1-Perfect Uniform and Distance Invariant Partitions *

J. Rifà, J. Pujol, J. Borges

Dept. d'Informàtica, Universitat Autònoma de Barcelona
08193-Bellaterra, Spain (e-mail: {jborges, jrifa, jpujol}@ccd.uab.es)

Abstract. Let F^n be the n-dimensional vector space over $\mathbb{Z}_2$. A *(binary) 1-perfect partition* of F^n is a partition of F^n into (binary) perfect single error-correcting codes or 1-perfect codes.

We define two metric properties for 1-perfect partitions: uniformity and distance invariance. Then we prove the equivalence between these properties and algebraic properties of the code (the class containing the zero vector). In this way, we characterize 1-perfect partitions obtained using 1-perfect translation invariant and not translation invariant propelinear codes.

The search for examples of 1-perfect uniform but not distance invariant partitions enabled us to deduce a non-Abelian propelinear group structure for any Hamming code of length greater than 7.

Keywords: Perfect propelinear codes, perfect uniform partitions, perfect distance invariant partitions.

1 Introduction

Let F^n be the n-dimensional vector space over $\mathbb{Z}_2$. A *(binary) 1-perfect partition* of F^n is a partition of F^n into (binary) perfect single error-correcting codes or 1-perfect codes. Given a 1-perfect code $\mathcal{C}$, we can always construct a 1-perfect partition by means of translates of $\mathcal{C}$, namely $\mathcal{C}$, $\mathcal{C} + e_1$, $\mathcal{C} + e_2$, $\ldots$, $\mathcal{C} + e_n$; where $e_1, \ldots, e_n$ are the vectors with exactly one nonzero entry.

*This work was partially supported by CICYT Grant TIC2000-0739-C04-01.

In [3], the question of the existence of a different 1-perfect partition containing a given 1-perfect code $\mathcal{C}$ as a class is proposed. The answer is given in [10], where it is proved that there always exist nonequivalent 1-perfect partitions containing a given 1-perfect code as a class.

In [7], a construction of 1-perfect codes is presented using the fact that a 1-perfect partition can be always seen as a quasigroup. This construction enables the full characterization of *1-perfect additive codes* in a subsequent paper ([2]). Now, in this paper we characterize a class of 1-perfect partitions, namely 1-perfect uniform partitions, by proving that the code in such partitions is always a 1-perfect propelinear code. Moreover, the subclass of 1-perfect distance invariant uniform partitions is characterized by proving that the code is always a 1-perfect translation invariant propelinear code.

The paper is organized as follows. In Section II, we give the basic definitions for 1-perfect codes, equivalence of partitions and propelinear codes. In Section III, we see the partial equivalence between 1-perfect propelinear codes and 1-perfect uniform partitions. In Section IV, we see the equivalence between 1-perfect translation invariant propelinear codes and 1-perfect distance invariant partitions. In Section V, we construct 1-perfect uniform partitions which are not distance invariant for all lengths $n = 2^t - 1$ with $t \geq 4$. This construction uses a propelinear and not translation invariant structure of translation invariant propelinear codes such as Hamming codes. In Section VI, we briefly discuss the case of 1-perfect distance invariant nonuniform partitions. Finally, in Section VII, we summarize the results and conclusions of this paper.

2 Preliminaries

2.1 1-Perfect codes

The *support* of a vector $v \in F^n$, denoted by $supp(v)$, is the set of nonzero coordinate positions of v. The *(Hamming) weight*, $\mathrm{wt}(v)$, of a vector $v \in F^n$ is the number of its nonzero coordinates, i.e. $\mathrm{wt}(v) = |supp(v)|$. We define the *(Hamming) distance* between two vectors $v, u \in F^n$ as $d(v, u) = \mathrm{wt}(v+u)$. If $X \subset F^n$ and $v \in F^n$, we will denote the *distance of v to X* by $d(v, X)$, that is, $d(v, X) = min\{d(v, x) \mid x \in X\}$. We also define the sum $X + Y$ as the set of all vectors that can be expressed as a sum of a vector in X plus a vector in Y. As usual, we will write $X + x$ instead of $X + \{x\}$.

A subset $\mathcal{C}$ of F^n is called a *(binary) code*. If $\mathcal{C}$ is a linear subspace, then $\mathcal{C}$ is a *linear* code. We call the elements of a code *codewords* or *codevectors*. We say that two codes, $\mathcal{C}_1$ and $\mathcal{C}_2$, are *isomorphic* if there exists a coordinate permutation π such that $\pi(\mathcal{C}_1) = \mathcal{C}_2$. Given two codes, $\mathcal{C}_1$ and $\mathcal{C}_2$, we say that $\mathcal{C}_1$ is a *translate* of $\mathcal{C}_2$ if there is a vector $v \in F^n$ such that $\mathcal{C}_1 = \mathcal{C}_2 + v$. Finally, we will say that two codes are *equivalent* if one is a translate of an isomorphic code to the other code. In this paper, we always consider binary codes containing the all-zero vector, denoted by $\mathbf{0}$, unless stated otherwise.

