Quantum Cryptography
Homework Set 2

(Answer Sheet)

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 $U_{\mathtt{CNOT}} \in \mathcal{U}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ by specifying its action on basis states of the computational basis:

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

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

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

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

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

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

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

Then,

$$\begin{aligned} U_{\mathtt{CNOT}} U_{\mathtt{CNOT}}^\dagger &= (\sum_{x,y} |x\rangle|x \oplus y\rangle\langle x|\langle y|)(\sum_{x',y'} |x'\rangle|y'\rangle\langle x'|\langle x' \oplus y'|) \\ &= \sum_{x,x',y,y'} |x\rangle|x \oplus y\rangle\langle x|x'\rangle\langle y|y'\rangle\langle x'|\langle x' \oplus y'| \\ &= \sum_{x,y} |x\rangle\langle x| \otimes |x \oplus y\rangle\langle x \oplus y| = \mathbb{I} \end{aligned}$$

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

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

$$\begin{aligned} U(H|a\rangle H|b\rangle) &= U\Big(\frac{|0\rangle + (-1)^a|1\rangle}{\sqrt{2}} \frac{|0\rangle + (-1)^b|1\rangle}{\sqrt{2}}\Big) \\ &= \tfrac{1}{2}(U|00\rangle + (-1)^a U|10\rangle + (-1)^b U|01\rangle + (-1)^{a\oplus b} U|11\rangle \\ &= \tfrac{1}{2}(|00\rangle + (-1)^a|11\rangle + (-1)^b|01\rangle + (-1)^{a\oplus b}|10\rangle) \\ &= \frac{|0\rangle + (-1)^{a\oplus b}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + (-1)^b|1\rangle}{\sqrt{2}} = H|a \oplus b\rangle H|b\rangle \end{aligned}$$

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

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

$$U|+\rangle|0\rangle = U\frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle = \frac{U|00\rangle + U|10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

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 $\mathbf{M} := \{M_1, M_2\}$ (or POVM $\mathbf{E} := \{E_1, E_2\}$) so that $p_1(\mathbf{M}, |\psi_1\rangle) = 1$ and $p_2(\mathbf{M}, |\psi_2\rangle) = 1$. 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:

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

and

$$\begin{aligned} p_2(\mathbf{M}, |\psi_2\rangle) &= \langle\psi_2|M_2|\psi_2\rangle = \langle\psi_2|(\mathbb{I} - |\psi_1\rangle\langle\psi_1|)|\psi_2\rangle \\ &= \langle\psi_2|\psi_2\rangle - \langle\psi_2||\psi_1\rangle\langle\psi_1||\psi_2\rangle = 1 - 0 = 1. \end{aligned}$$

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 $|\psi_1\rangle = (1, 0, \dots, 0)^\dagger \in \mathbb{C}^d$.

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 $|\alpha_1| = |\langle\psi_1|\psi_2\rangle| > 0$. We will now show that it follows by linearity that requiring that $p_1(\mathbf{M}, |\psi_1\rangle) = 1$ implies that $p_1(\mathbf{M}, |\psi_2\rangle)$ is nonzero, which is a violation of the requirements for perfectly distinguishing the states. Choose M_1 such that $p_1(\mathbf{M}, |\psi_1\rangle) = \langle\psi_1|M_1|\psi_1\rangle = 1$. Then,

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

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:

$$\langle 1|+\rangle = \langle 1|\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}.$$

We know that non-orthogonal states cannot be perfectly distinguished. Nevertheless, we can construct a three-outcome POVM $\mathbf{E} := \{E_1, E_+, E_?\}$ that correctly distinguishes the states or returns "?". Formally, we require that $p_1(\mathbf{E}, |+\rangle) = 0 = p_+(\mathbf{E}, |1\rangle)$. We define E_1 and E_+ as $E_1 := \alpha P_+^\perp$ and $E_+ := \alpha P_1^\perp$, where the $\{P_i^\perp\}_{i\in\{1,+\}}$ are rank-1 projectors on the subspaces *orthogonal* to $|1\rangle$ and $|+\rangle$ respectively, and $\alpha \in \mathbb{R}$ is a scalar.

d) Find $P_1^\perp$ and $P_+^\perp$.

