New structural insights and a syndrome-based decoding approach for Trombetti–Zhou codes

Chunlei Li[1], **Angelica Piccirillo**[2], **Olga Polverino**[3], **Ferdinando Zullo**[3]

[1] Department of Informatics,
University of Bergen, Norway

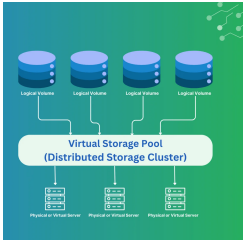
[2] Department of Mathematics,
Technische Universität München, Germany

[3] Dipartimento di Matematica e Fisica,
Università degli Studi della Campania "Luigi Vanvitelli", Italy

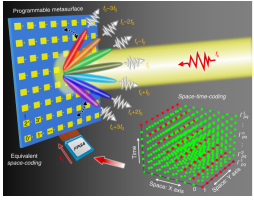
OpeRa 2026 - Bordeaux

27.02.2026

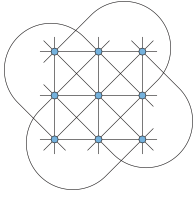
Code-based cryptography



Distributed storage

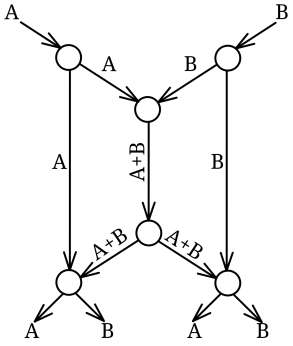


Space-time coding



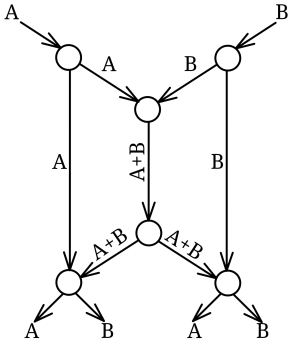
Finite Geometry

D. Silva, F. R. Kschischang and R. Kötter
A Rank-Metric Approach to Error Control in Random Network Coding
In: *IEEE Transactions on Information Theory* (2008).



Network coding

D. Silva, F. R. Kschischang and R. Kötter
A Rank-Metric Approach to Error Control in Random Network Coding
In: *IEEE Transactions on Information Theory* (2008).



Network coding

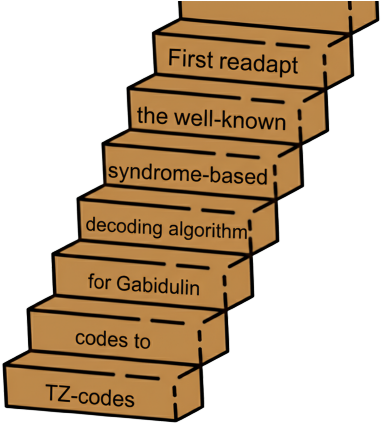
Gabidulin codes

- $k \leq n \leq m$
- $\mathcal{L}_k(\mathbb{F}_{q^m}) = \left\{ g_0 x + g_1 x^q + \ldots + g_{k-1} x^{q^{k-1}} \mid g_i \in \mathbb{F}_{q^m} \right\}$
- $\mathbb{F}_q$-linearly independent $\beta_0, \beta_1, \ldots, \beta_{n-1} \in \mathbb{F}_{q^m}$

$$\mathcal{G}_{n,k}(\underline{\beta}) = \left\{ (g(\beta_0), \ldots, g(\beta_{n-1})) \mid g(x) \in \mathcal{L}_k(\mathbb{F}_{q^m}) \right\} \subseteq \mathbb{F}_{q^m}^n$$

Readapt the Generalized decoding algorithm for Gabidulin codes arising from Random Network coding to Trombetti-Zhou codes.

Readapt the Generalized decoding algorithm for Gabidulin codes arising from Random Network coding to Trombetti-Zhou codes.



Trombetti-Zhou (TZ) codes

$$\mathbb{F}_{q^{2n}}^{2n} = \left\{\underline{x} = (x_0, \ldots, x_{2n-1}) : x_i \in \mathbb{F}_{q^{2n}}\right\}$$

R. Trombetti and Y. Zhou

A New Family of MRD Codes in $\mathbb{F}_q^{2n\times 2n}$ With Right and Middle Nuclei $\mathbb{F}_{q^n}$

In: *IEEE Transactions on Information Theory* 65.2 (2019), pp. 1054-1062.

Trombetti-Zhou (TZ) codes

$$\mathbb{F}_{q^{2n}}^{2n} = \left\{\underline{x} = (x_0, \ldots, x_{2n-1}) : x_i \in \mathbb{F}_{q^{2n}}\right\}$$

R. Trombetti and Y. Zhou

A New Family of MRD Codes in $\mathbb{F}_q^{2n\times 2n}$ With Right and Middle Nuclei $\mathbb{F}_{q^n}$

In: *IEEE Transactions on Information Theory* 65.2 (2019), pp. 1054-1062.

Let

- $k \leq 2n$;

Trombetti-Zhou (TZ) codes

$$\mathbb{F}_{q^{2n}}^{2n} = \left\{\underline{x} = (x_0, \ldots, x_{2n-1}) : x_i \in \mathbb{F}_{q^{2n}}\right\}$$

R. Trombetti and Y. Zhou

A New Family of MRD Codes in $\mathbb{F}_q^{2n\times 2n}$ With Right and Middle Nuclei $\mathbb{F}_{q^n}$

In: *IEEE Transactions on Information Theory* 65.2 (2019), pp. 1054-1062.

Let

- $k \leq 2n$;
- $\gamma \in \mathbb{F}_{q^{2n}}$ such that $N_{q^{2n}/q}(\gamma) = \gamma^{\frac{q^{2n}-1}{q-1}}$ is a non-square element in $\mathbb{F}_q$

$$\mathbb{F}_{q^{2n}}^{2n} = \left\{\underline{x} = (x_0, \ldots, x_{2n-1}) : x_i \in \mathbb{F}_{q^{2n}}\right\}$$

R. Trombetti and Y. Zhou

A New Family of MRD Codes in $\mathbb{F}_q^{2n\times 2n}$ With Right and Middle Nuclei $\mathbb{F}_{q^n}$

In: *IEEE Transactions on Information Theory* 65.2 (2019), pp. 1054-1062.

Let

- $k \leq 2n$;
- $\gamma \in \mathbb{F}_{q^{2n}}$ such that $N_{q^{2n}/q}(\gamma) = \gamma^{\frac{q^{2n}-1}{q-1}}$ is a non-square element in $\mathbb{F}_q$($\Rightarrow q$ CANNOT be even);

$$\mathbb{F}_{q^{2n}}^{2n} = \left\{\underline{x} = (x_0, \ldots, x_{2n-1}) : x_i \in \mathbb{F}_{q^{2n}}\right\}$$

R. Trombetti and Y. Zhou

A New Family of MRD Codes in $\mathbb{F}_q^{2n\times 2n}$ With Right and Middle Nuclei $\mathbb{F}_{q^n}$

In: *IEEE Transactions on Information Theory* 65.2 (2019), pp. 1054-1062.

Let

- $k \leq 2n$;
- $\gamma \in \mathbb{F}_{q^{2n}}$ such that $N_{q^{2n}/q}(\gamma) = \gamma^{\frac{q^{2n}-1}{q-1}}$ is a non-square element in $\mathbb{F}_q$($\Rightarrow q$ CANNOT be even);
- $\mathcal{D}_k(\gamma) = \left\{ax + f_1 x^q + f_2 x^{q^2} + \ldots + f_{k-1} x^{q^{k-1}} + \gamma b x^{q^k} : f_i \in \mathbb{F}_{q^{2n}},\ a, b \in \mathbb{F}_{q^n}\right\}$;

$$\mathbb{F}_{q^{2n}}^{2n} = \{\underline{x} = (x_0, \ldots, x_{2n-1}) : x_i \in \mathbb{F}_{q^{2n}}\}$$

R. Trombetti and Y. Zhou

A New Family of MRD Codes in $\mathbb{F}_q^{2n\times 2n}$ With Right and Middle Nuclei $\mathbb{F}_{q^n}$

In: *IEEE Transactions on Information Theory* 65.2 (2019), pp. 1054-1062.

