Chapter 7

Codes over Subfields

In Chapter 6 we looked at various general methods for constructing new codes from old codes. Here we concentrate on two more specialized techniques that result from writing the field F as a vector space over its subfield K. We will start with linear codes over F and finish with linear codes over K. Of particular practical importance is the case with $K = \mathbb{F}_2$. Our work on generalized Reed-Solomon codes over F has given us many powerful codes, but by Theorem 5.1.1 their length is bounded by $|F|$. Binary generalized Reed-Solomon codes are rendered trivial.

7.1 Basics

Let $\dim_K(F) = m$, and choose $e_1, \ldots e_m$ to be a K-basis for F. We define the map $\phi\colon F \longrightarrow K^m$ given by

$$\phi(\alpha) = (a_1, \ldots a_m) \text{ where } \alpha = a_1 e_1 + \cdots + a_m e_m \,.$$

For brevity, we shall write $\hat{\alpha}$ for the $1 \times m$ row vector $\phi(\alpha)$ and $\check{\alpha}$ for its transpose $\phi(\alpha)^\top = (a_1, \ldots a_m)^\top$, an $m \times 1$ column vector. We extend this notation to any $p \times q$ matrix $A \in F^{p,q}$, with i, j entry $a_{i,j}$ by letting $\widehat{A} \in K^{p,mq}$ be the matrix

$$\begin{bmatrix} \hat{a}_{1,1} & \hat{a}_{1,2} & \cdots & \hat{a}_{1,j} & \cdots & \hat{a}_{1,q} \\ \hat{a}_{2,1} & \hat{a}_{2,2} & \cdots & \hat{a}_{2,j} & \cdots & \hat{a}_{1,q} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \hat{a}_{i,1} & \hat{a}_{i,2} & \cdots & \hat{a}_{i,j} & \cdots & \hat{a}_{1,q} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \hat{a}_{p,1} & \hat{a}_{p,2} & \cdots & \hat{a}_{p,j} & \cdots & \hat{a}_{p,q} \end{bmatrix}$$

and $\check{A} \in K^{mp,q}$ be the matrix

$$\begin{bmatrix} \check{a}_{1,1} & \check{a}_{1,2} & \cdots & \check{a}_{1,j} & \cdots & \check{a}_{1,q} \\ \check{a}_{2,1} & \check{a}_{2,2} & \cdots & \check{a}_{2,j} & \cdots & \check{a}_{1,q} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \check{a}_{i,1} & \check{a}_{i,2} & \cdots & \check{a}_{i,j} & \cdots & \check{a}_{1,q} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \check{a}_{p,1} & \check{a}_{p,2} & \cdots & \check{a}_{p,j} & \cdots & \check{a}_{p,q} \end{bmatrix}$$

For our constructions, A might be a spanning or control matrix for a linear code over F. Then the matrices $\widehat{A}$ and $\check{A}$ can be thought of as spanning or control matrices for linear codes over K.

It must be emphasized that these maps are highly dependent upon the choice of the initial map ϕ, even though ϕ has been suppressed in the notation. We shall see below that a careful choice of ϕ can be of great help. (The general situation in which ϕ is an arbitrary injection of F into K^p, for some field K and some p, is of further interest. Here we will be concerned with the linear case, but see the Problem 7.2.3 below.)

7.2 Expanded codes

If C is a code in F^n, then the code

$$\widehat{C} = \{\, \hat{\mathbf{c}} \,|\, \mathbf{c} \in C \,\}$$

expanded code

in K^{mn} is called an *expanded code*.

(7.2.1) THEOREM. *If C is an $[n, k, d]$ code, then $\widehat{C}$ is an $[mn, mk, \geq d]$ code.*

PROOF. The map $\mathbf{x} \mapsto \hat{\mathbf{x}}$ (induced by ϕ) is one-to-one and has

$$\widehat{r\mathbf{a} + s\mathbf{b}} = r\hat{\mathbf{a}} + s\hat{\mathbf{b}}\,,$$

for all $r, s \in K$ and $\mathbf{a}, \mathbf{b} \in F^n$. Thus $\widehat{C}$ is a linear code over K with

$$|\widehat{C}| = |C| = |F|^k = (|K|^m)^k = |K|^{mk}\,,$$

hence $\widehat{C}$ has K-dimension mk. (This counting argument is a cheat unless F is finite, the case of greatest interest to us. Instead, one should construct a K-basis for $\widehat{C}$ out of that for F and an F-basis for C. We do this below, constructing a generator matrix for $\widehat{C}$ from one for C.)

