Chapter 6
Lagrange Codes

6.1 Introduction

Joseph Louis Lagrange was a famous eighteenth century Italian mathematician [1] credited with minimum degree polynomial interpolation amongst his many other achievements. Polynomial interpolation may be applied straightforwardly using Galois Fields and provides the basis for an extensive family of error-correcting codes. For a Galois Field $GF(2^m)$, the maximum code length is 2^{m+1}, consisting of 2^m data symbols and 2^m parity symbols. Many of the different types of codes originated by Goppa [3, 4] may be linked to Lagrange codes.

6.2 Lagrange Interpolation

The interpolation polynomial, $p(z)$, is constructed such that the value of the polynomial for each element of $GF(2^m)$ is equal to a data symbol x_i also from $GF(2^m)$. Thus,

$$\begin{bmatrix} p(0) & = & x_0 \\ p(1) & = & x_1 \\ p(\alpha^1) & = & x_2 \\ p(\alpha^2) & = & x_3 \\ \cdots & \cdots & \cdots \\ p(\alpha^{2^m-3}) & = & x_{2^m-2} \\ p(\alpha^{2^m-2}) & = & x_{2^m-1} \end{bmatrix}$$

Using the method of Lagrange, the interpolation polynomial is constructed as a summation of 2^m polynomials, each of degree $2^m - 1$. Thus,

M. Tomlinson et al., *Error-Correction Coding and Decoding*,
Signals and Communication Technology,
DOI 10.1007/978-3-319-51103-0_6

Table 6.1 $GF(8)$ extension field defined by $1 + \alpha^1 + \alpha^3 = 0$

$\alpha^0 = 1$
$\alpha^1 = \alpha$
$\alpha^2 = \alpha^2$
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

$$p(z) = \sum_{i=0}^{2^m-1} p_i(z) \tag{6.1}$$

where

$$p_i(z) = x_i \frac{z}{\alpha^i} \prod_{j=0, j\neq i}^{j=2^m-2} \frac{z - \alpha^j}{\alpha^i - \alpha^j} \quad \text{for} \quad i \neq 0 \tag{6.2}$$

and

$$p_0(z) = x_0 \prod_{j=0}^{j=2^m-2} \frac{z - \alpha^j}{(-\alpha^j)} \tag{6.3}$$

The idea is that each of the $p_i(z)$ polynomials has a value of zero for z equal to each element of $GF(2^m)$, except for the one element corresponding to i (namely α^{i-1} except for $i = 0$).

A simpler form for the polynomials $p_i(z)$ is given by

$$p_i(z) = x_i \frac{(\alpha^i - \alpha^j)}{\alpha^i(\alpha^i - 1)} \frac{z(z^{2^m-1} - 1)}{z - \alpha^j} \quad \text{for} \quad i \neq 0 \tag{6.4}$$

and

$$p_0(z) = -x_0(z^{2^m-1} - 1) \tag{6.5}$$

In an example using $GF(2^3)$, where all the nonzero field elements may express as a power of a primitive root α of the primitive polynomial $1 + x + x^3$, modulo $1 + x^7$. The nonzero field elements are tabulated in Table 6.1.

All of the 8 polynomials $p_i(z)$ are given below

$$\begin{aligned}
p_0(z) &= x_0(z^7 \quad +1) \\
p_1(z) &= x_1(z^7 \quad +z^6 \quad +z^5 \quad +z^4 \quad +z^3 \quad +z^2 \quad +z) \\
p_2(z) &= x_2(z^7 \quad +\alpha z^6 \quad +\alpha^2 z^5 \quad +\alpha^3 z^4 \quad +\alpha^4 z^3 \quad +\alpha^5 z^2 \quad +\alpha^6 z) \\
p_3(z) &= x_3(z^7 \quad +\alpha^2 z^6 \quad +\alpha^4 z^5 \quad +\alpha^6 z^4 \quad +\alpha z^3 \quad +\alpha^3 z^2 \quad +\alpha^5 z) \\
p_4(z) &= x_4(z^7 \quad +\alpha^3 z^6 \quad +\alpha^6 z^5 \quad +\alpha^2 z^4 \quad +\alpha^5 z^3 \quad +\alpha z^2 \quad +\alpha^4 z) \\
p_5(z) &= x_5(z^7 \quad +\alpha^4 z^6 \quad +\alpha z^5 \quad +\alpha^5 z^4 \quad +\alpha^2 z^3 \quad +\alpha^6 z^2 \quad +\alpha^3 z) \\
p_6(z) &= x_6(z^7 \quad +\alpha^5 z^6 \quad +\alpha^3 z^5 \quad +\alpha z^4 \quad +\alpha^6 z^3 \quad +\alpha^4 z^2 \quad +\alpha^2 z) \\
p_7(z) &= x_7(z^7 \quad +\alpha^6 z^6 \quad +\alpha^5 z^5 \quad +\alpha^4 z^4 \quad +\alpha^3 z^3 \quad +\alpha^2 z^2 \quad +\alpha z)
\end{aligned}$$

These polynomials are simply summed to produce the Lagrange interpolation polynomial $p(z)$

$$\begin{aligned}
p(z) = \; & z^7(x_0 \quad +x_1 \quad +x_2 \quad +x_3 \quad +x_4 \quad +x_5 \quad +x_6 \quad +x_7) \\
& + z^6(\alpha x_1 \quad +\alpha^2 x_2 \quad +\alpha^3 x_3 \quad +\alpha^4 x_4 \quad +\alpha^5 x_5 \quad +\alpha^6 x_6 \quad +x_7) \\
& + z^5(\alpha^2 x_1 \quad +\alpha^4 x_2 \quad +\alpha^6 x_3 \quad +\alpha x_4 \quad +\alpha^3 x_5 \quad +\alpha^5 x_6 \quad +x_7) \\
& + z^4(\alpha^3 x_1 \quad +\alpha^6 x_2 \quad +\alpha^2 x_3 \quad +\alpha^5 x_4 \quad +\alpha x_5 \quad +\alpha^4 x_6 \quad +x_7) \\
& + z^3(\alpha^4 x_1 \quad +\alpha x_2 \quad +\alpha^5 x_3 \quad +\alpha^2 x_4 \quad +\alpha^6 x_5 \quad +\alpha^3 x_6 \quad +x_7) \\
& + z^2(\alpha^5 x_1 \quad +\alpha^3 x_2 \quad +\alpha x_3 \quad +\alpha^6 x_4 \quad +\alpha^4 x_5 \quad +\alpha^2 x_6 \quad +x_7) \\
& + z(\alpha^6 x_1 \quad +\alpha^5 x_2 \quad +\alpha^4 x_3 \quad +\alpha^3 x_4 \quad +\alpha^2 x_5 \quad +\alpha x_6 \quad +x_7) \\
& + \quad x_0
\end{aligned} \tag{6.6}$$

This can be easily verified by evaluating $p(z)$ for each element of $GR(2^3)$ to produce

$$\begin{aligned}
p(0) &= x_0 \\
p(1) &= x_1 \\
p(\alpha) &= x_2 \\
p(\alpha^2) &= x_3 \\
p(\alpha^3) &= x_4 \\
p(\alpha^4) &= x_5 \\
p(\alpha^5) &= x_6 \\
p(\alpha^6) &= x_7
\end{aligned}$$

6.3 Lagrange Error-Correcting Codes

The interpolation polynomial $p(z)$ may be expressed in terms of its coefficients and used as a basis for defining error-correcting codes.

$$p(z) = \sum_{i=0}^{2^m-1} \mu_i z^i \tag{6.7}$$

It is clear that an interpolation equation and a parity check equation are equivalent, and for the 8 identities given by the interpolation polynomial we may define 8 parity check equations:

$$\begin{aligned} x_0 + p(0) &= 0 \\ x_1 + p(1) &= 0 \\ x_2 + p(\alpha) &= 0 \\ x_3 + p(\alpha^2) &= 0 \\ x_4 + p(\alpha^3) &= 0 \\ x_5 + p(\alpha^4) &= 0 \\ x_6 + p(\alpha^5) &= 0 \\ x_7 + p(\alpha^6) &= 0 \end{aligned} \tag{6.8}$$

The 8 parity check equations become

$$\begin{array}{llllllll} x_0+ & \mu_0 & & & & & & = 0 \\ x_1+ & \mu_1+ & \mu_2+ & \mu_3+ & \mu_4+ & \mu_5+ & \mu_6+ & \mu_7 = 0 \\ x_2+ & \alpha\mu_1+ & \alpha^2\mu_2+ & \alpha^3\mu_3+ & \alpha^4\mu_4+ & \alpha^5\mu_5+ & \alpha^6\mu_6+ & \mu_7 = 0 \\ x_3+ & \alpha^2\mu_1+ & \alpha^4\mu_2+ & \alpha^6\mu_3+ & \alpha\mu_4+ & \alpha^3\mu_5+ & \alpha^5\mu_6+ & \mu_7 = 0 \\ x_4+ & \alpha^3\mu_1+ & \alpha^6\mu_2+ & \alpha^2\mu_3+ & \alpha^5\mu_4+ & \alpha\mu_5+ & \alpha^4\mu_6+ & \mu_7 = 0 \\ x_5+ & \alpha^4\mu_1+ & \alpha\mu_2+ & \alpha^5\mu_3+ & \alpha^2\mu_4+ & \alpha^6\mu_5+ & \alpha^3\mu_6+ & \mu_7 = 0 \\ x_6+ & \alpha^5\mu_1+ & \alpha^3\mu_2+ & \alpha\mu_3+ & \alpha^6\mu_4+ & \alpha^4\mu_5+ & \alpha^2\mu_6+ & \mu_7 = 0 \\ x_7+ & \alpha^6\mu_1+ & \alpha^5\mu_2+ & \alpha^4\mu_3+ & \alpha^3\mu_4+ & \alpha^2\mu_5+ & \alpha\mu_6+ & \mu_7 = 0 \end{array} \tag{6.9}$$

A number of different codes may be derived from these equations. Using the first 4 equations, apart from the first, and setting x_2 and x_3 equal to 0, the following parity check matrix is obtained, producing a (9, 5) code:

$$\mathbf{H}_{9,5} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & 1 \\ 0 & 0 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 & 1 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 & 1 \end{bmatrix}$$