Let

- $k \leq 2n$;
- $\gamma \in \mathbb{F}_{q^{2n}}$ such that $N_{q^{2n}/q}(\gamma) = \gamma^{\frac{q^{2n}-1}{q-1}}$ is a non-square element in $\mathbb{F}_q$ ($\Rightarrow q$ CANNOT be even);
- $\mathcal{D}_k(\gamma) = \left\{ax + f_1 x^q + f_2 x^{q^2} + \ldots + f_{k-1} x^{q^{k-1}} + \gamma b x^{q^k} : f_i \in \mathbb{F}_{q^{2n}},\ a, b \in \mathbb{F}_{q^n}\right\}$;
- $\lambda_0, \lambda_1, \ldots, \lambda_{2n-1}$, $\mathbb{F}_q$-linearly independent elements of $\mathbb{F}_{q^{2n}}$.

$$\mathbb{F}_{q^{2n}}^{2n} = \{\underline{x} = (x_0, \ldots, x_{2n-1}) : x_i \in \mathbb{F}_{q^{2n}}\}$$

R. Trombetti and Y. Zhou

A New Family of MRD Codes in $\mathbb{F}_q^{2n\times 2n}$ With Right and Middle Nuclei $\mathbb{F}_{q^n}$

In: *IEEE Transactions on Information Theory* 65.2 (2019), pp. 1054-1062.

Let

- $k \le 2n$;
- $\gamma \in \mathbb{F}_{q^{2n}}$ such that $N_{q^{2n}/q}(\gamma) = \gamma^{\frac{q^{2n}-1}{q-1}}$ is a non-square element in $\mathbb{F}_q$ ($\Rightarrow q$ CANNOT be even);
- $\mathcal{D}_k(\gamma) = \left\{ax + f_1 x^q + f_2 x^{q^2} + \ldots + f_{k-1} x^{q^{k-1}} + \gamma b x^{q^k} : f_i \in \mathbb{F}_{q^{2n}},\ a, b \in \mathbb{F}_{q^n}\right\}$;
- $\lambda_0, \lambda_1, \ldots, \lambda_{2n-1}$, $\mathbb{F}_q$-linearly independent elements of $\mathbb{F}_{q^{2n}}$.

$$\mathcal{TZ}_k(\gamma) = \{(f(\lambda_0), f(\lambda_1), \ldots, f(\lambda_{2n-1})) \in \mathbb{F}_{q^{2n}}^{2n} \mid f(x) \in \mathcal{D}_k(\gamma)\}$$

$$\mathbb{F}_{q^{2n}}^{2n} = \{\underline{x} = (x_0, \ldots, x_{2n-1}) : x_i \in \mathbb{F}_{q^{2n}}\}$$

R. Trombetti and Y. Zhou

A New Family of MRD Codes in $\mathbb{F}_q^{2n\times 2n}$ With Right and Middle Nuclei $\mathbb{F}_{q^n}$

In: *IEEE Transactions on Information Theory* 65.2 (2019), pp. 1054-1062.

Let

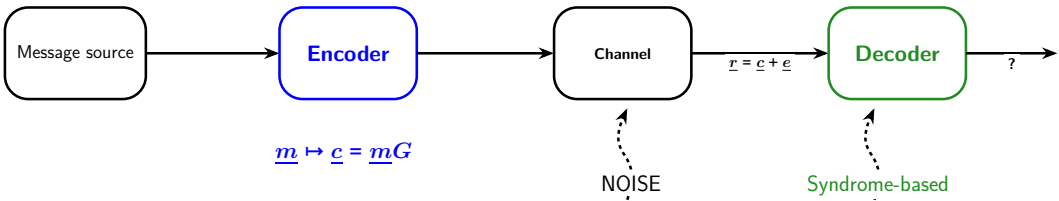
- $k \le 2n$;
- $\gamma \in \mathbb{F}_{q^{2n}}$ such that $N_{q^{2n}/q}(\gamma) = \gamma^{\frac{q^{2n}-1}{q-1}}$ is a non-square element in $\mathbb{F}_q$ ($\Rightarrow q$ CANNOT be even);
- $\mathcal{D}_k(\gamma) = \left\{ax + f_1 x^q + f_2 x^{q^2} + \ldots + f_{k-1} x^{q^{k-1}} + \gamma b x^{q^k} : f_i \in \mathbb{F}_{q^{2n}},\ a, b \in \mathbb{F}_{q^n}\right\}$;
- $\lambda_0, \lambda_1, \ldots, \lambda_{2n-1}$, $\mathbb{F}_q$-linearly independent elements of $\mathbb{F}_{q^{2n}}$.

$$\mathcal{TZ}_k(\gamma) = \{(f(\lambda_0), f(\lambda_1), \ldots, f(\lambda_{2n-1})) \in \mathbb{F}_{q^{2n}}^{2n} \mid f(x) \in \mathcal{D}_k(\gamma)\}$$

is an MRD q^n-$\left[2n, 2k, 2n-k+1\right]_{q^{2n}/q}$ code.

$\mathcal{TZ}_k(\gamma)$ codes are $\mathbb{F}_{q^n}$-linear codes in $\mathbb{F}_{q^{2n}}^{2n}$ and NOT $\mathbb{F}_{q^{2n}}$-linear!

$\mathcal{TZ}_k(\gamma)$ codes are $\mathbb{F}_{q^n}$-linear codes in $\mathbb{F}_{q^{2n}}^{2n}$ and NOT $\mathbb{F}_{q^{2n}}$-linear!



$\mathcal{TZ}_k(\gamma)$ codes are $\mathbb{F}_{q^n}$-linear codes in $\mathbb{F}_{q^{2n}}^{2n}$ and NOT $\mathbb{F}_{q^{2n}}$-linear!

~~Generator matrix and usual encoding~~

$\mathcal{TZ}_k(\gamma)$ codes are $\mathbb{F}_{q^n}$-linear codes in $\mathbb{F}_{q^{2n}}^{2n}$ and NOT $\mathbb{F}_{q^{2n}}$-linear!

~~Generator matrix and usual encoding~~

~~Parity-check matrix~~

$\mathcal{TZ}_k(\gamma)$ codes are $\mathbb{F}_{q^n}$-linear codes in $\mathbb{F}_{q^{2n}}^{2n}$ and NOT $\mathbb{F}_{q^{2n}}$-linear!

~~Generator matrix and usual encoding~~

~~Parity-check matrix~~

~~Syndrome~~

$\mathcal{TZ}_k(\gamma)$ codes are $\mathbb{F}_{q^n}$-linear codes in $\mathbb{F}_{q^{2n}}^{2n}$ and NOT $\mathbb{F}_{q^{2n}}$-linear!

$\mathbb{F}_{q^n}$-Generator matrix together with a slightly different encoding ✓

~~**Parity-check matrix**~~

~~**Syndrome**~~

$\mathcal{TZ}_k(\gamma)$ codes are $\mathbb{F}_{q^n}$-linear codes in $\mathbb{F}_{q^{2n}}^{2n}$ and NOT $\mathbb{F}_{q^{2n}}$-linear!

