QDCS - Intro Quantum
Homework # 1
Due on Friday, Oct 10 2025, 9am

Recall that $\mathcal{H}$ is the Hilbert space generated from $|0\rangle, |1\rangle$.

1 Basis (3 pts)

Show that the following vectors form an orthonormal basis for $\mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}$ (known as the SHIFT basis)

$$|000\rangle, |111\rangle, |{+}01\rangle, |{-}01\rangle, |1{+}0\rangle, |1{-}0\rangle, |01{+}\rangle, |01{-}\rangle,$$

where for example $|01{+}\rangle$ stands for $|0\rangle \otimes |1\rangle \otimes |+\rangle$.

Do as few computations as possible.

Solution

First, there are 8 vectors, and the dimension of the space is 8.
We can also see that each vector is of norm 1: indeed, they are tensors of vectors of norm 1.
It remains to check their pairwise orthogonality. We know that $|0\rangle \perp |1\rangle$ and $|+\rangle \perp |-\rangle$. We also know that whenever two vectors $|\phi_1\rangle$ and $|\phi_2\rangle$ are orthogonal, so are $|\psi_1\rangle \otimes |\phi_1\rangle \otimes |\psi_1'\rangle$ and $|\psi_2\rangle \otimes |\phi_2\rangle \otimes |\psi_2'\rangle$. In the following table, we indicate a position in the list for two orthogonal vectors.

	$\|000\rangle$	$\|111\rangle$	$\|{+}01\rangle$	$\|{-}01\rangle$	$\|1{+}0\rangle$	$\|1{-}0\rangle$	$\|01{+}\rangle$	$\|01{-}\rangle$
$\|000\rangle$	/	1	3	3	1	1	2	2
$\|111\rangle$	1	/	2	2	3	3	1	1
$\|{+}01\rangle$	3	2		1	3	2	2	2
$\|{-}01\rangle$	3	2	1	/	3	3	2	2
$\|1{+}0\rangle$	0	3	3	3	/	2	1	1
$\|1{-}0\rangle$	0	3	3	3	2	/	1	1
$\|01{+}\rangle$	2	1	2	2	1	1	/	3
$\|01{-}\rangle$	2	1	2	2	1	1	3	/

2 Reversible Computation (7 pts)

Consider the set $\mathcal{B} \triangleq \{e_0, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ and the bijection σ on the set $\mathcal{B}$ defined as e_k to $e_{3k \bmod 8}$. In other word, it is defined as

$$\begin{array}{cccc} e_0 \mapsto e_0 & e_2 \mapsto e_6 & e_4 \mapsto e_4 & e_6 \mapsto e_2 \\ e_1 \mapsto e_3 & e_3 \mapsto e_1 & e_5 \mapsto e_7 & e_7 \mapsto e_5 \end{array}$$

Let $\mathcal{E}$ be the Hilbert space generated by $\mathcal{B}$, and U the linear map $\mathcal{E} \to \mathcal{E}$ defined as

$$U : |e_k\rangle \mapsto |\sigma(e_k)\rangle \qquad \text{for } k = 0, \ldots, 7$$

1. Write a matrix for U using the basis ordering $e_0, e_1, e_2, e_3, e_4, e_5, e_6, e_7$. (1 pt)
2. What does it means when $U_{m,n} = 1$? (1 pt)
3. Explain why U is unitary. (2 pts)
4. U can be regarded as an action on a register of 3 qubits. Design a circuit for U, acting on $\mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}$, using only X, CNOT and Toffoli gates. Even if they are not necessary (in fact, 4 gates are enough), you can use ancillas but beware: we want a unitary circuit. As an encoding on bitstring, set the least significant bit on the right. (3 pts)

Sketch of Solution

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

If $U_{m,n} = 1$, it means that $U|e_n\rangle = |e_m\rangle$, meaning that $\sigma(e_n) = e_m$.

The matrix U is unitary: indeed, for all m, n we have $(U^*)_{m,n} = U_{n,m}$ (since it is a real number). We then have

$$(UU^*)_{m,m} = \sum_{k=0}^{7} U_{m,k} U^*_{k,m}$$

and $U_{m,k} U^*_{k,m}$ is zero for all $k \neq n$ and 1 when $k = n$. Now, when $m \neq n$, $U_{m,k} U^*_{k,n}$ is zero for all k: $U_{m,k} \neq 0$ only when $k = n$, but $U^*_{k,n} \neq 0$ only when $k = m \neq n$. So UU^* is the identity.

