Partial Permutation Decoding for abelian codes

José Joaquín Bernal and Juan Jacobo Simón

Abstract

In [3], we introduced a technique to construct an information set for every semisimple abelian code over an arbitrary field, solely in terms of its defining set. In this paper we apply the geometrical properties of those information sets to obtain sufficient conditions for a t-error correcting abelian code to have a b-PD-set for every $b \leq t$. These conditions are simply given in terms of the structure of the defining set of the code.

I. Introduction

Permutation decoding was introduced by F. J. MacWilliams in [14] and it is fully described in [9] and [15]. For a fixed information set of a given linear code, this technique uses a special set of permutation automorphisms of the code called 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. But, how can we determine when all errors have been moved out of the information positions? Given a t-error correcting code with a fixed information set and parity check matrix in standard form, it is proved (see, for example, [9, Theorem 8.1]) that a received vector has syndrome with weight less than or equal to t if and only if all its information symbols are correct.

Finding adequate information sets and PD-sets is not trival. Many authors have studied families of codes for which it is possible to develop methods to find PD-sets with respect to certain types of information sets. in all cases the techniques used depend on family which is being studied. We are interested in the family of abelian codes. Some important families of codes are abelian, for instance: cyclic codes, Reed-Muller codes, extended Reed-Solomon codes and others.

The existence of PD-sets relies on the information set considered as reference. In fact, it may happen that for an error correcting code the selection of the information set causes the non-existence of a PD-set. Hence the importance of methods and algorithms to construct information sets. In the case of cyclic codes, McWilliams uses the well-known fact that for a cyclic code of dimension k, any selection of k consecutive positions defines an information set. In [10], H. Imai gave a method to obtain information sets for binary two dimensional cyclic (TDC) codes of odd area. Later, S. Sakata [16] gave an alternative method for the same purpose. Imai's algorithm relies on the structure of the roots of the code, while the algorithm of Sakata is somehow based on the division algorithm for polynomials. Up to our knowledge, these are the sole techniques for TDC codes. Following the ideas in the two papers mentioned above, H. Chabanne [7] gave a method to calculate syndromes by using the division algorithm for polymonials in several variables and Groebner basis; by using it he generalized the McWilliam's permutation decoding procedure. The techniques used by Chabanne involve a generalization of the information sets obtained by Sakata to binary abelian codes.

In [3] we presented a method for constructing information sets valid for every semisimple abelian code, not necessarily binary. It is based on the computation of the cardinalities of certain cyclotomic cosets on different extensions of the ground field and it generalizes Imai's method in the case of TDC codes. Such cosets are completely determined by the structure of the defining set of the code. This technique allows us to design codes with suitable information sets in order to use permutation decoding (see [4]).

In this paper we find sufficient conditions for an abelian code, viewed as an ideal of a multivariate polynomial quotient ring, to have a PD-set contained in the translations associated to each variable. Moreover, the goal of this paper is that such conditions may be written solely in terms of the q-cyclotomic structure of the defining set of abelian codes (see below for all definitions).

In Section II we review basic facts about abelian codes and permutation decoding. In Section III we reproduce without proofs the construction of sets of check positions (and hence information sets) given in [3]. In Section IV, we apply the results of the previous section to get sets of check positions for a code $\mathcal{C}$ and its dual $\mathcal{C}^{\perp}$. Then, as a first part of our main results, we study the relationship between them, which we denote by $\Gamma(\mathcal{C})$ and $\Gamma(\mathcal{C}^{\perp})$ respectively. More precisely, we show that there exists a simple bijection from the complementary set $\Gamma(\mathcal{C})^c$ to $\Gamma(\mathcal{C}^{\perp})$ (Theorem 14). Among other applications, this allows us to show that it is equivalent to use one or the other in order to determine a PD-set. We also show that the set $\Gamma(\mathcal{C}^{\perp})$ may be determined from the complement of the set of roots of $\mathcal{C}$ (Corollary 11). In Section V we include the second part of our

An extended abstract of this paper, with the same title, appears in the proceedings of 2012 IEEE International Symposium on Information Theory (ISIT'2012), Cambridge, Mass.

Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia. Spain.
email: josejoaquin.bernal@um.es, jsimon@um.es

Partially supported by MINECO (Ministerio de Economía y Competitividad), (Fondo Europeo de Desarrollo Regional) project MTM2012-35240 and Fundación Séneca of Murcia.

main results, namely, we give sufficient conditions for a semisimple abelian code to have a partial PD-set in the set of those translations associated to each variable. These conditions make use of the previous results about the dual code (Theorems 21, 22, 23 and Proposition 26). Finally, Section VI contains applications that show us how we may use the conditions obtained to design and exhibit codes that improve the parameters of best known permutation decodable abelian codes for certain lengths.

II. Preliminaries

Throughout $\mathbb{F}$ denotes the field with q elements where q is a power of a prime p. Let $\mathcal{C}$ be a linear code of dimension k, and length l over the field $\mathbb{F}$, that is, a subspace of $\mathbb{F}^l$ with dimension k. We call the elements of $\mathcal{C}$ codewords. An information set for $\mathcal{C}$ is a set of positions $\{i_1,\dots,i_k\}\subseteq\{1,\dots,l\}$ such that restricting the codewords to these positions we get the whole space $\mathbb{F}^k$. For every codeword the symbols in the positions corresponding to an information set are called information symbols and the other $l-k$ positions are called check positions [13]. A generator matrix for $\mathcal{C}$ is a $k\times l$ matrix G whose rows form a basis for $\mathcal{C}$. We say that G is in standard form if it is of the form $[I_k \mid A]$, where I_k is the identity matrix of order k. We denote by $\mathcal{C}^\perp$ the dual code of $\mathcal{C}$ under the ordinary inner product, that is, $\mathcal{C}^\perp=\{v\in\mathbb{F}^l \mid u\cdot v=0 \text{ for all } u\in\mathcal{C}\}$. A parity check matrix for $\mathcal{C}$ is a generator matrix for $\mathcal{C}^\perp$. If G is a generator matrix in standard form, it is easy to check that $H=[-A^T \mid I_{l-k}]$ is a parity check matrix. In this case we say that H is also in standard form.

As usual, for any codeword $c\in\mathcal{C}$ we denote its support by $supp(c)$; that is, the set of its non-zero entries. We consider the parameter $t=\left\lfloor\frac{d-1}{2}\right\rfloor$, where d is the minimum distance of $\mathcal{C}$, that measures the error-correction capability of $\mathcal{C}$. Then we say that $\mathcal{C}$ is an $[l,k]$ t-error-correcting code.

We see the group of permutations on l symbols, S_l, acting on $\mathbb{F}^l$ via $\sigma(c_1,\dots,c_l)=\left(c_{\sigma^{-1}(1)},\dots,c_{\sigma^{-1}(l)}\right)$ with $\sigma\in S_l$. Then the permutation automorphism group of $\mathcal{C}$ is

$$\mathrm{PAut}(\mathcal{C})=\{\sigma\in S_l \mid \sigma(\mathcal{C})=\mathcal{C}\}.$$

Two linear codes $\mathcal{C}$ and $\mathcal{C}'$ are said to be permutation equivalent if there exists $\sigma\in S_l$ such that $\sigma(\mathcal{C})=\mathcal{C}'$. It is easy to see that any linear code is permutation equivalent to a code which has a generator matrix in standard form.

Now, we recall some basic facts about the family of abelian codes and their permutation automorphisms (the reader may see [1] for details).

A. Abelian codes

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

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

We denote this quotient algebra by $\mathbb{A}(r_1,\dots,r_n)$. So, we identify the codewords with polynomials $P(X_1,\dots,X_n)$ 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 $P\in\mathbb{A}(r_1,\dots,r_n)$ as $P=P(X_1,\dots,X_n)=\sum a_{\mathbf{j}}X^{\mathbf{j}}$, where $\mathbf{j}=(j_1,\dots,j_n)\in\mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n}$ 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 always assume that $\gcd(r_i,q)=1$ for every $i=1,\dots,n$.

Our construction makes use of the structure of roots of the ideals in $\mathbb{A}(r_1,\dots,r_n)$; so let us recall some basic facts about it. For a fixed primitive r_i-th root of unity α_i in some extension of $\mathbb{F}$, $i=1,\dots,n$, every abelian code $\mathcal{C}$ in $\mathbb{A}(r_1,\dots,r_n)$ is totally determined by its *root* set,

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

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

$$\begin{aligned}D_\alpha(\mathcal{C}) \quad = \quad & \{(a_1,\dots,a_n)\in\mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n} \mid\\ & (\alpha_1^{a_1},\dots,\alpha_n^{a_n})\in\mathcal{Z}(\mathcal{C})\}.\end{aligned}$$

Given an abelian code $\mathcal{C}\subseteq\mathbb{A}(r_1,\dots,r_n)$ with defining set $D_\alpha(\mathcal{C})$ if one chooses different primitive roots of unity, say $\beta=\{\beta_1,\dots,\beta_n\}$, 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 brevity, we refer to abelian codes without any mention to the primitive roots that we are using as reference, and we denote the defining set of $\mathcal{C}$ by $D(\mathcal{C})$.

Recall that, for $\gamma\in\mathbb{N}$, the q^γ-cyclotomic coset of an integer a modulo r is the set

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

We extend the concept of q-cyclotomic coset of an integer to several components.

Definition 1. *Given an element $(a_1,\dots,a_n)\in\mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n}$, we define its q-orbit modulo $(r_1,\dots,r_n)$ as*

$$\begin{aligned} Q(a_1,\dots,a_n) &= \left\{\left(a_1\cdot q^i,\dots,a_n\cdot q^i\right) \mid i\in\mathbb{N}\right\}\subseteq \\ &\quad \mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n}. \end{aligned}$$

It is easy to see that for every abelian code $\mathcal{C}\subseteq\mathbb{A}(r_1,\dots,r_n)$, $D\left(\mathcal{C}\right)$ 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 $(r_1,\dots,r_n)$. Conversely, every union of q-orbits modulo $(r_1,\dots,r_n)$ defines an abelian code in $\mathbb{A}(r_1,\dots,r_n)$. For the sake of simplicity we only write q-orbit, and the tuple of integers will be clear from the context. The structure of q-orbits of the defining set is the essential ingredient for our algorithm of construction of information sets, which will be described in Section III.

B. Permutation decoding

This decoding algorithm was introduced by F. J. MacWilliams in [14]. The method is described fully in [15] and [9]. For a fixed information set of a given linear code $\mathcal{C}$, this technique uses a special set of permutation automorphisms of the code called PD-set.

Definition 2. *Let $\mathcal{C}$ be an $[l,k]$ t-error-correcting 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. In case $s=t$, we say that P is a PD-set (see [12], [14]).*

Given a t-error-correcting code with a PD-set with respect to some information 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 vector with weight less or equal than t are correct. We denote the Hamming weight of a vector $v\in\mathbb{F}^l$ by $wt(v)$.

Theorem 3 ([9], Theorem 8.1)**.** *Let $\mathcal{C}$ be an $[l,k]$ t-error-correcting 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 $wt\left(Hr^T\right)\leq t$.*

Once we have found a PD-set $P\subseteq\mathrm{PAut}(\mathcal{C})$ for the given code $\mathcal{C}$ with respect to the information set $\mathcal{I}$, the algorithm of permutation decoding is as follows: take a parity 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 get the redundancy symbols and then we can construct a codeword $c'\in\mathcal{C}$. 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. Moreover, it is clear that the algorithm is more efficient when the PD-set is small.

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 it acting on $\mathbb{A}(r_1,\dots,r_n)$ via $\tau\left(\sum_{\mathbf{j}}a_{\mathbf{j}}X^{\mathbf{j}}\right)=\sum_{\mathbf{j}}a_{\mathbf{j}}X^{\tau(\mathbf{j})}$. From this point of view the permutation automorphism group of an abelian code $\mathcal{C}$ in $\mathbb{A}(r_1,\dots,r_n)$ may be described as

$$\mathrm{PAut}(\mathcal{C})=\left\{\tau\in S_{r_1\times\cdots\times r_n}\mid \tau(\mathcal{C})=\mathcal{C}\right\}.$$

Let T_j be the transformation from $\mathbb{A}(r_1,\dots,r_n)$ into itself, given by $T_j(P)=X_j\cdot P$, for $j=1,\dots,n$. Then it is clear that T_j induces a permutation in $S_{r_1\times\cdots\times r_n}$, which we also denote by T_j, via $T_j\left(i_1,\dots,i_n\right)=(i_1,\dots,i_j+1,\dots,i_n)$. Then $\langle\{T_j\}_{j=1}^n\rangle$ may be viewed as a subgroup of permutation automorphisms for every abelian code in $\mathbb{A}(r_1,\dots,r_n)$. We shall look for PD-sets contained in the subgroup $\langle\{T_j\}_{j=1}^n\rangle$.

III. Information sets in abelian codes

In this section we describe the method for the construction of sets of check positions for abelian codes (not necessarily binary) given in [4]. It depends solely on the defining set of the code. The reader may see the mentioned paper for details.

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

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

and

$$m\left(e\right)=\left|C_{(q',r_j)}(e_j)\right|, \tag{1}$$

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

As we have noted, in the semisimple case every defining set of 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 parameters (1) on a special set of representatives of the q-orbits. In fact, the representatives must satisfy the conditions given by the following definition.

Definition 4. *Let D be a union of q-orbits modulo $(r_1,\ldots,r_n)$ and fix an 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 represantives****, 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 a union of q-orbits always exist. Moreover, the construction of the information set does not depend on the selection on the representatives (see [4]). However, 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 the q-orbits in $D(\mathcal{C})$, with respect to the default ordering on the indeterminates. As before, for each $1\le i\le n$, we denote by $D_i(\mathcal{C})$ and $\overline{D}_i(\mathcal{C})$ the projection onto the first i-coordinates of $D(\mathcal{C})$ and $\overline{D}(\mathcal{C})$ respectively.

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

$$R(e)=\{a\in\mathbb{Z}_{r_{i+1}}\mid(e,a)\in\overline{D}_{i+1}(\mathcal{C})\},\tag{2}$$

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

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

$$M(e)=\sum_{a\in R(e)}m\left(e,a\right)\tag{3}$$

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

$$f[1]>\cdots>f[s]>0=f[s+1],\tag{4}$$

that is, we denote by $f[s]$ the minimun value of the parameters $M(\cdot)$ 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 $n\ge3$. Then we continue as follows:

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

$$\Omega_u(e)=\{a\in R(e)\mid M(e,a)\ge f[u]\}$$

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 and we get the sequence

$$f[u,1]>\cdots>f[u,s(u)]>0=f[u,s(u)+1],$$

where $f[u,s(u)]$ denotes the minimum value of the parameters $\mu_u(\cdot)$ 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, when $n-1>j\geq 1$. For the sake of brevity, in what follows we denote $\delta = n-j+2$.

$$\begin{aligned}&\{f[u_n,\dots,u_\delta,1] > \cdots > f[u_n,\dots,u_\delta,s(u_n,\dots,u_\delta)] >\\ &\quad > 0 = f[u_n,\dots,u_\delta,s(u_n,\dots,u_\delta)+1] \mid (u_n,\dots,u_\delta)\\ &\qquad \in \Upsilon_j(\mathcal{C})\}\end{aligned}$$

where, for every $i=2,\dots,n$,

$$\begin{aligned}\Upsilon_i(\mathcal{C}) \quad = \quad & \{(u_n,\dots,u_{n-i+2}) \mid 1\leq u_n \leq s \text{ and}\\ & 1 \leq u_\delta \leq s(u_n,\dots,u_{\delta+1}) \text{ for}\\ & \delta = n-i+2,\dots,n-1\}.\end{aligned} \tag{5}$$

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

$$\begin{aligned}&f[u_n,\dots,u_\delta,1] > \cdots > f[u_n,\dots,u_\delta,s(u_n,\dots,u_\delta)] >\\ &\qquad > 0 = f[u_n,\dots,u_\delta,s(u_n,\dots,u_\delta)+1].\end{aligned}$$

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

$$\Omega_{u_n,\dots,u_\delta,u}(e) = \{a \in R(e) \mid \mu_{u_n,\dots,u_\delta}(e,a) \geq f[u_n,\dots,u_\delta,u]\}$$

and

$$\mu_{u_n,\dots,u_\delta,u}(e) = \sum_{a\in\Omega_{u_n,\dots,u_\delta,u}(e)} m(e,a).$$

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

$$\begin{aligned}f[u_n,\dots,u_\delta,u,1] \quad &> \quad \cdots > f[u_n,\dots,u_\delta,u,s(u_n,\dots,u_\delta,u)]\\ &> \quad 0 = f[u_n,\dots,u_\delta,u,s(u_n,\dots,u_\delta,u)+1],\end{aligned}$$

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

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

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

$$g[u_n,\dots,u_2] = \begin{cases} \displaystyle\sum_{\substack{e\in\overline{D}_1(\mathcal{C})\\ M(e)\geq f[u_2]}} m(e) & \text{if } n=2,\\[2ex] \displaystyle\sum_{\substack{e\in\overline{D}_1(\mathcal{C})\\ \mu_{u_n,\dots,u_3}(e)\geq\\ f[u_n,\dots,u_2]}} m(e) & \text{if } n>2.\end{cases} \tag{6}$$

So the last family of sequences is

$$\begin{aligned}&\{g[u_n,\dots,u_3,1] < \cdots < g[u_n,\dots,u_3,s(u_n,\dots,u_3)] <\\ &< g[u_n,\dots,u_3,s(u_n,\dots,u_3)] \mid (u_n,\dots,u_3) \in \Upsilon_{n-1}(\mathcal{C})\}\,.\end{aligned} \tag{7}$$

The algorithm yields the following set

$$\begin{aligned}\Gamma(\mathcal{C}) \quad = \quad & \{(i_1,\dots,i_n) \in \mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n} \mid\\ & \text{there exists } \ (u_n,\dots,u_2) \in \Upsilon_n(\mathcal{C}) \text{ such that}\\ & f[u_n,\dots,u_j+1] \leq i_j < f[u_n,\dots,u_j],\\ & \text{for } j=2,\dots,n, \text{ and } 0 \leq i_1 < g[u_n,\dots,u_2]\}.\end{aligned} \tag{8}$$

The following theorem, proved in [4], establishes that $\Gamma(\mathcal{C})$ is a set of check positions for $\mathcal{C}$.

