1 Binary Goppa Codes

1.1 Definition

- Typically, a Binary Goppa Code is defined by a list

$$L = a_1 + a_2 + \cdots + a_n$$

  of distinct integers n over finite field F_q, where $q = 2^m$, which is also called the support.

- It must also have a square-free polynomial $g(x) \in F_q[x]$, with degree t such that $g(a) \neq 0$ for all $a \in L$.

- Finally, $g(x)$ should also be irreducible over F_q, meaning it cannot be reduced to its roots over F_q.

- So, the corresponding Binary Goppa Code can be defined as

$$\gamma(L, g) = \{\mathbf{x} \in F_q^n | \sum_{i=1}^{n} \frac{c_i}{x - L_i} \equiv 0 \mod g(x)\}$$

The code defined by (g, L) posseses a dimension of at least n - mt, and a distance of at least 2t+1. This means that it will be able to encode messages with a length of at least n - mt that are comprised of codewords of at least size n, and will be able to correct at least

$$\frac{(2t+1) - 1}{2}$$

errors.