

## A study of Superregular Matrices and MDS Codes

Fábio C.C. Meneghetti\*, Sara D. Cardell, Marcelo Firer

### Abstract

In this work we study the form and properties of the generator matrices of codes with a maximum and almost-maximum distance profile with the Hamming metric. We wrote programs to make tests on various linear codes, and found a relationship between the generalized Hamming distances of a code, and its systematic generator matrix.

### Key words:

Error-correcting codes, MDS codes, Superregular matrices.

### Introduction

Let  $\mathbb{F}_q$  be a Galois field with  $q$  elements. We define a **linear block code**  $\mathcal{C}$  as a subspace of the vector space  $\mathbb{F}_q^n$ . The vectors of  $\mathcal{C}$  are called *codewords*.

If  $\mathcal{C}$  is a vector space with basis  $\beta = \{b_1, \dots, b_k\}$ , then the  $k \times n$  matrix  $G$  whose rows are the vectors  $b_1, \dots, b_k$  is called a **generator matrix** for the code  $\mathcal{C}$ . Without loss of generality, we can assume that the code  $\mathcal{C}$  has a generator matrix in the called **systematic form**  $G = [I|P]$ , where  $I$  is the  $k \times k$  identity matrix, and  $P$  is a  $k \times (n - k)$  matrix.

We can also define a distance for linear block codes. The most commonly used is the **Hamming distance**, in which the distance between two words is the number of coordinates in which they differ:  $d(x, y) = |\{i : x_i \neq y_i\}|$ . The minimum distance  $d$  between two different words of the code is called the **minimum distance** of the code.

An important fact about linear block codes is that they respect the **Singleton Bound**, that is,  $d \leq n - k + 1$ .

A code that achieves equality in this bound (i.e.  $d = n - k + 1$ ) is called an **MDS** (maximum distance separable) code.

**Theorem 1:** A linear block code  $\mathcal{C}$  is MDS iff  $\mathcal{C}$  has a generator matrix in the systematic form  $G = [I|P]$  such that every square submatrix of  $P$  is non-singular<sup>1</sup>.

A matrix like  $P$ , in the previous theorem, is called a **superregular matrix**.

The objective of this research is to study properties of these matrices, and to study the relationship between the generator matrix of a code, and the generalized Hamming distances.

### Results and Discussion

We went to study linear block codes with properties very similar to those of a MDS code. For this, we introduce the **generalized Hamming distances** of a code. We define the  $i$ -th generalized Hamming distance as:

$$d_i(\mathcal{C}) = \min \{D : D \text{ is a subcode of } \mathcal{C}, \dim(\mathcal{C}) = i\}.$$

The generalized Singleton bound states that  $d_i \leq n - k + i$ .

For example, **AMDS codes** are codes for which  $d_1(\mathcal{C}) = n - k$ . **NMDS codes** are codes where  $d_1(\mathcal{C}) = n - k$ , and  $d_i = n - k + i$  for  $i > 1$ .

In order to find the relationship between the generalized Hamming distances and the generator matrix of a linear

code, we wrote some computer programs in GAP<sup>2</sup> with the package GUAVA<sup>3</sup>.

We wrote a program that calculates the generalized Hamming distances of a given code, and one that lists all possible ranks of submatrices of a given matrix. We then tried to relate the possible ranks of a generator matrix of a code with the Hamming distances, by trying many examples.

Consider, for example, an  $[8, 3]$ -linear code. In this case,  $P$  is a  $3 \times 5$  matrix. The only way for  $d_1$  to be 1 is if we have a  $1 \times 5$  submatrix with rank 0. If  $d_1$  is not 1, then the only way for it to be 2 is if we have a  $2 \times 5$  submatrix with rank 1 or a  $1 \times 4$  submatrix with rank 0. And so on.

Following this reasoning, we conjectured and proved the following theorem:

**Theorem 2:** Let  $\mathcal{C}$  be a  $[n, k]$ -linear code with generator matrix  $G = [I|P]$ , and generalized Hamming distances  $\{d_1, \dots, d_k\}$ . If the integer  $x \geq -k$  is the smallest integer such that:

a) if  $Q$  is an  $h \times (h + y)$  submatrix of  $P$ , with  $y > x$ , then  $\text{rank}(Q) > h - i$  and

b) if there are  $g \times (g + x)$  submatrices of  $P$ , then at least one of them has a rank  $\leq g - i$ , then  $d_i = n - k - x$ . The reciprocal is also true.

### Conclusions

We wrote programs that allowed us to verify the generalized Hamming distances, and the ranks of submatrices of various linear codes. We concluded that there is a relationship between the generalized Hamming distances of a given code and the generator matrix of the code in the systematic form, as shown in the proved theorem.

### Acknowledgement

I want to thank Sara D. Cardell and Marcelo Firer, for guiding me in my research, the Institute of Mathematics, Statistics and Scientific Computing at Unicamp, for providing my study, and Fapesp for my research grant (Process 2015/25812-3).

<sup>1</sup>Roman, S; Coding and Information Theory

<sup>2</sup>The GAP Group; Groups, Algorithms and Programming, Version 4.8.4; 2016. (<http://www.gap-system.org>)

<sup>3</sup>R. Baart, T. Boothby, J. Cramwinckel, J. Fields, D. Joyner, R. Miller, E. Minkes, E. Roijackers, L. Ruscio, C. Tjhai; GUAVA – a GAP package, Version 3.13, 2016. (<https://osj1961.github.io/guava/>)