Projective Metrics for Coding Theory

Gabor Riccardi

University of Pavia (UniPv)

with **Hugo Sauerbier Couvée** , Technical University of Munich (TUM)

20 September 2023

Introduction to Coding Theory

- Retrieve information from corrupted messages

Introduction to Coding Theory

- Retrieve information from corrupted messages
- Store data (which is just sending a message to your future self)

Introduction to Coding Theory

- Retrieve information from corrupted messages
- Store data (which is just sending a message to your future self)
- Data compression

Introduction to Coding Theory

- Retrieve information from corrupted messages
- Store data (which is just sending a message to your future self)
- Data compression
- Cryptography

How?

How?

Redundancy!

How?

Redundancy!

(Smartly)

How?

Redundancy!
(Smartly)

Let's repeat each row of a message three times and then send it.

Redundancy!
(Smartly)

Let's repeat each row of a message three times and then send it.
If we obtain the message:

Redundancy!
(Smartly)

Let's repeat each row of a message three times and then send it.
If we obtain the message:

0	0	0	1	0	1	0	0	0
0	0	0	1	1	1	0	0	0
0	0	0	1	1	1	0	0	0

How?

Redundancy!
(Smartly)

Let's repeat each row of a message three times and then send it.
If we obtain the message:

0	0	0	1	0	1	0	0	0
0	0	0	1	1	1	0	0	0
0	0	0	1	1	1	0	0	0

Since "1" appears twice and "0" once, we may assume more likely that the original message was:

How?

Redundancy!
(Smartly)

Let's repeat each row of a message three times and then send it.
If we obtain the message:

0	0	0	1	0	1	0	0	0
0	0	0	1	1	1	0	0	0
0	0	0	1	1	1	0	0	0

Since "1" appears twice and "0" once, we may assume more likely that the original message was:

0	0	0	1	1	1	0	0	0

Redundancy!
(Smartly)

Let's repeat each row of a message three times and then send it.
If we obtain the message:

0	0	0	1	0	1	0	0	0
0	0	0	1	1	1	0	0	0
0	0	0	1	1	1	0	0	0

Since "1" appears twice and "0" once, we may assume more likely that the original message was:

0	0	0	1	1	1	0	0	0

But this way, we took three times the length of the message to correct one error!

How?

Redundancy!
(Smartly)

Let's repeat each row of a message three times and then send it.
If we obtain the message:

Since "1" appears twice and "0" once, we may assume more likely that the original message was:

0	0	0	1	1	1	0	0	0

But this way, we took three times the length of the message to correct one error!

Btw the message says SOS in Morse, so maybe go seek help.

A better way to do it

We rearrange the original message $\boxed{0}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{0}$ in a 4 by 4 grid:

A better way to do it

We rearrange the original message

0	0	0	1	1	1	0	0	0

in a 4 by 4 grid:

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

A better way to do it

We rearrange the original message

0	0	0	1	1	1	0	0	0

in a 4 by 4 grid:

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

Where the red cells are the four redundant bits which encode the parity of subsets of columns or rows in the following way.

A BETTER WAY TO DO IT

We rearrange the original message

0	0	0	1	1	1	0	0	0

in a 4 by 4 grid:

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

Where the red cells are the four redundant bits which encode the parity of subsets of columns or rows in the following way.

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

$$\boxed{0} = \boxed{1} + \boxed{1}$$

A better way to do it

We rearrange the original message

0	0	0	1	1	1	0	0	0

in a 4 by 4 grid:

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

Where the red cells are the four redundant bits which encode the parity of subsets of columns or rows in the following way.

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

$$\boxed{0} = \boxed{1} + \boxed{1}$$

A better way to do it

We rearrange the original message | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | in a 4 by 4 grid:

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

Where the red cells are the four redundant bits which encode the parity of subsets of columns or rows in the following way.

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

$\boxed{1} = \boxed{1}$

A better way to do it

We rearrange the original message

0	0	0	1	1	1	0	0	0

in a 4 by 4 grid:

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

Where the red cells are the four redundant bits which encode the parity of subsets of columns or rows in the following way.

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

$$\boxed{0} = \boxed{1} + \boxed{1}$$

A better way to do it

We rearrange the original message

0	0	0	1	1	1	0	0	0

in a 4 by 4 grid:

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

Where the red cells are the four redundant bits which encode the parity of subsets of columns or rows in the following way.

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

$$\boxed{0} = \boxed{1} + \boxed{1}$$

Since $2^4 =$ total number of bits $+$ (case in which there is no error) $= 15 + 1$ and if there is up to one error, every redundant bit halvens the number the possible locations of where the error might be, we can always correct up to one error in the message.

Hamming Codes

The subset of codes in $\mathbb{F}_2^{15}$ constructed the same way are called **Hamming Codes**.

Hamming Codes

The subset of codes in $\mathbb{F}_2^{15}$ constructed the same way are called **Hamming Codes**.

	0	0	1
0	0	0	1
1	0	1	1
0	1	0	0

+

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

=

	0	0	1
1	0	0	0
1	1	0	1
0	1	0	0

Hamming Codes

The subset of codes in $\mathbb{F}_2^{15}$ constructed the same way are called **Hamming Codes**.

	0	0	1
0	0	0	1
1	0	1	1
0	1	0	0

+

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

=

	0	0	1
1	0	0	0
1	1	0	1
0	1	0	0

We observe that if we sum two Hamming codes, it remains an Hamming code (that is the parity checks remain valid also for the result of the sum):

HAMMING CODES

The subset of codes in $\mathbb{F}_2^{15}$ constructed the same way are called **Hamming Codes**.

