The Subfield Metric and Applications to Quantum Error Correction

Anna-Lena Horlemann

University of St.Gallen, Switzerland

NCM - Aalborg
July 7th 2023



Joint work with Markus Grassl and Violetta Weger.

1. Motivation for a New Metric in Quantum Error Correction
2. The Subfield Weight(s) and Metric
3. Upper and Lower Bounds in the λ-Subfield Metric
4. Reed-Solomon Codes in the λ-Subfield Metric
5. Summary and Conclusions

Quantum Error Correction in $\mathbb{F}_{q^2}^n$

- Two types of quantum errors:
  - symbol errors (bit flips)
  - phase errors
- Symbol errors can be corrected as in classical (linear) codes.
- Phase errors can be turned into symbol errors after Fourier transformation and then be corrected as usual.

[1] Hermitian inner product for linear codes.

Quantum Error Correction in $\mathbb{F}_{q^2}^n$

- Two types of quantum errors:
  - symbol errors (bit flips)
  - phase errors
- Symbol errors can be corrected as in classical (linear) codes.
- Phase errors can be turned into symbol errors after Fourier transformation and then be corrected as usual.
- We can create a length n stabilizer quantum code from certain additive codes in $\mathbb{F}_q^{2n}$, where
  - symbol errors are corrected in the first half,
  - phase errors are corrected in the second half.
- If we use

$$\mathbb{F}_q^{2n} \cong \mathbb{F}_{q^2}^n$$

and use self-orthogonal codes w.r.t. the trace-symplectic[1] form, we can correct errors w.r.t. Hamming metric in $\mathbb{F}_{q^2}^n$.

[1] Hermitian inner product for linear codes.

Asymmetric Quantum Error Correction

- In most quantum systems phase errors happen a lot more than symbol errors.
  $\Longrightarrow$ **asymmetric error behavior**
- **Other approaches:** Use different minimum distance in front and back half for the two error types.
- **Our approach:** with

$$\begin{aligned} \mathbb{F}_q^{2n} &\longrightarrow \mathbb{F}_{q^2}^n \\ (v_1, \ldots, v_{2n}) &\longmapsto (\gamma v_1 + v_{n+1}, \ldots, \gamma v_n + v_{2n}) \end{aligned}$$

  the **phase errors** are represented as elements in $\mathbb{F}_q^*$ and any **general error** (combination of symbol and phase error) is represented as an element in $\mathbb{F}_{q^2} \backslash \mathbb{F}_q$.

1. Motivation for a New Metric in Quantum Error Correction
2. The Subfield Weight(s) and Metric
3. Upper and Lower Bounds in the λ-Subfield Metric
4. Reed-Solomon Codes in the λ-Subfield Metric
5. Summary and Conclusions

The λ-Subfield Weight

Definition

Let $\lambda \geq 1/2$. We define the **λ-subfield weight** on $\mathbb{F}_{q^m}$ as

$$\mathrm{wt}_\lambda(x) := \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \in \mathbb{F}_q \setminus \{0\}, \\ \lambda & \text{if } x \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q, \end{cases}$$

and extend it additively coordinate-wise to $\mathbb{F}_{q^m}^n$.
The **λ-subfield distance** between $x, y \in \mathbb{F}_{q^m}^n$ is defined as

$$d_\lambda(x, y) := \mathrm{wt}_\lambda(x - y).$$

The λ-Subfield Weight

Definition

Let $\lambda \geq 1/2$. We define the **λ-subfield weight** on $\mathbb{F}_{q^m}$ as

$$\mathrm{wt}_\lambda(x) := \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \in \mathbb{F}_q \setminus \{0\}, \\ \lambda & \text{if } x \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q, \end{cases}$$

and extend it additively coordinate-wise to $\mathbb{F}_{q^m}^n$.
The **λ-subfield distance** between $x, y \in \mathbb{F}_{q^m}^n$ is defined as

$$d_\lambda(x, y) := \mathrm{wt}_\lambda(x - y).$$

Theorem

The λ-subfield distance is a metric on $\mathbb{F}_{q^m}^n$.

