INFORMATION SETS IN ABELIAN CODES: DEFINING SETS AND GROEBNER BASIS

JOSÉ JOAQUÍN BERNAL AND JUAN JACOBO SIMÓN

Abstract. In [BS2] we introduced a technique to construct information sets for every semisimple abelian code by means of its defining set. This construction is a non trivial generalization of that given by H. Imai [Im] in the case of binary two-dimensional cyclic (TDC) codes. On the other hand, S. Sakata [Sak] showed a method for constructing information sets for binary TDC codes based on the computation of Groebner basis which agrees with the information set obtained by Imai. Later, H.Chabanne [Chab] presents a generalization of the permutation decoding algorithm for binary abelian codes by using Groebner basis, and as a part of his method he constructs an information set following the same ideas introduced by Sakata. In this paper we show that, in the general case of q-ary multidimensional abelian codes, both methods, that based on Groebner basis and that defined in terms of the defining sets, also yield the same information set.

1. Introduction

Information sets are essential ingredients in order to know as well as possible the properties and parameters of any error-correcting code. The fact that every codeword in a linear code is determined by its information simbols remains crucial in order to study any encoding and decoding techniques (information set decoding [Cof, Pra]); even to study certain types of cryptographic attacks [Pet]. Hence it is important to describe effective algorithms for finding them. Moreover, usually, in order to apply a fixed decoding algorithm there exist information sets better than the others. In fact the frame in which codes are constructed sometimes yields the possible techniques for constructing information sets. This is the case of codes from geometries and codes from designs [Key2, KV, Sen]. This is the topic of this paper for the family of abelian codes [Ber, Cam]. Some relevant families of codes are abelian, for instance: cyclic codes, Reed-Muller codes, extended Reed-Solomon codes and others.

Regarding binary two dimensional cyclic (TDC) codes, H. Imai [Im] gave a method to obtain information sets for TDC codes of odd area. Later, S. Sakata [Sak] gave an alternative method for the same purpose. On the one hand, Imai's algorithm used the structure of the roots of the code. On the other hand, the algorithm of Sakata is somehow based on the division algorithm for polynomials. Up to our knowledge, these are the only techniques available for TDC codes. It is known that both constructions yield the same information set (see [Im2, pp. 47-49] and [PH, Proposition 6.3]).

Since then, two generalizations has been done. The fist one is that given by H. Chabanne in [Chab], where a variant of permutation decoding was given. The

Research supported by D.G.I. of Spain and Fundación Séneca of Murcia.

implementation of the decoding algorithm given by Chabanne has two phases: The first one is devoted to construct an information set in order to get a check matrix. The second one is devoted to describe the premutation decoding algorithm. The second one is that given in [BS, BS2], where we presented a technique based on the computation of the cardinalities of certain cyclotomic cosets on different extensions of the ground field. Such cosets are completely determined by the structure of the defining set of the code. This method is valid for every semi simple abelian code, not necessarily binary, and it generalizes Imai's method.

As it was done for the constructions by Sakata and Imai, in this paper we study the relationship between the first phase of Chabanne's construction and our construction. In fact, we focus on the construction used by Chabanne to the case of binary semisimple abelian codes and we generalize it to q-ary codes with $q \geq 2$. Then we prove that if the ordering considered to compute polynomial degrees is the lexicographical ordering, then both information sets coincide. To do this, we first describe briefly both constructions and then we prove our main theorem.

Finally, we present some applications to permutation decoding. We deal with the problem of correcting all errors with a fixed weight. The applications in Chabnne's paper show us examples of codes capable to correct (few) errors quickly, as well as a higher number of errors, with a high percentage. We will see that one can get an overview of the permutation decoding properties of all abelian codes in a given algebra.

2. Preliminaries

We denote by $\mathbb{F}$ the field with q elements where q is a power of a prime p. Take $\mathcal{C}$ a linear code of dimension k and length l over the field $\mathbb{F}$. An information set for $\mathcal{C}$ is a set of positions $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, l\}$ such that restricting its codewords to these positions we get the whole space $\mathbb{F}^k$; the other $l - k$ positions are called check positions [MacSlo, PlHu].

An abelian code is an ideal of a group algebra $\mathbb{F}G$, where G is an abelian group. It is well-known that a decomposition $G \simeq C_{r_1} \times \cdots \times C_{r_n}$, with C_{r_i} the cyclic group of order r_i, induces a canonical isomorphism of $\mathbb{F}$-algebras from $\mathbb{F}G$ to

$$\mathbb{F}[X_1, \ldots, X_n] / \langle X_1^{r_1} - 1, \ldots, X_n^{r_n} - 1 \rangle .$$

We denote this quotient algebra by $\mathbb{A}(r_1, \ldots, r_n)$. So, we identify the codewords with polynomials $P(X_1, \ldots, X_n)$ such that every monomial satisfy that the degree of the indeterminate X_i is in $\mathbb{Z}_{r_i}$, the set of non negative integers less than r_i. We write the elements $P \in \mathbb{A}(r_1, \ldots, r_n)$ as $P = P(X_1, \ldots, X_n) = \sum a_{\mathbf{j}} X^{\mathbf{j}}$, where $\mathbf{j} = (j_1, \ldots, j_n) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$ and $X^{\mathbf{j}} = X_1^{j_1} \cdots X_n^{j_n}$.

We deal with abelian codes in the semisimple case, that is, we assume that $\gcd(r_i, q) = 1$, for every $i = 1, \ldots, n$. Then, every abelian code $\mathcal{C}$ is a principal ideal; we call a generator polynomial of $\mathcal{C}$ to every generator of $\mathcal{C}$ as an ideal of $\mathbb{A}(r_1, \ldots, r_n)$. We use as main references [Ber, Cam].

Fixed a primitive r_i-th root of unity α_i in some extension of $\mathbb{F}$, for each $i = 1, \ldots, n$, every abelian code $\mathcal{C}$ of $\mathbb{A}(r_1, \ldots, r_n)$ is totally determined by its *root* set,

$$\mathcal{Z}(\mathcal{C}) \quad = \quad \{(\alpha_1^{a_1}, \ldots, \alpha_n^{a_n}) \mid P(\alpha_1^{a_1}, \ldots, \alpha_n^{a_n}) = 0 \text{ for all } P(X_1, \ldots, X_n) \in \mathcal{C}\} .$$

The *defining* set of $\mathcal{C}$ with respect to $\alpha = \{\alpha_1, \ldots, \alpha_n\}$ is

$$D_\alpha(\mathcal{C}) = \{(a_1, \ldots, a_n) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n} \mid (\alpha_1^{a_1}, \ldots, \alpha_n^{a_n}) \in \mathcal{Z}(\mathcal{C})\} .$$

Given an abelian code $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_n)$, with defining set $D_\alpha(\mathcal{C})$ if one chooses different primitive roots of unity, say $\beta = \{\beta_1, \ldots, \beta_n\}$ then the set $D_\beta(\mathcal{C})$ detemines a new code, say $\mathcal{C}'$, which is permutation equivalent to $\mathcal{C}$. So, for the sake of shortness, we refer to abelian codes without any mention to the primitive roots that we are using as reference, and we denote its defining set as $D(\mathcal{C})$.

