(iii) The total number of codes $\mathscr{A}(\alpha, y)$ in $\mathscr{F}$ is equal to the number of choices for $v$, which is $(q^m - 1)^n$. So if this number exceeds (7), there exists an $\mathscr{A}(\alpha, y)$ with dimension $\geqslant h$ and minimum distance $\geqslant \delta$. This proves (a). Asymptotically, when $n$ is large and $h/n$ fixed, (6) is the same as the Gilbert–Varshamov bound (Theorem 12 of Ch. 1, Theorem 30 of Ch. 17).

Q.E.D.

Of course Theorem 3 doesn't say which alternant codes are the best, only that good ones exist. Since the class of alternant codes is so large, it is useful to have names for some subclasses. In the following sections we shall describe the subclasses known as Goppa, Srivastava and Chien–Choy generalized BCH codes. These are obtained by placing restrictions on $\alpha$ or $y$, or both.

**Problem.** (1) Consider the binary alternant code with $n = 6$, $\alpha_i = \alpha^{i+1}$ for $i = 0, \ldots, 5$ where $\alpha$ is a primitive element of GF($2^3$), all $y_i = 1$, $g_1(x) = 1 + x$ and $g_2(x) = x$. Show that this is a $[6, 2, 4]$ code.

## §3. Goppa codes

This is the most interesting subclass of alternant codes. Just as cyclic codes are specified in terms of a generator polynomial (Theorem 1 of Ch. 7), so Goppa codes are described in terms of a Goppa polynomial $G(z)$. In contrast to cyclic codes, where it is difficult to estimate the minimum distance $d$ from the generator polynomial, Goppa codes have the property that $d \geqslant \deg G(z) + 1$. We first give the definition in terms of Goppa polynomials and then show that these are alternant codes.

The definition of a Goppa code of length $n$ with symbols from GF($q$) calls for two things: a polynomial $G(z)$ called the *Goppa polynomial*, having coefficients from GF($q^m$), for some fixed $m$, and a subset $L = \{\alpha_1, \ldots, \alpha_n\}$ of GF($q^m$) such that $G(\alpha_i) \neq 0$ for all $\alpha_i \in L$. Usually $L$ is taken to be all the elements of GF($q^m$) which are not zeros of $G(z)$.

With any vector $a = (a_1, \ldots, a_n)$ over GF($q$) we associate the rational function

$$R_a(z) = \sum_{i=1}^{n} \frac{a_i}{z - \alpha_i}. \tag{8}$$

**Definition.** The Goppa code $\Gamma(L, G)$ (or $\Gamma$) consists of all vectors $a$ such that

$$R_a(z) \equiv 0 \bmod G(z), \tag{9}$$

or equivalently such that $R_a(z) = 0$ in the polynomial ring GF($q^m$)$[z]/G(z)$.

If $G(z)$ is irreducible then $\Gamma$ is called an *irreducible* Goppa code.

Figure 12.3 shows the basic properties of these codes. Examples will be given after Theorem 6.

$\Gamma(L, G)$ is a linear code over GF($q$), defined by Equation (9).

$$\text{length } n = |L|$$
$$\text{dimension } k \geqslant n - mr,\ r = \deg G(z)$$
$$\text{minimum distance } d \geqslant r + 1.$$

$\Gamma(L, G) =$ alternant code $\mathcal{A}(\alpha, y)$ where $y_i = G(\alpha_i)^{-1}$. $\Gamma(L, G)^{\perp} = T_m(\text{GRS}_r(\alpha, y))$. In the binary case if $G(z)$ has no multiple zeros then $d \geqslant 2r + 1$. There exist long Goppa codes which meet the Gilbert–Varshamov bound. Extended binary double-error-correcting Goppa codes are cyclic (§5).

Fig. 12.3. Properties of the Goppa code $\Gamma(L, G)$.

