1. Reed-Solomon Codes

We consider now an important class of linear codes: let $\mathbb{F} = \mathbb{F}_{q^m}$ be a finite field. We fix $n \mid (q^m - 1)$, $k < n$ and $\mathbf{x} = (x_0, \cdots, x_{n-1}) \in \mathbb{F}^n$, where the x_i are nonzero and distinct. Let

$$P_k = \{f(x) \in \mathbb{F}[x] : \deg(f) < k\}.$$

We take as source messages the vectors $(a_0, \cdots, a_{k-1}) \in \mathbb{F}^k$, which are identified with polynomials:

$$(a_0, \cdots, a_{k-1}) \to f(x) = \sum_{i=0}^{k-1} a_i x^i.$$

The message is then encoded as

$$f(x) \to (f(x_0), \cdots, f(x_{n-1})).$$

Definition 1. *The $[n, k, d]$-linear code*

$$C(\mathbf{x}) = \{(f(x_0), \cdots, f(x_{n-1})) : f(x) \in P_k\} \subset \mathbb{F}^n$$

*is called a **Reed-Solomon Code**.*

Remark 2. *We will not include, in general, the reference to the vector $\mathbf{x}$ in the notation for the code.*

The generator matrix for C depends on the choice of basis for P_k. If the choice is the canonical basis $1, x, \cdots, x^{k-1}$, we get

$$G = \begin{bmatrix} 1 & \cdots & 1 \\ x_0 & \cdots & x_{n-1} \\ x_0^{k-1} & \cdots & x_{n-1}^{k-1} \end{bmatrix}$$

Remark 3. *From now on, we will present matrices, most of the times, indicating the form of the general term, together with the dimensions. We will also start the indices of rows and columns at 0. The matrix G is then*

$$G = \left[x_j^i\right]_{i<k}^{j<n}.$$

Example 4. *Let $\mathbb{F}_7$, $n = 6$, $\mathbf{x} = (1, 2, 3, 4, 5, 6)$ and $k = 4$. The generator matrix of this Reed-Solomon code, with respect to the canonical basis of P_4, is*

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

and an example of encoding is

$$3 + 2x^2 + x^3 \rightsquigarrow (3, 0, 2, 1)G = (6, 5, 6, 1, 3, 4)$$

Theorem 5. *If C is a Reed-Solomon $[n, k, d]$-linear code, then $d = n - k + 1$, ie, C is a MDS code.*

Proof. If $f_1, f_2 \in P_k$, $f_1(x_i) = f_2(x_i)$ can happen for at most $k-1$ coordinates, and so, putting $c_i = (f_i(x_0), \cdots, f_i(x_{k-1}))$, we have $\text{dist}(c_1, c_2) \geq n - (k-1)$. The opposite inequality is valid for any block code over a finite field by Singleton's bound. □

Remark 6. *Recall that the error-correcting capability of a code is*

$$t = \lfloor \frac{d-1}{2} \rfloor = \begin{cases} \frac{d-1}{2} & d \text{ odd} \\ \frac{d-2}{2} & d \text{ even} \end{cases}$$

ie, the same value of t is attained with $d = 2t+1$ and with $d = 2t+2$.
This means, in the case of Reed-Solomon codes, that for a fixed n, and considering only the resulting information rate and error correcting capability, it is better to choose a code with odd minimum distance.

Recall that the dual of an MDS code is also MDS. It is thus natural to ask if the dual of a Reed-Solomon code is also a Reed-Solomon code, defined by the same or by another vector $\mathbf{x}$. It turns out that we have such a property if we slightly generalize the definition.

Definition 7. *Let $\mathbf{x}$ be defined as above and $\mathbf{a} = (a_0, \cdots, a_{n-1}) \in \mathbb{F}^n$ be a vector with nonzero coordinates.*
*A **generalized Reed-Solomon** code $C(\mathbf{a}, \mathbf{x})$ is defined as*

$$C(\mathbf{a}, \mathbf{x}) = \{(a_0 f(x_0), \cdots, a_{n-1} f(x_{n-1})) : f(x) \in P_k\} \subset \mathbb{F}^n.$$

The generator matrix, with respect to the canonical basis of P_k, is $G = [a_j x_j^i]_{i<k}^{j<n}$.

