Goppa codes are part of a larger family of codes known as Alternant Codes. Alternant Codes, which are related to Generalized Reed-Solomon codes, include in addition to Goppa Codes, BCH Codes, and Srivastava codes. Discovered in 1971 by the Russian Scientist Vladimir D. Goppa, interest in Goppa codes grew after 1982, when Tsfasman, Vladut, and Zink showed that some Goppa codes assymptotically have better error-correcting capability than the Gilbert-Varshamov bound.

Prime Power Fields

Prime power fields are essential to the construction of Goppa codes. We will reffer to a prime power field as GF(p^m), where p is a prime, and m is some positive power. They can be represented in different forms:

• As polynomial field over a prime field, for example GF(2)$[x]/(x^2+x+1)$ is a field with 4 elements.

• As columns vectors of length m, with entries in GF(p). The first entry would represent the constant terms of the polynomial, while the m'th entry is the element of GF(p) by which we multiply the $m-1$ power of x.

• As powers of some polynomial, here denoted by a Greek letter α.

Vandermonde Matrices

• All Alternant Codes have parity check marices that can be factored into a full rank matrix, and a Vandermonde matrix.

• A Vandermonde matrix is an $r \times r$ matrix of the form

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ a_1 & a_2 & \cdots & a_{r-1} & a_r \\ a_1^2 & a_2^2 & \cdots & a_{r-1}^2 & a_r^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1^{r-2} & a_2^{r-2} & \cdots & a_{r-1}^{r-2} & a_r^{r-2} \\ a_1^{r-1} & a_2^{r-1} & \cdots & a_{r-1}^{r-1} & a_r^{r-1} \end{pmatrix}$$

Where $a_1, a_2, \cdots, a_{r-1}, a_r$ are distinct non-zero elements of a field, GF(q^m).

• Vandermonde matrices have full rank.

• The r columns of a Vandermonde Matrix are linearly independent.

Construction of Goppa Codes

We need the following to construct a Goppa Code:

• A field GF(q^m) where m is fixed.

• A Goppa polynomial $G(x)$, which we will consider over the field GF(q^m)

• A subset $L = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ of GF(q^m). The only property needed for L is that the Goppa polynomial does not have a zero in L.

We can now construct a rational function

$$R_{\mathbf{a}}(x) = \sum_{i=1}^{n} \frac{a_i}{x - \alpha_i}$$

which is defined for any vector $\mathbf{a} = a_1, a_2, ..., a_n$ in GF$^n(q)$

Definition of Goppa Codes

Definition 1 *The Goppa Code* $\Gamma(L, G)$ *is the set of all vectors* $\mathbf{a} \in \mathsf{GF}^n(q)$*, with the property that*

$$R_{\mathbf{a}}(x) \equiv 0 \pmod{G(x)}$$

The statement $R_{\mathbf{a}}(x) \equiv 0 \pmod{G(x)}$ means that the polynomial equivalent to $R_{\mathbf{a}}(x)$ can be written as the product of some polynomial with $G(x)$.

In fact, with some algebra, we obtain a result saying that if $R_{\mathbf{a}}(x) \equiv 0 \pmod{G(x)}$, then $R_{\mathbf{a}}(x) = 0$

• We can also see that Goppa Codes are linear. The best way to find the parameters of a Goppa Code is through a parity check matrix.

A Parity Check Matrix

• The parity check matrix for the Goppa code is

$$\begin{pmatrix} G(\alpha_1)^{-1} & G(\alpha_2)^{-1} & \cdots & G(\alpha_n)^{-1} \\ \alpha_1 G(\alpha_1)^{-1} & \alpha_2 G(\alpha_2)^{-1} & \cdots & \alpha_n G(\alpha_n)^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{r-2} G(\alpha_1)^{-1} & \alpha_2^{r-2} G(\alpha_2)^{-1} & \cdots & \alpha_n^{r-2} G(\alpha_n)^{-1} \\ \alpha_1^{r-1} G(\alpha_1)^{-1} & \alpha_2^{r-1} G(\alpha_2)^{-1} & \cdots & \alpha_n^{r-1} G(\alpha_n)^{-1} \end{pmatrix}$$

where r is the order of the Goppa polynomial.

• The parity check matrix for the Goppa code can be factored as the product of a diagonal matrix with

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} & \alpha_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{r-2} & \alpha_2^{r-2} & \cdots & \alpha_{n-1}^{r-2} & \alpha_n^{r-2} \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_{n-1}^{r-1} & \alpha_n^{r-1} \end{pmatrix}$$

Parameters of Goppa Codes

• By truncating $n - r$ rows, this parity check matrix would look like a Vandermonde Matrix. So at least r columns are linearly independent.

• To get a parity check matrix with elements in GF(p), we have to replace each entry with the column vector that represents it.

• Moving to elements in does not change the number of linearly independent columns. Since at least r columns are linearly independent, we get $d \geq r + 1$.

• Upon row reducing the parity check matrix, we find that the number of linearly independent rows is from r to mr. So $\Gamma(L, G)$ has dimension k, where $n - mr \leq k \leq n - r$.

The field of Order 8

• We will consider the field of 8 elements, GF(8), which we can also write as GF(2)$[x]/(x^3+x+1) = \{0, 1, x, x^2, x+1, x+x^2, 1+x+x^2, 1+x^2\}$.

• Now, let $\alpha = x$, then, we can see how the three different representations for elements of a prime power field are equivalent

$$\begin{bmatrix} 0 & 0 & 000 \\ 1 & 1 & 100 \\ \alpha & x & 010 \\ \alpha^2 & x^2 & 001 \\ \alpha^3 & 1+x & 110 \\ \alpha^4 & x+x^2 & 011 \\ \alpha^5 & 1+x+x^2 & 111 \\ \alpha^6 & 1+x^2 & 101 \end{bmatrix}$$

The Polynomial $x^2 + 1$

- If we choose $G(x) = x^2 + 1$, then,

$$\begin{array}{lllll}
G(0) & = & G(0) & = & 1 & = & 1 \\
G(1) & = & G(1) & = & 0 & = & 0 \\
G(\alpha) & = & G(x) & = & x^2 + 1 & = & \alpha^6 \\
G(\alpha^2) & = & G(x^2) & = & 1 + x + x^2 & = & \alpha^5 \\
G(\alpha^3) & = & G(1 + x) & = & x^2 & = & \alpha^2 \\
G(\alpha^4) & = & G(x + x^2) & = & 1 + x & = & \alpha^3 \\
G(\alpha^5) & = & G(1 + x + x^2) & = & x & = & \alpha \\
G(\alpha^6) & = & G(1 + x^2) & = & x + x^2 & = & \alpha^4
\end{array}$$

- We can now choose $L = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ since $G(x)$ is non-zero at all these values.

The Parity Check Matrix

• From the previous results about the parity check matrix of Goppa codes, the parity check matrix of this code should be

$$\begin{pmatrix} \frac{1}{1} & \frac{1}{\alpha^6} & \frac{1}{\alpha^5} & \frac{1}{\alpha^2} & \frac{1}{\alpha^3} & \frac{1}{\alpha} & \frac{1}{\alpha^4} \end{pmatrix}$$

• Using the previous table for $GF(8)$, we can simplify the parity check matrix:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha^3 \end{pmatrix}$$

• We can now easily find the parity check matrix of the code in binary, and it is:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$