Twisted Reed–Solomon Codes and preliminary work on their Decoding

Peter Beelen[1], Martin Bossert[2] Sven Puchinger[3], Johan Rosenkilde[1]

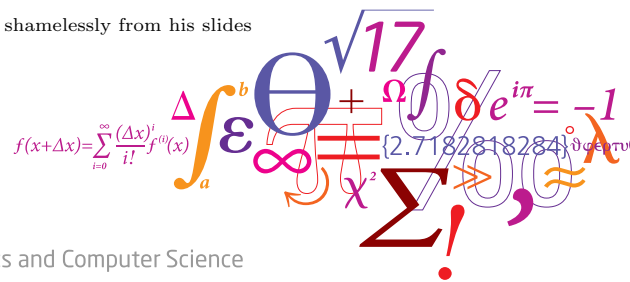
[1]Technical University of Denmark

[2]Technical University of Ulm

[3]Technical University of München

†: Thanks to Sven for letting me steal shamelessly from his slides

Zürich 27/03/2019



DTU Compute
Department of Applied Mathematics and Computer Science

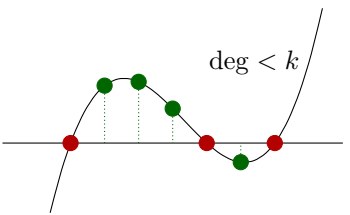
Reed–Solomon Codes – and Beyond?

Definition

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ distinct and $k < n$. Reed–Solomon (RS) code:

$$\mathcal{C}_{\mathrm{RS}}(n,k) = \Big\{ \big(f(\alpha_1), \ldots, f(\alpha_n)\big) : f \in \mathbb{F}_q[x], \deg f < k \Big\}$$

Maximum distance separable (MDS): $d = n - k + 1$



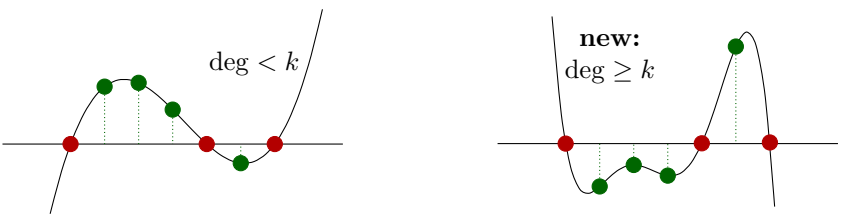
Reed–Solomon Codes – and Beyond?

Definition

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ distinct and $k < n$. Reed–Solomon (RS) code:

$$\mathcal{C}_{\mathrm{RS}}(n,k) = \Big\{ \big(f(\alpha_1), \ldots, f(\alpha_n)\big) : f \in \mathbb{F}_q[x], \deg f < k \Big\}$$

Maximum distance separable (MDS): $d = n - k + 1$



$$\#\,\bullet < k \quad \Rightarrow \quad \#\,\bullet \geq n - k + 1$$

Idea

Describe $\mathbb{F}_q$-linear spaces of polynomials of degree $\geq k$ which each having $< k$ roots among $\alpha_1, \ldots, \alpha_n \implies$ New MDS codes!

A Simple Twist of Fate

$f_0, \ldots, f_{k-1} \in \mathbb{F}_q$

$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1}$

A Simple Twist of Fate

$f_0, \ldots, f_{k-1} \in \mathbb{F}_q$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1}$$

Similar to Twisted Gabidulin Codes [Sheekey, 2017]

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} + \eta f_0 x^k \qquad \eta \in \mathbb{F}_q$$

A Simple Twist of Fate

$f_0, \ldots, f_{k-1} \in \mathbb{F}_q$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1}$$

Similar to Twisted Gabidulin Codes [Sheekey, 2017]

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} + \eta f_0 x^k \qquad \eta \in \mathbb{F}_q$$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} + \eta f_0 x^{k-1+t} \qquad 0 < t < n - k$$

A Simple Twist of Fate

$f_0, \ldots, f_{k-1} \in \mathbb{F}_q$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1}$$

Similar to Twisted Gabidulin Codes [Sheekey, 2017]

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} + \eta f_0 x^k \qquad \eta \in \mathbb{F}_q$$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} + \eta f_0 x^{k-1+t} \qquad 0 < t < n - k$$

$$f(x) = f_0 + \cdots + f_h x^h + \cdots + f_{k-1} x^{k-1} + \eta f_h x^{k-1+t} \qquad 0 \leq h < k$$

- h: the hook;
- t: the twist;
- η: the twist coefficient

Twisting an RS Code

Definition

$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$ all distinct, $\eta \in \mathbb{F}_q$, $h < k < n$, and $0 < t < n - k$.
Twisted RS Code:

$$\mathcal{C}_{\mathrm{TRS}}(n,k) = \left\{ \underbrace{\big(f(\alpha_1), \ldots, f(\alpha_n)\big)}_{\mathrm{ev}(f)} \;\middle|\; \underbrace{f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_h x^{k-1+t}}_{\text{the twisted polynomials}},\ f_i \in \mathbb{F}_q \right\}$$

How do we choose t, h, $\eta \in \mathbb{F}_q$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ s.t. $\mathcal{C}_{\mathrm{TRS}}$ is ...

- ... MDS?
- ... not equivalent to an RS code?[1]

[1] ... or any other known MDS code (e.g. Roth–Lempel codes).

Overview

1. Reed–Solomon: What's twists got to do with it? ✓
2. Infinitely many twisted MDS codes should be enough for everyone
3. Why twist once when you can twist twice?
4. That's all very nice - but can you decode?
5. What else can we say about twisted codes?

MDS when the hook is zero

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_0 x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_0 x^k \neq 0$ has $< k$ roots among the α_i.

MDS when the hook is zero

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_0 x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_0 x^k \neq 0$ has $< k$ roots among the α_i.

- Assume

$$f(x) = \eta f_0 \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$

where $|\mathcal{I}| = k$ and $f_0 \neq 0$.

MDS when the hook is zero

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_0 x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_0 x^k \neq 0$ has $< k$ roots among the α_i.

- Assume

$$f(x) = \eta f_0 \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$

  where $|\mathcal{I}| = k$ and $f_0 \neq 0$.

- Then

$$f_0 = (-1)^k \eta f_0 \prod_{i \in \mathcal{I}} \alpha_i$$

MDS when the hook is zero

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_0 x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_0 x^k \neq 0$ has $< k$ roots among the α_i.

- Assume

$$f(x) = \eta f_0 \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$

  where $|\mathcal{I}| = k$ and $f_0 \neq 0$.

- Then

$$f_0 = (-1)^k \eta f_0 \prod_{i \in \mathcal{I}} \alpha_i$$

- i.e.

$$(-1)^k \eta^{-1} = \prod_{i \in \mathcal{I}} \alpha_i \ .$$

MDS when the hook is zero

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_0 x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_0 x^k \neq 0$ has $< k$ roots among the α_i.

- Assume

$$f(x) = \eta f_0 \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$

  where $|\mathcal{I}| = k$ and $f_0 \neq 0$.

- Then

$$f_0 = (-1)^k \eta f_0 \prod_{i \in \mathcal{I}} \alpha_i$$

- i.e.

$$(-1)^k \eta^{-1} = \prod_{i \in \mathcal{I}} \alpha_i \ .$$

- So we should choose η so that $(-1)^k \eta^{-1}$ avoids any k-product of the α_i.