The Base-Roof Weight

Definition

For $x \in \mathbb{F}_{q^m}^n$ we define its

- **base weight**

$$\mathrm{wt}_b(x) := |\{i \in \{1, \ldots, n\} \mid x_i \in \mathbb{F}_q \setminus \{0\}\}|$$

- **roof weight** as

$$\mathrm{wt}_r(x) := |\{i \in \{1, \ldots, n\} \mid x_i \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q\}|.$$

- **base-roof (BR)-weight** of x as

$$\mathrm{wt}_{BR}(x) := (\mathrm{wt}_b(x), \mathrm{wt}_r(x)).$$

Analogously, we define the **BR-distance** as

$$d_{BR}(x, y) := (\mathrm{wt}_b(x - y), \mathrm{wt}_r(x - y)).$$

The Base-Roof Distance

The BR-distance is not a metric, however:

Theorem

Consider the following partial order on $\mathbb{N}_0^2$*:*

$$(s,t) \preceq (s',t') :\iff s \leq s' \text{ and } t \leq t'.$$

Let $x, y \in \mathbb{F}_{q^m}^n$*. Then*

1. $d_{BR}(x,y) = (0,0)$ *if and only if* $x = y$.
2. $d_{BR}(x,y) \succ (0,0)$ *for* $x \neq y$.
3. $d_{BR}(x,y) = d_{BR}(y,x)$.
4. $d_{BR}(x,y) \not\succ d_{BR}(x,z) + d_{BR}(z,y)$ *for* $x, y, z \in \mathbb{F}_{q^m}^n$.

Error Correction Capabilities

Lemma

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a code with minimum λ-subfield distance d. Then any error vector of λ-weight at most $\lfloor \frac{d-1}{2} \rfloor$ can uniquely be corrected, i.e., there is one unique closest codeword $c \in \mathcal{C}$ to a received word $r = c + e$ if $\mathrm{wt}_\lambda(e) \leq \lfloor \frac{d-1}{2} \rfloor$.

Error Correction Capabilities

Lemma

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a code with minimum λ-subfield distance d. Then any error vector of λ-weight at most $\lfloor \frac{d-1}{2} \rfloor$ can uniquely be corrected, i.e., there is one unique closest codeword $c \in \mathcal{C}$ to a received word $r = c + e$ if $\mathrm{wt}_\lambda(e) \leq \lfloor \frac{d-1}{2} \rfloor$.

What about the BR-distance?

Error Correction Capabilities

Lemma

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a code with minimum λ-subfield distance d. Then any error vector of λ-weight at most $\lfloor \frac{d-1}{2} \rfloor$ can uniquely be corrected, i.e., there is one unique closest codeword $c \in \mathcal{C}$ to a received word $r = c + e$ if $\mathrm{wt}_\lambda(e) \leq \lfloor \frac{d-1}{2} \rfloor$.

What about the BR-distance?

Definition

We define the *set of BR-minimal distances*

$$d_{BR}(\mathcal{C}) := \min\{d_{BR}(x, y) \in \mathbb{N}_0^2 \mid x, y \in \mathcal{C}, x \neq y\},$$

where $\min(D) := \{(s, t) \in D \mid \nexists (s', t') \in D \colon (s', t') \prec (s, t)\}$.

The BR-minimum distance(s) uniquely determine(s) the λ-subfield distance and the error correction capability from above applies.

Example

Consider $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 = \alpha + 1$, and the code $\mathcal{C} \subseteq \mathbb{F}_4^6$ generated by

$$G = \begin{pmatrix} 1 & 1 & 1 & \alpha & \alpha & \alpha \end{pmatrix}.$$

c	$\mathrm{wt}_{BR}(c)$
$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$(0,0)$
$\begin{pmatrix} 1 & 1 & 1 & \alpha & \alpha & \alpha \end{pmatrix}$	$(3,3)$
$\begin{pmatrix} \alpha^2 & \alpha^2 & \alpha^2 & 1 & 1 & 1 \end{pmatrix}$	$(3,3)$
$\begin{pmatrix} \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 \end{pmatrix}$	$(0,6)$

