PROJECTIVE METRICS FOR CODING THEORY

Gabor Riccardi

University of Pavia (UniPv)

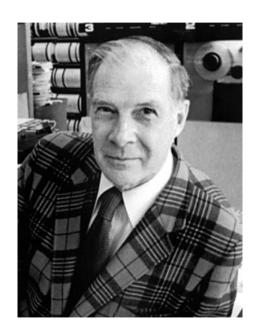
with **Hugo Sauerbier Couvée** , Technical University of Munich (TUM)

20 September 2023

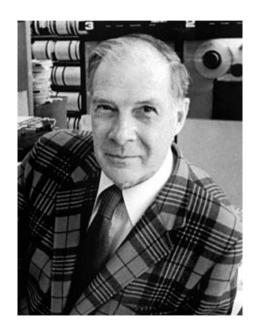
► In 1948 Shannon published "A Mathematical Theory of Communication".

- ► In 1948 Shannon published "A Mathematical Theory of Communication".
- ▶ In 1949 the Binary Goolay Codes where developed, capable of correcting up to 3 errors in a 24 bit string.

- ► In 1948 Shannon published "A Mathematical Theory of Communication".
- ▶ In 1949 the Binary Goolay Codes where developed, capable of correcting up to 3 errors in a 24 bit string.
- ► In 1959 Hamming develops the Hamming codes

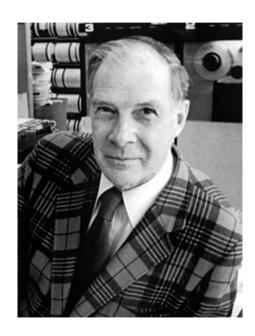


- ► In 1948 Shannon published "A Mathematical Theory of Communication".
- ▶ In 1949 the Binary Goolay Codes where developed, capable of correcting up to 3 errors in a 24 bit string.
- ► In 1959 Hamming develops the Hamming codes out of frustration:



- ► In 1948 Shannon published "A Mathematical Theory of Communication".
- ▶ In 1949 the Binary Goolay Codes where developed, capable of correcting up to 3 errors in a 24 bit string.
- ► In 1959 Hamming develops the Hamming codes out of frustration:

"Damn it, if the machine can detect an error, why can't it locate the position of the error and correct it?"



Redundancy!

Redundancy!

Redundancy!

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

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

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

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

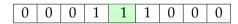
0	0	0	1	0	1	0	0	0
0	0	0	1	1	1	0	0	0
0	0	0	1	1	1	0	0	0

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

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

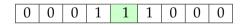
Since "1" appears twice and "0" once, we may assume more likely that the original message was:



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:

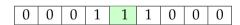


But this way, we took three times the length of the message to correct one error!

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:



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.

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

We rearrange the original message 0 0 0 1 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

We rearrange the original message 0 0 0 1 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

We rearrange the original message 0 0 0 1 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

	0 ,						
	0	0	0				
1	0	0	1				
0	1	1	0				
0	0	0	0				

We rearrange the original message 0 0 0 1 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

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

We rearrange the original message 0 0 0 1 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

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

We rearrange the original message 0 0 0 1 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

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

We rearrange the original message 0 0 0 1 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	

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.

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

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

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

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

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

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

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

4

	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

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):

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

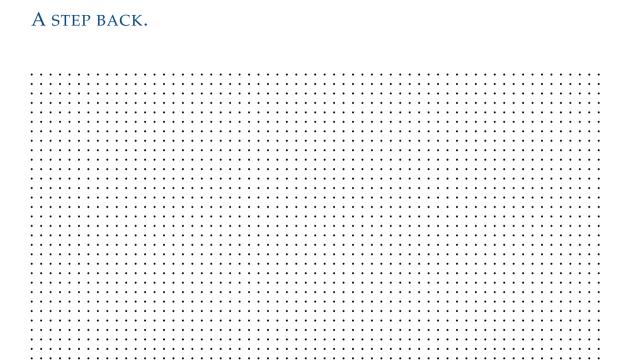


	0	0	0
1	0	0	1
0	1	1	0
0	0	0	0

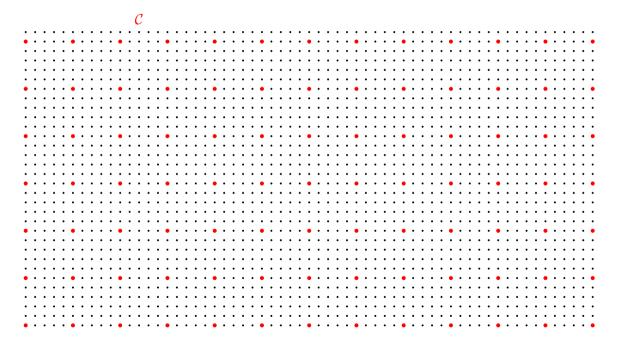
	0	0	1
1	0	0	0
1	1	0	1
0	1	0	0

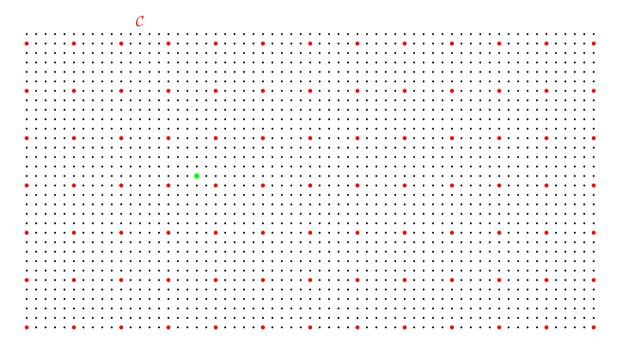
We observe that if we sum two Hamming codes, it remains an Hamming code (that is the parity checks remain valid also for the result of the sum):

