Code-Based Cryptography

1. Error-Correcting Codes and Cryptography
2. McEliece Cryptosystem
3. Message Attacks (ISD)
4. **Key Attacks**
5. Other Cryptographic Constructions Relying on Coding Theory

4. Key Attacks

1. Introduction
2. Support Splitting Algorithm
3. Distinguisher for GRS codes
4. Attack against subcodes of GRS codes
5. **Error-Correcting Pairs**
6. Attack against GRS codes
7. Attack against Reed-Muller codes
8. Attack against Algebraic Geometry codes
9. Goppa codes still resist

4. Key Attacks

1. Introduction
2. Support Splitting Algorithm
3. Distinguisher for GRS codes
4. Attack against subcodes of GRS codes
5. **Error-Correcting Pairs**
6. Attack against GRS codes
7. Attack against Reed-Muller codes
8. Attack against Algebraic Geometry codes
9. Goppa codes still resist

An efficient decoding algorithm for GRS codes - ECP

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^\perp = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^\perp)$

An efficient decoding algorithm for GRS codes - ECP

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$

Consider the codes $\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{1})$

An efficient decoding algorithm for GRS codes - ECP

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^\perp = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^\perp)$

Consider the codes $\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^\perp)$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{1})$

sent codeword

$$\mathbf{y} = \mathbf{c} + \mathbf{e}$$

received word

error vector

An efficient decoding algorithm for GRS codes - ECP

Let $\boxed{\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d})} \Longrightarrow \boxed{\mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})}$

Consider the codes $\boxed{\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})}$ and $\boxed{\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{1})}$

$$\underbrace{\mathbf{y}}_{\text{received word}} = \overbrace{\mathbf{c}}^{\text{sent codeword}} + \underbrace{\mathbf{e}}_{\text{error vector}}$$

Define:

$$K_{\mathbf{y}} = \left\{ \mathbf{a} \in \mathcal{A} \mid \langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = 0 \text{ , for all } \mathbf{b} \in \mathcal{B} \right\}$$

An efficient decoding algorithm for GRS codes - ECP

$K_y = K_e$**?**

An efficient decoding algorithm for GRS codes - ECP

$K_y = K_e$**?**

Take notice that:

$$\mathcal{A} * \mathcal{B} \quad = \quad \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1})$$

An efficient decoding algorithm for GRS codes - ECP

$K_y = K_e$**?**

Take notice that:

$$\begin{aligned} \boxed{\mathcal{A}} * \boxed{\mathcal{B}} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_t(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \end{aligned}$$

An efficient decoding algorithm for GRS codes - ECP

$K_y = K_e$**?**

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_t(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) \end{aligned}$$

An efficient decoding algorithm for GRS codes - ECP

$\boxed{K_y = K_e\text{?}}$

Take notice that:

$$\begin{aligned}
\boxed{\mathcal{A}} * \boxed{\mathcal{B}} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\
&= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\
&= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \boxed{\mathcal{C}^{\perp}}
\end{aligned}$$

An efficient decoding algorithm for GRS codes - ECP

$K_y = K_e$**?**

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_t(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle$$

An efficient decoding algorithm for GRS codes - ECP

$K_y = K_e$**?**

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{c} + \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

An efficient decoding algorithm for GRS codes - ECP

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_t(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{c} + \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \underbrace{\langle \mathbf{c}, \mathbf{a} * \mathbf{b} \rangle}_{=0} + \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

An efficient decoding algorithm for GRS codes - ECP

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

An efficient decoding algorithm for GRS codes - ECP

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

Or equivalently, $K_{\mathbf{y}} = K_{\mathbf{e}}$

An efficient decoding algorithm for GRS codes - ECP

$K_{\mathbf{y}} = K_{\mathbf{e}}$**?**

YES, since $\mathcal{A} * \mathcal{B} = \mathcal{C}^{\perp}$

Take notice that:

$$\begin{aligned}\mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp}\end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

Or equivalently, $K_{\mathbf{y}} = K_{\mathbf{e}}$

An efficient decoding algorithm for GRS codes - ECP

There exists a nonzero a $\in K_y$?