We hence get

$$d_{BR}(\mathcal{C}) = \{(3,3),(0,6)\}.$$

In the λ-subfield metric, we get the minimum distance

$$d_\lambda(\mathcal{C}) = \min\{3+3\lambda, 6\lambda\}.$$

Example

Consider $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 = \alpha + 1$, and the code $\mathcal{C} \subseteq \mathbb{F}_4^6$ generated by

$$G = \begin{pmatrix} 1 & 1 & 1 & \alpha & \alpha & \alpha \end{pmatrix}.$$

c	$\mathrm{wt}_{BR}(c)$
$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$(0,0)$
$\begin{pmatrix} 1 & 1 & 1 & \alpha & \alpha & \alpha \end{pmatrix}$	$(3,3)$
$\begin{pmatrix} \alpha^2 & \alpha^2 & \alpha^2 & 1 & 1 & 1 \end{pmatrix}$	$(3,3)$
$\begin{pmatrix} \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 \end{pmatrix}$	$(0,6)$

For $\lambda = 2$ and $d_\lambda(\mathcal{C}) = 9$, we can correct

- 4 base errors and 0 roof errors,
- 2 base errors and 1 roof error, or
- 0 base errors and 2 roof errors.

Example

Consider $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 = \alpha + 1$, and the code $\mathcal{C} \subseteq \mathbb{F}_4^6$ generated by

$$G = \begin{pmatrix} 1 & 1 & 1 & \alpha & \alpha & \alpha \end{pmatrix}.$$

c	$\mathrm{wt}_{BR}(c)$
$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$(0,0)$
$\begin{pmatrix} 1 & 1 & 1 & \alpha & \alpha & \alpha \end{pmatrix}$	$(3,3)$
$\begin{pmatrix} \alpha^2 & \alpha^2 & \alpha^2 & 1 & 1 & 1 \end{pmatrix}$	$(3,3)$
$\begin{pmatrix} \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 \end{pmatrix}$	$(0,6)$

For $\lambda = 2$ and $d_\lambda(\mathcal{C}) = 9$, we can correct

- 4 base errors and 0 roof errors,
- 2 base errors and 1 roof error, or
- 0 base errors and 2 roof errors.

The minimum Hamming distance is 6 $\implies$ 2 errors correctable.

1 Motivation for a New Metric in Quantum Error Correction

2 The Subfield Weight(s) and Metric

3 Upper and Lower Bounds in the λ-Subfield Metric

4 Reed-Solomon Codes in the λ-Subfield Metric

5 Summary and Conclusions

Sphere Packing and Covering Bound

Theorem

$$
\begin{aligned}
A_{q^m,\lambda}(n,d) &\leq \frac{\left|\mathbb{F}_{q^m}^n\right|}{\left|B_{\lfloor \frac{d-1}{2} \rfloor,\lambda}(\mathbb{F}_{q^m}^n)\right|} \\
&= \frac{q^{mn}}{\sum_{j=0}^{\lfloor \frac{d-1}{2} \rfloor} \sum_{i=0}^{\lfloor \frac{j}{\lambda} \rfloor} (q^m-q)^i \binom{n}{i} (q-1)^{j-\lambda i} \binom{n-i}{j-\lambda i}} \\
A_{q^m,\lambda}(n,d) &\geq \frac{\left|\mathbb{F}_{q^m}^n\right|}{\left|B_{d-1,\lambda}(\mathbb{F}_{q^m}^n)\right|} \\
&= \frac{q^{mn}}{\sum_{j=0}^{d-1} \sum_{i=0}^{\lfloor \frac{j}{\lambda} \rfloor} (q^m-q)^i \binom{n}{i} (q-1)^{j-\lambda i} \binom{n-i}{j-\lambda i}}.
\end{aligned}
$$

Singleton-type Bound

Theorem

Let $\lambda \geq 1$ and $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a code (not necessarily linear) with minimum λ-subfield distance d_λ. Then

$$\left\lfloor \frac{d_\lambda - 1}{\lambda} \right\rfloor \leq n - \lceil \log_{q^m}(|\ \mathcal{C}\ |) \rceil.$$

