Q. Inf. Science 3 (8.372 / 18.S996) — Fall 2022

Assignment 1

Due: **Friday**, *Sep 16, 2022 at* ***5pm***

Turning in your solutions: Upload a single pdf file (typed or neatly handwritten) to gradescope.

Collaboration policy: You may work individually or together in small groups but should write up your solutions individually.

Recommended collaboration approach: We recommend that you find 1-2 other people to work with. You can use psetpartners.mit.edu to find partners if you don't already know people in the class.

Then for each problem, attempt it first on your own, and work until you get stuck. When you meet with the group, discuss each problem *even if you've already solved it.* If the whole group is stuck then we can answer questions on Piazza, in office hours, and can also schedule meetings at other times.

1. **Trace distance** [50 pts]

   Suppose that you are given one of two possible d-dimensional states σ_1 or σ_2, with probabilities p_1 and $p_2 = 1 - p_1$ respectively. Your task is to perform a two-outcome measurement and then try to guess which state you had been given, minimizing the probability of error.

   If the measurement elements are nonnegative Hermitian matrices $M_1 = M$ and $M_2 = I - M$ then the probability of guessing wrong is

   $$P_{err} = p_1 \operatorname{tr}(\sigma_1 M_2) + p_2 \operatorname{tr}(\sigma_2 M_1). \tag{1}$$

   (a) [4 pts] Show that

   $$P_{err} = p_1 + \operatorname{tr}[M\Delta], \tag{2}$$

   where $\Delta = p_2\sigma_2 - p_1\sigma_1$.

   (b) [15 pts] *Math interlude: duality of S_1 and S_∞ norms.* Consider Hermitian matrices X, Λ. Let $\|X\|_1$ denote the Schatten 1-norm, i.e. the sum of the absolute values of the eigenvalues of X, and let $\|\Lambda\|_\infty$ denote the Schatten ∞-norm, i.e. the maximum absolute value of the eigenvalues of Λ. Prove that

   $$\|X\|_1 = \max_{\|\Lambda\|_\infty \le 1} \operatorname{tr}[X\Lambda] \tag{3}$$

   $$\|\Lambda\|_\infty = \max_{\|X\|_1 \le 1} \operatorname{tr}[X\Lambda] \tag{4}$$

   (These relations say that the Schatten 1-norm and the Schatten ∞-norm are *dual* to each other.)

(c) [15 pts] Find the PSD operator M that minimizes P_{err}. Show that the resulting error probability is $P_{err,opt} = p_1 - \sum_{i:\lambda_i<0} |\lambda_i|$, where $\{\lambda_i\}$ are the eigenvalues of Δ.

(d) [16 pts] Evaluate $P_{err,opt}$ in the following cases:

i. $p_1 = 1$, $p_2 = 0$ and σ_1, σ_2 are arbitrary.

ii. $p_1 \geq p_2 \geq 0$ are arbitrary (subject to $p_1 + p_2 = 1$) and $\sigma_1 = \sigma_2$.

iii. $p_1 = p_2 = \frac{1}{2}$ and σ_1, σ_2 are arbitrary. Express your answer in terms of $\|\sigma_1 - \sigma_2\|_1$.

iv. $p_1 = p_2 = \frac{1}{2}$, $\sigma_1 = |\psi_1\rangle\langle\psi_1|$, $\sigma_2 = |\psi_2\rangle\langle\psi_2|$. Express your answer in terms of $|\langle\psi_1|\psi_2\rangle|^2$.

2. **Bit commitment** [50 points; 10 / section]

(a) Consider the following bit commitment (BC) protocol. Alice samples a uniformly random bit $r \in \{0, 1\}$. To commit to a bit b, in the commit phase she sends Bob a qubit $|\psi\rangle := H^b |r\rangle$ (with H the Hadamard gate), or more concretely:

b	r	$\|\psi\rangle$
0	0	$\|0\rangle$
0	1	$\|1\rangle$
1	0	$\|+\rangle$
1	1	$\|-\rangle$

In the reveal phase, she tells Bob b, r, he measures in the basis defined by b (i.e. either $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$) and checks whether he has the claimed state. If so he accepts, and otherwise he rejects.

