Assignment 2 - QT 207

Z SHAUKAT AZIZ (22171)

20th October 2025

1 Quantum States and Entanglement

3.3.1: Entanglement of the Bell State

Exercise 3.3.1

Consider the 2-qubit state $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$. Show that this state is **entangled** by proving that there are no possible values $\alpha_0, \alpha_1, \beta_0, \beta_1$ such that:

$$|\psi\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_0|0\rangle + \beta_1|1\rangle).$$

Solution

For $|\psi\rangle$ to be a product state, we must be able to equate the coefficients of the computational basis states in the expansion of the product state to the given state:

$$(\alpha_0\beta_0)|00\rangle + (\alpha_0\beta_1)|01\rangle + (\alpha_1\beta_0)|10\rangle + (\alpha_1\beta_1)|11\rangle = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + 0|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Equating coefficients yields a system of four equations:

1. $\alpha_0\beta_0 = \frac{1}{\sqrt{2}}$
2. $\alpha_0\beta_1 = 0$
3. $\alpha_1\beta_0 = 0$
4. $\alpha_1\beta_1 = \frac{1}{\sqrt{2}}$

- From (1) and (4), since the Right-Hand Side is non-zero, all four coefficients $\alpha_0, \alpha_1, \beta_0, \beta_1$ must be non-zero individually.
- From (2): $\alpha_0\beta_1 = 0$. Since $\alpha_0 \neq 0$ (from Eq. 1), this requires $\beta_1 = 0$.
- From (3): $\alpha_1\beta_0 = 0$. Since $\beta_0 \neq 0$ (from Eq. 1), this requires $\alpha_1 = 0$.

Substituting $\alpha_1 = 0$ and $\beta_1 = 0$ into (4) gives:

$$\alpha_1\beta_1 = (0)(0) = 0$$

The system of equations is incosistent and does not satisfy all four equations simultaneously. Thus, there are no values of $\alpha_0, \alpha_1, \beta_0, \beta_1$ that satisfy the equations. $\implies$ the state $|\psi\rangle$ is **entangled**. i.e cannot be written as a product state.

Exercise 3.4.1: Properties of Projectors and State Decomposition

Exercise 3.4.1 (a)

Prove that if the operators P_i satisfy $P_i^\dagger = P_i$ (Hermitian) and $P_i^2 = P_i$ (Projector), then $P_iP_j = 0$ for all $i \neq j$. (Assume $\sum_k P_k = I$).

Solution

We assume the set of projectors $\{P_k\}$ forms a **complete** measurement, meaning the identity operator I can be decomposed as $I = \sum_k P_k$.

1. Start with the completeness relation:

$$\sum_k P_k = I$$

2. Multiply by P_i on the left:

$$P_i\left(\sum_k P_k\right) = P_i I \implies \sum_k P_i P_k = P_i$$

3. Separate the term where $k = i$:

$$P_i P_i + \sum_{k\neq i} P_i P_k = P_i$$

4. Since P_i is a projector, $P_i^2 = P_i$:

$$P_i + \sum_{k\neq i} P_i P_k = P_i$$

5. Subtract P_i from both sides:

$$\sum_{k\neq i} P_i P_k = 0$$

   Since P_i and P_j are orthogonal projectors, the operator $\sum_{k\neq i} P_i P_k$ is a sum of positive semi-definite operators. Since this sum is the zero operator, each term in the sum must be the zero operator.

Thus, $\mathbf{P_i P_j = 0}$ for $i \neq j$.

Exercise 3.4.1 (b)

Prove that any pure state $|\psi\rangle$ can be decomposed as $|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$ where $\alpha_i = \sqrt{p(i)}$, $p(i) = \langle\psi|P_i|\psi\rangle$, and $|\psi_i\rangle = \frac{P_i|\psi\rangle}{\sqrt{p(i)}}$. Also prove that $\langle\psi_i|\psi_j\rangle = \delta_{i,j}$.

