University of Trento

Department of Mathematics

Ph.D. in Mathematics
XXVII Cycle

On Boolean functions, symmetric cryptography and algebraic coding theory

Marco Calderini

Supervisor: Prof. Massimiliano Sala

Head of PhD School: Prof. Francesco Serra Cassano

April 2015

University of Trento

Department of Mathematics

Ph.D. in Mathematics
XXVII Cycle

On Boolean functions, symmetric cryptography and algebraic coding theory

Ph.D.Thesis of: Marco Calderini

Supervisor: Prof. Massimiliano Sala

Head of PhD School: Prof. Francesco Serra Cassano

April 2015

Contents

Introduction

This thesis is divided into two main parts. In the first part we report the work done with my supervisor Massimiliano Sala and in the second the work done jointly with Eimear Byrne, coming from a collaboration started during a period of research at University College Dublin.

In the first part we study a particular type of trapdoors, which can be embedded in a block cipher. Block ciphers combine simple operations to construct a complex encryption transformation. This tradition has its roots in Shannon's paper [Sha49] connecting cryptography with information theory. Shannon suggested building a strong cipher system out of simple components that substantiate the so-called confusion and diffusion of data applying these components iteratively in a number of rounds. Each of these components, seen as a single function, would be cryptographically weak and only their composition can be strong. Feistel [Fei73] and Feistel *et al.* [FNS75] were the first to introduce a practical architecture based on Shannon's concepts. The most prominent example of a Feistel type cipher is probably the Data Encryption Standard (DES) [Nat77].

Most modern block ciphers are built using components whose cryptographic strength is evaluated in terms of the resistance offered to attacks on the whole cipher. In particular, linear and differential properties of Boolean functions are studied for the S-Boxes to thwart linear and differential cryptanalysis ([Mat94],[BS93]). Little is known on similar properties to avoid trapdoors in the design of the block cipher. By a trapdoor we mean the presence of a secret that, if known, allows to disclose the cipher, i.e. to read a ciphertext without knowing the key, or to compute the encryption key. In the DES algorithm, no trapdoors have been found in more than 20 years, but many users are still suspicious about the DES S-boxes. The discussion of trapdoor issues has been directed towards individuating trapdoors in known ciphers. Belgian scientists V. Rijmen and B. Preneel [RP97] formulated the trapdoor topic in another way, proposing for the first time a family of trapdoor block ciphers. We find this approach fascinating.

A way to consider trapdoors is to employ (permutation) group theory, as follows. An iterated block cipher can be regarded as a set of permutations of a message space.

Some properties of the group generated by the round functions of such a cipher are known to be of cryptanalytic interest. Kenneth Paterson [Pat99] has considered iterated block ciphers in which the group generated by the one-round functions acts imprimitively on the message space, with the aim of exploring the possibility that this might lead to the design of trapdoors. In particular, Paterson constructed an example of a DES-like cipher where the group generated by the one-round functions is imprimitive. In [CDS09b] the authors investigated the minimal properties for the S-Boxes (and the mixing layer) of an AES-like cipher (more precisely, a translation-based cipher, or tb cipher) to thwart the trapdoor coming from the imprimitivity action. More refined group theory can be used to insert additional trapdoors, as elaborated below.

In [Li03], Li observed that if V is a vector space over a finite field $\mathbb{F}_p$, the symmetric group $\mathrm{Sym}(V)$ will contain many isomorphic copies of the affine group $\mathrm{AGL}(V)$, which are its conjugates in $\mathrm{Sym}(V)$. So there are several structures $(V, \circ)$ of a $\mathbb{F}_p$-vector space on the set V , where $(V, \circ)$ is the abelian additive group of the vector space. Each of these structure will yield in general a different copy $\mathrm{AGL}(V, \circ)$ of the affine group within $\mathrm{Sym}(V)$. Thus, if the group generated by the one-round functions of a block cipher is contained in a copy of $\mathrm{AGL}(V)$ this might lead to the design of trapdoors coming from alternative vector space structure, which we call *hidden sums*. Our main results along this direction are the following: Theorem 2.1.21, that characterizes hidden sums corresponding to translations group generated by affine maps and that are normalized by the usual translations maps. This characterization allows us to give a complete classification of elementary abelian subgroups contained in the affine group of a binary vector space of dimension at most 6. In Theorem 2.2.9 we establish a lower bound on the differential uniformity of the maps contained in the affine groups related to the hidden sums. Then we show in Theorem 2.4.1 that hidden sums trapdoors can be practical. Several minor results are scattered in this part of the thesis, such as the study of trapdoors coming from mixing-layers, keyschedule and even combining functions (these for stream ciphers).

In the second part of this thesis we report the results obtained jointly with Eimear Byrne on the Index Coding problem. The Index Coding with Side Information (ICSI) problem was introduced by Birk and Kol [BK98], in origin called *coding on demand by an informed Source* (ISCOD). There are several applications which motived the study of this problem as video on demand, daily newspaper delivery, or opportunistic wireless-network. The index coding problem is described in the following scenario. There is a server (sender) which broadcasts a set of messages to a set of clients

(receivers). During the transmission, each client might miss a certain part of the data, due to intermittent reception, limited storage capacity or any other reason. The server has to find a way to deliver to each client all the missing messages, yet spending a minimum number of transmissions. Via a slow backward channel, the clients let the server know which messages they already have in their possession, and which messages they request. By exploiting this information, the amount of the overall transmissions can be significantly reduced. For example suppose we have a single sender who has four message $\{x_i : 1 \leq i \leq 4\}$ and there are 4 receivers R_i, each with side information packets $\{x_j : 1 \leq j \leq 4, j \neq i\}$. Suppose R_i requests the data x_i for each i. The sender can satisfy the demands of all receivers by sending only one packet $z = \sum_{i=1}^{4} x_i$, since each receiver can recover its required message via $x_i = z + \sum_{i=j,j\neq i}^{4} x_i$. The ICSI problem has been the subject of several recent studies [ALS+08, BYBJK06, BL11, CASL11, DSC13]. This problem can be regarded as a special case of the well-known Network Coding (NC) problem [KM03]. In particular, it was shown that every instance of the NC problem can be reduced to an instance of the ICSI problem [ERSG08, ERSG10].

Several previous works focused on the design of efficient index codes. Given an instance of the ICSI problem, Bar-Yossef et al. [BYBJK06, BYBJK11] proved that finding the best binary scalar linear index code is equivalent to finding the so-called min-rank of a (di)graph. The concept of min-rank of a graph was first introduced by Haemers [Hae78], which serves as an upper bound for the celebrated Shannon capacity of a graph [Sha56]. Unfortunately, as shown by Peeters [Pee96], computing the min-rank of a general graph (that is, the MinRank problem) is a hard task. More specifically, Peeters showed that deciding whether a graph has min-rank three is an NP-complete problem. Exact and heuristic algorithms to find the min-rank over $\mathbb{F}_2$ of a hypergraph (and a (di)graph as a special case) were developed in the work of Chaudhry and Sprintson [CASL11]. The min-ranks of random (di)graphs are investigated by Haviv and Langberg [HL12]. The work in [DSC14] identifies the side information graphs whose optimal IC can be found efficiently, given a classification of graphs with near-extreme min-rank (i.e. $1, 2, n-1, n$).

In [DSC13], the authors considered the problem of index coding across a noisy channel. In this generalization, the sender has a vector $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{F}_q^n$, each receiver requests a component x_i of x and lets the server know which bits it already has. The sender linearly encodes the vector $\mathbf{x}$ as $\mathbf{c} = (c_1, ..., c_N) = L\mathbf{x}^T$ using an $N \times n$ matrix L (satisfying certain constraints) over $\mathbb{F}_q$ and transmits the symbols of $\mathbf{c}$ using N transmissions. This encoding is referred to as δ-error-correcting if each receiver can retrieve its desired bit after N transmissions, as long as fewer than δ erroneous transmissions have occurred. Syndrome decoding is applied to correct errors and

retrieve the required data at each receiver, which is computationally demanding.

One common point of preceding works is that coded packets in each user's cache are not utilized. It is more likely that certain coded packets may exist in some users' cache, which may aid the decoding and hence may improve transmission efficiency. In [SDS12] Shum *et al.* generalized the index coding problem so that coded packets of a data vector x may be broadcast or part of a user's cache. This is called Index Coding with Coded Side Information (ICCSI) problem. This finds applications, for example, in broadcast channels with helper relay nodes.

Here we investigate the optimal length of an index code, in particular in Theorem 5.1.4 we extend the so called clique-covering bound to the case of hypergraph, which permits to improve the bound on the graphs in some particular cases. We characterize also the directed graph having min-rank equals to $n-1$ over a sufficient large field, Theorem 5.2.5. Moreover we show that the decision problem whether a directed graph has min-rank $n-1$ can be solved in a polynomial time over a finite field of a cardinality $q > n$.

Subsequently, the ICCSI problem is taken into account. We extend the min-rank notion to this more general case, showing (Lemma 6.1.3) that is equal to the length of an optimal scalar linear index code. Then, several bounds and constructions for linear error-correcting index codes are extended from the ICSI case in Proposition 6.2.3, Proposition 6.2.5 and Proposition 6.2.6. Also two decoding schemes are investigated.

Organization of this Thesis

The first part of this thesis is divided in 3 chapters.

In Chapter 1 we summarize some known facts about block ciphers, in particular we introduce the translation based ciphers class, and we give some results on security properties of the cipher linked to the group of its round functions.

Chapter 2 studies some properties of the vector space structure $(V, \circ)$ which can be individuated over a binary vector space. In particular we characterize the affine groups which contain the usual translation group and such that the translation groups related to the new operations $\circ$'s are generated by affine maps. For that particular case we prove that a trapdoor coming from these hidden sums is practical.

Some necessary properties on S-boxes to avoid this kind of trapdoor are studied in Chapter 3, where we introduce the notion of anti-crooked function.

The second part starts with a chapter reporting some notions and basic results on coding theory, incident structures and graphs. Then we provide backgrounds on the ICSI problem. It also contains some bounds on the optimal length of an Index Code

and introduced the error correction for the ICSI problem.

In Chapter 5 we give some bounds on the optimal length of an index code, extending the so-called sandwich property to the case of hypergraph and using the t-designs. We also characterize the directed graphs having min-rank one less than the order.

In Chapter 6 we discuss the error correction for the more general case of the ICCSI problem. Bounds and constructions for error-correcting index codes of the ICSI problem case are extended to this more general case.

Part I

Hidden sum trapdoors

Preliminaries on Block Ciphers

In the first section of this chapter we report some preliminary results and the notations which will be used along the thesis. In Section 1.2, we outline some basic ideas about block ciphers, their security and their cryptanalysis. In the last section, we introduce the round-function group of a block cipher and some security properties that can be derived from it.

As reference we use here [LN97, Wat79, Lan12, Car06, Sti95, DR02a, CW09].

1.1 Notations and backgrounds

1.1.1 Linear algebra and group theory terminology

For any positive integer n, we let $[n] = \{1, \ldots, n\}$. We write $\mathbb{F}_q$ to denote the finite field of q elements, where q is a power of prime, and $\mathbb{F}_q^{N \times n}$ to denote the set of all matrices with entries over $\mathbb{F}_q$ with N rows and n columns. We write $\mathbb{F} = \mathbb{F}_2$. We use

$$\mathbf{e}_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i}) \in \mathbb{F}_q^n$$

to denote the unit vector, which has a one at the i-th position, and zeros elsewhere. The vector (sub)space generated by the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is denoted by $\mathrm{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Let $V = \mathbb{F}_q^n$, we denote by $\mathrm{Sym}(V)$, $\mathrm{Alt}(V)$, respectively, the symmetric and the alternating group acting on V. By $\mathrm{AGL}(V)$ and $\mathrm{GL}(V)$ we denote the affine and linear group of V. We write $\langle g_1, \ldots, g_n \rangle$ for the group generated by $g_1, \ldots, g_n$ in $\mathrm{Sym}(V)$.

Let G be a finite group acting on V. We write the action of a permutation $g \in G$ on a vector $\mathbf{v} \in V$ as $\mathbf{v}g$.

Definition 1.1.1. *Let G be a group acting on V. G is called* **transitive** *if for all $\mathbf{x}, \mathbf{y} \in V$ there exists $g \in G$ such that $\mathbf{x}g = \mathbf{y}$.*

G is called **regular** *if for all $\mathbf{x}, \mathbf{y} \in V$ there exists a unique $g \in G$ such that $\mathbf{x}g = \mathbf{y}$.*

Remark 1.1.2. G is regular if and only if G is transitive and $|G| = |V|$.

Definition 1.1.3. *A partition $\mathcal{B}$ of V is G-invariant if for any $B \in \mathcal{B}$ and $g \in G$, one has $Bg \in \mathcal{B}$. A partition $\mathcal{B}$ is trivial if $\mathcal{B} = \{V\}$ or $\mathcal{B} = \{\{\mathbf{v}\} \mid \mathbf{v} \in V\}$. If $\mathcal{B}$ is non-trivial and G-invariant then $\mathcal{B}$ is a* **block system** *for the action of G on V. If a block system exists, then we say that G is* **imprimitive** *in its action on V. If G is not imprimitive (and it is transitive), then we say that G is* **primitive**.

Definition 1.1.4. *An element r of a ring R is called* **nilpotent** *if $r^n = 0$ for some $n \geq 1$. $r \in R$ is called* **unipotent** *if $r - 1$ is nilpotent, i.e. $(r-1)^n = 0$ for some $n \geq 1$.*

Let $G \subseteq \mathrm{GL}(V)$ be a subgroup consisting of unipotent permutations, then G is called unipotent.

Definition 1.1.5. *An element $\kappa \in \mathrm{GL}(V)$ is said* **upper triangular** *in a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ if and only if*

$$\mathbf{v}_i\kappa - \mathbf{v}_i \in \mathrm{Span}\{\mathbf{v}_{i+1}, \ldots, \mathbf{v}_n\}$$

for all $1 \leq i \leq n$. The matrices upper triangular in the canonical basis are called **upper unitriangular matrices**. *We denote by $\mathcal{U}(V)$ the upper unitriangular matrices group.*

Remark 1.1.6. Usually the definition of upper triangular matrix in a basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is that

$$\mathbf{v}_i\kappa - \mathbf{v}_i \in \mathrm{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}\}.$$

Our definition comes from the fact that the map κ acts on the right of $\mathbf{x}$ also when the action is seen as a multiplication of a vector times a matrix, i.e. $\mathbf{x}\kappa = \mathbf{x}M$ where M is the matrix associated to κ.

The following theorem is well-known (see for instance [Wat79]).

Theorem 1.1.7. *Let G be a group consisting of unipotent matrices. Then there is a basis in which all elements of G are upper triangular.*

Definition 1.1.8. *Let A be an $n \times n$ matrix over a field $\mathbb{K}$, with $\lambda \in \mathbb{K}$ along the main diagonal and 1 along the diagonal above it, that is*

$$A = \begin{bmatrix} \lambda & 1 & & \ldots & 0 \\ 0 & \lambda & 1 & \ldots & 0 \\ \vdots & & & & \vdots \\ 0 & \ldots & & & \lambda \end{bmatrix}.$$

Then A is called the $n \times n$ elementary **Jordan matrix** *or Jordan block of size n.*

Definition 1.1.9. *A matrix A defined over a field $\mathbb{K}$ is said to be in* **Jordan canonical form** *if A is block-diagonal where each block is a Jordan block defined over $\mathbb{K}$.*

The following theorem is well-known (see for instance [Lan12]).

Theorem 1.1.10. *Let A be an $n \times n$ matrix over a field $\mathbb{K}$ such that any eigenvalue of A is contained in $\mathbb{K}$, then there exists J defined over $\mathbb{K}$ in Jordan canonical form such that J is similar to A.*

1.1.2 Boolean functions terminology

Definition 1.1.11. *A* **Boolean function** *(B.f.) is a function $f : \mathbb{F}^n \to \mathbb{F}$. The set of all Boolean functions from $\mathbb{F}^n$ to $\mathbb{F}$ will be denoted by $\mathcal{B}_n$.*

Each Boolean function $f \in \mathcal{B}_n$ can be written in as unique way as a polynomial in $\mathbb{F}[X] = \mathbb{F}[x_1, \ldots, x_n]$.

$$f(X) = \sum_{S \subseteq [n]} a_S X_S,$$

where $X_S = \prod_{i \in S} x_i$. Such a representation is said **Algebraic Normal Form** (ANF).

The **algebraic degree** of a B.f. f coincides with the degree of its ANF

$$\deg(f) = \max\{|S| : a_S \neq 0\}.$$

Let $\mathcal{A}_n$ be the set of all affine functions from $\mathbb{F}^n$ to $\mathbb{F}$, i.e. the set of the Boolean functions in $\mathcal{B}_n$ with algebraic degree less than or equal to 1. The ANF of an affine function $\alpha \in \mathbf{A}_n$ is

$$\alpha = \sum_{i=1}^{n} a_i x_i + a_0.$$

Let $\mathbb{F}_2^n$ be labelled as $\mathbb{F} = \{v_1, \ldots, v_{2^n}\}$ we can associate to a B.f. f the vector $\bar{f} = (f(v_1), \ldots, f(v_{2^n})) \in \mathbb{F}^{2^n}$, $\bar{f}$ is called the **value vector** of f.

The distance between two B.f.'s $f, g \in \mathcal{B}_n$ is the Hamming distance between their value vectors, namely

$$d(f, g) = |\{i \mid f(v_i) \neq g(v_i)\}|.$$

Definition 1.1.12. *Let $f \in \mathcal{B}_n$. The* **non-linearity** *of f is the minimum of the distance between f and any affine function*

$$N(f) = d(f, \mathcal{A}_n).$$

Theorem 1.1.13 (Covering radius bound)**.** $N(f) \leq 2^{n-1} - \frac{1}{2}2^{n/2}$.

Definition 1.1.14. *A B.f. f is called* **bent** *if $N(f) = 2^{n-1} - \frac{1}{2}2^{n/2}$.*

Bent functions can exist only if n is even, as $2^{n-1} - \frac{1}{2}2^{n/2}$ has to be an integer.

Definition 1.1.15. *A B.f.* $f : \mathbb{F}^n \to \mathbb{F}$ *is called* **balanced** *if* $|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$.

Definition 1.1.16. *A function* $f : \mathbb{F}^n \to \mathbb{F}^m$ *is called* **vectorial Boolean function** *(v.B.f).*

We focus on the case $m = n$. In this case we can, also, identify a v.B.f. with a univariate polynomial over $\mathbb{F}_{2^n}$, since $\mathbb{F}_2^n$ is isomorphic to $\mathbb{F}_{2^n}$ as vector spaces over $\mathbb{F}$.

Theorem 1.1.17 ([LN97])**.** *If* $\mathbb{F}_q$ *is a finite field and* $f : \mathbb{F}_q \to \mathbb{F}_q$ *is a function, then* f *can be represented by a polynomial* $f \in \mathbb{F}_q[x]$ *with* $\deg(f) \leq q - 1$.

Let f be a v.B.f, we denote by $f_{\mathbf{v}}$ the components relating to $\mathbf{v} \in \mathbb{F}^n$, that is the function $x \mapsto < \mathbf{v}, f(x) >$ ($< \mathbf{u}, \mathbf{v} >$ is usual scalar product). Clearly, each component is a Boolean function. The degree of a vectorial Boolean function is the maximum degree of its components:

$$\deg(f) = \max_{\mathbf{v} \in \mathbb{F}_2^n} \deg(f_{\mathbf{v}}).$$

With $n_i(f)$ we denote the number of components of f with degree i.

We can now extend the notion of non-linearity to the vectorial Boolean functions and give the first measure of non-linearity for an S-Box.

Definition 1.1.18. *Let* f *be a v.B.f., the non-linearity of* f *is*

$$N(f) = \min_{\mathbf{v} \in \mathbb{F}^n} N(f_{\mathbf{v}}).$$

Definition 1.1.19. *A v.B.f.* $f : \mathbb{F}^n \to \mathbb{F}^m$ *is called* **balanced** *if for all* $v_1, v_2 \in \mathbb{F}^m$ $|f^{-1}(v_1)| = |f^{-1}(v_2)| = 2^{n-m}$.

Remark 1.1.20. A v.B.f. f is balanced if and inky if all components are balanced. In particular a permutation is always balanced.

Here we report other more measures of non-linearity. Let $\hat{f}_u(x) := f(x+u) + f(x)$ be the **derivative** of f w.r.t. u.

Definition 1.1.21. *Let* $m, n \geq 1$. *Let* $f : \mathbb{F}^m \to \mathbb{F}^n$, *for any* $a \in \mathbb{F}^m$ *and* $b \in \mathbb{F}^n$ *we define*

$$\delta_f(a, b) = |\{x \in \mathbb{F}^m \mid \hat{f}_a(x) = b\}|.$$

The **differential uniformity** *of* f *is*

$$\delta(f) = \max_{\substack{a \in \mathbb{F}^m,\, b \in \mathbb{F}^n \\ a \neq 0}} \delta_f(a, b).$$

f *is said* δ-differentially uniform *if* $\delta = \delta(f)$.

The smaller is δ, the highest is the non-linearity of the function. From this point of view the best S-Boxes are those which realize $\delta = 2$, the so called **Almost Perfect Non-linear** (APN) functions. In odd dimension there exist APN functions, which are also permutations. As regards even dimension only for the case $n = 6$ we have examples of APN permutations and no APN permutation over $\mathbb{F}^4$ exists. The case $n \geq 8$ is still open.

Definition 1.1.22. *Let f be a v.B.f. f is* **weakly-δ differentially uniform** *if*

$$|\mathrm{Im}(\hat{f}_a)| > \frac{2^{n-1}}{\delta}, \quad \forall\, a \in \mathbb{F}^n \setminus \{0\}.$$

If f is weakly-2 differential uniform, it is called **weakly-APN**.

Remark 1.1.23. Weakly-APN permutations exist for any $n \geq 3$, e.g. the inversion function $x \mapsto x^{-1}$.

Remark 1.1.24. Let f be a v.B.f. If f is δ-differentially uniform then f is weakly δ-differential uniform.

Definition 1.1.25. *A function f is l-***anti-invariant** *if for any subspace $U \subseteq \mathbb{F}_2^n$ such that $f(U) = U$ we have $\dim(U) < n - l$ or $U = \mathbb{F}_2^n$.*

Definition 1.1.26. *A function f is* **strongly l-anti-invariant** *if for any two subspaces $U, W \subseteq \mathbb{F}_2^n$ such that $f(U) = W$ then either $\dim(U) = \dim(W) < n - l$ or $U = W = \mathbb{F}_2^n$.*

Definition 1.1.27. *Let f be a v.B.f, then*

$$\hat{n}(f) := \max_{a \in \mathbb{F}_2^n \setminus \{0\}} |\{\mathbf{v} \in \mathbb{F}_2^n \setminus \{0\} \mid \deg(< \mathbf{v}, \hat{f}_a >) = 0\}|.$$

Remark 1.1.28. For $n = 4$, $\hat{n}(f) = 0$ is a sufficient condition to guarantee f weakly-APN. As we will see it is not true in general.

Definition 1.1.29. *Two permutations $f, g : \mathbb{F}^n \to \mathbb{F}^n$ are* **affine equivalent** *if there exist two $\gamma_1, \gamma_2 \in \mathrm{AGL}(V)$ such that $g(x) = \gamma_1 f \gamma_2(x)$. Those properties which are invariant under the action of the affine group are called* **affine-invariant**.

The following characteristics are affine-invariant:

- Non-linearity,
- Algebraic degree,
- Differential uniformity,
- Weakly differential uniformity
- $\hat{n}(f)$.

1.2 Introduction to Block ciphers

Block ciphers form an important class of cryptosystems in symmetric key cryptography. Stream ciphers ([Rue92]) form another class. Here we are interested only in cryptosystems of type block cipher. These are algorithms that encrypt and decrypt block of data according to a shared secret key. They are commonly used to provide confidentiality during information transmission and storage. We can formally describe such a system using the following definition.

Definition 1.2.1. *A cryptosystem is a pair $(\mathcal{M}, \mathcal{K})$, where:*

- *$\mathcal{M}$ is a finite set of possible messages (plaintext, ciphertext);*
- *$\mathcal{K}$ is a finite set of possible keys;*
- *for any $k \in \mathcal{K}$ we have an encryption and decryption functions*

$$\varphi_k : \mathcal{M} \to \mathcal{M}, \quad \psi_k : \mathcal{M} \to \mathcal{M}, \quad \varphi_k, \psi_k \in \mathrm{Sym}(\mathcal{M})$$

such that $\psi_k = \varphi_k^{-1}$.

Following the most used structure in modern ciphers, in the previous definition the plaintext space coincides with the ciphertext space. W.l.o.g., we can consider $\mathcal{M} = \mathbb{F}_q^r$ and $\mathcal{K} = \mathbb{F}_q^l$, with $l \geq r \geq 1$, and we adapt our previous definition.

Definition 1.2.2. *Let r and l be natural numbers. Let φ be any function*

$$\varphi : \mathbb{F}_q^r \times \mathbb{F}_q^l \to \mathbb{F}_q^r.$$

For any $k \in \mathbb{F}_q^l$, we denote by φ_k the function

$$\varphi_k : \mathbb{F}_q^r \to \mathbb{F}_q^r, \quad \varphi_k(x) = \varphi(x, k).$$

We say that φ is an **algebraic block cipher** *if φ_k is a permutation of $\mathbb{F}_q^r$ for all key $k \in \mathbb{F}_q^l$.*

Under this conditions, we can also consider a block cipher as an indexed set of permutations $\mathbb{F}_q^l \to \mathrm{Sym}(\mathbb{F}_q^r)$. Any key $k \in \mathcal{K}$ induces a permutation φ_k on $\mathcal{M}$. Since $\mathcal{M}$ is usually $V = \mathbb{F}^r$ for some $r \in \mathbb{N}$, we can consider $\varphi_k \in \mathrm{Sym}(V)$.

Most modern block ciphers are iterated ciphers, i.e. they are obtained by the composition of a finite number N of rounds.

In each round (except possibly for a couple, which may be slightly different) the iterated ciphers perform a non-linear substitution operation (or S-box) on disjoint parts of the input that provide "confusion", followed by a permutation (usually a

linear transformation) on the whole data that provide "diffusion". A cryptosystem reaches "confusion" if the relationship between plaintext, ciphertext and key is very complicated. The "diffusion" idea consists of spreading the influence of all part of the input (plaintext and key) to all parts of the ciphertext. The operation performed in a a round form the **round function**. The round function at the j-th round ($1 \leq j \leq N$) takes as inputs both the output of the $(j-1)$-th round and the subkey $k^{(j)}$ (also called **round-key**). Any round key $k^{(j)}$ is constructed starting from a (session key) master key k (nowadays we have $2^{64} \leq |\mathcal{K}| \leq 2^{256}$). The **key schedule** is a public algorithm (strictly dependent on the cipher) which constructs $N+1$ subkeys $(k^{(0)}, \ldots, k^{(N)})$.

Several independent formal definitions have been proposed for an iterated block cipher, e.g. *substitution permutation network* [Sti95] and *key-alternating block cipher* [DR02a]. Here we present one more recent definition [CDS09b] that define a class large enough to include some common ciphers (AES, SERPENT, PRESENT), but with enough algebraic structure to allow for security proofs.

Let $V = \mathbb{F}_2^r$ with $r = mb$, $b \geq 2$. The vector space V is a direct sum

$$V = V_1 \oplus \cdots \oplus V_b,$$

where each V_i has the same dimension m (over $\mathbb{F}_2$). For any $\mathbf{v} \in V$, we will write $\mathbf{v} = \mathbf{v}_1 \oplus \ldots \mathbf{v}_b$, where $\mathbf{v}_i \in V_i$. Also, we consider the projections $\pi_i : V \to V_i$ mapping $\mathbf{v} \mapsto \mathbf{v}_i$.

Any $\gamma \in \mathrm{Sym}(V)$ that acts as $\mathbf{v}\gamma = \mathbf{v}_1\gamma_1 \oplus \cdots \oplus \mathbf{v}_b\gamma_b$, for some $\gamma_i \in \mathrm{Sym}(V_i)$, is a **bricklayer transformation** (a "parallel map") and any γ_i's is a **brick**. Traditionally, the maps γ_i's are called $S-boxes$ and γ a "parallel S-box". A linear map $\lambda : V \to V$ is traditionally said a "Mixing Layer" when used in composition with parallel maps. We denote by $\sigma_{\mathbf{v}}$ the translation by $\mathbf{v} \in V$, namely $\mathbf{x}\sigma_{\mathbf{v}} = \mathbf{x} + \mathbf{v}$.

For any $I \subset [b]$, with $I \neq \emptyset, [b]$, we define $\bigoplus_{i \in I} V_i$ a **wall**.

Definition 1.2.3. *A linear map $\lambda \in \mathrm{GL}(V)$ is a* **proper mixing layer** *if no wall is invariant under λ.*

We can characterize the translation-based class by the following:

Definition 1.2.4. *A block cipher $\mathcal{C} = \{\varphi_k \mid k \in \mathcal{K}\}$ over $\mathbb{F}_2$ is called* **translation based (tb)** *if:*

- *it is the composition of a finite number of rounds, such that any round $\rho_{k,h}$ can be written*[1] *as $\gamma\lambda\sigma_{\bar{k}}$, where*
  - *γ is a round-dependent bricklayer transformation (but it does not depend on k),*

[1] *we drop the round indices*

- *λ is a round-dependent linear map (but it does not depend on k),*
- *$\bar{k}$ is in V and depends on both k and the round ($\bar{k}$ is called a "round key"),*

- *for at least one round we have (at the same time) that λ is proper and that the map $\mathcal{K} \to V$ given by $k \mapsto \bar{k}$ is surjective, (a "proper" round).*

Remark 1.2.5. A generalization is obtained by allowing a key-independent permutation at the beginning and/or another at the end. This is the case for example for the SERPENT cipher. Since these permutations have no influence on the cryptanalysis of a cipher, we implicitly ignore them.

Remark 1.2.6. A round consisting of only a translation is still acceptable, by assuming $\gamma = \lambda = 1_V$ (the identity map on V), although obviously it is not proper. Indeed, from now on we can always assume that the first round is of this kind, otherwise we can remove its γ and λ (Remark 1.2.5). Then, we can also assume that $0\gamma = 0$, since we can add 0γ to the round key of the previous round.

Remark 1.2.7. To allow affine mixing layers, rather than linear mixing layers, seems a generalization. However, this case is indeed already present in Definition 1.2.4, since it is enough to change $\sigma_{\mathbf{v}}$ to incorporate the "translation part" of the mixing layer.

1.2.1 Perfect secrecy

Shannon, several decades ago, in [Sha49] formalized the concept of *perfect secrecy*. The *perfect ciphers* (e.g. One Time Pad) are ciphers with a very strong model because one assumes that Eve's computational power is infinite. They are impractical for a real use, as they require at least as many key bits as the message length. Consider[2] the set of plaintexts $\mathcal{P}$ and ciphertexts $\mathcal{C}$, and assume that a particular key $k \in \mathcal{K}$ is used for only one encryption $p \mapsto \varphi_k(p)$. Let X be the random variable defined by the plaintexts and Y be the random variable defined by the ciphertexts.

Definition 1.2.8. *A crypto-system is said to have the property of perfect secrecy if, for all $p \in \mathcal{P}$ and $c \in \mathcal{C}$, the two probability distributions satisfy*

$$Pr(X = p|Y = c) = Pr(X = p).$$

Perfect secrecy means that the *a posteriori* distribution of the plaintext p after viewing the ciphertext c is identical to the *a priori* distribution of the plaintext.

Theorem 1.2.9. *Suppose that $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. A cryptosystem provides perfect secrecy if and only if every key is used with equal probability $1/|\mathcal{K}|$ and the action of $\{\varphi_k \mid k \in \mathcal{K}\}$ on $\mathcal{P} = \mathcal{C}$ is a regular action.*

[2] In this case the two spaces may not be the same

1.2.2 "Good" block cipher

Up to now, there is no received definition of "good block cipher", but there are several criteria that contribute to the evaluation of a cipher. We list some of them.

Security

The most important criterion in the evaluation of a block cipher consists of estimating its security level. Obviously, the security of a block cipher is highly dependent on the properties of the different components:

- substitution layer consisting of a number of highly non-linear S-boxes (which are v.B.f.'s, see [Car06]),
- affine or linear invertible transformations.

However, there is no mathematical method to prove the security of a given block cipher, although it is sometimes possible to prove the insecurity of such a cipher. What usually happens is that a relative measure of the security of a block cipher (for instance the K-security in [DR02b]) is given. Some necessary requests on the ciphers are made and it is a very hard problem to determine the sufficient conditions that guarantee the security. To evaluate the security, an additional concept is often considered: practical security. According to this concept, a block cipher is considered secure if the best-known attack requires too many resources by a suitable and acceptable margin. One can test the block cipher with different known attacks and assign a certain security level to it. Obviously, it is impossible to predict the security of the underlying block cipher with respect to yet unknown attacks.

Efficiency

It refers to the amount of resources required to perform φ or ψ. In fact, in software implementations the speed of φ/ψ and the required amount of working memory/memory storage are relevant. When quoting the speed of a cipher, one often makes the silent assumption that a large amount of data is encrypted with the same key. In that case, the key schedule can be neglected. However, if a cipher key is used to secure only a few messages, the amount of cycles taken by the computation of the key-schedule becomes important. The ability to efficiently change keys is called key agility. Block ciphers are often used to encrypt large amounts of data; this makes data throughput an important evaluation criterion as well. One often differentiates hardware and software cases, the speed of the algorithm setup, the key setup, a key change and the encryption and decryption operations.

Flexibility

An expected important property of a block cipher is that it offers a large flexibility. For instance, a flexible algorithm may offer several possible block and key sizes, allowing to tailor an instance of the block cipher to precise external requirements. Another

flexibility form concerns implementation issues. Finally, a block cipher can be used as a building block in various cryptographic constructions (like a hash function, an authentication code, or a stream cipher); if it offers an acceptable security level in all of these situations, then one can consider that it is a flexible block cipher.

1.2.3 Cryptanalytic scenarios

Traditionally, the goal of Eve consists of recovering the plaintext or even the key. According to the possibilities and the capabilities of Eve, we can classify the different modes of attack (from the most practical to the most hypothetical, or equivalently, from the least powerful to the most powerful) as follows:

- *Ciphertext-only*: Eve tries to deduce some information about the key (or about the plaintext) starting from the sole knowledge of several ciphertexts and, usually, assuming some properties about the distribution of the plaintexts. This is a very unlikely scenario for modern block ciphers.

- *Known-plaintext*: in this kind of attack, we assume that Eve knows a certain amount of (plaintext,ciphertext) pairs in order to recover the key. This is a realistic scenario and there are two types. The first where Eve can observe encrypted version of well-known data and, for instance, exploit the fact that messages have redundancy. The second type assumes that the collected plaintexts form a random sample. Linear cryptanalysis [Mat94] is a typical example of such an attack.

- *Chosen-plaintext or chosen-ciphertext*: when performing this kind of attack, Eve is able to choose plaintexts and obtain the corresponding ciphertexts. Subsequently, Eve uses any information deduced in order to recover either the key, or plaintexts corresponding to previously unseen ciphertexts. A typical example is differential cryptanalysis [AC09].

- *Adaptive chosen-plaintext or ciphertext*: such an attack consists of a chosen-plaintext (or chosen-ciphertext) attack wherein the choice of the plaintext (or ciphertext) depends on the information learned during the attack.

- *Combined chosen-plaintext and chosen-ciphertext*: this is a powerful type of adaptive attack which assumes that Eve can encrypt and decrypt arbitrary messages as she desires. A typical example of such an attack is Wagner's boomerang attack (see [Wag99]).

- *Related-key*: in this model, Eve knows (or can choose) additionally some mathematical relations between the keys used for encryption, but not their values.

This is usually employed in conjunction with some of the scenarios above. Even if in itself this attack may not be considered to be a practical threat against a block cipher (because it lives in a too strong threat model), it may be practical when a block cipher is used as a primitive for a hash function.

By considering one of the attacks described above and according to the type of information recovered during it, the possible outcomes of an attack could be classified as follows. We describe only the main outcomes from the least favorable for Eve to the most favorable. (For more details, see e.g. Knudsen [Knu99]).

- *Distinguishing attack*: Eve is able to tell whether the attacked block cipher is a permutation (chosen uniformly at random from the set of all permutations) or one of the permutations $\{\varphi_k\}_{k\in\mathcal{K}}$. In fact, most modern block ciphers are designed to model a random permutation. Even if distinguishing attacks are considered as the least serious threat in practice, they often indicate some structural weaknesses of the cipher and they might be transformed into a Key recovery (or a Global deduction).

- *Local deduction*: Eve finds the plaintext (or ciphertext) of an intercepted ciphertext (or plaintext) which she did not obtain from the legitimate sender. If the number of likely plaintexts (or ciphertexts) is small, such an attack may be fatal for the cryptosystem.

- *Partial Key Recovery*: Eve is able to get some information on the key k (e.g. some relations, some bits). An efficient partial key recovery is very undesirable because it could be used to determine the remaining bits of the key.

- *Global deduction*: Eve finds an algorithm functionally equivalent to φ_k or ψ_k, without knowing the actual value of the key k. For instance, a possibility of global deduction is when an attacker is able to recover the round subkeys but not the key. A more dangerous case is when the encryption function is actually linear, allowing the deduction of the matrix representing the encryption (and then its inverse will represent the decryption). A historical example is Hill's cipher.

- *Key recovery* (Total break): Eve is able to recover (or reconstruct) the secret key $k \in \mathcal{K}$, thus reaching the highest goal of the attacker.

The security of a cipher against the types of attack described above is in practice measured by several additional parameters that are necessary:

- *time complexity*: it measures the computational processing required to perform an attack, i.e. it is closely related to the input. Usually, the choice of the computational unit is done to compare the attack with an exhaustive key search.
- *data complexity*: it is the number of collected data (like ciphertexts, (known/-chosen)-plaintext,...) required to perform an attack, according to a specific model.
- *success probability*: it measures the frequency at which the attack is successful when repeated a certain number of times in a statistically independent way.
- *memory complexity*: it measures the amount of memory units necessary to store pre-computed/obtained data necessary to perform the attack.

Usually, an attack is considered to be successful (and the attacked block cipher is considered to be broken) if the time/data/memory complexity is significantly smaller than 2^l evaluations of the block ciphers, with $\mathcal{K} = \mathbb{F}^l$, and a success probability close to 1.

1.2.4 Trapdoors

A **trapdoor** is a hidden structure of the cipher; knowledge of this structure allows an attacker to obtain information on the key or to decrypt certain ciphertexts. The discussion of trapdoor issues in symmetric cryptographic papers has been one-sided for a long time. In particular, it was directed towards looking for trapdoors in ciphers that had already been designed. Rijmen and Preneel [RP97] proposed for the first time a family of trapdoor block ciphers. As defined in [RP97] a **full trapdoor** is some secret information which allows an attacker to obtain knowledge on the key (or a global deduction) by using a very small number of known plaintexts, no matter what these plaintexts are or what the key is. A **partial trapdoor**, is a trapdoor that not necessarily work for all keys, or that give an attacker only partial information on the key. Moreover, a trapdoor is said to be **detectable (undetectable)** if it is computationally feasible (infeasible) to find it even if one knows the general form of the trapdoor.

In [RP97] the authors constructed a cipher within a partial trapdoor. In this family of ciphers, a trapdoor is hidden in S-boxes and it was claimed to be undetectable for properly chosen parameters. Given the trapdoor, the secret key (used for encryption and decryption) can be recovered easily by applying Matsuis linear cryptanalysis [Mat93]. Interestingly, the work of [WBDY98] shows that these trapdoors are either easily detected or yield only attacks requiring an infeasible number of plaintext/ciphertext pairs. A full trapdoor is given in [Pat99], but Paterson claim that it is also

detectable. This trapdoor is based on the imprimitive action of the round functions group of the block cipher.

1.3 Group theoretic properties

Let $\mathcal{C}$ be a tb cipher, whit the plaintext space $V = \mathbb{F}^d$, for some $d \in \mathbb{N}$.

$$\mathcal{C} = \{\varphi_k \mid k \in \mathcal{K}\}$$

It would be very interesting to determine the group $\Gamma(\mathcal{C}) = \langle \varphi_k \mid k \in \mathcal{K} \rangle \subseteq \mathrm{Sym}(V)$ generated by the permutations φ_k. Unfortunately, for many classical cases (e.g. AES [DR99], SERPENT [ABK98], DES [Nat77]) this appears to be a difficult problem. However, more manageable overgroups of Γ have been investigated (see [Wer93, HSW94, Wer02, SW08]), such as the ones that we now define. Define the groups for each h

$$\Gamma_h(\mathcal{C}) = \langle \varphi_{k,h} \mid k \in \mathcal{K} \rangle \subseteq \mathrm{Sym}(V),$$

here $\varphi_{k,h} = \lambda_h \gamma_h \sigma_{h,k}$ is the round function, and the group

$$\Gamma_\infty(\mathcal{C}) = \langle \Gamma_h(\mathcal{C}) \mid h = 1, \ldots, l \rangle.$$

For a given cipher, it is an interesting problem to determine $\Gamma_\infty(\mathcal{C})$, that is the permutation group generated by its round functions (with the key varying in the key space), since this group might reveal weaknesses of the cipher. Paterson [Pat99], as said before, showed that if this group is imprimitive, then it is possible to embed a trapdoor in the cipher.

We give the idea of the basic (chosen-plaintext) attack of Paterson. Let $X_1, \ldots, X_r$ be a complete non-trivial block system for the group Γ_∞. Suppose further that, given $m \in V$, there is a description of the blocks such that it is easy to compute the i with $m \in X_i$. Choose one plaintext m_i in each set X_i and obtain the corresponding ciphertext c_i. Then the effect of φ_k on each block X_i is determined. From the imprimitivity of Γ_∞,

$$c_i = m_i \varphi_k \in X_j \Rightarrow X_i \varphi_k = X_j.$$

Now given any further ciphertext c, we compute l such that $c \in X_l$. Then, we can find the plaintext m of c examining the block X_i corresponding to X_l. Then the plaintext m corresponding to c satisfies $m \in X_l {\varphi_k}^{-1}$. Thus r chosen plaintexts determine that the message corresponding to any ciphertext must lie in a set of size $\frac{|V|}{r}$. Hence the security of the system is severely compromised. The plaintext m itself can be found by examining the set of meaningful message $X_l {\varphi_k}^{-1}$.

Paterson give this trapdoor for a DES-like cipher, but it can be extended to the case of tb ciphers.

For a tb cipher, in [CDS09b] the authors provided conditions on the S-boxes which ensure that the group Γ_∞ is primitive.

Theorem 1.3.1 ([CDS09b])**.** *Let $\mathcal{C}$ be a tb cipher, with h a proper round, and $1 \leq r < m/2$. If any brick of γ_h is:*

(1) weakly $2r$-uniform and

(2) strongly r-anti-invariant,

then $\Gamma_h(\mathcal{C})$ is primitive (and hence $\Gamma_\infty(\mathcal{C})$ is primitive).

A cipher may be regarded as having a weakness, also if this group is small in size, since not every possible permutation of the message space can be realized by the cipher[CG75, EG83]. Attacks on ciphers whose encryptions generate small groups were given in [KJRS88].

Caranti *et al.* in [CDS09a] established some extra conditions on S-boxes of a tb cipher such that $\Gamma_\infty(\mathcal{C})$ is either $\mathrm{Alt}(V)$ or $\mathrm{Sym}(V)$, obtaining the following theorem.

Theorem 1.3.2 ([CDS09a])**.** *Let $d = mn$, with $m, n > 1$. Let $\mathcal{C}$ be a tb cipher such that*

(1) $\mathcal{C}$ satisfies the hypothesis of Theorem 1.3.1, and

(2) for all non-zero $a \in V_i$, $\mathrm{Im}(\hat{\gamma}_{ia})$ is not a coset of a subspace of V_i.

Then the group $\Gamma_\infty(\mathcal{C})$ is either $\mathrm{Alt}(V)$ or $\mathrm{Sym}(V)$.

However the ability of a cipher (or its round functions) to generate a large group does not alone guarantee security: an example of a weak cipher generating the symmetric group is given in [MPW94].

Hidden sums

In [Li03], Li observed that if V is a vector space over a finite field $\mathbb{F}_p$, the symmetric group $\mathrm{Sym}(V)$ will contain many isomorphic copies of the affine group $\mathrm{AGL}(V)$, which are its conjugates in $\mathrm{Sym}(V)$. As we will see below, there are several structures $(V, \circ)$ of a $\mathbb{F}_p$-vector space on the set V , where $(V, \circ)$ is the abelian additive group of the vector space. Each of these structure will yield in general a different copy $\mathrm{AGL}(V, \circ)$ of the affine group within $\mathrm{Sym}(V)$. In particular the result of Li is the following theorem, which is a particular case of the O'Nan-Scott theorem.

Theorem 2.0.3 ([Li03])**.** *Let G be a primitive group of degree p^b, with $b > 1$. Suppose G contains a regular abelian subgroup T. Then G is one of the following.*

(1) Affine, $G \subseteq \mathrm{AGL}(e, p)$, for some prime p and $e \geq 1$.

(2) Wreath product, that is

$$G \cong (S_1 \times \cdots \times S_t).O.P,$$

with $p^b = c^t$ for some c and $t > 1$.Here $T = T_1 \times \cdots \times T_t$, with$T_i \subseteq S_i$ and $|T_i| = c$ for each i, $S_1 \cong \ldots \cong S_t$, $O \subseteq \mathrm{Out}(S_1) \times \cdots \times \mathrm{Out}(S_t)$, P permutes transitively the S_i, and one of the following holds:

(i) $(S_i, T_i) = (PSL_2(11), \mathbb{Z}_{11})$, $(S_i, T_i) = (M_{11}, \mathbb{Z}_{11})$, $(S_i, T_i) = (M_{23}, \mathbb{Z}_{23})$;

(ii) $S_i = \mathrm{Sym}(c)$ or $\mathrm{Alt}(c)$, and T_i is an abelian group of order c.

(3) Almost simple, that is, $S \leq G \leq \mathrm{Aut}(S)$, for a non-abelian simple group S.

Here the notation $S.T$ denotes an extension of the group S by the group T.

We refer to these structures $(V, \circ)$ as **hidden sums**. Note that if h is a proper round of a tb cipher $\mathcal{C}$, then $\Gamma_h(\mathcal{C}) = \langle \lambda_h \gamma_h, T(V) \rangle$, where $T(V)$ is the translation group. Thus it could be that Γ_∞ is contained in a isomorphic copy of $\mathrm{AGL}(V)$, if it happens the abelian additive group $(V, \circ)$ is said a **hidden sum trapdoor**.

