Coding Theory: Reed-Solomon Codes

Generalized Reed-Solomon codes

Choose nonzero $v_1, \ldots, v_n$ and distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. Set $\mathbf{v} = (v_1, \ldots, v_n)$ and $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$. For $k \leq n$: $GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) =$ $\{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)), f(X$ $\mathbb{F}_q[X],\ \deg f(X) \leq$ $k-1\}$.

If $\mathbf{v}$ is the whole 1 vector, we speak of Reed-Solomon codes.

Choose distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. For $k \leq n$: $GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{1}) = \{(f(\alpha_1), \ldots, f(\alpha_n)), f(X) \in \mathbb{F}_q[X],\ \deg f(X) \leq k-1\}$.

Choose distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. For $k \leq n$: $GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{1}) = \{(f(\alpha_1), \ldots, f(\alpha_n)), f(X) \in \mathbb{F}_q[X],\ \deg f(X) \leq k-1\}$.

- Take $\mathbb{F}_q = \mathbb{F}_4$.
- Choose $\alpha_1 = 1$, $\alpha_2 = w$, $\alpha_3 = w^2$ (thus $n = 3$).
- Choose $k = 2$, so $f(X) = f_0 + f_1 X$.
- $GRS_{3,2}((1, w, w^2), \mathbf{1}) = \{(f_0 + f_1, f_0 + f_1 w, f_0 + f_1 w^2),\ f_0, f_1 \in \mathbb{F}_4\}$.

$GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ are MDS codes.

Length $= n \leq |\mathbb{F}_q|$, dimension $= k$, we need to prove that $d = n - k + 1$.

Every codeword is of the form $(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n))$, for a coordinate to be 0, we need $f(\alpha_i)$ to be zero, this means α_i is a zero of f, but f has degree at most $k-1$, so the weight is $n-$(number of zeros) $\geq n-(k-1) = n-k+1$, but the Singleton bound tells us that the weight should be $\leq n-k+1$, thus equality.

$GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)), f(X) \in \mathbb{F}_q[X],\ \deg f(X) \leq k-1\}$.

$$\begin{bmatrix} v_1 & v_2 & \ldots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \ldots & v_n\alpha_n \\ \vdots & & & \vdots \\ v_1\alpha_1^i & v_2\alpha_2^i & \ldots & v_n\alpha_n^i \\ \vdots & & & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \ldots & v_n\alpha_n^{k-1} \end{bmatrix}$$

$GRS_{3,2}((1,w,w^2),\mathbf{1}) = \{(f_0+f_1, f_0+f_1w, f_0+f_1w^2),\ f_0,f_1 \in \mathbb{F}_4\}.$

$GRS_{3,2}((1, w, w^2), \mathbf{1}) = \{(f_0 + f_1, f_0 + f_1 w, f_0 + f_1 w^2),\ f_0, f_1 \in \mathbb{F}_4\}$.

$$[f_0, f_1] \begin{bmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \end{bmatrix}$$

Exercise. Construct an MDS code of length 9 and rate 1/3.

Exercise. Construct an MDS code of length 9 and rate 1/3.

To have a rate of 1/3, recall that the rate is $k/n = 1/3$. Since we know $n = 9$, it means $k = 3$.

Exercise. Construct an MDS code of length 9 and rate 1/3.

To have a rate of 1/3, recall that the rate is $k/n = 1/3$. Since we know $n = 9$, it means $k = 3$. To build a length $n = 9$ Reed-Solomon code, we could use $\mathbb{F}_9$.

Exercise. Construct an MDS code of length 9 and rate 1/3.

To have a rate of 1/3, recall that the rate is $k/n = 1/3$. Since we know $n = 9$, it means $k = 3$. To build a length $n = 9$ Reed-Solomon code, we could use $\mathbb{F}_9$. $GRS_{9,k}(\boldsymbol{\alpha}, \mathbf{1}) = \{(f(\alpha_1), \ldots, f(\alpha_9)), f(X) \in \mathbb{F}_9[X],\ \deg f(X) \leq k-1\}$.

$\cdot$	0	1	w	w^2
0	0	0	0	0
1	0	1	w	w^2
w	0	w	w^2	1
w^2	0	w^2	1	w

$$
\begin{aligned}
\mathbf{w} &= (w^0, w^1, w^2) \\
\mathbf{w}^{(a)} &= ((w^0)^a, (w^1)^a, (w^2)^a) \\
&= (w^{a0}, w^{a1}, w^{a2}). \\
\mathbf{w}^{(1)} &= ((w^0)^1, (w^1)^1, (w^2)^1) = \mathbf{w} \\
\mathbf{w}^{(0)} &= ((w^0)^0, (w^1)^0, (w^2)^0) = \mathbf{1}
\end{aligned}
$$

$\cdot$	0	1	w	w^2
0	0	0	0	0
1	0	1	w	w^2
w	0	w	w^2	1
w^2	0	w^2	1	w

$$\begin{aligned} \mathbf{w} &= (w^0, w^1, w^2) \\ \mathbf{w}^{(a)} &= ((w^0)^a, (w^1)^a, (w^2)^a) \\ &= (w^{a0}, w^{a1}, w^{a2}). \\ \mathbf{w}^{(1)} &= ((w^0)^1, (w^1)^1, (w^2)^1) = \mathbf{w} \\ \mathbf{w}^{(0)} &= ((w^0)^0, (w^1)^0, (w^2)^0) = \mathbf{1} \end{aligned}$$

Choose nonzero $v_1 = w^{a0}, \ldots, v_n = w^{a(n-1)}$ and distinct $\alpha_1 = w^0, \ldots, \alpha_n = w^{n-1} \in \mathbb{F}_q$. Set $\mathbf{v} = (w^{a0}, \ldots, w^{a(n-1)}) = \mathbf{w}^{(a)}$ and $\boldsymbol{\alpha} = (w^0, \ldots, w^{n-1})$. For $k \leq n$:
$GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) = \{(w^{a0} f(w^0), \ldots, w^{a(n-1)} f(w^{n-1})), f(X) \in \mathbb{F}_q[X], \ \deg f(X) \leq k-1\}$.