For any $\gamma \in \mathbb{N}$ the q^γ-cyclotomic coset of an integer a modulo r is the set

$$C_{(q^\gamma, r)}(a) = \left\{ a \cdot q^{\gamma \cdot i} \mid i \in \mathbb{N} \right\} \subseteq \mathbb{Z}_r.$$

Given an element $(a_1, \ldots, a_n) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$, we define its *$q$-orbit* modulo $(r_1, \ldots, r_n)$ as

$$Q(a_1, \ldots, a_n) = \left\{ \left(a_1 \cdot q^i, \ldots, a_n \cdot q^i \right) \mid i \in \mathbb{N} \right\} \subseteq \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}. \tag{1}$$

It is easy to see that for every abelian code $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_n)$, $D(\mathcal{C})$ is closed under multiplication by q in $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$, and then $D(\mathcal{C})$ is necessarily a disjoint union of q-orbits modulo $(r_1, \ldots, r_n)$. Conversely, every union of q-orbits modulo $(r_1, \ldots, r_n)$ defines an abelian code in $\mathbb{A}(r_1, \ldots, r_n)$. For the sake of simplicity we only write q-orbit, and the tuple of integers will be clear by context. The structure of q-orbits of the defining set is the essential ingredient for our algorithm, which will be described in Section 4.

Now we present a brief introduction to orderings and Groebner basis. A term ordering on $\mathbb{N}^n$ is a total ordering, which we denote by $\leq$, satisfying the following conditions

a) $\mathbf{j} \leq \mathbf{j} + \mathbf{j}'$ for every $\mathbf{j}, \mathbf{j}' \in \mathbb{N}^n$.
b) If $\mathbf{j} \leq \mathbf{j}'$ then $\delta + \mathbf{j} \leq \delta + \mathbf{j}'$ for every $\mathbf{j}, \mathbf{j}', \delta \in \mathbb{N}^n$.

As an example of a term ordering, we consider $\leq_L$ the lexicographical ordering in $\mathbb{N}^n$ defined as follows: $\mathbf{j} = (j_1, \ldots, j_n) \leq \delta = (\delta_1, \ldots, \delta_n)$ if and only if $\mathbf{j} = \delta$ or there exists $1 \leq i_0 \leq n$ such that $j_i = \delta_i$, for $i > i_0$, and $j_{i_0} < \delta_{i_0}$.

Let $\leq$ be a term ordering. For every polynomial $P = \sum a_{\mathbf{j}} X^{\mathbf{j}} \in \mathbb{F}[X_1, \ldots, X_n]$ we define the leading term of P with respect to $\leq$ as

$$\mathrm{lt}(P) = \max\{\mathbf{j} \mid a_{\mathbf{j}} \neq 0\}.$$

For the sake of shortness, we are not including in the notation $\mathrm{lt}(P)$ the reference to the term ordering considered, which will always be clear from the context.

In order to simplify notation we introduce a partial ordering on $\mathbb{N}^n$ defined by the following rule: for every $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ in $\mathbb{N}^n$

$$(a_1, \ldots, a_n) \preceq (b_1, \ldots, b_n) \text{ if } a_i \leq b_i \text{ for all } i = 1, \ldots, n. \tag{2}$$

Let $0 \neq I \leq \mathbb{F}[X_1, \ldots, X_n]$ be an ideal and fix a term ordering $\leq$ on $\mathbb{N}^n$. We denote by $\mathrm{Lt}(I)$ the set of leading terms of the elements of I with respect to $\leq$. Then a Groebner basis for I with respect to $\leq$ is a subset $\mathrm{Gb}(I) = \{g_1, \ldots, g_s\} \subseteq I$ verifying that if $\mathbf{j} \in \mathrm{Lt}(I)$ then there exist $1 \leq i \leq s$ such that $\mathrm{lt}(g_i) \preceq \mathbf{j}$ (see (2)). One can prove that for every ideal $I \neq 0$ there always exist a Groebner basis (see [Buch, Cox]).

3. Information sets by using Groebner basis

H. Chabanne showed in [Chab] a method of calculating syndromes for semisimple binary abelian codes by using Groebner bases. The author applied this method to give an alternative permutation decoding procedure. Given an abelian code, H.

Chabanne works with a set of check positions constructed from its generator polynomial and based on calculating an appropriate Groebner basis. This set coincides with that introduced by S. Sakata in [Sak] in the case of semisimple binary TDC codes. In this section we adapt Chabanne's construction to q-ary abelian codes not necessarily semisimple.

Let $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_n)$ be an abelian code generated by $\{P_1, \ldots, P_t\}$. Take $I_{\mathcal{C}}$ the ideal of $\mathbb{F}[X_1, \ldots, X_n]$ generated by $\{P_1, \ldots, P_t\}$ and the set $\{X_i^{r_i} - 1\}_{i=1}^n$. Fix $\leq$, a term ordering on $\mathbb{N}^n$. Let us consider that $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$ inherits from $\mathbb{N}^n$ the ordering defined in (2). Take $\mathrm{Gb}(I_{\mathcal{C}}) = \{g_1, \ldots, g_s\}$ a Groebner basis with respect to $\leq$.Then we define

$$\Sigma(\mathcal{C}, \leq) = \{\mathbf{j} \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n} \mid \mathrm{lt}(g_i) \preceq \mathbf{j} \text{ for some } 1 \leq i \leq s\}, \tag{3}$$

where the leading terms are calculated with respect to the term ordering $\leq$.

Note that the structure of $\Sigma(\mathcal{C}, \leq)$ depends on the Groebner basis chosen, which, in turn, depends heavily on the term ordering chosen. Indeed, the permutation decoding algorithm could work with respect to certain ordering and not with respect to some other. We denote its complementary set by $\Gamma(\mathcal{C}, \leq)$; that is, $\Gamma(\mathcal{C}, \leq) = \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n} \setminus \Sigma(\mathcal{C}, \leq)$.

From the results in [Chab] one follows that, for every binary abelian code $\mathcal{C}$, the set $\Sigma(\mathcal{C}, \leq)$ is an information set and so $\Gamma(\mathcal{C}, \leq)$ is a set of check positions. As we will see, a direct consequence of Theorem 6 is that $\Gamma(\mathcal{C}, \leq_L)$ is a set of check positions for every q-ary abelian code C, with q a power of an arbitrary prime number.

The next result, which will be useful in Section 5, shows that the set $\Sigma(\mathcal{C}, \leq)$ is, in fact, the set of leading terms of $\mathcal{C}$.

Lemma 1. *Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1, \ldots, r_n)$ and let $\leq$ be a term ordering on $\mathbb{N}^n$. Then $\Sigma(\mathcal{C}, \leq) = \mathrm{Lt}(\mathcal{C})$.*

Proof. Let $\{P_1, \ldots, P_t\}$ be a generator set of $\mathcal{C}$ as an ideal in $\mathbb{A}(r_1, \ldots, r_n)$. Let $I_{\mathcal{C}}$ be the ideal in $\mathbb{F}[X_1, \ldots, X_n]$ generated by $\{P_1, \ldots, P_t\}$ and the set $\{X_1^{r_1} - 1, \ldots, X_n^{r_n} - 1\}$. Then, we compute $\mathrm{Gb}(I_{\mathcal{C}}) = \{g_1, \ldots, g_s\}$ a Groebner basis for $I_{\mathcal{C}}$ with respect to $\leq$.