Theorem 5 ([4]). *Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1,\dots,r_n)$. Assume that $\gcd(r_i,q)=1$, for every $i=1,\dots,n$, and $n\geq 2$. Then $\Gamma(\mathcal{C})$ is a set of check positions for $\mathcal{C}$.*

We conclude this section with an example which will be referred to later.

Example 6. Let $q = 2$, $n = 2$, $r_1 = 7$, $r_2 = 5$, and consider the abelian code $\mathcal{C}$ with the following defining set with respect to certain roots of unity:

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

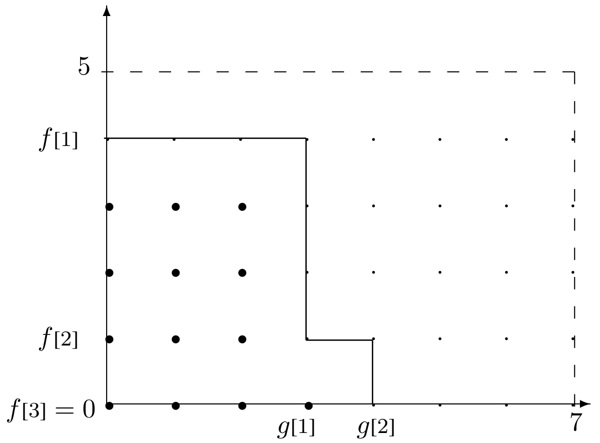
We choose $\overline{D}(\mathcal{C}) = \{(0,0),\,(1,1)\}$ as a complete set of restricted representatives (see Definition 4). Then, by following (1) and (3) we compute $M(0) = 1,\ M(1) = 4$ and $m(0) = 1,\ m(1) = 3$. Using these values we may get the sequences

$$f[1] = 4 > f[2] = 1 > f[3] = 0$$

and

$$g[1] = 3 < g[2] = 4$$

which correspond to (4) and (6) respectively. We use them to produce the marks in the following picture.



So, a set of check positions for $\mathcal{C}$ is (see (8))

$$\begin{aligned} \Gamma(C) = \quad & \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2), \\ & (1,3),(2,0),(2,1),(2,2),(2,3),(4,0)\}. \end{aligned}$$

IV. Dual code

For any abelian code $\mathcal{C}$ in $\mathbb{A}\,(r_1,\ldots,r_n)$, we denote by $\mathcal{C}^\perp$ its dual code. By the previous section, we know that $\Gamma\left(\mathcal{C}^\perp\right)$ and the complementary set $\Gamma(\mathcal{C})^c \subseteq \prod_{i=1}^n \mathbb{Z}_{r_i}$ are information sets for $\mathcal{C}$. In this section, we will see that these information sets may be identified; that is, we will prove that there is a permutation $\kappa \in S_{r_1\times\cdots\times r_n}$ such that for any abelian code $\mathcal{C}$, $\kappa \in \mathrm{PAut}(\mathcal{C})$ and, furthermore, $\kappa\left(\Gamma(\mathcal{C})\right) = \Gamma\left(\mathcal{C}^\perp\right)^c$. Using this, we will conclude that, in order to apply the permutation decoding algorithm, both sets are equivalent. This fact will be used in the following section.

Now, to relate information sets of abelian codes and their duals we need to determine both sets of check positions with some notational compatibility. For this reason, we are going to add to the construction of $\Gamma(\mathcal{C})$ some "trivial" values of the parameters used. As the reader will see, they do not imply any changes in the information sets obtained. We note that this variant in the definition of the set of check positions will be used exclusively in this section.

So we begin by considering an abelian code $\mathcal{C}$ with defining set $D(\mathcal{C})$ with respect to certain primitive roots of unity. To avoid any confusion with the original definition of $\Gamma(\mathcal{C})$ we will make a change on the symbols used to determine it. The new set determined by the new parameters will be denoted by $\widehat{\Gamma}(\mathcal{C})$. Later, we will see that they coincide.

Now we choose a set of restricted representatives $\overline{D}$ of the q-orbits of the whole set $D = \mathbb{Z}_{r_1} \times \ldots \times \mathbb{Z}_{r_n}$ as in Definition 4. Then, in order to construct $\Gamma(\mathcal{C})$, we take the set $\overline{D}(\mathcal{C}) = \overline{D} \cap D(\mathcal{C})$ as our set of restricted representatives of the q-orbits of $D(\mathcal{C})$. Recall that we are considering as default ordering that given by $X_1 < \cdots < X_n$. For every $i \in \{1,\ldots,n-1\}$, let us denote by $\overline{D}_i$ and $\overline{D}_i(\mathcal{C})$, the image of the projection onto the first i-coordinates of $\overline{D}$ and $\overline{D}(\mathcal{C})$, respectively. For any $1 \le i \le n-1$ and $e \in \overline{D}_i$, we define

$$\begin{aligned} R_0(e) \quad &= \quad \left\{a \in \mathbb{Z}_{r_{i+1}} \mid (e,a) \in \overline{D}_{i+1}\right\} \quad \text{and} \\ \widehat{R}(e) \quad &= \quad \left\{a \in \mathbb{Z}_{r_{i+1}} \mid (e,a) \in \overline{D}_{i+1}(\mathcal{C})\right\}. \end{aligned}$$

Under this notation, $e \in \overline{D}_i(\mathcal{C})$ if and only if $\emptyset \neq \widehat{R}(e)$, and in this case $\widehat{R}(e) = R(e)$, where $R(e)$ has been defined in (2).

Again, the algorithm is based on the computation of n families of sequences of natural numbers. For each $e \in \overline{D}_{n-1}$, set

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

Note that, from (3) we have that $e \in \overline{D}_{n-1}(\mathcal{C})$ if and only if $0 \neq \widehat{M}(e) = M(e)$. Then, we order the different values $\widehat{M}(\cdot)$ and we define

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

So we obtain a sequence as in (4)

$$r_n = \widehat{f}[0] \geq \widehat{f}[1] > \cdots > \widehat{f}[t] \geq \widehat{f}[t+1] = 0, \tag{9}$$

where $\widehat{f}[0] = r_n$ and $\widehat{f}[t+1] = 0$ by definition. In this case, $t = s$ if and only if $D_{n-1} = \overline{D}_{n-1}(\mathcal{C})$ and $t = s+1$, otherwise, that is, if and only if, there exists $e \in \overline{D}_{n-1} \setminus \overline{D}_{n-1}(\mathcal{C})$ for which $\widehat{M}(e) = 0$.

The sequence given in (9) is the initial one for any value of n and it defines the first family. Now, suppose that $n \geq 3$. Then, for each $0 \leq u \leq t$ and $e \in \overline{D}_{n-2}$ we define

$$\begin{aligned} \widehat{\Omega}_0(e) &= \emptyset, \\ \widehat{\Omega}_u(e) &= \left\{ a \in R_0(e) \mid \widehat{M}(e,a) \geq \widehat{f}[u] \right\}, \end{aligned}$$

whenever $u \neq 0$, and

$$\widehat{\mu}_u(e) = \sum_{a \in \widehat{\Omega}_u(e)} m(e,a).$$

Note that $\widehat{\mu}_0(e) = 0$ and $\widehat{\mu}_t(e) = r_{n-1}$, for all $e \in \overline{D}_{n-2}$, and it may happen that $\widehat{\mu}_u(e) = 0$ even if $e \in \overline{D}_{n-2}(\mathcal{C})$.

Then we define

$$\begin{aligned} \widehat{f}[u,1] &= \max_{e \in \overline{D}_{n-2}} \{\widehat{\mu}_u(e)\} \qquad \text{and} \\ \widehat{f}[u,i] &= \max_{e \in \overline{D}_{n-2}} \{\widehat{\mu}_u(e) \mid \widehat{\mu}_u(e) < f[u,i-1]\}. \end{aligned}$$

Then we obtain the family of sequences (one for each $u \in \{0, \ldots, t\}$)

$$\begin{aligned} \{ \quad & r_{n-1} = \widehat{f}[u,0] \geq \widehat{f}[u,1] > \cdots > \widehat{f}[u,t(u)] \geq \\ & \widehat{f}[u,t(u)+1] = 0 \mid 0 \leq u \leq t \quad \}, \end{aligned}$$

where $\widehat{f}[u,t(u)]$ denotes the minimum value of the parameters $\widehat{\mu}_u(\cdot)$ and the equalities $\widehat{f}[u,t(u)+1] = 0, \widehat{f}[u,0] = r_{n-1}$ are given by definition.

In a similar way to Section III we describe how to define a family of sequences from the previous ones. Suppose that we have constructed the j-th family, when $n-1 > j \geq 1$. For the sake of brevity, in what follows we denote $\delta = n-j+2$.

$$\begin{aligned} &\Big\{ r_{\delta-1} = \widehat{f}[u_n, \ldots, u_\delta, 0] \geq \widehat{f}[u_n, \ldots, u_\delta, 1] > \ldots \\ &\widehat{f}[u_n, \ldots, u_\delta, t(u_n, \ldots, u_\delta)] > 0 = \widehat{f}[u_n, \ldots, u_\delta, t(u_n, \ldots, u_\delta)+1] \\ &\mid (u_n, \ldots, u_\delta) \in \widehat{\Upsilon}_j(\mathcal{C}) \Big\}, \end{aligned}$$

where, for every $i = 2, \ldots, n$,

$$\begin{aligned} \widehat{\Upsilon}_i(\mathcal{C}) \quad = \quad & \{(u_n, \ldots, u_{n-i+2}) \mid 0 \leq u_n \leq t \text{ and} \\ & 0 \leq u_\delta \leq t(u_n, \ldots, u_{\delta+1}) \text{ for} \\ & \delta = n-i+2, \ldots, n-1\}. \end{aligned} \tag{10}$$

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

$$\begin{aligned} &r_{\delta-1} = \widehat{f}[u_n, \ldots, u_\delta, 0] \geq \widehat{f}[u_n, \ldots, u_\delta, 1] > \ldots \\ &\widehat{f}[u_n, \ldots, u_\delta, t(u_n, \ldots, u_\delta)] > 0 = \widehat{f}[u_n, \ldots, u_\delta, t(u_n, \ldots, u_\delta)+1]. \end{aligned}$$

Take $u \in \{0, \dots, t(u_n, \dots, u_\delta)\}$. Then, for every $e \in \overline{D}_{n-j-1}$ we define

$$\begin{aligned} \widehat{\Omega}_{u_n,\dots,u_\delta,0}(e) &= \emptyset, \\ \widehat{\Omega}_{u_n,\dots,u_\delta,u}(e) &= \{a \in R_0(e) \mid \widehat{\mu}_{u_n,\dots,u_\delta}(e,a) \\ &\qquad \geq \widehat{f}[u_n, \dots, u_\delta, u]\}, \end{aligned} \tag{11}$$

whenever $u \neq 0$, and

$$\widehat{\mu}_{u_n,\dots,u_\delta,u}(e) = \sum_{a \in \widehat{\Omega}_{u_n,\dots,u_\delta,u}(e)} m(e,a).$$

By ordering the values above, we get

$$\begin{aligned} & r_{n-j} = \widehat{f}[u_n, \dots, u_\delta, u, 0] \geq \widehat{f}[u_n, \dots, u_\delta, u, 1] > \dots \\ & \widehat{f}[u_n, \dots, u, t(u_n, \dots, u)] \geq \widehat{f}[u_n, \dots, u, t(u_n, \dots, u) + 1] = 0, \end{aligned}$$

with the first and last equalities given by definition. Then we obtain the $(j+1)$-th family of sequences

$$\begin{aligned} \{ \quad & r_{n-j} = \widehat{f}[u_n, \dots, u_{n-j+1}, 0] \geq \widehat{f}[u_n, \dots, u_{n-j+1}, 1] > \dots \\ & \widehat{f}[u_n, \dots, u_{n-j+1}, t(u_n, \dots, u_{n-j+1})] \geq \\ & \widehat{f}[u_n, \dots, u_{n-j+1}, t(u_n, \dots, u_{n-j+1}) + 1] = 0, \\ & \mid (u_n, \dots, u_{n-j+1}) \in \widehat{\Upsilon}_{j+1}(\mathcal{C}) \quad \}. \end{aligned}$$

We follow the previous process until to get $n-1$ families of sequences. Then, by using all the previous ones, we define the last family. For every $(u_n, \dots, u_2) \in \widehat{\Upsilon}_n(\mathcal{C})$ we set

$$\widehat{g}[u_n, \dots, u_2] = \begin{cases} 0 & \text{if } u_2 = 0 \\ \displaystyle\sum_{\substack{e \in \overline{D}_1 \\ \widehat{M}(e) \geq \widehat{f}[u_2]}} m(e) & \text{if } n = 2, \text{ and } u_2 \neq 0 \\ \displaystyle\sum_{\substack{e \in \overline{D}_1 \\ \widehat{\mu}_{u_n,\dots,u_3}(e) \geq \\ \widehat{f}[u_n,\dots,u_2]}} m(e) & \text{if } n > 2, \text{ and } u_2 \neq 0 \end{cases} \tag{12}$$

Finally, as in Section III, we define

$$\begin{aligned} \widehat{\Gamma}(\mathcal{C}) = \; & \{(i_1, \dots, i_n) \in \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_n} \mid \\ & \text{there exists } (u_n, \dots, u_2) \in \widehat{\Upsilon}_n(\mathcal{C}) \text{ such that} \\ & \widehat{f}[u_n, \dots, u_j + 1] \leq i_j < \widehat{f}[u_n, \dots, u_j], \\ & \text{for } j = 2, \dots, n, \text{ and } 0 \leq i_1 < \widehat{g}[u_n, \dots, u_2]\}. \end{aligned} \tag{13}$$

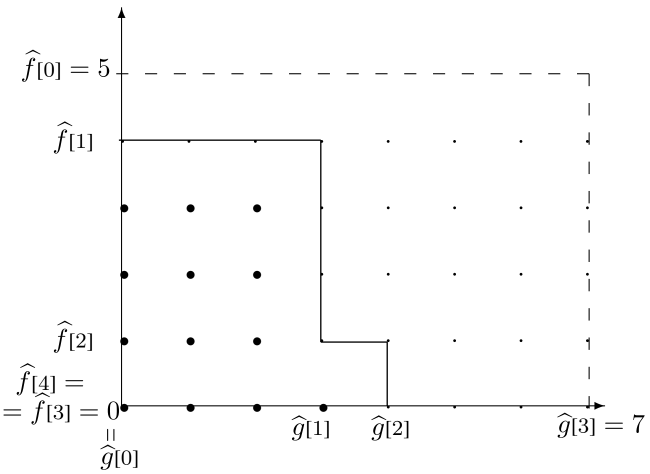
Example 7. Let $q = 2$, $n = 2$, $r_1 = 7$, $r_2 = 5$, and consider the abelian code $\mathcal{C}$ given in Example 6. In this case we choose $\overline{D} = \{(0,0), (0,1), (1,0), (1,1), (3,0), (3,1)\}$ as restricted representatives of the 2-orbits of $D = \mathbb{Z}_7 \times \mathbb{Z}_5$. Then $\overline{D}(\mathcal{C}) = \{(0,0), \; (1,1)\}$. Then we compute $\widehat{M}(0) = 1$, $\widehat{M}(1) = 4$, $\widehat{M}(3) = 0$ and $m(0) = 1$, $m(1) = 3$, $m(3) = 3$. Using these values we get the new sequences

$$\widehat{f}[0] = 5 > \widehat{f}[1] = 4 > \widehat{f}[2] = 1 > \widehat{f}[3] = 0 = \widehat{f}[4]$$

and

$$\widehat{g}[0] = 0 < \widehat{g}[1] = 3 < \widehat{g}[2] = 4 < \widehat{g}[3] = 7.$$

Now, following (13), we get the picture



The reader may check that even though we have added four marks, all of them are superfluos, that is, this picture is the same as that of Example 6.

Now we shall see that, in fact, the sets $\Gamma(\mathcal{C})$ and $\widehat{\Gamma}(\mathcal{C})$ are the same. Let us recall that the values $t(\cdot)$ and $s(\cdot)$ represent the lengths of the sequences involved in the construction of $\Gamma(\mathcal{C})$.

Lemma 8. *Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1,\dots,r_n)$. Let $(v_n,\dots,v_2)\in\Upsilon_n(\mathcal{C})$ (see (5)). Then*
a) $t = s$ or $s+1$ and $f[v_n] = \widehat{f}[v_n] \neq 0$,
and for every $j = 2,\dots,n-1$, the following conditions hold:
b) $t(v_n,\dots,v_{j+1}) = s(v_n,\dots,v_{j+1})$ or $s(v_n,\dots,v_{j+1})+1$,
c) $\widehat{\mu}_{v_n,\dots,v_{j+1}}(e) = \begin{cases} \mu_{v_n,\dots,v_{j+1}}(e) & \text{if } e \in \overline{D}_{j-1}(\mathcal{C}), \\ 0 & \text{if } e \in \overline{D}_{j-1}\setminus\overline{D}_{j-1}(\mathcal{C}), \end{cases}$
d) $f[v_n,\dots,v_j] = \widehat{f}[v_n,\dots,v_j] \neq 0$.
Moreover,
e) $g[v_n,\dots,v_2] = \widehat{g}[v_n,\dots,v_2] \neq 0$.

Proof: Let $D(\mathcal{C})$ denote the defining set of $\mathcal{C}$. Take $\overline{D}$ a restricted set of representatives of the q-orbits of $\mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n}$. Then we choose $\overline{D}(\mathcal{C}) = \overline{D}\cap D(\mathcal{C})$ as a set of restricted representatives of the q-orbits of $D(\mathcal{C})$.

First, note that given $e\in\overline{D}_{n-1}$, we have that $e\in\overline{D}_{n-1}(\mathcal{C})$ if and only if $\widehat{M}(e)\neq 0$, and in this case $\widehat{M}(e) = M(e)$. This implies that $t = s$ if and only if $\overline{D}_{n-1} = \overline{D}_{n-1}(\mathcal{C})$ and $t = s+1$ otherwise. Moreover, in the former case, $\widehat{f}[t] = \widehat{f}[t+1] = 0$. So, for all $u\in\{1,\dots,s\}$ one has that $0\neq f[u] = \widehat{f}[u]$ and $f[u+1] = \widehat{f}[u+1]$. This gives us a).

