Quantum Cryptography

Homework Set 2

Note that we sometimes mix between alternative ways of writing tensor products between kets or bras, i.e. $|0\rangle \otimes |0\rangle = |0\rangle |0\rangle = |00\rangle$.

1 The CNOT Gate

The controlled-NOT (CNOT) operation is a unitary matrix acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$. We define $U_{\text{CNOT}} \in U(\mathbb{C}^2 \otimes \mathbb{C}^2)$ by specifying its action on basis states of the computational basis:

$$U_{\text{CNOT}}(|a\rangle |b\rangle) = |a\rangle |a \oplus b\rangle, \quad \forall a, b \in \{0, 1\}.$$

a) Find the matrix representation of $U_{\text{CNOT}}$.

**Answer:** Can be found by applying $U_{\text{CNOT}}$ to all basis states of $\mathbb{C}^2 \otimes \mathbb{C}^2$, i.e. $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

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

b) Prove that $U_{\text{CNOT}}$ is indeed unitary.

**Answer:** First of all, it is easy to see from a) that the columns of $U_{\text{CNOT}}$ form the standard orthonormal basis, hence $U_{\text{CNOT}}$ is unitary. Alternatively, we can write

$$U_{\text{CNOT}} = \sum_{x,y} |x\rangle |x \oplus y\rangle \langle x| \langle y|.$$

Then,

$$U_{\text{CNOT}}U_{\text{CNOT}}^\dagger = \left(\sum_{x,y} |x\rangle |x \oplus y\rangle \langle x| \langle x'| \langle x' \oplus y'|ight)$$

$$= \sum_{x,x',y,y'} |x\rangle |x \oplus y\rangle \langle x' \oplus y'\rangle$$

$$= \sum_{x,y} |x\rangle \langle x\rangle \otimes |x \oplus y\rangle \langle x \oplus y| = \mathbb{1}$$

c) Prove that $U_{\text{CNOT}}(H|a\rangle H|b\rangle) = H|a \oplus b\rangle H|b\rangle$.

**Answer:** Let $U := U_{\text{CNOT}}$.

$$U(H|a\rangle H|b\rangle) = U\left(\frac{|0\rangle + (-1)^a|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + (-1)^b|1\rangle}{\sqrt{2}}\right)$$

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

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

$$= \frac{|0\rangle + (-1)^{a+b}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + (-1)^b|1\rangle}{\sqrt{2}} = H|a \oplus b\rangle H|b\rangle$$

d) Compute the result of applying $U_{\text{CNOT}}$ to the state $|+\rangle |0\rangle$.

**Answer:** Let $U := U_{\text{CNOT}}$.

$$U|+\rangle |0\rangle = U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) = \frac{|00\rangle + U|10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

I.e., we obtain an EPR pair.

2 State Identification using a POVM

a) If two states $|\psi_1\rangle \in \mathcal{H}$ and $|\psi_2\rangle \in \mathcal{H}$ are orthogonal, then they can be perfectly distinguished, i.e. there exists a measurement $M := \{M_1, M_2\}$ (or POVM $E := \{E_1, E_2\}$) so that $p_1(M, |\psi_1\rangle) = 1$ and $p_2(M, |\psi_2\rangle) = 1$. Suppose that $|\psi_1\rangle$ and $|\psi_2\rangle$ are indeed orthogonal states. Construct such a measurement that distinguishes $|\psi_1\rangle$ and $|\psi_2\rangle$ perfectly. Verify your construction by showing that the measurement matrices (or the POVM elements) satisfy the completeness condition.
Answer: We construct $M_1$ as the rank-1 projector on the subspace spanned by $|\psi_1\rangle$, i.e. $M_1 := |\psi_1\rangle\langle \psi_1|$. We let $M_2$ be the projector on the orthogonal subspace, i.e. $M_2 := \mathbb{I} - M_1$. Because both measurement matrices are projectors, the completeness condition simplifies to $\sum_{i\in\{1,2\}} M_i = \mathbb{I}$, and hence is satisfied by construction. The construction indeed distinguishes the states:

$$p_1(M, |\psi_1\rangle) = \langle \psi_1 | M_1 | \psi_1 \rangle = \langle \psi_1 | \psi_1 \rangle |\psi_1\rangle |\psi_1\rangle = 1$$

and

$$p_2(M, |\psi_2\rangle) = \langle \psi_2 | M_2 | \psi_2 \rangle = \langle \psi_2 | (\mathbb{I} - |\psi_1\rangle\langle \psi_1|) |\psi_2\rangle = \langle \psi_2 | \psi_2 \rangle - \langle \psi_2 | \psi_1 \rangle |\psi_1\rangle |\psi_2\rangle = 1 - 0 = 1,$$

where in the last line we used the orthogonality, i.e. that $\langle \psi_1 | \psi_2 \rangle = 0$.

b) Prove that if two states $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal, then they cannot be perfectly distinguished. Hint: w.l.o.g. you can assume that $|\psi_1\rangle = (1,0,\ldots,0)^T \in \mathbb{C}^d$.

