1. Algebraic Constructions of Codes

We have met already some methods to construct new codes from old ones (puncturing, shortening, etc). We focus now in different methods.

1.1. **Subfield and Trace codes.**

1.1.1. *Subfield subcodes.* Let q be a prime power and C a $[n, k, d]$ code over $\mathbb{F}_{q^m}$. Then

$$C_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$$

is a linear code of length n over $\mathbb{F}_q$ (**HW**).
Given a parity-check matrix H for C, this subcode may be characterized as

$$C_{\mathbb{F}_q} = \{x \in \mathbb{F}_q^n : Hx^t = 0\}.$$

A parity-check matrix for $C_{\mathbb{F}_q}$ is obtained in the following way: let $\mathbb{F}_{q^m} = \mathbb{F}_q[\beta]$; then $1, \beta, \cdots, \beta^{m-1}$ is a basis for $\mathbb{F}_{q^m}$ as a $\mathbb{F}_q$ vector space; each $x \in \mathbb{F}_q[\beta]$ has a unique representation

$$x = \sum_{i=0}^{m-1} x_i \beta i.$$

Replacing each entry $x = \sum_{i=0}^{m-1} x_i \beta^i$ of H by the column vector (x_i), we obtain a $(n-k)m$ by n matrix over $\mathbb{F}_q$. If we eliminate linear dependent rows the resulting matrix is a parity-check matrix for $C_{\mathbb{F}_q}$, because if $c = (c_j) \in C_{\mathbb{F}_q}$ and (x_j) is a row of H, with $x_j = \sum_{i=0}^{m-1} x_{i\,j} \beta^i$,

$$\sum_j x_j c_j = 0 \Leftrightarrow \sum_i \left(\sum_j x_{i\,j} c_j \right) \beta^i = 0 \Leftrightarrow \sum_j x_{i\,j} c_j = 0 \,\forall i.$$

Example 1. *Let $\mathbb{F}_4 = \mathbb{F}_2[\beta]$ with $\beta^2 = \beta + 1$. Recall that the code over $\mathbb{F}_4$ with generator*

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & \beta & \beta \\ 0 & 1 & 0 & \beta & 1 & \beta \\ 0 & 0 & 1 & \beta & \beta & 1 \end{bmatrix}$$

is called the hexacode; it is a $[6, 3, 4]$ code.
Applying the construction described above to the parity-check

$$H = \begin{bmatrix} 1 & \beta & \beta & 1 & 0 & 0 \\ \beta & 1 & \beta & 0 & 1 & 0 \\ \beta & \beta & 1 & 0 & 0 & 1 \end{bmatrix}$$

we obtain first

$$\tilde{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

and

$$H_{\mathbb{F}_2} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

By Gauss-Jordan reduction we find that the subfield subcode of the hexacode has generator

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

ie, it is the $[6, 1, 6]$ *repetition code.*

Example 2. *Let* $\mathbb{F}_{5^2} = \mathbb{F}_5[\beta]$, *where* $\beta^2 = 2$ *and* C *be the* $[8, 4, d]$ *cyclic code over* $\mathbb{F}_{5^2}$ *with generator*

$g(x) = x^4 + (2\beta+4)x^3 + (3\beta+2)x^2 + (\beta+1)x + 2 = (x-\beta)(x-\beta^2)(x-\beta^3)(x-\beta^4).$

We verify that

$$x^8 - 1 = g(x)(x^4 + (3\beta+1)x^3 + (3\beta+2)x^2 + (4\beta+4)x + 2)$$

*and so the dual code is generated by the polynomial (**HW**)*

$$x^4 + +(\beta+1)x^3 + (4\beta+1)x^2 + (4\beta+3)x + 3,$$

which determines the parity-check matrix for C

$$H = \begin{bmatrix} 3 & 4\beta+3 & 4\beta+1 & 2\beta+2 & 1 & 0 & 0 & 0 \\ & & & \cdots & & & & \end{bmatrix}$$

We then obtain

$$\tilde{H} = \begin{bmatrix} 3 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 4 & 4 & 2 & 0 & 0 & 0 & 0 \\ & & & \cdots & & & & \end{bmatrix}$$

and, finally, eliminating row dependencies, the parity-check matrix for $C_{\mathbb{F}_5}$ *is*

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 3 \end{bmatrix}$$

$\mathbb{C}_{F_5}$ *has dimension* 2 *and minimal distance* 6.

Example 3. *Let* $\mathbb{F}_{16} = \mathbb{F}_2[\lambda]$ *where* λ *is a primitive* 5*-root of unity satisfying* $\lambda^4 = \lambda^3 + \lambda^2 + \lambda + 1$.

$$H = \begin{bmatrix} 1 & \lambda & \lambda^2 & \lambda^3 & \lambda^4 \\ 1 & \lambda^2 & \lambda^4 & \lambda & \lambda^3 \end{bmatrix}$$

is a parity-check matrix for the $[5, 3, 3]$ *Reed-Solomon code* C. *We want to determine* $C_{\mathbb{F}_4}$.

We define $\mathbb{F}_4 = \mathbb{F}_2[\beta]$, $\beta^2 = \beta + 1$. $\{1, \lambda\}$ is a basis of $\mathbb{F}_{16}$ over $\mathbb{F}_4$. To compute the parity-check matrix for $C_{\mathbb{F}_4}$ we need the coefficients in this basis for the powers of λ. Putting $\lambda^2 = a + b\lambda$, where $a, b \in \mathbb{F}_4$ are to be determined, we obtain successively

$$\begin{aligned}&\lambda^3 = a\lambda + b\lambda^2 = ab + (a + b^2)\lambda,\\ &\lambda^4 = a^2 + ab^2 + b^3\lambda,\\ &\lambda^5 = ab^3 + (a^2 + ab^2 + b^4)\lambda\end{aligned}$$

But we know (why?) that a and b are not zero, and on the other hand $\lambda^5 = 1$, so the coefficients are determined by

$$\begin{cases} ab^3 = 1 \\ a^2 + ab^2 + b^4 = 0 \end{cases} \Leftrightarrow \begin{cases} a = 1 \\ b^2 + b = 1 \end{cases}$$

We may choose $b = \beta$ or $b = \beta^2 = \beta + 1$. With the first choice,

$$\lambda^2 = 1 + \beta\lambda, \qquad \lambda^3 = \beta + \beta\lambda, \qquad \lambda^4 = \beta + \lambda$$

and

$$\tilde{H} = \begin{bmatrix} 1 & 0 & 1 & \beta & \beta \\ 0 & 1 & \beta & \beta & 1 \\ 1 & 1 & \beta & 0 & \beta \\ 0 & \beta & 1 & 1 & 0 \end{bmatrix}$$

which has already linearly independent rows. The matrix is in fact row equivalent, over $\mathbb{F}_4$, to

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

confirming that $C_{\mathbb{F}_4}$ is the repetition $[5, 1, 5]$ code.

