Translation-Invariant Propelinear Codes

Josep Rifà, *Member, IEEE*, and Jaume Pujol

***Abstract*—A class of binary group codes is investigated. These codes are the propelinear codes, defined over the Hamming metric space $\boldsymbol{F}^n$, $\boldsymbol{F}=\{0,1\}$, with a group structure. Generally, they are neither Abelian nor translation-invariant codes but they have good algebraic and combinatorial properties. Linear codes and Z_4-linear codes can be seen as a subclass of propelinear codes. It is shown here that the subclass of translation-invariant propelinear codes is of type $Z_2^{k_1}\oplus Z_4^{k_2}\oplus Q_8^{k_3}$ where Q_8 is the non-Abelian quaternion group of eight elements. Exactly, every translation-invariant propelinear code of length n can be seen as a subgroup of $Z_2^{k_1}\oplus Z_4^{k_2}\oplus Q_8^{k_3}$ with $k_1+2k_2+4k_3=n$. For $k_2=k_3=0$ we obtain linear binary codes and for $k_1=k_3=0$ we obtain Z_4-linear codes. The class of additive propelinear codes—the Abelian subclass of the translation-invariant propelinear codes—is studied and a family of nonlinear binary perfect codes with a very simply construction and a very simply decoding algorithm is presented.**

***Index Terms*—Propelinear codes, translation-invariant propelinear codes, additive codes, perfect codes, Z_4-linear codes, Q_8-codes.**

I. Introduction

USUALLY, we define codes over a metric space (X,d) as a subset C of X. Moreover, if X has a group structure then we will require that C be a subgroup of X. The combinatorial properties of C depend on the metric structure of X and the algebraic properties of C depend on the group structure of X.

If we consider the direct product group X^n then we can consider codes over X^n with the Hamming distance $d(x,y)$, between x and y, defined as the number of positions in which x and y disagree. This class of codes has been studied in [1] and [2]. If X is an Abelian group then the Hamming distance is a translation-invariant distance, i.e., $d(x,y)=d(x\star z,y\star z)$ for all $x,y,z\in X^n$ where $\star$ is the group operation over X. The case when X is the finite field $\mathrm{GF}(q)$ has usually been used in the algebraic coding theory (see [3]–[5]).

In a general way (see [6], [7]) we can study codes over X when X has an Abelian group structure and there is a metric defined over X such that it is translation-invariant. These codes are the group codes by Delsarte [6], called additive codes by Brouwer [7].

Recently (see [8]), for $n=2k$, an additive group structure over $\boldsymbol{F}^n$ has been defined such that the Hamming metric is a translation-invariant metric. The subgroups of this structure are Z_4-linear codes. We present this construction in a more general way: Let G be a group and ϕ an injective map from G to $\boldsymbol{F}^n$. $\phi(G)=C$ is a code in $\boldsymbol{F}^n$ and it can be fitted with the group structure of G. Generally, we do not know when there exists a group G such that $\phi(G)=\boldsymbol{F}^n$ and, with this group structure, the Hamming metric is a translation-invariant metric. When $\phi(G)=\boldsymbol{F}^n$ is an Abelian group and the Hamming metric is a translation-invariant metric, then we obtain additive codes.

This point of view is too general because C could not be equal to $\boldsymbol{F}^n$ and the Hamming metric could not be a translation-invariant metric. We need to assume some restrictions over the code C.

On the other hand, from distance regular graph theory, Rifà (see [9]) introduced the class of *propelinear codes* which have important algebraic properties. Generally, these codes are neither Abelian nor translation-invariant but they include linear and Z_4-linear codes.

The goal of Section IV consists of the characterization of conditions for the class of propelinear codes to be translation-invariant and also the characterization to be additive, i.e., they have an Abelian group structure for which the Hamming distance leads to a translation-invariant code. The main theorem of this section states that every translation-invariant propelinear code is of type $Z_2^{k_1}\oplus Z_4^{k_2}\oplus Q_8^{k_3}$.

In Section V we further investigate the additive propelinear codes. These codes are codes of type $Z_2^{k_1}\oplus Z_4^{k_2}$. For this class of codes we can define, as in the linear case, the concept of duality and we can use the McWilliams Identity. Finally, we construct a family of perfect additive propelinear codes with the same properties as those of the Hamming codes but which are not linear. Moreover, we give a simply decoding algorithm for this kind of nonlinear codes.

II. Preliminaries

Let $\boldsymbol{F}^n$ be a vector space of dimension n over $\mathrm{GF}(2)$. We denote by Z_2^n the additive group of $\boldsymbol{F}^n$. A subset of $\boldsymbol{F}^n$ is a binary code of length n. The *Hamming distance* between vectors $x,y\in\boldsymbol{F}^n$, denoted $d(x,y)$, is the number of coordinates in which x and y differ. The *Hamming weight* of x is given by $\mathrm{wt}_H(x)=d(x,\mathbf{0})$, where $\mathbf{0}$ denotes the all-zero vector. We shall assume, unless stated otherwise, that $\mathbf{0}\in C$, where $C\subset\boldsymbol{F}^n$ is a binary code.

If $|C|=M$ and $d=\min\{d(u,v)\mid u,v\in C\}$ we will say that C is a code of parameters (n,M,d), i.e., length n, cardinal M, and minimum distance d. We will say that C is e-error correcting where $e=\lfloor\frac{d-1}{2}\rfloor$. Let $w=\min\{\mathrm{wt}_H(u)\mid u\in C\}$ be the minimum weight of C. If C is a vector subspace of $\boldsymbol{F}^n$ of dimension k then we will say that C is a linear code of parameters (n,k,d).

Let $E=\{e_1,\cdots,e_n\}$ be the n vectors of $\boldsymbol{F}^n$ of weight 1. Thus for every $v\in\boldsymbol{F}^n$, $v=\sum\lambda_i e_i$ with $\lambda_i\in\{0,1\}$. Let I be

Manuscript received May 15, 1995; revised May 14, 1996. This work was supported in part by Spanish CICYT under Grant TIC94-0331.

The authors are with Department d'Informàtica, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain.

Publisher Item Identifier S 0018-9448(97)00625-1.

the set $\{1,2,\cdots,n\}$, we define, $\sup(v)=\{i\in I \mid \lambda_i=1\}$. Then

$$\mathrm{wt}_H(v)=\sum \lambda_i.$$

We will say that $(X,\mathcal{R})$ is a translation association scheme ([7], [6]) if $(X,\mathcal{R})$ is an association scheme where the underlying set X has the structure of an Abelian group and, for all classes $R\in\mathcal{R}$

$$(x,y)\in R \Rightarrow (x+z,y+z)\in R$$

An *additive code* in a translation association scheme $(X,\mathcal{R})$ is a subgroup of X. $\boldsymbol{F}^n$ with the metric defined by Hamming distance, is a translation association scheme and linear codes are additive codes if you see $\boldsymbol{F}^n$ as a translation association scheme.

We are interested in additive codes where the metric defined in $\boldsymbol{F}^n$ is the Hamming metric but the additive group of $\boldsymbol{F}^n$ is not Z_2^n.

A code $C\subset \boldsymbol{F}^n$ is said to be *distance-invariant* [3] if the Hamming weight distribution of its translates $C+u$ are the same for all $u\in C$. In a distance-invariant code the minimum distance coincides with the minimum weight. Clearly, every linear code is distance-invariant.

The *weight enumerator* polynomial associated to a binary code C is

$$W_C(X,Y)=\sum_{u\in C} X^{n-wt_H(u)}Y^{wt_H(u)}.$$

For additive codes it is defined the dual code (see [7]) and, for a linear code C, its *dual* is the linear code

$$C^{\perp}=\{w\in \boldsymbol{F}^n \mid (w,u)=0\}$$

where $(w,u)=w_1u_1+\cdots+w_nu_n$ is the usual inner product on $\boldsymbol{F}^n$. The weight enumerator polynomials of C and $C^{\perp}$ are related by the *McWilliams Identity*

$$W_{C^{\perp}}(X,Y)=\frac{1}{|C|}W_C(X+Y,X-Y).$$

We say that two codes $C_1,C_2\subset \boldsymbol{F}^n$ are *equivalent* if there exists a Hamming isometry π in $\boldsymbol{F}^n$ such that $\pi(C_1)=C_2$.

