

The Subfield Metric and Applications to Quantum Error Correction

Anna-Lena Horlemann

University of St.Gallen, Switzerland

Combinatorics 2024

June 4th 2024



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 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.

¹Hermitian 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-symplectic¹ form, we can correct errors w.r.t. Hamming metric in $\mathbb{F}_{q^2}^n$.

¹Hermitian inner product for linear codes.

Asymmetric Quantum Error Correction

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

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

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 $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

- 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 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

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

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

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

The λ -Subfield Weight

Definition

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

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

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

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

Theorem

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

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 $\text{wt}_\lambda(e) \leq \lfloor \frac{d-1}{2} \rfloor$.

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	$\text{wt}_\lambda(c)$
$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	0
$\begin{pmatrix} 1 & 1 & 1 & \alpha & \alpha & \alpha \end{pmatrix}$	$3 + 3\lambda$
$\begin{pmatrix} \alpha^2 & \alpha^2 & \alpha^2 & 1 & 1 & 1 \end{pmatrix}$	$3 + 3\lambda$
$\begin{pmatrix} \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 \end{pmatrix}$	6λ

We hence get

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

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	$\text{wt}_\lambda(c)$
$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	0
$\begin{pmatrix} 1 & 1 & 1 & \alpha & \alpha & \alpha \end{pmatrix}$	$3 + 3\lambda$
$\begin{pmatrix} \alpha^2 & \alpha^2 & \alpha^2 & 1 & 1 & 1 \end{pmatrix}$	$3 + 3\lambda$
$\begin{pmatrix} \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 \end{pmatrix}$	6λ

For $\lambda = 2$ we get $d_\lambda(\mathcal{C}) = 9$, and 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	$\text{wt}_\lambda(c)$
$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	0
$\begin{pmatrix} 1 & 1 & 1 & \alpha & \alpha & \alpha \end{pmatrix}$	$3 + 3\lambda$
$\begin{pmatrix} \alpha^2 & \alpha^2 & \alpha^2 & 1 & 1 & 1 \end{pmatrix}$	$3 + 3\lambda$
$\begin{pmatrix} \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 \end{pmatrix}$	6λ

For $\lambda = 2$ we get $d_\lambda(\mathcal{C}) = 9$, and 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 Summary and Conclusions

Sphere Packing and Covering Bound

Theorem

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

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

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

For linear codes of dimension k we get

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

(Look at the reduced row echelon form of the generator matrix.)

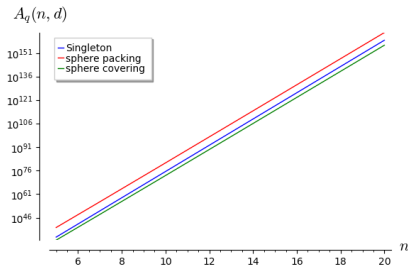
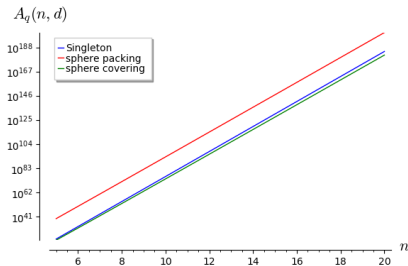
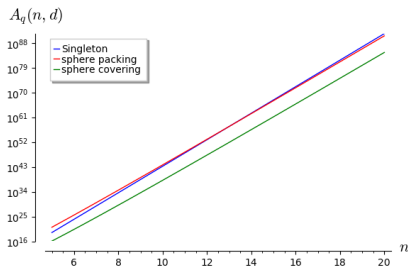
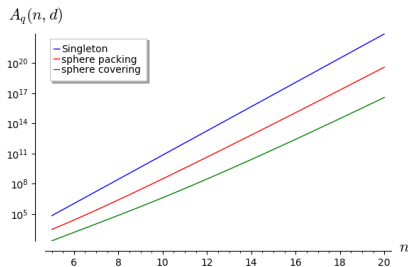
Plotkin Bound

Theorem

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

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

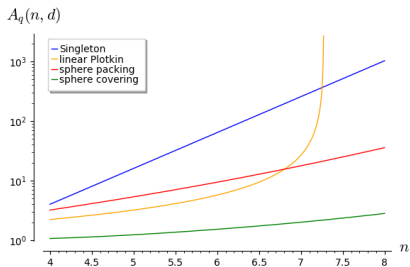
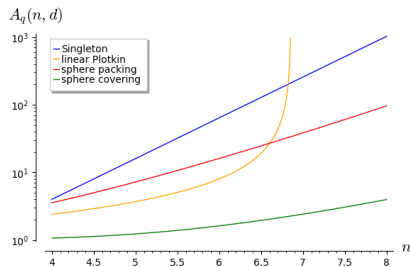
Comparison of Bounds



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

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

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

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

*for $\lambda \geq 1$. Thus, the code achieves the Singleton-type bound and is an **MLD** (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

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

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

$\implies$ MRD is M λ D!

Optimal Codes

Theorem

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

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

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

$\implies$ MRD is M λ D!

Corollary

M λ D 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 Summary and Conclusions

Summary and Outlook

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

Summary and Outlook

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

Summary and Outlook

- In applications like quantum error correction we observe different error types with different frequencies.
⇒ **asymmetric error correction**
- We distinguish errors from the base field and those outside of it (roof errors).
⇒ **λ -subfield metric**
- We show that this is a metric, and derive sphere covering, sphere packing, Singleton and Plotkin bound.
- MRD codes are M λ D codes.

Summary and Outlook

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

Summary and Outlook

- In applications like quantum error correction we observe different error types with different frequencies.
⇒ **asymmetric error correction**
- We distinguish errors from the base field and those outside of it (roof errors).
⇒ **λ -subfield metric**
- We show that this is a metric, and derive sphere covering, sphere packing, Singleton and Plotkin bound.
- MRD codes are M λ D codes.
- Also: Macwilliams identities for square extensions (only).
- **Open question:** Good efficiently decodable code constructions?!

Summary and Outlook

- In applications like quantum error correction we observe different error types with different frequencies.
⇒ **asymmetric error correction**
- We distinguish errors from the base field and those outside of it (roof errors).
⇒ **λ -subfield metric**
- We show that this is a metric, and derive sphere covering, sphere packing, Singleton and Plotkin bound.
- MRD codes are M λ D codes.
- Also: Macwilliams identities for square extensions (only).
- **Open question:** Good efficiently decodable code constructions?!

Thank you for your attention!

Questions? – Comments?