Exercise 4. *Let C be the cyclic code with length 9 over $\mathbb{F}_4$ with generator polynomial $g(x) = \beta^2 + \beta^2 x + x^3 + x^4$.*

a) *Verify that C is a $[9, 5, 3]$ code.*

b) *Find generator and parity-check matrices for the subfield subcode C_{F_2} and determine its dimension and minimal distance.*

Proposition 5. *If C is a $[n, k, d]$ linear code over $\mathbb{F}_{q^m}$ and $C_{\mathbb{F}_q}$ is a $[n, k_q, d_q]$ code,*

a) *$n - m(n - k) \leq k_q \leq k$;*

b) *$d \leq d_q$.*

Proof. (**HW**: Notice that k and k_q are dimensions of spaces over different fields; find bounds for the rank of the parity-check matrix of the subfield subcode). □

The following simple result will be used later:

Proposition 6. *If C has a basis $v_1, \cdots, v_k$ with $v_i \in \mathbb{F}_q^n$, then $v_1, \cdots, v_k$ is also a basis for C_{F_q}.*

Proof. (**HW**). □

Remark 7. *There is no straightforward general formula for d_q in terms of n, k, d, m and q.*

For cyclic codes we may say a bit more:

Proposition 8. *If C is a $[n,k,d]$ cyclic code over $\mathbb{F}_{q^m}$ then $C_{\mathbb{F}_q}$ is also cyclic. Let β be a primitive n-root of unity in $\mathbb{F}_{q^m}$; if C has generator $g(x) = \prod_{l \in L}(x - \beta^l)$, then the generator of $C_{\mathbb{F}_q}$ is $\prod_k (x-\beta^k)$ where k runs through the union of cyclotomic cosets, modulo n and with respect to q, containing L.*

Proof. **HW**. □

Example 9. *Consider the cyclic code $C \subset (\mathbb{F}_{25})^8$ with generator*

$$g(x) = x^4 + (2\beta+4)x^3 + (3\beta+2)x^2 + (\beta+1)x + 2 = (x-\beta)(x-\beta^2)(x-\beta^3)(x-\beta^4)$$

used before.
The cyclotomic cosets modulo 8 *with respect to* 5 *are :* $(0),(1,5),(2),(3,7),(4),(6)$.
So the generator for $C_{\mathbb{F}_5}$ is

$$(x-\beta)(x-\beta^5)(x-\beta^2)(x-\beta^3)(x-\beta^7)(x-\beta^4) = x^6 + 4x^5 + 3x^4 + x^2 + 4x + 3$$

Suppose C is a $[2^m-1,k,d]$ Reed-Solomon code over $\mathbb{F}_{2^m} = \mathbb{F}_2[\beta]$ with β a primitive element. It is a cyclic code with generator polynomial

$$g(x) = \prod_{i=1}^{n-k}(x-\beta^i).$$

Then $C_{\mathbb{F}_2}$ is also a cyclic code whose generator polynomial is the product of the minimal polynomials over $\mathbb{F}_2$ of the β^i $(1 \leq i \leq n-k)$.
Although $C_{\mathbb{F}_2}$ needs not be a Reed-Solomon code, Peterson's decoding algorithm works effectively for the subfield subcode.

Example 10. *Let $\mathbb{F}_{16} = \mathbb{F}_2[\beta]$ with β satisfying $\beta^4 = \beta + 1$ and $k = 9$. C is the Reed Solomon $[15,9,7]$ code over $\mathbb{F}_{16}$*

$$\{(u(\beta^j))_{0 \leq j < 15} : u(x) \in \mathbb{F}_{16}[x] \text{ with degree } < 9\}$$

has generator polynomial

$$g(x) = \prod_{i=1}^{6}(x-\beta^i) = x^6 + \beta^{10}x^5 + \beta^{14}x^4 + \beta^4x^3 + \beta^6x^2 + \beta^9x + \beta^6.$$

The cyclotomic cosets containing $\{1,2,3,4,5,6\}$ are

$$(1,2,4,8),\ (3,6,12,9),\ (5,10)$$

and so, if S denotes the union of these sets, $C_{\mathbb{F}_2}$ has generator polynomial

$$g_2(x) = \prod_{i \in S}(x-\beta^i) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

and $C_{\mathbb{F}_2}$ is a $[15,5,d]$ cyclic code with $d \geq 7$.
Let

$$r(x) = x^2 + x^7 + x^8 + x^9 + x^{10} + x^{11}$$

be a received message. This may be decoded by the error-trapping algorithm for cyclic codes but also by Peterson's algorithm: the syndrome of $r(x)$) with respect to the parity-check matrix of C is $(\beta^{14}, \beta^{13}, \beta^{6}, \beta^{11}, \beta^{5}, \beta^{12})$; the locator polynomial is

$$Q_1(x) = x^3 + \beta^{14}x^2 + \beta^4 x + \beta^7 = (x-1)(x-\beta^{10})(x-\beta^{12}).$$

Assuming the original codeword $c(x)$ belongs to $C_{\mathbb{F}_2}$ we may easily decode as

$$c(x) = 1 + x^2 + x^7 + x^8 + x^9 + x^{11} + x^{12}.$$

*The confirmation that $c(x) \in C$, as well as the details of the computations, are left as an exercise (**HW**).*

1.1.2. *Trace Codes.* Another construction of a code over $\mathbb{F}_q$ from a code C over $\mathbb{F}_{q^m}$ is by means of the trace function

$$Tr : \mathbb{F}_{q^m} \to \mathbb{F}_q, \qquad Tr(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

This definition was considered before, in the case of q prime, but it is direcly applicable to the general case, with the same properties.
Because, given a field $\mathbb{F}_{q^m}$, there is a trace function for each subfield, a more precise notation includes the reference to the two fields ($Tr_{\mathbb{F}_{q^m},\mathbb{F}_q}$ in the case above) but we will not use this notation, unless necessary.
The definition of the trace map for any extension of finite fields is based on the generalization of the Frobenius automorphism. The verification that this generalization has the same properties is left as an exercise.

Example 11. *Consider the fields*

$$\mathbb{F}_{2^6} = \mathbb{F}_2[\alpha],\ \alpha^6 = \alpha^5 + 1, \qquad \mathbb{F}_{2^2} = \mathbb{F}_2[\beta],\ \beta^2 = \beta + 1.$$

In this case we may define

$$Tr : \mathbb{F}_{2^6} \to F_{2^2},\ Tr(x) = x + x^4 + x^{16}.$$

$1, \alpha, \alpha^2$ *is a basis of* $\mathbb{F}_{2^6}$ *over* $\mathbb{F}_{2^2}$*, and we find that*

$$\alpha^3 = \beta + \beta\alpha + \beta^2\alpha^2.$$

So, for example,

$$Tr(\alpha) = \alpha + \alpha^4 + \alpha^{16} = \alpha + 1 + (\beta^2\alpha) + (\beta + \beta\alpha) = \beta^2.$$

The details are left as an exercise.

Extending Tr to $\mathbb{F}_{q^m}^n$ coordinatewise we obtain the **trace code** of C

$$Tr(C) = \{(Tr(c_i)) : (c_i) \in C\}.$$

The properties of the trace map imply that $Tr(C)$ is a linear code of length n. If $\mathbb{F}_{q^m} = \mathbb{F}_q[\beta]$, and G is a generator matrix for C,
$Tr(C)$ is generated by the vectors $Tr(\beta^i c)$ where c is a row of G and $0 \leq i < m$.

Example 12. *The trace code of the hexacode is generated by $Tr(\beta^j v_i)$ where the v_i are a basis of the hexacode and $j \in \{0, 1, 2\}$; for example*

$$Tr(1, 0, 0, 1, \beta, \beta) = (0, 0, 0, 0, 1, 1), \qquad Tr(\beta, 0, 0, \beta, \beta^2, \beta^2) = (1, 0, 0, 1, 1, 1).$$

*It turns out (**HW**) that a generator matrix is*

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

ie, the trace code of the hexacode is the dual of its subfield subcode.