*The parity check matrix of* $\Gamma$. It is obvious that $\Gamma$ is a linear code. The parity check matrix can be found from (9). For in the ring of polynomials mod $G(z)$, $z - \alpha_i$ has an inverse (since it does not divide $G(z)$). The inverse is

$$(z - \alpha_i)^{-1} = -\frac{G(z) - G(\alpha_i)}{z - \alpha_i} G(\alpha_i)^{-1},$$

for indeed

$$-(z - \alpha_i)\frac{(G(z) - G(\alpha_i))}{z - \alpha_i} G(\alpha_i)^{-1} \equiv 1 \bmod G(z).$$

Therefore $a$ is in $\Gamma(L, G)$ iff

$$\sum_{i=1}^{n} a_i \frac{G(z) - G(\alpha_i)}{z - \alpha_i} G(\alpha_i)^{-1} = 0 \tag{10}$$

as a polynomial (not mod $G(z)$). If $G(z) = \Sigma_{i=0}^{r} g_i z^i$, with $g_i \in \text{GF}(q^m)$ and $g_r \neq 0$, then

$$\frac{G(z) - G(\alpha_i)}{z - \alpha_i} = g_r(z^{r-1} + z^{r-2}\alpha_i + \cdots + \alpha_i^{r-1}) + g_{r-1}(z^{r-2} + \cdots + \alpha_i^{r-2}) + \cdots$$
$$+ g_2(z + \alpha_i) + g_1.$$

Equating the coefficients of $z^{r-1}, z^{r-2}, \ldots, 1$ to zero in (10) we see that $a$ is in $\Gamma(L, G)$ iff $Ha^{tr} = 0$, where

$$H = \begin{bmatrix} g_r G(\alpha_1)^{-1} & \cdots & g_r G(\alpha_n)^{-1} \\ (g_{r-1} + \alpha_1 g_r) G(\alpha_1)^{-1} & \cdots & (g_{r-1} + \alpha_n g_r) G(\alpha_n)^{-1} \\ \cdots\cdots\cdots & \cdots & \cdots\cdots\cdots \\ (g_1 + \alpha_1 g_2 + \cdots + \alpha_1^{r-1} g_r) G(\alpha_1)^{-1} & \cdots & (g_1 + \alpha_n g_2 + \cdots + \alpha_n^{r-1} g_r) G(\alpha_n)^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} g_r & 0 & 0 & \cdots & 0 \\ g_{r-1} & g_r & 0 & \cdots & 0 \\ g_{r-2} & g_{r-1} & g_r & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_1 & g_2 & g_3 & \cdots & g_r \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix} \cdot \begin{bmatrix} G(\alpha_1)^{-1} & & & 0 \\ & G(\alpha_2)^{-1} & & \\ & & \ddots & \\ 0 & & & G(\alpha_n)^{-1} \end{bmatrix}$$

$$= CXY \quad \text{(say)}, \tag{11}$$

is a parity check matrix for $\Gamma(L, G)$. Since $C$ is invertible, by Problem 31 of Ch. 7 another parity check matrix is

$$H' = XY$$

$$= \begin{bmatrix} G(\alpha_1)^{-1} & \cdots & G(\alpha_n)^{-1} \\ \alpha_1 G(\alpha_1)^{-1} & \cdots & \alpha_n G(\alpha_n)^{-1} \\ \cdots & \cdots & \cdots \\ \alpha_1^{r-1} G(\alpha_1)^{-1} & \cdots & \alpha_n^{r-1} G(\alpha_n)^{-1} \end{bmatrix}, \tag{12}$$

and this is usually the simplest to use.

A parity check matrix with elements from GF($q$) is then obtained by replacing each entry of $H$ (or $H'$) by the corresponding column vector of length $m$ from GF($q$).

Comparing (11) with (3) we see that $\Gamma(L, G)$ is an alternant code $\mathcal{A}(\alpha, y)$ with $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $y = (G(\alpha_1)^{-1}, \ldots, G(\alpha_n)^{-1})$. Therefore $\Gamma(L, G)$ has dimension $k \geqslant n - rm$ and minimum distance $d \geqslant r + 1$.

In fact it is easy to find the generalized Reed–Solomon code which produces $\Gamma(L, G)$.

**Theorem 4.** *$\Gamma(L, G)$ is the restriction to* GF($q$) *of* GRS$_{n-r}(\alpha, v)$, *where $v = (v_1, \ldots, v_n)$ and*

$$v_i = \frac{G(\alpha_i)}{\prod_{j \neq i} (\alpha_i - \alpha_j)}, \quad i = 1, \ldots, n.$$