Thus for linear codes of dimension k, we get

$$\left\lfloor \frac{d_\lambda - 1}{\lambda} \right\rfloor \leq n - k$$

$$\iff \lambda(n-k) + 1 \leq d_\lambda \leq \lambda(n-k+1)$$

Plotkin Bound

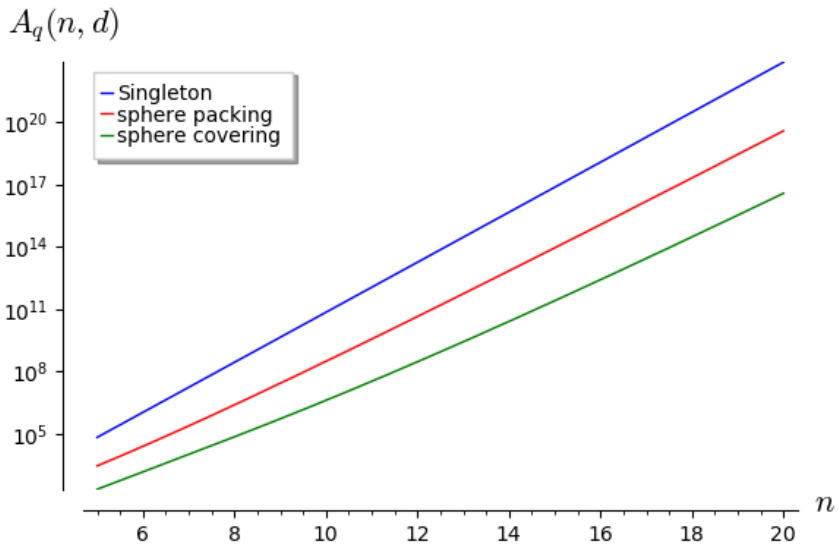
Theorem

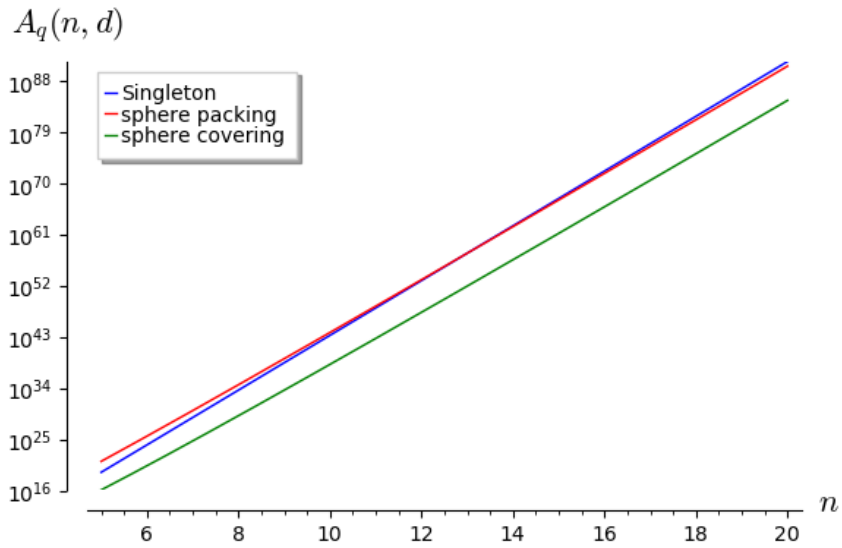
Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code, then

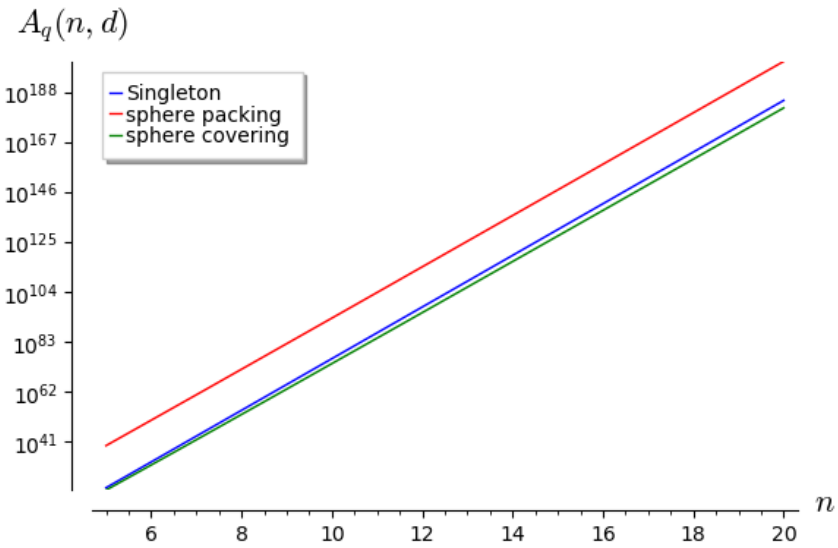
$$d_\lambda(\mathcal{C}) \leq \frac{|\mathcal{C}|}{|\mathcal{C}| - 1} n(\lambda - (\lambda - 1)q^{1-m} - q^{-m}).$$