Take $P \in \mathcal{C}$ different from 0. On the one hand $\mathrm{lt}(P) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$. On the other hand, there exist $\beta \in \langle\{X_1^{r_1} - 1, \ldots, X_n^{r_n} - 1\}\rangle$ and $\beta_1, \ldots, \beta_t \in \mathbb{F}[X_1, \ldots, X_n]$ such that $P = \beta + \beta_1 P_1 + \cdots + \beta_t P_t \in I_{\mathcal{C}}$. So, there exists $i \in \{1, \ldots, s\}$ such that $\mathrm{lt}(g_i) \preceq \mathrm{lt}(P)$. Therefore $\mathrm{lt}(P) \in \Sigma(\mathcal{C}, \leq)$. This implies that $\mathrm{Lt}(\mathcal{C}) \subseteq \Sigma(\mathcal{C}, \leq)$.

Now let us see the reverse inclusion. Observe that

$$\Sigma(\mathcal{C}, \leq) = \{\mathrm{lt}(g_i) + \delta \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n} \mid \delta \in \mathbb{N}^n \text{ and } 1 \leq i \leq s\}.$$

Take $k \in \{1, \ldots, s\}$ and $\delta \in \mathbb{N}^n$ such that $\mathrm{lt}(g_k) + \delta \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$. Then $\mathrm{lt}(g_k) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$, moreover $\mathrm{lt}(g_k) + \delta = \mathrm{lt}(X^\delta g_k)$, where $X^\delta = X_1^{\delta_1} \cdots X_n^{\delta_n}$, with $\delta = (\delta_1, \ldots, \delta_n)$. Let us see that $\mathrm{lt}(X^\delta g_k) \in \mathrm{Lt}(\mathcal{C})$. Let $X^\delta g_k = c + e$, where $c \in \mathcal{C}$ and $e \in \langle\{X_1^{r_1} - 1, \ldots, X_n^{r_n} - 1\}\rangle$. From the properties of term orderings one has that $\mathrm{lt}(e) \notin \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$. So $\mathrm{lt}(X^\delta g_k) = \mathrm{lt}(c) \in \mathrm{Lt}(\mathcal{C})$ and we are done. □

4. Information sets from defining sets

In this section we describe the method of constructing sets of check positions for abelian codes (not necessarily binary) given in [BS2]. It depends solely on the defining set of the code. The reader may see the mentioned paper for details.

Let us consider the algebra $\mathbb{A}(r_1, \ldots, r_n)$ under the assumptions $(r_i, q) = 1$, for all $i = 1, \ldots, n$, and $n \geq 2$. Let D be a union of q-orbits modulo $(r_1, \ldots, r_n)$ (see (1)). For each $i = 1, \ldots, n$, let D_i denotes the projection of the elements of D onto the first i-coordinates. Then, given $e = (e_1, \ldots, e_j) \in D_j$, with $1 \leq j \leq n$, we define

$$\gamma(e) = |Q(e)|$$

and

$$m\,(e) = \left|C_{(q', r_j)}(e_j)\right|, \tag{4}$$

where $q' = q$, in case $j = 1$, and $q' = q^{\gamma(e_1, \ldots, e_{j-1})}$ otherwise.

As we have said, in the semisimple case every defining set for an abelian code in $\mathbb{A}(r_1, \ldots, r_n)$ is a union of q-orbits modulo $(r_1, \ldots, r_n)$. Our construction is based on the computation of the paremeters (4) on a special set of representatives of the q-orbits. In fact, the representatives must verify the conditions given by the following definition.

Definition 2. *Let D be a union of q-orbits modulo $(r_1, \ldots, r_n)$ and fix and ordering $X_{i_1} < \cdots < X_{i_n}$. A set $\overline{D}$ of representatives of the q-orbits of D is called a* ***restricted set of representives****, with respect to the fixed ordering, if for every $e = (e_1, \ldots, e_n)$ and $e' = (e'_1, \ldots, e'_n)$ in $\overline{D}$ one has that, for all $j = 1, \ldots, n$, the equality $Q(e_{i_1}, \ldots, e_{i_j}) = Q(e'_{i_1}, \ldots, e'_{i_j})$ implies that $(e_{i_1}, \ldots, e_{i_j}) = (e'_{i_1}, \ldots, e'_{i_j})$.*

One can prove that restricted sets of representatives of the elements of the defining set always exist and the construction does not depend on the election on the representatives. Although, different orderings on the indeterminates may yield different information sets. From now on we consider as default ordering the following one: $X_1 < \cdots < X_n$.

Now we describe our construction. Let $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_n)$ be an abelian code with defining set $D(\mathcal{C})$. Let $\overline{D}(\mathcal{C})$ be a restricted set of representatives of q-orbits in $D(\mathcal{C})$, with respect to the default ordering on the indeterminates. As before, for each $1 \leq i \leq n$, we denote by $D_i(\mathcal{C})$ and $\overline{D}_i(\mathcal{C})$ the projection of $D(\mathcal{C})$ and $\overline{D}(\mathcal{C})$ respectively, onto the first i-coordinates.

Given $e \in \overline{D}_i(\mathcal{C})$, let

$$R(e) = \{a \in \mathbb{Z}_{r_{i+1}} \mid (e, a) \in \overline{D}_{i+1}(\mathcal{C})\},$$

where (e, a) has the obvious meaning; that is, if $e = (e_1, \ldots, e_i)$ then $(e, a) = (e_1, \ldots, e_i, a)$.

The algorithm lies in calculate n families of sequences of natural numbers. For each $e \in \overline{D}_{n-1}(\mathcal{C})$, we define

$$M(e) = \sum_{a \in R(e)} m\,(e, a)$$

and consider the set $\{M(e)\}_{e\in\overline{D}_{n-1}(\mathcal{C})}$. Then we denote the different values of the $M(e)$'s as follows,

$$\begin{aligned} f_{[1]} &= \max_{e\in\overline{D}_{n-1}(\mathcal{C})}\{M(e)\} \qquad \text{and} \\ f_{[i]} &= \max_{e\in\overline{D}_{n-1}(\mathcal{C})}\{M(e) \mid M(e) < f_{[i-1]}\}. \end{aligned}$$

So, we obtain the sequence

$$f_{[1]} > \cdots > f_{[s]} > 0 = f_{[s+1]},$$

that is, we denote by $f_{[s]}$ the minimun value of the paremeters $M(\cdot)$ and we set $f_{[s+1]} = 0$ by convention. Note that $M(e) > 0$, for all $e \in \overline{D}_{n-1}(\mathcal{C})$, by definition.