If the coordinate c_i of $\mathbf{c}$ is nonzero, then $\hat{c}_i$ is not the zero vector of K^m. Therefore each nonzero entry in $\mathbf{c}$ corresponds to a nonzero m-tuple $\hat{c}_i$ within $\hat{\mathbf{c}}$ and $\mathrm{w_H}(\mathbf{c}) \leq \mathrm{w_H}(\hat{\mathbf{c}})$. In particular $\mathrm{d_{min}}(C) \leq \mathrm{d_{min}}(\widehat{C})$. □

The argument of the last paragraph shows that we would be very unlucky indeed to have $\mathrm{d_{min}}(C) = \mathrm{d_{min}}(\widehat{C})$. For this to happen we would need a minimum weight codeword $\mathbf{c}$ in C for which every nonzero c_i had $\hat{c}_i$ of weight 1. In

the next section we shall see two examples in which the minimum distance of an expanded codes goes up over that of its parent.

Let G be a generator matrix for C with rows $\mathbf{g}_i$, for $i = 1, \ldots, k$. Notice that $\mathbf{g}_i$ and $e_j\mathbf{g}_i$ are F-scalar multiples but are linearly independent over K. The mk vectors $e_j\mathbf{g}_i$ (for $1 \le j \le m$, $1 \le i \le k$) form a basis for C, thought of as a K-space of dimension mk. If we let G_0 be the $mk \times n$ matrix whose rows are the various $e_j\mathbf{g_i}$, then G_0 is a spanning matrix for C and $\widehat{G}_0$ is a generator matrix for $\widehat{C}$.

A vector is a *burst* of length f if all of its nonzero entries are restricted to a set of f consecutive positions. For instance, (00011101000) is a burst of length 5 (and 6, 7, ..., 11, as well). Certain channels are prone to burst errors. (Think of a scratch on a CD.) Expanded codes give some easy protection against burst errors, since an error in m consecutive positions of $\widehat{C}$ corresponds to only one or two errors for the parent code C. burst

(7.2.2) PROPOSITION. *If the linear code C can be used to correct burst errors of length e (in particular, if C is an e error-correcting code), then $\widehat{C}$ can be used to correct all burst errors of length up to $1 + (e-1)m$.*

PROOF. A burst in K^{mn} of length at most $1 + (e-1)m$ has as preimage in F^n a burst of length at most e. □

(7.2.3) PROBLEM. (*a*) *Consider an injection ϕ of $\mathbb{F}_4$ into $\mathbb{F}_2^3$ with the property that*

$$\phi(\mathbb{F}_4) = \{001, 110, 010, 101\}\,.$$

Prove that, for any code $C \subseteq \mathbb{F}_4^n$, the corresponding expanded code $\hat{C}$ in $\mathbb{F}_2^{3n}$ has the property that each codeword has no more than three consecutive 0's and no more than three consecutive 1's among its entries. (This is a 'run-length-limited' constraint of the sort that is made for magnetic recording and on compact discs.)

(*b*) *Prove that there are exactly four 4-subsets of $\mathbb{F}_2^3$ with the property discussed in* (*a*).

Expanding is often used as an easy way to construct good binary codes for bursty channels from codes over larger fields of characteristic 2. For instance, one code that has been used by NASA and the European Space Agency, (for space communication) and IBM, Phillips, and Sony (for tape and CD storage) is the binary expansion of a *GRS* code of length $255\,(= 2^8 - 1)$ and dimension 223 over $\mathbb{F}_{2^8}$. (The vector $\boldsymbol{\alpha}$ contains all nonzero field elements as entries, while $\mathbf{v} = \mathbf{1}$.) Expanding from $\mathbb{F}_{2^8}$ to $\mathbb{F}_2$ (so that $m = 8$) allows symbols of the *GRS* code to be written as bytes of data. The associated binary expanded code has length $mn = 8(255) = 2040$ and dimension $mk = 8(223) = 1784$. The parent *GRS* code has $\mathrm{d}_{\min} = 255 - 223 + 1 = 33$, so it can correct up to 16 errors. Therefore the expanded code can correct any burst error of length at most $1 + (16-1)8 = 121$ as well as any random error of weight at most 8.