	0	0	1
0	0	0	1
1	0	1	1
0	1	0	0

+

	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

=

	0	0	1
1	0	0	0
1	1	0	1
0	1	0	0

We observe that if we sum two Hamming codes, it remains an Hamming code (that is the parity checks remain valid also for the result of the sum):
Thus, since we can choose the numbers inside the 11 blue cells arbitrarily they form a 11 dimensional linear subspace of $\mathbb{F}_2^{15}$. For this reason these codes are referred to as [15,11] Hamming Codes.

What are we actually doing when decoding a message?

- Note given a code in $\mathbb{F}_2^{15}$ by changing one bit we can always recover an Hamming Code. Thus what we are doing to correct a message is simply taking the closest valid message!

What are we actually doing when decoding a message?

- Note given a code in $\mathbb{F}_2^{15}$ by changing one bit we can always recover an Hamming Code. Thus what we are doing to correct a message is simply taking the closest valid message!
- We partition the message space into balls centered on the codewords. If we receive a message, then we simply look at what ball it is in and then the center of that ball is the most likely correct message (This is called nearest neighbour decoder (nnd)).

What are we actually doing when decoding a message?

- Note given a code in $\mathbb{F}_2^{15}$ by changing one bit we can always recover an Hamming Code. Thus what we are doing to correct a message is simply taking the closest valid message!
- We partition the message space into balls centered on the codewords. If we receive a message, then we simply look at what ball it is in and then the center of that ball is the most likely correct message (This is called nearest neighbour decoder (nnd)).
- To decode as many messages as possible, we take the largest radius such that the balls remain disjoint.

What are we actually doing when decoding a message?

- Note given a code in $\mathbb{F}_2^{15}$ by changing one bit we can always recover an Hamming Code. Thus what we are doing to correct a message is simply taking the closest valid message!
- We partition the message space into balls centered on the codewords. If we receive a message, then we simply look at what ball it is in and then the center of that ball is the most likely correct message (This is called nearest neighbour decoder (nnd)).
- To decode as many messages as possible, we take the largest radius such that the balls remain disjoint.
- This radius equals to $\lfloor \frac{d-1}{2} \rfloor$ where d is *the minimum distance* of the code (the set containing all the m codewords).

What are we actually doing when decoding a message?

- Note given a code in $\mathbb{F}_2^{15}$ by changing one bit we can always recover an Hamming Code. Thus what we are doing to correct a message is simply taking the closest valid message!
- We partition the message space into balls centered on the codewords. If we receive a message, then we simply look at what ball it is in and then the center of that ball is the most likely correct message (This is called nearest neighbour decoder (nnd)).
- To decode as many messages as possible, we take the largest radius such that the balls remain disjoint.
- This radius equals to $\lfloor \frac{d-1}{2} \rfloor$ where d is *the minimum distance* of the code (the set containing all the m codewords).
- The minimum distance d is a simple measure of the goodness of a code.

Classical Sphere Packing Results

- Given a message length n and a minimum distance d, we want to find the largest code with minimum distance d.
- This can also be seen as the sphere packing problem for spheres of radius $\lfloor \frac{d-1}{2} \rfloor$.

Theorem 1 (Hamming Bound)

Let $\mathcal{C} < \mathbb{F}_q^n$ be a code with $d_H(\mathcal{C}) = d$ then:

$$|\mathcal{C}| \leq \frac{q^n}{\sum_{i=o}^{t} \binom{n}{i} (q-1)^i}$$

Where $t := \lfloor \frac{d-1}{2} \rfloor$.

Theorem 2 (Singleton Bound)

Let $\mathcal{C} < \mathbb{F}_q^n$ be a code with $d_H(\mathcal{C}) = t$ then:

$$|\mathcal{C}| \leq q^{n-d+1}.$$

The codes satisfying the Hamming bound or the Singleton bound are called respectively **Perfect codes** and **MDS codes** (maximum distance separable codes).

Proof of Hamming bound

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code.

Proof of Hamming bound

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code. Let t be the maximum radius such that the union $\cup_{c \in \mathcal{C}} B_t(c)$ is disjoint.

Proof of Hamming bound

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code. Let t be the maximum radius such that the union $\cup_{c \in \mathcal{C}} B_t(c)$ is disjoint. It can be seen that $t = \lfloor \frac{d-1}{2} \rfloor$ (Similarly to the euclidean case).

Proof of Hamming bound

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code. Let t be the maximum radius such that the union $\cup_{c\in\mathcal{C}} B_t(c)$ is disjoint. It can be seen that $t = \lfloor \frac{d-1}{2} \rfloor$ (Similarly to the euclidean case).
Then $|\sqcup_{c\in\mathcal{C}} B_t(c)| \leq |\mathbb{F}_q^n| = q^n$ and

Proof of Hamming bound

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code. Let t be the maximum radius such that the union $\cup_{c\in\mathcal{C}} B_t(c)$ is disjoint. It can be seen that $t = \lfloor \frac{d-1}{2} \rfloor$ (Similarly to the euclidean case).
Then $|\sqcup_{c\in\mathcal{C}} B_t(c)| \leq |\mathbb{F}_q^n| = q^n$ and $|\cup_{c\in\mathcal{C}} B_t(c)| = |\mathcal{C}| b_t$. Where b_t is the size of the ball of radius t.