Let G be a group (not necessarily Abelian). Let ϕ be an injective map from G to $\boldsymbol{F}^n$ such that $\phi(e)=\mathbf{0}$ where e is the identity of G. Then, we will say that $\phi(G)=C$ is a code in $\boldsymbol{F}^n$ and that G is the group associated with C. Every subgroup $G'\subset G$ gives a subcode $C'\subset C$. We can define a group structure in C by

$$u\star v=\phi(\phi^{-1}(u)\phi^{-1}(v)).$$

In this way, there is a one-to-one correspondence between subgroups of G and subcodes of $C'\subset C$. If C' is a subcode of C we will say that C' is a code *of type* (G,ϕ).

If $G=Z_2^n$ and we fix the basis E in $\boldsymbol{F}^n$ then $Id: G\to \boldsymbol{F}^n$ defines codes of type (Z_2^n,Id) which coincides with linear codes. If $G=Z_4^k$ then the Gray map (see [8]) $\phi: Z_4^k\to \boldsymbol{F}^n$ where $n=2k$ defines Z_4-linear codes of type (Z_4^k,ϕ).

Let G be a group that acts on $\boldsymbol{F}^n$, that is, we have a map from $G\times \boldsymbol{F}^n$ into $\boldsymbol{F}^n$ such that for $g,h\in G$, $g(hx)=(gh)x$ and $ex=x$ for all $x\in \boldsymbol{F}^n$. An *orbit* of G is a set $Gx=\{gx \mid g\in G\}$; clearly, the orbits partition $\boldsymbol{F}^n$. We write G_x for the *stabilizer* in G of x, that is, the subgroup $\{g\in G \mid gx=x\}$. If $G_x=\{e\}$ for all $x\in \boldsymbol{F}^n$ then $|G|=|Gx|$ and $|G|=2^k$.

III. Propelinear Codes

Let S_n be the permutation group over the set $I=\{1,\cdots,n\}$.

Definition 1: Let C be a subset of $\boldsymbol{F}^n$ that contains the zero element of $\boldsymbol{F}^n$, that is, $\mathbf{0}\in C$. We will say that C is a *propelinear code* if there exists a permutation subset $\Pi=\{\pi_v \mid v\in C\}\subset S_n$ such that

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

In [9] it is shown that (C,Π) has a group structure, not necessarily Abelian. The operation on C is defined by

$$u\star v=u+\pi_u(v)\in C$$

for all $u,v\in C$.

The following proposition explains some algebraic properties of propelinear codes:

Propsition 2: Let (C,Π) be a binary propelinear code of length n:

1) Π is a subgroup of the isometric group of $\boldsymbol{F}^n$ and C is linear if and only if Π is a subgroup of $\mathrm{Aut}(C)$.
2) C acts over $\boldsymbol{F}^n$, that is, for every $v\in C$ and $x\in \boldsymbol{F}^n$

$$v\star x=v+\pi_v(x)\in \boldsymbol{F}^n.$$

For every $x\in \boldsymbol{F}^n$, $C\star x$ is an orbit from the action of C over $\boldsymbol{F}^n$. The set of orbits partitions $\boldsymbol{F}^n$ in *cosets* of C.

Proof: Straightforward. ∎

Definition 3: Let C be a propelinear code. We will say that C is a *translation-invariant propelinear code* if for all $u,v\in C$ and $x\in \boldsymbol{F}^n$

$$d(u,v)=d(u\star x,v\star x)$$

that is, the action of C over $\boldsymbol{F}^n$ preserves Hamming distance.

The next proposition explains some combinatorial properties of propelinear codes.

Proposition 4: Let (C,Π) be a propelinear code of length n.

1) If C is an e-error correcting code $(e\geq 1)$ then all the vectors of weight at most e are in different cosets.
2) C is a distance-invariant code but, not necessarily, a translation-invariant code.
3) $\forall x,y\in \boldsymbol{F}^n$ and $\forall v\in C$,

$$d(x,y)=d(v\star x,v\star y).$$

Proof: The proof can be seen in [9] and [10]. ∎

Since a propelinear code (C,Π) has a group structure we will denote by $(G(C),\phi_C)$ the group associated to C where ϕ_C is a group automorphism from $G(C)$ to the group structure of C.

Generally, a propelinear code is not a translation-invariant code. From Proposition 4 we obtain

Lemma 5: Let (C,Π) be a propelinear code, C is a translation-invariant code if and only if

$$\mathrm{wt}_H(v) = d(x, v\star x)$$

$\forall x \in \boldsymbol{F}^n$ and $\forall v \in C$

Proof: If C is a translation-invariant code then

$$\begin{aligned}\mathrm{wt}_H(v) &= d(0,v)\\ &= d(x, v\star x) \quad \forall x \in \boldsymbol{F}^n.\end{aligned}$$

Conversely, for $u, v \in C$ and by Proposition 4

$$d(u,v) = d(0, u^{-1}\star v).$$

For every $x \in \boldsymbol{F}^n$, we can apply the hypothesis

$$d(0, u^{-1}\star v) = \mathrm{wt}_H(u^{-1}\star v) = d(x, u^{-1}\star v\star x).$$

And if we apply again Proposition 4

$$\begin{aligned}d(u,v) &= d(x, (u^{-1}\star v)\star x)\\ &= d(x, u^{-1}\star(v\star x))\\ &= d(u\star x, v\star x)\end{aligned}$$

■

Corollary 6: If C is a translation-invariant propelinear code, then $|C| = 2^k$.

Proof: For $x \in \boldsymbol{F}^n$, if $v\star x = x$ then $0 = d(v\star x, x) = \mathrm{wt}_H(v)$ from the previous lemma. Hence, the stabilizer $C_x = \{\mathbf{0}\}$ and $|C|$ divides $|\boldsymbol{F}^n|$, so $|C| = 2^k$. ■

Example 1: Let $C \subset \boldsymbol{F}^n$ be a binary linear code. Then C is a propelinear code with $\Pi = \{Id \mid \forall v \in C\}$. All linear codes are codes of type (Z_2^n, Id). The orbits are the additive cosets $C + x$ for every $x \in \boldsymbol{F}^n$. Clearly, C is a translation-invariant code.

Example 2: The Z_4-linear codes (see [8]) are linear codes over the ring Z_4 (the integers $\bmod 4$). In the set $\boldsymbol{F}^2 = \{00, 01, 10, 11\}$ we can define a propelinear structure in the following way:

$$\boldsymbol{F}^2 = \{(00,\pi_{00})(01,\pi_{01}),(11,\pi_{11}),(10,\pi_{10})\}$$

where $\pi_{00} = \pi_{11} = Id$, $\pi_{01} = \pi_{10} = (1,2)$, and (i,j) represents the coordinate transposition of indices i and j. With this structure $\boldsymbol{F}^2$ is a cyclic group of order 4. That is, Z_4 is isomorphic to $\boldsymbol{F}^2$ by $\phi_4(1) = (01, \pi_{01})$ where $\pi_{01} = (1,2)$ and Π is isomorphic to Z_2. Thus every Z_4-linear code can be seen as a propelinear code in $\boldsymbol{F}^{2n}$ with the propelinear structure defined in $\boldsymbol{F}^2$. They are codes of type (Z_4^n, ϕ_4^n) and it is straightforward to show that every Z_4-linear code is a translation-invariant code.

Example 3: Define

$$\begin{aligned}\boldsymbol{a} &= (1010, \pi_{1010}) \in \boldsymbol{F}^4\\ \boldsymbol{b} &= (1001, \pi_{1001}) \in \boldsymbol{F}^4\end{aligned}$$

where $\pi_{1010} = (1,2)(3,4)$ and $\pi_{1001} = (1,3)(2,4)$.

The propelinear code generated by $\boldsymbol{a}$ and $\boldsymbol{b}$ will be called a *quaternion propelinear code*, $C = \langle \boldsymbol{a}, \boldsymbol{b}\rangle$. This code is the smallest propelinear code that contains $\boldsymbol{a}$ and $\boldsymbol{b}$ and, therefore, it contains $(\boldsymbol{a}\star\boldsymbol{b}, \pi_{\boldsymbol{a}\star\boldsymbol{b}}) = (1100, \pi_{1100})$ where $\pi_{1100} = (1,4)(2,3)$. It is easy to show that the only vectors u with $\pi_u = Id$ are $u = (0000)$ and $u = (1111)$.