Note that this description of the protocol is for what honest participants should do. Security requires that it remain binding/hiding even when Alice/Bob deviates from the honest protocol arbitrarily.

Is this scheme valid? Hiding? Binding? Prove your answers. (Don't just cite the no-go theorem. If the answer to one of these is "no" because of an attack on the protocol, you should explicitly describe it.)

(b) Since that first protocol didn't work, let's try again. Consider a scheme that is the same as above except now $|\psi\rangle = H^r |b\rangle$, i.e.

b	r	$\|\psi\rangle$
0	0	$\|0\rangle$
0	1	$\|+\rangle$
1	0	$\|1\rangle$
1	1	$\|-\rangle$

Now the measurement basis is determined by r, not b, but still Bob can check whether his qubit is indeed in the state $|\psi\rangle$ corresponding to the values of r, b that Alice tells him.

Again determine whether the scheme is perfectly valid, hiding and/or binding.

Here the answers to the hiding/binding questions may be that they are neither perfectly binding nor hiding. To quantify this, suppose that after the commit phase Bob attempts to guess b. In a perfectly hiding protocol, his probability of success P_{guess} would be $1/2$. (Assume for simplicity that b is uniformly distributed.) How high can his P_{guess} be in this protocol?

Suppose that Bob plays honestly and Alice acts arbitrarily up to the commit phase. Describe Alice's actions by the variable $\mathcal{A}$. Now suppose that after the commit phase, Alice attempts to reveal the bit b, i.e. telling Bob that her bit was b all along. (Here $\mathcal{A}$ could have been a commitment to a determinstic or random bit, or something else entirely.) Let $\Pr[\text{accept } b|\mathcal{A}]$ be the probability that she convinces Bob to accept b. We abbreviate this by $P_b := \Pr[\text{accept } b|\mathcal{A}]$, leaving the $\mathcal{A}$ dependence implicit. In a perfectly binding protocol, we should have

$$\max_{\mathcal{A}}[P_0 + P_1] \leq 1 \tag{5}$$

The important feature of this equation is that Alice's actions before the commit phase do not depend on her choice of bit b, but after the commit phase, they do.

In this protocol, is $\max_{\mathcal{A}}[P_0 + P_1]$ equal to 1 or > 1? If $= 1$ then justify your answer. If > 1, then describe a protocol for Alice achieving this.

(c) Suppose that the qubits are stored in photons, which are relatively easy to prepare and measure, but hard to store for long periods of time. What implications, if any, does this have for the practical security of the scheme in part (a)?

(d) Suppose that Alice and Bob can perform a BC scheme that is perfectly valid and binding but imperfectly hiding, so that $P_{\text{guess}} = 1/2 + \epsilon$. Analyze the following "hiding amplification" scheme. Alice wishes to commit the bit b. She chooses bits b_1, b_2 randomly subject to the constraint that $b_1 + b_2 = b \bmod 2$, i.e. if $b = 0$ then b_1, b_2 are either $0, 0$ or $1, 1$ and if $b = 1$ then b_1, b_2 are either $0, 1$ or $1, 0$. Then she commits bits b_1 and b_2 separately with the original imperfect scheme. After Alice reveals b_1, b_2, Bob uses these to compute b. How well hidden is b? i.e. in the new scheme, what is P_{guess}? Assume that Bob's best strategy is just to try to guess b_1 and b_2 separately, and not to make any kind of collective measurement.

(e) Suppose that Alice and Bob have a protocol for performing oblivious transfer (OT), also known as "1 out of 2 oblivious transfer". In OT, Alice inputs bits x_0, x_1, Bob inputs a bit b, Alice receives no output and Bob receives only the output x_b. In other words, he learns one of Alice's input bits but not the other, and Alice doesn't learn which one Bob chose.

Show how the ability to perform OT implies the ability to perform BC. The BC protocol should be almost perfect, meaning perfectly or almost perfectly hiding, binding and valid. For partial credit, show how to achieve a BC protocol that yields some improvement over what is possible with only classical communication.