Proof of Hamming bound

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code. Let t be the maximum radius such that the union $\cup_{c \in \mathcal{C}} B_t(c)$ is disjoint. It can be seen that $t = \lfloor \frac{d-1}{2} \rfloor$ (Similarly to the euclidean case).
Then $| \sqcup_{c \in \mathcal{C}} B_t(c)| \leq |\mathbb{F}_q^n| = q^n$ and $| \cup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}| b_t$. Where b_t is the size of the ball of radius t.
Since $b_t = \sum_{i=1}^t s_i$ where s_i is the size of the sphere of radius i.

Proof of Hamming bound

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code. Let t be the maximum radius such that the union $\cup_{c \in \mathcal{C}} B_t(c)$ is disjoint. It can be seen that $t = \lfloor \frac{d-1}{2} \rfloor$ (Similarly to the euclidean case).
Then $| \sqcup_{c \in \mathcal{C}} B_t(c)| \leq |\mathbb{F}_q^n| = q^n$ and $| \cup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}| b_t$. Where b_t is the size of the ball of radius t.
Since $b_t = \sum_{i=1}^{t} s_i$ where s_i is the size of the sphere of radius i.
The latter equals the number of way we can choose exactly i non null coordinates in a vector of length n, thus $s_i = \binom{n}{i}(q-1)^i$.

Proof of Hamming bound

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code. Let t be the maximum radius such that the union $\cup_{c\in\mathcal{C}} B_t(c)$ is disjoint. It can be seen that $t = \lfloor \frac{d-1}{2} \rfloor$ (Similarly to the euclidean case).
Then $| \sqcup_{c\in\mathcal{C}} B_t(c)| \leq |\mathbb{F}_q^n| = q^n$ and $| \cup_{c\in\mathcal{C}} B_t(c)| = |\mathcal{C}| b_t$. Where b_t is the size of the ball of radius t.
Since $b_t = \sum_{i=1}^t s_i$ where s_i is the size of the sphere of radius i.
The latter equals the number of way we can choose exactly i non null coordinates in a vector of length n, thus $s_i = \binom{n}{i}(q-1)^i$.Thus $| \cup_{c\in\mathcal{C}} B_t(c)| = |\mathcal{C}| \sum_{i=1}^t \binom{n}{i}(q-1)^i \leq q^n$.

We observe how knowing the sphere size was a central part of the proof.

Proof of Hamming bound

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code. Let t be the maximum radius such that the union $\cup_{c \in \mathcal{C}} B_t(c)$ is disjoint. It can be seen that $t = \lfloor \frac{d-1}{2} \rfloor$ (Similarly to the euclidean case).
Then $| \sqcup_{c \in \mathcal{C}} B_t(c)| \leq |\mathbb{F}_q^n| = q^n$ and $| \cup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}| b_t$. Where b_t is the size of the ball of radius t.
Since $b_t = \sum_{i=1}^t s_i$ where s_i is the size of the sphere of radius i.
The latter equals the number of way we can choose exactly i non null coordinates in a vector of length n, thus $s_i = \binom{n}{i}(q-1)^i$.Thus $| \cup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}| \sum_{i=1}^t \binom{n}{i}(q-1)^i \leq q^n$.

We observe how knowing the sphere size was a central part of the proof.

Remark: 1) Codes are perfect if the balls of size t centered on the codewords completely fill up $\mathcal{V}$
2)The Hamming codes are Perfect codes, while the "send the same message multiple times"-codes are not perfect.

Other metrics

- The Hamming metric is suitable when errors occur bit-wise with equal probability. For different error scenarios, alternative metrics must be considered.

Other metrics

- The Hamming metric is suitable when errors occur bit-wise with equal probability. For different error scenarios, alternative metrics must be considered.
- For each metric it is important to try to get analogous results to 1 and 2 bounds.

Other metrics

- The Hamming metric is suitable when errors occur bit-wise with equal probability. For different error scenarios, alternative metrics must be considered.
- For each metric it is important to try to get analogous results to 1 and 2 bounds.
- In particular we are interested in the sphere sizes

Other metrics

- The Hamming metric is suitable when errors occur bit-wise with equal probability. For different error scenarios, alternative metrics must be considered.
- For each metric it is important to try to get analogous results to 1 and 2 bounds.
- In particular we are interested in the sphere sizes
- Generally each metric is studied individually.

Other metrics

- The Hamming metric is suitable when errors occur bit-wise with equal probability. For different error scenarios, alternative metrics must be considered.
- For each metric it is important to try to get analogous results to 1 and 2 bounds.
- In particular we are interested in the sphere sizes
- Generally each metric is studied individually.
- A different approach is to try to get analogous results on a family of metrics.

Other metrics

- The Hamming metric is suitable when errors occur bit-wise with equal probability. For different error scenarios, alternative metrics must be considered.
- For each metric it is important to try to get analogous results to 1 and 2 bounds.
- In particular we are interested in the sphere sizes
- Generally each metric is studied individually.
- A different approach is to try to get analogous results on a family of metrics.
- In this presentation we show our results on the family of projective metrics.

Let $\mathcal{F} = \{f_1, \ldots, f_N\} \subset V$ be a set of such that $\langle f_1, f_2, \ldots, f_N \rangle = V$.

Let $\mathcal{F} = \{f_1, \ldots, f_N\} \subset V$ be a set of such that $\langle f_1, f_2, \ldots, f_N \rangle = V$.