Now, take $(v_n,\dots,v_2)\in\Upsilon_n(\mathcal{C})$. We are going to prove that b), c) and d) hold for every $j = 2,\dots,n-1$. We use induction on $n-j$. First, we prove the case $j = n-1$. As we have seen, $\widehat{f}[v_n] = f[v_n]\neq 0$, and so, for every $e\in\overline{D}_{n-2}$, $\widehat{\Omega}_{v_n}(e) = \emptyset$ in case $e\in\overline{D}_{n-2}\setminus\overline{D}_{n-2}(\mathcal{C})$ and $\widehat{\Omega}_{v_n}(e) = \Omega_{v_n}(e)$ in case $e\in\overline{D}_{n-2}(\mathcal{C})$. That is, $\widehat{\mu}_{v_n}(e) = 0$ if $e\in\overline{D}_{n-2}\setminus\overline{D}_{n-2}(\mathcal{C})$ and $\widehat{\mu}_{v_n}(e) = \mu_{v_n}(e)$ if $e\in\overline{D}_{n-2}(\mathcal{C})$. Then, for all $u\in\{1,\dots,s(v_n)\}$ one has that $f[v_n,u] = \widehat{f}[v_n,u]\neq 0$; in particular, $f[v_n,v_{n-1}] = \widehat{f}[v_n,v_{n-1}]\neq 0$. Moreover, $t(v_n) = s(v_n)$ if and only if $\widehat{\Omega}_{v_n}(e)\neq\emptyset$ for every $e\in\overline{D}_{n-2}$, and $t(v_n) = s(v_n)+1$ otherwise. This shows the case $j = n-1$.

Assume that we have proved b), c) and d) for some $j\in\{3,\dots,n-1\}$. Then, let us prove these conditions in the case $j-1$. Applying c) and d) with j, we have that $\widehat{\Omega}_{v_n,\dots,v_j}(e) = \Omega_{v_n,\dots,v_j}(e)$ for every $e\in\overline{D}_{j-2}(\mathcal{C})$, and $\widehat{\Omega}_{v_n,\dots,v_j}(e) = \emptyset$ if $e\in\overline{D}_{j-2}\setminus\overline{D}_{j-2}(\mathcal{C})$. Hence, we obtain that $\widehat{\mu}_{v_n,\dots,v_j}(e) = \mu_{v_n,\dots,v_j}(e)$, for every $e\in\overline{D}_{j-2}(\mathcal{C})$ and $\widehat{\mu}_{v_n,\dots,v_j}(e) = 0$ if $e\in\overline{D}_{j-2}\setminus\overline{D}_{j-2}(\mathcal{C})$. Then $f[v_n,\dots,v_j,u] = \widehat{f}[v_n,\dots,v_j,u]\neq 0$, for any $u\in\{1,\dots,s(v_n,\dots,v_j)\}$; in particular, $f[v_n,\dots,v_{j-1}] = \widehat{f}[v_n,\dots,v_{j-1}]\neq 0$. This shows b), c) and d). In addition, we have obtained that the equality $t(v_n,\dots,v_j) = s(v_n,\dots,v_j)$ holds if and only if $\widehat{\Omega}_{v_n,\dots,v_j}(e)\neq\emptyset$ for every $e\in\overline{D}_{j-2}$ and $t(v_n,\dots,v_j) = s(v_n,\dots,v_j)+1$ otherwise.

Finally d) follows from the definitions (12) and (6) and from c) and d) with $j = 2$ (if $n = 2$, we use that $\widehat{M}(e) = M(e)\neq 0$ if and only if $e\in\overline{D}_{n-1}(\mathcal{C})$). ■

Proposition 9. *Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1,\dots,r_n)$. Let $\Gamma(\mathcal{C})$ and $\widehat{\Gamma}(\mathcal{C})$ the sets of check positions defined in (8) and (13) respectively. Then $\Gamma(\mathcal{C}) = \widehat{\Gamma}(\mathcal{C})$.*

Proof: Let $D(\mathcal{C})$ be the defining set of $\mathcal{C}$. Recall that the set $\Gamma(\mathcal{C})$ does not depend on the choice of the restricted set of representatives of the q-orbits of $D(\mathcal{C})$. Take $\overline{D}$ a restricted set of representatives of the q-orbits of $\mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n}$. Then we choose $\overline{D}(\mathcal{C}) = \overline{D}\cap D(\mathcal{C})$ as a set of restricted representatives of the q-orbits of $D(\mathcal{C})$ and we construct $\Gamma(\mathcal{C})$ and $\widehat{\Gamma}(\mathcal{C})$.

First, let us note that by using a) and b) in Lemma 8 we have that $\Upsilon_n(\mathcal{C})\subseteq\widehat{\Upsilon}_n(\mathcal{C})$. Indeed, if $(v_n,\dots,v_2)\in\Upsilon_n(\mathcal{C})$ then $0\leq v_n\leq s\leq t$ and $0\leq v_i\leq s(v_n,\dots,v_{i+1})\leq t(v_n,\dots,v_{i+1})$, with $i = 2,\dots,n-1$. This implies that $(v_n,\dots,v_2)\in\widehat{\Upsilon}_n(\mathcal{C})$.

Now, we are going to prove that $\Gamma(\mathcal{C}) \subseteq \widehat{\Gamma}(\mathcal{C})$. To do this we take $(i_1, \dots, i_n) \in \Gamma(\mathcal{C})$. Then there exists $(v_n, \dots, v_2) \in \Upsilon_n(\mathcal{C})$ such that

$$f[v_n, \dots, v_j] > i_j \geq f[v_n, \dots, v_j + 1],$$

for every $j = 2, \dots, n$, and

$$0 \leq i_1 < g[v_n, \dots, v_2].$$

So, by the previous paragraph, $(v_n, \dots, v_2) \in \widehat{\Upsilon}_n(\mathcal{C})$. By applying $a)$, $d)$ and $e)$ in Lemma 8 we have that $\widehat{f}[v_n, \dots, v_j] > i_j \geq \widehat{f}[v_n, \dots, v_j + 1]$, for every $j = 2, \dots, n$, and $0 \leq i_1 < \widehat{g}[v_n, \dots, v_2]$. Therefore, $(i_1, \dots, i_n) \in \widehat{\Gamma}(\mathcal{C})$.

Let us see the inclusion $\widehat{\Gamma}(\mathcal{C}) \subseteq \Gamma(\mathcal{C})$. Let $(i_1, \dots, i_n) \in \widehat{\Gamma}(\mathcal{C})$. Then there exists $(v_n, \dots, v_2) \in \widehat{\Upsilon}_n(\mathcal{C})$ such that

$$\widehat{f}[v_n, \dots, v_j] > i_j \geq \widehat{f}[v_n, \dots, v_j + 1],$$

for every $j = 2, \dots, n$, and

$$0 \leq i_1 < \widehat{g}[v_n, \dots, v_2].$$

We will prove that $(v_n, \dots, v_2) \in \Upsilon_n(\mathcal{C})$. We claim that $v_j \neq 0$ for every $j = 2, \dots, n$. Assume that this is not true and let j_0 be the minimum in $\{2, \dots, n\}$ such that $v_{j_0} = 0$. Since $0 \leq i_1 < \widehat{g}[v_n, \dots, v_2]$ and $\widehat{g}[v_n, \dots, v_3, 0] = 0$, by the definition (12), we have that $j_0 > 2$. Then, by using (11) we have that $\widehat{\mu}_{v_n, \dots, v_{j_0+1}, 0}(e) = 0$, for every $e \in \overline{D}_{j_0 - 2}$, and hence $t(v_n, \dots, v_{j_0+1}, 0) = 1$. So we get the following sequence

$$\begin{aligned} r_{j_0 - 1} = \widehat{f}[v_n, \dots, v_{j_0+1}, 0, 0] > \widehat{f}[v_n, \dots, v_{j_0+1}, 0, 1] = \\ = \widehat{f}[v_n, \dots, v_{j_0+1}, 0, 2] = 0. \end{aligned}$$

This implies that $\widehat{f}[v_n, \dots, v_{j_0+1}, 0, 1] \leq i_{j_0 - 1} < \widehat{f}[v_n, \dots, v_{j_0+1}, 0, 0]$ an so $v_{j_0 - 1} = 0$. This contradicts the minimality of j_0. Then our claim is proved.

Finally we are going to show that $v_n \neq s + 1$ and $v_j \neq s(v_n, \dots, v_{j+1}) + 1$, for every $j = 2, \dots, n$. Suppose that there exists j_0 the minimum in $\{2, \dots, n\}$ such that eihter $v_n = s + 1$, in case $j_0 = n$, or $v_{j_0} = s(v_n, \dots, v_{j_0+1}) + 1$. If $j_0 = n$ then $v_n = s + 1$ and so, by using Lemma 8 $a)$, we have that $v_n = t$ and $0 = \widehat{f}[t + 1] = \widehat{f}[t]$. This is a contradiction because $\widehat{f}[t + 1] \leq i_n < \widehat{f}[t] = f[s + 1] = 0$. Let us assume that $j_0 < n$, then $v_{j_0} = s(v_n, \dots, v_{j_0+1}) + 1 = t(v_n, \dots, v_{j_0+1})$. Hence $0 = \widehat{f}[v_n, \dots, v_{j_0+1}, t(v_n, \dots, v_{j_0+1})] = f[v_n, \dots, v_{j_0+1}, t(v_n, \dots, v_{j_0+1}) + 1]$. This contradicts that

$$\begin{aligned} &\widehat{f}[v_n, \dots, t(v_n, \dots, v_{j_0+1}) + 1] \leq i_{j_0} < \\ &f[v_n, \dots, t(v_n, \dots, v_{j_0+1})] = \widehat{f}[v_n, \dots, s(v_n, \dots, v_{j_0+1}) + 1] = 0. \end{aligned}$$

Thus, we have proved that $(v_n, \dots, v_2) \in \Upsilon_n(\mathcal{C})$. Now, by applying $a)$, $d)$ and $e)$ in Lemma 8 we have that $f[v_n, \dots, v_j] > i_j \geq f[v_n, \dots, v_j + 1]$, for every $j = 2, \dots, n$, and $0 \leq i_1 < g[v_n, \dots, v_2]$. This implies that $(i_1, \dots, i_n) \in \Gamma(\mathcal{C})$ and we are done. ■

Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1, \dots, r_n)$ with defining set $D(\mathcal{C})$ with respect to certain choice of roots of unity. Then we define

$$-D(\mathcal{C}) = \{(r_1 - e_1, \dots, r_n - e_n) \mid (e_1, \dots, e_n) \in D(\mathcal{C})\},$$

and we denote by $\mathcal{C}^{-1}$ the code with defining set $-D(\mathcal{C})$ with respect to the same set of roots of unity, that is, $D(\mathcal{C}^{-1}) = -D(\mathcal{C})$. One may check that $D(\mathcal{C})$ and $-D(\mathcal{C})$ have the same q-orbits structure, and so they yield the same parameters $m(\cdot)$ (see (1)). Therefore, $\Gamma(\mathcal{C}) = \Gamma(\mathcal{C}^{-1})$ (see (8)).

The following lemma is well known. It establishes the relationship between the defining sets of $\mathcal{C}^{-1}$ and $\mathcal{C}^{\perp}$ respectively. The reader may find a proof in [13, p. 836].

Lemma 10. *Let $\widetilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ be a choice of primitive roots of unity. Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1, \dots, r_n)$ with defining set $D_{\widetilde{\alpha}}(\mathcal{C})$, and let $\mathcal{C}^{\perp}$ denote the dual code. Then*

$$D_{\widetilde{\alpha}}(\mathcal{C}^{\perp}) = (\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}) \setminus D_{\widetilde{\alpha}}(\mathcal{C}^{-1}).$$

Given $\mathcal{C}$ an abelian code in $\mathbb{A}(r_1, \dots, r_n)$ with defining set $D(\mathcal{C})$ with respect to certain roots of unity, we denote by $\mathcal{C}'$ the abelian code with defining set $D(\mathcal{C}') = (\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}) \setminus D(\mathcal{C})$ with respect to the same choice of roots of unity. The following result follows from Lemma 10 and what we have mentioned above about $\mathcal{C}^{-1}$.

Corollary 11. *Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1, \dots, r_n)$ and let $C^{\perp}$ be its dual code. For a fixed set of primitive roots of unity we have that*

$$\Gamma(\mathcal{C}^{\perp}) = \Gamma(\mathcal{C}').$$

The two previous results say that in order to study the relationship between $\widehat{\Gamma}(\mathcal{C})$ and $\widehat{\Gamma}(\mathcal{C}^{\perp})$ we can use the sets $\widehat{\Gamma}(\mathcal{C})$ and $\widehat{\Gamma}(\mathcal{C}')$. The advantage of using the code $\mathcal{C}'$ instead of $\mathcal{C}^{\perp}$ relies on the fact that we can compute the defining set of $\mathcal{C}'$ and $\mathcal{C}$ at the same time. This allows us to easily relate the respective sets of check positions.

Let us denote by $\widehat{f'}[\cdot]$, $\widehat{g'}[\cdot]$, $\widehat{M'}(\cdot)$, $\widehat{\Omega}'(\cdot)$, $\widehat{\mu}'_{\cdot}(\cdot)$, t' and $t'(\cdot)$, the parameters used in the construction of $\widehat{\Gamma}(\mathcal{C}')$. The Lemma 13 establishes the relationship between these new parameters and that used in the construction of $\widehat{\Gamma}(\mathcal{C})$. First, we need to introduce the following recursive notation.

Notation 12. Given $(u_n,\ldots,u_2)\in\widehat{\Upsilon}_n(\mathcal{C})$ (see (10)) we define

$$\omega_1(u_n)=t'-u_n.$$

Suppose that we have defined $\omega_{i-1}(u_n,\ldots,u_{n-i+2})$, with $2\leq i<n$. Then we write ($\delta=n-i+2$)

$$\begin{aligned}&\omega_i(u_n,\ldots,u_{\delta-1})=\\&[\omega_{i-1}(u_n,\ldots,u_\delta),t'\left(\omega_{i-1}(u_n,\ldots,u_\delta)\right)-u_{\delta-1}]\,.\end{aligned}$$

We also set

$$\omega_i^+(u_n,\ldots,u_{\delta-1})=\omega_i(u_n,\ldots,u_i,u_{\delta-1}-1)$$

$$=[\omega_{i-1}(u_n,\ldots,u_\delta),t'\left(\omega_{i-1}(u_n,\ldots,u_\delta)\right)-u_{\delta-1}+1].$$

Lemma 13. *Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1,\ldots,r_n)$. Then, for every $(u_n,\ldots,u_2)\in\widehat{\Upsilon}_n(\mathcal{C})$, we have that*
a) $t=t'$ *y* $t(u_n,\ldots,u_i)=t'(\omega_{n-i+1}(u_n,\ldots,u_i))$*, with* $i=3,\ldots,n$*,*
b) $\widehat{f}[u_n,\ldots,u_i]=r_i-\widehat{f'}[\omega^+_{n-i+1}(u_n,\ldots,u_i)]$*, with* $i=2,\ldots,n$*,*
c) $\widehat{g}[u_n,\ldots,u_2]=r_1-\widehat{g'}[\omega_{n-1}(u_n,\ldots,u_2)]$*.*

Proof: Let $\widetilde{\alpha}=(\alpha_1,\ldots,\alpha_n)$ be a choice of primitive roots of unity. Let us denote $D(\mathcal{C})=D_{\widetilde{\alpha}}(\mathcal{C})$ and $D(\mathcal{C}')=D_{\widetilde{\alpha}}(\mathcal{C}')$, the defining sets of $\mathcal{C}$ and $\mathcal{C}'$ respectively, with respect to $\widetilde{\alpha}$. Let $\overline{D}$ be a set of restricted representatives of the q-orbits of $\mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_n}$. Take

$$\overline{D}(\mathcal{C})=\overline{D}\cap D(\mathcal{C})\ \text{ and }\ \overline{D}(\mathcal{C}')=\overline{D}\cap D(\mathcal{C}')$$

as sets of restricted representatives of the q-orbits of $D(\mathcal{C})$ and $D(\mathcal{C}')$ respectively. Then one has that $\overline{D}(\mathcal{C})\cup\overline{D}(\mathcal{C}')=\overline{D}$, where the union is disjoint. Let us recall that for every $i\in\{1,\ldots,n-1\}$, the images of the projections onto the first i coordinates of $\overline{D},\overline{D}(\mathcal{C})$ and $\overline{D}(\mathcal{C}')$ are denoted by $\overline{D}_i$, $\overline{D}_i(\mathcal{C})$ and $\overline{D}_i(\mathcal{C}')$, respectively.

Then for every $e\in\overline{D}_{n-1}$, we have that $\widehat{M}(e)+\widehat{M'}(e)=r_n$. This implies that $t=t'$ and so, by the definitions of $\widehat{f}[\cdot]$ and $\widehat{f'}[\cdot]$, we obtain *b)* in case $i=n$.

In order to prove the remaining cases in a) and b), we use induction on $n-i$. The key is to prove that for every $i\in\{3,\ldots,n\}$, $(u_n,\ldots,u_i)\in\widehat{\Upsilon}_{n-i+2}(\mathcal{C})$ and $e\in\overline{D}_{i-2}$ the following condition holds

$$\widehat{\mu}_{u_n,\ldots,u_i}(e)+\widehat{\mu'}_{\omega_{n-i+1}(u_n,\ldots,u_i)}(e)=r_{i-1}. \tag{14}$$

Take $(u_n,\ldots,u_2)\in\widehat{\Upsilon}_n(\mathcal{C})$. We are going to prove (14) in case $i=n$ and consequently we will obtain *b)* with $i=n-1$ and *a)* with $i=n$. Let $e\in\overline{D}_{n-2}$. First, suppose that $u_n\neq 0$. For every $a\in R_0(e)$, we have that $a\in R_0(e)\setminus\left(\widehat{\Omega}_{u_n}(e)\right)$ if and only if $\widehat{M}(e,a)<\widehat{f}[u_n]$. Since we have proved b) in case $i=n$, we have that $a\in R_0(e)\setminus\left(\widehat{\Omega}_{u_n}(e)\right)$ if and only if $\widehat{M'}(e,a)>\widehat{f'}[\omega^+_1(u_n)]$. This last inequality is equivalent to $a\in\widehat{\Omega'}_{\omega_1(u_n)}(e)$ because $\widehat{f'}[\omega_1(u_n)]>\widehat{f'}[\omega^+_1(u_n)]=\widehat{f'}[\omega_1(u_n)+1]$. So, $R_0(e)\setminus\left(\widehat{\Omega}_{u_n}(e)\right)=\widehat{\Omega'}_{\omega_1(u_n)}(e)$.