In this chapter we characterize the translation and affine group related to a hidden sum, in particular we focus on translation groups generated by affine maps. In Section 2.4 we explain why this case is more interesting. Moreover, always, in Section 2.4 we give an example of a toy-cipher with a hidden sum trapdoor.

2.1 On affine groups of hidden sums

In the following, if not specified, V will be an n dimensional vector space over $\mathbb{F}$ and p a prime number.

With the symbol $+$ we refer to the usual sum over the vector space V, and we denote by T_+, $\mathrm{AGL}(V,+)$ and $\mathrm{GL}(V,+)$, respectively, the translation, affine and linear groups w.r.t. $+$.

Remark 2.1.1. An elementary group acting on $V = \mathbb{F}_p^n$ is obviously a p-elementary group. The translation group of V is an elementary abelian regular group. Vice versa, we claim that if T is an elementary abelian regular group, there exists a vector space structure $(V,\circ)$ such that T is the related translation group. In fact, from the regularity of T we have $T = \{\tau_{\mathbf{a}} \mid \mathbf{a} \in V\}$ where $\tau_{\mathbf{a}}$ is the unique map in T such that $0 \mapsto \mathbf{a}$. Then, defining the sum $\mathbf{x} \circ \mathbf{a} := \mathbf{x}\tau_{\mathbf{a}}$, it is easy to check that $(V,\circ)$ is an additive group. Moreover, let the multiplication of a vector by an element of $\mathbb{F}_p$ defined by

$$s\mathbf{v} := \underbrace{\mathbf{v} \circ \cdots \circ \mathbf{v}}_{s}, \text{ for all } s \in \mathbb{F}_p,$$

then it is easy to check that for all $s,t \in \mathbb{F}_p$, and $\mathbf{v},\mathbf{w} \in V$

$$s(\mathbf{v} \circ \mathbf{w}) = s\mathbf{v} \circ s\mathbf{w},$$

$$(s+t)\mathbf{v} = s\mathbf{v} \circ t\mathbf{v},$$

$$(st)\mathbf{v} = s(t\mathbf{v})$$

and being T elementary $p\mathbf{v} = 0$. Thus $(V,\circ)$ is a vector space over $\mathbb{F}_p$. Observe that $(V,\circ)$ and $(V,+)$ are isomorphic vector space (since $|V| < \infty$).

For abelian regular subgroups of the affine group in [CDS06] the authors give an easy description of these in terms of commutative associative algebras that one can impose on the vector space $(V,+)$. We report the principal result shown in [CDS06]. Recall that a (Jacobson) radical ring is a ring $(V,+,\cdot)$ in which every element is invertible with respect to the circle operation $\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \mathbf{y} + \mathbf{x} \cdot \mathbf{y}$, so that $(V,\circ)$ is a group. The circle operation may induce a vector space structure on V or not.

Theorem 2.1.2. *Let $\mathbb{K}$ be any (finite or infinite) field, and $(V,+)$ a vector space of any dimension over $\mathbb{K}$.*

There is a one-to-one correspondence between

1 *(not necessarily elementary) abelian regular subgroups T of $\mathrm{AGL}(V,+)$, and*

2 *commutative, associative $\mathbb{K}$-algebra structures $(V,+,\cdot)$ that one can impose on the vector space structure $(V,+)$, such that the resulting ring is radical.*

In this correspondence, isomorphism classes of $\mathbb{K}$*-algebras correspond to conjugacy classes of abelian regular subgroups of* $\mathrm{AGL}(V,+)$*, where the conjugation is under the action of* $\mathrm{GL}(V,+)$.

We do not report their proof, but we write explicitly the correspondence, as follows.

Let $T = \{\tau_{\mathbf{a}} \mid \mathbf{a} \in V\}$, any $\tau_{\mathbf{a}} \in T$ can be written as $\tau_{\mathbf{a}} = \kappa\sigma$ with $\kappa \in \mathrm{GL}(V)$ and $\sigma \in T_+$. Then for all $\mathbf{a} \in V$ we consider the map $\delta_{\mathbf{a}} = \kappa - 1_V$, with κ as before. The product operation on V defined by $\mathbf{x} \cdot \mathbf{a} = \mathbf{x}\delta_{\mathbf{a}}$ is such that the structure $(V, +, \cdot)$ results a commutative $\mathbb{K}$-algebra and the resulting ring is radical.

Remark 2.1.3. From the theorem above we can note that in characteristic 2, algebras corresponding to *elementary* abelian regular subgroups of $\mathrm{AGL}(V,+)$ are exterior algebras or a quotient thereof, without the part of 0 degree. Indeed, algebras related to elementary groups are such that $\mathbf{x}^2 = 0$ for all $\mathbf{x} \in V$ and the exterior algebra is the universal objet with that characteristic. We do not consider the part of degree 0, because the algebras have to be nilpotent and -1 would have no inverse w.r.t. $\circ$, as $-1 \circ \mathbf{a} = -1$ for all $\mathbf{a} \in V$.

We recall that $\sigma_{\mathbf{a}}$ denotes the translation in T_+ such that $\mathbf{x} \mapsto \mathbf{x} + \mathbf{a}$. We will use $T_\circ$ and $\mathrm{AGL}(V, \circ)$ to denote the translation and affine group corresponding to a hidden sum $\circ$, that is when $(V, \circ)$ is a vector space and so $T_\circ$ is elementary abelian and regular.
As noted in the remark above, since $T_\circ$ is regular, for each $\mathbf{a} \in V$ there is a unique map $\tau_{\mathbf{a}} \in T_\circ$ such that $0 \mapsto \mathbf{a}$. Thus

$$T_\circ = \{\tau_{\mathbf{a}} \mid \mathbf{a} \in V\}.$$

The relation between $T_\circ$ and $\mathrm{AGL}(V, \circ)$ is that $\mathrm{AGL}(V, \circ)$ is the normalizer of $T_\circ$ in $\mathrm{Sym}(V)$. Indeed, $\mathrm{AGL}(V,+)$ is the normalizer of T_+ and they are, respectively, the isomorphic images of $\mathrm{AGL}(V, \circ)$ and $T_\circ$.

With 1_V we will denote the identity map of V, clearly, $1_V \in \mathrm{AGL}(V, \circ)$ for any $\circ$.

Remark 2.1.4. If $T_\circ \subseteq \mathrm{AGL}(V,+)$, being the semi direct product $\mathrm{AGL}(V,+) = \mathrm{GL}(V,+) \ltimes T_+$, then $\tau_{\mathbf{a}}$ can be written as $\kappa\sigma_{\mathbf{b}}$ for one $\kappa \in \mathrm{GL}(V,+)$ and one $\mathbf{b} \in V$. From $0\tau_{\mathbf{a}} = \mathbf{a}$ we have $\mathbf{b} = \mathbf{a}$. We can denote by $\kappa_{\mathbf{a}}$ the map κ corresponding to $\tau_{\mathbf{a}}$ and by $\Omega(T_\circ) = \{\kappa_{\mathbf{a}} \mid \mathbf{a} \in V\} \subset \mathrm{GL}(V,+)$.

Let $T \subseteq \mathrm{AGL}(V,+)$ and define the set

$$U(T) = \{\mathbf{a} \mid \tau_{\mathbf{a}} = \sigma_{\mathbf{a}}\}.$$

It is easy to check that $U(T)$ is a subspace of V (whenever T is a subgroup). If $T = T_\circ$ for some operation $\circ$, then $U(T_\circ)$ is not empty for the following lemma.

Lemma 2.1.5 ([CDS06])**.** *Let $T \subseteq \mathrm{AGL}(V,+)$ be a regular subgroup. Then, if V is finite $T_+ \cap T$ is nontrivial.*

In particular we claim our first result:

Proposition 2.1.6. *Let $T \subseteq \mathrm{AGL}(V,+)$ be an elementary abelian regular subgroup. If $T \neq T_+$, then $1 \leq \dim(U(T)) \leq n-2$.*

Proof. From the lemma above we have $1 \leq \dim(U(T))$. If $\dim(U(T)) = n$ then $T = T_+$. Let $T \neq T_+$ and suppose that $U(T)$ contains $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$ linear independent vectors. Let $\mathbf{v}_n$ be a vector linear independent from $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$. Being T elementary abelian regular subgroup, then $T = T_\circ$ for some operation $\circ$. For all $1 \leq i \leq n-1$, $\mathbf{v}_i \circ \mathbf{v}_n = \mathbf{v}_i + \mathbf{v}_n$, thus we have $\mathbf{v}_i \kappa_{\mathbf{v}_n} = \mathbf{v}_i$ for all $1 \leq i \leq n-1$. Moreover, $\mathbf{v}_n \circ \mathbf{v}_n = 0$ implies $\mathbf{v}_n \kappa_{\mathbf{v}_n} = \mathbf{v}_n$. Then for all $\mathbf{v} \in V$ we have $\mathbf{v} \circ \mathbf{v}_n = (\sum_{i<n} \alpha_i \mathbf{v}_i + \alpha_n \mathbf{v}_n)\kappa_{\mathbf{v}_n} + \mathbf{v}_n = \sum_{i<n} \alpha_i \mathbf{v}_i + \alpha_n \mathbf{v}_n + \mathbf{v}_n = \mathbf{v} + \mathbf{v}_n$. This implies $\dim(U(T)) = n$, which leads to a contradiction. □

Let W be a subspace of V, then for all $\gamma \in \mathrm{GL}(V)$ such that $W\gamma = W$, it is well defined the action of γ over V/W, i.e. the map $\bar{\gamma} : [\mathbf{v}] \mapsto [\mathbf{v}\gamma]$ in $\mathrm{GL}(V/W)$.

Lemma 2.1.7. *Let $V = \mathbb{F}_p^n$, with p prime number. Let $T = \langle \tau_{\mathbf{e}_1}, \ldots, \tau_{\mathbf{e}_n} \rangle$ be a subgroup of $\mathrm{AGL}(V,+)$, where $\tau_{\mathbf{e}_i} : \mathbf{x} \mapsto \mathbf{x}\kappa_{\mathbf{e}_i} + \mathbf{e}_i$ for all i, such that*

(1) $\{\kappa_{\mathbf{e}_i} | 1 \leq i \leq n\} \subseteq \mathcal{U}(V)$

(2) the action of $\kappa_{\mathbf{e}_i}$ over $V/\mathrm{Span}\{\mathbf{e}_{i+1}, \ldots, \mathbf{e}_n\}$ is the identity map for all $1 \leq i \leq n$.

Then T is transitive.

Proof. Note that the action of $\kappa_{\mathbf{e}_i}$ over $V/\mathrm{Span}\{\mathbf{e}_{i+1}, \ldots, \mathbf{e}_n\}$ is well defined, and from the conditions (1) and (2) when we apply the map $\tau_{\mathbf{e}_i}$ to a vector $\mathbf{v}$ the first $i-1$ entries of $\mathbf{v}$ do not change.

Consider two vectors $\mathbf{v} = (v_1, \ldots, v_n)$ and $\bar{\mathbf{v}} = (\bar{v}_1, \ldots, \bar{v}_n)$. We will show that there exists $\tau \in T$ such that $\mathbf{v}\tau = \bar{\mathbf{v}}$. We start considering $v_1 \in \mathbb{F}_p$. If v_1 is equal to $\bar{v}_1$ then we continue considering v_2. Otherwise, $\bar{v}_1 = v_1 + c$ for some $c \in \mathbb{F}_p$. So applying $\tau_{\mathbf{e}_1}$ for c times to $\mathbf{v}$ we obtain from the conditions (1) and (2),

$$\mathbf{v}\tau_{\mathbf{e}_1}^c = \mathbf{v}' = (\bar{v}_1, v_2 + c_2, \ldots, v_n + c_n),$$

for some c_i's in $\mathbb{F}_p$.

Now we consider $v_2' = v_2 + c_2$, if it is equal to $\bar{v}_2$ then we move to v_3'. Otherwise, $\bar{v}_2 = v_2' + c'$ for some $c' \in \mathbb{F}_p$ and applying c' times the map $\tau_{\mathbf{e}_2}$ to $\mathbf{v}'$ we obtain

$$\mathbf{v}'\tau_{\mathbf{e}_2}^{c'} = \mathbf{v}'' = (\bar{v}_1, \bar{v}_2, v_3' + c_3' \ldots, v_n' + c_n').$$

Iterating this process we obtain the maps that we have to compose to obtain τ.

□

Corollary 2.1.8. *Let $T = \langle \tau_{\mathbf{e}_1}, \ldots, \tau_{\mathbf{e}_n} \rangle \subseteq \mathrm{AGL}(V, +)$ satisfying the condition* (1) *and* (2) *of Lemma 2.1.7. If T is an elementary abelian subgroup, then T is regular.*

Proof. From Lemma 2.1.7 T is transitive, that implies $|T| \geq |V| = p^n$. Now, T elementary and abelian implies that we can obtain from the composition of $\tau_{\mathbf{e}_1}, \ldots, \tau_{\mathbf{e}_n}$ at most p^n maps. So T is also regular. □

Remark 2.1.9. These last two results imply that if T is an elementary abelian subgroup as above, then $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is a basis of the associated vector space structure $(V, \circ)$. In general the canonical basis may not be a basis w.r.t. a new sum $\circ$.

Example 2.1.10. Let $V = \mathbb{F}^3$ and

$$T_\circ = \langle \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} + (1,0,1), \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} + (0,1,1), 1_V + (1,1,1) \rangle.$$

The translations $\tau_{\mathbf{e}_1}, \tau_{\mathbf{e}_2}, \tau_{\mathbf{e}_3}$ are given by

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} + \mathbf{e}_2, \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} + \mathbf{e}_3.$$

Then $\mathbf{e}_1 \circ \mathbf{e}_2 = \mathbf{e}_1 \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} + \mathbf{e}_2 = \mathbf{e}_3.$

We come back to the more general situation.

Lemma 2.1.11. *Let $V = \mathbb{F}^n$ and $T \subseteq \mathrm{AGL}(V, +)$ be an elementary abelian regular subgroup. Then for each $\mathbf{a} \in V$, $\kappa_\mathbf{a}$ has order 2 and it is unipotent. In particular $\Omega(T)$ is a unipotent subgroup of $\mathrm{GL}(V, +)$.*

Proof. We know that $\tau_\mathbf{a}$ has order 2, because T is elementary. Then $\tau_\mathbf{a}^2 = 1_V$ implies $\mathbf{a}\tau_\mathbf{a} = 0$, in particular $\mathbf{a}\kappa_\mathbf{a} = \mathbf{a}$. So

$$\mathbf{x} = \mathbf{x}\tau_\mathbf{a}^2 = (\mathbf{x}\kappa_\mathbf{a} + \mathbf{a})\kappa_\mathbf{a} + \mathbf{a} = \mathbf{x}\kappa_\mathbf{a}^2 + \mathbf{a} + \mathbf{a} = \mathbf{x}\kappa_\mathbf{a}^2 \quad \text{for all } \mathbf{x} \in V.$$

Which implies $(\kappa_\mathbf{a} - 1_V)^2 = \kappa_\mathbf{a}^2 - 1_V = 0$. □

Remark 2.1.12. The lemma above can be extended to any characteristic p, in this case the order of $\kappa_\mathbf{a}$ is p.

Lemma 2.1.13. *Let $V = \mathbb{K}^n$, with $\mathbb{K}$ any field. Let $G \subseteq \mathrm{GL}(V)$ be a unipotent subgroup and let $W \subseteq V$ be a subspace such that for all $\mathbf{v} \in W$ and $g \in G$ $\mathbf{v}g = \mathbf{v}$, i.e. G is contained in the stabilizer of W. Then all elements of G are upper triangular in a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_{n-k+1}, \ldots, \mathbf{v}_n\}$, where $\{\mathbf{v}_{n-k+1}, \ldots, \mathbf{v}_n\}$ is any basis of W.*

Proof. The vectors of W are fixed by all elements of G. So, G acts by unipotent maps on V/W. From Theorem 1.1.7 there exists a basis $[\mathbf{v}_1], \ldots, [\mathbf{v}_{n-k}]$ of V/W, such that $[\mathbf{v}_i]g - [\mathbf{v}_i]$ lies in $\mathrm{Span}\{[\mathbf{v}_{i+1}], \ldots, [\mathbf{v}_{n-k}]\}$ for all elements of G. Then all elements of G are upper triangular in the basis $\mathbf{v}_1, \ldots, \mathbf{v}_{n-k}, \mathbf{v}_{n-k+1}, \ldots, \mathbf{v}_n$, since $\mathbf{v}_i g - \mathbf{v}_i = 0$ for all $n - k + 1 \leq i \leq n$. □

Corollary 2.1.14. *Let $V = \mathbb{K}^n$ and $T \subseteq \mathrm{AGL}(V, +)$ be an abelian regular subgroup such that $\Omega(T)$ is a unipotent group. Then all elements of $\Omega(T)$ are upper triangular in a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_{n-k+1}, \ldots, \mathbf{v}_n\}$, with $\{\mathbf{v}_{n-k+1}, \ldots, \mathbf{v}_n\}$ any basis of $U(T)$.*

Proof. By definition, for all $\mathbf{v} \in U(T)$ and $\kappa \in \Omega(T)$, $\mathbf{v}\kappa = \mathbf{v}$. So from Lemma 2.1.13 we have our claim. □

Remark 2.1.15. Let $V = \mathbb{F}_p^n$ then any elementary abelian regular subgroup $T \subseteq \mathrm{AGL}(V, +)$ is unipotent. Thus we obtain the following corollary.

Corollary 2.1.16. *Let $V = \mathbb{F}_p^n$ and $T \subseteq \mathrm{AGL}(V, +)$ be an elementary abelian regular subgroup. Then there exists a subgroup T' conjugated to T such that $\Omega(T') \subseteq \mathcal{U}(V)$ and $U(T') = \mathrm{Span}\{\mathbf{e}_{n-k+1}, \ldots, \mathbf{e}_n\}$, where $k = \dim(U(T))$.*

Proof. From Corollary 2.1.14 we have that all the elements of $\Omega(T)$ are upper triangular with respect to a basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$, with the last k vectors which are a basis of $U(T)$. Let, now, consider $g \in \mathrm{GL}(V)$ such that $\mathbf{v}_i g = \mathbf{e}_i$ for all i. Since $\Omega(g^{-1}Tg) = g^{-1}\Omega(T)g$, for all $\kappa \in \Omega(T)$ we have

$$\mathbf{e}_i g^{-1}\kappa g - \mathbf{e}_i = \mathbf{v}_i \kappa g - \mathbf{v}_i g = (\mathbf{v}_i\kappa - \mathbf{v}_i)g.$$

So, being $\mathbf{v}_i\kappa - \mathbf{v}_i \in \mathrm{Span}\{\mathbf{v}_{i-1}, \ldots, \mathbf{v}_n\}$ it results $(\mathbf{v}_i\kappa - \mathbf{v}_i)g \in \mathrm{Span}\{\mathbf{e}_{i-1}, \ldots, \mathbf{e}_n\}$. To conclude, from the fact that $g^{-1}\tau_{\mathbf{v}}g : \mathbf{x} \mapsto \mathbf{x}g^{-1}\kappa_{\mathbf{v}}g + \mathbf{v}g$, we have also $U(g^{-1}Tg) = U(T)g = \mathrm{Span}\{\mathbf{e}_{n-k+1}, \ldots, \mathbf{e}_n\}$. □

Now, we want to characterize the translation groups that contains T_+ in their affine groups. We report the following lemma proved in [CDS06].

Lemma 2.1.17. *Let V be a vector space over any field $\mathbb{K}$ and $T \subseteq \mathrm{AGL}(V, +)$ be an abelian regular subgroup. Then for all $\sigma_{\mathbf{x}} \in T_+$ and $\tau_{\mathbf{y}} \in T$*

$$[\sigma_{\mathbf{x}}, \tau_{\mathbf{y}}] = \sigma_{\mathbf{x}\cdot\mathbf{y}}.$$

Where $\mathbf{x} \cdot \mathbf{y}$ is the product of the $\mathbb{K}$-algebra related to T as in Theorem 2.1.2, and $[\sigma_{\mathbf{x}}, \tau_{\mathbf{y}}] = \sigma_{\mathbf{x}}^{-1}\tau_{\mathbf{y}}^{-1}\sigma_{\mathbf{x}}\tau_{\mathbf{y}}$.

From Lemma 2.1.17 we obtain that T_+ normalizes $T_\circ \subseteq \mathrm{AGL}(V,+)$ if and only if $\sigma_{\mathbf{xy}} \in T_\circ$ for all $\mathbf{x},\mathbf{y} \in V$, that is $\mathbf{xyz}=0$ for all $\mathbf{x},\mathbf{y},\mathbf{z} \in V$. Indeed, if T_+ normalizes $T_\circ$ for all $\sigma_{\mathbf{x}} \in T_+$, $\sigma_{\mathbf{x}}^{-1} T_\circ \sigma_{\mathbf{x}} = T_\circ$, thus

$$\sigma_{\mathbf{xy}} = \underbrace{\sigma_{\mathbf{x}}^{-1}\tau_{\mathbf{y}}^{-1}\sigma_{\mathbf{x}}}_{\in T_\circ}\tau_{\mathbf{y}} \in T_\circ.$$

Conversely if $\sigma_{\mathbf{xy}} \in T_\circ$ then

$$\sigma_{\mathbf{xy}}\tau_{\mathbf{y}}^{-1} = \sigma_{\mathbf{x}}^{-1}\tau_{\mathbf{y}}^{-1}\sigma_{\mathbf{x}} \in T_\circ.$$

In the case of the field $\mathbb{F}$, from Remark 2.1.3 we obtain the following result.

Theorem 2.1.18. *If* $\dim(V) \leq 6$*, then* $T_+ \subseteq \mathrm{AGL}(V,\circ)$ *if and only if* $T_\circ \subseteq \mathrm{AGL}(V,+)$

Proof. By contradiction we assume that there exists $T_\circ \subseteq \mathrm{AGL}(V,+)$ such that $T_+ \nsubseteq \mathrm{AGL}(V,\circ)$.

From Lemma 2.1.17 we have that there exist $\mathbf{x},\mathbf{y},\mathbf{z} \in V$ such that $\mathbf{xyz} \neq 0$.

Consider the vectors $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$, $\mathbf{xy}$, $\mathbf{xz}$, $\mathbf{yz}$ and $\mathbf{xyz}$, they are all non-zero. Suppose now that there exist $\lambda_{\mathbf{x}}$, $\lambda_{\mathbf{y}}$, $\lambda_{\mathbf{z}}$, $\lambda_{\mathbf{xy}}$, $\lambda_{\mathbf{xz}}$, $\lambda_{\mathbf{yz}}$, $\lambda_{\mathbf{xyz}} \in \mathbb{F}$ such that

$$\lambda_{\mathbf{x}}\mathbf{x} + \lambda_{\mathbf{y}}\mathbf{y} + \lambda_{\mathbf{z}}\mathbf{z} + \lambda_{\mathbf{xy}}\mathbf{xy} + \lambda_{\mathbf{xz}}\mathbf{xz} + \lambda_{\mathbf{yz}}\mathbf{yz} + \lambda_{\mathbf{xyz}}\mathbf{xyz} = 0. \tag{2.1}$$

Multiplying by $\mathbf{yz}$ the Equation 2.1, and recalling that $\mathbf{a}^2 = 0$ for all $\mathbf{a} \in V$, we have $\lambda_{\mathbf{x}}\mathbf{xyz} = 0$, that implies $\lambda_{\mathbf{x}} = 0$. Analogously multiplying by $\mathbf{xz}$, $\mathbf{xy}$, $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ we obtain $\lambda_{\mathbf{y}} = \lambda_{\mathbf{z}} = \lambda_{\mathbf{xy}} = \lambda_{\mathbf{xz}} = \lambda_{\mathbf{yz}} = 0$. So, it results $\lambda_{\mathbf{xyz}}\mathbf{xyz} = 0$, that implies $\lambda_{\mathbf{xyz}} = 0$.

Then $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$, $\mathbf{xy}$, $\mathbf{xz}$, $\mathbf{yz}$ and $\mathbf{xyz}$ are linear independents, and $\dim(V) \geq 7$.

Conversely we can invert the sum $+$ and $\circ$ in Theorem 2.1.2 so we obtain the same result only changing $+$ with $\circ$. □

Theorem 2.1.19. *If* $\dim(V) \geq 7$*, then there exists* $T_\circ \subseteq \mathrm{AGL}(V,+)$ *such that* $T_+ \nsubseteq \mathrm{AGL}(V,\circ)$.

Proof. Let n be the dimension of V, then $V = V_1 \oplus V_2$ where

$$V_1 = \mathrm{Span}\{\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3,\mathbf{e}_4,\mathbf{e}_5,\mathbf{e}_6,\mathbf{e}_7\}$$

and

$$V_2 = \mathrm{Span}\{\mathbf{e}_8,\ldots,\mathbf{e}_n\}.$$

If $n = 7$ then we consider only V_1.

Over V_1 we consider the algebra structure induced by the exterior algebra over a vector space of dimension 3, that is

$$\mathbf{e}_1 \wedge \mathbf{e}_2 = \mathbf{e}_4, \mathbf{e}_1 \wedge \mathbf{e}_3 = \mathbf{e}_5, \mathbf{e}_2 \wedge \mathbf{e}_3 = \mathbf{e}_6, \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3 = \mathbf{e}_7,$$

and over V_2 the algebra structure is given by $\mathbf{x} * \mathbf{y} = 0$ for each $\mathbf{x}, \mathbf{y} \in V_2$.

So over V we individuate the structure $(\mathbf{v}_1, \mathbf{v}_2) \cdot (\mathbf{w}_1, \mathbf{w}_2) = (\mathbf{v}_1 \wedge \mathbf{w}_1, \mathbf{v}_2 * \mathbf{w}_2)$ where $\mathbf{v}_1, \mathbf{w}_1 \in V_1$ and $\mathbf{v}_2, \mathbf{w}_2 \in V_2$.

$(V, +, \cdot)$ is a commutative associative $\mathbb{F}$-algebra such that the resulting ring is radical. This algebra corresponds to an elementary abelian regular subgroup $T_\circ$ of $\mathrm{AGL}(V, +)$ for Theorem 2.1.2 and because $\mathbf{x} \circ \mathbf{x} = 0$ for all $\mathbf{x} \in V$. From Lemma 2.1.17 we have our claim, in fact $\mathbf{e}_1 \cdot \mathbf{e}_2 \cdot \mathbf{e}_3 \neq 0$. □

Remark 2.1.20. Let $V = \mathbb{K}^n$, with $\mathbb{K}$ any field. Let $T \subseteq \mathrm{AGL}(V, +)$ be an abelian regular subgroup such that T_+ is in the normalizer of T. Then any conjugate to T in $\mathrm{AGL}(V, +)$ is conjugate under the action of $\mathrm{GL}(V, +)$. In fact, let $\tau \in \mathrm{AGL}(V, +)$ with $\tau = \kappa\sigma$ for some $\kappa \in \mathrm{GL}(V, +)$ and $\sigma \in T_+$ and let $T' = \tau T \tau^{-1}$. Because T_+ normalizes T, we have

$$\kappa\sigma T \sigma^{-1} \kappa^{-1} = \kappa T \kappa^{-1}.$$

The following theorem is reported for any finite field $\mathbb{F}_p$.

Theorem 2.1.21. *Let $V = \mathbb{F}_p^{n+k}$, with $n \geq 2$, $k \geq 1$, and $T_\circ \subseteq \mathrm{AGL}(V, +)$ be such that $U(T_\circ) = \mathrm{Span}\{\mathbf{e}_{n+1}, \ldots, \mathbf{e}_{n+k}\}$. Then, $T_+ \subseteq \mathrm{AGL}(V, \circ)$ if and only if for all $\kappa_{\mathbf{y}} \in \Omega(T_\circ)$ there exists a matrix $B_{\mathbf{y}} \in \mathbb{F}_p^{n \times k}$ such that*

$$\kappa_{\mathbf{y}} = \begin{bmatrix} I_{n \times n} & B_{\mathbf{y}} \\ 0 & I_{k \times k} \end{bmatrix}.$$

Proof. Let $T_\square$ conjugated to $T_\circ$ be such that $\Omega(T_\square) \subseteq \mathcal{U}(V)$, such a group exists for Corollary 2.1.16. Let $\mathbf{y} \in V$ and

$$\kappa_{\mathbf{y}} = \begin{bmatrix} U_{\mathbf{y}} & B_{\mathbf{y}} \\ 0 & I_{k \times k} \end{bmatrix},$$

for some $B_{\mathbf{y}} \in \mathbb{F}_p^{n \times k}$ and $U_{\mathbf{y}} \in \mathbb{F}_p^{n \times n}$. Lemma 2.1.17 implies $T_+ \subseteq \mathrm{AGL}(V, \square)$ if and only if $\mathbf{x} \cdot \mathbf{y} \in U(T_\square)$ for all $\mathbf{x}, \mathbf{y} \in V$. Recall that $\mathbf{x} \cdot \mathbf{y} = \mathbf{x}\kappa_{\mathbf{y}} - \mathbf{x}$ for all $\mathbf{x}, \mathbf{y} \in V$. Thus $\mathbf{x} \cdot \mathbf{y} \in U(T_\square)$ if and only if $\mathbf{x}\kappa_{\mathbf{y}} - \mathbf{x} \in U(T_\square)$. Consider, now, $W = \mathrm{Span}\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, then for all $\mathbf{x} \in W$ we have that $\mathbf{x}\kappa_{\mathbf{y}} - \mathbf{x} \in U(T_\square)$ if and only if $U_{\mathbf{y}} = I_{n \times n}$.

Now, we need to proof only that any conjugate $T_\circ$ of $T_\square$ is such that all the matrices in the group $\Omega(T_\circ)$ have this form, whenever the space $U(T_\circ)$ is spanned by the last k elements of the canonical basis.

Let $g \in \mathrm{GL}(V,+)$ be such that $U(g^{-1}T_\square g) = U(T_\circ) == \mathrm{Span}\{\mathbf{e}_{n+1},\dots,\mathbf{e}_{n+k}\}$. This implies $U(T_\square)g = U(T_\square)$ and also $U(T_\square)g^{-1} = U(T_\square)$, so

$$g = \begin{bmatrix} G_1 & G_2 \\ 0 & G_3 \end{bmatrix}, \quad g^{-1} = \begin{bmatrix} G_1^{-1} & G_2' \\ 0 & G_3^{-1} \end{bmatrix},$$

for some $G_1 \in \mathbb{F}_p^{n\times n}, G_2, G_2' \in \mathbb{F}_p^{n\times k}$ and $G_3 \in \mathbb{F}_p^{k\times k}$. Then for all $\kappa \in \Omega(T_\circ)$ we have

$$g^{-1}\kappa g = \begin{bmatrix} G_1^{-1} & G_2' \\ 0 & G_3^{-1} \end{bmatrix} \begin{bmatrix} I_{n\times n} & B_{n\times k} \\ 0 & I_{k\times k} \end{bmatrix} \begin{bmatrix} G_1 & G_2 \\ 0 & G_3 \end{bmatrix} = \begin{bmatrix} I_{n\times n} & B'_{n\times k} \\ 0 & I_{k\times k} \end{bmatrix}.$$

□

Remark 2.1.22. Let $T \subseteq \mathrm{AGL}(V,+)$ be an abelian regular group and $\tau_{\mathbf{e}_i}, \tau_{\mathbf{e}_j} \in T$ be the affinities related to the canonical vectors $\mathbf{e}_i, \mathbf{e}_j$. Then from

$$\mathbf{e}_i \circ \mathbf{e}_j = \mathbf{e}_i\kappa_{\mathbf{e}_j} + \mathbf{e}_j = \mathbf{e}_j\kappa_{\mathbf{e}_i} + \mathbf{e}_i = \mathbf{e}_j \circ \mathbf{e}_i$$

we obtain that the i-th row of $\kappa_{\mathbf{e}_j}$ and the j-th row of $\kappa_{\mathbf{e}_i}$ differ only in the position i and j.

Lemma 2.1.23. *Let $T \subseteq \mathrm{AGL}(V,+)$ be an abelian regular subgroup such that $\Omega(T) \subset \mathcal{U}(V)$. Then the action of $\kappa_{\mathbf{e}_i}$ over $V/\mathrm{Span}\{\mathbf{e}_{i+1},\dots,\mathbf{e}_n\}$ is the identity map, for all $1 \le i \le n$.*

Proof. It follows directly from the remark above and from $\Omega(T) \subset \mathcal{U}(V)$. □

In characteristic 2 we obtain also that if $2 \le n \le 5$ then the matrices are always in the form of Theorem 2.1.21.

Proposition 2.1.24. *Let $V = \mathbb{F}^{n+k}$, with $2 \le n \le 5$ and $k \ge 1$. If $T \subseteq \mathrm{AGL}(V,+)$ is an elementary abelian regular subgroup with $U(T) = \mathrm{Span}\{\mathbf{e}_{n+1},\dots,\mathbf{e}_{n+k}\}$, then for all $\kappa_{\mathbf{v}} \in \Omega(T)$ there exists a matrix $B_{\mathbf{v}} \in \mathbb{F}^{n\times k}$ such that*

$$\kappa_{\mathbf{v}} = \begin{bmatrix} I_{n\times n} & B_{\mathbf{v}} \\ 0 & I_{k\times k} \end{bmatrix}.$$

Proof. We report only the proof for $n = 5$, the others are analogous. Let T be such that $\Omega(T) \subseteq \mathcal{U}(V)$ and $U(T) = \mathrm{Span}\{\mathbf{e}_{n+1},\dots,\mathbf{e}_{n+k}\}$, such a group there exists for Corollary 2.1.16. Also, from Lemma 2.1.7 and Lemma 2.1.23, we have that T is generated by the maps related to the vectors of the canonical basis. For those vectors,

from Lemma 2.1.23 and Remark 2.1.22 we have that the maps $\kappa_{\mathbf{e}_i}$ are of the form

$$\kappa_{\mathbf{e}_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & a_1^{(1,2)} & a_2^{(1,2)} & a_3^{(1,2)} & \mathbf{b}_2^{(1)} \\ & & 1 & a_1^{(1,3)} & a_2^{(1,3)} & \mathbf{b}_3^{(1)} \\ & & & 1 & a_1^{(1,4)} & \mathbf{b}_4^{(1)} \\ & & & & 1 & \mathbf{b}_5^{(1)} \\ & & & & & I_{k\times k} \end{bmatrix} \quad \kappa_{\mathbf{e}_2} = \begin{bmatrix} 1 & 0 & a_1^{(1,2)} & a_2^{(1,2)} & a_3^{(1,2)} & \mathbf{b}_2^{(1)} \\ & 1 & 0 & 0 & 0 & 0 \\ & & 1 & a_1^{(2,3)} & a_2^{(2,3)} & \mathbf{b}_3^{(2)} \\ & & & 1 & a_1^{(2,4)} & \mathbf{b}_4^{(2)} \\ & & & & 1 & \mathbf{b}_5^{(2)} \\ & & & & & I_{k\times k} \end{bmatrix}$$

$$\kappa_{\mathbf{e}_3} = \begin{bmatrix} 1 & 0 & 0 & a_1^{(1,3)} & a_2^{(1,3)} & \mathbf{b}_3^{(1)} \\ & 1 & 0 & a_1^{(2,3)} & a_2^{(2,3)} & \mathbf{b}_3^{(2)} \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & a_1^{(3,4)} & \mathbf{b}_4^{(3)} \\ & & & & 1 & \mathbf{b}_5^{(3)} \\ & & & & & I_{k\times k} \end{bmatrix} \quad \kappa_{\mathbf{e}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & a_1^{(1,4)} & \mathbf{b}_4^{(1)} \\ & 1 & 0 & 0 & a_1^{(2,4)} & \mathbf{b}_4^{(2)} \\ & & 1 & 0 & a_1^{(3,4)} & \mathbf{b}_4^{(3)} \\ & & & 1 & 0 & 0 \\ & & & & 1 & \mathbf{b}_5^{(4)} \\ & & & & & I_{k\times k} \end{bmatrix}$$

$$\kappa_{\mathbf{e}_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \mathbf{b}_5^{(1)} \\ & 1 & 0 & 0 & 0 & \mathbf{b}_5^{(2)} \\ & & 1 & 0 & 0 & \mathbf{b}_5^{(3)} \\ & & & 1 & 0 & \mathbf{b}_5^{(4)} \\ & & & & 1 & 0 \\ & & & & & I_{k\times k} \end{bmatrix} \quad \kappa_{\mathbf{e}_i} = 1_V \text{ for } i > 5,$$

with $a_i^{(j,h)} \in \mathbb{F}$ and $\mathbf{b}_j^{(i)} \in \mathbb{F}^k$ for all i, j, h. Now, we will show that if there exists $a_i^{(j,h)} \neq 0$ then it will be $U(T) \neq \mathrm{Span}\{\mathbf{e}_{n+1}, \ldots, \mathbf{e}_{n+k}\}$. We have these two conditions

I $\kappa_{\mathbf{e}_i}^2 = 1_V$;

II $\kappa_{\mathbf{e}_i}\kappa_{\mathbf{e}_j} = \kappa_{\mathbf{e}_j}\kappa_{\mathbf{e}_i}$;

which imply

$$a_1^{(i,4)}\mathbf{b}_5^{(i)} = 0 \tag{2.2a}$$

$$a_1^{(i,4)}\mathbf{b}_5^{(4)} = 0 \quad \text{for all } i < 4 \tag{2.2b}$$

and

$$a_1^{(i,4)}\mathbf{b}_5^{(j)} = a_1^{(j,4)}\mathbf{b}_5^{(i)} \quad \text{for all } i, j < 4. \tag{2.3}$$

Now, supposing that $a_1^{(i,4)} = 1$ for some $1 \leq i \leq 3$, from Equation (2.2) and (2.3) we have $\mathbf{b}_5^{(j)} = 0$ for all j and then $\mathbf{e}_5 \in U(T)$. Thus $a_1^{(i,4)} = 0$ for all i.

Now from the conditions I and II we obtain

$$a_1^{(i,3)}\mathbf{b}_4^{(i)} + a_2^{(i,3)}\mathbf{b}_5^{(i)} = 0 \tag{2.4a}$$
$$a_1^{(i,3)}\mathbf{b}_4^{(3)} + a_2^{(i,3)}\mathbf{b}_5^{(3)} = 0 \tag{2.4b}$$
$$a_1^{(i,3)}\mathbf{b}_5^{(4)} = 0 \tag{2.4c}$$
$$a_2^{(i,3)}\mathbf{b}_5^{(4)} = 0 \quad \text{for all } i < 3 \tag{2.4d}$$

and

$$a_1^{(1,3)}\mathbf{b}_4^{(2)} + a_2^{(1,3)}\mathbf{b}_5^{(2)} = a_1^{(2,3)}\mathbf{b}_4^{(1)} + a_2^{(2,3)}\mathbf{b}_5^{(1)}, \tag{2.5}$$

moreover

$$a_1^{(1,2)}a_1^{(1,3)} = 0 \tag{2.6a}$$
$$a_1^{(1,2)}a_2^{(1,3)} = 0 \tag{2.6b}$$
$$a_1^{(1,2)}a_1^{(2,3)} = 0 \tag{2.6c}$$
$$a_1^{(1,2)}a_2^{(2,3)} = 0. \tag{2.6d}$$

$$a_1^{(1,2)}\mathbf{b}_3^{(1)} + a_2^{(1,2)}\mathbf{b}_4^{(1)} + a_3^{(1,2)}\mathbf{b}_5^{(1)} = 0 \tag{2.7a}$$
$$a_1^{(1,2)}\mathbf{b}_3^{(2)} + a_2^{(1,2)}\mathbf{b}_4^{(2)} + a_3^{(1,2)}\mathbf{b}_5^{(2)} = 0 \tag{2.7b}$$

Suppose $(a_1^{(1,3)}, a_2^{(1,3)}) = (1,0)$, we obtain from Equation (2.4) that $\mathbf{b}_4^{(1)} = \mathbf{b}_4^{(3)} = \mathbf{b}_5^{(4)} = 0$, thus $\mathbf{b}_4^{(2)}$ has to be equal to 1 otherwise $\mathbf{e}_4 \in U(T)$. So from (2.5) we have $a_2^{(2,3)} = \mathbf{b}_5^{(1)} = 1$. Now, from (2.6) we obtain $a_1^{(1,2)} = 0$ and (2.7a) becomes $a_3^{(1,2)}\mathbf{b}_5^{(1)} = 0$, which implies $a_3^{(1,2)} = 0$. So (2.7b) becomes $a_2^{(1,2)}\mathbf{b}_4^{(2)} = 0$, and $a_2^{(1,2)} = 0$. Consider, then, the matrix $\kappa_{\mathbf{e}_2}\kappa_{\mathbf{e}_3}$, we have that $(\kappa_{\mathbf{e}_2}\kappa_{\mathbf{e}_3})^2 = 1_V$ implies

$$a_1^{(1,3)}\mathbf{b}_4^{(2)} + a_2^{(1,3)}\mathbf{b}_5^{(2)} = \mathbf{b}_4^{(2)} = 0,$$

and we have a contradiction. So $(a_1^{(1,3)}, a_2^{(1,3)}) \neq (1,0)$. The cases $(a_1^{(1,3)}, a_2^{(1,3)}) = (0,1)$, $(a_1^{(2,3)}, a_2^{(2,3)}) = (1,0)$ and $(a_1^{(2,3)}, a_2^{(2,3)}) = (0,1)$ lead to a contradiction in a similar way. Then the last possible cases are: $(a_1^{(1,3)}, a_2^{(1,3)})$ and $(a_1^{(1,3)}, a_2^{(1,3)})$ are together $(1,1)$ or one is $(0,0)$ and the other $(1,1)$. Note that in all the two cases we obtain $\mathbf{b}_4^{(2)} + \mathbf{b}_5^{(2)} = \mathbf{b}_4^{(1)} + \mathbf{b}_5^{(1)} = \mathbf{b}_4^{(3)} + \mathbf{b}_5^{(3)} = \mathbf{b}_5^{(4)} = 0$ from (2.4) and (2.5), which means $\mathbf{e}_4 + \mathbf{e}_5 \in U(T)$. Thus, also, $(a_1^{(2,3)}, a_2^{(2,3)}) = (a_1^{(2,3)}, a_2^{(2,3)}) = (0,0)$.

Consider now $(a_1^{(1,2)}, a_2^{(1,2)}, a_3^{(1,2)})$, if it is different from zero, then (2.7) implies that $a_1^{(1,2)}\mathbf{e}_3 + a_2^{(1,2)}\mathbf{e}_4 + a_3^{(1,2)}\mathbf{e}_5 \in U(T)$. So, also, these values have to be equal to zero.

To conclude, as in Theorem 2.1.21 we have that any conjugate to such a group, maintaining unvaried the space $U(T)$, has the maps $\kappa_{\mathbf{y}}$'s in this form. □

Example 2.1.25. Proposition 2.1.24 does not hold, in general, for $n \geq 6$. Let $(V, +, \cdot)$ be the exterior algebra over a vector space of dimension three, spanned by $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$. That is, V has basis

$$\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4 = \mathbf{e}_1 \wedge \mathbf{e}_2, \mathbf{e}_5 = \mathbf{e}_1 \wedge \mathbf{e}_3, \mathbf{e}_6 = \mathbf{e}_2 \wedge \mathbf{e}_3, \mathbf{e}_7 = \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3.$$

The associated translation group $T_\circ$ is such that $U(T_\circ) = \mathrm{Span}\{\mathbf{e}_7\}$, but we have

$$\kappa_{\mathbf{e}_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & \boxed{1} & 0 & 0 & 0 \\ & & 1 & 0 & \boxed{1} & 0 & 0 \\ & & & 1 & 0 & 0 & 0 \\ & & & & 1 & 0 & 0 \\ & & & & & 1 & 1 \\ & & & & & & 1 \end{bmatrix}.$$

Let $n \geq 2$ and $k \geq 1$ and define for all $1 \leq i \leq n$ the matrix

$$\kappa_i = \begin{bmatrix} & b_{1,1}^{(i)} & \dots & b_{1,k}^{(i)} \\ I_{n\times n} & \vdots & & \vdots \\ & b_{n,1}^{(i)} & \dots & b_{n,k}^{(i)} \\ & & I_{k\times k} & \end{bmatrix}. \tag{2.8}$$

Lemma 2.1.26. *Let $N = n + k$ and $V = \mathbb{F}^N$, with $n \geq 2$ and $k \geq 1$. The elementary abelian regular subgroups $T_\circ \subseteq \mathrm{AGL}(V, +)$ such that $\dim(U(T)) = k$ and $T_+ \subseteq \mathrm{AGL}(V, \circ)$ are*

$$\begin{bmatrix} N \\ k \end{bmatrix}_2 \cdot |\mathcal{V}(\mathcal{I}_k)|$$

where $\mathcal{I}_k$ is the ideal generated by

$$\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$$

with

$$\mathcal{S}_1 = \left\{ \prod_{i=1}^{n} \prod_{j=1}^{k} \left(1 + \sum_{s \in S} b_{i,j}^{(s)} \right) \mid S \subseteq [n], S \neq \emptyset \right\},$$
$$\mathcal{S}_2 = \{ b_{i,j}^{(s)} - b_{s,j}^{(i)} | i, s \in [n], j \in [k] \},$$
$$\mathcal{S}_3 = \{ b_{i,j}^{(i)} | i \in [n], j \in [k] \},$$

$\mathcal{V}(\mathcal{I}_k)$ is the variety over $\mathbb{F}$ of $\mathcal{I}_k$ and $\begin{bmatrix} N \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^{N-i}-1}{q^{k-i}-1}$ is the Gaussian Binomial.

Proof. Let $T_\circ \subseteq \mathrm{AGL}(V, +)$ such that $U(T_\circ)$ is generated by the last k elements of the canonical basis and $T_+ \subseteq \mathrm{AGL}(V, \circ)$. From Theorem 2.1.21 we have that the

matrices κ_i's for $1 \leq i \leq n$ are as in (2.8). Let S be a subset of $[n]$ and denoting by κ_S the product of κ_i's with $i \in S$ then

$$\kappa_S = \begin{bmatrix} & \sum_{i\in S} b_{1,1}^{(i)} & \dots & \sum_{i\in S} b_{1,k}^{(i)} \\ I_{n\times n} & \vdots & & \vdots \\ & \sum_{i\in S} b_{n,1}^{(i)} & \dots & \sum_{i\in S} b_{n,k}^{(i)} \\ & & I_{k\times k} & \end{bmatrix}.$$

For all $S \subseteq [n]$ we have that $\kappa_S \neq 1_V$ otherwise the vector $\sum_{i\in S} \mathbf{e}_i$ lies in $U(T_\circ)$. Thus there exist h, j such that $\sum_{i\in S} b_{h,j}^{(i)} = 1$ and it happens if and only if

$$\prod_{i=1}^{n}\prod_{j=1}^{k}\left(1 + \sum_{s\in S} b_{i,j}^{(s)}\right) = 0.$$

The others conditions come from the Remark 2.1.22 and from the fact that κ_i fixes $\mathbf{e}_i$. Imposing only these two conditions and from the fact that the matrices are in this form, the group is always elementary and abelian, then from Corollary 2.1.16 it is also regular. Thus we do not need to add more equations. So, there are $\#\mathcal{V}(\mathcal{I}_k)$ subgroups with $U(T_\circ) = \mathrm{Span}\{\mathbf{e}_{n+1}, \dots, \mathbf{e}_{n+k}\}$.

