Information Theory 2023
Programming Assignment 3

Lakshmi Prasad Natarajan

Due on Apr 30, 11.59pm

Submission Link

Please submit on Google Classrooms.

Submission Format

You must submit a single python script file with .py extension. The name of the file must be "Serial_num.py" where 'num' is your serial number. For instance, if your serial number is 7, then your submission will be "Serial_7.py".

The file submitted must contain the definition of a python function by the name `HammingDecoder`. This function must be callable as follows.

```
# import the function from your submission "Serial_7.py"
from Serial_7 import HammingDecoder
import numpy as np

# Sample output of binary symmetric channel
y = np.array([0,1,1,0,1,1,0,1,0,0,1,1,1,1,0])

# decoding the most likely codeword of the Hamming code
x = HammingDecoder(y)
```

If there is an error when your function is called as above, I will not be able to debug your submission, and no marks will be awarded.

Problem Description

In this programming assignment we will consider a channel code for the BSC for which the optimal decoder can be constructed with low complexity. The code $\mathcal{C}$ we will consider is the Hamming code of length $n = 15$. This code has $M = 2^{11}$ codewords, and hence, is of rate $R = 11/15$. The minimum distance of this code is $d_{\min} = 3$, and hence, this code can correct $t = 1$ bit-flip in the BSC (see Questions 4 and 5 in Practice Set 11 for reference).

The $M = 2^{11}$ codewords of this code are arranged in an extremal fashion in the space $\{0,1\}^{15}$: for each vector $\boldsymbol{y}$ in $\{0,1\}^{15}$, there is exactly one codeword at a Hamming distance of at the most 1. That is, for every $\boldsymbol{y} \in \{0,1\}^{15}$, there is exactly one $\boldsymbol{x} \in \mathcal{C}$ such that $d(\boldsymbol{x}, \boldsymbol{y}) \leq 1$.

The naive way to perform optimal decoding of this code is to go through all the 2^{11} codewords and pick the one that is closest to $\boldsymbol{y}$. This involves $2^{11} \times 15$ bit-wise comparisons. However, the algebraic structure of the code allows us to decode it optimally with far fewer computations. This is what we will implement in this programming assignment. The decoding algorithm described next is called *syndrome decoding*, and it gives the same output as the optimal decoder.

Backgound

We will use a 4×15 binary matrix $\boldsymbol{H}$ to identify the Hamming code of length 15 and to help us in decoding. This is called the *parity-check matrix* of this code. Let the entry of $\boldsymbol{H}$ in row i and column j be $h_{i,j}$. For $j = 1, \ldots, 15$, the j^{th} column of $\boldsymbol{H}$ is the binary representation of the integer j. For instance, the fifth column of $\boldsymbol{H}$ is

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix},$$

since $5 = 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$.

We multiply a binary vector $\boldsymbol{y}$ with $\boldsymbol{H}$ as follows to get the syndrome $\boldsymbol{H} \otimes \boldsymbol{y} = \boldsymbol{s} = (s_1, s_2, s_3, s_4) \in \{0,1\}^4$:

$$s_i = \sum_{j=1}^{15} h_{i,j} y_j \mod 2.$$

That is, we multiply $\boldsymbol{H}$ with $\boldsymbol{y}$ using the usual matrix-vector multiplication but in the end we perform modulo 2 reduction on each entry, so that each entry of the syndrome lies in $\{0,1\}$. We will denote this operation as $\boldsymbol{s} = \boldsymbol{H} \otimes \boldsymbol{y}$.

The Hamming Code of Length 15

The code is defined as the collection of all length 15 binary vectors whose syndrome is equal to the all-zero vector of length 4, that is

$$\mathcal{C} = \left\{ \boldsymbol{x} \in \{0,1\}^{15} \ : \ \boldsymbol{H} \otimes \boldsymbol{x} = (0,0,0,0) \right\}.$$

Using linear algebra it can be shown that this code has exactly 2^{11} codewords, any two codewords differ in at least 3 positions, and every $\boldsymbol{y} \in \{0,1\}^{15}$ has exactly one codeword at a Hamming distance of 1 or less.

Syndrome Decoding

Suppose $\boldsymbol{y}$ is the channel output, and $\boldsymbol{x} \in \mathcal{C}$ is the codeword closest to it. Then $d(\boldsymbol{x}, \boldsymbol{y}) \leq 1$. If $d(\boldsymbol{x}, \boldsymbol{y}) = 0$, then $\boldsymbol{x} = \boldsymbol{y}$, and hence, the syndrome of $\boldsymbol{y}$ is $\boldsymbol{H} \otimes \boldsymbol{y} = (0,0,0,0)$.

Now, if $d(\boldsymbol{x}, \boldsymbol{y}) = 1$, then these two vectors differ in exactly one position. If we can find this position then we can find $\boldsymbol{x}$ by using $\boldsymbol{y}$ and flipping the bit value of $\boldsymbol{y}$ in this position. The information about this position is available in the syndrome $\boldsymbol{s} = \boldsymbol{H} \otimes \boldsymbol{y}$. If the syndrome $\boldsymbol{s}$ is the binary representation of the integer j, then $\boldsymbol{x}$ and $\boldsymbol{y}$ differ in coordinate j. For instance, if $\boldsymbol{s} = (0,1,0,1)$, then $\boldsymbol{x}$ and $\boldsymbol{y}$ differ in position 5. The decoder flips the fifth bit of $\boldsymbol{y}$ to obtain $\boldsymbol{x}$, and then outputs this $\boldsymbol{x}$ as the decoded codeword.

Note that this decoding technique uses far fewer computations than the naive implementation of the optimal decoder.

Evaluation

The maximum marks for this assignment is 10. Each student must work individually, and submit a file on their own.