# Exercise Sheet 7

**Exercise 7.1.** Let $C$ be the binary cyclic code of length 15 with generator $x^2 + x + 1$. Show that $C$ is a BCH code but not a Goppa code.

**Exercise 7.2.**

1. Let $\Gamma = \Gamma(L, g)$ be a Goppa code with $L = \{0, 1, \alpha, \ldots, \alpha^6\}$, where $\alpha$ is a primitive element of $\mathbb{F}_8$, and $g(z) := z^2 + z + 1$. Find lower bounds on the dimension and the distance of this code.

2. Compute a parity check matrix for the code. Use the following binary representation of $\mathbb{F}_8 = \mathbb{F}_2[X]/(\alpha^3 + \alpha + 1)$:

| $i$ | representation of $\alpha^i$ |
|---|---|
| 0 | 100 |
| 1 | 010 |
| 2 | 001 |
| 3 | 110 |
| 4 | 011 |
| 5 | 111 |
| 6 | 101 |

3. Find the list of codewords.

**Exercise 7.3.** Let $\Gamma = \Gamma(L, g)$ be a binary Goppa code of length $n$ with $L = \{1, \alpha, \ldots, \alpha^{n-1}\}$, where $\alpha$ is a primitive $n$th root of unity in $\mathbb{F}_{2^m}$.

1. For a polynomial $a(x) := \sum_{i=0}^{n-1} a_i x^i$, where $a_i \in \mathbb{F}_2$, define $A_i := a(\alpha^i)$ and $A(z) := \sum_{i=0}^{n-1} A_{-i} z^i$. This is called the *Mattson-Solomon polynomial* of $a(x)$. Show the inverse relation
$$a(x) = \frac{1}{n} \sum_{i=0}^{n-1} A(\alpha^i) x^i.$$

2. Let
$$R_a(z) := \sum_{i=0}^{n-1} \frac{a_i}{z + \alpha^i}.$$
Show that $R_a(z) = \sum_{i=0}^{n-1} A(\alpha^i)/(z + \alpha^i)$.

3. Show that $(z^n + 1)R_a(z) = \sum_{i=0}^{n-1} a_i \prod_{j \neq i}(z + \alpha^j)$.

4. Show that
$$z \prod_{j \neq i}(z + \alpha^j) \equiv \sum_{j=0}^{n-1} \alpha^{-ij} z^j \pmod{z^n + 1}.$$
(Hint: multiply both sides by $z + \alpha^i$).

5. Conclude that $A(z) \equiv z(z^n + 1)R_a(z) \pmod{z^n + 1}$.

6. Using previous parts, show that $(a_0, \ldots a_{n-1}) \in \Gamma$ iff

$$(z^{n-1}A(z) \bmod (z^n + 1)) \equiv 0 \pmod{g(z)}.$$

(Hint: First show that $(a_0, \ldots a_{n-1})$ is a codeword iff $R_a(z)(z^n + 1) \equiv 0 \mod g(z)$.)

**Exercise 7.4.** Same as the previous exercise, let $\Gamma = \Gamma(L, g)$ be a binary Goppa code of length $n$ with $L = \{1, \alpha, \ldots, \alpha^{n-1}\}$, where $\alpha$ is a primitive $n$th root of unity in $\mathbb{F}_{2^m}$.

1. Let $a(x) = \sum_{i=0}^{n-1} a_i x^i$ and $a'(x) = x^{n-1}a(x) \pmod{x^n - 1}$ be its cyclic shift. Show that $A'(z) = A(\alpha z)$.
2. Let $(a_0, \ldots a_{n-1})$ be a codeword of even weight and $a(x)$ be its polynomial representation. Show that $A(z)$ is divisible by $z$ and $A(z)/z$ is a multiple of $g(z)$. (Hint: Use the previous exercise)
3. Show that if $\Gamma$ is cyclic, then $g(z) = z^r$ for some $r$. (Hint: Show that if $g$ has a nonzero root $\beta$ over some extension field, then $A(\beta) = 0$ for any even weight word. Then use cyclicity to conclude that $A(z)$ would have too many roots.)