}$$

(ii) Again use $\mathrm{Tr}(X) = \sum_i \langle i|X\,|i\rangle$:

$$\mathrm{Tr}(A\,|\phi\rangle\langle\psi|) = \sum_i \langle i|A\,|\phi\rangle\langle\psi|\,|i\rangle = \sum_i \langle\psi|\,|i\rangle\langle i|A\,|\phi\rangle = \langle\psi|\left(\sum_i |i\rangle\langle i|\right) A\,|\phi\rangle = \langle\psi|A\,|\phi\rangle. \tag{8}$$

d) Pauli algebra. Recall from Problem set 0 that the Pauli matrices can be written in the form:

$$\begin{aligned} \mathbb{1} &= |0\rangle\langle 0| + |1\rangle\langle 1|, \\ \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0|, \\ \sigma_y &= -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|, \\ \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1|. \end{aligned} \tag{9}$$

(i) Use these expressions to show $\sigma_i^\dagger = \sigma_i$ and $\sigma_i^2 = \mathbb{1}$ for $i \in \{x, y, z\}$.

(ii) Compute the three cyclic permutations:

$$\sigma_x\sigma_y = i\sigma_z, \qquad \sigma_y\sigma_z = i\sigma_x, \qquad \sigma_z\sigma_x = i\sigma_y. \tag{10}$$

Conclude the compact product rule

$$\sigma_i\sigma_j = \delta_{ij}\mathbb{1} + i\sum_{k\in\{x,y,z\}} \varepsilon_{ijk}\sigma_k, \qquad \text{for } i,j \in \{x,y,z\}, \tag{11}$$

where ε_{ijk} is totally antisymmetric (changes sign when any two indices are swapped and is 0 if any two indices coincide) and $\varepsilon_{xyz} = +1$. Deduce in particular that $\sigma_i\sigma_j = -\sigma_j\sigma_i$ for $i \neq j$, and that

$$[\sigma_i, \sigma_j] = 2i\sum_k \varepsilon_{ijk}\sigma_k, \qquad \{\sigma_i, \sigma_j\} = 2\delta_{ij}\mathbb{1}. \tag{12}$$

Solution:
(i) Hermiticity:

$$\begin{aligned} \sigma_x^\dagger &= (|0\rangle\langle 1|)^\dagger + (|1\rangle\langle 0|)^\dagger = |1\rangle\langle 0| + |0\rangle\langle 1| = \sigma_x, \\ \sigma_y^\dagger &= (-i\,|0\rangle\langle 1|)^\dagger + (i\,|1\rangle\langle 0|)^\dagger = i\,|1\rangle\langle 0| - i\,|0\rangle\langle 1| = \sigma_y, \end{aligned} \tag{13}$$

and $\sigma_z^\dagger = \sigma_z$ is immediate.

Compute the squares:

$$\begin{aligned} \sigma_x^2 &= (|0\rangle\langle 1| + |1\rangle\langle 0|)^2 = |0\rangle\langle 1|\;|1\rangle\langle 0| + |1\rangle\langle 0|\;|0\rangle\langle 1| = |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{1}, \\ \sigma_y^2 &= (-i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|)^2 = (-i)(i)\,|0\rangle\langle 0| + (i)(-i)\,|1\rangle\langle 1| = |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{1}, \\ \sigma_z^2 &= (|0\rangle\langle 0| - |1\rangle\langle 1|)^2 = |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{1}. \end{aligned} \tag{14}$$

(ii) Similarly, compute products:

$$\begin{aligned} \sigma_x\sigma_y &= (|0\rangle\langle 1| + |1\rangle\langle 0|)(-i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|) = i\,|0\rangle\langle 0| - i\,|1\rangle\langle 1| = i(|0\rangle\langle 0| - |1\rangle\langle 1|) = i\sigma_z, \\ \sigma_y\sigma_z &= (-i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|)(|0\rangle\langle 0| - |1\rangle\langle 1|) = i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0| = i\sigma_x, \\ \sigma_z\sigma_x &= (|0\rangle\langle 0| - |1\rangle\langle 1|)(|0\rangle\langle 1| + |1\rangle\langle 0|) = |0\rangle\langle 1| - |1\rangle\langle 0| = i\sigma_y. \end{aligned} \tag{15}$$

Reversing the order flips the sign (e.g. $\sigma_y\sigma_x = (\sigma_x\sigma_y)^\dagger = -i\sigma_z$), so $\sigma_i\sigma_j = -\sigma_j\sigma_i$ for $i \neq j$.

