QSIT: Quantum Information Theory.
Series 11.

Autumn 2012
Prof. M. Christandl

Exercise 1. *Properties of the variational distance*

Given two probability distributions P_X and Q_X with the same alphabet, the variational distance between them is defined as

$$D(P_X, Q_X) = \frac{1}{2} \sum_x |P_X(x) - Q_X(x)|. \tag{1}$$

(a) **Operational meaning.** Suppose that you are given one of two dice, P and Q, at random with equal probability. Your task is to guess which die you were given. You know that both dice are biased: the probability of obtaining the different outcomes $X = \{1, \dots, 6\}$ are given by distributions P_X for die P and Q_X for Q. You are allowed to throw the die only once. Show that your probability of guessing correctly is given by

$$\Pr(\checkmark) = \frac{1}{2}\left(1 + D(P_X, Q_X)\right). \tag{2}$$

(b) **Triangle inequality.** Show that, for any three probability distributions P_X, Q_X and R_X,

$$D(P_X, Q_X) + D(Q_X, R_X) \geq D(P_X, R_X). \tag{3}$$

(c) **Distance to uniform distribution.** Let $P_X = (p, 1-p)$ be a binary probability distribution. Show that

$$D(P_X, 1 - P_X) = 2D(P_X, U_x), \tag{4}$$

where $U_X = (\frac{1}{2}, \frac{1}{2})$ is the uniform distribution.

(d) **Joint distributions.** Let P_{XY} be a joint probability distribution, with marginals P_X and P_Y that have the same alphabet. Show that

(i) $D(P_X, P_Y) \leq \Pr[X \neq Y]$,

(ii) $D(1 - P_X, P_Y) \leq \Pr[X = Y]$.

Exercise 2. *Playing Eve*

You are Eve, and are trying your best to thwart Alice and Bob's plans to share a secret key using the quantum key distribution protocol BB84. You will hack into their insecure quantum channel, capture the qubit sent by Alice, measure it in some basis, and then send it to Bob. [Note that this is not the most general attack possible.] You are trying to pick the best possible basis to measure Alice's qubit. Remember that you want to minimize the errors that can be detected by Alice and Bob, while trying to maxime the number of bits you guess correctly. Let's try a few different bases. For each case, compute the fraction of bits that you guess correctly, and the error rate induced in Alice and Bob's key, after sifting.

(a) In your first attempt, you will measure all of Alice's qubits in the Z basis.

(b) In your second attempt, you will pick X or Z at random, with equal probability, for each qubit.

(c) More generally, you can measure in an orthonormal basis of the form

$$\left\{ \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle, \cos\frac{\theta+\pi}{2}|0\rangle + \sin\frac{\theta+\pi}{2}|1\rangle \right\}.$$

For instance, picking $\theta = 0$ gives you the Z basis, while $\theta = \frac{\pi}{2}$ results in the X basis. What happens for $\theta = \frac{\pi}{4}$?

Exercise 3. ***Chained Bell inequalities***

Consider the following setting. Alice and Bob own one black box each. Alice's box takes an input a from a set $A = \{0, 2, \ldots, 2N-2\}$ and outputs a bit $x \in \{0,1\}$. Similarly, Bob's box takes an input b from a set $B = \{1, 3, \ldots, 2N-1\}$ and outputs $y \in \{0,1\}$.

We define the following measure of correlations,

$$I_N = \Pr(X = Y | A = 0, B = 2N-1) + \sum_{|a-b|=1} \Pr(X \neq Y | A = a, B = b) \tag{5}$$

We want I_N to be small, because then it is possible to show that the outcomes of adjacent inputs a and $b = a \pm 1$ are the same, and unknown to an adversary, with high probability. [This is a generalization of the theorem from the lecture, with $I_2 \mapsto I_N$.]

(a) We will see a physical example of a family of "black boxes" that achieves $I_N \to 0$. Each box corresponds to a quantum measurement device that acts on a single qubit. The qubits to be measured, one in Alice's box and one in Bob's, are maximally entantled.

Let $\{|\uparrow\rangle, |\downarrow\rangle\}$ be an orthonormal basis for a qubit (for instance the Z basis). Suppose that Alice's choices of input a correspond to a POVM $\{E_0^a, E_1^a\}$, on a single qubit, with E_0^a is the projector onto state $|\frac{a}{2N}\pi\rangle$, and E_1^a is the projector onto state $|\left(\frac{a}{2N}+1\right)\pi\rangle$, with $|\theta\rangle = \cos\frac{\theta}{2}|\uparrow\rangle + \sin\frac{\theta}{2}|\downarrow\rangle$. The same holds for Bob's measurements b. Furthermore, suppose that the POVMs on Alice's and Bob's sides act each on a qubit of the Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Show that, in these conditions,

$$I_N = 2N \sin^2 \frac{\pi}{4N} \leq \frac{\pi^2}{8N}. \tag{6}$$

(b) How would you adapt the protocol from the lecture to take advantge of this Bell inequality?