Consider, now, a k dimensional vector subspace W. Let $g \in \mathrm{GL}(V, +)$ be such that $Wg = \mathrm{Span}\{\mathbf{e}_{n+1}, \dots, \mathbf{e}_{n+k}\}$. Let $T_1, \dots, T_{\#\mathcal{V}(\mathcal{I}_k)}$ denote the distinct groups with $U(T_i) = \mathrm{Span}\{\mathbf{e}_{n+1}, \dots, \mathbf{e}_{n+k}\}$. Then the groups $T_1', \dots, T_{\#\mathcal{V}(\mathcal{I}_k)}'$, with $T_i' = gT_ig^{-1}$ are all distinct and $U(T_i') = W$. Now, let T be such that $U(T) = W$, $U(g^{-1}Tg) = \mathrm{Span}\{\mathbf{e}_{n+1}, \dots, \mathbf{e}_{n+k}\}$, which implies $g^{-1}Tg = T_i$ for some i, and so $T = T_i'$. Being the number of k dimensional vector subspace of V given by $\begin{bmatrix} N \\ k \end{bmatrix}_2$ we have our claim. □

Proposition 2.1.27. *Let $\mathcal{I}_k$ defined as in Lemma 2.1.26, then*

$$\begin{bmatrix} N \\ k \end{bmatrix}_2 \cdot |\mathcal{V}(\mathcal{I}_k)| \leq \begin{bmatrix} N \\ k \end{bmatrix}_2 \cdot \left[2^{k\frac{n(n-1)}{2}} - 1 - \sum_{r=1}^{n-2} \binom{n}{r} \prod_{i=1}^{\frac{(n-r)(n-r-1)}{2}} \left(2^k - 1\right)\right].$$

Proof. Let consider the vector

$$(\mathbf{b}_1^{(1)}, \dots, \mathbf{b}_n^{(1)}, \mathbf{b}_1^{(2)}, \dots, \mathbf{b}_n^{(2)}, \dots, \mathbf{b}_1^{(n)}, \dots, \mathbf{b}_n^{(n)}),$$

where $\mathbf{b}_i^{(j)} = (b_{i,1}^{(j)}, \cdots^{(j)}_{i,k}) \in \mathbb{F}^k$ for all i, j as in (2.8). From the conditions in $\mathcal{S}_3$ we have $\mathbf{b}_i^{(i)} = 0$ for all i, and from $\mathcal{S}_2$, $\mathbf{b}_j^{(i)} = \mathbf{b}_i^{(j)}$ for all $i > j$. Thus we can consider only the vector formed by

$$\mathbf{B} = (\mathbf{b}_2^{(1)}, \dots, \mathbf{b}_n^{(1)}, \mathbf{b}_3^{(2)}, \dots, \mathbf{b}_n^{(2)}, \dots, \mathbf{b}_n^{(n-1)}),$$

so we have $2^{k\frac{n(n-1)}{2}}$ solution of the equations in $\mathcal{S}_2 \cup \mathcal{S}_3$. Now the entries of $\mathbf{B}$ have to satisfy the conditions given by $\mathcal{S}_1$, so we can exclude some cases where, for any subset S of $[n]$ the matrices κ_i's, as in (2.8), with $i \in S$ are equal to the identity and the others no, in particle we consider vectors $\mathbf{B}$ such that the only zero $\mathbf{b}^{(i)}$'s are those necessary to obtain the identity maps. Note that if any κ_i is equal to the identity and the others not, then $n-1$ entries of $\mathbf{B}$ are zero and the others are all non-zero. Similarly, if any pairs κ_i, κ_j are equal to the identity and the others not then $n-1+n-2$ entries of $\mathbf{B}$ are zero and the others are all non-zero. In fact suppose $i < j$ then the zero entries of $\mathcal{B}$ must be $\mathbf{b}_i^{(1)}, \dots, \mathbf{b}_i^{(i-1)}, \mathbf{b}_{i+1}^{(i)}, \dots, \mathbf{b}_n^{(i)}$ to have $\kappa_i = 1_V$ and $\mathbf{b}_j^{(1)}, \dots, \mathbf{b}_j^{(j-1)}, \mathbf{b}_{j+1}^{(j)}, \dots, \mathbf{b}_n^{(j)}$ to have $\kappa_j = 1_V$, considering the fact that $\mathbf{b}_j^{(i)}$ is already zero from the condition on κ_i. Iterating, if we consider r maps that have to be the identity then $\sum_{i=1}^{r} n-i$ entries of $\mathbf{B}$ are zero and the others are all non-zero. To conclude, if $n-1$ maps of the κ_i's are the identity, by the conditions of $\mathcal{S}_2 \cup \mathcal{S}_3$ also the last one is the identity, and this append when $\mathcal{B}$ is zero. □

When $U(T)$ has co-dimension 2 and 3 we have the following results.

Corollary 2.1.28. *Let $V = \mathbb{F}^n$. There exist $\begin{bmatrix} n \\ n-3 \end{bmatrix}_2 \cdot (2^{3(n-3)} - 7(2^{n-3}-1) - 1)$ distinct elementary abelian regular subgroups of $\mathrm{AGL}(V,+)$ such that $\dim(U(T)) = n-3$.*

Proof. From Lemma 2.1.26, we need to compute the number of groups such that $U(T) = \mathrm{Span}\{\mathbf{e}_3, \dots, \mathbf{e}_n\}$. To do this we count the case when the $\kappa_S = 1_V$ for $S \subseteq \{1,2,3\}$. From Lemma 2.1.24 and Remark 2.1.22 we have

$$\kappa_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ & 1 & 0 & b_{2,1}^{(1)} & \dots & b_{2,n-3}^{(1)} \\ & & 1 & b_{3,1}^{(1)} & \dots & b_{3,n-3}^{(1)} \\ & & & & & \\ & & & I_{n-3\times n-3} & & \\ & & & & & \end{bmatrix} \quad \kappa_2 = \begin{bmatrix} 1 & 0 & 0 & b_{2,1}^{(1)} & \dots & b_{2,n-3}^{(1)} \\ & 1 & 0 & 0 & \dots & 0 \\ & & 1 & b_{3,1}^{(2)} & \dots & b_{3,n-3}^{(2)} \\ & & & & & \\ & & & I_{n-3\times n-3} & & \\ & & & & & \end{bmatrix}$$

$$\kappa_3 = \begin{bmatrix} 1 & 0 & 0 & b_{3,1}^{(1)} & \dots & b_{3,n-3}^{(1)} \\ & 1 & 0 & b_{3,1}^{(2)} & \dots & b_{3,n-3}^{(2)} \\ & & 1 & 0 & \dots & 0 \\ & & & & & \\ & & & I_{n-3\times n-3} & & \\ & & & & & \end{bmatrix}$$

$$\kappa_{\{1,2\}} = \begin{bmatrix} 1 & 0 & 0 & b_{2,1}^{(1)} & \dots & b_{2,n-3}^{(1)} \\ & 1 & 0 & b_{2,1}^{(1)} & \dots & b_{2,n-3}^{(1)} \\ & & 1 & b_{3,1}^{(1)} + b_{3,1}^{(2)} & \dots & b_{3,n-3}^{(1)} + b_{3,n-3}^{(2)} \\ & & & & & \\ & & & & I_{n-3\times n-3} & \\ & & & & & \end{bmatrix}$$

$$\kappa_{\{1,3\}} = \begin{bmatrix} 1 & 0 & 0 & b_{3,1}^{(1)} & \dots & b_{3,n-3}^{(1)} \\ & 1 & 0 & b_{2,1}^{(1)} + b_{3,1}^{(2)} & \dots & b_{2,n-3}^{(1)} + b_{3,n-3}^{(2)} \\ & & 1 & b_{3,1}^{(1)} & \dots & b_{3,n-3}^{(1)} \\ & & & & & \\ & & & & I_{n-3\times n-3} & \\ & & & & & \end{bmatrix}$$

$$\kappa_{\{2,3\}} = \begin{bmatrix} 1 & 0 & 0 & b_{2,1}^{(1)} + b_{3,1}^{(1)} & \dots & b_{2,n-3}^{(1)} + b_{3,n-3}^{(1)} \\ & 1 & 0 & b_{3,1}^{(2)} & \dots & b_{3,n-3}^{(2)} \\ & & 1 & b_{3,1}^{(2)} & \dots & b_{3,n-3}^{(2)} \\ & & & & & \\ & & & & I_{n-3\times n-3} & \\ & & & & & \end{bmatrix}$$

$$\kappa_{\{1,2,3\}} = \begin{bmatrix} 1 & 0 & 0 & b_{2,1}^{(1)} + b_{3,1}^{(1)} & \dots & b_{2,n-3}^{(1)} + b_{3,n-3}^{(1)} \\ & 1 & 0 & b_{2,1}^{(1)} + b_{3,1}^{(2)} & \dots & b_{2,n-3}^{(1)} + b_{3,n-3}^{(2)} \\ & & 1 & b_{3,1}^{(1)} + b_{3,1}^{(2)} & \dots & b_{3,n-3}^{(1)} + b_{3,n-3}^{(2)} \\ & & & & & \\ & & & & I_{n-3\times n-3} & \\ & & & & & \end{bmatrix}.$$

Denoting by $\mathbf{b}_2^{(1)} = (b_{2,1}^{(1)}, \dots, b_{2,n-3}^{(1)}), \mathbf{b}_3^{(1)} = (b_{3,1}^{(1)}, \dots, b_{3,n-3}^{(1)}), \mathbf{b}_3^{(2)} = (b_{3,1}^{(2)}, \dots, b_{3,n-3}^{(2)})$, we have the following cases

1 $\kappa_1 = 1_V \Leftrightarrow \mathbf{b}_2^{(1)} = 0$ and $\mathbf{b}_3^{(1)} = 0$;

2 $\kappa_2 = 1_V \Leftrightarrow \mathbf{b}_2^{(1)} = 0$ and $\mathbf{b}_3^{(2)} = 0$;

3 $\kappa_3 = 1_V \Leftrightarrow \mathbf{b}_3^{(1)} = 0$ and $\mathbf{b}_3^{(2)} = 0$;

4 $\kappa_{\{1,2\}} = 1_V \Leftrightarrow \mathbf{b}_2^{(1)} = 0$ and $\mathbf{b}_3^{(1)} = \mathbf{b}_3^{(2)}$;

5 $\kappa_{\{1,3\}} = 1_V \Leftrightarrow \mathbf{b}_3^{(1)} = 0$ and $\mathbf{b}_2^{(1)} = \mathbf{b}_3^{(2)}$;

6 $\kappa_{\{2,3\}} = 1_V \Leftrightarrow \mathbf{b}_2^{(1)} = \mathbf{b}_3^{(1)}$ and $\mathbf{b}_3^{(2)} = 0$;

7 $\kappa_{\{1,2,3\}} = 1_V \Leftrightarrow \mathbf{b}_2^{(1)} = \mathbf{b}_3^{(1)}$, $\mathbf{b}_2^{(1)} = \mathbf{b}_3^{(2)}$ and $\mathbf{b}_3^{(1)} = \mathbf{b}_3^{(2)}$.

Each case admits 2^{n-3} values for $(\mathbf{b}_2^{(1)}, \mathbf{b}_3^{(1)}, \mathbf{b}_3^{(2)})$ and the only common solution is $(\mathbf{b}_2^{(1)}, \mathbf{b}_3^{(1)}, \mathbf{b}_3^{(2)}) = (0,0,0)$. Thus we have $2^{3(n-3)} - 7(2^{n-3}-1) - 1$ subgroups with $U(T) = \mathrm{Span}\{\mathbf{e}_3, \ldots, \mathbf{e}_n\}$. □

Corollary 2.1.29. *Let $V = \mathbb{F}^n$. There exist $\begin{bmatrix} n \\ n-2 \end{bmatrix}_2 \cdot (2^{n-2}-1)$ distinct elementary abelian regular subgroups of $\mathrm{AGL}(V,+)$ such that $\dim(U(T)) = n-2$.*

Proof. As above for T such that $U(T) = \mathrm{Span}\{\mathbf{e}_3, \ldots, \mathbf{e}_n\}$ we have

$$\kappa_1 = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ & 1 & b_{2,1}^{(1)} & \ldots & b_{2,n-3}^{(1)} \\ & & & & \\ & & I_{n-2\times n-2} & & \\ & & & & \end{bmatrix} \quad \kappa_2 = \begin{bmatrix} 1 & 0 & b_{2,1}^{(1)} & \ldots & b_{2,n-3}^{(1)} \\ & 1 & 0 & \ldots & 0 \\ & & & & \\ & & I_{n-2\times n-2} & & \\ & & & & \end{bmatrix}$$

$$\kappa_{\{1,2\}} = \begin{bmatrix} 1 & 0 & b_{2,1}^{(1)} & \ldots & b_{2,n-3}^{(1)} \\ & 1 & b_{2,1}^{(1)} & \ldots & b_{2,n-3}^{(1)} \\ & & & & \\ & & I_{n-2\times n-2} & & \\ & & & & \end{bmatrix}$$

and the cases

1 $\kappa_1 = 1_V \Leftrightarrow \mathbf{b}_2^{(1)} = 0$;

2 $\kappa_2 = 1_V \Leftrightarrow \mathbf{b}_2^{(1)} = 0$;

3 $\kappa_{\{1,2\}} = 1_V \Leftrightarrow \mathbf{b}_2^{(1)} = 0$.

Then there exist $2^{n-2}-1$ elementary abelian regular subgroups with $U(T) = \mathrm{Span}\{\mathbf{e}_3, \ldots, \mathbf{e}_n\}$ and $\begin{bmatrix} n \\ n-2 \end{bmatrix}_2 \cdot (2^{n-2}-1)$ subgroups of $\mathrm{AGL}(V,+)$ such that $\dim U(T) = n-2$. □

Proposition 2.1.30. *The groups of Corollary 2.1.29 are all conjugated.*

Proof. We need to proove that the groups such that $U(T) = \mathrm{Span}\{\mathbf{e}_3, \ldots, \mathbf{e}_n\}$ are all conjugated.

Each of those groups correspond to a vector $\mathbf{b}_2^{(1)} \in \mathbb{F}^{n-2} \setminus \{0\}$ as above. Consider two groups, $T = \langle \tau_{\mathbf{e}_1}, \ldots, \tau_{\mathbf{e}_n} \rangle$ and $T' = \langle \tau'_{\mathbf{e}_1}, \ldots, \tau'_{\mathbf{e}_n} \rangle$ corresponding to $\mathbf{b} = (b_{2,1}^{(1)}, \ldots, b_{2,n-3}^{(1)})$ and $\mathbf{b}' = (b_{2,1}^{\prime(1)}, \ldots, b_{2,n-3}^{\prime(1)})$, with same Hamming weight $w(\mathbf{b}) = w(\mathbf{b}')$. Then, there exists a permutation matrix $P \in \mathbb{F}^{n-2\times n-2}$ such that $\mathbf{b}P = \mathbf{b}'$. Let $P' \in \mathbb{F}^{n\times n}$ be the permutation matrix given by

$$P' = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & P & \\ 0 & 0 & & & \end{bmatrix}.$$

Note that when we multiply a matrix M by P' on the right, i.e. MP', we are permuting the last $n-2$ columns of M. On other hands when we multiply M by P'^{-1} on the left, we are permuting the last $n-2$ rows of M. So, we have $P'^{-1}\tau_{\mathbf{e}_i}P' = \tau'_{\mathbf{e}_iP'} = \tau'_{\mathbf{e}_{\sigma(i)}}$, where σ is the permutation on the indices related to P', thus $P'^{-1}TP' = T'$. That implies that two groups corresponding to vectors with same weight are conjugated.

Consider now two vectors in $\mathbb{F}^{n-2}$

$$(\underbrace{1,\dots,1}_{i},0,\dots,0) \text{ and } (\underbrace{1,\dots,1}_{i+1},0,\dots,0)$$

and the corresponding groups $T = \langle\tau_{\mathbf{e}_1},\dots,\tau_{\mathbf{e}_n}\rangle, T' = \langle\tau'_{\mathbf{e}_1},\dots,\tau'_{\mathbf{e}_n}\rangle$.

Let $P \in \mathbb{F}^{n\times n}$ be the matrix with rows $P_j = \mathbf{e}_j$ if $j \neq i+2$ and $P_{i+2} = \mathbf{e}_{i+2} + \mathbf{e}_{i+3}$,

$$P = \begin{bmatrix} 1 & 0 & & 0 & \dots & 0 \\ 0 & 1 & & 0 & \dots & 0 \\ \vdots & \vdots & & & & 0 \\ 0 & \dots & 1 & 1 & \dots & 0 \\ 0 & \dots & 0 & 1 & \dots & 0 \\ 0 & 0 & & & \dots & 1 \end{bmatrix}.$$

Note that when we multiply a matrix M by P on the right, we are changing the $i+3$-th column of M summing to it the $i+2$-th row. On other hands when we multiply a matrix M by $P^{-1} = P$ on the left, we are changing the $i+2$-th row of M summing to it the $i+3$-th row. So, we have $P\tau_{\mathbf{e}_j}P = \tau'_{\mathbf{e}_j}$ for $j \neq i+2$ and $P\tau_{(\mathbf{e}_{i+2}+\mathbf{e}_{i+3})}P = \tau'_{\mathbf{e}_{i+2}}$, implying $PTP = T'$. Then, all the groups are conjugated. □

2.1.1 Classes in small dimension

Here we report the classification of elementary abelian regular subgroups in $\mathrm{AGL}(V,+)$. We take into account $\dim(V) = 3,4,5,6$, the case 1 and 2 are obvious. We report these cases in Table 2.1.1 with the number of classes ($\mathcal{C}$'s), their cardinality ($|\mathcal{C}|$) and the dimension of the space $U(T)$ ($\dim(U_{\mathcal{C}})$). In Appendix A there are also reported the representatives of each class.

Remark 2.1.31. The cases $\dim(V) = 3,4$ are consequence of Corollary 2.1.28 and Corollary 2.1.29. For the other two cases we used MAGMA to obtain the classification.

n	$\mathcal{C}$'s	$\lvert\mathcal{C}\rvert$	$\dim(U_{\mathcal{C}})$
3	2	$\lvert\mathcal{C}_1\rvert = 1$	3
		$\lvert\mathcal{C}_2\rvert = 7$	1
4	2	$\lvert\mathcal{C}_1\rvert = 1$	4
		$\lvert\mathcal{C}_2\rvert = 105,$	2
5	4	$\lvert\mathcal{C}_1\rvert = 1$	5
		$\lvert\mathcal{C}_2\rvert = 1085$	3
		$\lvert\mathcal{C}_3\rvert = 6510$	2
		$\lvert\mathcal{C}_4\rvert = 868$	1
6	8	$\lvert\mathcal{C}_1\rvert = 1$	6
		$\lvert\mathcal{C}_2\rvert = 9765$	4
		$\lvert\mathcal{C}_3\rvert = 234360$	3
		$\lvert\mathcal{C}_4\rvert = 410130$	3
		$\lvert\mathcal{C}_5\rvert = 8202260$	2
		$\lvert\mathcal{C}_6\rvert = 218736$	2
		$\lvert\mathcal{C}_7\rvert = 546844$	2
		$\lvert\mathcal{C}_8\rvert = 1093680$	2

Table 2.1: Classes table

2.2 Differential properties of $\circ$-affine maps

In this section we establish a lower bound on the δ-differential uniformity of the maps lie in some $\mathrm{AGL}(V, \circ)$. We will consider the cases of affine group $\mathrm{AGL}(V, \circ)$ such that $T_\circ \subseteq \mathrm{AGL}(V, +)$ and/or $T_+ \subseteq \mathrm{AGL}(V, \circ)$. In all the two cases in the following proofs we can consider w.l.o.g. maps γ such that $0\gamma = 0$. Because in the first case we can compose γ with $\tau_{0\gamma}$ that maps 0γ in 0 and in the second case we compose with $\sigma_{0\gamma}$, in all the cases we compose with an affine map.

Lemma 2.2.1. *Let $T_\circ \subseteq \mathrm{AGL}(V, +)$ and $\dim(U(T_\circ)) = k$ and $\gamma \in \mathrm{AGL}(V, \circ)$, then $\delta(\gamma) \geq 2^k$.*

Proof. Let $\mathbf{a} \in U(T_\circ)$, then for all $\mathbf{x} \in V$

$$\begin{aligned}(\mathbf{x} + \mathbf{a})\gamma + \mathbf{x}\gamma &= (\mathbf{x} \circ \mathbf{a})\gamma + \mathbf{x}\gamma \\ &= (\mathbf{x}\gamma \circ \mathbf{a}\gamma) + \mathbf{x}\gamma.\end{aligned}$$

So, for all $\mathbf{x}\gamma \in U(T_\circ)$ we have

$$(\mathbf{x}\gamma \circ \mathbf{a}\gamma) + \mathbf{x}\gamma = (\mathbf{x}\gamma + \mathbf{a}\gamma) + \mathbf{x}\gamma = \mathbf{a}\gamma,$$

that means $U(T_\circ)\gamma^{-1} \subseteq \{\mathbf{x} \mid (\mathbf{x}+\mathbf{a})\gamma+\mathbf{x}\gamma = \mathbf{a}\gamma\}$, which implies $|\{\mathbf{x} \mid (\mathbf{x}+\mathbf{a})\gamma+\mathbf{x}\gamma = \mathbf{a}\gamma\}| \geq 2^k$. □

When $T_+ \subseteq \mathrm{AGL}(V,\circ)$, we can define $U_\circ(T_+) = \{\mathbf{a} \mid \sigma_\mathbf{a} \in T_+ \cap T_\circ\}$ and it is a vector subspace of $(V,\circ)$, and of $(V,+)$. Then we obtain, analogously, the following lemma.

Lemma 2.2.2. *Let $T_+ \subseteq \mathrm{AGL}(V,\circ)$ and $\dim(U_\circ(T_+)) = k$, as subspace of $(V,\circ)$. If $\gamma \in \mathrm{AGL}(V,\circ)$, then $\delta(\gamma) \geq 2^k$.*

Remark 2.2.3. By definition a square matrix is unipotent if and only if its characteristic polynomial $P(t)$ is a power of $t-1$, i.e. it has a unique eigenvalue equals to 1.

Lemma 2.2.4. *Let $T_\circ \subseteq \mathrm{AGL}(V,+)$. For each $\mathbf{a} \in V$, $\kappa_\mathbf{a}$ fixes at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ elements of V.*

Proof. $\kappa_\mathbf{a}$ has a unique eigenvalue equals to $1 \in \mathbb{F}_2$, then from Theorem 1.1.10 there exists a matrix over $\mathbb{F}_2$ in the Jordan form similar to $\kappa_\mathbf{a}$. Thus, $\kappa_\mathbf{a} = AJA^{-1}$, for some $A, J \in \mathrm{GL}(V,+)$ with

$$J = \begin{bmatrix} 1 & \alpha_1 & & \dots & 0 \\ 0 & 1 & \alpha_2 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & \dots & & 1 & \alpha_{n-1} \\ 0 & \dots & & & 1 \end{bmatrix} \text{ and } J^2 = \begin{bmatrix} 1 & 0 & \alpha_1\alpha_2 & & \dots & 0 \\ 0 & 1 & 0 & \alpha_2\alpha_3 & \dots & 0 \\ \vdots & & & & & \vdots \\ 0 & \dots & & 1 & 0 & \alpha_{n-2}\alpha_{n-1} \\ 0 & \dots & & & 1 & 0 \\ 0 & \dots & & & & 1 \end{bmatrix}.$$

where $\alpha_i \in \mathbb{F}_2$ for $1 \leq i \leq n-1$.

From the fact that J is conjugated to $\kappa_\mathbf{a}$ we have $J^2 = 1_V$, and that implies $\alpha_i\alpha_{i+1} = 0$ for all $1 \leq i \leq n-2$.

Note that if $\alpha_i = 1$ then α_{i-1} and α_{i+1} have to be equal to 0. Thus we have that when n is even at most $\frac{n}{2}$ α_i's can be equal to 1 and at least $\frac{n}{2}$ elements of the canonical basis are fixed by J. When n is odd we have at most $\frac{n-1}{2}$ α_i's equal to 1 then at least $\frac{n-1}{2}+1$ elements of the canonical basis are fixed by J. Our claim follows from the fact that $\kappa_\mathbf{a}$ is conjugated to J. □

In terms of algebras we have the following corollary.

Corollary 2.2.5. *Let $T_\circ \subseteq \mathrm{AGL}(V,+)$, and let $(V,+,\cdot)$ be the associated algebra of Theorem 2.1.2. Then for each $\mathbf{a} \in V$, $\mathbf{a}\cdot\mathbf{x}$ is equal to 0 for at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ $\mathbf{x} \in V$.*

Remark 2.2.6. The bound on the number of elements fixed by $\kappa_\mathbf{a}$ given in Lemma 2.2.4 is tight. In fact let $(V,+,\cdot)$ be the exterior algebra over a vector space of

dimension three, spanned by $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$. We have that $\mathbf{e}_1 \cdot \mathbf{x} = 0$ for all $\mathbf{x} \in E = \langle \mathbf{e}_1, \mathbf{e}_1 \wedge \mathbf{e}_2, \mathbf{e}_1 \wedge \mathbf{e}_3, \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3 \rangle$. So, for all $\mathbf{x} \in E$

$$\mathbf{x} \circ \mathbf{e}_1 = \mathbf{x} + \mathbf{e}_1 + \mathbf{x} \cdot \mathbf{e}_1 = \mathbf{x} + \mathbf{e}_1.$$

Vice versa if $\mathbf{x} \circ \mathbf{e}_1 = \mathbf{x} + \mathbf{e}_1$ then $\mathbf{x} \in E$. The cardinality of E is 2^4.

In fact, considering the translation by $\mathbf{e}_1$ with respect the new sum $\circ$. $\kappa_{\mathbf{e}_1}$ is given by the matrix

$$\kappa_{\mathbf{e}_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 1 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 0 & 0 \\ & & & 1 & 0 & 0 & 0 \\ & & & & 1 & 0 & 0 \\ & & & & & 1 & 1 \\ & & & & & & 1 \end{bmatrix},$$

and its Jordan form is

$$J = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 0 & 0 & 0 \\ & & & 1 & 1 & 0 & 0 \\ & & & & 1 & 0 & 0 \\ & & & & & 1 & 1 \\ & & & & & & 1 \end{bmatrix}$$

Lemma 2.2.7. *Let $T_\circ \subseteq \mathrm{AGL}(V, +)$ and $\gamma \in \mathrm{AGL}(V, \circ)$, then $\delta(\gamma) \geq 2^{\lfloor \frac{n-1}{2} \rfloor + 1}$.*

Proof. From Lemma 2.1.5 there exists $a \in U(T_\circ)$ different from zero. So

$$(\mathbf{x} + \mathbf{a})\gamma + \mathbf{x}\gamma = (\mathbf{x} \circ \mathbf{a})\gamma + \mathbf{x}\gamma = (\mathbf{x}\gamma \circ \mathbf{a}\gamma) + \mathbf{x}\gamma =$$

$$(\mathbf{x}\gamma + \mathbf{a}\gamma + \mathbf{a}\gamma \cdot \mathbf{x}\gamma) + \mathbf{x}\gamma$$

Now, from Corollary 2.2.5 we have that $\mathbf{a}\gamma \cdot \mathbf{x}\gamma = 0$ for at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ elements of V.

This implies $|\{\mathbf{x} \mid (\mathbf{x} + \mathbf{a})\gamma + \mathbf{x}\gamma = \mathbf{a}\gamma\}| \geq 2^{\lfloor \frac{n-1}{2} \rfloor + 1}$. □

Lemma 2.2.8. *Let $T_+ \subseteq \mathrm{AGL}(V, \circ)$ and $\gamma \in \mathrm{AGL}(V, \circ)$, then $\delta(\gamma) \geq 2^{\lfloor \frac{n-1}{2} \rfloor + 1}$.*

Proof. Note that Theorem 2.1.2, Lemma 2.1.5 and Corollary 2.2.5 hold also inverting the operation $\circ$ and $+$. Then, there exists $\mathbf{a} \in V$ different from zero such that $\mathbf{x}+\mathbf{a} = \mathbf{x}\circ\mathbf{a}$ for all $\mathbf{x} \in V$. Considering the algebra $(V, \circ, \cdot)$ such that $\mathbf{x}+\mathbf{y} = \mathbf{x}\circ\mathbf{y}\circ\mathbf{x}\cdot\mathbf{y}$ for all $\mathbf{x}, \mathbf{y} \in V$, we have

$$(\mathbf{x} + \mathbf{a})\gamma + \mathbf{x}\gamma = (\mathbf{x} \circ \mathbf{a})\gamma + \mathbf{x}\gamma = (\mathbf{x}\gamma \circ \mathbf{a}\gamma) + \mathbf{x}\gamma =$$

$$(\mathbf{x}\gamma \circ \mathbf{a}\gamma) \circ \mathbf{x}\gamma \circ \mathbf{x}\gamma \cdot (\mathbf{x}\gamma \circ \mathbf{a}\gamma) =$$

$$\mathbf{x}\gamma \circ \mathbf{a}\gamma \circ \mathbf{x}\gamma \circ \mathbf{x}\gamma \cdot \mathbf{x}\gamma \circ \mathbf{x}\gamma \cdot \mathbf{a}\gamma.$$

From Remark 2.1.3, we have $\mathbf{y}^2 = 0$ for all $\mathbf{y} \in V$, and from Corollary 2.2.5 $\mathbf{x}\gamma \cdot \mathbf{a}\gamma = 0$ for at least $2^{\lfloor \frac{n-1}{2} \rfloor + 1}$ elements. Thus $|\{\mathbf{x} \,|\, (\mathbf{x}+\mathbf{a})\gamma + \mathbf{x}\gamma = \mathbf{a}\gamma\}| \geq 2^{\lfloor \frac{n-1}{2} \rfloor + 1}$. □

So we obtain:

Theorem 2.2.9. *Let $T_\circ \subseteq \mathrm{AGL}(V,+)$ ($T_+ \subseteq \mathrm{AGL}(V,\circ)$, respectively) and $\gamma \in \mathrm{AGL}(V,\circ)$, then $\delta(\gamma) \geq 2^m$, where $m = \max\{\lfloor \frac{n-1}{2} \rfloor + 1, \dim(U(T_\circ))\}$ ($m = \max\{\lfloor \frac{n-1}{2} \rfloor + 1, \dim(U_\circ(T_+))\}$, respectively).*

For the case when $T_\circ \subseteq \mathrm{AGL}(V,+)$ and $T_+ \subseteq \mathrm{AGL}(V,\circ)$ we can obtain also the following.

Lemma 2.2.10. *Let $T_\circ \subseteq \mathrm{AGL}(V,+)$ be such that $T_+ \subseteq \mathrm{AGL}(V,\circ)$. If $\gamma \in \mathrm{AGL}(V,\circ)$, then $\delta(\gamma) \geq 2^{n-k}$, where $k = \dim(U(T_\circ))$.*

Proof. W.l.o.g. $U(T_\circ) = \mathrm{Span}\{\mathbf{e}_{n-k+1}, \ldots, \mathbf{e}_n\}$. From Theorem 2.1.21 for all $\mathbf{v} \in V$

$$\kappa_{\mathbf{v}} = \begin{bmatrix} I_{n-k \times n-k} & B_{\mathbf{v}} \\ 0 & I_{k \times k} \end{bmatrix},$$

$B_{\mathbf{v}} \in \mathbb{F}^{n-k \times k}$. Let $B_{\mathbf{v}}^\perp = \{\mathbf{x} \in V \mid x_{n-k+1} = \cdots = x_n = 0, (x_1, \ldots, x_{n-k})B_{\mathbf{v}} = 0\}$, then $\dim(B_{\mathbf{v}}^\perp) \geq n - 2k$. Let $W = B_{\mathbf{v}}^\perp \oplus U(T_\circ)$, thus for all $\mathbf{w} \in W$ we have $\mathbf{v} \cdot \mathbf{w} = 0$, where the product is that of the algebra associated to $T_\circ$. Let $\gamma \in \mathrm{AGL}(V,\circ)$ and $\mathbf{a} \in U(T_\circ)$, then

$$\begin{aligned}(\mathbf{x}+\mathbf{a})\gamma + \mathbf{x}\gamma &= (\mathbf{x}\gamma \circ \mathbf{a}\gamma) + \mathbf{x}\gamma \\ &= \mathbf{a}\gamma + \mathbf{x}\gamma\mathbf{a}\gamma.\end{aligned}$$

For all $\mathbf{x}\gamma \in B_{\mathbf{a}\gamma}^\perp \oplus U(T_\circ)$ we have $(\mathbf{x}+\mathbf{a})\gamma + \mathbf{x}\gamma = \mathbf{a}\gamma$, thus $|\{\mathbf{x} \,|\, (\mathbf{x}+\mathbf{a})\gamma + \mathbf{x}\gamma = \mathbf{a}\gamma\}| \geq 2^{n-k}$ □

Theorem 2.2.11. *Let $T_\circ \subseteq \mathrm{AGL}(V,+)$ be such that $T_+ \subseteq \mathrm{AGL}(V,\circ)$. If $\gamma \in \mathrm{AGL}(V,\circ)$, then $\delta(\gamma) \geq 2^m$, where $m = \max\{\dim(U(T_\circ)), n - \dim(U(T_\circ))\}$.*

2.2.1 Differential Uniformity for $\dim(V) = 3, 4, 5$

For the cases with $3 \leq \dim(V) \leq 5$ we found the minimum differential uniformity of the function in an affine group $\mathrm{AGL}(V,\circ)$, containing the usual translation group, using the software MAGMA. For case $\dim(V) = 2$ we already know that $\mathrm{Sym}(V) = \mathrm{AGL}(V,+)$, thus it is not interesting. Up to compose by an affine map we can

study only the maps lie in $GL(V, \circ)$. Moreover the classes are conjugated w.r.t. an element of $\mathrm{AGL}(V, +)$, then we can take into account only a representative for each class of elementary abelian regular subgroups. We can restrict our study to the set $H = \{\gamma \in \mathrm{GL}(V, \circ) \mid \mathbf{v}_1\gamma \neq \mathbf{v}_2 \text{ for all } \mathbf{v}_1, \mathbf{v}_2 \in U(T_\circ) \setminus \{0\}\}$, because if $\mathbf{v}_1\gamma = \mathbf{v}_2$, for some $\mathbf{v}_1, \mathbf{v}_2 \in U(T_\circ)$, we have $|\{\mathbf{x} \mid (\mathbf{x} + \mathbf{v}_1)\gamma + \mathbf{x}\gamma = \mathbf{v}_2\}| = 2^n$. By an exhaustive research we obtain the following theorem.

Theorem 2.2.12. *Let $3 \leq \dim(V) = n \leq 5$, and let $T_+ \subseteq \mathrm{AGL}(V, \circ)$. Then for each $\gamma \in \mathrm{AGL}(V, \circ)$, $\delta(\gamma) \geq 2^{n-1}$.*

For the case $n = 6$ it is not possible to do a direct check of the differential uniformity of the affine groups, but for $n = 7$ we will prove that there exists $\gamma \in \mathrm{AGL}(V, \circ)$ with $\delta(\gamma) = 2^{7-2}$ for some operation $\circ$ such that $T_+ \subseteq \mathrm{AGL}(V, \circ)$.

Lemma 2.2.13. *Let $T_{\circ_1}$ and $T_{\circ_2}$ be elementary abelian regular groups such that $T_{\circ_1} \subseteq \mathrm{AGL}(V, +)$, $T_+ \subseteq \mathrm{AGL}(V, \circ_2)$ and the associated algebra are isomorphic. Define $\delta_{\circ_1}(\gamma) = \max_{\mathbf{a},\mathbf{b}} |\{\mathbf{x} \mid (\mathbf{x} \circ_1 \mathbf{a})\gamma \circ_1 \mathbf{x}\gamma = \mathbf{b}\}|$, then there exists $\gamma' \in \mathrm{AGL}(V, +)$ with $\delta_{\circ_1}(\gamma') = \delta$ if and only if there exists $\gamma \in \mathrm{AGL}(V, \circ_2)$ with $\delta(\gamma) = \delta$*

Proof. From Theorem 2.1.2 there exist two algebra $(V, +, \cdot)$ and $(V, \circ_2, *)$ related to $T_{\circ_1}$ and T_+ respectively. Consider $\phi : (V, \circ_2, *) \to (V, +, \cdot)$ be an isomorphism of algebra and let $\gamma \in \mathrm{AGL}(V, \circ_2)$, then $\gamma' = \phi^{-1}\gamma\phi \in \mathrm{AGL}(V, +)$.

Let $\mathbf{a} \in V$, thus, recalling that $\mathbf{x} \circ_1 \mathbf{y} = \mathbf{x} + \mathbf{y} + \mathbf{x} \cdot \mathbf{y}$ and $\mathbf{x} + \mathbf{y} = \mathbf{x} \circ_2 \mathbf{y} \circ_2 \mathbf{x} * \mathbf{y}$ we have $(\mathbf{x} \circ_1 \mathbf{y})\phi^{-1} = \mathbf{x}\phi^{-1} + \mathbf{y}\phi^{-1}$ and

$$\begin{aligned}(\mathbf{x} \circ_1 \mathbf{a})\gamma' \circ_1 \mathbf{x}\gamma' &= (\mathbf{x}\phi^{-1} + \mathbf{a}\phi^{-1})\gamma\phi \circ_1 \mathbf{x}\phi^{-1}\gamma\phi \\ &= ((\mathbf{x}\phi^{-1} + \mathbf{a}\phi^{-1})\gamma + \mathbf{x}\phi^{-1}\gamma)\phi.\end{aligned}$$

Then $|\{\mathbf{x} \mid (\mathbf{x} \circ_1 \mathbf{a})\gamma' \circ_1 \mathbf{x}\gamma' = \mathbf{b}\}| = |\{\mathbf{x} \mid (\mathbf{x} + \mathbf{a}\phi^{-1})\gamma + \mathbf{x}\gamma = \mathbf{b}\phi\}|$. □

Corollary 2.2.14. *Let $n = 7$. There exists $T_\circ$ such that $T_+ \subseteq \mathrm{AGL}(V, \circ)$ and $\gamma \in \mathrm{AGL}(V, \circ)$ with $\delta(\gamma) = 2^{n-2}$.*

Proof. Consider $T_{\circ_1}$ corresponding to the algebra as in Remark 2.2.6. Let $\phi : (V, \circ_1) \to (V, +)$ be an isomorphism of vector space. Then $\phi^{-1}T_{\circ_1}\phi = T_+$, in fact for all $\mathbf{x}, \mathbf{y} \in V$ we have $\mathbf{x}\phi^{-1}\tau_{\mathbf{y}}\phi = (\mathbf{x}\phi^{-1} \circ_1 \mathbf{y})\phi = \mathbf{x} + \mathbf{y}\phi$. So, considering $T_{\circ_2} = \phi^{-1}T_+\phi$, we have $T_+ \subseteq \mathrm{AGL}(V, \circ_2) = \phi^{-1}\mathrm{AGL}(V, +)\phi$. Let $(V, +, \cdot)$ and $(V, \circ_2, *)$ be the associated algebras of $T_{\circ_1}$ and T_+, respectively, then ϕ is an isomorphism of algebra. In fact, let $\mathbf{y} \in V$ and $\sigma_{\mathbf{y}} : \mathbf{x} \mapsto \mathbf{x} + \mathbf{y}$, thus $\mathbf{x}\phi^{-1}\sigma_{\mathbf{y}}\phi = \mathbf{x} \circ_2 \mathbf{y}\phi$ from the fact that $0\sigma_{\mathbf{y}} = \mathbf{y}$ and $0\phi^{-1} = 0$. Then $(\mathbf{x} + \mathbf{y})\phi = \mathbf{x}\phi\phi^{-1}\sigma_{\mathbf{y}}\phi = \mathbf{x}\phi \circ_2 \mathbf{y}\phi$. More over

$$(\mathbf{x} \circ_1 \mathbf{y})\phi = (\mathbf{x} + \mathbf{y} + \mathbf{x} \cdot \mathbf{y})\phi = \mathbf{x}\phi \circ_2 \mathbf{y}\phi \circ_2 (\mathbf{x} \cdot \mathbf{y})\phi$$

and

$$(\mathbf{x} \circ_1 \mathbf{y})\phi = \mathbf{x}\phi + \mathbf{y}\phi = \mathbf{x}\phi \circ_2 \mathbf{y}\phi \circ_2 \mathbf{x}\phi * \mathbf{y}\phi,$$

this implies $(\mathbf{x} \cdot \mathbf{y})\phi = \mathbf{x}\phi * \mathbf{y}\phi$ for all $\mathbf{x}, \mathbf{y} \in V$, thus ϕ is an isomorphism of algebra.

Let $\gamma \in \mathrm{AGL}(V, +)$ given from the univariate polynomial

$$\gamma(x) = e^{105}x^{64} + e^{88}x^{32} + e^{10}x^{16} + e^{12}x^8 + e^{50}x^4 + e^{37}x^2 + e^{60}x$$

where e is a primitive element of $\mathbb{F}_{2^7}$, it results $\delta_{\circ_1}(\gamma) = 2^{7-2}$. From the lemma above we have our claim. □

Moreover in dimension 8 we have the following example.

Example 2.2.15. Let $T_\circ \subseteq \mathrm{AGL}(V, +)$ be such that

$$\kappa_{\mathbf{e}_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 0 & 1 & 1 \\ & & & 1 & 0 & 0 & 0 & 1 \\ & & & & 1 & 0 & 0 & 0 \\ & & & & & 1 & 1 & 0 \\ & & & & & & 1 & 0 \\ & & & & & & & 1 \end{bmatrix} \quad \kappa_{\mathbf{e}_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 0 & 0 & 1 & 0 \\ & & & 1 & 0 & 0 & 1 & 0 \\ & & & & 1 & 0 & 1 & 1 \\ & & & & & 1 & 0 & 1 \\ & & & & & & 1 & 0 \\ & & & & & & & 1 \end{bmatrix}$$

$$\kappa_{\mathbf{e}_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ & & 1 & 0 & 0 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 & 0 & 1 \\ & & & & 1 & 0 & 0 & 1 \\ & & & & & 1 & 0 & 0 \\ & & & & & & 1 & 0 \\ & & & & & & & 1 \end{bmatrix} \quad \kappa_{\mathbf{e}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ & & 1 & 0 & 0 & 0 & 0 & 1 \\ & & & 1 & 0 & 0 & 0 & 0 \\ & & & & 1 & 0 & 0 & 1 \\ & & & & & 1 & 1 & 1 \\ & & & & & & 1 & 0 \\ & & & & & & & 1 \end{bmatrix}$$

$$\kappa_{\mathbf{e}_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 0 & 0 & 0 & 1 \\ & & & 1 & 0 & 0 & 0 & 1 \\ & & & & 1 & 0 & 0 & 0 \\ & & & & & 1 & 0 & 1 \\ & & & & & & 1 & 0 \\ & & & & & & & 1 \end{bmatrix} \quad \kappa_{\mathbf{e}_6} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 & 1 & 1 \\ & & & & 1 & 0 & 0 & 1 \\ & & & & & 1 & 0 & 0 \\ & & & & & & 1 & 0 \\ & & & & & & & 1 \end{bmatrix}$$

and $\kappa_{\mathbf{e}_7} = \kappa_{\mathbf{e}_8} = 1_V$. From Theorem 2.1.21 $T_+ \subseteq \mathrm{AGL}(V, \circ)$ and by a computer check, let α be a primitive element of $\mathbb{F}_{2^8}$ such that $\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$,

$$\begin{aligned} f(x) =& \alpha^{160}x^{224} + \alpha^{14}x^{208} + \alpha^{161}x^{200} + \alpha^{191}x^{196} + \alpha^{109}x^{194} + \alpha^{251}x^{193} + \alpha^{33}x^{192} + \alpha^{226}x^{176} + \\ & \alpha^{27}x^{168} + \alpha^{202}x^{164} + \alpha^{15}x^{162} + \alpha^{230}x^{161} + \alpha^{32}x^{160} + \alpha^{2}x^{152} + \alpha^{22}x^{148} + \alpha^{250}x^{146} + \\ & \alpha^{96}x^{145} + \alpha^{65}x^{144} + \alpha^{50}x^{140} + \alpha^{104}x^{138} + \alpha^{161}x^{137} + \alpha^{152}x^{136} + \alpha^{181}x^{134} + \alpha^{215}x^{133} + \\ & \alpha^{217}x^{132} + \alpha^{236}x^{131} + \alpha^{226}x^{130} + \alpha^{33}x^{129} + \alpha^{7}x^{128} + \alpha^{58}x^{112} + \alpha^{73}x^{104} + \alpha^{68}x^{100} + \\ & \alpha^{48}x^{98} + \alpha^{146}x^{97} + \alpha^{47}x^{96} + \alpha^{235}x^{88} + \alpha^{142}x^{84} + \alpha^{186}x^{82} + \alpha^{157}x^{81} + \alpha^{157}x^{80} + \alpha^{184}x^{76} + \\ & \alpha^{150}x^{74} + \alpha^{29}x^{73} + \alpha^{230}x^{72} + \alpha^{16}x^{70} + \alpha^{218}x^{69} + \alpha^{47}x^{68} + \alpha^{49}x^{67} + \alpha^{99}x^{66} + \alpha^{208}x^{65} + \\ & \alpha^{23}x^{64} + \alpha^{209}x^{56} + \alpha^{123}x^{52} + \alpha^{60}x^{50} + \alpha^{175}x^{49} + \alpha^{3}x^{48} + \alpha^{90}x^{44} + \alpha^{33}x^{42} + \alpha^{35}x^{41} + \\ & \alpha^{180}x^{40} + \alpha^{119}x^{38} + \alpha^{30}x^{37} + \alpha^{206}x^{36} + \alpha^{133}x^{35} + \alpha^{159}x^{34} + \alpha^{222}x^{33} + \alpha^{42}x^{32} + \alpha^{16}x^{28} + \\ & \alpha^{104}x^{26} + \alpha^{27}x^{25} + \alpha^{31}x^{24} + \alpha^{32}x^{22} + \alpha^{41}x^{21} + \alpha^{124}x^{20} + \alpha^{218}x^{19} + \alpha^{28}x^{17} + \alpha^{150}x^{16} + \\ & \alpha^{92}x^{14} + \alpha^{241}x^{13} + \alpha^{192}x^{12} + \alpha^{147}x^{11} + \alpha^{24}x^{10} + \alpha^{197}x^{9} + \alpha^{119}x^{8} + \alpha^{53}x^{7} + \alpha^{218}x^{6} + \\ & \alpha^{86}x^{5} + \alpha^{14}x^{4} + \alpha^{139}x^{3} + \alpha^{88}x^{2} + \alpha^{85}x + \alpha^{34} \end{aligned}$$

is 2^6-differentially uniform and $f \in \mathrm{AGL}(V, \circ)$. In this case we have that the bound given in Theorem 2.2.11 is thigh.