Rearranging the order of the columns produces a parity check matrix, $\hat{\mathbf{H}}$ identical to the MDS (9, 5, 5) code based on the doubly extended Reed–Solomon code [7].

$$\hat{\mathbf{H}}_{(9,5,5)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & 0 & 0 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 & 0 & 0 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 & 0 & 1 \end{bmatrix}$$

Correspondingly, we know that the code with parity check matrix, $\mathbf{H}_{9,5}$ derived from the Lagrange interpolating polynomial is MDS and has a minimum Hamming distance of 5. Useful, longer codes can also be obtained. Adding the first row of (6.9) to the second equation of the above example and setting x_0 equal to x_1, a parity check matrix for a (10, 6) code is obtained:

$$\mathbf{H_{10,6}} = \begin{bmatrix} 0\,1\,0\;\;1\;\;\;1\;\;\;1\;\;\;1\;\;\;1\;\;\;1 \\ 1\,1\,0\;\;\alpha\;\;\alpha^2\;\alpha^3\;\alpha^4\;\alpha^5\;\alpha^6\;1 \\ 0\,0\,0\;\alpha^2\;\alpha^4\;\alpha^6\;\;\alpha\;\;\alpha^3\;\alpha^5\;1 \\ 0\,0\,1\;\alpha^3\;\alpha^6\;\alpha^2\;\alpha^5\;\;\alpha\;\;\alpha^4\;1 \end{bmatrix}$$

It is straightforward to map any code with $GF(2^m)$ symbols into a binary code by simply mapping each $GF(2^m)$ symbol into a $m \times m$ binary matrix using the $GF(2^m)$ table of field elements. If the codeword coordinate is α^i, the coordinate is replaced with the matrix, where each column is the binary representation of the $GF(2^m)$ symbol:

$$\left[\alpha^i\;\alpha^{i+1}\;\alpha^{i+2}\;\ldots\;\alpha^{i+m-1}\right]$$

As an example for $GF(2^3)$, if the codeword coordinate is α^3, the symbol is replaced with the binary matrix whose columns are the binary values of α^3, α^4, and α^5 using Table 6.1.

$$\begin{bmatrix} 1\,0\,1 \\ 1\,1\,1 \\ 0\,1\,1 \end{bmatrix}$$

In another example the symbol α^0 produces the identity matrix

$$\begin{bmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{bmatrix}$$

The (10, 6) GF(8) code above forms a (30, 18) binary code with parity check matrix

$$\mathbf{H_{30,18}} = \begin{bmatrix} 0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1 \\ \\ 1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0 \\ 0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,1 \\ \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1 \\ \\ 0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,0\,0\,0\,1 \end{bmatrix}$$

The minimum Hamming distance of this code has been evaluated and it turns out to be 4. Methods for evaluating the minimum Hamming distance are described in Chap. 5. Consequently, extending the length of the code by one symbol has reduced the d_{min} by 1. The d_{min} may be increased by 2 by adding an overall parity bit to the first two symbols plus an overall parity bit to all bits to produce a (32, 18, 6) code with parity check matrix

$$\mathbf{H_{32,18}} = \left[\begin{array}{c}
0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0 \\
0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0 \\
0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0 \\
\\
1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0 \\
0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0 \\
0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0 \\
1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 \\
\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0 \\
\\
0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0\,0 \\
1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1
\end{array}\right]$$

This is a good code as weight spectrum analysis shows that it has the same minimum Hamming distance as the best known (32, 18, 6) code [5]. It is interesting to note that in extending the length of the code beyond the MDS length of 9 symbols for $GF(2^3)$, two *weak* symbols are produced but these are counterbalanced by adding an overall parity bit to these two symbols.

6.4 Error-Correcting Codes Derived from the Lagrange Coefficients

In another approach, we may set some of the equations defining the Lagrange polynomial coefficients to zero, and then use these equations to define parity checks for the code. As an example, using $GF(2^3)$, from Eq. (6.6) we may set coefficients μ_7, μ_6, μ_5, μ_4 and μ_3 equal to zero. The parity check equations become

$$\begin{array}{ccccccccc}
x_0 & +x_1 & +x_2 & +x_3 & +x_4 & +x_5 & +x_6 & +x_7 & = 0 \\
\alpha x_1 & +\alpha^2 x_2 & +\alpha^3 x_3 & +\alpha^4 x_4 & +\alpha^5 x_5 & +\alpha^6 x_6 & +x_7 & & = 0 \\
\alpha^2 x_1 & +\alpha^4 x_2 & +\alpha^6 x_3 & +\alpha x_4 & +\alpha^3 x_5 & +\alpha^5 x_6 & +x_7 & & = 0 \\
\alpha^3 x_1 & +\alpha^6 x_2 & +\alpha^2 x_3 & +\alpha^5 x_4 & +\alpha x_5 & +\alpha^4 x_6 & +x_7 & & = 0 \\
\alpha^4 x_1 & +\alpha x_2 & +\alpha^5 x_3 & +\alpha^2 x_4 & +\alpha^6 x_5 & +\alpha^3 x_6 & +x_7 & & = 0
\end{array} \tag{6.10}$$

and the corresponding parity check matrix is

$$\mathbf{H_{8,3}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & 1 \\ 0 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 & 1 \\ 0 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 & 1 \\ 0 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 & 1 \end{bmatrix} \tag{6.11}$$

As a $GF(2^3)$ code, this code is MDS with a d_{min} of 6 and equivalent to the extended Reed–Solomon code. As a binary code with the following parity check matrix a (24, 9, 8) code is obtained. This is a good code as it has the same minimum Hamming distance as the best known (24, 9, 8) code [5].

$$\mathbf{H_{24,9}} = \begin{bmatrix} 1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0 \\ 0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1 \\ \\ 0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0 \\ 0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,1 \\ \\ 0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0 \\ 0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1 \\ \\ 0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0 \\ 0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,0\,0\,0\,1 \\ \\ 0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0\,0 \\ 0\,0\,0\,1\,1\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,0\,1\,0 \\ 0\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,1 \end{bmatrix}$$

6.5 Goppa Codes

So far codes have been constructed using the Lagrange interpolating polynomial in a rather ad hoc manner. Goppa defined a family of codes [3] in terms of the Lagrange interpolating polynomial, where the coordinates of each codeword $\{c_0, c_1, c_2, \ldots c_{2^m-1}\}$ with $\{c_0 = x_0, c_1 = x_1, c_2 = x_2, \ldots c_{2^m-1} = x_{2^m-1}\}$ satisfy the congruence $p(z)$ *modulo* $g(z) = 0$ where $g(z)$ is known as the Goppa polynomial.

Goppa codes have coefficients from $GF(2^m)$ and provided $g(z)$ has no roots which are elements of $GF(2^m)$ (which is straightforward to achieve) the Goppa codes have parameters $(2^m, k, 2^m - k + 1)$. These codes are MDS codes and satisfy the Singleton

bound [8]. Goppa codes as binary codes, provided that $g(z)$ has no roots which are elements of $GF(2^m)$ and has no repeated roots, have parameters $(2^m, 2^m - mt, d_{min})$ where $d_{min} \geq 2t + 1$, the Goppa code bound on minimum Hamming distance. Most binary Goppa codes have equality for the bound and t is the number of correctable errors for hard decision, bounded distance decoding. Primitive binary BCH codes have parameters $(2^m - 1, 2^m - mt - 1, d_{min})$, where $d_{min} \geq 2t + 1$ and so binary Goppa codes usually have the advantage over binary BCH codes of an additional information bit for the same minimum Hamming distance. However, depending on the cyclotomic cosets, many cases of BCH codes can be found having either $k > 2^m - mt - 1$ for a given t, or $d_{min} > 2t + 1$, giving BCH codes the advantage for these cases.

For a Goppa polynomial of degree r, there are r parity check equations derived from the congruence $p(z)$ *modulo* $g(z) = 0$. Denoting $g(z)$ by

$$g(z) = g_r z^r + g_{r-1} z^{r-1} + g_{r-2} z^{r-2} + \cdots + g_1 z + g_0 \tag{6.12}$$

$$\sum_{i=0}^{2^m-1} \frac{c_i}{z - \alpha_i} = 0 \quad \text{modulo } g(z) \tag{6.13}$$

Since (6.13) is modulo $g(z)$ then $g(z)$ is equivalent to 0, and we can add $g(z)$ to the numerator. Noting that

$$g(z) = (z - \alpha_i) q_i(z) + r_m \tag{6.14}$$

where r_m is the remainder, an element of $GF(2^m)$ after dividing $g(z)$ by $z - \alpha_i$. Dividing each term $z - \alpha_i$ into $1 + g(z)$ produces the following:

$$\frac{g(z) + 1}{z - \alpha_i} = q_i(z) + \frac{r_m + 1}{z - \alpha_i} \tag{6.15}$$

As r_m is a scalar, we may simply pre-weight $g(z)$ by $\frac{1}{r_m}$ so that the remainder cancels with the other numerator term which is 1.

$$\frac{\frac{g(z)}{r_m} + 1}{z - \alpha_i} = \frac{q_i(z)}{r_m} + \frac{\frac{r_m}{r_m} + 1}{z - \alpha_i} = \frac{q_i(z)}{r_m} \tag{6.16}$$

As a result of

$$g(z) = (z - \alpha_i) q_i(z) + r_m$$

when $z = \alpha_i$, $r_m = g(\alpha_i)$

Substituting for r_m in (6.16) produces

$$\frac{\frac{g(z)}{g(\alpha_i)} + 1}{z - \alpha_i} = \frac{q_i(z)}{g(\alpha_i)} \tag{6.17}$$

Since $\frac{g(z)}{g(\alpha_i)}$ modulo $g(z) = 0$

$$\frac{1}{z - \alpha_i} = \frac{q_i(z)}{g(\alpha_i)} \tag{6.18}$$

The quotient polynomial $q_i(z)$ is a polynomial of degree $r - 1$, with coefficients which are a function of α_i and the Goppa polynomial coefficients. Denoting $q_i(z)$ as

$$q_i(z) = q_{i,0} + q_{i,1}z + q_{i,2}z^2 + q_{i,3}z^3 + \cdots + q_{i,(r-1)}z^{r-1} \tag{6.19}$$

Since the coefficients of each power of z sum to zero, the r parity check equations are given by

$$\sum_{i=0}^{2^m-1} \frac{c_i q_{i,j}}{g(\alpha_i)} = 0 \quad \text{for} \quad j = 0 \quad \text{to} \quad r - 1 \tag{6.20}$$

If the Goppa polynomial has any roots which are elements of $GF(2^m)$, say α_j, then the codeword coordinate c_j has to be permanently set to zero in order to satisfy the parity check equations. Effectively, the code length is shortened by the number of roots of $g(z)$ which are elements of $GF(2^m)$. Usually, the Goppa polynomial is chosen to have distinct roots which are not in $GF(2^m)$.