Given two vectors $\mathbf{a}$ and $\mathbf{b}$, the codes $C(\mathbf{a}, \mathbf{x})$ and $C(\mathbf{b}, \mathbf{x})$ are monomially equivalent (**HW**).

Proposition 8. *If $C(\mathbf{a}, \mathbf{x})$ is a $[n, k, n-k+1]$ code, its dual is also a generalized Reed-Solomon code $C(\mathbf{b}, \mathbf{x})$.*

Proof. The dual code is MDS, with parameters $[n, n-k, k+1]$. First, notice that $(b_0, \cdots, b_{n-1}) \in (C(\mathbf{a}, \mathbf{x}))^\perp$ if and only if

$$\forall f(x) \in P_k \qquad \sum_j b_j a_j f(x_j) = 0 \Leftrightarrow \sum_j b_j a_j x_j^i \ \forall 0 \leq i < k.$$

On the other hand, the dual of the $[n, n-1, 2]$ code $C(\mathbf{a}, \mathbf{x})$ is a $[n, 1, n]$ code, with basis constituted by a vector $(b_0, \cdots, b_{n-1})$ with nonzero coordinates. This dual code is clearly a generalized Reed-Solomon code $C(\mathbf{b}, \mathbf{x})$.
Suppose now that $C(\mathbf{a}, \mathbf{x})$ has dimension $k < n-1$; then, for any $h(x) \in P_{n-k}$, $(b_0 h(x_0), \cdots, b_{n-1} h(x_{n-1})) \in (C(\mathbf{a}, \mathbf{x}))^\perp$: if $f(x) \in P_k$, $f(x)h(x) \in P_{n-1}$; but by construction

$$\sum_{j=0}^{n-1} b_j a_j \phi(x_j) = 0, \ \forall \phi(x) \in P_{n-1}.$$

We just concluded that the $[n, n-k, k+1]$ generalized Reed-Solomon code $C(\mathbf{b}, \mathbf{x})$ is contained in $(C(\mathbf{a}, \mathbf{x}))^\perp$ and we have equality as they have the same dimension. □

Corollary 9. *A parity-check matrix for the code $C(\mathbf{a}, \mathbf{x})$ is*

$$H = [b_j x_j^i]_{i<n-k}^{j<n}.$$

Remark 10. *The proof indicates that the vector* $\mathbf{b}$ *may be chosen as a member of the kernel of $[a_j x_j^i]_{i<k}^{j<n}$, with nonzero coordinates. This solution is in general not unique, even up to multiplication by a scalar.*

Exercise 11. *Show that the dual $C^\perp$ of the code in example 4 is not Reed-Solomon and find a vector* $\mathbf{b}$ *such that $C^\perp$ is the generalized Reed-Solomon code $C(\mathbf{b}, \mathbf{x})$.*

The most simple choice for the construction of a Reed-Solomon code is to take $x_i = \lambda^i$ where λ is a primitive n-th root of unity in $\mathbb{F}$, and in fact any Reed-Solomon code is equivalent to one defined in this way (**HW**).
We obtain straightforward formulas for both generator and parity-check matrices:

Lemma 12. *The $[n, k]$ Reed Solomon code $\{(f(1), f(\lambda), \cdots, f(\lambda^{k-1})) : f(x) \in P_k\}$ has generator and parity-check matrices*

$$G = \left[\lambda^{ij}\right]_{i<k}^{j<n} \qquad H = \left[\lambda^{(i+1)j}\right]_{i<n-k}^{j<n}.$$