For any value of n, this is the initial family of sequences and it is always formed by a single sequence. Now, suppose that $n \geq 3$. Then we continue as follows:

Given $1 \leq u \leq s$, we define for every $e \in \overline{D}_{n-2}(\mathcal{C})$

$$\Omega_u(e) = \{a \in R(e) \mid M(e,a) \geq f_{[u]}\} \text{ and } \mu_u(e) = \sum_{a\in\Omega_u(e)} m(e,a).$$

Observe that the set $\Omega_u(e)$ may eventually be the empty set. In this case, the corresponding value $\mu_u(e)$ will be zero.

We define

$$\begin{aligned} f_{[u,1]} &= \max_{e\in\overline{D}_{n-2}(\mathcal{C})}\{\mu_u(e)\} \qquad \text{and} \\ f_{[u,i]} &= \max_{e\in\overline{D}_{n-2}(\mathcal{C})}\{\mu_u(e) \mid 0 < \mu_u(e) < f_{[u,i-1]}\}. \end{aligned}$$

We order the previous parameters getting the sequence

$$f_{[u,1]} > \cdots > f_{[u,s(u)]} > 0 = f_{[u,s(u)+1]},$$

where again $f_{[u,s(u)]}$ denotes the minimum value of the paremeters $\mu_u(\cdot)$ and $f_{[u,s(u)+1]} = 0$ by definition. So we obtain the second family of sequences

$$\{f_{[u,1]} > \cdots > f_{[u,s(u)]} > 0 = f_{[u,s(u)+1]} \mid u = 1,\ldots,s\}.$$

In order to describe how to define a family of sequences from the previous ones, suppose that we have constructed the j-th family ($n-1 > j \geq 1$)

$$\begin{aligned} &\{f_{[u_n,\ldots,u_{n-j+2},1]} > \cdots > f_{[u_n,\ldots,u_{n-j+2},s(u_n,\ldots,u_{n-j+2})]} > \\ &> 0 = f_{[u_n,\ldots,u_{n-j+2},s(u_n,\ldots,u_{n-j+2})+1]} \mid (u_n,\ldots,u_{n-j+2}) \in \Upsilon_n(\mathcal{C})\}, \end{aligned}$$

where

$$\begin{aligned} \Upsilon_j(\mathcal{C}) &= \{(u_n,\ldots,u_{n-j+2}) \mid 1 \leq u_n \leq s \text{ and} \\ &\qquad 1 \leq u_i \leq s(u_n,\ldots,u_{i+1}) \text{ for } i = n-j+2,\ldots,n-1\}. \end{aligned} \tag{5}$$

For every $(u_n,\ldots,u_{n-j+2}) \in \Upsilon_j(\mathcal{C})$ we take the corresponding sequence:

$$\begin{aligned} &f_{[u_n,\ldots,u_{n-j+2},1]} > \cdots > f_{[u_n,\ldots,u_{n-j+2},s(u_n,\ldots,u_{n-j+2})]} > \\ &\qquad > 0 = f_{[u_n,\ldots,u_{n-j+2},s(u_n,\ldots,u_{n-j+2})+1]}. \end{aligned}$$

Let $u \in \{1,\ldots,s(u_n,\ldots,u_{n-j+2})\}$. Then, for every $e \in \overline{D}_{n-j-1}(\mathcal{C})$ we define

$$\Omega_{u_n,\ldots,u_{n-j+2},u}(e) = \left\{a \in R(e) \mid \mu_{u_n,\ldots,u_{n-j+2}}(e,a) \geq f_{[u_n,\ldots,u_{n-j+2},u]}\right\}$$

and

$$\mu_{u_n,\ldots,u_{n-j+2},u}(e) = \sum_{a\in\Omega_{u_n,\ldots,u_{n-j+2},u}(e)} m(e,a).$$

By ordering the differents values $\mu_{u_n,\ldots,u_{n-j+2},u}(e)$, with $e \in \overline{D}_{n-j-1}(\mathcal{C})$, we obtain

$$\begin{aligned} f[u_n,\ldots,u_{n-j+2},u,1] &> \cdots > f[u_n,\ldots,u_{n-j+2},u,s(u_n,\ldots,u_{n-j+2},u)] \\ &> 0 = f[u_n,\ldots,u_{n-j+2},u,s(u_n,\ldots,u_{n-j+2},u)+1], \end{aligned} \tag{6}$$

where $f[u_n,\ldots,u_{n-j+2},u,s(u_n,\ldots,u_{n-j+2},u)+1] = 0$ by convention. Then the $(j+1)$-th family of sequences is

$$\begin{aligned} &\{f[u_n,\ldots,u_{n-j+1},1] > \cdots > f[u_n,\ldots,u_{n-j+1},s(u_n,\ldots,u_{n-j+1})] > \\ &> 0 = f[u_n,\ldots,u_{n-j+1},s(u_n,\ldots,u_{n-j+1})+1] \mid (u_n,\ldots,u_{n-j+1}) \in \Upsilon_{j+1}(\mathcal{C})\}. \end{aligned}$$

We follow the previous process until to get $n-1$ families of sequences. Finally, by using all the previous sequences, we define, for any value of n, the last family of sequences. For every $(u_n,\ldots,u_2) \in \Upsilon_n(\mathcal{C})$ we define

$$g[u_n,\ldots,u_2] = \begin{cases} \displaystyle\sum_{\substack{e\in\overline{D}_1(C)\\ M(e)\geq f[u_2]}} m(e) & \text{if } n=2, \\ \\ \displaystyle\sum_{\substack{e\in\overline{D}_1(C)\\ \mu_{u_n,\ldots,u_3}(e)\geq f[u_n,\ldots,u_2]}} m(e) & \text{if } n>2. \end{cases}$$

So the last family of sequences is

$$\begin{aligned} &\{g[u_n,\ldots,u_3,1] < \cdots < g[u_n,\ldots,u_3,s(u_n,\ldots,u_3)] < \\ &< g[u_n,\ldots,u_3,s(u_n,\ldots,u_3)] \mid (u_n,\ldots,u_3) \in \Upsilon_{n-1}(\mathcal{C})\}. \end{aligned}$$

The algorithm yields the following set

$$\begin{aligned} \Gamma(\mathcal{C}) = \{&(i_1,\ldots,i_n) \in \mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n} \mid \\ &\text{there exists } (u_n,\ldots,u_2) \in \Upsilon_n(\mathcal{C}) \text{ such that} \\ &f[u_n,\ldots,u_j+1] \leq i_j < f[u_n,\ldots,u_j], \text{ for } j=2,\ldots,n, \text{ and} \\ &0 \leq i_1 < g[u_n,\ldots,u_2]\}. \end{aligned} \tag{7}$$

The following theorem, proved in [BS2], establishes that $\Gamma(\mathcal{C})$ is a set of check positions for $\mathcal{C}$.

