HOMOMORPHIC ENCODERS OF PROFINITE ABELIAN GROUPS
II

MARÍA V. FERRER AND SALVADOR HERNÁNDEZ

ABSTRACT. Let \( \{G_i : i \in \mathbb{N}\} \) be a family of finite Abelian groups. We say that a subgroup \( G \leq \prod_{i \in \mathbb{N}} G_i \) is order controllable if for every \( i \in \mathbb{N} \) there is \( n_i \in \mathbb{N} \) such that for each \( c \in G \), there exists \( c_1 \in G \) satisfying that \( c_{1|[1,i]} = c_{|[1,i]} \), \( \text{supp}(c_1) \subseteq [1, n_i] \), and \( \text{order}(c_1) \) divides \( \text{order}(c_{|[1,n_i]}) \). In this paper we investigate the structure of order controllable group codes. It is proved that if \( G \) is an order controllable, shift invariant, group code over a finite abelian group \( H \), then \( G \) possesses a finite canonical generating set. Furthermore, our construction also yields that \( G \) is algebraically conjugate to a full group shift.

1. Introduction

In coding theory, a code refers to a set of sequences (the codewords), with good error-correcting properties, used to transmit information over nosy channels. In communication technology most codes are linear (that is, vector spaces on a finite field) and there are two main classes of codes: block codes, in which the codewords are finite sequences all of the same length, and convolutional codes, in which the codewords can be infinite sequences. However, some very powerful codes that were first thought to be nonlinear can be described as additive subgroups of \( A^n \), where \( A \) is a cyclic abelian group (see [1, 9]). This fact motivated the study of a more general class of codes.

Date: today.

Research Partially supported by the Spanish Ministerio de Economía y Competitividad, grant: MTM/PID2019-106529GB-I00 (AEI/FEDER, EU) and by the Universitat Jaume I, grant UJI-B2019-06.

2010 Mathematics Subject Classification. Primary 20K25. Secondary 22C05, 20K45, 54H11, 68P30, 37B10

Key Words and Phrases: profinite abelian group, controllable group, order controllable group, group code, generating set, homomorphic encoder.
According to Forney and Trott \[9, 10\], a *group code* \( G \) is a subgroup of a product

\[
X = \prod_{i \in I} G_i,
\]

where each \( G_i \) is a group and the composition law is the componentwise group operation. The subgroup

\[
G_f := G \cap \bigoplus_{i \in \mathbb{Z}} G_i
\]

is called the *finite subcode* of \( G \). It may happen that all elements of \( G \) has finite support, which means that \( G \) coincides with \( G_f \).

If all code symbols are drawn from a common group \( H \), then \( G \leq H^I \) and \( G \) will be called a group code over \( H \) defined on \( I \).

A key point in the study of group codes is the finding of appropriate *encoders*

**Definition 1.1.** Given a group code \( G \), a *homomorphic encoder* is a continuous homomorphism \( \Phi: \prod_{i \in I} H_i \to G \) that sends a full direct product of (topological) groups onto \( G \). Of special relevance are the so called *noncatastrophic encoders*, that is, homomorphic continuous encoders \( \alpha \) that are one-to-one and such that \( \Phi(\bigoplus_{i \in I} H_i) = G_f \) (see \[4, 9, 10\] for some references).

From here on, we deal with a *group shift* (or *group code*) \( G \) over a finite abelian group \( H \). That is, \( G \) is a closed, shift-invariant subgroup of the full shift group \( X = H^\mathbb{Z} \).

Therefore, if \( \sigma: X \to X \) denotes the *backward shift operator*

\[
\sigma[x](i) := x(i + 1), \; \forall x \in X, \; i \in \mathbb{Z},
\]

we have that \( \sigma(G) = G \). For simplicity’s sake, we denote the *forward shift operator* by \( \rho \), that is \( \rho[x](i) := x(i - 1), \; \forall x \in X, \; i \in \mathbb{Z} \). A group shift \( G \) over a finite abelian group \( H \) is *irreducible or transitive* if there is \( x \in G \) such that the partial forward orbit
\[ \{\sigma^n(x) : n \geq n_0\} \text{ is dense in } G \text{ for all } n_0 \in \mathbb{Z}. \]

Given two group codes \( G \) and \( \bar{G} \) if there is a homeomorphism (resp. topological group isomorphism) \( \Phi : G \rightarrow \bar{G} \) so that \( \sigma \circ \Phi = \Phi \circ \sigma \) then we say that \( G \) and \( \bar{G} \) are \textit{topologically conjugate} (resp. \textit{algebraically and topologically conjugate}) (see [11, 12, 16]).

In [8], Forney proved that every (linear) convolutional code is conjugate to a full shift, via a linear conjugacy. Subsequently, it was proved by several authors (see [9, 11, 13, 14]) that every irreducible group shift is conjugate to a full shift. In fact, one might expect that the conjugacy was also a group homomorphism (algebraic conjugacy). But, for group shifts, this turns to be false in general (cf. [11, 13]). In this sense, Fagnani [2] has obtained necessary and sufficient conditions for a group shift to be algebraically conjugate to the full shift over a finite group. His approach is based on Pontryagin duality, which let one reduce the question to its discrete dual group that turns out to be a finitely generated module of Laurent polynomials.