Proof. (**HW**). **Hint**: multiply H on the right by

$$L = \left[\lambda^{(j+1)(n-i)}\right]_{i<n}^{j<n-k}.$$

□

1.1. **Reed-Solomon Codes as Cyclic Codes.** It is clear from the definition that Reed-Solomon codes defined with $x_i = \lambda^i$ are cyclic: if $\left(f(\lambda^i)\right)_{0\le i<n} \in C$ then

$$\left(f(\lambda^{i+1})\right)_{0\le i<n} = \left(h(\lambda^i)\right)_{0\le i<n}$$

where the exponents are taken modulo n and $h(x) = f(\lambda x)$.
We will now identify the generating polynomial $g(x) = \sum_{i=0}^{n-k} g_i x^i$. We recall that codewords $(c_0, \cdots, c_{n-1})$ of cyclic codes have been interpreted as coefficients of polynomials:

$$(c_0, \cdots, c_{n-1}) \to c(x) = \sum_{i=0}^{n-1} c_i x^i = f(x)g(x) \mod (x^n - 1)$$

where $f(x) \in P_k$. On the other hand, a codeword of the Reed-Solomon code has been defined as $(f(1), f(\lambda), \cdots, f(\lambda^{n-1}))$.
To reconcile these two presentations, if $f(x) = \sum_{i=0}^{k-1} a_i x^i$,

$$(f(1), f(\lambda), \cdots, f(\lambda^{n-1})) = (c_0, \cdots, c_{n-1})$$

implies that

$$c(x) = \sum_{i=0}^{n-1} f(\lambda^i) x^i = \sum_{i=0}^{n-1} \sum_{s=0}^{k-1} a_s \lambda^{is} x^i = \sum_{s=0}^{k-1} a_s \sum_{i=0}^{n-1} \lambda^{is} x^i,$$

and so, for any $1 \leq j \leq n-k$,

$$c(\lambda^j) = \sum_{s=0}^{k-1} a_s \sum_{i=0}^{n-1} \lambda^{(s+j)i} =$$

as $1 \leq s+j \leq n-1$, and so $\lambda^{s+j} \neq 1$,

$$= \sum_{i=0}^{n-1} \frac{\lambda^{(s+j)n} - 1}{\lambda^{s+j} - 1} = 0.$$

This implies in particular that that $g(\lambda^i) = 0$ for $1 \leq i \leq n-k$ and so, as $g(x)$ is a monic polynomial with degree $n-k$,

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

This could also be confirmed noting that

$$G = \left[\lambda^{ij}\right]_{i<k}^{j<n} \qquad H = \left[\lambda^{(i+1)j}\right]_{i<n-k}^{j<n}$$

are respectively generator and check-parity matrices for C, and that, as the matrix G_g whose i-th row are the coefficients of $x^i g(x)$ is also a generator, $G_g H^T = 0$.

This was in fact the motivation for the definition of this class of codes, ie, to define cyclic codes with a defining set containing a long array of consecutive elements, in order to take advantage of the BCH bound for the distance.

Example 13. *Taking $\lambda = 3$, we obtain a code equivalent to the one in example 4, with generator and parity-check matrices*

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \end{bmatrix} \qquad H = \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{bmatrix}$$

The generator polynomial is $g(x) = (x-3)(x-2) = x^2 + 2x + 6$. An example of encoding is

$$3 + 2x^2 + x^3 \rightsquigarrow (3,0,2,1)G = (6,6,5,4,1,3)$$

which corresponds to the polynomial

$$c(x) = 6 + 6x + 5x^2 + 4x^3 + x^4 + 3x^5 = g(x)(3x^3 + 2x^2 + 3x + 1).$$

1.2. **Decoding: Peterson's Algorithm.** The structure of these codes allows for particular decoding algorithms, of which we present one, the so called **Peterson's algorithm**.
We assume that $d = n - k + 1$ is odd, and so that $t = \frac{d-1}{2}$. The definition of the decoding procedure is presented for the general case but the concrete computations are developed only for the case $x_i = \lambda^i$.
The strategy for decoding is to compute, from a received message $r = (r_i)_{0 \leq i < n}$, polynomials $Q_0(x), Q_1(x) \in \mathbb{F}[x]$ satisfying

1) $\deg(Q_0(x)) \leq s = n - 1 - t$;
2) $\deg(Q_1(x)) \leq t$;
3) $Q_0(x_i) + r_i Q_1(x_i) = 0 \ \forall i < n$.