7.3 Golay codes and perfect codes

We construct four of the most famous and important codes using expanded codes.

7.3.1 Ternary Golay codes

Here we have $F = \mathbb{F}_9$, $K = \mathbb{F}_3$, and $m = 2$ in Theorem 7.2.1.

Let i be a root of the imprimitive polynomial $x^2 + 1 \in \mathbb{F}_3[x]$. We then write the field $\mathbb{F}_9$ as $\{a + bi \,|\, a, b \in \mathbb{F}_3\}$, having chosen the $\mathbb{F}_3$-basis of $e_1 = 1$ and $e_2 = i$ for $\mathbb{F}_9$, so that the associated expansion map is

$$\beta = a\,1 + b\,i \mapsto \phi(\beta) = \hat{\beta} = (a, b)\,,$$

for $a, b \in \mathbb{F}_3$. For each $\beta = a + bi \in \mathbb{F}_9$, let $\bar{\beta} = a - bi$, the conjugate of β.

Let A be a unitary 3×3 matrix with entries from $\mathbb{F}_9$, that is $A\bar{A}^\top = I$; and let $\alpha \in \mathbb{F}_9$ satisfy $\alpha\bar{\alpha} = -1$. Here by $\bar{A}$ we mean the matrix whose i, j entry is $\bar{a}_{i,j}$, where $a_{i,j}$ is the i, j entry of A.

EXAMPLE.

$$A = \begin{bmatrix} 1+i & i & i \\ i & 1+i & i \\ i & i & 1+i \end{bmatrix} \text{ and } \alpha = 1 - i\,.$$

Consider then the $[6, 3]$ linear code C over $\mathbb{F}_9$ with generator matrix

$$G = [\, I \;;\; \alpha A \,]\ ,$$

for example,

$$G = \begin{bmatrix} 1 & 0 & 0 & -1 & 1+i & 1+i \\ 0 & 1 & 0 & 1+i & -1 & 1+i \\ 0 & 0 & 1 & 1+i & 1+i & -1 \end{bmatrix}\,.$$

We then may calculate

$$G\bar{G}^\top = I + \alpha\bar{\alpha}A\bar{A}^\top = I + (-1)I = 0\,;$$

so

$$H = \bar{G} = \left[\, I \;;\; \bar{\alpha}\bar{A} \,\right]$$

is a check matrix for C. In particular $C^\perp$ equals $\bar{C}$, the code composed of the various $\bar{\mathbf{c}}$ as $\mathbf{c}$ runs through C. As G has standard form, a second check matrix for C is

$$H' = \left[\, -\alpha A^\top \;;\; I \,\right]\,.$$

Therefore a second generator matrix is

$$\bar{H}' = \left[\, -\bar{\alpha}\bar{A}^\top \;;\; I \,\right]\,.$$

(7.3.1) PROPOSITION. *Assume that A has no entry equal to 0. Then C has minimum distance 4 and so is an MDS code.*

PROOF. We have $\mathrm{d}_{\min}(A) \leq 6 - 3 + 1 = 4$ by the Singleton Bound 3.1.14, so we must show that C has no codewords of weight 1, 2, or 3. Consider a nonzero codeword $\mathbf{c} = (c^{(1)}; c^{(2)})$ of weight 1, 2, or 3, where $c^{(1)}, c^{(2)} \in \mathbb{F}_9^3$. By the pigeonhole principle, either $c^{(1)}$ or $c^{(2)}$ has weight at most 1.

First suppose $c^{(1)}$ has weight at most 1. In view of the generator matrix G, the only codeword with $c^{(1)}$ equal to 0 is the $\mathbf{0}$-word. A codeword with $c^{(1)}$ of weight 1 is a scalar multiple of some row of G and so has weight 4, since by assumption no entry of A is 0. Thus a nonzero codeword $\mathbf{c}$ with $c^{(1)}$ of weight at most 1 has weight 4.

