

A BRIEF SURVEY OF METRICS IN CODING THEORY

Ernst Gabidulin

Abstract: *The main objects of Coding theory are metric vector or matrix spaces. Subsets of spaces are known as codes. The main problem is constructing codes of given pairwise distance and having maximal cardinality. Most known and most investigated spaces are Hamming spaces. Thousands papers and books are devoted to codes in the Hamming metric. We mention here only two books [1; 2] and will not consider this metric in details. Other metrics are investigated much less. In this paper, we give many examples of useful metrics. It is still non exhaustive review.*

Keywords: *metrics and norms, the uniform and non-uniform Hamming metrics, the Lee and Sharma-Kaushik metrics, the city block (Manhattan) metric, the Varshamov metric, the burst metric, the 2-dimensional burst metric, the term rank metric, the rank metric, combinatorial metrics, projective metrics, graph metrics, the subspace metric.*

ACM Classification Keywords: A.0 General Literature - Conference proceedings

MSC: 94B05, 94B20, 94B25

Introduction

Coding theory studies techniques to correct errors arising during communications through noisy channels. Its distinguishing features are using discrete signals and introducing the artificial redundancy. Discreteness allows to describe signals in terms of abstract symbols not connected with any physical realization. The artificial redundancy gives possibilities to correct errors using hard enough combinatorial constructions of signals. One can say that coding theory uses a wide spectrum of mathematical tools from simple binary arithmetic to modern algebraic geometry. The main objects of Coding theory are metric vector spaces. Subsets of spaces are known as codes. Main problem is constructing codes of given cardinality and having maximal pairwise distance as large as possible. Most known and most investigated spaces are Hamming spaces. The distance function between two vectors is defined as the number of non identical their coordinates. Thousands papers and books are devoted to the Hamming metrics. We mention here only two books [1; 2]. Other metrics are investigated much less.

In this paper, we describe connections between channels and metrics and give many examples of useful metrics. It is still non exhaustive review. Also it is important to mention that not all metrics allow the good mathematic theory.

General properties of codes

Let \mathcal{X} be an alphabet of q elements. Let \mathcal{X}^n be the space of all vectors over \mathcal{X} of dimension n .

A code $\mathcal{C} \subseteq \mathcal{X}^n$ of size $|\mathcal{C}| = M$ and length n is defined as any set of n -vectors over \mathcal{X}^n :

$$\mathcal{C} = \{\underline{\mathbf{x}}_1, \underline{\mathbf{x}}_2, \dots, \underline{\mathbf{x}}_M\}.$$

We assume also that the space of vectors \mathcal{X}^n is considered as a *metric* space. A metric can be defined either by a *distance function*, or by a *norm function*.

We shall consider only integer-valued distance functions and norms.

A distance $d(\underline{x}, \underline{y})$ between a n -vectors $\underline{x}, \underline{y}$ is a function satisfying conditions

$$\begin{aligned} d(\underline{x}, \underline{y}) &\geq 0, \forall \underline{x}, \underline{y}; && \text{(Non-negative).} \\ d(\underline{x}, \underline{y}) &= 0 \iff \underline{x} = \underline{y}; && \text{(Zero value).} \\ d(\underline{x}, \underline{y}) &= d(\underline{y}, \underline{x}); && \text{(Symmetry).} \\ d(\underline{x}, \underline{y}) &\leq d(\underline{x}, \underline{z}) + d(\underline{z}, \underline{y}), \forall \underline{x}, \underline{y}, \underline{z} && \text{(Triangle inequality).} \end{aligned}$$

A norm function $\mathcal{N}(\underline{x})$ should satisfy next axioms:

$$\begin{aligned} \mathcal{N}(\underline{x}) &\geq 0, \forall \underline{x}; && \text{(Non-negative).} \\ \mathcal{N}(\underline{x}) &= 0 \iff \underline{x} = 0; && \text{(Zero value).} \\ \mathcal{N}(\underline{x} + \underline{y}) &\leq \mathcal{N}(\underline{x}) + \mathcal{N}(\underline{y}), \forall \underline{x}, \underline{y} && \text{(Triangle inequality).} \end{aligned}$$

The norm function allows to construct the distance function as follows:

$$d(\underline{x}, \underline{y}) := \mathcal{N}(\underline{x} - \underline{y}).$$

Often distance and norm functions are defined coordinate-wise. A distance $d(x, y)$ between letters of the alphabet \mathcal{X} (respectively, $\mathcal{N}(x)$, $x \in \mathcal{X}$) is defined first. Assume that the distance takes all values $0, 1, \dots, D$, where D is the maximal possible value. Then the distance between n -vectors $\underline{x}, \underline{y} \in \mathcal{X}^n$ is defined as follows:

$$d(\underline{x}, \underline{y}) = \sum_{i=1}^n d(x_i, y_i).$$

This distance takes values $0, 1, \dots, nD$.

There exist still distance functions which are not coordinate-wise. For instance, the Varshamov distance and the rank distance (see, below) can not be represented in such a manner.

Similarly, for the coordinate-wise norm, we have

$$\mathcal{N}_n(\underline{x}) = \sum_{i=1}^n \mathcal{N}(x_i).$$

It is useful for applications to introduce the generator norm function

$$W(z) = \sum_{i=0}^D N(i)z^i,$$

where $N(i) = |\{x \in \mathcal{X} : \mathcal{N}(x) = i\}|$, $i = 0, 1, \dots, D$, is the number of elements \mathcal{X} with norm i . D means the maximal norm.

The generator norm function of the extended norm $\mathcal{N}_n(\cdot)$ is clearly

$$W_n(z) = \sum_{i=0}^{nD} N_n(i)z^i = W(z)^n = \left(\sum_{i=0}^D N(i)z^i \right)^n.$$

We shall consider metrics defined by a coordinate-wise norm $\mathcal{N}_n(\cdot)$. The main problem of coding theory is constructing codes $\mathcal{C}_n \subseteq \mathcal{X}^n$ of maximal cardinality M if minimal distance d is given. For a metric on \mathcal{X} we define the *average norm* \overline{N} and the *average pair-wise distance* \overline{D} by

$$\begin{aligned} \overline{N} &= \frac{\sum_{x \in \mathcal{X}} \mathcal{N}(x)}{q} = \frac{\sum_{i=0}^D iN(i)}{q}; \\ \overline{D} &= \frac{\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{X}} \mathcal{N}(x-y)}{q(q-1)} = \frac{\sum_{x \in \mathcal{X}} \overline{N}(x)}{q}, \end{aligned}$$

where $\overline{N}(x)$ denotes the average distance from $\mathcal{X} \setminus x$ to x .

If \mathcal{X} is an additive group, then $\overline{N}(x)$ does not depend on x . Moreover $\overline{N}(x) = \frac{q}{q-1} \overline{N}$. Hence in this case $\overline{D} = \frac{q}{q-1} \overline{N}$.

For the extended metric $\mathcal{N}_n(\underline{\mathbf{x}})$ we have $\overline{N}_n = \overline{N}n$, $\overline{D}_n = \frac{q^n}{q^n-1} \overline{N}_n$.