The pattern is exactly

$$\sigma_i\sigma_j = \delta_{ij}\mathbb{1} + i\sum_k \varepsilon_{ijk}\sigma_k, \tag{16}$$

which implies

$$[\sigma_i,\sigma_j] = \sigma_i\sigma_j - \sigma_j\sigma_i = 2i\sum_k \varepsilon_{ijk}\sigma_k, \qquad \{\sigma_i,\sigma_j\} = \sigma_i\sigma_j + \sigma_j\sigma_i = 2\delta_{ij}\mathbb{1}. \tag{17}$$

Problem 2: Bloch sphere rotations (J. Gulla, O. Leinonen)

Throughout this problem we work in the computational basis $\{|0\rangle, |1\rangle\}$ and use $\sigma_x, \sigma_y, \sigma_z$. Consider the normalized qubit state

$$|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{e^{i\pi/3}}{2}|1\rangle = \begin{pmatrix} \sqrt{3}/2 \\ e^{i\pi/3}/2 \end{pmatrix}. \tag{18}$$

The Bloch vector of a pure state is defined by

$$\vec{r}(\psi) = \langle\psi|\vec{\sigma}\,|\psi\rangle = \big(\langle\psi|\sigma_x|\psi\rangle, \langle\psi|\sigma_y|\psi\rangle, \langle\psi|\sigma_z|\psi\rangle\big), \qquad \vec{\sigma} = (\sigma_x,\sigma_y,\sigma_z). \tag{19}$$

a) Bloch angles and vector.

(i) Explain briefly why any normalized qubit state can be written as

$$|\psi(\theta,\phi)\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \qquad \text{for } \theta\in[0,\pi],\ \phi\in[0,2\pi), \tag{20}$$

up to a global phase. Find (θ,ϕ) for (18).

(ii) Compute $\vec{r}(\theta,\phi)$ and show

$$\vec{r}(\theta,\phi) = (\sin\theta\cos\phi,\ \sin\theta\sin\phi,\ \cos\theta). \tag{21}$$

Use this to compute $\vec{r}(\psi)$ for (18), and verify that $\|\vec{r}(\psi)\| = 1$. Hint[1].

Solution:
(i) Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. Multiply by a global phase so that α becomes real and nonnegative: $\alpha \mapsto |\alpha|$. Then set $|\alpha| = \cos(\theta/2)$, $|\beta| = \sin(\theta/2)$, and define the relative phase ϕ from $\beta = e^{i\phi}|\beta|$. This gives the stated form.

For (18), $\alpha = \sqrt{3}/2 > 0$, so it is already in this gauge. We have $\cos(\theta/2) = \sqrt{3}/2 \Rightarrow \theta/2 = \pi/6 \Rightarrow \theta = \pi/3$, and $\beta = e^{i\pi/3}/2$ with $\sin(\theta/2) = 1/2$, so $\phi = \pi/3$.

(ii) With $|\psi(\theta,\phi)\rangle = \begin{pmatrix} \cos(\theta/2) \\ e^{i\phi}\sin(\theta/2) \end{pmatrix}$, we compute $r_i = \langle\psi|\sigma_i|\psi\rangle$:

$$\begin{aligned} r_x &= \langle\psi|\sigma_x|\psi\rangle = \cos\frac{\theta}{2}\,e^{i\phi}\sin\frac{\theta}{2} + e^{-i\phi}\sin\frac{\theta}{2}\,\cos\frac{\theta}{2} = 2\cos\frac{\theta}{2}\sin\frac{\theta}{2}\cos\phi = \sin\theta\cos\phi, \\ r_y &= \langle\psi|\sigma_y|\psi\rangle = -i\cos\frac{\theta}{2}\,e^{i\phi}\sin\frac{\theta}{2} + ie^{-i\phi}\sin\frac{\theta}{2}\,\cos\frac{\theta}{2} = 2\cos\frac{\theta}{2}\sin\frac{\theta}{2}\sin\phi = \sin\theta\sin\phi, \\ r_z &= \langle\psi|\sigma_z|\psi\rangle = \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} = \cos\theta. \end{aligned} \tag{22}$$

[1] Use $e^{i\phi} + e^{-i\phi} = 2\cos\phi$ and $e^{i\phi} - e^{-i\phi} = 2i\sin\phi$, and the double-angle identities $2\cos(\theta/2)\sin(\theta/2) = \sin\theta$ and $\cos^2(\theta/2) - \sin^2(\theta/2) = \cos\theta$.