The code contains eight elements

$$\begin{aligned}C = \{&(\mathbf{0}, Id), (\boldsymbol{a}, \pi_{\boldsymbol{a}}),\\ &(\boldsymbol{a}^2, Id), (\boldsymbol{a}^3, \pi_{\boldsymbol{a}}),\\ &(\boldsymbol{b}, \pi_{\boldsymbol{b}}), (\boldsymbol{a}\star\boldsymbol{b}, \pi_{\boldsymbol{a}\star\boldsymbol{b}}),\\ &(\boldsymbol{a}^2\star\boldsymbol{b}, \pi_{\boldsymbol{b}}), (\boldsymbol{a}^3\star\boldsymbol{b}, \pi_{\boldsymbol{a}\star\boldsymbol{b}})\}\end{aligned}$$

and fulfills the following relations:

$$\boldsymbol{a}^4 = \mathbf{0} \qquad \boldsymbol{a}^2 = \boldsymbol{b}^2 \qquad \boldsymbol{a}\star\boldsymbol{b}\star\boldsymbol{a} = \boldsymbol{b}.$$

Notice that C is isomorphic to the quaternion group Q_8; that is, C is of type (Q_8, ϕ_8) where ϕ_8 is the isomorphism from Q_8 to C. We also remark that Π is isomorphic to $Z_2 \oplus Z_2$.

It is not difficult to show that the propelinear codes of type (Q_8^k, ϕ_8^k) are translation-invariant propelinear codes. In fact, it suffices to see that code C is a translation-invariant propelinear code and this is so because for every $x \in \boldsymbol{F}^4$ and $v \in C$

$$\mathrm{wt}_H(v) = d(x, v\star x) \quad \text{(see Lemma 5)}.$$

The verification is left to the reader.

C is an example of a propelinear, non-Abelian, but translation-invariant code.

Example 4: Define

$$\begin{aligned}\boldsymbol{a} &= (1010, \pi_{1010}) \in \boldsymbol{F}^4\\ \boldsymbol{b} &= (1100, \pi_{1100}) \in \boldsymbol{F}^4\end{aligned}$$

where $\pi_{1010} = (1,2)(3,4)$ and $\pi_{1100} = (1,3)(2,4)$.

The propelinear code $C = \langle \boldsymbol{a}, \boldsymbol{b}\rangle$, generated by $\boldsymbol{a}$ and $\boldsymbol{b}$ is an Abelian propelinear code of eight elements but it is not translation-invariant. In fact

$$\mathrm{wt}_H(\boldsymbol{a}\star\boldsymbol{b}) = \mathrm{wt}_H(0110) = 2$$

but

$$d(0100, \boldsymbol{a}\star\boldsymbol{b}\star(0100)) = \mathrm{wt}_H(0000) = 0$$

in contradiction to Lemma 5. This code is defined by the relations $\boldsymbol{a}^4 = 0$, $\boldsymbol{b}^2 = \boldsymbol{a}^2$, and $\boldsymbol{a}\star\boldsymbol{b} = \boldsymbol{b}\star\boldsymbol{a}$. It is of type $(Z_2 \oplus Z_4, \phi)$ where $\phi(0,1) = \boldsymbol{a}$ and $\phi(1,1) = \boldsymbol{b}$ and $\phi(x,y) = \boldsymbol{a}^{y-x}\star\boldsymbol{b}^x$ where $x \in Z_2$ and $y \in Z_4$.

Notice that C is not of type $(Z_2 \oplus Z_4, (Id, \phi_4))$, where ϕ_4 is the map defined in Exemple 2.

Example 5: The standard Preparata code $\mathcal{P}(\sigma)$, the extended Preparata code $\overline{\mathcal{P}}(\sigma)$, and related codes are other examples of propelinear codes. Following [11], let $\mathcal{F}$ be the field GF(2^m) where $m \geq 3$. Let $x \to x^\sigma$ be an automorphism of $\mathcal{F}$. We require that both $x \to x^{\sigma+1}$ and $x \to x^{\sigma-1}$ are one-to-one mappings.

For the admissible values of σ we shall define a code $\mathcal{C}$ of length $2n + 2 = 2^{m+1}$. The codewords will be described by pairs (X, Y), where $X \subset \mathcal{F}$, $Y \subset \mathcal{F}$. We interpret the pair

(X,Y) as the corresponding pair of characteristic functions, i.e., as a $(0,1)$-vector of length 2^{m+1}.

The *extended Preparata code* $\bar{\mathcal{P}}(\sigma)$ of length 2^{m+1} consists of the codewords described by pairs (X,Y) satisfying

1) $|X|$ is even, $|Y|$ is even,

2) $\sum_{x\in X} x = \sum_{y\in Y} y$,

3) $\sum_{x\in X} x^{\sigma+1} + \left(\sum_{x\in X} x\right)^{\sigma+1} = \sum_{y\in Y} y^{\sigma+1}$.

The code $\mathcal{P}(\sigma)$ is obtained by deleting the coordinate that corresponds to the zero-element of $\mathcal{F}$ in the X-part.

Symmetric difference of two sets X_1, X_2 is denoted by $X_1 \triangle X_2$ and it corresponds to addition of codewords.

Given $X \subset \mathcal{F}$ we define

$$\alpha = \sum_{x\in X} x \in \mathcal{F}$$

and $\pi_X : \mathcal{F} \to \mathcal{F}$ by $\pi_X(y) = y + \alpha$. Thus given $(X,Y),(U,V) \in \bar{\mathcal{P}}(\sigma)$

$$(X,Y)\star(U,V) = (X\triangle\pi_X(U), Y\triangle V)$$

where $\pi_X(U) = U + \alpha$.

With this operation $\bar{\mathcal{P}}(\sigma)$ is a propelinear code. Related codes, $\mathcal{P}(\sigma)$, Goethals, and Delsarte–Goethals codes, have a propelinear structure too. However, these propelinear structures are neither Abelian nor translation-invariant as the reader can see in the following counter-example:

Let β be a primitive element of GF(2^m). For $m = 3$ we take $(U,V) \in \bar{\mathcal{P}}(2)$ defined by $U = \{0,\beta\}$ and $V = \{\beta,\beta^2,\beta^3,\beta^5\}$. Then $(V,U) \in \bar{\mathcal{P}}(2)$ too (see [11]), and

$$\begin{aligned}(U,V)\star(V,U) &= (U\triangle\pi_U(V), V\triangle U)\\ &= (U\triangle\{0,1,\beta^4,\beta^6\}, V\triangle U)\\ &= (\{1,\beta,\beta^4,\beta^6\}, V\triangle U)\end{aligned}$$

$$\begin{aligned}(V,U)\star(U,V) &= (V\triangle\pi_V(U), U\triangle V)\\ &= (V\triangle\{0,\beta\}, U\triangle V)\\ &= (\{0,\beta,\beta^3,\beta^5\}, U\triangle V)\end{aligned}$$

so $(U,V)\star(V,U) \neq (V,U)\star(U,V)$. That is, the propelinear structure of $\bar{\mathcal{P}}(\sigma)$ is not Abelian.

Moreover, given $(X,Y) \subset \mathcal{F}\times\mathcal{F}$ defined by $X = \{\beta\}$ and $Y = \emptyset$, we obtain

$$\begin{aligned}(U,V)\star(X,Y) &= (U\triangle\pi_U(X), V)\\ &= (U\triangle\{0\}, V)\\ &= (\{\beta\}, V).\end{aligned}$$

Now we compute $\mathrm{wt}_H(U,V) = 6$ and $d((X,Y),(U,V)\star(X,Y)) = 5$ which contradicts Lemma 5, so the translation-invariant condition is not satisfied.

Notice that Kerdock and Preparata-like codes (as they were defined in [8]) are translation-invariant propelinear codes.