If \mathcal{C}_n is a code of cardinality M and of distance $d > \overline{N}_n$, then the Plotkin-style bound is valid:

$$M \leq \frac{d}{d - \overline{N}_n}.$$

Let

$$S_{d-1}(\underline{\mathbf{0}}) = \{\underline{\mathbf{y}} : \mathcal{N}_n(\underline{\mathbf{y}}) \leq d - 1\}$$

be the ball of radius $d - 1$ with the center at the all zero vector $\underline{\mathbf{0}}$. Then asymptotically, when $n \rightarrow \infty$ and $x = \frac{d-1}{Dn} < \overline{N}$, the volume of the ball is equal to

$$V_{d-1} = |S_{d-1}(\underline{\mathbf{0}})| \asymp cq^{n(1-R)},$$

where

$$1 - R = H(\alpha_0, \alpha_1, \dots, \alpha_D) + \sum_{i=1}^D \alpha_i \log_q N_i;$$

$$\alpha_i = \frac{N_i \gamma^i}{W(\gamma)}, \quad i = 0, 1, \dots, D;$$

$$\gamma \text{ is the positive root of } \frac{\gamma W'(\gamma)}{W(\gamma)} = xD,$$

$$H(\alpha_0, \alpha_1, \dots, \alpha_D) = - \sum_{i=0}^D \alpha_i \log_q \alpha_i.$$

It follows the upper Gilbert-style bound for a code with rate $R = \frac{\log_q M}{n}$ and distance $d - 1 = xDn$:

$$R = 1 - H(\alpha_0, \alpha_1, \dots, \alpha_D) - \sum_{i=1}^D \alpha_i \log_q N_i.$$

One can show that this equation can be reduced to the next simple form:

$$R = 1 - \log_q W(\gamma) + xD \log \gamma;$$

$$xD = \frac{\gamma W'(\gamma)}{W(\gamma)}.$$

Examples of metrics

Hamming metric

The most known is the Hamming metric.

The Hamming norm $w_H(\underline{\mathbf{x}})$ of a vector $\underline{\mathbf{x}}$ is defined as the number of its non zero coordinates.

The Hamming distance between $\underline{\mathbf{x}}$ and $\underline{\mathbf{y}}$ is the norm of its difference: $d(\underline{\mathbf{x}}, \underline{\mathbf{y}}) = w_H(\underline{\mathbf{x}} - \underline{\mathbf{y}})$.

The Hamming metric is matched strongly with all full symmetrical memoryless channels.

Full symmetrical channels are channels such that all non diagonal elements of the transfer probability matrix are identical.

Huge amount of papers are devoted to this metric.

Norms and metrics for \mathbb{Z}_q

Let the alphabets \mathcal{X} be the integer ring $\mathbb{Z}_q = \{0, 1, \dots, q-1\}$. Integer-valued norms and metrics can be defined in many ways.

It is clear that for any norm $\mathcal{N}(i) = \mathcal{N}(q-i)$, $i \in \mathbb{Z}_q$.

All elements of \mathbb{Z}_q can be divided into subsets of equal weight elements $B_j = \{a : a \in \mathbb{Z}_q, \mathcal{N}(a) = j\}$, $j = 0, 1, \dots, D$, where $D \leq \lfloor \frac{q}{2} \rfloor$ is the maximal norm. If $a \in B_j$, then also $q-a \in B_j$.

The maximal norm D can take values between 1 and $\lfloor \frac{q}{2} \rfloor$.

Open problem: find all possible values of D for \mathbb{Z}_q .

Open problem: describe all non-equivalent norms for \mathbb{Z}_q .

Two extreme cases are the **Hamming** metric ($D = 1$) and the **Lee** metric ($D = \lfloor \frac{q}{2} \rfloor$).

The Hamming metric is defined by

$$\mathcal{N}(i) = \begin{cases} 0, & \text{if } i = 0; \\ 1, & \text{if } i = 1, \dots, q-1; \end{cases}$$

so $D = 1$. The subsets of equal weight elements are

$$B_0 = \{0\}, B_1 = \{1, 2, \dots, q-1\}.$$

The Lee metric is defined by

$$\mathcal{N}(i) = \begin{cases} 0, & \text{if } i = 0; \\ i, & \text{if } 1 \leq i \leq \lfloor \frac{q}{2} \rfloor; \\ \mathcal{N}(q-i), & \text{if } \lfloor \frac{q}{2} \rfloor < i \leq q-1; \end{cases}$$

so $D = \lfloor \frac{q}{2} \rfloor$. The subsets of equal weight elements are

$$B_0 = \{0\}, B_1 = \{1, q-1\}, B_2 = \{2, q-2\}, \dots, B_{\lfloor \frac{q}{2} \rfloor} = \left\{ \left\lfloor \frac{q}{2} \right\rfloor, q - \left\lfloor \frac{q}{2} \right\rfloor \right\}.$$

Main results for codes with the Lee metric were obtained by Berlekamp [7]:

- The weight generator function

$$W(z) = \begin{cases} 1 + 2z + 2z^2 + \dots + 2z^{\frac{q-1}{2}}, & \text{if } q \text{ odd;} \\ 1 + 2z + 2z^2 + \dots + 2z^{\frac{q-2}{2}} + z^{\frac{q}{2}}, & \text{if } q \text{ even.} \end{cases}$$

- The average vector weight

$$\bar{N}_n = \begin{cases} n \frac{q^2-1}{4q}, & \text{if } q \text{ odd;} \\ n \frac{q}{4}, & \text{if } q \text{ even.} \end{cases}$$

- The Plotkin-style bound for cardinality M of a code with Lee distance d :

$$M \leq \frac{d}{d - \bar{N}_n}, \text{ if } d > \bar{N}_n.$$

- The asymptotic Gilbert-style bound: a code with cardinality M and Lee distance d exists, if

$$R = \frac{\log_q M}{n} = 1 - \log_q W(\gamma) + xD \log \gamma;$$

$$xD = \frac{\gamma W'(\gamma)}{W(\gamma)},$$

where $D = \lfloor \frac{q}{2} \rfloor$ and $xD = \frac{d-1}{n}$.

All non-equivalent norms for \mathbb{Z}_4

1. The Hamming metrics with the subsets of equal weight elements $B_0 = \{0\}$, $B_1 = \{1, 2, 3\}$, and with the distance matrix

$$\mathbf{D} = \begin{bmatrix} x \backslash y & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 & 1 \\ 3 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

2. The Lee metrics with the subsets of equal weight elements $B_0 = \{0\}$, $B_1 = \{1, 3\}$, $B_2 = \{2\}$, and with the distance matrix

$$\mathbf{D} = \begin{bmatrix} x \backslash y & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 3 & 1 & 2 & 1 & 0 \end{bmatrix}.$$

3. A new non-Lee metrics (never investigated) with the subsets of equal weight elements $B_0 = \{0\}$, $B_1 = \{2\}$, $B_2 = \{1, 3\}$, and with the distance matrix

$$\mathbf{D} = \begin{bmatrix} x \backslash y & 0 & 1 & 2 & 3 \\ 0 & 0 & 2 & 1 & 2 \\ 1 & 2 & 0 & 2 & 1 \\ 2 & 1 & 2 & 0 & 2 \\ 3 & 2 & 1 & 2 & 0 \end{bmatrix}.$$

Sharma-Kaushik metrics for \mathbb{Z}_q

Many norms for \mathbb{Z}_q were proposed by Sharma and Kaushik [3; 4; 5; 6].

