Note
Relating propelinear and binary $G$-linear codes

Marcelo M.S. Alves$^{a,*}$, João R. Gerônimo$^b$, Reginaldo Palazzo Jr.$^c,^2$, Sueli I.R. Costa$^a$, J. Carmelo Interlando$^d,^3$, Martinho C. Araújo$^{a,e}$

$^a$Departamento de Matemática, Instituto de Matemática, Universidade Estadual de Campinas (UNICAMP), 13081-970 Campinas, SP, Brazil
$^b$Departamento de Matemática, Universidade Estadual de Maringá (UEM), Paraná, Brazil
$^c$Departamento de Telemática, UNICAMP, 13081-970 Campinas, Brazil
$^d$Departamento de Matemática, Universidade Estadual Paulista (UNESP), 15054-000, São José do Rio Preto, Brazil
$^e$Departamento de Matemática - UFMT, Rondonópolis, Brazil

Received 5 January 1999; revised 6 December 2000; accepted 22 January 2001

Abstract

In this paper we establish the connections between two different extensions of $Z_4$-linearity for binary Hamming spaces. We present both notions – propelinearity and $G$-linearity – in the context of isometries and group actions, taking the viewpoint of geometrically uniform codes extended to discrete spaces. We show a double inclusion relation: binary $G$-linear codes are propelinear codes, and translation-invariant propelinear codes are $G$-linear codes. © 2002 Elsevier Science B.V. All rights reserved.

Keywords: Binary codes; $Z_4$-linearity; Propelinear codes; Isometry groups; $G$-linearity.

1. Introduction

The main concepts involved in this paper are the ones related to binary propelinear and binary $G$-linear codes. Both concepts have the same objective, that is, to induce a group structure into nonlinear codes. The search for such a structure arises from the possibility of reducing the decoding complexity.

* Corresponding author.

E-mail addresses: muniz@ime.unicamp.br (M.M.S. Alves), geronimo@dma.uem.br (J.R. Gerônimo), palazzo@dt.fee.unicamp.br (R.Jr.), sueli@ime.unicamp.br (S.I.R. Costa), carmelo@mat.ibilce.unesp.br (J.C. Interlando), martinho@dt.fee.unicamp.br (M.C. Araújo).

1 Supported by FAPESP - Brazil, 97/12270-8
2 Supported partially by FAPESP, 95/4720-8, and by CNPq - Brazil, 301416/85-0
3 Partially supported by CNPq - Brazil, 300187/95-5

0012-365X/02/$-see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0012-365X(01)00206-0
The $\mathbb{Z}_4$-linearity, established in [9], disclosed a correspondence between several well known classes of good binary nonlinear codes and submodules of $\mathbb{Z}_4^n$. Attempts to extend this concept have been done independently and in different ways, namely the concepts of propelinearity [12] for binary codes, and of $G$-linearity for $m$-ary codes [7,5,1].

The $\mathbb{Z}_4$-linear codes are based on the Gray map $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ given by $\phi(0) = 00$, $\phi(1) = 10$, $\phi(2) = 11$, $\phi(3) = 01$. This mapping extends coordinatewise to a mapping from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ where the Lee weight is preserved (where the Lee weight $w$ in $\mathbb{Z}_4^n$ is given by $w((v_1, ..., v_n)) = \sum \min\{v_i, 4 - v_i\}$).

A closer look at the Gray map gives ideas on how to extend the $\mathbb{Z}_4$-linearity. In the Hamming space $\mathbb{Z}_2^n$, consider the action of the symmetric group $S_n$ by coordinate permutations. For $u, v \in \mathbb{Z}_2^n$ and $\pi \in S_n$, let $(v, \pi)\cdot u = v + \pi(u)$. It is easy to see that this mapping preserves Hamming distance between vectors, that is, it is an isometry. We denote by $\Gamma(\mathbb{Z}_2^n, d_H)$ the symmetry group, that is, the group of isometries of the Hamming space $(\mathbb{Z}_2^n, d_H)$. In particular, for $n = 2$, $\Gamma(\mathbb{Z}_2^2, d_H) = \mathbb{D}_4$ is isomorphic to the symmetry group of a square. In this group, $g = (10, (12))$ is an element of order 4, and hence induces an action of $\mathbb{Z}_4$ on $(\mathbb{Z}_2^2, d_H)$ via $\tilde{\phi} : \mathbb{Z}_4 \to \langle g \rangle$, $\tilde{\phi}(k) = g^k$. Then we have $\phi(k) = \tilde{\phi}(k)(00)$, which means that the Gray map $\phi$ can be naturally obtained via an action of $\mathbb{Z}_4$ on $\mathbb{Z}_2^2$.