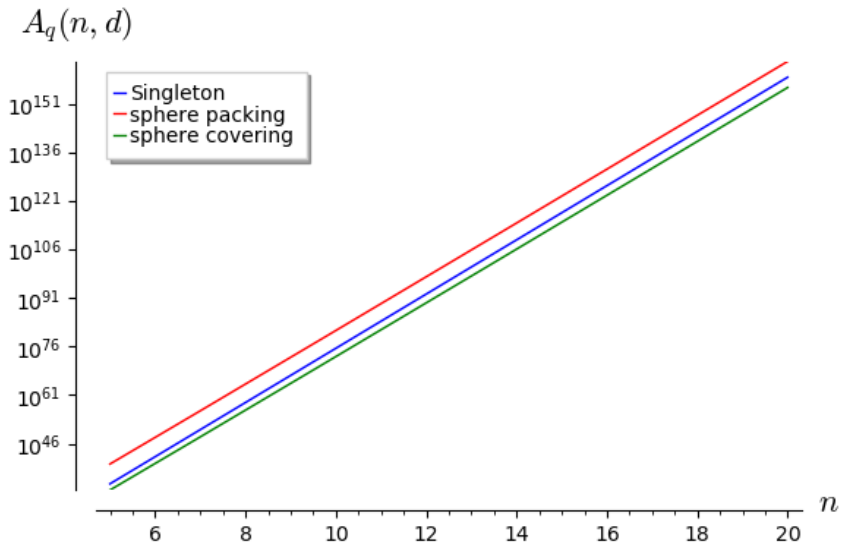
(Analogous result for non-linear codes.)