The Sharma-Kaushik norm \mathcal{N}_{SK} is defined in terms of disjoint sets $B_0 \cup B_1 \cup \dots \cup B_{m-1}$ with conditions:

1. $B_0 = \{0\}$.
2. If $x \in B_i$, then $q - x \in B_i$.
3. If $x \in B_i, y \in B_j$ and $i < j$, then the Lee norm $\mathcal{N}_{Lee}(x) < \mathcal{N}_{Lee}(y)$.
4. $|B_0| \leq |B_1| \leq \dots \leq |B_{m-2}|$, but $|B_{m-1}| \geq |B_{m-2}|/2$.
5. $\mathcal{N}_{SK}(x) = s \iff x \in B_s$.
6. $d_{SK}(\underline{x}, \underline{y}) = \sum_{i=1}^n \mathcal{N}_{SK}(x_i - y_i)$

Example: Sharma-Kaushik metrics for \mathbb{Z}_9 .

Let

$$1. B_0 = \{0\}, B_1 = \{1, 8\}, B_2 = \{2, 3, 6, 7\}, B_3 = \{4, 5\}.$$

This is a Sharma-Kaushik metric.

Let

$$2. B_0 = \{0\}, B_1 = \{4, 5\}, B_2 = \{2, 3, 6, 7\}, B_3 = \{1, 8\}.$$

This is not a metric because Triangle inequality axiom is not satisfied: $\mathcal{N}(4+4) = \mathcal{N}(8) = 3 > \mathcal{N}(4) + \mathcal{N}(4) = 2$.

City block metric

The city block metric is known also as the Manhattan metric, or, the modular metric.

Let $\underline{x} = (x_1, x_2, \dots, x_n)$ and $\underline{y} = (y_1, y_2, \dots, y_n)$ be integer-valued vectors, $x_i, y_i \in \{0, 1, \dots, q-1\}$, $i = 1, 2, \dots, n$. Then the distance function is defined by

$$d_M(\underline{x}, \underline{y}) = \sum_{i=1}^n |x_i - y_i|.$$

This metrics is popular in psychology and related areas but not well known in communications. The possible reason is that *there exist no channels* matched MLD with city block metrics, *there exist no channels* matched MDD with city block metrics. Still channels exist matched ECD with city block metrics. Such channels appear when a signal limiter is used at the receiver. Error correcting was investigated first by [8] (without any metrics). Few results and code constructions are known. We present several new results.

- The weight generator function

$$W(z) = 1 + z + z^2 + \dots + z^{q-1}.$$

- The average vector weight

$$\overline{N} = \frac{q-1}{2}; \quad \overline{N}_n = n \frac{q-1}{2}.$$

- The average pair-wise distance

$$\overline{D} = \frac{q+1}{3}; \quad \overline{D}_n = n \frac{q+1}{3} \frac{q^n - q^{n-1}}{q^n - 1}.$$

- The Plotkin-style bound for cardinality M of a code with city block distance d :

$$M \leq \frac{d}{d - \overline{N}_n}, \text{ if } d > \overline{N}_n.$$

- The asymptotic Gilbert-style bound is unknown for city block metrics because balls of radius t have different cardinalities for different centers. For example, if $q = 3$, $n = 3$, $t = 3$, then the ball with the center $(0, 0, 0)$ has cardinality 17, while the ball with the center $(1, 1, 1)$ has cardinality 27, i.e., contains all elements!

For integer s , define the s -ary entropy by

$$H_s(x) = x \log_s(s-1) - x \log_s x - (1-x) \log_s(1-x).$$

We explain by examples how to derive the alternative bound. Let $q = 3$. We want to get the rate as a function of the normalized minimal city distance $x = \frac{d}{n(q-1)} = \frac{d}{2n}$. Note that any ternary code in the Hamming metric with minimal distance d_H is a code with the same distance in city block metric. We have the Gilbert bound for these codes in the form

$$R_1 = 1 - H_3\left(\frac{d_H}{n}\right),$$

or, in terms of city block distance

$$R_{1CB} = 1 - H_3(2x),$$

Hence we have the non-zero rate for small distances $2x \leq 2/3$. It goes to the 1, when x runs to 0. Consider now *binary* codes in the Hamming metrics with distance d_H . If we replace each "1" in code words

by $q - 1 = 2$, we obtain a code in city block metrics with minimal distance $d = (q - 1)d_H = 2d_H$. We have the Gilbert bound for these codes in the form

$$R_2 = 1 - H_2\left(\frac{d_H}{n}\right),$$

or, in terms of city block distance

$$R_{2CB} = (1 - H_2(x)) \log_3 2.$$

It gives the non-zero exponent for all allowable distances but for small distances the rate is less than 1. We get, combine both bounds, that a code with cardinality $M = q^{nR_{CB}}$ and with city block distance $d = x(q - 1)n$ exists, if

$$R_{CB}^{(3)} = \max\{R_{1CB}, R_{2CB}\} = \max\{1 - H_3(2x), (1 - H_2(x)) \log_3 2\},$$

for $0 \leq x \leq \frac{1}{2}$. We can obtain in a similar manner for $q = 5$ that

$$R_{CB}^{(5)} = \max\{R_{1CB}^{(5)}, R_{2CB}^{(5)}, R_{3CB}^{(5)}\},$$

where

$$R_{1CB}^{(5)} = 1 - H_5(5x);$$

$$R_{2CB}^{(5)} = (1 - H_3(2x)) \log_5 3;$$

$$R_{3CB}^{(5)} = (1 - H_2(x)) \log_5 2.$$

Rates as functions of the normalized city block distance are shown on Fig.1.

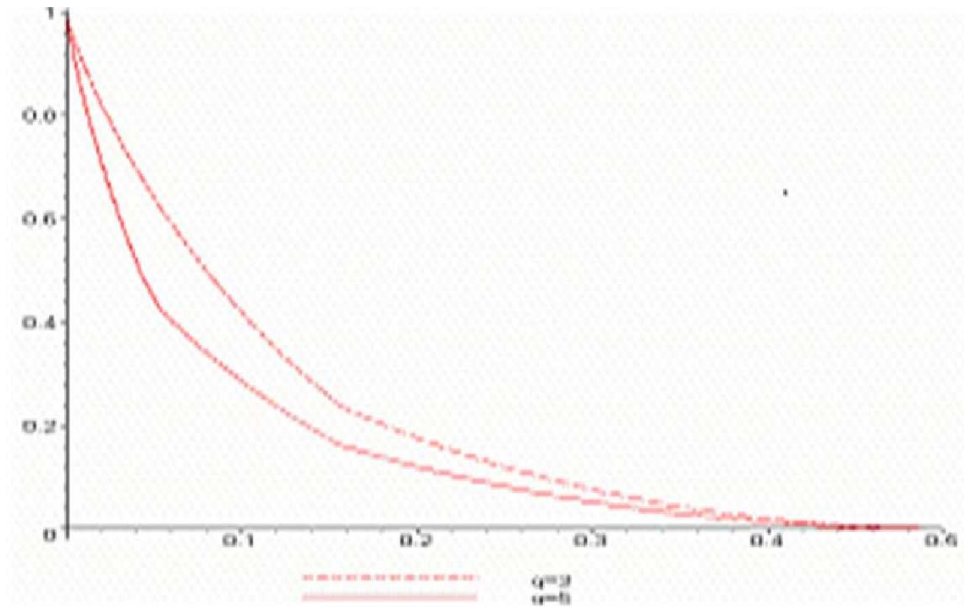


Figure 1: Bounds for City block metrics, $q=3$ (dash), $q=5$ (solid)

The Varshamov metric was introduced to describe asymmetric errors in the paper [9]. Let $\underline{x} = (x_1, x_2, \dots, x_n)$ and $\underline{y} = (y_1, y_2, \dots, y_n)$ be binary n -vectors. The distance-function is defined as

$$d_V(\underline{x}, \underline{y}) = \frac{1}{2} [w_H(\underline{x} - \underline{y}) + |w_H(\underline{x}) - w_H(\underline{y})|],$$

where $w_H(\underline{x})$ denotes the Hamming weight of \underline{x} .