Now, suppose that $u_n=0$. Then $\widehat{\Omega}_0(e)=\emptyset$ and $\omega_1(0)=t=t'$. By the definition of t', we have that $\widehat{M'}(e,a)\geq\widehat{f'}[t']$ for every $a\in R_0(e)$. So $R_0(e)\setminus\left(\widehat{\Omega}_0(e)\right)=R_0(e)=\widehat{\Omega'}_{\omega_1(0)}(e)$. This implies that for every $u_n\in\{0,\ldots,t\}$ and $e\in\overline{D}_{n-2}$ the condition (14) with $i=n$ holds. Hence

$$t(u_n)=t'(\omega_1(u_n))$$

and

$$\widehat{f}[u_n,u_{n-1}]+\widehat{f'}[\omega^+_2(u_n,u_{n-1})]=r_{n-1}.$$

This gives us a) with $i=n$ and b) with $i=n-1$.

Suppose that we have proved (14) for $i=i_0+1$, where $2\leq i_0<n$. Then

$$\widehat{f}[u_n,\ldots,u_{i_0}]+\widehat{f'}[\omega^+_{n-i_0+1}(u_n,\ldots,u_{i_0})]=r_{i_0} \tag{15}$$

and

$$t(u_n,\ldots,u_{i_0+1})=t'(\omega_{n-i_0}(u_n,\ldots,u_{i_0+1})), \tag{16}$$

that is, we have *b)* with $i=i_0$ and *a)* for $i=i_0+1$.

Let us prove (14) with $i=i_0$ and we will obtain *b)* with $i=i_0-1$ and *a)* with $i=i_0$.

Take $e \in \overline{D}_{i_0-2}$. We distinguish in two cases again. First, suppose that $u_{i_0} \neq 0$. Then $a \in R_0(e) \setminus \left(\widehat{\Omega}_{u_n,\dots,u_{i_0}}(e)\right)$ if and only if

$$\widehat{\mu}_{u_n,\dots,u_{i_0+1}}(e,a) < \widehat{f}[u_n,\dots,u_{i_0}],$$

By using (14), with $i = i_0 + 1$, and (15), this is equivalent to

$$\widehat{\mu'}_{\omega_{n-i_0}(u_n,\dots,u_{i_0+1})}(e,a) > \widehat{f'}[\omega^+_{n-i_0+1}(u_n,\dots,u_{i_0})],$$

and this occurs if and only if $a \in \widehat{\Omega'}_{\omega_{n-i_0+1}(u_n,\dots,u_{i_0})}(e)$, because

$$\widehat{f'}[\omega_{n-i_0+1}(u_n,\dots,u_{i_0})] > \widehat{f'}[\omega^+_{n-i_0+1}(u_n,\dots,u_{i_0})].$$

Now, suppose that $u_{i_0} = 0$. Then, $\widehat{\Omega}_{u_n,\dots,u_{i_0+1},0}(e) = \emptyset$ and

$$\begin{array}{l} \omega_{n-i_0+1}(u_n,\dots,u_{i_0+1},0) = \\ \left[\omega_{n-i_0}(u_n,\dots,u_{i_0+1}), t'(\omega_{n-i_0}(u_n,\dots,u_{i_0+1}))\right]. \end{array}$$

By the definition of $t'(\omega_{n-i_0}(u_n,\dots,u_{i_0+1}))$, for every $a \in R_0(e)$ we have that

$$\begin{array}{l} \widehat{\mu'}_{\omega_{n-i_0}(u_n,\dots,u_{i_0+1})}(e,a) \geq \\ \widehat{f'}[\omega_{n-i_0}(u_n,\dots,u_{i_0+1}), t'(\omega_{n-i_0}(u_n,\dots,u_{i_0+1}))]; \end{array}$$

so

$$\begin{array}{l} R_0(e) \setminus \left(\widehat{\Omega}_{u_n,\dots,u_{i_0},0}(e)\right) = R_0(e) = \\ \qquad\qquad \widehat{\Omega'}_{\omega_{n-i_0+1}(u_n,\dots,u_{i_0+1},0)}(e). \end{array}$$

Therefore, we conclude that for every $e \in \overline{D}_{i_0-2}$ we have that

$$\widehat{\mu}_{u_n,\dots,u_{i_0}}(e) + \widehat{\mu'}_{\omega_{n-i_0+1}(u_n,\dots,u_{i_0})}(e) = r_{i_0-1}$$

and then

$$t(u_n,\dots,u_{i_0}) = t'(\omega_{n-i_0+1}(u_l,\dots,u_{i_0}))$$

and

$$\widehat{f}[u_n,\dots,u_{i_0-1}] + \widehat{f'}[\omega^+_{n-i_0+2}(u_n,\dots,u_{i_0-1})] = r_{i_0-1}.$$

This proves (14), *a)* and *b)*.

To finish the proof let us deal with *c)*. From the previous paragraphs,

$$\begin{array}{rcl} \widehat{\mu}_{u_n,\dots,u_3}(e) + \widehat{\mu'}_{\omega_{n-2}(u_n,\dots,u_3)}(e) & = & r_2 \quad \text{and} \\ \widehat{f}[u_n,\dots,u_2] + \widehat{f'}[\omega^+_{n-1}(u_n,\dots,u_2)] & = & r_2, \end{array}$$

then

$$\begin{array}{rcl} r_1 & = & \displaystyle\sum_{e \in \overline{D}_1} m(e) = \\ & = & \displaystyle\sum_{\substack{\{e \in \overline{D}_1 \mid \\ \widehat{\mu}_{u_n,\dots,u_3}(e) \geq \\ \widehat{f}[u_n,\dots,u_2]\}}} m(e) + \sum_{\substack{\{e \in \overline{D}_1 \mid \\ \widehat{\mu}_{u_n,\dots,u_3}(e) < \\ \widehat{f}[u_n,\dots,u_2]\}}} m(e) \\ & = & \displaystyle\sum_{\substack{\{e \in \overline{D}_1 \mid \\ \widehat{\mu}_{u_n,\dots,u_3}(e) \geq \\ \widehat{f}[u_n,\dots,u_2]\}}} m(e) + \sum_{\substack{\{e \in \overline{D}_1 \mid \\ \widehat{\mu}_{\omega_{n-1}(u_n,\dots,u_3)}(e) \geq \\ \widehat{f'}[\omega_{n-1}(u_n,\dots,u_2)]\}}} m(e) \\ & = & \widehat{g}[u_n,\dots,u_2] + \widehat{g'}[\omega_{n-1}(u_n,\dots,u_2)]. \end{array}$$

So we are done.

■

The following theorem is the main result of this section. It gives us the relationship between $\Gamma(\mathcal{C})$ and $\Gamma(\mathcal{C}^\perp)$.

Theorem 14. *Let $\mathcal{C}$ be an abelian code in $\mathbb{A}(r_1,\dots,r_n)$. Let $\kappa : \prod_{i=1}^n \mathbb{Z}_{r_i} \to \prod_{i=1}^n \mathbb{Z}_{r_i}$ be the bijection given by $\kappa(i_1,\dots,i_n) = (r_1 - i_1 - 1,\dots,r_n - i_n - 1)$. Then*

$$\kappa\left(\Gamma(\mathcal{C})\right) = \left(\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}\right) \setminus \Gamma(\mathcal{C}^\perp).$$

Proof: Let $(i_1, \dots, i_n) \in \widehat{\Gamma}(\mathcal{C}) = \Gamma(\mathcal{C})$. Then, there is a list $(u_n, \dots, u_2) \in \Upsilon_n(\mathcal{C})$ satisfying that

$$f[u_n, \dots, u_j + 1] = \widehat{f}[u_n, \dots, u_j + 1] \leq i_j < \\ \widehat{f}[u_n, \dots, u_j] = f[u_n, \dots, u_j],$$

for $j = 2, \dots, n$, and

$$0 \leq i_1 < \widehat{g}[u_n, \dots, u_2] = g[u_n, \dots, u_2].$$

For every $j = 2, \dots, n$ we write $\kappa_j(i_j) = r_j - i_j - 1$. Then

$$r_j - \widehat{f}[u_n, \dots, u_j] - 1 < \kappa_j(i_j) \leq r_j - \widehat{f}[u_n, \dots, u_j + 1] - 1$$

and

$$r_1 - \widehat{g}[u_n, \dots, u_2] - 1 < \kappa_1(i_1) \leq r_1 - 1.$$

Then, by applying Lemma 13 we have that for each $2 \leq j \leq n$,

$$\widehat{f'}[\omega^+_{n-j+1}(u_n, \dots, u_j)] \leq \kappa_j(i_j) < \widehat{f'}[\omega^+_{n-j+1}(u_n, \dots, u_j + 1)], \tag{17}$$

and

$$\widehat{g'}[\omega_{n-1}(u_n, \dots, u_2)] \leq \kappa_1(i_1) < r_1. \tag{18}$$

Now, note that $\omega^+_{n-j+1}(u_n, \dots, u_j + 1) = \omega_{n-j+1}(u_n, \dots, u_j)$. So, by (17) and (13), $(\kappa_1(i_1), \dots, \kappa_n(i_n)) \in \widehat{\Gamma}(\mathcal{C}^\perp)$ if and only if $\kappa_1(i_1) < \widehat{g'}[\omega_{n-1}(u_n, \dots, u_2)]$. But this contradicts (18). Hence $\kappa(\Gamma(\mathcal{C})) \subseteq \Gamma(\mathcal{C}^\perp)^c$. Finally, from the fact that $|\Gamma(\mathcal{C})| = |D(\mathcal{C})|$ (see [3]) and Corollary 11 we have that

$$\left|\Gamma(\mathcal{C}^\perp)^c\right| = |\Gamma(\mathcal{C}')^c| = \prod_{i=1}^{n} r_i - |D(\mathcal{C}')| = \\ = \prod_{i=1}^{n} r_i - \left(\prod_{i=1}^{n} r_i - |D(\mathcal{C})|\right) = |\Gamma(\mathcal{C})|,$$

which yields the reverse inclusion. ■

Note that the bijection κ may be extended to a bijection of $\mathbb{A}(r_1, \dots, r_n)$ via $\kappa(P(X_1, \dots, X_n)) = \sum a_{\kappa^{-1}(\mathbf{j})} X^{\mathbf{j}}$, for every $P(X_1, \dots, X_n) = \sum a_{\mathbf{j}} X^{\mathbf{j}}$. We also denote by κ this extension. It is clear that κ is exactly the composition $T_1^{r_1 - 1} \circ \cdots \circ T_n^{r_n - 1}$ (see Section II for notation) and so it belongs to the permutation automorphism group of every abelian code. Then, Theorem 14 implies that we can use equivalently $\Gamma(\mathcal{C})^{\mathrm{c}}$ or $\Gamma(\mathcal{C}^\perp)$ in order to apply the algorithm of permutation decoding. Indeed, the reader may check that $\mathcal{P} \subseteq \langle T_i \mid i = 1, \dots, n \rangle$ is a partial PD-set for $\mathcal{C}$ and the information set $\Gamma(\mathcal{C}^\perp)^c$ if and only if $\kappa \circ \mathcal{P} \circ \kappa^{-1}$ is a partial PD-set for $\mathcal{C}^\perp$ and the information set $\Gamma(\mathcal{C}^\perp)$.

V. Partial PD-sets for abelian codes

In the following two sections we study how to apply the permutation decoding algorithm to abelian codes by taking as reference the information sets given in the previous sections. Since these information sets depends only on their defining sets, we may construct good abelian codes (in order to apply the permutation decoding algorithm) from a suitable choice of their defining sets (see Section VI). We shall show sufficient conditions to find (partial) PD-sets contained in the subgroup of the permutation automorphisms of any abelian code, generated by the translations $T_j(i_1, \dots, i_n) = (i_1, \dots, i_j + 1, \dots, i_n)$, for $j = 1, \dots, n$, which were introduced in Section II.

As we have seen, for a given abelian code $\mathcal{C}$ in $\mathbb{A}(r_1, \dots, r_n)$ both sets $\Gamma(\mathcal{C})^c$ and $\Gamma\left(\mathcal{C}^\perp\right) (= \Gamma(\mathcal{C}'))$ are information sets that we may use equivalently. We prefer to make use of the set $\Gamma(\mathcal{C}')$ because, on the one hand, we think that in this context the proofs may be written in a simpler form and on the other hand, examples may be also constructed in an easier way, as the reader may check in next section. As we have noted in the previous section, we can compute the defining sets of $\mathcal{C}'$ and $\mathcal{C}$ simultaneously; we can take one or the other as it suits us.

We denote by $f'[\cdot]$, $g'[\cdot]$, $M'(\cdot)$, $\Omega'(\cdot)$, $\mu'_{\cdot}(\cdot)$, s' and $s'(\cdot)$, the parameters used in the construction of $\Gamma(\mathcal{C}')$. It may be necessary to revise this construction in Section III, more precisely the definitions from (4) to (8).

Let $\mathcal{C}$ be an abelian t-error-correcting code in $\mathbb{A}(r_1, \dots, r_n)$ with defining set $D(\mathcal{C})$ and information set $\Gamma(\mathcal{C}')$. Let $b \leq t$ a natural number and let $e \in \mathbb{A}(r_1, \dots, r_n)$ an error vector with $supp(e) = \{p_1, \dots, p_b\} \subseteq \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$. We set $p_j = (p_j^1, \dots, p_j^n)$ for $j = 1, \dots, b$. We are going to use the subgroup $\left\langle \{T_j\}_{j=1}^n \right\rangle$ to move $supp(e)$ outside of $\Gamma(\mathcal{C}')$. Following the notation in Section III, if $p_j \in \Gamma(\mathcal{C}')$, for some $1 \leq j \leq b$, then there exists $(u_n, \dots, u_2) \in \Upsilon_n(\mathcal{C}')$ satisfying $f'[u_n, \dots, u_i + 1] \leq p_j^i < f'[u_n, \dots, u_i]$, for every $i = 2, \dots, n$, and $g'[u_n, \dots, u_2] > p_j^1 \geq 0$. Therefore, in order to move p_j outside of $\Gamma(\mathcal{C}')$, we look for a suitable $T \in \left\langle \{T_j\}_{j=1}^n \right\rangle$ such that $T(p_j) \notin \Gamma(\mathcal{C}')$; that is, such that for $T(p_j)$ there no exist $(u_n, \dots, u_2)$ satisfying the conditions mentioned above. (For instance, the existence of $i \in \{1, \dots, n\}$ and $\alpha \in \mathbb{N}$ such that $f'[u_n, \dots, u_i] \leq p_j^i + \alpha \bmod r_i$ implies that $T_i^\alpha(p_j) \notin \Gamma(\mathcal{C}')$.)

Remark 15. As we have seen in Section III, our information sets depend on the chosen ordering in the indeterminates $X_1, \ldots, X_n$. In this section we will use the default ordering, that is, $X_1 < \cdots < X_n$. The reader may check that all the results can be adapted to any other ordering.

First, we need some technical results and some additional notation. All throughout $\mathcal{C}$ will be an abelian code in $\mathbb{A}\left(r_1, \ldots, r_n\right)$ with defining set $D(\mathcal{C})$ and information set $\Gamma(\mathcal{C}')$.

Notation 16. Let $v = (v_n, \ldots, v_j) \in \Upsilon_{n-j+2}(\mathcal{C}')$, with $j \in \{2, \ldots, n\}$. We define

- $S^0\left(v\right) = v$,
- $S\left(v\right) = (v, s'(v)) = (v_n, \ldots, v_j, s'(v_n, \ldots, v_j))$ (if $n \geq 3$),
  and if we assume that $S^i(v)$ is defined, where $0 \leq i < j-2$, we set
- $S^{i+1}\left(v\right) = \left(S^i(v), s'\left(S^i(v)\right)\right)$.

Finally we define $S^{-1}(v) = (v_n, \ldots, v_{j+1})$, in case $j < n$, and $S^{-1}(v_n) = \emptyset$.

Lemma 17. *Let $h, j \in \mathbb{N}$ such that $2 \leq h \leq j \leq n$. Then for every $(u_n, \ldots, u_2) \in \Upsilon_n(\mathcal{C}')$ and an integer w, such that $u_j \leq w \leq s'(u_n, \ldots, u_{j+1})$, we have that:*

a) $f'[u_n, \ldots, u_{h+1}, u_h] \leq f'[S^{j-1-h}\left(u_n, \ldots, u_{j+1}, w\right), 1]$,

b) $g'[u_n, \ldots, u_2] \leq g'[S^{j-2}\left(u_n, \ldots, u_{j+1}, w\right)]$.

Proof: Let $\overline{D}(\mathcal{C}')$ be a restricted set of representatives of $D(\mathcal{C}')$. In order to avoid the distinction in cases, we will assume that, for every $e \in \overline{D}_{n-1}(\mathcal{C}')$, $\mu'_{u_n,\ldots,u_{i+1}}(e) = M'(e)$, when $i = n$ and $\mu'_{\emptyset}(e) = M'(e)$.