Comparison of Bounds





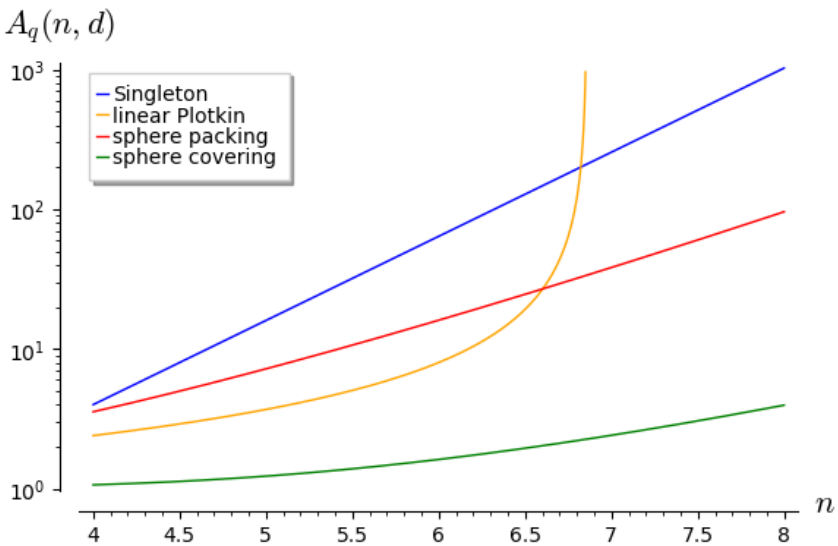


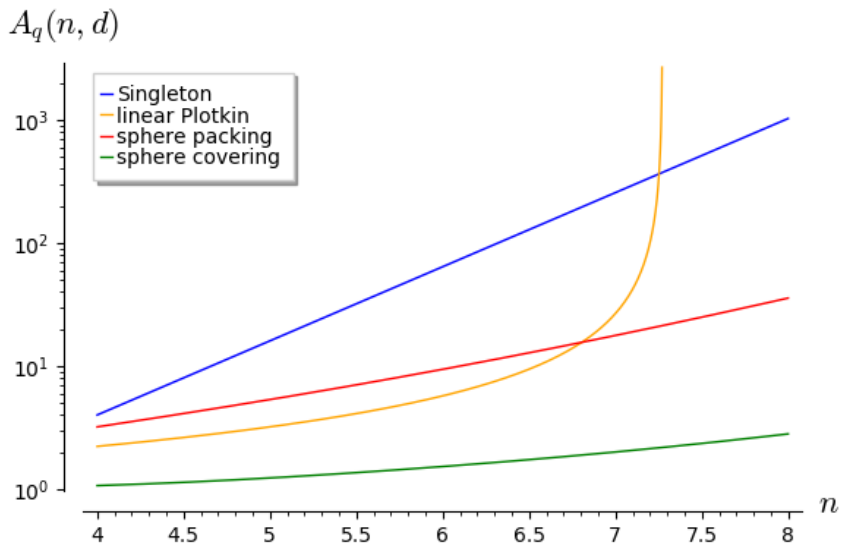


$q = 4, m = 2, \lambda = 4, d = 7,$ $\quad q = 4, m = 8, \lambda = 5, d = 10$

$q = 521, m = 4, \lambda = 3, d = 10,$ $\quad q = 5, m = 12, \lambda = 3, d = 5$

Comparison of Bounds





$q = 521, m = 4, \lambda = 3, d = 10, \quad q = 5, m = 12, \lambda = 3, d = 5$

Optimal Codes

Theorem

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code. Then the minimal λ-subfield distance satisfies

$$\lambda(n-k)+1 \leq d_\lambda \leq \lambda(n-k+1)$$

for $\lambda \geq 1$. Thus, the code achieves the Singleton-type bound and is an ***MλD (maximal λ-subfield distance)*** *code.*

Optimal Codes

Theorem

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code. Then the minimal λ-subfield distance satisfies

$$\lambda(n-k)+1 \leq d_\lambda \leq \lambda(n-k+1)$$

*for $\lambda \geq 1$. Thus, the code achieves the Singleton-type bound and is an **MλD (maximal λ-subfield distance)** code.*

$\Longrightarrow$ MRD is MλD!

Optimal Codes

Theorem

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code. Then the minimal λ-subfield distance satisfies

$$\lambda(n-k)+1 \leq d_\lambda \leq \lambda(n-k+1)$$

*for $\lambda \geq 1$. Thus, the code achieves the Singleton-type bound and is an **MλD (maximal λ-subfield distance)** code.*

$\Longrightarrow$ MRD is MλD!

Corollary

MλD codes are dense in the set of all codes whenever MRD codes are dense (in particular for linear codes and growing m).

1 Motivation for a New Metric in Quantum Error Correction

2 The Subfield Weight(s) and Metric

3 Upper and Lower Bounds in the λ-Subfield Metric

4 Reed-Solomon Codes in the λ-Subfield Metric

5 Summary and Conclusions

Reed-Solomon Codes

- For any code we have $d_\lambda(\mathcal{C}) \geq d_H(\mathcal{C})$.
- RS codes include all-one vector.

$\implies$ $[n, k]$-RS code has minimum λ-subfield distance

$$n - k + 1 \leq d_\lambda(\mathcal{C}) \leq n.$$

Reed-Solomon Codes

- For any code we have $d_\lambda(\mathcal{C}) \geq d_H(\mathcal{C})$.
- RS codes include all-one vector.