If instead $c^{(2)}$ has weight at most 1, then we may use the generator matrix $\bar{H}'$ and argue as in the previous paragraph to see again that nonzero $\mathbf{c}$ has weight 4. □

Assume now, as in the example and proposition, that A has been chosen to have none of its entries equal to 0. The $[12, 6, \geq 4]$ ternary code $\widehat{C}$ gotten by expanding C using the map $a + bi \mapsto (a, b)$ is called an *extended ternary Golay code*, as is anything monomially equivalent to it. (For different choices of A this construction will produce different codes $\widehat{C}$, but it turns out that they are all monomially equivalent.)

extended ternary Golay code

If we puncture $\widehat{C}$ at any coordinate position we get an $[11, 6]$ linear code which is called a *ternary Golay code*.

ternary Golay code

(7.3.2) THEOREM. (M. GOLAY, 1949.) (1) *An extended ternary Golay code is a self-dual* $[12, 6, 6]$ *linear code over* $\mathbb{F}_3$.

(2) *A ternary Golay code is a perfect* 2*-error-correcting* $[11, 6]$ *linear code over* $\mathbb{F}_3$.

PROOF. Let $\mathbf{x} = (x_1, \ldots x_6)$, $\mathbf{y} = (y_1, \ldots y_6) \in \mathbb{F}_9^6$ with $x_j = a_j + b_j i$ and $y_j = c_j + d_j i$. Then we easily find

$$\mathbf{x} \cdot \bar{\mathbf{y}} = \hat{\mathbf{x}} \cdot \hat{\mathbf{y}} + f\, i\,,$$

for some $f \in \mathbb{F}_3$. In particular if $\mathbf{x} \cdot \bar{\mathbf{y}} = 0$, then $\hat{\mathbf{x}} \cdot \hat{\mathbf{y}} = 0$.

Since $C^{\perp}$ equals $\bar{C}$, the expanded code $\widehat{C}$ is a self-dual ternary $[12, 6]$ linear code. By Problem 3.1.11(b) all weights of $\widehat{C}$ are multiples of 3. By the Singleton Bound 3.1.14 and Theorem 7.2.1

$$12 - 6 + 1 = 7 \geq \mathrm{d}_{\min}(\widehat{C}) \geq 4 = \mathrm{d}_{\min}(C)\,,$$

hence $\mathrm{d}_{\min} = 6$.

Puncturing $\widehat{C}$ at any position, we find a code of minimum distance at least 5; so every ternary Golay code is a 2-error-correcting code. To complete (2) and the theorem, we check equality in the Sphere Packing Condition 2.2.5 for a

ternary Golay code:

$$\begin{aligned} 3^{11} &\geq 3^6 \sum_{i=0}^{2} \binom{11}{i} (3-1)^i \\ &= 3^6 \Big(\binom{11}{0} + + \binom{11}{1} 2 + \binom{11}{2} 4 \Big) \\ &= 3^6 (1 + 22 + 220) \\ &= 3^6 (243) = 3^6 3^5 = 3^{11} . \qquad \square \end{aligned}$$

7.3.2 Binary Golay codes

Here we have $F = \mathbb{F}_8$, $K = \mathbb{F}_2$, and $m = 3$ in Theorem 7.2.1.

Let α be a root in $\mathbb{F}_8$ of the primitive polynomial $x^3 + x + 1 \in \mathbb{F}_2[x]$, and let

$$\boldsymbol{\alpha} = (0, 1, \alpha, \alpha^2, \ldots, \alpha^6) \in \mathbb{F}_8^8 .$$

In this subsection we begin with the code $D = \mathrm{GRS}_{8,4}(\boldsymbol{\alpha}, \mathbf{1})$, which is a self-dual code by Theorem 5.1.6 and Problem 5.1.5(b). As in Problem A.3.18 of the Appendix, choose, as basis for $\mathbb{F}_8$ over $\mathbb{F}_2$, the elements

$$e_1 = \alpha^3, \; e_2 = \alpha^5, \; e_3 = \alpha^6 .$$

Then, for each $\beta = b_1 e_1 + b_2 e_2 + b_3 e_3$ in $\mathbb{F}_8$, we set

$$\phi(\beta) = \hat{\beta} = (b_1, b_2, b_3) .$$

Expand the $[8, 4]$ code D over $\mathbb{F}_8 = \mathbb{F}_{2^3}$ to a $[24, 12]$ code $\widehat{D}$ over $\mathbb{F}_2$ using this map. Then $\widehat{D}$ or any code equivalent to it is called an *extended binary Golay code*. If we puncture an extended binary Golay code at any coordinate position we get a $[23, 12]$ linear code which is called a *binary Golay code*.

extended binary Golay code

binary Golay code

(7.3.3) THEOREM. (M. GOLAY, 1949.) (1) *An extended binary Golay code is a self-dual* $[24, 12, 8]$ *linear code over* $\mathbb{F}_2$.