Let $(u_n, \ldots, u_2) \in \Upsilon_n(\mathcal{C}')$. Let i and j be natural numbers such that $2 \leq i \leq j \leq n$ and $w \in \{u_j, \ldots, s'(u_n, \ldots, u_{j+1})\}$. We are going to prove the following claim:

$$\left.\begin{array}{l} \text{if } e \text{ is an element of } \overline{D}_{i-1}(\mathcal{C}') \text{ such that} \\ \mu'_{u_n,\ldots,u_{i+1}}(e) \geq f'[u_n, \ldots, u_i] \\ \text{then} \\ \mu'_{S^{j-1-i}(u_n,\ldots,u_{j+1},w)}(e) \geq \\ f'[S^{j-i}\left(u_n, \ldots, u_{j+1}, w\right)]. \end{array}\right\} \tag{19}$$

The condition (19) will be used repeatedly through the proof. First, in case $i = j$ we have that

$$\begin{array}{rcl} \mu'_{S^{j-1-i}(u_n,\ldots,u_{j+1},w)}(e) & = & \mu'_{u_n,\ldots,u_{j+1}}(e) \geq \\ f'[u_n; \ldots, u_{j+1}, u, j] & \geq & f'[u_n, \ldots, u_{j+1}, w] = \\ f'[S^{j-i}(u_n, \ldots, u_{j+1}, w)] & & \end{array}$$

becasuse $w \geq u_j$. Assume that $i < j$ (note that this implies $i < n$) and that there exists $e \in \overline{D}_{i-1}(\mathcal{C}')$ such that $\mu'_{u_n,\ldots,u_{i+1}}(e) \geq f'[u_n, \ldots, u_i]$. Then $\mu'_{u_n,\ldots,u_{i+1}}(e) \neq 0$, and so there exists $a_1 \in R(e)$ verifying that $\mu'_{u_n,\ldots,u_{i+2}}(e, a_1) \geq f'[u_n, \ldots, u_{i+1}]$. Hence $\mu'_{u_n,\ldots,u_{i+2}}(e, a_1) \neq 0$. By repeating this argument $j-i$ times we get $j-i$ natural numbers $a_1 \in R(e), \ldots, a_{j-i} \in R(e, a_1, \ldots, a_{j-i-1})$ such that $\mu'_{u_n,\ldots,u_{j+1}}(e, a_1, \ldots, a_{j-i}) \geq f'[u_n, \ldots, u_j]$. So, $\mu'_{u_n,\ldots,u_{j+1}}(e, a_1, \ldots, a_{j-i}) \geq f'[u_n, \ldots, u_{j+1}, w]$ because $w \geq u_j$. Then one follows that

$$\mu'_{u_n,\ldots,u_{j+1},w}(e, a_1, \ldots, a_{j-i-1}) \neq 0,$$

and hence

$$\mu'_{u_n,\ldots,u_{j+1},w}(e, a_1, \ldots, a_{j-i-1}) \geq f'[S(u_n, \ldots, u_{j+1}, w)].$$

Therefore, $\mu'_{S(u_n,\ldots,u_{j+1},w)}(e, a_1, \ldots, a_{j-i-2}) \neq 0$. Now, we repeat this process $j-i$ times and we remove the numbers a_i, with $i = 1, \ldots, j-i$, until to get

$$\mu'_{S^{j-i-1}(u_n,\ldots,u_{j+1},w)}(e) \geq f'[S^{j-i}(u_n, \ldots, u_{j+1}, w)].$$

This proves (19).

Let us prove $a)$. Let h be a natural number with $2 \leq h \leq j \leq n$. If $h = j$, then the proof of $a)$ is straightforward. So suppose that $h < j$. Then one has

$$\begin{array}{c} f'[u_n, \ldots, u_{h+1}, u_h] \leq f'[u_n, \ldots, u_{h+1}, 1] = \\ \max\limits_{e \in \overline{D}_{h-1}(\mathcal{C}')} \left\{ \mu'_{u_n,\ldots,u_{h+1}}(e) \right\} = \\ \max\limits_{e \in \overline{D}_{h-1}(\mathcal{C}')} \left\{ \sum\limits_{a \in \Omega'_{u_n,\ldots,u_{h+1}}(e)} m(e,a) \right\}. \end{array}$$

Recall that

$$\Omega'_{u_n,\ldots,u_{h+1}}(e) = \{a \in R(e) \mid \mu'_{u_n,\ldots,u_{h+2}}(e,a) \geq f'[u_n,\ldots,u_{h+1}]\}.$$

On the other hand,

$$f'[S^{j-1-h}(u_n,\ldots,u_{j+1},w),1] = \max_{e\in\overline{D}_{h-1}(\mathcal{C}')} \left\{\mu'_{S^{j-1-h}(u_n,\ldots,u_{j+1},w)}(e)\right\} = \max_{e\in\overline{D}_{h-1}(\mathcal{C}')} \left\{ \sum_{a\in\Omega'_{S^{j-1-h}(u_n,\ldots,u_{j+1},w)}(e)} m(e,a) \right\},$$

where

$$\Omega'_{S^{j-1-h}(u_n,\ldots,u_{j+1},w)}(e) = \{a \in R(e) \mid \mu'_{S^{j-2-h}(u_n,\ldots,u_{j+1},w)}(e,a) \geq f'[S^{j-1-h}(u_n,\ldots,u_{j+1},w)]\}.$$

Now, by applying (19) with $i = h+1$ we have a).

Finally let us prove b). By definition,

$$g'[u_n,\ldots,u_2] = \sum_{\mu'_{u_n,\ldots,u_3}(e)\geq f'[u_n,\ldots,u_2]} m(e).$$

Then by taking $v = (u_n,\ldots,u_{j+1},w)$ we have that

$$g'[S^{j-2}(v)] = \sum_{\mu'_{S^{j-3}(v)}(e)\geq f'[S^{j-2}(v)]} m(e).$$

Therefore, by (19) with $i = 2$ we obtain b). ■

Now we present some definitions that will be used in our main results.

Definition 18. *Given $v \in \{1,\ldots,s'\}$ we define*

$$\widetilde{\Lambda}(v) = \{i \in \{2,\ldots,n\} \mid f'[S^{n-i-1}(v),1] < r_i\},$$

where, if $i = n$ then $f'[S^{-1}(v),1] = f'[1]$. From $\widetilde{\Lambda}(v)$ we define

$$\Lambda(v) = \begin{cases} \widetilde{\Lambda}(v) & \textit{if } g'[S^{n-2}(v)] = r_1, \\ \widetilde{\Lambda}(v) \cup \{1\} & \textit{otherwise.} \end{cases}$$

Now, for every $i \in \Lambda(v)$, we define

$$\lambda_i(v) = \max\left\{\lambda \in \mathbb{N} \mid f'[S^{n-i-1}(v),1] < \left\lceil \frac{r_i}{\lambda} \right\rceil\right\},$$

in case $i > 1$, and in case $i = 1$ we set

$$\lambda_1(v) = \max\left\{\lambda \in \mathbb{N} \mid g'[S^{n-2}(v)] < \left\lceil \frac{r_1}{\lambda} \right\rceil\right\}.$$

Note that, by Lemma 17, given $v, v' \in \{1,\ldots,s'\}$ we have that

$$\text{if } v \geq v' \text{ then } \Lambda(v) \subseteq \Lambda(v'). \tag{20}$$

The following two lemmas will be used several times in the proofs of the subsequent results. Given $r > 0$ and x integers, we denote by

$$[x]_r$$

the remainder of the division of x between r.

Lemma 19. *Let $r, h, x_1, \ldots, x_h$ be natural numbers such that $0 \leq x_1 < x_2 < \cdots < x_h < r$. Then there exists $\beta \in \mathbb{N}$ verifying that*

$$\left\lceil \frac{r}{h} \right\rceil - 1 \leq [x_i + \beta]_r < r,$$

for every $i = 1,\ldots,h$, and $[x_j + \beta]_r = r-1$ for some $j \in \{1,\ldots,h\}$.

Proof: For every $i \in \{2, \dots, h\}$ we denote $d_i = x_i - x_{i-1}$ and we set $d_1 = r - (x_h - x_1)$. So $r = \sum_{i=1}^{h} d_i$. Suppose that $d_i < \lceil \frac{r}{h} \rceil$ for every $i = 1, \dots, h$. Then $d_i < \frac{r}{h}$, for every $i = 1, \dots, h$. Hence

$$r = \sum_{i=1}^{h} d_i < h \cdot \frac{r}{h} = r,$$

a contradiction. Therefore there exists $k \in \{1, \dots, h\}$ such that $d_k \geq \lceil \frac{r}{h} \rceil$. Take $\beta = r - x_{k-1} - 1$, where we assume $x_0 = x_h$. Then, on the one hand, we have that $x_i + \beta < 2r$, for every $i = 1, \dots, h$. On the other hand, if $k \neq 1$ then

$$x_k + \beta \geq \beta \geq x_k - x_{k-1} - 1 \geq \left\lceil \frac{r}{h} \right\rceil - 1,$$

and if $k = 1$ then

$$x_1 + \beta = r - x_h - 1 + x_1 = d_1 - 1 \geq \left\lceil \frac{r}{h} \right\rceil - 1.$$

So, one has that

$$\begin{gathered} 0 \leq \lceil \tfrac{r}{h} \rceil - 1 \leq x_1 + \beta < \cdots < x_{k-1} + \beta = r - 1 < r \leq \\ r + \lceil \tfrac{r}{h} \rceil - 1 \leq x_k + \beta < \cdots < x_h + \beta < 2r, \end{gathered}$$

and we are done. ■

Lemma 20. *Let B be a subset of $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$ with cardinality b. Let $A \subseteq B$ and $\{\lambda_i(u)\}_{i \in I}$ a set of integers, with $I \subseteq \Lambda(u)$ for certain $u \in \{1, \dots, s'\}$. For any non negative integer η such that $\eta \leq |A|$ and*

$$\eta + \sum_{i \in I} \lambda_i(u) \geq b,$$

there exist $J = \{i_1, \dots, i_h\} \subseteq I$ and a family of sets $\{X_k\}_{k=1}^{h}$ ($X_k \subseteq \mathbb{Z}_{r_k}$) such that

$$B = A \cup B_1 \cup \cdots \cup B_h,$$

where the union is disjoint, and for each $k \in \{1, \dots, h\}$,

$$B_k = \{x \in B \setminus (A \cup B_1 \cup \cdots \cup B_{k-1}) \mid \pi_{i_k}(x) \in X_k\}.$$

Moreover, there exists a family of non negative integers $\{\beta_k\}_{k=1}^{h}$ verifying that for every $k = 1, \dots, h$, given $a \in X_k$ and $v = (v_n, \dots, v_{i_k+1}) \in \Upsilon_{n-i_k+1}(\mathcal{C}')$, where $v_n \leq u$, the following properties hold
a) $[a + \beta_k]_{r_{i_k}} \geq f'[v, 1]$, si $i_k \neq 1$,
b) $[a + \beta_1]_{r_1} \geq g'[v]$, si $i_k = 1$.

Proof: Suppose that we have $A \subseteq B$, $\{\lambda_i(u)\}_{i \in I}$ and η satisfying the conditions of the statement. First of all, note that if $A = B$ then the lemma follows strightforward by taking $J = \emptyset$. So, we assume that $A \neq B$.

We denote $\lambda_i(u) = \lambda_i$, for short, and the elements of I by $I = \{i_1, \dots, i_m\}$. We are going to construct $J = \{i_1, \dots, i_h\}$, where we will get h and the family of sets $\{X_k\}_{k=1}^{h}$ as a consequence of a recursive procedure. To do this we will make use of an intermediate family of sets $\{L_k\}_{k=1}^{h}$, with $L_k \subseteq \mathbb{Z}_{r_k}$. For each $k \in \{1, \dots, m\}$ we define

$$\begin{aligned} L_k &= \pi_{i_k}\left[B \setminus (A \cup B_1 \cup \cdots \cup B_{k-1})\right]; \\ X_k &= \begin{cases} X \subseteq L_k \text{ such that } |X| = \lambda_{i_k}, & \text{if } |L_k| > \lambda_{i_k}, \\ L_k, & \text{if } |L_k| \leq \lambda_{i_k}, \end{cases} \end{aligned}$$

and

$$B_k = \{x \in B \setminus (A \cup B_1 \cup \cdots \cup B_{k-1}) \mid \pi_{i_k}(x) \in X_k\}.$$

We set $h = \min\{1 \leq k \leq m \mid |L_k| \leq \lambda_{i_k}\}$. Let us see that $\{1 \leq k \leq m \mid |L_k| \leq \lambda_{i_k}\} \neq \emptyset$, that is, let us check that h is well defined. Suppose that this is not true. Then we have that $|L_m| > \lambda_{i_m}$. This implies that $|B \setminus (A \cup B_1 \cup \cdots \cup B_m)| = |B| - (|A| + \sum_{k=1}^{m} |B_k|) > 0$, because $|X_m| = \lambda_{i_m} < |L_m|$. So

$$\eta + \sum_{k=1}^{m} \lambda_{i_k} \leq |A| + \sum_{k=1}^{m} |B_k| < |B| = b,$$

a contradiction. Therefore $|L_h| \leq \lambda_{i_h}$, and then $X_h = L_h$. Hence

$$\begin{aligned} B_h = \left\{ x \in B \setminus \left(A \cup \bigcup_{k=1}^{h-1} B_k \right) \mid \pi_{i_h}(x) \in L_h \right\} = \\ = B \setminus \left(A \cup \bigcup_{k=1}^{h-1} B_k \right), \end{aligned}$$

and so $B = A \cup B_1 \cup \cdots \cup B_h$.

Now, for every $k \in \{1, \dots, h\}$, we use Lemma 19 applied to the elements of each X_k and r_{i_k}. Then we get $\beta_1, \dots, \beta_h \in \mathbb{N}$ such that

$$\left\lceil \frac{r_{i_k}}{\lambda_{i_k}} \right\rceil - 1 \le \left\lceil \frac{r_{i_k}}{|X_k|} \right\rceil - 1 \le [a + \beta_k]_{r_{i_k}} < r_{i_k}$$

for all $a \in X_k$. Note that $|X_k| \le \lambda_k$ for every $k = 1, \dots, h$. On the other hand, by using that $i_k \in \Lambda(u)$ for every $k = 1, \dots, h$, and Lemma 17, we have that for every $a \in X_k$ and $v = (v_n, \dots, v_{i_k+1}) \in \Upsilon_{n-i_k+1}(\mathcal{C}')$, with $v_n \le u$,

$$[a + \beta_k]_{r_{i_k}} \ge f'[S^{n-i_k-1}(u), 1] \ge f'[v, 1], \tag{21}$$

in case $i_k \neq 1$, and

$$[a + \beta_k]_{r_1} \ge g'[S^{n-2}(u)] \ge g'[v], \tag{22}$$

in case $i_k = 1$. This finishes the proof. ■

Now, we are ready to present our first sufficient condition to have a (partial) PD-set contained in the group $\langle T_i \mid i = 1, \dots, n \rangle$. Given p in $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$, for every $i = 1, \dots, n$, we denote by $\pi_i(p)$ the i-th coordinate of p. In general, if B is a subset of $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$, then $\pi_i(B)$ denotes the set of i-th coordinates of the elements of B.

Theorem 21. *Let $\mathcal{C}$ be a t-error-correcting abelian code in $\mathbb{A}(r_1, \dots, r_n)$. Let b a positive integer such that $b \le t$. If there exists a subset $I \subseteq \Lambda(s')$ (see (18)) verifying*

$$\sum_{i \in I} \lambda_i(s') \ge b$$

then the group $\langle T_i \mid i \in I \rangle$ is a b-PD-set for $\mathcal{C}$ with respect to the information set $\Gamma(\mathcal{C}')$.

Proof: Let B a subset in $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$ with cardinality b. Suppose that there exists $I = \{i_1, \dots, i_m\}$ contained in $\Lambda(s')$ such that $\sum_{k=1}^{m} \lambda_{i_k}(s') \ge b$. We denote $\lambda_{i_k}(s') = \lambda_{i_k}$ for brevity. Then by applying the Lemma 20 to B, $A = \emptyset$ and $\{\eta, \lambda_{i_1}, \dots, \lambda_{i_m}\}$, with $\eta = 0$, we obtain a family of sets $X_1 \subseteq \mathbb{Z}_{r_{i_1}}, \dots, X_h \subseteq \mathbb{Z}_{r_{i_h}}$, with $h \le m$, satisfying that $B = B_1 \cup \cdots \cup B_h$, where, for every $k \in \{1, \dots, h\}$

$$B_k = \left\{ x \in B \setminus \bigcup_{j=1}^{k-1} B_j \mid \pi_{i_k}(x) \in X_k \right\}.$$

Moreover, there exists a family of positive integers $\{\beta_k\}_{k=1}^{h}$ such that for every $k = 1, \dots, h$, given $a \in X_k$ and $v = (v_n, \dots, v_{i_k+1}) \in \Upsilon_{n-i_k+1}(\mathcal{C}')$ one has that

$$[a + \beta_k]_{r_{i_k}} \ge f'[v, 1], \tag{23}$$

in case $i_k \neq 1$, and

$$[a + \beta_1]_{r_1} \ge g'[v], \tag{24}$$

in case $i_k = 1$. Note that every $(v_n, \dots, v_{i_k+1}) \in \Upsilon_{n-i_k+1}(\mathcal{C}')$ satisfies that $v_n \le s'$.

Now, take $p \in B$ and let us see that $\left(\prod_{j=1}^{h} T_{i_j}^{\beta_j}\right)(p) \notin \Gamma(\mathcal{C}')$. Let $k \in \{1, \dots, h\}$ such that $p \in B_k$. Let us denote $q = \left(\prod_{j=1}^{h} T_{i_j}^{\beta_j}\right)(p)$ and suppose that $q \in \Gamma(\mathcal{C}')$. Then there exists $v = (v_n, \dots, v_2) \in \Upsilon_n(\mathcal{C}')$ such that

$$f'[v_n, \dots, v_{i_k}] > \pi_{i_k}(q) \ge f'[v_n, \dots, v_{i_k} + 1],$$

in case $i_k \neq 1$, and

$$g'[v_n, \dots, v_2] > \pi_1(q) \ge 0,$$

in case $i_k = 1$. On the other hand, $\pi_{i_k}(q) = \pi_{i_k}\left(T_{i_k}^{\beta_k}(p)\right) = [\pi_{i_k}(p) + \beta_k]_{r_{i_k}}$ and by definition $\pi_{i_k}(p) \in X_k$. So, in cases $i_k \neq 1$ and $i_k = 1$ we reach a contradiction with (23) and (24) respectively (observe that $f'[v_n, \dots, v_{i_k+1}, v_{i_k}] \le f'[v_n, \dots, v_{i_k+1}, 1]$). ■

The previous theorem is based on the existence of certain subsets of $\Lambda(s')$. The following result deals with subsets $\Lambda(u)$, for some $u \in \{1, \dots, s'\}$. So, in some sense it improves Theorem 21 (see (20)). Although, the following theorem implies a growth of the (partial) PD-set. More precisely, it supposes the addition of the subgroup $\langle T_n \rangle$. This means that in some cases we might obtain PD-sets bigger than that given by the Theorem 21.

