Binary Representation of Elements in GF(2^m)

Representation of Elements in GF(2^m) as Vectors over GF(2)

Let $p(x) = \sum_{i=0}^{m} p_i x^i$ be a primitive polynomial over GF(2) of degree m with $\alpha \in$ GF(2^m) as a root. Since $p(\alpha) = 0$ and $p(x)$ has degree m, then $\alpha^m = \sum_{i=0}^{m-1} p_i \alpha^i$. As all nonzero elements in GF(2^m) are powers of α, it follows that each element β in this field, including the zero element, can be written uniquely as $\beta = \sum_{i=0}^{m-1} b_i \alpha^i$, for some unique $b_i \in$ GF(2), $0 \leq i < m$. In particular, the element β in GF(2^m) can be identified with the binary vector $\mathbf{V}(\beta) = (b_0, b_1, \ldots, b_{m-1})$, which we call the *binary vector representation* of β. This representation is most useful to reduce addition and multiplication of elements in GF(2^m) to addition and multiplication of vectors over GF(2). Notice that the binary vector representation of the element zero in GF(2^m) is the all-zero vector of length m.

Let β and γ be in GF(2^m) with binary vector representations $\mathbf{V}(\beta) = (b_0, b_1, \ldots, b_{m-1})$ and $\mathbf{V}(\gamma) = (c_0, c_1, \ldots, c_{m-1})$, respectively. Then, we clearly have

$$\mathbf{V}(\beta + \gamma) = \mathbf{V}(\beta) + \mathbf{V}(\gamma). \tag{1}$$

This can be generalized as follows. Let $\beta_0, \beta_1, \ldots, \beta_{N-1}$ be elements in GF(2^m) and let $a_0, a_1, \ldots, a_{N-1}$ be elements in GF(2). Then,

$$\mathbf{V}(\sum_{j=0}^{N-1} a_j \beta_j) = \sum_{j=0}^{N-1} a_j \mathbf{V}(\beta_j). \tag{2}$$

For multiplication of the elements $\beta, \gamma \in$ GF(2^m), we use $(c_0^{(i)}, c_1^{(i)}, \ldots, c_{m-1}^{(i)})$ to denote the binary vector representation $\mathbf{V}(\alpha^i \gamma)$ of the element $\alpha^i \gamma \in$ GF(2^m) for $i = 0, 1, \ldots, m-1$. Then,

$$\begin{aligned}\beta\gamma &= (\sum_{i=0}^{m-1} b_i \alpha^i)\gamma = \sum_{i=0}^{m-1} b_i (\alpha^i \gamma) \\ &= \sum_{i=0}^{m-1} b_i \sum_{j=0}^{m-1} c_j^{(i)} \alpha^j = \sum_{j=0}^{m-1} (\sum_{i=0}^{m-1} b_i c_j^{(i)}) \alpha^j.\end{aligned}$$

Hence, the binary vector representation of $\beta\gamma$ is given by

$$\mathbf{V}(\beta\gamma) = \left(\sum_{i=0}^{m-1} b_i c_0^{(i)}, \sum_{i=0}^{m-1} b_i c_1^{(i)}, \ldots, \sum_{i=0}^{m-1} b_i c_{m-1}^{(i)} \right) = \mathbf{V}(\beta)\mathbf{M}(\gamma), \tag{3}$$

where $\mathbf{M}(\gamma)$ is the $m \times m$ matrix with $\mathbf{V}(\alpha^i\gamma)$ as its ith row for $i = 0, 1, \ldots, m-1$.

Example 1 The elements $0, 1, \alpha, \alpha^2, \ldots, \alpha^6$, where α is a root of the primitive polynomial $p(x) = 1 + x + x^3$ over GF(2) are the elements of GF(8). Table I shows the binary vector representation $\mathbf{V}(\beta)$ and the matrix $\mathbf{M}(\beta)$ of each element β in the field based on this choice of $p(x)$.

For example, to verify the entries for α^4, notice that since $p(\alpha) = 0$, then $\alpha^3 = 1 + \alpha$ and $\alpha^4 = \alpha + \alpha^2$. Therefore, the binary vector representation of α^4 is $\mathbf{V}(\alpha^4) = (0, 1, 1)$. We also have

$$\mathbf{M}(\alpha^4) = \begin{pmatrix} \mathbf{V}(\alpha^4) \\ \mathbf{V}(\alpha^5) \\ \mathbf{V}(\alpha^6) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

As an application, the binary vector representation of α^2 times α^4 is given by

$$\mathbf{V}(\alpha^2\alpha^4) = \mathbf{V}(\alpha^2)\mathbf{M}(\alpha^4) = (0, 0, 1) \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = (1, 0, 1),$$

which is indeed the binary vector representation of α^6. □

Representation of Parity-Check Matrices over GF(2^m) of Codes over GF(2^m) as Matrices over GF(2)

