On the Properties of Propelinear and G-Linear Codes

Martinho da Costa Araújo, and Reginaldo Palazzo Jr.
Universidade Federal de Mato Grosso, UFMT/CUR, Rondonópolis, MT, Brazil
Universidade Estadual de Campinas, Campinas SP, Brazil

Abstract— **The aim of this paper is to establish some of the structural properties which are common to the classes of binary translation-invariant propelinear codes and binary G-linear codes. In general, the codes in these classes are nonlinear codes, however they are part of the same symmetry group decomposition $\Gamma\left(\mathbb{Z}_2^n\right)$ of $\mathbb{Z}_2^n$. We show that binary G-linear codes can be seen as translation-invariant propelinear codes. Finally, we establish a result which allows to identify when a code is a G-linear code.**

I. Introduction

In [1], Rifa, Basart and Hughet introduced the basic concepts of binary propelinear codes. In [2], Rifa and Pujol improved the previous work both by characterizing the class of translation-invariant binary propelinear codes of blocklength n and by classifying them as a subgroup of $\mathbb{Z}_2^{k_1} \oplus \mathbb{Z}_4^{k_2} \oplus \mathbb{Q}_8^{k_3}$, of the type (k_1, k_2, k_3), where $k_1 + 2k_2 + 4k_3 = n$. These codes can also be obtained by the action of a subgroup of the semidirect product of $\mathbb{Z}_2^n$ by the symmetric group $\mathbf{S}_n$ of degree n, denoted by $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$, over the signal set $\mathbb{Z}_2^n$ such that the Hamming distance is invariant by this action.

From the $\mathbb{Z}_4$-linearity [3], it was shown the interplay between certain classes of known binary nonlinear block codes with certain classes of linear codes over $\mathbb{Z}_4$. In [4], it was established the class of G-linear codes, where G is a group. These codes can be seen as a set of signals which are effectively matched to the group G, [4] and [5]. Since the action of a group on a set can be interpreted as a slight generalization of the symmetry group of the corresponding signal set, it follows that the search for G-linear codes is such that one has to find G as a subgroup of the symmetry group $\Gamma\left(\mathbb{Z}_2^n\right)$ of $\mathbb{Z}_2^n$ which acts sharply transitively on $\mathbb{Z}_2^n$, that is, such codes belong to the class of geometrically uniform codes, GU, [8]. On the other hand, the computational complexity associated to the search of G-linear codes increases as $2^n n!$. Although the theoretical computational complexity in searching for propelinear codes is bounded by $2^n n!$ some of its structural properties reduce considerably the computational complexity. Furthermore, it is worthwhile going forward in this direction since the GU codes have Voronoi regions which are congruents simplifying considerably the performance analysis of such codes. For further simplification we make use of the algebraic properties of the translation-invariant propelinear codes. We show that it is possible to classify G-linear codes by use of the translation-invariant propelinear codes, for further details see [6] and [7]. Finally, we establish the condition under which a code can be classified as a G-linear code.

Martinho C. Araújo is with the Departamento de Matemática, Universidade Federal de Mato Grosso, UFMT/CUR, Rondonópolis, MT - Brazil. Reginaldo Palazzo Jr. is with the Departamento de Telemática, Faculdade de Engenharia Elétrica e de Computação, 13081-970, Phone: +55 19 3788 3753 Fax: +55 19 3289 1395, E-mail: palazzo@dt.fee.unicamp.br. This work has been supported

This paper aims at establishing some of the structural properties which are common to the classes of binary translation-invariant propelinear codes and binary G-linear codes; by showing that binary G-linear codes can be seen as translation-invariant propelinear codes; and by identifying when a code is a G-linear code.

II. Propelinear and G-linear Codes

In this section the translation-invariant propelinear codes and the G-linear codes are defined. We describe some of their properties by emphasizing their algebraic structure. Some examples of these codes will be presented.

Definition II.1: Let $(\mathbb{Z}_2^n,\ d_H)$ be the n-dimensional Hamming space, and $\mathbf{S}_n$ the symmetric group of degree n. We say that a subset $C \subseteq \mathbb{Z}_2^n$, with $\mathbf{0} \in C$ is a *propelinear code* with blocklength n, if there exists a function $\pi : C \to \mathbf{S}_n$, defined as $\pi(v) = \pi_v$, such that its graph $\Omega(\pi) = \{(v, \pi_v) \text{ for every } v \in C\}$ is a subgroup of $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$.

Definition II.2: Let G be a group, d_G a metric in G and C a binary code of blocklength n in $(\mathbb{Z}_2^n,\ d_H)$. We say that C is $\mathbb{G}$-linear, if $C = \phi(\hat{C})$, for some subgroup $\hat{C}$ of G, where $\phi : G^n \to \mathbb{Z}_2^{kn}$, for $k \geq 2$, is an isometry.