An efficient decoding algorithm for GRS codes - ECP

There exists a nonzero $\mathbf{a} \in K_{\mathbf{y}}$?

We define $f(X) = \prod_{i \in \mathrm{supp}(\mathbf{e})} (X - c_i) \implies \deg(f) = t < t + 1$, i.e. $f \in L_{t+1}$

An efficient decoding algorithm for GRS codes - ECP

There exists a nonzero $\mathbf{a} \in K_y$?

We define $f(X) = \prod_{i \in \mathrm{supp}(\mathbf{e})} (X - c_i) \implies \deg(f) = t < t+1$, i.e. $f \in L_{t+1}$

$$\mathbf{a} = \mathbf{d}^{\perp} * f(\mathbf{c}) = \mathrm{ev}_{\mathbf{c},\mathbf{d}^{\perp}}(f) \in \boxed{\mathcal{A}} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$$

An efficient decoding algorithm for GRS codes - ECP

There exists a nonzero $\mathbf{a} \in K_y$?

We define $f(X) = \prod_{i \in \mathrm{supp}(\mathbf{e})} (X - c_i) \implies \deg(f) = t < t+1$, i.e. $f \in L_{t+1}$

$$\mathbf{a} = \mathbf{d}^{\perp} * f(\mathbf{c}) = \mathrm{ev}_{\mathbf{c},\mathbf{d}^{\perp}}(f) \in \mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$$

Moreover, $\mathbf{a} * \mathbf{e} = \mathbf{0}$. Thus $\mathbf{a} \in K_{\mathbf{y}}$

An efficient decoding algorithm for GRS codes - ECP

There exists a nonzero a $\in K_y$?

YES, since $\boxed{K(\mathcal{A}) > t}$

We define $f(X) = \prod_{i \in \mathrm{supp}(\mathbf{e})} (X - c_i) \implies \deg(f) = t < t + 1$, i.e. $f \in L_{t+1}$

$$\mathbf{a} = \mathbf{d}^{\perp} * f(\mathbf{c}) = \mathrm{ev}_{\mathbf{c},\mathbf{d}^{\perp}}(f) \in \boxed{\mathcal{A}} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$$

Moreover, $\mathbf{a} * \mathbf{e} = \mathbf{0}$. Thus $\mathbf{a} \in K_{\mathbf{y}}$

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$, $\mathbf{a} \neq \mathbf{0} \implies \mathrm{supp}(\mathbf{e}) \subseteq \overline{\mathrm{supp}(\mathbf{a})}$?

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$, $\mathbf{a} \neq \mathbf{0} \implies \mathrm{supp}(\mathbf{e}) \subseteq \overline{\mathrm{supp}(\mathbf{a})}$?

Indeed,

$$0 = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e} * \mathbf{a}, \mathbf{b} \rangle \implies \mathbf{e} * \mathbf{a} \in \mathcal{B}^{\perp}$$

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$, $\mathbf{a} \neq \mathbf{0} \implies \mathrm{supp}(\mathbf{e}) \subseteq \overline{\mathrm{supp}(\mathbf{a})}$?

Indeed,

$$0 = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e} * \mathbf{a}, \mathbf{b} \rangle \implies \mathbf{e} * \mathbf{a} \in \mathcal{B}^{\perp}$$

But $\mathrm{w}_H(\mathbf{e} * \mathbf{a}) \leq \mathrm{w}_H(\mathbf{e}) < t < d(\mathcal{B}^{\perp})$

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$, $\mathbf{a} \neq \mathbf{0} \implies \mathrm{supp}(\mathbf{e}) \subseteq \overline{\mathrm{supp}(\mathbf{a})}$?