We next collect some definitions and basic facts introduced in [6].

\textbf{Definition 1.2.} Let \( G \) be a group shift over a finite abelian group \( H \). We have the following notions:

(1) \( G \) is \textit{weakly controllable} if \( G \cap H^{(\mathbb{Z})} \) is dense in \( G \); here \( H^{(\mathbb{Z})} \) denotes the subgroup of \( H^{\mathbb{Z}} \) consisting of the elements with finite support.

(2) \( G \) is \textit{controllable} \footnote{It is easily verified that every controllable group code \( G \) is irreducible (see [11]).} (equivalently \textit{irreducible} or \textit{transitive}) if there is a positive integer \( n_c \) such that for each \( g \in G \), there exists \( g_1 \in G \) such that \( g_1|(-\infty,0] = g|(-\infty,0] \) and \( g_1|n_c,\infty) = 0 \) (we assume that \( n_c \) is the least integer satisfying this property).

Remark that this property implies the existence of \( g_2 := g - g_1 \in G \) such that \( g = g_1 + g_2 \), \( \text{supp}(g_1) \subseteq (-\infty, n_c] \) and \( \text{supp}(g_2) \subseteq [1, +\infty[. \)
(3) \( G \) is order controllable if there is a positive integer \( n_o \) such that for each \( g \in G \), there exists \( g_1 \in G \) such that \( g_{1|(-\infty,0]} = g|(-\infty,0] \), \( \text{supp}(g_1) \subseteq (-\infty, n_o] \), and \( \text{order}(g_{1|[1,n_o]}) \) divides \( \text{order}(g|_{[1,n_o]} \)). Again, this implies the existence of \( g_2 \in G \) such that \( g = g_1 + g_2 \), \( \text{supp}(g_2) \subseteq [1, +\infty[ \), and \( \text{order}(g_2) \) divides \( \text{order}(g) \). Here, the order of \( g \) is taken in the usual sense, as an element of the group \( G \).

We now state our main result.

**Theorem 1.3.** Let \( G \) be an order controllable group shift over a finite abelian group \( H \). Then there is a noncatastrophic isomorphic encoder for \( G \). As a consequence \( G \) is algebraically and topologically conjugate to a full group shift.

### 2. Group shifts

In this section, we apply the result accomplished in [6, Theorem 3.2] in order to prove that order controllable group shifts over a finite abelian group possess canonical generating sets. Furthermore, our construction also yields that they are algebraically conjugate to a full group shift.

In the sequel \( H^{(\mathbb{Z})} \) will denote the subgroup of \( H^\mathbb{Z} \) consisting of all elements with finite support.

**Theorem 2.1.** Let \( G \) be a weakly controllable, group shift over a finite abelian \( p \)-group \( H \). If \( G[p] \) is weakly controllable, then there is a finite generating subset \( B_0 := \{x_j : 1 \leq j \leq m\} \subseteq G_f[p], \) where \( x_j = p^{h_j}y_j, \ y_j \in G_f, \) and each \( x_j \) is selected with the maximal possible height \( h_j \) in \( G_f \) with \( h_j \geq h_{j+1}, \ 1 \leq j < m, \) such that the following assertions hold true:
(1) There is a canonically defined $\sigma$-invariant, onto, group homomorphism
\[
\Phi: \left( \prod_{1 \leq j \leq m} \mathbb{Z}(p^{h_j}+1) \right)^\mathbb{Z} \to G.
\]

(2) $\Phi$ is a noncatastrophic, isomorphic encoder for $G$ if there is a finite block $[0, N] \subseteq \mathbb{N}$ such that the set
\[
\{ \sigma^n[x_j][0,N] \neq 0 : n \in \mathbb{Z}, 1 \leq j \leq m \}
\]
is linearly independent.

Proof. (1) Using that $G$ and $G[p]$ are weakly controllable, we can proceed as in [6] Theorem 3.2 in order to define a subset $B_0 := \{ x_1, \ldots, x_m \} \subseteq G_f[p][0,\infty)$ such that $\pi[0](B_0)$ forms a basis of $\pi[0](G_{[0,\infty]}[p])$ and for each $x_j \in B_0$ there is a nonnegative integer $h_j$ and an element $y_j \in G_f$ such that $x_j = p^{h_j}y_j$, where each $x_j$ has the maximal possible height $h_j$ in $G_f$ and $h_1 \geq h_2 \geq \cdots \geq h_m$. Now define
\[
\phi_0: \mathbb{Z}(p)^m \to G[p]
\]
by
\[
\phi_0[\lambda_1, \ldots, \lambda_m] = \lambda_1 x_1 + \cdots + \lambda_m x_m
\]
and, for each $n \in \mathbb{Z}, n > 0$, set $B_n := \rho^n(B_0) \subseteq G_f[p][n,\infty)$ and define
\[
\phi_n: \mathbb{Z}(p)^m \to G[p]
\]
by
\[
\phi_n[\lambda_1, \ldots, \lambda_m] = \lambda_1 \rho^n(x_1) + \cdots + \lambda_m \rho^n(x_m).
\]

Now, we can define
\[
\bigoplus_n \phi_n: \bigoplus_{n \geq 0} (\mathbb{Z}(p)^m)_n \to G_f[p][0,\infty)
\]
by
\[ \oplus_n \varphi_n \left[ \sum_{n \geq 0} (\lambda_{1n}, \lambda_{2n}, \ldots, \lambda_{mn}) \right] := \sum_{n \geq 0} \varphi_n [(\lambda_{1n}, \lambda_{2n}, \ldots, \lambda_{mn})], \]
where \((\mathbb{Z}(p)^m)_n = \mathbb{Z}(p)^m\) for all \(n \geq 0\).