$\mathbb{F}_{q^n}$-**Generator matrix together with a slightly different encoding** ✓

$\mathbb{F}_{q^n}$-**Parity-check matrix** ✓

~~**Syndrome**~~

$\mathcal{TZ}_k(\gamma)$ codes are $\mathbb{F}_{q^n}$-linear codes in $\mathbb{F}_{q^{2n}}^{2n}$ and NOT $\mathbb{F}_{q^{2n}}$-linear!

$\mathbb{F}_{q^n}$-Generator matrix together with a slightly different encoding ✓

$\mathbb{F}_{q^n}$-Parity-check matrix ✓

$\mathbb{F}_{q^n}$-Syndrome ✓

$\mathbb{F}_{q^n}$-Generator Matrix and encoding of TZ-codes

$\mathcal{TZ}_k(\gamma) \subseteq \mathbb{F}_{q^{2n}}^{2n}$ are $\mathbb{F}_{q^n}$-linear codes of $\mathbb{F}_{q^{2n}}^{2n}$ of $\mathbb{F}_{q^n}$-dimension $2k$

$\mathbb{F}_{q^n}$-Generator Matrix and encoding of TZ-codes

$\mathcal{TZ}_k(\gamma) \subseteq \mathbb{F}_{q^{2n}}^{2n}$ are $\mathbb{F}_{q^n}$-linear codes of $\mathbb{F}_{q^{2n}}^{2n}$ of $\mathbb{F}_{q^n}$-dimension $2k$

$N_{q^{2n}/q}(\gamma)$ is a non-square element in $\mathbb{F}_q$ $\implies$ $\gamma \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ $\implies$ $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^n}(\gamma)$

$\mathcal{TZ}_k(\gamma) \subseteq \mathbb{F}_{q^{2n}}^{2n}$ are $\mathbb{F}_{q^n}$-linear codes of $\mathbb{F}_{q^{2n}}^{2n}$ of $\mathbb{F}_{q^n}$-dimension $2k$

$N_{q^{2n}/q}(\gamma)$ is a non-square element in $\mathbb{F}_q$ $\implies$ $\gamma \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ $\implies$ $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^n}(\gamma)$

$$\mathcal{D}_k(\gamma) = \left\{ ax + f_1 x^q + f_2 x^{q^2} + \ldots + f_{k-1} x^{q^{k-1}} + \gamma b x^{q^k} : f_i \in \mathbb{F}_{q^{2n}},\ a, b \in \mathbb{F}_{q^n} \right\}$$

$\mathbb{F}_{q^n}$-Generator Matrix and encoding of TZ-codes

$\mathcal{TZ}_k(\gamma) \subseteq \mathbb{F}_{q^{2n}}^{2n}$ are $\mathbb{F}_{q^n}$-linear codes of $\mathbb{F}_{q^{2n}}^{2n}$ of $\mathbb{F}_{q^n}$-dimension $2k$

$N_{q^{2n}/q}(\gamma)$ is a non-square element in $\mathbb{F}_q$ $\implies$ $\gamma \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ $\implies$ $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^n}(\gamma)$

$$\mathcal{D}_k(\gamma) = \left\langle x, x^q, \gamma x^q, \ldots, x^{q^{k-1}}, \gamma x^{q^{k-1}}, \gamma x^{q^k} \right\rangle_{\mathbb{F}_{q^n}}$$

$\mathcal{TZ}_k(\gamma) \subseteq \mathbb{F}_{q^{2n}}^{2n}$ are $\mathbb{F}_{q^n}$-linear codes of $\mathbb{F}_{q^{2n}}^{2n}$ of $\mathbb{F}_{q^n}$-dimension $2k$

$N_{q^{2n}/q}(\gamma)$ is a non-square element in $\mathbb{F}_q$ $\implies$ $\gamma \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ $\implies$ $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^n}(\gamma)$

$$\mathcal{D}_k(\gamma) = \left\langle x, x^q, \gamma x^q, \ldots, x^{q^{k-1}}, \gamma x^{q^{k-1}}, \gamma x^{q^k} \right\rangle_{\mathbb{F}_{q^n}}$$

$$G = \begin{pmatrix} \lambda_0 & \lambda_1 & \lambda_2 & \cdots & \lambda_{2n-1} \\ \lambda_0^q & \lambda_1^q & \lambda_2^q & \cdots & \lambda_{2n-1}^q \\ \gamma\lambda_0^q & \gamma\lambda_1^q & \gamma\lambda_2^q & \cdots & \gamma\lambda_{2n-1}^q \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_0^{q^{k-1}} & \lambda_1^{q^{k-1}} & \lambda_2^{q^{k-1}} & \cdots & \lambda_{2n-1}^{q^{k-1}} \\ \gamma\lambda_0^{q^{k-1}} & \gamma\lambda_1^{q^{k-1}} & \gamma\lambda_2^{q^{k-1}} & \cdots & \gamma\lambda_{2n-1}^{q^{k-1}} \\ \gamma\lambda_0^{q^k} & \gamma\lambda_1^{q^k} & \gamma\lambda_2^{q^k} & \cdots & \gamma\lambda_{2n-1}^{q^k} \end{pmatrix} \in \mathbb{F}_{q^{2n}}^{2k \times 2n} \tag{1}$$

$\mathcal{TZ}_k(\gamma) \subseteq \mathbb{F}_{q^{2n}}^{2n}$ are $\mathbb{F}_{q^n}$-linear codes of $\mathbb{F}_{q^{2n}}^{2n}$ of $\mathbb{F}_{q^n}$-dimension $2k$

$N_{q^{2n}/q}(\gamma)$ is a non-square element in $\mathbb{F}_q$ $\implies$ $\gamma \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ $\implies$ $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^n}(\gamma)$

$$\mathcal{D}_k(\gamma) = \left\langle x, x^q, \gamma x^q, \dots, x^{q^{k-1}}, \gamma x^{q^{k-1}}, \gamma x^{q^k} \right\rangle_{\mathbb{F}_{q^n}}$$

$$G = \begin{pmatrix} \lambda_0 & \lambda_1 & \lambda_2 & \dots & \lambda_{2n-1} \\ \lambda_0^q & \lambda_1^q & \lambda_2^q & \dots & \lambda_{2n-1}^q \\ \gamma\lambda_0^q & \gamma\lambda_1^q & \gamma\lambda_2^q & \dots & \gamma\lambda_{2n-1}^q \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_0^{q^{k-1}} & \lambda_1^{q^{k-1}} & \lambda_2^{q^{k-1}} & \dots & \lambda_{2n-1}^{q^{k-1}} \\ \gamma\lambda_0^{q^{k-1}} & \gamma\lambda_1^{q^{k-1}} & \gamma\lambda_2^{q^{k-1}} & \dots & \gamma\lambda_{2n-1}^{q^{k-1}} \\ \gamma\lambda_0^{q^k} & \gamma\lambda_1^{q^k} & \gamma\lambda_2^{q^k} & \dots & \gamma\lambda_{2n-1}^{q^k} \end{pmatrix} \in \mathbb{F}_{q^{2n}}^{2k \times 2n} \tag{2}$$

Encoding process:

$$\underline{\tilde{f}} = (a, f_{1,1}, f_{1,2}, \dots, f_{k-1,1}, f_{k-1,2}, b) \in \mathbb{F}_{q^n}^{2k} \mapsto \underline{c} = \underline{\tilde{f}} G \in \mathcal{TZ}_k(\gamma) \subseteq \mathbb{F}_{q^{2n}}^{2n}$$

The *syndrome* of $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$ is zero iff $\underline{a} \in \mathcal{C}$

$\mathbb{F}_{q^n}$-Parity-Check Matrix and $\mathbb{F}_{q^n}$-syndrome

The *syndrome* of $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$ is zero iff $\underline{a} \in \mathcal{C}$

The usual inner product DOES NOT "preserve" the $\mathbb{F}_{q^n}$-linearity!