Indeed,

$$0 = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e} * \mathbf{a}, \mathbf{b} \rangle \implies \mathbf{e} * \mathbf{a} \in \mathcal{B}^{\perp}$$

But $\mathrm{w}_H(\mathbf{e} * \mathbf{a}) \leq \mathrm{w}_H(\mathbf{e}) < t < d(\mathcal{B}^{\perp})$
Thus $\mathbf{e} * \mathbf{a} = \mathbf{0}$, i.e.

$$\mathrm{supp}(\mathbf{e}) \subseteq \{1, \ldots, n\} - \mathrm{supp}(\mathbf{a}) = \overline{\mathrm{supp}(\mathbf{a})}$$

An efficient decoding algorithm for GRS codes - ECP

Let a $\in K_{\mathbf{y}}$, a $\neq \mathbf{0} \Longrightarrow \mathrm{supp}(\mathbf{e}) \subseteq \overline{\mathrm{supp}(\mathbf{a})}$?

YES, since $d(\mathcal{B}^{\perp}) > t$

Indeed,

$$0 = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e} * \mathbf{a}, \mathbf{b} \rangle \Longrightarrow \mathbf{e} * \mathbf{a} \in \mathcal{B}^{\perp}$$

But $\mathrm{w}_H(\mathbf{e} * \mathbf{a}) \leq \mathrm{w}_H(\mathbf{e}) < t < d(\mathcal{B}^{\perp})$
Thus $\mathbf{e} * \mathbf{a} = \mathbf{0}$, i.e.

$$\mathrm{supp}(\mathbf{e}) \subseteq \{1, \ldots, n\} - \mathrm{supp}(\mathbf{a}) = \overline{\mathrm{supp}(\mathbf{a})}$$

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.

If there have been no more than t errors (i.e. $\mathrm{w}_H(\mathbf{e}) \leq t$), then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \quad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\mathrm{supp}(\mathbf{a})}$$

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.
If there have been no more than t errors (i.e. $\mathrm{w}_H(\mathbf{e}) \leq t$), then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \qquad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\mathrm{supp}(\mathbf{a})}$$

Is the solution unique?

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.
If there have been no more than t errors (i.e. $\mathrm{w}_H(\mathbf{e}) \leq t$), then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \quad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\mathrm{supp}(\mathbf{a})}$$

Is the solution unique?

Suppose that $\mathbf{e}_1$ and $\mathbf{e}_2$ are solutions of the above system.

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.

If there have been no more than t errors (i.e. $\mathrm{w}_H(\mathbf{e}) \leq t$), then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \qquad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\mathrm{supp}(\mathbf{a})}$$

Is the solution unique?

Suppose that $\mathbf{e}_1$ and $\mathbf{e}_2$ are solutions of the above system. Then,

$$\langle \mathbf{e}_1, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}_2, \mathbf{a} * \mathbf{b} \rangle \text{ with } \begin{cases} \mathrm{supp}(\mathbf{e}_1) \subseteq \overline{\mathrm{supp}(\mathbf{a})} \\ \mathrm{supp}(\mathbf{e}_2) \subseteq \overline{\mathrm{supp}(\mathbf{a})} \end{cases}$$

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.
If there have been no more than t errors (i.e. $\mathrm{w}_H(\mathbf{e}) \leq t$), then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \qquad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\mathrm{supp}(\mathbf{a})}$$

Is the solution unique?

Suppose that $\mathbf{e}_1$ and $\mathbf{e}_2$ are solutions of the above system. Then,

$$\langle \mathbf{e}_1, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}_2, \mathbf{a} * \mathbf{b} \rangle \text{ with } \begin{cases} \mathrm{supp}(\mathbf{e}_1) \subseteq \overline{\mathrm{supp}(\mathbf{a})} \\ \mathrm{supp}(\mathbf{e}_2) \subseteq \overline{\mathrm{supp}(\mathbf{a})} \end{cases}$$

Then $\mathbf{e}_1 - \mathbf{e}_2 \in \mathcal{C}$, but

$$\mathrm{w}_H(\mathbf{e}_1 - \mathbf{e}_2) \leq n - |\mathrm{supp}(\mathbf{a})| \leq d(\mathcal{C}) - 1$$

which **contradicts** the minimality of $d(\mathcal{C})$.

An efficient decoding algorithm for GRS codes - ECP

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.