MDS when the hook is zero

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_0 x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_0 x^k \neq 0$ has $< k$ roots among the α_i.

- Assume
$$f(x) = \eta f_0 \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$
where $|\mathcal{I}| = k$ and $f_0 \neq 0$.
- Then
$$f_0 = (-1)^k \eta f_0 \prod_{i \in \mathcal{I}} \alpha_i$$
- i.e.
$$(-1)^k \eta^{-1} = \prod_{i \in \mathcal{I}} \alpha_i \ .$$
- So we should choose η so that $(-1)^k \eta^{-1}$ avoids any k-product of the α_i.

$\Leftarrow$: **Choose all α_i in some mult. subgroup $G \subsetneq \mathbb{F}_q^*$ and $(-1)^k \eta^{-1} \notin G$**

$(*)$-twisted Reed-Solomon Codes

Theorem

Let $(t, h) = (0, 0)$. Let G be a proper subgroup of $(\mathbb{F}_q^*, \cdot)$.
Let $\alpha_1, \ldots, \alpha_n \in G \cup \{0\}$ and $\eta \neq 0$ such that $(-1)^k \eta^{-1} \notin G$.
Then the corresponding twisted RS Code is MDS.

Possible code lengths for q odd:

- Choose $|G| = \frac{q-1}{2}$ $\quad \Rightarrow n \leq \frac{q+1}{2}$ possible
- Any $\alpha_1, \ldots, \alpha_n$ with $n > \frac{q+1}{2}$ results in a non-MDS code.

  Follows from [Roth, Lempel 1992] using *k-sum generators*.

MDS when the hook is $k-1$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_{k-1} x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_{k-1} x^k \neq 0$ has $< k$ roots among α_i.

MDS when the hook is $k-1$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_{k-1} x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_{k-1} x^k \neq 0$ has $< k$ roots among α_i.

- Assume

$$f(x) = \eta f_{k-1} \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$

where $|\mathcal{I}| = k$ and $f_{k-1} \neq 0$.

MDS when the hook is $k-1$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_{k-1} x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_{k-1} x^k \neq 0$ has $< k$ roots among α_i.

- Assume
$$f(x) = \eta f_{k-1} \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$
where $|\mathcal{I}| = k$ and $f_{k-1} \neq 0$.
- Then
$$f_{k-1} = -\eta f_{k-1} \sum_{i \in \mathcal{I}} \alpha_i$$

MDS when the hook is $k-1$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_{k-1} x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_{k-1} x^k \neq 0$ has $< k$ roots among α_i.

- Assume
$$f(x) = \eta f_{k-1} \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$
where $|\mathcal{I}| = k$ and $f_{k-1} \neq 0$.
- Then
$$f_{k-1} = -\eta f_{k-1} \sum_{i \in \mathcal{I}} \alpha_i$$
- i.e.
$$-\eta^{-1} = \sum_{i \in \mathcal{I}} \alpha_i \ .$$

MDS when the hook is $k-1$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_{k-1} x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_{k-1} x^k \neq 0$ has $< k$ roots among α_i.

- Assume
$$f(x) = \eta f_{k-1} \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$
where $|\mathcal{I}| = k$ and $f_{k-1} \neq 0$.
- Then
$$f_{k-1} = -\eta f_{k-1} \sum_{i \in \mathcal{I}} \alpha_i$$
- i.e.
$$-\eta^{-1} = \sum_{i \in \mathcal{I}} \alpha_i \ .$$
- So we should choose η so that $-\eta^{-1}$ avoids any k-sum of the α_i.

MDS when the hook is $k-1$

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \quad + \eta f_{k-1} x^k$$

We want that $f(x) = \sum_{i=0}^{k-1} f_i x^i + \eta f_{k-1} x^k \neq 0$ has $< k$ roots among α_i.

- Assume
$$f(x) = \eta f_{k-1} \prod_{i \in \mathcal{I}} (x - \alpha_i) \ ,$$
where $|\mathcal{I}| = k$ and $f_{k-1} \neq 0$.
- Then
$$f_{k-1} = -\eta f_{k-1} \sum_{i \in \mathcal{I}} \alpha_i$$
- i.e.
$$-\eta^{-1} = \sum_{i \in \mathcal{I}} \alpha_i \ .$$
- So we should choose η so that $-\eta^{-1}$ avoids any k-sum of the α_i.

$\Leftarrow$: **Choose all α_i in some additive subgroup $V \subsetneq \mathbb{F}_q$ and $\eta^{-1} \notin V$**

(+)-twisted Reed–Solomon Codes

Theorem

Let $(t, h) = (0, k-1)$. Let V be proper subgroup of $(\mathbb{F}_q, +)$.
Let $\alpha_1, \ldots, \alpha_n \in V$ and $\eta^{-1} \in \mathbb{F}_q \setminus V$.
Then the corresponding twisted RS Codes is MDS.

Possible code lengths for $q = 2^m$:

- Choose $V \subset \mathbb{F}_{2^m}$ to be $(m-1)$-dimensional $\implies n \leq q/2 + 1$ possible
- Any $\alpha_1, \ldots, \alpha_n, \eta$ results in a non-MDS code when

$$n > \begin{cases} q/2 + 1, & 3 < k < \frac{q}{2} - 3 \\ q/2 + 2, & k = 3 \text{ or } k = \frac{q}{2} - 3 \end{cases}$$

MDS for any twist and hook?

$$f(x) = f_0 + \cdots + f_h x^h + \cdots + f_{k-1} x^{k-1} + \eta f_h x^{k-1+t}$$

MDS for any twist and hook?

$$f(x) = f_0 + \cdots + f_h x^h + \cdots + f_{k-1}x^{k-1} \qquad +\eta f_h x^{k-1+t}$$

- A generator matrix for the code is

$$G = \begin{bmatrix} \alpha_1^0 & \alpha_2^0 & \cdots & \alpha_n^0 \\ \vdots & & \vdots & \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \alpha_1^h + \eta\alpha_1^{k-1+t} & \alpha_2^h + \eta\alpha_2^{k-1+t} & \cdots & \alpha_n^h + \eta\alpha_n^{k-1+t} \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \vdots & & \vdots & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}$$

MDS for any twist and hook?

$$f(x) = f_0 + \cdots + f_h x^h + \cdots + f_{k-1}x^{k-1} \qquad +\eta f_h x^{k-1+t}$$

- A generator matrix for the code is

$$G = \begin{bmatrix} \alpha_1^0 & \alpha_2^0 & \cdots & \alpha_n^0 \\ \vdots & & \vdots & \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \alpha_1^h + \eta\alpha_1^{k-1+t} & \alpha_2^h + \eta\alpha_2^{k-1+t} & \cdots & \alpha_n^h + \eta\alpha_n^{k-1+t} \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \vdots & & \vdots & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}$$

- So $\det G_{\mathcal{I}} = T_{\mathcal{I}}^{(0)} + \eta T_{\mathcal{I}}^{(1)}$, where $T_{\mathcal{I}}^{(0)}, T_{\mathcal{I}}^{(1)} \in \mathbb{F}_q[\alpha_{i_1}, \ldots, \alpha_{i_k}]$.