Theorem 3 ([BS2]). *Let $\mathcal{C} \leq \mathbb{A}(r_1,\ldots,r_n)$ be an abelian code. Assume that $(r_i,q)=1$, for every $i=1,\ldots,n$, and $n\geq 2$. Then $\Gamma(\mathcal{C})$ is a set of check positions for $\mathcal{C}$.*

5. Relationship between both constructions

Now, we study the relationship between the sets $\Gamma(\mathcal{C},\leq)$ and $\Gamma(\mathcal{C})$ described in Sections 3 and 4 respectively. First, we need the following theorem due to S. Sakata which uses the following notation: Given a subset $S \subseteq \mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n}$ one defines

$$\mathcal{P}(S) = \left\{ \sum_{\mathbf{j}\in S} a_{\mathbf{j}} X^{\mathbf{j}} \in \mathbb{F}[X_1,\ldots,X_l] \setminus \{0\} \right\}.$$

Theorem 4 ([Sak])**.** *Let $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_n)$ be an abelian code with dimension k. Let S be a subset of $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$. Then S is a set of check positions for $\mathcal{C}$ if and only if the following conditions hold:*

a) $\mathcal{C} \cap \mathcal{P}(S) = \emptyset$.

b) S is maximal in $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$ such that a) is valid, or equivanletly, $|S| = \prod_{i=1}^{n} r_i - k$.

Let us see that $\Gamma(\mathcal{C}, \leq)$ satisfies the condition $a)$ given by the previous theorem.

Lemma 5. *Let $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_n)$ be an abelian code with dimension k and let $\leq$ be a term ordering. Then $\Gamma(\mathcal{C}, \leq)$ satisfies that $\mathcal{C} \cap \mathcal{P}(\Gamma(\mathcal{C}, \leq)) = \emptyset$.*

Proof. Let $\{P_1, \ldots, P_t\}$ be a set of generators of $\mathcal{C}$ as an ideal in $\mathbb{A}(r_1, \ldots, r_n)$. As before, we write $I_{\mathcal{C}}$ to denote the ideal in $\mathbb{F}[X_1, \ldots, X_l]$ generated by $\{P_1, \ldots, P_t\}$ and the set $\{X_1^{r_1} - 1, \ldots, X_n^{r_n} - 1\}$. Let $\mathrm{Gb}(I_{\mathcal{C}}) = \{g_1, \ldots, g_s\}$ be a Groebner basis for $I_{\mathcal{C}}$ with respect to $\leq$.

Take $P \in \mathcal{C}$ different from zero and denote $\mathbf{j}_0 = \mathrm{lt}(P)$, where the leading term is calculated by using the fixed ordering $\leq$. Then $\mathbf{j}_0 \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$. On the other hand, there exist $\beta \in \langle \{X_1^{r_1} - 1, \ldots, X_n^{r_n} - 1\} \rangle$ and $\beta_1, \ldots, \beta_t \in \mathbb{F}[X_1, \ldots, X_n]$ such that $P = \beta + \beta_1 P_1 + \cdots + \beta_t P_t \in I_{\mathcal{C}}$. By definition of Groebner basis, there exists $i \in \{1, \ldots, s\}$ such that $\mathrm{lt}(g_i) \preceq \mathbf{j}_0$. Therefore, $\mathbf{j}_0 \in \Sigma(\mathcal{C}, \leq)$, and hence $\mathbf{j}_0 \notin \Gamma(\mathcal{C}, \leq)$. One follows that $P \notin \mathcal{P}(\Gamma(\mathcal{C}, \leq))$. □

The next theorem shows that if we take as term ordering the lexicographical one defined in Section 2, we have the equality between the sets $\Gamma(\mathcal{C}, \leq_L)$ and $\Gamma(\mathcal{C})$.

Theorem 6. *Let $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_n)$ be an abelian code. Assume that $(r_i, q) = 1$, for every $i = 1, \ldots, n$, and $n \geq 2$. Then $\Gamma(\mathcal{C}) = \Gamma(\mathcal{C}, \leq_L)$.*

Proof. For each $i = 1, \ldots, n$, fix a primitive r_i-th root of unity α_i in some extension of $\mathbb{F}$. Let $D(\mathcal{C})$ be the defining set of $\mathcal{C}$ with respect to $\{\alpha_1, \ldots, \alpha_n\}$. Take $\overline{D}(\mathcal{C})$ a restricted set of representatives of the q-orbits of $D(\mathcal{C})$.

Given $u \in \{1, \ldots, s+1\}$ we define

$$H_u = \{e \in \overline{D}_{n-1}(\mathcal{C}) \mid M(e) \geq f_{[u]}\}$$

and for every $(u_n, \ldots, u_{i+1}) \in \Upsilon_{n-i+1}(\mathcal{C})$ (see (5)) and $u \in \{1, \ldots, s(u_n, \ldots, u_{i+1}) + 1\}$, with $2 \leq i \leq n-1$, we define

$$H_{u_n, \ldots, u_{i+1}, u} = \{e \in \overline{D}_{i-1}(\mathcal{C}) \mid \mu_{u_n, \ldots, u_{i+1}}(e) \geq f_{[u_n, \ldots, u_{i+1}, u]}\}.$$

First, we shall prove that $\Gamma(\mathcal{C}) \subseteq \Gamma(\mathcal{C}, \leq_L)$. To do this we show that for every $P \in \mathcal{C}$ one has that $\mathrm{lt}(P) \notin \Gamma(\mathcal{C})$, where the leading term is calculated by using the ordering $\leq_L$. This fact, together with Lemma 1 will give us the inclusion.

Let $P \in \mathcal{C}$. Suppose that $\mathrm{lt}(P) \in \Gamma(\mathcal{C})$. We consider P as a polynomial in n indeterminates; that is, $P = P(X_1, \ldots, X_n)$. Let us denote $\mathrm{lt}(P) = (\eta_1, \ldots, \eta_n)$. By the definition of $\Gamma(\mathcal{C})$, there exists $(v_n, \ldots, v_2) \in \Upsilon_n(\mathcal{C})$ such that

$$\begin{aligned} & f_{[v_n, \ldots, v_j + 1]} \leq \eta_j < f_{[v_n, \ldots, v_j]}, \text{ with } j = 2, \ldots, n, \\ & \text{and} \\ & 0 \leq \eta_1 < g_{[v_n, \ldots, v_2]}. \end{aligned} \tag{8}$$

Then we define

$$w = \min \quad \{u \in \{1, \ldots, s+1\} \mid \text{ there exists } e = (e_1 \ldots, e_{n-1}) \in H_u \text{ with } P\left(\alpha_1^{e_1}, \ldots, \alpha_{n-1}^{e_{n-1}}, X_n\right) \neq 0\},$$

where by convention $w = s+1$ in case that $P(\alpha_1^{e_1}, \ldots, \alpha_{n-1}^{e_{n-1}}, X_n) = 0$ for all $e = (e_1 \ldots, e_{n-1}) \in \overline{D}_{n-1}(\mathcal{C})$. Note that $\overline{D}_{n-1}(\mathcal{C}) = H_1 \cup \cdots \cup H_{s+1}$, and then w must exist. If $w < s+1$ then there exists $e = (e_1, \ldots, e_{n-1}) \in H_w$ such that $P\left(\alpha_1^{e_1}, \ldots, \alpha_{n-1}^{e_{n-1}}, X_n\right) \neq 0$, and hence

$$\eta_n \geq \sum_{a \in R(e)} m(e, a) = M(e) \geq f_{[w]}.$$

Since $f_{[s+1]} = 0$, for any value of w we conclude that $\eta_n \geq f_{[w]}$ and so $v_n < w$. Moreover, for all $u < w$ and $e = (e_1 \ldots, e_{n-1}) \in H_u$ one has that $P(\alpha_1^{e_1}, \ldots, \alpha_{n-1}^{e_{n-1}}, X_n) = 0$. We write

$$P\left(X_1, \ldots, X_n\right) = \sum_{t=0}^{\eta_n} P_t\left(X_1, \ldots, X_{n-1}\right) {X_n}^t.$$

Then we have $P_{\eta_n}(\alpha_1^{e_1}, \ldots, \alpha_{n-1}^{e_{n-1}}) = 0$ for all $e = (e_1 \ldots, e_{n-1}) \in H_{v_n}$.