Example 13. *Let C be the $[8,4,5]$ cyclic code over $\mathbb{F}_{5^2}$ with generator matrix*

$$G = \begin{bmatrix} 2 & \beta+1 & 3\beta+2 & 2\beta+4 & 1 & 0 & 0 & 0 \\ & & & \cdots & & & & \end{bmatrix}$$

seen in a example above. We have

$$Tr(1) = 2, Tr(2) = 4, \cdots, Tr(\beta) = \beta + \beta^5 = 0,$$

and so

$$Tr(2 \quad \beta+1 \quad 3\beta+2 \quad 2\beta+4 \quad 1 \quad 0 \quad 0 \quad 0) = (4 \quad 2 \quad 4 \quad 3 \quad 2 \quad 0 \quad 0 \quad 0)$$

Computing $Tr(c)$ and $Tr(\beta c)$ for all the rows c in a basis of C, we find that $Tr(C)$ is a $[8,6,2]$ code.

1.1.3. *Delsarte's Theorem and related results.* Subfield codes and trace codes are intimately related:

Theorem 14 (Delsarte)**.** *If C is a linear code over $\mathbb{F}_{q^m}$ then*

$$\left(C_{\mathbb{F}_q}\right)^{\perp} = Tr\left(C^{\perp}\right).$$

Proof. Suppose $v \in C^{\perp}$ and $x \in C_{\mathbb{F}_q}$; then, because $x \in C$, we have $< x, v > \sum_i x_i v_i = 0$, and so

$$xTr(v) = \sum_i x_i Tr(v_i) = \sum_i Tr(x_i v_i) = Tr(< x, v >) = 0.$$

This shows that $Tr\left(C^{\perp}\right) \subset \left(C_{\mathbb{F}_q}\right)^{\perp}$.
On the other hand

$$Tr\left(C^{\perp}\right) \supset \left(C_{\mathbb{F}_q}\right)^{\perp} \Leftrightarrow \left(Tr\left(C^{\perp}\right)\right)^{\perp} \subset C_{\mathbb{F}_q}.$$

Given $u \in \left(Tr\left(C^{\perp}\right)\right)^{\perp}$, certainly $u \in \mathbb{F}_q^n$, so we must only prove that $u \in C$ or, equivalently, $< u, v >= 0$ for all $v \in C^{\perp}$. To prove this, we must remeber that, because the trace map is not constantly zero (it is in fact surjective), given a nonzero $\lambda \in \mathbb{F}_{q^m}$, there exists some α such that $Tr(\alpha\lambda) \neq 0$ (if $Tr(z) \neq 0$, take $\alpha = z\lambda^{-1}$). Let $v \in C^{\perp}$ and $\alpha \in \mathbb{F}_{q^m}$; $\alpha v \in C^{\perp}$ so

$$0 =< u, Tr(\alpha v) >= \sum_i u_i Tr(\alpha v_i) = \sum_i Tr(u_i \alpha v_i) = Tr(< \alpha u v >).$$

But if $\lambda =< u, v > \neq 0$, there exists some α such that $Tr(\alpha\lambda) \neq 0$, a contradiction. □

We have already seen that passing to a subfield subcode may determine a loss of dimension and consequently of information rate. The next theorem identifies the cases where this does not happen.

Theorem 15. *Let C be a $[n,k]$ linear code over $\mathbb{F}_{q^m}$. Then the following are equivalent:*

1) *C has a basis $\{v_1,\cdots,v_k\}$ with $v_i\in\mathbb{F}_q^n$, for all $i\leq k$.*
2) *$dim_{\mathbb{F}_q}\left(C_{\mathbb{F}_q}\right)=dim_{\mathbb{F}_{q^m}}(C)$;*
3) *$Tr(C)=C_{\mathbb{F}_q}$;*
4) *$C^q=C$, where $C^q=\{(c_i^q)_{i\leq n}:(c_i)_{i\leq n}\in C\}$, ie, the code is invariant under the application (coordinatewise) of the Frobenius automorphism.*

Proof. The proof that 1) and 2) are equivalent is left as an exercise.

Let's see that 1) $\Longrightarrow$ 4): we use the simplified notation $u^q=(u_1^q,\cdots,u_n^q)$; let $\{v_1,\cdots,v_k\}$ be a basis of C with $v_j\in\mathbb{F}_q^n$, for all $j\leq k$; if $c=\sum_{j=1}^k\alpha_jv_j$ then

$$c^q=\left(\sum_{j=1}^k\alpha_jv_j\right)^q=\sum_{j=1}^k\alpha_j^qv_j$$

because the coordinates of the v_i are fixed by Frobenius automorphism; this implies that $c^q\in C$ and that C^q is a subcode of C. But the extension of the Frobenius automorphism to vectors $c\to c^q$ is injective and so $\dim(C^q)=\dim(C)$ and we must have equality.

Next we prove that 4) $\Longrightarrow$ 3): One of the inclusions is true in general: by Delsarte's Theorem, $Tr(C)=\left(C_{\mathbb{F}_q}^{\perp}\right)^{\perp}$, and so (**HW**) $Tr(C)\supset C_{\mathbb{F}_q}$ is true in general.
But if $C^q\subset C$ then for any $c\in C$, $c^{q^j}\in C$ and so

$$Tr(c)=\sum_{j=0}^{m-1}c^{q^j}\in C\cap\mathbb{F}_q^n=C_{\mathbb{F}_q}.$$

Finally, we verify that 3) $\Longrightarrow$ 2). Let $k_q=dim_{\mathbb{F}_q}\left(C_{\mathbb{F}_q}\right)$; as noticed before, we need only show that $k_q\geq k$. If $Tr(C)=C_{\mathbb{F}_q}$,

$$k_q=n-dim_{\mathbb{F}_q}\left(C_{\mathbb{F}_q}\right)^{\perp}=n-dim_{\mathbb{F}_q}\left(C^{\perp}\right)_{\mathbb{F}_q},$$

but

$$dim_{\mathbb{F}_q}\left(C^{\perp}\right)_{\mathbb{F}_q}\leq dim_{\mathbb{F}_{q^m}}C^{\perp}=n-k$$

and so $k_q\geq k$.

□

We observed that for a code with properties $1)-4)$, passing to the subfield subcode does not reduce the information rate. This advantage comes with a price: the minimal distance does not increase:

Corollary 16. *If C is a $[n,k,d]$ code over $\mathbb{F}_{q^m}$ satisfying the conditions in the previous theorem then*

i) $(C_{\mathbb{F}^q})^{\perp} = \left(C^{\perp}\right)_{\mathbb{F}_q}$.

ii) *Any vector $v \in C$ of weight d is a multiple of a $u \in C_{\mathbb{F}_q}$. In particular, $d_q = d$.*