Remark that all the maps set above are well defined group homomorphisms since each of these maps involves finite sums in its definition. Furthermore, since the range of \(\varphi_n\) is contained in \(G_f[p]_{[n, \infty)}\) for all \(n \geq 0\), it follows that the map \(\oplus_n \varphi_n\) is continuous when its domain (and its range) is equipped with the product topology. Therefore, there is a canonical extension of \(\oplus_n \varphi_n\) to a continuous group homomorphism
\[ \Phi_0 : \prod_{n \geq 0} (\mathbb{Z}(p)^m)_n \to G[p]_{[0, \infty)}. \]

Now, repeating the same arguments as in \([6, \text{Theorem 3.2}]\), it follows that
\[ G_f[p]_{[0, \infty)} \subseteq \Phi_0 (\prod_{n \geq 0} (\mathbb{Z}(p)^m)_n), \]
which implies that \(\Phi_0\) is a continuous onto group homomorphism because \(G_f[p]_{[0, \infty)}\) is dense in \(G[p]_{[0, \infty)}\). Furthermore, using the \(\sigma\)-invariance of \(G\), we can extend \(\Phi_0\) canonically to continuous onto group homomorphism
\[ \Phi_N : \prod_{n \geq -N} (\mathbb{Z}(p)^m)_n \to G[p]_{[-N, \infty)} \]
by
\[ \Phi_N [ \sum_{n \geq -N} (\lambda_{1n}, \lambda_{2n}, \ldots, \lambda_{mn})] := \sigma^N [ \Phi_0 [ \rho^N [ \sum_{n \geq -N} (\lambda_{1n}, \lambda_{2n}, \ldots, \lambda_{mn}) ]]], \]
for every \(N > 0\). Now, if we identify \(\prod_{n \geq -N} (\mathbb{Z}(p)^m)_n\) with the subgroup \((\prod_{n \in \mathbb{Z}} (\mathbb{Z}(p)^m)_n)_{[-N, +\infty)}\), remark that \(\Phi_{(N+1)}\) restricted to \(\prod_{n \geq -N} (\mathbb{Z}(p)^m)_n\) is equal to \(\Phi_N\). Therefore, we have defined a map
\[ \Phi_\infty : \bigcup_{N > 0} \prod_{n \geq -N} (\mathbb{Z}(p)^m)_n \to G[p]. \]
Again, because \( \bigcup_{N > 0} \prod_{n \geq -N} (\mathbb{Z}(p)^m)_n \) is dense in \((\mathbb{Z}(p)^m)^\mathbb{Z}\), it follows that we can extend \( \Phi_\infty \) to a continuous onto group homomorphism

\[
\Phi : (\mathbb{Z}(p)^m)^\mathbb{Z} \longrightarrow G[p].
\]

Now, taking into account that \( \lim_{n \to \pm \infty} \sigma^n(y_j) = 0 \) for all \( 1 \leq j \leq m \), we proceed as in [6, Theorem 3.2] in order to lift \( \Phi \) to a continuous onto group homomorphism

\[
\Phi : \left( \prod_{1 \leq j \leq m} \mathbb{Z}(p^{h_j+1}) \right)^\mathbb{Z} \longrightarrow G.
\]

This completes the proof of (1).

(2) First, we remark that repeating the proof accomplished in [6, Theorem 3.2], it follows that the sets \( \{ \sigma^n[x_j] : n \in \mathbb{Z}, 1 \leq j \leq m \} \) and \( \{ \sigma^n[y_j] : n \in \mathbb{Z}, 1 \leq j \leq m \} \) are both (linearly) independent.

Furthermore, since all elements \( x_j \) \( (1 \leq j \leq m) \) have finite support, it follows that the set \( \{ \sigma^n[x_j]|_{[0,N]} \neq 0 : n \in \mathbb{Z}, 1 \leq j \leq m \} \) is finite. Thus, using the \( \sigma \)-invariance of \( G \), we proceed as in [6, Theorem 3.2] to obtain that \( \Phi \) is one-to-one.

In order to prove that \( \Phi \) is noncatastrophic, that is \( \Phi^{-1}(\mathbb{Z}(p)) \subseteq G_f \), first notice that \( \Phi^{-1} \) is continuous, being the inverse map a continuous one-to-one group homomorphism. Now, reasoning by contradiction, suppose there is \( w \in G_f \) such that \((\lambda_n) = \Phi^{-1}(w)\) is an infinite sequence, let us say, without loss of generality, an infinite sequence on the right side. Then we have that the sequence \( (\sigma^n(w))_{n > 0} \) converges to 0 in \( G \). However, since \((\lambda_n)\) is infinite on the right side, it follows that the sequence \( (\Phi^{-1}(\sigma^n(w)))_{n > 0} = (\sigma^n((\lambda_n)))_{n > 0} \) does not converge to 0 in \((\prod_{1 \leq j \leq m} \mathbb{Z}(p^{h_j+1}))^\mathbb{Z}\). This contradiction completes the proof. \( \square \)
Definition 2.2. In the sequel, a set \( \{ y_1, \ldots, y_m \} \) (resp. \( \{ x_1, \ldots, x_m \} \)) that satisfies the properties established in Theorem 2.1 is called topological generating set of \( G \) (resp. \( G[p] \)).

