Slide #3.

- Let $r = 2$ and construct GF(2^r) from $h(x) = x^2 + x + 1$. We have

$$\text{GF}(2^r) = \text{GF}(2^2) = \{0, 1, \beta, \beta^2\},$$

  where β is a primitive element and $\beta^2 = \beta + 1$.

- Let $n = 3$. GF$(2^r)^n$ is a vector space over GF(2^r). The elements of GF$(2^r)^n$ are listed below. There are $(2^r)^n = (2^2)^3 = 64$ of them.

$(0\,0\,0), (1\,0\,0), (\beta\,0\,0), (\beta^2\,0\,0), (0\,1\,0), (1\,1\,0), (\beta\,1\,0), (\beta^2\,1\,0),$

$(0\,\beta\,0), (1\,\beta\,0), (\beta\,\beta\,0), (\beta^2\,\beta\,0), (0\,\beta^2\,0), (1\,\beta^2\,0), (\beta\,\beta^2\,0), (\beta^2\,\beta^2\,0),$

$(0\,0\,1), (1\,0\,1), (\beta\,0\,1), (\beta^2\,0\,1), (0\,1\,1), (1\,1\,1), (\beta\,1\,1), (\beta^2\,1\,1),$

$(0\,\beta\,1), (1\,\beta\,1), (\beta\,\beta\,1), (\beta^2\,\beta\,1), (0\,\beta^2\,1), (1\,\beta^2\,1), (\beta\,\beta^2\,1),$

$(\beta^2\,\beta^2\,1), (0\,0\,\beta), (1\,0\,\beta), (\beta\,0\,\beta), (\beta^2\,0\,\beta), (0\,1\,\beta), (1\,1\,\beta), (\beta\,1\,\beta),$

$(\beta^2\,1\,\beta), (0\,\beta\,\beta), (1\,\beta\,\beta), (\beta\,\beta\,\beta), (\beta^2\,\beta\,\beta), (0\,\beta^2\,\beta), (1\,\beta^2\,\beta), (\beta\,\beta^2\,\beta),$

$(\beta^2\,\beta^2\,\beta), (0\,0\,\beta^2), (1\,0\,\beta^2), (\beta\,0\,\beta^2), (\beta^2\,0\,\beta^2), (0\,1\,\beta^2), (1\,1\,\beta^2), (\beta\,1\,\beta^2),$

$(\beta^2\,1\,\beta^2), (0\,\beta\,\beta^2), (1\,\beta\,\beta^2), (\beta\,\beta\,\beta^2), (\beta^2\,\beta\,\beta^2), (0\,\beta^2\,\beta^2), (1\,\beta^2\,\beta^2),$
$(\beta\,\beta^2\,\beta^2), (\beta^2\,\beta^2\,\beta^2).$

Slide #4. Let $r = 4$, $q = 2^r = 2^4$ and construct GF(2^4) from $h(x) = x^4 + x + 1$ just as in Table 5.1, p. 114. Let, for instance,

$$\alpha_1 = 1,\ \alpha_2 = \beta^5,\ \alpha_3 = \beta^9.$$

Then

$$\begin{aligned} g(x) &= (x+\alpha_1)\cdot(x+\alpha_2)\cdot(x+\alpha_3) \\ &= (x+1)\cdot(x+\beta^5)\cdot(x+\beta^9) \\ &= x^3 + \beta^{13}x^2 + \beta^8 x + \beta^{14} \end{aligned}$$

generates a cyclic code of length $n = 2^r - 1 = 15$ over GF(2^4). Note that the coefficients of $g(x)$ are not necessarily binary, that is, they do not necessarily belong to the binary field $K = \mathrm{GF}(2) = \{0, 1\}$.

Slide #6. Derivation of a parity-check matrix for the Reed-Solomon code. Observe that

$$v = (v_0, v_1, v_2, \ldots, v_{n-1}) \in RS(2^r, \delta)$$

or

$$v(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_{n-1} x^{n-1} \in RS(2^r, \delta)$$

if and only if

$$v(\beta^{m+1}) = v(\beta^{m+2}) = \cdots = v(\beta^{m+\delta-1}) = 0,$$

that is, if and only if

$$\begin{cases} v(\beta^{m+1}) = v_0 + v_1\beta^{m+1} + v_2(\beta^{m+1})^2 + \cdots v_{n-1}(\beta^{m+1})^{n-1} = 0 \\ v(\beta^{m+2}) = v_0 + v_1\beta^{m+2} + v_2(\beta^{m+2})^2 + \cdots v_{n-1}(\beta^{m+2})^{n-1} = 0 \\ \cdots \\ v(\beta^{m+\delta-1}) = v_0 + v_1\beta^{m+\delta-1} + v_2(\beta^{m+\delta-1})^2 + \cdots v_{n-1}(\beta^{m+\delta-1})^{n-1} = 0. \end{cases}$$

The above system can be written as $(v_0, v_1, \ldots, v_{n-1}) \cdot H = 0$ where

$$H = \begin{bmatrix} 1 & 1 & & 1 \\ \beta^{m+1} & \beta^{m+2} & & \beta^{m+\delta-1} \\ (\beta^{m+1})^2 & (\beta^{m+2})^2 & \cdots & (\beta^{m+\delta-1})^2 \\ \vdots & \vdots & & \vdots \\ (\beta^{m+1})^{n-1} & (\beta^{m+2})^{n-1} & \cdots & (\beta^{m+\delta-1})^{n-1} \end{bmatrix}.$$

Slide #7. Recall:

$$\det \begin{bmatrix} ka_{11} & ka_{12} & \cdots & ka_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = k \cdot \det \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}.$$

* * *

Slide #7. Let $x_1, x_2, \dots, x_n$ be any elements of a field (finite or not). The *Vandermonde* determinant of order n is defined as

$$V := \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}.$$

It is possible to show that

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Property: If $x_1, x_2, \dots, x_n$ are all distinct, then $V \neq 0$.