Solution

Decomposition: Using the completeness relation $I = \sum_i P_i$:

$$|\psi\rangle = I|\psi\rangle = \sum_i P_i|\psi\rangle$$

We define the normalized state $|\psi_i\rangle$ by first considering the unnormalized state $|\phi_i\rangle = P_i|\psi\rangle$. The squared norm of $|\phi_i\rangle$ is:

$$\langle\phi_i|\phi_i\rangle = \langle\psi|P_i^\dagger P_i|\psi\rangle = \langle\psi|P_i^2|\psi\rangle = \langle\psi|P_i|\psi\rangle = p(i)$$

We define the coefficients $\alpha_i = \sqrt{p(i)}$ and the normalized states $|\psi_i\rangle = \frac{P_i|\psi\rangle}{\sqrt{p(i)}}$. Substituting back into the decomposition:

$$P_i|\psi\rangle = \sqrt{p(i)}\frac{P_i|\psi\rangle}{\sqrt{p(i)}} = \alpha_i|\psi_i\rangle$$

Therefore, $|\psi\rangle = \sum_i P_i|\psi\rangle = \sum_i \alpha_i|\psi_i\rangle$.
Orthogonality: We calculate the inner product $\langle\psi_i|\psi_j\rangle$:

$$\langle\psi_i|\psi_j\rangle = \left(\frac{\langle\psi|P_i^\dagger}{\sqrt{p(i)}}\right)\left(\frac{P_j|\psi\rangle}{\sqrt{p(j)}}\right) = \frac{1}{\sqrt{p(i)p(j)}}\langle\psi|P_i P_j|\psi\rangle$$

- **If** $i \neq j$: $P_i P_j = 0$ (from part a).

$$\langle\psi_i|\psi_j\rangle = \frac{1}{\sqrt{p(i)p(j)}}\langle\psi|0|\psi\rangle = 0$$

- **If** $i = j$: $P_i P_i = P_i$ and $\langle\psi|P_i|\psi\rangle = p(i)$.

$$\langle\psi_i|\psi_i\rangle = \frac{1}{p(i)}\langle\psi|P_i|\psi\rangle = \frac{p(i)}{p(i)} = 1$$

Thus, $\langle\psi_i|\psi_j\rangle = \delta_{i,j}$.

Exercise 3.4.1 (c)

Prove that any decomposition $I = \sum_i P_i$ of the identity operator on a Hilbert space of dimension **N** into a sum of nonzero projectors P_i can have at most **N** terms in the sum.

Solution

Let $\mathcal{H}$ be the Hilbert space with dimension N.

1. The **Rank** of an orthogonal sum of operators is the sum of their ranks. Since P_i are orthogonal projectors ($P_i P_j = 0$ for $i \neq j$), we have:

$$\text{rank}(I) = \text{rank}\left(\sum_i P_i\right) = \sum_i \text{rank}(P_i)$$

2. The rank of the identity operator I on an N-dimensional space is N: $\text{rank}(I) = N$.

3. Since each P_i is a **nonzero** projector, its rank is at least 1: $\text{rank}(P_i) \geq 1$.

4. Let M be the number of terms in the sum. Substituting the bounds:

$$N = \sum_{i=1}^{M} \text{rank}(P_i) \geq \sum_{i=1}^{M} 1 = M$$

Therefore, the number of nonzero orthogonal projectors M cannot exceed the dimension of the space N. The decomposition can have at most **N** terms in the sum ($M \leq N$).

Exercise 3.4.2: Equivalence of Observables

Exercise 3.4.2

Show that measuring the observable $|1\rangle\langle 1|$ is equivalent to measuring the observable **Z** up to a relabelling of the measurement outcomes.

Solution

Two observables are equivalent (up to relabelling) if they have the exact same set of **projectors** onto their eigenspaces, as these projectors determine the physical action (state collapse) and probabilities of measurement.

1. Observable $M_1 = |1\rangle\langle 1|$:

$$M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

- **Eigenvalues (Outcomes):** $\lambda_0 = 0$ and $\lambda_1 = 1$.
- **Projectors:**
  - For outcome 0 (eigenvector $|0\rangle$): $P_0 = |0\rangle\langle 0|$.
  - For outcome 1 (eigenvector $|1\rangle$): $P_1 = |1\rangle\langle 1|$.