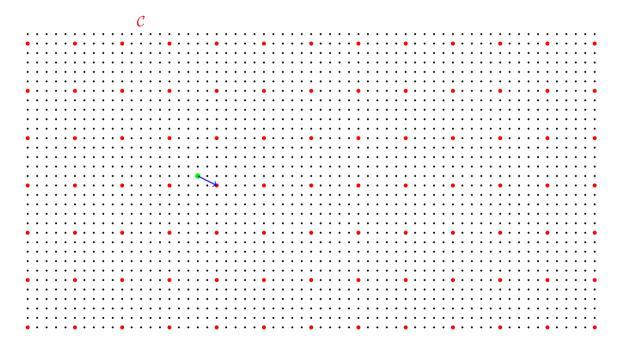
Thus, since we can choose the numbers inside the 11 blue cells arbitrarily they form a 11 dimensional linear subspace of \mathbb{F}_2^{15} . For this reason these codes are referred to as [15,11] Hamming Codes.

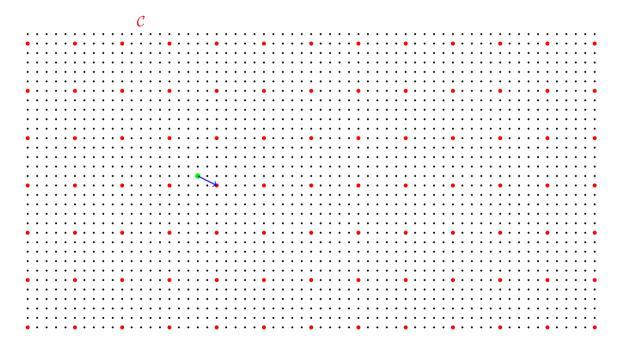


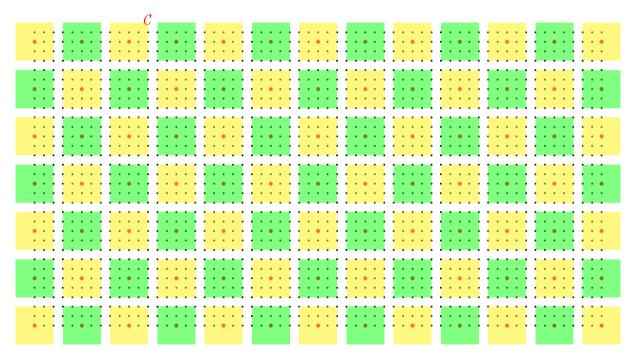
A STEP BACK.