MDS for any twist and hook?

$$f(x) = f_0 + \cdots + f_h x^h + \cdots + f_{k-1}x^{k-1} \qquad +\eta f_h x^{k-1+t}$$

- A generator matrix for the code is

$$G = \begin{bmatrix} \alpha_1^0 & \alpha_2^0 & \cdots & \alpha_n^0 \\ \vdots & & \vdots & \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \alpha_1^h + \eta\alpha_1^{k-1+t} & \alpha_2^h + \eta\alpha_2^{k-1+t} & \cdots & \alpha_n^h + \eta\alpha_n^{k-1+t} \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \vdots & & \vdots & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}$$

- So $\det G_{\mathcal{I}} = T_{\mathcal{I}}^{(0)} + \eta T_{\mathcal{I}}^{(1)}$, where $T_{\mathcal{I}}^{(0)}, T_{\mathcal{I}}^{(1)} \in \mathbb{F}_q[\alpha_{i_1}, \ldots, \alpha_{i_k}]$.
- $T_{\mathcal{I}}^{(0)} \neq 0$ since $\eta = 0$ is an RS code which is MDS.

MDS for any twist and hook?

$$f(x) = f_0 + \cdots + f_h x^h + \cdots + f_{k-1}x^{k-1} \qquad +\eta f_h x^{k-1+t}$$

- A generator matrix for the code is

$$G = \begin{bmatrix} \alpha_1^0 & \alpha_2^0 & \cdots & \alpha_n^0 \\ \vdots & & \vdots & \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \alpha_1^h + \eta\alpha_1^{k-1+t} & \alpha_2^h + \eta\alpha_2^{k-1+t} & \cdots & \alpha_n^h + \eta\alpha_n^{k-1+t} \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \vdots & & \vdots & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}$$

- So $\det G_{\mathcal{I}} = T_{\mathcal{I}}^{(0)} + \eta T_{\mathcal{I}}^{(1)}$, where $T_{\mathcal{I}}^{(0)}, T_{\mathcal{I}}^{(1)} \in \mathbb{F}_q[\alpha_{i_1}, \ldots, \alpha_{i_k}]$.
- $T_{\mathcal{I}}^{(0)} \neq 0$ since $\eta = 0$ is an RS code which is MDS.
- We should choose η such that $T_{\mathcal{I}}^{(0)} + \eta T_{\mathcal{I}}^{(1)} \neq 0$ for any choice of $\mathcal{I}$.

MDS for any twist and hook?

$$f(x) = f_0 + \cdots + f_h x^h + \cdots + f_{k-1}x^{k-1} \qquad +\eta f_h x^{k-1+t}$$

- A generator matrix for the code is

$$G = \begin{bmatrix} \alpha_1^0 & \alpha_2^0 & \cdots & \alpha_n^0 \\ \vdots & & \vdots & \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \alpha_1^h + \eta\alpha_1^{k-1+t} & \alpha_2^h + \eta\alpha_2^{k-1+t} & \cdots & \alpha_n^h + \eta\alpha_n^{k-1+t} \\ \alpha_1^{h-1} & \alpha_2^{h-1} & \cdots & \alpha_n^{h-1} \\ \vdots & & \vdots & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}$$

- So $\det G_{\mathcal{I}} = T_{\mathcal{I}}^{(0)} + \eta T_{\mathcal{I}}^{(1)}$, where $T_{\mathcal{I}}^{(0)}, T_{\mathcal{I}}^{(1)} \in \mathbb{F}_q[\alpha_{i_1}, \ldots, \alpha_{i_k}]$.
- $T_{\mathcal{I}}^{(0)} \neq 0$ since $\eta = 0$ is an RS code which is MDS.
- We should choose η such that $T_{\mathcal{I}}^{(0)} + \eta T_{\mathcal{I}}^{(1)} \neq 0$ for any choice of $\mathcal{I}$.

$\Leftarrow$: **Choose all α_i in some subfield $\mathbb{F}_s \subsetneq \mathbb{F}_q$ and $\eta \in \mathbb{F}_q \setminus \mathbb{F}_s$**

Exotic twists

Theorem

Let $\mathbb{F}_s \subsetneq \mathbb{F}_q$ be a subfield. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_s$ and let $\eta \in \mathbb{F}_q \setminus \mathbb{F}_s$. Then for any (t, h) the corresponding twisted RS Code is MDS.

- So for $q = p^{2m}$ we can get $n = p^m = \sqrt{q}$.
- **What about larger n?**

Exotic twists

Theorem

Let $\mathbb{F}_s \subsetneq \mathbb{F}_q$ be a subfield. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_s$ and let $\eta \in \mathbb{F}_q \setminus \mathbb{F}_s$. Then for any (t, h) the corresponding twisted RS Code is MDS.

- So for $q = p^{2m}$ we can get $n = p^m = \sqrt{q}$.
- **What about larger n?**
- We don't know! Computer search indicates that $\approx q/2$ is possible:

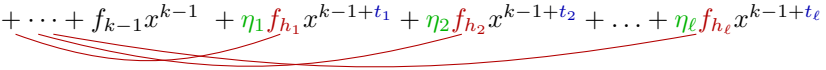
Proposition

For $q \leq 19$, then for **any** choice of (t, h), and **any** k with $3 \leq k \leq n-3$, there is an MDS twisted RS code $\neq$ GRS with $n = \lfloor n/2 \rfloor$, except when

$$(t, h) = (1, k-1) \quad \text{and} \quad (q, k) = (17, 4), (19, *) \ .$$

Multiple Twists

$$f(x) = f_0 + \cdots + f_{k-1}x^{k-1} + \eta_1 f_{h_1} x^{k-1+t_1} + \eta_2 f_{h_2} x^{k-1+t_2} + \ldots + \eta_\ell f_{h_\ell} x^{k-1+t_\ell}$$



Theorem

Let $\mathbb{F}_{s_0} \subsetneq \mathbb{F}_{s_1} \subsetneq \ldots \subsetneq \mathbb{F}_{s_\ell} = \mathbb{F}_q$ be a chain of subfields of $\mathbb{F}_q$. If $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{s_0}$, and $\eta_i \in \mathbb{F}_{s_i} \setminus \mathbb{F}_{s_{i-1}}$, then for any valid choice of $(t_1, h_1), \ldots, (t_\ell, h_\ell)$, the corresponding twisted RS code is MDS.

Multiple Twists

$$f(x) = f_0 + \cdots + f_{k-1}x^{k-1} + \eta_1 f_{h_1} x^{k-1+t_1} + \eta_2 f_{h_2} x^{k-1+t_2} + \ldots + \eta_\ell f_{h_\ell} x^{k-1+t_\ell}$$

Theorem

Let $\mathbb{F}_{s_0} \subsetneq \mathbb{F}_{s_1} \subsetneq \ldots \subsetneq \mathbb{F}_{s_\ell} = \mathbb{F}_q$ be a chain of subfields of $\mathbb{F}_q$. If $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{s_0}$, and $\eta_i \in \mathbb{F}_{s_i} \setminus \mathbb{F}_{s_{i-1}}$, then for any valid choice of $(t_1, h_1), \ldots, (t_\ell, h_\ell)$, the corresponding twisted RS code is MDS.

- So $n \approx q^{1/2^\ell}$. That's pretty short

Multiple Twists

$$f(x) = f_0 + \cdots + f_{k-1}x^{k-1} + \eta_1 f_{h_1} x^{k-1+t_1} + \eta_2 f_{h_2} x^{k-1+t_2} + \ldots + \eta_\ell f_{h_\ell} x^{k-1+t_\ell}$$

Theorem

Let $\mathbb{F}_{s_0} \subsetneq \mathbb{F}_{s_1} \subsetneq \ldots \subsetneq \mathbb{F}_{s_\ell} = \mathbb{F}_q$ be a chain of subfields of $\mathbb{F}_q$. If $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{s_0}$, and $\eta_i \in \mathbb{F}_{s_i} \setminus \mathbb{F}_{s_{i-1}}$, then for any valid choice of $(t_1, h_1), \ldots, (t_\ell, h_\ell)$, the corresponding twisted RS code is MDS.