Remark 1: These examples show that a subset C of $\boldsymbol{F}^n$ can have more than one propelinear structure. For instance, the subset

$$C = \{u \in \boldsymbol{F}^4 \mid \mathrm{wt}_H(u) = 0 \pmod 2\}$$

has the following propelinear structures: The linear structure (see Example 1), the Z_4-linear structure (see Example 2), the Q_8-structure (see Example 3), and the $(Z_2\oplus Z_4,\phi)$ structure (see Example 4).

IV. Translation-Invariant Propelinear Codes

We know some important examples of translation-invariant propelinear codes: linear codes are of this type. Kerdock, Preparata-like, and related codes (see [8]) are other examples of translation-invariant propelinear codes. In Section V we will see a construction of perfect codes which are translation-invariant propelinear codes but not linear.

Definition 7: Let $C \subset \boldsymbol{F}^n$ be a binary code of length n. We will say that C is a code *of type* (k_1,k_2,k_3) if C is a translation-invariant propelinear code of type

$$\left(Z_2^{k_1}\oplus Z_4^{k_2}\oplus Q_8^{k_3}, (Id,\phi_4^{k_2},\phi_8^{k_3})\right)(k_1+2k_2+4k_3 = n)$$

where Id, ϕ_4, and ϕ_8 are the maps defined in Examples 1, 2, and 3, respectively.

In this section we will show that every translation-invariant propelinear code of length n is of type

$$(k_1,k_2,k_3)(k_1+2k_2+4k_3 = n).$$

Notice that if $k_2 = k_3 = 0$ we obtain linear codes and if $k_1 = k_3 = 0$ we obtain Z_4-linear codes (see [8]). The perfect code family of Section V is of type $(\frac{n-1}{2}, \frac{n+1}{4}, 0)$, for $n = 2^m - 1$ $(m \geq 3)$.

We remark that a code of type (k_1,k_2,k_3) is not necessarily a direct sum of linear codes, Z_4-linear codes, and Q_8-type propelinear codes. A code of type (k_1,k_2,k_3) is a subgroup of the group

$$\left(Z_2^{k_1}\oplus Z_4^{k_2}\oplus Q_8^{k_3}, (Id,\phi_4^{k_2},\phi_8^{k_3})\right).$$

as we state in the preliminary definitions on Section I.

In the next example we construct the linear Hamming code of length 7 as a translation-invariant propelinear code of type $(3,0,1)$.

Example 6: Let $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$ be three binary codewords of length 7 defined by

$$\begin{aligned}\boldsymbol{a} &= (100 \mid 1010, \pi_{100|1010})\\ \boldsymbol{b} &= (010 \mid 1001, \pi_{010|1001})\\ \boldsymbol{c} &= (111 \mid 1111, \pi_{111|1111})\end{aligned}$$

where

$$\begin{aligned}\pi_{100|1010} &= Id \mid (4,5)(6,7)\\ \pi_{010|1001} &= Id \mid (4,6)(5,7)\end{aligned}$$

and

$$\pi_{111|1111} = Id \mid Id.$$

Then, the propelinear code generated by $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$ is a perfect translation-invariant propelinear code of length 7.

This code contains the following codewords:

$$\begin{array}{ll}(000 \mid 0000, \pi_{000|0000}) & (111 \mid 1111, \pi_{111|1111}) \\ (100 \mid 1010, \pi_{100|1010}) & (011 \mid 0101, \pi_{011|0101}) \\ (010 \mid 1001, \pi_{010|1001}) & (101 \mid 0110, \pi_{101|0110}) \\ (110 \mid 1100, \pi_{110|1100}) & (001 \mid 0011, \pi_{001|0011}) \\ (000 \mid 1111, \pi_{000|1111}) & (111 \mid 0000, \pi_{111|0000}) \\ (100 \mid 0101, \pi_{100|0101}) & (011 \mid 1010, \pi_{011|1010}) \\ (010 \mid 0110, \pi_{010|0110}) & (101 \mid 1001, \pi_{101|1001}) \\ (110 \mid 0011, \pi_{110|0011}) & (001 \mid 1100, \pi_{001|1100})\end{array}$$

where

$$\begin{aligned}\pi_{000|0000} &= \pi_{111|1111} = \pi_{000|1111} \\ &= \pi_{111|0000} = Id \mid Id \\ \pi_{100|1010} &= \pi_{011|0101} = \pi_{100|0101} \\ &= \pi_{011|1010} = Id \mid (4,5)(6,7) \\ \pi_{010|1001} &= \pi_{101|0110} = \pi_{010|0110} \\ &= \pi_{101|1001} = Id \mid (4,6)(5,7) \\ \pi_{110|1100} &= \pi_{001|0011} = \pi_{110|0011} \\ &= \pi_{001|1100} = Id \mid (4,7)(5,6).\end{aligned}$$

Note that it is a translation-invariant propelinear code of type $(3,0,1)$, that is, a subgroup of $(Z_2^3 \oplus Q_8, (Id, \phi_8))$ where ϕ_8 is the isomorphism defined in Example 3.

All the lemmas we need to prove the following theorem have been placed in the Appendix at the end of the paper.

Theorem 8: Let C be a translation-invariant propelinear code of length n, then C is of type (k_1, k_2, k_3).

Proof: We want to prove that C is a subgroup of $Z_2^{k_1} \oplus Z_4^{k_2} \oplus Q_8^{k_3}$. To do this we will construct a partition of the index set $I = \{1, 2, \cdots, n\} = I_1 \cup I_2 \cup I_3$ where $|I_1| = k_1$, $|I_2| = 2k_2$, $|I_3| = 4k_3$, and $n = k_1 + 2k_2 + 4k_3$ and we will define a translation-invariant propelinear structure on $Z_2^{k_1} \oplus Z_4^{k_2} \oplus Q_8^{k_3}$ of which C be a subgroup.

Let I_1 be the subset of I which contains all the indices $i \in I$ such that $\pi_u(e_i) = e_i$ for all $u \in C$.

Let $\{i,j\}$, $i \neq j$ be two indices not belonging to I_1 such that for all $u \in C$, either $\pi_u(e_i) = e_j$ or $\pi_u(e_i) = e_i$ and $\pi_u(e_j) = e_j$. If $\pi_u(e_i) = e_j$ then, from Proposition 15, $\pi_u(e_j) = e_i$ and from Lemma 14, either $i \in \sup(u)$ and $j \notin \sup(u)$ or $i \notin \sup(u)$ and $j \in \sup(u)$. Thus the restriction of u to the set of indices $\{i,j\}$ is a Z_4-linear code, that is, a code of type (Z_4, ϕ_4) as we have seen in Example 2.

Now, suppose $v \in C$ for which $\pi_v(e_i) = e_i$ and $\pi_v(e_j) = e_j$, then we assert that $i,j \in \sup(v)$ or $i,j \notin \sup(v)$ because if it were not true we can deduce $i,j \in \sup(v \star u)$ or $i,j \notin \sup(v \star u)$ and, from Lemma 5

$$\begin{aligned}\mathrm{wt_H(v \star u)} &= \mathrm{wt}_H((v \star u) \star e_i + e_i) \\ &= \mathrm{wt}_H((v \star u) + \pi_v \circ \pi_u(e_i) + e_i \\ &= \mathrm{wt}_H((v \star u) + e_j + e_i) \\ &< \mathrm{wt}_H(v \star u).\end{aligned}$$

Hence, $i,j \in \sup(v)$ or $i,j \notin \sup(v)$ and the restriction of v to the set of indices $\{i,j\}$ is the same Z_4-linear code previously defined.

Let I_2 be the subset of I which contains all the pairs of indices $\{i,j\}$, $i \neq j$, such that for all $u \in C$, either $\pi_u(e_i) = e_j$ or $\pi_u(e_i) = e_i$ and $\pi_u(e_j) = e_j$.

Let $I_3 = I \backslash (I_1 \cup I_2)$ and suppose $I_3 \neq \emptyset$. Then, there exists $i \in I_3$ and two codewords u, v such that $\pi_u(e_i) = e_j$ and $\pi_v(e_i) = e_k$ with $k \neq j$, $k \neq i$ and $i \neq j$.