Before we start the computation of these polynomials, we notice that such polynomials do exist: putting

$$Q_0(x) = \sum_{i=0}^{s} Q_{0,i} x^i, \qquad Q_1(x) = \sum_{i=0}^{t} Q_{1,i} x^i$$

condition 3) gives a set of n equations on the $Q_{0,i}$ and $Q_{1,i}$:

$$\left[x_i^j | r_i x_i^j \right] \begin{pmatrix} Q_{0,i} \\ Q_{1,i} \end{pmatrix}$$

where in the first block of the matrix $0 \leq j \leq s$ while in the second, $0 \leq j \leq t$. Because $s + 1 + t + 1 = n + 1$ and the system has n equation, there always exists a non-zero solution.

Suppose $r = c + e$, where $c \in C$ is the encoding of a polynomial $c(x)$ (ie, $c = (c(x_0, \cdots, c(x_{n-1}))$, e is the error pattern, and $w(e) \leq t$. By construction

$$Q_0(x_i) + (c(x_i) + e_i) Q_1(x_i) = 0 \ \forall i$$

but $e_i = 0$ for at least $n - t$ coordinates; so

$$Q(x) = Q_0(x) + c(x) Q_1(x)$$

has at least $n - t$ roots. However,

$$\deg(Q(x)) \leq \max\{\deg(Q_0(x)), \deg(c(x) + Q_1(x))\} \leq n - t - 1,$$

and so (always under the assumption that $w(e) \leq t$) $Q(x)$ is the zero polynomial, implying that the original message is recovered as

$$c(x) = -\frac{Q_0(x)}{Q_1(x)}.$$

Remark 14. *We notice also that $e_i \neq 0 \implies Q_1(x_i) = 0$. So the knowledge of the polynomial $Q_1(x)$ allows us to locate the position of the possible errors: these may only occur at the coordinates corresponding to roots of $Q_1(x)$*
For this reason the polynomial $Q_1(x)$ is also called the ***locator polynomial****.*

We now describe the computation of the coefficients, in the case $x_i = \lambda^i$: the system of equations becomes

$$\left[\lambda^{ij} \right] (Q_{0,j}) + \left[r_i \lambda^{ij} \right] (Q_{1,j}) = 0,$$

where the first matrix $R_0 = \left[\lambda^{ij}\right]$ has dimensions $n \times (s+1)$ while the second $R_1 = \left[r_i\lambda^{ij}\right]$ has dimensions $n \times (t+1)$;

multiplying on the left by $B = \left[\lambda^{(i+1)j}\right]_{i<t}^{j<n}$ we get (**HW**)

$$BR_1(Q_{1,j}) = 0.$$

On the other hand, the entries of the matrix $D(r) = BR_1$ may be computed directly as coordinates of the syndrome of r

$$Hr^T = (S_0, \cdots, S_{n-k-1})^T.$$

Identifying $r = (r_0, \cdots, r_{n-1})$ with the polynomial $r(x) = \sum_{i=0}^{n-1} r_i x^i$, the syndrome of r is

$$(r(\lambda), \cdots, r(\lambda^{n-k})).$$

A direct computation (**HW**) shows that

$$D(r) = [S_{i+j}]_{i<t}^{j<t+1}.$$

Remark 15. *The number $n-k$ of syndrome coordinates coincides with the number $2t = d-1$ of entries in $D(r)$ because of the choice of d being odd. If we were to choose a even d and $t = \lfloor \frac{d-1}{2} \rfloor$ and follow the same decoding procedure, using the values $s = n-1-t$ and $l = s-k+1 = d-1-t$ as upper bounds for the degrees of the polynomials $Q_0(x)$ and $Q_1(x)$, we still get the same properties, but the entries of the matrix $D(r)$ coincide with the syndrome coordinates only up to $i+j+1 = d-1$ and so the last entry of the matrix can not be read directly from the syndrome.*