- So $n \approx q^{1/2^\ell}$. That's pretty short
- Another new construction has $n \approx q^{1/\ell}$. Better, but still pretty bad.

Multiple Twists

$$f(x) = f_0 + \cdots + f_{k-1}x^{k-1} + \eta_1 f_{h_1} x^{k-1+t_1} + \eta_2 f_{h_2} x^{k-1+t_2} + \ldots + \eta_\ell f_{h_\ell} x^{k-1+t_\ell}$$

Theorem

Let $\mathbb{F}_{s_0} \subsetneq \mathbb{F}_{s_1} \subsetneq \ldots \subsetneq \mathbb{F}_{s_\ell} = \mathbb{F}_q$ be a chain of subfields of $\mathbb{F}_q$. If $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{s_0}$, and $\eta_i \in \mathbb{F}_{s_i} \setminus \mathbb{F}_{s_{i-1}}$, then for any valid choice of $(t_1, h_1), \ldots, (t_\ell, h_\ell)$, the corresponding twisted RS code is MDS.

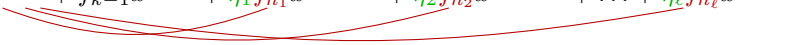
- So $n \approx q^{1/2^\ell}$. That's pretty short
- Another new construction has $n \approx q^{1/\ell}$. Better, but still pretty bad.
- **Open question: Can we get longer ℓ-twisted codes that are MDS?**

Decoding ℓ-twisted codes

Decoding: Take 1

Let $\mathcal{C}$ be a twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.

$$f(x) = f_0 + \cdots + f_{k-1}x^{k-1} + \eta_1 f_{h_1} x^{k-1+t_1} + \eta_2 f_{h_2} x^{k-1+t_2} + \ldots + \eta_\ell f_{h_\ell} x^{k-1+t_\ell}$$



Decoding: Take 1

Let $\mathcal{C}$ be a twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.

$$f(x) = f_0 + \cdots + f_{k-1}x^{k-1} + \eta_1 f_{h_1} x^{k-1+t_1} + \eta_2 f_{h_2} x^{k-1+t_2} + \ldots + \eta_\ell f_{h_\ell} x^{k-1+t_\ell}$$

Then $\mathcal{C} \subseteq \mathcal{D}$, where $\mathcal{D}$ is the $[n, k']$ RS code with $k' = k + t_\ell$.

Decoding: Take 1

Let $\mathcal{C}$ be a twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.

$$f(x) = f_0 + \cdots + f_{k-1}x^{k-1} + \eta_1 f_{h_1} x^{k-1+t_1} + \eta_2 f_{h_2} x^{k-1+t_2} + \ldots + \eta_\ell f_{h_\ell} x^{k-1+t_\ell}$$

Then $\mathcal{C} \subseteq \mathcal{D}$, where $\mathcal{D}$ is the $[n, k']$ RS code with $k' = k + t_\ell$.

We can decode up to $(n - k')/2$ errors in $\mathcal{D}$ in complexity $O\tilde{}(n)$:-).

Decoding: Take 1

Let $\mathcal{C}$ be a twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.

$$f(x) = f_0 + \cdots + f_{k-1}x^{k-1} + \eta_1 f_{h_1} x^{k-1+t_1} + \eta_2 f_{h_2} x^{k-1+t_2} + \ldots + \eta_\ell f_{h_\ell} x^{k-1+t_\ell}$$

Then $\mathcal{C} \subseteq \mathcal{D}$, where $\mathcal{D}$ is the $[n, k']$ RS code with $k' = k + t_\ell$.

We can decode up to $(n - k')/2$ errors in $\mathcal{D}$ in complexity $O\tilde{}(n)$:-).

This is usually far from $(n - k)/2$:-(

Decoding: Take 2

Let $\mathcal{C}$ be a twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.

Decoding: Take 2

Let $\mathcal{C}$ be a twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.

The sent codeword was $\boldsymbol{c} = \mathrm{ev}(f)$, where

$$f(x) = \sum_{i=0}^{k-1} f_i x^i + \sum_{j=1}^{\ell} \eta_j f_{h_j} x^{k-1+t_j} \ .$$

We receive $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$.

Decoding: Take 2

Let $\mathcal{C}$ be a twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.

The sent codeword was $\boldsymbol{c} = \mathrm{ev}(f)$, where

$$f(x) = \sum_{i=0}^{k-1} f_i x^i + \sum_{j=1}^{\ell} \eta_j f_{h_j} x^{k-1+t_j} \ .$$

We receive $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$.

Let $f'_{h_1}, f'_{h_2}, \ldots, f'_{h_\ell} \in \mathbb{F}_q$ be a guess for the values $f_{h_1}, f_{h_2}, \ldots, f_{h_\ell} \in \mathbb{F}_q$.

Compute

$$\boldsymbol{r}' = \boldsymbol{r} - \mathrm{ev}\left(\sum_{j=1}^{\ell} \eta_j f'_{h_j} x^{k-1+t_j} \right) = \boldsymbol{c}' + \boldsymbol{e} \ .$$

Decoding: Take 2

Let $\mathcal{C}$ be a twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.

The sent codeword was $\boldsymbol{c} = \mathrm{ev}(f)$, where

$$f(x) = \sum_{i=0}^{k-1} f_i x^i + \sum_{j=1}^{\ell} \eta_j f_{h_j} x^{k-1+t_j} \ .$$

We receive $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$.

Let $f'_{h_1}, f'_{h_2}, \ldots, f'_{h_\ell} \in \mathbb{F}_q$ be a guess for the values $f_{h_1}, f_{h_2}, \ldots, f_{h_\ell} \in \mathbb{F}_q$.

Compute

$$\boldsymbol{r}' = \boldsymbol{r} - \mathrm{ev}\left(\sum_{j=1}^{\ell} \eta_j f'_{h_j} x^{k-1+t_j} \right) = \boldsymbol{c}' + \boldsymbol{e} \ .$$

Guess correct: $\boldsymbol{c}' = \mathrm{ev}(\sum_{i=0}^{k-1} f_i x^i) \in \mathcal{D}$, where $\mathcal{D}$ is the $[n, k]$ RS code.
$\implies$ Decode $\boldsymbol{r}'$ in $\mathcal{D}$ in complexity $O\tilde{}(n)$.

Decoding: Take 2

Let $\mathcal{C}$ be a twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.

The sent codeword was $\boldsymbol{c} = \mathrm{ev}(f)$, where

$$f(x) = \sum_{i=0}^{k-1} f_i x^i + \sum_{j=1}^{\ell} \eta_j f_{h_j} x^{k-1+t_j} \ .$$

We receive $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$.

Let $f'_{h_1}, f'_{h_2}, \ldots, f'_{h_\ell} \in \mathbb{F}_q$ be a guess for the values $f_{h_1}, f_{h_2}, \ldots, f_{h_\ell} \in \mathbb{F}_q$.