(2) *A binary Golay code is a perfect* 3*-error-correcting* $[23, 12]$ *linear code over* $\mathbb{F}_2$.

PROOF. We have already remarked that D is self-dual by Theorem 5.1.6 and Problem 5.1.5(b). Therefore by Theorem 7.2.1 and Problem A.3.18 of the Appendix the extended Golay code $\widehat{D}$ is a self-dual binary $[24, 12, \geq 5]$ linear code. As $\widehat{D}$ is self-dual, $\mathrm{d}_{\min}$ is even by Problem 3.1.11(a) and so at least 6.

Let G be the canonical generator matrix of D with rows $\mathbf{g}_0, \mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3$:

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

As seen earlier, one generator matrix for $\widehat{D}$ has as rows the twelve codewords $\mathbf{c}_{i,j} = \widehat{e_j \mathbf{g}_i}$, for $1 \le j \le 3$ and $0 \le i \le 3$. Each $\mathbf{c} = \mathbf{c}_{i,j}$ consists of eight binary triples:

$$\mathbf{c} = (c^{(1)}; c^{(2)}; c^{(3)}; c^{(4)}; c^{(5)}; c^{(6)}; c^{(7)}; c^{(8)}) .$$

If $\mathbf{c} = \mathbf{c}_{0,j}$, then the $c^{(a)}$ are all equal and of weight one, hence $\mathbf{c}$ has weight 8. If $\mathbf{c} = \mathbf{c}_{i,j}$ with $i \neq 0$, then

$$\{ c^{(a)} \mid 1 \le a \le 8 \} = \{000, 001, 010, 011, 100, 101, 110, 111\} ,$$

and $\mathbf{c}$ has weight 12. Therefore in all cases $\mathbf{c} = \mathbf{c}_{i,j}$ has weight a multiple of 4. As these span the self-dual code $\widehat{D}$, Problem 3.1.11(a) guarantees that all weights of $\widehat{D}$ must have weight a multiple of 4. Thus $\mathrm{d}_{\min}(\widehat{D}) \ge 8$. We have equality, since each $\mathbf{c}_{0,j}$ has weight 8.

Puncturing $\widehat{D}$ at any position, we find a code of minimum distance at least 7; so every binary Golay code is a 3-error-correcting code. To complete (2) and the theorem, we check equality in the Sphere Packing Condition 2.2.5 for a binary Golay code:

$$\begin{aligned} 2^{23} &\ge 2^{12} \sum_{i=0}^{3} \binom{23}{i} (2-1)^i \\ &= 2^{12} \Big(\binom{23}{0} + + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} \Big) \\ &= 2^{12}(1 + 23 + 253 + 1771) \\ &= 2^{12}(2048) = 2^{12} 2^{11} = 2^{23} . \qquad \square \end{aligned}$$

7.3.3 Perfect codes

Although we will not at present devote much time to perfect codes, we emphasize the speciality of the Golay codes by reporting

(7.3.4) THEOREM. (TIETÄVÄINEN AND VAN LINT, 1971.) *A perfect e-error-correcting code C of length n over $\mathbb{F}_q$ satisfies one of:*

(1) $|C| = 1$, $e = n$;
(2) $|C| = q^n$, $e = 0$;
(3) $|C| = 2$, $q = 2$, $n = 2e + 1$;
(4) $|C| = 3^6$, $q = 3$, $e = 2$, $n = 11$;
(5) $|C| = 2^{12}$, $q = 2$, $e = 3$, $n = 23$;
(6) $|C| = q^{n-r}$, $e = 1$, $n = (q^r - 1)/(q - 1)$, *any* $r > 0$. $\square$

Notice that we make no assumption of linearity.

The codes of (1) and (2) are called trivial perfect codes. The repetition codes are examples for (3) and are nearly trivial. The Golay codes are examples in (4) and (5), and the Hamming codes occur under (6).

The codes of (1) through (5) are unique up to affine equivalence. This is easy to prove for (1) through (3) but difficult for the Golay codes. In most cases

there exist perfect codes with the same parameters as a Hamming code but not affine equivalent to a Hamming code.

Best and Hong have proven that Theorem 7.3.4 remains valid for all finite alphabets A, not just those of prime power order, provided $e \geq 3$.