Hence

$$\vec{r}(\theta,\phi) = (\sin\theta\cos\phi,\ \sin\theta\sin\phi,\ \cos\theta). \tag{23}$$

For $(\theta,\phi) = (\pi/3, \pi/3)$,

$$\vec{r}(\psi) = \left(\frac{\sqrt{3}}{4},\ \frac{3}{4},\ \frac{1}{2}\right). \tag{24}$$

Then

$$\|\vec{r}(\psi)\|^2 = \frac{3}{16} + \frac{9}{16} + \frac{1}{4} = 1, \tag{25}$$

so $\|\vec{r}(\psi)\| = 1$.

b) Rotation about x and z axes. For parameters $\alpha, \beta \in \mathbb{R}$, define

$$U_x(\alpha) = \exp\left(-i\frac{\alpha}{2}\sigma_x\right), \qquad U_z(\beta) = \exp\left(-i\frac{\beta}{2}\sigma_z\right). \tag{26}$$

(i) You may use that σ_x has eigenvectors

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \qquad \sigma_x |\pm\rangle = \pm |\pm\rangle. \tag{27}$$

Use the spectral theorem to show

$$U_x(\alpha) = e^{-i\alpha/2}\,|+\rangle\langle+| + e^{i\alpha/2}\,|-\rangle\langle-|, \tag{28}$$

and simplify this to the closed form

$$U_x(\alpha) = \cos\frac{\alpha}{2}\,\mathbb{1} - i\sin\frac{\alpha}{2}\,\sigma_x. \tag{29}$$

Write $U_x(\alpha)$ as a 2×2 matrix in the computational basis.

(ii) Show directly, using that σ_z is diagonal, that

$$U_z(\beta) = \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} = \cos\frac{\beta}{2}\,\mathbb{1} - i\sin\frac{\beta}{2}\,\sigma_z. \tag{30}$$

Solution:
(i) The spectral theorem says that if an operator A has an orthonormal eigenbasis $\{|v_k\rangle\}$ with eigenvalues λ_k, then we can define operator functions of A as

$$f(A) = \sum_k f(\lambda_k)\ |v_k\rangle\langle v_k|. \tag{31}$$

The Pauli matrices are Hermitian, and thus normal, meaning that they have an orthonormal eigenbasis. Here $\sigma_x |\pm\rangle = \pm|\pm\rangle$, so the eigenvalues are ± 1 and the spectral theorem gives

$$U_x(\alpha) = \exp\left(-i\frac{\alpha}{2}\sigma_x\right) = e^{-i\alpha/2}\,|+\rangle\langle+| + e^{i\alpha/2}\,|-\rangle\langle-|. \tag{32}$$

To simplify, compute the projectors explicitly in the computational basis. Using

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \qquad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}, \tag{33}$$

we get

$$|+\rangle\langle+| = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}, \qquad |-\rangle\langle-| = \frac{1}{2}\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}. \tag{34}$$

Therefore

$$\begin{aligned} U_x(\alpha) &= \frac{1}{2}\left(e^{-i\alpha/2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} + e^{i\alpha/2}\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\right) \\ &= \frac{1}{2}\begin{pmatrix}e^{-i\alpha/2}+e^{i\alpha/2} & e^{-i\alpha/2}-e^{i\alpha/2}\\ e^{-i\alpha/2}-e^{i\alpha/2} & e^{-i\alpha/2}+e^{i\alpha/2}\end{pmatrix} \\ &= \begin{pmatrix}\cos(\alpha/2) & -i\sin(\alpha/2)\\ -i\sin(\alpha/2) & \cos(\alpha/2)\end{pmatrix}. \end{aligned} \tag{35}$$

Finally, since

$$\cos\frac{\alpha}{2}\,\mathbb{1} - i\sin\frac{\alpha}{2}\,\sigma_x = \begin{pmatrix}\cos(\alpha/2) & -i\sin(\alpha/2)\\ -i\sin(\alpha/2) & \cos(\alpha/2)\end{pmatrix}, \tag{36}$$

we have shown the required form.

$$U_x(\alpha) = \cos\frac{\alpha}{2}\,\mathbb{1} - i\sin\frac{\alpha}{2}\,\sigma_x. \tag{37}$$

(ii) Since $\sigma_z = \mathrm{diag}(1,-1)$,

$$U_z(\beta) = \exp\left(-i\frac{\beta}{2}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right) = \begin{pmatrix}e^{-i\beta/2} & 0\\ 0 & e^{i\beta/2}\end{pmatrix}. \tag{38}$$

Also,

$$\cos\frac{\beta}{2}\,\mathbb{1} - i\sin\frac{\beta}{2}\,\sigma_z = \begin{pmatrix}\cos(\beta/2) - i\sin(\beta/2) & 0\\ 0 & \cos(\beta/2) + i\sin(\beta/2)\end{pmatrix} = \begin{pmatrix}e^{-i\beta/2} & 0\\ 0 & e^{i\beta/2}\end{pmatrix}. \tag{39}$$

c) Rotation about an arbitrary axis. Let $\hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ be a unit vector and define

$$\sigma_{\hat{n}} = \hat{n}\cdot\vec{\sigma} = n_x\sigma_x + n_y\sigma_y + n_z\sigma_z. \tag{40}$$