2. Observable $M_2 = Z$ (Pauli Z):

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

- **Eigenvalues (Outcomes):** $\lambda'_1 = 1$ and $\lambda'_{-1} = -1$.
- **Projectors:**
  - For outcome 1 (eigenvector $|0\rangle$): $P'_1 = |0\rangle\langle 0|$.
  - For outcome -1 (eigenvector $|1\rangle$): $P'_{-1} = |1\rangle\langle 1|$.

The set of projectors for M_1 is $\mathcal{P}_1 = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. The set of projectors for M_2 is $\mathcal{P}_2 = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. Since $\mathcal{P}_1 = \mathcal{P}_2$, the physical collapse of the state is identical for both measurements. The only difference is the classical label recorded:

$$\text{Outcome } 0 \text{ from } M_1 \iff \text{Outcome } 1 \text{ from } Z$$

$$\text{Outcome } 1 \text{ from } M_1 \iff \text{Outcome } -1 \text{ from } Z$$

Thus, the measurements are equivalent up to a relabelling of the outcomes.

4 Quantum Gates and Circuits

Exercise 4.2.3: Rotation Gate Conjugation and Euler Decomposition

Exercise 4.2.3 (a)

Prove $XR_y(\theta)X = R_y(-\theta)$ and $XR_z(\theta)X = R_z(-\theta)$.

Solution

The matrices are: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $R_y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$, and $R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$.

Proof 1: $XR_y(\theta)X = R_y(-\theta)$

$$\begin{aligned} XR_y(\theta)X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \sin(\theta/2) & \cos(\theta/2) \\ \cos(\theta/2) & -\sin(\theta/2) \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \end{aligned}$$

The definition of $R_y(-\theta)$ is:

$$R_y(-\theta) = \begin{pmatrix} \cos(-\theta/2) & -\sin(-\theta/2) \\ \sin(-\theta/2) & \cos(-\theta/2) \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

Since the results are equal, the identity is proven.
Proof 2: $XR_z(\theta)X = R_z(-\theta)$

$$\begin{aligned} XR_z(\theta)X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & e^{i\theta/2} \\ e^{-i\theta/2} & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix} \end{aligned}$$

The definition of $R_z(-\theta)$ is:

$$R_z(-\theta) = \begin{pmatrix} e^{-i(-\theta)/2} & 0 \\ 0 & e^{i(-\theta)/2} \end{pmatrix} = \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix}$$

Since the results are equal, the identity is proven.

Exercise 4.2.3 (b)

Prove **Corollary 4.2.1**: Any single-qubit unitary operator U can be written as $U = e^{i\alpha}AXBXC$, where A, B, C are single-qubit unitaries (from hint: $A \equiv R_z(\beta)R_y(\gamma/2)$, $B \equiv R_y(-\gamma/2)R_z(-(\delta+\beta)/2)$ and $C \equiv R_z((\delta-\beta)/2)$).

Solution

Any unitary operator $U \in \mathrm{U}(2)$ can be decomposed into a global phase $e^{i\alpha}$ and a special unitary operator $U_{\mathrm{SU}(2)}$ using the Euler decomposition:

$$U_{\mathrm{SU}(2)} = R_z(\beta)R_y(\gamma)R_z(\delta)$$

We are asked to prove $U_{\mathrm{SU}(2)} = AXBXC$ using the provided definitions for A, B, and C. We substitute A, B, C into the expression $AXBXC$:

$$AXBXC = (R_z(\beta)R_y(\gamma/2))\,X\,(R_y(-\gamma/2)R_z(-(\delta+\beta)/2))\,X\,(R_z((\delta-\beta)/2))$$