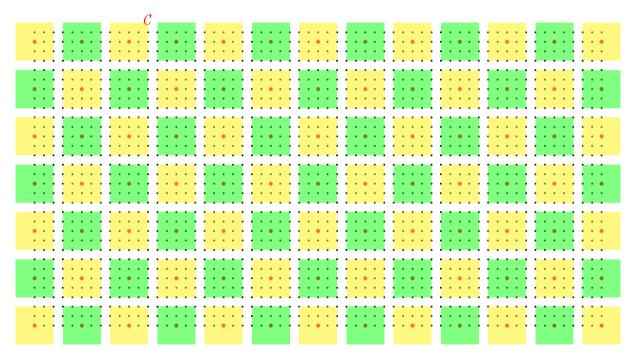


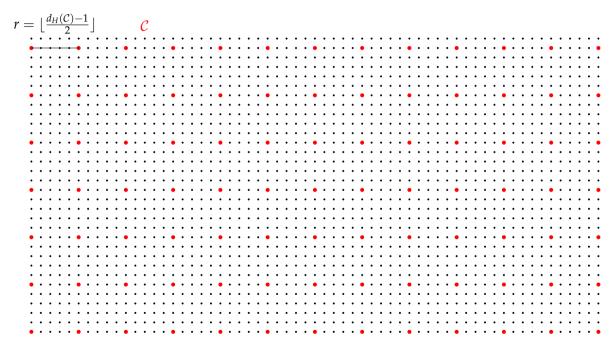


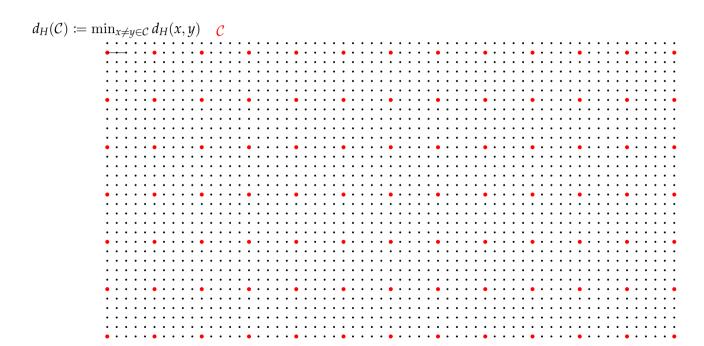




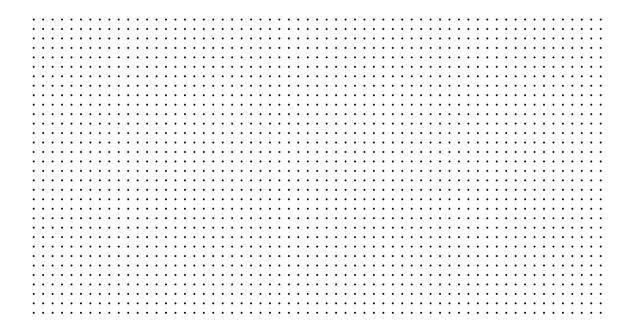




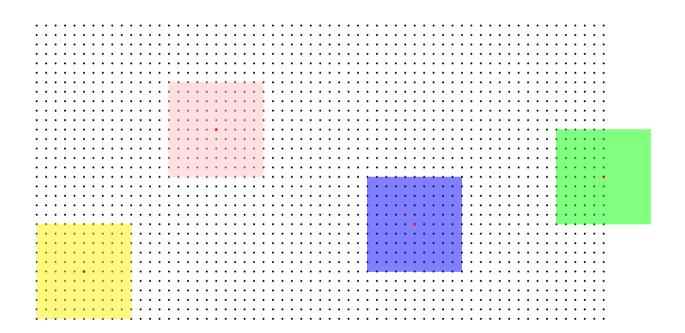




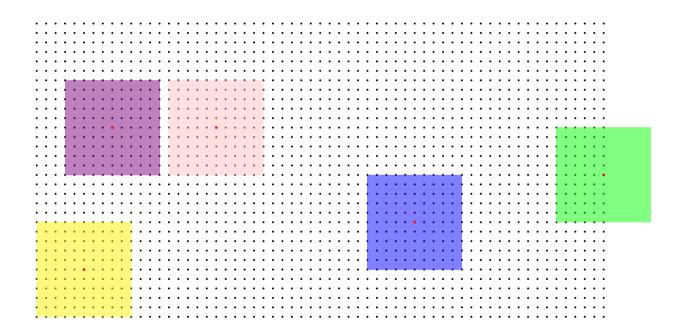
SPHERE PACKING



SPHERE PACKING



SPHERE PACKING



► Given a message length *N*,

▶ Given a message length *N*, and a minimum distance *d*,

ightharpoonup Given a message length N, and a minimum distance d, we want to find the largest code with minimum distance d.

▶ Given a message length *N*, and a minimum distance *d*, we want to find the largest code with minimum distance *d*.

Theorem 1 (Hamming Bound)

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

$$|\mathcal{C}| \le \frac{q^N}{\sum_{i=0}^t \binom{N}{i} (q-1)^i}$$

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

▶ Given a message length *N*, and a minimum distance *d*, we want to find the largest code with minimum distance *d*.

Theorem 1 (Hamming Bound)

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

$$|\mathcal{C}| \le \frac{q^N}{\sum_{i=0}^t \binom{N}{i} (q-1)^i}$$

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

Theorem 2 (Singleton Bound)

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

$$|\mathcal{C}| \le q^{N-d+1}.$$

:

► Given a message length *N*, and a minimum distance *d*, we want to find the largest code with minimum distance *d*.

Theorem 1 (Hamming Bound)

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

$$|\mathcal{C}| \le \frac{q^N}{\sum_{i=0}^t \binom{N}{i} (q-1)^i}$$

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

Theorem 2 (Singleton Bound)

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

$$|\mathcal{C}| \le q^{N-d+1}$$
.

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

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

Let $C \subset \mathbb{F}_q^N$ be a code. $t = \lfloor \frac{d-1}{2} \rfloor$ is the maximum radius such that the union $\cup_{c \in C} B_t(c)$ is disjoint.

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

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

Let $\mathcal{C} \subset \mathbb{F}_q^N$ be a code. $t = \lfloor \frac{d-1}{2} \rfloor$ is the maximum radius such that the union $\bigcup_{c \in \mathcal{C}} B_t(c)$ is disjoint. Then $|\bigcup_{c \in \mathcal{C}} B_t(c)| \leq |\mathbb{F}_q^N| = q^N$ and $|\bigcup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}|b_t$. Where b_t is the size of the ball of radius t. Since $b_t = \sum_{i=0}^t s_i$ where s_i is the size of the sphere of radius i.

Let $\mathcal{C} \subset \mathbb{F}_q^N$ be a code. $t = \lfloor \frac{d-1}{2} \rfloor$ is the maximum radius such that the union $\bigcup_{c \in \mathcal{C}} B_t(c)$ is disjoint.

Then $|\sqcup_{c\in\mathcal{C}} B_t(c)| \leq |\mathbb{F}_q^N| = q^N$ and $|\sqcup_{c\in\mathcal{C}} B_t(c)| = |\mathcal{C}|b_t$. Where b_t is the size of the ball of radius t.

Since $b_t = \sum_{i=0}^t s_i$ 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 $s_i = \binom{N}{i} (q-1)^i$.