Now, we define

$$w(v_n) = \min \quad \{u \in \{1, \ldots, s(v_n)+1\} \mid \text{ there exists } e = (e_1, \ldots, e_{n-2}) \in H_{v_n,u} \text{ with } P_{\eta_n}\left(\alpha_1^{e_1}, \ldots, \alpha_{n-2}^{e_{n-2}}, X_{n-1}\right) \neq 0\},$$

where by convention $w(v_n) = s(v_n) + 1$ in case that $P_{\eta_n}\left(\alpha_1^{e_1}, \ldots, \alpha_{n-2}^{e_{n-2}}, X_{n-1}\right) = 0$ for all $e = (e_1, \ldots, e_{n-2}) \in \overline{D}_{n-2}(\mathcal{C})$. Note that $\overline{D}_{n-2}(\mathcal{C}) = H_{v_n,1} \cup \cdots \cup H_{v_n,s+1}$, and hence $w(v_n)$ must exist. If $w(v_n) < s(v_n) + 1$ then there exists $e = (e_1, \ldots, e_{n-2}) \in H_{v_n,w(v_n)}$ such that $P_{\eta_n}\left(\alpha_1^{e_1}, \ldots, \alpha_{n-2}^{e_{n-2}}, X_{n-1}\right) \neq 0$. This implies that

$$\eta_{n-1} \geq \sum_{a \in \Omega_{v_n}(e)} m(e, a) = \mu_{v_n}(e) \geq f_{[v_n, w(v_n)]}.$$

Since $f_{[v_n, s(v_n)+1]} = 0$, we may conclude that for any value of $w(v_n)$ one has that $\eta_{n-1} \geq f_{[v_n, w(v_n)]}$, and hence $v_{n-1} < w(v_n)$. Moreover, for all $u < w(v_n)$ and $e = (e_1 \ldots, e_{n-2}) \in H_{v_n,u}$, $P(\alpha_1^{e_1}, \ldots, \alpha_{n-2}^{e_{n-2}}, X_{n-1}) = 0$. We denote

$$P_{\eta_n}\left(X_1, \ldots, X_{n-1}\right) = \sum_{t=0}^{\eta_{n-1}} P_{\eta_n,t}\left(X_1, \ldots, X_{n-2}\right) {X_{n-1}}^t.$$

Then we have that $P_{\eta_n,\eta_{n-1}}(\alpha_1^{e_1}, \ldots, \alpha_{n-2}^{e_{n-2}}) = 0$ for all $e = (e_1 \ldots, e_{n-2}) \in H_{v_n,v_{n-1}}$.

We continue this process until to obtain a polynomial $P_{\eta_l,\ldots,\eta_2}(X_1)$ in $\mathbb{F}[X_1]$ such that $P_{\eta_l,\ldots,\eta_2}(\alpha_1^{e_1}) = 0$ for all $e_1 \in H_{v_n,\ldots,v_2}$. Therefore,

$$\eta_1 \geq \sum_{a \in H_{v_n,\ldots,v_2}} m(a) = g_{[v_n, \ldots, v_2]},$$

where the equality of the right hand side follows from the fact that

$$H_{u_n,\ldots,u_2} = \{e \in \overline{D}_1(\mathcal{C}) \mid \mu_{u_n,\ldots,u_3}(e) \geq f_{[u_n, \ldots, u_2]}\}.$$

This contradicts (8). So $\Gamma(\mathcal{C}) \subseteq \Gamma(\mathcal{C}, \leq_L)$.

Finally, by aplying Theorem 3, Lemma 5 and Theorem 4 we obtain directly the reverse inclusion $\Gamma(\mathcal{C}) = \Gamma(\mathcal{C}, \leq_L)$. □

Let us remark that if we take an ordering of the indeterminates different from that chosen to get $\Gamma(\mathcal{C})$, to wit, $X_1 < \cdots < X_n$, one can prove analogously that the corresponding new set $\Gamma(\mathcal{C})$ equals $\Gamma(\mathcal{C}, \leq_{L'})$ with $\leq_{L'}$ the lexicographical ordering in $\mathbb{N}^n$ associated with the new ordering on the indeterminates. This fact will be used in Section 6.

The following corollary follows directly from the previous theorem.

Corollary 7. *Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1, \ldots, r_n)$. Assume that $(r_i, q) = 1$, for every $i = 1, \ldots, n$, and $n \geq 2$. Then $\Gamma(\mathcal{C}, \leq_L)$ is a set of check positions for $\mathcal{C}$.*

6. Applications

In the previous section we have checked that in the case of semi simplicity and lexicographical ordering in the variables, both constructions afford the same information set. However, the behavior of each of these two constructions, determines the scope of its applicabilty. In Chabnne's paper we may find examples of codes capable to correct (few) errors quickly, as well as a higher number of errors, with a high percentage. We deal with the problem of correcting all errors with a fixed weight. With our method, one can get an overview of the permutation decoding properties of all codes in a given algebra $\mathbb{A}(r_1, \ldots, r_n)$.

Before we present our examples let us give a brief introduction to the (original) permutation decoding algorithm. Permutation decoding was introduced by F. J. MacWilliams in [Mac] and it is fully described in [Hu] and [MacSlo]. Fixed an information set for a given linear code $\mathcal{C}$, this technique uses a special set of permutation automorphisms of the code called PD-set.

We denote the permutation group on $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$ by $S_{r_1 \times \cdots \times r_n}$ and we consider its extension to automorphisms of $\mathbb{A}(r_1, \ldots, r_n)$ via $\tau\left(\sum_{\mathbf{j}} a_{\mathbf{j}} X^{\mathbf{j}}\right) = \sum_{\mathbf{j}} a_{\tau^{-1}(\mathbf{j})} X^{\mathbf{j}}$. Under this point of view the permutation automorphism group of an abelian code $\mathcal{C} \leq \mathbb{A}(r_1, \ldots, r_n)$ is $\mathrm{PAut}(\mathcal{C}) = \{\tau \in S_{r_1 \times \cdots \times r_n} \mid \tau(\mathcal{C}) = \mathcal{C}\}$.