First, use the identity $R_z(\theta)X = XR_z(-\theta)$, derived from part (a):

$$R_z(-(\delta+\beta)/2)X = XR_z((\delta+\beta)/2)$$

Substitute this back:

$$\begin{aligned} AXBXC &= R_z(\beta)R_y(\gamma/2)XR_y(-\gamma/2)\,(\mathbf{XR_z}((\delta+\beta)/\mathbf{2}))\,R_z((\delta-\beta)/2) \\ &= R_z(\beta)R_y(\gamma/2)\mathbf{XR_y}(-\gamma/\mathbf{2})\mathbf{X}R_z\left(\frac{\delta+\beta}{2}+\frac{\delta-\beta}{2}\right) \end{aligned}$$

Next, use the identity $XR_y(-\theta)X = R_y(\theta)$ (from part a with $\theta \to -\theta$):

$$XR_y(-\gamma/2)X = R_y(\gamma/2)$$

Substitute this identity and simplify the R_z product:

$$\begin{aligned} AXBXC &= R_z(\beta)R_y(\gamma/2)\mathbf{R_y}(\gamma/\mathbf{2})R_z\left(\frac{2\delta}{2}\right) \\ &= R_z(\beta)R_y(\gamma)R_z(\delta) \\ &= U_{\mathrm{SU}(2)} \end{aligned}$$

Therefore, $\mathbf{U = e^{i\alpha}AXBXC}$ is proven.

Exercise 4.2.4: CNOT in Different Bases

Exercise 4.2.4 (a)

Describe the effect of the **CNOT gate** with respect to the basis $B_1 = \{|0\rangle|+\rangle, |0\rangle|-\rangle, |1\rangle|+\rangle, |1\rangle|-\rangle\}$. Express your answers in Dirac notation and matrix notation.

Solution

The CNOT gate acts on $|c\rangle|t\rangle$ as $CNOT|c\rangle|t\rangle = |c\rangle|t \oplus c\rangle$. The basis B_1 uses the computational basis for the control qubit ($|0\rangle, |1\rangle$) and the Hadamard basis for the target qubit ($|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$).
Dirac Notation:

- **Control $|0\rangle$:** The target is unchanged (Target gate is I).

$$CNOT|0\rangle|\pm\rangle = |0\rangle I|\pm\rangle = |0\rangle|\pm\rangle$$

- **Control $|1\rangle$:** The target is flipped (Target gate is X).

$$CNOT|1\rangle|\pm\rangle = |1\rangle X|\pm\rangle$$

Since $X|+\rangle = |+\rangle$ and $X|-\rangle = -|-\rangle$ (eigenstates of X are $|\pm\rangle$ with eigenvalues ± 1):

$$CNOT|1\rangle|+\rangle = |1\rangle|+\rangle$$

$$CNOT|1\rangle|-\rangle = -|1\rangle|-\rangle$$

Matrix Notation (U_{B_1}): The basis order is $B_1 = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle\}$. The mapping is:

$$|0+\rangle \to 1 \cdot |0+\rangle$$

$$|0-\rangle \to 1 \cdot |0-\rangle$$

$$|1+\rangle \to 1 \cdot |1+\rangle$$

$$|1-\rangle \to -1 \cdot |1-\rangle$$

Since the basis vectors are eigenvectors of $CNOT$ in this basis, the matrix is diagonal with the eigenvalues $\{1, 1, 1, -1\}$:

$$U_{B_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Exercise 4.2.4 (b)

Describe the effect of the **CNOT gate** with respect to the basis $B_2 = \{|+\rangle|+\rangle, |+\rangle|-\rangle, |-\rangle|+\rangle, |-\rangle|-\rangle\}$. Express your answers in Dirac notation and matrix notation.