The **projective weight function** $\mathrm{wt}_{\mathcal{F}}(\cdot) : V \to \mathbb{N}_{\geq 0}$ corresponding to $\mathcal{F}$ is

$$\mathrm{wt}_{\mathcal{F}}(x) := \min\{t \in \mathbb{N}_{\geq 0} \mid x \text{ is in the linear span of } t \text{ projective points } \langle f_i \rangle \in \mathcal{F}\}$$

Let $\mathcal{F} = \{f_1, \ldots, f_N\} \subset V$ be a set of such that $\langle f_1, f_2, \ldots, f_N \rangle = V$.

The **projective weight function** $\mathrm{wt}_{\mathcal{F}}(\cdot) : V \to \mathbb{N}_{\geq 0}$ corresponding to $\mathcal{F}$ is

$$\mathrm{wt}_{\mathcal{F}}(x) := \min\{t \in \mathbb{N}_{\geq 0} \mid x \text{ is in the linear span of } t \text{ projective points } \langle f_i \rangle \in \mathcal{F}\}$$

Let $\mathcal{F} = \{f_1, \ldots, f_N\} \subset V$ be a set of such that $\langle f_1, f_2, \ldots, f_N \rangle = V$.

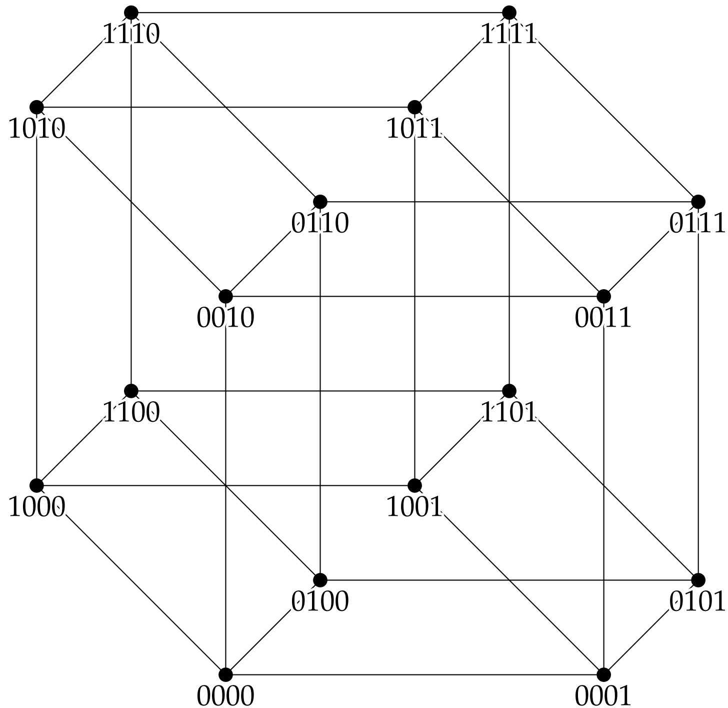
The **projective weight function** $\mathrm{wt}_{\mathcal{F}}(\cdot) : V \to \mathbb{N}_{\geq 0}$ corresponding to $\mathcal{F}$ is

$$\mathrm{wt}_{\mathcal{F}}(x) := \min\{t \in \mathbb{N}_{\geq 0} \mid x \text{ is in the linear span of } t \text{ projective points } \langle f_i \rangle \in \mathcal{F}\}$$

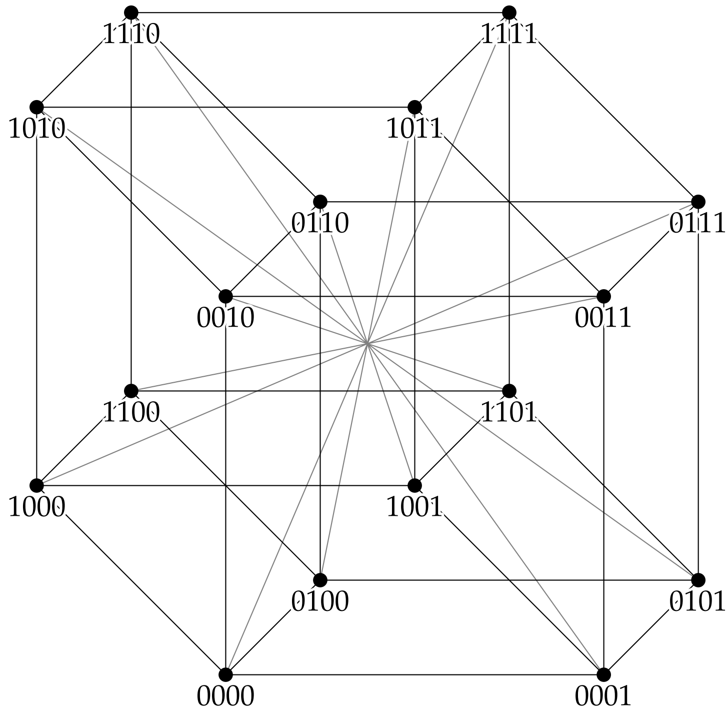
The **projective metric** $d_{\mathcal{F}}(\cdot, \cdot) : V \times V \to \mathbb{N}_{\geq 0}$ corresponding to $\mathcal{F}$ is