Consider an example of a Goppa (32, 28, 5) code. There are 4 parity check symbols defined by the 4 parity check equations and the Goppa polynomial has degree 4. Choosing somewhat arbitrarily the polynomial $1 + z + z^4$ which has roots in $GF(16)$ but not in $GF(32)$, we determine $q_i(z)$ by dividing by $z - \alpha_i$.

$$q_i(z) = z^3 + \alpha_i z^2 + \alpha_i^2 z + (1 + \alpha_i^3) \tag{6.21}$$

The 4 parity check equations are

$$\sum_{i=0}^{31} \frac{c_i}{g(\alpha_i)} = 0 \tag{6.22}$$

$$\sum_{i=0}^{31} \frac{c_i \alpha_i}{g(\alpha_i)} = 0 \tag{6.23}$$

$$\sum_{i=0}^{31} \frac{c_i \alpha_i^2}{g(\alpha_i)} = 0 \tag{6.24}$$

$$\sum_{i=0}^{31} \frac{c_i(1+\alpha_i^3)}{g(\alpha_i)} = 0 \tag{6.25}$$

Using Table 6.2 to evaluate the different terms for $GF(2^5)$, the parity check matrix is

$$\mathbf{H}_{(32,\,28,\,5)} = \begin{bmatrix} 1 & 1 & \alpha^{14} & \alpha^{20} & \alpha^{25} & \dots & \alpha^{10} \\ 0 & 1 & \alpha^{15} & \alpha^{22} & \alpha^{28} & \dots & \alpha^{9} \\ 0 & 1 & \alpha^{16} & \alpha^{24} & 1 & \dots & \alpha^{8} \\ 0 & 1 & \alpha^{17} & \alpha^{26} & \alpha^{3} & \dots & \alpha^{7} \end{bmatrix} \tag{6.26}$$

To implement the Goppa code as a binary code, the symbols in the parity check matrix are replaced with their m-bit binary column representations of each respective $GF(2^m)$ symbol. For the (32, 28, 5) Goppa code above, each of the 4 parity symbols will be represented as a 5 bit symbol from Table 6.2. The parity check matrix will now have 20 rows for the binary code. The minimum Hamming distance of the binary Goppa code is improved from $r+1$ to $2r+1$, namely from 5 to 9. Correspondingly, the binary Goppa code becomes a (32, 12, 9) code with parity check matrix

Table 6.2 $GF(32)$ nonzero extension field elements defined by $1+\alpha^2+\alpha^5=0$

$\alpha^0 = 1$	$\alpha^{16} = 1+\alpha+\alpha^3+\alpha^4$
$\alpha^1 = \alpha$	$\alpha^{17} = 1+\alpha+\alpha^4$
$\alpha^2 = \alpha^2$	$\alpha^{18} = 1+\alpha$
$\alpha^3 = \alpha^3$	$\alpha^{19} = \alpha+\alpha^2$
$\alpha^4 = \alpha^4$	$\alpha^{20} = \alpha^2+\alpha^3$
$\alpha^5 = 1+\alpha^2$	$\alpha^{21} = \alpha^3+\alpha^4$
$\alpha^6 = \alpha+\alpha^3$	$\alpha^{22} = 1+\alpha^2+\alpha^4$
$\alpha^7 = \alpha^2+\alpha^4$	$\alpha^{23} = 1+\alpha+\alpha^2+\alpha^3$
$\alpha^8 = 1+\alpha^2+\alpha^3$	$\alpha^{24} = \alpha+\alpha^2+\alpha^3+\alpha^4$
$\alpha^9 = \alpha+\alpha^3+\alpha^4$	$\alpha^{25} = 1+\alpha^3+\alpha^4$
$\alpha^{10} = 1+\alpha^4$	$\alpha^{26} = 1+\alpha+\alpha^2+\alpha^4$
$\alpha^{11} = 1+\alpha+\alpha^2$	$\alpha^{27} = 1+\alpha+\alpha^3$
$\alpha^{12} = \alpha+\alpha^2+\alpha^3$	$\alpha^{28} = \alpha+\alpha^2+\alpha^4$
$\alpha^{13} = \alpha^2+\alpha^3+\alpha^4$	$\alpha^{29} = 1+\alpha^3$
$\alpha^{14} = 1+\alpha^2+\alpha^3+\alpha^4$	$\alpha^{30} = \alpha+\alpha^4$
$\alpha^{15} = 1+\alpha+\alpha^2+\alpha^3+\alpha^4$	

$$\mathbf{H}_{(\mathbf{32},\,\mathbf{12},\,\mathbf{9})} = \begin{bmatrix} 1\,1\,1\,0\,1\ldots1 \\ 0\,0\,0\,0\,0\ldots0 \\ 0\,0\,1\,1\,0\ldots0 \\ 0\,0\,1\,1\,1\ldots0 \\ 0\,0\,1\,0\,1\ldots1 \\ 0\,1\,1\,1\,0\ldots0 \\ 0\,0\,1\,0\,1\ldots1 \\ 0\,0\,1\,1\,1\ldots0 \\ 0\,0\,1\,0\,0\ldots1 \\ 0\,0\,1\,1\,1\ldots1 \\ 0\,1\,1\,0\,1\ldots1 \\ 0\,0\,1\,1\,0\ldots0 \\ 0\,0\,0\,1\,0\ldots1 \\ 0\,0\,1\,1\,0\ldots1 \\ 0\,0\,1\,1\,0\ldots0 \\ 0\,1\,1\,1\,0\ldots0 \\ 0\,0\,1\,1\,0\ldots0 \\ 0\,0\,0\,1\,0\ldots1 \\ 0\,0\,0\,0\,1\ldots0 \\ 0\,0\,1\,1\,0\ldots1 \end{bmatrix} \tag{6.27}$$

6.6 BCH Codes as Goppa Codes

Surprisingly, the family of Goppa codes includes as a subset the family of BCH codes with codeword coefficients from $GF(2^m)$ and parameters $(2^m-1, 2^m-1-t, t+1)$. As binary codes, using codeword coefficients $\{0, 1\}$, the BCH codes have parameters $(2^m-1, 2^m-1-mt, 2t+1)$.

For a nonbinary BCH code to correspond to a Goppa code, the Goppa polynomial, $g(z)$, is given by

$$g(z) = z^t \tag{6.28}$$

There are t parity check equations relating to the codeword coordinates $\{c_0, c_1, c_2, \ldots, c_{2^m-2}\}$ and these are given by

$$\sum_{i=0}^{2^m-2} \frac{c_i}{z-\alpha^i} = 0 \quad \text{modulo } z^t \tag{6.29}$$

Dividing 1 by $z-\alpha^i$ starting with α^i produces

$$\frac{1}{z-\alpha^i} = \alpha^{-i} + \alpha^{-2i}z + \alpha^{-3i}z^2 + \alpha^{-3i}z^3 + \cdots + \alpha^{-ti}z^{t-1} + \frac{\alpha^{-(t+1)i}z^t}{z-\alpha^i} \tag{6.30}$$

As $\alpha^{-(t+1)i}z^t$ modulo $z^t = 0$, the t parity check equations are given by

$$\sum_{i=0}^{2^m-2} c_i(\alpha^{-i} + \alpha^{-2i}z + \alpha^{-3i}z^2 + \alpha^{-4i}z^3 + \cdots + \alpha^{-ti}z^{t-1}) = 0 \tag{6.31}$$

Every coefficient of z^0 through to z^{t-1} is equated to zero, producing t parity check equations. The corresponding parity check matrix is

$$\mathbf{H}_{(\mathbf{2^m-1},\,\mathbf{2^m-t},\,\mathbf{t+1})} = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \dots & \alpha^{-(2^m-2)} \\ 1 & \alpha^{-2} & \alpha^{-4} & \alpha^{-6} & \alpha^{-8} & \dots & \alpha^{-2(2^m-2)} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \dots & \alpha^{-3(2^m-2)} \\ & \dots & \dots & \dots & \dots & \dots & \\ 1 & \alpha^{-t} & \alpha^{-2t} & \alpha^{-3t} & \alpha^{-4t} & \dots & \alpha^{-t(2^m-2)} \end{bmatrix} \tag{6.32}$$

To obtain the binary BCH code, as before, the $GF(2^m)$ symbols are replaced with their m-bit binary column representations for each corresponding $GF(2^m)$ value for each symbol. As a result, only half of the parity check equations are independent and the dependent equations may be deleted. To keep the same number of independent parity check equations as before, the degree of the Goppa polynomial is doubled. The Goppa polynomial is now given by

$$g(z) = z^{2t} \tag{6.33}$$

The parity check matrix for the binary Goppa BCH code is

$$\mathbf{H}_{(\mathbf{2^m-1},\,\mathbf{2^m-mt},\,\mathbf{2t+1})} = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \dots & \alpha^{-(2^m-2)} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \dots & \alpha^{-3(2^m-2)} \\ 1 & \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \dots & \alpha^{-5(2^m-2)} \\ & \dots & \dots & \dots & \dots & \dots & \\ 1 & \alpha^{-2t-1} & \alpha^{-2(2t-1)} & \alpha^{-3(2t-1)} & \alpha^{-4(2t-1)} & \dots & \alpha^{-(2t-1)(2^m-2)} \end{bmatrix}$$

For binary codes, any parity check equation may be squared and the resulting parity check equation will still be satisfied. As a consequence, only one parity check equation is needed for each representative from each respective cyclotomic coset. This is clearer with an example.