Compute

$$\boldsymbol{r}' = \boldsymbol{r} - \mathrm{ev}\left(\sum_{j=1}^{\ell} \eta_j f'_{h_j} x^{k-1+t_j} \right) = \boldsymbol{c}' + \boldsymbol{e} \ .$$

Guess correct: $\boldsymbol{c}' = \mathrm{ev}(\sum_{i=0}^{k-1} f_i x^i) \in \mathcal{D}$, where $\mathcal{D}$ is the $[n, k]$ RS code.
$\implies$ Decode $\boldsymbol{r}'$ in $\mathcal{D}$ in complexity $O\tilde{}(n)$.

We need q^ℓ guesses to be successful, i.e. cost is $O\tilde{}(q^\ell n)$:-(
The algorithm list-decodes up to $(n-k)/2$ errors even when $\mathcal{C}$ is not MDS :-)

Decoding: Take 3

Decoding: Take 3

Let's review a classical way to decode RS codes:
Say $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ and $\boldsymbol{c} = \mathrm{ev}(f)$ with $\deg f < k$.
Then

$$\Lambda(x)R(x) \equiv \Lambda(x)f(x) \mod G(x) \text{ , where}$$

$$G(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

$$R(x): \ R(\alpha_i) = r_i \wedge \deg R < n$$

$$\Lambda(x) = \prod_{i|e_i \neq 0}(x - \alpha_i) \qquad \text{the "error locator"}$$

Decoding: Take 3

Let's review a classical way to decode RS codes:
Say $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ and $\boldsymbol{c} = \mathrm{ev}(f)$ with $\deg f < k$.
Then

$$\Lambda(x)R(x) \equiv \Lambda(x)f(x) \mod G(x) \text{ , where}$$

$$G(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

$$R(x): \ R(\alpha_i) = r_i \wedge \deg R < n$$

$$\Lambda(x) = \prod_{i|e_i \neq 0}(x - \alpha_i) \qquad \text{the "error locator"}$$

Theorem

Let $\lambda(x), \psi(x)$ be solutions to the following (linear) constraints:

1. $\lambda R \equiv \psi \mod G$
2. $\max\big(\deg \lambda;\ \deg \psi - k + 1\big)$ is minimal
3. λ is monic

If $\mathrm{wt}(\boldsymbol{e}) < (n-k)/2$, then $\lambda = \Lambda$ and $\psi = \Lambda f$.

Decoding: Take 3

Consider single-twisted RS code with parameters (t, h, η).
Let $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ with $\boldsymbol{c} = \mathrm{ev}(f)$ and
$f(x) = \underbrace{f_0 + f_1 x + \ldots + f_{k-1} x^{k-1}}_{\hat{f}(x)} + \eta f_h x^{k-1+t}$.

Then

$$\Lambda(x) R(x) \equiv \Lambda(x)(\hat{f} + \eta f_h x^{k-1+t}) \mod G(x)$$

i.e.

$$\Lambda(x) R(x) - (f_h \Lambda(x)) \eta x^{k-1+t} \equiv \Lambda(x) \hat{f}(x) \mod G(x)$$

Decoding: Take 3

Consider single-twisted RS code with parameters (t, h, η).
Let $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ with $\boldsymbol{c} = \mathrm{ev}(f)$ and
$f(x) = \underbrace{f_0 + f_1 x + \ldots + f_{k-1} x^{k-1}}_{\hat{f}(x)} + \eta f_h x^{k-1+t}$.

Then

$$\Lambda(x)R(x) \equiv \Lambda(x)(\hat{f} + \eta f_h x^{k-1+t}) \mod G(x)$$

i.e.

$$\Lambda(x)R(x) - (f_h \Lambda(x))\eta x^{k-1+t} \equiv \Lambda(x)\hat{f}(x) \mod G(x)$$

Observation

Let $\lambda_1(x), \lambda_2(x), \psi(x)$ be solutions to the following linear constraints:

1. $\lambda_1(x)R(x) + \lambda_2(x)\eta x^{k-1+t} \equiv \psi(x) \mod G(x)$.
2. $\max(\deg \lambda_1;\ \deg \lambda_2;\ \deg \psi - k + 1)$ is minimal.
3. $\lambda_1(x)$ is monic.

If $\boldsymbol{e}$ is random with $\mathrm{wt}(\boldsymbol{e}) < (n-k)/3$, then $\lambda_1(x) = \Lambda(x)$ seems to occur almost always.

Decoding: Take 3

Consider single-twisted RS code with parameters (t, h, η).
Let $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ with $\boldsymbol{c} = \mathrm{ev}(f)$ and
$f(x) = \underbrace{f_0 + f_1 x + \ldots + f_{k-1} x^{k-1}}_{\hat{f}(x)} + \eta f_h x^{k-1+t}$.

Then

$$\Lambda(x)R(x) \equiv \Lambda(x)(\hat{f} + \eta f_h x^{k-1+t}) \mod G(x)$$

i.e.

$$\Lambda(x)R(x) - (f_h \Lambda(x))\eta x^{k-1+t} \equiv \Lambda(x)\hat{f}(x) \mod G(x)$$

Observation

Let $\lambda_1(x), \lambda_2(x), \psi(x)$ be solutions to the following linear constraints:

1. $\lambda_1(x)R(x) + \lambda_2(x)\eta x^{k-1+t} \equiv \psi(x) \mod G(x)$.
2. $\max(\deg \lambda_1;\ \deg \lambda_2;\ \deg \psi - k + 1)$ is minimal.
3. $\lambda_1(x)$ is monic.

If $\boldsymbol{e}$ is random with $\mathrm{wt}(\boldsymbol{e}) < (n-k)/3$, then $\lambda_1(x) = \Lambda(x)$ seems to occur almost always.

We can solve for the constraints in $O^{\sim}(n)$ time :-)
$(n-k)/3$ is far from $(n-k)/2$:-(
We don't know how to prove if the algorithm always works :-(

Decoding: Take 4

Continue with single-twisted RS code with parameters (t, h, η).
Since

$$\Lambda(x)R(x) - (f_h\Lambda(x))\eta x^{k-1+t} \equiv \Lambda(x)\hat{f}(x) \mod G(x) ,$$

then also for any $i \in \mathbb{Z}_{\geq 0}$:

$$(f_h^i\Lambda(x))R(x) - (f_h^{i+1}\Lambda(x))\eta x^{k-1+t} \equiv f_h^i\Lambda(x)\hat{f}(x) \mod G(x) ,$$

Decoding: Take 4

Continue with single-twisted RS code with parameters (t, h, η).
Since

$$\Lambda(x)R(x) - (f_h\Lambda(x))\eta x^{k-1+t} \equiv \Lambda(x)\hat{f}(x) \mod G(x) ,$$

then also for any $i \in \mathbb{Z}_{\geq 0}$:

$$(f_h^i\Lambda(x))R(x) - (f_h^{i+1}\Lambda(x))\eta x^{k-1+t} \equiv f_h^i\Lambda(x)\hat{f}(x) \mod G(x) ,$$

Observation

Let $m \in \mathbb{Z}_{>0}$. Let $\lambda_1(x), \ldots, \lambda_{m+1}(x), \psi_1(x), \ldots, \psi_m(x)$ be solutions to the following linear constraints:

1. $\lambda_i(x)R(x) + \lambda_{i+1}(x)\eta x^{k-1+t} \equiv \psi_i(x) \mod G(x)$ for $i = 1, \ldots, m$.
2. $\max(\deg \lambda_i;\ \deg \psi_j - k + 1)_{i,j}$ is minimal.
3. $\lambda_1(x)$ is monic.