Solution

The basis B_2 is the product of Hadamard bases for both qubits. The CNOT gate in the Hadamard basis is equivalent to the CNOT gate with the control and target qubits swapped in the computational basis ($CNOT_{21}$), as:

$$(H \otimes H)CNOT_{12}(H \otimes H) = CNOT_{21}$$

where $CNOT_{21}$ flips the first qubit (target) if the second qubit (control) is $|1\rangle$.
Dirac Notation (using $CNOT_{21}$ equivalence):

- **Control $|+\rangle$ (qubit 1):** $|\pm\rangle$ is the control. CNOT is flipped, so qubit 2 is the control. We use the definition of $CNOT_{12}$:

$$CNOT|+\rangle|+\rangle = CNOT\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= \frac{1}{2}(|00\rangle + |01\rangle + |11\rangle + |10\rangle) = |+\rangle|+\rangle$$

$$CNOT|+\rangle|-\rangle = CNOT\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

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

$$CNOT|-\rangle|+\rangle = CNOT\frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle)$$

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

$$CNOT|-\rangle|-\rangle = CNOT\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

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

The mappings are:

$$\begin{aligned}
CNOT|+\rangle|+\rangle &= |+\rangle|+\rangle \\
CNOT|+\rangle|-\rangle &= |-\rangle|-\rangle \\
CNOT|-\rangle|+\rangle &= |-\rangle|+\rangle \\
CNOT|-\rangle|-\rangle &= |+\rangle|-\rangle
\end{aligned}$$

Matrix Notation (U_{B_2}): The basis order is $B_2 = \{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$.

- $|++\rangle \to |++\rangle$
- $|+-\rangle \to |--\rangle$ (swaps with the 4th element's position)
- $|-+\rangle \to |-+\rangle$
- $|--\rangle \to |+-\rangle$ (swaps with the 2nd element's position)

The resulting matrix is:

$$U_{B_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

5 Measurement in Quantum Computing

Exercise 5.2.1: Bell State Decomposition Identity

Exercise 5.2.1

Prove that

$$|\psi\rangle|\beta_{00}\rangle = \frac{1}{2}|\beta_{00}\rangle|\psi\rangle + \frac{1}{2}|\beta_{01}\rangle(X|\psi\rangle) + \frac{1}{2}|\beta_{10}\rangle(Z|\psi\rangle) + \frac{1}{2}|\beta_{11}\rangle(XZ|\psi\rangle).$$

Solution

We label the three registers as 1,2,3: register 1 holds the arbitrary single-qubit state $|\psi\rangle_1$, and registers 2–3 hold the Bell state $|\beta_{00}\rangle_{23}$. The Bell-basis resolution of identity on registers 1 and 2 is given by:

$$I_{12} = \sum_{a,b\in\{0,1\}} |\beta_{ab}\rangle_{12} \langle\beta_{ab}| \,.$$

Thus

$$|\psi\rangle_1 |\beta_{00}\rangle_{23} = \sum_{a,b} |\beta_{ab}\rangle_{12} \Big(\langle\beta_{ab}|_{12} \left(|\psi\rangle_1 |\beta_{00}\rangle_{23}\right)\Big).$$

We evaluate the overlap

$$\mathcal{C}_{ab} := \langle\beta_{ab}|_{12} \left(|\psi\rangle_1 |\beta_{00}\rangle_{23}\right).$$

Use $|\beta_{ab}\rangle_{12} = (I \otimes X^b Z^a)\, |\beta_{00}\rangle_{12}$, so

$$\langle\beta_{ab}|_{12} = \langle\beta_{00}|_{12}\, (I \otimes Z^a X^b).$$

Therefore

$$\mathcal{C}_{ab} = \langle\beta_{00}|_{12}\, (I \otimes Z^a X^b)\big(\, |\psi\rangle_1 |\beta_{00}\rangle_{23}\,\big).$$

Now use the maximally-entangled identity $(I \otimes M)\,|\beta_{00}\rangle = (M^\mathsf{T} \otimes I)\,|\beta_{00}\rangle$ (and $X^\mathsf{T} = X,\ Z^\mathsf{T} = Z$) to move $Z^a X^b$ onto register 1:

$$(I_1 \otimes Z_2^a X_2^b)\big(\, |\psi\rangle_1 |\beta_{00}\rangle_{23}\,\big) = \big((X^b Z^a\, |\psi\rangle)_1\big) \otimes |\beta_{00}\rangle_{23} \,.$$

Hence

$$\mathcal{C}_{ab} = \langle\beta_{00}|_{12}\, \big((X^b Z^a\, |\psi\rangle)_1 \otimes |\beta_{00}\rangle_{23}\,\big).$$