$\mathbb{F}_{q^n}$-Parity-Check Matrix and $\mathbb{F}_{q^n}$-syndrome

The *syndrome* of $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$ is zero iff $\underline{a} \in \mathcal{C}$

The usual inner product DOES NOT "preserve" the $\mathbb{F}_{q^n}$-linearity!

Find $H \in \mathbb{F}_{q^{2n}}^{(4n-2k)\times 2n}$ such that for all $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$

The *syndrome* of $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$ is zero iff $\underline{a} \in \mathcal{C}$

The usual inner product DOES NOT "preserve" the $\mathbb{F}_{q^n}$-linearity!

Find $H \in \mathbb{F}_{q^{2n}}^{(4n-2k)\times 2n}$ such that for all $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$,

$$Tr_{q^{2n}/q^n}(\underline{a}H^\top) = \underline{a}H^\top + \left(\underline{a}H^\top\right)^{q^n} \text{ is zero iff } \underline{a} \in \mathcal{TZ}_k(\gamma)$$

The *syndrome* of $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$ is zero iff $\underline{a} \in \mathcal{C}$

The usual inner product DOES NOT "preserve" the $\mathbb{F}_{q^n}$-linearity!

Find $H \in \mathbb{F}_{q^{2n}}^{(4n-2k)\times 2n}$ such that for all $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$,

$$Tr_{q^{2n}/q^n}(\underline{a}H^\top) = \underline{a}H^\top + \left(\underline{a}H^\top\right)^{q^n} \text{ is zero iff } \underline{a} \in \mathcal{TZ}_k(\gamma)$$

If $\underline{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_{2n-1})$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$

$$\Downarrow$$

there exists a unique $\mathbb{F}_q$-basis $\underline{\mu} = (\mu_0, \mu_1, \ldots, \mu_{2n-1})$ of $\mathbb{F}_{q^{2n}}$

The *syndrome* of $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$ is zero iff $\underline{a} \in \mathcal{C}$

The usual inner product DOES NOT "preserve" the $\mathbb{F}_{q^n}$-linearity!

Find $H \in \mathbb{F}_{q^{2n}}^{(4n-2k)\times 2n}$ such that for all $\underline{a} \in \mathbb{F}_{q^{2n}}^{2n}$,

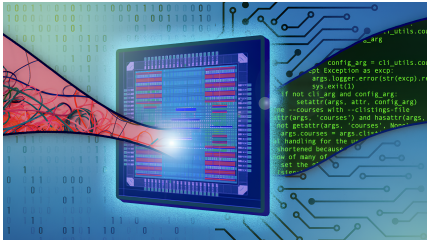
$$Tr_{q^{2n}/q^n}(\underline{a}H^\top) = \underline{a}H^\top + \left(\underline{a}H^\top\right)^{q^n} \text{ is zero iff } \underline{a} \in \mathcal{TZ}_k(\gamma)$$

If $\underline{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_{2n-1})$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$

$$\Downarrow$$

there exists a unique $\mathbb{F}_q$-basis $\underline{\mu} = (\mu_0, \mu_1, \ldots, \mu_{2n-1})$ of $\mathbb{F}_{q^{2n}}$

$$H = \begin{pmatrix} \gamma^{q^{2n-k}}\mu_0 & \gamma^{q^{2n-k}}\mu_1 & \gamma^{q^{2n-k}}\mu_2 & \cdots & \gamma^{q^{2n-k}}\mu_{2n-1} \\ \mu_0^{q^{k+1}} & \mu_1^{q^{k+1}} & \mu_2^{q^{k+1}} & \cdots & \mu_{2n-1}^{q^{k+1}} \\ \gamma\mu_0^{q^{k+1}} & \gamma\mu_1^{q^{k+1}} & \gamma\mu_2^{q^{k+1}} & \cdots & \gamma\mu_{2n-1}^{q^{k+1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mu_0^{q^{2n-1}} & \mu_1^{q^{2n-1}} & \mu_2^{q^{2n-1}} & \cdots & \mu_{2n-1}^{q^{2n-1}} \\ \gamma\mu_0^{q^{2n-1}} & \gamma\mu_1^{q^{2n-1}} & \gamma\mu_2^{q^{2n-1}} & \cdots & \gamma\mu_{2n-1}^{q^{2n-1}} \\ \mu_0^{q^k} & \mu_1^{q^k} & \mu_2^{q^k} & \cdots & \mu_{2n-1}^{q^k} \end{pmatrix} \in \mathbb{F}_{q^{2n}}^{(4n-2k)\times 2n} \tag{3}$$



E. M. Gabidulin
Theory of codes with maximum rank distance
In: *P.P.I.* 21.1 (1985), pp. 3-16.

A. Wachter-Zeh
Decoding of block and convolutional codes in rank metric
General Mathematics [math.GM]. Université de Rennes; Universität Ulm, 2013.

Decoding of Trombetti-Zhou codes $\mathcal{TZ}_k(\gamma)$: a new syndrome-based decoding approach

Decoding of Trombetti-Zhou codes $\mathcal{TZ}_k(\gamma)$: a new syndrome-based decoding approach

Sent message:

$$\underline{\tilde{f}} = (a, f_{1,1}, f_{1,2}, \ldots, f_{k-1,1}, f_{k-1,2}, b) \in \mathbb{F}_q^{2k}$$

Decoding of Trombetti-Zhou codes $\mathcal{TZ}_k(\gamma)$: a new syndrome-based decoding approach

Sent message:

$$\underline{\tilde{f}} = (a, f_{1,1}, f_{1,2}, \ldots, f_{k-1,1}, f_{k-1,2}, b) \in \mathbb{F}_{q^n}^{2k}$$

Received word:

$$\underline{r} = \underline{\tilde{f}}G + \underline{e} \in \mathbb{F}_{q^{2n}}^{2n}$$

Decoding of Trombetti-Zhou codes $\mathcal{TZ}_k(\gamma)$: a new syndrome-based decoding approach

Sent message:

$$\underline{\tilde{f}} = (a, f_{1,1}, f_{1,2}, \ldots, f_{k-1,1}, f_{k-1,2}, b) \in \mathbb{F}_{q^n}^{2k}$$

Received word:

$$\underline{r} = \underline{\tilde{f}}G + \underline{e} \in \mathbb{F}_{q^{2n}}^{2n}$$

Algorithm correction capability: Let $w_R(\underline{e}) \coloneqq d_R(\underline{e}, \underline{0})$,

$$\begin{cases} w_R(\underline{e}) = t \leq \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{2n-k}{2} \right\rfloor \\ w_R(\underline{e}) = n - \frac{k}{2} \text{ with } \underline{e} \in \mathbb{F}_{q^n}^{2n} \end{cases}$$

Decoding of Trombetti-Zhou codes $\mathcal{TZ}_k(\gamma)$: a new syndrome-based decoding approach

Sent message:

$$\underline{\tilde{f}} = (a, f_{1,1}, f_{1,2}, \ldots, f_{k-1,1}, f_{k-1,2}, b) \in \mathbb{F}_{q^n}^{2k}$$

Received word:

$$\underline{r} = \underbrace{\underline{\tilde{f}}G}_{=\underline{c}} + \underline{e} \in \mathbb{F}_{q^{2n}}^{2n}$$

Algorithm correction capability: Let $w_R(\underline{e}) \coloneqq d_R(\underline{e}, \underline{0})$,

$$\begin{cases} w_R(\underline{e}) = t \leq \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{2n-k}{2} \right\rfloor \\ w_R(\underline{e}) = n - \frac{k}{2} \text{ with } \underline{e} \in \mathbb{F}_{q^n}^{2n} \end{cases}$$

