Quantum Cryptography

Homework Set 2

Please send your answers – either typeset on a computer, or handwritten (but readable) and scanned, preferably in PDF format – to `bouman@cwi.nl` *before March 14, 23h59. Do not forget to put your name on the first page. Good luck!*

1 The CNOT Gate

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

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

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

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

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

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

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.

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

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.

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 $P_+^\perp$.

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.

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 $y = \{\{i_1, j_1\}, \ldots, \{i_{N/2}, j_{N/2}\}\}$ 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 $\mathcal{X} \times \mathcal{Y}$.

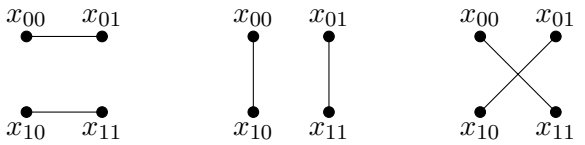

Figure 1: The set of all perfect matchings on $\{0,1\}^2$, depicted as graphs.

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 $v[P_{AB|XY}](\mathfrak{G}) > \frac{1}{2}$.)

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.

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 $|\psi'\rangle := (U_x \otimes \mathbb{I})|\psi\rangle$.

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)?

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

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

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

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).