There are two basic tools in the proof of such theorems. One is the Sphere Packing Condition 2.2.5, in the form

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i \mid q^n \,,$$

of particular value when the alphabet size q is a prime power and $e > 1$. Indeed the only solution to this equation for $q\,(\leq 100)$ a prime power with $n \leq 1000$ and $1 < e \leq 1000$, other than the ones implied by the existence of the perfect codes above, is

$$1 + \binom{90}{1} + \binom{90}{2} = 2^{12} \,,$$

which would correspond to a perfect binary 2-error-correcting code of length 90 (but see Problem 7.3.5 below).

The second main tool for proving nonexistence of perfect codes is Lloyd's Theorem, which is proven below as Theorem 9.4.9. This is a deep result saying that a certain polynomial, determined entirely by the parameters n, q, and e, must have all its roots positive integers in order for there to exist a corresponding perfect code. The analysis of the roots of the Lloyd polynomial is delicate but far reaching. As q has more prime factors, the Sphere Packing Condition becomes less restrictive; so Best and Hong's proof must rely almost entirely on Lloyd's theorem.

As an example of the kind of argument that goes into Theorem 7.3.4 and its relatives, we present the special case of binary, perfect 2-error-correcting codes as Theorem 9.4.11 below.

(7.3.5) PROBLEM. *(a) In a binary perfect e error-correcting code of length n we must have $n+1$ a multiple of $e+1$. (*HINT: *Assume that the code contains the* **0***-vector. Consider the $n-e$ words of weight $e+1$, having common ones in a fixed set of e coordinate positions, and the distribution of these words into spheres of radius e around codewords.)*

(b) Prove that a perfect binary 2-error-correcting code of length 90 does not exist.

(7.3.6) PROBLEM. *Prove that a binary, perfect 1-error-correcting code of length 7 is a coset of a Hamming code.*

(7.3.7) PROBLEM. *Let C be a binary, perfect 1-error-correcting code of length n that contains* **0**.

*(a) Prove that C contains $n(n-1)/6$ codewords of weight 3. (*HINT: *Every word of weight 2 is inside a unique sphere of radius 1 around a codeword of weight 3.)*

*(b) Prove that C contains $n(n-1)(n-3)/24$ codewords of weight 4. (*HINT: *Every word of weight 3 is either a codeword or is inside a unique sphere of radius 1 around a codeword of weight 4.)*

(7.3.8) PROBLEM. *Explain how, in theory, one could find recursively the number of codewords of any fixed weight in the perfect e-error-correcting code C (containing $\mathbf{0}$) in terms of e, the length n, and the size q of the alphabet.*

7.4 Subfield subcodes

An expanded code is longer than its parent code but has the same number of codewords. Subfield subcodes have the same length but are smaller than their parents.

Again let the field F have a subfield K, and let C be a code of length n over F. Then the *subfield subcode* $C|_K$ equals $C \cap K^n$, the set of those codewords of C all of whose coordinate entries belong to the subfield K. As before, the concept makes sense for nonlinear codes, but we shall concentrate on the linear case.

subfield subcode

Of course it initially seems possible that a subfield subcode will be too small to be of use. For linear C, the subcode $C|_K$ contains the $\mathbf{0}$-vector, but does it contain anything else? We shall respond to this by proving that, for H a check matrix for C, the matrix $\check{H}$ is a control matrix for $C|_K$. This will give us an upper bound for the redundancy of $C|_K$ and so a lower bound for its dimension.

The next lemma is used to prove this observation. As before we let $e_1, \ldots, e_m$ a basis for F over K. The $a_{*,j} \in K$ are the entries of column $\check{\alpha}_j$ of the matrix $\check{\boldsymbol{\alpha}}$ and the vector $\boldsymbol{\alpha}^{[i]}$ is row i of the matrix.

