TC08 / Problems 60-69 (10.12, SX)

60. Let $K = \mathbb{Z}_{11}$ and $\alpha = [4]_{11}$. Then $\alpha$ has order 5 and if $\alpha = (1, \alpha, \alpha^2, \alpha^3, \alpha^4)$, then $a = (1, 4, 5, 9, 3)$. Let

$$g = (x - 2)(x - 6)(x - 7) \in K[x] \text{ and } C = \Gamma(g, \alpha).$$

Show that $C \simeq [5,2,4]_{11}$ (hence, it is MDS).

61. Use $\overline{K} = \mathbb{F}_{16}$ and $g = X^3 + X + 1$ to construct a binary Goppa code $C = \Gamma(g, \alpha)$ of maximum length, and find its dimension and minimum distance.

62. Use $\overline{K} = \mathbb{F}_{27}$ and $g = X^3 - X + 1$ to construct a ternary Goppa code $C = \Gamma(g, \alpha)$ of maximum length, and find its dimension and minimum distance.

63. Let $K = \mathbb{Z}_5$ and $\overline{K} = \mathbb{Z}_5[x]/(x^2 - 2)$. By the alternant bound, the minimum distance $d$ of the Goppa code $C = \Gamma(g, \alpha)$, with $g = T^6 + T^3 + T + 1 \in \overline{K}[T]$ and $\alpha$ the non-zero elements $\alpha \in K$ such that $g(\alpha) \neq 0$, satisfies $d \geq 7$. Prove that $d = 8$. 
(Alternative definition of the Goppa codes). Let \( K = \mathbb{F}_q \) and \( \bar{K} = \mathbb{F}_{q^m} \), \( m \) a positive integer. Let \( g \in K[T] \) be a polynomial of degree \( r > 0 \) and \( \alpha = \alpha_1, \ldots, \alpha_n \in \bar{K} \) the elements such that \( g(\alpha_i) \neq 0 \) for all \( i \). Let us set, following the original definition of Goppa,

\[
\Gamma'(g, \alpha) = \left\{ \alpha \in K^n \mid \sum_{i=1}^{n} \frac{a_i}{x-\alpha_i} \equiv 0 \mod g \right\}.
\]

[*]

In this problem we will see that \( \Gamma'(g, \alpha) = \Gamma(g, \alpha) \).

1) Given \( \alpha \in \bar{K} \) such that \( g(\alpha) \neq 0 \), show that \( x-\alpha \) is invertible mod \( g \) and that

\[
\frac{1}{x-\alpha} = -\frac{1}{g(\alpha)} \frac{g(x)-g(\alpha)}{x-\alpha} \mod g
\]

(note that \( \frac{g(x)-g(\alpha)}{x-\alpha} \) is a polynomial of degree \( < r \) with coefficients in \( \bar{K} \)).

2) Show that the condition

\[
\sum_{i=1}^{n} \frac{a_i}{x-\alpha_i} \equiv 0 \mod g
\]

is equivalent to
$$\sum_{i=1}^{n} \frac{a_i}{g(\alpha_i)} \frac{g(x) - g(\alpha_i)}{x - \alpha_i} = 0.$$ 

3) Use this relation to prove that the code defined by [*] admits a control matrix of the form

$$H^* = U \cdot H = U \cdot V_r(\alpha_1, ..., \alpha_n) \cdot \text{diag}(h_1, ..., h_n),$$

where $h_i = 1/g(\alpha_i)$ and $U = (g_{r-i+j})_{1 \leq i, j \leq r}$, $g = g_0 + g_1X + \cdots + g_rX^r$ (and taking $g_l = 0$ if $l < 0$ or $l > r$).

4) Since $U$ is invertible, the code defined by [*] also admits a control matrix of the form

$$H = V_r(\alpha_1, ..., \alpha_n) \cdot \text{diag}(h_1, ..., h_n),$$

and this establishes that $\Gamma'(g, \alpha) = \Gamma(g, \alpha)$.

65 (Improving the minimum distance bound for binary Goppa codes). With the same notations as in the preceding problem, let $\bar{g}$ be the monic polynomial of minimum degree with the conditions that it is a square and that it is a multiple of $g$. If $K = \mathbb{Z}_2$, we will see that $\Gamma(g, \alpha) = \Gamma(\bar{g}, \alpha)$ and therefore that we have
\( d \geq \bar{r} + 1 \), where \( d \) is the minimum distance of \( \Gamma(g, \alpha) \). In particular we see that \( d \geq 2r + 1 \) if \( g \) has no repeated roots.

1) Suppose that \( \mathbf{a} \in K^n \) satisfies \( \sum_{i=1}^{n} \frac{a_i}{x-\alpha_i} \equiv 0 \mod g \) and let \( S = S(\mathbf{a}) \) be the support of \( \mathbf{a} \) (thus \( s = |S| \) is the weight of \( \mathbf{a} \)). Let \( f_a = \prod_{i \in S}(X - \alpha_i) \). Show that

\[
f_a \cdot \sum_{i \in S} \frac{1}{x-\alpha_i} = f'_a
\]

(\( f'_a \) is the derivative of \( f_a \)).

