MATLAB Simulation of Linear Block Codes: Hamming (7,4), Reed-Muller (8,4), and Golay (24,12)

Nikola Janjušević, EE ’19 *The Cooper Union*

***Abstract*—Three linear block codes were simulated to obtain bit error rate (BER) vs. EbNo curves.**

I. Introduction

This report details the encoding and decoding of three specific linear block codes: the Hamming (7,4), Reed-Muller (8,4)[1], and the Golay (24,12). These codes were chosen to have similar rates to allow for comparison between each other.

The remainder of the report is structured as follows: Sections II, III, and IV discuss the Hamming, Reed-Muller, and Golay codes respectively. In each of these sections, the methods used for encoding and decoding are presented. Section V details a comparison of all three of these codes in the form of a bit error rate (BER) vs. EbNo plot.

II. Hamming (7,4) Code

Hamming codes are linear block codes defined by a single parameter, m. For $m \geq 3$, there exists a Hamming code with the following properties: [1]

- Code length: $n = 2^m - 1$
- Number of information symbols: $k = 2^m - 1 - m$
- Error-correcting-capability: $t = \lfloor d_{min}/2 \rfloor = \lfloor 3/2 \rfloor = 1$

Furthermore, matrix $Q \in M^{m \times k}$, defined by its k columns being the m-tuples of weight 2 or more, is used to define the generator, G, and parity-check, H, matrices of the code as follows: [1]

$$G = \begin{bmatrix} Q^T & I_k \end{bmatrix} \qquad H = \begin{bmatrix} I_m & Q \end{bmatrix}$$

Where I_n is the $n \times n$ identity. The matrix,

$$Q = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

was used for this implementation of the (7,4) code. As with all linear block codes, a message $u \in M^{1 \times k}$ is coded to codeword $v \in M^{1 \times n}$ by $v = uG$.

[1]more commonly referred to as RM(1,3)

A. Decoding

Syndrome decoding provides a fast method for reconstruction of estimated message signal. For each received code vector r, its syndrome $s = rH \in M^{1 \times m}$ is computed. The decoding process is generally described via look-up table to find the error vector (coset leaders) for the syndrome, however, this operation can be easily realized through boolean logic of the syndrome bits. For the Hamming (7,4) code, this is realized as follows:

$$\begin{aligned} e_0 &= s_0(s_1+1)(s_2+1) & e_1 &= (s_0+1)s_1(s_2+1) \\ e_2 &= (s_0+1)(s_1+1)s_2 & e_3 &= s_0 s_1(s_2+1) \\ e_4 &= (s_0+1)s_1 s_2 & e_5 &= s_0 s_1 s_2 \\ e_6 &= s_0(s_1+1)s_2 & & \end{aligned}$$

[2] [1] (Example 3.9, Section 3.5)

Where $e = [e_0, e_1, ..., e_6]$, and $s = [s_0, s_1, s_2]$. It follows that the estimated message vector $\hat{u} = (v+e)[0_{k \times m} I_k]$ as the Hamming code is systematic.

III. Reed-Muller (8,4) Code

Reed-Muller (RM) codes are defined by an integer m, and integer $r, 0 \leq r \leq m$. For any integer m, there exists an r-th order Reed-Muller code, RM(r,m) with the following characteristics: [1]

- Code length: $n = 2^m$
- Number of information symbols: $k = \sum_{i=0}^{r} \binom{m}{i}$ [3]
- Error-correcting-capability: $t = \lfloor 2^{m-r-1} \rfloor$

Hence RM codes are referred to as multiple-correction-codes.

There exists several different ways to encode and decode RM codes. First-order RM codes are especially *nice* to deal with as they maximize the codes error correcting capabilities and are able to use Hadamard matrices for decoding. The generator matrix, G, may be defined recursively, as seen in [2]. This report deals with RM(1,3) which is a rate (8,4) code.

[2]we’re in GF(2), so this is mod-2 multiplication and addition, otherwise known as logical AND and NOT

[3]often referred to as the dimension for added confusion

A. Decoding

The following is a summary of decoding construction provided by [2]. Perform decoding, a matrix H_m is constructed by successive Kronecker products of the Hadamard matrix $H = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$

IV. Golay (24,12) Code

A. Decoding

V. Comparison

VI. Conclusion

Appendix

References

[1] S. Lin and D. J. Costello, *Error Control Coding, Second Edition*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2004.

[2] M. Malek, "Reed-muller codes, coding theory," California State University, East Bay, http://www.mcs.csueastbay.edu/ malek/Class/Reed-Muller.pdf.