Let $C \subset \mathbb{F}_q^N$ be a code. $t = \lfloor \frac{d-1}{2} \rfloor$ is the maximum radius such that the union $\bigcup_{c \in C} B_t(c)$ is disjoint. Then $|\bigcup_{c \in C} B_t(c)| \leq |\mathbb{F}_q^N| = q^N$ and $|\bigcup_{c \in C} B_t(c)| = |C|b_t$. Where b_t is the size of the ball of radius t. Since $b_t = \sum_{i=0}^t s_i$ 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 $|\sqcup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}| \sum_{i=0}^t \binom{N}{i}(q-1)^i \leq q^N$.

Let $\mathcal{C} \subset \mathbb{F}_q^N$ be a code. $t = \lfloor \frac{d-1}{2} \rfloor$ is the maximum radius such that the union $\bigcup_{c \in \mathcal{C}} B_t(c)$ is disjoint. Then $|\bigcup_{c \in \mathcal{C}} B_t(c)| \leq |\mathbb{F}_q^N| = q^N$ and $|\bigcup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}|b_t$. Where b_t is the size of the ball of radius t. Since $b_t = \sum_{i=0}^t s_i$ 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 $|\sqcup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}| \sum_{i=0}^t \binom{N}{i}(q-1)^i \leq q^N$.

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

Let $C \subset \mathbb{F}_q^N$ be a code. $t = \lfloor \frac{d-1}{2} \rfloor$ is the maximum radius such that the union $\bigcup_{c \in C} B_t(c)$ is disjoint. Then $|\bigcup_{c \in C} B_t(c)| \leq |\mathbb{F}_q^N| = q^N$ and $|\bigcup_{c \in C} B_t(c)| = |C|b_t$. Where b_t is the size of the ball of radius t. Since $b_t = \sum_{i=0}^t s_i$ 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 $|\sqcup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}| \sum_{i=0}^t \binom{N}{i}(q-1)^i \leq q^N$.

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 *V*

Let $C \subset \mathbb{F}_q^N$ be a code. $t = \lfloor \frac{d-1}{2} \rfloor$ is the maximum radius such that the union $\bigcup_{c \in C} B_t(c)$ is disjoint. Then $|\bigcup_{c \in C} B_t(c)| \leq |\mathbb{F}_q^N| = q^N$ and $|\bigcup_{c \in C} B_t(c)| = |C|b_t$. Where b_t is the size of the ball of radius t. Since $b_t = \sum_{i=0}^t s_i$ 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 $|\sqcup_{c \in \mathcal{C}} B_t(c)| = |\mathcal{C}| \sum_{i=0}^t \binom{N}{i}(q-1)^i \leq q^N$.

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 *V* 2)The Hamming codes are Perfect codes, while the "send the same message multiple times"-codes are not perfect.

Hamming metric

Hamming metric

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \to \ \mathrm{wt}_{\mathrm{Rank}} = 3$$

Hamming metric

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \rightarrow \operatorname{wt}_{\operatorname{Rank}} = 3$$

Cover metric (rows and columns)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \rightarrow \operatorname{wt}_{\operatorname{Cover}} = 3$$

Hamming metric

$$(0\ 1\ 0\ 0\ 1\ 0\ 1) \rightarrow wt_{Hamming} = 3$$

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \rightarrow \operatorname{wt}_{\operatorname{Rank}} = 3$$

Cover metric (rows and columns)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \rightarrow \operatorname{wt}_{\operatorname{Cover}} = 3$$

Phase-rotation metric

$$(1 \ 1 \ 0 \ 1) = (1 \ 1 \ 1 \ 1) + (0 \ 0 \ 1) \rightarrow wt_{Phase-Rot} = 1 + 1 = 2$$

Hamming metric

Rank metric

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \rightarrow \text{wt}_{\text{Rank}} = 3$$

Cover metric (rows and columns)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \rightarrow \text{wt}_{\text{Cover}} = 3$$

Phase-rotation metric

More: burst metric, tensor metric, combinatorical metrics, etc.

MOTIVATION

► Introduced by Gabidulin and Simonis (1997)

MOTIVATION

- ► Introduced by Gabidulin and Simonis (1997)
- ▶ A **generalization** of many metrics in coding theory

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

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

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

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

PROJECTIVE METRICS

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

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

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

PROJECTIVE METRICS

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

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

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

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

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

Rank metric

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

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \rightarrow \mathcal{F} = \mathcal{B}$$
 the canonical basis.

Rank metric

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

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \rightarrow \mathcal{F} = \mathcal{B}$$
 the canonical basis.

Rank metric

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

Cover metric (rows and columns)

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

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \rightarrow \mathcal{F} = \mathcal{B}$$
 the canonical basis.

Rank metric

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

Cover metric (rows and columns)

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

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \rightarrow \mathcal{F} = \mathcal{B}$$
 the canonical basis.

Rank metric

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

Cover metric (rows and columns)

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

Phase-rotation metric

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \rightarrow \mathcal{F} = \mathcal{B}$$
 the canonical basis.