The equivalent definition was introduced in [10]:

$$d_V(\underline{x}, \underline{y}) = \max \{N_{01}(\underline{x}, \underline{y}), N_{10}(\underline{x}, \underline{y})\},$$

where

$$N_{01}(\underline{x}, \underline{y}) = \# \{(x_i, y_i) : x_i = 0, y_i = 1\}, N_{10}(\underline{x}, \underline{y}) = \# \{(x_i, y_i) : x_i = 1, y_i = 0\}$$

Many results and code constructions are known.

Main theoretical result sounds that

$$M_H(n, 2d - 1) \leq M_V(n, d) \leq dM_H(n, 2d - 1),$$

where $M_H(n, d)$ and $M_V(n, d)$ denote maximal cardinalities of codes with minimal distance d in the Hamming metric and in the Varshamov metric, respectively.

The burst metric for dependent errors

The b -burst metric was introduced first in the paper [11], though codes correcting burst were invented much earlier. The burst norm $\mathcal{N}_b(\underline{x})$ of a vector \underline{x} is defined as follows. Represent this vector as

$$\underline{x} = (x_1, x_2, \dots, x_n) = (0^{m_1} u_1 v_1^{b-1} 0^{m_2} u_2 v_2^{b-1} \dots),$$

where $u_j \neq 0$, 0^m means the all zero string of length $m \geq 0$, v^{b-1} means any string of length $b - 1$. Such representation is unique. Then the b -burst norm of \underline{x} is equal to the number of b -tuples:

$$\mathcal{N}_b(\underline{x}) = \# (b\text{-tuples of type } (uv^{b-1})).$$

For example, if $b = 4$ and the ternary vector is $\underline{x} = (0, 0, 2, 2, 1, 1, 1, 1, 0, 0, 2, 0, 0, 0, 0, 1, 2, 1)$, then the representation as a sequence of b -tuples is $\underline{x} = (0, 0, \dot{:}2, 2, 1, 1, \dot{:} :1, 1, 0, 0, \dot{:} :2, 0, 0, 0, \dot{:} , 0, \dot{:} 1, 2, 1, \dot{:})$, so $\mathcal{N}_4(\underline{x}) = 4$.

The b -burst distance is defined as

$$d_b(\underline{x}, \underline{y}) = \mathcal{N}_b(\underline{x} - \underline{y}).$$

Many constructions and decoding algorithms are published devoted to correcting burst errors. Still the notion "metric" is used not very often.

Several general facts about b -burst correcting codes are listed below.

1. The generator weight function of n -dimensional vectors:

$$W_n(z) = \sum_{i=1}^{D_n} A_i(n) z^i,$$

where $A_i(n)$ denotes the number of vectors with the b -burst i and $D_n = \lceil \frac{n}{b} \rceil$ is the maximal possible b -norm of \underline{x} . Here

$$A_1(n) = \begin{cases} q^n - 1, & 1 \leq n \leq b; \\ (q-1)q^{b-1}(n-b+1) + q^{b-1} - 1, & n > b; \end{cases}$$

$$A_i(n) = [(q-1)q^{b-1}]^{i-1} \sum_{j=0}^{n-b(i-1)} \binom{j+i-2}{i-2} A_1(n-b(i-1)-j); \quad i > 1.$$

For large n , the average norm $W_n = \frac{\sum_{i=0}^{D_n} N_i}{q^n} \approx \frac{q-1}{1+b(q-1)}$. The normalized average norm $\delta = \frac{N_n}{D_n} \approx \frac{b(q-1)}{1+b(q-1)}$.

2. The upper bound (can be improved) [12].

For any q -ary code with minimal b -distance d and cardinality M we have

$$R = \frac{\log_q M}{n} \leq b \left[1 - H_{q^b} \left(\frac{q_b - 1}{q_b} - \frac{q_b - 1}{q_b} \sqrt{1 - \frac{q_b}{q_b - 1} x} \right) \right],$$

where $x = \frac{d}{D_n}$ is the normalized minimal distance.

3. The lower bound (can be improved) [12].

There exists a q -ary code with minimal b -distance d and cardinality M such that

$$\begin{aligned} R &= \frac{\log_q M}{n} = \max\{R_1, R_2\}, \\ R_1 &= \left(1 - \frac{b-1}{b}x\right) \left[1 - H_2 \left(\frac{x}{b-(b-1)x}\right) \log_2 q\right] - \frac{x}{b} \log_q (q-1), \\ R_2 &= \max_{s \geq 2} \frac{1}{s} \left[1 - H_{q^b} \left(\frac{xs}{s-1}\right)\right]. \end{aligned}$$

Combinatorial Metrics

Combinatorial metrics were introduced in [13]. Sometimes specific spots of errors are most probable in channels. Then often we can define a matched metric.

We shall consider both vector signals ($\mathbf{x} \in \mathcal{X}^n$) and matrix signals ($\mathbf{X} \in \mathcal{X}^{m \times n}$). To describe coordinates of signals, we consider two types of index sets:

the Line index set

$$\mathbf{I} = \{i \mid 0 \leq i \leq n-1\},$$

and the Array index set

$$\mathbf{I} = \{\{i, j\} \mid 0 \leq i \leq m-1, 0 \leq j \leq n-1\}.$$

Hence the set of all signals can be denote equally

$$\mathcal{X}^{\mathbf{I}} = \{\mathbf{x} \mid \mathbf{x} = (x(u), u \in \mathbf{I})\}.$$

For a signal $\mathbf{x} \in \mathcal{X}^{\mathbf{I}}$, the **support** is defined by

$$Q(\mathbf{x}) = \{i \mid x_i \neq 0, i \in \mathbf{I}\}.$$

Choose a subset $T \in \mathbf{I}$.

A word $\mathbf{x} \in \mathcal{X}^{\mathbf{I}}$ is said to be a T -spot, or T -burst, if

$$Q(\mathbf{x}) \subseteq T.$$

General Definition.