Theorem 22. *Let $\mathcal{C}$ be a t-error-correcting abelian code in $\mathbb{A}(r_1, \dots, r_n)$. Let b be a positive integer such that $b \le t$. We define*

$$\lambda_0 = \begin{cases} 0 & \text{if} \quad f'[1] = r_n, \\ 1 & \text{if} \quad \left\lceil \frac{r_n}{b} \right\rceil \le f'[1] < r_n, \\ b & \text{if} \quad f'[1] < \left\lceil \frac{r_n}{b} \right\rceil. \end{cases}$$

Let $u = \min\left\{x \in \{2, \ldots, s'+1\} \mid f'[x] < \left\lceil \frac{r_n}{b} \right\rceil\right\}$*. If there exists a subset* $I \subseteq \Lambda(u-1) \setminus \{n\}$ *such that*

$$\lambda_0 + \sum_{i \in I} \lambda_i(u-1) \geq b \tag{25}$$

then the group generated by T_n *and* $\{T_i\}_{i \in I}$ *is a* b*-PD-set for* $\mathcal{C}$ *with respect to the information set* $\Gamma(\mathcal{C}')$*.*

Proof: Let B be a subset of $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$ with cardinality b. We define $L_0 = \pi_n(B)$. Then by applying the Lemma 19 to the elements of L_0 and r_n, we have that there exists $\beta_0 \in \mathbb{N}$ such that

$$f'[u] \leq \left\lceil \frac{r_n}{b} \right\rceil - 1 \leq \left\lceil \frac{r_n}{|L_0|} \right\rceil - 1 \leq [a + \beta_0]_{r_n} < r_n \tag{26}$$

for every $a \in L_0$ (observe that, by definition, $|L_0| \leq b$). Moreover, we have that there exists $a_0 \in L_0$ verifying that

$$[a_0 + \beta_0]_{r_n} = r_n - 1. \tag{27}$$

Let $X_0 = \{p \in B \mid \pi_n(p) = a_0\}$. We define

$$B_0 = \begin{cases} B & \text{if} \quad \lambda_0 = b, \\ X_0 & \text{if} \quad \lambda_0 = 1, \\ \emptyset & \text{if} \quad \lambda_0 = 0. \end{cases}$$

Note that if $\lambda_0 = b$ then the hypothesis (25) holds with $I = \emptyset$. This fact together with (26) imply that $T_n^{\beta_0}(p) \notin \Gamma(\mathcal{C}')$ for every $p \in B$; that is, the group generated by T_n is a b-PD-set for $\mathcal{C}$ with respect to the information set $\Gamma(\mathcal{C}')$, and we are done. Then, in what follows we assume that $\lambda_0 < b$. Note that this implies that $\lambda_0 \leq |B_0|$.

Now, assume that there exists a subset $I = \{i_1, \ldots, i_m\} \subseteq \Lambda(u-1) \setminus \{n\}$ such that $\lambda_0 + \sum_{k=1}^m \lambda_{i_k}(u-1) \geq b$. We write $\lambda_{i_k}(u-1) = \lambda_{i_k}$. We continue the proof in a similar way to that of Theorem 21. We apply the Lemma 20 to B, $A = B_0$, $\{\lambda_{i_1}, \ldots, \lambda_{i_m}\}$ and $\eta = \lambda_0$. Then we obtain two families of sets, $\{X_k\}_{k=1}^h$, with

$$X_1 \subseteq \mathbb{Z}_{r_{i_1}}, \ldots, X_h \subseteq \mathbb{Z}_{r_{i_h}}$$

($h \leq m$) and $\{B_k\}_{k=1}^h$, satisfying that $B = B_0 \cup B_1 \cup \cdots \cup B_h$, where, for every $k \in \{1, \ldots, h\}$, $\pi_{i_k}(x) \in X_k$, for all $x \in B_k$. Moreover, there exists a family of positive integers $\{\beta_k\}_{k=1}^h$ such that for every $k = 1, \ldots, h$, given $a \in X_k$ and $v = (v_n, \ldots, v_{i_k+1}) \in \Upsilon_{n-i_k+1}(\mathcal{C}')$, with $v_n \leq u-1$, one has that

$$[a + \beta_k]_{r_{i_k}} \geq f'[v, 1], \tag{28}$$

in case $i_k \neq 1$, and

$$[a + \beta_1]_{r_1} \geq g'[v], \tag{29}$$

in case $i_k = 1$.

Take $p \in B$ and let us see that $\left[\left(\prod_{j=1}^h T_{i_j}^{\beta_j}\right) \circ T_n^{\beta_0}\right](p) \notin \Gamma(\mathcal{C}')$. Denote $q = \left[\left(\prod_{j=1}^h T_{i_j}^{\beta_j}\right) \circ T_n^{\beta_0}\right](p)$ and suppose that $q \in \Gamma(\mathcal{C}')$. Then there exists $v = (v_n, \ldots, v_2) \in \Upsilon_n(\mathcal{C}')$ such that

$$f'[v_n, \ldots, v_i] > \pi_i(q) \geq f'[v_n, \ldots, v_i + 1], \text{ for } i = 2, \ldots, n, \tag{30}$$

and

$$g'[v_n, \ldots, v_2] > \pi_n(q) \geq 0. \tag{31}$$

Let $k \in \{0, \ldots, h\}$ such that $p \in B_k$. We distinguish two cases: $k = 0$ and $k \neq 0$.

If $k = 0$ then $p \in B_0$, and hence $\pi_n(p) = a_0$. So, by (27),

$$\pi_n(q) = \pi_n\left(T_n^{\beta_0}(p)\right) = [a_0 + \beta_0]_{r_n} = r_n - 1.$$

This is a contradiction with (30), for $i = n$, because we are assuming that $\lambda_0 < b$, which means that $f'[v_n] \leq f'[1] < r_n$.

Now, suppose that $k \neq 0$. Then, on the one hand,

$$\pi_n(q) = \pi_n\left(T_n^{\beta_0}(p)\right) = [\pi_n(p) + \beta_0]_{r_n},$$

where $\pi_n(p) \in L_0$ by definition. So (26) together with (30), with $i = n$, imply that $v_n \leq u-1$. On the other hand, $\pi_{i_k}(p) \in X_k$ and

$$\pi_{i_k}(q) = \pi_{i_k}\left(T_{i_k}^{\beta_k}(p)\right) = [\pi_{i_k}(p) + \beta_k]_{r_{i_k}}.$$

Therofore, if $i_k \neq 1$ then (30), for $i = i_k$, yields a contradiction with (28). Last, if $i_k = 1$ then (31) contradicts (29). ■

Our next result gives us a sufficient condition under the assumptions $n \geq 3$ and $f'[1] = r_n$. This new condition can hold even when Theorem 22 does not do, as it will be shown in Example 24.

Theorem 23. *Let $\mathcal{C}$ be a t-error-correcting abelian code in $\mathbb{A}(r_1,\dots,r_n)$. Let b a positive integer such that $b \leq t$. Suppose that $n \geq 3$, $f'[1] = r_n$ and assume that there exists $v = (v_n,\dots,v_{\tau+1},1) \in \Upsilon_{n-\tau+2}(\mathcal{C}')$ (with $1 < \tau < n$) such that $f'[v_n,\dots,v_{\tau+1},1] < r_\tau$. Then, we define*

$$u = \begin{cases} v_n + 1 & \textbf{\textit{in case}}\ f'[v_n+1] < \left\lceil \frac{r_n}{b} \right\rceil, \\ \min\{\{v_n+1 \leq x \leq s' \mid \\ f'[v_n] - f'[x] > r_n - \left\lceil \frac{r_n}{b} \right\rceil\} \cup \{s'+1\}\} \\ \qquad\qquad \textbf{\textit{in case}}\ f'[v_n+1] \geq \left\lceil \frac{r_n}{b} \right\rceil. \end{cases} \tag{32}$$

If there exists a subset I of $\Lambda(u-1) \setminus \{\tau,\dots,n\}$ verifying that

$$1 + \sum_{i \in I} \lambda_i(u-1) \geq b,$$

then the group generated by $\{T_\tau,\dots,T_n\}$ and $\{T_i\}_{i\in I}$ is a b-PD-set for $\mathcal{C}$ with respect to $\Gamma(\mathcal{C}')$.

Proof: Suppose that $f'[1] = r_n$ and $n \geq 3$. Let us also assume that there exists $v = (v_n,\dots,v_{\tau+1},1) \in \Upsilon_{n-\tau+2}(\mathcal{C}')$ (with $1 < \tau < n$) such that $f'[v_n,\dots,v_{\tau+1},1] < r_\tau$.

Let B be a subset of $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$ with cardinality b. We define $L_0 = \pi_n(B)$. We claim that there exist $a_0 \in L_0$ and $\beta_0 \in \mathbb{N}$ verifying that

$$f'[v_n+1] \leq [a_0 + \beta_0]_{r_n} < f'[v_n] \tag{33}$$

and

$$f'[u] \leq [a + \beta_0]_{r_n} < r_n, \text{ for all } a \in L_0. \tag{34}$$

Indeed, by applying the Lemma 19 to the elements of L_0 and r_n we obtain $\beta_0' \in \mathbb{N}$ such that

$$\left\lceil \frac{r_n}{b} \right\rceil - 1 \leq \left\lceil \frac{r_n}{|L_0|} \right\rceil - 1 \leq [a + \beta_0']_{r_n} < r_n$$

for every $a \in L_0$. In addition, there exists $a_1 \in L_0$ such that $[a_1 + \beta_0']_{r_n} = r_n - 1$.

Suppose that $f'[v_n+1] \geq \left\lceil \frac{r_n}{b} \right\rceil$. Take $\beta_0'' = r_n - f'[v_n]$. Then,

$$f'[v_n+1] \leq [a_1 + \beta_0' - \beta_0'']_{r_n} = f'[v_n] - 1 < f'[v_n].$$

So, since

$$u = \min\left\{v_n + 1 \leq x \leq s' \mid f'[v_n] - f'[x] > r_n - \left\lceil \frac{r_n}{b} \right\rceil\right\},$$

one has that for every $a \in L_0$

$$[a + \beta_0' - \beta_0'']_{r_n} \geq \left\lceil \frac{r_n}{b} \right\rceil - 1 - r_n + f'[v_n] \geq f'[u].$$

Now, if we assume that $u = s'+1$, then $0 = f'[u] \leq [a + \beta_0' - \beta_0'']_{r_n}$ for all $a \in L_0$. Therefore, for any value of u, (33) and (34) hold with $\beta_0 = \beta_0' - \beta_0''$ and $a_0 = a_1$.

Now, let us suppose that $f'[v_n+1] < \left\lceil \frac{r_n}{b} \right\rceil$ and let us denote $a_2 = \min\limits_{a \in L_0}\{[a + \beta_0']_{r_n}\}$. Then there exists $\beta_0'' \in \mathbb{N}$ such that

$$f'[v_n+1] \leq [a_2 + \beta_0' - \beta_0'']_{r_n} < f'[v_n]$$

and

$$f'[u] = f'[v_n+1] \leq [a + \beta_0' - \beta_0'']_{r_n} < r_n,$$

for every $a \in L_0$. So, by taking $\beta_0 = \beta_0' - \beta_0''$ and $a_0 = a_2$ one has (33) and (34). This finishes the proof of (33) and (34).

Let $p_0 \in \{p \in B \mid \pi_n(p) = a_0\}$. Then, by (33), $f'[v_n+1] \leq [\pi_n(p_0) + \beta_0]_{r_n} < f'[v_n]$. Take $\nu_\tau, \nu_{\tau+1},\dots,\nu_{n-1} \in \mathbb{N}$ such that $f'[v_n,\dots,v_i+1] \leq [\pi_i(p_0) + \nu_i]_{r_i} < f'[v_n,\dots,v_i]$, for every $i = \tau+1,\dots,n-1$ and $f'[v_n,\dots,v_{\tau+1},1] \leq [\pi_\tau(p_0) + \nu_\tau]_{r_\tau} = r_\tau - 1$. Note that by hypothesis $f'[v_n,\dots,v_{\tau+1},1] < r_\tau$. Then

$$\left(\prod_{i=\tau}^{n-1} T_i^{\nu_i} \circ T_n^{\beta_0}\right)(p_0) \notin \Gamma(\mathcal{C}').$$

Moreover, we have that

$$\sigma \circ \left(\prod_{i=\tau}^{n-1} T_i^{\nu_i} \circ T_n^{\beta_0}\right)(p_0) \notin \Gamma(\mathcal{C}'), \tag{35}$$

for any σ in the group generated by $\{T_1,\dots,T_{\tau-1}\}$.

Let us suppose that there exists a subset $I = \{i_1,\dots,i_m\} \subseteq \Lambda(u-1) \setminus \{\tau,\dots,n\}$ such that $1 + \sum_{i\in I} \lambda_i(u-1) \geq b$. For bervity, we write $\lambda_i(u-1) = \lambda_i$. The proof continues in a similar way to that of the previous theorem. We apply the

Lemma 20 to B, $A = \{p_0\}$ and $\{\eta, \lambda_{i_1}, \ldots, \lambda_{i_m}\}$, where we define $\eta = 1$. Then we obtain two families of sets, $\{X_k\}_{k=1}^{h}$, with

$$X_1 \subseteq \mathbb{Z}_{r_{i_1}}, \ldots, X_h \subseteq \mathbb{Z}_{r_{i_h}}$$

($h \leq m$), and $\{B_k\}_{k=1}^{h}$, such that $B = \{p_0\} \cup B_1 \cup \cdots \cup B_h$, where, for every $k \in \{1, \ldots, h\}$, $\pi_{i_k}(x) \in X_k$, for all $x \in B_k$. Moreover, there exists a family of positive integers $\{\beta_k\}_{k=1}^{h}$ such that for every $k = 1, \ldots, h$, given $a \in X_k$ and $v = (v_n, \ldots, v_{i_k+1}) \in \Upsilon_{n-i_k+1}(\mathcal{C}')$, with $v_n \leq u - 1$, one has that

$$[a + \beta_k]_{r_{i_k}} \geq f'[v, 1], \tag{36}$$

in case $i_k \neq 1$, and

$$[a + \beta_1]_{r_1} \geq g'[v], \tag{37}$$

in case $i_k = 1$.

Take $p \in B$ and denote $q = \left[\left(\prod_{j=1}^{h} T_{i_j}^{\beta_j}\right) \circ \left(\prod_{i=\tau}^{n-1} T_i^{\nu_i}\right) \circ T_n^{\beta_0}\right](p)$. Let us see that $q \notin \Gamma(\mathcal{C}')$. If $p = p_0$ then (35) gives us what we wanted. So, suppose that $p \neq p_0$ and $q \in \Gamma(\mathcal{C}')$. Then there exists $v = (v_n, \ldots, v_2) \in \Upsilon_n(\mathcal{C}')$ such that

$$f'[v_n, \ldots, v_i] > \pi_i(q) \geq f'[v_n, \ldots, v_i + 1], \tag{38}$$

for $i = 2, \ldots, n$, and

$$g'[v_n, \ldots, v_2] > \pi_1(q) \geq 0. \tag{39}$$

Let $k \in \{1, \ldots, h\}$ such that $p \in B_k$. Then, on the one hand,

$$\pi_n(q) = \pi_n\left(T_n^{\beta_0}(p)\right) = [\pi_n(p) + \beta_0]_{r_n},$$

where $\pi_n(p) \in L_0$. So (34) together with (38), for $i = n$, imply that $v_n \leq u - 1$. On the other hand, $\pi_{i_k}(p) \in X_k$ and

$$\pi_{i_k}(q) = \pi_{i_k}\left(T_{i_k}^{\beta_k}(p)\right) = [\pi_{i_k}(p) + \beta_k]_{r_{i_k}}.$$

Therefore, if $i_k \neq 1$ then (38), for $i = i_k$, yields a contradiction with (36). Last, if $i_k = 1$ then (39) contradicts (37). This finishes the proof. ■

Example 24. We are going to see an abelian code $\mathcal{C}$ for which Theorem 23 asserts that it has a 2-PD-set with respect to $\Gamma(\mathcal{C}')$, while by applying Theorem 22 we get at most a 1-PD-set with respect to $\Gamma(\mathcal{C}')$.

Consider the algebra $\mathbb{A}(3, 3, 7)$ over $\mathbb{F}_2$. We take the $[63, 37, 6]$-code $\mathcal{C}$ given by

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

In this case, $\Gamma(\mathcal{C}')$ is determined by the following parameters (recall the definitions from (4) to (8))

$$\begin{gathered} f'[1] = 7 > f'[2] = 6 > f'[3] = 4 > f'[4] = 1 \\ f'[1,1] = 1;\;\; f'[2,1] = 2;\;\; f'[3,1] = 3;\;\; f'[4,1] = 3 \\ g'[1,1] = 2;\;\; g'[2,1] = 2;\;\; g'[3,1] = 2;\;\; g'[4,1] = 3 \end{gathered}$$

By applying Theorem 22 we have that $\lambda_0 = 0$, $u = 4$, $\Lambda(3) \setminus \{3\} = \{1\}$ and $\lambda_1(3) = 1$ (see Definition 18); so that we get just a 1-PD-set.

Now, we apply Theorem 23. By following its corresponding notation we get $v = (2, 1)$, $v_3 = 2$, $\tau = 2$, $u = 4$, $\Lambda(3) \setminus \{2, 3\} = \{1\}$; which yields a 2-PD-set.

To finish this section, we are going to study the case of correcting errors with weight at most 3. In this situation, we will present a result for the existence of (partial) PD-sets which improves the condition given by Theorem 22. First, we need the following lemma.