**Proof.** (i) Take $u \in \text{GRS}_{n-r}(\alpha, v) \mid \text{GF}(q)$. Then

$$u_i = v_i F(\alpha_i) = \frac{F(\alpha_i) G(\alpha_i)}{\prod_{j \neq i} (\alpha_i - \alpha_j)},$$

where $F(z)$ is a polynomial of degree $< n - r$. Thus

$$\sum_{i=1}^{n} \frac{u_i}{z - \alpha_i} = \frac{1}{\prod_{i=1}^{n} (z - \alpha_i)} \sum_{i=1}^{n} F(\alpha_i) G(\alpha_i) \prod_{j \neq i} \frac{(z - \alpha_j)}{(\alpha_i - \alpha_j)}.$$

Let

$$N(z)=\sum_{i=1}^{n} F(\alpha_i)G(\alpha_i)\prod_{j\neq i}(z-\alpha_j)/(\alpha_i-\alpha_j).$$

Then $N(\alpha_i)=F(\alpha_i)G(\alpha_i)$ for $i=1,\ldots,n$. Also $\deg N(z)\leq n-1$ and $\deg F(z)G(z)\leq n-1$. Since the polynomial $N(z)-F(z)G(z)$ is determined by its values at $n$ points, $N(z)=F(z)G(z)$. Therefore

$$\sum_{i=1}^{n}\frac{u_i}{z-\alpha_i}=\frac{F(z)G(z)}{\prod_{i=1}^{n}(z-\alpha_i)}$$

and hence $u\in\Gamma(L,G)$. Thus

$$\Gamma(L,G)\supset \mathrm{GRS}_{n-r}(\alpha,v)\,|\,\mathrm{GF}(q)$$

(ii) The converse is similar and is left to the reader. Q.E.D.

From Theorem 2 we obtain:

**Theorem 5.** *The dual of a Goppa code is given by*

$$\Gamma(L,G)^{\perp}=T_m(\mathrm{GRS}_r(\alpha,y)) \tag{13}$$

*where* $y_i=G(\alpha_i)^{-1}$.

**Problem.** (2) Prove directly that $\mathrm{GRS}_r(\alpha,y)$, where $y_i=G(\alpha_l)^{-1}$, and $\mathrm{GRS}_{n-r}(\alpha,y')$, where

$$y_i'=\frac{G(\alpha_i)}{\prod_{j\neq i}(\alpha_j-\alpha_i)},$$

are dual codes.

*Binary Goppa codes.* Just as for BCH codes one can say a bit more in the binary case (cf. §6 of Ch. 7). Suppose $\Gamma=\Gamma(L,G)$ is a binary Goppa code (with $q=2$). Let $a=(a_1\cdots a_n)$ be a codeword of weight $w$ in $\Gamma$, with $a_{l_1}=\cdots=a_{l_w}=1$, and define

$$f_a(z)=\prod_{i=1}^{w}(z-\alpha_{l_i}). \tag{14}$$

Then

$$f_a'(z)=\sum_{i=1}^{w}\prod_{j\neq i}(z-\alpha_{l_j}),$$

$$R_a(z)=\sum_{i=1}^{w}\frac{1}{z-\alpha_{l_i}}=\frac{f_a'(z)}{f_a(z)}\quad\text{from (8)} \tag{15}$$

The $\alpha_i$'s are distinct. from the definition of $\Gamma$, so $f_a'(z)$ and $f_a(z)$ have no common factors, and (15) is in lowest terms. Since $G(\alpha_i)\neq 0$, $f_a(z)$ and $G(z)$

are relatively prime, and so from (15)

$$R_a(z) \equiv 0 \bmod G(z) \text{ iff } G(z) \mid f_a'(z).$$

We are working mod 2, so $f_a'(z)$ contains only even powers and is a perfect square. Let $\bar{G}(z)$ be the lowest degree perfect square which is divisible by $G(z)$. Then

$$G(z) \mid f_a'(z) \text{ iff } \bar{G}(z) \mid f_a'(z).$$

We conclude that

$$\begin{aligned} a \in \Gamma \text{ iff } & R_a(z) \equiv 0 \bmod G(z) \\ \text{iff } & \bar{G}(z) \mid f_a'(z). \end{aligned} \tag{16}$$

In particular, if $a \neq 0$, $\deg f_a'(z) \geq \deg \bar{G}(z)$. Hence

$$\text{min. distance of } \Gamma \geq \deg \bar{G}(z) + 1. \tag{17}$$

An important special case is:

**Theorem 6.** *Suppose $G(z)$ has no multiple zeros, so that $\bar{G}(z) = G(z)^2$. Then*

$$\textit{min. distance of } \Gamma \geq 2 \deg G(z) + 1. \tag{18}$$

If $G(z)$ has no multiple zeros then $\Gamma$ is called a *separable* Goppa code.