Show that $\sigma_{\hat{n}}$ is Hermitian and that $\sigma_{\hat{n}}^2 = \mathbb{1}$. Using the power-series definition of the exponential, show that

$$U(\hat{n},\alpha) = \exp\left(-i\frac{\alpha}{2}\sigma_{\hat{n}}\right) = \cos\frac{\alpha}{2}\,\mathbb{1} - i\sin\frac{\alpha}{2}\,\sigma_{\hat{n}}. \tag{41}$$

Show that $U(\hat{n},\alpha)$ is unitary. Hint[2].

Solution: Since $n_x, n_y, n_z \in \mathbb{R}$ and each Pauli matrix is Hermitian, we have $\sigma_{\hat{n}}^\dagger = (n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)^\dagger = n_x\sigma_x + n_y\sigma_y + n_z\sigma_z = \sigma_{\hat{n}}$.

To compute $\sigma_{\hat{n}}^2$, expand:

$$\sigma_{\hat{n}}^2 = (n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)^2 = \sum_i n_i^2\sigma_i^2 + \sum_{i\neq j} n_i n_j \sigma_i\sigma_j. \tag{42}$$

Since $\sigma_i^2 = \mathbb{1}$, the first sum gives $(n_x^2 + n_y^2 + n_z^2)\mathbb{1} = \mathbb{1}$ because $\hat{n}$ is a unit vector. For $i \neq j$ the Pauli matrices anticommute, so $\sigma_i\sigma_j = -\sigma_j\sigma_i$ and the cross terms cancel in pairs:

$$n_i n_j \sigma_i\sigma_j + n_j n_i \sigma_j\sigma_i = n_i n_j(\sigma_i\sigma_j + \sigma_j\sigma_i) = 0. \tag{43}$$

[2] Use the properties of the Pauli matrices found in Problem 1. Expand $(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)^2$ and see that cross terms cancel in pairs because $\sigma_i\sigma_j + \sigma_j\sigma_i = 0$ for $i \neq j$. For the power series, split it into even and odd powers.

Hence $\sigma_{\hat{n}}^2 = \mathbb{1}$.

Now use the power series:

$$e^{-i\alpha\sigma_{\hat{n}}/2} = \sum_{m=0}^{\infty} \frac{1}{m!} \left(-i\frac{\alpha}{2}\sigma_{\hat{n}}\right)^m. \tag{44}$$

Because $\sigma_{\hat{n}}^2 = \mathbb{1}$, we have $\sigma_{\hat{n}}^{2m} = \mathbb{1}$ and $\sigma_{\hat{n}}^{2m+1} = \sigma_{\hat{n}}$, so

$$\begin{aligned} e^{-i\alpha\sigma_{\hat{n}}/2} &= \sum_{m=0}^{\infty} \frac{1}{(2m)!} \left(-i\frac{\alpha}{2}\right)^{2m} \mathbb{1} + \sum_{m=0}^{\infty} \frac{1}{(2m+1)!} \left(-i\frac{\alpha}{2}\right)^{2m+1} \sigma_{\hat{n}} \\ &= \cos\frac{\alpha}{2}\,\mathbb{1} - i\sin\frac{\alpha}{2}\,\sigma_{\hat{n}}. \end{aligned} \tag{45}$$

Finally, using $\sigma_{\hat{n}}^\dagger = \sigma_{\hat{n}}$, the adjoint of the closed form is

$$U^\dagger(\hat{n},\alpha) = \cos\frac{\alpha}{2}\,\mathbb{1} + i\sin\frac{\alpha}{2}\,\sigma_{\hat{n}}. \tag{46}$$

Multiply and use $\sigma_{\hat{n}}^2 = \mathbb{1}$:

$$U^\dagger(\hat{n},\alpha)U(\hat{n},\alpha) = \left(\cos^2\frac{\alpha}{2} + \sin^2\frac{\alpha}{2}\right)\mathbb{1} = \mathbb{1}, \tag{47}$$

so $U(\hat{n},\alpha)$ is unitary.

d) z rotations shift ϕ. Let

$$U_z(\beta) = e^{-i\beta\sigma_z/2} \qquad \text{and} \qquad |\psi(\theta,\phi)\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle. \tag{48}$$

(i) Show that

$$U_z(\beta)\,|\psi(\theta,\phi)\rangle \sim |\psi(\theta,\phi+\beta)\rangle, \tag{49}$$

where $\sim$ means equality up to a global phase.