Definition II.3: Let G be a group that acts on a nonempty set S. The orbit of $x \in S$, under G, is a subset of S given by

$$Orb_G(x) = \{g(x) \ : g \in G\}.$$

We say that the group G acts transitively on S, if for all $a, b \in S$ there exists $g \in G$ such that $g(a) = b$. We say that G acts sharply transitively on S, if there exists a unique $g \in G$ for each $a, b \in S$. In this case, both sets have equal cardinalities, that is, $|G| = |S|$.

Under these conditions, we observe that code C is propelinear, since there is a natural identification of C with a subgroup $(\Omega(\pi), *)$ of $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$. This identification implies a sharply transitively action of $(\Omega(\pi), *)$ on C defined by the function

$$f : (\Omega(\pi), *) \times C \to C$$

such that

$$f((v, \pi_v), x) = (v, \pi_v) * x = v + \pi_v(x) = v * x,$$

for every $(v, \pi_v) \in (\Omega(\pi), *)$, and $x \in C$.

Therefore, for every $x \in C$ we have $Orb_{\Omega(\pi)}(x) = C$. When a code C is G-linear it follows, by definition and by [5], that the alphabet $\mathbb{Z}_2^k$ is effectively matched to the group G, that is, G is isomorphic to a subgroup of the symmetry group $\Gamma\left(\mathbb{Z}_2^n\right)$ of $\mathbb{Z}_2^n$

Example II.1: Consider $\pi : \mathbb{Z}_2^n \to \mathbf{S}_n$, such that $(\Omega(\pi), *)$ is a subgroup of $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$, this implies a propelinear code given by

1. For $n = 2$

v	00	11	01	10
π_v	id	id	(12)	(12)

Note that $(\Omega(\pi), *)$ is a subgroup of $\mathbb{Z}_2^2 \rtimes \mathbf{S}_2 \cong \mathbb{D}_4$, where $\mathbb{D}_4$ denotes the dihedral group with 8 elements, generated by $(v, \pi_v) = ((01), (12))$, that is, $(\Omega(\pi), *) = \langle 01, (12) \rangle \cong \mathbb{Z}_4$. Since $\mathbb{Z}_4$ acts sharply transitively on $\mathbb{Z}_2^2$, it follows that this propelinear code is also a $\mathbb{Z}_4$-linear code.

2. For $n = 3$

v	000	011	100	111	001	010	101	110
π_v	id	id	id	id	(23)	(23)	(23)	(23)

Note that $(\Omega(\pi), *) = \langle (100, id),\ (110,\ (23)) \rangle$, is isomorphic to the direct product $\mathbb{Z}_2 \times \mathbb{Z}_4$. Furthermore, $(\Omega(\pi), *)$ acts sharply transitively on $\mathbb{Z}_2^3$. Therefore, this propelinear code is also a $\mathbb{Z}_2 \times \mathbb{Z}_4$-linear code.

3. For $n = 3$

v	000	011	101	110	001	010	100	111
π_v	id	id	id	id	(23)	(23)	(23)	(23)

Note that $(\Omega(\pi), *) = \langle (110, id),\ (100,\ (23)) \rangle \cong \mathbb{D}_4$. This propelinear code is also a $\mathbb{D}_4$-linear code.

Definition II.4: [2] A propelinear code C is *translation-invariant*, if

$$d_H(u, v) = d_H(u * x, v * x),$$

for every $u, v \in C$ and for every $x \in \mathbb{Z}_2^n$.

Definition II.5: Let G be a group that acts on a nonempty set X. The *stabilizer* of $x \in X$ is a subgroup of G given by

$$Stab_G(x) = \{g \in G : g(x) = x\}.$$

Lemma II.1: [2] A propelinear code C is *translation-invariant*, if and only if,

$$w_H(v) = d_H(x, v * x),$$

for every $v \in C$, and for every $x \in \mathbb{Z}_2^n$.

Corollary II.1: If C is a translation-invariant propelinear code then the stabilizer

$$Stab_C(x) = \{(\mathbf{0}, \mathbf{id})\}.$$

Proof: By the natural identification of C with $(\Omega(\pi), *)$ we have

$$Stab_{\Omega(\pi)}(x) = \{(v, \pi_v) \in (\Omega(\pi), *) : (v, \pi_v)(x) = v * x = x\}$$

Since C is translation-invariant, it follows that

$$v * x = x \Rightarrow 0 = d_H(x, v * x) = w_H(v) \Rightarrow v = 0,$$

$$\forall x \in \mathbb{Z}_2^n, \text{that is, } (v, \pi_v) = (0, id).$$

Corollary II.2: [2] If C is a translation-invariant propelinear code, then $|C| = 2^k$, for $k \leq n$.