✓ **Information already available**

✗ **Information to be obtained step by step**

✓ **Information already available**

✗ **Information to be obtained step by step**

Key points of the decoding algorithm

✓ **Information already available**

✗ **Information to be obtained step by step**

Key points of the decoding algorithm

1. Let $\underline{\beta} = (\beta_0, \beta_1, \ldots, \beta_{2n-1})$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$

$$\underline{e} = \underline{\beta}(A \cdot B) = \underline{a} \cdot B,$$

where

- $\underline{a} = (a_0, a_1, \ldots, a_{t-1}) \in \mathbb{F}_{q^{2n}}^t, \quad \dim_q(\langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}) = t,$
- $B \in \mathbb{F}_q^{t \times 2n}, \quad \operatorname{rank}(B) = t.$

✓ **Information already available**

✗ **Information to be obtained step by step**

Key points of the decoding algorithm

1. Let $\underline{\beta} = (\beta_0, \beta_1, \ldots, \beta_{2n-1})$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$

$$\underline{e} = \underline{\beta}(A \cdot B) = \underline{a} \cdot B,$$

where

- $\underline{a} = (a_0, a_1, \ldots, a_{t-1}) \in \mathbb{F}_{q^{2n}}^t, \quad \dim_q(\langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}) = t,$
- $B \in \mathbb{F}_q^{t \times 2n}, \quad \operatorname{rank}(B) = t.$

2. Introduction of the intermediate unknown *vector of error locators*:

$$\underline{d}^\top := B \cdot \underline{\mu}^{q^{k^\top}}.$$

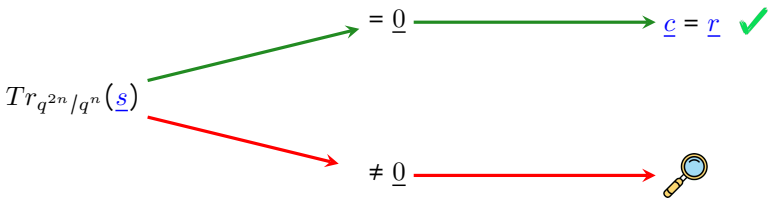
Main steps of the algorithm

Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$-*syndrome*: $\underline{s} = \underline{r} \cdot H^{\top}$

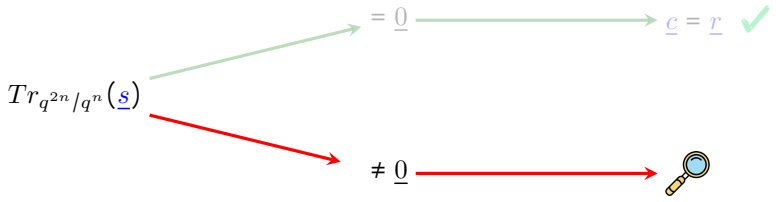
Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$-*syndrome*: $\underline{s} = \underline{r} \cdot H^{\top}$
- $\mathbb{F}_{q^n}$-**Syndrome check**:



Main steps of the algorithm

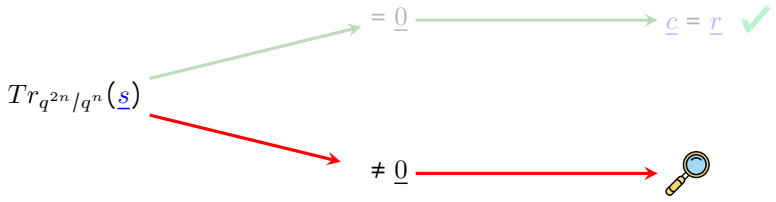
- **Compute** the $\mathbb{F}_{q^n}$-*syndrome*: $\underline{s} = \underline{r} \cdot H^{\top}$
- $\mathbb{F}_{q^n}$-**Syndrome check**:



↝**Reconstruct a potential decomposition of the error as** $\underline{e} = \underline{a} \cdot B$

Main steps of the algorithm

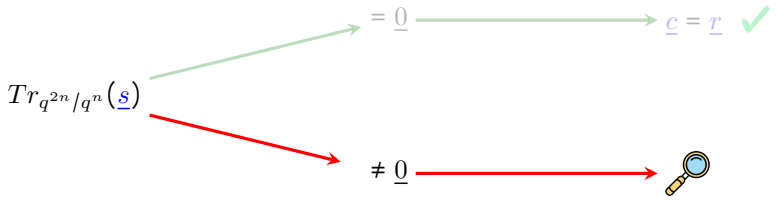
- **Compute** the $\mathbb{F}_{q^n}$-*syndrome*: $\underline{s} = \underline{r} \cdot H^\top$
- $\mathbb{F}_{q^n}$-**Syndrome check**:



- **Identify** $\underline{a}$ of a potential decomposition

Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$*-syndrome*: $\underline{s} = \underline{r} \cdot H^{\top}$
- $\mathbb{F}_{q^n}$**-Syndrome check**:

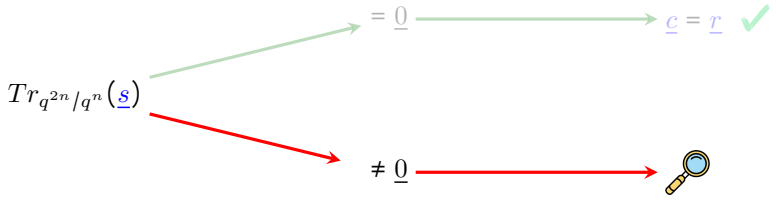



↝**Reconstruct a potential decomposition of the error as** $\underline{e} = \underline{a} \cdot B$

- **Identify** $\underline{a}$ of a potential decomposition: Solve an homogeneous linear system to determine $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$

Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$*-syndrome*: $\underline{s} = \underline{r} \cdot H^\top$
- $\mathbb{F}_{q^n}$**-Syndrome check**:



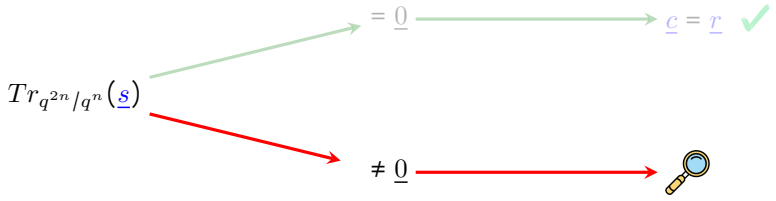

↝**Reconstruct a potential decomposition of the error as** $\underline{e} = \underline{a} \cdot B$

- **Identify** $\underline{a}$ of a potential decomposition: Solve an homogeneous linear system to determine $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ such that

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$*-syndrome*: $\underline{s} = \underline{r} \cdot H^\top$
- $\mathbb{F}_{q^n}$**-Syndrome check**:




⇝**Reconstruct a potential decomposition of the error as** $\underline{e} = \underline{a} \cdot B$

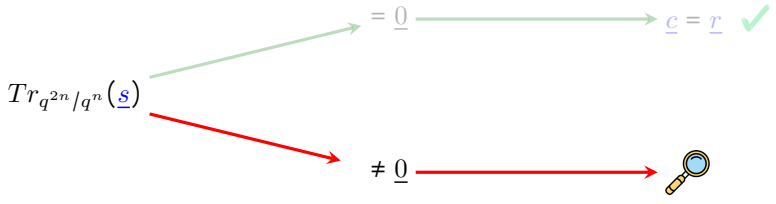
- **Identify** $\underline{a}$ of a potential decomposition: Solve an homogeneous linear system to determine $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ such that

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

- **Determine** $\underline{d}$

Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$*-syndrome*: $\underline{s} = \underline{r} \cdot H^\top$
- $\mathbb{F}_{q^n}$**-Syndrome check**:




$\rightsquigarrow$**Reconstruct a potential decomposition of the error as** $\underline{e} = \underline{a} \cdot B$