The same can be done for U^*U.

To build a circuit for U, we choose the lexicographic ordering $|q_1 q_2 q_3\rangle$ as follows:

$$|e_0\rangle \equiv |000\rangle, |e_1\rangle \equiv |001\rangle, |e_2\rangle \equiv |010\rangle, |e_3\rangle \equiv |011\rangle$$

$$|e_4\rangle \equiv |100\rangle, |e_5\rangle \equiv |101\rangle, |e_6\rangle \equiv |110\rangle, |e_7\rangle \equiv |111\rangle$$

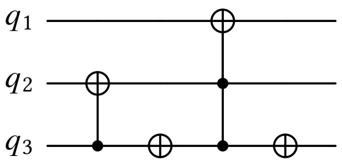
The action of σ is as follows

before			after		
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	1	1	0
0	1	1	0	0	1
1	0	0	1	0	0
1	0	1	1	1	1
1	1	0	0	1	0
1	1	1	1	0	1

Some facts:

- q_3 is not changed.
- when $q_3 = 1$, q_2 is flipped.
- q_1 is changed only twice, when $q_2 q_3$ is 10.

This describes the following circuit:



3 Measuring 2 Qubits (4 pts)

Consider the two-qubit system

$$\alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle .$$

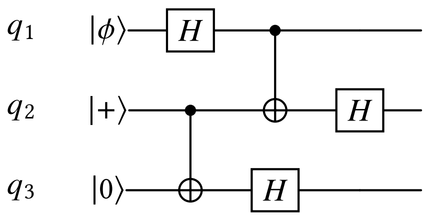
Show the detailed computation of why measuring the first qubit THEN the second qubit yields the same result as measuring the second qubit THEN the first qubit.

Sketch of Solution

This is just a matter of reproducing carefully what we did on the board and what can be found in Section 3.8.10++.

4 An example of measure (3 pts)

Let $|\phi\rangle$ be $\alpha |0\rangle + \beta |1\rangle$, and consider the circuit



If we measure q_1 and q_2 at the end of the circuit, what is the result?
Show your computation.

Sketch of Solution

Step by step, the computation is as follows. Originally, we have

$$|\phi\rangle \otimes |+\rangle \otimes |0\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

$$= \frac{1}{\sqrt{2}}(\alpha |000\rangle + \alpha |010\rangle + \beta |100\rangle + \beta |110\rangle)$$

After CNOT on q_2, q_3:

$$\frac{1}{\sqrt{2}}(\alpha |000\rangle + \alpha |011\rangle + \beta |100\rangle + \beta |111\rangle)$$

After H on q_1:

$$\frac{1}{\sqrt{2}}\left(\begin{array}{c} \alpha|000\rangle+\alpha|011\rangle+\beta|000\rangle+\beta|011\rangle) \\ +\alpha|100\rangle+\alpha|111\rangle-\beta|100\rangle-\beta|111\rangle) \end{array}\right)$$

After CNOT on q_1, q_2:

$$\frac{1}{\sqrt{2}}\left(\begin{array}{c} \alpha|000\rangle+\alpha|011\rangle+\beta|000\rangle+\beta|011\rangle) \\ +\alpha|110\rangle+\alpha|101\rangle-\beta|110\rangle-\beta|101\rangle) \end{array}\right)$$

$$=\frac{1}{\sqrt{2}}((\alpha+\beta)|000\rangle+(\alpha+\beta)|011\rangle+(\alpha-\beta)|110\rangle+(\alpha-\beta)|101\rangle)$$