Proof. The proof of i) is left as an exercise (**HW**). Let $v \in C$ have minimal weight d. Then $w(Tr(v)) \leq d$ because $Tr(0) = 0$. But, by Proposition 3, either $w(Tr(v)) = d$ and v and $Tr(v)$ have the same nonzero entries, or $Tr(v) = 0$. By the same reasoning used in the second part of Delsarte's theorem, we may assume that $Tr(v) \neq 0$. Let v_i be a nonzero coordinate of v. Then

$$w(v_i Tr(v) - Tr(v_i)v) < d$$

and so $v = (Tr(v_i))^{-1} v_i Tr(v)$ is a multiple of $Tr(v)$. □

1.2. **Alternant Codes.** The prime subfield subcodes of generalized Reed-Solomon codes are usually called alternant codes: recall that given two sets $\{y_1, \cdots, y_n\}$, $\{\}\alpha_1, \cdots, \alpha_n\}$ of non-zero elements of $\mathbb{F}_{q^m}$, with the α_i distinct,

$$C_{y,\alpha} = \{(y_1 f(\alpha_1), \cdots, y_n f(\alpha_n)) : f \in \mathbb{F}_{q^m}[x] \ \deg(f) < n - r\},$$

is a generalized Reed-Solomon code.
It has a parity-check matrix of the form

$$H = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \\ h_1\alpha_1 & h_2\alpha_2 & \cdots & h_n\alpha_n \\ h_1\alpha_1^2 & h_2\alpha_2^2 & \cdots & h_n\alpha_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ h_1\alpha_1^{r-1} & h_2\alpha_2^{r-1} & \cdots & h_n\alpha_n^{r-1} \end{bmatrix}.$$

Definition 17. *The alternant code $A_{h,\alpha}$ is defined by*

$$A_{h,\alpha} = C_{y,\alpha} \cap \mathbb{F}_q^n.$$

So $A_{h,\alpha}$ consists of all vectors $v \in \mathbb{F}_q^n$ satisfying $Hv = 0$.

We recall that

Proposition 18. *$A_{h,\alpha}$ is a $[n, k, d]$ code with*

$$n - mr \leq k \leq n - r, \qquad d \geq r + 1.$$

Alternant codes constitute a large class of codes with nice properties:

Theorem 19. *Let q be a fixed prime. Given integers n, L and δ, if m is a divisor of $n - L$ satisfying*

$$\sum_{i=1}^{\delta-1} \binom{n}{i} (q-1)^i < (q^m - 1)^{\frac{n-L}{m}},$$

there exists an alternant $[n, k, d]$ code $A_{h,\alpha}$, with $k \geq L$ and $d \geq \delta$.

Before the proof of the theorem, we justify that it implies the existence of asymptotically good families of alternant codes. Recall that

Definition 20. *A family C_n of codes is* ***asymptotically good*** *if it contains a subset C_{n_i} with parameters $[n_i, k_i, d_i]$ satisfying:*

i) $\lim_{i\to+\infty} n_i = +\infty$;
ii) $\liminf_{i\to+\infty} \frac{k_i}{n_i} > 0$;
iii) $\liminf_{i\to+\infty} \frac{d_i}{n_i} > 0$.

*A family is **asymptotically bad** if it does not contain such a subfamily.*

The next exercise, together with the theorem, shows that there exists asymptotically good families of alternant codes:

Exercise 21. *Fix positive constants ε and μ, such that $\varepsilon + \mu < 1$ and a prime q. Show that there exist sequences*

$$n_i, L_i, \delta_i \text{ and } m_i$$

satisfying the condition in the theorem, and such that

$$m_i \mid (n_i - L_i), \frac{L_i}{n_i} \geq \varepsilon, \frac{\delta_i}{n_i} \geq \mu.$$

Proof. Let $a \in \mathbb{F}_q^n$. We estimate the number of generalized Reed-Solomon codes $C_{v,\alpha}$, over $\mathbb{F}_{q^m}$, and for a fixed choice of α, with length n and dimension k_0 (to be chosen later) that contain a: $a \in C_{v,\alpha}$ if there exists a polynomial $f(x)$ with degree less than k_0 satisfying

$$f(\alpha_i) = \frac{a_i}{v_i};$$

we may define f by choosing the v_i for $1 \leq i \leq k_0$; the remaining v_i are then determined by that condition. So there are $(q^m - 1)^{k_0}$ choices of v.
This means that there are at most $(q^m - 1)^{k_0}$ alternant codes $A_{h,\alpha}$ that are subcodes of those $C_{v,\alpha}$ and so contain a. Moreover, the dimension k of $A_{h,\alpha}$ will satisfy

$$k \geq n - m(n - k_0);$$

so if we choose $k_0 = n - \frac{n-L}{m}$ we get the desired lower bound on k.
We now let a take all possible values of vectors with weight less than δ, and conclude that the number of alternant codes with length n, dimension $k \geq L$ and minimal distance $d < \delta$, that are subcodes of some $C_{v,\alpha}$ over $\mathbb{F}_{q^m}$ is bounded above by

$$(q^m - 1)^{n - \frac{n-L}{m}} \sum_{i=1}^{\delta-1} \binom{n}{i} (q-1)^i.$$

But the total number of generalized Reed-Solomon codes (always with fixed n, k_0 and α) is $(q^m - 1)^n$, ie, the number of possible v. So, if the inequality in the theorem is satisfied, there is some alternant code with minimal distance $d \geq \delta$. □

1.3. **Decoding of alternant codes: the GCD algorithm.** The extended Euclidean algorithm applied to polynomials provides an efficient decoding algorithm for alternant codes, that may also be applied to the original Reed-Solomon codes. We review briefly the properties of the Euclidean algorithm in this special case.

Let $\mathbb{F}$ denote any field and $f(x), g(x) \in \mathbb{F}[x]$ two polynomials. Recall the contents of Lemma 9 and 10 from Notes VII:

1 - The division algorithm defines the sequence

$$r_{-1}(x) = f(x),\ r_0(x) = g(x), \qquad r_k(x) = r_{k-2}(x) - q_k(x) r_{k-1}(x);$$

so r_k is the remainder of division of r_{k-2} by r_{k-1}.

2 - the monic multiple of the last non-zero r_k is the greatest common divisor of $f(x)$ and $g(x)$;

3 - the sequences

$$a_{-1}(x) = 1,\ a_0(x) = 0, \qquad a_k(x) = a_{k-2}(x) - q_k(x) a_{k-1}(x),$$

and

$$b_{-1}(x) = 0,\ b_0(x) = 1, \qquad b_k(x) = b_{k-2}(x) - q_k(x) b_{k-1}(x),$$

satisfy

$$r_k(x) = a_k(x) f(x) + b_k(x) g(x).$$

4 - Moreover, for $k \geq 1$,

$$\deg a_k(x) = \sum_{i=2}^{k} \deg q_i(x), \qquad \deg b_k(x) = \sum_{i=1}^{k} \deg q_i(x),$$

and

$$\deg r_k(x) = \deg f(x) - \sum_{i=1}^{k+1} \deg q_i(x).$$

5 -

$$a_k(x) b_{k+1}(x) - a_{k+1}(x) b_k(x) = (-1)^{k+1};$$

in particular $a_k(x)$ and $b_k(x)$ are co-prime;

6 -

$$r_k(x) b_{k+1}(x) - r_{k+1}(x) b_k(x) = (-1)^{k+1} f(x); \qquad r_{k+1}(x) a_k(x) - r_k(x) a_{k+1}(x) = (-1)^{k+1} g(x).$$

Let $A_{h,\alpha}$ be an alternant code with parity-check matrix (over $\mathbb{F}_{q^m}$)

$$H = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \\ h_1\alpha_1 & h_2\alpha_2 & \cdots & h_n\alpha_n \\ h_1\alpha_1^2 & h_2\alpha_2^2 & \cdots & h_n\alpha_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ h_1\alpha_1^{r-1} & h_2\alpha_2^{r-1} & \cdots & h_n\alpha_n^{r-1} \end{bmatrix}.$$

We assume r is even and that $t \leq r/2$ errors occur in the transmission of a codeword. Suppose the error e has non-zero entries $e_{i_1}, \cdots, e_{i_t}$ in the positions $\alpha_{i_1}, \cdots, \alpha_{i_t}$. The syndrome of e is $(s_0, \cdots, s_{r-1}) = eH^T$, where

$$s_l = \sum_{j=1}^{t} h_{i_j} e_{i_j} \alpha_{i_j}^l.$$

The **syndrome polynomial** is $S(x) = \sum_{l=0}^{r-1} s_l x^l$.