The cyclotomic cosets of 31, expressed as negative integers for convenience, are as follows

$$\begin{aligned} C_0 &= \{0\} \\ C_{-1} &= \{-1, -2, -4, -8, -16\} \\ C_{-3} &= \{-3, -6, -12, -24, -17\} \\ C_{-5} &= \{-5, -10, -20, -9, -18\} \\ C_{-7} &= \{-7, -14, -28, -25, -19\} \\ C_{-11} &= \{-11, -22, -13, -26, -21\} \\ C_{-15} &= \{-15, -30, -29, -27, -23\} \end{aligned}$$

To construct the $GF(32)$ nonbinary (31, 27) BCH code, the Goppa polynomial is $g(z) = z^4$ and there are 4 parity check equations with parity check matrix:

$$\mathbf{H}_{(31,27,5)} = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \dots & \alpha^{-30} \\ 1 & \alpha^{-2} & \alpha^{-4} & \alpha^{-6} & \alpha^{-8} & \dots & \alpha^{-29} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \dots & \alpha^{-28} \\ 1 & \alpha^{-4} & \alpha^{-8} & \alpha^{-12} & \alpha^{-16} & \dots & \alpha^{-27} \end{bmatrix} \tag{6.34}$$

As a binary code with binary codeword coefficients, the parity check matrix has only two independent rows. To construct the binary parity check matrix, each $GF(32)$ symbol is replaced with its 5-bit column vector so that each parity symbol will require 5 rows of the binary parity check matrix. The code becomes a (31, 21, 5) binary code. The parity check matrix for the binary code after removing the dependent rows is given by

$$\mathbf{H}_{(31,21,5)} = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \dots & \alpha^{-30} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \dots & \alpha^{-28} \end{bmatrix} \tag{6.35}$$

To maintain 4 independent parity check equations for the binary code, the Goppa polynomial is doubled in degree to become $g(z) = z^8$. Replacing each $GF(32)$ symbol with its 5-bit column vector will produce a (31, 11) binary code. The parity check matrix for the binary code is given by:

$$\mathbf{H}_{(31,11,9)} = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \dots & \alpha^{-30} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \dots & \alpha^{-28} \\ 1 & \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \dots & \alpha^{-26} \\ 1 & \alpha^{-7} & \alpha^{-14} & \alpha^{-21} & \alpha^{-28} & \dots & \alpha^{-24} \end{bmatrix} \tag{6.36}$$

Looking at the cyclotomic cosets for 31, it will be noticed that α^{-9} is in the same coset as α^{-5}, and for codewords with binary coefficients, we may use the Goppa polynomial $g(z) = z^{10}$ with the corresponding parity check matrix

$$\mathbf{H}_{(31,11,11)} = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \dots & \alpha^{-30} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \alpha^{-15} & \alpha^{-18} & \dots & \alpha^{-28} \\ 1 & \alpha^{-7} & \alpha^{-14} & \alpha^{-21} & \alpha^{-28} & \alpha^{-4} & \alpha^{-11} & \dots & \alpha^{-24} \\ 1 & \alpha^{-9} & \alpha^{-18} & \alpha^{-27} & \alpha^{-5} & \alpha^{-14} & \alpha^{-23} & \dots & \alpha^{-22} \end{bmatrix} \tag{6.37}$$

Alternatively, we may use Goppa polynomial $g(z) = z^8$ with parity check matrix given by (6.36). The result is the same code. From this analysis we can see why the d_{min} of this BCH code is greater by 2 than the BCH code bound because the degree of the Goppa polynomial is 10.

To find other exceptional BCH codes we need to look at the cyclotomic cosets to find similar cases where a row of the parity check matrix is equivalent to a higher degree row. Consider the construction of the $(31, 6, 2t + 1)$ BCH code which will

have 5 parity check equations. From the cyclotomic cosets for 31, it will be noticed that α^{-13} is in the same coset as α^{-11}, and so we may use the Goppa polynomial $g(z) = z^{14}$ and obtain a (31, 6, 15) binary BCH code. The BCH bound indicates a minimum Hamming distance of 11. Another example is evident from the cyclotomic cosets of 127 where α^{-17} is in the same coset as α^{-9}. Setting the Goppa polynomial $g(z) = z^{30}$ produces the (127, 71, 19) BCH code, whilst the BCH bound indicates a minimum Hamming distance of 17.

To see the details in the construction of the parity check matrix for the binary BCH code, we will consider the (31, 11, 11) code with parity check matrix given by matrix (6.37). Each $GF(32)$ symbol is replaced with the binary representation given by Table 6.2, as a 5-bit column vector, where α is a primitive root of the polynomial $1 + x^2 + x^5$.

The binary parity check matrix that is obtained is given by matrix (6.38).

$$\mathbf{H}_{(31,\,11,\,11)} = \begin{bmatrix} 1\,0\,1\,0\,1\,1\,1\,\ldots\,0 \\ 0\,1\,0\,1\,1\,1\,0\,\ldots\,1 \\ 0\,0\,0\,1\,0\,1\,0\,\ldots\,0 \\ 0\,0\,1\,0\,1\,0\,1\,\ldots\,0 \\ 0\,1\,0\,1\,0\,1\,1\,\ldots\,0 \\ \\ 1\,0\,1\,1\,0\,1\,0\,\ldots\,0 \\ 0\,1\,0\,0\,1\,1\,0\,\ldots\,0 \\ 0\,1\,0\,1\,1\,0\,1\,\ldots\,0 \\ 0\,0\,1\,0\,0\,1\,1\,\ldots\,1 \\ 0\,1\,1\,1\,0\,1\,1\,\ldots\,0 \\ \\ 1\,1\,0\,1\,1\,0\,0\,\ldots\,1 \\ 0\,1\,0\,1\,1\,1\,1\,\ldots\,0 \\ 0\,1\,0\,0\,1\,0\,0\,\ldots\,1 \\ 0\,0\,1\,1\,0\,1\,0\,\ldots\,0 \\ 0\,1\,1\,1\,0\,0\,0\,\ldots\,0 \\ \\ 1\,1\,0\,0\,1\,1\,1\,\ldots\,0 \\ 0\,0\,0\,0\,1\,1\,0\,\ldots\,1 \\ 0\,1\,1\,0\,1\,0\,1\,\ldots\,0 \\ 0\,0\,1\,0\,0\,0\,1\,\ldots\,1 \\ 0\,1\,1\,1\,1\,1\,0\,\ldots\,1 \end{bmatrix} \tag{6.38}$$

Evaluating the minimum Hamming distance of this code confirms that it is 11, an increase of 2 over the BCH bound for the minimum Hamming distance.

6.7 Extended BCH Codes as Goppa Codes

In a short paper in 1971 [4], Goppa showed how a binary Goppa code could be constructed with parameters $(2^m + (m-1)t, 2^m - t, 2t+1)$. Each parity check symbol, m bits long has a Forney concatenation [2], i.e. an overall parity bit on each symbol. In a completely novel approach by Goppa, each parity symbol, apart from 1 bit in each symbol, is external to the code as if these are additional parity symbols. These symbols are also independent of each other extending the length of the code and, importantly, increasing the d_{min} of the code. Sugiyama et al. [9, 10] described a construction technique mixing the standard Goppa code construction with the Goppa external parity check construction. We give below a simpler construction method applicable to BCH codes and to more general Goppa codes.

Consider a binary BCH code constructed as a Goppa code with Goppa polynomial $g(z) = z^{2t}$ but extended by including an additional root α_0, an element of $GF(2^m)$. The Goppa polynomial is now $g(z) = (z^{2t+1} + \alpha_0 z^{2t})$. The parity check equations are given by

$$\sum_{i=0}^{2^m-2} \frac{c_i}{z-\alpha^i} = 0 \quad \text{modulo } g(z) \quad \alpha^i \neq \alpha_0 \tag{6.39}$$

Substituting for r_m and $q(z)$, as in Sect. 6.5

$$\frac{1}{z-\alpha^i} \quad \text{modulo } g(z) = \frac{g(z)+g(\alpha^i)}{g(\alpha^i)(z-\alpha^i)} \tag{6.40}$$

For the extended binary BCH code with Goppa polynomial $g(z) = (z^{2t+1} + \alpha z^{2t})$ the parity check equations are given by

$$\begin{aligned} \textstyle\sum_{i=1}^{2^m-2} \frac{c_i}{z-\alpha^i} &= \textstyle\sum_{i=1}^{2^m-2} c_i \left(\frac{z^{2t}}{\alpha^{i2t}(\alpha^i+\alpha_0)} + \frac{z^{2t-1}}{\alpha^{i2t}} + \frac{z^{2t-2}}{\alpha^{i(2t-1)}} + \frac{z^{2t-3}}{\alpha^{i(2t-2)}} + \cdots + \frac{1}{\alpha^i} \right) \\ &= 0 \end{aligned} \tag{6.41}$$

Equating each coefficient of powers of z to zero and using only the independent parity check equations (as it is a binary code) produces $t+1$ independent parity check equations with parity check matrix

$$\mathbf{H}_{(\mathbf{2^m-2,\ 2^m-2-mt-m})} = \begin{bmatrix} \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \cdots & \alpha^{-(2^m-2)} \\ \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \cdots & \alpha^{-3(2^m-2)} \\ \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \cdots & \alpha^{-5(2^m-2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha^{-2t+1} & \alpha^{-2(2t-1)} & \alpha^{-3(2t-1)} & \cdots & \alpha^{-(2t-1)(2^m-2)} \\ \frac{\alpha^{-2t}}{\alpha+\alpha_0} & \frac{\alpha^{-4t}}{\alpha^2+\alpha_0} & \frac{\alpha^{-6t}}{\alpha^3+\alpha_0} & \cdots & \frac{\alpha^{-2t(2^m-2)}}{\alpha^{2^m-2}+\alpha_0} \end{bmatrix} \tag{6.42}$$