(ii) Use this and $\vec{r}(\theta,\phi) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ to show that $U_z(\beta)$ rotates the Bloch vector about the z axis by angle β:

$$\begin{pmatrix} r_x \\ r_y \\ r_z \end{pmatrix} \mapsto R_z(\beta) \begin{pmatrix} r_x \\ r_y \\ r_z \end{pmatrix}, \qquad R_z(\beta) = \begin{pmatrix} \cos\beta & -\sin\beta & 0 \\ \sin\beta & \cos\beta & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{50}$$

Solution:
(i) From the previous subproblem,

$$U_z(\beta) = \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}. \tag{51}$$

Then

$$U_z(\beta)\,|\psi(\theta,\phi)\rangle = e^{-i\beta/2}\cos\frac{\theta}{2}\,|0\rangle + e^{i\beta/2}e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle. \tag{52}$$

Factor out the global phase $e^{-i\beta/2}$:

$$U_z(\beta)\,|\psi(\theta,\phi)\rangle \sim \cos\frac{\theta}{2}\,|0\rangle + e^{i(\phi+\beta)}\sin\frac{\theta}{2}\,|1\rangle = |\psi(\theta,\phi+\beta)\rangle. \tag{53}$$

(ii) Let $\vec{r}'$ be the Bloch vector of the state $U_z(\beta)\,|\psi(\theta,\phi)\rangle$. Since θ is unchanged and $\phi \mapsto \phi+\beta$, we get

$$\begin{aligned} r'_x &= \sin\theta\cos(\phi+\beta) = r_x\cos\beta - r_y\sin\beta,\\ r'_y &= \sin\theta\sin(\phi+\beta) = r_x\sin\beta + r_y\cos\beta,\\ r'_z &= \cos\theta = r_z. \end{aligned} \tag{54}$$

Equivalently,

$$\begin{pmatrix} r'_x\\ r'_y\\ r'_z \end{pmatrix} = R_z(\beta)\begin{pmatrix} r_x\\ r_y\\ r_z \end{pmatrix}, \qquad R_z(\beta) = \begin{pmatrix} \cos\beta & -\sin\beta & 0\\ \sin\beta & \cos\beta & 0\\ 0 & 0 & 1 \end{pmatrix}. \tag{55}$$

e) Larmor precession. Consider a spin-$\frac{1}{2}$ particle in a uniform magnetic field $\vec{B} = B\,\hat{z}$ with Hamiltonian

$$H = -\frac{\hbar\gamma}{2}\,\vec{B}\cdot\vec{\sigma} = -\frac{\hbar\omega}{2}\sigma_z, \qquad \omega = \gamma B. \tag{56}$$

Let $|\psi(t)\rangle = U(t)\,|\psi(0)\rangle$ with $U(t) = e^{-iHt/\hbar}$ and define $\vec{r}(t)$ from $|\psi(t)\rangle$.

(i) Show that

$$U(t) = e^{-iHt/\hbar} = e^{i\omega t\,\sigma_z/2} = U_z(-\omega t). \tag{57}$$

(ii) Use the previous subproblem to show that if $|\psi(0)\rangle = |\psi(\theta_0,\phi_0)\rangle$, then

$$|\psi(t)\rangle \sim |\psi(\theta_0,\phi_0-\omega t)\rangle. \tag{58}$$

Write down $(r_x(t), r_y(t), r_z(t))$ in terms of $(r_x(0), r_y(0), r_z(0))$.

(iii) Show that $\vec{r}(t)$ satisfies the Bloch equation

$$\dot{\vec{r}}(t) = -\omega\,\hat{z}\times\vec{r}(t). \tag{59}$$

Solution:
(i) Insert $H = -(\hbar\omega/2)\sigma_z$:

$$U(t) = e^{-iHt/\hbar} = \exp\!\left(-i\frac{t}{\hbar}\left(-\frac{\hbar\omega}{2}\sigma_z\right)\right) = \exp\!\left(i\frac{\omega t}{2}\sigma_z\right) = \exp\!\left(-i\frac{(-\omega t)}{2}\sigma_z\right) = U_z(-\omega t). \tag{60}$$

(ii) From the earlier result, $U_z(\beta)$ shifts $\phi \mapsto \phi+\beta$ up to a global phase. Here $\beta = -\omega t$, so

$$|\psi(t)\rangle = U_z(-\omega t)\,|\psi(\theta_0,\phi_0)\rangle \sim |\psi(\theta_0,\phi_0-\omega t)\rangle. \tag{61}$$