Answer:

$$P_1^\perp := |0\rangle\langle 0| \qquad P_+^\perp := |-\rangle\langle -|.$$

The third POVM element, $E_?$, represents the inconclusive result and is defined as $E_? := \mathbb{I} - E_1 - E_+$. Because $E_?$ is a POVM element, it needs to be positive semidefinite.

e) Determine the largest α such that $E_?$ is positive semidefinite. *Hint:* Use the fact that a matrix is positive semidefinite if all of its eigenvalues are nonnegative.

Answer:

$$\begin{aligned} E_? &= \mathbb{I} - \alpha(P_1^\perp + P_+^\perp) = \mathbb{I} - \alpha\big(|0\rangle\langle 0| + \tfrac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)\big) \\ &= \mathbb{I} - \alpha(\tfrac{3}{2}|0\rangle\langle 0| - \tfrac{1}{2}|0\rangle\langle 1| - \tfrac{1}{2}|1\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|) \\ &= \begin{pmatrix} 1 - \frac{3}{2}\alpha & \frac{1}{2}\alpha \\ \frac{1}{2}\alpha & 1 - \frac{1}{2}\alpha \end{pmatrix} \end{aligned}$$

We find the eigenvalues via the charateristic equation:

$$\begin{aligned} \det(E_? - \lambda\mathbb{I}) &= (1 - \tfrac{1}{2}\alpha - \lambda)(1 - \tfrac{3}{2}\alpha - \lambda) - \tfrac{1}{4}\alpha^2 \\ &= \lambda^2 + (2\alpha - 2)\lambda + (1 - 2\alpha + \tfrac{1}{2}\alpha^2) \end{aligned}$$

Solve $\det(E_? - \lambda\mathbb{I}) = 0$ for λ gives $\lambda_{1,2} = \frac{1}{2}(2 - 2\alpha \pm \alpha\sqrt{2})$. Setting $\lambda_{12} = 0$ and solving for positive α yields $\alpha = 2/(2 + \sqrt{2})$.

3 Non-Local Games

Let $N := 2^n$ for some $n \in \mathbb{N}$. Consider the game $\mathfrak{G} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \pi, V)$ played by Alice and Bob. Inputs for Alice are taken from $\mathcal{X} := \{0, 1\}^N$; we understand $x \in \mathcal{X}$ as a sequence $x = (x_i)_{i\in\{0,1\}^n}$ of bits indexed by n-bit strings. The set of Bob's possible inputs, $\mathcal{Y}$, is the set of all perfect matchings on $\{0,1\}^n$. A *perfect matching* on $\{0,1\}^n$ is a disjoint decomposition of $\{0,1\}^n$ into $N/2$ pairs, i.e., it is a set $y = \{\{i_1, j_1\}, \dots, \{i_{N/2}, j_{N/2}\}\}$ such that $\{0,1\}^n = \bigcup_{k\in[N/2]}\{i_k, j_k\}$. Figure 1 depicts the set of all perfect matchings on $\{0,1\}^2$. The distribution π is uniform on $\mathcal{X} \times \mathcal{Y}$.

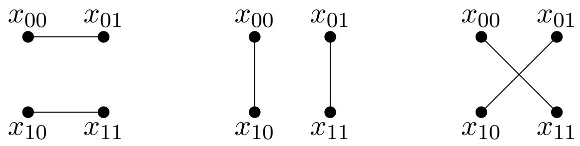

Figure 1: The set of all perfect matchings on $\{0,1\}^2$, depicted as graphs.

The set of possible answers for Alice is $\mathcal{A} := \{0,1\}^n$. Bob replies with $b = (c, i, j) \in \mathcal{B} := \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n$, 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

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

where the two "$\oplus$" at the left-hand side are *bitwise* addition mod 2, and the "$\cdot$"-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 $v[P_{AB|XY}](\mathfrak{G})$ for your strategy? (At least you should be able to find a strategy for which $v[P_{AB|XY}](\mathfrak{G}) > \frac{1}{2}$).)