Lemma 25. *Let s, r be natural numbers with $r \geq 2$ and $1 \leq s \leq 3$ and let $r, x_1, \ldots, x_s$ be positive integers such that $0 \leq x_1 < \cdots < x_s < r$. Let ψ be a map from $\{x_i\}_{i=1}^{s}$ to the set of positive integers such that $\sum_{i=1}^{s} \psi(x_i) = 3$. Let $\chi_1 = \left\lceil \frac{r}{3} \right\rceil - 1$ and $\chi_2 = r - \epsilon - \left\lceil \frac{r}{3} \right\rceil$, where $\epsilon = 1$ if $\frac{r}{3} \in \mathbb{N}$ and $\epsilon = 0$ otherwise. Then there exists $\beta \in \mathbb{N}$ satisfying the following conditions:*

a) $\chi_1 \leq [x_i + \beta]_r < r$, for every $i = 1, \ldots, s$.

b) There exists $\mathcal{A} \subseteq \{1, \ldots, s\}$ such that $\chi_2 \leq [x_i + \beta]_r < r$, for all $i \in \mathcal{A}$, $\sum_{i \in \mathcal{A}} \psi(x_i) \geq 2$, and $[x_{i_0} + \beta]_r = r - 1$ for some $i_0 \in \mathcal{A}$.

Proof: First of all, note that it follows straightforward that $\chi_1 < \chi_2 < r$ for any positive integer r. We are going to distinguish in cases depending on the different values of s.

The case $s = 1$ is clear by taking $\beta = r - 1 - x_1$.

Suppose that $s = 2$. Then we can assume without loss of generality that $\psi(x_2) = 2$. Take $\beta' = r - 1 - x_2$. Then $0 \leq [x_1 + \beta']_r < [x_2 + \beta']_r = r - 1 < r$. So, if $[x_1 + \beta']_r \geq \chi_1$, then β' satisfies the required conditions and we are done. Now, suppose that $[x_1 + \beta']_r < \chi_1$ and take $\beta'' = r - 1 - [x_1 + \beta']_r$. Then,

$$\begin{aligned} 0 < [x_1 + \beta' + \beta'']_r = r - 1 < r < [x_2 + \beta']_r + \beta'' = \\ = 2r - 2 - [x_1 + \beta']_r < 2r. \end{aligned}$$

Hence, $[x_2 + \beta' + \beta'']_r = r - 2 - [x_1 + \beta']_r$. On the other hand,

$$r - 2 - [x_1 + \beta']_r > r - 2 - \chi_1 = r - 1 - \left\lceil \frac{r}{3} \right\rceil \geq \chi_2 - 1 \geq \chi_1.$$

Therefore, by taking $\beta = \beta' + \beta''$ we obtain what we wanted.

Finally suppose that $s = 3$. In this case, $\psi(x_i) = 1$, for all $i = 1, 2, 3$. By applying Lemma 19 to $\{x_1, x_2, x_3\}$ and r, one has that there exists $\beta' \in \mathbb{N}$ such that $\chi_1 \leq [x_i + \beta']_r$, for all $i = 1, 2, 3$, and $[x_j + \beta']_r = r - 1$, for some $j \in \{1, 2, 3\}$. Assume WLOG that

$$\chi_1 \leq [x_1 + \beta']_r < [x_2 + \beta']_r < [x_3 + \beta']_r = r - 1.$$

Then, if $[x_2 + \beta']_r \geq \chi_2$, we get the result by taking $\beta = \beta'$. So, suppose that $[x_2 + \beta']_r < \chi_2$. This implies that $[x_2 + \beta']_r - [x_1 + \beta']_r < \chi_2 - \chi_1$. Then, we take $\beta'' = r - 1 - [x_2 + \beta']_r$. So,

$$\begin{aligned} [x_1 + \beta']_r + \beta'' < [x_2 + \beta' + \beta'']_r = r - 1 < \\ [x_3 + \beta']_r + \beta'' = 2r - 2 - [x_2 + \beta']_r < 2r, \end{aligned}$$

and then $[x_3 + \beta' + \beta'']_r = r - 2 - [x_2 + \beta']_r$. Now, on the one hand,

$$r - 2 - [x_2 + \beta']_r > r - 2 - \chi_2 = \left\lceil \frac{r}{3} \right\rceil + \epsilon - 2 = \chi_1 + \epsilon - 1 \geq \chi_1 - 1.$$

On the other hand,

$$\begin{aligned} [x_1 + \beta' + \beta'']_r = [x_1 + \beta']_r + r - 1 - [x_2 + \beta']_r > \\ r - 1 - \chi_2 + \chi_1 = 2\left\lceil \frac{r}{3} \right\rceil + \epsilon - 2 = \chi_2 - \delta, \end{aligned}$$

where $\delta = r - 3\left\lceil \frac{r}{3} \right\rceil - 2\epsilon + 2$. It is easy to see that $\delta = 0$ or 1 for any value of r, and so $[x_1 + \beta' + \beta'']_r \geq \chi_2$. ■

Proposition 26. *Let $\mathcal{C}$ be a t-error-correcting abelian code in $\mathbb{A}(r_1, \ldots, r_n)$, with $t \geq 3$. Let $\chi_1 = \left\lceil \frac{r_n}{3} \right\rceil - 1$ and $\chi_2 = r_n - \epsilon - \left\lceil \frac{r_n}{3} \right\rceil$, where $\epsilon = 1$ if $\frac{r_n}{3} \in \mathbb{N}$ and $\epsilon = 0$ otherwise. We define*

$$\lambda_0 = \begin{cases} 0 & \text{if} \quad f'[1] = r_n, \\ 1 & \text{if} \quad \chi_2 < f'[1] < r_n, \\ 2 & \text{if} \quad \chi_1 < f'[1] \leq \chi_2, \\ 3 & \text{if} \quad f'[1] \leq \chi_1. \end{cases}$$

Let $u_i = \min\{x \in \{2, \ldots, s' + 1\} \mid f'[x] \leq \chi_i\}$, for $i = 1, 2$. If $\lambda_0 = 3$ or there exist subsets $I \subseteq \Lambda(u_2 - 1) \setminus \{n\}$ and $\emptyset \neq J \subseteq I \cap \Lambda(u_1 - 1)$ such that

$$\lambda_0 + \sum_{i \in I \setminus J} \lambda_i(u_2 - 1) + \sum_{i \in J} \lambda_i(u_1 - 1) \geq 3,$$

then the group generated by T_n and $\{T_i\}_{i \in I}$ is a 3-PD-set for $\mathcal{C}$ with respect to the information set $\Gamma(\mathcal{C}')$.

Proof: Let B be a subset of $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_n}$ with cardinality 3. Consider $L_0 = \pi_n(B)$ and the map $\psi : L_0 \to \mathbb{Z}$ given by $\psi(a) = |\{p \in B \mid \pi_n(p) = a\}|$. Then we apply the Lemma 25 to the elements of L_0, r_n and the map ψ. So we obtain $\beta_0 \in \mathbb{N}$ such that

$$\chi_1 \leq [a + \beta_0]_{r_n} < r_n, \tag{40}$$

for all $a \in L_0$. Moreover, there exists $\mathcal{A}' \subseteq L_0$ such that $\sum_{a \in \mathcal{A}'} \psi(a) \geq 2$ and

$$\chi_2 \leq [a + \beta_0]_{r_n} < r_n, \tag{41}$$

for all $a \in \mathcal{A}'$, and

$$[a_0 + \beta_0]_{r_n} = r_n - 1, \tag{42}$$

for some $a_0 \in \mathcal{A}'$.

If $\lambda_0 = 3$ then $f'[1] \leq \chi_1$. So, by (40) one has that $T_n^{\beta_0}(p) \notin \Gamma(\mathcal{C}')$, for all $p \in B$. Hence the group generated by T_n is a 3-PD-set for $\mathcal{C}$ with respect to $\Gamma(\mathcal{C}')$ and we are done. From now on we suppose that $\lambda_0 < 3$ and that there exist I and J verifying the required conditions.

Let us set

$$X_0 = \begin{cases} \{a_0\} & \text{if } \lambda_0 = 1, \\ \mathcal{A}' & \text{if } \lambda_0 = 2, \\ \emptyset & \text{if } \lambda_0 = 0, \end{cases}$$

and $B_0 = \{p \in B \mid \pi_n(p) \in X_0\}$ (note that by definition $\lambda_0 \leq |B_0|$). Then, by (41) and (42) one has that

$$\pi_n\left(T_n^{\beta_0}(p)\right) \geq f'[1], \tag{43}$$

for all $p \in B_0$. We claim that

$$\left(\tau \circ T_n^{\beta_0}\right)(p) \notin \Gamma(\mathcal{C}'), \tag{44}$$

for any τ in the group generated by $\{T_1, \ldots, T_{n-1}\}$. Indeed, suppose that $q = \left(\tau \circ T_n^{\beta_0}\right)(p) \in \Gamma(\mathcal{C}')$. Then there exists $v_n \in \{1, \ldots, s'\}$ such that $f'[v_n] > \pi_n(q) \geq f'[v_n + 1]$. On the other hand, by (43) one has that $\pi_n(q) = \pi_n\left(T_n^{\beta_0}(p)\right) \geq f'[1]$. This yields a contradiction.

Now, let us define $\mathcal{B}_1 = \{p \in B \mid \pi_n(p) = a \text{ for some } a \in \mathcal{A}\}$ and $\mathcal{B}_2 = B \setminus \mathcal{B}_1$ ($\mathcal{B}_1 = B_0$ in case $\lambda_0 = 2$). Observe that $|\mathcal{B}_1| \geq 2$ and then $|\mathcal{B}_2| \leq 1$. Assume WLOG that $I \setminus J = \{i_1, \ldots, i_{m'}\}$, with $m' < m$, and set $Y = \sum_{k=1}^{m'} \lambda_{i_k}(u_2 - 1)$. We continue the proof by distinguishing in cases:

Case 1: $\mathcal{B}_2 \neq \emptyset$ and $Y = 0$. Note that, by hypothesis, in this case $\lambda_0 + \sum_{k=m'+1}^{m} \lambda_{i_k}(u_1 - 1) \geq 3$. Then, we apply Lemma 20 to B, $A = B_0$, $\eta = \lambda_0$ and $\{\lambda_{i_k}(u_1 - 1)\}_{k=m'+1}^{m}$, having in mind that $i_k \in \Lambda(u_1 - 1)$ for every $k = m' + 1, \ldots, m$. So, we obtain two families of sets $\{X_j\}_{j=m'+1}^{h}$ and $\{B_j\}_{j=m'+1}^{h}$, such that $B = B_0 \cup B_{m'+1} \cup \cdots \cup B_h$, where, for each $k \in \{m' + 1, \ldots, h\}$, $\pi_{i_k}(x) \in X_k$, for all $x \in B_k$.

One also has that there exists a family of positive integers $\{\beta_k\}_{k=m'+1}^{h}$ such that for every $k = m' + 1, \ldots, h$, given $a \in X_k$ and $v = (v_n, \ldots, v_{i_k+1}) \in \Upsilon_{n-i_k+1}(\mathcal{C}')$, with $v_n \leq u_1 - 1$, the following conditions hold:

$$[a + \beta_k]_{r_{i_k}} \geq f'[v, 1], \tag{45}$$

in case $i_k \neq 1$, and

$$[a + \beta_1]_{r_1} \geq g'[v], \tag{46}$$

in case $i_k = 1$.

Take $p \in B$. Let us see that $\left[\left(\prod_{j=m'+1}^{h} T_{i_j}^{\beta_j}\right) \circ T_n^{\beta_0}\right](p) \notin \Gamma(\mathcal{C}')$. The case $p \in B_0$ was proved in (44). Suppose that $p \in B \setminus B_0$ and let $k \in \{m' + 1, \ldots, h\}$ such that $p \in B_k$. Let us denote $q = \left[\left(\prod_{j=m'+1}^{h} T_{i_j}^{\beta_j}\right) \circ T_n^{\beta_0}\right](p)$ and suppose that $q \in \Gamma(\mathcal{C}')$. Then there exists $v = (v_n, \ldots, v_2) \in \Upsilon_n(\mathcal{C}')$ such that

$$f'[v_n, \ldots, v_i] > \pi_i(q) \geq f'[v_n, \ldots, v_i + 1], \text{ for } i = 2, \ldots, n, \tag{47}$$

and

$$g'[v_n, \ldots, v_2] > \pi_1(q) \geq 0. \tag{48}$$

Now, on the one hand, it follows from (40) that $\pi_n(q) = \pi_n\left(T_n^{\beta_0}(p)\right) \geq \chi_1$. Hence (47), with $i = n$, implies that $v_n \leq u_1 - 1$. On the other hand, $\pi_{i_k}(p) \in X_k$ and

$$\pi_{i_k}(q) = \pi_{i_k}\left(T_{i_k}^{\beta_k}(p)\right) = [\pi_{i_k}(p) + \beta_k]_{r_{i_k}}.$$

Therefore, if $i_k \neq 1$ then (47), with $i = i_k$, yields a contradiction with (45). Last, if $i_k = 1$ then (48) contradicts (46). This finishes the proof of this case.

Case 2: $\mathcal{B}_2 \neq \emptyset$ and $Y = 1$. Note that in this case $\lambda_0 + \sum_{k=m'+1}^{m} \lambda_{i_k}(u_1 - 1) \geq 2$. Assume without loss of generality that $\lambda_{i_1}(u_2 - 1) = 1$ (this implies that $m' \geq 1$). Take $p_1 \in \mathcal{B}_1$. Then $[\pi_n(p_1) + \beta_0]_{r_n} \geq \chi_2$. Suppose that $i_1 \neq 1$. Then, since $i_1 \in \Lambda(u_2 - 1)$, one has that $f'[S^{n-i_1-1}(u_2 - 1), 1] < r_{i_1}$. Let $v = (v_n, \ldots, v_{i_1}) \in \Upsilon_{n-i_1+2}(\mathcal{C}')$ such that $v_n \leq u_2 - 1$. By Lemma 17 *a)* we have that $f'[v_n, \ldots, v_{i_1}] \leq f'[S^{n-i_1-1}(u_2 - 1), 1]$. So, we take $\beta_1 = r_{i_1} - \pi_{i_1}(p_1) - 1$, and then

$$\pi_{i_1}\left(T_{i_1}^{\beta_1}(p_1)\right) = [\pi_{i_1}(p_1) + \beta_1]_{r_{i_1}} = r_{i_1} - 1 \geq f'[v_n, \ldots, v_{i_1}]. \tag{49}$$

If $i_1 = 1$, a similar argument using $\pi_1(p_1)$ and the parameters $g'[\cdot]$ instead of $f'[\cdot]$, leads us to the following inequality

$$\pi_1\left(T_1^{\beta_1}(p_1)\right) \geq g'[v_n, \ldots, v_2]. \tag{50}$$

Now we apply the Lemma 20 to $B \setminus \{p_1\}$, $A = B_0$, $\eta = \lambda_0$ and $\{\lambda_{i_k}(u_1 - 1)\}_{k=m'+1}^{m}$, having in mind that $i_k \in \Lambda(u_1 - 1)$ for every $k = m' + 1, \ldots, m$. By using an analogous procedure as in the previous case, we obtain $\{X_k\}_{k=m'+1}^{h}$ and $\{B_k\}_{k=m'+1}^{h}$ such that $B \setminus \{p_1\} = B_0 \cup B_{m'+1} \cup \cdots \cup B_h$, for all $x \in B_k$ one has that $\pi_{i_k}(x) \in X_k$, and there exists a family $\{\beta_k\}_{k=m'+1}^{h}$ such that (45) and (46) hold.

Take $p \in B$ and let us see that $\left[\left(\prod_{j=m'+1}^{h} T_{i_j}^{\beta_j}\right) \circ T_{i_1}^{\beta_1} \circ T_n^{\beta_0}\right](p) \notin \Gamma(\mathcal{C}')$. The case $p \in B_0$ has been already proved. Let us denote again

$$q = \left[\left(\prod_{j=m'+1}^{h} T_{i_j}^{\beta_j}\right) \circ T_{i_1}^{\beta_1} \circ T_n^{\beta_0}\right](p)$$

and suppose that $p \notin B_0$ and $q \in \Gamma(\mathcal{C}')$. Then there exists $v = (v_n, \ldots, v_2) \in \Upsilon_n(\mathcal{C}')$ which verifies (47) and (48).

Suppose that $p \in B \setminus B_0$ and $p \neq p_1$. Let $k \in \{m'+1, \ldots, h\}$ such that $p \in B_k$. Then, by applying (40) one has that $\pi_n(q) = \pi_n\left(T_n^{\beta_0}(p)\right) \geq \chi_1$. So, $v_n \leq u_1 - 1$, by (47) with $i = n$. On the other hand, $\pi_{i_k}(p) \in X_k$ and

$$\pi_{i_k}(q) = \pi_{i_k}\left(T_{i_k}^{\beta_k}(p)\right) = [\pi_{i_k}(p) + \beta_k]_{r_{i_k}}.$$

Therefore, if $i_k \neq 1$ then (47), with $i = i_k$, yields a contradiction with (45). If $i_k = 1$ then (48) contradicts (46). Last, let $p = p_1$. Then, (41) implies that $\pi_n(q) \geq \chi_2$, so $v_n \leq u_2 - 1$. On the other hand, $\pi_{i_1}(q) = \pi_{i_1}\left(T_{i_1}^{\beta_1}(p_1)\right) = [\pi_{i_1}(p_1) + \beta_1]_{r_{i_1}}$. So, if $i_1 \neq 1$ then (47), with $i = i_1$, yields a contradiction with (49). If $i_1 = 1$ then (48) contradicts (50).

