RS code 是基于有限域的一种编码算法，有限域又称为 Galois Field，是以法国著名数学家 Galois 命名的，在 RS code 中使用 $GF(2^w)$，其中 $2^w \geq n+m$。

RS code 定义了一个 $(n+m)*n$ 的 Distribution Matrix。

$$\boldsymbol{B} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ B_{11} & B_{12} & B_{13} & B_{14} & B_{15} \\ B_{21} & B_{22} & B_{23} & B_{24} & B_{25} \\ B_{31} & B_{32} & B_{33} & B_{34} & B_{35} \end{bmatrix}$$

对于每一段数据，都可以通过 $\boldsymbol{B} * \boldsymbol{D}$ 得到。

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ B_{11} & B_{12} & B_{13} & B_{14} & B_{15} \\ B_{21} & B_{22} & B_{23} & B_{24} & B_{25} \\ B_{31} & B_{32} & B_{33} & B_{34} & B_{35} \end{bmatrix} \times \begin{bmatrix} D_1 \\ D_2 \\ D_3 \\ D_4 \\ D_5 \end{bmatrix} = \begin{bmatrix} D_1 \\ D_2 \\ D_3 \\ D_4 \\ D_5 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix}$$

假如 D_1、D_4、C_2 失效，通过从矩阵 $\boldsymbol{B}$ 和 $\boldsymbol{B} * \boldsymbol{D}$ 中去掉相应的行（$\boldsymbol{B'}$ 和 Survivors，可以得到如下等式：

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ B_{11} & B_{12} & B_{13} & B_{14} & B_{15} \\ B_{31} & B_{32} & B_{33} & B_{34} & B_{35} \end{bmatrix} \times \begin{bmatrix} D_1 \\ D_2 \\ D_3 \\ D_4 \\ D_5 \end{bmatrix} = \begin{bmatrix} D_2 \\ D_3 \\ D_5 \\ C_1 \\ C_3 \end{bmatrix}$$

$$\boldsymbol{B'} \times \boldsymbol{D} = \boldsymbol{Survivors}$$

等式左右两端乘以 $\boldsymbol{B'}$ 矩阵的逆，即可求得 $\boldsymbol{D}$