Lab2 Team Ukulele

Balzan Pietro, Mancini Eleonora, Mari Daniele

November 2020

1 Implementation

In order to implement the uniform channel for an input with length n with at most l errors a possible strategy is to sample the number of errors k with probability

$$P(k) = \frac{\binom{n}{k}}{\sum_{i=0}^{l} \binom{n}{i}}$$

and after that the k bits to be flipped need to be sampled without replacement between the n bits of the input to the channel. From figure 1(the plots were obtained by running the channel 10^6 times) it is possible to see that the representations obtained starting from a fixed message are uniformly distributed over the reachable configurations. It is important to know that in all 3 cases the x labels represent the integer value corresponding to the binary array, for the joint probability y and z were concatenated into a single vector. Considering the plot in the middle that shows $P_{z|x}(b|x = 1001000)$ it is possible to see that over all the reachable words, i.e those with distance smaller or equal than 3 from 1001000, the probability is uniform while for all the others it is always zero.

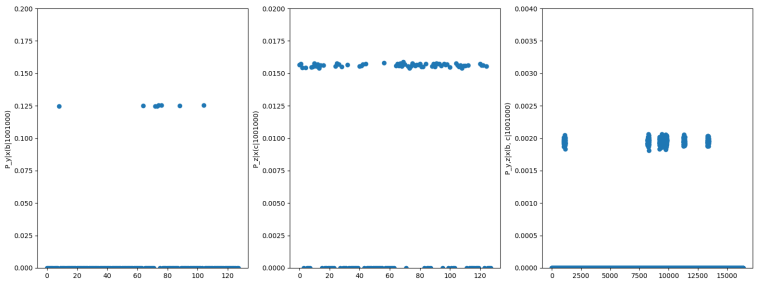

Figure 1: probability distribution of y, z, and joint distribution between y and z

Most of the implemented utility functions use numpy binary arrays in order to solve the particular task they are designed for, the only exception is the encoder where the binary representation of integers is used instead.

Task 2 and 3 were implemented as suggested in the instructions pdf, since no particular design choices were needed in order to complete them. Tests were run in order to make sure that perfect decodability is achieved with the implementation, meaning that it should be correct.

In task 4 since the message distribution is not specified, it was assumed to be uniform. Now it is easy to find an estimate of $P_{z|u}(c|d)$ by computing multiple times the output z with a fixed u. By repeating this procedure for all possible u (only 8 in total since u has only 3 bits) it is possible to compute the conditional distribution wrt all messages u. From this we can now compute $P_{u,z}(d,c) = P_{z|u}(c|d)P_u(d)$ and the marginal probability for z as

$$P_z(c) = \sum_{d \in \mathcal{M}} P_{u,z}(d,c)$$

At this point the mutual information can also be computed with the formula written in the instructions pdf. A plot of $P_{z|u}(c|d)$ can be seen in figure 2, the labels in the u and z axis are the integer representation of the binary arrays u and z. As expected the conditional probability is uniform over all possible values of z. The plot was obtained by running the simulation 10^5 times. With the data shown in the plot the mutual information value obtained was 0.0007475 that is very small as expected, since theoretically z and u should be independent. To support this hypothesis is also the fact that as we increase the number of trials by a factor of 10 also the mutual information estimation decreases accordingly, hinting the fact that as the number of trials increases it should tend towards 0.

The BSC implementation is very straight forward since it just consists in flipping every bit with probability ϵ as if each single error was a Bernoulli random variable.

The first two points of task 6 are a repetition of what was done before but with the binary symmetric channel instead of the uniform one. The error rate over Bob was computed for multiple values of epsilon,

$$\epsilon \in \{0.001, 0.01, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 0.99, 0.999\}.$$

The resulting plot can be seen in figure 3. Since the error rate is not equal to 0 unless $\epsilon = 0$ then it is possible to see that the system does not provide perfect decodability anymore. For task 6.3 It is possible to see that the mutual information between u and z, i.e the information shared between the two RV, is actually the measure of secrecy that we are looking for. In case of perfect secrecy, as for the uniform channel, since u and z are independent, the mutual information is 0; the less independent the two of them are, the higher the mutual information will be. In particular, if z is a deterministic function of u, then the mutual information is $\mathrm{H}(u) = 3$. It is possible to see the mutual information between u and z as a function of δ (same range of values as ϵ) in figure 4, its value is 0 only in case $\delta = 0.5$ so in general perfect secrecy is lost.