This approach of considering codes linked to these mappings composed of translations and coordinate permutations was done in [11,12] as an extension of the $\mathbb{Z}_4$-linearity. However, one can look at the Gray map from another viewpoint. The mapping $(10, (12))$ is an isometry of $\mathbb{Z}_2^2$, and $\mathbb{Z}_4$ corresponds to the subgroup of isometries of $\mathbb{Z}_2^2$ generated by a quarter of a turn rotation on the square $\mathbb{Z}_2^2$. Furthermore, we may consider subgroups of isometries of $\mathbb{Z}_2^2$ other than $\mathbb{Z}_4$, with some extra constraints on their actions in order to still get some of the good properties of the $\mathbb{Z}_4$-linearity. This concept was introduced in [7,5] under the name of $G$-linearity. This extension was defined in a very broad sense for metric spaces in general.

We can say that the $G$-linearity is also an adaptation of the concept of geometrically uniform codes [6] to discrete spaces. We point out that the $\mathbb{Z}_4$-linearity is a very special case of the $G$-linearity, when restricted to $m$-ary codes, in the sense that $\mathbb{Z}_4$ is the only cyclic group that fits the definition when considering either the Lee metric [5,2] or the Hamming metric [10,3,4] in $\mathbb{Z}_m^n$.

Under the restriction that the Hamming space is binary, we show that the propelinearity and the $G$-linearity are closely related.

We consider also the concept of translation-invariant propelinear codes introduced and completely classified in [12]. From this classification and from the results presented in this paper, the connections between the previously mentioned extensions of the $\mathbb{Z}_4$-linearity can be set for codes in the Hamming space $\mathbb{Z}_2^n$ as

Translation-Invariant Propelinear Codes $\subset G$-linear Codes $\subset$ Propelinear Codes.

In doing so, we also provide a geometric viewpoint of the propelinearity, showing that the group structure of a propelinear code is induced by the group structure of the symmetry group of the Hamming space where this code lies.
This paper is organized as follows. In Section 2, the basic definitions and examples are established. In Section 3, Theorems 1 and 2 establish the connection between propelinear codes and the mentioned symmetry groups. As a consequence, the inclusions just set are realized.

2. Preliminaries

Originally, the group structure of a propelinear code is induced by coordinate permutation, whereas in the \( G \)-linear code it is induced by a subgroup of the symmetry group acting freely and transitively in a Hamming space. Although these concepts employ distinct procedures of inducing a group structure into nonlinear codes, we show that both use basically symmetry subgroups and that a binary \( G \)-linear code is always propelinear.

In this paper, we specialize the concept of \( G \)-linearity introduced in [7,5] for \( m \)-ary codes in \( Z_m^n \) considered as a metric space with either the Lee or Hamming distance. We denote by \( \Gamma(Z_m^n, d) \) the full symmetry group, that is, the group of all mappings in \( Z_m^n \) which preserve the considered distance. Let \( G \) be a subgroup of \( \Gamma(Z_m^n, d) \) of order \( m^n \) and \( ev : G \to Z_m^n \) be the evaluation map \( ev(g) = g(0) \). If this mapping is onto, we have a free and transitive action of \( G \) and \( ev \) is called a labeling map. Let \( H \subset G \) be a subgroup. Then \( C = ev(H) \) is a code in \( Z_m^n \), which has many properties coming from homogeneity, such as the same distance profile for each codeword. We may also consider the extended action of \( G^k \) on \( Z_m^{kn} \) and an \( m \)-ary code \( \mathcal{C} = \tilde{ev}(\mathcal{H}) \), where \( \mathcal{H} \) is a subgroup of \( G^k \). In other words, \( C \) is the orbit \( \mathcal{H}(0) \) in \( Z_m^{kn} \). Such a code \( \mathcal{C} \) is called a \( G \)-linear code. Hence, we have the following:

Definition 1. Let \( G \) be a subgroup of \( \Gamma(Z_m^n, d) \) of order \( m^n \) such that the evaluation map \( ev(g) = g(0) \) is onto. Let \( G^k \) act on \( Z_m^{kn} \) via the natural extension of the action of \( G \) on \( Z_m^n \), and consider the evaluation map \( \tilde{ev} : G^k \to Z_m^{kn}, \tilde{ev}(g) = g(0) \). A code \( \mathcal{C} \subset Z_m^{kn} \) is \( G \)-linear if \( \mathcal{C} = \tilde{ev}(\mathcal{H}) \), where \( \mathcal{H} \) is a subgroup of \( G^k \).

Note that the \( G \)-linearity is an extension of the \( Z_4 \)-linearity inspired by the concept of geometrically uniform codes. Since in this paper we consider \( Z_2^n \), the Lee metric \( d_L \) and the Hamming metric \( d_H \) coincide.

In the following examples, we consider \( Z_2^n \) either naturally embedded in \( \mathbb{R}^n \) or identified with the vertex set \( V^n \) of a hypercube, \( V^n = \{ (\pm 1, \pm 1, \ldots, \pm 1) \} \). The group of isometries of the Hamming space \( \Gamma(Z_2^n, d_H) \) is precisely the Euclidean group of symmetries of the hypercube [7,5]. This consideration extends the geometric fact underlying the Gray map for \( n = 2 \). We will consider separately the cases \( n = 3, 4 \) and general \( n \).

Example 1. For \( n = 3 \), \( \Gamma(Z_2^3, d_H) \) is the Euclidean symmetry group of a cube which has 48 elements. The subgroups \( G \) of \( \Gamma(Z_2^3, d_H) \) which are either isomorphic to \( Z_4 \times Z_2 \)
or to the dihedral group $\mathbb{D}_4$ are the unique subgroups generating $G$-linear codes (besides the linear codes, where $G = \mathbb{Z}_2^4$ acts via translations).

A $\mathbb{Z}_4 \times \mathbb{Z}_2$ action $\Psi$ in $\mathbb{Z}_2^3 \cong V^3$ can be defined by identifying $(a,b) \in \mathbb{Z}_4 \times \mathbb{Z}_2$ with the isometry in $V^3$ given by the matrix

$$g(a,b) = \begin{bmatrix} 0 & -1^a & 0 \\ 1 & 0 & 0 \\ 0 & 0 & (-1)^b \end{bmatrix}, \quad \Psi(a,b) \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} := g(a,b) \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}.$$

In the cube $V^3$, this action is generated by a quarter-of-a-turn rotation, $R_2 = g(1,0)$, with respect to the vertical axis passing through the center, $O$, of the cube and by the reflection $g(0,1)$ on the horizontal plane through $O$. In the standard $\mathbb{Z}_2^3$ coordinates, $\Psi$ can be written as follows. For $(a,b) \in \mathbb{Z}_4 \times \mathbb{Z}_2$ and $(v_1, v_2, v_3) \in \mathbb{Z}_2^3$, $\Psi(a,b)(v_1, v_2, v_3) = (\phi(a)(v_1, v_2), b + v_3)$, where $\phi$ is the action induced by the Gray map $\phi$. A $\mathbb{D}_4$ action $\Theta$ in $\mathbb{Z}_2^3 \cong V^3$ can be generated by the symmetry $R_2$ in the cube $V^3$ just described and a half-of-a-turn rotation $\rho$ with respect to the horizontal axis $O\overline{y}$ ($\rho(v_1, v_2, v_3) = (-v_1, v_2, -v_3)$). This means that, if we consider the presentation of $\mathbb{D}_4$ given by $\mathbb{D}_4 = \langle r, s \mid r^4 = s^2 = \text{id}, srs = r^{-1} \rangle$ the action $\Theta$ maps the generators $r$ and $s$ to $R_2$ and $\rho$, respectively.