$\implies$ $[n, k]$-RS code has minimum λ-subfield distance

$$n - k + 1 \leq d_\lambda(\mathcal{C}) \leq n.$$

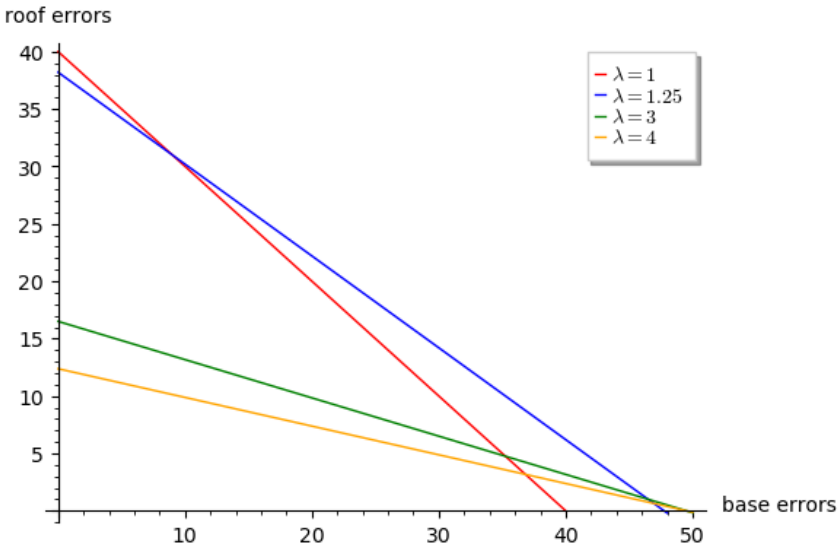
Theorem

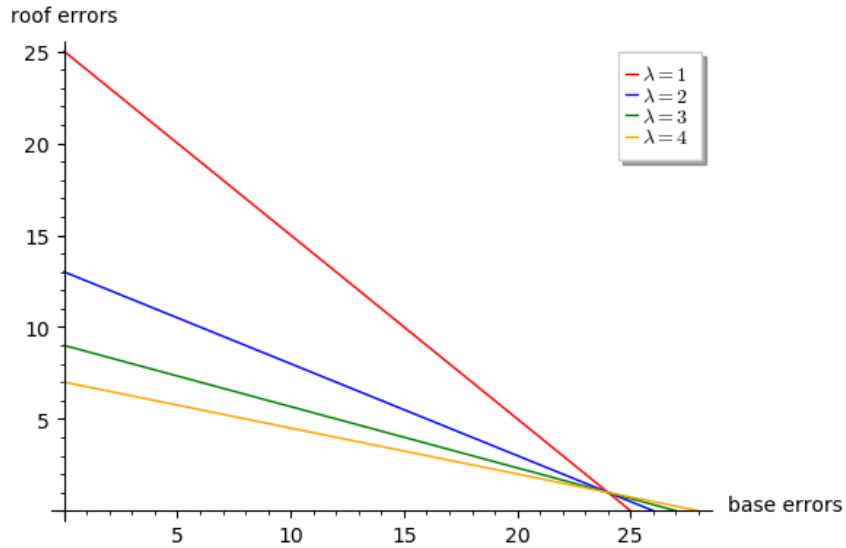
Let $\lambda \geq 1$ and $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a Reed-Solomon code of dimension k. If $\lambda n - ((\lambda - 1)q + 1)(k - 1) \leq n$ then

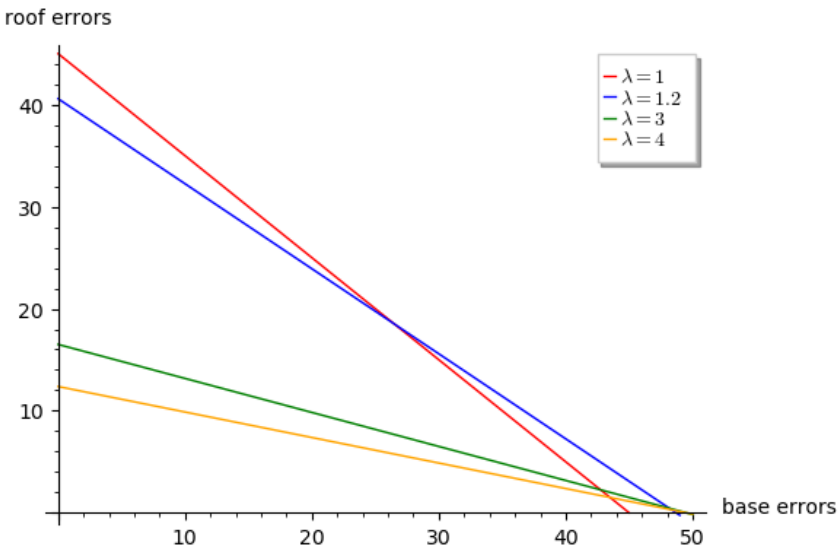
$$d_\lambda(\mathcal{C}) \geq \lambda n - ((\lambda - 1)q + 1)(k - 1).$$