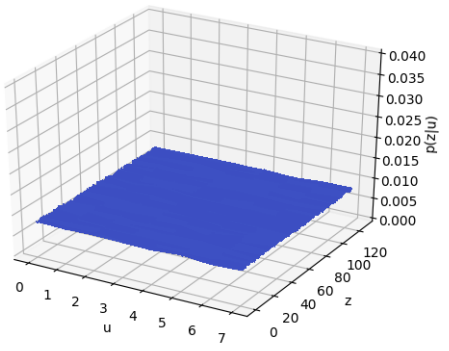

Figure 2: Plot of the conditional probability $P(z|u)$

Finally, for task 6.4, let M be the implemented mechanism and let M^* be its ideal counterpart. It is known that

$$d(M, M^*) \leq \max_{a \in \mathcal{M}} P(\hat{u} \neq u | u = a) + \frac{1}{2}\sqrt{I(u; z)},$$

where $\hat{u}$ is the message reconstructed by Bob and z is the encoded message received by Eve.
$I(u; z)$ was computed in the previous task, $\max_{a \in \mathcal{M}} P(\hat{u} \neq u | u = a) = P(\hat{u} \neq u | u = a)$ for each $a \in \mathcal{M}$ since it doesn't matter what the initial message is, in this system the probability of not being able to decode z is always the same independently on u. So we can compute $d(M, M^*)$ for different values of ϵ and δ. The result can be seen in figure 5, this plot represents the upper bound to $d(M, M^*)$ as a function of ϵ, δ. It is possible to see that as expected we have the minimum where $\epsilon = 0, \delta = 0.5$ and maximum where $\epsilon = 0.5, \delta = 0$.

2 Questions

2.1 Question 1

The scheme achieves perfect secrecy, since u and z are independent, so the number of secret bits per word sent is actually 3, i.e the entropy of the message distribution. The remaining 4 bits are redundancy used for error correction and to achieve perfect secrecy. So, since a word is 7 bits long, it means that for each binary digit $\frac{3}{7}$ secret bits are obtained.

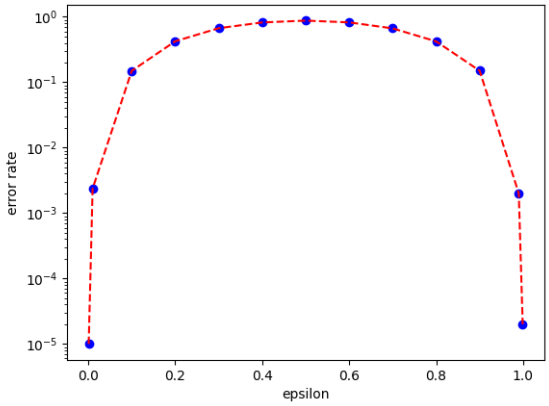

Figure 3: Error rate at Bob's side as a function of ϵ, (10^5 realizations of the system for each point)

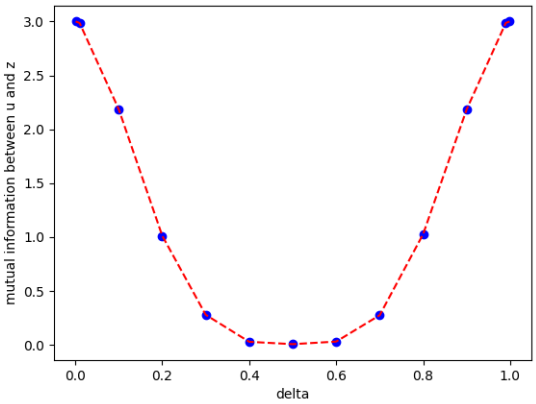

Figure 4: Mutual information between u and z as a function of δ(10^4 realizations of the system for each point)

