IDEA League School - Quantum Information - Aachen 2015
Randomness, Entropy and QKD
Solutions

March 28, 2015

1. (Distinguishing quantum states) To distingiush the two states, we perform a measurement with two outcomes '0' and '1'. When we get outcome '0' we will guess that the state was ρ_0, and when we get outcome '1', we will guess ρ_1. Since we only care about the probability of success, we can consider a POVM described by measurement operators M_0, M_1 satisfying $M_0, M_1 \geq 0$ and $M_0 + M_1 \leq \mathbb{I}$, where we associate the subscript with the measurement outcome. The probability of obtaining measurement outcome x, given the state was actually ρ_x can then be written as $\mathrm{tr}(M_x\rho_x)$. For a particular choice of measurement, the success probability can thus be written as

$$P_{\mathrm{succ}} = p_0 \,\mathrm{tr}(M_0\rho_0) + p_1 \,\mathrm{tr}(M_1\rho_1) = \frac{1}{2}\,\mathrm{tr}(M_0\rho_0) + \frac{1}{2}\,\mathrm{tr}(M_1\rho_1)\ . \tag{1}$$

Using the fact that $M_1 = \mathbb{I} - M_0$ we can rewrite this as

$$P_{\mathrm{succ}} = \frac{1}{2}\,\mathrm{tr}(M_0\rho_0) + \frac{1}{2}(\mathrm{tr}(\rho_1) - \mathrm{tr}(M_0\rho_0)) = \frac{1}{2} + \frac{1}{2}\,\mathrm{tr}(M_0(\rho_0 - \rho_1))\ , \tag{2}$$

which allows you to evaluate the success probability for your choice of measurement. Let us now find the optimal measurement. To maximize this quantity we want to maximize $\mathrm{tr}(M_0 A)$ where $A = \rho_0 - \rho_1$ over all $0 \leq M_0 \leq \mathbb{I}$. Note that since A is a Hermitian operator, we can compute its eigendecomposition

$$A = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j| \tag{3}$$

for eigenvalues λ_j and (normalized) eigenvectors $|\psi_j\rangle$. We can write $A = A^+ - A^-$ for

$$A^+ = \sum_{\lambda_j \geq 0} \lambda_j |\psi_j\rangle\langle\psi_j| \tag{4}$$

$$A^- = \sum_{\lambda_j < 0} |\lambda_j| |\psi_j\rangle\langle\psi_j| \tag{5}$$

$$\tag{6}$$

Note that $A^+, A^- \geq 0$, and hence since $M_0 \geq 0$ we have $\mathrm{tr}(A^+ M_0) \geq 0$ and $\mathrm{tr}(A^- M_0) \geq 0$. Using furthermore that $M_0 \leq \mathbb{I}$ and hence $\mathrm{tr}(A^+ M_0) \leq \mathrm{tr}(A^+)$ we have

$$\mathrm{tr}(AM_0) = \mathrm{tr}(A^+ M_0) - \mathrm{tr}(A^- M_0) \leq \mathrm{tr}(A^+ M_0) \leq \mathrm{tr}(A^+) \ . \tag{7}$$

Equality is achieved for

$$M_0 = \sum_{\substack{j \\ \lambda_j \geq 0}} |\psi_j\rangle\langle\psi_j| \ . \tag{8}$$

To maximize the probability of distingiushing ρ_0 and ρ_1 we thus perform a measurement in which M_0 is the projector onto the positive eigenspace of $A = \rho_0 - \rho_1$.

In our example, we have

$$A = \rho_0 - \rho_1 = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \ . \tag{9}$$

The eigenvalues of A are $1/\sqrt{2}$ and $-1/\sqrt{2}$ with unormalized eigenvectors $v_1 = (-1-\sqrt{2}, 1)$ and $v_2 = (-1+\sqrt{2}, 1)$ respectively. The best measurement is thus given by

$$M_0 = |\Phi\rangle\langle\Phi| \ \text{ with } |\Phi\rangle = v_1/\sqrt{2(2+\sqrt{2})} \ , \tag{10}$$

$$M_1 = \mathbb{I} - M_0 \tag{11}$$

The success probability is then

$$P_{\mathrm{succ}} = \frac{1}{2} + \frac{1}{2\sqrt{2}} \ . \tag{12}$$

2. (Distingiushing classical states) Given we see symbol s, we are going to make a guess for the die for which this symbol was the most likely one. That is, given s we will guess die $x \in \{0, 1\}$ such that $x = \mathrm{argmax}_x \, p_{x|s}$ where $p_{x|s}$ is the probability the die was x given symbol s . For our example, this means we will guess die 0, if $1 \leq s \leq 5$ and die 1 if $s = 6$. In quantum language, our problem is equivalent to distingiushing states ρ_0 and ρ_1 which have the probabilities on the diagonal. That is,

$$\rho_0 = diag(1/6, 1/6, 1/6, 1/6, 1/6, 1/6) \tag{13}$$

$$\rho_1 = diag(1/7, 1/7, 1/7, 1/7, 1/7, 2/7) \ . \tag{14}$$

By the same argument as above, we obtain $p_{\mathrm{succ}} \approx 0.56$. As a remark aside, noting that $\mathrm{tr}(A^+) = \mathrm{tr}(A^-)$ since $\mathrm{tr}(A) = \mathrm{tr}(\rho_0 - \rho_1) = 0$ we see that

$$P_{\mathrm{succ}} = \frac{1}{2} + \frac{1}{4} \sum_{x \in \{1,\ldots,6\}} |P_X(x) - P_Y(x)| \ . \tag{15}$$

The quantity $1/2 \sum_x |P_X(x) - P_Y(x)|$ is precisely the statistical distance between the two distributions.