If there have been no more than t errors (i.e. $\mathrm{w}_H(\mathbf{e}) \leq t$), then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \quad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\mathrm{supp}(\mathbf{a})}$$

Is the solution unique?

YES, since

$$d(\mathcal{A}) + d(\mathcal{C}) > n$$

Suppose that $\mathbf{e}_1$ and $\mathbf{e}_2$ are solutions of the above system. Then,

$$\langle \mathbf{e}_1, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}_2, \mathbf{a} * \mathbf{b} \rangle \text{ with } \begin{cases} \mathrm{supp}(\mathbf{e}_1) \subseteq \overline{\mathrm{supp}(\mathbf{a})} \\ \mathrm{supp}(\mathbf{e}_2) \subseteq \overline{\mathrm{supp}(\mathbf{a})} \end{cases}$$

Then $\mathbf{e}_1 - \mathbf{e}_2 \in \mathcal{C}$, but

$$\mathrm{w}_H(\mathbf{e}_1 - \mathbf{e}_2) \leq n - |\mathrm{supp}(\mathbf{a})| \leq d(\mathcal{C}) - 1$$

which **contradicts** the minimality of $d(\mathcal{C})$.

Error-correcting pairs (ECP)

- **GRS** code are the prime examples of codes that have a t-ECP.

Error-correcting pairs (ECP)

- **GRS** code are the prime examples of codes that have a t-ECP.
- Let $\mathcal{D}$ be a code that has $(\mathcal{A}, \mathcal{B})$ as t-ECP and suppose that $\mathcal{C} \subseteq \mathcal{D}$. Then $(\mathcal{A}, \mathcal{B})$ is also a t-ECP for $\mathcal{C}$.

Error-correcting pairs (ECP)

- **GRS** code are the prime examples of codes that have a t-ECP.
- Let $\mathcal{D}$ be a code that has $(\mathcal{A}, \mathcal{B})$ as t-ECP and suppose that $\mathcal{C} \subseteq \mathcal{D}$. Then $(\mathcal{A}, \mathcal{B})$ is also a t-ECP for $\mathcal{C}$.

  In particular **subcodes of GRS** codes have a t-ECP

  1. **Alternant codes**
  2. **Goppa codes**

Error-correcting pairs (ECP)

- **GRS** code are the prime examples of codes that have a t-ECP.
- Let $\mathcal{D}$ be a code that has $(\mathcal{A}, \mathcal{B})$ as t-ECP and suppose that $\mathcal{C} \subseteq \mathcal{D}$. Then $(\mathcal{A}, \mathcal{B})$ is also a t-ECP for $\mathcal{C}$.

  In particular **subcodes of GRS** codes have a t-ECP

  1. **Alternant codes**
  2. **Goppa codes**
- **AG** codes also have a t-ECP

Error-correcting pairs (ECP)

- **GRS** code are the prime examples of codes that have a t-ECP.
- Let $\mathcal{D}$ be a code that has $(\mathcal{A}, \mathcal{B})$ as t-ECP and suppose that $\mathcal{C} \subseteq \mathcal{D}$. Then $(\mathcal{A}, \mathcal{B})$ is also a t-ECP for $\mathcal{C}$.

  In particular **subcodes of GRS** codes have a t-ECP

  1. **Alternant codes**
  2. **Goppa codes**
- **AG** codes also have a t-ECP
- ECP for **cyclic codes** were investigated by Duursma and Kötter.

I. Duursma
Decoding codes from curves and cyclic codes.
Ph.D thesis, Eindhoven University of Technology (1993)

I. Duursma, R. Kötter.
Error-locating pairs for cyclic codes.
IEEE Trans. Inform. Theory, Vol.40, 1108–1121 (1994)

Error-correcting pairs (ECP)

Error-correcting pairs (ECP)

Let:

- $\mathcal{C}$ be an $[n, K(\mathcal{C})]_q$ code. and

R. Pellikaan
On decoding by error location and dependent sets of error positions.
Discrete Math., 106–107: 369–381 (1992).

R. Kötter.
A unified description of an error locating procedure for linear codes.
In Proceedings of Algebraic and Combinatorial Coding Theory, 113–117. Voneshta Voda (1992).