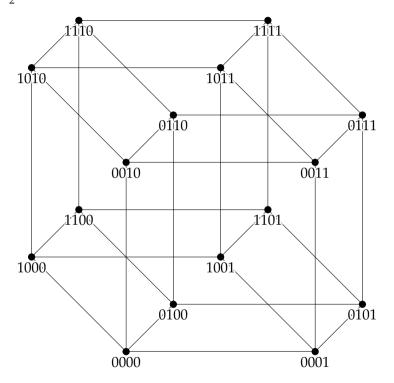
Rank metric

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

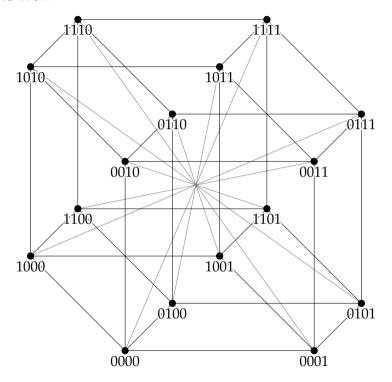
Cover metric (rows and columns)

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

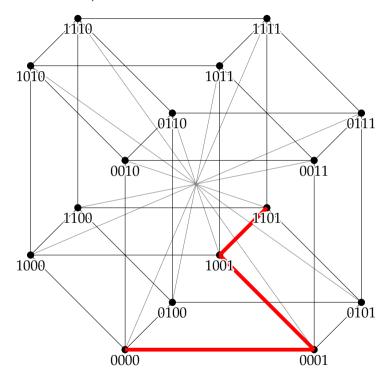
Phase-rotation metric

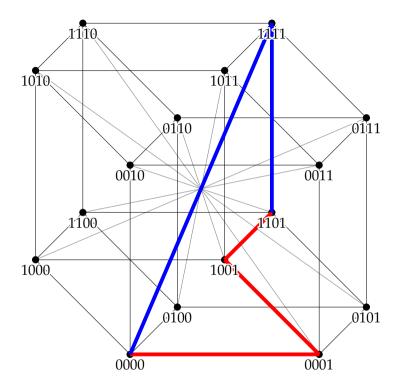


Distance from 0000 to 1101:



Distance from 0000 to 1101: red: 3,





Singleton-type bound!

Singleton-type bound!

Singleton-type bound!

Definition

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

Singleton-type bound!

Definition

Let $t \in \{0, 1, 2, ..., N\}$. 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;

Singleton-type bound!

Definition

Let $t \in \{0, 1, 2, ..., N\}$. 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;
- 2. All $v \in \langle \mathcal{G} \rangle$ have $\operatorname{wt}_{\mathcal{F}}(v) \leq t$.

Singleton-type bound!

Definition

Let $t \in \{0, 1, 2, ..., N\}$. 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;
- 2. All $v \in \langle \mathcal{G} \rangle$ have $\operatorname{wt}_{\mathcal{F}}(v) \leq t$.

Theorem 3 (General Singleton-type bound)

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

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

Singleton-type bound!

Definition

Let $t \in \{0, 1, 2, ..., N\}$. 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;
- 2. All $v \in \langle \mathcal{G} \rangle$ have $\operatorname{wt}_{\mathcal{F}}(v) \leq t$.

Theorem 3 (General Singleton-type bound)

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

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

Coincides with Singleton bounds for specific projective metrics!

Write $\mu := \mu_{\mathcal{F}}(d-1)$ and let $\mathcal{G} = \{g_1, \dots, g_{\mu}\} \subseteq \mathcal{F}$ be the linearly independent subset of size μ from the definition of $\mu_{\mathcal{F}}(t)$.

Write $\mu := \mu_{\mathcal{F}}(d-1)$ and let $\mathcal{G} = \{g_1, \dots, g_{\mu}\} \subseteq \mathcal{F}$ be the linearly independent subset of size μ from the definition of $\mu_{\mathcal{F}}(t)$. (thus $\operatorname{wt}_{\mathcal{F}}(\langle \mathcal{G} \rangle) \leq d-1$).

Write $\mu := \mu_{\mathcal{F}}(d-1)$ and let $\mathcal{G} = \{g_1, \dots, g_{\mu}\} \subseteq \mathcal{F}$ be the linearly independent subset of size μ from the definition of $\mu_{\mathcal{F}}(t)$. (thus $\operatorname{wt}_{\mathcal{F}}(\langle \mathcal{G} \rangle) \leq d-1$). We can extend \mathcal{G} to a basis \mathcal{B} for V:

$$\mathcal{B} = \{g_1, \dots, g_{\mu}, g_{\mu+1}, \dots, g_N\}$$

Write $\mu := \mu_{\mathcal{F}}(d-1)$ and let $\mathcal{G} = \{g_1, \dots, g_{\mu}\} \subseteq \mathcal{F}$ be the linearly independent subset of size μ from the definition of $\mu_{\mathcal{F}}(t)$. (thus $\operatorname{wt}_{\mathcal{F}}(\langle \mathcal{G} \rangle) \leq d-1$). We can extend \mathcal{G} to a basis \mathcal{B} for V:

$$\mathcal{B} = \{g_1, \dots, g_{\mu}, g_{\mu+1}, \dots, g_N\}$$

Consider the projection:

$$\operatorname{Proj}: \mathcal{C} \to \mathbb{F}_q^{N-\mu}$$

$$\sum_{i=1}^N c_i g_i \mapsto (c_{\mu+1}, \dots, c_N)$$

Write $\mu := \mu_{\mathcal{F}}(d-1)$ and let $\mathcal{G} = \{g_1, \dots, g_{\mu}\} \subseteq \mathcal{F}$ be the linearly independent subset of size μ from the definition of $\mu_{\mathcal{F}}(t)$. (thus $\operatorname{wt}_{\mathcal{F}}(\langle \mathcal{G} \rangle) \leq d-1$). We can extend \mathcal{G} to a basis \mathcal{B} for V:

$$\mathcal{B} = \{g_1, \dots, g_{\mu}, g_{\mu+1}, \dots, g_N\}$$

Consider the projection:

$$\operatorname{Proj}: \mathcal{C} \to \mathbb{F}_q^{N-\mu}$$

$$\sum_{i=1}^N c_i g_i \mapsto (c_{\mu+1}, \dots, c_N)$$

If Proj is injective, then $|\mathcal{C}| \leq q^{N-\mu(d-1)}$ which is the Singleton Bound.

Write $\mu := \mu_{\mathcal{F}}(d-1)$ and let $\mathcal{G} = \{g_1, \dots, g_{\mu}\} \subseteq \mathcal{F}$ be the linearly independent subset of size μ from the definition of $\mu_{\mathcal{F}}(t)$. (thus $\operatorname{wt}_{\mathcal{F}}(\langle \mathcal{G} \rangle) \leq d-1$). We can extend \mathcal{G} to a basis \mathcal{B} for V:

$$\mathcal{B} = \{g_1, \dots, g_{\mu}, g_{\mu+1}, \dots, g_N\}$$

Consider the projection:

$$\operatorname{Proj}: \mathcal{C} \to \mathbb{F}_q^{N-\mu}$$

$$\sum_{i=1}^N c_i g_i \mapsto (c_{\mu+1}, \dots, c_N)$$

If Proj is injective, then $|\mathcal{C}| \le q^{N-\mu(d-1)}$ which is the Singleton Bound. Let $a,b \in \mathcal{C}$ and suppose $\operatorname{Proj}(a) = \operatorname{Proj}(b)$.

16

Write $\mu := \mu_{\mathcal{F}}(d-1)$ and let $\mathcal{G} = \{g_1, \dots, g_{\mu}\} \subseteq \mathcal{F}$ be the linearly independent subset of size μ from the definition of $\mu_{\mathcal{F}}(t)$. (thus $\operatorname{wt}_{\mathcal{F}}(\langle \mathcal{G} \rangle) \leq d-1$). We can extend \mathcal{G} to a basis \mathcal{B} for V:

$$\mathcal{B} = \{g_1, \dots, g_{\mu}, g_{\mu+1}, \dots, g_N\}$$

Consider the projection:

$$\operatorname{Proj}: \mathcal{C} \to \mathbb{F}_q^{N-\mu}$$

$$\sum_{i=1}^N c_i g_i \mapsto (c_{\mu+1}, \dots, c_N)$$

If Proj is injective, then $|\mathcal{C}| \leq q^{N-\mu(d-1)}$ which is the Singleton Bound. Let $a, b \in \mathcal{C}$ and suppose $\operatorname{Proj}(a) = \operatorname{Proj}(b)$. Then $\operatorname{Proj}(a-b) = 0$, so $a - b \in \langle \mathcal{G} \rangle$.

Write $\mu := \mu_{\mathcal{F}}(d-1)$ and let $\mathcal{G} = \{g_1, \dots, g_{\mu}\} \subseteq \mathcal{F}$ be the linearly independent subset of size μ from the definition of $\mu_{\mathcal{F}}(t)$. (thus $\operatorname{wt}_{\mathcal{F}}(\langle \mathcal{G} \rangle) \leq d-1$). We can extend \mathcal{G} to a basis \mathcal{B} for V:

$$\mathcal{B} = \{g_1, \dots, g_{\mu}, g_{\mu+1}, \dots, g_N\}$$

Consider the projection:

$$\operatorname{Proj}: \mathcal{C} \to \mathbb{F}_q^{N-\mu}$$

$$\sum_{i=1}^N c_i g_i \mapsto (c_{\mu+1}, \dots, c_N)$$

If Proj is injective, then $|\mathcal{C}| \leq q^{N-\mu(d-1)}$ which is the Singleton Bound. Let $a,b \in \mathcal{C}$ and suppose $\operatorname{Proj}(a) = \operatorname{Proj}(b)$. Then $\operatorname{Proj}(a-b) = 0$, so $a-b \in \langle \mathcal{G} \rangle$. But this means that

$$d_{\mathcal{F}}(a,b) = \operatorname{wt}_{\mathcal{F}}(a-b) \le d-1 < d,$$

so a = b.

WHAT CAN WE DO?

Let
$$\mathcal{F} = \{f_1, \dots, f_{\mathbf{N}}\}$$
, consider:

WHAT CAN WE DO?

Let
$$\mathcal{F} = \{f_1, \dots, f_{\mathbf{N}}\}$$
, consider:

$$\varphi: \mathbb{F}_q^{\mathbf{N}} \to V \tag{1}$$
$$e_i \mapsto f_i \tag{2}$$

$$e_i \mapsto f_i$$
 (2)

WHAT CAN WE DO?