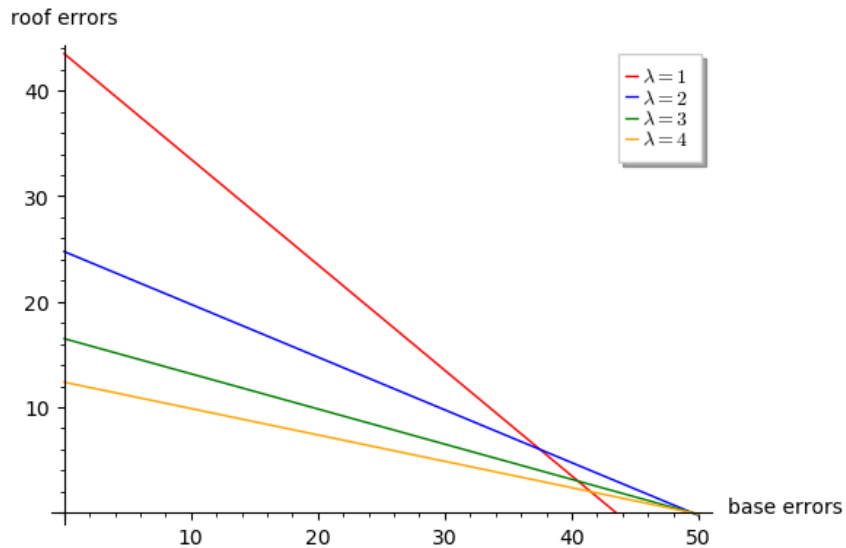
Otherwise, $d_\lambda(\mathcal{C}) = n$.

Error Correction Capabilities









$n = 100, k = 20, q = 2, \quad n = 100, k = 50, q = 2$

$n = 100, k = 10, q = 7, \quad n = 100, k = 14, q = 7$

1 Motivation for a New Metric in Quantum Error Correction

2 The Subfield Weight(s) and Metric

3 Upper and Lower Bounds in the λ-Subfield Metric

4 Reed-Solomon Codes in the λ-Subfield Metric

5 Summary and Conclusions

Summary and Outlook

- In applications like quantum error correction we observe different error types with different frequencies.
  $\Longrightarrow$ **asymmetric error correction**

Summary and Outlook

- In applications like quantum error correction we observe different error types with different frequencies.
  $\Longrightarrow$ **asymmetric error correction**
- We distinguish errors from the base field and those outside of it (roof errors).
  $\Longrightarrow$ **λ-subfield metric**

Summary and Outlook

- In applications like quantum error correction we observe different error types with different frequencies.
  $\Longrightarrow$ **asymmetric error correction**
- We distinguish errors from the base field and those outside of it (roof errors).
  $\Longrightarrow$ **λ-subfield metric**
- We show that this is a metric, and derive sphere covering, sphere packing, Singleton and Plotkin bound.
- MRD codes are MλD codes.
- Low rate RS codes can correct more errors with higher λ.

Summary and Outlook

- In applications like quantum error correction we observe different error types with different frequencies.
  $\Longrightarrow$ **asymmetric error correction**
- We distinguish errors from the base field and those outside of it (roof errors).
  $\Longrightarrow$ **λ-subfield metric**
- We show that this is a metric, and derive sphere covering, sphere packing, Singleton and Plotkin bound.
- MRD codes are MλD codes.
- Low rate RS codes can correct more errors with higher λ.
- Also: Macwilliams identities for square extensions (only).

Summary and Outlook

- In applications like quantum error correction we observe different error types with different frequencies.
  $\Longrightarrow$ **asymmetric error correction**
- We distinguish errors from the base field and those outside of it (roof errors).
  $\Longrightarrow$ **λ-subfield metric**
- We show that this is a metric, and derive sphere covering, sphere packing, Singleton and Plotkin bound.
- MRD codes are MλD codes.
- Low rate RS codes can correct more errors with higher λ.
- Also: Macwilliams identities for square extensions (only).

Thank you for your attention!

Questions? – Comments?