**Example 2.** For $n = 4$, besides the subgroups considered previously, we have a labeling of $\mathbb{Z}_2^4$ by the group $\mathbb{Q}_8 \cong \mathbb{Z}_2$ which generates $\mathbb{Q}_8 \cong \mathbb{Z}_2$-linear codes. Here we consider the following identifications: $\mathbb{R}^4$ with the quaternion algebra $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, and $V^4 \cong \mathbb{Z}_2^4$ with the set $C = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}$. $C$ is invariant under the action of the quaternionic group $\mathbb{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ (via left multiplication).

Besides, $C$ is also invariant under the $\mathbb{Z}_2$ action $\sigma$ via quaternionic conjugation: $\sigma(a + bi + cj + dk) = a - bi - cj - dk$. We can combine both actions, via composition, in a semidirect product $\mathbb{Q}_8 \rtimes \mathbb{Z}_2$ action. We point out that all group actions involved are free and correspond to isometries in the Hamming space. This extends an example given in [12] for $\mathbb{Q}_8$, and the $\mathbb{Q}_8 \cong \mathbb{Z}_2$-linear codes thus obtained include some translation-invariant propelinear codes.

**Example 3.** For general $n$, using the above construction for $n = 3$ we can induce through successive reflections group actions in $\mathbb{Z}_2^n \cong V^n$ by $G_1 = (\mathbb{Z}_4 \times \mathbb{Z}_2) \times \mathbb{Z}_2^{n-3} = (\mathbb{Z}_4 \times \mathbb{Z}_2^{n-2})$ and $G_2 = \mathbb{D}_4 \times \mathbb{Z}_2^{n-3}$ on $\mathbb{Z}_2^n$ and consider the associated $G_i$-linear codes in $\mathbb{Z}_2^n$, $n \geq 4$. In the same way, we can consider $(\mathbb{Q}_8 \rtimes \mathbb{Z}_2) \times \mathbb{Z}_2^{n-4}$-linear codes in $\mathbb{Z}_2^n$, $n \geq 5$, starting from the previous construction for $n = 4$.

$G$-linearity is an extension of the $Z_4$-linearity inspired by the concept of geometrically uniform codes, whereas propelinearity extends the $Z_4$-linearity via permutation groups.

**Definition 2 (Rifà and Pujol [12]).** Let $C$ be a subset of $\mathbb{Z}_2^n$ that contains the zero codeword. We say that $C$ is a propelinear code if there exists a set of permutations...
\( \Pi = \{ \pi_v \mid v \in C \} \subset S_n \) such that

1. For every \( v \in C \), \( v + \pi_v(s) \in C \) if and only if \( s \in C \);
2. For every \( \pi_u, \pi_v \in \Pi \), \( \pi_u \pi_v = \pi_w \in \Pi \), where \( w = u + \pi_v(v) \).

Considering the operation

\[ \star : C \times C \rightarrow C, \quad (u, v) \mapsto u \star v := u + \pi_u(v), \]

we define a subclass of the class of all propelinear codes by:

**Definition 3 (Rifà and Pujol [12])**. Let \( C \) be a propelinear code. We say that \( C \) is a translation-invariant propelinear code if and only if the operation \( \star \) preserves Hamming distance, that is, for all \( u, v \in C \) and \( x \in Z_2^n \), we have \( d(u, v) = d(u \star x, v \star x) \).

In the next section we describe the propelinearity concept in terms of symmetry groups and show that

Translation-invariant Propelinearity \( \Rightarrow \) \( G \)-linearity \( \Rightarrow \) Propelinearity.