On the Bloch sphere this is a rotation about the z axis by angle $-\omega t$, so

$$\begin{aligned} r_x(t) &= r_x(0)\cos(\omega t) + r_y(0)\sin(\omega t),\\ r_y(t) &= -r_x(0)\sin(\omega t) + r_y(0)\cos(\omega t),\\ r_z(t) &= r_z(0). \end{aligned} \tag{62}$$

(iii) Differentiate the expressions in (ii):

$$\dot{r}_x(t) = \omega r_y(t), \qquad \dot{r}_y(t) = -\omega r_x(t), \qquad \dot{r}_z(t) = 0. \tag{63}$$

Thus

$$\dot{\vec{r}}(t) = (\omega r_y(t), -\omega r_x(t), 0) = -\omega\,\hat{z}\times\vec{r}(t), \tag{64}$$

since for $\hat{z} = (0,0,1)$ we have $\hat{z}\times\vec{r} = (-r_y, r_x, 0)$.

Problem 3: Classical computing, universality, reversibility, and dual-rail encoding (J. Gulla)

In this problem we review a few key ideas from classical circuit complexity and reversible computation, and connect them to the constraints of quantum gates (unitaries). In the last parts we also consider a simple redundancy encoding, dual-rail, to practice the viewpoint that logical information can live in a constrained subset, a code space, of a larger physical system.

We use standard Boolean notation throughout:

- Bits are elements of $\{0, 1\}$, where 0 means false and 1 means true.
- Negation is written $\overline{x}$ and corresponds to the gate $\mathrm{NOT}(x)$.
- Conjunction is written $x \wedge y$ and corresponds to $\mathrm{AND}(x, y)$.
- Disjunction is written $x \vee y$ and corresponds to $\mathrm{OR}(x, y)$.
- Exclusive OR (XOR) is written $x \oplus y$ and means addition modulo 2.

A gate set is called universal if it can be used to implement any Boolean function as a finite circuit (with wires, and with COPY or constants when allowed).

a) NAND with COPY. The NAND gate is

$$\mathrm{NAND}(x, y) = \overline{x \wedge y}. \tag{65}$$

Assume you have access to fan-out, i.e. a COPY operation, that can be applied to any bit on a wire. Show that the gate set $\{\mathrm{NAND}, \mathrm{COPY}\}$ can generate NOT, AND, and OR without using external constant inputs. Why does this imply that $\{\mathrm{NAND}, \mathrm{COPY}\}$ is universal for classical computation even though it only contains a single nontrivial gate, NAND? Hint[3].

Solution: Using COPY, we can feed the same bit into both inputs of a NAND gate.

NOT:

$$\mathrm{NAND}(x, x) = \overline{x \wedge x} = \overline{x} = \mathrm{NOT}(x). \tag{66}$$

AND: Since $\mathrm{NAND}(x, y) = \overline{x \wedge y}$,

$$\mathrm{AND}(x, y) = x \wedge y = \overline{\overline{x \wedge y}} = \mathrm{NOT}(\mathrm{NAND}(x, y)) = \mathrm{NAND}(\mathrm{NAND}(x, y), \mathrm{NAND}(x, y)). \tag{67}$$

OR: By De Morgan,

$$\mathrm{OR}(x, y) = x \vee y = \overline{\overline{x} \wedge \overline{y}} = \mathrm{NAND}(\overline{x}, \overline{y}) = \mathrm{NAND}(\mathrm{NAND}(x, x), \mathrm{NAND}(y, y)). \tag{68}$$

Thus $\{\mathrm{NAND}, \mathrm{COPY}\}$ generates $\{\mathrm{NOT}, \mathrm{AND}, \mathrm{OR}\}$. Since $\{\mathrm{NOT}, \mathrm{AND}, \mathrm{OR}\}$ is functionally complete, any Boolean function can be built from these gates, so the set is universal.

b) NAND without COPY. Now assume you do not have access to a COPY gate as a primitive operation. Do *not* use the shortcut $\mathrm{NOT}(x) = \mathrm{NAND}(x, x)$. Instead, you are allowed access to constant inputs 0 and 1 as many times as you need. Show that NAND together with constants can generate NOT, AND, and OR without using COPY. Which step is the one that uses the constant 1, and why does this again imply universality?

[3] Use De Morgan's laws: $\overline{x \wedge y} = \overline{x} \vee \overline{y}$ and $\overline{x \vee y} = \overline{x} \wedge \overline{y}$.

Solution: Since we are not allowed to use the shortcut $\mathrm{NAND}(x, x)$, we implement negation using the constant input 1.