(7.4.1) LEMMA. *For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in F^n$, let $\check{\alpha}_j = (a_{1,j}, \ldots, a_{m,j})^\top$ (for $1 \le j \le n$) and $\boldsymbol{\alpha}^{[i]} = (a_{i,1}, a_{i,2}, \ldots, a_{i,n})$ (for $1 \le i \le m$). For $\mathbf{b} = (b_1, \ldots, b_n) \in K^n$,*

$$\boldsymbol{\alpha} \cdot \mathbf{b} = 0 \text{ in } F^n$$

if and only if

$$\boldsymbol{\alpha}^{[i]} \cdot \mathbf{b} = 0 \text{ in } K^n, \text{ for all } 1 \le i \le m\,.$$

PROOF.

$$\begin{array}{rcrcl}
\boldsymbol{\alpha} \cdot \mathbf{b} = 0 & \iff & \sum_{j=1}^n \alpha_j b_j & = & 0 \\
& \iff & \sum_{j=1}^n (\sum_{i=1}^m a_{i,j} e_i) b_j & = & 0 \\
& \iff & \sum_{i=1}^m (\sum_{j=1}^n a_{i,j} b_j) e_i & = & 0 \\
& \iff & \sum_{j=1}^n a_{i,j} b_j & = & 0\,, \text{ for all } i \\
& \iff & \boldsymbol{\alpha}^{[i]} \cdot \mathbf{b} & = & 0\,, \text{ for all } i. \qquad \square
\end{array}$$

Let H be a check (or control) matrix for the code C over F. Thus

$$\mathbf{x} \in C \text{ if and only if } H\mathbf{x}^\top = \mathbf{0}\,.$$

For a vector $\mathbf{b}$ with all its entries from K, we then have

$$\mathbf{b} \in C|_K \text{ if and only if } H\mathbf{b}^\top = \mathbf{0}\,,$$

which, by Lemma 7.4.1, is equivalent to

$$\text{for } \mathbf{b} \in K^n,\ \mathbf{b} \in C|_K \text{ if and only if } \check{H}\mathbf{b}^\top = \mathbf{0}\,.$$

Therefore $\check{H}$ is a control matrix for $C|_K$, as claimed.

(7.4.2) THEOREM. *If C is an $[n,k,d]$ linear code over F, then the subfield subcode $C|_K = C \cap K^n$ is a $[n, k' \geq n - mr, d' \geq d]$ linear code over K, where $r = n - k$.*

PROOF. If $\mathbf{a}, \mathbf{b} \in C|_K$ and $t, s \in K$, then $t\mathbf{a} + s\mathbf{b}$ is in K^n, as all entries are from K, and is in C, since C is linear over $F \geq K$. Therefore $t\mathbf{a} + s\mathbf{b} \in C|_K$, and the subfield subcode is linear.

Clearly $C|_K$ has length n. Since it is contained within the linear code C, we must have $\mathrm{d}_{\min}(C|_K) \geq \mathrm{d}_{\min}(C)$. It remains to verify the bound on its dimension. The redundancy of C is $n-k = r$, and that is the number of rows in a check matrix H for C. We have above constructed from a H a control matrix $\check{H}$ for $C|_K$, having m rows for each row of H. We can get a check matrix for $C|_K$ by discarding any unneeded rows from $\check{H}$. Thus the redundancy of $C|_K$ is at most mr, hence its dimension is at least $n - mr$, as claimed. □

We shall see in the next section that the bounds on dimension and distance in the theorem can be met and can be exceeded.

7.5 Alternant codes

If $\mathrm{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ is a generalized Reed-Solomon code over the field F and K is a subfield of F, then the subfield subcode $K^n \cap \mathrm{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ is an *alternant code*. The code is *strict* if no α_i equals 0. Clearly alternant codes can be decoded as *GRS* codes, but a new type of decoding default is possible—decoding to a codeword in the parent *GRS* code but not in the child alternant code. Recall that the strict generalized Reed-Solomon codes were somewhat easier to decode than those that are not strict.

alternant code
strict

An immediate consequence of Theorem 7.4.2 is

(7.5.1) THEOREM. *The alternant code $K^n \cap \mathrm{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ is an $[n, k', d']$ linear code over K with $k' \geq n - (n-k)m$ and $d' \geq n - k + 1$.* □

In our earlier work on generalized Reed-Solomon codes, the scaling vector $\mathbf{v}$ played little role. It enlarged the family of codes to the point that we could prove, in Theorem 5.1.6, that the dual of a generalized Reed-Solomon codes is also a generalized Reed-Solomon code. Other than that, it has been benign; and in most of our decoding examples we assumed it to be $\mathbf{1}$, the vector of 1's. Now in the study of alternant codes, the scaling vector $\mathbf{v}$ comes to life. Different choices produce different codes.