Consider a set of **Basic subsets**

$$\mathbf{T} = \{T_0 = \emptyset, T_1, T_2, \dots, T_s\}, T_j \subseteq \mathbf{I}$$

with the only restriction

$$\bigcup_{i=0}^s T_i = \mathbf{I}.$$

The \mathbf{T} -norm is defined by

1. $\mathcal{N}_{\mathbf{T}}(\mathbf{x}) = 0 \iff Q(\mathbf{x}) = \emptyset$.
2. $\mathcal{N}_{\mathbf{T}}(\mathbf{x}) = 1 \iff Q(\mathbf{x}) \subseteq T_i$ for some i .
3. $\mathcal{N}_{\mathbf{T}}(\mathbf{x}) = k \iff$
 $Q(\mathbf{x}) \subseteq \{ \text{a junction of exactly } k \text{ subsets from } \mathbf{T} \},$
but
 $Q(\mathbf{x}) \not\subseteq \{ \text{a junction of } k - 1 \text{ or less subsets from } \mathbf{T} \}$

A combinatorial metric for the Line index set is said to be Translation invariant if and only if

$$T_i = T_1 + (i - 1) \pmod{n}, \quad i = 1, \dots, n.$$

A combinatorial metric for the Array index set is said to be Translation invariant if and only if

$$T_{ij} = T_{11} + \{(i - 1), (j - 1)\} \pmod{n_1}, \pmod{n_2} \\ i = 1, \dots, n_1, \quad j = 1, \dots, n_2.$$

Let $\mathcal{N}_{\mathbf{T}_1}(\mathbf{x})$ and $\mathcal{N}_{\mathbf{T}_2}(\mathbf{x})$ be two metrics defined on $\mathcal{X}^{\mathbf{I}}$, such that $\mathcal{N}_{\mathbf{T}_1}(\mathbf{x}) \leq \mathcal{N}_{\mathbf{T}_2}(\mathbf{x}), \forall \mathbf{x} \in \mathcal{X}^{\mathbf{I}}$. Then $M_1(n, d) \leq M_2(n, d)$, where $M_i(n, d), i = 1, 2$, are maximal cardinalities of codes.

Examples of combinatorial metrics

Previous metrics

The **Hamming metric** can be considered as a combinatorial metric defined by Basic subsets

$$T_1 = \{0\}, T_2 = \{1\}, \dots, T_n = \{n - 1\}.$$

Its generalization is **the non-uniform Hamming Metric** defined by the following Basic subsets:

$$\begin{aligned} T_1 &= \{0, 1, \dots, n_1 - 1\}, \\ T_2 &= \{n_1, n_1 + 1, \dots, n_1 + n_2 - 1\}, \\ \dots &\dots \dots \\ T_s &= \left\{ \sum_{k=1}^{s-1} n_k, \sum_{k=1}^{s-1} n_k + 1, \dots, \sum_{k=1}^{s-1} n_k + n_s - 1 \right\}; \\ \sum_{k=1}^s n_k &= n \end{aligned}$$

The metric is useful to construct codes when the different coordinates belong to different alphabets. Main results about codes in this metric can be found in [14].

The b-burst metric can be considered as a combinatorial metric defined by Basic subsets

$$\begin{aligned} T_1 &= \{0, 1, \dots, b - 1\}, \\ T_2 &= \{1, 2, \dots, b\}, \\ \dots &\dots \dots \\ T_{n-b+1} &= \{n - b, n - b + 1, \dots, n\}. \end{aligned}$$

Vectors of weight 1 in this metric are vectors such that all the non zero coordinates can be covered by the only string of length b .

Its generalization is the 1-dimensional **cyclic b -burst metric** defined by Basic subsets

$$\begin{aligned}
 T_1 &= \{0, 1, \dots, b-1\}, \\
 T_2 &= \{1, 2, \dots, b\}, \\
 &\dots \quad \dots \quad \dots \\
 T_{n-b+1} &= \{n-b, n-b+1, \dots, n\}, \\
 T_{n-b+2} &= \{n-b+1, n-b+2, \dots, 0\}, \\
 &\dots \quad \dots \quad \dots \\
 T_n &= \{n, 0, \dots, b-2\},
 \end{aligned}$$

Vectors of weight 1 are vectors such that all the non zero coordinates can be covered by the only *cyclic* string of length b .

The 1-dimensional Hamming-burst (t, b) metric

This metric is defined by Basic subsets

$$\begin{aligned}
 T_\alpha &= \{\alpha = \{i_1, i_2, \dots, i_t\} \mid 0 \leq i_1 < i_2 < \dots < i_t \leq n-1\} \\
 T_1 &= \{0, 1, \dots, b-1\}, \\
 T_2 &= \{1, 2, \dots, b\}, \\
 &\dots \quad \dots \quad \dots \\
 T_{n-b+1} &= \{n-b, n-b+1, \dots, n\}, \\
 T_{n-b+2} &= \{n-b+1, n-b+2, \dots, 0\}, \\
 &\dots \quad \dots \quad \dots \\
 T_n &= \{n, 0, \dots, b-2\},
 \end{aligned}$$

Vectors of weight 1 are: all the vectors of the Hamming weight t and all vectors such that all the non zero coordinates can be covered by the only cyclic string of length b .

Codes of T -distance 3 correct all single errors in this metric, i. e., t -fold random errors, or all single b -burst errors. Such linear (n, k) codes exist, if

$$\begin{aligned}
 &\sum_{i=0}^{2t-1} \binom{n-1}{i} (q-1)^i + \left[\sum_{i=t+1}^{b-1} \binom{b-1}{i} (q-1)^i \right] \left[\sum_{i=0}^{t-1} \binom{n-b-1}{i} (q-1)^i \right] + \\
 &\left[\sum_{i=t}^{b-1} \binom{b-1}{i} (q-1)^i \right] \left[\sum_{i=0}^t (i+1) \binom{n-b}{i} (q-1)^i \right] + \left[\sum_{i=t+1}^{b-1} \binom{b-1}{i} (q-1)^i \right] \left[\sum_{i=t}^{b-1} \binom{b-1}{i} (q-1)^i \right] + \\
 &\left[\sum_{i=t}^{b-1} \binom{b-1}{i} (q-1)^i \right]^2 (n-2b+1)(q-1) < q^{n-k}.
 \end{aligned}$$

Let $\delta = 2t/n$, $\gamma = b/n$. Then we have asymptotically that there exist linear codes with rate

$$R = \begin{cases} 1 - 2\gamma, & 0 \leq \delta \leq \delta_1(\gamma); \\ (1 - \gamma)H_2\left(\frac{\delta}{2(1-\gamma)}\right) \log_2 q + \frac{\delta}{2} \log_q(q-1), & \delta_1(\gamma) \leq \delta \leq \delta_2(\gamma); \\ 1 - H_q(\delta), & \delta_2(\gamma) \leq \delta \leq \frac{q-1}{q} \end{cases},$$

where $\delta_1(\gamma)$, $\delta_2(\gamma)$ are roots of equations

$$\begin{aligned}
 (1 - \gamma)H_2\left(\frac{\delta_1}{2(1-\gamma)}\right) \log_2 q + \frac{\delta_1}{2} \log_q(q-1) &= \gamma; \\
 (1 - \gamma)H_2\left(\frac{\delta_2}{2(1-\gamma)}\right) \log_2 q + \frac{\delta_2}{2} \log_q(q-1) + \gamma &= H_q(\delta_2).
 \end{aligned}$$

In particular, this means that ordinary linear codes correcting up to t random errors can also correct single b -bursts, if $\delta \geq \delta_2(\gamma)$.