Finally use the overlap identity $\langle\beta_{00}|_{12}\,\big(\,|\phi\rangle_1 \otimes |\beta_{00}\rangle_{23}\,\big) = \frac{1}{2}\,|\phi\rangle_3$ (valid for any single-qubit $|\phi\rangle$). With $|\phi\rangle = X^b Z^a\, |\psi\rangle$ we get

$$\mathcal{C}_{ab} = \tfrac{1}{2}\, (X^b Z^a\, |\psi\rangle)_3.$$

Substituting back into the sum gives

$$|\psi\rangle_1 |\beta_{00}\rangle_{23} = \tfrac{1}{2} \sum_{a,b\in\{0,1\}} |\beta_{ab}\rangle_{12}\, (X^b Z^a\, |\psi\rangle)_3,$$

which, when expanded term-by-term, is exactly

$$|\psi\rangle_1 |\beta_{00}\rangle_{23} = \tfrac{1}{2}\, |\beta_{00}\rangle_{12}\, |\psi\rangle_3 + \tfrac{1}{2}\, |\beta_{01}\rangle_{12}\, (X\, |\psi\rangle)_3 + \tfrac{1}{2}\, |\beta_{10}\rangle_{12}\, (Z\, |\psi\rangle)_3 + \tfrac{1}{2}\, |\beta_{11}\rangle_{12}\, (XZ\, |\psi\rangle)_3.$$

6 Quantum Algorithms

Exercise 6.4.1: Multiqubit Hadamard Transform

Exercise 6.4.1

Prove that

$$\left(\frac{|0\rangle+(-1)^{x_1}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+(-1)^{x_2}|1\rangle}{\sqrt{2}}\right)\cdots$$
$$\cdots\left(\frac{|0\rangle+(-1)^{x_n}|1\rangle}{\sqrt{2}}\right)=\frac{1}{\sqrt{2^n}}\sum_{z_1z_2\ldots z_n\in\{0,1\}^n}(-1)^{x_1z_1+x_2z_2+\cdots+x_nz_n}$$
$$\times|z_1\rangle|z_2\rangle\cdots|z_n\rangle.$$

Solution

We prove the identity by expanding each factor and then taking the tensor product. For each k:

$$\frac{|0\rangle+(-1)^{x_k}|1\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\sum_{z_k\in\{0,1\}}(-1)^{x_kz_k}|z_k\rangle,$$

because when $z_k=0$ the term equals $\frac{1}{\sqrt{2}}|0\rangle$ and when $z_k=1$ it equals $\frac{(-1)^{x_k}}{\sqrt{2}}|1\rangle$. Now take the tensor product over $k=1,\ldots,n$:

$$\bigotimes_{k=1}^{n}\frac{|0\rangle+(-1)^{x_k}|1\rangle}{\sqrt{2}}=\left(\prod_{k=1}^{n}\frac{1}{\sqrt{2}}\right)\bigotimes_{k=1}^{n}\sum_{z_k\in\{0,1\}}(-1)^{x_kz_k}|z_k\rangle=\frac{1}{\sqrt{2^n}}\bigotimes_{k=1}^{n}\sum_{z_k\in\{0,1\}}(-1)^{x_kz_k}|z_k\rangle.$$

Expanding the tensor product of sums gives a single sum over all n-bit strings $z=(z_1,\ldots,z_n)$:

$$\bigotimes_{k=1}^{n}\sum_{z_k\in\{0,1\}}(-1)^{x_kz_k}|z_k\rangle=\sum_{z_1,\ldots,z_n\in\{0,1\}}\left(\prod_{k=1}^{n}(-1)^{x_kz_k}\right)|z_1\rangle|z_2\rangle\cdots|z_n\rangle.$$

Since

$$\prod_{k=1}^{n}(-1)^{x_kz_k}=(-1)^{\sum_{k=1}^{n}x_kz_k},$$

we obtain

$$\bigotimes_{k=1}^{n}\frac{|0\rangle+(-1)^{x_k}|1\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}(-1)^{\sum_{k=1}^{n}x_kz_k}|z_1\rangle|z_2\rangle\cdots|z_n\rangle,$$

which is the desired identity.