From the last equation we compute the coefficients of $Q_1(x)$, which we may choose with the lowest possible degree. Going back to the original equation

$$R_0(Q_{0,j}) + R_1(Q_{1,j}) = 0,$$

we know that the second summand (with $Q_1(x)$ already computed) lies in the kernel of B. We saw above that the columns of R_0 lie also in this space, so to prove the existence of a solution $Q_{0,j}$ to the equation it is enough to prove that those $s+1$ columns of R_0 span the kernel of B.
We derive this fact from a useful general result:

Proposition 16. *For any $m > 0$ and $x_0, \cdots, x_{m-1}$ the **Vandermonde** matrix*

$$V(x_0, \cdots, x_{m-1}) = \left[x_j^i\right]_{i<m}^{j<m}$$

has determinant $\prod_{0 \le u < v < m}(x_v - x_u)$.

Proof. (**HW**) By induction on m. The case $m = 1$ is obvious. Assuming the statement to be true for $m-1$,

$$L(z) = \det(V(x_0, \cdots, x_{m-2}, z))$$

is a polynomial on z with degree $(m-2)$. We know its zeros and main coefficient and so we have a factorization; using the induction hypothesis and putting $z = x_m$ the induction step is completed. □

In particular, $V(1, \lambda, \lambda^2, \cdots, \lambda^{n-1})$ has nonzero determinant, because λ is a primitive n-th root of unity in $\mathbb{F}$. Multiplying on the right by the diagonal matrix $\mathrm{diag}(1, \lambda, \cdots, \lambda^{n-1})$, we obtain an invertible matrix whose first t rows are the matrix B defined above.
This implies that B is surjective, its rank is t and its kernel has dimension $n - t = s + 1$.
By the same reasoning, the matrix R_0 may be extended, by adding $n - s - 1 = t$ columns, to the same Vandermonde matrix $V(1, \lambda, \cdots, \lambda^{n-1})$. This implies that the matrix R_0 is injective, ie, the columns are linearly independent and so they span the kernel of B.
So there exists a vector $Q_{0,j}$ satisfying the equation, for each $Q_{1,j}$ in the kernel of $D(r)$.

In fact, for this choice of x_i this deduction is not strictly necessary because the computations are made easier by the following observation, whose proof is left as an exercise:

Lemma 17.

$$\sum_{i=0}^{n-1} \left(\lambda^{-j}\right)^i \lambda^{ki} = \begin{cases} n & \text{if } k = j \\ 0 & \text{otherwise} \end{cases}$$

This implies that the equation for the $Q_{0,i}$ may be solved as

$$(Q_{0,i}) = -n^{-1} C R_1 (Q_{1,j})$$

where $C = \left[\lambda^{-ij}\right]_{i<s+1}^{j<n}$.

We illustrate the construction of Reed-Solomon codes and the application of Peterson's algorithm with a couple of examples:

Example 18. *Let $q = 11$, $\lambda = 3$, $n = 5$ and $k = 3$. So $d = 3$, $t = 1$ and $s = 3$. The generator matrix is in this case*

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 9 & 5 & 4 \\ 1 & 9 & 4 & 3 & 5 \end{bmatrix}$$

while the corresponding parity-check matrix is

$$H = \begin{bmatrix} 1 & 3 & 9 & 5 & 4 \\ 1 & 9 & 4 & 3 & 5 \end{bmatrix}.$$

If $r = (\ 5 \quad 9 \quad 1 \quad 2 \quad 0\ )$ we compute the syndrome $Hr^T = (7, 8)^T$ and we obtain the matrix $D(r) = [\ 7 \quad 8\ ]$.
A possible choice for the locator polynomial is $Q_1(x) = x + 2$. The computation of $Q_0(x)$ follows from the solution of the linear equation