After the last two H:

$$=\frac{1}{2\sqrt{2}}\left(\begin{array}{c} (\alpha+\beta)|000\rangle+(\alpha+\beta)|000\rangle+(\alpha-\beta)|100\rangle+(\alpha-\beta)|100\rangle) \\ +(\alpha+\beta)|001\rangle-(\alpha+\beta)|001\rangle+(\alpha-\beta)|101\rangle-(\alpha-\beta)|101\rangle) \\ +(\alpha+\beta)|010\rangle-(\alpha+\beta)|010\rangle-(\alpha-\beta)|110\rangle+(\alpha-\beta)|110\rangle) \\ +(\alpha+\beta)|011\rangle+(\alpha+\beta)|011\rangle-(\alpha-\beta)|111\rangle-(\alpha-\beta)|111\rangle) \end{array}\right)$$

$$=\frac{1}{2\sqrt{2}}\left(\begin{array}{c} (2\alpha+2\beta)|000\rangle+0|001\rangle+0|010\rangle+(2\alpha+2\beta)|011\rangle \\ +(2\alpha-2\beta)|100\rangle+0|101\rangle+0|110\rangle+(2\beta-2\alpha)|111\rangle \end{array}\right)$$

$$=\frac{1}{\sqrt{2}}\left(\begin{array}{c} (\alpha+\beta)|000\rangle+(\alpha+\beta)|011\rangle \\ +(\alpha-\beta)|100\rangle+(\beta-\alpha)|111\rangle \end{array}\right).$$

Measuring the two first qubits corresponds to projecting into the subspaces

$$|00\rangle\otimes\mathcal{H}, |01\rangle\otimes\mathcal{H}, |10\rangle\otimes\mathcal{H}, |11\rangle\otimes\mathcal{H}.$$

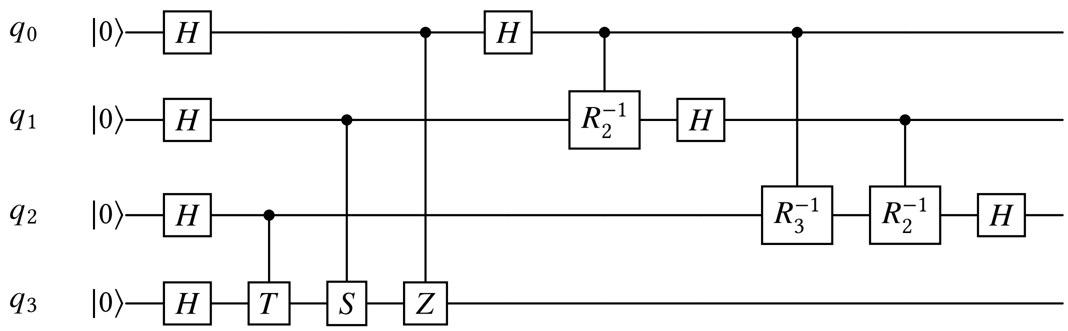
and renormalizing. We get

- with probability $\frac{(\alpha+\beta)^2}{2}$ the state $|000\rangle$
- with probability $\frac{(\alpha+\beta)^2}{2}$ the state $|011\rangle$
- with probability $\frac{(\alpha-\beta)^2}{2}$ the state $|110\rangle$
- with probability $\frac{(\alpha-\beta)^2}{2}$ the state $|111\rangle$

If we forget the result of the measurements, the third qubit is in state $|0\rangle$ and in the state $|1\rangle$ with probability $\frac{1}{2}$.

5 A Mysterious Circuit (3 pts)

Consider the following circuit.



where R_n is

$$R_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{2^n}} \end{pmatrix}.$$

Using what you know from QPE, give the state-vector resulting from running the circuit. Explain your reasoning.

Sketch of Solution

We right-hand-side of the circuit is the inverse QFT, with the least significant bit on the top wire. The overall circuit is QPE(T) with 3 bits of precision applied to the state $|+\rangle$ (the action of the bottom-left H on $|0\rangle$). QPE is a linear operation: when the memory is written in the order $q_0q_1q_2q_3$ (top qubit on the left):

$$\mathrm{QPE}(T)(|000\rangle \otimes |+\rangle) = \frac{1}{\sqrt{2}}(\mathrm{QPE}(T)(|000\rangle \otimes |0\rangle) + \mathrm{QPE}(T)(|000\rangle \otimes |1\rangle))$$

The ket $|0\rangle$ is an eigenvector of T with eigenvalue $1 = e^{2i\pi\cdot 0}$ and $|1\rangle$ an eigenvector of T with eigenvalue $e^{i\pi/4} = e^{2i\pi\cdot 1/8}$. The phases of the eigenvalues are in binary respectively 000 and 001 (when the least significant bit is on the right). We then read:

$$\frac{1}{\sqrt{2}}(|000\rangle \otimes |0\rangle + |100\rangle \otimes |0\rangle)$$

(least significant bit on the top qubit)