Let $\mathcal{F} = \{f_1, \dots, f_{\mathbf{N}}\}$, consider:

$$\varphi: \mathbb{F}_q^{\mathbf{N}} \to V \tag{1}$$
$$e_i \mapsto f_i \tag{2}$$

$$e_i \mapsto f_i$$
 (2)

 φ is called a **parent function** of $\mathrm{wt}_\mathcal{F}$ and

WHAT CAN WE DO?

Let $\mathcal{F} = \{f_1, \dots, f_{\mathbf{N}}\}$, consider:

$$\varphi: \mathbb{F}_q^{\mathbf{N}} \to V \tag{1}$$

$$e_i \mapsto f_i$$
 (2)

 φ is called a **parent function** of $\operatorname{wt}_{\mathcal{F}}$ and $\mathcal{P} := \operatorname{Ker}(\varphi)$ is a **parent code** of $\operatorname{wt}_{\mathcal{F}}$.

WHAT CAN WE DO?

Let $\mathcal{F} = \{f_1, \dots, f_{\mathbf{N}}\}$, consider:

$$\varphi: \mathbb{F}_q^{\mathbf{N}} \to V \tag{1}$$

$$e_i \mapsto f_i$$
 (2)

 φ is called a **parent function** of $\operatorname{wt}_{\mathcal{F}}$ and $\mathcal{P} := \operatorname{Ker}(\varphi)$ is a **parent code** of $\operatorname{wt}_{\mathcal{F}}$.

Theorem 4

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

Where $\bar{P}r_{\mathbf{N}}(V)$ is 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 $\mathbf{N}-N$.

A CONNECTION TO CLASSICAL CODING THEORY

Definition 0.1 (Perfect codes)

Given a distance function d on V and a code $C \subseteq V$, we say that C is **perfect** with respect to d if there exists a $t \in \mathbb{N}$ such that:

$$\bigsqcup_{c \in \mathcal{C}} B_t(c) = V \tag{3}$$

where $B_t(c) := \{x \in V : d(x,c) \le t\}$ are disjoint balls of radius t centered around codewords.

A CONNECTION TO CLASSICAL CODING THEORY

Definition 0.1 (Perfect codes)

Given a distance function d on V and a code $C \subseteq V$, we say that C is **perfect** with respect to d if there exists a $t \in \mathbb{N}$ such that:

$$\bigsqcup_{c \in \mathcal{C}} B_t(c) = V \tag{3}$$

where $B_t(c) := \{x \in V : d(x,c) \le t\}$ are disjoint balls of radius t centered around codewords.

Proposition 1

A linear code C < V is \mathcal{F} -perfect if and only if $\varphi^{-1}(C)$ is Hamming perfect.

A CONNECTION TO CLASSICAL CODING THEORY

Definition 0.1 (Perfect codes)

Given a distance function d on V and a code $C \subseteq V$, we say that C is **perfect** with respect to d if there exists a $t \in \mathbb{N}$ such that:

$$\bigsqcup_{c \in \mathcal{C}} B_t(c) = V \tag{3}$$

where $B_t(c) := \{x \in V : d(x,c) \le t\}$ are disjoint balls of radius t centered around codewords.

Proposition 1

A linear code C < V is \mathcal{F} -perfect if and only if $\varphi^{-1}(C)$ is Hamming perfect.

Remark 1: There is a complete characterization for Hamming perfect codes which could be leveraged for projective metrics.

A CONNECTION TO CLASSICAL CODING THEORY

Definition 0.1 (Perfect codes)

Given a distance function d on V and a code $C \subseteq V$, we say that C is **perfect** with respect to d if there exists a $t \in \mathbb{N}$ such that:

$$\bigsqcup_{c \in \mathcal{C}} B_t(c) = V \tag{3}$$

where $B_t(c) := \{x \in V : d(x,c) \le t\}$ are disjoint balls of radius t centered around codewords.

Proposition 1

A linear code C < V is \mathcal{F} -perfect if and only if $\varphi^{-1}(C)$ is Hamming perfect.

Remark 1: There is a complete characterization for Hamming perfect codes which could be leveraged for projective metrics.

Which is kind of fun, because you are using one specific metric to get results on a class of metrics, containing the metric itself.

CHARACTERIZATION OF PROJECTIVE ISOMETRIES

WHAT CAN WE DO?

Definition 0.2

An \mathcal{F} -isometry is a linear isomorphism $L: V \to V$ such that $d_{\mathcal{F}}(Lx, Ly) = d_{\mathcal{F}}(x, y)$ for all $x, y \in V$.

CHARACTERIZATION OF PROJECTIVE ISOMETRIES

WHAT CAN WE DO?

Definition 0.2

An \mathcal{F} -isometry is a linear isomorphism $L: V \to V$ such that $d_{\mathcal{F}}(Lx, Ly) = d_{\mathcal{F}}(x, y)$ for all $x, y \in V$. The set of \mathcal{F} -isometries, with the operation of composition, forms a group denoted as $\mathrm{Isom}_{\mathcal{F}}(V)$.

CHARACTERIZATION OF PROJECTIVE ISOMETRIES

WHAT CAN WE DO?

Definition 0.2

An \mathcal{F} -isometry is a linear isomorphism $L: V \to V$ such that $d_{\mathcal{F}}(Lx, Ly) = d_{\mathcal{F}}(x, y)$ for all $x, y \in V$. The set of \mathcal{F} -isometries, with the operation of composition, forms a group denoted as $\mathrm{Isom}_{\mathcal{F}}(V)$.