Now, from Proposition 17 in the Appendix, if we restrict the action of Π to the set of coordinates $\{i,j,k,l\}$ then $\pi'_u = (i,j)(k,l)$, $\pi'_v = (i,k)(j,l)$, and $\pi'_{u \star v} = (i,l)(j,k)$. We have four possibilities for the coordinate i:

1) $i \in \sup(u)$ and $i \in \sup(v)$.
   In this case $j \notin \sup(u)$ and $k \notin \sup(v)$.
2) $i \notin \sup(u)$ and $i \in \sup(v)$.
   In this case $j \in \sup(u)$ and $k \notin \sup(v)$.
3) $i \in \sup(u)$ and $i \notin \sup(v)$.
   In this case $j \notin \sup(u)$ and $k \in \sup(v)$.
4) $i \notin \sup(u)$ and $i \notin \sup(v)$.
   In this case $j \in \sup(u)$ and $k \in \sup(v)$.

From

$$\mathrm{wt}_H(u+v) = d(u,v) = d(u \star e_i, v \star e_i) = \mathrm{wt}_H(u + e_j + v + e_k)$$

we derive, respectively, two possibilities for each of the previous cases.

1) $j \notin \sup(v)$ and $k \in \sup(u)$
   or $j \in \sup(v)$ and $k \notin \sup(u)$.
2) $j \notin \sup(v)$ and $k \notin \sup(u)$
   or $j \in \sup(v)$ and $k \in \sup(u)$.
3) $j \notin \sup(v)$ and $k \notin \sup(u)$
   or $j \in \sup(v)$ and $k \in \sup(u)$.
4) $j \notin \sup(v)$ and $k \in \sup(u)$
   or $j \in \sup(v)$ and $k \notin \sup(u)$.

So, we have eight possibilities, and the restrictions of vectors u and v to the $\{i,j,k,l\}$ coordinates are

1) $u = (1010, \pi'_u)$, $v = (1001, \pi'_v)$.
2) $u = (1001, \pi'_u)$, $v = (1100, \pi'_v)$.
3) $u = (0101, \pi'_u)$, $v = (1001, \pi'_v)$.
4) $u = (0110, \pi'_u)$, $v = (1100, \pi'_v)$.
5) $u = (1001, \pi'_u)$, $v = (0011, \pi'_v)$.
6) $u = (1010, \pi'_u)$, $v = (0110, \pi'_v)$.
7) $u = (0110, \pi'_u)$, $v = (0011, \pi'_v)$.
8) $u = (0101, \pi'_u)$, $v = (0110, \pi'_v)$.

where $\pi'_u = (i,j)(k,l)$ and $\pi'_v = (i,k)(j,l)$.

In each case it is straightforward to see that the code generated by the $\{i,j,k,l\}$ coordinates of u and v is a translation-invariant propelinear code isomorphic to Q_8 (see Example 3).

Note that in the previous list there are two nonisomorphic Q_8-codes: 1), 3), 6), and 8) are the same code, and 2), 4), 5), and 7) are the same code, too. But, both codes cannot coincide in the same four coordinates. In fact, let C' be the Q_8-code 1), 3), 6), or 8). It can be defined by

$$\left(1010, \pi'_{1010}\right), \quad \left(1001, \pi'_{1001}\right) \tag{1}$$

where $\pi'_{1010} = (i,j)(k,l)$ and $\pi'_{1001} = (i,k)(j,l)$.

Let C'' be the Q_8-code 2), 4), 5), or 7) defined by

$$\left(1001, \pi'_{1001}\right), \quad \left(1100, \pi'_{1100}\right) \tag{2}$$

where $\pi'_{1001} = (i,j)(k,l)$ and $\pi'_{1100} = (i,k)(j,l)$

Then there exist $u \in C'$ such that $\pi_u = (i,j)(k,l)$, $v \in C''$ such that $\pi_v = (i,j)(k,l)$ and the codeword $u \star v$ is different from (0000) and different from (1111) over the set $\{i,j,k,l\}$ but $\pi_{u\star v} = Id$, and this contradicts the construction of Q_8 (see Example 4).

Now, we must show that if $w \in C$ and $\pi_w(e_i) = e_m$, $m \neq i$, $m \neq j$, $m \neq k$ then, either $m = l$ and w belong to the Q_8-code generated by u, v or $m \neq l$ and w cannot be in a translation-invariant propelinear code.

If $m = l$ then, from Proposition 17, $\pi'_w = (i,l)(j,k)$ and the previous construction ensure that $w = u \star v$ or $w = v \star u$.

If $m \neq l$ then we can construct the Q_8-codes $\langle u, v\rangle$, $\langle v, w\rangle$, and $\langle u \star v, w\rangle$. But this contradicts to Lemma 18.

Finally, for every $v \in Z_2^{k_1} \oplus Z_4^{k_2} \oplus Q_8^{k_3}$ we define an isometry π_v in the following way:

1) For all $i \in I_1$, $\pi_v(e_i) = e_i$.
2) For all $\{i,j\} \in I_2$ we define,
   a) $\pi_v(e_i) = e_j$ if $i \in \sup(v)$ and $j \notin \sup(v)$ or $i \notin \sup(v)$ and $j \in \sup(v)$.
   b) $\pi_v(e_i) = e_i$ and $\pi_v(e_j) = e_j$ if $i \in \sup(v)$ and $j \in \sup(v)$ or $i \notin \sup(v)$ and $j \notin \sup(v)$.
3) For all $\{i,j,k,l\} \in I_3$ we can define π_v from (1) or (2) depending on the Q_8-code defined in the four coordinates $\{i,j,k,l\}$.

Hence, $Z_2^{k_1} \oplus Z_4^{k_2} \oplus Q_8^{k_3}$ has one translation-invariant propelinear structure such that C is a subgroup of $Z_2^{k_1} \oplus Z_4^{k_2} \oplus Q_8^{k_3}$. That is, C is of type (k_1, k_2, k_3) with $k_1 + 2k_2 + 4k_3 = n$. ■

If $k_3 = 0$ then we obtain additive codes, that is

Corollary 9: Every additive propelinear code in $\boldsymbol{F}^n$ is of type $(k_1, k_2, 0)$.

V. Propelinear Additive Codes

From Corollary 9 we can state that every additive propelinear code is of type $(k_1, k_2, 0)$. In this way, if we fix the basis $E = \{e_1, \cdots, e_n\}$ there is a one-to-one correspondence between subgroups of $(Z_2^{k_1} \oplus Z_4^{k_2})$ and additive propelinear codes in $\boldsymbol{F}^n$ where $n = k_1 + 2k_2$.

In this section we will use the Z-module structure of $Z_2^{k_1} \oplus Z_4^{k_2}$, denoted by $\boldsymbol{R}$. We define the map

$$\Phi : \boldsymbol{R} \longrightarrow \boldsymbol{F}^n \quad n = k_1 + 2k_2$$

by $\Phi = (Id^{k_1}, \phi_4^{k_2})$ where ϕ_4 is the map defined in the Example 2. Φ is a bijection from $\boldsymbol{R}$ to $\boldsymbol{F}^n$. If $\mathcal{C} \subset \boldsymbol{R}$ is an additive subgroup then $\Phi(\mathcal{C}) = C$ is a binary additive propelinear code of length n. We will call $\mathcal{C}$ an *additive code* in $\boldsymbol{R}$, thus additive codes in $\boldsymbol{R}$ correspond to additive propelinear codes in $\boldsymbol{F}^n$.

We denote the addition in $\boldsymbol{R}$ by $+$. Let $u, v \in \boldsymbol{R}$ be two vectors, then

$$u + v = (u_1 \oplus v_1, \cdots, u_{k_1} \oplus v_{k_1}, u_{k_1+1} + v_{k_1+1}, \cdots, u_{k_1+k_2} + v_{k_1+k_2})$$

where

$$u = (u_1, \cdots, u_{k_1}, u_{k_1+1}, \cdots, u_{k_1+k_2})$$
$$v = (v_1, \cdots, v_{k_1}, v_{k_1+1}, \cdots, v_{k_1+k_2})$$

$\oplus$ denotes the binary addition in Z_2, and $+$ the quaternary addition in Z_4. Also, Φ gives a one-to-one correspondence between cosets of $\mathcal{C}$ and cosets of $C = \Phi(\mathcal{C})$, that is, $\Phi(\mathcal{C} + \tilde{x}) = C \star x$ where $x = \Phi(\tilde{x})$.