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 9 & 5 \\ 1 & 9 & 4 & 3 \\ 1 & 5 & 3 & 4 \\ 1 & 4 & 5 & 9 \end{bmatrix} \begin{pmatrix} Q_{0,0} \\ Q_{0,1} \\ Q_{0,2} \\ Q_{0,3} \end{pmatrix} = -diag(\ 5 \quad 9 \quad 1 \quad 2 \quad 0\ ) \begin{bmatrix} 1 & 1 \\ 1 & 3 \\ 1 & 9 \\ 1 & 5 \\ 1 & 4 \end{bmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = - \begin{pmatrix} 4 \\ 1 \\ 0 \\ 3 \\ 0 \end{pmatrix}$$

Applying Gauss-Jordan reduction or directly by the formula obtained above, we obtain $Q_0(x) = -(2x^2 + 7x + 6)$ *and so the polynomial that generated the sent message is*

$$f(x) = \frac{2x^2 + 7x + 6}{x + 2} = 2x + 3$$

and the message is

$$(\ f(1) \quad f(3) \quad f(9) \quad f(5) \quad f(4)\ ) = (\ 5 \quad 9 \quad 10 \quad 2 \quad 0\ ).$$

This information could also be obtained from the fact that $Q_1(x)$ *is the locator polynomial: if* $e_i \neq 0$ *then* $Q_1(x_i) = 0$*; in our case the only possible solution is* $x_i = 9 = 3^2$*. We could then compute the error pattern* $e = (\ 0 \quad 0 \quad e_2 \quad 0 \quad 0\ )$ *by solving*

$$He^T = Hr^T = S$$

which reduces to

$$9e_2 = 7 \Leftrightarrow e_2 = 2.$$

So the sent message is

$$r - e = (\ 5 \quad 9 \quad 1 \quad 2 \quad 0\ ) - (\ 0 \quad 0 \quad 2 \quad 0 \quad 0\ ) = (\ 5 \quad 9 \quad 10 \quad 2 \quad 0\ ).$$

Example 19. *A* $[8, 4, 5]$ *Reed-Solomon code over* $\mathbb{F}_{25}$*:*
We may start the construction of the desired field from any degree 2 *polynomial, irreducible over* $\mathbb{F}_5$*: one possible choice would be* $p(x) = x^2 + 4x + 2$*; the field* $\mathbb{F}_5[x]/(p(x)) = \mathbb{F}_5[\alpha]$ *(with* $\alpha^2 + 4\alpha + 2 = 0$*) has* α *as one of its primitive elements. However, to construct the code we need an* 8*-th primitive root of unity; the obvious choice is* $\beta = \alpha^3 = 4\alpha + 3$ *which satisfies* $\beta^2 = 2$*. From this point on we will represent the field elements with respect to* β*; because* β *is not a primitive element, we are not able to represent all nonzero field elements as powers.*

Remark 20. *We could of course start directly with the, also irreducible, polynomial* $p(x) = x^2 + 3$*.*

The generator matrix is then

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

while the corresponding parity-check matrix is

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

The parameters of the code imply that $t = 2$ *and* $s = 5$*.*
Suppose the received message is

$$r = (0, \beta + 4, \beta, 3\beta + 1, 4, 4\beta + 1, 4, 2\beta + 1);$$

the corresponding syndrome is $s = (1, 4\beta+1, 4\beta+4, \beta+1)^T$ *and so we obtain the matrix*

$$D(r) = \begin{bmatrix} 1 & 4\beta+1 & 4\beta+4 \\ 4\beta+1 & 4\beta+4 & \beta+1 \end{bmatrix},$$

and compute the coefficients of Q_1*: this is simpler if we first perform a Gauss-Jordan reduction to obtain*

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

from which we read directly the solution $(3\beta, \beta+3, 1)^T$*, ie*

$$Q_1(x) = x^2 + (\beta+3)x + 3\beta = (x-2)(x-4\beta);$$

this means that the nonzero entries of the associated error pattern are at positions 3 *(corresponding to* $\beta^2 = 2$*) and* 6 *(corresponding to* $\beta^5 = 4\beta$*), ie,*