The last row may be simplified by noting that

$$\frac{1+\alpha_0^{-2t}\alpha^{2t}}{(\alpha_0+\alpha)\alpha^{2t}} = \frac{\alpha_0^{-1}}{\alpha^{2t-1}} + \frac{\alpha_0^{-2}}{\alpha^{2t-2}} + \frac{\alpha_0^{-3}}{\alpha^{2t-3}} + \cdots + \frac{\alpha_0^{-2t+1}}{\alpha} \tag{6.43}$$

Rearranging produces

$$\frac{1}{(\alpha_0+\alpha)\alpha^{2t}} = \frac{\alpha_0^{-2t}\alpha^{2t}}{(\alpha_0+\alpha)\alpha^{2t}} + \frac{\alpha_0^{-1}}{\alpha^{2t-1}} + \frac{\alpha_0^{-2}}{\alpha^{2t-2}} + \frac{\alpha_0^{-3}}{\alpha^{2t-3}} + \cdots + \frac{\alpha_0^{-2t+1}}{\alpha} \tag{6.44}$$

and

$$\frac{\alpha^{-2t}}{(\alpha_0+\alpha)} = \frac{\alpha_0^{-2t}}{(\alpha_0+\alpha)} + \frac{\alpha_0^{-1}}{\alpha^{2t-1}} + \frac{\alpha_0^{-2}}{\alpha^{2t-2}} + \frac{\alpha_0^{-3}}{\alpha^{2t-3}} + \cdots + \frac{\alpha_0^{-2t+1}}{\alpha} \tag{6.45}$$

The point here is because of the above equality, the last parity check equation in (6.42) may be replaced with a simpler equation to produce the same Cauchy style parity check given by Goppa in his 1971 paper [4]. The parity check matrix becomes

$$\mathbf{H}_{(\mathbf{2^m-2,\ 2^m-2-mt-m})} = \begin{bmatrix} \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \cdots & \alpha^{-(2^m-2)} \\ \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \cdots & \alpha^{-3(2^m-2)} \\ \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \cdots & \alpha^{-5(2^m-2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha^{-2t+1} & \alpha^{-2(2t-1)} & \alpha^{-3(2t-1)} & \cdots & \alpha^{-(2t-1)(2^m-2)} \\ \frac{1}{\alpha+\alpha_0} & \frac{1}{\alpha^2+\alpha_0} & \frac{1}{\alpha^3+\alpha_0} & \cdots & \frac{1}{\alpha^{2^m-2}+\alpha_0} \end{bmatrix} \tag{6.46}$$

The justification for this is that from (6.45), the last row of (6.42) is equal to a scalar weighted linear combination of the rows of the parity check matrix(6.46), so that these rows will produce the same code as the parity check matrix (6.42). By induction, other roots of $GF(2^m)$ may be used to produce similar parity check equations to increase the distance of the code producing parity check matrices of the form:

$$\mathbf{H} = \begin{bmatrix} \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \cdots & \alpha^{-(2^m-2)} \\ \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \cdots & \alpha^{-3(2^m-2)} \\ \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \cdots & \alpha^{-5(2^m-2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \\ \alpha^{-2t+1} & \alpha^{-2(2t-1)} & \alpha^{-3(2t-1)} & \alpha^{-4(2t-1)} & \cdots & \alpha^{-(2t-1)(2^m-2)} \\ \frac{1}{\alpha+\alpha_0} & \frac{1}{\alpha^2+\alpha_0} & \frac{1}{\alpha^3+\alpha_0} & \frac{1}{\alpha^4+\alpha_0} & \cdots & \frac{1}{\alpha^{2^m-2}+\alpha_0} \\ \frac{1}{\alpha+\alpha_1} & \frac{1}{\alpha^2+\alpha_1} & \frac{1}{\alpha^3+\alpha_1} & \frac{1}{\alpha^4+\alpha_1} & \cdots & \frac{1}{\alpha^{2^m-2}+\alpha_1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \\ \frac{1}{\alpha+\alpha_{s_0-1}} & \frac{1}{\alpha^2+\alpha_{s_0-1}} & \frac{1}{\alpha^3+\alpha_{s_0-1}} & \frac{1}{\alpha^4+\alpha_{s_0-1}} & \cdots & \frac{1}{\alpha^{2^m-2}+\alpha_{s_0-1}} \end{bmatrix} \tag{6.47}$$

The parity symbols given by the last s_0 rows of this matrix are in the Cauchy matrix style [7] and will necessarily reduce the length of the code for each root of the

Goppa polynomial which is an element of $GF(2^m)$. However, Goppa was the first to show [4] that the parity symbols may be optionally placed external to the code, without decreasing the length of the code. For binary codes the length of the code increases as will be shown below. Accordingly, with external parity symbols, the parity check matrix becomes

$$\mathbf{H} = \begin{bmatrix} \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \dots & \alpha^{-(2^m-2)} & 0 & 0 & 0 & 0 \\ \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \dots & \alpha^{-3(2^m-2)} & 0 & 0 & 0 & 0 \\ \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \dots & \alpha^{-5(2^m-2)} & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha^{-2t+1} & \alpha^{-2(2t-1)} & \alpha^{-3(2t-1)} & \alpha^{-4(2t-1)} & \dots & \alpha^{-(2t-1)(2^m-2)} & 0 & 0 & 0 & 0 \\ \frac{1}{\alpha+\alpha_0} & \frac{1}{\alpha^2+\alpha_0} & \frac{1}{\alpha^3+\alpha_0} & \frac{1}{\alpha^4+\alpha_0} & \dots & \frac{1}{\alpha^{2^m-2}+\alpha_0} & 1 & 0 & 0 & 0 \\ \frac{1}{\alpha+\alpha_1} & \frac{1}{\alpha^2+\alpha_1} & \frac{1}{\alpha^3+\alpha_1} & \frac{1}{\alpha^4+\alpha_1} & \dots & \frac{1}{\alpha^{2^m-2}+\alpha_1} & 0 & 1 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{1}{\alpha+\alpha_{s_0-1}} & \frac{1}{\alpha^2+\alpha_{s_0-1}} & \frac{1}{\alpha^3+\alpha_{s_0-1}} & \frac{1}{\alpha^4+\alpha_{s_0-1}} & \dots & \frac{1}{\alpha^{2^m-2}+\alpha_{s_0-1}} & 0 & 0 & 0 & 1 \end{bmatrix} \tag{6.48}$$

As an example of the procedure, consider the (31, 11, 11) binary BCH code described in Sect. 6.6. We shall add one external parity symbol to this code according to the parity check matrix in (6.48) and eventually produce a (36, 10, 13) binary BCH code. Arbitrarily, we shall choose $\alpha_0 = 1$. This means that the first column of the parity check matrix for the (31, 11, 11) code given in (6.38) is deleted and there is one additional parity check row. The parity check matrix for this (35, 10, 12) extended BCH code is given below. Note we will add later an additional parity bit in a Forney concatenation of the external parity symbol to produce the (36, 10, 13) code as a last step.

$$\mathbf{H}_{(35,\,10,\,12)} = \begin{bmatrix} \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \dots & \alpha^{-30} & 0 \\ \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \alpha^{-15} & \alpha^{-18} & \dots & \alpha^{-28} & 0 \\ \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \alpha^{-25} & \alpha^{-30} & \dots & \alpha^{-26} & 0 \\ \alpha^{-9} & \alpha^{-18} & \alpha^{-27} & \alpha^{-5} & \alpha^{-14} & \alpha^{-23} & \dots & \alpha^{-22} & 0 \\ \frac{1}{\alpha+1} & \frac{1}{\alpha^2+1} & \frac{1}{\alpha^3+1} & \frac{1}{\alpha^4+1} & \frac{1}{\alpha^5+1} & \frac{1}{\alpha^6+1} & \dots & \frac{1}{\alpha^{29}+1} & 1 \end{bmatrix} \tag{6.49}$$

Evaluating the last row by carrying out the additions, and inversions, referring to the table of $GF(32)$ symbols in Table 6.2 produces the resulting parity check matrix

$$\mathbf{H}_{(35,\,10,\,12)} = \begin{bmatrix} \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \dots & \alpha^{-30} & 0 \\ \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \alpha^{-15} & \alpha^{-18} & \dots & \alpha^{-28} & 0 \\ \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \alpha^{-25} & \alpha^{-30} & \dots & \alpha^{-26} & 0 \\ \alpha^{-9} & \alpha^{-18} & \alpha^{-27} & \alpha^{-5} & \alpha^{-14} & \alpha^{-23} & \dots & \alpha^{-22} & 0 \\ \alpha^{-13} & \alpha^{-26} & \alpha^{-2} & \alpha^{-21} & \alpha^{-29} & \alpha^{-4} & \dots & \alpha^{-14} & 1 \end{bmatrix} \tag{6.50}$$

The next step is to determine the binary parity check matrix for the code by replacing each $GF(32)$ symbol by its corresponding 5-bit representation using Table 6.2, but as

a 5-bit column vector. Also we will add an additional parity check row to implement the Forney concatenation of the external parity symbol. The resulting binary parity check matrix in (6.51) is obtained. Evaluating the minimum Hamming distance of this code using one of the methods described in Chap. 5 verifies that it is indeed 13.