Exercise 6.5.1: Action of Multiqubit Hadamard on a Superposition

Exercise 6.5.1

Let $x,y\in\{0,1\}^n$ and let $s=x\oplus y$. Show that

$$H^{\otimes n}(\frac{1}{\sqrt{2}}|x\rangle+\frac{1}{\sqrt{2}}|y\rangle)=\frac{1}{\sqrt{2^{n-1}}}\sum_{z\in\{s\}^\perp}(-1)^{x\cdot z}|z\rangle.$$

Solution

1. Apply $H^{\otimes n}$ to the Superposition We use the multi-qubit Hadamard formula $H^{\otimes n}|w\rangle=$

$\frac{1}{\sqrt{2^n}}\sum_z(-1)^{w\cdot z}|z\rangle$:

$$\begin{aligned}
H^{\otimes n}\left(\frac{1}{\sqrt{2}}|x\rangle+\frac{1}{\sqrt{2}}|y\rangle\right) &= \frac{1}{\sqrt{2}}H^{\otimes n}|x\rangle+\frac{1}{\sqrt{2}}H^{\otimes n}|y\rangle \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^n}}\sum_z(-1)^{x\cdot z}|z\rangle\right)+\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^n}}\sum_z(-1)^{y\cdot z}|z\rangle\right) \\
&= \frac{1}{\sqrt{2^{n+1}}}\sum_{z\in\{0,1\}^n}\left((-1)^{x\cdot z}+(-1)^{y\cdot z}\right)|z\rangle
\end{aligned}$$

2. Analyze the Coefficient $C_z=(-1)^{x\cdot z}+(-1)^{y\cdot z}$ Since $s=x\oplus y$, the dot product $s\cdot z$ relates $x\cdot z$ and $y\cdot z$ modulo 2: $s\cdot z=(x\cdot z)\oplus(y\cdot z)\pmod 2$.

- **Case 1:** $z\in\{s\}^\perp$ **(where** $s\cdot z=0\pmod 2$**)** If $s\cdot z=0$, then $x\cdot z$ and $y\cdot z$ have the same parity, so $(-1)^{x\cdot z}=(-1)^{y\cdot z}$.

$$C_z=(-1)^{x\cdot z}+(-1)^{x\cdot z}=2(-1)^{x\cdot z}$$

- **Case 2:** $z\notin\{s\}^\perp$ **(where** $s\cdot z=1\pmod 2$**)** If $s\cdot z=1$, then $x\cdot z$ and $y\cdot z$ have opposite parity, so $(-1)^{y\cdot z}=-(-1)^{x\cdot z}$.

$$C_z=(-1)^{x\cdot z}+(-(-1)^{x\cdot z})=0$$

3. Final Substitution Only the terms where $z\in\{s\}^\perp$ survive, which is a subspace of dimension $n-1$:

$$\begin{aligned}
H^{\otimes n}\left(\frac{1}{\sqrt{2}}|x\rangle+\frac{1}{\sqrt{2}}|y\rangle\right) &= \frac{1}{\sqrt{2^{n+1}}}\sum_{z\in\{s\}^\perp}\left(2(-1)^{x\cdot z}\right)|z\rangle \\
&= \frac{2}{\sqrt{2^n\cdot 2}}\sum_{z\in\{s\}^\perp}(-1)^{x\cdot z}|z\rangle \\
&= \frac{\sqrt{4}}{\sqrt{2^n\cdot 2}}\sum_{z\in\{s\}^\perp}(-1)^{x\cdot z}|z\rangle \\
&= \frac{\sqrt{2}}{\sqrt{2^n}}\sum_{z\in\{s\}^\perp}(-1)^{x\cdot z}|z\rangle \\
&= \frac{1}{\sqrt{2^{n-1}}}\sum_{z\in\{s\}^\perp}(-1)^{x\cdot z}|z\rangle
\end{aligned}$$