COMBINATÓRIA E TEORIA DE CÓDIGOS
Exercise List 8

9/5/2011

1. Show that the interleaved code of degree s, $C^{(s)}$, is equivalent to the sum code $C \oplus \cdots \oplus C$ of s copies of C. Conclude that $\mathrm{dist}(C^{(s)}) = \mathrm{dist}(C)$.

2. Let $C = \mathrm{Ham}(3, 2)$ be the binary Hamming code with redundancy 3 and generator polynomial $g(t) = 1 + t + t^3$.

   (a) Find the parameters and the generator polynomial of $C^{(3)}$.

   (b) Show that $C^{(3)}$ corrects all burst-m errors with $m \leq 3$.

   (c) Using the Burst Error Trapping Algorithm, decode the following received vector
   $$y(t) = t + t^3 + t^5 + t^7 + t^8 + t^9 + t^{11} \ .$$

3. A q-ary cyclic code, with length n, is called *degenerate* if there is $r \in \mathbb{N}$ such that r divides n and each code word is of the form $c = c'c' \cdots c'$ with $c' \in \mathbb{F}_q^r$, i.e., each code word consists in n/r identical copies of a sequence c' with length r.

   (a) Show that the interleaved code $C^{(s)}$ of a repetition code C is degenerate.

   (b) Show that the generator polynomial of a degenerate cyclic code with lenth n is of the form
   $$g(t) = a(t)(1 + t^r + t^{2r} + \cdots + t^{n-r}) \ .$$

   (c) Show that a cyclic code with lenght n and check polymonial $h(t)$ is degenerate if and only if there is $r \in \mathbb{N}$ such that r divides n and $h(t)$ divides $t^r - 1$.

4. Let C be the binary linear code with the following parity-check matrix
$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \ .$$

   (a) Find the minimum distance $\mathrm{dist}(C)$, and determine the code capacity for detecting and correcting random errors.

   (b) Show that C detects all burst-m errors with $m \leq 3$.

(c) Let C' be the ponctured code, in the last coordinate, of the dual code$C^{\perp}$. Show that C' is a degenerate cyclic code, and determine its generator polynomial.

5. Determine all degenerate, cyclic and binary codes with length 9, writing the generator polynomials and the corresponding r-sequences.

6. Let α be a root of $1 + t^2 + t^3 \in \mathbb{F}_2[t]$ and consider the map $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ defined by $\phi(a_1 + a_2\alpha + a_3\alpha^2) = (a_1, a_2, a_3)$, where $a_1, a_2, a_3 \in \mathbb{F}_2$. Consider the linear code
$$A = \langle(\alpha + 1, \alpha^2 + 1, 1)\rangle$$
over $\mathbb{F}_8$. What are the parameters of $\phi^*(A)$?

7. Let α be a root of $1 + t + t^2 \in \mathbb{F}_2[t]$. Consider the linear code
$$A = \langle(1, 1), (\alpha, 1 + \alpha)\rangle \ ,$$
over $\mathbb{F}_4$, and the binary code $B = \{0000, 1100, 1010, 0110\}$. Let $\phi : \mathbb{F}_4 \to B$ be the map defined by $\phi(1) = 1100$ e $\phi(\alpha) = 1010$. What are the parameters $C = \phi^*(A)$?

8. Write a generator matrix and a parity-check matrix for a Reed-Solomon code $[6, 4]$, and determine its minimum distance.

9. Determine the generator polynomial of a Reed-Solomon over $\mathbb{F}_{16}$ with dimention 11. Write a parity-check matrix for that code.

10. Show that the dual of a Reed-Solomon code is a Reed-Solomon code.

11. Let C be the q-ary Reed-solomon code with generator polynomial
$$g(t) = (t - \alpha^a)(t - \alpha^{a+1}) \cdots (t - \alpha^{a+\delta-1}) \ .$$
Show that $c(t) \in \mathbb{F}_q[t]/\langle t^{q-1} - 1\rangle$ is a code word if and only if $c(\alpha^i) = 0$ for all $i = a, \dots, a + \delta - 1$.

12. Consider the code over $\mathbb{F}_{11}$ with generator matrix
$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \end{bmatrix} \ .$$
In Exercise List 6, you have already justified that this code is equivalent to a cyclic code C. Determine the generator polymonial and conclude that C is a Reed-Solomon code.

13. Generalize the previous exercise for a $[q-1,k]$ code, over $\mathbb{F}_q$, with generator matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \alpha^{3(k-1)} & \cdots & \alpha^{(q-2)(k-1)} \end{bmatrix},$$

where α is a primitive element in $\mathbb{F}_q$.

14. Let C be the Reed-Solomon code over $\mathbb{F}_8$ with generator polynomial $g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^3)$, where $\alpha \in \mathbb{F}_8$ is a root of $1+t+t^3$.

    (a) Justifify that α is a primitive element in $\mathbb{F}_8$.

    (b) Find the parameters of C.

    (c) Find the parameters of the dual code $C^{\perp}$.

    (d) Find the parameters of of the extended code $\widehat{C}$.

    (e) Find the parameters of the concatenation code $C^* = \phi^*(C)$, where $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ is the linear map defined by $\phi(1) = 100$, $\phi(\alpha) = 010$ and $\phi(\alpha^2) = 101$.

15. (a) Write the generator polynomial for a Reed-Solomon code C, with parameters $[7,2]$.

    (b) Let α be a root of $1+t+t^3 \in \mathbb{F}_2[t]$ and consider the map $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ defined by $\phi(a_0 + a_1\alpha + a_2\alpha^2) = (a_0, a_1, a_2)$. Find the parameters of $C^* = \phi^*(C)$.

    (c) Let $\hat{\phi} : \mathbb{F}_8 \to \mathbb{F}_2^4$ be defined by $\hat{\phi}(a_0+a_1\alpha+a_2\alpha^2) = (a_0, a_1, a_2, a_0+a_1+a_2)$. Find the parameters of $C' = \hat{\phi}^*(C)$.

    (d) What can you say about the capacity of C^* and C' for correcting random errors and/or burst errors?

16. Consider the Reed-Solomon code C over $\mathbb{F}_8$ with the following generator polynomial:

$$g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^3)(t-\alpha^4) = \alpha^3 + \alpha t + t^2 + \alpha^3 t^3 + t^4 \ ,$$

where we identify $\mathbb{F}_8$ with the quotient $\mathbb{F}_2[t]/\langle 1+t+t^3 \rangle$, and $\alpha \in \mathbb{F}_8$ is a root of $1+t+t^3$.

    (a) Find the parameters $[n,k,d]$ de C.

    (b) Apply The Error Trapping Algorithm to decode the following received vectors
    $$y = (0,1,0,\alpha^2,0,0,0) \quad \text{and} \quad z = (0,\alpha^3,0,1,\alpha^3,1,1).$$

    (c) Let $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ be a linear isomorphism over $\mathbb{F}_2$. What can you say about the capacity of the concatenation code $C^* = \phi^*(C)$ for correcting burst errors?