Adding the external parity symbol has increased the minimum Hamming distance by 2, but at the cost of one data symbol. Instead of choosing $\alpha_0 = 1$, a good idea is to choose $\alpha_0 = 0$, since 0 is a multiple root of the Goppa polynomial $g(z) = z^{10}$ which caused the BCH code to be shortened from length 2^m to $2^m - 1$ in the first place. (The length of a Goppa code with Goppa polynomial $g(z)$ having no roots in $GF(2^m)$ is 2^m). The resulting parity check matrix is given in (6.52).

$$\mathbf{H}_{(\mathbf{36},\,\mathbf{10},\,\mathbf{13})} = \left[\begin{array}{c}
0\,1\,0\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
1\,0\,1\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,1\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,1\,0\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
1\,0\,1\,0\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
\\
0\,1\,1\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
1\,0\,0\,1\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
1\,0\,1\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,1\,0\,0\,1\,1\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0 \\
1\,1\,1\,0\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
\\
1\,0\,1\,1\,0\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0 \\
1\,0\,1\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
1\,0\,0\,1\,0\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0 \\
0\,1\,1\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
1\,1\,1\,0\,0\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
\\
1\,0\,0\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0 \\
1\,1\,0\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,1\,0\,0\,0\,1\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0 \\
1\,1\,1\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0 \\
\\
1\,1\,1\,1\,0\,1\,\ldots\,1\,1\,0\,0\,0\,0\,0\,0 \\
1\,0\,0\,0\,0\,1\,\ldots\,1\,0\,1\,0\,0\,0\,0\,0 \\
0\,1\,0\,0\,1\,0\,\ldots\,0\,0\,0\,1\,0\,0\,0\,0 \\
0\,0\,1\,0\,0\,1\,\ldots\,0\,0\,0\,0\,1\,0\,0\,0 \\
0\,0\,0\,1\,0\,0\,\ldots\,1\,0\,0\,0\,0\,1\,0\,0 \\
0\,0\,0\,0\,0\,0\,\ldots\,0\,1\,1\,1\,1\,1\,1\,1
\end{array}\right] \tag{6.51}$$

$$\mathbf{H}_{(\mathbf{36},\,\mathbf{11})} = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \dots & \alpha^{-30} & 0 \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \alpha^{-15} & \alpha^{-18} & \dots & \alpha^{-28} & 0 \\ 1 & \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \alpha^{-25} & \alpha^{-30} & \dots & \alpha^{-26} & 0 \\ 1 & \alpha^{-9} & \alpha^{-18} & \alpha^{-27} & \alpha^{-5} & \alpha^{-14} & \alpha^{-23} & \dots & \alpha^{-22} & 0 \\ 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \dots & \alpha^{-30} & 1 \end{bmatrix} \tag{6.52}$$

The problem with this is that the minimum Hamming distance is still 11 because the last row of the parity check matrix is the same as the first row, apart from the external parity symbol because 0 is a root of the Goppa polynomial. The solution is to increase the degree of the Goppa polynomial but still retain the external parity symbol. Referring to the cyclotomic cosets of 31, see (6.35), we should use $g(z) = z^{12}$ to produce the parity check matrix

$$\mathbf{H}_{(\mathbf{36},\,\mathbf{11})} = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \dots & \alpha^{-30} & 0 \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \alpha^{-15} & \alpha^{-18} & \dots & \alpha^{-28} & 0 \\ 1 & \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \alpha^{-25} & \alpha^{-30} & \dots & \alpha^{-26} & 0 \\ 1 & \alpha^{-9} & \alpha^{-18} & \alpha^{-27} & \alpha^{-5} & \alpha^{-14} & \alpha^{-23} & \dots & \alpha^{-22} & 0 \\ 1 & \alpha^{-11} & \alpha^{-22} & \alpha^{-2} & \alpha^{-13} & \alpha^{-24} & \alpha^{-4} & \dots & \alpha^{-20} & 1 \end{bmatrix} \tag{6.53}$$

As before, the next step is to determine the binary parity check matrix for the code from this matrix by replacing each $GF(32)$ symbol by its corresponding 5 bit representation using Table 6.2 as a 5 bit column vector. Also we will add an additional parity check row to implement the Forney concatenation of the external parity symbol. The resulting binary parity check matrix is obtained

$$\begin{bmatrix} 1\,0\,1\,0\,1\,1\,1 \dots 0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,1\,1\,0 \dots 1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,1\,0 \dots 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,1\,0\,1 \dots 0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,0\,1\,1 \dots 0\,0\,0\,0\,0\,0\,0 \\ \\ 1\,0\,1\,1\,0\,1\,0 \dots 0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,1\,1\,0 \dots 0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,1\,0\,1 \dots 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,1\,1 \dots 1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,1 \dots 0\,0\,0\,0\,0\,0\,0 \\ \\ 1\,1\,0\,1\,1\,0\,0 \dots 1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,1\,1\,1 \dots 0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,1\,0\,0 \dots 1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,0\,1\,0 \dots 0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,0\,0 \dots 0\,0\,0\,0\,0\,0\,0 \end{bmatrix}$$

$$\mathbf{H}_{(37,\,11,\,13)} = \begin{bmatrix} 1\,1\,0\,0\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,1\,\ldots\,1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0 \\ \\ 1\,0\,0\,1\,1\,0\,1\,\ldots\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,1\,0\,1\,\ldots\,1\,0\,1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,1\,0\,\ldots\,1\,0\,0\,1\,0\,0\,0 \\ 0\,1\,1\,1\,0\,0\,1\,\ldots\,0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,1\,0\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,\ldots\,0\,1\,1\,1\,1\,1\,1 \end{bmatrix} \tag{6.54}$$

Weight spectrum analysis of this code confirms that the d_{min} is indeed 13. One or more Cauchy style parity check equations may be added to this code to increase the d_{min} of the code. For example, with one more parity check equation again with the choice of $\alpha_0 = 1$, the parity check matrix for the (42,10) code is

$$\mathbf{H}_{(42,\,10)} = \begin{bmatrix} \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \ldots & \alpha^{-30} & 0 & 0 \\ \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \alpha^{-15} & \alpha^{-18} & \ldots & \alpha^{-28} & 0 & 0 \\ \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \alpha^{-25} & \alpha^{-30} & \ldots & \alpha^{-26} & 0 & 0 \\ \alpha^{-9} & \alpha^{-18} & \alpha^{-27} & \alpha^{-5} & \alpha^{-14} & \alpha^{-23} & \ldots & \alpha^{-22} & 0 & 0 \\ \alpha^{-11} & \alpha^{-22} & \alpha^{-2} & \alpha^{-13} & \alpha^{-24} & \alpha^{-4} & \ldots & \alpha^{-20} & 1 & 0 \\ \alpha^{-18} & \alpha^{-5} & \alpha^{-29} & \alpha^{-10} & \alpha^{-2} & \alpha^{-27} & \ldots & \alpha^{-17} & 0 & 1 \end{bmatrix} \tag{6.55}$$

Replacing each $GF(32)$ symbol by its corresponding 5 bit representation using Table 6.2 as a 5-bit column vector and adding an additional parity check row to each external parity symbol produces the binary parity check matrix for the (42, 10, 15) code.

$$\begin{bmatrix} 0\,1\,0\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,1\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,1\,0\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ \\ 0\,1\,1\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,0\,1\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,1\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,1\,1\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,1\,0\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ \\ 1\,0\,1\,1\,0\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,1\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,0\,1\,0\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,1\,0\,0\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \end{bmatrix}$$

$$\mathbf{H}_{(42,\,10,\,15)} = \left[\begin{array}{c}
1\,0\,0\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
1\,1\,0\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,0\,0\,1\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
1\,1\,1\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
\\
0\,0\,1\,1\,0\,1\,\ldots\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,1\,0\,1\,\ldots\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
1\,0\,0\,0\,1\,0\,\ldots\,1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
1\,1\,1\,0\,0\,1\,\ldots\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,\ldots\,0\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\\
\\
0\,1\,0\,0\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,0\,0\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\\
1\,1\,1\,0\,0\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\\
1\,0\,0\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\\
1\,1\,0\,1\,0\,1\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\\
0\,0\,0\,0\,0\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1
\end{array}\right] \tag{6.56}$$

Weight spectrum analysis of this code confirms that the d_{min} is indeed 15. In this construction the information bit coordinate corresponding to $\alpha_0 = 1$ is deleted, reducing the dimension of the code by 1. This is conventional practice when the Goppa polynomial $g(z)$ contains a root that is in $GF(2^m)$. However, on reflection, this is not essential. Certainly, in the parity check symbol equations of the constructed code, there will be one parity check equation where the coordinate is missing, but additional parity check equations may be used to compensate for the missing coordinate(s).

Consider the (42, 10) code above, given by parity check matrix (6.55) without the deletion of the first coordinate. The parity check matrix for the (42, 11) code becomes

$$\mathbf{H}_{(42,\,11)} = \begin{bmatrix}
1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \ldots & \alpha^{-30} & 0 & 0\\
1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \alpha^{-15} & \alpha^{-18} & \ldots & \alpha^{-28} & 0 & 0\\
1 & \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \alpha^{-25} & \alpha^{-30} & \ldots & \alpha^{-26} & 0 & 0\\
1 & \alpha^{-9} & \alpha^{-18} & \alpha^{-27} & \alpha^{-5} & \alpha^{-14} & \alpha^{-23} & \ldots & \alpha^{-22} & 0 & 0\\
1 & \alpha^{-11} & \alpha^{-22} & \alpha^{-2} & \alpha^{-13} & \alpha^{-24} & \alpha^{-4} & \ldots & \alpha^{-20} & 1 & 0\\
0 & \alpha^{-18} & \alpha^{-5} & \alpha^{-29} & \alpha^{-10} & \alpha^{-2} & \alpha^{-27} & \ldots & \alpha^{-17} & 0 & 1
\end{bmatrix} \tag{6.57}$$

It will be noticed that the first coordinate is not in the last parity check equation. Constructing the binary code as before by replacing each $GF(32)$ symbol by its corresponding 5-bit representation using Table 6.2 as a 5-bit column vector and adding an additional parity check row to each external parity symbol produces a (42, 11, 13) binary code. There is no improvement in the d_{min} of the (42, 11, 13) binary code compared to the (37, 11, 13) binary code despite the 5 additional parity bits. However, weight spectrum analysis of the (42, 11, 13) binary code shows that there

is only 1 codeword of weight 13 and only 3 codewords of weight 14. All of these low weight codewords contain the first coordinate which is not surprising. Two more parity check equations containing the first coordinate need to be added to the parity check matrix to compensate for the coordinate not being in the last equation of the parity check symbol matrix (6.57).

It turns out that the coordinate in question can always be inserted into the overall parity check equation to each external parity symbol without any loss, so that only one additional parity check equation is required for each root of $g(z)$ that is in $GF(2^m)$.