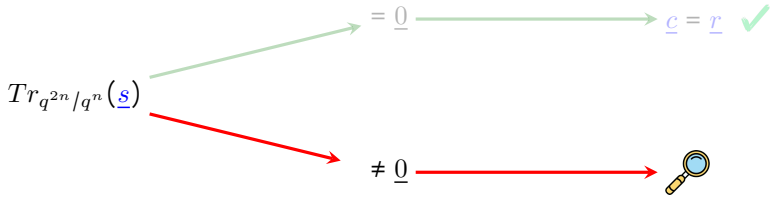
- **Identify** $\underline{a}$ of a potential decomposition: Solve an homogeneous linear system to determine $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ such that

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

- **Determine** $\underline{d}$: solve a determined linear system arising from $\underline{a}$ and the $\mathbb{F}_{q^n}$-syndrome $\underline{s}$

Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$*-syndrome*: $\underline{s} = \underline{r} \cdot H^\top$
- $\mathbb{F}_{q^n}$**-Syndrome check**:



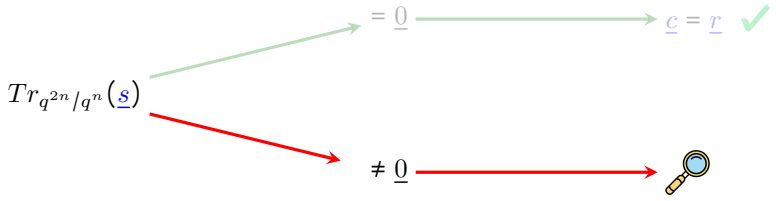

- **Identify** $\underline{a}$ of a potential decomposition: Solve an homogeneous linear system to determine $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ such that

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

- **Determine** $\underline{d}$: solve a determined linear system arising from $\underline{a}$ and the $\mathbb{F}_{q^n}$-syndrome $\underline{s}$
- **Determine** B

Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$-*syndrome*: $\underline{s} = \underline{r} \cdot H^\top$
- $\mathbb{F}_{q^n}$-**Syndrome check**:



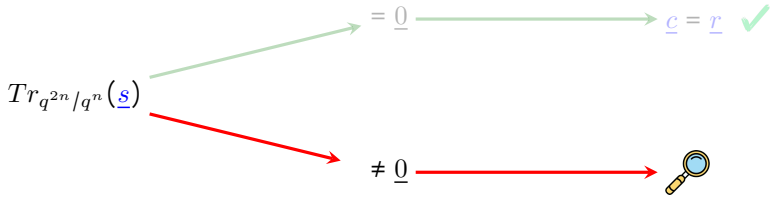

- **Identify** $\underline{a}$ of a potential decomposition: Solve an homogeneous linear system to determine $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ such that

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

- **Determine** $\underline{d}$: solve a determined linear system arising from $\underline{a}$ and the $\mathbb{F}_{q^n}$-syndrome $\underline{s}$
- **Determine** B from $\underline{d}^\top = B \cdot \underline{\mu}^{q^{k^\top}}$

Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$*-syndrome*: $\underline{s} = \underline{r} \cdot H^\top$
- $\mathbb{F}_{q^n}$**-Syndrome check**:



↝**Reconstruct a potential decomposition of the error as** $\underline{e} = \underline{a} \cdot B$

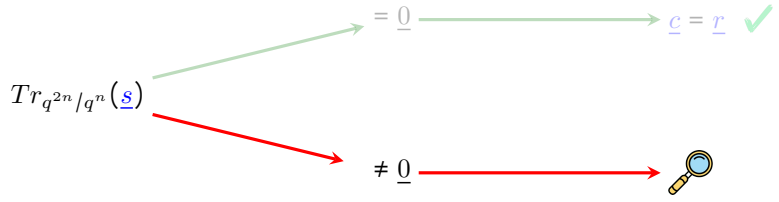
- **Identify** $\underline{a}$ of a potential decomposition: Solve an homogeneous linear system to determine $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ such that

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

- **Determine** $\underline{d}$: solve a determined linear system arising from $\underline{a}$ and the $\mathbb{F}_{q^n}$-syndrome $\underline{s}$
- **Determine** B from $\underline{d}^\top = B \cdot \underline{\mu}^{q^{k^\top}}$
- **Reconstruction of the sent codeword:** $\underline{c} = \underline{r} - \underline{a}B$

Main steps of the algorithm

- **Compute** the $\mathbb{F}_{q^n}$-*syndrome*: $\underline{s} = \underline{r} \cdot H^\top$
- $\mathbb{F}_{q^n}$-**Syndrome check**:



$\rightsquigarrow$**Reconstruct a potential decomposition of the error as** $\underline{e} = \underline{a} \cdot B$

- **Identify** $\underline{a}$ of a potential decomposition: Solve an homogeneous linear system to determine $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ such that

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

- **Determine** $\underline{d}$: solve a determined linear system arising from $\underline{a}$ and the $\mathbb{F}_{q^n}$-syndrome $\underline{s}$
- **Determine** B from $\underline{d}^\top = B \cdot \underline{\mu}^{q^{k^\top}}$
- **Reconstruction of the sent codeword:** $\underline{c} = \underline{r} - \underline{a}B$

Determine $\underline{a}$ by employing the error span polynomial

$$\Lambda(x) = \prod_{\vartheta \in \langle a_0, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}} (x - \vartheta) = \Lambda_0 x + \Lambda_1 x^q + \ldots + \Lambda_t x^{q^t} \tag{4}$$

Determine $\underline{a}$ by employing the error span polynomial

$$\Lambda(x) = \prod_{\vartheta \in \langle a_0, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}} (x - \vartheta) = \Lambda_0 x + \Lambda_1 x^q + \ldots + \Lambda_t x^{q^t} \tag{4}$$

By construction $\ker(\Lambda(x)) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$

Determine $\underline{a}$ by employing the error span polynomial

$$\Lambda(x) = \prod_{\vartheta \in \langle a_0, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}} (x - \vartheta) = \Lambda_0 x + \Lambda_1 x^q + \ldots + \Lambda_t x^{q^t} \tag{4}$$

By construction $\ker(\Lambda(x)) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$

Theorem

Let $H \in \mathbb{F}_{q^{2n}}^{(4n-2k)\times 2n}$ be an $\mathbb{F}_{q^n}$-parity-check matrix of $\mathcal{TZ}_k(\gamma)$ as in (3) and let $\underline{s}$ be the syndrome of the received word $\underline{r}$ through H. If $\Lambda_0, \Lambda_1, \ldots, \Lambda_t$ are the coefficients of the error span polynomial in (4), then

$$\begin{pmatrix} s_{2(t+1)-1} & \cdots & s_3^{q^{t-1}} & s_1^{q^t} \\ s_{2(t+2)-1} & \cdots & s_5^{q^{t-1}} & s_3^{q^t} \\ \vdots & \ddots & \vdots & \vdots \\ s_{4n-2k-3} & \cdots & s_{4n-2k-1-2t}^{q^{t-1}} & s_{4n-2k-3-2t}^{q^t} \end{pmatrix} \cdot \begin{pmatrix} \Lambda_0 \\ \Lambda_1 \\ \vdots \\ \Lambda_t \end{pmatrix} = \underline{0}^\top.$$

Case 1: $2t + k < 2n$

Decoding of TZ-codes
$\mathcal{TZ}_k(\gamma)$

Decoding of Gabidulin codes
$\mathcal{G}_{2n,k+1}(\underline{\lambda})$

Case 1: $2t + k < 2n$

Decoding of TZ-codes
$\mathcal{TZ}_k(\gamma)$

Decoding of Gabidulin codes
$\mathcal{G}_{2n,k+1}(\underline{\lambda})$

- **Determine** $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ up to a scalar factor