Next, we are going to use the preceding results in order to characterize the existence of noncatastrophic, isomorphic encoders. As a consequence, we also characterize when a group shift is algebraically conjugate to a full group shift. First we need the following notions.

Definition 2.3. A group shift \( G \subseteq X = H^\mathbb{Z} \) is a shift of finite type (equivalently, is an observable group code) if it is defined by forbidding the appearance a finite list of (finite) blocks. As a consequence, there is \( N \in \mathbb{N} \) such that if \( x_1, x_2 \) belong to \( G \) and they coincide on an \( N \)-block \( [k, \ldots, k + N] \), then there is \( x \in G \) such that \( x|_{[-\infty, k+N]} = x_1|_{[-\infty, k+N]} \) and \( x|[k, \infty) = x_2|[k, \infty) \). It is known that if \( G \) is an irreducible group shift over a finite group \( H \), then \( G \) is also a group shift of finite type (see [11, Prop. 4]). Moreover, since every order controllable group shift \( G \) is irreducible, it follows that order controllable group shifts are of finite type.

Given an element \( x \in G_f \) with \( \text{supp}(x) = \{ i \in \mathbb{Z} : x(i) \neq 0 \} \), the first index (resp. last index) \( i \in \text{supp}(x) \) is denoted by \( i_f(x) \) (resp. \( i_l(x) \)). The length of \( \text{supp}(x) \) is defined as \( |\text{supp}(x)| := i_l(x) - i_f(x) + 1 \).

Proposition 2.4. Let \( G \) be a weakly controllable, group shift of finite type over a finite abelian \( p \)-group \( H \). If \( \exp(H) = p \), then there is a noncatastrophic isomorphic encoder for \( G \). As a consequence \( G \) is algebraically and topologically conjugate to a full group shift.
Proof. First, remark that $G = G[p]$ in this case. By Theorem 2.1, there is a topological generating subset $\mathcal{B}_0 := \{x_j : 1 \leq j \leq m\} \subseteq G_{f[0,\infty]}[p] = G_{f[0,\infty]}$ such that $\pi_{[0]}(\mathcal{B}_0)$ forms a basis of $\pi_{[0]}(G_{[0,\infty]})$ and there is a canonically defined $\sigma$-invariant, onto, group homomorphism

$$\Phi : (\mathbb{Z}(p)^m)^2 \to G.$$ 

Furthermore, we select each element $x_j$ with minimal support in $G_{f[0,\infty]}$ and such that $|\text{supp}(x_1)| \leq \cdots \leq |\text{supp}(x_m)|$.

By Theorem 2.1 (2), it will suffice to verify that there is a finite block $[0, N] \subseteq \mathbb{N}$ such that the set $\{\sigma^n[x_j][0,N] \neq 0 : n \in \mathbb{Z}, 1 \leq j \leq m\}$ is linearly independent. Indeed, let $N$ be a natural number such that $\text{supp}(x_j) \subseteq [0, N]$ for all $1 \leq j \leq m$ and satisfying the condition of being a group shift of finite type for $G$. That is, if $\omega_1, \omega_2$ belong to $G$ and they coincide on any $N$-block $[k, \ldots, k+N]$, then there is $w \in G$ such that $w|_{(-\infty, k+N]} = w_1|_{(-\infty, k+N]}$ and $w|[k,N) = w_2|[k,N)$.

Reasoning by contradiction, let us suppose that there is a linear combination

$$\sum \lambda_{nj} \sigma^n(x_j)[0,N] = 0.$$ 

Since the set $\{\sigma^n[x_j] : n \in \mathbb{Z}, 1 \leq j \leq m\}$ is linearly independent, there must be an element $u = \sigma^{n_1}[x_{j_1}]$ (for some $n_1$ and $j_1$) such that $\text{supp}(u) \cap (-\infty, 0) \neq \emptyset$.

As a consequence, there exist $\{\alpha_{nj}\} \subseteq \mathbb{Z}(p)$ such that

$$u|[0,N] = \sum_{n \neq n_1, j \neq j_1} \alpha_{nj} \sigma^n(x_j)[0,N].$$
We select $u$ such that $i_f(u)$ is minimal among the elements satisfying this property. Set

$$v := \sum_{(n \neq n_1, j \neq j_1)} \alpha_{n,j} \sigma^n(x_j).$$

We have that $(u - v)_{[0,N]} = 0$.

Since $G$ is of finite type for $N$-blocks, there exists $w \in G$ such that $w_{(-\infty,N]} = (u - v)_{(-\infty,N]}$ and $w_{[0,\infty)} = 0$.