*Examples of binary Goppa codes.* (1) Take $G(z) = z^2 + z + 1$, $L = GF(2^3) = \{0, 1, \alpha, \ldots, \alpha^6\}$ where $\alpha$ is primitive, $q = 2$, and $q^m = 8$. Certainly $G(\beta) \neq 0$ for $\beta \in GF(2^3)$, for the zeros of $z^2 + z + 1$ belong to $GF(2^2)$, $GF(2^4)$, $GF(2^6), \ldots$ but not to $GF(2^3)$ – see Theorem 8 of Ch. 4. We obtain an irreducible Goppa code $\Gamma$ of length $n = |L| = 8$, dimension $k \geq 8 - 2.3 = 2$, and minimum distance $d \geq 5$. From (12) a parity check matrix is

$$H = \begin{bmatrix} \dfrac{1}{G(0)} & \dfrac{1}{G(1)} & \dfrac{1}{G(\alpha)} & \cdots & \dfrac{1}{G(\alpha^6)} \\[2ex] \dfrac{0}{G(0)} & \dfrac{1}{G(1)} & \dfrac{\alpha}{G(\alpha)} & \cdots & \dfrac{\alpha^6}{G(\alpha^6)} \end{bmatrix}$$

From Fig. 4.5 we find

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

$$= \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{array} \\ \left[\begin{array}{cccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right] \end{array}.$$

The codewords are

$$\begin{array}{cccccccc} 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \end{array}$$
$$\left\{\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array}\right\},$$

so this is an [8, 2, 5] Goppa code. By adding an overall parity check and reordering the columns the following [9, 2, 6] code is obtained:

$$\begin{array}{ccccccccc} 1 & \alpha^4 & \alpha^6 & \infty & \alpha^2 & \alpha^5 & 0 & \alpha & \alpha^3 \\ \end{array}$$
$$\left\{\begin{array}{ccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{array}\right\}. \qquad (19)$$

This code is cyclic! An explanation for this phenomenon will be given in §5.

This example can also be used as an illustration of Theorem 4. Here $n - r = 8 - 2 = 6$, and $v_i = G(\alpha_i) = \alpha^{2i} + \alpha^i + 1$, since $\Pi_{j \neq i}(\alpha_j - \alpha_i) = 1$ for all $i$. Thus Theorem 4 states that the [8, 2, 5] Goppa code is the restriction to GF(2) of the code over GF($2^3$) with generator matrix

$$\begin{bmatrix} 1 & 1 & \alpha^5 & \alpha^3 & \alpha^5 & \alpha^6 & \alpha^6 & \alpha^3 \\ 0 & 1 & \alpha^6 & \alpha^5 & \alpha & \alpha^3 & \alpha^4 & \alpha^2 \\ 0 & 1 & 1 & 1 & \alpha^4 & 1 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 & 1 & \alpha^4 & 1 & 1 \\ 0 & 1 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha & \alpha^5 & \alpha^6 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^6 & \alpha^5 & \alpha^3 & \alpha^5 \end{bmatrix}.$$

It is readily checked that

$$\begin{aligned} \text{row } 1 + \text{row } 2 + \text{row } 6 &= 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0, \\ \text{row } 1 + \text{row } 5 + \text{row } 6 &= 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1, \\ \text{row } 2 + \text{row } 5 &= 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1. \end{aligned}$$

(2) Take $G(z) = z^3 + z + 1$ and $L = \mathrm{GF}(2^5)$. Again $G(\beta) \neq 0$ for $\beta \in L$ (using Theorem 8 of Ch. 4). Then $\Gamma(L, G)$ is a [32, 17, 7] irreducible Goppa code, with parity check matrix given by Equation (12) (here $\alpha$ is a primitive element of GF($2^5$)):