The 2-dimensional $(b_1 \times b_2)$ -burst metric

The Basic subsets for this metrics are all the 2-dimensional cyclic shifts $(\text{mod } n_1, \text{mod } n_2)$ of the subset T_{11} , where T_{11} is a rectangle of size $b_1 \times b_2$ in the upper left hand corner of the Array index set:

$$T_{11} = \begin{bmatrix} (0, 0) & (0, 1) & \cdots & (0, b_2 - 1) \\ \cdots & \cdots & \cdots & \cdots \\ (b_1 - 1, 0) & (b_1 - 1, 1) & \cdots & (b_1 - 1, b_2 - 1) \end{bmatrix}$$

Matrices of weight 1 are matrices such that all the non zero coordinates can be covered by the only *cyclic* $b_1 \times b_2$ rectangle.

The Weight Enumerator is known for special cases only.

Several results can be found in [15].

The Term Rank Metric

The metric was proposed in [16; 18]. The Array index set is used. The Basic subsets are as follows:

$$\{\text{All rows of the Array Index Set}\} \cup \{\text{All columns of the Array Index Set}\}$$

This metric is not translation invariant. Matrices of weight 1 are all matrices such that all the non zero coordinates can be covered by the only row or by the only column.

The Weight Enumerator is unknown for this metric.

Another definition can be given in combinatorial terms. If

$$\mathbf{X} = \begin{bmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{m-1,0} & x_{m-1,1} & \cdots & x_{m-1,n-1} \end{bmatrix}$$

is a $m \times n$ matrix over the field $GF(q)$, then the *Term Rank Norm* of a matrix \mathbf{X} , $\mathcal{N}_{TR}(\mathbf{X})$, is defined as the *minimal* number of lines (rows or columns) containing all *nonzero* elements of a matrix.

Easy decodable optimal codes for this metric are described in [19; 20].

Projective metrics

Projective metrics were proposed in [21; 22].

Let F_q^n be a vector space of dimension n over a finite field F_q .

Let

$$\mathcal{F} = \{\mathbf{f}_1, \mathbf{f}_2, \cdots, \mathbf{f}_N\}$$

be a set of non-zero distinct column vectors from F_q^n containing a basis. This means that $N \geq n$ and there exist n linearly independent vectors in \mathcal{F} .

It is convenient to treat \mathcal{F} as a $n \times N$ matrix.

Each vector $\mathbf{f} \in F_q^n$ can be represented (not uniquely) as a linear combination of columns from \mathcal{F} :

$$\mathbf{f} = a_1 \mathbf{f}_1 + a_2 \mathbf{f}_2 + \cdots + a_N \mathbf{f}_N.$$

The projective \mathcal{F} -norm $\mathcal{N}_{\mathcal{F}}(\mathbf{f})$ of a vector \mathbf{f} is defined as a minimal possible number of non-zero coefficients among all representations of \mathbf{f} :

$$\mathcal{N}_{\mathcal{F}}(\mathbf{f}) = \min \#(a_i \neq 0 : \mathbf{f} = a_1 \mathbf{f}_1 + a_2 \mathbf{f}_2 + \cdots + a_N \mathbf{f}_N).$$

This definition defines very rich family of metrics which can be useful to describe errors in channels with an additive noise.

All the vectors $\mathbf{f}_i \in \mathcal{F}$ and its multiples (and only these vectors) are of norm 1 and are considered as 1-fold errors.

Examples of projective metrics

The Hamming metric. Let $N = n$ and let

$$\mathcal{F} = \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \right\}$$

Then this set defines the Hamming norm and the Hamming distance.

If \mathcal{F} is a non singular matrix, then it defines formally the new metric but *equivalent* to the Hamming metric.

The metric for a channel with phase rotation. If a receiver should recover synchronization, then sometimes data are received as negative:

$$\text{Input data } \dots 0011101 \dots \implies \dots 1100010 \dots \text{ Output data}$$

Extra redundancy is needed to discover and to remove the phase rotation. An alternative is use of a special metric.

Let $N = n + 1$ and let

$$\mathcal{F} = \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \cdots & \vdots & \\ 0 & 0 & \cdots & 1 & 1 \end{pmatrix} \right\}$$

The phase rotation is treated as adding to transmitted blocks the all 1's block. Declare this block as a 1-fold error. Use codes correcting 1-folds errors. Such codes are constructed in [23; 24].

The Rank metric

This metric was introduced in [17; 18; 25].

Let $q = p^m$, let F_p be a base field and let $\text{rank}(\mathbf{f}; F_p)$ be the rank of a vector $\mathbf{f} \in F_q^n$ over the base field F_p . Let \mathcal{F} be the set of all the vectors of rank 1:

$$\mathcal{F} = \{ \mathbf{f} : \mathbf{f} \in F_q^n, \text{rank}(\mathbf{f}; F_p) = 1. \}$$

This set defines the Rank metric.

The theory of codes in the rank metric is presented in [25].

Linear optimal (n, k, d) codes are called Maximal Rank Distance codes, or, MRD codes. They can be defined in terms of *generator* matrices of the form

$$\mathbf{G} = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_n^{q^2} \\ \cdots & \cdots & \cdots & \cdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{bmatrix},$$

where g_1, g_2, \dots, g_n is a set of elements of \mathbb{F}_{q^N} which are linearly independent over \mathbb{F}_q . MRD codes have the following parameters:

Code length $n \leq N$; Dimension k ; Rank and Hamming code distance $d = r + 1 = n - k + 1$.

Let $A_i(n, d)$ be the number of vectors of a MRD code of rank weight i . Spectra of (n, k, d) MRD codes are given by the next equations:

$$\begin{aligned} A_0(n, d) &= 1; \\ A_i(n, d) &= \begin{bmatrix} n \\ i \end{bmatrix} \sum_{j=0}^{i-d} (-1)^{j+i-d} \begin{bmatrix} i \\ d+j \end{bmatrix} q^{(m-j)(m-j-1)/2} (q^{N(j+1)} - 1), \quad i \geq d. \end{aligned}$$

Here $\begin{bmatrix} n \\ i \end{bmatrix}$ is the notation for Gaussian numbers:

$$\begin{bmatrix} n \\ i \end{bmatrix} = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{i-1})}{(q^i - 1)(q^i - q) \dots (q^i - q^{i-1})}.$$

There exist fast decoding algorithms for MRD codes [25].

The Vandermonde metric

The Vandermonde \mathcal{F} -metric is defined as follows.

Vectors $\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_N$ that specify the \mathcal{F} -metrics are chosen as columns of the Vandermonde matrix:

$$\mathbf{F} = \begin{pmatrix} u_1 & u_2 & \dots & u_N \\ u_1 x_1 & u_2 x_2 & \dots & u_N x_N \\ u_1 x_1^2 & u_2 x_2^2 & \dots & u_N x_N^2 \\ \dots & \dots & \dots & \dots \\ u_1 x_1^{n-1} & u_2 x_2^{n-1} & \dots & u_N x_N^{n-1} \end{pmatrix}.$$

Here $n \leq N$, $x_i \in \mathbb{F}_q$ should be different, $u_i \in \mathbb{F}_q$ should be non-zero, $i = 1, \dots, N$.