Let $\mathbf{H} = [\beta_{ij}]_{0 \le i < R, 0 \le j < N}$ be an $R \times N$ matrix over GF(2^m). Define the matrix $\mathbf{M}(\mathbf{H}) = [\mathbf{M}^{\mathsf{T}}(\beta_{ij})]_{0 \le i < R, 0 \le j < N}$, where T denotes transposition, i.e., $\mathbf{M}(\mathbf{H})$ is obtained by replacing each entry β_{ij} in $\mathbf{H}$ by the transpose of the matrix $\mathbf{M}(\beta_{ij})$. Then, $\mathbf{M}(\mathbf{H})$ is an $mR \times mN$ matrix over GF(2). We will argue in the following that a vector $(\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$ is in the null space of $\mathbf{H}$ if and only if $(\mathbf{V}(\gamma_0), \mathbf{V}(\gamma_1), \ldots, \mathbf{V}(\gamma_{N-1}))$ is in the null space of $\mathbf{M}(\mathbf{H})$. Indeed, $(\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$ is in the null space of $\mathbf{H}$ if and only if $\sum_{j=0}^{N-1} \beta_{ij}\gamma_j = 0$ for $0 \le i < R$. From (2) and (3), we get

$$\begin{aligned} \mathbf{V}(\sum_{j=0}^{N-1} \beta_{ij}\gamma_j) &= \sum_{j=0}^{N-1} \mathbf{V}(\beta_{ij}\gamma_j) \\ &= \sum_{j=0}^{N-1} \mathbf{V}(\gamma_j)\mathbf{M}(\beta_{ij}) \end{aligned}$$

Table I: Binary representation vectors for GF(8) based on the primitive polynomial $1+x+x^3$

$\beta \in \mathrm{GF}(8)$	$\mathbf{V}(\beta)$	$\mathbf{M}(\beta)$
0	$(0,0,0)$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
1	$(1,0,0)$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
α	$(0,1,0)$	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$
α^2	$(0,0,1)$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$
α^3	$(1,1,0)$	$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$
α^4	$(0,1,1)$	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$
α^5	$(1,1,1)$	$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$
α^6	$(1,0,1)$	$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

$$= \quad (\mathbf{V}(\gamma_0), \mathbf{V}(\gamma_1), \ldots, \mathbf{V}(\gamma_{N-1})) \begin{pmatrix} \mathbf{M}(\beta_{i0}) \\ \mathbf{M}(\beta_{i1}) \\ \vdots \\ \mathbf{M}(\beta_{i,N-1}) \end{pmatrix}.$$

Since an element in GF(2^m) is zero if and only if its binary vector representation is zero, it follows that $\sum_{j=0}^{N-1} \beta_{ij}\gamma_j = 0$ if and only if $(\mathbf{V}(\gamma_0), \mathbf{V}(\gamma_1), \ldots, \mathbf{V}(\gamma_{N-1}))$ is in the null space of the $mN \times m$ binary matrix $(\mathbf{M}^{\mathsf{T}}(\beta_{i0}), \mathbf{M}^{\mathsf{T}}(\beta_{i1}), \ldots, \mathbf{M}^{\mathsf{T}}(\beta_{i,N-1}))$. Considering all values of $0 \le i < R$, we deduce that $(\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$ is in the null space of $\mathbf{H}$ if and only if $(\mathbf{V}(\gamma_0), \mathbf{V}(\gamma_1), \ldots, \mathbf{V}(\gamma_{N-1}))$ is in the null space of $\mathbf{M}(\mathbf{H})$. If $\mathbf{H}$ has rank r, then its null space is of dimension $N - r$ over GF(2^m) and, therefore, of size $2^{m(N-r)}$. Hence, the null space of $\mathbf{H}(\mathbf{M})$ is of size $2^{m(N-r)}$ and, therefore, of dimension $m(N-r)$ over GF(2). We conclude that the rank of $\mathbf{H}(\mathbf{M})$ is mr.

Example 2 Consider the matrix $\mathbf{H}$ over GF(8) given by

$$\mathbf{H} = (\alpha^{ij}) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \end{pmatrix},$$

where α is a root of $1 + x + x^3$. This is the parity-check matrix of the Reed-Solomon code of length $n = 7$, dimension $k = 5$, and minimum distance $d = 3$. Using Table I, we get

$$\mathbf{M}(\mathbf{H}) = [\mathbf{M}^{\mathsf{T}}(\alpha^{ij})] = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right).$$

The vector $(\gamma_0, \gamma_1, \ldots, \gamma_6)$ over GF(8) is in the null space of $\mathbf{H}$, i.e., a codeword in the Reed-Solomon code, if and only if the vector $(\mathbf{V}(\gamma_0), \mathbf{V}(\gamma_1), \ldots, \mathbf{V}(\gamma_6))$ is in the null space of $\mathbf{M}(\mathbf{H})$. For example, $(\alpha^6, \alpha^4, 0, 0, 1, 0, \alpha^3)$ is in the null space of $\mathbf{H}$ and

$$(\mathbf{V}(\alpha^6), \mathbf{V}(\alpha^4), \mathbf{V}(0), \mathbf{V}(0), \mathbf{V}(1), \mathbf{V}(0), \mathbf{V}(\alpha^3)) = (101|011|000|000|100|000|110)$$

is in the null space of $\mathbf{M}(\mathbf{H})$. Notice that the ranks of $\mathbf{H}$ and $\mathbf{M}(\mathbf{H})$ are two and six, respectively. □