$$H = \begin{bmatrix} \dfrac{1}{G(0)} & \dfrac{1}{G(1)} & \dfrac{1}{G(\alpha)} & \cdots & \dfrac{1}{G(\alpha^{30})} \\ \dfrac{0}{G(0)} & \dfrac{1}{G(1)} & \dfrac{\alpha}{G(\alpha)} & \cdots & \dfrac{\alpha^{30}}{G(\alpha^{30})} \\ \dfrac{0^2}{G(0)} & \dfrac{1^2}{G(1)} & \dfrac{\alpha^2}{G(\alpha)} & \cdots & \dfrac{\alpha^{60}}{G(\alpha^{30})} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & \alpha^4 & \alpha^8 & \alpha^{14} & \cdots & \alpha^{26} \\ 0 & 1 & \alpha^5 & \alpha^{10} & \alpha^{17} & \cdots & \alpha^{25} \\ 0 & 1 & \alpha^6 & \alpha^{12} & \alpha^{20} & \cdots & \alpha^{24} \end{bmatrix}$$

$$= \left[\begin{array}{cccccccc} 1 & 1 & 0 & 1 & 1 & & 1 \\ 0 & 0 & 0 & 0 & 0 & & 1 \\ 0 & 0 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 1 & 1 & & 0 \\ 0 & 0 & 1 & 0 & 1 & & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & & 1 \\ 0 & 0 & 0 & 0 & 1 & & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & & 1 \\ 0 & 0 & 0 & 1 & 1 & & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & & 0 \\ 0 & 0 & 1 & 1 & 0 & & 1 \\ 0 & 0 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & 1 & 1 & & 1 \\ 0 & 0 & 0 & 0 & 0 & & 1 \end{array}\right]$$

where we have used the table of GF($2^5$) given in Fig. 4.5. The weight distribution of $\Gamma(L, G)$ was found (by computer) to be:

| $i$: | 0 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|
| $A_i$: | 1 | 128 | 400 | 800 | 1903 | 4072 | 6876 | 10360 | 14420 | 17448 |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|
| 18381 | 17336 | 14330 | 10360 | 6860 | 4136 | 2068 | 760 | 250 | 136 | 47 |

(3) Of course the coefficients of $G(z)$ need not be restricted to 0's and 1's. For example we could take $G(z) = z^2 + z + \alpha^3$, where $\alpha$ is a primitive element of GF($2^4$). From Theorem 15 of Ch. 9 $G(z)$ is irreducible over GF($2^4$), since $T_4(\alpha^3) = \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9 = 1$. Therefore we can take $L = \text{GF}(2^4)$, and obtain a $[16, 8, 5]$ irreducible Goppa code.

**Problem.** (3) Find a parity check matrix for this code.

(4) *Irreducible Goppa codes.* Consider $G(z) = z^3 + z + 1$, which is irreducible over GF(2). The zeros of $G(z)$ lie in GF($2^3$) and hence by Theorem 8 of Ch. 4 are in GF($2^6$), GF($2^9$), .... Provided $m$ is not a multiple of 3 we can take $L = \text{GF}(2^m)$, and obtain an

$$[n = 2^m, k \geqslant 2^m - 3m, d \geqslant 7] \quad (\text{for } 3 \nmid m) \tag{20}$$

irreducible Goppa code. When $m = 5$, the bounds for $k$ and $d$ are exact, as we saw in example (2).

Alternatively, taking $G(z)$ to be an irreducible cubic over $\mathrm{GF}(2^m)$ we get a code with parameters (20) for any $m$.

More generally, taking $G(z)$ to be an irreducible polynomial of degree $r$ over $\mathrm{GF}(2^m)$ we obtain an

$$[n = 2^m, k \geq 2^m - rm, d \geq 2r + 1] \tag{21}$$

irreducible Goppa code for any $r$ and $m$. The comparable primitive BCH code has parameters

$$[n = 2^m - 1, k \geq 2^m - 1 - rm, d \geq 2r + 1], \tag{22}$$

which (if equality holds for $k$ and $d$ in (21) and (22)) has one fewer information symbol.

**Problem.** (4) Let $G(z)$ have degree $r$, distinct zeros, coefficients in $\mathrm{GF}(2^s)$, and satisfy $G(0) \neq 0$, $G(1) \neq 0$. Let $\mathrm{GF}(2^t)$ be the smallest field which contains all the zeros of $G(z)$. Show that we can choose $L = \mathrm{GF}(2^m)$ for any $m$ such that $s \mid m$ and $(t, m) = 1$, and obtain a Goppa code with parameters (21).