Assume random $\boldsymbol{e}$ with $\mathrm{wt}(\boldsymbol{e}) < \frac{m}{2(m+1)}(n-k)$. Then $\lambda_1(x) = \Lambda(x)$ seems to occur almost always.

Decoding: Take 4

Continue with single-twisted RS code with parameters (t, h, η).
Since

$$\Lambda(x)R(x) - (f_h\Lambda(x))\eta x^{k-1+t} \equiv \Lambda(x)\hat{f}(x) \mod G(x) ,$$

then also for any $i \in \mathbb{Z}_{\geq 0}$:

$$(f_h^i\Lambda(x))R(x) - (f_h^{i+1}\Lambda(x))\eta x^{k-1+t} \equiv f_h^i\Lambda(x)\hat{f}(x) \mod G(x) ,$$

Observation

Let $m \in \mathbb{Z}_{>0}$. Let $\lambda_1(x), \ldots, \lambda_{m+1}(x), \psi_1(x), \ldots, \psi_m(x)$ be solutions to the following linear constraints:

1. $\lambda_i(x)R(x) + \lambda_{i+1}(x)\eta x^{k-1+t} \equiv \psi_i(x) \mod G(x)$ for $i = 1, \ldots, m$.
2. $\max(\deg \lambda_i;\ \deg \psi_j - k + 1)_{i,j}$ is minimal.
3. $\lambda_1(x)$ is monic.

Assume random $\boldsymbol{e}$ with $\mathrm{wt}(\boldsymbol{e}) < \frac{m}{2(m+1)}(n-k)$. Then $\lambda_1(x) = \Lambda(x)$ seems to occur almost always.

We can solve for the constraints in roughly $O\tilde{}(m^3 n)$ time :-)
Decoding arbitrarily close to $(n-k)/2$:-)
We don't know how to prove when the algorithm works :-(

What else do we know about twisted RS codes?

When is a twisted RS code $\mathcal{C}$ not a GRS code?

Answer: When it doesn't behave like a GRS code!

When is a twisted RS code $\mathcal{C}$ not a GRS code?

Answer: When it doesn't behave like a GRS code!
Consider the *Schur square* of an $[n, k]$ linear code $\mathcal{C}$:

$$\mathcal{C}^2 := \langle \boldsymbol{c}_1 \star \boldsymbol{c}_2 \mid \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C} \rangle_{\mathbb{F}_q},$$

where $(c_{11}, \ldots, c_{1n}) \star (c_{21}, \ldots, c_{2n}) = (c_{11}c_{21}, \ldots, c_{1n}c_{2n})$.

When is a twisted RS code $\mathcal{C}$ not a GRS code?

Answer: When it doesn't behave like a GRS code!
Consider the *Schur square* of an $[n, k]$ linear code $\mathcal{C}$:

$$\mathcal{C}^2 := \langle \boldsymbol{c}_1 \star \boldsymbol{c}_2 \mid \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C} \rangle_{\mathbb{F}_q},$$

where $(c_{11}, \ldots, c_{1n}) \star (c_{21}, \ldots, c_{2n}) = (c_{11}c_{21}, \ldots, c_{1n}c_{2n})$.

If $\boldsymbol{c}_1 = \mathrm{ev}(f_1)$ and $\boldsymbol{c}_2 = \mathrm{ev}(f_2)$ for polynomials $f_1(x), f_2(x)$.

When is a twisted RS code $\mathcal{C}$ not a GRS code?

Answer: When it doesn't behave like a GRS code!
Consider the *Schur square* of an $[n, k]$ linear code $\mathcal{C}$:

$$\mathcal{C}^2 := \langle \boldsymbol{c}_1 \star \boldsymbol{c}_2 \mid \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C} \rangle_{\mathbb{F}_q},$$

where $(c_{11}, \ldots, c_{1n}) \star (c_{21}, \ldots, c_{2n}) = (c_{11}c_{21}, \ldots, c_{1n}c_{2n})$.

If $\boldsymbol{c}_1 = \mathrm{ev}(f_1)$ and $\boldsymbol{c}_2 = \mathrm{ev}(f_2)$ for polynomials $f_1(x), f_2(x)$.
Then $\boldsymbol{c}_1 \star \boldsymbol{c}_2 = \mathrm{ev}(f_1 \cdot f_2)$.

When is a twisted RS code $\mathcal{C}$ not a GRS code?

Answer: When it doesn't behave like a GRS code!
Consider the *Schur square* of an $[n, k]$ linear code $\mathcal{C}$:

$$\mathcal{C}^2 := \langle \boldsymbol{c}_1 \star \boldsymbol{c}_2 \mid \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C} \rangle_{\mathbb{F}_q},$$

where $(c_{11}, \ldots, c_{1n}) \star (c_{21}, \ldots, c_{2n}) = (c_{11}c_{21}, \ldots, c_{1n}c_{2n})$.

If $\boldsymbol{c}_1 = \mathrm{ev}(f_1)$ and $\boldsymbol{c}_2 = \mathrm{ev}(f_2)$ for polynomials $f_1(x), f_2(x)$.
Then $\boldsymbol{c}_1 \star \boldsymbol{c}_2 = \mathrm{ev}(f_1 \cdot f_2)$.
Evaluation at $\alpha_1, \ldots, \alpha_n$ is an $\mathbb{F}_q$-linear isomorphism for polys of degree $< n$.

When is a twisted RS code $\mathcal{C}$ not a GRS code?

Answer: When it doesn't behave like a GRS code!
Consider the *Schur square* of an $[n, k]$ linear code $\mathcal{C}$:

$$\mathcal{C}^2 := \langle \boldsymbol{c}_1 \star \boldsymbol{c}_2 \mid \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C} \rangle_{\mathbb{F}_q},$$

where $(c_{11}, \ldots, c_{1n}) \star (c_{21}, \ldots, c_{2n}) = (c_{11}c_{21}, \ldots, c_{1n}c_{2n})$.

If $\boldsymbol{c}_1 = \mathrm{ev}(f_1)$ and $\boldsymbol{c}_2 = \mathrm{ev}(f_2)$ for polynomials $f_1(x), f_2(x)$.
Then $\boldsymbol{c}_1 \star \boldsymbol{c}_2 = \mathrm{ev}(f_1 \cdot f_2)$.
Evaluation at $\alpha_1, \ldots, \alpha_n$ is an $\mathbb{F}_q$-linear isomorphism for polys of degree $< n$.
So all distinct degrees $< n$ appearing as $f_1 \cdot f_2$ contribute a dimension to $\mathcal{C}^2$.

When is a twisted RS code $\mathcal{C}$ not a GRS code?

Answer: When it doesn't behave like a GRS code!
Consider the *Schur square* of an $[n, k]$ linear code $\mathcal{C}$:

$$\mathcal{C}^2 := \langle \boldsymbol{c}_1 \star \boldsymbol{c}_2 \mid \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C} \rangle_{\mathbb{F}_q},$$

where $(c_{11}, \ldots, c_{1n}) \star (c_{21}, \ldots, c_{2n}) = (c_{11}c_{21}, \ldots, c_{1n}c_{2n})$.

If $\boldsymbol{c}_1 = \mathrm{ev}(f_1)$ and $\boldsymbol{c}_2 = \mathrm{ev}(f_2)$ for polynomials $f_1(x), f_2(x)$.
Then $\boldsymbol{c}_1 \star \boldsymbol{c}_2 = \mathrm{ev}(f_1 \cdot f_2)$.
Evaluation at $\alpha_1, \ldots, \alpha_n$ is an $\mathbb{F}_q$-linear isomorphism for polys of degree $< n$.
So all distinct degrees $< n$ appearing as $f_1 \cdot f_2$ contribute a dimension to $\mathcal{C}^2$.

