1. Balanced functions

Let B_2 denote the set of all 2-bit strings, B_3 denote the set of all 3-bit strings, and $B_1 = \{0, 1\}$.

(a) Write down the six balanced functions $f : B_2 \to B_1$; for each one you should give the value of $f(x_1x_2)$ on each input. You should give a table with the values, and for each function write it in the form as an explicit function of x_1 and x_2.

(b) For any function $f : B_2 \to B_1$, consider the two-qubit state

$$|f\rangle = \frac{1}{2} \sum_{x_1,x_2=0}^{1} (-1)^{f(x_1x_2)} |x_1, x_2\rangle.$$

Find a pair of balanced functions that have the property that the associated states $|f\rangle$ are orthogonal.

Find another pair of balanced functions that have the property that the associated states $|f\rangle$ are not orthogonal.

(c) Show that all the states $|f\rangle$ associated to balanced functions $f : B_2 \to B_1$ are orthogonal to the state associated to the constant function $g(x_1x_2) = 0$.

(d) Give a table of values for the following functions $f : B_3 \to B_1$:
$f_1(x_1x_2x_3) = x_1 + x_2 \bmod 2$, $f_2(x_1x_2x_3) = x_1x_2 \bmod 2$, $f_3(x_1x_2x_3) = x_1x_2 + x_2x_3 + x_3x_1 \bmod 2$,
$f_4(x_1x_2x_3) = x_1x_2x_3 + x_1 + x_2 + x_3 \bmod 2$.
Which of these functions are balanced?

2. Functions from one trit to one trit

A trit is an object that can be in one of three states 0,1,2. The functions considered in this question are all from one trit to one trit.

(a) How many such functions are there?

(b) Consider the function $f_1(x) = x + 2 \bmod 3$. How many different values does f_1 take?

(c) Consider the function defined by $f_2(0) = 1$, $f_2(1) = 0$, $f_2(2) = 2$. Find constants a, b, c each of which can be 0,1,2, such that $f_2(x)$ can be written in the form $f_2(x) = ax^2 + bx + c \bmod 3$.

(d) Show that $f_3(x) = x^3 \bmod 3$ and $f_4(x) = x^4 \bmod 3$ can also both be written in the form $ax^2 + bx + c \bmod 3$.

3. Identifying functions

Let B_2 denote the set of 2-bit strings and $B_1 = \{0, 1\}$. For any function $g : B_2 \mapsto B_1$ let

$$V_g|x\rangle = (-1)^{g(x)}|x\rangle$$

where for any 2-bit string $x = x_1x_2$, $|x\rangle = |x_1\rangle|x_2\rangle$, and $|0\rangle$ and $|1\rangle$ are the standard orthonormal basis elements for $\mathbb{C}^2$.

Let us define the four functions $f_a : B_2 \to B_1$, $a = 00, 01, 10, 11$ (i.e. the functions are enumerated in binary). The functions are defined by

$$f_{00}(x) = 0 \;\forall\; x \qquad f_{01}(x) = \begin{cases} 0 & \text{if } x = 00 \text{ or } 01, \\ 1 & \text{otherwise.} \end{cases}$$

$$f_{10}(x) = \begin{cases} 0 & \text{if } x = 00 \text{ or } 10, \\ 1 & \text{otherwise.} \end{cases} \qquad f_{11}(x) = \begin{cases} 0 & \text{if } x = 00 \text{ or } 11, \\ 1 & \text{otherwise.} \end{cases}$$

(a) Consider we are given a black box associated to one of these functions f_a, but we do not know which one, and we would like to find out (i.e. to learn the two-bit string a).

We query the black box by inserting $x = 00$ into it. Given the value of the output, what can we say about which black box it is?

What is the minimum number of times that we need to query the black box to be certain which one it is? Give a brief explanation of your answer.

(b) Write down the Dirac form for V_g for an arbitrary function g (not necessarily one of the f_a's) and show that V_g is unitary.

(c) To any classical function g from 2 bits to one bit, we associate the quantum state $|g\rangle$ defined by

$$|g\rangle = V_g \left(H \otimes H\right) |00\rangle$$

Consider that we have two qubits which are in one of the four states $|f_{00}\rangle$, $|f_{01}\rangle$, $|f_{10}\rangle$, $|f_{11}\rangle$ (but we don't know which), and make a measurement in the computational basis. What can we say about which state we have, given the outcome of the measurement.

(d) Consider now that we have access to one of the four quantum operators V_{f_a} for some a, but we do not know which. Consider the quantum protocol

A. Start with two qubits in the state $|00\rangle$.

B. Apply $H \otimes H$

C. Apply V_{f_a},

D. Apply $H \otimes H$

E. Measure in the computational basis

Show that the outcome of the measurement in step E enables us to find which V_{f_a} we have, with certainty.

4. Periodic states

The quantum Fourier transform in dimension N is defined as follows in the standard basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$:

$$QFT|a\rangle = \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} \exp\left(\frac{2\pi i a b}{N}\right) |b\rangle, \qquad 0 \leq a \leq N-1.$$

(a) Write down the matrix for the quantum Fourier transform in six dimensions in terms of $\omega = \exp(i\pi/3)$.

(b) A state is called periodic if it is (up to normalization) of the form

$$|a\rangle + |a+r\rangle + |a+2r\rangle ...$$

r is the period of the state.

Three periodic states in dimension six are

$$\begin{aligned} &\frac{1}{\sqrt{6}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle) \\ &\frac{1}{\sqrt{3}}(|0\rangle + |2\rangle + |4\rangle) \\ &\frac{1}{\sqrt{3}}(|1\rangle + |3\rangle + |5\rangle) \end{aligned} \tag{3.1}$$

Suppose we are given a particle that is in the state $|\tau\rangle$; $|\tau\rangle$ is one of the three states in equation (3.1). If we measure the particle in the standard basis, can we determine whether the state has period 2 or not?

(c) We now start again with a particle that is in the state $|\tau\rangle$; $|\tau\rangle$ is one of the three states in equation (3.1). We now apply the six dimensional quantum Fourier transform to the state then measure the particle in the standard basis.

We want to announce that we know the period of the state, but will only do so if we are certain what the period is. If the period was actually 2, what is the probability that our procedure will allow us to announce the period?

5. Quantum Cryptography

(a) If, rather than Alice sending $|0\rangle$ and $|+\rangle$, and Bob measuring X and Z, as in the protocol in the lectures, Alice sends $|0\rangle$ and $|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \omega|1\rangle)$ with equal probability, and Bob measures Z and C with equal probability. $\omega = e^{2\pi i/3}$ and C is the operator with eigenvalues +1 and -1, and the +1 eigenstate of C is $|u\rangle$. What is the probability that Bob is certain which state Alice sent (assuming there is no eavesdropper)?

(a) If, rather than Alice sending $|0\rangle$ and $|+\rangle$, and Bob measuring X and Z, as in the protocol in the lectures, Alice and Bob try to use the following protocol: Alice sends one of $|0\rangle$, $|+\rangle$ or $|y+\rangle$ with equal probability (the latter is the +1 eigenstate of Y) and Bob measures one of X, Y or Z with equal probability. Will this scheme be useful for quantum cryptography?