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

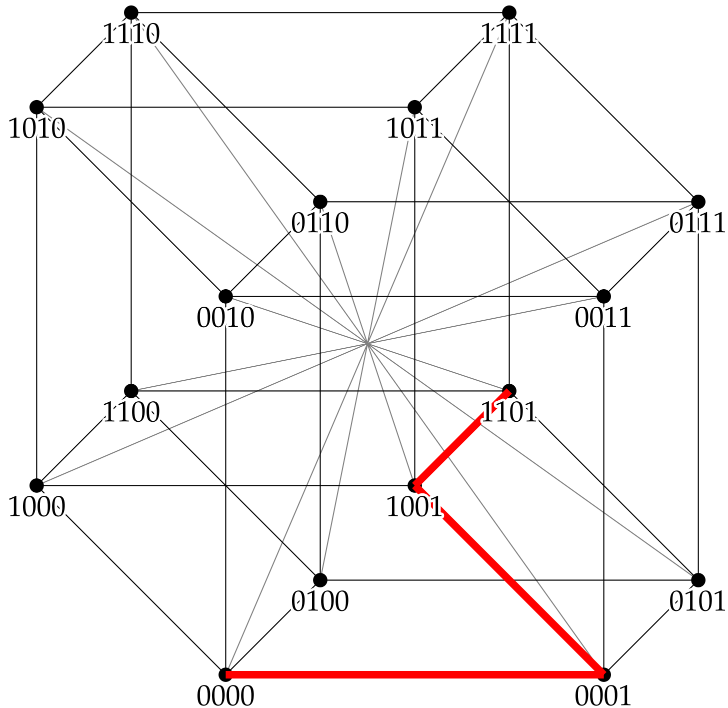
Vertices: vectors of $\mathbb{F}_2^4$



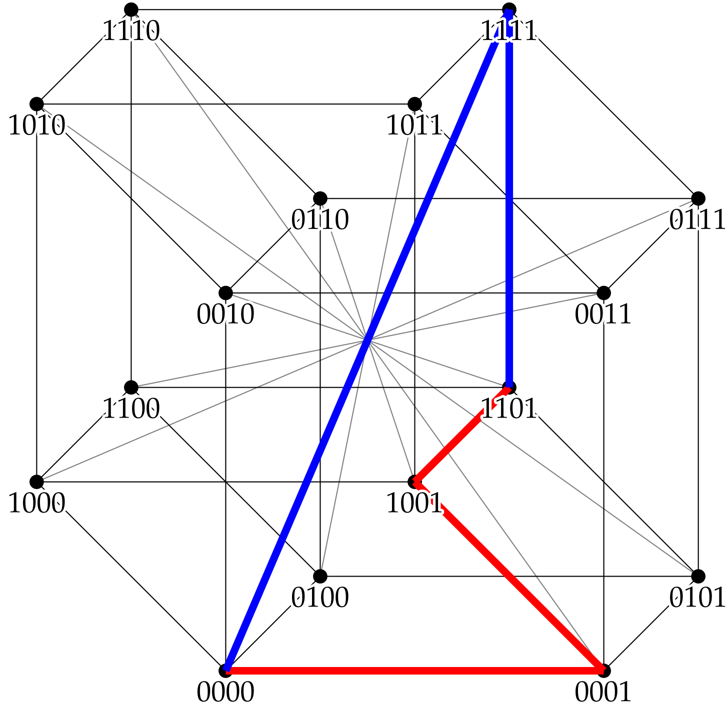
Distance from 0000 to 1101:



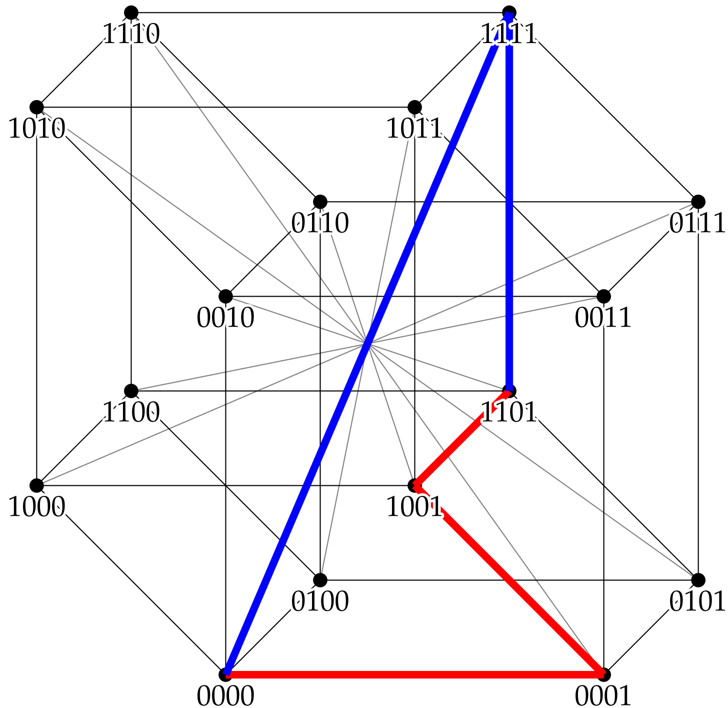
Distance from 0000 to 1101: red: 3,



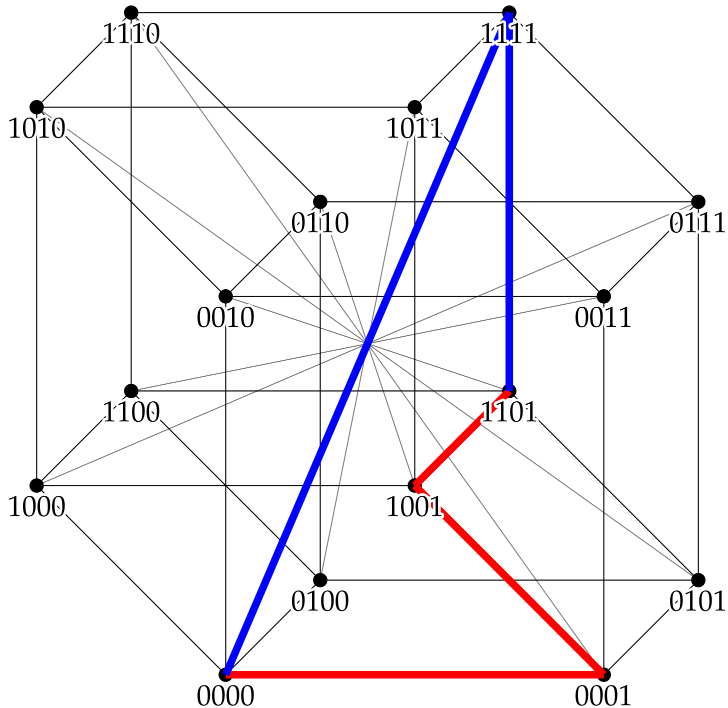
Distance from 0000 to 1101: red: 3, blue: 2



Graph distance on Clebsch graph $=$ **Phase-rotation metric/distance** on $\mathbb{F}_2^4$



Graph distance on Clebsch graph $=$ **Phase-rotation metric/distance** on $\mathbb{F}_2^4$
An edge is a Hamming error or the all-bits-flip error



Hamming metric

$$\begin{pmatrix} 0 & \colorbox{pink}{1} & 0 & 0 & \colorbox{pink}{1} & 0 & \colorbox{pink}{1} \end{pmatrix}$$

Hamming metric

$$\begin{pmatrix} 0 & \colorbox{pink}{1} & 0 & 0 & \colorbox{pink}{1} & 0 & \colorbox{pink}{1} \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of standard basis vectors}\}$$

Hamming metric

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \rightarrow \; \mathcal{F} = \{\text{spans of standard basis vectors}\}$$

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Hamming metric

$$\begin{pmatrix} 0 & \colorbox{pink}{1} & 0 & 0 & \colorbox{pink}{1} & 0 & \colorbox{pink}{1} \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of standard basis vectors}\}$$

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of rank 1 matrices}\}$$

Hamming metric

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \rightarrow \ \mathcal{F} = \{\text{spans of standard basis vectors}\}$$

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \rightarrow \ \mathcal{F} = \{\text{spans of rank 1 matrices}\}$$

Sum-Rank metric

$$\left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right)$$

Hamming metric

$$\begin{pmatrix} 0 & \boxed{1} & 0 & 0 & \boxed{1} & 0 & \boxed{1} \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of standard basis vectors}\}$$

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of rank 1 matrices}\}$$

Sum-Rank metric

$$\left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right) \quad \to \mathcal{F} = \left\{\text{spans of } \left(\text{ some 0 blocks} \;\middle|\; \text{rank 1 matrix} \;\middle|\; \text{some 0 blocks } \right)\right\}$$

Hamming metric

$$\begin{pmatrix} 0 & \colorbox{pink}{1} & 0 & 0 & \colorbox{pink}{1} & 0 & \colorbox{pink}{1} \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of standard basis vectors}\}$$

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of rank 1 matrices}\}$$

Sum-Rank metric

$$\left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right) \quad \to \mathcal{F} = \{\text{spans of } (\text{ some 0 blocks} \mid \text{rank 1 matrix} \mid \text{some 0 blocks })\}$$

Cover metric (rows and columns)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Hamming metric

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \rightarrow \ \mathcal{F} = \{\text{spans of standard basis vectors}\}$$

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \rightarrow \ \mathcal{F} = \{\text{spans of rank 1 matrices}\}$$

Sum-Rank metric

$$\left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right) \quad \rightarrow \ \mathcal{F} = \Big\{\text{spans of } \Big(\text{ some 0 blocks } \Big| \text{ rank 1 matrix } \Big| \text{ some 0 blocks } \Big)\Big\}$$

Cover metric (rows and columns)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \rightarrow \ \mathcal{F} = \{\text{spans of matrices with 1 non-zero row or 1 non-zero column}\}$$

Hamming metric

$$\begin{pmatrix} 0 & \colorbox{pink}{1} & 0 & 0 & \colorbox{pink}{1} & 0 & \colorbox{pink}{1} \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of standard basis vectors}\}$$

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of rank 1 matrices}\}$$

Sum-Rank metric

$$\left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right) \quad \to \mathcal{F} = \left\{\text{spans of } \left(\text{ some 0 blocks } \middle| \text{ rank 1 matrix } \middle| \text{ some 0 blocks } \right)\right\}$$

Cover metric (rows and columns)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of matrices with 1 non-zero row or 1 non-zero column}\}$$

Phase-rotation metric

$$\begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & \colorbox{pink}{1} & 0 \end{pmatrix}$$

Hamming metric

$$\begin{pmatrix} 0 & \boxed{1} & 0 & 0 & \boxed{1} & 0 & \boxed{1} \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of standard basis vectors}\}$$

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of rank 1 matrices}\}$$

Sum-Rank metric

$$\left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right) \quad \to \mathcal{F} = \left\{\text{spans of } \left(\text{ some 0 blocks } \middle| \text{ rank 1 matrix } \middle| \text{ some 0 blocks } \right)\right\}$$

Cover metric (rows and columns)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of matrices with 1 non-zero row or 1 non-zero column}\}$$

Phase-rotation metric

$$\begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & \boxed{1} & 0 \end{pmatrix} \quad \to \mathcal{F} = \{\text{spans of standard basis vectors or all-1}\}$$

What can we do?