Let α be a primitive element in the field $\mathbb{F}_{2^m}$, and set

$$\boldsymbol{\alpha} = (1, \alpha, \alpha^2, \ldots, \alpha^j, \ldots, \alpha^{n-1})\,,$$

where $n = 2^m - 1$ is the order of α and the length of the vector $\boldsymbol{\alpha}$. Let $\mathbf{1}$ be the vector of length n consisting of n entries 1. Then by Theorem 5.1.6 and Problem 5.1.5(c) (or direct calculation)

$$\mathrm{GRS}_{n,a}(\boldsymbol{\alpha}, \boldsymbol{\alpha})^{\perp} = \mathrm{GRS}_{n,b}(\boldsymbol{\alpha}, \mathbf{1})$$

whenever $a + b = n$.

We will consider some related subfield subcodes. In doing this, choose as $\mathbb{F}_2$-basis for $\mathbb{F}_{2^m}$ the decreasing powers of α:

$$e_1 = \alpha^{m-1}, \ldots, e_i = \alpha^{m-i}, \ldots, e_m = 1\,.$$

The code $\mathrm{GRS}_{n,n-1}(\boldsymbol{\alpha}, \boldsymbol{\alpha})$ has dimension $n-1$ and minimum distance $2 = n - (n-1) + 1$. It has as check matrix H the canonical generator matrix of its dual $\mathrm{GRS}_{n,1}(\boldsymbol{\alpha}, \mathbf{1})$, a code of dimension 1 spanned by the vector $\mathbf{1}$. Therefore

$$H = \mathbf{1} \text{ and } \check{H} = (\check{1}, \check{1}, \ldots, \check{1})\,,$$

a matrix whose first $m-1$ rows are $\mathbf{0}$ and whose last row is $\mathbf{1}$. The subfield subcode $\mathbb{F}_2^n \cap \mathrm{GRS}_{n,n-1}(\boldsymbol{\alpha}, \boldsymbol{\alpha})$ therefore has, as check matrix, the single vector $\mathbf{1}$ and is revealed as the parity check code of length n, also of minimum distance 2.

On the other hand, the code $\mathrm{GRS}_{n,n-1}(\boldsymbol{\alpha}, \mathbf{1})$ also has dimension $n-1$ and minimum distance 2 but has as check matrix L the canonical generator matrix $\boldsymbol{\alpha}$ of its dual $\mathrm{GRS}_{n,1}(\boldsymbol{\alpha}, \boldsymbol{\alpha})$. We have

$$L = \boldsymbol{\alpha} \text{ and } \check{L} = (\check{1}, \check{\alpha}, \ldots, \check{\alpha}^j, \ldots, \check{\alpha}^{n-1})\,.$$

Now the subfield subcode $\mathbb{F}_2^n \cap \mathrm{GRS}_{n,n-1}(\boldsymbol{\alpha}, \mathbf{1})$ has, as check matrix, the matrix $\check{L}$ in which each nonzero m-tuple appears exactly once as a column $\check{\alpha}^j$, for the appropriate j. The subfield subcode $\mathbb{F}_2^n \cap \mathrm{GRS}_{n,n-1}(\boldsymbol{\alpha}, \mathbf{1})$ is thus seen to be a binary Hamming code.

In summary, the alternant codes

$$\mathbb{F}_2^n \cap \mathrm{GRS}_{n,n-1}(\boldsymbol{\alpha}, \boldsymbol{\alpha}) \text{ and } \mathbb{F}_2^n \cap \mathrm{GRS}_{n,n-1}(\boldsymbol{\alpha}, \mathbf{1})\,,$$

which differ only in the choice of scaling vector $\mathbf{v}$, are very different codes. The first is a parity check code. Its dimension is $n - 1\,(> n - m)$ and minimum distance is 2, meeting the lower bound of Theorem 7.5.1 (and Theorem 7.4.2). The second is a Hamming code. It has dimension $n - m$, meeting the bound of Theorem 7.5.1 (and Theorem 7.4.2), and minimum distance $3\,(> 2)$.

(7.5.2) PROBLEM. *We have shown above that certain binary Hamming codes arise as alternant codes. More generally, prove that all Hamming codes (binary or not) can be realized as alternant codes.*

(7.5.3) PROBLEM. *Prove that extended alternant codes (that is, the subfield subcodes coming from extended generalized Reed-Solomon codes) are strict alternant codes. In particular, all generalized Reed-Solomon codes can be realized as strict alternant codes.*