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 gives a brief 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 $v = uG$.

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 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. This report deals with RM(1,3), which is a rate (8,4) code with a 1-bit error correcting capability.

The generator for an arbitrary RM code may be defined recursively as follows (reproduced from [2]:

For $r = 0$, $G(r,m) := [11...1] \in M^{1,2^m}$. For $r = m$, define

$$G(m,m) := \begin{bmatrix} \multicolumn{5}{c}{G(m-1,m)} \\ 0 & 0 & \ldots & 0 & 1 \end{bmatrix}$$

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

[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

Now for an arbitrary generator matrix of $RM(r,m)$,

$$G(r,m) := \begin{bmatrix} G(r,m-1) & G(r,m-1) \\ \mathbf{0} & G(r-1,m-1) \end{bmatrix}$$

[2]

A. Decoding

The following is a summary of decoding construction provided by [2]. Details are left to said source. Perform decoding, a matrix H_{RM} is constructed by successive Kronecker products of the Hadamard matrix $H_2 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$, as defined by,

$$H_m^j = I_{2^{m-j}} \otimes H_2 \otimes I_{2^{j-1}}$$
$$H_{RM} = H_m^1 H_m^2 ... H_m^m$$

The decoding of a received vector $v \in GF(2)^{1 \times 2^m}$ proceeds as follows,

1) let $w_0 = 2v + \mathbf{1}$, where $\mathbf{1}$ is the all ones vector
2) compute $w_m = w_m H_{RM}$
3) find the index, j, where the component $w_{m,j}$ of $w_m = [w_{m,0} w_{m,1} ... w_{m,2^{m-1}}]$ is the largest in magnitude. Set bit $s = sign(w_{m,j})$
4) let $bin(d)$ be the operator that maps positive integer, d, to a binary coded decimal array of size m, with the least significant bit first. The decoded message is estimated to be $\hat{u} = [s \quad bin(j)]$.

IV. Golay (24,12) Code

The Golay (24,12) code is supposedly a beautiful code with interesting structural properties. Its generator matrix, $G = [P \quad I_{12}]$, may be constructed by 10 left-cyclic-shifts of the vector $p = [10001110110]$, and with each shift ,i, $p^(i)$ populates a successive row of P_{11x11}. Then P is made by concatenating a row and a column of 11 ones to the ends of P_{11x11}, where the last entry of P is a zero,

$$P = \begin{bmatrix} p^(0) & 1 \\ p^(1) & 1 \\ \vdots & \vdots \\ p^(10) & 1 \\ \mathbf{1} & 0 \end{bmatrix}$$

As $P = P^T$, the parity check matrix $H = [I_{12} \quad P]$.

A. Decoding

Syndrome decoding of the received message bit may exploit the structure of the code to go through certain steps based on the weight of the syndrome vector and transformations of it. See [1] pg. 128 for details.

V. Comparison

Figure 1 shows a comparison between the three linear block codes in the form of an BER vs. EbNo plot. The Hamming code is the only one that breaks through the uncoded BPSK curve to provide some coding gain past a BER of 10^{-3}. The Golay and Reed-Muller codes left behind, losing the tradeoff between forward encoding putting more energy into the system. It looks as though these other two codes may provide some gains at higher EbNos, however, their respective bit error rates were two low for these simulations.

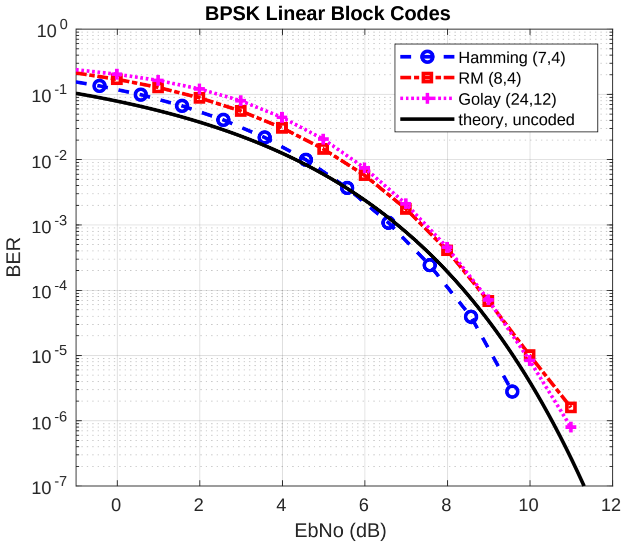

Fig. 1. BER vs. EbNo simulation of 3 linear block codes compared to uncoded BPSK

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.