Case 1: $2t + k < 2n$

Decoding of TZ-codes
$\mathcal{TZ}_k(\gamma)$

Decoding of Gabidulin codes
$\mathcal{G}_{2n,k+1}(\underline{\lambda})$

- **Determine** $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ up to a scalar factor
- **Identify** $\underline{a}$ of a potential decomposition as

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

- **Determine** $\underline{d}$: solve a determined linear system arising from $\underline{a}$ and the $\mathbb{F}_{q^n}$-syndrome $\underline{s}$
- **Determine** B from $\underline{d}^\top = B \cdot \underline{\mu}^{q^{k^\top}}$
- **Reconstruction of the sent codeword:** $\underline{c} = \underline{r} - \underline{a}B$

Case 2: k is even and $t = n - \frac{k}{2}$

Theorem

Let $H \in \mathbb{F}_{q^{2n}}^{(4n-2k)\times 2n}$ be an $\mathbb{F}_{q^n}$-parity-check matrix of $\mathcal{TZ}_k(\gamma)$ as in (3) and let $\underline{s}$ be the syndrome of the received word $\underline{r}$ through H. If $\Lambda_0, \Lambda_1, \ldots, \Lambda_t$ are the coefficients of the error span polynomial in (4), then the solution set of

$$\begin{pmatrix} s_{2(t+1)-1} & \cdots & s_3^{q^{t-1}} & s_1^{q^t} \\ s_{2(t+2)-1} & \cdots & s_5^{q^{t-1}} & s_3^{q^t} \\ \vdots & \ddots & \vdots & \vdots \\ s_{2(2t-1)-1} & \cdots & s_{2t-1}^{q^{t-1}} & s_{2(t-1)-1}^{q^t} \end{pmatrix} \cdot \begin{pmatrix} \Lambda_0 \\ \Lambda_1 \\ \vdots \\ \Lambda_t \end{pmatrix} = \underline{0}^\top$$

has dimension two.

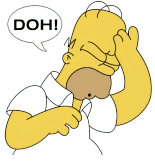
Case 2: k is even and $t = n - \frac{k}{2}$

Theorem

Let $H \in \mathbb{F}_{q^{2n}}^{(4n-2k)\times 2n}$ be an $\mathbb{F}_{q^n}$-parity-check matrix of $\mathcal{TZ}_k(\gamma)$ as in (3) and let $\underline{s}$ be the syndrome of the received word $\underline{r}$ through H. If $\Lambda_0, \Lambda_1, \ldots, \Lambda_t$ are the coefficients of the error span polynomial in (4), then the solution set of

$$\begin{pmatrix} s_{2(t+1)-1} & \cdots & s_3^{q^{t-1}} & s_1^{q^t} \\ s_{2(t+2)-1} & \cdots & s_5^{q^{t-1}} & s_3^{q^t} \\ \vdots & \ddots & \vdots & \vdots \\ s_{2(2t-1)-1} & \cdots & s_{2t-1}^{q^{t-1}} & s_{2(t-1)-1}^{q^t} \end{pmatrix} \cdot \begin{pmatrix} \Lambda_0 \\ \Lambda_1 \\ \vdots \\ \Lambda_t \end{pmatrix} = \underline{0}^\top$$

has dimension two.



More information is needed!

System of $2t$ equations in $t+1$ unknowns:

$$S_{\exp} \cdot \underline{\Lambda}^{\top} = \begin{pmatrix} s_{2(t+1)-1} & \cdots & s_3^{q^{t-1}} & s_1^{q^t} \\ \vdots & \ddots & \vdots & \vdots \\ s_{2(2t-1)-1} & \cdots & s_{2t-1}^{q^{t-1}} & s_{2(t-1)-1}^{q^t} \\ Tr_{q^{2n}/q^n}(s_{2t-1}) & \cdots & Tr_{q^{2n}/q^n}\left(s_1^{q^{t-1}}\right) & Tr_{q^{2n}/q^n}\left(s_{4t-1}^{q^t}\right) \\ Tr_{q^{2n}/q^n}(s_{2t+1}) & \cdots & Tr_{q^{2n}/q^n}\left(s_3^{q^{t-1}}\right) & Tr_{q^{2n}/q^n}\left(s_1^{q^t}\right) \\ \vdots & \ddots & \vdots & \vdots \\ Tr_{q^{2n}/q^n}(s_{2(2t-1)-1}) & \cdots & Tr_{q^{2n}/q^n}\left(s_{2t-1}^{q^{t-1}}\right) & Tr_{q^{2n}/q^n}\left(s_{2(t-1)-1}^{q^t}\right) \\ Tr_{q^{2n}/q^n}(s_0) & \cdots & Tr_{q^{2n}/q^n}\left(\gamma^{q^{2t}} s_{2t-3}^{q^{t-1}}\right) & Tr_{q^{2n}/q^n}\left(\gamma^{q^{2t}} s_{2t-1}^{q^t}\right) \end{pmatrix} \cdot \begin{pmatrix} \Lambda_0 \\ \Lambda_1 \\ \vdots \\ \Lambda_t \end{pmatrix} = \underline{0}^{\top}$$

Theorem

The dimension of the solution space of $S_{\exp} \cdot \underline{\Lambda}^{\top} = \underline{0}^{\top}$ is one.

Theorem

The dimension of the solution space of $S_{\exp} \cdot \underline{\Lambda}^{\top} = \underline{0}^{\top}$ is one.

- **Determine** $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ up to a scalar factor
- **Identify** $\underline{a}$ of a potential decomposition as

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

- **Determine** $\underline{d}$: solve a determined linear system arising from $\underline{a}$ and the $\mathbb{F}_{q^n}$-syndrome $\underline{s}$
- **Determine** B from $\underline{d}^{\top} = B \cdot \underline{\mu}^{q^{k^{\top}}}$
- **Reconstruction of the sent codeword:** $\underline{c} = \underline{r} - \underline{a}B$

Theorem

The dimension of the solution space of $S_{\exp} \cdot \underline{\Lambda}^\top = \underline{0}^\top$ is one.

- **Determine** $(\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$ up to a scalar factor
- **Identify** $\underline{a}$ of a potential decomposition as

$$\ker(\Lambda_0 x + \Lambda_1 x^q \ldots + \Lambda_t x^{q^t}) = \langle a_0, a_1, \ldots, a_{t-1} \rangle_{\mathbb{F}_q}$$

- **Determine** $\underline{d}$: solve a determined linear system arising from $\underline{a}$ and the $\mathbb{F}_{q^n}$-syndrome $\underline{s}$
- **Determine** B from $\underline{d}^\top = B \cdot \underline{\mu}^{q^{k^\top}}$
- **Reconstruction of the sent codeword:** $\underline{c} = \underline{r} - \underline{a}B$

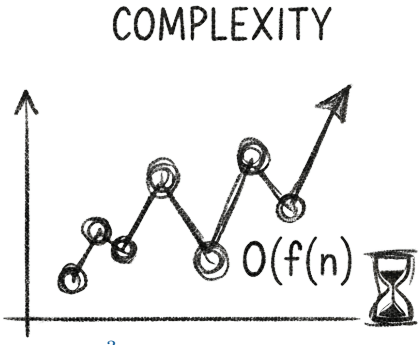
Is there anything under the rug?

Algorithm 1: Decoding of Trombetti-Zhou codes: a new syndrome-based decoding approach.