Optimal linear (n, k, d) codes in this metric can be defined in terms of generator matrices of the form:

$$\mathbf{G} = \begin{pmatrix} v_1 & v_1 y_1 & \dots & v_1 y_1^{n-1} \\ v_2 & v_2 y_2 & \dots & v_2 y_2^{n-1} \\ v_3 & v_3 y_3 & \dots & v_3 y_3^{n-1} \\ \dots & \dots & \dots & \dots \\ v_k & v_k y_k & \dots & v_k y_k^{n-1} \end{pmatrix}.$$

Here $v_i \in \mathbb{F}_q$ are non-zero, and $y_i \in \mathbb{F}_q$ are different. Moreover, we must choose y_j that differs from each x_i .

A dimension k of the code C must satisfy $k + N \leq q + 1$ (it is a necessary condition for the fast decoding algorithm).

There exist a fast decoding algorithm for these codes.

Codes are used in the modified Niederreiter public key cryptosystem [26].

Some graph metrics

It is clear that distance among nodes in a connected graph constitutes a metric. The distance, $d(n_1, n_2)$, between two nodes n_1 and n_2 in a connected graph is the length of the shortest path joining them and the diameter is the maximum of all the distances between any pair of nodes. It is known that Hamming distance among codewords can be seen as the graph distance among vertices in a Hypercube graph. In the same way, the Lee metric in two-dimensional signal sets can be associated to minimal routing in a Torus graph.

Examples of graph metrics

Circulant Graph Distances over Gaussian Integer Constellations. The *Gaussian integers* $\mathbb{Z}[i]$ is the subset of the complex numbers with integer real and imaginary parts, that is:

$$\mathbb{Z}[i] := \{x + yi \mid x, y \in \mathbb{Z}\}.$$

$\mathbb{Z}[i]$ is an Euclidean domain and the norm is defined as:

$$\begin{aligned} \mathcal{N} : \quad \mathbb{Z}[i] &\longrightarrow \mathbb{Z}^+ \\ x + yi &\longmapsto x^2 + y^2 \end{aligned}$$

If $0 \neq \alpha \in \mathbb{Z}[i]$, we consider $\mathbb{Z}[i]_\alpha$ the ring of the classes of $\mathbb{Z}[i]$ modulo the ideal (α) generated by α .

A new metric over these subsets of the Gaussian integers is defined in a very natural way. This metric is applicable when using any value of α (not necessarily with prime norm) and it corresponds to the distance among nodes in its associated circulant graph.

For $\beta, \gamma \in \mathbb{Z}[i]_\alpha$, consider $x + yi$ in the class of $\beta - \gamma$ with $|x| + |y|$ minimum. The distance D_α between β and γ is

$$D_\alpha(\beta, \gamma) = |x| + |y|.$$

D_α defines a distance over the quotient ring $\mathbb{Z}[i]_\alpha$.

A new family of circulant graphs of degree four whose nodes are labeled by Gaussian integers and their adjacency is determined by the distance D_α was introduced in [27].

Given $\alpha = a + bi \in \mathbb{Z}[i]$ with $\gcd(a, b) = 1$ we define the graph $G_\alpha = (V, E)$ where:

1. $V = \mathbb{Z}[i]_\alpha$ is the node set, and
2. $E = \{(\beta, \gamma) \in V \times V \mid D_\alpha(\beta, \gamma) = 1\}$ is the edge set.

Perfect codes over quotient rings of Gaussian integers were constructed correcting 1-fold errors.

Eisenstein-Jacobi integers and circulant graphs of degree six. The ring of the *Eisenstein-Jacobi integers* is defined as:

$$\mathbb{Z}[\rho] = \{x + y\rho \mid x, y \in \mathbb{Z}\},$$

where $\rho = (-1 + \sqrt{-3})/2$. The ring $\mathbb{Z}[\rho]$ is an Euclidean domain with norm

$$\begin{aligned} \mathcal{N} : \mathbb{Z}[\rho] &\longrightarrow \mathbb{N} \\ x + y\rho &\longmapsto x^2 + y^2 - xy \end{aligned}$$

The units of $\mathbb{Z}[\rho]$ are the elements with unitary norm, that is $\{\pm 1, \pm\rho, \pm\rho^2\}$.

For every $0 \neq \alpha \in \mathbb{Z}[\rho]$ we can consider $\mathbb{Z}[\rho]_\alpha = \{\beta \pmod{\alpha} \mid \beta \in \mathbb{Z}[\rho]\}$.

Let $0 \neq \alpha = a + b\rho \in \mathbb{Z}[\rho]$ with $\gcd(a, b) = 1$ and consider $\mathbb{Z}[\rho]_\alpha$. Denote the *Eisenstein-Jacobi graph* generated by α as $EJ_\alpha = (V, E)$ and it is defined as follows:

- $V = \mathbb{Z}[\rho]_\alpha$ is the set of nodes and
- $E = \{(\beta, \gamma) \in V \times V \mid (\gamma - \beta) \equiv \pm 1, \pm\rho, \pm\rho^2 \pmod{\alpha}\}$ is the set of edges.

Let $\alpha = a + b\rho \in \mathbb{Z}[\rho]$ be such that $\gcd(a, b) = 1$. Denote the distance between nodes β and γ in EJ_α as $D_\alpha(\beta, \gamma)$. This distance can be expressed as:

$$D_\alpha(\beta, \gamma) = \min\{|x| + |y| + |z| \mid x + y\rho + z\rho^2 \equiv (\gamma - \beta) \pmod{\alpha}\}.$$

Perfect codes over quotient rings of Eisenstein–Jacobi integers were constructed correcting 1-fold errors.

The subspace metric

A subspace approach for network coding has been proposed in [28]. It allows to overcome many previous restrictions on network configurations. Coding schemes using this approach are developed in [29]. The subspace approach is based on the subspace metric.

Let \mathbb{F}_q be a finite field of q elements. Denote by $W_{N,q}$ a fixed N -dimensional vector space over the field \mathbb{F}_q . Let $\mathcal{P}(W_{N,q})$ be the set of all subspaces of $W_{N,q}$.

The **subspace distance** between two subspaces U and V is defined as follows:

$$d(U, V) = \dim(U \uplus V) - \dim(U \cap V). \tag{1}$$

Codes for network coding are proposed in several papers (see, [28] - [34]).

Conclusion

Metrics are used in many practical applications. The brief survey of such metrics is given.

General properties of codes are considered including simple bounds.

Many examples of metrics are described. In particular, the uniform and non-uniform Hamming metrics, the Lee and Sharma-Kaushik metrics, the city block (Manhattan) metric, the Varshamov metric, the burst metric, the 2-dimensional burst metric, the term rank metric, the rank metric, combinatorial metrics, projective metrics, graph metrics, the subspace metric.

Open problems are pointed.

Acknowledgements

This work is supported in part by Grant of Ministry of Education 8.4414.2011(0704 T 019).