Answer: A simple (but not the best) strategy is the following. Alice outputs a such that $(a \oplus 00) \cdot (00 \oplus 01) = x_{00} \oplus x_{01}$. 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 thic case.
Thus,

$$v[P_{AB|XY}](\mathfrak{G}) = \frac{2}{3} \cdot \frac{1}{2} + \frac{1}{3} = \frac{2}{3}.$$

In the remainder of this exercise we will see that $v_q(\mathfrak{G}) = 1$ by deriving a (quantum) strategy for Alice and Bob that, when Alice and Bob share n EPR pairs, achieves this optimal value.

b) Let $\{|i\rangle\}_{i\in\{0,1\}^n}$ be an orthonormal basis for $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^N$. Let $U_x := \sum_{i\in\{0,1\}^n}(-1)^{x_i}|i\rangle\langle i|$. Prove that U_x is a unitary matrix.

Answer:

$$U_x^\dagger U_x = \sum_{i,j\in\{0,1\}^n} (-1)^{x_i\oplus x_j}|i\rangle\langle i||j\rangle\langle j| = \sum_{i\in\{0,1\}^n} (-1)^{x_i\oplus x_i}|i\rangle\langle i| = \mathbb{I}$$

Alice and Bob share the state $|\psi\rangle := \frac{1}{\sqrt{N}}\sum_{i\in\{0,1\}^n}|i\rangle|i\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$.

c) Given her input $x \in \mathcal{X}$, Alice applies U_x to her part of the state. Compute the resulting state $|\psi'\rangle := (U_x \otimes \mathbb{I})|\psi\rangle$.

Answer:

$$\begin{aligned}|\psi'\rangle &= (U_x \otimes \mathbb{I})|\psi\rangle = (\sum_{i\in\{0,1\}^n}(-1)^{x_i}|i\rangle\langle i| \otimes \mathbb{I})(\frac{1}{\sqrt{N}}\sum_{j\in\{0,1\}^n}|j\rangle|j\rangle)\\ &= \frac{1}{\sqrt{N}}\sum_{i,j}(-1)^{x_i}\langle i|j\rangle|i\rangle|j\rangle = \frac{1}{\sqrt{N}}\sum_{i}(-1)^{x_i}|i\rangle|i\rangle\end{aligned}$$

Let $P_{ij} := |i\rangle\langle i| + |j\rangle\langle j|$ for every $(i, j) \in y$ where $y \in \mathcal{Y}$.

d) Show that P_{ij} is an orthogonal projector for every edge $(i, j) \in y$. Furthermore, what is the rank of P_{ij} for every edge $(i, j) \in y$? What is the rank of the matrix $Q = |i\rangle\langle i| + |i\rangle\langle i|$? Is Q a projector? Why (not)?

Answer: First of all, note that $P_x := |x\rangle\langle x|$ is an orthogonal projector because $P_x = P_x^\dagger$ and $P_xP_x = |x\rangle\langle x||x\rangle\langle x| = |x\rangle\langle x| = P_x$. Note furthermore that P_x has rank 1. Since (i, j) is an edge from y, it holds that $i \neq j$. Hence, $|i\rangle$ and $|j\rangle$ are always orthogonal, hence the corresponding projectors project to orthogonal subspaces, and therefore the rank of P_{ij} for every $(i, j) \in y$ is two. The projector P_{ij} is obviously Hermitian and

$$\begin{aligned}P_{ij}P_{ij} &= (|i\rangle\langle i| + |j\rangle\langle j|)(|i\rangle\langle i| + |j\rangle\langle j|)\\ &= |i\rangle\langle i||j\rangle\langle j| + |i\rangle\langle i||j\rangle\langle j| + |j\rangle\langle j||i\rangle\langle i| + |j\rangle\langle j||j\rangle\langle j| = |i\rangle\langle i| + |j\rangle\langle j|,\end{aligned}$$

hence P_{ij} is an orthogonal projector for every edge $(i, j) \in y$. The rank of Q is only one, and Q is not a projector because $QQ = (2|i\rangle\langle i|)(2|i\rangle\langle i|) = 4|i\rangle\langle i| = 2Q \neq Q$.