We have that $i_f(u) \leq i_f(w)$ and $i_l(w) < i_l(u)$. Therefore, we have found an element $w \in G_f$ with $|\text{supp}(w)| < |\text{supp}(u)|$. Therefore, we can replace $x_{j_1}$ by $\tilde{x}_{j_1} := \sigma^{-n_1}(w)$ and $|\text{supp}(\tilde{x}_{j_1})| < |\text{supp}(x_{j_1})|$. This is a contradiction with our previous selection of the (ordered) set $\{x_j : 1 \leq j \leq m\}$, which completes the proof. \qed

**Lemma 2.5.** Let $G$ be an order controllable group shift over a finite abelian $p$-group $H$. Then $G[p]$ and $p^rG$ are order controllable group shifts for all $r$ with $p^r < \exp(H)$. As a consequence, it holds that $(p^rG)_f = p^rG_f$ for all $r$ with $p^r < \exp(H)$.

**Proof.** It is obvious that $G[p]$ is order controllable. Regarding the group $p^rG$, take an arbitrary element $x = p^r y \in p^r G$. By the order controllability of $G$, there is $z \in G$ and $n_0 \in \mathbb{N}$ such that $y_{(-\infty,0]} = z_{(-\infty,0]}$, $\text{supp}(z) \subseteq (-\infty,n_0]$ and $\text{order}(z_{[1,n_0]})$ divides $\text{order}(y_{[1,n_0]})$. Then $p^r z \in p^r G$, $x_{(-\infty,0]} = p^r z_{(-\infty,0]}$, $\text{supp}(p^r z) \subseteq (-\infty,n_0]$ and $\text{order}(p^r z_{[1,n_0]})$ divides $\text{order}(x_{[1,n_0]})$.

Finally, it is clear that $p^r G_f \subseteq (p^rG)_f$. Next we check the reverse implication.

Let $y \in G$ such that $x = p^r y \in (p^rG)_f$. Then there are two integers $m, M$ such that $x \in G_{[m,M]}$. Assume that $M \geq 0$ without loss of generality. By order controllability,
Lemma 2.6. Let $z \in G$ such that $\sigma^{M}(y)_{(-\infty,0]} = z_{(-\infty,0]}$, $\text{supp}(z) \subseteq (-\infty, n_{0}]$ and $\text{order}(z)_{[1,n_{0}]}$ divides $\text{order}(\sigma^{M}(y))_{[1,n_{0}]}$. Hence, if $v = \sigma^{-M}(z)$, we have $y_{(-\infty,M]} = v_{(-\infty,M]}$, $\text{supp}(v) \subseteq (-\infty, M+n_{0}]$ and $\text{order}(v)_{[M+1,M+n_{0}]}$ divides $\text{order}(y)_{[M+1,M+n_{0}]}$. Therefore $x = p^{r}v$ with $v \in G_{(-\infty,M+n_{0})}$.

If $m - n_{o} > 0$, by order controllability, there is $u \in G$ such that $v_{(-\infty,0]} = u_{(-\infty,0]}$, $\text{supp}(u) \subseteq (-\infty, n_{0}] \subseteq (-\infty, m - 1]$ and $\text{order}(u)_{[1,n_{0}]}$ divides $\text{order}(v)_{[1,n_{0}]}$. Set $w = v - u$. We have that $w \in G_{[1,M+n_{0}]}$ and $x = p^{r}w$, which yields $x \in p^{r}G_{f}$.

If $m - n_{o} \leq 0$, set $N = m - n_{o} - 1$. By order controllability, there is $u_{1} \in G$ such that $\sigma^{N}(v)_{(-\infty,0]} = u_{1}(-\infty,0]$, $\text{supp}(u_{1}) \subseteq (-\infty, n_{0}]$ and $\text{order}(u_{1})_{[1,n_{0}]}$ divides $\text{order}(\sigma^{N}(v))_{[1,n_{0}]}$. Hence, if $u_{2} = \sigma^{-N}(u_{1})$, we have $v_{(-\infty,N]} = u_{2}(-\infty,N]$, $\text{supp}(u_{2}) \subseteq (-\infty, N+n_{0}] \subseteq (-\infty, m - 1]$ and $\text{order}(u_{2})_{[N+1,N+n_{0}]}$ divides $\text{order}(v)_{[N+1,N+n_{0}]}$. Set $w = v - u_{2}$. We have that $w \in G_{[N+1,M+n_{0}]}$ and $x = p^{r}w$, which again yields $x \in p^{r}G_{f}$.

This completes the proof.