Bibliography

- [1] F. J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes. I, II*. North-Holland Mathematical Library, Vol. 16, Amsterdam: North-Holland Publishing Co., 1977.
- [2] S. G. Vlăduț, D. J. Nogin, M. A. Tsfasman, *Algebraic-geometric codes. Fundamentals*. (in Russian) — M.:MCCME, 2003.—P. 504.
{See also, M. A. Tsfasman and S. G. Vlăduț, *Algebraic-geometric codes*, vol. 58 of *Mathematics and Its Applications (Soviet Series)*. Dordrecht: Kluwer Academic Publishers Group, 1991.}
- [3] Sharma B. D. and Kaushik M. L., Limites intensity random and burst error codes with class-weight considerations, *Elektron. Inform.-verarb. Kybernetik* 15 (1979), 315-321.
- [4] Sharma B. D. and Kaushik M. L., Algebra of Sharma and Kaushik's metric inducing partitions of Z_q , *J. Combin. Inform. System Sci.* 11 (1986), 19 - 32.
- [5] Sharma, B. D. and Sookoo, N., Association and other schemes related to Sharma-Kaushik class of distances over finite rings, *Le Matematiche*, Vol. XLV, Fasc. I (1990), 163-185.
- [6] Sharma B. D. and Sookoo N., The difference matrices of the classes of a Sharma-Kaushik partition, *ARCHIVUM MATHEMATICUM (BRNO)*. Tomus 40 (2004), 23 - 31.
- [7] Berlekamp E. R., *Algebraic coding theory*. McGraw-Hill, New York, 1968.
- [8] Ulrich, BSTJ, 1957, No. 6
- [9] Varshamov R. R., On theory of asymmetric codes.— *Doclady of AS USSR*, 1965, vol. 164, No. 4, P. 757-760.
- [10] Rao T. R. N., Chawla A. S., Asymmetric error codes for some LSI semiconductor memories. — Proc. 7-th Ann. Southeast Symp. Syst. Theory, Auburn-Tuskegee, 1975, New York, N. J., 170-171.
- [11] Bridewell J. D., Wolf J. K., Burst distance and multiple burst correction.— *Bell. Syst. Tech. J.*, 1979, 49, 889-909.
- [12] Gabidulin E. M., Bassalygo L. A., Sidorenko V.R., Varshamov-Gilbert Bound is improvable for Codes Correcting Multiple Burst Errors.—In: Proc. of the 6-th International Symposium on Information Theory, Part II, pp. 78-80, 1984, Moscow-Tashkent.
- [13] Gabidulin E. M., Combinatorial metrics in coding theory.— In: *Proc. of the 2-nd International Symposium on Information Theory*, Budapest, 1971, 169-176.
- [14] Vladimir Sidorenko, Georg Schmidt, Ernst Gabidulin, Martin Bossert, Valentin Afanassiev, "On polyalphabetic block codes, " Proc. of the ITW2005 - IEEE ITSOC Information Theory Workshop 2005 on Coding and Complexity, 28th/29th Aug. - 1st Sept. 2005 - Rotorua, New Zealand.
- [15] Gabidulin E. M., Zanin V. V., Codes Correcting Array Errors.— In: B. Honary, M. Darnell, P. Farrell (Eds), *COOMUNICATION THEORY AND APPLICATIONS II*, HW Communications Ltd. 1994.
- [16] Gabidulin E. M., A Class of Two-Dimensional Codes Correcting Lattice-Pattern Errors.— In: Proc. of the 2-nd International Symposium on Information Theory, pp. 44-47, 1971, Moscow-Yerevan.
- [17] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory A*, vol. 25, pp. 226-241, 1978.
- [18] Gabidulin E. M., Optimal Codes Correcting Array Errors.— In: Proc. of the 6-th International Symposium on Information Theory, Part II, pp. 75-77, 1984, Moscow-Tashkent.

-
-
- [19] Gabidulin E. M., Optimal Codes Correcting Array Errors.– *Problems of Information Transmission*, v. 21, No. 2, pp. 3-11, 1985.
- [20] Gabidulin E. M., Lund D., Honary B., A New Family of Optimal Codes Correcting Term Rank Errors.– In: Proc. of the 2000 IEEE International Symposium on Information Theory, 25 - 30 June, 2000, p. 115, Sorrento, Italy.
- [21] Gabidulin E. M., Simonis J., Metrics Generated by a Projective Point Set.– In: Proc. of the 1997 IEEE International Symposium on Information Theory, June 29 - July 4, 1997, p. 248, Ulm, Germany.
- [22] Gabidulin E. M., Simonis J., Metrics Generated by Families of Subspaces.– *IEEE Trans. Inform. Theory*, vol. 44, pp. 1336-1341, May 1998.
- [23] Gabidulin E. M., Bossert M., Codes Resistant to the Phase Rotation.– In: Proc. of the 4-th Symposium on Communication and Applications, pp. 253-257, July 1997, pp. 65-84, Charlotte Mason College, Lake District, UK.
- [24] Gabidulin E. M., Bossert M., Hard and Soft Decision Decoding of Phase Rotation Invariant Block Codes.– In: Proceedings of the 1998 International Zurich Seminar on Broadband Communications - Accessing, Transmission, Networking - 17-19 February, 1998, ETH Zurich, Switzerland.
- [25] Gabidulin E. M., Theory of Codes with Maximum Rank Distance.– *Problems of Information Transmission*, v. 21, No. 1, pp. 3-14, 1985.
- [26] Gabidulin E. M., Obernikhin V. A., Codes in the Vandermonde \mathcal{F} -metric and applications.– *Problems of Information Transmission*, v. 39, No. 2, pp. 3-14, 2003.
- [27] C. Martínez, R. Beivide, J. Gutierrez and E. Gabidulin. "On the Perfect t -Dominating Set Problem in Circulant Graphs and Codes over Gaussian Integers". Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT'05). Adelaide, Australia. September, 2005.
- [28] Koetter R., Kschischang F. R.: Coding for errors and erasures in random network coding. In: Proc. of the 2007 IEEE International Symposium on Information Theory (ISIT 2007), pp. 791-795. Nice, France, 24-29 June (2007)
- [29] Silva D., Kschischang F. R.: Using rank-metric codes for error correction in random network coding. In: Proc. of the 2007 IEEE International Symposium on Information Theory (ISIT 2007), pp. 796-800. Nice, France, 24-29 June (2007)
- [30] Gabidulin E., Bossert M.: Codes for Network Coding. In: Proc. of the 2008 IEEE International Symposium on Information Theory (ISIT 2008), pp. 867-870. Toronto, ON, Canada, 6-11 July (2008)
- [31] Gabidulin E.M., Bossert M.: A Family of Algebraic Codes for Network Coding. *Probl. Inform. Transm.* Vol. 45. No. 4, pp. 54–68 (2009)
- [32] Skachek V.: Recursive Code Construction for Random Networks. *IEEE Trans. On Inform. Theory*. V. 56. No. 3, pp. 1378-1382 (2010)
- [33] Etzion T., Silberstein N.: Error-Correcting Codes in Projective Spaces Via Rank-Metric Codes and Ferrers Diagrams. *IEEE Trans. On Inform. Theory*. V. 55. No. 7, pp. 2909–2919 (2009).
- [34] Gadouleau M., Yan Z.: Construction and Covering Properties of Constant-Dimension Codes. In: Proc. of the 2009 IEEE International Symposium on Information Theory (ISIT 2009), pp. 2221-2225. Nice, France, 24-29 June (2007)

Authors' Information



Ernst Gabidulin - Professor, Moscow Institute of Physics and Technology (State University), Dept. of Radio Engineering and Telecommunications,
P.O. Box: 141700, Dolgoprudny Moscow region, Russia; e-mail: ernst_gabidulin@yahoo.com
Major Fields of Scientific Research: Algebraic coding, Cryptography, Sequences