Set $\mathbf{v} = (w^{a0}, w^{a1}, w^{a2})$ and $\boldsymbol{\alpha} = (w^0, w^1, w^2)$. For $k \leq 3$:
$GRS_{3,k}(\boldsymbol{\alpha}, \mathbf{v}) = \{(w^{a0} f(w^0), w^{a1} f(w), w^{a2} f(w^2)), f(X) \in \mathbb{F}_q[X],\ \deg f(X) \leq k-1\}$.
Say $k = 2$:

$$\begin{bmatrix} w^{a0} & w^{a1} & w^{a2} \\ w^{a0} w^0 & w^{a1} w & w^{a2} w^2 \end{bmatrix} = \begin{bmatrix} \mathbf{w}^{(a)} \\ \mathbf{w}^{(a+1)} \end{bmatrix}$$

For $k \leq n$:
$GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) = \{(w^{a0}f(w^0), \ldots, w^{a(n-1)}f(w^{n-1})), f(X) \in \mathbb{F}_q[X],\ \deg f(X) \leq k-1\}$.

$$\begin{bmatrix} w^{a0} & w^{a1} & \ldots & w^{a(n-1)} \\ w^{a0}w^0 & w^{a1}w^1 & \ldots & w^{a(n-1)}w^{n-1} \\ \vdots & & & \vdots \\ w^{a0}(w^0)^i & w^{a1}(w^1)^i & \ldots & w^{a(n-1)}(w^{n-1})^i \\ \vdots & & & \vdots \\ w^{a0}(w^0)^{k-1} & w^{a1}(w^1)^{k-1} & \ldots & w^{a(n-1)}(w^{n-1})^{k-1} \end{bmatrix} = \begin{bmatrix} \mathbf{w}^{(a)} \\ \mathbf{w}^{(a+1)} \\ \vdots \\ \mathbf{w}^{(a+i)} \\ \vdots \\ \mathbf{w}^{(a+(n-1))} \end{bmatrix}$$

A shift of $\mathbf{w}^{(a)}$ is a scalar multiple of $\mathbf{w}^{(a)}$.

Shift $\mathbf{w}^{(a)} = (w^{0a}, w^{1a}, w^{2a})$ to get $(w^{2a}, w^{0a}, w^{1a}) = w^{-a}(w^{0a}, w^{1a}, w^{2a}) = w^{-a}\mathbf{w}^{(a)}$ [recall $w^3 = 1$ thus $w^2 = w^{-1}$].

This works more generally for a $w \in \mathbb{F}_q$ such that $w, w^2, \ldots, w^{n-1}, w^n = 1$:
Take $\mathbf{w}^{(a)} = (w^{0a}, w^{1a}, \ldots, w^{(n-1)a})$ and shift it to get $(w^{(n-1)a}, w^{0a}, w^{1a}, \ldots, w^{(n-2)a}) = w^{-a}(w^{0a}, w^{1a}, \ldots, w^{(n-1)a}) = w^{-a}\mathbf{w}^{(a)}$.

For $k \leq n$:
$GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) = \{(w^{a0} f(w^0), \ldots, w^{a(n-1)} f(w^{n-1})), f(X) \in \mathbb{F}_q[X],\ \deg f(X) \leq k-1\}$.

$$\begin{bmatrix} w^{a0} & w^{a1} & \ldots & w^{a(n-1)} \\ w^{a0} w^0 & w^{a1} w^1 & \ldots & w^{a(n-1)} w^{n-1} \\ \vdots & & & \vdots \\ w^{a0} (w^0)^i & w^{a1} (w^1)^i & \ldots & w^{a(n-1)} (w^{n-1})^i \\ \vdots & & & \vdots \\ w^{a0} (w^0)^{k-1} & w^{a1} (w^1)^{k-1} & \ldots & w^{a(n-1)} (w^{n-1})^{k-1} \end{bmatrix} = \begin{bmatrix} \mathbf{w}^{(a)} \\ \mathbf{w}^{(a+1)} \\ \vdots \\ \mathbf{w}^{(a+i)} \\ \vdots \\ \mathbf{w}^{(a+(n-1))} \end{bmatrix}$$

Shifts of every row is a scalar multiple of the row, thus the code is cyclic.

$GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ with $\boldsymbol{\alpha} = \mathbf{w}$ and $\mathbf{v} = \mathbf{w}^{(a)}$ are cyclic Reed-Solomon codes.

$GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ with $\boldsymbol{\alpha} = \mathbf{w}$ and $\mathbf{v} = \mathbf{w}^{(a)}$ are cyclic Reed-Solomon codes.

They are said to be narrow-sense if $a = 0$. In this case, Reed-Solomon codes are often interpreted in terms of polynomial evaluation and interpolation.

$GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ with $\boldsymbol{\alpha} = \mathbf{w}$ and $\mathbf{v} = \mathbf{w}^{(a)}$ are cyclic Reed-Solomon codes.

They are said to be narrow-sense if $a = 0$. In this case, Reed-Solomon codes are often interpreted in terms of polynomial evaluation and interpolation.

They are said to be primitive if $n = |\mathbb{F}_q| - 1$. Since the length is limited by the size of the field, one may want large fields to have large lengths.

Reed-Solomon codes

MDS, length, cyclic