Remark 2.2.16. Note that if we consider a 4 differentially uniform boolean function γ over $\mathbb{F}^4$. Then the parallel map (γ, γ) acting on $\mathbb{F}^8$ results 2^6 differentially uniform. Thus the differential uniformity may not guarantee, alone, security from a hidden sum trapdoor.

2.3 Some conditions coming from the mixing layer

Recalling that a square-matrix A is MDS (Maximum Distance Separable) if each minor of A is non-zero, we give the following definition.

Definition 2.3.1. *Let $\lambda \in \mathrm{GL}(V)$ be a mixing layer of a block cipher acting on the message space $V = V_1 \oplus \cdots \oplus V_n$, with $V_i = \mathbb{F}^m$ for all i, then λ is called MDS mixing layer if there exists an equivalent map $\lambda' \in \mathrm{GL}(\mathbb{F}_{2^m}^n)$ that is an MDS matrix.*

Many modern block ciphers, such as Square [DKR97], SHARK [RDP+96], AES, use MDS mixing layer. This MDS property is used to ensure that the number of active S-boxes involved in a differential or linear attack increases rapidly, and the security against these particular attacks can be established.

Proposition 2.3.2. *Let $V = \bigoplus_{i=1}^{s} V_i$ and $\gamma = (\gamma_1, \ldots, \gamma_s)$ be a parallel S-box with $\gamma_i \notin \mathrm{AGL}(V_i, +)$ for all i. If λ is a MDS mixing layer and $\gamma\lambda \in \mathrm{AGL}(V, \circ)$, for some operation $\circ$, then $\circ$ cannot be an operation that works in parallel on the bricks.*

Proof. Assume by contradiction $\circ = (\circ_1, \dots, \circ_s)$ where $\circ_i$ is such that $(V_i, \circ_i)$ is a vector space for all i.

Let the MDS map λ'

$$\lambda' = \begin{bmatrix} \mathbf{a}_{1,1} & \dots & \mathbf{a}_{1,s} \\ \vdots & & \vdots \\ \mathbf{a}_{s,1} & \dots & \mathbf{a}_{s,s} \end{bmatrix}$$

and the corresponding MDS mixing layer λ

$$\lambda = \begin{bmatrix} A_{1,1} & \dots & A_{1,s} \\ \vdots & & \vdots \\ A_{s,1} & \dots & A_{s,s} \end{bmatrix}.$$

λ MDS mixing layer implies that $A_{i,j} \in \mathrm{GL}(V_j)$ for all i, j. W.l.o.g. we can suppose $0\gamma = 0$. Let $\mathbf{x} = (\mathbf{x}_1, 0, \dots, 0)$ and $\mathbf{y} = (\mathbf{y}_1, 0, \dots, 0)$, then $\mathbf{x} \circ \mathbf{y} = (\mathbf{x}_1 \circ_1 \mathbf{y}_1, 0, \dots, 0)$.

$\gamma\lambda \in \mathrm{GL}(V, \circ)$ implies $\mathbf{x}\gamma\lambda \circ \mathbf{y}\gamma\lambda = (\mathbf{x} \circ \mathbf{y})\gamma\lambda$, that is

$$(\mathbf{x}_1\gamma_1 A_{1,1} \circ_1 \mathbf{y}_1\gamma_1 A_{1,1}, \dots, \mathbf{x}_1\gamma_1 A_{1,s} \circ_1 \mathbf{y}_1\gamma_1 A_{1,s}) = ((\mathbf{x}_1 \circ_1 \mathbf{y}_1)\gamma_1 A_{1,1}, \dots, (\mathbf{x}_1 \circ_1 \mathbf{y}_1)\gamma_1 A_{1,s})$$

That implies

$$\mathbf{x}_1\gamma_1 A_{1,1} \circ_1 \mathbf{y}_1\gamma_1 A_{1,1} = (\mathbf{x}_1 \circ_1 \mathbf{y}_1)\gamma_1 A_{1,1}$$

for all $\mathbf{x}_1, \mathbf{y}_1 \in V_1$, then $\gamma_1 \mathbf{A}_{1,1} \in \mathrm{GL}(V_1, \circ_1)$.

Similarly, considering $\mathbf{x} = (\mathbf{x}_1, 0, \dots, 0)$ and $\mathbf{y} = (0, \mathbf{y}_2, \dots, 0)$ we obtain

$$\mathbf{x}_1\gamma_1 A_{1,1} \circ_1 \mathbf{y}_2\gamma_2 A_{2,1} = \mathbf{x}_1\gamma_1 A_{1,1} + \mathbf{y}_2\gamma_2 A_{2,1}$$

for all $\mathbf{x}_1 \in V_1$. This is equivalent to $\mathbf{x} \circ_1 \mathbf{y} = \mathbf{x} + \mathbf{y}$ for all $\mathbf{x}, \mathbf{y} \in V_1$, then $\circ_1$ coincides with the sum $+$, and $A_{1,1}\gamma_1 \in \mathrm{GL}(V_1, +)$. So $\gamma_1 \in \mathrm{GL}(V_1, +)$, that is not possible. □

Proposition 2.3.3. *Let $\lambda \in \mathrm{GL}(V, +)$ and $T_\circ \subset \mathrm{AGL}(V, +)$. If $\lambda \in \mathrm{GL}(V, \circ)$, then $U(T_\circ)\lambda = U(T_\circ)$.*

Proof. Let $\mathbf{w} \in U(T_\circ)$, for all $\mathbf{v} \in V$ we have

$$\mathbf{w}\lambda \circ \mathbf{v}\lambda = (\mathbf{w} \circ \mathbf{v})\lambda = (\mathbf{w} + \mathbf{v})\lambda = \mathbf{w}\lambda + \mathbf{v}\lambda$$

thus $\mathbf{w}\lambda \in U(T_\circ)$ and $U(T_\circ)\lambda = U(T_\circ)$. □

2.4 Attack based on hidden sum

2.4.1 Affine maps normalized by the translation group

In this subsection we want to explain the reason why we concentrate our studies on translation groups coming from subgroups in $\mathrm{AGL}(V, +)$, which are normalized by the usual translation group T_+.

To embed a hidden sum trapdoor in a block cipher we need $\Gamma_\infty \subseteq \mathrm{AGL}(V, \circ)$ for some hidden sum $\circ$, thus a first condition is $T_+ \subseteq \mathrm{AGL}(V, \circ)$, as $T_+ \subset \Gamma_\infty$. Now, let $T_\circ \subseteq \mathrm{AGL}(V, +)$ be such that $T_+ \subseteq \mathrm{AGL}(V, \circ)$. Consider the vector space $U(T_\circ)$, which has dimension k for some $k \geq 1$. Let $g \in \mathrm{GL}(V, +)$ be such that $U(T_\circ)g = \mathrm{Span}\{\mathbf{e}_{n-k+1}, \ldots, \mathbf{e}_n\} = U(T_\square)$, with $T_\square = g^{-1}T_\circ g$. It is easy to check that g is an isomorphism of vector space between $(V, \circ)$ and $(V, \square)$. From Theorem 2.1.21 we have that the maps relatives to the canonical basis vectors are

$$\kappa_{\mathbf{e}_i} = \begin{bmatrix} I_{n-k \times n-k} & B_{\mathbf{e}_i} \\ 0 & I_{k \times k} \end{bmatrix},$$

for some $B_{\mathbf{e}_i} \in \mathbb{F}^{n-k \times k}$. Moreover from Lemma 2.1.7 we have also that $\mathbf{e}_1, \ldots, \mathbf{e}_n$ is a basis of $(V, \square)$ and to write $\mathbf{v} \in V$ as a linear combination of these w.r.t. to the sum $\square$, i.e. $\mathbf{v} = \lambda_1 \mathbf{e}_1 \square \ldots \square \lambda_n \mathbf{e}_n$, we can use the Algorithm 1.

Algorithm 1.
Input: *vector* $\mathbf{v} = (v_1, \ldots, v_n) \in V$
Output: *coefficients* $\lambda_1 \ldots \lambda_n$.
[1] $\lambda_i \leftarrow v_i$ *for* $1 \leq i \leq n - k$;
[2] $\mathbf{v}' \leftarrow \mathbf{v}\tau_{\mathbf{e}_1}^{\lambda_1} \cdots \tau_{\mathbf{e}_{n-k}}^{\lambda_{n-k}}$;
[3] $\lambda_i \leftarrow v'_i$ *for* $n - k + 1 \leq i \leq n$;
return $\lambda_1, \ldots, \lambda_n$,

Where $\tau_{\mathbf{e}_i}$ is the translation $x \mapsto x \square \mathbf{e}_i$ and the notation $\mathbf{x}\tau_{\mathbf{v}}^b$, with $b \in \mathbb{F}_2$, denote either $\mathbf{x}\tau_{\mathbf{v}}$ (when $b = 1$) or $\mathbf{x}$ (when $b = 0$). Thus, let $\mathbf{v}_i = \mathbf{e}_i g^{-1}$ for all i, applying Algorithm 1 to $\mathbf{v}g$ we can obtain the combination of $\mathbf{v}_i$'s w.r.t the sum $\circ$ of the vector $\mathbf{v}$. The complexity of this procedure is $\mathcal{O}(n^3)$.

If $T_+ \subseteq \mathrm{AGL}(V, \circ)$, but $T_\circ \nsubseteq \mathrm{AGL}(V, +)$, then for any basis of $(V, \circ)$ there exists a vector $\mathbf{v}$ such that $\tau_{\mathbf{v}} \notin \mathrm{AGL}(V, +)$, thus we need to apply a non-linear map to vectors of length n, which might implies an huge quantity of memory.

2.4.2 Basic attack

Let $\mathcal{C} = \{\varphi_k \mid k \in \mathcal{K}\}$ be a tb cipher such that $\Gamma_\infty \subseteq \mathrm{AGL}(V, \circ)$ for some operation $\circ$, and also $T_\circ \subseteq \mathrm{AGL}(V, +)$. Let $\dim(U(T_\circ)) = k$. Let $g \in \mathrm{GL}(V, +)$ be a linear transformation such that $U(T_\circ)g = \mathrm{Span}\{\mathbf{e}_{n-k+1}, \ldots, \mathbf{e}_n\}$. Denote by

$$[\mathbf{v}] = [\lambda_1, \ldots, \lambda_n]$$

the vector with the coefficients obtained from Algorithm 1. Let $\varphi = \varphi_{\bar{k}}$ be the encryption function, with a given unknown session key $\bar{k}$. We are able to mount an

attack, computing the matrix M and the translation vector t defining $\varphi \in \mathrm{AGL}(V, \circ)$. Chose the plaintext $0\varphi, \mathbf{v}_1\varphi, \ldots, \mathbf{v}_n\varphi$, where $\mathbf{v}_i = \mathbf{e}_i g^{-1}$, and compute $[0\varphi g]$, $[\mathbf{v}_1\varphi g], \ldots, [\mathbf{v}_n\varphi g]$, since the translation vector is $[t] = [0\varphi g]$ and the $[\mathbf{e}_i\varphi g] + [t]$'s are the matrix rows. In other words, we will have

$$[\mathbf{v}\varphi g] = [\mathbf{v}g] \cdot M + [t], \quad [\mathbf{v}\varphi^{-1} g] = ([\mathbf{v}g] + [t]) \cdot M^{-1},$$

for all $\mathbf{w} \in V$, where the product row by column is the standard scalar product. The knowledge of M and M^{-1} provides a global deduction (reconstruction), since it becomes trivial to encrypt and decrypt. Moreover from $[\mathbf{v}g] = [\lambda_1 \ldots, \lambda_n]$ we obtain that $\mathbf{v} = 0\tau_{\mathbf{v}_1}^{\lambda_1} \cdots \tau_{\mathbf{v}_n}^{\lambda_n}$, where $\tau_{\mathbf{v}_i} : x \mapsto x \circ \mathbf{v}_i$. So, we need only $n + 1$ plaintext to reconstruct the cipher and the cost of this attack is given from the algorithm above to compute the combinations plus the cost of $n + 1$ encryptions.

Our discussion has thus proved the following result.

Theorem 2.4.1. *Hidden sum trapdoors coming from translation groups such that $T_\circ \subseteq \mathrm{AGL}(V, +)$ are (practical) full trapdoors.*

2.4.3 A toy-block cipher with a hidden sum

In this section we give an example, in a small dimension, of a translation based block cipher in which it is possible to embed a hidden-sum trapdoor.

Let $m = 3$, $n = 2$, then $d = 6$ and we have the message space $V = \mathbb{F}^6$. The mixing layer of our toy cipher is given by the matrix

$$\lambda = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Note that λ is a proper mixing layer. The bricklayer transformation $\gamma = (\gamma_1, \gamma_2)$ of our toy cipher is given by two identical S-boxes

$$\gamma_1 = \gamma_2 = \alpha^5 x^6 + \alpha x^5 + \alpha^2 x^4 + \alpha^5 x^3 + \alpha x^2 + \alpha x$$

where α is a primitive element of $\mathbb{F}_{2^3}$ such that $\alpha^3 = \alpha + 1$.

We show now the existence of a hidden-sum trapdoor for our toy cipher. We consider the hidden sum $\circ$ over $V_1 = V_2 = \mathbb{F}^3$ induced by the elementary abelian

regular group $T_\circ = \langle \tau_1, \tau_2, \tau_3 \rangle$, where

$$\mathbf{x}\tau_1 = \mathbf{x} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} + \mathbf{e}_1,\ \mathbf{x}\tau_2 = \mathbf{x} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \mathbf{e}_2,\ \mathbf{x}\tau_3 = \mathbf{x} \cdot \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \mathbf{e}_3. \tag{2.9}$$

Obviously $T = T_\circ \times T_\circ$ is an elementary abelian group inducing the hidden sum $(\mathbf{x}_1, \mathbf{x}_2) \circ' (\mathbf{y}_1, \mathbf{y}_2) = (\mathbf{x}_1 \circ y_1, \mathbf{x}_2 \circ \mathbf{y}_2)$ on $V = V_1 \times V_2$.

Theorem 2.4.2. $\langle T_+, \gamma\lambda \rangle \subseteq \mathrm{AGL}(V, \circ')$.

Proof. By a computer cheek $\gamma\lambda \in \mathrm{AGL}(V, \circ')$, and from Theorem 2.1.18 $T_+ \subseteq \mathrm{AGL}(V, \circ')$. □

Thanks to the previous theorem, $\circ'$ is a hidden sum for our toy cipher, but it remains to verify whether it is possible to use it to attack the toy cipher with an attack that costs less than brute force. We have not discussed the key schedule and the number of rounds yet. We have in mind a cipher where the number of rounds is so large to make any classical attack useless (such as differential cryptanalysis) and the key scheduling offer no weakness. Therefore, the hidden sum will actually be essential to break the cipher only if the attack that we build will cost significantly less than 64 encryptions, considering that the key space is $\mathbb{F}^6$.

Remark 2.4.3. Given a sum $\square$, the vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ may not be a linear basis of $(V_1, \square)$. For this specific sum $\circ$, the vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ actually form a basis for $(V_1, \circ)$ as their $\circ$-translation generate $T_\circ$. Let $\mathbf{x} = (x_1, x_2, x_3) \in V_1$, from (2.9) we can simply write

$$\mathbf{x}\tau_1 = (x_1 + 1, x_2 + x_3, x_3), \mathbf{x}\tau_2 = (x_1, x_2 + 1, x_3), \mathbf{x}\tau_3 = (x_1, x_1 + x_2, x_3 + 1).$$

Let us write $\mathbf{x}$ as a linear combination of $\mathbf{e}_1$, $\mathbf{e}_2$ and $\mathbf{e}_3$ w.r.t. to the sum $\circ$, i.e. $\mathbf{x} = \lambda_1\mathbf{e}_1 \circ \lambda_2\mathbf{e}_2 \circ \lambda_3\mathbf{e}_3$. We claim that $\lambda_1 = x_1$, $\lambda_3 = x_3$ and $\lambda_2 = \lambda_1\lambda_3 + x_2$. In fact

$$\begin{aligned} \mathbf{x} &= (\lambda_1\mathbf{e}_1 \circ \lambda_2\mathbf{e}_2) \circ \lambda_3\mathbf{e}_3 = (\lambda_1\mathbf{e}_1 \circ \lambda_2\mathbf{e}_2)\tau_3^{\lambda_3} = ((\lambda_1\mathbf{e}_1)\tau_2^{\lambda_2})\tau_3^{\lambda_3} = ((\lambda_1\mathbf{e}_1)\tau_3^{\lambda_3})\tau_2^{\lambda_2} \\ &= ((\lambda_1, 0, 0)\tau_3^{\lambda_3})\tau_2^{\lambda_2} = (\lambda_1, \lambda_3\lambda_1, \lambda_3)\tau_2^{\lambda_2} = (\lambda_1, \lambda_1\lambda_3 + \lambda_2, \lambda_3). \end{aligned}$$

So

$$(x_1, x_2, x_3) = \mathbf{x} = (\lambda_1, \lambda_1\lambda_3 + \lambda_2, \lambda_3)$$

and our claim is proved.

Thanks to the previous remark we can find the coefficients of a vector $\mathbf{w} = (\mathbf{v}, \mathbf{u}) \in V$ with respect to $\circ'$ by using the following algorithm separately on the two bricks of $\mathbf{w}$.

Algorithm 2.
Input: *vector* $\mathbf{x} \in \mathbb{F}_2^3$
Output: *coefficients* λ_1, λ_2 *and* λ_3.
[1] $\lambda_1 \leftarrow x_1$;
[2] $\lambda_3 \leftarrow x_3$;
[3] $\lambda_2 \leftarrow \lambda_1\lambda_3 + x_2$;
return $\lambda_1, \lambda_2, \lambda_3$.

Let $\mathbf{w} = (\mathbf{v}, \mathbf{u}) \in V$, we write

$$\mathbf{v} = \lambda_1^{\mathbf{v}}\mathbf{e}_1 \circ \lambda_2^{\mathbf{v}}\mathbf{e}_2 \circ \lambda_3^{\mathbf{v}}\mathbf{e}_3 \text{ and } \mathbf{u} = \lambda_1^{\mathbf{u}}\mathbf{e}_1 \circ \lambda_2^{\mathbf{u}}\mathbf{e}_2 \circ \lambda_3^{\mathbf{u}}\mathbf{e}_3.$$

We denote by

$$[\mathbf{w}] = [\lambda_1^{\mathbf{v}}, \lambda_2^{\mathbf{v}}, \lambda_3^{\mathbf{v}}, \lambda_1^{\mathbf{u}}, \lambda_2^{\mathbf{u}}, \lambda_3^{\mathbf{u}}]$$

the vector with the coefficients obtained from the bricks of $\mathbf{w}$ using Algorithm 2.

Let $\varphi = \varphi_k$ be the encryption function, with a given unknown session key k. We want to mount two attacks by computing the matrix M and the translation vector t defining $\varphi \in \mathrm{AGL}(V, \circ')$, which exist thanks to Theorem 2.4.2.
Assume we can call the encryption oracle. Then M can be computed from the 7 ciphertexts $0\varphi, \mathbf{e}_1\varphi, \ldots, \mathbf{e}_6\varphi$ as seen before. In other words, we will have

$$[\mathbf{w}\varphi] = [\mathbf{w}] \cdot M + [t], \quad [\mathbf{w}\varphi^{-1}] = ([\mathbf{w}] + [t]) \cdot M^{-1},$$

for all $\mathbf{w} \in V$. However, we have an alternative depending on how we compute φ^{-1}:

- if we compute M^{-1} from M, by applying for example Gaussian reduction, we will need only our 7 initial encryptions;
- else we can compute M^{-1} from the action of φ^{-1}, assuming we can call the decryption oracle, simply by performing the 7 decryptions $\mathbf{e}_i\varphi^{-1}$ and $0\varphi^{-1}$; indeed, the rows of M^{-1} will obviously be $[\mathbf{e}_i\varphi^{-1}] + [0\varphi^{-1}]$.

The first attack requires more binary operations, since we need a matrix inversion, but only 7 encryptions. The second attack requires both 7 encryptions and 7 decryptions, but less binary operations. The first attack is a chosen-plaintext attack, while the second is a chosen-plaintext/chosen-ciphertext attack. Both obtain the same goal, that is, the complete reconstruction of the encryption and decryption functions. Note that, since an encryption/decryption will cost a huge number of binary operations in our assumptions (we are supposing that many rounds are present), the first attack is more dangerous and its cost is approximately that of 7 encryptions, while the cost of the second attack is approximately 14 encryptions (being the cost of an encryption close to the cost of a decryption).

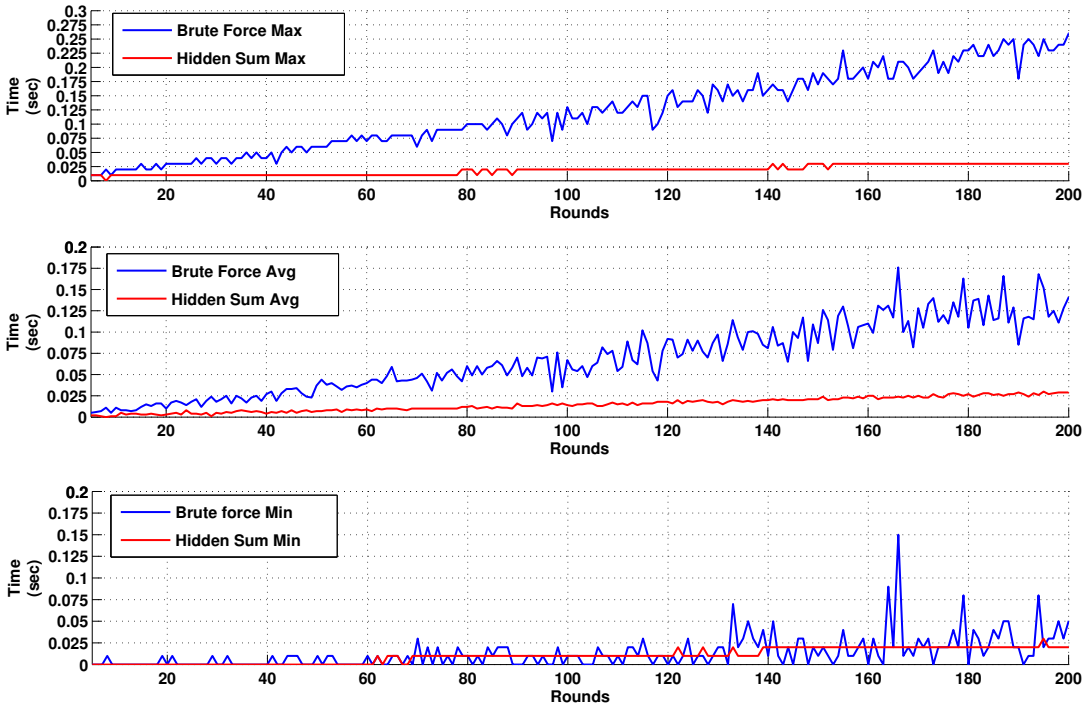


Figure 2.1: Attacks on the toy cipher

In Figure 2.4.3 we compare the brute force attack and hidden sum attack (chosen plaintext) on our toy cipher. For each fixed number of rounds we implement 10 attacks, there we give the plot of maximum, minimum and average time complexity of the attacks. As expected, the attack complexity grows linearly with the number of rounds.

Remark 2.4.4. Concentrating on the cases $T_+ \subseteq \mathrm{AGL}(V, \circ)$ it permits to implement a hidden sum trapdoor independently from the action of the key-schedule. However, if the translation group T_+ is not properly contained in the affine group of the hidden sum, but the intersection $T_+ \cap \mathrm{AGL}(V, \circ)$ is non-trivial, then the translations in that intersection represent a set of weakly keys for the cipher. The set of weakly keys can be huge and for any key there exist different hidden sums which linearize it. That permits to have an hight probability to break the cipher with the hidden sum trapdoor. Thus, it could be possible to create a partial trapdoor.

2.5 A result on scalar Boolean functions

In this section we report a result on scalar Boolean functions that are linear with respect to a sum $\circ$.

Note that $f : \mathbb{F}^n \to \mathbb{F}$ is linear with respect to $\circ$ if f is a morphism of vector space between $(\mathbb{F}^n, \circ)$ and $(\mathbb{F}, +)$.

Lemma 2.5.1. *Let $m = n$ if n is even or $m = n - 1$ if n is odd. Then*

$$\sum_{i=0}^{\frac{m}{2}} \binom{n}{2i} = 2^{n-1}.$$

Proof. Recalling that

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1},$$

we have

$$\sum_{i=0}^{\frac{m}{2}} \binom{n}{2i} = \binom{n}{0} + \sum_{i=1}^{\frac{m}{2}} \left(\binom{n-1}{2i-1} + \binom{n-1}{2i} \right). \tag{2.10}$$

If n is odd, then (2.10) is equal to

$$\binom{n}{0} + \sum_{i=1}^{n-1} \binom{n-1}{i} = 2^{n-1}.$$

If n is even, then (2.10) is equal to

$$\binom{n}{0} + \sum_{i=1}^{n-1} \binom{n-1}{i} + \binom{n-1}{n} = 2^{n-1}.$$

□

Remark 2.5.2. This lemma means that if we consider a vector space over $\mathbb{F}$ of dimension n, then half of the the vectors are obtained combining an even number of vectors of any basis and the other half combining an odd number of vectors.

Theorem 2.5.3. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a non zero Boolean function ($f(0) = 0$). If f is linear over $\mathbb{F}_2^n$ with respect to a sum $\circ$ then f is balanced ($|f^{-1}(0)| = |f^{-1}(1)|$). Vice versa if f is balanced then there exists a sum $\circ$ s.t. f is linear with respect to $\circ$.*

Proof. Let f be a morphism between $(\mathbb{F}^n, \circ)$ and $(\mathbb{F}, +)$. Suppose by contradiction that f is not balanced. We can distinguish 2 case, the case where $|f^{-1}(0)| > |f^{-1}(1)|$ and the case when $|f^{-1}(0)| < |f^{-1}(1)|$.

If $|f^{-1}(0)| > |f^{-1}(1)|$. Then $|f^{-1}(0)| > 2^{n-1}$, that implies $\mathrm{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{|f^{-1}(0)|}\} = \mathbb{F}^n$, where $\mathbf{v}_i$ is such that $f(\mathbf{v}_i) = 0$ for any $1 \leq i \leq |f^{-1}(0)|$ and the span is w.r.t. the operation $\circ$.

So, considering $\mathbf{v} \in f^{-1}(1) \neq \emptyset$, we have $\mathbf{v} = \bigcirc_i \lambda_i \mathbf{v}_i$ for some $\lambda_i \in \mathbb{F}_2$. From the linearity of f we obtain

$$f(\mathbf{v}) = \sum_i \lambda_i f(\mathbf{v}_i) = 0,$$

which leads to a contradiction.

Suppose, now, $|f^{-1}(0)| < |f^{-1}(1)|$. Then, $|f^{-1}(1)| > 2^{n-1}$ and $\mathrm{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{|f^{-1}(1)|}\} = \mathbb{F}^n$, where $\mathbf{v}_i$ is such that $f(\mathbf{v}_i) = 1$ for any $1 \leq i \leq |f^{-1}(1)|$. W.l.o.g. $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis. From Lemma 2.5.1 there exists $\mathbf{v}_j$ with $j \in \{1, \ldots, |f^{-1}(1)|\}$ which is a combination of an even numbers of elements of the basis $\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k}$. This implies

$$f(\mathbf{v}_j) = \sum_{l=1}^{k} f(\mathbf{v}_{i_k}) = k \cdot 1,$$

with k even, that is $f(\mathbf{v}_j) = 0$.

Vice versa, let f be balanced . Choose $n-1$ non zero vectors in $f^{-1}(0)$, $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$, and $\mathbf{v}_n \in f^{-1}(1)$.

We can construct a bijection $\psi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ s.t. $\psi(\mathbf{v}_i) = \mathbf{e}_i$, for all $1 \leq i \leq n$, $\psi(f^{-1}(0)) = \{\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{F}_2^n \,|\, w_n = 0\}$ and $\psi(f^{-1}(1)) = \{\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{F}_2^n \,|\, w_n = 1\}$.

Now we define the combination with respect to a new sum $\circ$ as following

$$\bigcirc_{i=1}^{n} \lambda_i \mathbf{v}_i := \psi^{-1}\left(\sum_{i=1}^{n} \lambda_i \mathbf{e}_i\right).$$

This is well defined by the fact that f is balanced, and f is linear with respect to $\circ$. □

Note that the operation $\circ$ could be related to a translation group $T_\circ \nsubseteq \mathrm{AGL}(V, +)$.

Example 2.5.4. Let $V = \mathbb{F}^3$ and consider the Boolean function with algebraic normal form $f(\mathbf{x}) = x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_3$. Then

$$\begin{array}{ll} (0,0,0) \mapsto 0 & (1,1,0) \mapsto 0 \\ (1,0,0) \mapsto 1 & (1,0,1) \mapsto 0 \\ (0,1,0) \mapsto 0 & (0,1,1) \mapsto 1 \\ (0,0,1) \mapsto 1 & (1,1,1) \mapsto 1 \end{array}.$$

If we consider over V the algebra structure induced by the exterior algebra of a 2 dimensional vector space, that is we have the basis

$$\mathbf{e}_1,\ \mathbf{e}_2,\ \mathbf{e}_3 = \mathbf{e}_1 \wedge \mathbf{e}_2,$$

and the corresponding sum $\circ$ defined by $\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \mathbf{y} + \mathbf{x} \wedge \mathbf{y}$. Then it is easy to check that f is linear with respect to $\circ$.

The same sum is obtained considering the vectors $\mathbf{v}_1 = (1,0,1), \mathbf{v}_2 = \mathbf{e}_2, \mathbf{v}_3 = \mathbf{e}_3$ and the bijection from $\mathbb{F}^3$ to $\mathbb{F}^3$ defined by

$$\psi(\mathbf{v}) = \begin{cases} \mathbf{e}_1 & \text{if } \mathbf{v} = (1,0,1), \\ \mathbf{v}_1 & \text{if } \mathbf{v} = \mathbf{e}_1, \\ \mathbf{v} & \text{otherwise} \end{cases}.$$

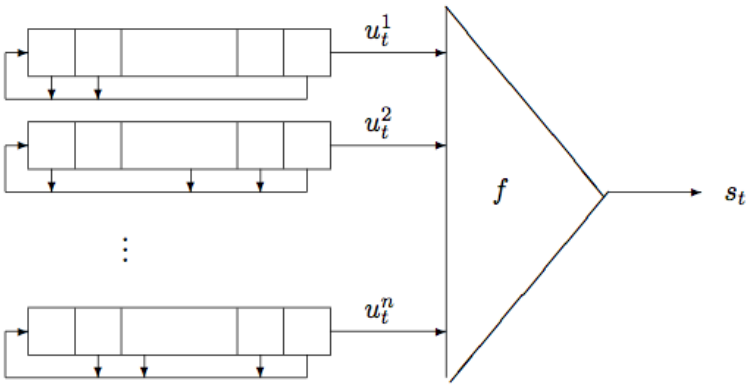
Then any combination of the $\mathbf{v}_i$'s is given by $\bigcirc_{i=1}^{3}\lambda_i\mathbf{v}_i := \psi^{-1}\left(\sum_{i=1}^{3}\lambda_i\mathbf{e}_i\right)$.

2.5.1 Application to stream cipher

A combination generator is a running-key generator for stream cipher applications. It is composed of several *linear feedback shift registers* (LFSRs) (see for instance [Kle13]) whose outputs are combined by a Boolean function to produce the key-stream. Then, the output sequence $(s_t)_{t\geq 0}$ of a combination generator composed of n LFSRs is given by

$$s_t = f(u_1^t, u_2^t, \ldots, u_n^t), \forall t \geq 0,$$

where $(u_i^t)_{t\geq 0}$ denotes the sequence generated by the i-th constituent LFSR and f is a function of n variables.



If the combining function f is balanced, then its output are uniformly distributed. Moreover Canteaut in [Can06] has observed that only balanced n-variables functions can have optimal algebraic immunity for odd n. This property is useful against algebraic attacks [CM03].

Consider the case to have n LFSRs working on vectors of length l and the function f is the XOR of the last bit of any register. Then we have a linear boolean function F from $\mathbb{F}^{nl}$ to $\mathbb{F}$ that is represented from a vector $\lambda \in \mathbb{F}^{nl}$, i.e. $F(v) = \lambda v^T = \sum_i \lambda_i v_i$. So collecting the stream outputs s_t's we have the relations

$$\begin{aligned} s_1 &= \lambda v_1^T \\ s_2 &= \lambda v_2^T \\ &\vdots \end{aligned}$$

where the state v_i depends in a linear way from v_{i-1}. An attack on this example of stream cipher can be done using the Berlekamp-Massey algorithm [Mas69] to reconstruct the initial state v_1.

In order to remove these linear relations in the combination generator we use a non-linear function f to combine the last bits of the LFSRs. If now we suppose to use a balanced non-linear function f to combine the last bits of the registers, then from Theorem 2.5.3 there exists at least a hidden sum $\circ$ such that the function $F : \mathbb{F}^{nl} \to \mathbb{F}$ (that is the composition of the projection of the bits with the function f) is linear. Using the notation as in Section 2.4 we can represent the action of F as $[\lambda][v]^T$ for some $[\lambda]$. So

$$\begin{aligned} s_1 &= [\lambda][v_1]^T \\ s_2 &= [\lambda][v_2]^T \\ &\vdots \end{aligned}$$

If also the action of the LFSRs on the states is linear with respect $\circ$ we obtain that $[v_i]$ depends in a linear way from $[v_{i-1}]$ and that might permit to recover the initial state.

Some stream ciphers, e.g. E0 [Kle13], use non-linear functions to update the state. If this update is linear in the operation $\circ$ we have again a linear correlation between $[v_i]$ and $[v_{i-1}]$, so it is possible to embed a weakness in the stream cipher.

The role of Boolean functions

As seen in Chapter 1.2 the S-boxes of a tb cipher play an important role in the primitivity of Γ_∞ and also to avoid hidden sum trapdoors. In fact in Theorem 1.3.2 the condition (2), i.e. no derivative of the S-boxes maps the space V in a proper affine subspace, was used in [CDS09a] by the authors to exclude the first case of Theorem 2.0.3. That means the round functions group is not contained in any affine isomorphic copy of $AGL(V)$. In this chapter we introduce the definition of anti-crooked function, giving some result for the case of power functions. In the last part we give, also, some results on weakly-APN functions.

3.1 Anti-Crooked functions

Definition 3.1.1. *A v.B.f. γ is called* **anti-crooked (AC)** *if for each $a \in V \setminus \{0\}$ the set*

$$\mathrm{Im}(\hat{f}_a) = \{f(x+a) + f(x) \mid x \in V\}$$

is not an affine subspace of V.

This condition is not always satisfy by the S-boxes of a block chipper, e.g. the PRESENT S-box is not AC. That may permit to embed a weakness in the block cipher.

In this section we give some properties on the anti-crookedness of a Boolean function. As said in Chapter 1, any vectorial Boolean function f from $\mathbb{F}^n$ to $\mathbb{F}^n$ can be expressed uniquely as a univariate polynomial in $\mathbb{F}_{2^n}[x]$.

A first result on vBf is the following.

Theorem 3.1.2. *Let f be a vBf weakly 2^t-differential uniform, but not weakly 2^{t-1}-differential uniform, and not 2^t-differential uniform. Then, there exists $a \neq 0 \in \mathbb{F}_{2^n}$, such that $\mathrm{Im}(\hat{f}_a)$ is not a coset of a subspace $W \subseteq \mathbb{F}_{2^n}$. In particular for $t = 1$, if f is weakly-APN but not APN, then, there exists $a \in \mathbb{F}_{2^n}$ nonzero such that $\mathrm{Im}(\hat{f}_a)$ is not a coset of a subspace $W \subseteq \mathbb{F}_{2^n}$.*

Proof. By contradiction suppose that for all $a \neq 0$ we have $\mathrm{Im}(\hat{f}_a) = w + W$ for some $w \in \mathbb{F}_{2^n}$ and W vector space. Since f is weakly 2^t-differential uniform, at

most, it results $2^{n-t-1} < |\mathrm{Im}(\hat{f}_a)| \leq 2^{n-t}$. Thus $\dim_{\mathbb{F}}(W) = n - t$. But then $\hat{f}_a$ is a 2^t-to-1 function for all $a \neq 0$, which means that f is 2^t-differential uniform, and this contradicts our hypothesis. In other words, there exists a such that $\mathrm{Im}(\hat{f}_a)$ is not a coset. □

Consider the following lemma for a power function (not necessarily a permutation).

Lemma 3.1.3. *Let us consider $\mathbb{F}_{2^n}$ as a vector space over $\mathbb{F}$. Let $f(x) = x^d$. If there exists $a \in \mathbb{F}_{2^n}$, $a \neq 0$, such that $\mathrm{Im}(\hat{f}_a)$ is a coset of a subspace of $\mathbb{F}_{2^n}$, then $\mathrm{Im}(\hat{f}_{a'})$ is a coset of subspace of $\mathbb{F}_{2^n}$ for all $a' \neq 0$.*

Proof. We have $\mathrm{Im}(\hat{f}_a) = w + W$ where W is a $\mathbb{F}$-vector subspace of $\mathbb{F}_{2^n}$ for some $w \in \mathbb{F}_{2^n}$. Now, let $a' \in \mathbb{F}_{2^n}$, $a' \neq 0$, we have

$$\hat{f}_{a'}(x) = (x + a')^d + x^d = \left(\frac{a'}{a}\right)^d \left[\left(x\frac{a}{a'} + a\right)^d + \left(x\frac{a}{a'}\right)^d\right] = \left(\frac{a'}{a}\right)^d \hat{f}_a\left(x\frac{a}{a'}\right).$$

So we have $\mathrm{Im}(\hat{f}_{a'}) = \left(\frac{a'}{a}\right)^d \mathrm{Im}(\hat{f}_a) = \left(\frac{a'}{a}\right)^d w + \left(\frac{a'}{a}\right)^d W = w' + W'$. Since $W' = (a'/a)^d W$ is again an $\mathbb{F}$-vector subspace of $\mathbb{F}_{2^n}$, our claim is proved. □

Thanks to Lemma 3.1.3, for power functions we can strengthen Theorem 3.1.2.

Corollary 3.1.4. *Let f be a vBf permutation on $\mathbb{F}_{2^n}$ that is weakly 2^t-differential uniform, but not 2^t-differential uniform. If $f(x) = x^d$, then f is AC.*

Remark 3.1.5. Given an arbitrary vBf there are three possible cases: f is either crooked or anti-crooked or neither. However, Lemma 3.1.3 shows that for a power function there are only **two** possible cases: f is either crooked or anti-crooked.

We want now to investigate condition that guaranty the anti-crookedness of a Boolean function.

A vBf can also be represented by n Boolean functions of n variables. For all $a \in \mathbb{F}^n \setminus \{0\}$, let V_a be the vector space

$$V_a = \{\mathbf{v} \in \mathbb{F}^n \setminus \{0\} : \deg(< \mathbf{v}, \hat{f}_a >) = 0\} \cup \{0\}.$$

By definition, if $t = \max_{a \in \mathbb{F}^n \setminus \{0\}} \dim(V_a)$, then $\hat{n}(f) = 2^t - 1$.

Proposition 3.1.6. *Let f be a vBf and $a \in \mathbb{F}^n \setminus \{0\}$. Then $f(a) + V_a^{\perp}$ is the smallest affine subspace of $\mathbb{F}^n$ containing $\mathrm{Im}(\hat{f}_a)$. In particular, $\hat{n}(f) = 0$ if and only if for any $a \in \mathbb{F}^n \setminus \{0\}$ there is no proper affine subspace of $\mathbb{F}^n$ containing $\mathrm{Im}(\hat{f}_a)$.*

Proof. Let $a \in \mathbb{F}^n \setminus \{0\}$. Note that $V_a = \{\mathbf{v} \in \mathbb{F}^n :< \mathbf{v}, \hat{f}_a > \text{ is constant}\}$. Let $\mathbf{x} \in \mathbb{F}^n$, then $\hat{f}_a(\mathbf{x}) = f(a) + \mathbf{w}$, for some $\mathbf{w} \in \mathbb{F}^n$, and $< \mathbf{v}, \hat{f}_a(\mathbf{x}) >= c \in \mathbb{F}$ for all $\mathbf{v} \in V_a$. In particular $c =< \mathbf{v}, \hat{f}_a(0) >=< \mathbf{v}, f(a) >$ and so $< \mathbf{w}, \mathbf{v} >= 0$, that is, $\mathbf{w} \in V_a^\perp$. Then we have $\mathrm{Im}(\hat{f}_a) \subseteq f(a) + V_a^\perp$. Now, let A be an affine subspace containing $\mathrm{Im}(\hat{f}_a)$, then $A = f(a) + V$, for some vector subspace V in $\mathbb{F}^n$. For all $\mathbf{v} \in V^\perp$, we have $< \mathbf{v}, \hat{f}_a >=< \mathbf{v}, f(a) >= c \in \mathbb{F}$ and so, by definition, $V^\perp \subseteq V_a$. Then A contains $f(a) + V_a^\perp$.
Finally, $\hat{n}(f) = 0$ if and only if $V_a = \{0\}$ for all $a \in \mathbb{F}^n \setminus \{0\}$, and so our claim follows. □

Obviously, for any affine subspace W, $\mathrm{Im}(\hat{f}_a) \not\subset W \implies \mathrm{Im}(\hat{f}_a) \neq W$ and so we have the next corollary.

Corollary 3.1.7. *Let f be a vBf. If $\hat{n}(f) = 0$ then f is AC.*

Coming back to power functions it is important to recall a result by Kyureghyan.

Theorem 3.1.8 ([Kyu07])**.** *The only crooked APN power functions in $\mathbb{F}_{2^n}$ are those with exponent $2^i + 2^j$, $\gcd(i - j, n) = 1$.*

Recalling that the known exponents of APN power functions (up to factor 2^i) are

$$2^k + 1, \quad \gcd(k, m) = 1 \quad \text{(Gold's exponent [BFDF98, Gol68])}$$
$$2^{2k} - 2^k + 1, \quad \gcd(k, m) = 1 \quad \text{(Kasami's exponent [Kas71])}$$
$$2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1, \quad m = 5k \quad \text{(Dobbertin's functions [Dob01])}$$

if $m = 2l + 1$ also

$$2^l + 3 \quad \text{(Welch's exponent [Dob99, CCD00, HX01])}$$
$$2^l + 2^{\frac{l}{2}} - 1 \quad \text{if } l \text{ is even and}$$
$$2^l + 2^{\frac{3l+1}{2}} - 1 \quad \text{if } l \text{ is odd} \quad \text{(Niho's exponent [Dob99, HX01])}$$
$$2^m - 2 \quad \text{(patched inversion [Nyb94])}$$

This implies that the only crooked power functions, among the known maps, are those with Gold's exponent. Thanks to Remark 3.1.5 we have:

Corollary 3.1.9. *Let x^d be one of the APN power functions above, with d not a Gold's exponent, then x^d is AC. In particular the power function x^{2^m-2} is AC for all $m \geq 3$.*

Proof. It follows directly from Lemma 3.1.3 and the theorem above. For the case of the patched inversion, from Corollary 3.1.4, it is AC also in even dimension. □

Having examined some anti-crooked functions we would like to show some properties of this notion.

Lemma 3.1.10. *If f is AC then f^{-1} is not necessarily AC.*

Proof. We provide an explicit example $f : \mathbb{F}^6 \to \mathbb{F}^6$ defined by $f(x) = x^{38}$, then $f^{-1}(x) = x^5$. A computer check shows that f is anti-crooked while f^{-1} is not. In particular, $\mathrm{Im}(\hat{f^{-1}}_{e^6})$ is an affine subspace of dimension 4, where e is a primitive element of $\mathbb{F}_{64}$ such that $e^6 = e^4 + e^3 + e + 1$. □

We recall that two vBf's f and f' are called CCZ-equivalent if their graphs $G_f = \{(x, f(x)) \mid x \in \mathbb{F}^n\}$ and $G_{f'} = \{(x, f'(x)) \mid x \in \mathbb{F}^n\}$ are affine equivalent. We recall also that f and f' are called EA-equivalent if there exist three affine functions g, g' and g'' such that $f' = g' f g + g''$.

Lemma 3.1.10 and the well-known fact that a vBf f is CCZ-equivalent to f^{-1} imply the following result.

Corollary 3.1.11. *The anti-crookedness is not CCZ invariant.*

On the other hand, anti-crookedness behaves well with EA invariance, as shown below.

Proposition 3.1.12. *The anti-crookedness is EA invariant.*

Proof. Let f be a vBf anti-crooked, and let f' be a vBf such that f and g are EA equivalent. Then, there exist three affinities $\lambda_1, \lambda_2, \lambda_3$ such that $g = \lambda_1 f \lambda_2 + \lambda_3$. Without loss of generality we can suppose $f(0) = g(0) = 0$ and $\lambda_i(0) = 0$ for all $i = 1, 2, 3$. Then

$$\begin{aligned}\hat{g}_a &= \lambda_1 f \lambda_2(x + a) + \lambda_1 f \lambda_2(x) + \lambda_3(x + a) + \lambda_3(x) \\ &= \lambda_1(f(\lambda_2(x) + \lambda_2(a)) + f(\lambda_2(x)) + \lambda_1^{-1}\lambda_3(a)),\end{aligned}$$

which implies

$$\mathrm{Im}(\hat{g}_a) = \lambda_1(\lambda_1^{-1}\lambda_3(a) + \mathrm{Im}(\hat{f}_{\lambda_2(a)})),$$

thus g is AC if and only if f is AC. □

3.2 Weakly-APN functions

Definition 3.2.1. *Let $f(x) = x^d$ and $0 \leq i \leq 2^n$. We denote by ω_i the number of output differences of b that occur i times, that is*

$$\omega_i(f) = |\{b \in \mathbb{F}^n \mid \delta_f(1, b) = i\}|.$$

The **differential spectrum** *of f is the set of $\omega_i(f)$'s, denoted by $\mathbf{S}(f)$.*

The following two results are well know (see for instance [BCC11]).