Definition 22. *The* ***error locator polynomial*** *associated with* e *is*

$$\sigma(x) = \prod_{j=1}^{t} (1 - \alpha_{i_j} x).$$

The roots of $\sigma(x)$ *are the inverses of the locations* α_{i_j} *of the non-zero error coordinates.*

We have also

Definition 23. *The* ***error evaluator polynomial*** *is*

$$\omega(x) = \sum_{j=1}^{t} h_{i_j} e_{i_j} \prod_{u \neq j} (1 - \alpha_{i_u} x) = \sum_{j=1}^{t} h_{i_j} e_{i_j} \frac{\sigma(x)}{1 - \alpha_{i_j} x)}.$$

The name is justified by the following computation (**HW**):

$$\omega(\alpha_{i_j}^{-1}) = h_{i_j} e_{i_j} \prod_{u \neq j} (1 - \alpha_{i_u} \alpha_{i_j}^{-1}),$$

ie,

$$e_{i_j} = \frac{\omega(\alpha_{i_j}^{-1})}{h_{i_j} \prod_{u \neq j} (1 - \alpha_{i_u} \alpha_{i_j}^{-1})}.$$

Of course, these polynomials depend on unknown data. However, we will see that it is possible to determine them in a indirect way. The starting point is

Lemma 24.

$$x^r \mid (\omega(x) - \sigma(x) S(x)).$$

Proof. (**HW**). □

This implies that there exists $\theta(x)$ such that

$$\omega(x) = \theta(x) x^r + \sigma(x) S(x),$$

and we are lead to apply the Euclidean algorithm to x^r and $S(x)$ to get $\omega(x)$ from one of the remainders $r_k(x)$.

Let $r_k(x) = a_k(x) x^r + b_k(x) S(x)$ be the first remainder satisfying $\deg(r_k(x)) < r/2$; the properties on the degrees of the $b_i(x)$ stated above imply (**HW**) that then $\deg(b_k(x)) \leq r/2$.
We have then

$$\begin{cases} \omega(x) = \theta(x) x^r + \sigma(x) S(x) \\ r_k(x) = a_k(x) x^r + b_k(x) S(x) \end{cases}$$

and so

$$b_k(x)\omega(x) - r_k(x)\sigma(x) = (b_k(x)\theta(x) - a_k(x)\sigma(x))\, x^r.$$

But the degree on the left side is strictly less than r and so

$$b_k(x)\omega(x) = r_k(x)\sigma(x), \qquad b_k(x)\theta(x) = a_k(x)\sigma(x).$$

As $a_k(x)$ and $b_k(x)$ are co-prime, the second equality implies (**HW**) that $b_k \mid \sigma(x)$.
But $\omega(x)$ and $\sigma(x)$ are also co-prime, as they have no roots in common in any

extension of $\mathbb{F}_{q^m}$. So, by the same reasoning, the first equality implies $\sigma(x) \mid b_k(x)$. So we finally have (**HW**)

$$\sigma(x) = b_k(0)^{-1} b_k(x).$$

The first equality above gives

$$\omega(x) = b_k(0)^{-1} r_k(x).$$

The details of the following example are left as a possible homework (**HW**)

Example 25. *Consider the* $[8,4,5]$ *Reed-Solomon code over* $\mathbb{F}_9 = \mathbb{F}_3[\beta]$*, where* β *satisfies* $\beta^2 = \beta + 1$*, with parity-check matrix*

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 \\ 1 & \beta^2 & \beta^4 & \beta^6 & 1 & \beta^2 & \beta^4 & \beta^6 \\ 1 & \beta^3 & \beta^6 & \beta & \beta^4 & \beta^7 & \beta^2 & \beta^5 \\ 1 & \beta^4 & 1 & \beta^4 & 1 & \beta^4 & 1 & \beta^4 \end{bmatrix}$$

Notice that, with the notation used in the discussion of the algorithm,

$$h_j = \alpha_j = \beta^{j-1}$$

and $r = 4$.
Suppose that the following output is received after a transmission of a codeword from the alternant code over $\mathbb{F}_3$ *determined by this parity-check matrix*

$$u = (2,0,1,0,0,1,2,0);$$

its syndrome is $(\beta^2, \beta, \beta^6, 1)$*; applying the extended Euclidean algorithm to* x^4 *and* $S(x) = x^3 + \beta^6 x^2 + \beta x + \beta^2$ *we find that the first* $r_k(x)$ *with degree less than* $r/2 = 2$*, and the corresponding* $a_k(x)$ *and* $b_k(x)$*, are*

$$r_2(x) = \beta^7, \qquad a_2(x) = \beta^6 x + \beta^4, \qquad b_2(x) = \beta^2 x^2 + x + \beta^5,$$

and so

$$\sigma(x) = \beta^5 x^2 + \beta^3 x + 1, \omega(x) = \beta^2.$$

Finding the zeros of $\sigma(x)$ *we get* $\sigma(x) = (1 - \beta x)(1 - \beta^4 x)$*, ie, the errors are in the second and fifth positions. Computing*

$$(0,a,0,0,b,0,0,0)H^T = (\beta^2, \beta, \beta^6, 1),$$

with $a, b \in \mathbb{F}_3$*, we find that the error pattern is* $e = (0,1,0,0,2,0,0,0)$*. It would also be possible to use the evaluator polynomial to compute, following the notation used in the discussion of the algorithm,*

$$e_2 = \beta^2 \left(\beta(1 - \beta^4 \beta^7)\right)^{-1} = 1, \qquad e_5 = \beta^2 \left(\beta^4(1 - \beta\beta^4)\right)^{-1} = 2.$$

1.4. **Concatenation.** The next construction is based not on one but two codes and is the basis of some of the best block codes known.
Let A be a $[N,K,D]$ code over $\mathbb{F}_{q^m}$ and B a $[n,m,d]$ code over $\mathbb{F}_q$. Identifying $\mathbb{F}_{q^m} = \mathbb{F}_q[\beta]$, we have a canonical mapping

$$\phi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m, \qquad \phi(\sum_{i=0}^{m-1} x_i \beta^i) = (x_i)_{0 \le i < m}.$$

This mapping may be extended coordinatewise (with the same denomination) to a mapping

$$\phi : (\mathbb{F}_{q^m})^N \to (\mathbb{F}_q)^{mN}.$$

On the other hand, given a basis $v_0, \cdots, v_{m-1}$ of B we have the isomorphism

$$\tau : \mathbb{F}_q^m \to B, \qquad \tau((x_i)) = \sum_{i=}^{m-1} x_i v_i.$$

We thus have a bijective $\mathbb{F}_q$-linear map

$$\tau \circ \phi : (\mathbb{F}_{q^m})^N \to B^N,$$

where B^N denotes the direct product of N copies of B.