If $\mathcal{C}$ is GRS with $k < n/2$ then $\dim \mathcal{C}^2 = 2k - 1$.

When is a twisted RS code $\mathcal{C}$ not a GRS code?

Answer: When it doesn't behave like a GRS code!
Consider the *Schur square* of an $[n, k]$ linear code $\mathcal{C}$:

$$\mathcal{C}^2 := \langle \boldsymbol{c}_1 \star \boldsymbol{c}_2 \mid \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C} \rangle_{\mathbb{F}_q},$$

where $(c_{11}, \ldots, c_{1n}) \star (c_{21}, \ldots, c_{2n}) = (c_{11}c_{21}, \ldots, c_{1n}c_{2n})$.

If $\boldsymbol{c}_1 = \mathrm{ev}(f_1)$ and $\boldsymbol{c}_2 = \mathrm{ev}(f_2)$ for polynomials $f_1(x), f_2(x)$.
Then $\boldsymbol{c}_1 \star \boldsymbol{c}_2 = \mathrm{ev}(f_1 \cdot f_2)$.
Evaluation at $\alpha_1, \ldots, \alpha_n$ is an $\mathbb{F}_q$-linear isomorphism for polys of degree $< n$.
So all distinct degrees $< n$ appearing as $f_1 \cdot f_2$ contribute a dimension to $\mathcal{C}^2$.

If $\mathcal{C}$ is GRS with $k < n/2$ then $\dim \mathcal{C}^2 = 2k - 1$.

Proposition

Let $\mathcal{C}$ be an $[n, k]$ twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.
Let $D = \{0, 1, \ldots, k-1\} \setminus \{h_i \mid i = 1, \ldots, \ell\} \cup \{k - 1 + t_i \mid i = 1, \ldots, \ell\}$. Then

$$\dim \mathcal{C}^2 \geq |\{d_1 + d_2 \mid d_1, d_2 \in D \wedge d_1 + d_2 < n\}| \, .$$

When is a twisted RS code $\mathcal{C}$ not a GRS code?

Answer: When it doesn't behave like a GRS code!
Consider the *Schur square* of an $[n, k]$ linear code $\mathcal{C}$:

$$\mathcal{C}^2 := \langle \boldsymbol{c}_1 \star \boldsymbol{c}_2 \mid \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C} \rangle_{\mathbb{F}_q},$$

where $(c_{11}, \ldots, c_{1n}) \star (c_{21}, \ldots, c_{2n}) = (c_{11}c_{21}, \ldots, c_{1n}c_{2n})$.

If $\boldsymbol{c}_1 = \mathrm{ev}(f_1)$ and $\boldsymbol{c}_2 = \mathrm{ev}(f_2)$ for polynomials $f_1(x), f_2(x)$.
Then $\boldsymbol{c}_1 \star \boldsymbol{c}_2 = \mathrm{ev}(f_1 \cdot f_2)$.
Evaluation at $\alpha_1, \ldots, \alpha_n$ is an $\mathbb{F}_q$-linear isomorphism for polys of degree $< n$.
So all distinct degrees $< n$ appearing as $f_1 \cdot f_2$ contribute a dimension to $\mathcal{C}^2$.

If $\mathcal{C}$ is GRS with $k < n/2$ then $\dim \mathcal{C}^2 = 2k - 1$.

Proposition

Let $\mathcal{C}$ be an $[n, k]$ twisted RS code with twists $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$.
Let $D = \{0, 1, \ldots, k-1\} \setminus \{h_i \mid i = 1, \ldots, \ell\} \cup \{k - 1 + t_i \mid i = 1, \ldots, \ell\}$. Then

$$\dim \mathcal{C}^2 \geq |\{d_1 + d_2 \mid d_1, d_2 \in D \wedge d_1 + d_2 < n\}| \, .$$

$\Longrightarrow$: **For almost all twists, a twisted RS code is not GRS!**

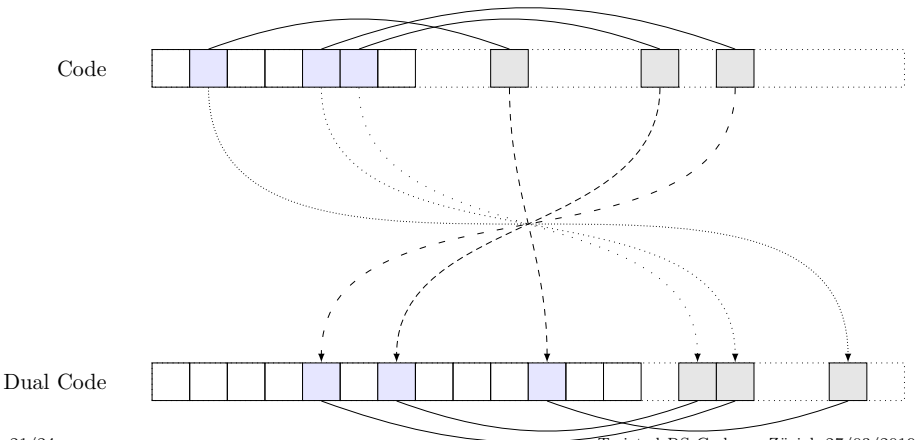
Duals of (some) twisted RS codes

Proposition

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ consist of a multiplicative subgroup of $\mathbb{F}_q^*$. Let $\mathcal{C}$ be an ℓ-twisted RS code with parameters $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$. Then $\mathcal{C}^\perp$ is again ℓ-twisted with parameters

$$t_i' = k - h_i \qquad h = n - k - t_i \qquad \eta' = -\eta_i$$

(up to column multipliers)



Duals of (some) twisted RS codes

$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) =$ multiplicative subgroup of $\mathbb{F}_q^*$. $\mathcal{C}$ is ℓ-twisted with parameters $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$. Then $\mathcal{C}^\perp$ is again ℓ-twisted with parameters

$$t_i' = k - h_i \qquad h = n - k - t_i \qquad \eta' = -\eta_i$$

Proof.

Let $\boldsymbol{V}$ be the $n \times n$ Vandermonde matrix, i.e. $\boldsymbol{V}[i,j] = \alpha_j^{i-1}$.

Duals of (some) twisted RS codes

$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) =$ multiplicative subgroup of $\mathbb{F}_q^*$. $\mathcal{C}$ is ℓ-twisted with parameters $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$. Then $\mathcal{C}^\perp$ is again ℓ-twisted with parameters

$$t_i' = k - h_i \qquad h = n - k - t_i \qquad \eta' = -\eta_i$$

Proof.

Let $\boldsymbol{V}$ be the $n \times n$ Vandermonde matrix, i.e. $\boldsymbol{V}[i,j] = \alpha_j^{i-1}$.
A generator matrix for $\mathcal{C}$ is

$$\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{L}] \cdot \boldsymbol{V}$$

where $\boldsymbol{L}[h_i + 1, t_i] = \eta_i$ for $i = 1, \ldots, \ell$, and $\boldsymbol{L}$ is 0 elsewhere.