Input: $\underline{r} = (r_0, r_1, \ldots, r_{2n-1}) \in \mathbb{F}_{q^{2n}}^{2n}$;
Set H as in (3);
$\mathbb{F}_{q^n}$-*syndrome* calculation: $\underline{s} \leftarrow \underline{r} \cdot H^\top \in \mathbb{F}_{q^{2n}}^{4n-2k}$;
if $Tr_{q^{2n}/q^n}(\underline{s}) = \underline{0}$ **then**
    Estimated codeword: $\underline{c} \leftarrow \underline{r}$
end
else
    if k *is even and* $\mathrm{rank}(S_{\exp}) = n - \frac{k}{2}$ **then**
        Set up $t = n - \frac{k}{2}$;
        Solve $S_{\exp} \cdot \underline{\Lambda}^\top = \underline{0}^\top$ for $\underline{\Lambda} = (\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$;
        if $\left(\frac{\Lambda_0}{\Lambda_t}, \frac{\Lambda_1}{\Lambda_t}, \ldots, \frac{\Lambda_{t-1}}{\Lambda_t}, 1\right) \notin \mathbb{F}_{q^n}^{t+1}$ **then**
            Declare decoding failure
        end
    end
    else
        Set up $S^{(t)}$ as in (5) for $t = \lfloor (2n - (k+1))/2 \rfloor$;
        while $\mathrm{rank}(S^{(t)}) < t$ **do**
            $t \leftarrow t - 1$;
            Set up $S^{(t)}$ as in (5)
        end
        Solve $S^{(t)} \cdot \underline{\Lambda}^T = \underline{0}$ for $\underline{\Lambda} = (\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$
    end
    Find basis $(a_0, a_1, \ldots, a_{\varepsilon-1}) \in \mathbb{F}_{q^{2n}}^{\varepsilon}$ of the root space of $\Lambda(x) = \sum_{i=0}^{t} \Lambda_i x^{[i]}$ over $\mathbb{F}_{q^{2n}}$;
    if $\varepsilon = t$ **then**
        Find $(d_0, d_1, \ldots, d_{t-1}) \in \mathbb{F}_{q^{2n}}^{t}$ by solving (6);
        Find $B = (B_{i,j})_{j \in \{0,\ldots,2n-1\}}^{i \in \{0,\ldots,t-1\}} \in \mathbb{F}_q^{t \times 2n}$ such that $d_i = \sum_{j=0}^{2n-1} B_{i,j} \mu_j^{[k]}$;
        Estimated codeword: $\underline{c} \leftarrow \underline{r} - \underline{a} \cdot B$
    end
    else
        Declare decoding failure
    end
end
Output: Estimated codeword $\underline{c} \in \mathbb{F}_{q^{2n}}^{2n}$ or "decoding failure"

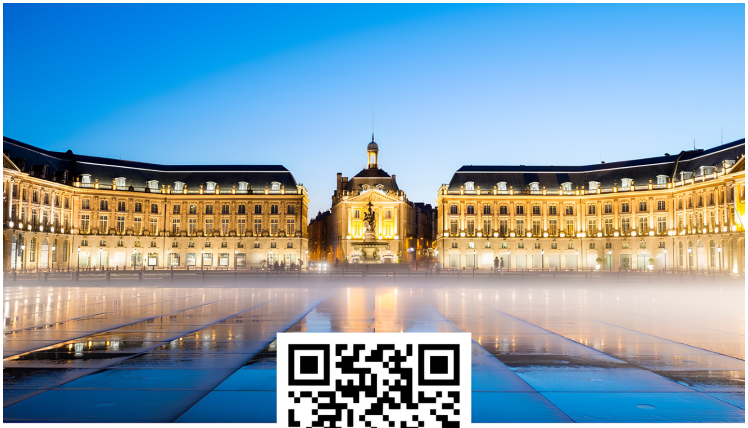
Algorithm 2: Decoding of Trombetti-Zhou codes: a new syndrome-based decoding approach.

Input: $\underline{r} = (r_0, r_1, \ldots, r_{2n-1}) \in \mathbb{F}_{q^{2n}}^{2n}$;
Set H as in (3);
$\mathbb{F}_{q^n}$-*syndrome* calculation: $\underline{s} \leftarrow \underline{r} \cdot H^\top \in \mathbb{F}_{q^{2n}}^{4n-2k}$;
if $Tr_{q^{2n}/q^n}(\underline{s}) = \underline{0}$ **then**
    Estimated codeword: $\underline{c} \leftarrow \underline{r}$
end
else
    if k *is even and* $\mathrm{rank}(S_{\exp}) = n - \frac{k}{2}$ **then**
        Set up $t = n - \frac{k}{2}$;
        Solve $S_{\exp} \cdot \underline{\Lambda}^\top = \underline{0}^\top$ for $\underline{\Lambda} = (\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$;
        if $\left(\frac{\Lambda_0}{\Lambda_t}, \frac{\Lambda_1}{\Lambda_t}, \ldots, \frac{\Lambda_{t-1}}{\Lambda_t}, 1\right) \notin \mathbb{F}_{q^n}^{t+1}$ **then**
            Declare decoding failure
        end
    end
    else
        Set up $S^{(t)}$ as in (5) for $t = \lfloor (2n - (k+1))/2 \rfloor$;
        while $\mathrm{rank}(S^{(t)}) < t$ **do**
            $t \leftarrow t - 1$;
            Set up $S^{(t)}$ as in (5)
        end
        Solve $S^{(t)} \cdot \underline{\Lambda}^\top = \underline{0}$ for $\underline{\Lambda} = (\Lambda_0, \Lambda_1, \ldots, \Lambda_t) \in \mathbb{F}_{q^{2n}}^{t+1}$
    end
    Find basis $(a_0, a_1, \ldots, a_{\varepsilon-1}) \in \mathbb{F}_{q^{2n}}^{\varepsilon}$ of the root space of $\Lambda(x) = \sum_{i=0}^{t} \Lambda_i x^{[i]}$ over $\mathbb{F}_{q^{2n}}$;
    if $\varepsilon = t$ **then**
        Find $(d_0, d_1, \ldots, d_{t-1}) \in \mathbb{F}_{q^{2n}}^{t}$ by solving (6);
        Find $B = (B_{i,j})_{j\in\{0,\ldots,t-1\}}^{i\in\{0,\ldots,2n-1\}} \in \mathbb{F}_q^{t\times 2n}$ such that $d_i = \sum_{j=0}^{2n-1} B_{i,j}\, \mu_j^{[k]}$;
        Estimated codeword: $\underline{c} \leftarrow \underline{r} - \underline{a} \cdot B$
    end
    else
        Declare decoding failure
    end
end
Output: Estimated codeword $\underline{c} \in \mathbb{F}_{q^{2n}}^{2n}$ or "decoding failure"



$\mathcal{O}(n^3)$ operations over $\mathbb{F}_{q^{2n}}$

Thanks for your attention!



Appendix

Let $[i] \coloneqq q^i$,

$$S^{(t)} = \begin{pmatrix} s_{2(t+1)-1}^{[0]} & \cdots & s_3^{[t-1]} & s_1^{[t]} \\ s_{2(t+2)-1}^{[0]} & \cdots & s_5^{[t-1]} & s_3^{[t]} \\ \vdots & \ddots & \vdots & \vdots \\ s_{2(2t)-1}^{[0]} & \cdots & s_{2t+1}^{[t-1]} & s_{2t-1}^{[t]} \end{pmatrix} \tag{5}$$

$$\begin{pmatrix} a_0^{[-1]} & a_1^{[-1]} & \cdots & a_{t-1}^{[-1]} \\ a_0^{[-2]} & a_1^{[-2]} & \cdots & a_{t-1}^{[-2]} \\ \vdots & \vdots & \ddots & \vdots \\ a_0^{[-(2n-k-1)]} & a_1^{[-(2n-k-1)]} & \cdots & a_{t-1}^{[-(2n-k-1)]} \end{pmatrix} \cdot \begin{pmatrix} d_0 \\ d_1 \\ \vdots \\ d_{t-1} \end{pmatrix} = \begin{pmatrix} s_1^{[-1]} \\ s_3^{[-2]} \\ \vdots \\ s_{4n-2k-3}^{[-(2n-k-1)]} \end{pmatrix} \tag{6}$$