Definition 26. *Under the above conditions, the image $A[B] = \tau \circ \phi(A)$ is called the **concatenation** of A with B. A is called the **outer code** and B the **inner code**.*

Example 27. *Let*

$$A = \{(0,0), (1,\beta), (\beta, 1+\beta), (1+\beta, 1)\},$$

a $[2,1,2]$ code over $\mathbb{F}_2[\beta]$, and

$$B = \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}$$

a $[3,2,2]$ code over $\mathbb{F}_2$.
With $\phi : \mathbb{F}_2[\beta] \to B$ defined by

$$\phi(0) = (0,0,0),\ \phi(1) = (1,1,0),\ \phi(\beta) = (1,0,1),\ \phi(1+\beta) = (0,1,1),$$

the concatenation of A with B is

$$A[B] = \{(0,0,0,0,0,0), (1,1,0,1,0,1), (1,1,0,0,1,1), (0,1,1,1,1,0)\},$$

which is a $[6,2,4]$ code.

Proposition 28. *$A[B]$ has length nN, dimension mK and minimal distance at least dD.*

Proof. (**HW**). □

1.4.1. *Encoding.* From the definition, we see that $A[B]$ receives an input vector $v \in \mathbb{F}_q^{mK}$ and encodes it as $u \in \mathbb{F}_q^{nN}$:

- v is broken into blocks $u_1, \cdots, u_K$ of length m;
- each u_i is then identified with an element of $\mathbb{F}_{q^m}$ by ϕ^{-1} resulting in a vector from $\mathbb{F}_{q^m}^K$, which is then encoded by A;
- the image of this outer encoding is then transformed by ϕ in a vector from $\mathbb{F}_q^{Nm}$ which is in its turn broken into N blocks of length m;
- each one of these blocks is encoded by B into a length n codeword, producing a concatenated string of length nN.

This may be summarized in the diagram

$$\begin{tikzcd}
v \in \mathbb{F}_q^{mK} \arrow[r] & (u_1, \cdots, u_K) \in \left(\mathbb{F}_q^m\right)^K \arrow[d, "\phi^{-1}"] \\
(\tau_1, \cdots, \tau_N) \in \left(\mathbb{F}_{q^m}\right)^N \arrow[d, "\phi"'] & (\alpha_1, \cdots, \alpha_K) \in \left(\mathbb{F}_{q^m}\right)^K \arrow[l, "A"'] \\
(a_1, \cdots, a_N) \in \left(\mathbb{F}_q^m\right)^N \arrow[r, "B"'] & (b_1, \cdots, b_N) \in \left(\mathbb{F}_q^n\right)^N
\end{tikzcd}$$

The computational details of the following example are left as an exercise (**HW**):

Example 29. *We construct the concatenated code $A[B]$ where A is the $[5, 3, 3]$ Reed-Solomon code over $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ (whit α satisfying $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$) with generator matrix*

$$G_A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha & \alpha^3 \end{bmatrix},$$

and B is the binary $[7, 4, 3]$ Hamming code with generator matrix

$$G_B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

We start by seeing an example of encoding:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \to (0010 \quad 1101 \quad 0110)$$

$$\xrightarrow[\phi^{-1}]{} (\alpha^2 \quad 1 + \alpha + \alpha^3 \quad \alpha + \alpha^2)$$

$$\xrightarrow[A]{} (1 + \alpha^3 \quad \alpha + \alpha^3 \quad \alpha + \alpha^3 \quad 1 + \alpha + \alpha^3 \quad \alpha + \alpha^2)$$

$$\xrightarrow[\phi]{} (1001 \quad 0101 \quad 0101 \quad 1101 \quad 0110)$$

$$\xrightarrow[B]{} (1001100 \quad 0101010 \quad 0101010 \quad 1101001 \quad 0110011)$$

1.4.2. *Concatenated decoding.* The structure of concatenated codes allows a decoding procedure that follows the reverse path:

- a message of length nN is broken into blocks of length n, each one of which is decoded, under B, into a length m vector;
- applying ϕ^{-1}, a vector from $\mathbb{F}_{q^m}^N$ is obtained and decoded by A into a vector from $\mathbb{F}_{q^m}^K$;
- this is transformed by ϕ into a message from $\mathbb{F}_q^{mK}$.

It should be noted that this decoding strategy may allow to correct more errors than established by the minimal distance but it may also fail to decode correctly error patterns with weight below $(d-1)/2$, depending on the way that the errors are distributed. It turns out, however, that in many cases this failure may be overcome.

We use the same code as above to exemplify and discuss the concatenated decoding procedure: let

$$r = (1110101 \quad 1111110 \quad 0111001 \quad 0110011 \quad 1100110)$$

be the output, already written in block form.
The parity-check matrix

$$H_B = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

gives the vector of syndromes

$$(101 \quad 001 \quad 101 \quad 000 \quad 000)$$

leading to the corrected codeword

$$c = (1010101 \quad 1111111 \quad 0011001 \quad 0110011 \quad 1100110).$$

c is the encoding of $(1010 \quad 1111 \quad 0011 \quad 0110 \quad 1100)$

$$\xrightarrow[\phi^{-1}]{} (1+\alpha^2 \quad \alpha^4 \quad \alpha^2+\alpha^3 \quad \alpha+\alpha^2 \quad 1+\alpha).$$

which we now decode using Peterson's algorithm. Computing the syndrom we obtain the matrix

$$D(r) = [\alpha+\alpha^3 \quad \alpha+\alpha^3]$$

and identify the locator polynomial $Q_1(x) = 1+x$ showing that we have an error in the first coordinate.
We could correct the error by syndrome decoding; instead, we compute the polynomial
$Q_0(x) = 1+\alpha^3+(\alpha^2+\alpha^3)x+(\alpha+\alpha)x^2+(1+\alpha)x^3$ and find that the input for A is

$$-\frac{Q_0(x)}{Q_1(x)} = 1+\alpha^3+(1+\alpha^2)x+(1+\alpha)x^2,$$

which corresponds to the original input $u \in \mathbb{F}_2^{12}$

$$u = (\ 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0\ ),$$

which was encoded to

$$c = (1111111 \quad 1111111 \quad 0011001 \quad 0110011 \quad 1100110).$$

We find that there were 2 errors in the first block and 1 error in the second and third blocks; the decoding for the Hamming code corrected these last two errors but gave a wrong answer in the correction of the first block; however the decoding for A fixed this problem.
It is clear that concatenated decoding would have succeeded in correcting an error pattern with weight up to 11, if all but one of the blocks had at most one error, with the remaining ones concentrated in the remaining block.

On the other hand, suppose, for simplicity, that the zero codeword is sent and

$$r = (1100000 \quad 1000010 \quad 0000000 \quad 0000000 \quad 0000000)$$

is received. The syndromes are then

$$(110 \quad 001 \quad 000 \quad 000 \quad 000)$$

leading to the (wrong) decoding

$$r = (1110000 \quad 1000011 \quad 0000000 \quad 0000000 \quad 0000000),$$

which would be the result of encoding the outer output $(1+\alpha+\alpha^2 \quad 1 \quad 0 \quad 0 \quad 0)$.

Application of Peterson's algorithm would lead to a locator polynomial with no roots of the form α^j for $0 \leq j < 5$, and thus to a failure in decoding. This happened because A has minimal distance 3 while the error pattern resulting from the inner decoding has weight 2.
However, we know that there are errors in the first two blocks. If we take those to be erasures we could correct them. In fact, in our case things are even simpler: A is a MDS code and so any three coordinates are an information set, ie, they determine the remaining coordinates.

We end with an example where inner decoding fails to decode (correctly or not) the output.