Let $G$ be a group shift over a finite abelian $p$-group $H$ and let $G/pG$ denote the quotient group defined by the map $\pi : G \to G/pG$. We define the subgroup

$$(G/pG)_{f} := \{ \pi(u) : u \in G \text{ and } u(n) \in pH \text{ for all but finitely many } n \in \mathbb{Z} \}$$

**Lemma 2.6.** Let $G$ be an order controllable group shift over a finite abelian $p$-group $H$ and let $\{x_{1}, \ldots, x_{m}\} \subseteq (pG_{f})_{[0,\infty)}$ be a topological generating set of $pG$, where $x_{i} = py_{i}$, $y_{i} \in G_{f}$, $1 \leq i \leq m$. If $u \in G_{f}$ then there exist $v \in G_{f}[p]$ and $w \in \{ \{\sigma^{n}(y_{j}) : n \in \mathbb{Z}, 1 \leq j \leq m \} \}$ such that $u = v + w$. 
Proof. Since \( \{x_1, \ldots, x_m\} \) is a topological generating set of \( pG \), we have

\[
pu = \sum_{n \in \mathbb{Z}} \sum_{i=1}^{m} \lambda_{in} \sigma^n(x_i) = \sum_{n \in \mathbb{Z}} \sum_{i=1}^{m} \lambda_{in} p \sigma^n(y_i) = p \sum_{n \in \mathbb{Z}} \sum_{i=1}^{m} \lambda_{in} \sigma^n(y_i).
\]

Furthermore, since the group shift \( pG \) is of finite type and \((pG)_f = p(G_f)\) by Lemma 2.5, we can apply Proposition 2.4 to the group shift \( pG \), in order to obtain that the sum in the equality above only involves non-null terms for a finite subset of indices \( F \subseteq \mathbb{Z} \). Therefore

\[
pu = p \sum_{n \in F} \sum_{i=1}^{m} \lambda_{in} \sigma^n(y_i).
\]

Set

\[
w := \sum_{n \in F} \sum_{i=1}^{m} \lambda_{in} \sigma^n(y_i) \in G_f.
\]

Then

\[
u = w + (u - w),
\]

where \( w \in \{\sigma^n(y_j) : n \in \mathbb{Z}, 1 \leq j \leq m\} \) and \( p(u - w) = 0 \). It now suffices to take \( v := u - w \). \( \square \)

**Theorem 2.7.** Let \( G \) be an order controllable group shift (therefore, of finite type) over a finite abelian \( p \)-group \( H \). Then there is a noncatastrophic isomorphic encoder for \( G \). As a consequence \( G \) is algebraically and topologically conjugate to a full group shift.

**Proof.** Using induction on the exponent of \( G \), we will prove that there is topological generating set \( B_0 \) of \( G[p] \), where \( B_0 := \{x_1, \ldots, x_m\} \subseteq (pG_f[p])_{[0, \infty)} \) such that \( \pi_{[0]}(B_0) \) forms a basis of \( \pi_{[0]}((pG[p])_{[0, \infty)}) \) and for each \( x_j \in B_0 \) there is an element \( y_j \in G_f \) such that \( x_j = p^{h_j} y_j \). Furthermore \( G \) is algebraically conjugate to the full group shift generated by \( \mathbb{Z}(p^{h_1}) \times \ldots \mathbb{Z}(p^{h_m}) \).
The case \(\exp(G) = p\) has already been done in Proposition 2.4. Now, suppose that the proof has been accomplished if \(\exp(G) = p^h\) and let us verify it for \(\exp(G) = p^{h+1}\). We proceed as follows:

First, take the closed, shift invariant, subgroup \(pG\). We have that \(\exp(pG) = p^h\) and by the induction hypothesis, there is topological generating set \(B_0 \subseteq (pG[p])_{(0,\infty)}\) such that \(\pi_{[0]}(B_0)\) forms a basis of \(\pi_{[0]}((pG[p])_{[0,\infty)})\) and for each \(x_j \in B_0\) there is an element \(y_j \in pG_f\) such that \(x_j = p^h y_j\).

Since \(y_j \in pG_f\), there is \(z_j \in G_f\) such that \(y_j = p z_j\), \(1 \leq j \leq m\). Furthermore, we may assume that there is a finite block \([0, N_1] \subseteq \mathbb{N}\) such that the set \(\{\sigma^n[y_j]|_{[0,N_1]} \neq 0 : n \in \mathbb{Z}, 1 \leq j \leq m\}\) is linearly independent. As a consequence, using similar arguments as in [6, Theorem 3.2], it follows that the set \(\{\sigma^n[z_j]|_{[0,N_1]} \neq 0 : n \in \mathbb{Z}, 1 \leq j \leq m\}\) also is linearly independent. Therefore there is a canonically defined \(\sigma\)-invariant, onto, group homomorphism

\[
\Phi: \left( \prod_{1 \leq j \leq m} \mathbb{Z}(p^{h_i}) \right)^\mathbb{Z} \rightarrow pG.
\]

Now, we complete the set \(B_0 := \{x_1, \ldots, x_m\} \subseteq (pG)[p]_{[0,\infty)}\) with a finite set \(B_1 := \{u_1, \ldots, u_k\} \subseteq G[p]_{[0,\infty)}\) such that \(\pi_{[0]}(B_0 \cup B_1)\) is a basis of \(\pi_{[0]}(G[p])\). Remark that we must have \(h(u_i) = 0\) for all \(1 \leq i \leq k\), since \(\pi_{[0]}(B_0)\) forms a basis of \(\pi_{[0]}((pG[p])\).

Furthermore, arguing as in Proposition 2.4 we may assume that there is a finite block \([0, N_2] \subseteq \mathbb{N}\) such that the set

\[
E := \{\sigma^n[u_i]|_{[0,N_2]} : \sigma^n[u_i]|_{[0,N_2]} \neq 0 : n \in \mathbb{Z}, 1 \leq i \leq k\}
\]

is an independent subset of \(G[p]|_{[0,N_2]}\).