$$e = (0, 0, a\beta+b, 0, 0, c\beta+d, 0, 0)^T.$$

The coefficients are determined by the equation $He = s$*, which is reduced to*

$$\begin{pmatrix} 2 \\ 4 \\ 3 \\ 1 \end{pmatrix}(a\beta+b) + \begin{pmatrix} 4\beta \\ 2 \\ 3\beta \\ 4 \end{pmatrix}(c\beta+d) = \begin{pmatrix} 1 \\ 4\beta+1 \\ 4\beta+4 \\ \beta+1 \end{pmatrix} \Leftrightarrow$$

$$\Leftrightarrow \begin{bmatrix} 2\beta & 2 & 3 & 4\beta \\ 4\beta & 4 & 2\beta & 2 \\ 3\beta & 3 & 1 & 3\beta \\ \beta & 1 & 4\beta & 4 \end{bmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 4\beta+1 \\ 4\beta+4 \\ \beta+1 \end{pmatrix}.$$

Remark 21. *Although this is a linear equation over* $\mathbb{F}_{25}$ *we may instead equate separately coefficients of* β *and "independent" terms (as with the real and imaginary parts in equations over* $\mathbb{C}$*); in this case we get*

$$\begin{bmatrix} 2 & 0 & 0 & 4 \\ 4 & 0 & 2 & 0 \\ 3 & 0 & 0 & 3 \\ 1 & 0 & 4 & 0 \end{bmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \\ 4 \\ 1 \end{pmatrix}$$

and

$$\begin{bmatrix} 0 & 2 & 3 & 0 \\ 0 & 4 & 0 & 2 \\ 0 & 3 & 1 & 0 \\ 0 & 1 & 0 & 4 \end{bmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 4 \\ 1 \end{pmatrix}.$$

The solution is that $e = (0, 0, \beta+3, 0, 0, 2, 0, 0)$ *and* r *is decoded into* $c = (0, \beta+4, 2, 3\beta+1, 4, 4\beta+4, 4, 2\beta+1)$*.*

We may also determine $Q_0(x) = 2x^5 + (2\beta+4)x^4 + (4\beta+4)x^3 + 4\beta x^2$ *and from that we find that the polynomial* $c(x)$ *that originated the encoded message is*

$$c(x) = -\frac{2x^5 + (2\beta+4)x^4 + (4\beta+4)x^3 + 4\beta x^2}{x^2 + (\beta+3)x + 3\beta} = 3x^3 + 2x^2.$$

Exercise 22. *Compute the generator and parity-check matrices for the* $[10, 6, 5]$ *Reed-Solomon code over* $\mathbb{F}_{11}$

$$C = \{(f(1), f(\lambda), \cdots, f(\lambda^9)) : f(x) \in P_6$$

with $\lambda = 2$.
Apply Peterson's algorithm to the decoding of

$$r = (4, 0, 0, 3, 0, 2, 1, 2, 2, 3).$$

Exercise 23. *Let* C *be the* $[15, 9, 7]$ *cyclic code over* $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ *(*$\alpha^4 = \alpha + 1$*) with defining set* $T = \{1, 2, 3, 4, 5, 6\}$.

a) *Determine the corresponding generator polynomial.*
b) *Decode* $r(x) = \alpha^7 x^{11} + \alpha^4 x^7 + \alpha^4 x^6 + \alpha^5 x^5 + \alpha^2 x^4 + x^3 + \alpha^{10} x^2 + \alpha^7$ *using Peterson's algorithm.*

Exercise 24. *Let* $\mathbb{F}_{7^2} = \mathbb{F}_7[x]/(x^2 + 6x + 6) = \mathbb{F}_7[\beta]$.

a) *Verify that* β *is a primitive* 16*-root of unity and use it to define a* $[16, 8, 9]$ *code over* $\mathbb{F}_{7^2}$.
b) *Determine the generator polynomial of the code.*
c) *Decode, both by error trapping and by Peterson's algorithm, the received message*

$(2, 5, 6\beta{+}2, \beta{+}5, 3\beta{+}2, 4\beta, 6\beta{+}3, 2\beta{+}3, 6, 4\beta{+}4, \beta{+}2, \beta{+}4, 4\beta{+}5, 6\beta{+}5, \beta{+}1, 3\beta{+}1)$