Catalog of matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

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

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

$$R_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

where $\theta, \varphi \in \mathbb{R}$.

Homework 1: Unitary matrices

Question 1. Prove that all the matrices in the catalog above are unitary.

Question 2. Show that if U is unitary, then $U^\dagger$ is unitary.

Question 3. Show that the product of two unitary matrices is unitary.

Question 4. For any complex $N \times N$ matrix U, we can uniquely write $U = R + iQ$, where R and Q have real entries. Show that if U is unitary, then so is the $2N \times 2N$ matrix U' given in block form by

$$U' = \begin{pmatrix} R & Q \\ -Q & R \end{pmatrix}$$

Thus, by doubling the dimension, we can remove the need for complex-number entries. Show the result of applying this construction to the Pauli matrix Y.

Question 5. Show that the four Pauli matrices X, Y, Z, I form an orthonormal basis for the space of 2×2 matrices. Thus, we can regard the space of 2×2 matrices as a 4-dimensional complex Hilbert space.

Homework 2: Hilbert spaces

Question 1. Define

$$H_2 = \mathbb{C}^2 = \{ \ \alpha|0\rangle + \beta|1\rangle \ \mid \ \alpha, \beta \in \mathbb{C} \ \}$$

The inner product in H_2 is defined by

$$\langle \ \alpha_1|0\rangle + \beta_1|1\rangle \mid \alpha_2|0\rangle + \beta_2|1\rangle \ \rangle \quad = \quad \alpha_1^\dagger\alpha_2 + \beta_1^\dagger\beta_2$$

for all $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{C}$. Show that the inner product satisfies the following four properties:

1. $\langle\varphi \mid \varphi\rangle \geq 0$
2. $\langle\varphi \mid \varphi\rangle = 0$ if and only if $|\varphi\rangle = 0$.
3. $\langle\varphi \mid \psi\rangle = \langle\psi \mid \varphi\rangle^\dagger$.
4. $\langle\varphi \mid \lambda_1\psi_1 + \lambda_2\psi_2\rangle = \lambda_1\langle\varphi \mid \psi_1\rangle + \lambda_2\langle\varphi \mid \psi_2\rangle$

for any $|\varphi\rangle, |\psi\rangle, |\psi_1\rangle, |\psi_2\rangle \in H_2$ and for any $\lambda_1, \lambda_2 \in \mathbb{C}$.

Question 2. Suppose f, g are Boolean functions on n inputs. Define $h(x) = f(x) \oplus g(x)$, where $\oplus$ denotes "exclusive or". Prove that h is always false (also written 0) if and only if f and g are the same function.

Question 3. For a Boolean string $x = x_1 \ldots x_n$, define

$$\begin{aligned} (-1)^x &= (-1)^{(x_1+\ldots+x_n)} \\ \mathsf{XOR}(x) &= x_1 \oplus \ldots \oplus x_n \end{aligned}$$

Show that $(-1)^x = 1$ if and only if $\mathsf{XOR}(x) = 0$.

Homework 3: Circuit identities

Let U be a 2×2 unitary matrix. The controlled-U is a two-qubit gate, which when applied to qubit registers q_1, q_2, is defined by:

$$\text{CNOT}[q_1, q_2]|k_{n-1} \ldots k_{q_2} \ldots k_{q_1} \ldots k_0\rangle \;=\; |k_{n-1}\rangle \ldots (U^{k_{q_1}}|k_{q_2}\rangle) \ldots |k_{q_1}\rangle \ldots |k_0\rangle$$

where q_1 is the control qubit and q_2 is the target qubit, and where every $k_i \in \{0, 1\}$. The matrix representation of $C(U)$ is

$$C(U) \;=\; \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

where I is the 2×2 identity matrix and 0 is the 2×2 matrix in which every entry is 0. Notice that CNOT $= C(X)$, where X is one of the Pauli matrices.