Proposition 3.2.2. *Let $f(x) = x^d$, $f \in \mathbb{F}_{2^n}[x]$, then for any $a, a' \in \mathbb{F}^n$, with $a, a' \neq 0$, and $0 \leq i \leq 2^n$*

$$|\{b \in \mathbb{F}^n \,:\, \delta_f(a', b) = i\}| = |\{b \in \mathbb{F}^n \,:\, \delta_f(a, b) = i\}|.$$

In other words, when f is a monomial function the differential characteristics given by $\{\delta_f(a, b)\}_{b \in \mathbb{F}^n}$ are determined by only one nonzero value a.

Lemma 3.2.3. *Let $f(x) = x^d$ with $\gcd(2^n - 1, d) = 1$. Let $g(x) = x^e$ such that $e \equiv 2^k d \mod (2^n - 1)$ or $ed \equiv 1 \mod (2^n - 1)$, then $\mathbf{S}(f) = \mathbf{S}(g)$.*

From Lemma 3.2.3 we obtain, for power function:

Theorem 3.2.4. *Let $f(x) = x^d$ with $\gcd(2^n-1, d) = 1$. Then f is weakly δ-differentially if and only if f^{-1} is weakly δ-differentially.*

Proof. For a power function we have

$$|\mathrm{Im}(\hat{f}_a)| = |\mathrm{Im}(\hat{f}_1)| = 2^n - \omega_0, \quad \forall a \neq 0.$$

From Lemma 3.2.3 we have $\omega_0(f) = \omega_0(f^{-1})$, and that concludes the proof. □

Lemma 3.2.5. *Suppose that f is not a power function. If f is weakly δ-differentially uniform then f^{-1} is not necessarily weakly δ-differentially uniform.*

Proof. We provide the following example $f : \mathbb{F}^4 \to \mathbb{F}^4$ defined by

$$\begin{aligned} f(x) = {} & x^{14} + e^{10}x^{13} + ex^{12} + e^2x^{11} + e^9x^{10} + e^8x^9 + e^3x^8 + e^5x^7 \\ & + e^5x^6 + e^{11}x^5 + e^8x^3 + e^{10}x^2 + ex + e^{12}, \end{aligned}$$

where e is a primitive element of $\mathbb{F}_{16}$ such that $e^4 = e + 1$, and the inverse of f

$$\begin{aligned} f^{-1}(x) = {} & x^{14} + e^{10}x^{13} + e^{14}x^{12} + e^8x^{11} + e^7x^{10} + e^{10}x^9 + x^8 + e^5x^7 + e^{14}x^6 \\ & + e^2x^5 + e^7x^4 + e^5x^3 + e^{14}x^2 + e^{11}x + e^{14}. \end{aligned}$$

We have that f is weakly-APN while f^{-1} is only weakly 4-differentially uniform. □

As before we obtain.

Corollary 3.2.6. *The weakly differential uniformity is not CCZ invariant.*

On the other hand:

Proposition 3.2.7. *The weakly differential uniformity is EA invariant.*

Proof. Let f be a vBf weakly δ-differential, and let g be a vBf such that f and g are EA equivalent. Then, there exists a vBf g' affine equivalent to f and $g = g' + \lambda$ where λ is an affinity over $\mathbb{F}^n$.

From the fact that the weakly differential uniformity is affine invariant we have $|\mathrm{Im}(\hat{g'}_a)| > 2^{n-1}/\delta$ for all $a \in \mathbb{F}^n$. So, $\mathrm{Im}(\hat{g}_a) = \{x + \lambda(a) \,|\, x \in \mathrm{Im}(\hat{g'}_a)\}$ implies $|\mathrm{Im}(\hat{g}_a)| = |\mathrm{Im}(\hat{g'}_a)| > 2^{m-1}/\delta$ for all $a \in \mathbb{F}^n$. □

We extend some results of [FPRS12] in the following theorem.

Lemma 3.2.8 ([Kyu07],Corollary 6)**.** *Let $f(x) = x^d$ be a permutation. Then $\hat{f}_1$ is constant if and only if* $\deg(f) = 2$.

Lemma 3.2.9 ([Her05], Theorem 1)**.** *Let $f(x) = x^d$, with $d = 2^{2k} - 2^k + 1$ (Kasami exponent),* $\gcd(k, n) = s$ *and n/s odd. Then $\hat{f}_1$ is a 2^s-to-1 function.*

Theorem 3.2.10. *Let f be a vBf permutation such that $\hat{n}(f) = 0$. Then*
(i) if $n = 3$ then f is weakly-APN;
(ii) if $n = 4$ then f is weakly-APN;
(iii) if $n = 2m$, with m odd, f is not necessarily weakly-APN.

Proof. (i) Let $\mathbb{F}^3 = \{x_1, \ldots, x_8\}$ and let M_a be the matrix of dimension 3×8, whose columns are $m_j = \hat{f}_a(x_j)$ for $1 \leq j \leq 8$. We claim that $\hat{n}(f) = 0$ implies $\mathrm{rank}(M_a) = 3$ for all a. Otherwise, we could obtain $(0, \ldots, 0) \in \mathbb{F}^3$ from a combination of the rows of M_a. If f is not weakly-APN, we have $|\mathrm{Im}(\hat{f}_a)| \leq 2$ for some $a \in \mathbb{F}_2^3 \setminus \{0\}$. So we have at most 2 distinct columns that means $\mathrm{rank}(M_a) \leq 2$.

(ii) See [FPRS12] Proposition 2 .

(iii) Let $t > 0$ be such that $\gcd(2^{2^{t+1}} - 2^{2^t} + 1, 2^n - 1) = 1$, and consider the power function $f(x) = x^d$, with $d = 2^{2^{t+1}} - 2^{2^t} + 1$. We have $\gcd(2^t, n) = 2$, thus f is 4-differential uniform and weakly 4-differential uniform from Lemma 3.2.9. Moreover, being $\deg(f)$ equals to the Hamming weight of the binary expansion of d, we have that f is not quadratic. Then, from Lemma 3.2.8 $\hat{n}(f) = 0$ □

In [FPRS12] it was shown that a weakly-APN f function over $\mathbb{F}^4$ has $n_3(f) \in \{12, 14, 15\}$, where $n_3(f)$ is the number of components of f with degree 3, moreover by a computer check on the class representatives the authors exclude the case $n_3(f) = 12$ (Fact 4 in [FPRS12]).
We give, now, a formal proof of this fact. We recall some results firstly.

For a Bf f the set $V(f) = \{a \in \mathbb{F}^n \,|\, \hat{f}_a \text{ is costant}\}$ is said the **set of linear structures** of f.

Theorem 3.2.11 ([CCK08]). *Let $f : \mathbb{F}^n \to \mathbb{F}$ be a quadratic Bf. Then the dimension of $V(f)$ is equal to $n - 2h$, $1 \leq h \leq \lfloor \frac{m}{2} \rfloor$. Moreover $\dim(V(f)) = 0$ if and only if f is bent.*

Theorem 3.2.12 ([FPRS12]). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a weakly-APN permutation. Then $\hat{n}(f) \leq 1$.*

Proposition 3.2.13 (Fact 4 in [FPRS12]). *Let $f : \mathbb{F}^4 \to \mathbb{F}^4$ be a weakly-APN permutation. Then $n_3(f) \in \{14, 15\}$.*

Proof. Assume by contradiction that $\deg(f_j) \leq 2$, $1 \leq j \leq 3$, for three distinct components of f.

From the Theorem 3.2.11, $\hat{f}_{j_a}$ is constant for every $a \in V(f_j)$ where $V(f_j) \subseteq \mathbb{F}^4$, i.e. the set of linear structures of f_j, is a vector subspace of dimension 0 if and only if f_j is bent, 4 if and only if f_j is linear (affine), and 2 otherwise. Since f is a permutation we have that f_j is balanced, so f_j is not bent for any j. If there exists $a \in V(f_i) \cap V(f_j)$ different from 0 for some i and j, then $\hat{n}(f) \geq 2$. But f weakly-APN implies $\hat{n}(f) \leq 1$ (Theorem 3.2.12). So, we obtain that $\deg(f_j) = 2$ and $V(f_i) \cap V(f_j) = \{0\}$, with $\dim(V(f_i)) = 2$, for all i, j. Without loss of generality, since $V(f_1) \oplus V(f_2) = \mathbb{F}^4$, we can assume
$V(f_1) = \langle (1,0,0,0), (0,1,0,0) \rangle$ and $V(f_2) = \langle (0,0,1,0), (0,0,0,1) \rangle$.

Let $f_1(x) = \sum_{i<j} c_{i,j} x_i x_j + \sum_i c_i x_i$. Since $f_1(x + (1,0,0,0)) + S_1(x)$ is constant we have that $c_{i,j} = 0$ if i or j equals 1. Similarly, since $f_1(x + (0,1,0,0)) + S_1(x)$ is constant we have $c_{i,j} = 0$ if i or j equals 2. Then $f_1(x) = x_3 x_4 + \sum_i c_i x_i$ and analogously we have $f_2(x) = x_1 x_2 + \sum_i c'_i x_i$, for some c'_i's.

So, $f_3(x) = x_1 x_2 + x_3 x_4 + \sum_i b_i x_i$, $b_i = c_i + c'_i$, and we can compute the derivate of S_3 with respect to $a \in \mathbb{F}^4$ as

$$(\hat{f}_3)_a(x) = a_2 x_1 + a_1 x_2 + a_4 x_3 + a_3 x_4 + c, \text{ where } c \text{ is constant.}$$

$(\hat{f}_3)_a(x)$ is constant if and only if $a = 0$, that implies f_3 is bent. This contradicts the fact that f is a permutation and each component is balanced. □

As was shown in [SZZ94] there is no APN quadratic permutation over $\mathbb{F}^n$ for n even. This result was extended by Nyberg [Nyb95] to the case of permutations with partially bent components (for n even). We are able to extend these results to the case of weakly-APN permutations defined over $\mathbb{F}^n$ with n even.

Definition 3.2.14 ([Car93]). *A Bf f is* **partially bent** *if there exists a linear subspace $V(f)$ of $\mathbb{F}^n$ such that the restriction of f to $V(f)$ is affine and the restriction of f to any complementary subspace U of $V(f)$, $V(f) \oplus U = \mathbb{F}^n$, is bent. In that case, f can be represented as a direct sum of the restricted functions, i.e., $f(y+z) = f(y) + f(z)$, for all $z \in V(f)$ and $y \in U$.*

Remark 3.2.15. The space $V(f)$ is formed by the linear structures of f, in fact

$$f(x+a)+f(x)=f(y+z+a)+f(y+z)=f(y)+f(z)+f(a)+f(y)+f(z)=f(a)$$

where $z, a \in V(f)$ and $y \in U$. Moreover, since bent function exist only in even dimension, $n-\dim(V(f))$ is even. That means if n is even, the dimension of $V(f)$ is even.

Theorem 3.2.16. *For n even, a weakly-APN permutation has at most $\frac{2^n-1}{3}$ partially bent components. In particular f cannot have all partially bent components.*

Proof. Let f be a weakly-APN permutation. Assume by contradiction that f has more than $\frac{2^n-1}{3}$ partially bent components, and denote those with $f_1, \ldots, f_s$. f is a permutation, then $\dim(V(f_i)) \neq 0$ for all $1 \leq i \leq s$, otherwise f_i is bent and it is not balanced. From Remark 3.2.15 we have that there exist at least three nonzero vectors in each $V(f_i)$. So

$$\sum_{i=1}^{s} |V(f_i)| \geq 3\,s > 2^n - 1.$$

Thus, there exist i and j such that $a \in V(f_i) \cap V(f_j)$ with $a \neq 0$. This implies $\hat{n}(f) \geq 2$, which contradicts that f is weakly-APN, since in that case $\hat{n}(f) \leq 1$. □

From the fact that a quadratic Boolean function is partially bent (see for instance [Nyb95]), we have immediately the following result.

Corollary 3.2.17. *There exists no weakly-APN quadratic permutation over $\mathbb{F}^n$, for n even.*

Corollary 3.2.18. *Let n even. Let f be a weakly-APN permutation. Then f has at most $2^{n-2}-1$ quadratic components.*

Proof. That depends on the fact that the set of components of degree less or equal to 2 is a vector space. □

Proposition 3.2.19. *Let $f : \mathbb{F}^n \to \mathbb{F}^n$ be a Boolean permutation such that $\hat{n}(f) = 0$. Then f has no partially bent (quadratic) components.*

Proof. $\hat{n}(f) = 0$ implies that the linear structures set of any component contains only 0. So if there exists a partially bent (quadratic) component, then it is bent. But f is a permutation, then this is not possible. □

For the particular case of 4-bit S-Boxes we obtain these two more results.

Corollary 3.2.20. *Let $f : \mathbb{F}^4 \to \mathbb{F}^4$ be a vBf permutation.*
(i) If $\hat{n}(f) = 0$. Then f is weakly-APN and $n_3(f) = 15$.
(ii) If f is weakly APN and $n_3(f) = 14$. Then $\hat{n}(f) = 1$.

Proof. Let f be weakly-APN, so $\hat{n}(f) \leq 1$. From Proposition 3.2.19, the thesis follows. □

So for weakly-APN function for $n = 4$ we have all the three cases:

- $\hat{n}(f) = 0$ and $n_3(f) = 15$ with ANF:

$$\begin{aligned} f_1 &= x_1x_2x_3 + x_2x_3x_4 + x_1x_3 + x_2x_3 + x_1 + x_2 + x_3 + x_4 \\ f_2 &= x_1x_2x_4 + x_1x_2 + x_1x_3 + x_2x_3 + x_2x_4 + x_4 \\ f_3 &= x_1x_3x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_3 + x_4 \\ f_4 &= x_2x_3x_4 + x_1x_4 + x_2x_4 + x_2 + x_3x_4 + x_3 + x_4 \end{aligned}$$

- $\hat{n}(f) = 1$ and $n_3(f) = 15$ with ANF:

$$\begin{aligned} f_1 &= x_1x_3x_4 + x_2x_3x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_1 \\ f_2 &= x_1x_2x_4 + x_1x_3 + x_1x_4 + x_2x_3 + x_2 \\ f_3 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 + x_1x_2 + x_3x_4 + x_3 \\ f_4 &= x_2x_3x_4 + x_1x_2 + x_1x_4 + x_2x_3 + x_4 \end{aligned}$$

- $\hat{n}(f) = 1$ and $n_3(f) = 14$, with ANF:

$$\begin{aligned} f_1 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3 + x_1 + x_2x_3x_4 + x_2x_3 + x_3x_4 \\ f_2 &= x_1x_2x_4 + x_1x_2 + x_1x_3x_4 + x_1x_3 + x_1x_4 + x_2 \\ f_3 &= x_1x_2x_4 + x_1x_2 + x_1x_3x_4 + x_1x_3 + x_2x_4 + x_3 \\ f_4 &= x_1x_3 + x_1x_4 + x_2x_3x_4 + x_2x_4 + x_4 \end{aligned}$$

Part II

Index Coding

Preliminaries on Index Coding

In this chapter we report some extra notations used in this second part. Then we introduce the ICSI problem exploiting some results on the optimal length of an index code and on error correction index codes, results and definitions are from [MS77, Ass92, W+01, ALS+08, BYBJK06, DSC13].

4.1 Notations and backgrounds

4.1.1 Linear Codes terminology

Let $M \in \mathbb{F}_q^{N\times n}$, we write M_i and M^j to denote the i-th row and j-th column of M, respectively. More generally, for subsets $S \subseteq [N]$ and $H \subseteq [n]$ we write M_S and M_H to denote the $|S| \times n$ and $N \times |H|$ submatrices of M comprised of the rows of M indexed by S and the columns of M indexed by H respectively. Moreover let M be a matrix we denote by $\text{rowsp}(M)$ the space spanned by the rows of M and by $\text{colsp}(M)$ the space spanned by the columns of M.

For the vectors $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$, the **(Hamming) distance** between $\mathbf{u}$ and $\mathbf{v}$ is defined to be the number of coordinates where u and v differ, namely,

$$d(\mathbf{u}, \mathbf{v}) = |\{i \in [n] : u_i \neq v_i\}|.$$

If $\mathbf{u} \in \mathbb{F}_q^n$ and $S \subseteq \mathbb{F}_q^n$ is a set of vectors,then the last definition can be extended to

$$d(\mathbf{u}, S) = \min_{\mathbf{v}\in S} d(\mathbf{u}, \mathbf{v}).$$

The **support** of a vector $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$ is defined to be the set $\text{Supp}(\mathbf{u}) = \{i \in [n] : u_i \neq 0\}$. The **(Hamming) weight** of a vector $\mathbf{u}$, denoted $w(\mathbf{u})$, is defined to be $|\text{Supp}(\mathbf{u})|$, the number of nonzero coordinates of $\mathbf{u}$.

Definition 4.1.1. *Let $\mathcal{C}$ be a k-dimensional subspace of $\mathbb{F}_q^n$. $\mathcal{C}$ is called a* **linear** $[n, k, d]_q$ **code** *if the minimum distance of C,*

$$d(\mathcal{C}) = \min_{\mathbf{u},\mathbf{v}\in\mathcal{C},\mathbf{u}\neq\mathbf{v}} d(\mathbf{u}, \mathbf{v})$$

is equal to d. We call n the length and k the dimension of the code. The vectors in $\mathcal{C}$ are called **codewords**.

Remark 4.1.2. It is easy to see that the minimum weight of a nonzero codeword in a linear code $\mathcal{C}$ is equal to its minimum distance $d(\mathcal{C})$.

A **generator matrix** G of an $[n,k,d]_q$ code $\mathcal{C}$ is a $k \times n$ matrix whose rows are linearly independent codewords of $\mathcal{C}$. Then $\mathcal{C} = \{\mathbf{y}G : \mathbf{y} \in \mathbb{F}_q^k\}$. The **parity-check matrix** of $\mathcal{C}$ is an $(n-k)\times n$ matrix H over $\mathbb{F}_q$ such that $c \in \mathcal{C}$ if and only if $Hc^T = 0^T$. Given q, k, and d, let $N_q[k,d]$ denote the length of the shortest linear code over F_q that has dimension k and minimum distance d. The **dual code** of $\mathcal{C}$ is defined as $\mathcal{C}^\perp = \{u \in \mathbb{F}_q^n | \mathbf{u}\mathbf{c}^T = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$.

The following upper bound on the minimum distance of a q-ary linear code is well known (see [MS77])

Theorem 4.1.3 (Singleton Bound)**.** *For an $[n,k,d]_q$ code, we have $d + k - 1 \leq n$.*

Codes attaining this bound are called **maximum distance separable** (MDS) codes.

The set $\mathcal{S}_q^r(n,\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}_q^n \mid d(\mathbf{x},\mathbf{y}) \leq r\}$ is called the **Hamming sphere** of radii r centered in $\mathbf{x}$. The volume of a sphere is denoted by $V_q(n,r)$ and

$$V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

For a prime power q, let H_q denote the q-ary entropy function

$$H_q(x) : (0,1) \to \mathbb{R}, \qquad H_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x).$$

The function $H_q(x)$ is continuous and increasing in $(0, 1-(1/q))$.

A proof of the following lemma can be found in [Loe94].

Lemma 4.1.4. *Let $\lambda \in (0, 1-(1/q))$ be such that $n\lambda$ is an integer. Then*

$$V_q(n, \lambda n) \leq q^{H_q(\lambda)n}.$$

4.1.2 Incidence structures and t-designs terminology

A finite **incidence structure** which we denote by $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, consists of two disjoint finite sets $\mathcal{P}$, the set of points, and $\mathcal{B}$, the set of blocks, and e subset $\mathcal{I}$ of $\mathcal{P} \times \mathcal{B}$. If (p, B) is in $\mathcal{I}$ we say that p is contained in B.

Definition 4.1.5. *An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a t-(v,k,λ)* **design***, where t, v, k and λ are non-negative integers, if*

(1) $|\mathcal{P}| = v$;

(2) $|B| = k$ *for all* $B \in \mathcal{B}$*;*

(3) every t *distinct points are together contained in precisely* λ *blocks.*

Theorem 4.1.6. *Let* $\mathcal{D}$ *be a* t-(v, k, λ) *design. Then for every integer* s *such that* $0 \leq s \leq t$, $\mathcal{D}$ *is a* s-(v, k, λ_s) *design with*

$$\lambda_s = \lambda \frac{(v-s)(v-s-1)\cdots(v-t+1)}{(k-s)(k-s-1)\cdots(k-t+1)}.$$

An important parameter of a design is its **order**, that is define as

$$n = \lambda \frac{\binom{v-2}{k-1}}{\binom{v-t}{k-t}}.$$

Definition 4.1.7. *Let* $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$*, with* $|\mathcal{P}| = v$ *and* $|\mathcal{B}| = b$*. Let the points be labelled* $\{p_1, \ldots, p_v\}$ *and the blocks be labelled* $\{B_1, \ldots, B_b\}$*. An* **incidence matrix** *for* $\mathcal{S}$ *is a* $b \times v$ *matrix* $A = (a_{i,j})$ *of* 0*'s and* 1*'s such that*

$$a_{i,j} = \begin{cases} 1 & \text{if } (p_j, B_i) \in \mathcal{I} \\ 0 & \text{if } (p_j, B_i) \notin \mathcal{I} \end{cases}$$

Definition 4.1.8. *Let* $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *be an incident structure and* A *the incident matrix of* $\mathcal{S}$*. The code of* $\mathcal{S}$ *over* $\mathbb{F}_q$ *is the subspace* $\mathcal{C}_q(\mathcal{S})$ *of* $\mathbb{F}_q^{|\mathcal{P}|}$ *spanned by the rows of* A*.*

Definition 4.1.9. *If* $\mathcal{S}$ *is any incident structure and* p *is any prime, the* p-**rank** *of* $\mathcal{S}$ *is the dimension of the code* $\mathcal{C}_p(\mathcal{S})$ *and is written*

$$\operatorname{rank}_p(\mathcal{S}) = \dim(\mathcal{C}_p(\mathcal{S})).$$

Theorem 4.1.10. *Let* $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ *be a* 2-(v, k, λ) *design of order* n *and let* p *be a prime dividing* n*. Then*

$$\operatorname{rank}_p(\mathcal{D}) \leq \frac{|\mathcal{B}| + 1}{2};$$

more over if p *does not divide* λ *and* p^2 *does not divide* n*, then*

$$\mathcal{C}_p(\mathcal{D})^{\perp} \subseteq \mathcal{C}_p(\mathcal{D})$$

and $rank_p(\mathcal{D}) \geq v/2$*.*

4.1.3 Projective planes

A 2-$(n^2+n+1, n+1, 1)$ design, for $n \geq 2$, is called a **projective plane** of order n.

Remark 4.1.11. A projective plane of order n has the same number of points and blocks, i.e. $|\mathcal{P}| = |\mathcal{B}|$.

Theorem 4.1.12 ([Ass92]). *Let Π be a projective plane of order n and p be a prime such that $p|n$. Then the p-ary code of Π, $\mathcal{C}_p(\Pi)$, has minimum distance $n+1$. Moreover the scalar multiples of the rows of the incidence matrix are the codewords of minimal weight.*

Chouinard, in [Cho00], proved that:

Theorem 4.1.13. *Let $\mathcal{C}_p(\Pi)$ be a code arising from a projective plane of prime order p. Then there are no codewords of weight in the interval $[p+2, 2p-1]$.*

4.1.4 Graphs terminology

Definition 4.1.14. *A* **simple graph** *is a pair $\mathcal{G} = (\mathcal{V}(\mathcal{G}), \mathcal{E}(\mathcal{G}))$ where:*

- *$\mathcal{V}(\mathcal{G})$ is the set of* **vertices** *of $\mathcal{G}$,*
- *$\mathcal{E}(\mathcal{G})$ is the set of* **edges** *of $\mathcal{G}$.*

A typical edge of $\mathcal{G}$ is of the form $\{u, v\}$ where $u, v \in \mathcal{V}(\mathcal{G})$, and $u \neq v$. If $e = \{u, v\} \in \mathcal{E}(\mathcal{G})$ we say that u and v are **adjacent**. *We also refer to u and v as the* **endpoints** *of e.*

Definition 4.1.15. *A* **simple digraph** *is a pair $\mathcal{D} = (\mathcal{V}(\mathcal{D}), \mathcal{E}(\mathcal{D}))$ where:*

- *$\mathcal{V}(\mathcal{D})$ is the set of vertices of $\mathcal{D}$,*
- *$\mathcal{E}(\mathcal{D})$ is the set of* **arcs** *(or directed edges) of $\mathcal{D}$.*

A typical arc of $\mathcal{D}$ is of the form $e = (u, v)$ where $u, v \in \mathcal{V}(\mathcal{D})$, and $u \neq v$. The vertices u is called **tail** *of e and v the* **head** *of e. The arc e is called an* **out-going arc** *of u and an* **in-coming arc** *of v. The* **out-degree** *of a vertex u, $\deg_O(u)$ is the number of out-going arcs, and the* **in-degree** *of a vertex u, $\deg_I(u)$ is the number of in-coming arcs.*

Simple (di)graphs have no loops and no parallel (arcs) edges. In this thesis, only simple (di)graphs are considered. Therefore, we use (di)graphs to refer to simple

(di)graphs for succinctness. A complete graph is a graph that contains all possible edges.

For a digraph $\mathcal{D} = (\mathcal{V}(\mathcal{D}), \mathcal{E}(\mathcal{D}))$, unless specified otherwise, we label the vertices of $\mathcal{D}$ by the natural numbers $1, 2, \ldots, |\mathcal{V}(\mathcal{D})|$. The number of vertices $|\mathcal{V}(\mathcal{D})|$ is called the **order** of $\mathcal{D}$, whereas the number of arcs $|\mathcal{E}(\mathcal{D})|$ is called the **size** of $\mathcal{D}$.

The **complement** of a digraph $\mathcal{D} = (\mathcal{V}(\mathcal{D}), \mathcal{E}(\mathcal{D}))$, denoted by $\bar{\mathcal{D}} = (\mathcal{V}(\bar{\mathcal{D}}), \mathcal{E}(\bar{\mathcal{D}}))$, is defined as follows. The vertex set is $\mathcal{V}(\bar{\mathcal{D}}) = \mathcal{V}(\mathcal{D})$. The arc set is

$$\mathcal{E}(\bar{\mathcal{D}}) = \{(u, v) : u, v \in \mathcal{V}(\bar{\mathcal{D}}), (u, v) \notin \mathcal{E}(\mathcal{D})\}.$$

Analogous conventions and concepts are also defined for graphs.

Definition 4.1.16. *Let V be a subset of vertices of a graph $\mathcal{G} = (\mathcal{V}(\mathcal{G}), \mathcal{E}(\mathcal{G}))$ (digraph $\mathcal{D} = (\mathcal{V}(\mathcal{D}), \mathcal{E}(\mathcal{D}))$, respectively). The subgraph of $\mathcal{G}$ ($\mathcal{D}$, respectively) induced by V is a graph (digraph, respectively) whose vertex set is V , and edge set (arc set, respectively) is $\{\{u, v\} : u, v \in V, \{u, v\} \in \mathcal{E}(\mathcal{G})\}$ ($\{(u, v) : u, v \in V, (u, v) \in \mathcal{E}(\mathcal{D})\}$). We refer to such a subgraph as an* **induced subgraph** *of $\mathcal{G}$ ($\mathcal{D}$).*

Definition 4.1.17. *A* **path** *in a graph $\mathcal{G}$ (digraph $\mathcal{D}$, respectively) is a sequence of distinct vertices $(u_1, u_2, \ldots, u_k)$, such that $\{u_i, u_{i+1}\} \in \mathcal{E}(\mathcal{G})$ ($(u_i, u_{i+1}) \in \mathcal{E}(\mathcal{D})$, respectively) for all $i \in [k-1]$. If a path is closed, i.e. $\{u_k, u_1\} \in \mathcal{E}(\mathcal{G})$ ($(u_k, u_1) \in \mathcal{E}(\mathcal{D})$, respectively), then it is called* **circuit**. *A (di)graph is called* **acyclic** *if it contains no circuits.*

Let $\nu(\mathcal{D})$ be the **circuit packing number** of $\mathcal{D}$, namely, the maximum number of vertex-disjoint circuits in $\mathcal{D}$. A **feedback vertex set** of $\mathcal{D}$ is a set of vertices whose removal destroys all circuits in $\mathcal{D}$. Let $\tau(\mathcal{D})$ denote the **minimum size of a feedback vertex set** of $\mathcal{D}$.

Definition 4.1.18. *An* **independent set** *in a graph $\mathcal{G}$ is a set of vertices of $\mathcal{G}$ with no edges connecting any two of them. An independent set in $\mathcal{G}$ of largest cardinality is called a* **maximum independent set** *in $\mathcal{G}$. The cardinality of such a maximum independent set is referred to as the* **independence number** *of $\mathcal{G}$, denoted by $\alpha(G)$.*

In the case of digraph we denote by $\alpha(\mathcal{D})$ the **maximum induced acyclic subgraph** (note that for the graphs case a maximum independent set is an acyclic subgraph).

Definition 4.1.19. *A* **clique** *of a (di)graph is a set of vertices that induces a complete subgraph of that (di)graph. A* **clique cover** *of a (di)graph is a set of cliques that partition its vertex set. A* **minimum clique cover** *of a (di)graph is a clique cover of minimum number of cliques. The number of cliques in such a minimum clique cover of a (di)graph is called the* **clique cover number** *of that (di)graph. We denote by* $\mathbf{cc}(\mathcal{G})$ *the clique cover number of a (di)graph $\mathcal{G}$.*

Definition 4.1.20. *Let $\mathcal{D} = (\mathcal{V}(\mathcal{D}), \mathcal{E}(\mathcal{D}))$ be a digraph of order n. A matrix $M = (m_{i,j}) \in \mathbb{F}_q^{n\times n}$ is said* **to fit** *$\mathcal{D}$ if*

$$m_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } (i,j) \notin \mathcal{E}(\mathcal{D}) \end{cases}$$

The minrank of $\mathcal{D}$ over $\mathbb{F}_q$ is defined to be

$$\text{minrk}_q(\mathcal{D}) = \min\{\text{rank}_q(M) : M \text{ fits } \mathcal{D}\}$$

We also have analogous definitions for a graph.

Definition 4.1.21. *A (directed)* **hypergraph** *$\mathcal{H}$ is a pair $(\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is a set of* **vertices** *and $\mathcal{E}$ is a set of* **hyperacrs***. A hyperarc e itself is an ordered pair (v, H), where $v \in \mathcal{V}$ and $H \subseteq \mathcal{V}$, they respectively represent the* **tail** *and the* **head** *of the hyperarc e.*

The **complement** of $\mathcal{H} = (\mathcal{V}, \mathcal{E})$, denoted by $\bar{\mathcal{H}} = (\bar{\mathcal{V}}, \bar{\mathcal{E}})$, is defined as follows. The vertex set is $\bar{\mathcal{V}} = \mathcal{V}$. The hyperarc set is $\bar{\mathcal{E}} = \{(v, [n] \setminus H \cup \{v\}) : (v, H) \in \mathcal{E}\}$.

Definition 4.1.22. *Let $|\mathcal{V}| = n$ and $|\mathcal{E}| = m$. Let the hyperarcs be labelled $\{e_1, \ldots, e_m\}$, a matrix $M = (m_{i,j}) \in \mathbb{F}_q^{m\times n}$* **fits** *the hypergraph if*

$$m_{i,j} = \begin{cases} 1 & \text{if } j \text{ is the tail of } e_i \\ 0 & \text{if } j \text{ does not lie in the head of } e_i \end{cases}$$

The minrank of $\mathcal{H}$ over $\mathbb{F}_q$ is defined to be

$$\text{minrk}_q(\mathcal{H}) = \min\{\text{rank}_q(M) : M \text{ fits } \mathcal{H}\}$$

4.2 An introduction to ICSI problem

4.2.1 Index Coding problem

The Index Coding with Side Information (ICSI) problem is described in the following scenario. There is a unique sender S, who has a vector of messages $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$. There are also m receivers $R_1, ..., R_m$, each with a request for a data packet x_i, and it is assumed that each receiver has some side-information, that is, R_i has a subset of messages $\{x_j\}_{j \in \mathcal{X}_i}$, where $\mathcal{X}_i \subseteq [n]$ for all $i \in [m]$. The requested packet by R_i is denoting by $x_{f(i)}$, where $f : [m] \to [n]$ is a (surjective) **demand function**. Here we assume that $f(i) \notin \mathcal{X}_i$ for all $i \in [m]$. We may assume that each i-th receiver requests only the message $x_{f(i)}$, since a receiver requesting more than one message can be split into multiple receivers, each of whom requests only one message and has the same side information set as the original [ALS+08].

Let $\mathcal{X} = (\mathcal{X}_1, \ldots, \mathcal{X}_n)$. An instance of the ICSI problem (or an ICSI instance, for short) is given by a quadruple $\mathcal{I} = \mathcal{I}(m, n, \mathcal{X}, f)$. It can also be conveniently described by a (directed) hypergraph [ALS+08].

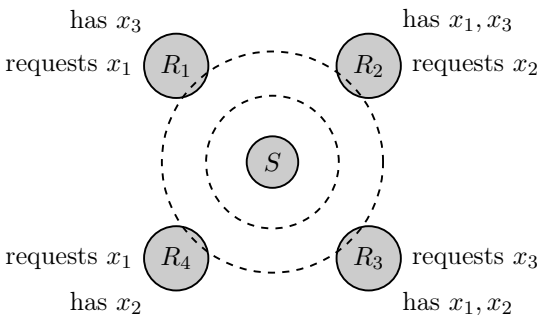
Definition 4.2.1. *Let $(m, n, \mathcal{X}, f)$ be an ICSI instance. The corresponding* **side information (directed) hypergraph** *$\mathcal{H} = \mathcal{H}(m, n, \mathcal{X}, f)$ is defined by the vertex set $\mathcal{V}(\mathcal{H}) = [n]$ and the hyperarc set $\mathcal{E}(\mathcal{H})$, where*

$$\mathcal{E}(\mathcal{H}) = \{(f(i), \mathcal{X}_i) : i \in [m]\}.$$

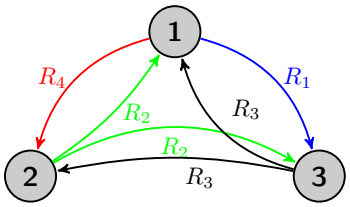
Example 4.2.2. Consider the scenario in Figure 4.2.2. The ICSI instance has $n = 3$ (three messages), $m = 4$ (four receivers), $f(1) = 1$, $f(2) = 2$, $f(3) = 3$, $f(4) = 1$, $\mathcal{X}_1 = \{3\}, \mathcal{X}_2 = \{1, 3\}, \mathcal{X}_3 = \{1, 2\}$, and $\mathcal{X}_4 = \{2\}$. The hypergraph $\mathcal{H}$ that describes this instance has three vertices $1, 2, 3$, and has four hyperarcs. These are $e_1 = (1, \{3\}), e_2 = (2, \{1, 3\}), e_3 = (3, \{1, 2\})$, and $e_4 = (2, \{2\})$. This hypergraph is depicted in Figure 4.2.2.

The sender can satisfy the demands of all receivers sending two messages, $x_1 + x_2$ and $x_1 + x_3$. Each receivers is able to recover the requesting packet using the side information.

Remark 4.2.3. If we have $m = n$ and $f(i) = i$ for all $i \in [n]$, the corresponding side information hypergraph has precisely n hyperarcs where each of them has a different origin vertex. Then it is simpler to describe such an ICSI instance by a digraph $\mathcal{G} = (\mathcal{V}(\mathcal{G}) = [n], \mathcal{E}(\mathcal{G}))$, so-called **side information (di)graph** [BYBJK06]. For each hyperarc $(i, \mathcal{X}_i)$ of $\mathcal{H}$, there will be $|\mathcal{X}_i|$ arcs (i, j) of $\mathcal{G}$, for $j \in \mathcal{X}_i$. Equivalently, $\mathcal{E}(\mathcal{G}) = \{(i, j) : i, j \in [n], j \in \mathcal{X}_i\}$.



(a) ICSI problem



(b) Side information hypergraph $\mathcal{H}$

Figure 4.1: An example of ICSI problem

Definition 4.2.4. *An* **index code** *over $\mathbb{F}_q$ for an ICSI instance $\mathcal{I}(m, n, \mathcal{X}, f)$ (also expressed $(m, n, \mathcal{X}, f)$-IC or $\mathcal{I}$-IC) of length N over $\mathbb{F}_q$ is an encoding map*

$$E : \mathbb{F}_q^n \to \mathbb{F}_q^N,$$

such that for each receiver R_i there is a decoding map

$$D_i : \mathbb{F}_q^N \times \mathbb{F}_q^{|\mathcal{X}_i|} \to \mathbb{F}_q,$$

satisfying

$$\forall \mathbf{x} \in \mathbb{F}_q^n,\ D_i(E(\mathbf{x}), \mathbf{x}_{\mathcal{X}_i}) = \mathbf{x}_{f(i)}.$$

We say that the $\mathcal{I}$-IC is linear if its encoding map E is $\mathbb{F}_q$-linear.

Definition 4.2.5. *An index code of minimum length is called* **optimal**.

Hereafter, we assume that the sets $\mathcal{X}_i$'s for $i \in [m]$ are known to S. In practice this can be achieved by a preliminary communication session.

The following lemma was implicitly formulated by Bar-Yossef *et al.* [BYBJK06, BYBJK11] for the case where $m = n$, $f(i) = i$ for all $i \in [m]$, and $q = 2$, then generalized to the case $m \neq n$ for any q by [DSC12]. This lemma specifies a sufficient condition on L to correspond to a linear $\mathcal{I}$-IC over $\mathbb{F}_q$.

Lemma 4.2.6. *An $(m, n, \mathcal{X}, f)$-IC of length N over $\mathbb{F}_q$ has a linear encoding map if and only if there exists a matrix $L \in \mathbb{F}_q^{N \times n}$ such that for each $i \in [m]$, there exists a vector $\mathbf{u}^{(i)} \in \mathbb{F}_q^n$ satisfying*

$$\mathrm{Supp}(\mathbf{u}^{(i)}) \subseteq \mathcal{X}_i \tag{4.1}$$

$$\mathbf{u}^{(i)} + \mathbf{e}_{f(i)} \in \mathrm{rowsp}(L). \tag{4.2}$$

Remark 4.2.7. The lemma above implies the existence of a vector $\mathbf{b}^{(i)} \in \mathbb{F}_q^N$ such that $\mathbf{b}^{(i)}L = \mathbf{u}^{(i)} + \mathbf{e}_{f(i)}$, in which case the receiver at i retrieves

$$x_{f(i)} = \mathbf{e}_{f(i)}\mathbf{x}^T = \mathbf{b}^{(i)}L\mathbf{x}^T - \mathbf{u}^{(i)}\mathbf{x}^T = \mathbf{b}^{(i)}\mathbf{y} - \mathbf{u}^{(i)}\mathbf{x}_{\mathcal{X}_i}^T.$$

As consequence we obtain the following corollary.

Corollary 4.2.8. *Let $\mathcal{I}(m, n, \mathcal{X}, f)$ be an instance of the ICSI problem, and $\mathcal{H}$ its hypergraph. Then the optimal length of a q-ary linear $\mathcal{I}$-IC is* $\text{minrk}_q(\mathcal{H})$.

Remark 4.2.9. Finding such an L with minimum number of rows by a careful selection of $\mathbf{u}^{(i)}$s is a difficult task (in fact, the corresponding decision problem is NP-complete [BYBJK06, Pee96]), which, however, yields a linear coding scheme with minimum number of transmissions.

4.2.2 Clique-covering bound and circuit-packing bound

Methods for constructing index codes (i.e. upper bounds for index coding) can be broadly separated in two categories: graph theoretic methods and algebraic methods relying on rank minimization. Here we report two upper bounds coming from graph theoretic methods.

The first comes from the well-known fact that all the users forming a clique in the side information digraph can be simultaneously satisfied by transmitting the sum of their packets [BK98]. This idea shows that the number of cliques required to cover all the vertices of the graph (the clique cover number) is an achievable upper bound.

A lower bound on the min-rank of a (di)graph was given in [BYBJK06]. An acyclic (di)graph has min-rank equal to its order (see for instance [BYBJK06]) and for any subgraph $\mathcal{G}'$ of a graph $\mathcal{G}$ we have

$$\text{minrk}_q(\mathcal{G}') \leq \text{minrk}_q(\mathcal{G}).$$

Let M be a matrix that fits $\mathcal{G}$, the sub-matrix M' of M restricted on the rows and columns indexed by the vertices in $\mathcal{V}(\mathcal{G}')$ is a matrix that fits $\mathcal{G}'$. These two results can be summarize in the following theorem.

Theorem 4.2.10 (Sandwich property)**.** *Let $\mathcal{G}$ be a (di)graph. Then*

$$\alpha(\mathcal{G}) \leq \text{minrk}_q(\mathcal{G}) \leq \mathbf{cc}(\mathcal{G}).$$

Instead of covering with cliques, one can cover the vertices with circuits. In [CASL11] was introduced the so called **circuit-packing bound**. This bound was implicitly introduced by the authors. Indeed, Chaudhry and Sprintson construct a

linear index code partitioning the graph of the ICSI instance in disjoint circuits. The same bound was also given in the work of Dau *et al.* [DSC14]. Let $\nu(\mathcal{G})$ be the circuit-packing number of $\mathcal{G}$. Then

$$\text{minrk}_q(\mathcal{G}) \leq n - \nu(\mathcal{G}),$$

where n is the order of the graph.

In general the two bounds are not comparable, here we report two cases when it is possible to establish which is the lowest.

Proposition 4.2.11. *Let $\mathcal{G}$ be a directed graph. If there exist $\nu(\mathcal{G})$ vertex-disjoint circuits of order 2, i.e. $\mathcal{C}_i = (v_{i,1}, v_{i,2})$ for $i \in [\nu(\mathcal{G})]$. Then*

$$\mathbf{cc}(\mathcal{G}) \leq n - \nu(\mathcal{G}).$$

Proof. Consider the subgraph $\mathcal{G}'$ of $\mathcal{G}$ with $\mathcal{V}(\mathcal{G}') = \mathcal{V}(\mathcal{G})$ and the set of arcs containing only the arcs relative to the circuits $\mathcal{C}_1, \ldots, \mathcal{C}_{\nu(\mathcal{G})}$. Thus $\mathbf{cc}(\mathcal{G}') = n - \nu(\mathcal{G})$, in fact we have $n - 2\nu(\mathcal{G})$ cliques composed only from single vertices, and $\nu(\mathcal{G})$ cliques of two vertices. From the fact that $\mathcal{G}'$ is a subgraph of $\mathcal{G}$ with same vertices set, our claim follows. □

Example 4.2.12. Consider the graph as in Figure 4.2.12. It is easy to check that $\nu(\mathcal{G}) = 2$, and we can obtain this considering 2 disjoint circuits of order 2 in the clique composed by the vertex $1, 2, 3, 4$. So we have $\mathbf{cc}(\mathcal{G}) = 2$ and $n - \nu(\mathcal{G}) = 3$.

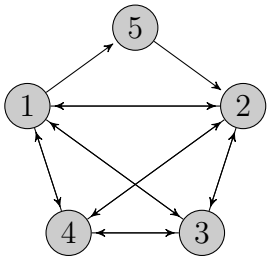


Figure 4.2: graph $\mathcal{G}$

Proposition 4.2.13. *Let $\mathcal{G}$ be a directed graph with at most two circuits of order 2. Then*

$$n - \nu(\mathcal{G}) \leq \mathbf{cc}(\mathcal{G}).$$

Proof. It follows from the fact that if the two circuits are vertex-disjoint we have at least $n - 2$ cliques and $\nu(\mathcal{G}) \geq 2$. Otherwise the cliques are at least $n - 1$ and $\nu(\mathcal{G}) \geq 1$. □

Example 4.2.14. Consider the graph as in Figure 4.2.14. It is easy to check that $\nu(\mathcal{G}) = 3$. So we have $\mathbf{cc}(\mathcal{G}) = 8$ and $n - \nu(\mathcal{G}) = 6$.

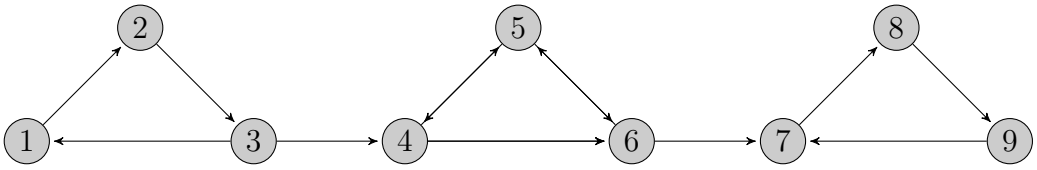


Figure 4.3: graph $\mathcal{G}$

4.2.3 Nonlinear Index Coding Outperforming the Linear Optimum

The graph parameter $\text{minrk}_q(\mathcal{G})$ completely characterizes the length of an optimal linear index code. Bar-Yossef et al. [BYBJK06, BYBJK11] showed that in various cases linear codes attain the optimal word length, and they conjectured that the minimum broadcast rate of a graph $\mathcal{G}$ was $\text{minrk}_2(\mathcal{G})$ also for non-linear codes. Lubetzky and Stav in [LS09] disproved this conjecture.

Definition 4.2.15. *Let $\mathcal{G}$ be a (di)graph related to an ICSI instance $\mathcal{I}$. The broadcast rate $\beta_q(\mathcal{G})$ over $\mathbb{F}_q$ of an IC (not necessarily linear) is the minimum number of symbols of $\mathbb{F}_q$ necessary to encode. Moreover the minimum broadcast rate $\beta(\mathcal{G})$ is the minimum broadcast possible over all $\mathbb{F}_q$, that is*

$$\beta(\mathcal{G}) = \inf_q \beta_q(\mathcal{G}).$$

By definition it results $\beta(\mathcal{G}) \leq \beta_q(\mathcal{G}) \leq \text{minrk}_q(\mathcal{G})$.

The result obtained by Lubetzky and Stav is the following.