This produces the following binary parity check matrix for the (43, 11, 15) code.

$$\mathbf{H}_{(\mathbf{43,\,11,\,15})} = \left[\begin{array}{l}
1\,0\,1\,0\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,1\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,1\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,1\,0\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,1\,0\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
\\
1\,0\,1\,1\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,0\,1\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,1\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,1\,0\,0\,1\,1\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,1\,1\,0\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
\\
1\,1\,0\,1\,1\,0\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,1\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,0\,1\,0\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,1\,1\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,1\,1\,0\,0\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
\\
1\,1\,0\,0\,1\,1\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,1\,0\,1\,0\,1\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,1\,0\,0\,0\,1\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,1\,1\,1\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
\\
1\,0\,0\,1\,1\,0\,1\,\ldots\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,1\,0\,1\,0\,1\,\ldots\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,0\,0\,1\,0\,\ldots\,1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,1\,1\,0\,0\,1\,\ldots\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,1\,0\,0\,1\,0\,\ldots\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,\ldots\,0\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
\\
0\,0\,1\,0\,0\,1\,0\,\ldots\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,1\,0\,0\,0\,0\,\ldots\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0
\end{array}\right] \tag{6.58}$$

$$\begin{bmatrix} 0\,1\,1\,1\,0\,0\,0\ldots 1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,1\,1\,0\ldots 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,1\,1\,0\,1\,0\,1\ldots 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0 \\ 1\,0\,0\,0\,0\,0\,0\ldots 0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,0 \\ 1\,0\,0\,0\,0\,0\,0\ldots 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix}$$

It will be noticed that the last but one row is the Forney concatenation on the last $GF(32)$ symbol of parity check matrix (6.57), the overall parity check on parity bits 36–41. Bit 0 has been added to this equation. Also, the last row of the binary parity check matrix is simply a repeat of bit 0. In this way, bit 0 has been fully compensated for not being in the last row of parity check symbol matrix (6.57).

BCH codes extended in length in this way can be very competitive compared to the best known codes [5]. The most efficient extensions of BCH codes are for $g(z)$ having only multiple roots of $z = 0$ because no additional deletions of information bits are necessary nor are compensating parity check equations necessary. However, n does need to be a Mersenne prime, and the maximum extension is 2 symbols with $2m + 2$ additional, overall parity bits, increasing the d_{min} by 4. Where n is not a Mersenne prime the maximum extension is 1 symbol with $m + 1$ additional, overall parity bits, increasing the d_{min} by 2.

However regardless of n being a Mersenne prime or not, multiple symbol extensions may be carried out if $g(z)$ has additional roots from $GF(2^m)$, increasing the d_{min} by 2 for each additional root. The additional root can also be $z = 0$.

As further examples, a (37, 11, 13) code and a (43, 11, 15) code can be constructed in this way by extending the (31, 11, 11) BCH code. Also a (135, 92, 13) code and a (143, 92, 15) code can be constructed by extending the (127, 92, 11) BCH code. A (135, 71, 21) code and a (143, 71, 23) code can be constructed by extending the (127, 71, 19) BCH code.

For more than 2 extended symbols for Mersenne primes, or more than 1 extended symbol for non-Mersenne primes, it is necessary to use mixed roots of $g(z)$ from $GF(2^m)$ and have either deletions of information bits or compensating parity check equations or both. As examples of these code constructions there are:

- An example of a non Mersenne prime, the (76, 50, 9) code constructed from the BCH (63, 51, 5) code with additional roots of $g(z)$ at $z = 0$ and α^0 deleting the first information bit.
- The (153, 71, 25) code extended from the (127, 71, 19) code with additional roots of $g(z)$ at $z = 0$, α^0 and α^1 with 2 additional, compensating parity check bits.
- The (151, 70, 25) code extended from the (127, 71, 19) code with additional roots of $g(z)$ at $z = 0$, α^0 and α^1 with the first coordinate deleted reducing the dimension by 1 and one additional, compensating parity check bit.
- The (160, 70, 27) code extended from the (127, 71, 19) code with additional roots of $g(z)$ at $z = 0$, α^0, α^1 and α^2 with the first coordinate deleted reducing the dimension by 1 and with 2 additional, compensating parity check bits.
- The (158, 69, 27) code extended from the (127, 71, 19) code with additional roots of $g(z)$ at $z = 0$, α^0, α^1, α^2 and α^3 with the first 2 coordinates deleted reducing

the dimension by 2 and one additional, compensating parity check bit. All of these codes are best known codes [5].

6.8 Binary Codes from MDS Codes

The Goppa codes and BCH codes, which are a subset of Goppa codes, when constructed as codes with symbols from $GF(q)$ are all MDS codes and are examples of generalised Reed–Solomon codes [7]. MDS codes are exceptional codes and there are not many construction methods for these codes. For (n, k) MDS codes the repetition code, having $k = 1$, can have any length of n independently of the field size q. For values $k = 3$ and $k = q-1$ and with q even the maximum value of n is $n = q+2$ [7]. For all other cases, the maximum value of n is $n = q + 1$ with a construction known as the doubly extended Reed–Solomon codes. The parity check matrix for a $(q + 1, k)$ doubly extended Reed–Solomon code is

$$\mathbf{H_{RS+}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots & 1 & 1 & 0 \\ 1 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \dots & \alpha_{q-2} & 0 & 0 \\ 1 & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 & \alpha_5^2 & \alpha_6^2 & \dots & \alpha_{q-2}^2 & 0 & 0 \\ 1 & \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \alpha_4^3 & \alpha_5^3 & \alpha_6^3 & \dots & \alpha_{q-2}^3 & 0 & 0 \\ 1 & \alpha_1^4 & \alpha_2^4 & \alpha_3^4 & \alpha_4^4 & \alpha_5^4 & \alpha_6^4 & \dots & \alpha_{q-2}^4 & 0 & 0 \\ & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ 1 & \alpha_1^{q-k} & \alpha_2^{q-k} & \alpha_3^{q-k} & \alpha_4^{q-k} & \alpha_5^{q-k} & \alpha_6^{q-k} & \dots & \alpha_{q-2}^{q-k} & 0 & 1 \end{bmatrix} \tag{6.59}$$

where the q elements of $GF(q)$ are $\{0, 1, \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{q-1}\}$.

As the codes are MDS, the minimum Hamming distance is $q + 2 - k$, forming a family of $(q + 1, k, q + 2 - k)$ codes meeting the Singleton bound [8].

The MDS codes may be used as binary codes simply by restricting the data symbols to values of {0 and 1} to produce a subfield subcode. Alternatively for $GF(2^m)$ each symbol may be replaced with a $m \times m$ binary matrix to produce the family of $((2^m + 1)m, mk, 2^m + 2 - k)$ of binary codes. As an example, with $m = 4$ and $k = 12$, the result is a (68, 48, 5) binary code. This is not a very competitive code because the equivalent best known code [5], the (68, 48, 8) code, has much better minimum Hamming distance.

However, using the Forney concatenation [2] on each symbol almost doubles the minimum Hamming distance with little increase in redundancy and produces the family of $((2^m + 1)(m + 1), mk, 2(2^m + 1 - k) + 1)$ of binary codes. With the same example values for m and k the (85, 48, 11) binary code is produced. Kasahara [6] noticed that it is sometimes possible with this code construction to add an additional information bit by adding the all 1's codeword to the generator matrix of the code. Equivalently expressed, all of the codewords may be complemented without degrading the minimum Hamming distance. It is possible to go further depending on the length of the code and the minimum Hamming distance. Since the binary

parity of each symbol is always even, then if $m+1$ is an odd number, then adding the all 1's pattern to each symbol will produce weight of at least 1 per symbol. For the (85, 48, 11) constructed binary code $m+1=5$, an odd number and the number of symbols is 17. Hence, adding the all 1's pattern (i.e. 85 1's) to each codeword will produce a minimum weight of at least 17. Accordingly, a (85, 49, 11) code is produced. Adding an overall parity bit to each codeword increases the minimum Hamming distance to 12 producing a (86, 49, 12) code and shortening the code by deleting one information bit produces a (85, 48, 12) code. This is a good code because the corresponding best known code is also a (85, 48, 12) code. However, the construction method is different because the best known code is derived from the (89, 56, 11) cyclic code.

Looking at constructing binary codes from MDS codes by simply restricting the data symbols to values of {0 and 1}, consider the example of the extended Reed–Solomon code of length 16 using $GF(2^4)$ with 2 parity symbols. The code is the MDS (16, 14, 3) code. The parity check matrix is

$$\mathbf{H}_{(16,14)} = \begin{bmatrix} 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} & 0 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 \end{bmatrix} \tag{6.60}$$

With binary codeword coordinates, denoted as c_i the first parity check equation from the first row of the parity check matrix is

$$\sum_{i=0}^{14} c_i \alpha^i = 0 \tag{6.61}$$

Squaring both sides of this equation produces

$$\sum_{i=0}^{14} c_i^2 \alpha^{2i} = 0 \tag{6.62}$$

As the codeword coordinates are binary, $c_i^2 = c_i$ and so any codeword satisfying the equations of (6.58) satisfies all of the following equations by induction from (6.60)

$$\mathbf{H}_{(16,14)} = \begin{bmatrix} 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} & 0 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} & \alpha^1 & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} & \alpha^{13} & 0 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^1 & \alpha^5 & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^4 & \alpha^{10} & \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^{11} & 0 \\ 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 & 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 & 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \end{bmatrix} \tag{6.63}$$

There are 4 consecutive zeros of the parent Reed–Solomon code from the first 4 rows of the parity check matrix indicating that the minimum Hamming distance may be 5

Table 6.3 $GF(16)$ extension field defined by $1 + \alpha^1 + \alpha^4 = 0$

$\alpha^0 = 1$
$\alpha^1 = \alpha$
$\alpha^2 = \alpha^2$
$\alpha^3 = \alpha^3$
$\alpha^4 = 1 + \alpha$
$\alpha^5 = \alpha + \alpha^2$
$\alpha^6 = \alpha^2 + \alpha^3$
$\alpha^7 = 1 + \alpha + \alpha^3$
$\alpha^8 = 1 + \alpha^2$
$\alpha^9 = \alpha + \alpha^3$
$\alpha^{10} = 1 + \alpha + \alpha^2$
$\alpha^{11} = \alpha + \alpha^2 + \alpha^3$
$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$
$\alpha^{13} = 1 + \alpha^2 + \alpha^3$
$\alpha^{14} = 1 + \alpha^3$

for the binary code. However, comparing the last column of this matrix with (6.57) indicates that this column is not correct.