Define SWAP to be the two-qubit gate that swaps the states of two qubit registers:

$$\text{SWAP}[q_1, q_2]|k_{n-1} \ldots k_{q_2} \ldots k_{q_1} \ldots k_0\rangle \;=\; |k_{n-1} \ldots k_{q_1} \ldots k_{q_2} \ldots k_0\rangle$$

where every $k_i \in \{0, 1\}$.

Question 1. Prove the following properties of controlled gates:

1. $\text{SWAP}[q_1, q_2] = C(X)[q_1, q_2]\ C(X)[q_2, q_1]\ C(X)[q_1, q_2]$.
2. $C(X)[p, q] = H[q]\ C(Z)[p, q]\ H[q]$.
3. $C(Z)[p, q] = C(Z)[q, p]$.
4. $H[p]\ H[q]\ C(X)[p, q]\ H[p]\ H[q] = C(X)[q, p]$.
5. $C(e^{i\alpha} I))[p, q] = R_\varphi[p]$.
6. $C(X)[p, q]\ X[p]\ C(X)[p, q] = X[p]\ X[q]$.
7. $C(X)[p, q]\ Y[p]\ C(X)[p, q] = Y[p]\ X[q]$.
8. $C(X)[p, q]\ Z[p]\ C(X)[p, q] = Z[p]$.
9. $C(X)[p, q]\ X[q]\ C(X)[p, q] = X[q]$.
10. $C(X)[p, q]\ Y[q]\ C(X)[p, q] = Z[p]\ X[q]$.
11. $C(X)[p, q]\ Z[q]\ C(X)[p, q] = Z[p]\ Z[q]$.
12. $C(X)[p, q]\ T[p] = T[p]\ C(X)[p, q]$.

Homework 4: Quantum states

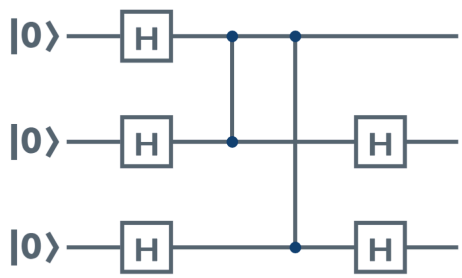
For a ket $|k_{n-1}\dots k_0\rangle$, we index the qubits from the right, starting with index 0.

Question 1. For the following state, suppose we measure the qubit with index 1 in the standard basis and get 0. Show the resulting state. Justify your answer.

$$\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{4}|10\rangle - \frac{\sqrt{7}}{4}|11\rangle$$

Question 2. Suppose we apply $H^{\otimes 3}$ to the state $|101\rangle$, after which we measure the two qubits with indexes 0,1 in the standard basis. What is the probability that we get 11 ?

Question 3. Consider the following circuit with three qubits.



Here H is the Hadamard gate, while each 2-qubit connection is CZ $= C(Z)$.

Suppose that at the end, we measure all three qubits in the standard basis. What is the probability that we will get 000 ? Justify your answer.

Question 4. Consider the following state.

$$\frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Suppose we measure the qubit with index 0 in the standard basis. What is the probability of getting 0, and if that happens, what is the state of the other qubit? Also, suppose we measure the qubit with index 1 in the standard basis. What is the probability of getting 1, and if that happens, what is the state of the other qubit?

Homework 5: Quantum algorithms

Question 1. Show, step by step, that the Deutsch-Jozsa algorithm works for the case of f, where $f(0) = f(1) = 1$.

Question 2. For the case of $n = 3$ and a function f where

$$\begin{array}{ccccc} f(000) & = & f(010) & = & 110 \\ f(001) & = & f(011) & = & 101 \end{array} \qquad \begin{array}{ccccc} f(100) & = & f(110) & = & 011 \\ f(111) & = & f(101) & = & 111 \end{array}$$

give two different examples of equations that the first step of Simon's algorithm may produce. Explain what those equations mean.

Question 3. Show, step-by-step, that Grover's algorithm works for the case of 2 qubits and a function f where $f(01) = 1$ and $f(00) = f(10) = f(11) = 0$.