2) Use the fact that \( f_a \) and \( f'_a \) have no common factors to prove that

\[
\sum_{i \in S} \frac{1}{x-\alpha_i} \equiv 0 \mod g
\]

if and only if \( g|f'_a \).

3) Show that \( f'_a \) is a square, and hence that \( g|f'_a \) if and only if \( \bar{g}|f_a \).

4) Conclude that \( \Gamma(g, \alpha) = \Gamma(\bar{g}, \alpha) \), as claimed.

66 (Alternative forms of the syndrome and error locator polynomials, the Forney formula and the key equation). Suppose that we define the polynomial
syndrome $S(z)$, the error locator polynomial $\sigma(z)$ and the error evaluator $\epsilon(z)$ as follows:

$$S(z) = S_0 z^{r-1} + \cdots + S_{r-1},$$

$$\sigma(z) = \prod_{i=1}^{s} (z - \eta_i),$$

$$\epsilon(z) = -\sum_{i=1}^{s} h_m e_m \eta_i^r \prod_{j \neq i} (z - \eta_i)$$

(thus we see that $\sigma$ is the monic polynomial whose roots are $\eta_1, \ldots, \eta_s$).

1) Show that

$$\sigma'(\eta_k) = \prod_{j \neq k} (\eta_k - \eta_j)$$

$$\epsilon(\eta_k) = -h_m \epsilon_m \eta_k^r \prod_{j \neq k} (\eta_k - \eta_j)$$

and, as a consequence, that we have the following (alternative) Forney formula:

$$e_m = -\frac{\epsilon(\eta_k)}{h_m \eta_k^r \sigma'(\eta_k)}.$$  

2) Prove the key equation is still valid:

$$\epsilon(z) \equiv \sigma(z) S(z) \mod z^r.$$
3) If we set \{\bar{\epsilon}, \bar{\sigma}\} to denote the pair delivered by sugiyama(\(Z^r, S, t\)), notice that the zeroes of \(\bar{\sigma}\) are the error locators, and that the alternative Forney formula used with \(\bar{\epsilon}\) and \(\bar{\sigma}\) gives the error values.

67. With the notations introduced in the Problem 64:

1) Prove that the syndrome \(S_y^*\) with respect to the control matrix

\[
H^* = U \cdot H = U \cdot V_r(\alpha) \cdot \text{diag}(h)
\]

of the received vector \(y\) corresponds to the polynomial

\[
S_y^*(z) = -\sum_{i=0}^{n-1} \frac{y_i \, g(z) - g(\alpha_i)}{g(\alpha_i) \, z - \alpha_i},
\]

and that this is the only polynomial of degree < \(r\) such that

\[
S_y^*(z) = \sum_{i=0}^{n-1} \frac{y_i}{z - \alpha_i} \mod g(z).
\]

Show also that \(S_y^*(z) = S_e^*(z)\), where \(e\) is the error vector.

2) If we define the error locator polynomial

\[
\sigma^*(z) = \prod_{i=1}^{s}(z - \eta_i)
\]
(as in Problem 66) and the error evaluating polynomial as

\[ \epsilon^*(z) = \sum_{i=1}^{s} e_{m_i} \prod_{i=1}^{s} (z - \eta_i), \]

then

\[ \deg(\sigma^*) = s, \quad \deg(\epsilon^*) < s, \quad \text{mcd}(\sigma^*, \epsilon^*). \]

Prove that

\[ e_{m_i} = \frac{\epsilon^*(\eta_i)}{\sigma^*((\eta_i))} \]

(Forney’s formular adapted to this case) and that the following key equation holds:

\[ \sigma^*(z)S^*(z) \equiv \epsilon^*(z) \mod g(z). \]

3) Describe a decoding algorithm by adapting the BMS algorithm to this case).

68. Find an RS code with rate 3/5 and which corrects 25 errors. What are its parameters? What is the minimum cardinal of the base field? Estimate the number of field operations that are necessary to decode a vector by the BMS algorithm.
69. Consider the code \( C = \Gamma(T^{10} + T^2 + T + 3, \alpha) \) over \( \mathbb{Z}_5 \), where \( \alpha \) is the vector of non-zero elements of \( \mathbb{F}_{25} \). Show that \( \dim(C) = 4 \). Note that it coincides with the minimum bound \( n - mr \) for the dimension \( k \) of alternant codes, as \( n = 24, r = 10 \) and \( m = 2 \). Note also that if we use the polynomial \( T^{10} \) instead of \( T^{10} + T^2 + T + 3 \), then the corresponding Goppa code, \( \Gamma(T^{10}, \alpha) \), has dimension 9.