Theorem 4.2.16 ([LS09])**.** *For any $\varepsilon > 0$ and any sufficient large n there is an n-vertex graph $\mathcal{G}$ such that:*

1) *any linear IC for $\mathcal{G}$ over some field $\mathbb{F}_q$ requires $\sqrt{n}$ symbols, i.e.* $\text{minrk}_q(\mathcal{G}) \geq \sqrt{n}$,

2) *there exists a non-linear IC using n^ε symbols that is $\beta(\mathcal{G})$.*

In the works of Alon *et al.* [ALS+08] and Shanmugam *et al.* [SDL14], it turns out that the idea based on coloring the vertex of the complement of the graph $\mathcal{G}$ lead to a family of stronger bounds on $\beta(\mathcal{G})$, starting with an LP relaxation called *fractional chromatic number* [ALS+08] and the stronger *fractional local chromatic number* [SDL14]. Let $\chi(\mathcal{G})$ denotes the chromatic number of a graph we recall that $\chi(\bar{\mathcal{G}}) = \mathbf{cc}(\mathcal{G})$. So denoting with $\chi_f(\mathcal{G})$ and $\chi_f^l(\mathcal{G})$ the fractional chromatic number and the fractional local chromatic number, respectively, we obtain the following theorem.

Theorem 4.2.17 ([ALS+08, SDL14])**.**

$$\beta(\mathcal{G}) \leq \chi_f^l(\mathcal{G}) \leq \chi_f(\mathcal{G}).$$

4.2.4 Error correction in ICSI problem

Dau *et al.* in [DSC13] studied the case that the transmitted symbols are subject to errors, introducing the error-correcting index codes (ECICs). In this model, given an $\mathcal{I}(m, n, \mathcal{X}, f)$-IC the sender S transmits the vector $E(\mathbf{x})$ and for each $i \in [m]$, R_i receives

$$\mathbf{y}_i = E(\mathbf{x}) + \varepsilon_i \in \mathbb{F}_q^N.$$

Definition 4.2.18. *An $\mathcal{I}(m, n, \mathcal{X}, f)$-IC over $\mathbb{F}_q$ of length N is called* δ**-error correcting** *(referred to as an $(\mathcal{I}, \delta)$-ECIC) if there is is an encoding function*

$$E : \mathbb{F}_q^n \to \mathbb{F}_q^N,$$

such that for each receiver R_i, $i \in [m]$, there exists a decoding function

$$D_i : \mathbb{F}_q^N \times \mathbb{F}_q^{|\mathcal{X}_i|} \to \mathbb{F}_q,$$

satisfying

$$\forall \mathbf{x} \in \mathbb{F}_q^n \text{ and } \forall \varepsilon_i \in \mathbb{F}_q^N,\ w(\varepsilon_i) \leq \delta\ :\ D_i(E(\mathbf{x}) + \varepsilon_i, \mathbf{x}_{\mathcal{X}_i}) = x_{f(i)}.$$

The code is called linear if E is $\mathbb{F}_q$-linear.

Given an ICSI instance $\mathcal{I}(m, n, \mathcal{X}, f)$, and $\mathcal{H}$ its hypergraph, for each $i \in [m]$, we define the following set:

$$\mathcal{Y}_i := [n] \setminus \mathcal{X}_i \cup \{f(i)\} \text{ and } \mathcal{Z}_i := [n] \setminus \mathcal{X}_i = \mathcal{Y}_i \cup \{f(i)\}.$$

A necessary and sufficient condition for a matrix L to correspond to a ECIC is the following.

Lemma 4.2.19 ([DSC13])**.** *The matrix L corresponds to an $(\mathcal{I}, \delta)$-ECIC over $\mathbb{F}_q$ if and only if for each $i \in [m]$*

$$w(L^{\mathcal{Z}_i}\mathbf{v}_{\mathcal{Z}_i}^T) \geq 2\delta + 1$$

for each $\mathbf{v} \in \mathbb{F}_q^n$ satisfying $\mathrm{Supp}(\mathbf{v}) \subset \mathcal{Z}_i$ and $v_{f(i)} \neq 0$.

Clearly any $(\mathcal{I}, \delta)$-ECIC can detect up to 2δ errors. The following Lemma is equivalent to Lemma 4.2.6.

Lemma 4.2.20. *An $(m, n, \mathcal{X}, f)$-IC of length N over $\mathbb{F}_q$ has a linear encoding map if and only if there exists a matrix $L \in \mathbb{F}_q^{N \times n}$ such that for each $i \in [m]$,*

$$L^{f(i)} \notin \mathrm{colsp}(L^{\mathcal{Y}_i}).$$

4.2.5 α-bound, κ-bound and Singleton bound

In [DSC13] the authors report some bounds on the optimal length of an ECIC, which we report in the following two results. Let

$$\mathcal{J}(\mathcal{H}) = \bigcup_{i\in[m]} \{\{f(i)\} \cup Y_i : Y_i \subseteq \mathcal{Y}_i\}.$$

Definition 4.2.21. *A subset H of $[n]$ is called a* **generalized independent set** *in $\mathcal{H}$ if every nonempty subset K of H belongs to $\mathcal{J}(\mathcal{H})$. The size of a maximum generalized independent set in $\mathcal{H}$ is denoted by $\alpha(\mathcal{H})$.*

We denote by $\mathcal{N}_q(\mathcal{I}, \delta)$ the optimal length N of an $(\mathcal{I}, \delta)$-ECIC and by $N_q(k, d)$ the optimal length of a k-dimensional linear code over $\mathbb{F}_q$ of minimum distance d.

Theorem 4.2.22 (α-bound and κ-bound)**.** *Let $\mathcal{H}$ be the side information hypergraph of the ICSI instance $\mathcal{I}$. Let $\kappa_q = \text{minrk}_q(\mathcal{H})$. Then an ECIC for the instance $\mathcal{I}$ satisfies*

$$N_q(\alpha(\mathcal{H}), 2\delta + 1) \leq \mathcal{N}_q(\mathcal{I}, \delta) \leq N_q(\kappa_q, 2\delta + 1).$$

It is shown in the example below that these inequalities can be strict.

Example 4.2.23. Let $q = 2$, $m = n = 5$, $\delta = 2$, and $f(i) = i$ for all $i \in [m]$. Assume

$$\mathcal{X}_1 = \{2, 5\}, \mathcal{X}_2 = \{1, 3\}, \mathcal{X}_3 = \{2, 4\}, \mathcal{X}_4 = \{3, 5\}, \mathcal{X}_5 = \{1, 4\}.$$

Let $\mathcal{H}$ the associated hypergraph. Then we have

$$\begin{aligned}\mathcal{J}(\mathcal{H}) = \{&\{1\}, \{1, 3\}, \{1, 4\}, \{1, 3, 4\}, \{2\}, \{2, 4\}, \{2, 5\},\\ &\{2, 4, 5\}, \{3\}, \{1, 3\}, \{3, 5\}, \{1, 3, 5\}, \{4\}, \{1, 4\},.\\ &\{2, 4\}, \{1, 2, 4\}, \{5\}, \{2, 5\}, \{3, 5\}, \{2, 3, 5\}\}\end{aligned}$$

It is easy to verify that $\alpha(\mathcal{H}) = 2$. It follows from [BYBJK11, Theorem 9] that $\text{minrk}_2(\mathcal{H}) = 3$. From [SS06] we have $N_2(2, 5) = 8$, $N_2(3, 5) = 10$ and from [DSC13] $\mathcal{N}_2(\mathcal{H}, 2) = 9$.

Theorem 4.2.24 (Singleton bound)**.** *Let $\mathcal{H}$ be the side information hypergraph of the ICSI instance $\mathcal{I}$. Let $\kappa_q = \text{minrk}_q(\mathcal{H})$. Then an ECIC for the instance $\mathcal{I}$ satisfies*

$$\mathcal{N}_q(\mathcal{I}, \delta) \geq \kappa_q + 2\delta$$

An implicit upper bound on the optimal length of the ECICs is based on constructing a random ECIC.

Theorem 4.2.25. *Let $\mathcal{I} = (m, n, \mathcal{X}, f)$ be an instance of the ICSI problem. Then there exists a linear $(\mathcal{I}, \delta)$-ECIC over $\mathbb{F}_q$ of length N if*

$$\sum_{i\in[m]} q^{n-|\mathcal{X}_i|-1} < \frac{q^N}{V_q(n, r)}.$$

4.2.6 Syndrom decoding

Consider the $(\mathcal{I}, \delta)$-ECIC over $\mathbb{F}_q$ based on a matrix L. Suppose that the receiver R_i, $i \in [m]$, receives the vector

$$\mathbf{y}_i = L\mathbf{x}^T + \varepsilon_i, \tag{4.3}$$

where $L\mathbf{x}^T$ is the codeword transmitted by S, and ε_i is the error pattern affecting this codeword. In the classical coding theory, the transmitted vector $\mathbf{c}$, the received vector $\mathbf{y}$, and the error pattern $\mathbf{e}$ are related by $\mathbf{y} = \mathbf{c} + \mathbf{e}$. Therefore, if $\mathbf{y}$ is known to the receiver, then there is a one-to-one correspondence between the values of unknown vectors $\mathbf{c}$ and $\mathbf{e}$, whenever it occurs at most $\lfloor \frac{d-1}{2} \rfloor$ errors. For index coding, however, this is no longer the case.

From (4.3), we have

$$\mathbf{y}_i = L^{f(i)} x_{f(i)} + L^{\mathcal{X}_i} \mathbf{x}_{\mathcal{X}_i}^T + L^{\mathcal{Y}_i} \mathbf{x}_{\mathcal{Y}_i}^T + \varepsilon_i.$$

and

$$\mathbf{y}_i - L^{\mathcal{X}_i} \mathbf{x}_{\mathcal{X}_i}^T - \varepsilon_i \in \mathrm{Span}_q\{L^{f(i)} \cup \{L^j\}_{j \in \mathcal{Y}_i}\}.$$

Let $\mathcal{C}^{(i)} = \mathrm{Span}_q\{L^{f(i)} \cup \{L^j\}_{j \in \mathcal{Y}_i}\}$, and let $H^{(i)}$ be a parity check matrix of $\mathcal{C}^{(i)}$. We obtain that

$$H^{(i)} \varepsilon_i = H^{(i)}(\mathbf{y}_i - L^{\mathcal{X}_i} \mathbf{x}_{\mathcal{X}_i}^T).$$

Let β_i be a column vector defined by

$$\beta_i = H^{(i)}(\mathbf{y}_i - L^{\mathcal{X}_i} \mathbf{x}_{\mathcal{X}_i}^T).$$

Observe that each R_i is capable of determining β_i. Thus we have the following decoding procedure for R_i

Imput: $\mathbf{y}_i, \mathbf{x}_{\mathcal{X}_i}, L$.

Step 1**:** Compute

$$H^{(i)}(\mathbf{y}_i - L^{\mathcal{X}_i} \mathbf{x}_{\mathcal{X}_i}^T) = \beta_i. \tag{4.4}$$

Step 2**:** Find lowest weight solution $\bar{\varepsilon}$ of

$$H^{(i)} \bar{\varepsilon} = \beta_i. \tag{4.5}$$

Step 3**:** Given $\hat{\mathbf{x}}_{\mathcal{X}_i} = \mathbf{x}_{\mathcal{X}_i}$ solve the system for $\hat{x}_{f(i)}$

$$\mathbf{y}_i = L\hat{\mathbf{x}}^T + \bar{\varepsilon}. \tag{4.6}$$

Remark 4.2.26. Step 2 is computationally hard. Indeed, the problem of finding $\bar{\varepsilon}$ over $\mathbb{F}_2$ of the lowest weight satisfying $H^{(i)} \bar{\varepsilon} = \beta_i$, for a given binary vector β_i corresponds to the decision problem coset weights, which was shown by Berlekamp et al. [BMVT78] to be NP-complete.

On the optimal length of Index Codes

In this chapter we extend the so-called sandwich property to the min-rank of a hypergraph, improving in some case also the clique-covering bound for the digraphs. Then we characterize the digraphs that have extreme min-rank $n-1$ over a sufficiently large finite field, obtaining also that the problem of deciding whether the min-rank of a digraph is equal to $n-1$ over a field of cardianlity $q > n$ can be solve in polynomial time. In the last part we report a bound on the length of an index code whenever a t-design is contained in the side information.

5.1 Sandwich property for hypergraphs

In this section we consider hypergraphs $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ such that for all nodes $i \in \mathcal{V}$ there exists a hyperarc $e \in \mathcal{E}$ with tail v. If $\mathcal{H}$ does not satisfy this condition we can reduce $\mathcal{H}$ to the hypergraph $\mathcal{H}'$ obtained from $\mathcal{H}$ removing all vertices that are not tail of any hyperarc. Then we have that $\text{minrk}_q(\mathcal{H}) = \text{minrk}_q(\mathcal{H}')$. Indeed, any matrix that fits $\mathcal{H}$ can be obtained from a matrix that fits $\mathcal{H}'$ adding the columns related to the deleted vertices. These columns can be zero so the rank is the same.

A hypergraph $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ can be associated with the directed graph $\mathcal{G}_{\mathcal{H}} = (\mathcal{V}, \mathcal{E}')$ defined in the following way. For each directed edge $(i, V) \in \mathcal{E}$ there will be $|V|$ directed edges $(i, v) \in \mathcal{E}'$, for $v \in V$. It is straightforward that $\text{minrk}_q(\mathcal{G}_{\mathcal{H}}) \leq \text{minrk}_q(\mathcal{H})$ (under the previous assumption on $\mathcal{H}$).

The last inequality in Theorem 4.2.10 is called the **clique-covering** bound for min-rank. If we have a hypergraph $\mathcal{H}$, and let $\mathcal{G}_{\mathcal{H}}$ be the related (di)graph. Then we cannot use the clique number $\mathbf{cc}(\mathcal{G}_{\mathcal{H}})$ to obtain a bound on the min-rank of $\mathcal{H}$.

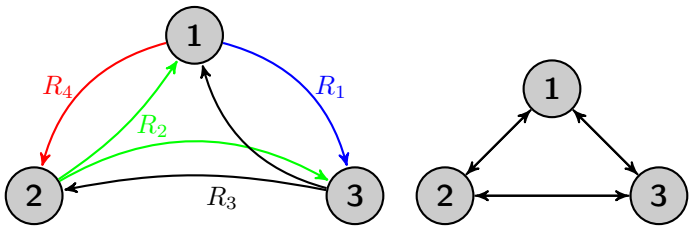
Example 5.1.1. Let $q = 2$, $n = 3$, $m = 4$, $f(i) = i$ for $i \in [3]$ and $f(4) = 1$. Assume

$$\mathcal{X}_1 = \{x_3\},\ \mathcal{X}_2 = \{x_1, x_3\},\ \mathcal{X}_3 = \{x_1, x_2\},\ \mathcal{X}_4 = \{x_2\}.$$

Let $\mathcal{H} = \mathcal{H}(4, 3, \mathcal{X}, f)$. Then it is easy to check that $\text{minrk}_2(\mathcal{H}) = 2$ and $\text{minrk}_2(\mathcal{G}_{\mathcal{H}}) = \mathbf{cc}(\mathcal{G}_{\mathcal{H}}) = 1$. In Figure 5.1 we have the graph $\mathcal{G}_{\mathcal{H}}$ and the hypergraph $\mathcal{H}$.

Remark 5.1.2. Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a (di)graph. Then

$$\mathbf{cc}(\mathcal{G}) = \min\{|\mathcal{P}| \mid \mathcal{P} \text{ is a partition of } \mathcal{V} \text{ composed by independent sets of } \bar{\mathcal{G}}\}.$$



(a) Hypergraph $\mathcal{H}$ (b) Graph $\mathcal{G}_{\mathcal{H}}$

Figure 5.1: Graphs of the Example 5.1.1

In fact, let $\mathcal{P}$ be a partition of $\mathcal{V}$ with independent sets of the graph $\bar{\mathcal{G}}$. Then each set of the partition form a clique in $\mathcal{G}$, so

$$\mathbf{cc}(\mathcal{G}) \leq |\mathcal{P}|.$$

Vice versa, the set of vertices in the same clique form an independent set of $\bar{\mathcal{G}}$.

Let $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ be a directed hypergraph we can always define an ICSI instance $(m, n, \mathcal{X}, f)$, as in the following:

- $n = |\mathcal{V}|$ and $m = |\mathcal{E}|$;
- let the vertices be labelled $\{v_1, \ldots, v_n\}$ and the blocks be labelled $\{e_1, \ldots, e_m\}$, then $f(i) = j$ if j is the tail of e_i and the set $\mathcal{X}_i$ is the head of e_i for all $i \in [m]$.

Remark 5.1.3. Let $\mathcal{H}$ be a hypergraph corresponding to an instance of the ICSI problem. Consider now the graph $\mathcal{G}_{\bar{\mathcal{H}}}$, we have that if there are no arcs between i and j, for some $i, j \in [n]$, then $i \notin \mathcal{Y}_l$, for all $l \in f^{-1}(j)$, and $j \notin \mathcal{Y}_h$, for all $h \in f^{-1}(i)$.

We report, now, our result on the clique-covering bound for the hypegraphs.

Theorem 5.1.4. *Let $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ be a hypergraph and $\bar{\mathcal{H}}$ its complement. Then*

$$\mathrm{minrk}_q(\mathcal{H}) \leq \mathbf{cc}(\bar{\mathcal{G}}_{\bar{\mathcal{H}}}).$$

Moreover, if the cardinalities of the edges' heads of $\bar{\mathcal{H}}$ are less than $\mathbf{cc}(\bar{\mathcal{G}}_{\bar{\mathcal{H}}}) - 1$. Then

$$\mathrm{minrk}_q(\mathcal{H}) \leq \mathbf{cc}(\bar{\mathcal{G}}_{\bar{\mathcal{H}}}) - 1.$$

Proof. We can suppose that $\mathcal{H}$ is related to an $(m, n, \mathcal{X}, f)$-ICSI instance. Let $\mathcal{P}$ be a partition of $\mathcal{V}$ composed by independent sets of $\mathcal{G}_{\bar{\mathcal{H}}}$. Then we can construct a matrix L such that two columns L_i, L_j are equal if i, j are in the same set of the partition and are linearly independents if i, j do not lie in the same set of the partition. Thus, such a matrix can be $L \in \mathbb{F}_q^{|\mathcal{P}| \times n}$ with $|\mathcal{P}|$ columns linearly independents. L is related to

the $(m, n, \mathcal{X}, f)$-ICSI instance from the Lemma 4.2.20 and the remark above. From Remark 5.1.2 we obtain the bound on the min-rank of the hypergraph.

Now suppose that for each edge e of $\bar{\mathcal{H}}$ we have $|U| < \mathbf{cc}(\bar{\mathcal{G}}_{\bar{\mathcal{H}}}) - 1$, where U is the head of e . Then we need, only, to construct $\mathbf{cc}(\bar{\mathcal{G}}_{\bar{\mathcal{H}}})$ vectors $\mathbf{cc}(\bar{\mathcal{G}}_{\bar{\mathcal{H}}}) - 1$ by $\mathbf{cc}(\bar{\mathcal{G}}_{\bar{\mathcal{H}}}) - 1$ linearly independents. These vectors can be of length $\mathbf{cc}(\bar{\mathcal{G}}_{\bar{\mathcal{H}}}) - 1$, e. g. we can use the vectors

$$\underbrace{(1, 0, \ldots, 0)}_{\mathbf{cc}(\bar{\mathcal{G}}_{\bar{\mathcal{H}}})-1}, (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1), (1, 1, \ldots, 1).$$

□

If $n = m$, then $\text{minrk}_q(\mathcal{H}) = \text{minrk}_q(\mathcal{G}_{\mathcal{H}})$ and $\mathcal{G}_{\bar{\mathcal{H}}} = \bar{\mathcal{G}}_{\mathcal{H}}$. So we obtain the following Corollary.

Corollary 5.1.5. *Let $\mathcal{G}$ be a directed graph. If the out-degree of the vertices of $\bar{\mathcal{G}}$ are less than $\mathbf{cc}(\mathcal{G}) - 1$, then*

$$\text{minrk}_q(\mathcal{G}) \leq \mathbf{cc}(\mathcal{G}) - 1.$$

Remark 5.1.6. For the case of a directed graph the Corollary 5.1.5 cannot be deduced from the Theorem 4.2.10. In [Hae78] the proof of Theorem 4.2.10 is based on the construction of the matrix $A = (a_{i,j})$, where

$$a_{i,j} = \begin{cases} 1 & \text{if } i, j \text{ same clique} \\ 0 & \text{otherwise} \end{cases}.$$

This matrix fits the directed graph $\mathcal{G}$ and $\text{rank}(A) = \mathbf{cc}(\mathcal{G})$. For the Corollary 5.1.5 we do not need to construct a matrix that fits $\mathcal{G}$, but only a matrix such that the rows satisfy the property of Lemma 4.2.20.

Example 5.1.7. Let $\mathcal{G}$ be a circuit of order n. We have that $\mathbf{cc}(\mathcal{G}) = n$, in fact there are no clique of order greaten than 1. Moreover, we note that for any $i \in \mathcal{V}(\bar{\mathcal{G}})$ with $i \leq n - 1$ $(i, j) \in \mathcal{E}(\bar{\mathcal{G}})$ if and only if $j \neq i$ and $j \neq i + 1$, and for $i = n$ $(n, j) \in \mathcal{E}(\bar{\mathcal{G}})$ if and only if $j \neq n$ and $j \neq 1$. That implies out-degree of i is equal to $n - 2$ for all $i \in \mathcal{V}(\bar{\mathcal{G}})$, from Corollary 5.1.5, we have $\text{minrk}_q(\mathcal{G}) \leq n - 1$. In that case we have the equality over any fields (see for instance [DSC14]).

5.2 On directed graphs with min-rank one less than the order

Recalling that $\tau(\mathcal{G})$ is the minimum number of vertices necessary to remove from $\mathcal{G}$ to obtain an acyclic subgraph, we have $n - \tau(\mathcal{G}) = \alpha(\mathcal{G})$, thus

$$n - \tau(\mathcal{G}) \leq \text{minrk}_q(\mathcal{G}) \leq n - \nu(\mathcal{G})$$

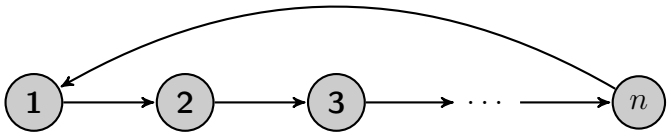


Figure 5.2: Circuit $\mathcal{G}$

over any finite field $\mathbb{F}_q$. In this section we characterize the graphs with min-rank one less than the order over finite fields with cardinality grater than n.

Lemma 5.2.1. *Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a directed graph of order n such that there exist $i_1, i_2 \in \mathcal{V}$ with*

(1) $(i_1, i_2) \in \mathcal{E}$ *and* $(i_2, i_1) \notin \mathcal{E}$

(2) $\deg_O(i_1) = 1$.

Let $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ with $\mathcal{V}' = \mathcal{V} \setminus \{i_1\}$ and $\mathcal{E}' = (\mathcal{E} \cup \{(j, i_2) \,|\, (j, i_1) \in \mathcal{E}\}) \setminus \{(i_1, i_2)\}$. Then

$$\text{minrk}_q(\mathcal{G}) = \text{minrk}_q(\mathcal{G}') + 1$$

for any q.

Proof. Let $M = (m_{i,j})$ be a matrix that fits $\mathcal{G}$ of minimum rank. W.l.o.g. we can suppose $i_1 = 1$ and $i_2 = 2$. then the first two rows of M are

$$M_1 = (1, \alpha, 0, \ldots, 0)$$

and

$$M_2 = (0, 1, m_{2,3}, \ldots, m_{2,n}).$$

If $\alpha = 0$ then it is easy to check that deleting the first row and the first column of M we obtain M' of rank $\text{rank}(M) - 1$ that fits $\mathcal{G}'$.

If $\alpha \neq 0$, we can suppose that the rows $M_1, M_2, \ldots, M_{\text{minrk}_q(\mathcal{G})}$ are linearly independents.

Denoting the vertices of $\mathcal{G}'$ with $\{i - 1 \mid \text{ for } i \in \mathcal{V} \setminus \{1\}\}$, that is the vertex 2 becomes 1, 3 becomes 2 and so on, we construct the matrix M' such that the i-th row is obtained by the $i + 1$-th row of M in the following way

$$M'_i = (m_{i+1,1} + m_{i+1,2}, m_{i+1,3}, \ldots, m_{i+1,n})$$

for $i = 1, \ldots, \text{minrk}_q(\mathcal{G}) - 1$. For $i = \text{minrk}_q(\mathcal{G}), \ldots, n - 1$ we define

$$M'_i = (m_{i+1,1} + m_{i+1,2} - \lambda_1(1 + \alpha), m_{i+1,3}, \ldots, m_{i+1,n})$$

where λ_1 is the coefficient of M_1 such that $M_{i+1} = \sum_{r=1}^{\text{minrk}_q(\mathcal{G})} \lambda_r M_r$. The matrix M' fits $\mathcal{G}'$, so

$$\text{minrk}_q(\mathcal{G}') \leq \text{rank}(M') \leq \text{minrk}_q(\mathcal{G}) - 1.$$

Vice versa, let $M' = (m'_{i,j})$ be a matrix that fits $\mathcal{G}'$ of rank $\text{minrk}_q(\mathcal{G}')$ and the rows $M'_1, M'_2, \ldots, M'_{\text{minrk}_q(\mathcal{G}')}$ are linear independents. Let $I = \{j \mid (j,1) \in \mathcal{E}\}$ be the set of vertices of $\mathcal{G}$ with outgoing arcs directed to 1. We construct the matrix M such that

$$M_1 = (1, -1, 0, \ldots, 0),$$
$$M_i = (m'_{i-1,1}, 0, m'_{i-1,2}, \ldots, m'_{i-1,n-1})$$

for $i = 2, \ldots, \text{minrk}_q(\mathcal{G}') + 1$ and $i \in I$, and

$$M_i = (0, m'_{i-1,1}, m'_{i-1,2}, \ldots, m'_{i-1,n-1})$$

for $i = 2, \ldots, \text{minrk}_q(\mathcal{G}') + 1$ and $i \notin I$. For $i > \text{minrk}_q(\mathcal{G}') + 1$ we have that the $i-1$-th row of M' is given by

$$M'_{i-1} = \sum_{r=1}^{\text{minrk}_q(\mathcal{G}')} \lambda_r M'_r,$$

with $\lambda_r \in \mathbb{F}_q$, thus we put

$$M_i = \left(m'_{i-1,1}, 0, m'_{i-1,2}, \ldots, m'_{i-1,n-1}\right)$$

if $i \in I$, and we obtain

$$M_i = \lambda M_1 + \sum_{r=2}^{\text{minrk}_q(\mathcal{G}')+1} \lambda_{r-1} M_r$$

where λ_r are the coefficient in the combination of M'_{i-1}, w.r.t the first rows of M', and $\lambda = \sum_{r \notin I} \lambda_{r-1}$.

If $i \notin I$

$$M_i = \left(0, m'_{i-1,1}, m'_{i-1,2}, \ldots, m'_{i-1,n-1}\right)$$

and

$$M_i = \lambda M_1 + \sum_{r=2}^{\text{minrk}_q(\mathcal{G}')+1} \lambda_{r-1} M_r$$

where $\lambda = -\sum_{r \in I} \lambda_{r-1}$.

M fits $\mathcal{G}$ and

$$\text{minrk}_q(\mathcal{G}) \leq \text{rank}(M) \leq \text{minrk}_q(\mathcal{G}') + 1.$$

□

Example 5.2.2. Let $\mathcal{G}$ and $\mathcal{G}'$ be two graphs as in Figure 5.2.2. The nodes 1 and 2 of $\mathcal{G}$ satisfy the condition (1) and (2) of the lemma above.

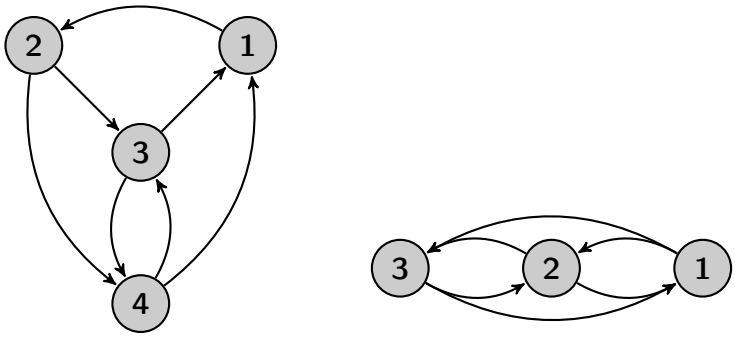
So we can reduce $\mathcal{G}$ to $\mathcal{G}'$, in fact consider the matrix

$$M = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

which fits $\mathcal{G}$. We have $M_3 = M_4 = M_1 + M_2$, constructing M' as in the lemma above we obtain

$$M' = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

M' fits $\mathcal{G}'$. Vice versa from M' we obtain M, and $\text{rank}(M) = \text{rank}(M') + 1$.



(a) $\mathcal{G}$ (b) $\mathcal{G}'$

Figure 5.3: Contraction

Here we report a proposition that will be proved in a more general case in the next chapter (see Corollary 6.3.4).

Proposition 5.2.3. *Let $\mathcal{G}$ be a graph of order n. Then*

$$\text{minrk}_q(\mathcal{G}) \leq n - \min_{v \in \mathcal{V}} \deg_O(v),$$

for any $q > n$.

Lemma 5.2.4. *Let $\mathcal{G}$ be a directed graph of order n such that $\tau(\mathcal{G}) = 2$. Then* $\text{minrk}_q(\mathcal{G}) = n - 2$*, for any $q > n$.*

Proof. We need only to prove $\text{minrk}_q(\mathcal{G}) \leq n - 2$.

W.l.o.g. we can suppose that there does not exist $i \in \mathcal{V}$ with out-degree less than 1, otherwise we can discharge the node and consider the subgraph without i, and the min-rank of $\mathcal{G}$ is the min-rank of the subgraph plus 1.

From the fact $\tau(\mathcal{G}) = 2$ we can have $\nu(\mathcal{G}) = 1, 2$. If it is equal to 2 then we have our claim immediately. So, assume $\nu(\mathcal{G}) = 1$. We can apply, now, Lemma 5.2.1, iteratively. Note that any time that we reduce $\mathcal{G}$ we obtain $\mathcal{G}'$ with $\tau(\mathcal{G}') = 2$ and $\nu(\mathcal{G}') = 1$, in fact any time that we reduce the graph we only shorten the circuits that pass trough the node that we delete, and we do not create any new circuit from the fact that the out degree of the node is 1.

When we cannot apply any more the Lemma 5.2.1, then we can have two possible cases:

1 the out degree of each node of the reduced graph $\mathcal{G}'$ is becamed at least 2,

2 there exists i_1 with out degree 1 and $(i_1, i_2), (i_2, i_1) \in \mathcal{E}'$.

This last case is not possible, in fact if we consider the circuit $C = (i_1, i_2)$, from $\tau(\mathcal{G}') = 2$ we have that there exists a circuit C' which, removing i_2, is not broken. Then, C' does not pass trough i_1 other wise it has to pass trough i_2. Then C and C' are disjoint, but this is not possible because $\nu(\mathcal{G}') = 1$.

So, reducing $\mathcal{G}$ we obtain $\mathcal{G}'$ with k less nodes and all nodes have out degree at least 2. From the proposition above and Lemma 5.2.1 it follows

$$\text{minrk}_q(\mathcal{G}) = \text{minrk}_q(\mathcal{G}') + k \leq n - 2.$$

□

We have now our main result of this section.

Theorem 5.2.5. *Let $\mathcal{G}$ a graph of order n and $q > n$. Then* $\text{minrk}_q(\mathcal{G}) = n - 1$ *if and only if $\tau(\mathcal{G}) = 1$*

Proof. If $\tau(\mathcal{G}) = 1$ then $\nu(\mathcal{G}) = 1$ and we have $\text{minrk}_q(\mathcal{G}) = n - 1$.

Vice versa assume by contradiction that $\tau(\mathcal{G}) \geq 2$, then we can consider a subgraph $\mathcal{G}'$ of $\mathcal{G}$ with $\tau(\mathcal{G}) = 2$. From Lemma 5.2.4 we have our claim. □

This last theorem implies that the problem to decide whether a digraph has min-rank $n - 1$, over a sufficiently large field, can be solved in polynomial time, using the Depth-first search algorithm (see for instance [CSRL01]), which verify in a polynomial time if a graph is acyclic.

Corollary 5.2.6. *Let $\mathcal{D}$ be a digraph of order n and $q > n$. Then deciding whether* $\text{minrk}_q(\mathcal{D}) = n - 1$ *can be done in polynomial time ($\mathcal{O}(n^3)$).*

In the following table we report the values of the min-rank for graphs and directed graphs with near-extreme min-rank (i.e. $1, 2, n-2, n-1$ and n).

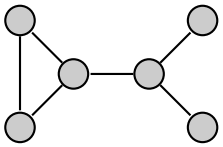


Figure 5.4: Forbidden subgraph

Min-rank	**Graph $\mathcal{G}$**	**Directed graph $\mathcal{D}$**
1	$\mathcal{G}$ is complete (trivial)	$\mathcal{D}$ is complete (trivial)
2	if $\bar{\mathcal{G}}$ is 2 colorable [Pee96]	for $q = 2$, if $\bar{\mathcal{D}}$ is 3-fair colorable [DSC14]
n-2	$\mathcal{G}$ has maximum matching 2 and does not contain the graph in Figure 5.2 [DSC14]	unknown
n-1	$\mathcal{G}$ is a star graph [DSC14]	for $q > n$, $\tau(\mathcal{D}) = 1$ Theorem 5.2.5
n	$\mathcal{G}$ has no edges (trivial)	$\mathcal{D}$ is acyclic (trivial) [BYBJK06]

5.3 A bound from t-designs

In this section we study the case when it is possible to individuate an incident structure in the side information. From that we obtain a bound on the min-rank of the hypergraph, when the incidence structure is a 2 design. Moreover we study the particular case when the design is a projective plane, i. e. a 2-$(n^2 + n + 1, n + 1, 1)$ design.

Definition 5.3.1. *We said that an instance, $(m, n, \mathcal{X}, f)$, of the ICSI problem* **contains an incident structure** $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ *if*

1) $\mathcal{P} = [n]$ *and* $|\mathcal{B}| \leq m$*;*

2) *for each $i \in [m]$ there exists $B \in \mathcal{B}$ such that $f(i) \in B$ and $B \setminus \{f(i)\} \subseteq \mathcal{X}_i$.*

More over we said that the instance **coincides** *with the incident structure $\mathcal{S}$ if it is satisfy*

2′) *for each* $i \in [m]$ *there exists* $B \in \mathcal{B}$ *such that* $f(i) \in B$ *and* $B \setminus \{f(i)\} = \mathcal{X}_i$.

We immediately obtain the following proposition.

Proposition 5.3.2. *Let* $(m, n, \mathcal{X}, f)$ *be an instance of ICSI problem and* $\mathcal{H}$ *let be the corresponding hypergraph. If the instance contains a* 2-(n, k, λ) *design* $\mathcal{D} = (\mathcal{P}, \mathcal{B})$. *Then for all* q *a power of a prime* p *such that* p *divides the order of* $\mathcal{D}$ *we have*

$$\text{minrk}_q(\mathcal{H}) \leq \frac{m+1}{2}.$$

Proof. Let D be the incident matrix of $\mathcal{D}$. Then for the Theorem 4.1.10 we have that the p-rank of $\mathcal{D}$ is less or equal to $\frac{m+1}{2}$.

Now, it is easy to check that D fits $\mathcal{H}$, so

$$\text{minrk}_q(\mathcal{H}) \leq \text{rank}_q(D) \leq \text{rank}_p(\mathcal{D})$$

and that concludes the proof. □

Remark 5.3.3. To compute the min-rank of a hypergraph is an NP-hard problem [Pee96]. When there exists a 2-design as in Proposition 5.3.2 it is possible to have a bound on this value and we can use the linear independents rows of its incident matrix to decrease the number of transmission.

Example 5.3.4. Consider the instance of the ICSI problem $\mathcal{I}$ given by $n = m = 7$, and $f(i) = i$ for $i = 1, \ldots, 7$. Let the side information be

$$\mathcal{X}_1 = \{2, 3\},\ \mathcal{X}_2 = \{6, 7\},\ \mathcal{X}_3 = \{5, 7\},\ \mathcal{X}_4 = \{2, 5\},$$

$$\mathcal{X}_5 = \{1, 6\},\ \mathcal{X}_6 = \{3, 4\},\ \mathcal{X}_7 = \{1, 4\}.$$

Consider the blocks

$$B_1 = \{1, 2, 3\},\ B_2 = \{2, 6, 7\}, B_3 = \{3, 5, 7\},\ B_4 = \{2, 4, 5\},$$

$$B_5 = \{1, 5, 6\},\ B_6 = \{3, 4, 6\},\ B_7 = \{1, 4, 7\}$$

These blocks form the Fano plane as in Figure 5.3.4. This is a 2-$(7, 3, 1)$ design of order 2 and the design is contained in the side information. The 2-rank of the design is 4. Then we can consider 4 linear independent rows of the incident matrix of the Fano plane, and encode the message using those. That permits to decrease the number of transmission from 7 to 4.

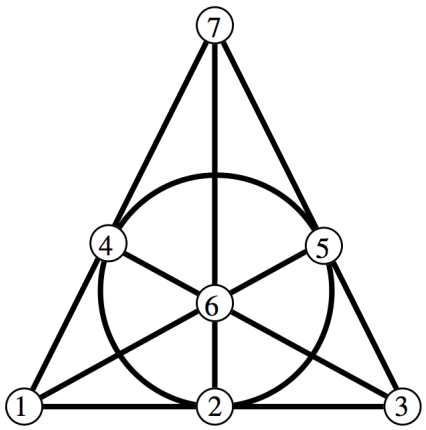


Figure 5.5: Fano plane

5.3.1 Security with projective planes

Here we consider the case when an instance $(m, n, \mathcal{X}, f)$ of the ICSI problem contains a 2-$(n^2+n+1, n+1, 1)$ design, and the matrix corresponding to the index code is composed from the independent rows of the incident matrix of the design. We recall that a 2-$(n^2+n+1, n+1, 1)$ design has order n and the code of the design over $\mathbb{F}_p$, with p a prime number s. t. p divides n, has minimum distance equal to $n+1$ (Theorem 4.1.12).

Theorem 5.3.5. *If the instance $\mathcal{I}$ of the ICSI problem coincides with the 2-$(n^2+n+1, n+1, 1)$ design, then each receiver R_i with $i \in [m]$ it is not able to recover a massage $x_j \notin \mathcal{X}_i \cup \{f(i)\}$.*

Proof. Let $\mathcal{D}$ be the 2-$(n^2+n+1, n+1, 1)$ design. Suppose that R_i wants to recover $x_j \notin \mathcal{X}_i \cup \{f(i)\}$. For the Lemma 3.2.3 it is able to do so if and only if there exists a vector $\mathbf{u} \in \mathbb{F}_p^N$, $N = n^2+n+1$, such that $\mathrm{Supp}(\mathbf{u}) \subseteq \mathcal{X}_i \cup \{f(i)\}$ and $\mathbf{u}+\mathbf{e}_j \in \mathcal{C}(\mathcal{D})$. If this vector is a codeword of the code, at least $n+1$ positions are different from 0. Now consider the vector $\mathbf{1}_{\mathcal{X}_i}+\mathbf{e}_{f(i)} \in \mathcal{C}(\mathcal{D})$, where with $\mathbf{1}_{\mathcal{X}_i}$ we means the vector in $\mathbb{F}_p^N$ with 1's in the positions contained in $\mathcal{X}_i$. We have $|\mathrm{Supp}(\mathbf{u}+\mathbf{e}_j) \cap \mathrm{Supp}(\mathbf{1}_{\mathcal{X}_i}+\mathbf{e}_{f(i)})| \geq n$ and also there are at least 2 positions of $\mathbf{u}+\mathbf{e_j}$ in this intersection that have the same value (we can use only the $p-1$ values of $\mathbb{F}_p \setminus \{0\}$ for these n positions). Suppose that this value is $\alpha \in \mathbb{F}_p \setminus \{0\}$, then we have $d(\mathbf{u}+\mathbf{e}_j, \alpha(\mathbf{1}_{\mathcal{X}_i}+\mathbf{e}_{f(i)})) \leq n$. So $\mathbf{u}+\mathbf{e_j}$ is not a codeword of $\mathcal{C}(\mathcal{D})$, that means that R_i is not able to recover x_j. □

Remark 5.3.6. Encoding with a matrix related to a projective plane guarantees the privacy of the transmission.

Assume, now, the presence of an adversary A who can listen to all transmissions. The adversary is assumed to possess side information $\{x_h \,|\, h \in \mathcal{X}_A \subseteq [n]\}$. In [DSC12],

it is shown that if $|\mathcal{X}_A| \leq d(\text{rowsp}(L)) - 2$, then A is not able to recover an element x_j with $j \notin \mathcal{X}_A$.

Now, consider an instance $(m, n, \mathcal{X}, f)$ of the ICSI problem containing a 2-$(p^2 + p + 1, p + 1, 1)$ design, and suppose that to transmit the messages we use the matrix L as above. Then we obtain the following result.

Theorem 5.3.7. *If $|\mathcal{X}_A| \leq 2p-2$ and for each block B of the design $|\mathcal{X}_A \cap B| \leq p-1$, then A is not able to recover x_j for all $j \notin \mathcal{X}_A$.*

Proof. If p is even, then the thesis follows from the fact that $|\mathcal{X}_A| \leq 1 = d - 2$. Let p be odd. We know,Theorem 4.1.13, that in the code related at the 2-$(p^2+p+1, p+1, 1)$ design there are not codewords with weight in $[p + 2, 2p - 1]$. To recover the message x_j, A needs a codewords of weight $p+1$. Those kinds of codewords are the codewords related to some block B, that is

$$\sum_{i \in B} \mathbf{e}_i$$

and the multiplies of these.

So A recovers x_j if and only if there exists $\mathbf{u} + \mathbf{e}_j \in \mathcal{C}$ with $\text{Supp}(\mathbf{u}) \subset \mathcal{X}_A$ and $|\text{Supp}(\mathbf{u})| = p$. Here $\mathcal{C}$ means the code of the projective space. Then $\text{Supp}(\mathbf{u}+\mathbf{e}_j) = B$ for some block B, and so $|(\mathcal{X}_A \cup \{j\}) \cap B| \geq p + 1$. □

Index Coding with Coded Side Information Problem

In this chapter we study the more general case where the side information can be coded packets. That problem was introduced by Shum *et al.* in [SDS12], where a linear index code with coded side-information can be found equivalently by solving a system of multi-variable polynomial equations, which is difficult to solve in general. Here, we extend the definition of min-rank at an instance of the index coding with coded side information (ICCSI) problem, showing that this is the optimal length for a linear index code related to the instance. Then we extend some results on the ECICs.

6.1 Broadcasting with coded side information

A simple example of the scenario is the following. The source node has three packets x_1, x_2 and x_3, which are elements in $\mathbb{F}_2$. There are three users. For $i = 1, 2, 3$, user i wants packet x_i. The transmitted packet is subject to independent erasures. It is assumed that there are feedback channels from the users, informing the transmitting node which packets are successfully received. Consider the following scenario. The source node transmits packets x_1, x_2 and x_3 in time slot $1, 2$ and 3 respectively. At the end of time slot 3, user 1 has packets x_2 and x_3, and user 2 has packets x_1 and x_3, while user 3 fails to receive any packet. The source node in time slot 4 transmits the coded packet $x_1 + x_2$, and hope that user 1 and user 2 can decode their packets. Unfortunately, only user 3 can receive the coded packet $x_1 + x_2$ in time slot 4. There is now a coding opportunity that utilizes the coded packet $x_1 + x_2$ in user 3s cache. The source can send the sum $x_1 + x_2 + x_3$ in time slot 5. If all three users can receive $x_1 + x_2 + x_3$ successfully, then all user can decode the required packets by linearly combining with the packets received earlier (see Fig. 6.1).

We present the coded model as follows. There is a data vector $\mathbf{x} \in \mathbb{F}_q^n$, $\mathbf{x} = (x_1, \ldots, x_n)$. For each $i \in [m]$, user R_i seeks some linear combination of the x_i's, say $\mathbf{r}_i\mathbf{x}^T$ for some $\mathbf{r}_i \in \mathbb{F}_q^n$. A user's cache comprises a pair $(V^{(i)}, \Lambda^{(i)})$

$$V^{(i)} \in \mathbb{F}_q^{d_i \times n} \text{ and } \Lambda^{(i)} \in \mathbb{F}_q^{d_i}$$

related by the equation

$$\Lambda^{(i)} = V^{(i)}\mathbf{x}^T.$$

Time slot	Packet sent	Received by R_1?	Received by R_2?	Received by R_3?
1	x_1	no	yes	no
2	x_2	yes	no	no
3	x_3	yes	yes	no
4	$x_1 + x_2$	no	no	yes
5	$x_1 + x_2 + x_3$	yes	yes	yes

Figure 6.1: Illustration of utilizing coded packets as side information.

While the vector $\mathbf{x}$ is unknown to R_i, it is assumed that any vector in the row spaces of $V^{(i)}$ can be generated by user R_i and for each vector $\mathbf{v}$ in the row space of $V^{(i)}$, R_i can determine $\mathbf{v}\mathbf{x}^T$ using $\Lambda^{(i)}$. We denote the row space by $\mathcal{X}^{(i)} := \text{rowsp}(V^{(i)})$ and the set of pairs $(\mathbf{v}, \mathbf{v}\mathbf{x}^T)$ by $\mathcal{L}^{(i)} := \{(\mathbf{v}, \mathbf{v}\mathbf{x}^T) \mid \mathbf{v} \in \mathcal{X}^{(i)}\}$ for each i. The side information of R_i is $(\mathcal{X}^{(i)}, \mathcal{L}^{(i)})$. Similarly, the sender has the pair $(\mathcal{X}^{(S)}, \mathcal{L}^{(S)})$ for matrix

$$V^{(S)} \in \mathbb{F}_q^{d_S \times n} \text{ and vector } \Lambda^{(S)} = V^{(S)}\mathbf{x}^T \in \mathbb{F}_q^{d_S}$$

and does not necessarily possess the vector $\mathbf{x}$ itself.

The user R_i requests a coded packet $\mathbf{r}_i\mathbf{x}^T$ with $\mathbf{r}_i \in \mathcal{X}^{(S)} \backslash \mathcal{X}^{(i)}$. We denote by R the $m \times n$ matrix over $\mathbb{F}_q$ with each ith row equal to $\mathbf{r}_i$. R represents the requests of all m users. We denote by

$$\mathcal{X} := \{A \in \mathbb{F}_q^{m \times n} : A_i \in \mathcal{X}^{(i)}, i \in [m]\},$$

so that $\mathcal{X} = \oplus_{i \in [m]} \mathcal{X}^{(i)}$ is the direct sum of the $\mathcal{X}^{(i)}$ as a vector space over $\mathbb{F}_q$. Similarly, we write $\tilde{\mathcal{X}} := \oplus_{i \in [m]} \mathcal{X}^{(S)} = \{Z \in \mathbb{F}_q^{m \times n} : Z_i \in \mathcal{X}^{(S)}\}$.