Proof: By considering $g \in (\Omega(\pi), *)$, we know that there always exists a bijection $F : Orb_G(x) \to G/Stab_G(x)$, defined by $F(gx) = gStab_G(x)$, for every $x \in \mathbb{Z}_2^n$. Since the order of a subgroup divides the order of the group, it follows that

$$\begin{aligned} |G| &= |Stab_G(x)|\ [G : Stab_G(x)] \\ &= |Stab_G(x)|\ |Orb_G(x)| \\ &= |Orb_G(x)|, \quad \forall x \in \mathbb{Z}_2^n \end{aligned}$$

that is, every coset has the same cardinality. Hence, $|G|$ divides $\mathbb{Z}_2^n$. Therefore, $|C| = 2^k$, for some $k \leq n$ ■

Theorem II.1: Let C be a translation-invariant propelinear code of blocklength n, with cardinality $|C| = 2^k$, for $k \leq n$, then C is a G-linear code.

Proof: As C is a translation-invariant propelinear code this implies that we can identify C with a subgroup $G = (\Omega(\pi), *)$ of $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$, it follows that we have a sharply transitively action of G on C, that is, $|G| = |C| = 2^k$, for some $k \leq n$. ■

Theorem II.2: Let G be a group, d_G a metric in G, and C a binary code with blocklength n in $(\mathbb{Z}_2^n, d_H)$. Code C is G-linear, if and only if the stabilizer $Stab_G(x) = \{id_G\}$, for every $x \in \mathbb{Z}_2^n$.

Proof: Let C be a G-linear code, this is equivalent to saying that G is isomorphic to a subgroup of $\Gamma(\mathbb{Z}_2^n)$ such that $Orb_G(x) = \mathbb{Z}_2^n$, and $|G| = |\mathbb{Z}_2^n|$, for every $x \in \mathbb{Z}_2^n$, $n \geq 2$. Equivalently, by $|G| = |Stab_G(x)|\ |Orb_G(x)|$, we have $|Stab_G(x)| = 1$, that is, $Stab_G(x) = id_G$, the identity of G. ■

Example II.2: From Example II.1, both codes $\mathbb{Z}_4$-linear and $\mathbb{Z}_2 \times \mathbb{Z}_4$-linear are translation-invariant whereas the code $\mathbb{D}_4$-linear is not.

Example II.3: Consider the mapping $\pi : \mathbb{Z}_2^n \to \mathbf{S}_n$, such that $(\Omega(\pi), *)$ is a subgroup of $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$. This implies a propelinear code given by

1. For $n = 3$

v	000	011	101	110	000	011	101	110
π_v	id	id	id	id	(12)	(12)	(12)	(12)

We have $(\Omega(\pi), *) \cong \mathbb{D}_4$ is a propelinear code, however it is neither translation-invariant, since for $x = 011$ and $(v, \pi_v) = (110, (12))$ Lemma II.1 is not satisfied, nor a $\mathbb{D}_4$-linear code, since $Stab_{\mathbb{D}_4}(100) = \{(000, \mathbf{id}), (110, (12))\} \neq \{(\mathbf{0}, \mathbf{id})\}$.

2. For $n = 4$

v	0000	0001	0010	0011
π_v	id	id	id	id
v	1100	1101	1110	1111
π_v	id	id	id	id
v	0100	0101	0110	0111
π_v	(12)	(12)	(12)	(12)
v	1000	1001	1010	1011
π_v	(12)	(12)	(12)	(12)

In this case $(\Omega(\pi), *) \cong \mathbb{Z}_2^2 \times \mathbb{Z}_4$. Therefore, the corresponding code is translation-invariant propelinear code and also a $\mathbb{Z}_2^2 \times \mathbb{Z}_4$-

3. For $n = 4$

v	0000	1111	0111	1000
π_v	id	id	(24)	(24)
v	0110	1001	0010	1101
π_v	(12)(34)	(12)(34)	(12)(34)	(12)(34)
v	0001	1110	0011	1100
π_v	(13)	(13)	(13)(24)	(13)(24)
v	0100	1011	0101	1010
π_v	(14)(32)	(14)(32)	(14)(23)	(14)(23)

In this case we have a $\mathbb{QD}_8$-linear code, that is, $(\Omega(\pi), *)$ is isomorphic to the *quasidihedral group of order 16*, denoted by $\mathbb{QD}_8$. We say that this code is a propelinear code, however it is not translation-invariant. Since for $x = 0001$ and $(v, \pi_v) = (1110, (13))$, Lemma II.1 is not satisfied.