NOT: Using $x \wedge 1 = x$,

$$\mathrm{NAND}(x, 1) = \overline{x \wedge 1} = \overline{x} = \mathrm{NOT}(x). \tag{69}$$

AND:

$$\mathrm{AND}(x, y) = x \wedge y = \overline{\overline{x \wedge y}} = \mathrm{NOT}(\mathrm{NAND}(x, y)) = \mathrm{NAND}(\mathrm{NAND}(x, y), 1). \tag{70}$$

OR: By De Morgan,

$$\mathrm{OR}(x, y) = x \vee y = \overline{\overline{x} \wedge \overline{y}} = \mathrm{NAND}(\overline{x}, \overline{y}) = \mathrm{NAND}(\mathrm{NAND}(x, 1), \mathrm{NAND}(y, 1)). \tag{71}$$

Thus, any circuit over $\{\mathrm{NOT}, \mathrm{AND}, \mathrm{OR}\}$ can be rewritten gate-by-gate using only NAND and the constants $0, 1$. Therefore, NAND together with constants is universal. The key use of constant 1 is to implement NOT; the later uses of 1 are just repeated applications of that NOT construction.

c) Reversibility.

(i) Explain briefly why quantum gates are always reversible.

(ii) Show that the classical NAND gate is irreversible, and explain why this prevents a direct implementation of NAND as a quantum gate.

Solution:
(i) Quantum gates are represented by unitary matrices U. A unitary is invertible with inverse $U^{-1} = U^\dagger$, so the map $|\psi\rangle \mapsto U\,|\psi\rangle$ is reversible. In other words, there always exists an inverse operation (the adjoint) that can reverse the action of the gate. Given an output state $|\psi'\rangle = U|\psi\rangle$, the original input state can uniquely be recovered by applying the inverse: $|\psi\rangle = U^\dagger|\psi'\rangle$.

(ii) NAND maps two input bits to one output bit:

$$(a, b) \mapsto \overline{a \wedge b}. \tag{72}$$

The truth table is

a	b	$\mathrm{NAND}(a, b)$
0	0	1
0	1	1
1	0	1
1	1	0

The gate maps 4 distinct input configurations to only 2 distinct output values, hence it is many-to-one (not injective). Specifically, three different inputs map to the output 1. It is therefore impossible to uniquely determine the input given only the output. Therefore, the NAND gate is irreversible and cannot be implemented as a unitary operator on the same number of basis states, because unitaries are bijections.

d) Toffoli simulates NAND. The Toffoli gate acts on three bits:

$$\mathrm{Toffoli}(a, b, c) = (a, b, c \oplus (a \wedge b)). \tag{73}$$

(i) Show that Toffoli is reversible by verifying $\mathrm{Toffoli}^2 = \mathbb{1}$.

(ii) Show that NAND can be simulated using Toffoli by fixing $c = 1$. What is the third output bit?

(iii) What does this imply about the relationship between classical and quantum computation?

Solution:
(i) Apply Toffoli twice:

$$(a, b, c) \mapsto (a, b, c \oplus (a \wedge b)) \mapsto (a, b, (c \oplus (a \wedge b)) \oplus (a \wedge b)). \tag{74}$$

Using the property that $x \oplus x = 0$ for any bit x, the third bit becomes:

$$(c \oplus (a \wedge b)) \oplus (a \wedge b) = c \oplus ((a \wedge b) \oplus (a \wedge b)) = c \oplus 0 = c$$

Thus, $\text{Toffoli}^2(a, b, c) = (a, b, c)$. Since applying the gate twice returns the original state, the gate is its own inverse ($U = U^{-1}$), which proves it is reversible.

(ii) If $c = 1$, the third output bit is

$$1 \oplus (a \wedge b) = \overline{a \wedge b} = \text{NAND}(a, b), \tag{75}$$

since XOR with 1 flips a bit. So the full output is $(a, b, \text{NAND}(a, b))$. The first two outputs are the unchanged inputs; they are retained to preserve reversibility. If you only care about the NAND value, these extra outputs are sometimes treated as unwanted ("garbage") bits, because they are necessary to preserve reversibility but are not part of the desired logic function output.

(iii) The NAND gate is universal for classical computation and we can simulate NAND using ancilla bits and Toffoli. The Toffoli gate is represented by a permutation, which acts on basis states as a unitary matrix. This shows that quantum computers can run reversible embeddings of classical circuits. (Note however that Toffoli alone is not a universal quantum gate set because it does not generate arbitrary superpositions/phases.)

e) Dual-rail encoding. Consider the dual-rail encoding of one logical bit into two physical bits, where valid strings have exactly one 1:

$$\widehat{0} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad \widehat{1} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{76}$$

(i) List the two invalid physical strings.

(ii) Show that a physical SWAP of the two wires implements a logical $\widehat{\text{NOT}}$ on valid codewords.