Answer: Let us regard $|\psi_1\rangle$ as the first basis vector, $|1\rangle$, of some orthonormal basis $\{|j\rangle\}_{j\in[d]}$ of $\mathbb{C}^d$. We can of course represent $|\psi_2\rangle$ in that basis: $|\psi_2\rangle = \sum_{j\in[d]} \alpha_j |j\rangle$, where $\alpha_j \in \mathbb{C}$ for all $j \in J$ and where by non-orthogonality $|\alpha_1|^2 = \langle \psi_1 | \psi_1 \rangle > 0$. We will now show that it follows by linearity that requiring that $p_1(M, |\psi_1\rangle) = 1$ implies that $p_1(M, |\psi_2\rangle)$ is nonzero, which is a violation of the requirements for perfectly distinguishing the states. Choose $M_1$ such that $p_1(M, |\psi_1\rangle) = \langle \psi_1 | M_1 | \psi_1 \rangle = 1$. Then,

$$p_1(M, |\psi_2\rangle) = \langle \psi_2 | M_2 | \psi_2 \rangle = \sum_{i,j} \alpha_i \alpha_j |i\rangle \langle M_1 | j\rangle = |\alpha_1|^2 + \sum_{(i,j)\neq(1,1)} \alpha_i \alpha_j |i\rangle \langle M_1 | j\rangle > 0.$$

Consider the two qubit states $|1\rangle$ and $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ in $\mathbb{C}^2$.

c) Show that $|1\rangle$ and $|+\rangle$ are non-orthogonal states.

Answer: This comes down to showing that their inner product is nonzero:

$$\langle 1 | + \rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}.$$
The set of possible answers for Alice is $$A := \{0,1\}^n$$. Bob replies with $$b = (c, i, j) \in B := \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n$$, where $$\{i, j\}$$ is supposed to be an element of the perfect matching $$y \in \mathcal{Y}$$ that Bob received as input.

The predicate $$V$$ satisfies $$V(a, b, x, y) = 1$$ if and only if $$\{i, j\} \in y$$ and

$$(a + c) \cdot (i + j) = x_i \oplus x_j,$$

where the two “$$\oplus$$” at the left-hand side are bitwise addition mod 2, and the “.$$-symbol denotes the standard inner product mod 2.

a) For $$n = 2$$, what is the best classical strategy for Alice and Bob (i.e. achieving the highest value) that you can find for this game? (You do not have to prove optimality of your strategy.) What is the value $$v[P_{AB|XY}|(\mathcal{E})$$ for your strategy? (At least you should be able to find a strategy for which $$v[P_{AB|XY}|(\mathcal{E}) > \frac{1}{2}]$$.)

**Answer:** A simple (but not the best) strategy is the following. Alice outputs $$a$$ such that $$(a + 00) \cdot (00 + 01) = x_{00} \oplus x_{01}$$ If Bob receives the matching that contains the edge $$(00, 01)$$ (this happens with prob. 1/3) then he outputs $$c = 00$$ and in this case they always win the game. In case Bob receives one of the other two matchings (this case occurs with probability 2/3) then he outputs a random choice for $$c$$ and hence they win only with probability 1/2 in this case.

Thus,

$$v[P_{AB|XY}|(\mathcal{E}) = \frac{2}{3} \cdot \frac{1}{2} + \frac{1}{3} = \frac{2}{3}.$$
e) Bob performs a Von Neumann measurement using \( P_{ij} \) and obtains the outcome \((i,j)\). Prove that the post-measurement state is given by 
\[
|\psi''\rangle = \frac{1}{\sqrt{2}}((-1)^{x_i}|i\rangle|i\rangle + (-1)^{x_j}|j\rangle|j\rangle).
\]