3. (Min-entropy)

   (a) $H_{\min}(X) = -\log_2 \max_x P_X(x) = -\log_2 2/3 \approx 0.585$

   (b) $H_{\min}(X|E) = -\log_2 P_{\text{guess(X|E)}}$ where $P_{\text{guess}}(X|E)$ is the probability of guessing X given E, maximized over all choices of measurements on E. We already computes this above $P_{\text{guess}}(X|E) = 1/2 + 1/(2\sqrt{2})$ given a min-entropy $H_{\min}(X|E) \approx 0.22$.

4. (Key exchange)

   (a) Alice and Bob generate two bit strings $r_A = r_A^1 \dots r_A^n \in \{0,1\}^n$ and $r_B = r_B^1 \dots r_B^n \in \{0,1\}^n$ respectively uniformly at random, and write them on the anonymous message board. They now compare all n bits: if $r_A^j = r_B^j$, then Alice and Bob discard bit j. Otherwise Alice sets key bit j to $k_A^j = r_A^j$, and Bob sets $k_B^j = 1 - r_B^j$. Note that the protocol is correct: $k_A = k_B$, i.e., Alice and Bob output the same key. To see that the protocol is secure note that in every round j the eavesdropper does not know whether r_A^j and r_B^j came from Alice or Bob respectively. Since Alice and Bob, chose their bits uniformly at random, from the perspective of Eve both $k_A^j = 0$ and $k_B^j = 1$ are equally likely.

   (b) Let X_A denote the string Alice generated in the rounds where $r_A^j \neq r_B^j$. Let X_B denote the corresponding string for Bob, where Bob has fillipped each bit such that $X_A = X_B$. Let ℓ be the length of this string. Using the chain rule of the min-entropy $H_{\min}(X_A|E) \geq H_{\min}(X_A) - \log|E| = H_{\min}(X_A) - 512$. Since the bits were randomly generated $H_{\min}(X_A) = \ell$. Thus $H_{\min}(X|E) \geq \ell - 512$. Thus if $\ell > 512$ Alice and Bob can still hope to generate a key: Instead of using the procedure above to produce the key directly, they use randomness extraction (privacy amplification). After the protocol above, Alice chooses a hash function indexed by the seed r and outputs the key $K_A = Ext(X_A, r)$. She communicates the hash function to Bob using a classical authenticated channel, and Bob computes $K_B = Ext(X_B, r)$. Since $X_A = X_B$, we have $K_A = K_B$ and hence the protocol is correct. The properties of privacy amplification ensure that the protocol remains secure. Specifically, the key will be ϵ-secure as long as the length m of the key obeys $m < \ell - 512 - 2\log(1/\epsilon)$.

5. Bonus question

   (a) We want to show that $D(\rho_{Ext(X,R)}, \frac{\mathbb{I}}{2^m} \otimes \rho_R) \leq \epsilon$. That is, the output is uniform and uncorrelated from the seed R. For simplicity, we have assumed that E is trivial in this exercise.

   (b) Note that a collision occurs $(R, Ext(X,R)) = (R', Ext(X', R')$ if and only if $R = R'$ and either $X = X'$, or if $X \neq X'$ but nevertheless $Ext(X,R) = Ext(X', R')$. Hence

$$p_{\text{coll}} := Pr[(R, Ext(X,R) = (R', Ext(X', R'))] \tag{16}$$

$$= Pr[R = R'] \left(Pr[X = X'] + Pr[Ext(X,R) = Ext(X', R') | X \neq X'] \right) \tag{17}$$

$$\leq \frac{1}{|\mathcal{F}|} \left(\frac{1}{k} + \frac{1}{2^m} \right). \tag{18}$$

where we have used the fact that there are $|\mathcal{F}|$ possible values for R, and R is chosen uniformly, the fact that $H_{\min}(X) \geq k$ and hence $p_x \leq 1/2^k$, and finally we have

$$Pr[Ext(X,R) = Ext(X',R')|X \neq X'] \leq \frac{1}{2^m} \ , \tag{19}$$

by the definition of a two-universal set of hash functions. Using that $k = m + 2\log(1/\epsilon)$ we obtain $p_{\text{coll}} \leq (1+\epsilon^2)/(|\mathcal{F}|2^m)$.

(c) We have

$$\sum_x (P_X(x) - P_Y(x))^2 \leq \sum_x P_X(x)^2 + P_Y(x)^2. \tag{20}$$

Hence we can bound

$$L2(\rho_{Ext(X,R)R}, \frac{\mathbb{I}}{|\mathcal{F}|} \otimes \frac{\mathbb{I}}{2^m}) \leq \frac{1}{2}\sqrt{p_{\text{coll}} + \frac{1}{|\mathcal{F}|2^m}} \tag{21}$$

$$\leq \frac{1}{2}\sqrt{\frac{\epsilon^2}{|\mathcal{F}|2^m}} \ . \tag{22}$$

(d) We can now use the relation of the L2 and the statistical distance. Noting that the size of the set $\mathcal{S}$ is given by $|\mathcal{S}| = |\mathcal{F}2^m$ for our example, we obtain

$$D(\rho_{Ext(X,R)R}, \frac{\mathbb{I}}{|\mathcal{F}|} \otimes \frac{\mathbb{I}}{2^m}) \leq \sqrt{|\mathcal{F}|2^m} L2(\rho_{Ext(X,R)R}, \frac{\mathbb{I}}{|\mathcal{F}|} \otimes \frac{\mathbb{I}}{2^m}) \leq \epsilon \ . \tag{23}$$