Error-correcting pairs (ECP)

Error-correcting pairs (ECP)

Let:

- $\mathcal{C}$ be an $[n, K(\mathcal{C})]_q$ code.

and

- A be an $[n, K(A)]_{q^m}$ code
- B be an $[n, K(B)]_{q^m}$ code

R. Pellikaan
On decoding by error location and dependent sets of error positions.
Discrete Math., 106–107: 369–381 (1992).

R. Kötter.
A unified description of an error locating procedure for linear codes.
In Proceedings of Algebraic and Combinatorial Coding Theory, 113–117. Voneshta Voda (1992).

Error-correcting pairs (ECP)

Error-correcting pairs (ECP)

Let:

- ➜ $\mathcal{C}$ be an $[n, K(\mathcal{C})]_q$ code.

and

- ➜ A be an $[n, K(A)]_{q^m}$ code
- ➜ B be an $[n, K(B)]_{q^m}$ code

(A, B) is a ***t*-ECP** for $\mathcal{C}$ if the following properties hold:

E.1 $(A * B) \perp \mathcal{C}$.

E.2 $K(A) > t$.

E.3 $d(B^{\perp}) > t$.

E.4 $d(A) + d(\mathcal{C}) > n$.

R. Pellikaan
On decoding by error location and dependent sets of error positions.
Discrete Math., 106–107: 369–381 (1992).

R. Kötter.
A unified description of an error locating procedure for linear codes.
In Proceedings of Algebraic and Combinatorial Coding Theory, 113–117. Voneshta Voda (1992).

Error-correcting pairs (ECP)

Error-correcting pairs (ECP)

Let:

- ➜ $\mathcal{C}$ be an $[n, K(\mathcal{C})]_q$ code.

and

- ➜ A be an $[n, K(A)]_{q^m}$ code
- ➜ B be an $[n, K(B)]_{q^m}$ code

(A, B) is a ***t*-ECP** for $\mathcal{C}$ if the following properties hold:

- E.1 $(A * B) \perp \mathcal{C}$.
- E.2 $K(A) > t$.
- E.3 $d(B^{\perp}) > t$.
- E.4 $d(A) + d(\mathcal{C}) > n$.

An $[n, k]_q$ code which has a t-ECP over $\mathbb{F}_{q^m}$ has an efficient decoding algorithm.

R. Pellikaan
On decoding by error location and dependent sets of error positions.
Discrete Math., 106–107: 369–381 (1992).

R. Kötter.
A unified description of an error locating procedure for linear codes.
In Proceedings of Algebraic and Combinatorial Coding Theory, 113–117. Voneshta Voda (1992).

Error-correcting pairs (ECP)

Let $(\mathcal{A}, \mathcal{B})$ be a t-ECP for $\mathcal{C}$.

sent codeword

$$\mathbf{y} = \mathbf{c} + \mathbf{e} \quad \text{with } \mathrm{w}_H(\mathbf{e}) \leq t$$

received word

error vector

1. There exists $\mathbf{a} \in \mathcal{A}$, $\mathbf{a} \neq \mathbf{0}$ such that
$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = 0 \text{ for all } \mathbf{b} \in \mathcal{B} \tag{1}$$
2. For every solution $\mathbf{a} \in \mathcal{A}$ of (1) we have that:
$$\mathbf{a} * \mathbf{e} = \mathbf{0}$$
3. Since $d(\mathcal{A}) + d(\mathcal{C}) \geq n$. Then, $\mathbf{e}$ is the **unique** solution of:
$$\langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \mathbf{0} \text{ with } \mathbf{e} * \mathbf{a} = 0 \text{ for all } \mathbf{b} \in \mathcal{B}$$

4. Key Attacks

1. Introduction
2. Support Splitting Algorithm
3. Distinguisher for GRS codes
4. Attack against subcodes of GRS codes
5. Error-Correcting Pairs
6. **Attack against GRS codes**
7. Attack against Reed-Muller codes
8. Attack against Algebraic Geometry codes
9. Goppa codes still resist