(5) *BCH codes*. Narrow-sense, primitive BCH codes are a special case of Goppa codes: choose $G(z) = z^r$ and $L = \{1, \alpha, \ldots, \alpha^{n-1}\}$ when $n = q^m - 1$ and $\alpha$ is a primitive element of $\mathrm{GF}(q^m)$. Then from Eq. (12),

$$H = \begin{bmatrix} 1 & \alpha^{-r} & \alpha^{-2r} & \cdots & \alpha^{-(n-1)r} \\ 1 & \alpha^{-(r-1)} & \alpha^{-2(r-1)} & \cdots & \alpha^{-(n-1)(r-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \end{bmatrix}$$

which becomes the parity check matrix of a BCH code (Equation (19) of Ch. 7) when $\alpha^{-1}$ is replaced by $\beta$.

To obtain a $t$-error-correcting *binary* BCH code we take $G(z) = z^{2t}$ and $L = \mathrm{GF}(2^m)^*$.

In examples (1) and (2) it turned out that $k$ and $d$ coincided with the bounds given in Fig. 12.3. But this is not always so, as the example of BCH codes shows.

**Research Problem** (12.1). Find the true dimension and minimum distance of a Goppa code.

**Problem.** (5) Another form for the parity check matrix. Suppose $G(z)$ has no multiple zeros, say $G(z) = (z - z_1) \cdots (z - z_r)$, where $z_1, \ldots, z_r$ are distinct elements of $\mathrm{GF}(2^s)$. Show that $a \in \Gamma(L, G)$ iff $Ha^T = 0$, where $H = (H_{ij})$, $H_{ij} = 1/(z_i - \alpha_j)$, for $1 \leq i \leq r$, $1 \leq j \leq n$.

**Remark.** Note that in this problem $H$ is a Cauchy matrix (see Problem 7 of

Ch. 11). If $H$ is the parity check matrix of a $t$-error-correcting code then every $2t$ columns of $H$ must be linearly independent, from Theorem 10 of Ch. 1. Now in classical matrix theory there are two *complex* matrices with the property that *every* square submatrix is nonsingular. These are the Vandermonde and Cauchy matrices – see Lemma 17 of Ch. 4 and Problem 7 of Ch. 11. The Vandermonde matrix is the basis for the definition of a BCH code (§6 of Ch. 7), and we have just seen that the Cauchy matrix is the basis for separable Goppa codes.

**Problem.** (6) A Goppa code with $G(z) = (z - \beta)^r$ for some $\beta$ is called *cumulative.* Show that there is a weight-preserving one-to-one mapping between $\Gamma(\mathrm{GF}(2^m) - \{\beta\}, (z - \beta)^r)$ and the BCH code $\Gamma(\mathrm{GF}(2^m)^*, z^r)$.

Example (1) suggests the following problem.

**Problem.** (7) (Cordaro and Wagner.) Let $\mathscr{C}_n$ be that $[n, 2, d]$ binary code with the highest $d$ and which corrects the most errors of weight $[\frac{1}{2}(d - 1)] + 1$. Set $r = [\frac{1}{3}(n + 1)]$. Show that $d = 2r$ if $n \equiv 0$ or $1 \bmod 3$, and $d = 2r - 1$ if $n \equiv 2 \bmod 3$; and that a generator matrix for $\mathscr{C}_n$ can be taken to consist of $r$ columns equal to $\binom{0}{1}$, $r$ columns equal to $\binom{1}{0}$, and the remaining columns equal to $\binom{1}{1}$.

## §4. Further properties of Goppa codes

*Adding an overall parity check.* Let $\Gamma(L, G)$ be a Goppa code over $\mathrm{GF}(q)$ of length $n = q^m$, with $L = \mathrm{GF}(q^m) = \{0, 1, \alpha, \ldots, \alpha^{n-2}\}$ and $G(z) =$ a polynomial of degree $r$ with no zeros in $\mathrm{GF}(q^m)$. From (12), $a = (a(0), a(1), \ldots, a(a^{n-2}))$ is in $\Gamma(L, G)$ iff

$$\sum_{\beta \in \mathrm{GF}(q^m)} \frac{\beta^i a(\beta)}{G(\beta)} = 0 \quad \text{for } i = 0, 1, \ldots, r - 1. \tag{23}$$

$\Gamma(L, G)$ may be extended by adding an overall parity check $a(\infty)$ given by

$$a(\infty) = - \sum_{\beta \in \mathrm{GF}(q^m)} a(\beta)$$

or

$$\sum_{\beta \in \mathrm{GF}(q^m) \cup \{\infty\}} a(\beta) = 0. \tag{24}$$

With the convention that $1/\infty = 0$, the range of summation in (23) can be