What can we do?

Singleton-type bound!

What can we do?

Singleton-type bound!

Let V be an n-dim vector space over $\mathbb{F}_q$. Let $\mathcal{F}$ be a spanning family for a projective metric.

What can we do?

Singleton-type bound!

Let V be an n-dim vector space over $\mathbb{F}_q$. Let $\mathcal{F}$ be a spanning family for a projective metric.

Definition

Let $t \in \{0, 1, 2, \ldots, n\}$. We define $\mu_{\mathcal{F}}(t)$ as the maximum cardinality of a subset $\mathcal{G} \subseteq \mathcal{F}$ satisfying

What can we do?

Singleton-type bound!

Let V be an n-dim vector space over $\mathbb{F}_q$. Let $\mathcal{F}$ be a spanning family for a projective metric.

Definition

Let $t \in \{0, 1, 2, \ldots, n\}$. We define $\mu_{\mathcal{F}}(t)$ as the maximum cardinality of a subset $\mathcal{G} \subseteq \mathcal{F}$ satisfying

1. All $f_i \in \mathcal{G}$ are linear independent from each other over $\mathbb{F}_q$;

What can we do?

Singleton-type bound!

Let V be an n-dim vector space over $\mathbb{F}_q$. Let $\mathcal{F}$ be a spanning family for a projective metric.

Definition

Let $t \in \{0, 1, 2, \ldots, n\}$. We define $\mu_{\mathcal{F}}(t)$ as the maximum cardinality of a subset $\mathcal{G} \subseteq \mathcal{F}$ satisfying

1. All $f_i \in \mathcal{G}$ are linear independent from each other over $\mathbb{F}_q$;
2. All $v \in \langle \mathcal{G} \rangle$ have $\mathrm{wt}_{\mathcal{F}}(v) \leq t$.

WHAT CAN WE DO?

Singleton-type bound!

Let V be an n-dim vector space over $\mathbb{F}_q$. Let $\mathcal{F}$ be a spanning family for a projective metric.

Definition

Let $t \in \{0, 1, 2, \ldots, n\}$. We define $\mu_{\mathcal{F}}(t)$ as the maximum cardinality of a subset $\mathcal{G} \subseteq \mathcal{F}$ satisfying

1. All $f_i \in \mathcal{G}$ are linear independent from each other over $\mathbb{F}_q$;
2. All $v \in \langle \mathcal{G} \rangle$ have $\mathrm{wt}_{\mathcal{F}}(v) \leq t$.

Theorem 3 (General Singleton-type bound)

Let $\mathcal{C} \subseteq V$ be a subset and let $d = \min\{d_{\mathcal{F}}(x, y) \mid x \neq y \in \mathcal{C})\}$. Then

$$|\mathcal{C}| \leq q^{n-\mu_{\mathcal{F}}(d-1)} \leq q^{n-d+1}$$

What can we do?

Singleton-type bound!

Let V be an n-dim vector space over $\mathbb{F}_q$. Let $\mathcal{F}$ be a spanning family for a projective metric.

Definition

Let $t \in \{0, 1, 2, \ldots, n\}$. We define $\mu_{\mathcal{F}}(t)$ as the maximum cardinality of a subset $\mathcal{G} \subseteq \mathcal{F}$ satisfying

1. All $f_i \in \mathcal{G}$ are linear independent from each other over $\mathbb{F}_q$;
2. All $v \in \langle \mathcal{G} \rangle$ have $\mathrm{wt}_{\mathcal{F}}(v) \leq t$.

Theorem 3 (General Singleton-type bound)

Let $\mathcal{C} \subseteq V$ be a subset and let $d = \min\{d_{\mathcal{F}}(x, y) \mid x \neq y \in \mathcal{C})\}$. Then

$$|\mathcal{C}| \leq q^{n-\mu_{\mathcal{F}}(d-1)} \leq q^{n-d+1}$$

Coincides with Singleton bounds for specific projective metrics!

Where two codes are equivalent if there exists a linear Hamming isometry sending one onto the other. The following result tells us that a projective metric is univocally determined by it's parent code.

Theorem 4

Let $\bar{P}r_{\mathbf{N}}(V)$ be the set containing the equivalence classes of projective metrics on V of size $\mathbf{N}$ and $\bar{G}r_{\mathbf{N}-N}(\mathbb{F}_q^{\mathbf{N}})$ be the set containing the equivalence classes of subspaces of $\mathbb{F}_q^{\mathbf{N}}$ of dimension $\mathbf{N}-N$. Then there exists a bijection:

$$\Psi : \bar{P}r_{\mathbf{N}}(V) \to \bar{G}r_{\mathbf{N}-N}(\mathbb{F}_q^{\mathbf{N}})$$
$$\bar{w}_{\mathcal{F}} \mapsto \bar{\mathcal{C}}_{\mathcal{F}}$$

Where $\bar{\mathcal{C}}_{\mathcal{F}}$ is the parent code of $\mathcal{F}$.