Definition 8. *Let $\mathcal{C}$ be a t-error-correcting $[l, k]$ code. Let $\mathcal{I}$ be an information set for $\mathcal{C}$. For $s \leq t$ a s-*PD-set *for $\mathcal{C}$ and $\mathcal{I}$ is a subset $P \subseteq \mathrm{PAut}(\mathcal{C})$ such that every set of s coordinate positions is moved out of $\mathcal{I}$ by at least one element of P (see* [Key, Mac]*). In case $s = t$, we say that P is a PD-set.*

The idea of permutation decoding is to apply the elements of the PD-set to the received vector until the errors are moved out of the fixed information set. The following theorem shows how to check that the information symbols of a codeword with weight less or equal than t are correct. We denote the weight of a vector $v \in \mathbb{F}^l$ by $wt(v)$.

Theorem 9 ([Hu], Theorem 8.1)**.** *Let $\mathcal{C}$ be a t-error-correcting $[l, k]$ code with parity check matrix H in standard form. Let $r = c + e$ be a vector, where $c \in \mathcal{C}$ and $wt(e) \leq t$. Then the information symbols in r are correct if and only if $wt\left(Hr^T\right) \leq t$.*

Then, once we have found a PD-set $P \subseteq \mathrm{PAut}(\mathcal{C})$ for the given code $\mathcal{C}$ and information set $\mathcal{I}$, the algorithm of permutation decoding is as follows: take a check-matrix H for $\mathcal{C}$ in standard form. Suppose that we receive a vector $r = c + e$, where $c \in \mathcal{C}$ and e represents the error vector and satisfies that $wt(e) \leq t$. Then we calculate the syndromes $H\left(\tau(r)\right)^T$, with $\tau \in P$, until we obtain a vector $H\left(\tau_0(r)\right)^T$

with weight less than or equal to t. By the previous theorem, the information symbols of the permuted vector $\tau(r)$ are correct, so by using the parity check equations we obtain the redundancy symbols and then we can construct a codeword c'. Finally, we decode to $\tau^{-1}(c') = c$.

In general to find t-PD-sets for a given t-error correcting code is not at all an easy problem. It depends on the chosen information set and they need not even to exist. Moreover, it is clear that the algorithm is more efficient the smaller the size of the PD-set.

Let T_s be the transformation from $\mathbb{A}(r_1, \ldots, r_n)$ into itself, given by

$$T_s(P(X_1, \ldots, X_n)) = X_s \cdot P(X_1, \ldots, X_n)$$

for $s = 1, \ldots, n$. Then it is clear that T_s can be seen as a permutation in $S_{r_1 \times \cdots \times r_n}$, via $T_s\,(i_1, \ldots, i_n) = (i_1, \ldots, i_s + 1, \ldots, i_n)$ and as such, $\langle \{T_s\}_{s=1}^n \rangle$ may be viewed as a subgroup of $\mathrm{PAut}(\mathcal{C})$ for every abelian code $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_n)$. We consider permutation decodable codes with respect to our information set and with a PD-set contained in the group generated by the translations $T_1, \ldots, T_n$.

Example 10. In [Chab, Example 1] Chabanne considers the $[49 = 7 \times 7, 18, 12]$ binary code, $\mathcal{L}_1$, with defining set

$$\begin{aligned} D(\mathcal{L}_1) \;=\; & Q(0,0) \cup Q(0,1) \cup Q(1,0) \cup Q(1,1) \cup Q(3,3) \cup \\ & Q(0,3) \cup Q(3,0) \cup Q(3,5) \cup Q(5,3) \cup Q(1,4) \cup Q(4,1). \end{aligned} \tag{9}$$

Chabanne explains how this information set works in order to make permutation decoding. He obtains that $\mathcal{L}_1$ may correct any error with weight less or equal than 3, by using the PD-set $\langle T_1, \sigma \rangle$, where $\sigma(P(X,Y)) = P(X^2, Y^2)$. Moreover, he made a probabilistic study on the permutation decoding capability of $\mathcal{L}_1$ for errors with weight greater than 3.

Now we are going to see how our tools work, and what kind of results one may obtain. Concretely, we will see that by studying the 2-orbit structure of the whole space $\mathbb{Z}_7 \times \mathbb{Z}_7$ we may get the 3-error correcting codes of length 49 with highest dimension, such that the group $\langle T_1,\ T_2 \rangle$ is a PD-set.

Example 11. The reader may check, in a direct fashion, that there are two shapes $\mathbf{A}_1$ and $\mathbf{A}_2$, in $\mathbb{Z}_7 \times \mathbb{Z}_7$ with the minimum area for which it is possible to put inside three positions.

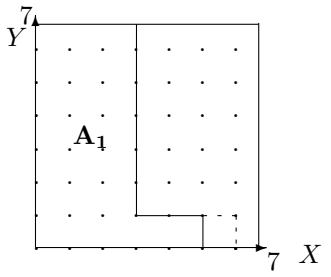

Figure 3

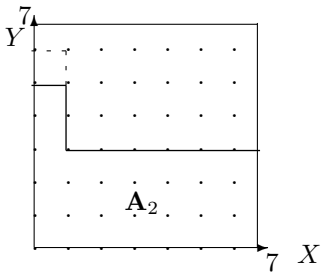

Figure 4

Now, the following table describes all minimal abelian codes in $\mathbb{A}(7,7)$. For $i = 1, \ldots, 17$, we call $E_i = (\mathbb{Z}_7 \times \mathbb{Z}_7) \setminus D(\mathcal{C}_i)$. Note that the parameters $m(-)$, and so $M(-)$, have been computed with respect to the ordering $X > Y$.

Code	E_i	$M(0)$	$M(1)$	$M(3)$	dimension
$\mathcal{C}_1$	$Q(0,0)$	1	0	0	1
$\mathcal{C}_2$	$Q(0,1)$	0	1	0	3
$\mathcal{C}_3$	$Q(0,3)$	0	0	1	3
$\mathcal{C}_4$	$Q(1,0)$	3	0	0	3
$\mathcal{C}_5$	$Q(3,0)$	3	0	0	3
$\mathcal{C}_6$	$Q(1,1)$	0	1	0	3
$\mathcal{C}_7$	$Q(3,3)$	0	0	1	3
$\mathcal{C}_8$	$Q(4,1)$	0	1	0	3
$\mathcal{C}_9$	$Q(5,3)$	0	0	1	3
$\mathcal{C}_{10}$	$Q(1,3)$	0	0	1	3
$\mathcal{C}_{11}$	$Q(5,1)$	0	1	0	3
$\mathcal{C}_{12}$	$Q(2,1)$	0	1	0	3
$\mathcal{C}_{13}$	$Q(6,3)$	0	0	1	3
$\mathcal{C}_{14}$	$Q(2,3)$	0	0	1	3
$\mathcal{C}_{15}$	$Q(3,1)$	0	1	0	3
$\mathcal{C}_{16}$	$Q(4,3)$	0	0	1	3
$\mathcal{C}_{17}$	$Q(6,1)$	0	1	0	3

Accordingly with the table above, one may check that there not exist any sum of minimal codes $\mathcal{C}$, for which $\Gamma(\mathcal{C}) = \mathbf{A}_1$ or $\mathbf{A}_2$. What we can find are codes such that their set of check positions agrees with the shape delimited by the dashed lines, and so all of them have dimension 25. This is the highest dimension for a 3-error correcting code of length 49 decodable with the PD-set $\langle T_1,\ T_2 \rangle$. However, in the case of Figure 4, any of such codes must contain the code $\mathcal{C}_1 + \mathcal{C}_4 + \mathcal{C}_5$ whose minimum distance is 6, and so, it is not a 3-error correcting code. In the case of Figure 3, the sums of minimal codes works better, and, for example, $\mathcal{L}_3 = \mathcal{C}_4 + \cdots + \mathcal{C}_9 + \mathcal{C}_{12} + \mathcal{C}_{13}$ has minimum distance, $d(\mathcal{L}_3) = 7$. Note that $\mathcal{L}_1 \subset \mathcal{L}_3$, and $\dim(\mathcal{L}_1) = 18 < \dim(\mathcal{L}_3) = 25$.