### 3. Relating propelinearity and \( G \)-linearity

We start with a geometric characterization of the propelinear codes. Considering the mapping \( \pi : C \rightarrow S_n \), \( \pi(v) = \pi_v \), given by Definition 2, its graph \( \Omega(\pi) = \{(v, \pi_v) \mid v \in C \}\) can be identified as a subset of the full symmetry group \( \Gamma(Z_2^n, d_{HI}) \). In fact, as we show next, this subset is a subgroup of \( \Gamma(Z_2^n, d_{HI}) \), which is isomorphic to \( Z_2^n \rtimes S_n \) (where the semidirect product is the wreath product of \( Z_2 \) and \( S_n \), see [8]).

Let \( C \) be a propelinear code, and consider the graph \( \Omega(\pi) \) of the map \( \pi \) from \( C \) into \( S_n \). For \( (v, \pi_v) \) and \( (u, \pi_u) \) in \( \Omega(\pi) \), we have

\[ (v, \pi_v)(u, \pi_u) = (v + \pi_v(u), \pi_v \pi_u) = (v + \pi_v(u), \pi_v + \pi_u(u)) \]

by (2) of Definition 2. Since \( u \in C \), it follows that \( v + \pi_v(u) \in C \) (by (1) of Definition 2), and then \( \Omega(\pi) \) is closed under group product. \( \Pi \) is a subgroup of \( S_n \), [11], and then \( C \ni 0 = u + \pi_u (-\pi_u^{-1}(u)) \) implies that \( -\pi_u^{-1}(u) \in C \) ((1) again). This finishes the proof that \( \Omega(\pi) \) is a subgroup, for \( (u, \pi_u)^{-1} = (-\pi_u^{-1}(u), \pi_u^{-1}) \in \Omega(\pi) \), for every \((u, \pi_u) \in \Omega(\pi) \).

On the other hand, suppose that for a code \( C \) we have a map \( \pi : C \rightarrow S_n \) with \( \Omega(\pi) = \{(v, \pi_v) \mid \forall v \in C \}\) being a subgroup of \( Z_2^n \rtimes S_n \). This is a straightforward verification for (2) of Definition 2. Item (1) is also easily checked: let \( v \in C \) and \( s \in Z_2^n \) be such that \( w = v + \pi_v(s) \in C \), and let \((w, \pi_w)\) be the corresponding element in \( \Omega(\pi) \). Since \( (-\pi_v^{-1}(v), \pi_v^{-1}) = (v, \pi_v)^{-1} \), \( s = \pi_v^{-1}(w) - \pi_v^{-1}(v) \) belongs to \( C \) since this is the first coordinate of the product \((-\pi_v^{-1}(v), \pi_v)(w, \pi_w) \in \Omega(\pi) \).

Now, it is clear that propelinear codes are in bijection with subgroups \( \Omega \) of \( \Gamma(Z_2^n) \) that can be obtained as graphs \( \Omega = \{(v, \pi_v) \mid v \in C \}\) for some subset \( C \) of \( Z_2^n \). Thus we have proved:
Lemma 1. Let \((\mathbb{Z}_2^n,d_H)\) be the \(n\)-dimensional Hamming space and \(S_n\) the symmetric group of degree \(n\). A subset \(C \subseteq \mathbb{Z}_2^n\) with \(0 \in C\) is a propelinear code with length \(n\) if and only if there exists a function

\[
\pi : C \rightarrow S_n
\]

\[
v \mapsto \pi_v
\]

such that its graph

\[
\Omega(\pi) = \{(v, \pi_v) \mid \forall v \in C\}
\]

is a subgroup of the isometry group of \(\mathbb{Z}_2^n\), denoted by \(\mathbb{Z}_2^n \triangleright S_n\).

This lemma leads directly to the main results of this paper:

Theorem 1. A binary code \(C\) containing the zero codeword is propelinear if and only if there exists a subgroup \(N\) of \(\text{Aut}(\mathbb{Z}_2^n) \cong \mathbb{Z}_2^n \triangleright S_n\) with \(C = N(0)\) and \(|C| = |N|\).

