Pries: M460 - Information and Coding Theory, Spring 2019
Handout 11M: BCH codes

Improvement: Reed-Solomon code - as BCH code

Choose α generator of $\mathbb{F}_q^*$. Let $n = q - 1$.

Choose t such that $2 \leq t \leq n$ and let $k = n - t + 1$ so that $n - 1 \geq k \geq 1$.

Choose the generator polynomial $g(x) \in \mathbb{F}_q[x]$ to be the polynomial of degree $t-1$ having roots α^i for $1 \leq i \leq t - 1$.

Codewords are coefficients of polynomials of degree $\leq n - 1$ which are multiples of $g(x)$.

Equivalently, $(c_0, \ldots, c_{n-1})$ codeword iff α^i root for $1 \leq i \leq n - k$ of

$$p(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

Polynomial division by $g(x)$ has remainder $r(x) \neq 0$ if and only if error.

The minimal distance is at least t.

Construct the new Reed-Solomon code in this situation.

Recall that $\mathbb{F}_9 = \{a + bi \mid a, b \in \mathbb{Z}/3\}$.

1. Show that the element $\beta = 1 + i$ is a generator of $\mathbb{F}_9^*$.
2. Choose $t = 3$. What are the length n and the dimension k? What is the number M of codewords?
3. What is $g(x)$? Find the generator matrix for the code.
4. Continuing with $t = 3$. Your data is $(1, i)$ which you use as the coefficients of the polynomial $h(x) = 1 + ix$. What is $g(x)h(x)$ and what is the encoded message?
5. Continuing with $t = 3$. You receive the message $(1, 0, 0, 0, 1, 0, 0, 0)$. Did an error occur?
6. What is the minimum distance of this code? How many errors can it detect and correct?

Pries: M460 - Information and Coding Theory, Spring 2019
Homework 9: New Reed Solomon Code. Due Friday 4/19.

1. Let $q = 7$ and $t = 3$. Choose $\alpha = 3$.
   (a) Find the generator polynomial $g(x)$ and the generator matrix for the new Reed Solomon code.
   (b) What are n, k, d?
   (c) Encode the data $(1, 2, 1, 0)$.
   (d) You receive the codeword $(5, 1, 1, 3, 0, 0)$. What is the data?
   (e) You receive the codeword $(3, 0, 5, 2, 0, 0)$. Show that an error occurred. If exactly one error occurred, find the data.

2. Recall that $\mathbb{F}_8 = \{a + b\beta + c\beta^2 \mid a, b, c \in \mathbb{Z}/2\}$ where β is a root of $x^3 + x + 1 \in \mathbb{Z}/2[x]$. In fact, β is a generator of $\mathbb{F}_8^*$. This problem is about the new Reed-Solomon code when $t = 2$.
   (a) What are the length n and the dimension k? What is the number M of codewords?
   (b) What is $g(x)$? Find the generator matrix for the code.
   (c) Your data is $(1, \beta^2, \beta + 1)$ which you use as the coefficients of the polynomial $h(x) = 1 + \beta^2 x + (\beta + 1)x^2$. What is $g(x)h(x)$ and what is the encoded message?
   (d) You receive the message $(\beta, \beta^2, \beta^2 + \beta, 0, 0, 0, 0)$. Did an error occur?
   (e) What is the minimum distance of this code? How many errors can it detect and correct?

3. Let $q = p^r$. What is the length, dimension, minimal distance, and generator polynomial of the new Reed-Solomon code when
   (a) $t = 2$.
   (b) $t = q - 1$. Which code is this?

4. Hand in extended outline and two references for your project.