Constructing the binary check matrix from the parity check equations, (6.58) using Table 6.3 substituting the respective 4 bit vector for each column vector of each nonzero $GF(16)$ symbol, (0 in $GF(16)$ is 0000) produces the following binary check matrix

$$\mathbf{H}_{(16,\,8)} = \begin{bmatrix} 1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0 \\ 0\,1\,0\,0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0 \\ \\ 1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0 \\ 0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0 \\ 0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0 \end{bmatrix} \tag{6.64}$$

Weight spectrum analysis indicates the minimum Hamming distance of this code is 4 due to a single codeword of weight 4,{0, 5, 10, 15}. Deleting the last column of the parity check matrix produces a (15, 8, 5) code. Another approach is needed to go from the MDS code to a binary code without incurring a loss in the minimum Hamming distance.

It is necessary to use the generalised Reed–Solomon MDS code. Here, each column of the parity check matrix is multiplied by a nonzero element of the $GF(2^m)$ field defined as $\{\mu_0, \mu_1, \mu_2, \mu_3, \ldots, \mu_{2^m}\}$. It is not necessary for these to be distinct, just to have a multiplicative inverse. The parity check matrix for the $(q + 1, k)$ generalised Reed–Solomon MDS code is

$$\mathbf{H_{GRS+}} = \begin{bmatrix} \nu_0 & \nu_1 & \nu_2 & \nu_3 & \nu_4 & \nu_5 & \dots & \nu_{q-2} & \nu_{q-1} & 0 \\ \nu_0 & \nu_1\alpha_1 & \nu_2\alpha_2 & \nu_3\alpha_3 & \nu_4\alpha_4 & \nu_5\alpha_5 & \dots & \nu_{q-2}\alpha_{q-2} & 0 & 0 \\ \nu_0 & \nu_1\alpha_1^2 & \nu_2\alpha_2^2 & \nu_3\alpha_3^2 & \nu_4\alpha_4^2 & \nu_5\alpha_5^2 & \dots & \nu_{q-2}\alpha_{q-2}^2 & 0 & 0 \\ \nu_0 & \nu_1\alpha_1^3 & \nu_2\alpha_2^3 & \nu_3\alpha_3^3 & \nu_4\alpha_4^3 & \nu_5\alpha_5^3 & \dots & \nu_{q-2}\alpha_{q-2}^3 & 0 & 0 \\ \nu_0 & \nu_1\alpha_1^4 & \nu_2\alpha_2^4 & \nu_3\alpha_3^4 & \nu_4\alpha_4^4 & \nu_5\alpha_5^4 & \dots & \nu_{q-2}\alpha_{q-2}^4 & 0 & 0 \\ & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \nu_0 & \nu_1\alpha_1^{q-k} & \nu_2\alpha_2^{q-k} & \nu_3\alpha_3^{q-k} & \nu_4\alpha_4^{q-k} & \nu_5\alpha_5^{q-k} & \dots & \nu_{q-2}\alpha_{q-2}^{q-k} & 0 & \nu_q \end{bmatrix}$$

It is clear that as a nonbinary code with codeword coefficients from $GF(2^m)$, the distance properties will remain unchanged as the generalised Reed–Solomon is still an MDS code. Depending on the coordinate position each nonzero element value has a unique mapping to another nonzero element value. It is as subfield subcodes that the generalised Reed–Solomon codes have an advantage. It should be noted that Goppa codes are examples of a generalised Reed–Solomon code.

Returning to the relatively poor (16, 8, 4) binary code derived from the (16, 14, 3) MDS code, consider the generalised (16, 14, 3) Reed–Solomon code with parity check matrix.

$$\mathbf{H_{(16,14)}} = \begin{bmatrix} \nu_0 & \nu_1 & \nu_2 & \nu_3 & \nu_4 & \nu_5 & \nu_6 & \dots & \nu_{13} & \nu_{14} & \nu_{15} \\ \nu_0 & \nu_1\alpha^1 & \nu_2\alpha^2 & \nu_3\alpha^3 & \nu_4\alpha^4 & \nu_5\alpha^5 & \nu_6\alpha^6 & \dots & \nu_{13}\alpha^{13} & \nu_{14}\alpha^{14} & 0 \end{bmatrix} \tag{6.65}$$

Setting the vector ν to

$$\{\alpha^{12}, \alpha^4, \alpha^3, \alpha^9, \alpha^4, \alpha^1, \alpha^8, \alpha^6, \alpha^3, \alpha^6, \alpha^1, \alpha^2, \alpha^2, \alpha^8, \alpha^9, \alpha^{12}\}$$

Constructing the binary check matrix from these parity check equations using Table 6.3 by substituting the respective 4 bit vector for each column vector of each nonzero $GF(16)$ symbol, (0 in $GF(16)$ is 0000) produces the following binary check matrix

$$\mathbf{H_{(16,8,5)}} = \begin{bmatrix} 1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,1 \\ 1\,1\,0\,1\,1\,1\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1 \\ 1\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0\,1 \\ 1\,0\,1\,1\,0\,0\,0\,1\,1\,1\,0\,0\,0\,0\,1\,1 \\ \\ 1\,0\,0\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0\,1\,0 \\ 1\,1\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0 \\ 1\,1\,1\,1\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0 \\ 1\,0\,0\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,0 \end{bmatrix} \tag{6.66}$$

Weight spectrum analysis indicates that the minimum Hamming distance of this code is 5 and achieves the aim of deriving a binary code from an MDS code without loss of minimum Hamming distance. Moreover, the additional symbol of 1, the last column in (6.59), may be appended to produce the following check matrix for the (17, 9, 5) binary code:

$$\mathbf{H}_{(\mathbf{17,9,5})} = \left[\begin{array}{cccccccccccccccc} 1&1&0&0&1&0&1&0&0&0&0&0&0&1&0&1&0\\ 1&1&0&1&1&1&0&0&0&0&1&0&0&0&1&1&0\\ 1&0&0&0&0&0&1&1&0&1&0&1&1&1&0&1&0\\ 1&0&1&1&0&0&0&1&1&1&0&0&0&0&1&1&0\\ & & & & & & & & & & & & & & & & \\ 1&0&0&1&1&0&1&1&0&1&0&1&1&0&1&0&1\\ 1&1&1&1&0&0&0&0&1&0&1&0&0&0&0&0&0\\ 1&1&1&1&1&1&0&1&1&0&1&1&0&1&1&0&0\\ 1&0&0&1&0&1&1&1&1&0&1&1&1&1&0&0&0 \end{array}\right] \tag{6.67}$$

Not surprisingly, this code has the same parameters as the best known code [5]. The reader will be asking, how is the vector v chosen?

Using trial and error methods, it is extremely difficult, and somewhat tiresome to find a suitable vector v, even for such a short code. Also weight spectrum analysis has to be carried out for each trial code.

The answer is that the vector v is constructed from an irreducible Goppa polynomial of degree 2 with $g(z) = \alpha^3 + z + z^2$. Referring to Table 6.3, the reader may verify using all elements of $GF(16)$, that v is given by $g(\alpha_i)^{-1}$ for $i = 0$ to 15.

Unfortunately the technique is only valid for binary codes with minimum Hamming distance of 5 and also m has to be even. Weight spectrum analysis has confirmed that the (65, 53, 5), (257, 241, 5), (1025, 1005, 5) and (4097, 4073, 5) codes can be constructed in this way from doubly extended, generalised Reed–Solomon, MDS codes.

6.9 Summary

It has been shown that interpolation plays an important, mostly hidden role in algebraic coding theory. The Reed–Solomon codes, BCH codes, and Goppa codes are all codes that may be constructed via interpolation. It has also been demonstrated that all of these codes form part of a large family of generalised MDS codes. The encoding of BCH and Goppa codes has been explored from the viewpoint of classical Lagrange interpolation. It was shown in detail how Goppa codes are designed and constructed starting from first principles. The parity check matrix of a BCH code was derived as a Goppa code proving that BCH codes are a subset of Goppa codes. Following from this result and using properties of the cyclotomic cosets it was explained how the minimum Hamming distance of some BCH codes is able to exceed the BCH bound producing outstanding codes. It was shown how these exceptional BCH codes can be identified and constructed. A little known paper by Goppa was discussed and as a result it was shown how Goppa codes and BCH codes may be extended in length with additional parity check bits resulting in increased minimum Hamming distance of the code. Several examples were given of the technique which results in some outstanding codes. Reed–Solomon codes were explored as a means of constructing binary codes resulting in improvements to the database of best known codes.

References

1. Bell, E.T.: Men of Mathematics: The Lives and Achievements of the Great Mathematicians from Zeno to Poincar. Simon and Schuster, New York (1986)
2. Forney Jr., G.D.: Concatenated Codes. MIT Press, Cambridge (1966)
3. Goppa, V.D.: A new class of linear error-correcting codes. Probl Inform Transm **6**, 24–30 (1970)
4. Goppa, V.D.: Rational representation of codes and (l; g)-codes. Probl Inform Transm **7**, 41–49 (1970)
5. Grassl, M.: Code Tables: Bounds on the parameters of various types of codes (2007). http://www.codetables.de
6. Kasahara, M., Sugiyama, Y., Hirasawa, S., Namekawa, T.: New classes of binary codes constructed on the basis of concatenated codes and product codes. IEEE Trans. Inf. Theory **IT–22**(4), 462–468 (1976)
7. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, New York (1977)
8. Singleton, R.C.: Maximum distance q-ary codes. IEEE Trans. Inf. Theory **IT–10**, 116–118 (1964)
9. Sugiyama, Y., Kasahara, M., Namekawa, T.: Some efficient binary codes constructed using srivastava codes. IEEE Trans. Inf. Theory **IT–21**(5), 581–582 (1975)
10. Sugiyama, Y., Kasahara, M., Namekawa, T.: Further results on goppa codes and their applications to constructing efficient binary codes. IEEE Trans. Inf. Theory **IT–22**(5), 518–526 (1976)