Let $\mathcal{C}$ be an additive code in $\boldsymbol{R}$. Althought $\mathcal{C}$ need not have a basis, we can consider a generator matrix for $\mathcal{C}$, that is,

$$G = (A \quad B)$$

where A is an $r \times k_1$ Z_2-matrix and B is an $r \times k_2$ Z_4-matrix, r being the number of rows of G. Thus every $u \in \mathcal{C}$, $u = (u_b, u_q)$ can be expressed as

$$u_b = \bigoplus_{i=1}^{r} (\lambda_i \bmod 2) v_b^i$$
$$u_q = \sum_{i=1}^{r} \lambda_i v_q^i$$

where $\lambda_i \in \{0,1,2,3\}$ and $v^i = (v_b^i, v_q^i)$ is a row of G.

A. Duality of Additive Propelinear Codes

From Delsarte [6] every additive code has associated a dual code such that the weigth enumerator polynomials are related by the McWilliams Identity.

Hence, the additive propelinear codes have associated a dual code. In this section we will define the dual code and we will discuss the weight properties of a code and its dual.

In $\boldsymbol{R}$ we define an inner product in the standard way: given u, v vectors in $\boldsymbol{R}$

$$u \bullet v = 2\left(\bigoplus_{i=1}^{k_1} u_i v_i\right) + \sum_{j=k_1+1}^{k_1+k_2} u_j v_j \in Z_4.$$

It is not difficult to show that $\bullet$ is an inner product on $\boldsymbol{R}$. If $\mathcal{C}$ is a code in $\boldsymbol{R}$ then we define the *dual code* in the standard way

$$\mathcal{C}^{\perp} = \{u \in \boldsymbol{R} \mid u \bullet v = 0 \ \forall v \in \mathcal{C}\}$$

and we define $C^{\perp} = \Phi(\mathcal{C}^{\perp})$. If $v \in \mathcal{C}$, we define the $\mathrm{wt}_H(v) = \mathrm{wt}_H(\Phi(v))$ and the weight enumerator polynomial of $\mathcal{C}$ as that of $C = \Phi(\mathcal{C})$, that is, $W_{\mathcal{C}}(X,Y) = W_{\Phi(\mathcal{C})=C}(X,Y)$.

It is easy to show that if $\mathcal{C}$ is an additive code in $\boldsymbol{R}$ then $\mathcal{C}^{\perp}$ is an additive code in $\boldsymbol{R}$ and $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

The McWilliams Identity (see [6]) related to additive codes is well known. We can see in [3] or [4] a proof for linear codes over $\boldsymbol{F}_q$ and in [8] for Z_4-linear codes. In [12] we can see a proof for linear codes over the ring Z_m (the integers $\bmod m$).

Theorem 10 (McWilliams Identity): Let $\mathcal{C}$ be an additive code in $\boldsymbol{R}$ and $\mathcal{C}^{\perp}$ its dual. If $W_{\mathcal{C}}(X,Y)$ is the weight enumerator polynomial of $\mathcal{C}$ and if $W_{\mathcal{C}^{\perp}}(X,Y)$ is the weight enumerator polynomial of $\mathcal{C}^{\perp}$ then

$$W_{\mathcal{C}^{\perp}}(X,Y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(X+Y, X-Y).$$

Example 7: The linear Hamming code, $\mathcal{H}(7,4)$ can be seen as a code in $\boldsymbol{R} = Z_2^3 \oplus Z_4^2$. The Hamming code is generated by $a = (1,0,0,3,3)$, $b = (0,1,0,3,1)$, and $c = (1,1,1,2,2)$. Its weight enumerator polynomial is

$$W_{\mathcal{H}}(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7.$$

Its dual code is $\mathcal{H}^{\perp}$ which consists of the following vectors:

$$(0,0,0,0,0)$$
$$(0,0,0,2,2)$$
$$(0,1,1,1,3)$$
$$(0,1,1,3,1)$$
$$(1,0,1,1,1)$$
$$(1,0,1,3,3)$$
$$(1,1,0,0,2)$$
$$(1,1,0,2,0)$$

and its weight enumerator polynomial is

$$W_{\mathcal{H}^{\perp}}(X,Y) = X^7 + 7X^3Y^4.$$

We remark that the dual code is generated by

$$u = (1,1,0,0,2),\ v = (0,1,1,1,3) \in Z_2^3 \oplus Z_4^2.$$

B. Decoding Additive Propelinear Codes

Let C be an e-error correcting additive propelinear code. Assume that a codeword $c \in C$ is transmitted through a binary-symmetric channel and a vector $x \in \boldsymbol{F}^n$ is received at the channel output. We wish to decode x, that is, find the unique codeword c of C at distance at most e from x. Such a codeword exists and is equal to c, provided $x = c \oplus \epsilon$, where the weight of the error vector ϵ is at most e.

Let $\mathcal{C}$ be the additive code in $\boldsymbol{R}$ such that $\mathcal{C} = \Phi^{-1}(C)$. Let $\mathcal{C}^{\perp}$ the dual code of $\mathcal{C}$ and let H be a generator matrix for $\mathcal{C}^{\perp}$. Thus H is a parity check matrix for the code $\mathcal{C}$, that is, $v \in \mathcal{C}$, if and only if $Hv^t = \mathbf{0}$.

Let $\tilde{x} \in \boldsymbol{F}^n$ be the codeword $\tilde{x} = \Phi^{-1}(x)$. We will see that if $\tilde{c}$ is the unique codeword of $\mathcal{C}$ at distance at most e from $\tilde{x}$ then $\Phi(\tilde{c}) = c \in C$ is the unique codeword of C at distance at most e from x.

For additive codes in $\boldsymbol{R}$ there exists an easy way to find the coset where $\tilde{x}$ is. For all $v \in \boldsymbol{R}$ we define the *syndrome* map

$$S : \boldsymbol{R} \to Z_4^r$$

by $S(v) = Hv^t \in Z_4^r$ where r is the number of rows in H.

As in the linear case there exists a one-to-one correspondence between syndromes and cosets, that is, for all $u, v \in \boldsymbol{R}$ $S(u) = S(v)$ if and only if $\mathcal{C} + u = \mathcal{C} + v$.

If $\tilde{x} \in \mathcal{C} + \tilde{\epsilon}$ where $\tilde{\epsilon}$ has minimum weight then $\tilde{x} = \tilde{c} + \tilde{\epsilon}$ and, from Proposition 4, $d(\tilde{c}, \tilde{x}) = d(\tilde{c}, \tilde{c} + \tilde{\epsilon}) = wt_H(\tilde{\epsilon})$ and $\tilde{c}$ is the unique codeword of $\mathcal{C}$ at distance at most e from $\tilde{x}$. Since $d(\tilde{c}, \tilde{x}) = d(c, x)$ where $c = \Phi(\tilde{c})$ and $x = \Phi(\tilde{x})$ we have that c is the unique codeword in C at distance at most e from x.

C. Perfect Additive Propelinear Codes

A binary code C of length n is a *ρ-perfect* code if there exists an integer $\rho \geq 0$ such that every $x \in \boldsymbol{F}^n$ is within distance ρ from exactly one codeword of C. The parameters of perfect codes are well known. It is shown in [13]–[15] that such codes exist only for $\rho = 0$, $\rho = n$, $\rho = (n-1)/2$ with n odd, $\rho = 1$ with $n = 2^m - 1$ and $\rho = 3$ with $n = 23$.

The first three cases are trivial codes. The last code is the Golay code and we know that it is linear and unique with its parameters. It is shown that the Golay code is not Z_4-linear (see [8]) and that the only propelinear structure is the linear one (see [9]).

The perfect linear 1-error correcting codes, namely Hamming codes, are unique but the full classification of nonlinear perfect 1-correcting codes is not known. For a good overview of this topic the reader can see the paper of Etzion and Vardy [16].

In this section we shall construct a family of perfect additive codes. They are not linear codes but of type $(k_1, k_2, 0)$ where $k_1 + 2k_2 = n$ and $n = 2^m - 1$, $(m \geq 4)$. Moreover, they have a very simply decoding algorithm.

