mettre le numro personnel de Lucas

Project Assignment 2: Report

Johannes Lemonde 960911-T357 and Lucas Streit 970606-T???

I. Introduction

The main concern of this project is to decode a signal which was distorted by an unknown time-invariant finite impulse response filter and which includes also some white noise. Such filters are commonly used by communication channels; our role here is to take a glimpse into the maths behind the receptor – in other words, to elaborate the algorithm able to decode this distorted signal back to the original signal.

We are provided with such a distorted signal consisting of a large sequence of real numbers, knowing that the original binary signal – before it was distorted – starts with a given binary sequence, which we also know.

The knowledge of this sequence at the beginning of the signal is needed by the receptor to compute a set of constant parameters, comparing the original and distorted signals – through a system of linear equations to solve –, which would then be used to determine the further bits of the original signal.

To make this project fancier, we are dived into a situation where the original signal is a key to decipher a picture. We are given an encrypted picture and the ciphering/deciphering algorithms, and the better the recovered key, the more accurate the deciphered picture.

II. Formalisation of the problem

The original binary signal – the key – is composed by a sequence $b(k) \in \{-1, 1\}, \quad k \in [1, M] \subset \mathbb{N}$, where M is the length of the key. The values $b(1), \ \dots \ , b(N)$ – referred to as the training sequence – are known to us, with $N = 32$. Before it was transmitted, the key has been subjected to an unknown filter h of order 3 and to the white noise $n(k)$ such as

$$r(k) = \sum_{l=0}^{3} h(l) \ b(k-l) \ + n(k), \quad k \in [1, M] \subset \mathbb{N}. \tag{1}$$

These values of r are known to us, and we are asked to reconstruct the sequence b.

III. Resolution

In order to do so, we apply an equalizer (an other filter) of order L such as

$$\hat{b}_r(k) = \sum_{l=0}^{L} w(l) \ r(k-l) \approx b(k), \tag{2}$$

where the coefficients $w(0), \ \dots \ , w(L+1)$ must be initialised using the training sequence. To do so, we define a matrix $\boldsymbol{R}$, a vector $\boldsymbol{w}$ and a vector $\boldsymbol{b}$ so that $\boldsymbol{Rw} = \boldsymbol{b}$ represent the equations in (2). Since $r(k)$ does not have values for k being null or negative, and since we have this subtraction of l in the argument of r in (2), we can only use (2) for $k = L+1, \ \dots \ , N$, which thus gives $\boldsymbol{Rw} = \boldsymbol{b} \Leftrightarrow$

$$\begin{pmatrix} r(L{+}1) & r(L) & \cdots & r(1) \\ r(L{+}2) & r(L{+}1) & \cdots & r(2) \\ \vdots & \vdots & \dots & \vdots \\ r(k) & r(k{+}1) & \cdots & r(k{-}L) \\ \vdots & \vdots & \dots & \vdots \\ r(N) & r(N{-}1) & \cdots & r(N{-}L) \end{pmatrix} \cdot \begin{pmatrix} w(0) \\ w(1) \\ \vdots \\ w(L) \end{pmatrix} = \begin{pmatrix} b(L{+}1) \\ b(L{+}2) \\ \vdots \\ b(k) \\ \vdots \\ b(N) \end{pmatrix} \tag{3}$$

Notice that $\boldsymbol{R}$ is not square for any value of L, so the system might have much more equations than unknowns. Thus, resolving the system for $\boldsymbol{w}$ results in resolving it in the approximation of the least squares: $\boldsymbol{w} \approx (\boldsymbol{R}^T \boldsymbol{R})^{-1} \boldsymbol{R}^T \ \boldsymbol{b}$. Matlab does this automatically for non-square matrices with the command `w = R\b`.

Once these coefficients $\boldsymbol{w}$ are computed, we can freely use the equation (2) to get the estimated values $\hat{b}_r(k)$ of the whole signal (for $k \leq N$, and especially for $k \leq L$, we use the known training sequence directly, instead), but we still need to convert them to a binary sequence. In order to do so, we apply a sign detector on the real-valued estimator of b, which gives: $\hat{b}(k) = sign(\hat{b}_r(k)) = \left\{ \begin{smallmatrix} +1, & \hat{b}_r(k) > 0 \\ -1, & \hat{b}_r(k) \leq 0 \end{smallmatrix} \right.$.

IV. Optimisation of the equaliser's order L

We have now everything needed to reconstruct the key, excepted from L. [[[[#######As the accuracy of the recovering of the key will depend on the choice made for the order of the equaliser, we have to ########]]]]

REFERENCES

[1] P. Handel, R. Ottoson, H. Hjalmarsson, *Signal Theory*, KTH, 2012