Example 30. *We take as outer code A the hexacode, a $[6,3,4]$ code over $\mathbb{F}_4 = \mathbb{F}_2[\beta]$ where $\beta^2 = \beta + 1$; it has generator matrix*

$$G_A = \begin{bmatrix} 1 & 0 & 0 & 1 & \beta & \beta \\ 0 & 1 & 0 & \beta & 1 & \beta \\ 0 & 0 & 1 & \beta & \beta & 1 \end{bmatrix}.$$

As inner code B we use the binary code with generator

$$G_B = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

The concatenation is thus a $[30,6,12]$ binary code. The ϕ mapping is in this case

$$\phi(0) = (00), \qquad \phi(1) = (10), \qquad \phi(\beta) = (01), \qquad \phi(\beta^2) = (11).$$

Suppose the received message is

$$r = (\ 01110 \quad 01010 \quad 01101 \quad 11110 \quad 00000 \quad 11111\ )$$

The inner decoding gives

$$(\ 11110 \quad ? \quad 01101 \quad 11110 \quad 00000 \quad 11110\ );$$

in the second block, the syndrome has two different coset leaders, both with weight 2, that would lead either to 11110 *or to* 00000 *as decoded vector; at this stage, there is no reason to choose one or the other and we will follow both paths: $(\tau \circ \phi)^{-1}$ produces, in each case, the $\mathbb{F}_4^6$ vectors*

$$(\beta^2\,\beta^2\,\beta\,\beta^2\,0\,\beta^2) \text{ or } (\beta^2\,0\,\beta\,\beta^2\,0\,\beta^2).$$

In the first case the syndrome is $(\beta^2\,1\,1)$ *which has unique coset leader* $(\beta^2\,0\,0\,0\,0\,0)$ *leading to the codeword (with respect to the outer code)*

$$(0\,\beta^2\,\beta\,\beta^2\,0\,\beta^2)$$

and so to the original message (001101110011).
However, in the second case the syndrome is $(\beta^2\,\beta\,0)$ *which has two coset leaders*

$$(0\,0\,0\,\beta^2\,\beta\,0), \qquad (0\,\beta\,0\,0\,0\,\beta^2).$$

We are naturally led to choose the first decoding.

The crucial observation that explains what is happening is that r *has two codewords at the same distance in* B^6 *but not in its subcode* $A[B]$.

1.4.3. *Burst error correction.* The simplest nontrivial case of concatenation may be the one where the inner code is a trivial $[m, m, 1]$ code over $\mathbb{F}_q$ and the outer code is for instance a Reed-Solomon code over $\mathbb{F}_{q^m}$. Recall that this last one is a MDS code, ie, it satisfies Singleton upper bound $d = n-k+1$. It should be noticed that in this special case, illustrated in the example below, we have $n = m$ and the decoding by B is trivial, since all vectors are codewords.

This concatenation is a $[nm, km, d]$ code particularly useful for burst correction: suppose a nm length message r is received; this is broken into a sequence of m length messages mapped by ϕ^{-1} into a n length message to be decoded. Suppose r contains a b-burst; the burst affects at most $a = \lfloor b/m \rfloor + 2$ of the n blocks. This means that the concatenated code corrects b-bursts for $b \leq (t-2)m$ where $t = \lfloor \frac{d-1}{2} \rfloor$, even if it corrects only up to t random errors.

The details of the following example are again left as an exercise (**HW**):

Example 31. *Let* C *be the concatenation of the Reed-Solomon* $[15, 9, 7]$ *code over* $\mathbb{F}_{16} = \mathbb{F}_2[\beta]$ *with* $\beta^4 = \beta + 1$*, and the* $[4, 4, 1]$ *code over* $\mathbb{F}_2$*. The concatenation is defined by*

$$\phi(x_0 + x_1\beta + x_2\beta^2 + x_3\beta^3) = (x_0, x_1, x_2, x_3).$$

Let r *be the received message (presented in "broken" form)*

(1000 0100 1001 0110 1011 1000 1100 1010 1010 0011 1110 1010 1101 0001 0100),

mapped by ϕ^{-1} *to*

$$(1, \beta, \beta^{14}, \beta^5, \beta^{13}, 1, \beta^4, \beta^8, \beta^8, \beta^6, \beta^{10}, \beta^8, \beta^7, \beta^3, \beta).$$

The syndrome gives origin to the matrix

$$\begin{bmatrix} 0 & \beta^{12} & \beta^4 & \beta^6 \\ \beta^{12} & \beta^4 & \beta^6 & \beta^{13} \\ \beta^4 & \beta^6 & \beta^{13} & \beta^4 \end{bmatrix}$$

and from it the locator polynomial

$$Q_1(x) = \beta^{12} + \beta^7 x + \beta^8 x^2 + x^3 = (x-1)(x-\beta^{13})(x-\beta^{14}).$$

The coset leader associated with the given syndrome is then

$$e(x) = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \beta^{13}, \beta^3)$$

and $\phi^{-1}(r)$ *is decoded into*

$$(0, \beta, \beta^{14}, \beta^5, \beta^{13}, 1, \beta^4, \beta^8, \beta^8, \beta^6, \beta^{10}, \beta^8, \beta^7, \beta^{12}, \beta^{14}),$$

corresponding to

(0000 0100 1001 0110 1011 1000 1100 1010 1010 0011 1110 1010 1101 1111 1001).

The error is thus a 9 *burst.*

1.4.4. *Interleaving.* We take the opportunity to refer briefly another code construction of a more combinatorial nature, which is also frequently applied to burst correction.
Let C be a $[n, k]$, b-burst error correcting, code over $\mathbb{F}$ and fix $t > 1$.
The interleaving to depth t of C, denoted $I(C, t)$, is a $[nt, kt]$ code constructed in the following way: each t-tuple $(x_1, x_1, \cdots, x_t) \in \left(\mathbb{F}^k\right)^t$ is encoded by C as the rows of the matrix

$$\to \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ & & \vdots & \\ c_{t1} & c_{t2} & \cdots & c_{tn} \end{bmatrix},$$

so, for each $i \leq t$, $(c_{i1} \quad c_{i2} \quad \cdots \quad c_{in}) = x_i G \in C$. The entries of the matrix are then read by columns, creating the codeword of $I(C, t)$

$$(\ c_{11} \quad c_{21} \quad \cdots \quad c_{t1} \quad c_{12} \quad c_{22} \quad \cdots \quad c_{t2} \quad \cdots \quad \cdots \quad c_{1n} \quad c_{2n} \quad \cdots \quad c_{tn}\ )$$

Proposition 32. $I(C, t)$ *is tb-burst error correcting.*

Proof. **HW**. □

1.5. **Good Concatenated Codes.** In this section we present a family of codes, constructed by concatenation, with asimptotically good parameters, the Justensen codes. We'll consider only the binary version.
The starting point for the definition of this family of codes is a simple idea that leads, pottentialy, to good codes.