Theorem 5

Let $stab_H(P)$ be the stabilizer of the parent code P respect to the Hamming isometries, then $isom_F(V) \cong stab_H(P)$

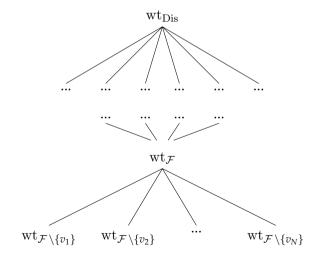
▶ Algorithms for calculating $\operatorname{wt}_{\mathcal{F}}(v)$ for $v \in V$

- ▶ Algorithms for calculating $\operatorname{wt}_{\mathcal{F}}(v)$ for $v \in V$
- ▶ Are there general methods for obtaining sphere sizes $|\{v \in V \mid \text{wt}_{\mathcal{F}}(v) = t\}|$ for $t \in \mathbb{N}$?

- ▶ Algorithms for calculating $\operatorname{wt}_{\mathcal{F}}(v)$ for $v \in V$
- ▶ Are there general methods for obtaining sphere sizes $|\{v \in V \mid \text{wt}_{\mathcal{F}}(v) = t\}|$ for $t \in \mathbb{N}$?
- ► Is there a natural way do generalize other concepts of coding theory? Dual Codes? MDS Codes? ...

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

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



(OF MATHEMATICS, NOT ALGEBRAIC FIELDS.)

► Graph Theory:

The Cayley graph of \mathbb{F}_q^N with generating set \mathcal{F} ;

(OF MATHEMATICS, NOT ALGEBRAIC FIELDS.)

► Graph Theory:

The Cayley graph of \mathbb{F}_a^N with generating set \mathcal{F} ; $\operatorname{wt}_{\mathcal{F}}(v)$ is the graph distance between v and v.

(OF MATHEMATICS, NOT ALGEBRAIC FIELDS.)

► Graph Theory:

The Cayley graph of \mathbb{F}_q^N with generating set \mathcal{F} ; $\operatorname{wt}_{\mathcal{F}}(v)$ is the graph distance between v and v.

► Classical Coding Theory:

The parent code \mathcal{P} of $\operatorname{wt}_{\mathcal{F}}$.

(OF MATHEMATICS, NOT ALGEBRAIC FIELDS.)

- ► Graph Theory:
 - The Cayley graph of \mathbb{F}_q^N with generating set \mathcal{F} ; $\operatorname{wt}_{\mathcal{F}}(v)$ is the graph distance between v and v.
- ► Classical Coding Theory:
 - The parent code \mathcal{P} of $\operatorname{wt}_{\mathcal{F}}$.
- **▶** Projective Geometry:
 - The projective weights are constant on the projective classes of P(V). pause

(OF MATHEMATICS, NOT ALGEBRAIC FIELDS.)

- ► Graph Theory:
 - The Cayley graph of \mathbb{F}_q^N with generating set \mathcal{F} ; $\operatorname{wt}_{\mathcal{F}}(v)$ is the graph distance between v and 0.
- ► Classical Coding Theory:
 - The parent code \mathcal{P} of $wt_{\mathcal{F}}$.
- **▶** Projective Geometry:
 - The projective weights are constant on the projective classes of P(V). pause And $\operatorname{wt}_{\mathcal{F}}$ -isometries are simply homographies fixing \mathcal{F} .

(OF MATHEMATICS, NOT ALGEBRAIC FIELDS.)

► Graph Theory:

The Cayley graph of \mathbb{F}_q^N with generating set \mathcal{F} ; $\operatorname{wt}_{\mathcal{F}}(v)$ is the graph distance between v and v.

► Classical Coding Theory:

The parent code \mathcal{P} of $wt_{\mathcal{F}}$.

▶ Projective Geometry:

The projective weights are constant on the projective classes of P(V). pause And $\operatorname{wt}_{\mathcal{F}}$ -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.

(OF MATHEMATICS, NOT ALGEBRAIC FIELDS.)

► Graph Theory:

The Cayley graph of \mathbb{F}_q^N with generating set \mathcal{F} ; $\operatorname{wt}_{\mathcal{F}}(v)$ is the graph distance between v and v.

► Classical Coding Theory:

The parent code \mathcal{P} of $wt_{\mathcal{F}}$.

► Projective Geometry:

The projective weights are constant on the projective classes of P(V). pause And 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.

► Matroid Theory:

We can observe the matroid associated with the family \mathcal{F} .

(OF MATHEMATICS, NOT ALGEBRAIC FIELDS.)

► Graph Theory:

The Cayley graph of \mathbb{F}_q^N with generating set \mathcal{F} ; $\operatorname{wt}_{\mathcal{F}}(v)$ is the graph distance between v and v.

► Classical Coding Theory:

The parent code \mathcal{P} of $wt_{\mathcal{F}}$.

► Projective Geometry:

The projective weights are constant on the projective classes of P(V). pause And $\operatorname{wt}_{\mathcal{F}}$ -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.

► Matroid Theory:

We can observe the matroid associated with the family \mathcal{F} . This seems to describe well the first two layers of the intersection lattice.

Thank you for your attention.