Let ${}^lH$ and H^r be two matrices constructed in the following way: ${}^lH$ is the parity-check matrix of the Hamming code of length $2^m - 1$, $(m \geq 3)$. H^r is the matrix obtained from ${}^lH$ by adding an all-zero first column. We define $\mathcal{H} = \Phi^{-1}({}^lH \mid H^r)$ where $\Phi : \boldsymbol{R} \to \boldsymbol{F}^n$ $(n = 2^{m+1} - 1)$ and $\boldsymbol{R} = Z_2^{(n-1)/2} \oplus Z_4^{(n+1)/4}$.

For example, for $m = 3$

$${}^lH = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$H^r = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\mathcal{H} = \left(\begin{array}{ccccccc|cccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 2 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right).$$

Theorem 11: Let $\mathcal{C}$ be the additive code in $\boldsymbol{R}$ generated by $\mathcal{H}$. Then $C = \Phi(\mathcal{C})$ is an additive propelinear code of length $n = 2^{m+1} - 1$. Its weight enumerator polynomial is

$$W_C(X,Y) = X^n + nX^{(n-1)/2}Y^{(n+1)/2}.$$

Proof: First, we compute $|\mathcal{C}|$. $\mathcal{H}$ is a generator matrix for $\mathcal{C}$. The first $m-1$ rows of $\mathcal{H}$ have order two and the last row has order four. Thus the additive code generated by $\mathcal{H}$ has order $2^{m-1} \cdot 4 = 2^{m+1} = n + 1$.

Next we compute its weight enumerator polynomial. The code generated by $\mathcal{H}^r$ is equivalent to first-order Reed–Muller code (see [8, Theorem 7] and [3, ch. 15]). It has $2^{m+1} - 2$ codewords of weight 2^{m-1}, one codeword of weight zero (the all-zero codeword), and one codeword of weight 2^m (the all-two codeword: $222\cdots2$).

Moreover, the linear code generated by ${}^lH$ is the simplex code and has $2^m - 1$ codewords of weight 2^{m-1} and one codeword of weight 0 (the all-zero codeword). This linear code belongs twice in $\mathcal{C}$ and its all-zero codeword forms the

codeword $(00\cdots0 \mid 00\cdots0)$ and the codeword $(00\cdots0 \mid 22\cdots2)$. Thus in $\mathcal{C}$ there exists one vector of weight zero, $2^{m+1}-2$ codewords of weight $2^{m-1}+2^{m-1}=2^m$, and one codeword of weight $0+2^m=2^m$, that is, $2^{m+1}-1=n$ codewords of weight $2^m=\frac{n+1}{2}$.

Thereby, the code $\mathcal{C}$ has the following weight enumerator polynomial:

$$W_{\mathcal{C}}(X,Y)=X^n+nX^{(n-1)/2}Y^{(n+1)/2}.$$

The theorem follows from the equality $W_{\mathcal{C}}(X,Y)=W_C(X,Y)$. ∎

Corollary 12: For $m\geq 3$, $\Phi(\mathcal{C}^\perp)$ is a perfect 1-error correcting nonlinear code of length $n=2^{m+1}-1$.

Proof: From the McWilliams Identity (Theorem 10) and from the previous theorem

$$\begin{aligned}W_{\Phi(\mathcal{C}^\perp)}(X,Y)&=W_{\mathcal{C}^\perp}(X,Y)\\&=\frac{1}{|\mathcal{C}|}W_{\mathcal{C}}(X+Y,X-Y)\\&=\frac{1}{|C|}W_C(X+Y,X-Y)\end{aligned}$$

that is, the weight enumerator polynomial of $\Phi(\mathcal{C}^\perp)$ coincides with the weight enumerator polynomial of a perfect 1-error correcting code (see [3, ch. 5]). Since $\Phi(\mathcal{C}^\perp)$ is a propelinear code then it is distance invariant (see Proposition 4) and the minimum distance of $\Phi(\mathcal{C}^\perp)$ is equal to the minimum weight. Hence, the code is perfect (see [16]).

Next we show that $\Phi(\mathcal{C}^\perp)$ is a nonlinear binary code. For instance, if we take $\tilde{u}=(0\cdots0010 \mid 30\cdots001)$ and $\tilde{v}=(0\cdots0100 \mid 10\cdots010)$, then $\tilde{u},\tilde{v}\in\mathcal{C}^\perp$. Thus

$$\Phi(\tilde{u})=u=(0\cdots0010 \mid 1000\cdots000001)\in\Phi(\mathcal{C}^\perp)$$

and

$$\Phi(\tilde{v})=v=(0\cdots0100 \mid 0100\cdots000100)\in\Phi(\mathcal{C}^\perp)$$

but

$$\begin{aligned}\Phi^{-1}(u\oplus v)&=\Phi^{-1}(0\cdots0110 \mid 1100\cdots000101)\\&=(0\cdots0110 \mid 20\cdots011)\notin\mathcal{C}^\perp.\end{aligned}$$ ∎

Remark 2: The previous theorem constructs nonlinear perfect codes of length 15, 31, 63, …. For $n=7$ there is only one perfect code, the Hamming code. Our construction can be applied here from

$${}^tH=\begin{pmatrix}0&1&1\\1&0&1\end{pmatrix}$$

and we obtain the description of Hamming code as the propelinear code seen in Example 7.

The Hamming codes have a very simply decoding algorithm (see [3], [4]). We will see that our family of additive perfect codes has a decoding algorithm which is comparable in complexity to the decoding algorithm for perfect 1-error correcting linear codes.

Let $c\in C$ be the transmitted codeword and let $x=c\oplus\epsilon\in\boldsymbol{F}^n$ be the received vector where $\mathrm{wt}_H(\epsilon)\leq 1$. We denote $\Phi^{-1}(c)$ by $\tilde{c}$ and $\Phi^{-1}(x)$ by $\tilde{x}$. If $d(\tilde{c},\tilde{x})=1$ then there exists $\tilde{\epsilon}\in\boldsymbol{R}$ with $\mathrm{wt}_H(\tilde{\epsilon})=1$ such that $\tilde{x}=\tilde{c}+\tilde{\epsilon}$ and $\tilde{\epsilon}=1$ or $\tilde{\epsilon}=3$.

Theorem 13 (Decoding Algorithm): Let $a=\mathcal{H}\tilde{x}^t$ be the syndrome of the received vector. Then a is a vector of m coordinates in Z_4. If $a=(a_1,a_2,\cdots,a_m)$ we define the number

$$p=\sum_{i=1}^{m}a_i2^{m-i}.$$

1) If $p=0$ then $x=\Phi(\tilde{x})$ is the transmitted codeword.
2) If $p=0\,(\mathrm{mod}\,2)$ then there is a single error in the $p/2$ coordinate of $\tilde{x}$.
3) If $p=1\,(\mathrm{mod}\,2)$ then there is a single error of weight 1 $(\tilde{\epsilon}=a_m)$ in the coordinate $k_1+\frac{p-a_m}{4}+1$ of $\tilde{x}$.

Proof: Let

$$h^1,h^2,\cdots,h^{k_1},h^{k_1+1},\cdots,h^{k_1+k_2}$$

be the k_1+k_2 columns of $\mathcal{H}$. If the error is in position j, with $j\leq k_1$ then $a=2h^j$ and

$$p=2\sum h_i^j2^{m-i}.$$

If the binary error is in position j, with $k_1+1\leq j\leq k_1+k_2$ then $\tilde{\epsilon}=a_m$ and $a_m=1$ or $a_m=3$. Hence,

$$p=\sum_{i=1}^{m-1}h_i^j2^{m-i}+a_m$$

and $p=1\pmod 2$. Let $D=(d^0,d^1,\cdots,d^{k_2-1})$ be a matrix whose columns are the binary representations of integers $0,1,\cdots,k_2-1$. Then, the submatrix of $\mathcal{H}^r$ constituted by the first $m-1$ rows is equal to the matrix $2D$. Now, for $k_1+1\leq j\leq k_1+k_2$

$$p-a_m=\sum_{i=1}^{m-1}h_i^j2^{m-i}=\sum_{i=1}^{m-1}2d_i^{j-(k_1+1)}2^{m-i}$$

and

$$\frac{p-a_m}{4}=\sum_{i=1}^{m-1}d_i^{j-(k_1+1)}2^{m-i-1}$$

where

$$\sum_{i=1}^{m-1}d_i^{j-(k_1+1)}2^{m-i-1}$$

is the decimal representation of the integer $j-(k_1+1)$. That is, the error is in the coordinate $(p-a_m)/4+k_1+1$. ∎

VI. Conclusion and Further Research

In this paper we have shown that propelinear binary codes are a good way to handle nonlinear binary codes. Moreover, when we consider translation-invariant propelinear codes then we obtain a classification theorem. This classification includes additive propelinear codes and some nonadditive but translation-invariant codes, the Q_8-codes. We think that Q_8-codes are not as good as additive propelinear codes but they have good algebraic and combinatorial properties. For instance, the Hamming code, $\mathcal{H}(7,4)$, has a Q_8-structure, exactly it is of type $(3,0,1)$ (see Example 6). Further results on this topic would be interesting to investigate.