Proof. Assume that \(C \subseteq \mathbb{Z}_2^n\) is a propelinear code. Hence, the graph \(\Omega(\pi)\) is a subgroup of \(\text{Aut}(\mathbb{Z}_2^n) \cong \mathbb{Z}_2^n \triangleright S_n\). The natural identification of \(\Omega(\pi)\) with \(C\) (given by \(f \mapsto f(0)\)) induces a transitive action of \(\Omega(\pi)\) on \(C\). We can also see that this action is free on \(C\): since \(f(0) \neq g(0)\) if \(f \neq g\), the stabilizer of \(0\), \(\Gamma_0(C) = \{f \in \Omega(\pi) \mid f(0) = 0\}\) is trivial. But for any other point \(x\) of \(C\) one has \(x = f(0)\) for some \(f \in \Omega(\pi)\), and its stabilizer is conjugate to \(\Gamma_0(C)\), therefore, it is also trivial (\(\Gamma_x(C) = \Gamma_f(0)(C) = f \Gamma_0(C) f^{-1}\)).

For the converse, let \(\bar{\pi} : \mathbb{Z}_2^n \triangleright S_n \rightarrow S_n\) be the projection \((v, \pi) \mapsto \pi\). The hypothesis on \(N\) and \(C\) implies that, for each \(v \in C\), there is only one \(f \in N\) such that \(f(0) = v\). Thus we obtain the required mapping \(\pi : C \rightarrow S_n\) given by \(\pi(v) = \pi(f(0)) = \bar{\pi}(f)\).

As a consequence of Theorem 1, we can conclude:

Theorem 2. Every binary \(G\)-linear code is a binary propelinear code.

What about the converse? It is false, as the following example shows.

Example 4. In \(\mathbb{Z}_2^3\) we have the propelinear code \(C = \{000, 011, 101\}\) with associated group \(\mathbb{Z}_3 \cong \langle (101), (123) \rangle\). This generator is a rotation of \(\pi/3\) around the axis of the cube that passes through 001 and 110. This code cannot be \(G\)-linear for any group \(G\), because this group would have order 8 and then a proper subgroup should have order 1, 2 or 4.

Next, we look for the relations between \(G\)-linear codes and translation-invariant propelinear codes. As we saw in Example 2, the propelinear codes with associated group \(\mathbb{Q}_8^4\) are also \(\mathbb{Q}_8 \gg \mathbb{Z}_2\)-linear codes. In [12] the translation-invariant propelinear codes are classified and it is shown that they are of the type \(\mathbb{Z}_2^m \oplus \mathbb{Z}_4^n \oplus \mathbb{Q}_8^m\).
This means that these codes are obtained from subgroups of \( \mathbb{Z}_2^{n_1} \oplus \mathbb{Z}_4^{n_2} \oplus \mathbb{Q}_8^{n_3} \) via the evaluation map. Since we can extend the action of \( \mathbb{Q}_8^k \) to an action of \( (\mathbb{Q}_8 \bowtie \mathbb{Z}_2)^k \) which is free and transitive on \( \mathbb{Z}_2^{4k} \), we conclude that all those codes are also \( \mathbb{Z}_2^{n_1} \oplus \mathbb{Z}_4^{n_2} \oplus (\mathbb{Q}_8 \bowtie \mathbb{Z}_2)^{n_3} \)-linear codes, or equivalently, are direct sums of linear, \( \mathbb{Z}_4 \)-linear and \( (\mathbb{Q}_8 \bowtie \mathbb{Z}_2) \)-linear codes.

One may ask if \( G \)-linear and translation-invariant propelinear are equivalent requirements for linear codes; the answer is negative again, and the easiest example is given by the action of \( D_4 \) on \( \mathbb{Z}_2^3 \) described in Example 1. Summing up, we have the following result:

**Theorem 3.** For binary codes, we have the strict inclusions: Translation-Invariant Propelinear Codes \( \subset \) Binary \( G \)-linear Codes \( \subset \) Propelinear Codes.

### 4. Conclusions

In this paper we presented the concepts of \( G \)-linearity and propelinearity in the context of isometries and group actions, establishing the relations between them and providing some examples. We believe that this viewpoint should shed some light on the group structure of propelinear codes and even in some aspects of the well known \( \mathbb{Z}_4 \)-linearity, which originated both concepts.

### Acknowledgements

The authors are grateful to the referee for valuable comments and suggestions.

### References