Definition 6.1.1. *An instance of an Index Coding with Coded Side Information (ICCSI) problem is a list $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ for some positive integers m, n, matrix $R \in \tilde{\mathcal{X}}$, $\mathcal{X}^{(S)}$ a d_S-dimensional subspace of $\mathbb{F}_q^n$ and $\mathcal{X} = \oplus_{i \in [m]} \mathcal{X}^{(i)}$ for d_i-dimensional subspaces $\mathcal{X}^{(i)} < \mathbb{F}_q^n$.*

Definition 6.1.2. *Let $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ be an instance of an ICCSI problem and let N be a positive integer. We say that the map*

$$E : \mathbb{F}_q^n \to \mathbb{F}_q^N,$$

is a code for $\mathcal{I}$ of length N if for each receiver R_i there exists a decoding map

$$D_i : \mathbb{F}_q^N \times \mathcal{X}^{(i)} \to \mathbb{F}_q,$$

satisfying

$$\forall \mathbf{x} \in \mathbb{F}_q^n \ : \ D_i(E(\mathbf{x}), \mathbf{v}) = \mathbf{r}_i\mathbf{x}^T,$$

for some vector $\mathbf{v} \in \mathcal{X}^{(i)}$. *$E$ is called a linear code for $\mathcal{I}$ if* $E(\mathbf{x}) = LV^{(S)}\mathbf{x}^T$ *for some* $L \in \mathbb{F}_q^{N \times d_S}$, *in which case we say that L represents the code E.*

Lemma 6.1.3. *Let* $L \in \mathbb{F}_q^{N \times d_S}$. *Then L represents a linear index code of length N over $\mathbb{F}_q$ for the instance* $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ *if and only if for each* $i \in [m]$,

$$\mathbf{r}_i \in \text{rowsp}\left(\begin{bmatrix} V^{(i)} \\ LV^{(S)} \end{bmatrix}\right).$$

Proof. Let $i \in [m]$ and let $\mathbf{r}_i \in \mathcal{X}^{(S)}$. Suppose that $\mathbf{y} = LV^{(S)}\mathbf{x}^T$ has been transmitted. If

$$\mathbf{r}_i \in \text{rowsp}\left(\begin{bmatrix} V^{(i)} \\ LV^{(S)} \end{bmatrix}\right),$$

then there exist $\mathbf{a} \in \mathbb{F}_q^{d_i}, \mathbf{b} \in \mathbb{F}_q^N$ such that $\mathbf{r}_i = \mathbf{a}V^{(i)} + \mathbf{b}LV^{(S)}$. Then for any $\mathbf{x} \in \mathbb{F}_q^n$ we have

$$\mathbf{r}_i\mathbf{x} = \mathbf{a}V^{(i)}\mathbf{x}^T + \mathbf{b}LV^{(S)}\mathbf{x}^T = \mathbf{a}\Lambda^{(i)} + \mathbf{b}\mathbf{y}.$$

Therefore, receiver R_i acquires $\mathbf{r}_i\mathbf{x}^T$.

Conversely, suppose that $\mathbf{r}_i$ is not contained in the row space of the matrix $\begin{bmatrix} V^{(i)} \\ LV^{(S)} \end{bmatrix}$ for some $i \in [m]$. Then for each $u \in \mathbb{F}_q$, we have

$$\begin{aligned} \text{rank}\left(\begin{bmatrix} \mathbf{r}_i & u \\ V^{(i)} & \Lambda^{(i)} \\ LV^{(S)} & \mathbf{y} \end{bmatrix}\right) &= 1 + \text{rank}\left(\begin{bmatrix} V^{(i)} & \Lambda^{(i)} \\ LV^{(S)} & \mathbf{y} \end{bmatrix}\right) \\ &= 1 + \text{rank}\left(\begin{bmatrix} V^{(i)} \\ LV^{(S)} \end{bmatrix}\right) = \text{rank}\left(\begin{bmatrix} \mathbf{r}_i \\ V^{(i)} \\ LV^{(S)} \end{bmatrix}\right). \end{aligned}$$

In particular, the linear system

$$\mathbf{r}_i\mathbf{x}^T = u, V^{(i)}\mathbf{x}^T = \Lambda^{(i)}, LV^{(S)}\mathbf{x}^T = \mathbf{y}$$

is consistent for each $u \in \mathbb{F}_q$. It follows that

$$Pr(\mathbf{r}_i\mathbf{x}^T = u | V^{(i)}\mathbf{x}^T = \Lambda^{(i)}, LV^{(S)}\mathbf{x} = \mathbf{y}) = \frac{1}{q}, \tag{6.1}$$

so in particular the side information of R_i conveys no information about $\mathbf{r}_i\mathbf{x}^T$ to R_i. □

We remark that the sufficiency of the statement of Lemma 6.1.3 has already been noted in [SDS12].

Given an instance $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ over $\mathbb{F}_q$, for each $i \in [m]$ we define the sets

$$\mathcal{Y}^{(i)} := \mathcal{X}^{(i)^\perp} \text{ and } \mathcal{Z}^{(i)} := \mathcal{X}^{(i)^\perp} \backslash \mathbf{r}_i{}^\perp,$$

where $\mathbf{r}_i^\perp$ is the vector space of the vectors orthogonal to $\mathbf{r}_i$.

Corollary 6.1.4. *Let $L \in \mathbb{F}_q^{N \times d_S}$. Then L represents a linear index code of length N over $\mathbb{F}_q$ for the instance $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ if and only if $\operatorname{rank}(LV^{(S)}\mathbf{z}^T) \geq 1$ for each $i \in [m]$, and $\mathbf{z} \in \mathcal{Z}^{(i)}$.*

Proof. Let $\mathbf{z}_0 \in \mathcal{Z}^i$, let $LV^{(S)}\mathbf{z}_0^T = \mathbf{w}$ and let $w \in \mathbb{F}_q$. Suppose that $\mathbf{r}_i$ is not contained in the row space of the matrix $\begin{bmatrix} V^{(i)} \\ LV^{(S)} \end{bmatrix}$. Then as in the proof of Lemma 6.1.3, the linear system

$$\mathbf{r}_i\mathbf{z}^T = w, V^{(i)}\mathbf{z}^T = 0, LV^{(S)}\mathbf{z}^T = \mathbf{w} \tag{6.2}$$

is consistent for every choice of w. In particular (6.2) has a solution $\mathbf{z}_1$ for $w = 0$, in which case $\mathbf{z}_1 \in \mathbf{r}_i^\perp \cap \mathcal{Y}^{(i)} = \mathcal{Y}^{(i)} \backslash \mathcal{Z}^{(i)}$. Then $\mathbf{z} = \mathbf{z}_0 - \mathbf{z}_1 \in \mathcal{Z}^{(i)}$ and $LV^{(S)}\mathbf{z} = 0$. It follows that if $\operatorname{rank}(LV^{(S)}\mathbf{z}^T) \geq 1$ then for each $i \in [m]$, and $\mathbf{z} \in \mathcal{Z}^{(i)}$ then L is a linear index code for the instance $\mathcal{I}$. Conversely, if there exist $\mathbf{a} \in \mathbb{F}_q^{d_i}, \mathbf{b} \in \mathbb{F}_q^N$ such that $\mathbf{r}_i = \mathbf{a}V^{(i)} + \mathbf{b}LV^{(S)}$ then

$$\mathbf{r}_i\mathbf{z}^T = \mathbf{a}V^{(i)}\mathbf{z}^T + \mathbf{b}LV^{(S)}\mathbf{z}^T = \mathbf{b}LV^{(S)}\mathbf{z}^T \neq 0,$$

so that $\operatorname{rank}(LV^{(S)}\mathbf{z}^T) \geq 1$ for any $\mathbf{z} \in \mathcal{Z}^{(i)}$. □

We extend now the definition of min-rank of an instance of the ICSI problem to the ICCSI problem.

Definition 6.1.5. *We define the min-rank of an instance $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ of the ICCSI problem over $\mathbb{F}_q$ to be*

$$\kappa_q(\mathcal{I}) \;=\; \min\{\operatorname{rank}_q(A + R) : A \in \mathbb{F}_q^{m \times n}, A_i \in \mathcal{X}^{(i)} \cap \mathcal{X}^{(S)} < \mathbb{F}_q^n,\ \forall i \in [m]\}.$$

Similar to Corollary 4.2.8, the minimum length of an instance $\mathcal{I}$ of the ICCSI problem over $\mathbb{F}_q$ is given by its min-rank.

Corollary 6.1.6. *The length of an optimal linear code for an instance $\mathcal{I}$ of the ICCSI problem $\mathbb{F}_q$ is $\kappa_q(\mathcal{I})$.*

Proof. Let $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ be an instance of the ICCSI problem $\mathbb{F}_q$. Let $A \in \mathbb{F}_q^{m \times n}$ with $A_i \in \mathcal{X}^{(i)} \cap \mathcal{X}^{(S)}$ for each $i \in [m]$. Suppose that $A + R$ has rank N. Since $A, R \in \tilde{\mathcal{X}}$, there exists $Z \in \mathbb{F}_q^{m \times d_S}$ of rank N satisfying $A + R = ZV^{(S)}$. Furthermore, there exist $B \in \mathbb{F}_q^{m \times N}$ and $L \in \mathbb{F}_q^{N \times d_S}$ such that $Z = BL$. Then $R = A - BLV^{(S)}$ so from Lemma 6.1.3 L represents a linear code of length N for the instance $\mathcal{I}$. The optimal length N is achieved for $N = \kappa_q(\mathcal{I})$. □

The reader will observe of course that the classical ICSI problem is indeed a special case of the index coding problem with coded side information. Setting $V^{(S)}$ to be the $n \times n$ identity matrix, $\mathbf{r}_i = \mathbf{e}_{f(i)}$ and $V^{(i)}$ to be the $d_i \times n$ matrix with rows $V^{(i)}_j = \mathbf{e}_{i_j}$ for each $i_j \in \mathcal{X}_i$ yields $\mathcal{X}^{(i)} = \text{Span}\{\mathbf{e}_j : j \in \mathcal{X}_i\}$, so that $\text{Supp}(v) \subset \mathcal{X}_i$ if and only if $v \in \mathcal{X}^{(i)}$.

6.2 Error correction in the ICCSI problem

Definition 6.2.1. *Let $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ be an instance of an ICCSI problem and let N be a positive integer. We say that the map*

$$E : \mathbb{F}_q^n \to \mathbb{F}_q^N,$$

is a δ-error correcting code for $\mathcal{I}$ of length N, and write $(\mathcal{I}, \delta)$-ECIC, if for each i-th receiver there exists a decoding map

$$D_i : \mathbb{F}_q^N \times \mathcal{X}^{(i)} \to \mathbb{F}_q,$$

satisfying

$$D_i(E(\mathbf{x}) + \mathbf{w}, \mathbf{v}) = \mathbf{r}_i \mathbf{x}^T$$

for all $\mathbf{x} \in \mathbb{F}_q^n$ and $\mathbf{w} \in \mathbb{F}_q^N$, $w(\mathbf{w}) \leq \delta$ for some vector $\mathbf{v} \in \mathcal{X}^{(i)}$. E is called a linear code for $\mathcal{I}$ if $E(\mathbf{x}) = LV^{(S)}\mathbf{x}^T$ for some $L \in \mathbb{F}_q^{N \times d_S}$, in which case we say that L represents the linear $(\mathcal{I}, \delta)$-ECIC E.

Theorem 6.2.2. *Let $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ be an instance of an ICCSI problem and let N be a positive integer. A matrix $L \in \mathbb{F}_q^{N \times d_S}$ represents a linear $(\mathcal{I}, \delta)$-ECIC if and only if for all $i \in [m]$ we have*

$$w\left(LV^{(S)}\mathbf{z}^T\right) \geq 2\delta + 1,$$

for all $\mathbf{z} \in \mathcal{Z}^{(i)}$.

Proof. For each $\mathbf{x} \in \mathbb{F}_q^n$, define

$$B(\mathbf{x}, \delta) = \{\mathbf{y} \,:\, \mathbf{y} = LV^{(S)}\mathbf{x}^T + \mathbf{w},\, \mathbf{w} \in \mathbb{F}_q^N,\, w(\mathbf{w}) \leq \delta\}.$$

Then the receiver R_i can correct δ errors if and only if

$$B(\mathbf{x}, \delta) \cap B(\mathbf{x}', \delta) = \emptyset$$

for each $\mathbf{x}, \mathbf{x}' \in \mathbb{F}_q^n$ such that $V^{(i)}\mathbf{x}^T = V^{(i)}\mathbf{x}'^T$ and $\mathbf{r}_i\mathbf{x}^T \neq \mathbf{r}_i\mathbf{x}'^T$

This is equivalent to

$$LV^{(S)}\mathbf{x}^T + \mathbf{w} \neq L\mathbf{x}'^T + \mathbf{w}', \tag{6.3}$$

for all $\mathbf{w}, \mathbf{w}' \in \mathbb{F}_q^N$ with $w(\mathbf{w}) \leq \delta$ and $w(\mathbf{w}') \leq \delta$.

It is easy to check that

$$\{\mathbf{w} - \mathbf{w}' \,|\, \mathbf{w}, \mathbf{w}' \in \mathbb{F}_q^N, w(\mathbf{w}) \leq \delta, w(\mathbf{w}') \leq \delta\} = \{\mathbf{w} \,|\, \mathbf{w} \in \mathbb{F}_q^N, w(\mathbf{w}) \leq 2\delta\},$$

so letting $\mathbf{z} = \mathbf{x} - \mathbf{x}'$, we see then (6.3) is equivalent to

$$LV^{(S)}\mathbf{z}^T \neq \mathbf{w}$$

for all $\mathbf{z}, \mathbf{w}$ satisfying $\mathbf{r}_i\mathbf{z}^T \neq 0, V^{(i)}\mathbf{z}^T = 0$ and $w(\mathbf{w}) \leq 2\delta$.

In particular, R_i corrects δ errors if and only if

$$w(LV^{(S)}\mathbf{z}^T) \geq 2\delta + 1$$

for all $\mathbf{z} \in {V^{(i)}}^{\perp} \setminus \mathbf{r}_i^{\perp}$. □

Clearly any $(\mathcal{I}, \delta)$-ECIC detects up to 2δ errors.

6.2.1 α-bound, κ-bound and Singleton bound

In the case of the ICCSI problem we obtain the same α-bound, κ-bound and Singleton bound given in Section 4.2.5. We first fix some further notation.

Define:

$$\mathcal{S}(\mathcal{I}) = \bigcup_{i \in [m]} \mathcal{Z}^{(i)} \subset \mathbb{F}_q^n$$

and

$$\mathcal{J}(\mathcal{I}) = \{U < \mathbb{F}_q^n \mid U \backslash \{0\} \subset \mathcal{S}(\mathcal{I})\}.$$

The maximum dimension of any subspace contained in $\mathcal{J}(\mathcal{I})$ is denoted by $\alpha(\mathcal{I})$.

We denote by $\mathcal{N}_q(\mathcal{I}, \delta)$ the optimal length N of an $(\mathcal{I}, \delta)$-ECIC and by $N_q(k, d)$ the optimal length ℓ of a k-dimensional $\mathbb{F}_q$-linear code in $\mathbb{F}_q^\ell$ of minimum distance d. We have the following results.

Proposition 6.2.3. *(α-bound)*

$$N_q(\alpha(\mathcal{I}), 2\delta + 1) \leq \mathcal{N}_q(\mathcal{I}, \delta).$$

Proof. Let $L \in \mathbb{F}_q^{N\times d_s}$ represent a linear $(\mathcal{I},\delta)$-ECIC. Let $U \in \mathcal{J}(\mathcal{I})$ have dimension k and let G be a rank k matrix in $\mathbb{F}_q^{n\times k}$ such that $U = \{G\mathbf{z}^T : \mathbf{z} \in \mathbb{F}_q^k\}$. Let $C_U = \{LV^{(S)}G\mathbf{z}^T : \mathbf{z} \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^N$. Then for all non-zero $\mathbf{z} \in \mathbb{F}_q^k$ we have $G\mathbf{z}^T \in \mathcal{Z}^{(i)}$ for some $i \in [m]$, and so $w(LV^{(S)}G\mathbf{z}^T) \geq 2\delta + 1$ for all non-zero $\mathbf{z}^T \in \mathbb{F}_q^k$. This furthermore implies that LV^SG has rank k over $\mathbb{F}_q$. It follows that C_U is an $\mathbb{F}_q$-$[N, k, 2\delta + 1]$ code with $N \geq N(k, 2\delta + 1)$. Choosing U of maximal dimension in $\mathcal{J}(\mathcal{I})$ for an $\mathcal{I}(\delta) - ECIC$ of optimal length we see that $N(\alpha(\mathcal{I}), 2\delta + 1) \leq \mathcal{N}(\mathcal{I}, \delta)$. □

Setting $\delta = 0$ in the above give the following as an immediate consequence.

Corollary 6.2.4.

$$\alpha(\mathcal{I}) \leq \kappa_q(\mathcal{I}).$$

Proposition 6.2.5. *(κ-bound)*

$$\mathcal{N}_q(\mathcal{I}, \delta) \leq N_q(\kappa_q(\mathcal{I}), 2\delta + 1).$$

Proof. Let $L \in \mathbb{F}_q^{N\times d_S}$ be an encoding matrix for an optimal linear index code of length $N = \kappa_g(\mathcal{I})$ for $\mathcal{I}$. Let $\phi : \mathbb{F}_q^N \longrightarrow \mathbb{F}_q^{N'}$ be an $\mathbb{F}_q$-monomorphism such that $C = \phi(\mathbb{F}_q^N)$ is an $[N', N, 2\delta + 1]$ linear code over $\mathbb{F}_q$ with $N' = N_q(N, 2\delta + 1)$. Then $LV^{(S)}\mathbf{z}^T$ is non-zero for all $\mathbf{z} \in \mathcal{Z}^{(i)}, i \in [m]$ and so $w(\phi(LV^{(S)}\mathbf{z}^T)) \geq 2\delta+1$ for all such $\mathbf{z}$. Then C is a linear $(\mathcal{I}, \delta)$-ECIC of length $N' = N_q(\kappa_q(\mathcal{I}), 2\delta + 1) \geq \mathcal{N}_q(\mathcal{I}, \delta)$. □

Recall from the Singleton bound we have $k + 2\delta \leq N$ for any $\mathbb{F}_q - [N, k, 2\delta + 1]$ code. In particular, $k + 2\delta \leq N_q(k, 2\delta + 1)$.

Proposition 6.2.6. *(Singleton bound for Index Codes)*

$$\mathcal{N}_q(\mathcal{I}, \delta) \geq \kappa_q(\mathcal{I}) + 2\delta.$$

Proof. Let $L \in \mathbb{F}_q^{N\times d_S}$ be a matrix for a linear with $(\mathcal{I}, \delta)$-ECIC. Suppose that $N = \mathcal{N}_q(\mathcal{I}, \delta)$. Let L' the matrix obtained by deleting any 2δ rows of L. By Theorem 6.2.2, $w\left(LV^{(S)}\mathbf{z}^T\right) \geq 2\delta + 1$ for all $i \in [m]$ and for all $\mathbf{z} \in \mathcal{Z}^{(i)}$, so that $w\left(L'V^{(S)}\mathbf{z}^T\right) \geq 1$, for all such $\mathbf{z}$. So L' is a linear index code of length $N - 2\delta$ for the instance $\mathcal{I}$. Now L' has at least $\kappa_q(\mathcal{I})$ rows so that $\kappa_q(\mathcal{I}) \leq \mathcal{N}_q(\mathcal{I}, \delta) - 2\delta$. □

In the case that there exists an $\mathbb{F}_q$-linear $[N, \kappa_q(\mathcal{I}), 2\delta + 1]$ code that is MDS we get $N_q(\kappa_q(\mathcal{I}), 2\delta + 1) = \kappa_q(\mathcal{I}) + 2\delta$.

Reed-Solomon codes are examples of MDS codes. In fact any extended generalized Reed-Solomon code over $\mathbb{F}_q$ is an MDS code of length $q + 1$ [HP03, Theorem 5.3.4]

so the existence of such codes is assured for such lengths. It is conjectured that any $\mathbb{F}_q - [N, k, d]$ MDS code satisfies $N \leq q + 1$ unless q is even and $k = 3$ or $k = q - 1$ (in which case $N \leq q + 2$) [HP03].

Corollary 6.2.7. *Suppose that $q \geq \kappa_q(\mathcal{I}) + 2\delta - 1$. Then*

$$\mathcal{N}_q(\mathcal{I}, \delta) = \kappa_q(\mathcal{I}) + 2\delta.$$

Proof. If $q \geq \kappa_q(\mathcal{I}) + 2\delta - 1$ then there exists an $\mathbb{F}_q$-linear $[q + 1, \kappa_q(\mathcal{I}), 2\delta + 1]$ MDS code, namely an extended Reed-Solomon code. So, we obtain

$$\kappa_q(\mathcal{I}) + 2\delta \leq \mathcal{N}_q(\mathcal{I}, \delta) \leq N_q(k_q(\mathcal{I}), 2\delta + 1) = \kappa_q(\mathcal{I}) + 2\delta.$$

□

6.3 Random index coding

In this section we extend the random construction to the ICCSI problem case.

A proof of the following Lemma can be found in [HKM$^+$03, Lemma 1]

Lemma 6.3.1. *Let a, b be positive integers and let P be a polynomial over $\mathbb{F}_q$ of degree less than or equal to ab, in which the largest exponent of any variable is at most a. The probability that P equals zero is at most $1 - (1 - a/q)^b$ for $q > a$.*

Remark 6.3.2. Before proving the following theorem, we note that if $X_1, \ldots, X_n$ are independent uniformly distributed random variables that take their values over a field $\mathbb{F}_q$, then the random variable

$$Z_\ell = \sum_{i=1}^{\ell} \alpha_i X_i,$$

for some $\ell \in [n]$, $\alpha_i \in \mathbb{F}_q^\times$, has a uniform distribution.

This is easily shown by an inductive argument. Clearly $P(Z_1 = \beta) = \frac{1}{q}$ for any $\beta \in \mathbb{F}_q$ since $\alpha_1 \neq 0$. Moreover, for any $\ell \in [n], \beta \in \mathbb{F}_q$,

$$\begin{aligned} P(Z_\ell = \beta) &= P(Z_{\ell-1} = \beta - \alpha_\ell X_\ell) \\ &= \sum_{\gamma \in \mathbb{F}_q} P(X_\ell = \gamma) P(Z_{\ell-1} = \beta - \alpha_\ell \gamma) = \frac{1}{q}. \end{aligned}$$

Theorem 6.3.3. *Let $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ be an instance of an ICCSI problem and let $k = \max\{n - d_i : i \in [m]\}$. If the entries of a matrix $L \in \mathbb{F}_q^{N \times d_S}$ are chosen uniformly at random in $\mathbb{F}_q$, then the probability that L represents a linear code for $\mathcal{I}$ is at least $(1 - m/q)^k$, for $q > m$.*

Proof. From Theorem 6.2.2, if $w\left(LV^{(S)}\mathbf{z}^T\right) \geq 1$ for each $\mathbf{z} \in \mathcal{Y}^{(i)}$ then L represents a code for $\mathcal{I}$. For each $i \in [m]$, let $Z^{(i)} \in \mathbb{F}_q^{n\times k_i}$ satisfy $V^{(i)}Z^{(i)} = 0$ and have rank $k_i = n - d_i$. Write $L^{(i)} = LV^{(S)}Z^{(i)}$. The matrix L represents a code for $\mathcal{I}$ if $L^{(i)}$ is a full-rank matrix for each $i \in [m]$, which holds if and only if there exists a non-zero $k_i \times k_i$ minor $M^{(i)}$ of $L^{(i)}$. Since the entries of L are uniformly distributed, so are the entries of $L^{(i)}$, from Remark 6.3.2. Now $\prod_{i\in[m]} M^{(i)}$ may be viewed as a polynomial in Nd_S variables of degree $\sum_{i\in[m]} k_i \leq mk$ with each variable appearing with multiplicity at most m in any term. Then the probability that L represents a code for $\mathcal{I}$ is the probability that $\prod_{i\in[m]} M^{(i)}$ is non-zero, which from Lemma 6.3.1 is at least $(1 - m/q)^N$, for $q > m$. □

As consequence we obtain immediately the following bound on the min-rank of an instance of the ICCSI problem.

Corollary 6.3.4. *Let $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ be an instance of the ICCSI problem. The min-rank of the instance $\mathcal{I}$, over a finite field $\mathbb{F}_q$ with $q > m$, satisfies*

$$\kappa_q(\mathcal{I}) \leq N = \max_{i\in[m]} \dim(\mathcal{Y}^{(i)}).$$

Remark 6.3.5. The corollary above implies the bound on the min-rank of a graph given in Proposition 5.2.3.

We now give a result on the existence of a linear encoding of length N for $(\mathcal{I}, \delta)$, extending Theorem 4.2.25. Recall that $V_q(N, s)$ denote the size of the set $\{\mathbf{x} \in \mathbb{F}_q^N : w(\mathbf{x}) \leq s\}$.

Theorem 6.3.6. *Let $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ be an $\mathbb{F}_q$-linear index code and let $L \in \mathbb{F}_q^{N\times d_S}$ for some positive integer N. The probability that L corresponds to an $(\mathcal{I}, \delta)$ is at least*

$$1 - \frac{\sum_{i\in[m]} q^{(n-d_i-1)}V_q(N, 2\delta)}{q^N}.$$

In particular, there exists such a matrix L if

$$\sum_{i\in[m]} q^{(n-d_i-1)} < \frac{q^N}{V_q(N, 2\delta)}.$$

Proof. From Theorem 6.2.2, a matrix $L \in \mathbb{F}_q^{N\times d_S}$ corresponds to an $(\mathcal{I}, \delta)$ if and only if for each $i \in [m]$, $w(LV^{(S)}\mathbf{z}^T) \geq 2\delta + 1$ for any $\mathbf{z} \in \mathcal{Z}^{(i)}$. Now $\mathcal{Y}^{(i)} = \mathcal{Y}^{(i)} \cap \mathbf{r}_i^\perp \oplus \mathcal{B}$ for some 1-dimensional subspace $\mathcal{B} = \mathrm{Span}\{\mathbf{b}\}$, with $\mathbf{b} \in \mathbb{F}_q^n \backslash \mathbf{r}_i^\perp$. Then any $\mathbf{z} \in \mathcal{Z}^{(i)}$ has the form $\mathbf{z} = \alpha\mathbf{b} + \mathbf{w}$ for some $\mathbf{w} \in \mathcal{Y}^{(i)} \cap \mathbf{r}_i^\perp$ and α non zero, so that $w(LV^{(S)}\mathbf{z}) = d(LV^{(S)}\mathbf{b}^T, \alpha^{-1}LV^{(S)}\mathbf{w}^T)$.

Let $\Phi_L : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^N : \mathbf{x} \mapsto LV^{(S)}\mathbf{x}^T$ and let ${}_{\mathbf{b}}\Phi : \mathbb{F}_q^{N\times d_S} \longrightarrow \mathbb{F}_q^N : X \mapsto XV^{(S)}\mathbf{b}^T$. If $d(LV^{(S)}\mathbf{b}^T, \mathbf{w}) \geq 2\delta + 1$ for all $\mathbf{w} \in \Phi_L(\mathcal{Y}^{(i)} \cap \mathbf{r}_i^{\perp})$, then $w(LV^{(S)}\mathbf{z}^T) \geq 2\delta + 1$ for all $\mathbf{z} \in \mathcal{Z}^{(i)}$. Since $\Phi_L(\mathcal{Y}^{(i)} \cap \mathbf{r}_i^{\perp})$ is an $\mathbb{F}_q$-space of dimension at most $(n - d_i - 1)$, there are at most $q^{(n-d_i-1)}V_q(N, 2\delta)$ vectors $LV^{(S)}\mathbf{b}^T \in \mathrm{Im}({}_{\mathbf{b}}\Phi) \subset \mathbb{F}_q^N$ within distance 2δ of $\Phi_L(\mathcal{Y}^{(i)} \cap \mathbf{r}_i^{\perp})$. Thus the probability that there exists some $\mathbf{z} \in \mathcal{Z}^{(i)} \subset \mathbb{F}_q^n$ such that $w(L\mathbf{z}^T) \leq 2\delta$ is upper bounded by

$$\frac{q^{(n-d_i-1)}V_q(N, 2\delta)}{|\mathrm{Im}({}_{\mathbf{b}}\Phi)|} = \frac{q^{(n-d_i-1)}V_q(N, 2\delta)}{q^N}$$

The result now follows from the union bound.

□

Theorem 4.2.25 is extended by the following corollary, from Lemma 4.1.4.

Corollary 6.3.7. *Let $\mathcal{I} = (m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ be an instance of the ICCSI problem. Let q be any prime power and let λ be any rational number such that $0 < \lambda < 1 - 1/q$. Let N be any integer such that $N - H_q(\lambda)N > \log_q\left(\sum_{i=1}^m q^{k_i-1}\right)$, where $k_i = \dim(\mathcal{Y}^{(i)})$ for $i \in [m]$, and λN is an integer. Then choosing the entries of $L \in \mathbb{F}_q^{N\times n}$ uniformly at random over the field $\mathbb{F}_q$, the probability that L corresponds to a $(\mathcal{I}', \delta)$-ECIC, with $\delta = \left\lfloor \frac{\lambda N}{2} \right\rfloor$, is at least*

$$1 - \sum_{i=1}^{m} \frac{q^{k_i-1}}{q^{N(1-H_q(\lambda))}}.$$

Remark 6.3.8. Corollary 6.3.7 implies a sufficient condition for the existence of a $(\mathcal{I}, \delta)$-ECIC, that is

$$N - H_q\left(\frac{2\delta}{N}\right) > \log_q\left(m \cdot q^M\right) > \log_q\left(\sum_{i=1}^{m} q^{k_i-1}\right), \; M = \max_{i\in[m]} \dim(\mathcal{Y}^{(i)}) - 1.$$

6.4 Decoding Schemes

6.4.1 Syndrome decoding revisited

In this section we take into account the classical case of ICSI problem where $V^{(S)}$ is the identity matrix and R_i requests an uncoded packet.

In the algorithm given in Chapter 4.2, each time that we decode, we have to solve the system (4.6). Here we report a possible modification of that procedure to avoid this step. Let $L \in \mathbb{F}_q^{N\times n}$ be a matrix corresponding to a $(\mathcal{I}, \delta)$-ECIC, and suppose that a receiver R_i, $i \in [m]$, receives the message

$$\mathbf{y}_i = L\mathbf{x}^T + \varepsilon_i,$$

where $L\mathbf{x}^T$ is the codeword transmitted by S and ε_i is the error.

Now consider the two codes

$$\mathcal{C}^{(i)} = \mathrm{Span}_q(\{L^{f(i)}\} \cup \{L^j\}_{j\in\mathcal{Y}_i})$$

and

$$\mathcal{C}_{(i)} = \mathrm{Span}_q(\{L^j\}_{j\in\mathcal{Y}_i}).$$

Remark 6.4.1. For each receiver R_i, $i \in [m]$, we have $\mathcal{C}_{(i)} \subseteq \mathcal{C}^{(i)}$ with $\dim(\mathcal{C}^{(i)}) = \dim(\mathcal{C}_{(i)}) + 1$. And ${\mathcal{C}^{(i)}}^{\perp} \subseteq {\mathcal{C}_{(i)}}^{\perp}$ with $\dim({\mathcal{C}_{(i)}}^{\perp}) = \dim({\mathcal{C}^{(i)}}^{\perp}) + 1$. Then we can consider $H_{(i)}$ a parity check matrix of $\mathcal{C}_{(i)}$ of the form

$$H_{(i)} = \left[\frac{h_{(i)}}{H^{(i)}}\right]. \tag{6.4}$$

Where $H^{(i)}$is a parity check matrix of $\mathcal{C}^{(i)}$ and $h_{(i)} \in {\mathcal{C}_{(i)}}^{\perp} \setminus {\mathcal{C}^{(i)}}^{\perp}$.

Moreover

$$H_{(i)}L^{f(i)} = (s_{f(i)}, 0, \ldots, 0)^T$$

where $s_{f(i)} \in \mathbb{F}_q \setminus \{0\}$.

We now describe the decoding procedure.

Step 1: Compute

$$H_{(i)}(\mathbf{y}_i - L^{\mathcal{X}_i}\mathbf{x}_{\mathcal{X}_i}^T) = (\alpha_i, \beta_i) \tag{6.5}$$

where $x_{f(i)}s_{f(i)} + h_{(i)} \cdot \varepsilon_i = \alpha_i$ and $\beta_i = H^{(i)}\varepsilon_i$.

Step 2: Find $\bar{\varepsilon}$ with $w(\bar{\varepsilon}) \leq \delta$ such that

$$H^{(i)}\bar{\varepsilon} = \beta_i. \tag{6.6}$$

Step 3: Compute

$$\hat{x}_{f(i)} = (\alpha_i - h_{(i)} \cdot \bar{\varepsilon})/s_{f(i)}. \tag{6.7}$$

Theorem 6.4.2. *If $w(\varepsilon_i) \leq \delta$. Then the procedure above has output $x_{f(i)}$.*

Proof. We have

$$H^{(i)}\varepsilon_i = H^{(i)}\bar{\varepsilon} = \beta_i.$$

Then $\varepsilon_i - \bar{\varepsilon} \in \mathcal{C}^{(i)}$ and $w(\varepsilon_i - \bar{\varepsilon}) \leq 2\delta$, that means $\varepsilon_i - \bar{\varepsilon} \in \mathcal{C}_{(i)}$.

So

$$(\alpha_i - h_{(i)}\bar{\varepsilon})/s_{f(i)} = (x_{f(i)}s_{f(i)} + \underbrace{h_{(i)}(\varepsilon_i - \bar{\varepsilon})}_{\mathbf{0}})/s_{f(i)} = x_{f(i)}.$$

□

Example 6.4.3. Let $q = 2$, $m = n = 5$, and $f(i) = i$ for each $i \in [5]$. Assume

$$\mathcal{X}_1 = \{2, 5\}, \mathcal{X}_2 = \{1, 3\}, \mathcal{X}_3 = \{2, 4\}, \mathcal{X}_4 = \{3, 5\}, \mathcal{X}_5 = \{1, 4\}.$$

Suppose that for this instance of the ICSI problem is used the matrix

$$L = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

That is a $(\mathcal{I}, 1)$-ECIC.

Let $\mathbf{x} = (1, 1, 1, 1, 1)$, and $L\mathbf{x}^T = (1, 0, 0, 1, 0, 0, 0)$.

Suppose now that R_1 receives

$$\mathbf{y}_1^T = (1, 0, 0, 1, 0, 1, 0).$$

Then $\varepsilon_1 = (0, 0, 0, 0, 0, 1, 0)$.

A parity check matrix of $C_{(1)} = Span\{L^3, L^4\}$ of the form (6.4) is

$$H_{(1)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

We have

$$\mathbf{y}_1 - L^{\mathcal{X}_1}\mathbf{x}_{\mathcal{X}_1}^T = (0, 1, 1, 1, 0, 0, 0),$$

and

$$H_{(1)}(\mathbf{y}_1 - L^{\mathcal{X}_1}\mathbf{x}_{\mathcal{X}_1}^T) = (1, 1, 0, 0, 0).$$

So $\alpha_1 = 1$, and $\beta_1 = (1,0,0,0)$. We obtain $\bar{\varepsilon} = (1,0,0,0,0,0,0)$, from Step 2.

Now we compute $\hat{x}_1 = (\alpha_1 - h_{(1)} \cdot \bar{\varepsilon})/s_1 = (1-0)/1 = 1 = x_1$.

Remark 6.4.4. In our algorithm we have to determine $h_{(i)}$ like in (6.4) solving the system

$$\left[\begin{array}{c|c} L^{f(i)} & L^{\mathcal{Y}_i} \end{array}\right]^T h_{(i)}^T = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

We can use the Gaussian elimination to solve the system.

6.4.2 Syndrome decoding for ICCSI problem

Now we extend the Syndrome decoding to the ICCSI problem.

Let $L \in \mathbb{F}_q^{N \times d_S}$ be a matrix corresponding to a $(\mathcal{I}, \delta)$-ECIC, and suppose that a receiver R_i, $i \in [m]$, receives the message

$$\mathbf{y}_i = LV^{(S)}\mathbf{x}^T + \varepsilon_i,$$

where $LV^{(S)}\mathbf{x}^T$ is the codeword transmitted by S and ε_i is the error.

Let $\mathbf{v}_1, \ldots, \mathbf{v}_{d_i}$ be a basis of $\mathcal{X}^{(i)}$ and $\mathbf{r}_i\mathbf{x}^T$ be the requested coded packet. Let $M_{(i)} \in \mathbb{F}_q^{n \times n}$ be an invertible matrix such that

$$\mathbf{v}_j M_{(i)} = \mathbf{e}_j \text{ for } 1 \leq j \leq d_i, \text{ and } \mathbf{r}_i M_{(i)} = \mathbf{e}_{f(i)}$$

for some $f(i) \notin [d_i]$. Defining $\mathbf{x}'^T = M_{(i)}^{-1}\mathbf{x}^T$, we have

$$\mathbf{v}_j\mathbf{x}^T = \mathbf{e}_j M_{(i)}^{-1}\mathbf{x}^T = \mathbf{x}'_j \text{ for } 1 \leq j \leq d_i$$

and

$$\mathbf{r}_i\mathbf{x}^T = \mathbf{e}_{f(i)} M_{(i)}^{-1}\mathbf{x}^T = \mathbf{x}'_{f(i)}.$$

Note that R_i already knows $\mathbf{v}_1\mathbf{x}^T, \ldots, \mathbf{v}_{d_i}\mathbf{x}^T$.

Lemma 6.4.5. *Let $E = \mathrm{Span}\{\mathbf{e}_1, \ldots, \mathbf{e}_{d_i}\}$. Then for all $\mathbf{z}' \in E^\perp$ with $\mathbf{z}'_{f(i)} \neq 0$*

$$w(LV^{(S)}M_{(i)}\mathbf{z}'^T) \geq 2\delta + 1.$$

Proof. From Theorem 6.2.2 for all $\mathbf{z} \in \mathcal{Y}^{(i)} \setminus \mathbf{r}_i^\perp$ we have

$$w(LV^{(S)}\mathbf{z}^T) \geq 2\delta + 1.$$

Let $\mathbf{z}' \in E^\perp$ be such that $\mathbf{z}'_{f(i)} \neq 0$, then $\mathbf{e}_j\mathbf{z}'^T = 0$ for $1 \leq j \leq d_i$ and $\mathbf{e}_{f(i)}\mathbf{z}'^T \neq 0$. Being $\mathbf{e}_j = \mathbf{v}_j M_{(i)}$ and $\mathbf{e}_{f(i)} = \mathbf{r}_i M_{(i)}$ we have

$$\mathbf{v}_j M_{(i)}\mathbf{z}'^T = 0 \text{ for } 1 \leq j \leq d_i, \text{ and } \mathbf{r}_i M_{(i)}\mathbf{z}'^T \neq 0,$$

thus $\mathbf{z}'M_{(i)}^T \in \mathcal{Y}^{(i)} \setminus \mathbf{r}_i^\perp$ and the claim follows. □

Define, now, the sets

$$\mathcal{X}'_i = \{1, \dots, , d_i\} \text{ and } \mathcal{Y}'_i = [n] \setminus \mathcal{X}'_i \cup \{f(i)\},$$

and let $L' = LV^{(S)}M_{(i)}$.

As in the previously subsection R_i can construct the parity check matrices $H^{(i)}$ and $H_{(i)}$ of $\mathcal{C}^{(i)} = \text{Span}_q(\{L'^{f(i)}\} \cup \{L'^j\}_{j \in \mathcal{Y}'_i})$ and $\mathcal{C}_{(i)} = \text{Span}_q(\{L'^j\}_{j \in \mathcal{Y}'_i})$, respectively, with

$$H_{(i)} = \left[\frac{h_{(i)}}{H^{(i)}} \right], \tag{6.8}$$

where, as before, $h_{(i)} \in {\mathcal{C}_{(i)}}^{\perp} \setminus {\mathcal{C}^{(i)}}^{\perp}$.

Analogously

$$H_{(i)}L'^{f(i)} = (s_{f(i)}, 0, \dots, 0)^T$$

for some $s_{f(i)} \in \mathbb{F}_q \setminus \{0\}$, and the decoding scheme is

Step 1: Compute

$$H_{(i)}(\mathbf{y}_i - L'^{\mathcal{X}'_i}\mathbf{x}'^T_{\mathcal{X}'_i}) = (\alpha_i, \beta_i) \tag{6.9}$$

where $x'_{f(i)}s_{f(i)} + h_{(i)} \cdot \varepsilon_i = \alpha_i$ and $\beta_i = H^{(i)}\varepsilon_i$.

Step 2: Find $\bar{\varepsilon}$ with $w(\bar{\varepsilon}) \leq \delta$ such that

$$H^{(i)}\bar{\varepsilon} = \beta_i. \tag{6.10}$$

Step 3: Compute

$$\hat{x'}_{f(i)} = (\alpha_i - h_{(i)} \cdot \bar{\varepsilon})/s_{f(i)}. \tag{6.11}$$

Remark 6.4.6. Note that R_i knows the matrix $LV^{(S)}$ and and the vector $\mathbf{x}'_{\mathcal{X}'_i}$ so it is able to perform Step 1.

Theorem 6.4.7. *If $w(\varepsilon_i) \leq \delta$. Then the procedure above has output $x'_{f(i)}$.*

Proof. It follows directly from Lemma 6.4.5 and from

$$\begin{aligned}\mathbf{y}_i =& LV^{(S)}\mathbf{x}^T + \varepsilon_i = LV^{(S)}M_{(i)}M_{(i)}^{-1}\mathbf{x}^T + \varepsilon_i \\ =& L'\mathbf{x}'^T + \varepsilon_i = L'^{\mathcal{X}'_i}\mathbf{x}'^T_{\mathcal{X}'_i} + L'^{\mathcal{Y}'_i}\mathbf{x}'^T_{\mathcal{Y}'_i} + L'^{f(i)}x'_{f(i)} + \varepsilon_i.\end{aligned}$$

□

6.4.3 Decoding Index Codes over Matrix Channels

Error correction for index code in general is non-trivial. In the model presented here, we assume that there is a data matrix $X \in \mathbb{F}_q^{n\times t}$ to transmit, and for each $i \in [m]$, receiver R_i seeks some linear combination of the rows of X. Thus a matrix Y is transmitted and that at any given sink, a matrix of the form $Y + W$ is received. Therefore the decoding algorithm of the additive matrix channel as described in [SKK10] may be considered.

Recall that given an $\mathbb{F}_q$-linear index code $\mathcal{I}(m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ with $N \times d_S$ encoding matrix L, each receiver R_i requires L, $V^{(S)}$ and $LV^{(S)}X$ in order to retrieve its required data $\mathbf{r}_i X$. Employing the method of [SKK10], we let

$$A = \begin{bmatrix} 0_{v\times v} & 0_{v\times t} \\ 0_{N\times v} & B \end{bmatrix},$$

where $B = LV^{(S)}X \in \mathbb{F}_q^{N\times t}$ if $LV^{(S)}$ is known to each receiver and $B = [LV^{(S)}|LV^{(S)}X] \in \mathbb{F}_q^{N\times(n+t)}$ if $LV^{(S)}$ is not known to all receivers. Given an error matrix W of rank $r \leq v$, we write

$$W = \begin{bmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} \end{bmatrix},$$

with $W_{11} \in \mathbb{F}_q^{v\times v}$, $W_{21} \in \mathbb{F}_q^{N\times v}$, $W_{12} \in \mathbb{F}_q^{v\times t}$, $W_{22} \in \mathbb{F}_q^{N\times t}$. If W_{11} has rank r then

$$r = \operatorname{rank}(W_{11}) \leq \operatorname{rank}\left(\begin{bmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} \end{bmatrix}\right) = \operatorname{rank}(W) = r,$$

so the rows of W_{21} are contained in the row space of W_{11}. Therefore, $TW_{11} = W_{21}$ for some $T \in \mathbb{F}_q^{N\times v}$. Then

$$r = \operatorname{rank}(W) = \operatorname{rank}(W_{11}) + \operatorname{rank}(TW_{12} - W_{22}) = r + \operatorname{rank}(TW_{12} - W_{22}),$$

so we must have $TW_{12} = W_{22}$. The matrix T can be easily computed, since the submatrices W_{11}, W_{21} are known to each receiver. Moreover, since W_{12} is also known, the decoder retrieves $B = -TW_{12} + W_{22} + B$.

From Lemma 6.1.3, the matrix L encodes the $\mathcal{I}'(m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ index code if and only if for each $i \in [m]$ there exist vectors $\mathbf{u} \in \mathbb{F}_q^n, \mathbf{a} \in \mathbb{F}_q^{d_i}$ and $\mathbf{b} \in \mathbb{F}_q^N$ such that

$$\mathbf{r}_i = \mathbf{a}V^{(i)} - \mathbf{b}LV^{(S)} \text{ and } \mathbf{u} = \mathbf{a}V^{(i)}.$$

Once $LV^{(S)}$ and $LV^{(S)}X$ is known at receiver R_i, its requested data $\mathbf{r}_i X$ can be computed as follows.

1. Choose $\mathbf{u} \in \mathcal{X}^{(i)}$. Equivalently, choose $\mathbf{a} \in \mathbb{F}_q^{d_i}$ and write $\mathbf{u} = \mathbf{a}V^{(i)}$.

2. Solve $\mathbf{r}_i + \mathbf{a}V^{(i)} = \mathbf{b}LV^{(S)}$ for some $\mathbf{b} \in \mathbb{F}_q^N$.

3. Compute $\mathbf{r}_i X = \mathbf{b}Y - \mathbf{a}\Lambda^{(i)}$.

In practice, the decoder computes $M = [A|B]$, the reduced-row echelon (RRE) form of the matrix

$$\begin{bmatrix} V^{(i)} & \Lambda^{(i)} \\ LV^{(S)} & Y \end{bmatrix}$$

and solves for $\mathbf{x}$ in $\mathbf{x}A = \mathbf{r}_i$ to retrieve $\mathbf{r}_i X = \mathbf{x}B$. In particular, if $\mathbf{r_i} = \mathbf{e}_j$ for some $j \in [N]$, then $\mathbf{r_i}$ already appears as a row of A, and the corresponding row of B gives the required vector sought.