Moreover, we have constructed a family of nonlinear 1-error correcting codes and the decoding algorithm to correct the error. This kind of constructed codes is additive and further research on this topic can include new families of nonadditive 1-error correcting codes.

APPENDIX

We assume that (C, Π) is a translation-invariant propelinear code.

Lemma 14: If $v \in C$ then either $\pi_v = Id$ or $\pi_v(v) \neq v$. In the last case, for every $i \in I$ such that $\pi_v(e_i) = e_j \neq e_i$ we have, if $i \in \sup(v)$ then $j \notin \sup(v)$ and if $i \notin \sup(v)$ then $j \in \sup(v)$.

Proof: Since C is a translation-invariant code, if $\pi_v \neq Id$, then there exist two coordinate vectors $e_i \neq e_j$ such that

$$\mathrm{wt}_H(v) = \mathrm{wt}_H(v \star e_i + e_i) = \mathrm{wt}_H(v + e_j + e_i)$$

according to Lemma 5. Hence, $i \in \sup(v)$ if and only if $j \notin \sup(v)$. ∎

Proposition 15: $\forall v \in C$, $\pi_v^2 = Id$, and Π has an Abelian group structure.

Proof: Since C is a translation-invariant code, from Lemma 5, $\forall v \in C$ and $\forall x \in F^n$

$$\mathrm{wt}_H(v) = d(x, v \star x) = \mathrm{wt}_H(x + v + \pi_v(x)).$$

This equality is true if $\pi_v = Id\ \forall v \in C$ or, otherwise, there exists $x \in \boldsymbol{F}^n$ such that $\pi_v(x) \neq x$ and, therefore, there exists a vector of weight 1, e_i, such that $\pi_v(e_i) \neq e_i$.

In this case, let $\pi_v(e_i) = e_j \neq e_i$ and suppose $\pi_v(e_j) = e_k$. Obviously, $e_k \neq e_j$ and, from Lemma 14, $i, k \in \sup(v)$ and $j \notin \sup(v)$ or $i, k \notin \sup(v)$ and $j \in \sup(v)$.

Suppose $e_k \neq e_i$. Then

$$\begin{aligned}&\mathrm{wt}_H((e_i + e_j) + v \star (e_i + e_j))\\ &\quad = \mathrm{wt}_H(e_i + e_j + v + \pi_v(e_i + e_j))\\ &\quad = \mathrm{wt}_H(e_i + e_j + v + e_j + e_k) < \mathrm{wt}_H(v)\end{aligned}$$

which contradicts to Lemma 5. So, $e_k = e_i$ and $\pi_v^2 = Id$. All the elements in Π are idempotents, so Π has an Abelian group structure. ∎

From this proposition we can assert that for every $v \in C$, $\pi_v = Id$ or π_v is a product of coordinate transpositions.

The next corollary is straightforward from the previous proposition.

Corollary 16: $\forall v \in C$, $v^4 = 0$.

Proposition 17: If $u, v \in C$ and $\pi_u(e_i) = e_j$, $\pi_v(e_i) = e_k$ with $j \neq k$, $j \neq i$ and $k \neq i$ then

1) $\pi_u(e_k) = \pi_v(e_j) = e_l$ with $l \neq i$, $l \neq j$ and $l \neq k$.
2) Let Π' be the restriction of Π over the set of coordinates $\{i, j, k, l\}$. Then $\pi'_u = (i, j)(k, l)$, $\pi'_v = (i, k)(j, l)$, and $\pi'_{u \star v} = \pi'_{v \star u} = (i, l)(j, k)$.

Proof: The first assertion is clear because Π is Abelian. For the second assertion we have

$$\pi'_{u \star v} = \pi'_u \circ \pi'_v = \pi'_v \circ \pi'_u = \pi'_{v \star u} = (i, l)(j, k).$$ ∎

Lemma 18: Let $a, b, c \in C$ be three codewords such that the subcodes $\langle a, b\rangle$ and $\langle b, c\rangle$ are different Q_8-codes (see Example 3). Then the subcode $\langle a \star b, c\rangle$ cannot be a Q_8-code.

Proof: The code $\langle a, b\rangle$ and the code $\langle b, c\rangle$ fulfil the conditions

$$x^4 = 0 \qquad x^2 = y^2 \qquad x \star y \star x = y$$

and, from this, $y \star x = y^3 \star x$.

Now, if $\langle a \star b, c\rangle$ were a Q_8-code then

$$(a \star b) \star c \star (a \star b) = c$$

but

$$\begin{aligned}(a \star b) \star c \star (a \star b) &= a \star (c^3 \star b) \star (a \star b)\\ &= (c \star a) \star b \star (a \star b)\\ &= c \star (a \star b) \star (a \star b)\\ &= c \star (a \star b)^2 = c \star c^2 = c^3 \neq c.\end{aligned}$$

So, the lemma is proved. ∎

ACKNOWLEDGMENT

The authors wish to thank the referees for their helpful comments, which helped very much to improve the presentation of the paper.

REFERENCES

[1] D. Slepian, "Group codes for the gaussian channel," *Bell Syst. Tech. J.*, vol. 47, pp. 575–602, Apr. 1968.
[2] G. D. Forney, "On the hamming distance properties of group codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 6, pp. 1797–1801, Nov. 1992.
[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[4] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge, U.K.: Cambridge Univ. Press, 1988.
[5] J. H. van Lint, *Introduction to Coding Theory*. New York: Springer-Verlag, 1982.
[6] P. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Res. Rep. Suppl.*, vol. 10, 1973.
[7] A. Brouwer, A. M. Cohen, and A. Neumaier, *Distance Regular Graphs*. New York: Springer-Verlag, 1989.
[8] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The Z_4-linearity of Kerdock, Preparata, Goethals and related codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 1, pp. 301–319, Jan. 1994.
[9] J. Rifà, J. M. Basart, and L. Huguet, "On completely regular propelinear codes," in *Proc. 6th Int. Conf., AAECC-6, Lecture Notes in Computer Science*, no. 357. New York: Springer-Verlag, 1989, pp. 341–355.
[10] J. Rifà, "On a categorial isomorphism between a class of completely regular codes and a class of distance regular graphs," in *Proc. 8th Int. Conf., AAECC-8, Lecture Notes in Computer Science*, no. 508. New York: Springer-Verlag, 1991, pp. 164–179.
[11] R. D. Baker, J. H. Van Lint, and R. M. Wilson, "On the Preparata and Goethals codes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 342–345, 1983.
[12] M. Klemm, "Über die identität von mcwilliams für die gewichtsfunktion von codes," *Arch. Math.*, vol. 49, pp. 400–406, 1987.
[13] J. H. van Lint, "Nonexistence theorems for perfect error-correcting-codes," *Computers in Algebra and Number Theory*, vol. IV, 1971.
[14] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, pp. 88–96, 1973.
[15] V. A. Zinov'ev and V. K. Leont'ev, "The nonexistence of perfect codes over galois fields," *Probl. Contr. Inform. Theory*, vol. 2, pp. 123–132, 1973.
[16] T. Etzion and A. Vardy, "Perfect binary codes: Constructions and properties and enumeration," *IEEE Trans. Inform. Theory*, vol. 40, pp. 754–763, 1994.