Case 3: $\mathcal{B}_2 \neq \emptyset$ **and** $Y \geq 2$. Let $\mathcal{B}_2 = \{p_1\}$. Then $[\pi_n(p_1) + \beta_0]_{r_n} \geq \chi_1$. Take $i_\rho \in J$, with $m'+1 \leq \rho \leq m$. Since $i_\rho \in \Lambda(u_1 - 1)$, one has that $f'[S^{n-i_\rho-1}(u_1-1), 1] < r_{i_\rho}$. Now, given $v = (v_n, \ldots, v_{i_\rho}) \in \Upsilon_{n-i_\rho+2}(\mathcal{C}')$ such that $v_n \leq u_1 - 1$, by the Lemma 17 $a)$ we have that $f'[v_n, \ldots, v_{i_\rho}] \leq f'[S^{n-i_\rho-1}(u_1-1), 1]$. So, we take $\beta_{i_\rho} = r_{i_\rho} - \pi_{i_\rho}(p_1) - 1$, and we obtain that

$$\pi_{i_\rho}\left(T_{i_\rho}^{\beta_{i_\rho}}(p_1)\right) = [\pi_{i_\rho}(p_1) + \beta_{i_\rho}]_{r_{i_\rho}} = r_{i_\rho} - 1 > f'[v_n, \ldots, v_{i_\rho}]. \tag{51}$$

In case $i_\rho = 1$, an analogous argument by using $\pi_1(p_1)$ and the parameters $g'[\cdot]$ instead of $f'[\cdot]$, leads us to the following inequality

$$\pi_1\left(T_n^{\beta_1}(p_1)\right) > g'[v_n, \ldots, v_2]. \tag{52}$$

Now, we apply the Lemma 20 to $\mathcal{B}_1$, $A = B_0$, $\eta = \lambda_0$ and $\{\lambda_{i_k}\}_{k=1}^{m'}$, having in mind that $i_k \in \Lambda(u_2 - 1)$ for every $k = 1, \ldots, m'$. So, we obtain two families of sets $\{X_j\}_{j=1}^h$ and $\{B_j\}_{j=1}^h$ $(h \leq m')$, such that $B = B_0 \cup B_1 \cup \cdots \cup B_h$, where $\pi_{i_k}(x) \in X_k$, for every $k \in \{1, \ldots, h\}$ and for all $x \in B_k$.

Moreover, one has that there exists a family of positive integers $\{\beta_k\}_{k=1}^h$ such that for every $k = 1, \ldots, h$, given $a \in X_k$ and $v = (v_n, \ldots, v_{i_k+1}) \in \Upsilon_{n-i_k+1}(\mathcal{C}')$, with $v_n \leq u_2 - 1$, (45) and (46) hold.

Take $p \in B$ and let us see that $q = \left[\left(\prod_{j=1}^{h} T_{i_j}^{\beta_j}\right) \circ T_{i_\rho}^{\beta_{i_\rho}} \circ T_n^{\beta_0}\right](p) \notin \Gamma(\mathcal{C}')$. Again, we can assume without loss of generality that $p \notin B_0$. Suppose that $q \in \Gamma(\mathcal{C}')$. Then there exists $v = (v_n, \ldots, v_2) \in \Upsilon_n(\mathcal{C}')$ satisfying (47) and (48). Suppose that $p \in \mathcal{B}_1$. Let $k \in \{1, \ldots, h\}$ such that $p \in B_k$. Then, by (41) one has that $[\pi_n(p) + \beta_0]_{r_n} \geq \chi_2$, so $v_n \leq u_2 - 1$, by (47), with $i = n$. On the other hand, $\pi_{i_k}(p) \in X_{i_k}$ and

$$\pi_{i_k}(q) = \pi_{i_k}\left(T_{i_k}^{\beta_k}(p)\right) = [\pi_{i_k}(p) + \beta_k]_{r_{i_k}}.$$

Therefore, if $i_k \neq 1$ then (47), with $i = i_k$, yields a contradiction with (45). If $i_k = 1$ then (48) contradicts (46). Last, let $p = p_1$. Then, on the one hand, $[\pi_n(p) + \beta_0]_{r_n} \geq \chi_1$, so $v_n \leq u_1 - 1$. On the other hand, $\pi_{i_\rho}(q) = \pi_{i_\rho}\left(T_{i_\rho}^{\beta_{i_\rho}}(p_1)\right) = [\pi_{i_\rho}(p_1) + \beta_{i_\rho}]_{r_{i_\rho}}$. So, if $i_\rho \neq 1$ then (47), with $i = i_\rho$, leads us to a contradiction with (51). If $i_\rho = 1$ then (48) contradicts (52).

Case 4: $\mathcal{B}_2 = \emptyset$**.** In this case we have that $B = \mathcal{B}_1$. The proof is analogous to Case 1, by applying the Lemma 20 to B, $A = B_0$, $\eta = \lambda_0$ and $\{\lambda_{i_j}\}_{j=1}^m$, and by using that $i_k \in \Lambda(u_2 - 1)$ for all $k = 1, \ldots, m$. ■

VI. Applications

In this section, we shall show some applications of our results. Concretely, we use Theorem 21, Theorem 22, Theorem 23 and Proposition 26 as criteria to design abelian codes having determined permutation decoding properties. Moreover, we may determine upper bounds on the dimension of codes of certain lengths satisfying such properties.

First, we present two examples of codes that we have chosen having in mind the tables in [18] and [19], together with the updates in [3]. Finally, we present an example of a ternary three-dimensional and 3-error-correcting abelian code, to show how our techniques work in a more general context than that considered in [7], [10], [16], [17], [19].

In [18] and [19], Shiva, Fung and Tan obtained upper bounds on the dimension of 2 and 3-error-correcting cyclic codes of certain lengths which are permutation decodable with respect to the usual information set (consecutive positions). They always obtain PD-sets generated by both the permutations T_j (that they denote by R_0) and some powers of the Frobenius automorphism of $\mathbb{F} = \mathbb{F}_q$, that we denote by σ, acting on $\mathbb{A}(r_1, \ldots, r_n)$ via $\sigma\left(\sum_j a_j X^j\right) = \sum_j a_j X^{q \cdot j}$. Shiva *et al.* denote the i-th power of the Frobenius automorphism by R_i, that is, $R_i = \sigma^i$.

Again, it may be necessary to revise the construction of $\Gamma(\mathcal{C})$ in Section III, more precisely the definitions from (4) to (8), and Definition 18.

We begin by updating 2-error-correcting cyclic codes of length 51. In [18, p. 642] Shiva *et al.*, assert that, for dimension $k > 33$ permutation decoding is not possible under the usual information set.

Example 27. We shall design a binary $(51, 34, 6)$ code $\mathcal{C}$, with maximum dimension such that it has a PD-set $\langle T_1,\ T_2\rangle$, with respect to the information set $\Gamma(\mathcal{C}')$. To do this, we begin by considering all 2-orbits modulo $(3, 17)$; that is, $r_1 = 3$ and $r_2 = 17$. Set $\overline{D}$ a set of restricted representatives (see Definition 4) of the whole space $\mathbb{Z}_3 \times \mathbb{Z}_{17}$, as in Section IV,

$$\overline{D} = \{(0,0),(0,1),(0,3),(1,0),(1,1),(1,2),(1,3),(1,6)\}\,.$$

We are going to construct our codes as sums of minimal codes. The following table describe all minimal abelian codes in $\mathbb{A}(3, 17)$ in terms of the corresponding defining sets.

Code	$\overline{D}(\mathcal{C}')$	$M'(0)$	$M'(1)$	dimension
$\mathcal{C}_1$	$(0,0)$	1	0	1
$\mathcal{C}_2$	$(0,1)$	8	0	8
$\mathcal{C}_3$	$(0,3)$	8	0	8
$\mathcal{C}_4$	$(1,0)$	0	1	2
$\mathcal{C}_5$	$(1,1)$	0	4	8
$\mathcal{C}_6$	$(1,2)$	0	4	8
$\mathcal{C}_7$	$(1,3)$	0	4	8
$\mathcal{C}_8$	$(1,6)$	0	4	8

First, we look for codes satisfying the condition given in Theorem 21. So, there must exist a subset I of $\Delta(s') \subseteq \{1,2\}$ such that $\sum_{i\in I} \lambda_i(s') \geq 2$. A first posibility is that $|I| = 1$. In this case, it must happen that $f'[1] < 9$ or $g'[s'] < 2$. Note that, under the condition $g'[s'] < 2$, all possible values for the $g'[\cdot]$ are $1, 2$ and 3, and then $s' = 1$. Having in mind the table above, we have that any sum of minimal codes that reaches the value $f'[1] < 9$ has dimension at most 24 (for example, $\mathcal{C} = \mathcal{C}_2 + \mathcal{C}_5 + \mathcal{C}_6$), while any sum of minimal codes reaching $g'[1] < 2$ has dimension at most 17 (there is only one case: $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2 + \mathcal{C}_3$). On the other hand, under the condition $|I| = 2$ it must happen that

$$f'[1] < 17 \quad \text{and} \quad g'[s'] < 3. \tag{53}$$

Again, having in mind the range of possible values for those $g'[\cdot]$'s, we obtain $s' = 1$. Any sum of minimal codes satisfying (53) has dimension at most 32. However, this dimension is reached only by $\mathcal{C} = \mathcal{C}_5 + \mathcal{C}_6 + \mathcal{C}_7 + \mathcal{C}_8$ and in this case, one may check that $d(\mathcal{C}) = 4$; so that it is not a 2-error-correcting code. All 2-error-correcting codes satisfying (53) have dimension at most 26 (for example, $\mathcal{C} = \mathcal{C}_4 + \mathcal{C}_5 + \mathcal{C}_6 + \mathcal{C}_7$).

Now we are looking for codes satisfying the condition in Theorem 22. We separate in two cases depending on the possible values of λ_0. In case $\lambda_0 = 2$ we get $f'[1] < 9$ which brings us back to the case of Theorem 21. For $\lambda_0 = 0$ we get $g'[u-1] = g'[1] < 2$, wich drives us to cases already seen. So, consider the case $\lambda_0 = 1$. Then $9 \leq f'[1] < 17$ and it must happen that $g'[u-1] < 3$ (note that $\Lambda(u-1) \setminus \{2\} \subseteq \{1\}$). It may appear at most two nonzero different values of parameters $M'[\cdot]$ and so the same happens with $f'[\cdot]$. So, if $u = 3$ then $s' = 2$ and $g'[2] = 3$. Hence, in order to get $g'[u-1] < 3$ it must be $u = 2$. If $s' = 1$ then we get condition (53). Therefore there is only one new case which is

$$9 \leq f'[1] < 17, \;\; 0 < f'[2] < 9 \quad \text{and} \quad g'[1] < 3. \tag{54}$$

Any sum of minimal codes satisfying these conditions has dimension at most 40. However, one may check that all codes reaching this dimension must contain the sum $\mathcal{C}_5 + \mathcal{C}_6 + \mathcal{C}_7 + \mathcal{C}_8$, and as we have already seen this implies that their minimum distance is at most 4. By putting out one of the above minimal summands we get that the codes with minimum distance greater or equal to 5, satisfying condition (54) have dimension at most 34. For example

$$\mathcal{C} = \mathcal{C}_2 + \mathcal{C}_4 + \mathcal{C}_5 + \mathcal{C}_6 + \mathcal{C}_7,$$

whose minimum distance is 6. These codes trascend the bounds given in [18]. All other sufficient conditions are not applicable to this example.

Now we update 3-error correcting cyclic codes of length 63. In [19, Table X] its is obtained the bound on the dimension $k \leq 21$ using $R_0 = \langle T_1,\ T_2\rangle$ and $k \leq 35$ involving the Frobenius automorphism; that is, using $\langle\{T_1,\ T_2\} \cup \{\sigma\}\rangle$.

Example 28. We shall present a sketch of the study of codes with length 63. The first thing is to select the ambient algebra. It can be $\mathbb{A}(63)$ for cyclic codes, $\mathbb{A}(9, 7)$ for TDC codes or $\mathbb{A}(3, 3, 7)$. We consider this last case to illustrate that it is possible to obtain very good codes in the multidimensional case ($n \geq 3$). The minimal codes associated with the 2-orbits are in the following table.

Code	$D(C')$	dim.		Code	$D(C')$	dim.
C_1	$Q(0,0,0)$	1		C_9	$Q(1,2,0)$	2
C_2	$Q(0,0,1)$	3		C_{10}	$Q(1,0,1)$	6
C_3	$Q(0,0,3)$	3		C_{11}	$Q(1,0,3)$	6
C_4	$Q(0,1,0)$	2		C_{12}	$Q(1,1,1)$	6
C_5	$Q(0,1,1)$	6		C_{13}	$Q(1,1,3)$	6
C_6	$Q(0,1,3)$	6		C_{14}	$Q(1,2,1)$	6
C_7	$Q(1,0,0)$	2		C_{15}	$Q(1,2,3)$	6
C_8	$Q(1,1,0)$	2				

The application of Theorem 21 and Theorem 22 is completely analogous to Example 27 above, giving bounds of dimension 24 and 31, respectively. In this case, we may also apply Theorem 23, obtaining a bound of dimension 15, which is not so interesting.

By applying Proposition 26 we obtain codes of dimension 35; however all these codes are not 3-error correcting. The greatest dimension for a 3-error correcting code is 33; for example,

$$\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_4 + \mathcal{C}_{10} + +\mathcal{C}_{11} + \mathcal{C}_{12} + \mathcal{C}_{13} + \mathcal{C}_{14}$$

which has minimum distance 8. The bound given in [19, Table IX] for the dimension of 3-error correcting cyclic codes of lenght 63, with a PD set contained in $\{T_i\}_{i=1}^{n}$ with respect to the usual information set is 21.

Finally, we shall use our design techniques to find the best ternary 3-error correcting code $\mathcal{C}$ in $\mathbb{A}(4,4,4)$ which is permutation decodable with respect to $\Gamma(\mathcal{C}')$ and with PD-set $\langle T_1, T_2, T_3 \rangle$.

Example 29. We shall show a sketch of the the study of codes with length 64 in $\mathbb{A}(4,4,4)$. As in the previous examples, one has to consider all minimal codes associates with the 3-orbits in $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$. As the list has 36 items, it will be omitted.

By analysing the structure of the 3-orbits, having in mind Proposition 26, we obtain an upper bound of dimension 37, for 3-error correcting codes. This bound is reached, for example, by the code $\mathcal{C}$, such that $D(\mathcal{C}')$ is

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

In this case, $\Gamma(\mathcal{C}')$ is determined by the parameters

$$\begin{array}{ccccc} f'[1] = 3 & > & f'[2] = 2 & > & f'[3] = 1 \\ f'[1,1] = 3 & ; & f'[2,1] = 4 & ; & f'[3,1] = 4 \\ g'[1,1] = 3 & ; & g'[2,1] = 3 & ; & g'[3,1] = 4 \end{array}$$

By using Proposition 26, with $\lambda_0 = 1$, $u_1 = 3$, $u_2 = 2$, $\Lambda(u_1 - 1) = \{3, 1\}$ and $\Lambda(u_2 - 1) = \{3, 2, 1\}$, we may check that $\langle T_1, T_2, T_3 \rangle$ is a 3-PD-set with respect to $\Gamma(\mathcal{C}')$. In fact, it is a PD-set, because a direct computation of the minimum distance shows that $d(\mathcal{C}) = 8$.

Acknowledgement

The authors sincerely thank professor Ángel del Río for his helpful comments and suggestions.

References

[1] S. D. Berman, *Semisimple cyclic and Abelian codes*, Cybernetics, vol. 3, no. 3, pp. 21-30, 1967.

[2] J.J. Bernal, Á. del Río and J.J. Simón, *An intrinsical description of group codes*, Des. Codes, Crypto., vol. 51 , pp. 289-300, 2009.

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

[4] J.J. Bernal and J.J. Simón, *Information sets in abelian codes: defining sets and Groebner basis*, Des. Codes Crypto., DOI 10.1007/s10623-012-9735-x.

[5] B. Buchberger, *Groebner bases: An algorithm method in polynomial ideal theory*, Recent Trends in Multidimensional System Theory, Bose, Ed. Dordrecht: Reidel, 1985.

[6] P. Camion, *Abelian codes*, MRC Tech. Sum. Rep. no. 1059, Univ. of Wisconsin, Madison, 1970.

[7] H. Chabanne, *Permutation decoding of abelian codes*, IEEE Transactions on Information Theory, vol. 38, no. 6, pp. 1826-1829, 1992.

[8] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms*, Springer, 1992.

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

[10] H. Imai, *A theory of two-dimesional cyclic codes*, Information and Control, 34 pp. 1-21, 1977.

[11] J. M. Jensen, *The concatenated structure of cyclic and abelian codes*, IEEE Trans. Inform. Theory, vol. IT-31, pp. 788-793, 1985.

[12] J.D.Key, T.P. McDonough, V.C.Mavron *Partial permutation decoding for codes from finite planes*, European Journal of Combinatorics 26, pp. 665-682, 2005.

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

[14] F. J. MacWilliams *Permutation decoding of systematic codes*, Bell System Tech. J., vol. 43, pp. 485-505, 1964.

[15] F.J. MacWilliams, N. J. A. Sloane *The theory of error-correcting codes*, North-Holland, Amsterdam, 1983.

[16] S. Sakata, *On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals*, IEEE Trans. Inform. Theory, vol. IT-27, no. 5, pp. 556-565, 1981

[17] S. Sakata, *General theory of doubly periodic arrays over an arbitrary field and its applicationes*, IEEE Trans. Inform. Theory, vol. IT-24, no. 6, pp. 719-730, 1978.

[18] S. G. S. Shiva, K. C. Fung and H. S. Y. Tan, *On permutation decoding of binary cyclic double-error-correcting codes of certain lengths (Corresp.)*, IEEE Trans. Inform. Theory, vol. 16, no. 5 , pp.641-643, 1970.

[19] S. G. S. Shiva and K. C. Fung, *Permutation decoding on certain triple-error-correcting binary codes*, IEEE Trans. Inform. Theory, vol. 16, no. 5, pp. 641-643, 1970

José Joaquín Bernal was born in Murcia, Spain, in May 1976. He received the B.S. degree in mathematics in 1999 and the M.S. degree in advanced mathematics in 2007 from the University of Murcia. He received the Ph. D degree in 2011 from the University of Murcia.

From 2006 he was an Associate Professor in the Applied Mathematics Department in the Faculty of Computer Sciences, and in the Quantitative Methods Department of the Faculty of Economics and Business. His research interests include information theory, coding theory and cryptography.

Juan Jacobo Simón received its degree in mathematics in the UNAM of Mxico in 1988 and its Ph.D. degree in mathematics in the University of Murcia, Spain, in 1992.

Since 1995 he is professor in the University of Murcia. Dr. Simn has published papers in ring theory, group rings and coding theory.