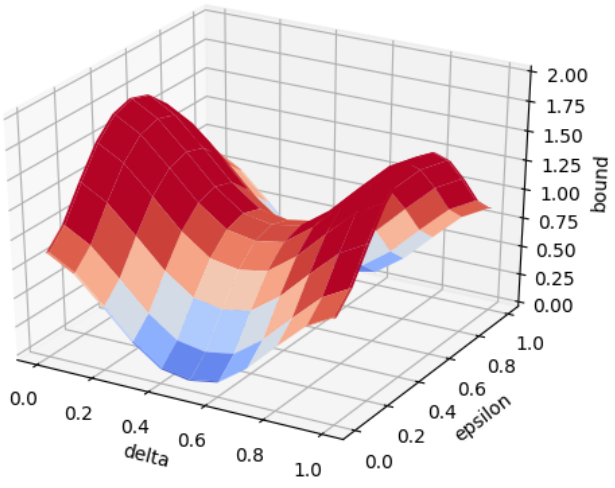

Figure 5: Plot of the upper bound of $d(M, M^*)$ as a function of ϵ, δ

2.2 Question 2

If in a single use of the channel 7 binary digits are sent and hamming code is used, then the answer is no. As a matter of fact, if a 4 bits long message u' was encoded with the hamming code, then the only possibility would be $T_{x|u} = hamming(u')$. With this encoder and the corresponding decoder the perfect decodability would still be ensured since hamming codes can correct up to 1 error, but perfect secrecy wouldn't.
As a matter of fact in the original scheme $T_{x|u} = hamming([0, u]), hamming([1, !u])$, where $!u$ is the word where all bits are flipped wrt u, and it is possible to see that

$$d_H(hamming([0, u]), hamming([1, !u]) = 7.$$

Because of that (with fixed u) z can take with uniform probability all the possible configurations of 7 bits. On the other hand, with $T_{x|u} = hamming(u')$ if Eve gets z then since the maximum number of errors is 3 it could rule out all the codewords x with hamming distance greater than 3 from z, leading to z not being independent from u anymore and thus violating the condition for perfect secrecy. This can also be seen from the formula that tells if both secrecy and reliability are achieved, as a matter of fact with 4 bits $|\mathcal{M}| = 16, |\mathcal{X}'| = 16, N_{x|u} = 1, |\mathcal{Y}| =$

$|\mathcal{Z}|, N_{z|x} = 64, N_{y|x} = 8$ so the bound is violated since

$$|\mathcal{M}| = 16 \leq \frac{N_{z|x}}{N_{y|x}} = 8$$

because as previously said perfect secrecy is not achieved.

2.3 Question 3

Yes It is possible to send only two secret bits per channel use, in this case the encoder should take the 2 bit message u, add the bits 00 at the beginning and find the associated hamming word x_{temp}. Also in this case $T_x = \{x_{temp}, !x_{temp}\}$. Since also in this case z will be uniformly distributed over all the sequences of 7 bits perfect secrecy is retained, plus due to the fact that Bob's channel makes at most one error it means that it can be always corrected and thus also perfect reliability is achieved. This can also be seen from the formula that tells if both secrecy and reliability are achieved, as a matter of fact with 2 bits $|\mathcal{M}| = 4, |\mathcal{X}'| = 8, N_{x|u} = 2, |\mathcal{Y}| = |\mathcal{Z}|, N_{z|x} = 64, N_{y|x} = 8$. Here all the bounds are respected and as a matter of fact both perfect secrecy and decodability are obtained. So with this encoder and the corresponding decoder it is possible to send two secret bits per channel use. Using the same reasoning it is also possible to send only one secret bit if we add 3 null bits at the beginning. In general though in order not to waste bandwidth it is probably just better to send 3 secret bits.

2.4 Question 4

It is reasonable to believe that Eve's error rate would be $\frac{7}{8}$ i.e. the random guessing error, given that the distribution for u is uniform, since z and u have been shown to be independent. Probably mutual information is used to evaluate the system because it tells how much information about u the optimal algorithm could obtain from z. While the error rate depends on the implemented strategy, so if this is not optimal the error rate could be very high even if, in principle, Eve could have a much lower one. So mutual information is used because it doesn't depend on the decoder implementation while the random guessing error does.