1.5.1. *Good binary codes with* $R = 1/2$. Fix $m > 1$ and let C_α be the $[2, 1, 2]$ code over $\mathbb{F}_{2^m}$

$$C_\alpha = \{(a, \alpha a) : a \in \mathbb{F}_{2^m}\},$$

where $\alpha \in \mathbb{F}_{2^m}$ is to be chosen. We notice that any non-zero element $(a, \alpha a)$ determines the constant α.
Given a presentation of the field as $\mathbb{F}_{2^m} = \mathbb{F}_2[\beta]$, we may obtain a $[2m, m, d]$ binary code, using the vector space isomorphism

$$\phi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m, \qquad \phi(\sum_{i=0}^{m-1} x_i \beta^i) = (x_i)_{0 \leq i < m};$$

the result can be seen as concatenation of C_α with the trivial binary code with length m, ie, $\mathbb{F}_2^m$, and so we will denote the binary code obtained in this way as $\mathbb{C}_\alpha[\mathbb{F}_2^m]$.
Let $\varepsilon < 0.5$. We will bound the number of codes $\mathbb{C}_\alpha[\mathbb{F}_2^m]$ containing a non-zero codeword with weight less than $2m\varepsilon$: assuming the worst case scenario, that all possible non-zero binary words with length $2m$ and weight less than $2m\varepsilon$ occur as codewords in distinct codes, we see that there would be at most $\sum_{1\leq i<2m\varepsilon}\binom{2m}{i}$ choices of α that lead to a code with minimal distance $d < 2m\varepsilon$.
We have the following

Lemma 33. *If $\varepsilon < 0.5$,*

$$\sum_{0\leq i<n\varepsilon}\binom{n}{i} \leq 2^{nH_2(\varepsilon)}.$$

Proof. (**HW**): notice that, for any $r > 0$,

$$2^{-rn\varepsilon}\sum_{1\leq i<n\varepsilon}\binom{n}{i} \leq \sum_{1\leq i<n\varepsilon} 2^{-ri}\binom{n}{i},$$

which, extending the sum to $0 \leq i \leq n$, is bounded above by $(1+2^{-r})^n$.
Choose $r = \log_2\left(\frac{1-\varepsilon}{\varepsilon}\right)$. □

If we take $0 < \varepsilon < 0.5$ satisfying $H_2(\varepsilon) < 1/4$ we have $2^{2mH_2(\varepsilon)} < 2^m - 1$ and so conclude that there is some $\alpha \in \mathbb{F}_{2^m}$ such that the code $\mathbb{C}_\alpha[\mathbb{F}_2^m]$ has minimal distance $d \geq 2m\varepsilon$. This shows that there is a family C_m of $[2m, m, d_m]$ binary codes such that $\liminf_m \frac{d_m}{2m} \geq \varepsilon > 0$.

This is a good family of codes, in asymptotic terms, although the individual codes in the family might be overshadowed by other codes with the same length and dimension.
But the main drawback of this nice idea is that it is non-constructive: we don't know how to choose a sequence of values of m for which there is an accessible way of determining the desired α. The way out of this difficulty found by Justensen is at the same time ingenious and simple: choose all the $\alpha \in \mathbb{F}_{2^m}$.

1.5.2. *Justensen codes.* The construction of Justensen codes is by concatenation, using as external code a $[N, K, D]$ Reed-Solomon code over $\mathbb{F}_{2^m}$, with $N = 2^m - 1$. The dimension K is chosen later. Recall that the code is

$$\{(f(x_1), f(x_2), \cdots, f(x_N)) : f \in \mathbb{F}_{2^m}[x]; \deg(f) < K\},$$

where the x_i enumerate all non-zero elements of the field.
Each entry $f(x_i)$ is then replaced by the block $(u_i, v_i) = (\phi(f(x_i)), \phi(x_i f(x_i))) \in \mathbb{F}_2^{2m}$, where ϕ is the isomorphism between $\mathbb{F}_{2^m}$ and $\mathbb{F}_2^m$ determined by some fixed choice of basis.
This construction results in a $[2m(2^m-1), mK, d_m]$ binary code with rate

$$R_m = \frac{K}{2(2^m-1)}.$$

To attain a good estimate on the minimal distance d_m and foremost on its asymptotic behaviour with m, we fix $R < 0.5$, independent of m, and choose K to be the minimum integer such that $R_m \geq R$, ie, we choose K to be the integer in the interval $[2(2^m-1)R, 2(2^m-1)R+1[$.

In each codeword there are at least $D = N - K + 1$ non-zero blocks (u_i, v_i) and these are all distinct.

The choice of K gives $D > (2^m - 1)(1 - 2R)$. And, given $0 < \varepsilon < 0.5$, the number of blocks with weight less than $2m\varepsilon$ in a nonzero codeword c is bounded above by $2^{2mH_2(\varepsilon)}$.
This implies that the weight of c satisfies

$$w(c) \geq \left((2^m - 1)(1 - 2R) - 2^{2mH_2(\varepsilon)}\right) 2m\varepsilon.$$

Choosing ε by $H_2(\varepsilon) = 1/2 - \frac{1}{\log_2(2m)}$, we have that ε is bounded away from zero, if we take $m > 2$. On the other hand, this choice implies (**HW**) that there is a positive constant C such that, for sufficiently large m,

$$w(c) \geq C2m(2^m - 1),$$

ie, $\frac{d_m}{2m(2^m-1)} > C$.
So Justensen codes constitute a good family of codes.

Remark 34. *For a concrete description of such a family, it is useful to know that there exist sequences of* m *for which the construction of the field extension is known: for example, taking* $m = 2 \times 3^j$*, the polynomial* $p(x) = x^m + x^{m/2} + 1$ *is irreducible over* $\mathbb{F}_2$.

On the other hand, the definition of the Reed-Solomon code is usually done putting $x_i = \lambda^{i-1}$*, for a primitive root of the extension field. This may lead to complicated computations, dependent on* m*. An alternative to this choice is the following: if* $\mathbb{F}_{2^m} = \mathbb{F}_2[\beta]$*, writing each* $1 \leq t \leq N$ *in binary form*

$$t = \sum_{i=0}^{m-1} r_i(t)2^i,$$

we may define

$$x_i = \sum_{i=0}^{m-1} r_i(t)\beta^i.$$

Justensen codes have, for large m, information rates below 0.5, but by puncturing adequately it is possible to define good families of codes with informations rates above 0.5.

1.6. **Supplementary Results and Problems.**

Exercise 35. *Let* A *be the Reed-Solomon code over* $\mathbb{F}_{3^2}$ *defined by*

$$C = \{(f(1), f(\lambda), \cdots, f(\lambda^7)) : f(x) \in P_4 \subset \mathbb{F}_{3^2}[x]\}$$

where λ *is a primitive* 8*-root of unity satisfying* $\lambda^2 = \lambda + 1$*, and* P_4 *denotes as usual the vector space of polynomials with degree less than* 4.

a) *Determine the dimension and minimal distance of the trace code* $Tr(A) \subset \mathbb{F}_3^8$.

b) *Let B be the $[4,2,3]$ code over F_3 with generator matrix*

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{bmatrix}.$$

Decode the following output from the concatenated code $A[B]$, using syndrome decoding for B and Peterson's algorithm or the GCD algorithm for A:

$$(2001 \quad 2201 \quad 2110 \quad 1002 \quad 1001 \quad 1011 \quad 0010 \quad 1011).$$

c) *Prove that the concatenated decoding algorithm used in b) corrects all errors with weight $w < 6$, but that there are errors with weight 6 that are not corrected. Prove also that the algorithm successfully decodes any burst with length $l < 8$.*

Exercise 36. *Consider the Reed-Solomon code A over $\mathbb{F}_2[\beta]$, where $\beta^3 = \beta + 1$,*

$$C = \{(f(1), f(\beta), \cdots, f(\beta^6)) : f(x) \in P_3[x]\}.$$

a) *Find the dimension of the subfield subcode $A_{\mathbb{F}_2}$.*

b) *The code C is the concatenation of A with the inner code B that has generator matrix*

$$G_B = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Apply the algorithm for decoding of concatenated codes to decode the output

$$r = (000000 \quad 010110 \quad 000100 \quad 100010 \quad 101111 \quad 010110 \quad 101101).$$