**Answer:** We have to compute 
\[
|\psi''\rangle = \frac{1}{\sqrt{\langle\psi'|\mathbb{I} \otimes P_{ij}\rangle}}(\mathbb{I} \otimes P_{ij})|\psi\rangle 
\]
We’ll start by computing the expression in the denominator in the expression above,
\[
\langle\psi'|(\mathbb{I} \otimes P_{ij})|\psi\rangle = \frac{1}{N} \sum_{k,\ell} (-1)^{x_k \oplus x_k} \langle k| \mathbb{I} \otimes (|i\rangle + |j\rangle)\rangle |\ell\rangle = \frac{1}{N}((-1)^{x_i \oplus x_i} + (-1)^{x_j \oplus x_j}) = \frac{2}{N}.
\]
We’ll proceed with (1).
\[
|\psi''\rangle = \sqrt{\frac{N}{2}}(\mathbb{I} \otimes (|i\rangle + |j\rangle)) \frac{1}{\sqrt{N}} \sum_k (-1)^{x_k} |k\rangle |k\rangle = \frac{1}{\sqrt{2}} \sum_k (-1)^{x_k} (|i\rangle + |j\rangle) |k\rangle = \frac{1}{\sqrt{2}}((-1)^{x_i}|i\rangle|j\rangle + (-1)^{x_j}|j\rangle|j\rangle).
\]

f) For notational convenience, we will use \( H^\otimes n = H \otimes \cdots \otimes H \) \((n\text{ times})\).
Prove that 
\[
H^\otimes n|i\rangle = \frac{1}{\sqrt{N}} \sum_{j \in \{0,1\}^n} (-1)^{x_j}|j\rangle
\]
holds for every \(i \in \{0,1\}^n\).

**Answer:**
\[
H^\otimes n|i\rangle = \bigotimes_{k=1}^n H|i_k\rangle = \bigotimes_{k=1}^n \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_k}|1\rangle)
\]
\[
= \frac{1}{\sqrt{2^n}} \sum_{j \in \{0,1\}^n} \prod_{k=1}^n (-1)^{x_j} = \frac{1}{\sqrt{N}} \sum_{j \in \{0,1\}^n} (-1)^{x_j}|j\rangle.
\]

\[
g) \quad \text{Both players apply the } n\text{-fold Hadamard } H^\otimes n \text{ to their parts of the state. Compute the resulting state } (H^\otimes n \otimes H^\otimes n)|\psi''\rangle \text{ and argue that measuring the two parts of the resulting state (in the considered basis) gives Alice } a \in \{0,1\}^n \text{ and gives Bob } c \in \{0,1\}^n \text{ with } (a \oplus c) \cdot (i \oplus j) = x_i \oplus x_j. \\
\text{Hint: Use the relation that you’ve just proved in f).}
\]

**Answer:**
\[
(H^\otimes n)(H^\otimes n)|\psi''\rangle = (H^\otimes n)H^\otimes n \frac{1}{\sqrt{2}}((-1)^{x_i}|i\rangle|i\rangle + (-1)^{x_j}|j\rangle|j\rangle)
\]
\[
= \frac{1}{\sqrt{2}}((-1)^{x_i} H^\otimes n|i\rangle|i\rangle + (-1)^{x_j} H^\otimes n|j\rangle|j\rangle)
\]
\[
= \frac{1}{N \sqrt{2}} \left( (-1)^{x_i} \sum_{a,c \in \{0,1\}^n} (-1)^{i \cdot a \oplus i \cdot c} |a\rangle \langle c| + (-1)^{x_j} \sum_{a',c' \in \{0,1\}^n} (-1)^{j \cdot a' \oplus j \cdot c'} |a'\rangle \langle c'| \right)
\]
\[
= \frac{1}{N \sqrt{2}} \sum_{a,c \in \{0,1\}^n} \left( (-1)^{x_i \oplus i \cdot a \oplus i \cdot c} + (-1)^{x_j \oplus j \cdot a \oplus j \cdot c} \right) |a\rangle \langle c|.
\]

In this last state, only \(a, c\) that satisfy \(V(a, b, x, y)\) have non-zero amplitude, because then the exponents of the “phase terms” are equal (both zero or both one). I.e., by equating those exponents and some manipulations,
\[
x_i \oplus i \cdot a \oplus i \cdot c = x_j \oplus j \cdot a \oplus j \cdot c
\]
\[
+ x_i \oplus x_j = i \cdot a \oplus i \cdot c \oplus j \cdot a \oplus j \cdot c
\]
\[
x_i \oplus x_j = i \cdot (a \oplus c) \oplus j \cdot (a \oplus c) = (i \oplus j) \cdot (a \oplus c)
\]
we retrieve the condition for which \(V(a, b, c, d) = 1\). Hence, Alice and Bob win the game with certainty.