Representation of Parity-Check Matrices over GF(2^m) of Codes over GF(2) as Matrices over GF(2)

Suppose that $\mathbf{H}$ is a parity-check matrix of a binary code, i.e., a code over GF(2). The code has a parity-check matrix $\mathbf{H}$ over GF(2^m), i.e., a binary vector $(\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$ over GF(2) is a codeword in the code if and only if it is in the null space of $\mathbf{H}$. Since 0 and 1 are the only two elements in GF(2) and their binary vector representations are $\mathbf{V}(0) = (0, 0, \ldots, 0)$ and $\mathbf{V}(1) = (1, 0, \ldots, 0)$, it follows that $\mathbf{V}(\gamma_j)$, for $0 \le j < N$, ends with $m - 1$ zeros. Based on the last section, $(\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$ is in the null space of $\mathbf{H}$ if and only if $(\mathbf{V}(\gamma_0), \mathbf{V}(\gamma_1), \ldots, \mathbf{V}(\gamma_{N-1}))$ is in the null space of $\mathbf{M}(\mathbf{H})$. Let $\mathbf{M}_{\text{red}}(\mathbf{H})$ be the reduced matrix obtained from $\mathbf{M}(\mathbf{H})$ by retaining the columns numbered $0, m, 2m, \ldots, (N-1)m$ and deleting all the rest. Then, $(\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$ is in the null space of $\mathbf{H}$ if and only if $(\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$ is in the null space of $\mathbf{M}_{\text{red}}(\mathbf{H})$. Hence, $\mathbf{M}_{\text{red}}(\mathbf{H})$ is a parity-check matrix of the code.

The matrix $\mathbf{M}(\mathbf{H}) = [\mathbf{M}^{\mathsf{T}}(\beta_{ij})]$ is obtained by replacing each entry β_{ij} in $\mathbf{H}$ by the transpose of the matrix $\mathbf{M}(\beta_{ij})$. The first column in $\mathbf{M}^{\mathsf{T}}(\beta_{ij})$ is thus the transpose of the first row in $\mathbf{M}(\beta_{ij})$ which is the binary vector representation of β_{ij}. Hence, the matrix $\mathbf{M}_{\text{red}}(\mathbf{H})$ can be obtained directly from the matrix $\mathbf{H} = [\beta_{ij}]_{0 \le i < R, 0 \le j < N}$ by replacing each element β_{ij} by the transpose of its binary vector representation, $\mathbf{V}(\beta_{ij})^{\mathsf{T}}$, which is a column vector of length m.

Actually, it is obvious that $\mathbf{M}_{\text{red}}(\mathbf{H})$ is a parity-check matrix of the code. Indeed, the binary vector $(\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$ is in the null space of $\mathbf{H} = [\beta_{ij}]_{0 \le i < R, 0 \le j < N}$ if and only if $\sum_{j=0}^{N-1} \gamma_j \beta_{ij} = 0$ for $0 \le i < R, 0 \le j < N$, which, from (2), is the case if and only if $\sum_{j=0}^{N-1} \gamma_j \mathbf{V}(\beta_{ij}) = 0$, i.e., $\sum_{j=0}^{N-1} \gamma_j \mathbf{V}(\beta_{ij})^{\mathsf{T}} = 0$, for $0 \le i < R$. Hence, $\mathbf{M}_{\text{red}}(\mathbf{H})$ is a parity-check matrix of the code.

Notice that there is no straightforward relation between the ranks of the matrices $\mathbf{H}$ and $\mathbf{M}_{\text{red}}(\mathbf{H})$.

Example 3 Consider the matrix $\mathbf{H}$ over GF(8) given by

$$\mathbf{H} = (\alpha^{ij}) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \end{pmatrix},$$

where α is a root of $1 + x + x^3$. This is the parity-check matrix of a binary BCH code of length $n = 7$, dimension $k = 4$ (since the minimal polynomial of α over GF(2) if of degree three), and minimum distance 3 (since the columns with indices 0, 1, and 3 add up to zero). Using Table I, we get

$$\mathbf{M}_{\text{red}}(\mathbf{H}) = \left(\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right).$$

The vector $(\gamma_1, \gamma_2, \ldots, \gamma_7)$ over GF(2) is in the null space of $\mathbf{H}$, i.e., a codeword in the BCH code, if and only if it is in the null space of $\mathbf{M}_{\text{red}}(\mathbf{H})$. For example, $(1, 1, 0, 1, 0, 0, 0)$ is in the null spaces of $\mathbf{H}$ and $\mathbf{M}_{\text{red}}(\mathbf{H})$. Notice that the rank of $\mathbf{M}_{\text{red}}(\mathbf{H})$ is $n - k = 3$. Indeed, the first three rows in $\mathbf{M}_{\text{red}}(\mathbf{H})$ are linearly independent, the fourth row is the same as the first, the fifth is the same as the third, and the sixth is the sum of the second and third. □