4. For $n = 4$

v	0000	1111	0100	1011
π_v	id	id	(34)	(34)
v	0001	1110	0110	1001
π_v	(12)	(12)	(12)(34)	(12)(34)
v	0000	1111	0001	1110
π_v	(13)(24)	(13)(24)	(13)(24)	(13)(24)
v	0100	1011	0110	1001
π_v	(14)(23)	(14)(23)	(14)(23)	(14)(23)

We have a propelinear code, with $(\Omega(\pi), *) \cong \mathbb{D}_8$. However, this code is neither a translation-invariant propelinear code, since for $x = 0001$ and $(v, \pi_v) = (1111, (13)(24))$ Lemma II.1 is not satisfied, nor a $\mathbb{D}_8$-linear code, since

$$Stab_{\mathbb{D}_8}(1000) = \{(000, \mathbf{id}), (1001, (14)(23))\} \neq \{(\mathbf{0}, \mathbf{id})\}.$$

5. For $n = 5$

v	00000	00001	00010	00011
π_v	id	id	id	id
v	00100	00101	00110	00111
π_v	id	id	id	id
v	11000	11001	11010	11011
π_v	id	id	id	id
v	11100	11101	11110	11111
π_v	id	id	id	id
v	01000	01001	01010	01011
π_v	(12)	(12)	(12)	(12)
v	01100	01101	01110	01111
π_v	(12)	(12)	(12)	(12)
v	10000	10001	10010	10011
π_v	(12)	(12)	(12)	(12)
v	10100	10101	10110	10111
π_v	(12)	(12)	(12)	(12)

We have a translation-invariant propelinear code, where

6. For $n = 5$

v	00000	00011	00100	00111
π_v	id	id	id	id
v	11000	11011	11100	11111
π_v	id	id	id	id
v	00001	00010	00101	00110
π_v	(34)	(34)	(34)	(34)
v	11001	11010	11101	11110
π_v	(34)	(34)	(34)	(34)
v	01000	01011	01100	01111
π_v	(12)	(12)	(12)	(12)
v	10000	10011	10100	10111
π_v	(12)	(12)	(12)	(12)
v	01001	01010	01101	01110
π_v	(12)(34)	(12)(34)	(12)(34)	(12)(34)
v	10001	10010	10101	10110
π_v	(12)(34)	(12)(34)	(12)(34)	(12)(34)

We have $(\Omega(\pi), *) \cong \mathbb{Z}_2 \times \mathbb{Z}_4^2$, which implies a $\mathbb{Z}_2 \times \mathbb{Z}_4^2$-linear code. This code is not a translation-invariant propelinear code since for $x = 01010$ and $(v, \pi_v) = (01110, (12)(34))$ Lemma II.1 is not satisfied. Observe that $Stab_{\Omega(\pi)}(x) = (\mathbf{0}, id), \quad \forall x \in \mathbb{Z}_2^n$, therefore implying the assertion that it is a $\mathbb{Z}_2 \times \mathbb{Z}_4^2$-linear code.

III. Conclusions

In this paper, we have established a procedure of classifying some G-linear codes from the translation-invariant propelinear codes. This classification includes such codes as the class of additive translation-invariant propelinear codes, that is, subgroups of $\mathbb{Z}_2^{k_1} \oplus \mathbb{Z}_4^{k_2}$, where $k_1 + 2k_2 = n$. We saw that the algebraic structure associated with these group codes is the semidirect product of groups. By using this structure, we exhibited an important result that allowed to establish when a code is a G-linear code. Finally, some examples relating these two classes of codes were presented.

References

[1] J. Rifá, J.M. Bassart, and J. Pujol, "On completely regular propelinear codes," *Proceedings 6th International Conference, AAECC-6, No. 357, LNCS, Lectures Notes in Computer Science* , pp. 341-355, Springer-Verlag,1989.

[2] J. Rifá, and J. Pujol, "Translation-invariant propelinear codes," *IEEE Trans. Inform. Theory*, vol.IT-43, pp. 590-598, March 1997.

[3] A.R. Hammons, Jr., A.R. Calderbanck, P.V. Kumar, N.J.A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol.IT-40, pp. 301-309, March 1994.

[4] J.R. Gerônimo, *Extension of the $\mathbb{Z}_4$-linearity via Symmetry Group*, Ph.D. Dissertation, DECOM-FEEC-UNICAMP, February 1997 (in Portuguese).

[5] H.A. Loeliger, "Signal sets matched to groups," *IEEE Trans. Inform. Theory*, vol. IT-37, pp. 1675-1682, November 1991.

[6] M.C. Araújo, *Algebraic and Geometric Characterizations of Propelinear Codes*, Ph.D. Dissertation, DT-FEEC-UNICAMP, May 2000 (in Portuguese).

[7] M.M.S. Alves, M.C. Araújo, R. Palazzo Jr., S.I.R. Costa, and J.C. Interlando, "Relating propelinear and G-linear codes," *Discrete Mathematics*, vol. 243/1-3, 2001, pp.187-194.

[8] G.D. Forney, Jr. "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. IT-37, pp.1241-1260, September 1991.