Now, consider the quotient group homomorphism

\[
qu: G \rightarrow G/pG
\]
and remark that \( G/pG \) is a group shift over \((H/pH)^\mathbb{Z}\). Making use of this quotient map, we select a basis

\[
V_1 := \{v_1, \ldots, v_k\} \subseteq G_f[p]_{[0, +\infty)}
\]
satisfying the following properties:

1. \( V_{1|[0,N_2]} \subseteq \{\{\sigma^n[u_i]|_{[0,N_2]} : \sigma^n[v_i]|_{[0,N_2]} \neq 0 : n \in \mathbb{Z}, 1 \leq i \leq k\}\}. \)
2. \( \pi_{[0]}(B_0 \cup V_1) \) is a basis of \( \pi_{[0]}(G[p]) \).
3. The set

\[
\{\sigma^n[v_i]|_{[0,N_2]} : \sigma^n[v_i]|_{[0,N_2]} \neq 0 : n \in \mathbb{Z}, 1 \leq i \leq k\}
\]

is independent.
4. Each \( q(v_i) \) has the minimal possible support in \((G/pG)_f\). That is

\[
|\text{supp}(q(v_1))| \leq \cdots \leq |\text{supp}(q(v_k))|
\]

where, if \( \text{supp}(q(v_i)) = \{\ldots, l_1, \ldots, l_p\} \), then \( |\text{supp}(q(v_i))| := l_p - l_1 + 1 \).

It is straightforward to verify that \( q(G_f) \subseteq (G/pG)_f \) and, as a consequence, it follows that the group \( G/pG \) is controllable and its controllability index is less than or equal to the controllability index of \( G \). As in Theorem 2.1, the topological generating set \( \{v_1, \ldots, v_k\} \cup \{z_1, \ldots, z_m\} \) defines a continuous onto group homomorphism

\[
\Phi : \left( \mathbb{Z}(p)^k \times \prod_{1 \leq j \leq m} (\mathbb{Z}_{p|m+1})^\mathbb{Z} \right) \to G
\]

By Theorem 2.1, in order to prove that \( \Phi \) is one-to-one, it will suffice to find some block \([0, N] \in \mathbb{Z}\) such that

\[
S := \left( \{\sigma^s[v_i]|_{[0,N]} \neq 0 : s \in \mathbb{Z}, 1 \leq i \leq k\} \cup \{\sigma^n[z_j]|_{[0,N]} \neq 0 : n \in \mathbb{Z}, 1 \leq j \leq m\} \right)_{[0,N]}
\]

forms and independent subset of \( G_{|[0,N]} \).
Since that this property holds separately for \( \{z_1, \ldots, z_m\} \) on the block \([0, N_1]\) and \( \{v_1, \ldots, v_k\} \) on the block \([0, N_2]\), it will suffice to verify that if we denote by \( Y \) to the group shift generated by \( \{z_1, \ldots, z_m\} \) and by \( U \) to the group shift generated by \( \{v_1, \ldots, v_k\} \), then there is an block \([0, N] \subseteq \mathbb{Z}\) such that

\[
(Y \cap U)_{|[0,N]} = \{0\}.
\]

Since this implies that \( S_{|[0,N]} \) is an independent subset.

Indeed, take \( N \geq \max(2N_1, 2N_2) \). Then, reasoning by contradiction, assume we have a sum

\[
\left( \sum \alpha_i \sigma^n(v_i) + \sum \beta_j \sigma^s(z_j) \right)_{|[0,N]} = \{0\}.
\]

Remark that we may assume that this sum is finite without loss of generality since \( G \) is order controllable. Then

\[
p\left( \sum \alpha_i \sigma^n(v_i) + \sum \beta_j \sigma^s(z_j) \right)_{|[0,N]} = \left( \sum p\alpha_i \sigma^n(v_i) + \sum p\beta_j \sigma^s(z_j) \right)_{|[0,N]} = \{0\}
\]

this yields

\[
\sum p\beta_j \sigma^s(z_j)_{|[0,N]} = \sum \beta_j \sigma^s(y_j)_{|[0,N]} = \{0\}.
\]

Since \( N \geq N_1 \), this implies that

\[
\sum \beta_j \sigma^s(y_j) = \{0\}.
\]

This means that \( \beta_j = p\gamma_{js} \) for every index \( js \). Thus we have

\[
\left( \sum \alpha_i \sigma^n(v_i) + \sum p\gamma_{js} \sigma^s(z_j) \right)_{|[0,N]} = \{0\}.
\]