Characterization of projective isometries

What can we do?

Definition 0.1

An $\mathbb{F}$-isometry is a linear isomorphism $L : V \to V$ such that $L(\mathcal{F}) = \mathcal{F}$. The set of $\mathbb{F}$-isometries, with the operation of composition, forms a group denoted as $isom_{\mathbb{F}}(V)$.

Theorem 5

Let $stab_H(\mathcal{C})$ be the stabilizer of the parent code $\mathcal{C}$ respect to the Hamming isometries, then $isom_{\mathcal{F}}(V) \cong stab_H(\mathcal{C})$

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.

And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.

And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.

And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.

And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.
- **Projective geometry:**
  Flats spanned by points in $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the smallest rank of such a flat that contains v.
  And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.
- **Projective geometry:**
  Flats spanned by points in $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the smallest rank of such a flat that contains v.
  And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.
- **Projective geometry:**
  Flats spanned by points in $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the smallest rank of such a flat that contains v.
  And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.
- **Subspace arrangements:**
  A ball of size t in projective metric corresponds to the size of the **subspace arrangement** generated by subsets of $\mathcal{F}$ of size less than t.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.
- **Projective geometry:**
  Flats spanned by points in $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the smallest rank of such a flat that contains v.
  And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.
- **Subspace arrangements:**
  A ball of size t in projective metric corresponds to the size of the **subspace arrangement** generated by subsets of $\mathcal{F}$ of size less than t.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.
- **Projective geometry:**
  Flats spanned by points in $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the smallest rank of such a flat that contains v.
  And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.
- **Subspace arrangments:**
  A ball of size t in projective metric corresponds to the size of the **subspace arrangement** generated by subsets of $\mathcal{F}$ of size less than t.
- **Matroid theory:**

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.
- **Projective geometry:**
  Flats spanned by points in $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the smallest rank of such a flat that contains v.
  And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.
- **Subspace arrangments:**
  A ball of size t in projective metric corresponds to the size of the **subspace arrangement** generated by subsets of $\mathcal{F}$ of size less than t.
- **Matroid theory:**
  We can see the Matroid Associated to the family $\mathcal{F}$. This seem do describe well the first two layers of the intersection lattice.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.
- **Projective geometry:**
  Flats spanned by points in $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the smallest rank of such a flat that contains v.
  And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.
- **Subspace arrangments:**
  A ball of size t in projective metric corresponds to the size of the **subspace arrangement** generated by subsets of $\mathcal{F}$ of size less than t.
- **Matroid theory:**
  We can see the Matroid Associated to the family $\mathcal{F}$. This seem do describe well the first two layers of the intersection lattice.
- **Q:** General ways to calculate $\mathrm{wt}_{\mathcal{F}}(v)$?

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.
- **Projective geometry:**
  Flats spanned by points in $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the smallest rank of such a flat that contains v.
  And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.
- **Subspace arrangments:**
  A ball of size t in projective metric corresponds to the size of the **subspace arrangement** generated by subsets of $\mathcal{F}$ of size less than t.
- **Matroid theory:**
  We can see the Matroid Associated to the family $\mathcal{F}$. This seem do describe well the first two layers of the intersection lattice.
- **Q:** General ways to calculate $\mathrm{wt}_{\mathcal{F}}(v)$?
  Q: For fixed t, how many v have $\mathrm{wt}_{\mathcal{F}}(v) = t$? $\rightarrow$ Hamming-like bound.

Equivalent notions of $\mathrm{wt}_{\mathcal{F}}(\cdot)$ in different contexts:

- **Graph theory:**
  Cayley graph of $\mathbb{F}_q^n$ with generating set $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- **Coding theory:**
  Certain code $\mathcal{C}$ (depends on $\mathcal{F}$); $\mathrm{wt}_{\mathcal{F}}(v)$ is the Hamming weight of the coset $v + \mathcal{C}$.
- **Projective geometry:**
  Flats spanned by points in $\mathcal{F}$; $\mathrm{wt}_{\mathcal{F}}(v)$ is the smallest rank of such a flat that contains v.
  And $\mathrm{wt}_{\mathcal{F}}$-isometries are simply homographies fixing $\mathcal{F}$.
- **Subspace arrangments:**
  A ball of size t in projective metric corresponds to the size of the **subspace arrangement** generated by subsets of $\mathcal{F}$ of size less than t.
- **Matroid theory:**
  We can see the Matroid Associated to the family $\mathcal{F}$. This seem do describe well the first two layers of the intersection lattice.
- **Q:** General ways to calculate $\mathrm{wt}_{\mathcal{F}}(v)$?
  Q: For fixed t, how many v have $\mathrm{wt}_{\mathcal{F}}(v) = t$? $\rightarrow$ Hamming-like bound.
- Please let me know if you know a (partial) answer in any of these contexts!

Current research

- Algorithms for calculating $\mathrm{wt}_{\mathcal{F}}(v)$ for $v \in V$
- Are there general methods for obtaining sphere sizes $|\{v \in V \mid \mathrm{wt}_{\mathcal{F}}(v) = t\}|$ for $t \in \mathbb{N}$?
- Is there a natural way do generilize other concepts of coding theory? Dual Codes? Perfect Codes? ecc...
- Approach?: using poset lattice of projective metrics, where $\mathrm{wt}_{\mathcal{F}} \preccurlyeq \mathrm{wt}_{\mathcal{G}}$ iff $\mathcal{F} \subseteq \mathcal{G}$