(iii) Show that any single physical bit-flip error maps a valid codeword to an invalid string. Explain briefly why this means the encoding can detect (although not correct) a single bit flip.

Solution:
(i) Valid codewords are $(0, 1)$ and $(1, 0)$. The remaining strings are invalid:

$$(0, 0), \qquad (1, 1). \tag{77}$$

(ii) SWAP exchanges the two physical bits:

$$(0, 1) \leftrightarrow (1, 0). \tag{78}$$

Thus SWAP acts as logical $\widehat{\text{NOT}}$ on codewords.

(iii) Flipping exactly one physical bit sends

$$(0,1) \mapsto (0,0) \text{ or } (1,1), \qquad (1,0) \mapsto (0,0) \text{ or } (1,1). \tag{79}$$

So any single bit flip takes a valid codeword to an invalid string, which can be detected by checking validity.

f) Logic gates on dual-rail. Assume you can apply the physical gates $\{\text{AND}, \text{OR}, \text{COPY}\}$ to the physical bits, and you can also apply physical SWAP, which acts as logical $\widehat{\text{NOT}}$ on codewords. Show that you can implement a logical $\widehat{\text{AND}}$ on encoded bits:

$$(\widehat{x}, \widehat{y}) \mapsto \widehat{x \wedge y}. \tag{80}$$

Conclude that $\widehat{\text{NOT}}$ and $\widehat{\text{AND}}$ form a universal logical gate set on the encoded bits. What does universality mean here in practice: how would you build a circuit for an arbitrary Boolean function of the *logical* bits using only operations on the *physical* bits? Hint[4].

Solution: Let $\widehat{x} = (x_0, x_1)$ and $\widehat{y} = (y_0, y_1)$ be dual-rail codewords, where x_0 is the bit on rail 0 and x_1 is the bit on rail 1 (and similarly for y). On valid codewords we have $x_1 = \overline{x_0}$ and $y_1 = \overline{y_0}$.

We want to construct $\widehat{z} = \widehat{x \wedge y}$. The truth table for logical $\widehat{\text{AND}}$ is:

- $\widehat{0}\ \widehat{\text{AND}}\ \widehat{0} = \widehat{0} \quad \Longrightarrow \quad (0,1)\ \widehat{\text{AND}}\ (0,1) \mapsto (0,1)$
- $\widehat{0}\ \widehat{\text{AND}}\ \widehat{1} = \widehat{0} \quad \Longrightarrow \quad (0,1)\ \widehat{\text{AND}}\ (1,0) \mapsto (0,1)$
- $\widehat{1}\ \widehat{\text{AND}}\ \widehat{0} = \widehat{0} \quad \Longrightarrow \quad (1,0)\ \widehat{\text{AND}}\ (0,1) \mapsto (0,1)$
- $\widehat{1}\ \widehat{\text{AND}}\ \widehat{1} = \widehat{1} \quad \Longrightarrow \quad (1,0)\ \widehat{\text{AND}}\ (1,0) \mapsto (1,0)$

We see that the first physical bit z_0 should be 1 only if $x_0 = 1$ and $y_0 = 1$. Thus, $z_0 = \text{AND}(x_0, y_0)$. The second physical bit z_1 should be 1 if $x_1 = 1$ or $y_1 = 1$. Thus, $z_1 = \text{OR}(x_1, y_1)$.

Define a circuit with output rails:

$$z_0 = \text{AND}(x_0, y_0), \qquad z_1 = \text{OR}(x_1, y_1). \tag{81}$$

Then for valid inputs,

$$z_1 = x_1 \vee y_1 = \overline{x_0} \vee \overline{y_0} = \overline{x_0 \wedge y_0} = \overline{z_0}, \tag{82}$$

where we used De Morgan's law $\overline{u \wedge v} = \overline{u} \vee \overline{v}$ in reverse. Thus (z_0, z_1) is a valid dual-rail bit, and it is exactly the dual-rail encoding of $\widehat{x \wedge y}$. Thus we can perform logical $\widehat{\text{AND}}$ on the encoded bits.

Since SWAP implements logical $\widehat{\text{NOT}}$, and $\{\text{NOT}, \text{AND}\}$ is universal for classical computation, we have universality on encoded bits. Concretely, any classical circuit on logical bits can be compiled into an encoded circuit by replacing each logical gate by its encoded implementation acting on the physical rails.

[4] Write $\widehat{x} = (x_0, x_1)$, $\widehat{y} = (y_0, y_1)$. Try $z_0 = x_0 \wedge y_0$ and use De Morgan to express $\overline{z_0}$ in terms of x_1, y_1. Find physical gates that output $z_0 = x_0 \wedge y_0$ and $z_1 = \overline{z_0}$.