The code $\mathcal{L}_3$, even it has not the best parameters (see http://codetables.de/), its relevance relies on the fact that it is the highest dimensional binary permutation decodable code in $\mathbb{A}(7,7)$.

Finally, we include a non binary example on three variables.

Example 12. The same procedure seen in the example above allows us to extend our designing of permutation decodable codes to three variables. We shall construct a 5-ary, 3-error correcting code in $\mathbb{A}(3,3,6)$, with the highest dimension satisfying that $\langle T_1, T_2, T_3 \rangle$ is a partial PD-set.

As above, by analizing the 3-dimensional shapes in $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_6$ one may check that the shape with minimum volume for which it is possible to put inside 3-positions, corresponds to the following parameters.

$$\begin{array}{l} f_{[1]} = 5 > f_{[2]} = 3 > f_{[3]} = 1 \\ f_{[1,1]} = 3;\ f_{[2,1]} = 3 > f_{[2,2]} = 1;\ f_{[3,1]} = 3 \\ g_{[1,1]} = 1;\ g_{[2,1]} = 1 < g_{[2,2]} = 3;\ g_{[3,1]} = 3 \end{array}$$

There are no any abelian code with this parameters, however, there are codes with information sets shapes very close to that considered. One of them is the code $\mathcal{C}$, with defining set

$$\begin{aligned} D(\mathcal{C}) \quad = \quad & Q(0,0,0) \cup Q(0,0,1) \cup Q(0,0,2) \cup Q(0,0,3) \cup Q(0,1,1) \cup \\ & Q(0,1,2) \cup Q(0,1,3) \cup Q(0,1,4) \cup Q(0,1,5) \cup Q(1,0,5) \cup \\ & Q(1,1,5) \cup Q(1,2,3) \cup Q(1,2,4) \cup Q(1,2,5). \end{aligned}$$

whose $\Gamma(\mathcal{C})$ is determined by the parameters

$$\begin{array}{l} f_{[1]} = 6 > f2 = 5 > f_{[3]} = 3 > f_{[4]} = 1 \\ f_{[1,1]} = 1;\ f_{[2,1]} = 3;\ f_{[3,1]} = 3 > f_{[3,2]} = 1;\ f_{[4,1]} = 3 \\ g_{[1,1]} = 1;\ g_{[2,1]} = 1;\ g_{[3,1]} = 1 < g_{[3,2]} = 3;\ g_{[4,1]} = 3. \end{array}$$

The code $\mathcal{C}$ is a $[54, 28, 8]$, 5-ary abelian code.

Acknowledgement: The authors would like to thank the referees for their comments, that contribute to give a clearer exposition.

References

[Ber] Berman, S. D.: Semisimple cyclic and Abelian codes. Cybernetics vol. 3 no. 3, pp. 21-30 (1967).

[BS] Bernal, J. J. and Simón, J. J.: Information sets for abelian codes. 2010 IEEE Information Theory Workshop - ITW 2010 Dublin.

[BS2] Bernal J. J. and Simón, J. J., Information sets from defining sets in abelian codes. IEEE Trans. Inform. Theory, vol. 57, no. 12, pp. 7990-7999 (2011).

[Buch] Buchberger, B., Groebner bases: An algorithm method in polynomial ideal theory. In: Bose (ed.) Recent trends in multidimensional system theory. Dordrecht: Reidel (1985).

[Cam] Camion, P., Abelian codes. MRC Tech. Sum. Rep. no. 1059, Univ. of Wisconsin, Madison (1970).

[Chab] Chabanne, H., Permutation decoding of abelian codes, IEEE Trans. on Inform. Theory, vol. 38, no. 6, pp. 1826-1829 (1992).

[Cof] Coffey, J. T. and Goodman, R. M. The complexity of information set decoding, IEEE Trans. Inform. Theory, vol. 36, no. 5, pp. 1031-1037 (1990).

[Cox] Cox, D., Little, J. and O'Shea, D., *Ideals, varieties, and algorithms*. Springer: New York (1992).

[Hu] Huffman, W. C., Codes and groups, in Pless, V. S., Huffman, W. C. and Brualdi, R. A. (editors), *Handbook of Coding Theory*, vol. II. North-Holland, Amsterdam, pp. 1345-1440 (1998).

[Im] Imai, H.: A theory of two-dimesional cyclic codes, Information and Control, vol. 34, pp. 1-21 (1977).

[Im2] Imai, H.: Multivariate polynomials in coding theory, AAECC-2, LNCS, vol. 228, pp. 36-60 (1986).

[Key] Key, J. D., McDonough, T. P. and Mavron, V. C., Partial permutation decoding for codes from finite planes, European Journal of Combinatorics, no. 26, pp. 665-682 (2005).

[Key2] Key, J. D., McDonough, T. P. and Mavron, V. C., Information sets and partial permutation decoding for codes from finite geometries, Finite Fields and their Applications, vol. 12, pp. 232-247 (2006).

[KV] Kroll, H. J. and Vincenti, R., PD-sets for the codes realted to some classical varieties, Discrete Mathematics vol. 301, pp. 89-105 (2005).

[Mac] MacWilliams, F. J., Permutation decoding of systematic codes, Bell. Syst. Tech. J. vol. 43, pp. 485-505 (1964).

[MacSlo] MacWilliams, F. J. and Sloane, N. J. A.: *The theory of error-correcting codes*, North-Holland, Amsterdam (1983).

[Pet] Peters, C., Information-set decoding for linear codes over F_q. 2010 Third International Workshop, PQCrypto, Darmstadt. Springer.

[PlHu] Pless, V. S., Huffman W. C. and Brualdi R. A. (editors), *Handbook of Coding Theory*, vol. I. North-Holland, Amsterdam (1998).

[PH] Poli, A. L. and Huguet, L.: *Codes Correcteurs*, Masson, Paris (1988).

[Pra] Prange, E., The use of information sets in decoding cyclic codes, IRE Trans., vol. IT-8, pp. S5-S9 (1962).

[Sak] Sakata, S.: On determining the independent point set for doubly periodic arrays and encond-ing two-dimensional cyclic codes and their duals, IEEE Trans. Inform. Theory, vol. IT-27, no. 5 556-565 (1981).

[Sen] P. Seneviratne, Partial permutation decoding for the first-order Reed-Muller codes, Discrete Mathemathics, vol. 309, pp. 1967-1970 (2009),

Departamento de Matemáticas, Universidad de Murcia, Spain