Duals of (some) twisted RS codes

$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) =$ multiplicative subgroup of $\mathbb{F}_q^*$. $\mathcal{C}$ is ℓ-twisted with parameters $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$. Then $\mathcal{C}^\perp$ is again ℓ-twisted with parameters

$$t_i' = k - h_i \qquad h = n - k - t_i \qquad \eta' = -\eta_i$$

Proof.

Let $\boldsymbol{V}$ be the $n \times n$ Vandermonde matrix, i.e. $\boldsymbol{V}[i,j] = \alpha_j^{i-1}$.
A generator matrix for $\mathcal{C}$ is

$$\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{L}] \cdot \boldsymbol{V}$$

where $\boldsymbol{L}[h_i + 1, t_i] = \eta_i$ for $i = 1, \ldots, \ell$, and $\boldsymbol{L}$ is 0 elsewhere.

We seek a parity check matrix (up to column multipliers). Observe that for any $\boldsymbol{X}$:

$$\boldsymbol{G} \cdot \left(\boldsymbol{X} \left[-\boldsymbol{L}^{\mathrm{T}} \mid \boldsymbol{I} \right] \boldsymbol{V}^{-1} \right)^{\mathrm{T}} = \boldsymbol{0} \, .$$

Duals of (some) twisted RS codes

$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) =$ multiplicative subgroup of $\mathbb{F}_q^*$. $\mathcal{C}$ is ℓ-twisted with parameters $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$. Then $\mathcal{C}^\perp$ is again ℓ-twisted with parameters

$$t_i' = k - h_i \qquad h = n - k - t_i \qquad \eta' = -\eta_i$$

Proof.

Let $\boldsymbol{V}$ be the $n \times n$ Vandermonde matrix, i.e. $\boldsymbol{V}[i,j] = \alpha_j^{i-1}$.
A generator matrix for $\mathcal{C}$ is

$$\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{L}] \cdot \boldsymbol{V}$$

where $\boldsymbol{L}[h_i + 1, t_i] = \eta_i$ for $i = 1, \ldots, \ell$, and $\boldsymbol{L}$ is 0 elsewhere.

We seek a parity check matrix (up to column multipliers). Observe that for any $\boldsymbol{X}$:

$$\boldsymbol{G} \cdot \left(\boldsymbol{X} \big[-\boldsymbol{L}^{\mathrm{T}} \mid \boldsymbol{I} \big] \boldsymbol{V}^{-1} \right)^{\mathrm{T}} = \boldsymbol{0} \, .$$

$\boldsymbol{V}^{-1} = \boldsymbol{J} \cdot \boldsymbol{V} \cdot \mathrm{diag}(\boldsymbol{\alpha}/n) \simeq \boldsymbol{J} \cdot \boldsymbol{V}$, where $\boldsymbol{J}$ is the anti-diagonal identity matrix. So

$$\boldsymbol{X} \big[-\boldsymbol{L}^{\mathrm{T}} \mid \boldsymbol{I} \big] \boldsymbol{V}^{-1} \simeq \boldsymbol{X} \big[-\boldsymbol{L}^{\mathrm{T}} \mid \boldsymbol{I} \big] \boldsymbol{J} \boldsymbol{V} \simeq \big[\boldsymbol{X}\boldsymbol{J} \mid -\boldsymbol{X}\boldsymbol{L}^{\mathrm{T}}\boldsymbol{J} \big] \boldsymbol{V}$$

Duals of (some) twisted RS codes

$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) =$ multiplicative subgroup of $\mathbb{F}_q^*$. $\mathcal{C}$ is ℓ-twisted with parameters $(t_i, h_i, \eta_i)_{i=1,\ldots,\ell}$. Then $\mathcal{C}^\perp$ is again ℓ-twisted with parameters

$$t_i' = k - h_i \qquad h = n - k - t_i \qquad \eta' = -\eta_i$$

Proof.

Let $\boldsymbol{V}$ be the $n \times n$ Vandermonde matrix, i.e. $\boldsymbol{V}[i,j] = \alpha_j^{i-1}$.
A generator matrix for $\mathcal{C}$ is

$$\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{L}] \cdot \boldsymbol{V}$$

where $\boldsymbol{L}[h_i + 1, t_i] = \eta_i$ for $i = 1, \ldots, \ell$, and $\boldsymbol{L}$ is 0 elsewhere.

We seek a parity check matrix (up to column multipliers). Observe that for any $\boldsymbol{X}$:

$$\boldsymbol{G} \cdot \left(\boldsymbol{X}\big[-\boldsymbol{L}^{\mathrm{T}} \mid \boldsymbol{I}\big]\boldsymbol{V}^{-1}\right)^{\mathrm{T}} = \boldsymbol{0}\,.$$

$\boldsymbol{V}^{-1} = \boldsymbol{J} \cdot \boldsymbol{V} \cdot \mathrm{diag}(\boldsymbol{\alpha}/n) \simeq \boldsymbol{J} \cdot \boldsymbol{V}$, where $\boldsymbol{J}$ is the anti-diagonal identity matrix. So

$$\boldsymbol{X}\big[-\boldsymbol{L}^{\mathrm{T}} \mid \boldsymbol{I}\big]\boldsymbol{V}^{-1} \simeq \boldsymbol{X}\big[-\boldsymbol{L}^{\mathrm{T}} \mid \boldsymbol{I}\big]\boldsymbol{J}\boldsymbol{V} \simeq \big[\boldsymbol{X}\boldsymbol{J} \mid -\boldsymbol{X}\boldsymbol{L}^{\mathrm{T}}\boldsymbol{J}\big]\boldsymbol{V}$$

We want this to look like a generator matrix for a twisted code.
Since $\boldsymbol{J}\boldsymbol{J} = \boldsymbol{I}$, then setting $\boldsymbol{X} = \boldsymbol{J}$ seems like a good idea:

$$\simeq \big[\boldsymbol{I} \mid \boldsymbol{J}(-\boldsymbol{L}^{\mathrm{T}})\boldsymbol{J}\big]\boldsymbol{V}$$

Conclusion

We have:

- New MDS codes with $n \approx q/2$ from single $(+)$ or $(*)$ twists: $t = 1$ and $h = 0, k - 1$.
- New MDS codes with $n \approx \sqrt{q}$ from single exotic twists.
- New MDS codes with $n \approx \sqrt[\ell]{q}$ from ℓ exotic twists.
- Heuristic decoding of single twisted codes close to $(n - k)/2$ in time $\approx O\tilde{}(n)$.
- Maybe heuristic decoding of ℓ-twisted codes in time $\approx O\tilde{}(2^{3\ell}n)$.
- Broadly settled inequivalence to GRS codes.
- Duals of twisted codes when the α_i form a multiplicative group.

Twisted codes for fun and profit:

- Twisting Gabidulin codes is fun and easy.
  As usual, some stuff is the same, some is different.
- Twisted crypto?
  Carefully ℓ-twisted RS codes in McEliece seem to resist many attacks.
  Carefully ℓ-twisted Gabidulin codes in GPT has small key size.

Conclusion 2

We DON'T have:

- MDS codes of length $n \approx q/2$ for single exotic twists (though they seem to exist).
  In particular $t = 1$ and $h \notin \{0, k-1\}$: Need a fake group structure on symmetric expression in between $(\mathbb{F}_q, +)$ and $(\mathbb{F}_q^*, \cdot)$.
- MDS codes of length $> \sqrt[\ell]{q}$. Could something like $q/(\ell+1)$ be possible?
- Proofs of decoding success or bounds for decoding failure. Should require introducing the special choice of twist parameters, which seems hard.