In the event that $\text{rank}(W_{11}) < \text{rank}\left(\begin{bmatrix} W_{11} \\ W_{21} \end{bmatrix}\right)$, the decoder detects that error-trapping has failed to occur. If $\text{rank}(W_{11}) = \text{rank}\left(\begin{bmatrix} W_{11} \\ W_{21} \end{bmatrix}\right) < \text{rank}(W)$, the decoder does not detect that error-trapping has failed, so a decoding failure will occur. As noted in [SKK10] this probability is given by

$$P_f < \frac{2r}{q^{1+v-r}}. \tag{6.12}$$

If $LV^{(S)}$ is known to each receiver in advance of the transmission, so that the sender has sent

$$A = \begin{bmatrix} 0_{v\times v} & 0_{v\times t} \\ 0_{N\times v} & LV^{(S)}X \end{bmatrix},$$

if the index code $\mathcal{I}(m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ is δ error correcting the decoder may apply an algorithm to determine $\mathbf{r}_i$ from the received submatrix $[W_{22} + LV^{(S)}X]$.

When is requested an uncoded packet

In [SKK10] is given also the following alternative decoding scheme for the NC problem. Let $L \in \mathbb{F}_q^{n\times n}$ be the encoding (full rank) matrix and $X \in \mathbb{F}_q^{n\times n}$ the data matrix. Then if we transmit

$$A = \begin{bmatrix} 0_{v\times v} & 0_{v\times n} & 0_{v\times n} \\ 0_{n\times v} & L & LX \end{bmatrix},$$

we can directly detect if error-trapping has failed or not and decode computing the RRE form of the received matrix $A + W$. Here we extend this decoding scheme on the case of the ICSI and ICCSI problem, when it is requested a row of the message X, i.e. $\mathbf{r}_i = \mathbf{e}_j$ for some $j \in [n]$.

ICSI problem case

Remark 6.4.8. Let L be a matrix corresponding to an $(m, n, \mathcal{X}, f)$ instance of the ICSI problem. The sender S sends the message $Y = LX$. Then a receiver R_i, $i \in [m]$, is interested to the vector $X_{f(i)}$, and he is able to recover this, solving the system

$$L\hat{X} = Y,$$

with $\hat{X}_{\mathcal{X}_i} = X_{\mathcal{X}_i}$.

It means that the values of the variable $\hat{X}_{f(i)}$ depends only on the values of the variables $\hat{X}_{\mathcal{X}_i}$.

Now if we rewrite the system in the following form

$$L'\hat{X}' = Y, \tag{6.13}$$

where

$$L' = \left[\begin{array}{c|c|c} L^{f(i)} & L^{\mathcal{Y}_i} & L^{\mathcal{X}_i} \end{array}\right], \tag{6.14}$$

and

$$\hat{X}' = \left[\begin{array}{c} \hat{X}_{f(i)} \\ \hline \hat{X}_{\mathcal{Y}_i} \\ \hline \hat{X}_{\mathcal{X}_i} \end{array}\right].$$

From Lemma 3.2.3, computing the reduced row echelon (RRE) form of the augmented matrix of the system, that is $[L' \,|\, Y]$, the receiver R_i obtains

$$RRE(L' \,|\, Y) = \left[\begin{array}{c|c|c|c} 1 & 0 \quad \dots \quad 0 & & \\ 0 & & & \\ \vdots & \quad U & U' & Y' \\ 0 & & & \end{array}\right],$$

where $U \in \mathbb{F}_q^{(N-1)\times|\mathcal{Y}_i|}$ and $U' \in \mathbb{F}_q^{N\times|\mathcal{X}_i|}$. So to determine $X_{f(i)}$ we have to compute $Y'_1 - U'_1 \cdot X_{\mathcal{X}_i}$.

As before S sends

$$A = \left[\begin{array}{cc} 0_{v\times v} & 0_{v\times t} \\ 0_{N\times v} & B \end{array}\right],$$

where $B = [L|LX] \in \mathbb{F}_q^{N\times(n+t)}$.

Given an error matrix W of rank $r \leq v$, we write

$$W = \left[\begin{array}{ccc} W_{11} & W_{12} & W_{13} \\ W_{21} & W_{22} & W_{23} \end{array}\right],$$

with $W_{11} \in \mathbb{F}_q^{v\times v}$, $W_{21} \in \mathbb{F}_q^{N\times v}$, $W_{12} \in \mathbb{F}_q^{v\times n}$, $W_{22} \in \mathbb{F}_q^{N\times n}$, $W_{13} \in \mathbb{F}_q^{v\times t}$, $W_{23} \in \mathbb{F}_q^{N\times t}$. Suppose that error trapping successful, then considering a permutation σ such that $\sigma(L) = L'$, with L' as in (6.14) we can permute the columns of $A + W$ to obtain

$$(A+W)' = \begin{bmatrix} W_{11} & \sigma(W_{12}) & W_{13} \\ W_{21} & \sigma(W_{22}+L) & W_{23}+LX \end{bmatrix}.$$

Computing the RRE form of $(A + W)'$ we obtain

$$RRE(A+W)' = \begin{bmatrix} \hat{W_{11}} & \hat{W_{12}} & \hat{W_{13}} \\ 0 & \hat{L'} & \hat{Y} \end{bmatrix},$$

for some $\hat{W_{11}} \in \mathbb{F}_q^{v\times v}$ in RRE form, $\hat{W_{12}} \in \mathbb{F}_q^{v\times n}$, $\hat{W_{13}} \in \mathbb{F}_q^{v\times t}$ and where $[\hat{L'}|\hat{Y}] = RRE([L'|Y])$. So we correct the error and solve the system at the same time.

ICCSI problem case

Remark 6.4.9. As noted before if we consider the matrix

$$\begin{bmatrix} LV^{(S)} & Y \\ V^{(i)} & \Lambda^{(i)} \end{bmatrix}$$

and we compute the RRE form then we obtain in the first columns block the rows $\mathbf{e}_{f(i)}$, so the corresponding row in the other columns block is the requested packet $X_{f(i)}$.

From remark above we have that for the $ICCSI$ problem case if we have the matrices A and W as above and error trapping is successful, then we can recover the requested packet adding to the matrix $A+W$ the extra rows $\begin{bmatrix} 0 & V^{(i)} & \Lambda^{(i)} \end{bmatrix}$ obtaining

$$\begin{bmatrix} W_{11} & W_{12} & W_{13} \\ W_{21} & W_{22}+LV^{(S)} & W_{23}+LV^{(S)}X \\ 0 & V^{(i)} & \Lambda^{(i)} \end{bmatrix}.$$

Computing the RRE form of the obtained matrix we decode and solve the system at the same time.

Bibliography

[ABK98] R. J. Anderson, E. Biham, and L.R. Knudsen, *SERPENT: A New Block Cipher Proposal*, Fast Software Encryption, LNCS, vol. 1372, Springer, 1998, pp. 222–238.

[AC09] Martin Albrecht and Carlos Cid, *Algebraic techniques in differential cryptanalysis*, Fast Software Encryption, Springer, 2009, pp. 193–208.

[ALS+08] N. Alon, E. Lubetzky, U. Stav, A. Weinstein, and A. Hassidim, *Broadcasting with side information*, Foundations of Computer Science, 2008. FOCS '08. IEEE 49th Annual IEEE Symposium on, Oct 2008, pp. 823–832.

[Ass92] Edvard F Assmus, *Designs and their codes*, no. 103, Cambridge University Press, 1992.

[BCC11] Céline Blondeau, Anne Canteaut, and Pascale Charpin, *Differential properties of $x \mapsto x^{2^t-1}$*, Information Theory, IEEE Transactions on **57** (2011), no. 12, 8127–8137.

[BFDF98] TD Bending and Dmitry Fon-Der-Flaass, *Crooked functions, bent functions, and distance regular graphs*, JOURNAL OF COMBINATORICS **5** (1998), 507–520.

[BK98] Y. Birk and T. Kol, *Informed-source coding-on-demand (iscod) over broadcast channels*, INFOCOM '98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 3, Mar 1998, pp. 1257–1264 vol.3.

[BL11] Yossi Berliner and Michael Langberg, *Index coding with outerplanar side information*, Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on, IEEE, 2011, pp. 806–810.

[BMVT78] E. Berlekamp, R.J. McEliece, and H.C.A. Van Tilborg, *On the inherent intractability of certain coding problems (corresp.)*, Information Theory, IEEE Transactions on **24** (1978), no. 3, 384–386.

[BS93] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, J. of Cryptology **4** (1993), 3–72.

[BYBJK06] Z. Bar-Yossef, Y. Birk, T.S. Jayram, and T. Kol, *Index coding with side information*, Foundations of Computer Science, 2006. FOCS '06. 47th Annual IEEE Symposium on, Oct 2006, pp. 197–206.

[BYBJK11] ———, *Index coding with side information*, Information Theory, IEEE Transactions on **57** (2011), no. 3, 1479–1494.

[Can06] Anne Canteaut, *Open problems related to algebraic attacks on stream ciphers*, Coding and cryptography, Springer, 2006, pp. 120–134.

[Car93] Claude Carlet, *Partially-bent functions*, Designs, Codes and Cryptography **3** (1993), no. 2, 135–145.

[Car06] C Carlet, *Boolean functions for cryptography and error correcting codes. chapter of the monography boolean methods and models, y. crama and p. hammer eds*, 2006.

[CASL11] M.A.R. Chaudhry, Z. Asad, A. Sprintson, and M. Langberg, *On the complementary index coding problem*, Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on, July 2011, pp. 244–248.

[CCD00] Anne Canteaut, Pascale Charpin, and Hans Dobbertin, *Binary m-sequences with three-valued crosscorrelation: a proof of welch's conjecture*, Information Theory, IEEE Transactions on **46** (2000), no. 1, 4–8.

[CCK08] Anne Canteaut, Pascale Charpin, and Gohar M. Kyureghyan, *A new class of monomial bent functions*, Finite Fields and Their Applications **14** (2008), no. 1, 221 – 241.

[CDS06] A. Caranti, F. Dalla Volta, and M. Sala, *Abelian regular subgroups of the affine group and radical rings*, Publ. Math. Debrecen **69** (2006), no. 3, 297–308.

[CDS09a] ———, *An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher*, Designs, Codes and Cryptography **52** (2009), no. 3, 293–301.

[CDS09b] ———, *On some block ciphers and imprimitive groups*, AAECC **20** (2009), no. 5-6, 229–350.

[CG75] Don Coppersmith and Edna Grossman, *Generators for certain alternating groups with applications to cryptography*, SIAM Journal on Applied Mathematics **29** (1975), no. 4, 624–627.

[Cho00] K Chouinard, *Weight distributions of codes from planes*, Ph.D. thesis, Ph. D Thesis, University of Virginia, 2000.

[CM03] Nicolas T Courtois and Willi Meier, *Algebraic attacks on stream ciphers with linear feedback*, Advances in CryptologyEUROCRYPT 2003, Springer, 2003, pp. 345–359.

[CSRL01] Thomas H. Cormen, Clifford Stein, Ronald L. Rivest, and Charles E. Leiserson, *Introduction to algorithms*, 2nd ed., McGraw-Hill Higher Education, 2001.

[CW09] C. Cid and R. P. Weinmann, *Block ciphers: algebraic cryptanalysis and Gröbner bases*, Gröbner Bases, Coding, and Cryptography (M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso, eds.), RISC Book Series, Springer, Heidelberg, 2009, pp. 307–327.

[DKR97] Joan Daemen, Lars Knudsen, and Vincent Rijmen, *The block cipher square*, Fast Software Encryption, Springer, 1997, pp. 149–165.

[Dob99] Hans Dobbertin, *Almost perfect nonlinear power functions on gf(2, n): The niho case*, Information and Computation **151** (1999), no. 1, 57–72.

[Dob01] ———, *Almost perfect nonlinear power functions on gf (2 n): a new case for n divisible by 5*, Finite Fields and Applications, Springer, 2001, pp. 113–121.

[DR99] Joan Daemen and Vincent Rijmen, *Aes proposal: Rijndael, aes algorithm submission, september 3, 1999*, URL http://www. nist. gov/CryptoToolKit (1999).

[DR02a] J. Daemen and V. Rijmen, *The design of Rijndael*, Information Security and Cryptography, Springer-Verlag, Berlin, 2002, AES - the Advanced Encryption Standard.

[DR02b] Joan Daemen and Vincent Rijmen, *The design of rijndael: Aes-the advanced encryption standard*, Springer Science & Business Media, 2002.

[DSC12] Son Hoang Dau, Vitaly Skachek, and Yeow Meng Chee, *On the security of index coding with side information*, Information Theory, IEEE Transactions on **58** (2012), no. 6, 3975–3988.

[DSC13] ———, *Error correction for index coding with side information*, Information Theory, IEEE Transactions on **59** (2013), no. 3, 1517–1531.

[DSC14] ———, *Optimal index codes with near-extreme rates*, Information Theory, IEEE Transactions on **60** (2014), no. 3, 1515.

[EG83] Shimon Even and Oded Goldreich, *Des-like functions can generate the alternating group.*, IEEE Transactions on Information Theory **29** (1983), no. 6, 863–865.

[ERSG08] Salim El Rouayheb, Alex Sprintson, and Costas Georghiades, *On the relation between the index coding and the network coding problems*, Information Theory, 2008. ISIT 2008. IEEE International Symposium on, IEEE, 2008, pp. 1823–1827.

[ERSG10] ———, *On the index coding problem and its relation to network coding and matroid theory*, Information Theory, IEEE Transactions on **56** (2010), no. 7, 3187–3195.

[Fei73] H. Feistel, *Cryptography and Computer Privacy*, Scientific American **228** (1973), no. 5, 15–23.

[FNS75] Horst Feistel, William A Notz, and J Lynn Smith, *Some cryptographic techniques for machine-to-machine data communications*, Proceedings of the IEEE **63** (1975), no. 11, 1545–1554.

[FPRS12] C. Fontanari, V. Pulice, A. Rimoldi, and M. Sala, *On weakly APN functions and 4-bit S-Boxes*, Finite Fields and Their Applications **18** (2012), no. 3, 522–528.

[Gol68] Robert Gold, *Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.)*, Information Theory, IEEE Transactions on **14** (1968), no. 1, 154–156.

[Hae78] WH Haemers, *An upper bound for the shannon capacity of a graph*, Algebraic Methods in Graph Theory **25** (1978), 267–272.

[Her05] Doreen Hertel, *A note on the kasami power function*, Cryptology ePrint Archive (2005), 1–3, `http://eprint.iacr.org/`.

[HKM+03] Tracey Ho, R Koetter, M Medard, DR Karger, and M Effros, *The benefits of coding over routing in a randomized setting*, Information Theory, 2003. Proceedings. IEEE International Symposium on, IEEE, 2003, p. 442.

[HL12] Ishay Haviv and Michael Langberg, *On linear index coding for random graphs*, Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on, IEEE, 2012, pp. 2231–2235.

[HP03] W Cary Huffman and Vera Pless, *Fundamentals of error-correcting codes*, Cambridge university press, 2003.

[HSW94] G Hornauer, W Stephan, and Ralph Wernsdorf, *Markov ciphers and alternating groups*, Advances in CryptologyEUROCRYPT93, Springer, 1994, pp. 453–460.

[HX01] Henk DL Hollmann and Qing Xiang, *A proof of the welch and niho conjectures on cross-correlations of binary m-sequences*, Finite Fields and Their Applications **7** (2001), no. 2, 253–286.

[Kas71] Tadao Kasami, *The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes*, Information and Control **18** (1971), no. 4, 369–394.

[KJRS88] Burton S Kaliski Jr, Ronald L Rivest, and Alan T Sherman, *Is the data encryption standard a group?(results of cycling experiments on des)*, Journal of Cryptology **1** (1988), no. 1, 3–36.

[Kle13] Andreas Klein, *Stream ciphers*, Springer, 2013.

[KM03] Ralf Koetter and Muriel Médard, *An algebraic approach to network coding*, Networking, IEEE/ACM Transactions on **11** (2003), no. 5, 782–795.

[Knu99] Lars R Knudsen, *Contemporary block ciphers*, Lectures on Data Security, Springer, 1999, pp. 105–126.

[Kyu07] Gohar M Kyureghyan, *Crooked maps in fn2*, Finite Fields and their applications **13** (2007), no. 3, 713–726.

[Lan12] Serge Lang, *Introduction to linear algebra*, Springer Science & Business Media, 2012.

[Li03] C. H. Li, *The finite primitive permutation groups containing an abelian regular subgroup*, Proc. London Math. Soc. **87** (2003), no. 3, 725–747.

[LN97] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[Loe94] H.-A. Loeliger, *An upper bound on the volume of discrete spheres*, Information Theory, IEEE Transactions on **40** (1994), no. 6, 2071–2073.

[LS09] Eyal Lubetzky and Uri Stav, *Nonlinear index coding outperforming the linear optimum*, Information Theory, IEEE Transactions on **55** (2009), no. 8, 3544–3551.

[Mas69] James L Massey, *Shift-register synthesis and bch decoding*, Information Theory, IEEE Transactions on **15** (1969), no. 1, 122–127.

[Mat93] M. Matsui, *Linear cryptanalysis method for DES cipher*, Proc. of EUROCRYPT 93, LNCS, vol. 765, 1993, pp. 386–397.

[Mat94] Mitsuru Matsui, *Linear cryptanalysis method for des cipher*, Advances in CryptologyEUROCRYPT93, Springer, 1994, pp. 386–397.

[MPW94] Sean Murphy, Kenneth Paterson, and Peter Wild, *A weak cipher that generates the symmetric group*, Journal of Cryptology **7** (1994), no. 1, 61–65.

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. II*, North-Holland Publishing Co., Amsterdam, 1977, North-Holland Mathematical Library, Vol. 16.

[Nat77] National Bureau of Standards, *The Data Encryption Standard*, Federal Information Processing Standards Publication (FIPS) 46, 1977.

[Nyb94] Kaisa Nyberg, *Differentially uniform mappings for cryptography*, Advances in cryptologyEurocrypt93, Springer, 1994, pp. 55–64.

[Nyb95] ———, *S-boxes and round functions with controllable linearity and differential uniformity*, Fast Software Encryption, Springer, 1995, pp. 111–130.

[Pat99] K. G. Paterson, *Imprimitive permutation groups and trapdoors in iterated block ciphers*, Fast software encryption, LNCS, vol. 1636, Springer, Berlin, 1999, pp. 201–214.

[Pee96] René Peeters, *Orthogonal representations over finite fields and the chromatic number of graphs*, Combinatorica **16** (1996), no. 3, 417–431.

[RDP+96] Vincent Rijmen, Joan Daemen, Bart Preneel, Antoon Bosselaers, and Erik De Win, *The cipher shark*, Fast Software Encryption, Springer, 1996, pp. 99–111.

[RP97] Vincent Rijmen and Bart Preneel, *A family of trapdoor ciphers*, Fast Software Encryption, Springer, 1997, pp. 139–148.

[Rue92] R. Rueppel, *Stream ciphers*, Contemporary cryptology - The science of information integrity, IEEE Press, 1992, pp. 65–134.

[SDL14] Karthikeyan Shanmugam, Alexandros G Dimakis, and Michael Langberg, *Graph theory versus minimum rank for index coding*, Information Theory (ISIT), 2014 IEEE International Symposium on, IEEE, 2014, pp. 291–295.

[SDS12] Kenneth W Shum, Mingjun Dai, and Chi Wan Sung, *Broadcasting with coded side information*, Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on, IEEE, 2012, pp. 89–94.

[Sha49] C. E. Shannon, *Communication theory of secrecy systems*, Bell System Tech. J. **28** (1949), 656–715.

[Sha56] Claude E Shannon, *The zero error capacity of a noisy channel*, Information Theory, IRE Transactions on **2** (1956), no. 3, 8–19.

[SKK10] Danilo Silva, Frank R Kschischang, and R Kotter, *Communication over finite-field matrix channels*, Information Theory, IEEE Transactions on **56** (2010), no. 3, 1296–1305.

[SS06] Rudolf Schürer and Wolfgang Ch Schmid, *Mint: A database for optimal net parameters*, Monte Carlo and Quasi-Monte Carlo Methods 2004, Springer, 2006, pp. 457–469.

[Sti95] D. R. Stinson, *Cryptography, Theory and Practice*, CRC Press, 1995.

[SW08] Rüdiger Sparr and Ralph Wernsdorf, *Group theoretic properties of rijndael-like ciphers*, Discrete Applied Mathematics **156** (2008), no. 16, 3139–3149.

[SZZ94] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng, *Pitfalls in designing substitution boxes*, Advances in CryptologyCRYPTO94, Springer, 1994, pp. 383–396.

[W+01] Douglas Brent West et al., *Introduction to graph theory*, vol. 2, Prentice hall Upper Saddle River, 2001.

[Wag99] David Wagner, *The boomerang attack*, Fast Software Encryption, Springer, 1999, pp. 156–170.

[Wat79] William C Waterhouse, *Introduction to affine group schemes*, vol. 66, Springer Science & Business Media, 1979.

[WBDY98] Hongjun Wu, Feng Bao, Robert H Deng, and Qin-Zhong Ye, *Cryptanalysis of rijmen-preneel trapdoor ciphers*, Advances in CryptologyAsiacrypt98, Springer, 1998, pp. 126–132.

[Wer93] Ralph Wernsdorf, *The one-round functions of the des generate the alternating group*, Advances in CryptologyEUROCRYPT92, Springer, 1993, pp. 99–112.

[Wer02] ———, *The round functions of rijndael generate the alternating group*, Fast Software Encryption, Springer, 2002, pp. 143–148.

Part III

Appendices

Translation groups in small dimension

In this appendix we report some computational results about the classes of elementary abelian regular subgroups of $AGL(V,+)$ up to dimension 6, giving also a representative of each class.

n	$\mathcal{C}$'s	$\lvert\mathcal{C}\rvert$	$\dim(U_{\mathcal{C}})$
3	2	$\lvert\mathcal{C}_1\rvert = 1$	3
		$\lvert\mathcal{C}_2\rvert = 7$	1

Table A.1: Classes in $\mathrm{AGL}(\mathbb{F}^3,+)$

Representatives:

$$\mathcal{C}_1 \longrightarrow T_+$$

$$\mathcal{C}_2 \longrightarrow T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 1 \\ & 1 & 0 \\ & & 1 \end{bmatrix} + \mathbf{e}_2, 1_V + \mathbf{e}_3 \rangle$$

n	$\mathcal{C}$'s	$\lvert\mathcal{C}\rvert$	$\dim(U_{\mathcal{C}})$
4	2	$\lvert\mathcal{C}_1\rvert = 1$	4
		$\lvert\mathcal{C}_2\rvert = 105,$	2

Table A.2: Classes in $\mathrm{AGL}(\mathbb{F}^4,+)$

Representatives:

$$\mathcal{C}_1 \longrightarrow T_+$$

$$\mathcal{C}_2 \longrightarrow T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 & 0 \\ & 1 & 1 & 0 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 1 & 0 \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix} + \mathbf{e}_2, 1_V + \mathbf{e}_3, 1_V + \mathbf{e}_4 \rangle$$

n	$\mathcal{C}$'s	$\lvert\mathcal{C}\rvert$	$\dim(U_{\mathcal{C}})$
5	4	$\lvert\mathcal{C}_1\rvert = 1$	5
		$\lvert\mathcal{C}_2\rvert = 1085$	3
		$\lvert\mathcal{C}_3\rvert = 6510$	2
		$\lvert\mathcal{C}_4\rvert = 868$	1

Table A.3: Classes in $\mathrm{AGL}(\mathbb{F}^5, +)$

Representatives:

$\mathcal{C}_1 \longrightarrow T_+$

$$\mathcal{C}_2 \longrightarrow T_\circ = \left\langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ & 1 & 1 & 0 & 1 \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ & 1 & 0 & 0 & 0 \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} + \mathbf{e}_2, 1_V + \mathbf{e}_3, 1_V + \mathbf{e}_4, 1_V + \mathbf{e}_5 \right\rangle$$

$$\mathcal{C}_3 \longrightarrow T_\circ = \left\langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 1 & 1 \\ & & 1 & 1 & 1 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 0 \\ & & 1 & 1 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} + \mathbf{e}_2, \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 1 & 0 \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} + \mathbf{e}_3, 1_V + \mathbf{e}_4, 1_V + \mathbf{e}_5 \right\rangle$$

$$\mathcal{C}_4 \longrightarrow T_\circ = \left\langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 \\ & & 1 & 0 & 0 \\ & & & 1 & 1 \\ & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 \\ & & 1 & 0 & 1 \\ & & & 1 & 1 \\ & & & & 1 \end{bmatrix} + \mathbf{e}_2, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 1 \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} + \mathbf{e}_3, \right.$$
$$\left. \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ & 1 & 0 & 0 & 1 \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} + \mathbf{e}_4, 1_V + \mathbf{e}_5 \right\rangle$$

Representatives:

$\mathcal{C}_1 \longrightarrow T_+$

n	$\mathcal{C}$'s	$\lvert\mathcal{C}\rvert$	$\dim(U_{\mathcal{C}})$
6	8	$\lvert\mathcal{C}_1\rvert = 1$	6
		$\lvert\mathcal{C}_2\rvert = 9765$	4
		$\lvert\mathcal{C}_3\rvert = 234360$	3
		$\lvert\mathcal{C}_4\rvert = 410130$	3
		$\lvert\mathcal{C}_5\rvert = 8202260$	2
		$\lvert\mathcal{C}_6\rvert = 218736$	2
		$\lvert\mathcal{C}_7\rvert = 546844$	2
		$\lvert\mathcal{C}_8\rvert = 1093680$	2

Table A.4: Classes in $\mathrm{AGL}(\mathbb{F}^6, +)$

$$\mathcal{C}_2 \longrightarrow T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 1 & 0 & 1 & 0 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_2,$$
$$1_V + \mathbf{e}_3, 1_V + \mathbf{e}_4, 1_V + \mathbf{e}_5, 1_V + \mathbf{e}_6\rangle$$

$$\mathcal{C}_3 \longrightarrow T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 1 & 1 & 0 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_2,$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 1 & 0 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_3, 1_V + \mathbf{e}_4, 1_V + \mathbf{e}_5, 1_V + \mathbf{e}_6\rangle$$

$$\mathcal{C}_4 \longrightarrow T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 1 & 1 & 0 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_2,$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_3, 1_V + \mathbf{e}_4, 1_V + \mathbf{e}_5, 1_V + \mathbf{e}_6 \rangle$$

$$\mathcal{C}_5 \longrightarrow T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_2,$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_3, \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_4, 1_V + \mathbf{e}_5, 1_V + \mathbf{e}_6 \rangle$$

$$\mathcal{C}_6 \longrightarrow T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_2,$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 1 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_3, \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 1 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_4, 1_V + \mathbf{e}_5, 1_V + \mathbf{e}_6 \rangle$$

$$\mathcal{C}_7 \longrightarrow T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_2,$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_3, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_4, 1_V + \mathbf{e}_5, 1_V + \mathbf{e}_6 \rangle$$

$$\mathcal{C}_8 \longrightarrow T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_2,$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & & 1 & 1 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_3, \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} + \mathbf{e}_4, 1_V + \mathbf{e}_5, 1_V + \mathbf{e}_6 \rangle$$

A.0.4 To be ∘-linear is not affine invariant

Here we report the procedure used to find an example, over $\mathbb{F}^3$, of a function f that is linear for some operation $\circ$ but admits an affine-equivalent map non-linear for all possible operations $\circ$ that induce a vector space structure over $\mathbb{F}^3$. To compute such a function we used MAGMA.

We consider all the conjugates of the translation group T_+ in $\mathrm{Sym}(\mathbb{F}^3)$, obtaining 30 distinct subgroups. We create all the affine groups $\mathrm{AGL}(\mathbb{F}^3, \circ)$ retlated to those groups. We fix the function f given by the permutation

$$f(x) = e^4x^6 + e^2x^5 + x^4$$

where e is a primitive element of $\mathbb{F}_{2^3}$ such that $e^3 = e + 1$. This is affine for the operation related to the elementary group given by

$$T_\circ = \langle \begin{bmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{bmatrix} + \mathbf{e}_1, \begin{bmatrix} 1 & 0 & 1 \\ & 1 & 0 \\ & & 1 \end{bmatrix} + \mathbf{e}_2, 1_V + \mathbf{e}_3 \rangle$$

Now considering the affinity $\tau \in \mathrm{AGL}(\mathbb{F}^3, +)$ given by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} + \mathbf{e}_1$$

we have $f\tau \notin \mathrm{AGL}(\mathbb{F}^3, \circ')$ for any operation $\circ'$.

Magma Code

Here we report some MAGMA functions used during this work.

B.1 Basic functions

Here we give the MAGMA code used to compute some properties of Boolean functions as anti-crookedness, (weakly) differential uniformity,....

```
1
2  WDiffUnif:=function(f)
3  local V, min, numV, A, y, division, val;
4  V:=Domain(f);
5  dim:=Degree(V);
6  char:=Root(#V,dim);
7  min:=#V;
8  numV:=char^(dim-1);
9  for u in V do
10   A:={};
11   if u ne 0 then
12     for x in V do
13       y := f(x + u) + f(x);
14       A := Include(A, y);
15     end for;
16     m := #A;
17     if(m lt min) then
18       min:=m;
19     end if;
20   end if;
21 end for;
22 for delta := 2 to #V by 2 do
23   m := numV/(delta);
24     if (m lt min) then
25       return (delta);
26     end if;
27 end for;
28 return "Error!";
29 end function;
30
31
32 ////////////////////////////////////
33
34 AntiCrooked:=function(f)
35 local V, A,Im,y;
36 V:=Domain(f);
37 for u in V do
38   Im:={};
39   if u ne 0 then
```

```
    for x in V do
      y := f(x + u) + f(x);
      Im := Include(Im, y);
    end for;
    A:=sub<V|[x+f(u)+f(V!0):x in Im]>;//
    if #A eq #Im then return "false";
    end if;
  end if;
end for;

return "true";
end function;



////////////////////////////////////
Deltadiff := function(f)
//given the function f as map
//return the delta differential uniformity of f

local V;//domain of f
local max;//delta
local numV;//cardinality of V
local m;//cardinality of the pre-images
V := Domain(f); max :=0;
numV := #V;
for a in V do
for b in V do
  if (a ne 0) or (b ne 0) then
  m:=0;
    for x in V do
      if ((f(x) + f(x+a)) eq b) then
      m:=m+1;
      end if;
    end for;
  if (m ge numV) then return m;
  elif (m gt max) then
  max := m;
  end if;
end if;
end for;
end for;
return max;
end function;
////////////////////////////////////

//////////////////////////////////////////////////////////////////

Anf:=function(f)
//given the function f as map
//return the ANF of f
//if f is vBf then return the ANF's of the components
//
local D;// domain of f
local C;// codomain of f
local d;//dimension of D
local PS;//Power set
local R;//polynomial ring
local c;//dimension of C
local Pol;//polynomial to return
```

```
100 local sum;
101
102 D:=Domain(f);
103 C:=Codomain(f);
104 d:=Dimension(D);
105 c:=Degree(C);
106 R<[x]>:=PolynomialRing(GF(2),d);
107 Pol:=ZeroMatrix(R,c,1);
108 PS:=Subsets({i : i in [1..d]});
109
110 if c gt 1 then
111   for I in PS do
112     sum:=C!0;
113     for v in D do
114       if Support(v) subset I then sum:=sum+f(v);
115       end if;
116     end for;
117     if I ne {} then
118       for i in [1..c] do
119   Pol[i][1]:=Pol[i][1]+sum[i]*&*[x[j]:j in I];
120       end for;
121     else
122       for i in [1..c] do
123   Pol[i][1]:=Pol[i][1]+sum[i];
124       end for;
125     end if;
126   end for;
127 else
128   for I in PS do
129     sum:=C!0;
130     for v in D do
131       if Support(v) subset I then sum:=sum+f(v);
132       end if;
133     end for;
134     if I ne {} then
135       for i in [1..c] do
136   Pol[i][1]:=Pol[i][1]+sum*&*[x[j]:j in I];
137       end for;
138    else
139      for i in [1..c] do
140        Pol[i][1]:=Pol[i][1]+sum;
141      end for;
142     end if;
143   end for;
144 end if;
145 return Pol;
146 end function;
147
148
149 ////////////////////////////////////////////////////////////
150 Element2Vector := function(c)
151 //given an element of F_q^n return the corresponding vector of length n over F_q
152   local FF, e, degree, char, VDeg, R, prim, v, ln, p;
153   FF := Parent(c);
154   if not IsField(FF) then
155     printf "Error! the argument of this function is not a field element!\n" ;
156     return -1 ;
157   end if ;
158   e := PrimitiveElement(FF);
159   degree := Degree(FF);
```

```
  if degree eq 1 then
    return Vector(FF,[c]);
  end if ;
  char := Characteristic(FF);
  VDeg := VectorSpace(GF(char), degree);

  if c eq 0 then
    v := Zero(VDeg);
  else
    R<x> := PolynomialRing(GF(char));
    prim := PrimitivePolynomial(GF(char), degree);
    v := [];

    if c eq 1 then
      ln := 0;
    else
      ln := Log(e, c);
    end if;
    p := x^ln mod(prim);
    for i in [1..degree] do
      v:=Append(v,Coefficient(p,degree-i));
    end for;
  end if;
  return VDeg!v;
end function;

////////////////////////////////////////////////////////////

Vector2Element := function(v)
//given a vector element over GF(q) of length n return the corresponding element
    of F_q^n
  local length, F, char, k;
  // NO check on the input!!
  length := NumberOfColumns(v);
  F := Parent(v[1]);
  char := #F;
  F<e> := GF(char,length);
  k := F!0;
  for i in [1..length] do
    k := k + v[i]*e^(length-i);
  end for;
  return k;
end function;
////////////////////////////////////////////////////////////
Univariate_Pol:=function(f)
//
//
local L;//list of lagrange polynomials
local n;//dimension
local V;//domain of f
local F;//finite field GF(2^n)
local e;//primitive element
local x;//variable
local El;//list of element of F
local R;//ring R[x]
local p;//polynomial
local j;
El:=[];
L:=[];
V:=Domain(f);
```

```
n:=Dimension(V);
F<e>:=GF(2^n);
El:=[Vector2Element(v) :v in V];
R<x>:=PolynomialRing(F);
for i in El do
  Append(~L,&*[(x-j)/(i-j): j in El | j ne i]);
end for;
p:=0;
j:=1;
for i in V do
  p:=p+Vector2Element(f(i))*L[j];
  j:=j+1;
end for;
return p;
end function;
```

B.2 Classes classification

The code used to classify the elementary abelian regular subgroups of $AGL(V)$ is given below.

```

//create the spaces
n:=6;//dimension
fix:=2;//dimension of u(T)
Vn:=VectorSpace(GF(2),n);
e:=[v:v in Vn| Weight(v) eq 1];//canonical basis
Vsn:={v:v in Vn};
Sn:=Sym(Vsn);//symmetric group
Id:=IdentityMatrix(GF(2),n);
t:=sub<Sn|[[v*Id+e[t]: v in Vsn]: t in [1..n]]>;//translation group
V:=VectorSpace(GF(2),(n-fix-1)*fix);
v0:=V!0;


//////////////B_ei,M_ei
Matrix_ei:=function(i,v,n_fix)
//given the element e_i and a vector v
//return a matrix in blocks form of type
// [ I  B]
// [ 0 I ]
//and B
l:=Eltseq(v);
l0:=[GF(2)!0:j in [1..n_fix]];
Insert(~l,n_fix*(i-1)+1, n_fix*(i-1),l0);
dimV:=Degree(e[i]);
B:=Matrix(GF(2),dimV-n_fix,n_fix,l);
I:=IdentityMatrix(GF(2),dimV);
return B,InsertBlock(I,B,1,dimV-n_fix+1);
end function;

//////////////
control:=function(i,v,B,n_fix,v_null)
//given the matrix constructed before it verifies
//if the rows match the rows of precedent matrices constructed
```

```
l:=&cat[Eltseq(B[j][i]):j in [1..i-1]];
return (v ne v_null) and (l eq Eltseq([v[j]:j in [1..(i-1)*fix]]));//control on
    v_null because if v is zero then e_i lies in U(T)
end function;


N_e:=[Id:j in [1..n]];B_e:=[ZeroMatrix(GF(2),n-fix,fix):j in [1..n]];//lists of
    matrices associated to e_i's
Gr:=[];//list of the groups that fix the last "fix" elements of canonical basis

Group:=procedure(~G,i,V,~B,~N,n,fix)

if i gt n-fix then
  g1:=sub<Sn|[[v*N[t]+e[t]: v in Vsn]: t in [1..n]]>;//create the group
  if #(g1 meet t) eq 2^fix then
  Append(~G,g1);//aggiungi gruppo
  end if;
else
  for vect in V do
    B[i],N[i]:=Matrix_ei(i,vect,fix);
    if not control(i,vect,B,fix,v0) then continue vect;
    else
      $$(~G,i+1,V,~B,~N,n,fix);//iteration to i+1
    end if;
  end for;
end if;
end procedure;
Group(~Gr,1,V,~B_e,~N_e,n,fix);
```

B.3 Non-affine invariance of ∘-linearization

To find the example of a ∘ linear map over $\mathbb{F}^3$ with an affine equivalent function non-linear for all possible ∘ over $\mathbb{F}^3$ we used the following code:

```

V:=VectorSpace(GF(2),3);
Vs:={v:v in V};
S:=Sym(Vs);
e:=[v:v in V| Weight(v) eq 1];
T:=[map<V->V| x:->x+ei> : ei in e];
t:=sub<S|[[t(v): v in Vs]:t in T]>;
C:=[x:x inClass(S,t)];
Agl:=[Normalizer(S,tr):tr in C];
Agl1:=Normalizer(S,t);
Agl_join:=&join[{m: m in agl}:agl in Agl];
for c in C do
if c subset Agl1 and {V!0^p: p in c meet t} eq {V!0, e[3]} then r:=Position(C,c);
end if;
end for;
f:=Random(Agl[r]);
for a in Agl1 do
  for b in Agl1 do
    if not a*f*b in Agl_join then A:=a;B:=b; "No"; break a;
    end if;
  end for;
```

```
end for;
```

B.4 Toy-Cipher

The toy block cipher of Chapter 2 and the brute force, hidden sum attack were implemented with the following code.

```


function kb(n)
  box  := [  [1,0,1,1,1,1]  , [1,1,1,0,1,1]  , [0,1,1,0,0,1]  , [1,0,1,0,1,0]  ,
    [0,0,1,1,1,1]  , [0,1,0,1,1,1]  , [0,1,1,1,0,0]  , [1,0,0,1,1,1]  ,
    [0,1,1,0,1,0]  , [1,0,0,1,1,0]  , [1,0,0,1,0,0]  , [0,1,0,0,1,1]  ,
    [1,1,1,1,0,0]  , [0,1,1,0,0,0]  , [0,1,1,1,0,1]  , [1,1,1,0,0,0]  ,
    [1,0,0,1,0,1]  , [1,1,1,1,1,1]  , [0,1,0,1,0,0]  , [1,1,1,1,0,1]  ,
    [1,1,0,1,1,1]  , [0,0,0,0,1,0]  , [0,1,1,1,1,0]  , [1,0,1,1,0,0]  ,
    [0,0,1,0,0,1]  , [0,0,1,0,1,0]  , [0,0,0,1,1,0]  , [0,1,0,1,1,0]  ,
    [1,1,0,1,0,1]  , [1,1,0,0,0,0]  , [1,1,0,0,1,1]  , [0,0,1,0,1,1]  ,
    [1,1,1,1,1,0]  , [1,1,0,1,0,0]  , [1,0,0,0,1,1]  , [0,1,0,0,1,0]  ,
    [0,0,1,1,1,0]  , [1,0,1,1,1,0]  , [0,0,0,0,0,0]  , [1,1,0,1,1,0]  ,
    [0,1,0,0,0,1]  , [1,0,1,0,0,0]  , [0,1,1,0,1,1]  , [0,0,0,1,0,0]  ,
    [0,1,1,1,1,1]  , [0,0,1,0,0,0]  , [0,0,0,1,0,1]  , [0,0,1,1,0,0]  ,
    [0,0,0,0,1,1]  , [0,1,0,0,0,0]  , [1,0,1,0,0,1]  , [1,0,0,0,1,0]  ,
    [1,0,0,0,0,1]  , [0,0,0,1,1,1]  , [1,0,1,1,0,1]  , [1,1,0,0,0,1]  ,
    [1,1,0,0,1,0]  , [1,1,1,0,1,0]  , [0,0,0,0,0,1]  , [0,1,0,1,0,1]  ,
    [1,0,1,0,1,1]  , [1,1,1,0,0,1]  , [1,0,0,0,0,0]  , [0,0,1,1,0,1]  ];
  return box[SequenceToInteger(n,2)+1];
end function;


function keySchedule(k,n)
  A := [];
  A := Append(A,k);
  for i in [1..n] do
    k := kb(k);
    A := Append(A,k);
  end for;
  return A;
end function;


function sbox(n)
  toyblock := [[0,0,0] ,[1,1,0] ,[0,1,1] ,[1,1,1] ,[1,0,0] ,[0,0,1] ,[1,0,1]
    ,[0,1,0] ];
  t1 := Reverse(n[1..3]);
  t2 := Reverse(n[4..6]);
  return (toyblock[SequenceToInteger(t1,2)+1]) cat
    (toyblock[SequenceToInteger(t2,2)+1]);
end function;

function mlayer(n)
  a1 := (n[3]) mod 2;
  a2 := (n[1]+n[2]+n[3]+n[4]+n[6]) mod 2;
  a3 := (n[1]+n[3]) mod 2;
  a4 := (n[4]+n[6]) mod 2;
```

```
  a5 := (n[1]+n[3]+n[4]+n[5]+n[6]) mod 2;
  a6 := (n[4]) mod 2;
  return [a1,a2,a3,a4,a5,a6];
end function;



function keysum(n,k)
  return [ ( n[i] + k[i] )mod 2 : i in [1..#n] ];
end function;


function ENtoyblock(m,k,n)
  K := keySchedule(k,n);
  //c := m;
  c := keysum(m,K[1]);
  for i in [1..n] do
    c := sbox(c);
    c := mlayer(c);
    c := keysum(c,K[i+1]);
  end for;
  return c;
end function;

////////////////////////////////////
/////// Hidden Sum attack //////////
////////////////////////////////////

function lambda(x)
//given a vector v return the coefficients w.r.t. the o-sum
  l1 := (x[1]) mod 2;
  l2 := (x[1]*x[3] + x[2]) mod 2;
  l3 := (x[3]) mod 2;
  return [l1,l2,l3];
end function;

function lambdaInv(l)
  x1 := (l[1]) mod 2;
  x2 := (l[2] + l[1]*l[3]) mod 2;
  x3 := (l[3]) mod 2;
  return [x1,x2,x3];
end function;

function vprime(v)
  return lambda(v[1..3]) cat lambda(v[4..6]);
end function;

function vprimeInv(v)
  return lambdaInv(v[1..3]) cat lambdaInv(v[4..6]);
end function;



function HSAttack(Block,c)

  A := [
    [1,0,0,0,0,0],
    [0,1,0,0,0,0],
    [0,0,1,0,0,0],
    [0,0,0,1,0,0],
```

```
    [0,0,0,0,1,0],
    [0,0,0,0,0,1]
  ];

  zero := [0,0,0,0,0,0];

  Caz := [ Block(A[i]) : i in [1..6] ];
  zeroc := Block(zero);

  lCaz := [ vprime(Caz[i]) : i in [1..6]];
  lzeroc := vprime(zeroc);

  lCaz2 := [ [ (lCaz[i][j] + lzeroc[j]) mod 2 : j in [1..6]] : i in [1..6] ];

  M := Matrix(GF(2),6,6, &cat lCaz2);

  V6:=VectorSpace(GF(2),6);
  cc := V6!vprime(c);

  mm := (cc + V6!lzeroc)*M^(-1);

  mc := vprimeInv([Integers()!ElementToSequence(mm)[i] : i in [1..6]]) ;

  return mc;

end function;

////////////////////////////////////
/////// Brute force attack ////////
////////////////////////////////////


function decToBin(n,k)
  tmp :=(Intseq(n,2));
  zero :=[];
  if #tmp eq k then
  else
    zero := [0 : i in [1..(k-#tmp)]];
  end if;
  return  tmp cat zero ;
end function;

function BFAttack(Block,c)
  for i in [0..(2^6 - 1)] do
    m := decToBin(i,6);

    if Block(m) eq c then
      return m;
    end if;
  end for;
end function;


function randomKey()
  v := ElementToSequence(Random(VectorSpace(GF(2),6)));
  return [Integers()| v[i] : i in [1..#v]];
end function;


procedure testAtt()
```

```
152
153   k := [0,0,0,0,0,0];
154   n := 5;
155
156   Block := function(m)
157     return ENtoyblock(m,k,n);
158   end function;
159
160   m := [1,0,1,0,1,0];
161
162   c := Block(m);
163
164   m1 := BFAttack(Block,c);
165
166   print (m1 eq m), " Brute Force";
167
168   m2 := HSAttack(Block,c);
169
170   print (m2 eq m), " Hidden Sum";
171
172 end procedure;
173
174 function average(x)
175
176   avg := &+ [x[i]/#x : i in [1..#x]];
177   min,_ := Minimum(x);
178   max,_ := Maximum(x);
179
180   return [min,avg,max];
181
182 end function;
183
184
185 function attRound(n)
186
187
188
189   t1 := [];
190   t2 := [];
191
192   for i in [1..10] do
193
194     k := randomKey();
195     m := randomKey();
196
197     Block := function(m)
198       return ENtoyblock(m,k,n);
199     end function;
200
201
202     c := Block(m);
203
204
205     // Brute Force Attack
206     t:= Cputime();
207     m1 := BFAttack(Block,c);
208     t1 := t1 cat [Cputime(t)];
209
210     // Hidden Sum Attack
211     t:= Cputime();
```

```
212     m1 := HSAttack(Block,c);
213     t2 := t2 cat [Cputime(t)];
214
215   end for;
216
217   return t1,t2;
218
219 end function;
220
221
222 procedure attackTime()
223
224   t1 := [];
225   t2 := [];
226
227   print "N Round \t BF Min \t BF Avg \t BF Max \t HS Min \t HS Avg \t HS Max";
228
229   for i in [5..100] do
230     tBF , tHS := attRound(i);
231     t1 := average(tBF);
232     t2 := average(tHS);
233
234     print (i),"\t",t1[1],"\t",t1[2],"\t",t1[3],"\t",t2[1],"\t",t2[2],"\t",t2[3];
235
236   end for;
237
238 end procedure;
```