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

$$|\psi''\rangle = \frac{1}{\sqrt{2}}\big((-1)^{x_i}|i\rangle|i\rangle + (-1)^{x_j}|j\rangle|j\rangle\big).$$

Answer: We have to compute

$$|\psi''\rangle = \frac{1}{\sqrt{\langle\psi'|(\mathbb{I}\otimes P_{ij})|\psi'\rangle}}(\mathbb{I}\otimes P_{ij})|\psi'\rangle \tag{1}$$

We'll start by computing the expression in the denominator in the expression above,

$$\begin{aligned}\langle\psi'|(\mathbb{I}\otimes P_{ij})|\psi'\rangle &= \frac{1}{N}\sum_{k,\ell}(-1)^{x_k\oplus x_\ell}\langle k|\langle k|(\mathbb{I}\otimes(|i\rangle\langle i| + |j\rangle\langle j|))|\ell\rangle|\ell\rangle \\ &= \frac{1}{N}\big((-1)^{x_i\oplus x_i} + (-1)^{x_j\oplus x_j}\big) = \frac{2}{N}.\end{aligned}$$

We'll proceed with (1).

$$\begin{aligned}|\psi''\rangle &= \sqrt{\frac{N}{2}}(\mathbb{I}\otimes(|i\rangle\langle i| + |j\rangle\langle j|)\frac{1}{\sqrt{N}}\sum_k(-1)^{x_k}|k\rangle|k\rangle \\ &= \frac{1}{\sqrt{2}}\sum_k(-1)^{x_k}(\mathbb{I}\otimes(|i\rangle\langle i| + |j\rangle\langle j|))|k\rangle|k\rangle \\ &= \frac{1}{\sqrt{2}}\big((-1)^{x_i}|i\rangle|i\rangle + (-1)^{x_j}|j\rangle|j\rangle\big).\end{aligned}$$

f) For notational convenience, we will use $H^{\otimes n} = H\otimes\cdots\otimes H$ (n times). Prove that

$$H^{\otimes n}|i\rangle = \frac{1}{\sqrt{N}}\sum_{j\in\{0,1\}^n}(-1)^{i\cdot j}|j\rangle$$

holds for every $i\in\{0,1\}^n$.

Answer:

$$\begin{aligned}H^{\otimes n}|i\rangle &= \bigotimes_{k=1}^{n} H|i_k\rangle = \bigotimes_{k=1}^{n}\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{i_k}|1\rangle) \\ &= \frac{1}{\sqrt{2^n}}\sum_{j\in\{0,1\}^n}|j\rangle\prod_{k=1}^{n}(-1)^{i_k j_k} = \frac{1}{\sqrt{N}}\sum_{j\in\{0,1\}^n}(-1)^{i\cdot j}|j\rangle.\end{aligned}$$

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

Answer:

$$\begin{aligned}(H^{\otimes n})(H^{\otimes n})|\psi''\rangle &= (H^{\otimes n})(H^{\otimes n})\frac{1}{\sqrt{2}}\big((-1)^{x_i}|i\rangle|i\rangle + (-1)^{x_j}|j\rangle|j\rangle\big) \\ &= \frac{1}{\sqrt{2}}\big((-1)^{x_i}H^{\otimes n}|i\rangle H^{\otimes n}|i\rangle + (-1)^{x_j}H^{\otimes n}|j\rangle H^{\otimes n}|j\rangle\big) \\ &= \frac{1}{N\sqrt{2}}\Big((-1)^{x_i}\sum_{a,c\in\{0,1\}^n}(-1)^{i\cdot a\oplus i\cdot c}|a\rangle|c\rangle \\ &\qquad + (-1)^{x_j}\sum_{a',c'\in\{0,1\}^n}(-1)^{j\cdot a'\oplus j\cdot c'}|a'\rangle|c'\rangle\Big) \\ &= \frac{1}{N\sqrt{2}}\sum_{a,c\in\{0,1\}^n}\Big((-1)^{x_i\oplus i\cdot a\oplus i\cdot c} + (-1)^{x_j\oplus j\cdot a\oplus j\cdot c}\Big)|a\rangle|c\rangle.\end{aligned}$$

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,

$$\begin{aligned}x_i\oplus i\cdot a\oplus i\cdot c &= x_j\oplus j\cdot a\oplus j\cdot c \\ x_i\oplus x_j &= i\cdot a\oplus i\cdot c\oplus j\cdot a\oplus j\cdot c \\ x_i\oplus x_j &= i\cdot(a\oplus c)\oplus j\cdot(a\oplus c) = (i\oplus j)\cdot(a\oplus c)\end{aligned}$$

we retrieve the condition for which $V(a, b, c, d) = 1$. Hence, Alice and Bob win the game with certainty.