Now, we select an element \( \sigma^n(v_i) \) such that \( i_j(q(\sigma^n(u_i))) \) is minimal among the elements satisfying this property. Suppose without loss of generality that \( \sigma^n(v_i) = \sigma^{n_1} v_1 \) for simplicity’s sake. Solving for \( \sigma^{n_1} v_1 \) in the equality above, we have

\[
\sigma^{n_1} v_1_{|[0,N]} = \left( \sum_{n \neq n_1, i \neq 1} \alpha_i' \sigma^n(v_i) + \sum p\gamma_{js}' \sigma^s(z_j) \right)_{|[0,N]} = \{0\}.
\]
Set
\[ w := \sum_{n \neq n_1, i \neq 1} \alpha'_m \sigma^n(v_i) \]
and set
\[ w_1 := \sigma^{n_1}v_1 - w. \]
Remark that \( pw_1 = 0 \), that is \( w_1 \in G[p] \) and
\[ w_1[0,N] = \sum p\gamma'_{js} \sigma^s(y_j)[0,N] \in pH. \]
Therefore
\[ \text{supp}(q(w_1)) \cap [0, N] = \emptyset. \]
Since \( G \) is a group shift of finite type, there is \( w_2 \in G \) such that
\[ w_2[(-\infty,N] = w_1[-\infty,N] \quad \text{and} \quad w_2[0,\infty) = \sum p\gamma'_{js} \sigma^s(y_j)[0,\infty). \]
From the way \( w_2 \) has been defined, we have that \( \sigma^{-n_1}(w_2) \in G_f[p][0,\infty) \) satisfies that
\[ \sigma^{-n_1}(w_2)[0,N_2] \in \{ \sigma^n[v_i][0,N_2] : \sigma^n[v_i][0,N_2] \neq 0 : n \in \mathbb{Z}, 1 \leq i \leq k \} \]
and
\[ |\text{supp}(q(w_2))| \leq |\text{supp}(q(\sigma^{n_1}(v_1)))|. \]
This is a contradiction and completes the proof. \( \square \)

We can now proof Theorem 1.3.

**Proof of Theorem 1.3.** Since every finite abelian group is the direct sum of all its nontrivial p-subgroups, the proof follows from Theorem 2.7 in like manner as [6, Theorem A] follows from [6, Theorem 3.2]. \( \square \)

**QUESTION:** Under what conditions is it possible to extend Theorem 1.3 to non-abelian groups?
References

[1] A. R. Calderbank, A. Roger Hammons Jr., P. Vijay Kumar, N. J. A. Sloane, Patrick Solé, A linear construction for certain Kerdock and Preparata codes. Bulletin AMS, 29 (1993), 218-222.
[2] F. Fagnani, Some results on the classification of expansive automorphisms of compact abelian groups, Ergodic Theory Dynam. Systems, 16, No. 5, (1996), 45-50.
[3] F. Fagnani, Shifts on compact and discrete Lie groups: Algebraic topological invariants and classification problems, Adv. Math., vol. 127, pp. 283-306, 1997.
[4] F. Fagnani, S. Zampieri, Dynamical Systems and Convolutional Codes Over Finite Abelian groups, IEEE Trans. Inform. Theory, vol. 42 (6), pp. 1892-1912, Nov. 1996.
[5] M.V. Ferrer, S. Hernández, Subdirect products of finite abelian groups, In: Ferrando J. (eds) Descriptive Topology and Functional Analysis II. TFA 2018. Springer Proceedings in Mathematics and Statistics, vol 286. Springer, (2019), 89-101.
[6] M.V. Ferrer, S. Hernández, Homomorphic encoders of profinite abelian groups I, Pending (2021).
[7] M.V. Ferrer, S. Hernández, D. Shakhmatov, Subgroups of direct products closely approximated by direct sums, Forum Mathematicum, 29, No. 5, (2017), 1125-1144.
[8] G. D. Forney, Convolutional codes I: Algebraic structure, IEEE Trans. Inform. Theory, vol. 16 (1970), 1491-1513.
[9] G. D. Forney, Jr. and M. D. Trott, The dynamics of group codes: State spaces, trellis diagrams and canonical encoders, IEEE Trans. Inform. Theory, vol. 39 (1993), 1491-1513.
[10] G. D. Forney, Jr. and M. D. Trott, The Dynamics of Group Codes: Dual Abelian Group Codes and Systems, Proc. IEEE Workshop on Coding, System Theory and Symbolic Dynamics (Mansfield, MA), pp. 35-65 (2004).
[11] B. Kitchens, Expansive dynamics on zero-dimensional groups, Ergodic Theory and Dynamical Systems, 7, no. 2, (1987), 249–261.
[12] B. P. Kitchens and K. Schmidt, Automorphisms of compact groups, Ergod. Th. Dynam. Sys. 9, (1989), 691–735.
[13] H.-A. Loeliger, T. Mittelholzer, Convolutional codes over groups, IEEE Trans. Inform. Theory, 42, no. 6, (1996), 1660–1686.
[14] G. Miles, R. K. Thomas, The breakdown of automorphisms of compact topological groups, Academic Press (Studies in probability and ergodic theory), Adv. in Math. Suppl. Stud. vol 2 (1978), 207–218.
[15] J. Rosenthal, S.M. Schumacher and E.V. York, On Behaviors and Convolutional Codes, IEEE Trans. on Information Theory, 42 (1996), no. 6, 1881–1891.
[16] K. Schmidt, Automorphisms of compact abelian groups and affine varieties, Proc. London Math. Soc. 61 (1990), 480–496.

Universitat Jaume I, Instituto de Matemáticas de Castellón, Campus de Riu Sec, 12071 Castellón, Spain.
Email address: merrer@mat.uji.es

Universitat Jaume I, INIT and Departamento de Matemáticas, Campus de Riu Sec, 12071 Castellón, Spain.
Email address: hernande@mat.uji.es