Communication Skills Assignment - 1 (Proofs)

Jimut Bahan Pal
(22D1594)

January 16, 2023

We have developed the Hamming Code in the class, through a little game we played, as an example of how many abstract mathematical concepts come together, to do something very useful, in the context of data sciences, robust data representation, error detection and correction. Students are expected to pretend that they have 'discovered' this Hamming code and write a formal statement and proof of the (4,7) Hamming Code error correction capability as also generalize the same to the (2^m - 1 - m, 2^m - 1) Hamming code, as a training in formal presentation of mathematical results. They commenced doing this during the session and are expected to complete it in about 2 hours.

Note: I'm proving this for the general case, the (4,7) hamming code is a generalization of this proof. Please note that this is not the perfect and concise proof, since the author have very little knowledge of theoritical counterparts. Please pardon my hasty writing and incorrect english.

Given, the code bits to send is of size $2^{\mathrm{m}} - 1 - m$ and the size of the code word to be transmitted is $2^{\mathrm{m}} - 1$. We assume that there will be only 1 corrupted bit in the transmitted word, and the reciever will be somehow able to pin-point the location of the incorrect bit.

Let the information word be $\mathbf{W_I}$ of dimension $1 \times 2^{\mathrm{m}} - 1 - m$. Let the generator $\mathbf{G} = [\mathbf{I}\ \mathbf{P}]$. First, we write all the possible binary permutation of m bits in ascending order, and stack the identity matrix $\mathbf{I}$ at top and sort the remaining bits as it is. Matrix $\mathbf{P}$ is below matrix $\mathbf{I}$ and have dimension $2^{\mathrm{m}} - 1 - m \times m$.

Now, we pad some additional row in $\mathbf{I}$ such that $\mathbf{I}$ & $\mathbf{P}$ matrices can be stacked together in $\mathbf{G}$. The dimension of $\mathbf{I}$ will be $2^{\mathrm{m}} - 1 - m \times 2^{\mathrm{m}} - 1 - m$. Hence, the matrix $\mathbf{G}$ is of dimension $2^{\mathrm{m}} - 1 - m \times 2^{\mathrm{m}} - 1$. The code word $\mathbf{W_c}$ can be written as $\mathbf{W_c} = \mathbf{W_I} \times \mathbf{G}$. The dimension of $\mathbf{W_I}$ is $1 \times 2^{\mathrm{m}} - 1 - m$ and the dimension of $\mathbf{W_c}$ is $1 \times 2^{\mathrm{m}} - 1$. We need to transmit the code word to a receiver, to get the received word which can be written as, $\mathbf{W_R} = \mathbf{W_c} + \mathbf{W_e}$.

Where, $\mathbf{W_e}$ is the error word obtained by changing just one bit of the code word. The dimension of all these words are same as $\mathbf{W_c}$ i.e., $1 \times 2^{\mathrm{m}} - 1$. This process can be modelled as a binary addition, which obeys some simple rule, i.e., $0+0=0, 0+1=1, 1+0=1, 1+1=0$ *and* $1+1+1=1$.

We now define a pointer word $\mathbf{W_P}$, which can be written as $\mathbf{W_P} = \mathbf{W_R} \times \mathcal{P}$. Here, $\mathcal{P} = [\substack{\mathbf{P} \\ \mathbf{I}}]$. Here, the dimension of $\mathbf{I}$ is $m \times m$. The dimension of $\mathbf{P}$ is $2^{\mathrm{m}} - 1 - m \times m$. Hence the dimension of $\mathcal{P}$ is $2^{\mathrm{m}} - 1 \times m$ and the dimension of $\mathbf{W_P}$ is $1 \times m$.

We need to show how this machinery is perfectly working by exactly pin-pointing the location of the incorrect bit. The received bit can be written as $\mathbf{W_R = W_c + W_e}$ which expands into:

$$\Rightarrow \mathbf{W_P} = (\mathbf{W_c} + \mathbf{W_e})[\substack{\mathbf{P} \\ \mathbf{I}}]$$

$$\Rightarrow \mathbf{W_P} = (\mathbf{W_I} \times \mathbf{G} + \mathbf{W_e})[\substack{\mathbf{P} \\ \mathbf{I}}]$$

$$\Rightarrow \mathbf{W_P} = (\mathbf{W_I}\ [\mathbf{I}\ \mathbf{P}] + \mathbf{W_e})[\substack{\mathbf{P} \\ \mathbf{I}}]$$

The multiplication of matrices which are conformable for multiplication can be broken down into sub-matrices, hence the above equation can be written as:

$$\Rightarrow \mathbf{W_P} = \mathbf{W_I}\ [\mathbf{I}\ \mathbf{P}][\substack{\mathbf{P} \\ \mathbf{I}}] + \mathbf{W_e}[\substack{\mathbf{P} \\ \mathbf{I}}]$$

We will see the left term of the summation turns to 0, since binary addition of two 1's turns into 0 and the $\mathbf{P}$ matrix have even number of 1's in each row. Hence, we can exactly pin-point the place of error by $\mathbf{W_e}[\substack{\mathbf{P} \\ \mathbf{I}}]$.