The *code distance* in $\mathcal{C}$ is $d_{\mathcal{C}} = min\{d(x,y) \mid x,y \in \mathcal{C}, x \neq y\}$. The *minimum weight* in $\mathcal{C}$ is $\mathrm{wt}_{\mathcal{C}} = min\{\mathrm{wt}(x) \mid x \in \mathcal{C} \setminus \{\mathbf{0}\}\}$.

A *perfect single error-correcting code* $\mathcal{C}$ *of length* n is a subset of F^n, such that the code distance of $\mathcal{C}$ is 3, and $d(v,\mathcal{C}) \leq 1$, for all $v \in F^n$. For a perfect single error-correcting code $\mathcal{C}$ of length n we have that $|\mathcal{C}|(n+1) = 2^n$, hence $n = 2^t - 1$ for some positive integer $t \geq 2$ (see [5]). In fact, for any $n = 2^t - 1$ ($t \geq 2$), there is exactly one 1-perfect linear code of length n, up to isomorphism, which is the well-known *Hamming code*. A perfect single error-correcting code will be called *1-perfect code*, from now on.

2.2 Equivalence of 1-perfect partitions

If $n = 2^t - 1$, then a 1-perfect code $\mathcal{C}$ of length n has 2^{n-t} codewords, and therefore, a 1-perfect partition in F^n will have $2^t = n + 1$ classes. Since we always assume that $\mathbf{0} \in \mathcal{C}$, given a 1-perfect partition we will call the class containing $\mathbf{0}$ *the code*. Let $e_0 = \mathbf{0}$ and e_i be the vector of weight 1 with the nonzero coordinate in the i^{th} position, for all $i = 1, \ldots, n$. Given a 1-perfect code $\mathcal{C}$, we can always define a 1-perfect partition as $\{\mathcal{C} + e_i\}_{i=0}^n$; we will call it the *trivial* partition.

Given a 1-perfect partition, if we apply a coordinate permutation and/or a translation by a fixed vector, then we obtain a (possibly) different 1-perfect partition. However, two such partitions will have the same properties.

Definition 1 *Let* $\Omega = \{C_0, C_1, \ldots, C_n\}$ *and* $\Omega' = \{C'_0, C'_1, \ldots, C'_n\}$ *be 1-perfect partitions of* F^n. *We say that* Ω *and* Ω' *are* isomorphic *if there is a coordinate permutation* σ *such that* $C_i = \sigma(C'_{\pi(i)})$, *for all* $i = 0, \ldots, n$ *and for some permutation* π *over the set* $\{0, \ldots, n\}$. *We say that* Ω *and* Ω' *are* equivalent *if there is a coordinate permutation* σ *and a vector* $x \in F^n$ *such that* $C_i = \sigma(C'_{\pi(i)}) + x$, *for all* $i = 0, \ldots, n$ *and for some permutation* π *over the set* $\{0, \ldots, n\}$.

2.3 Propelinear codes

For the definitions and properties included in this subsection we follow [9] and [8].

Let $\mathcal{S}_n$ denote the symmetric group of permutations over the set $\{1,\dots,n\}$. For any vector $v=(v_1,\dots,v_n)\in F^n$, we will write $\pi(v)$, where $\pi\in\mathcal{S}_n$, to denote the vector $(v_{\pi^{-1}(1)},\dots,v_{\pi^{-1}(n)})$.

A code $\mathcal{C}$ of length n is said to be *propelinear* if for any codeword $x\in\mathcal{C}$ there is $\pi_x\in\mathcal{S}_n$ verifying the properties:

1. $x+\pi_x(y)\in\mathcal{C}$ if $y\in\mathcal{C}$.
2. $\pi_x\circ\pi_y=\pi_z \quad \forall y\in\mathcal{C}$, where $z=x+\pi_x(y)$.

We define the binary operation $\star:\mathcal{C}\times F^n\longrightarrow F^n$ such that

$$x\star y=x+\pi_x(y)\ \ \forall x\in\mathcal{C}\ \ \forall y\in F^n.$$

This operation is clearly associative and closed in $\mathcal{C}$. Since, for any codeword $x\in\mathcal{C}$, $x\star y=x\star z$ implies $y=z$, we have that $x\star y\in\mathcal{C}$ if and only if $y\in\mathcal{C}$. Thus, there must be a codeword e such that $x\star e=x$. It follows that $e=\mathbf{0}$ is a codeword and, from 2, we deduce that $\pi_{\mathbf{0}}$ is the identity permutation. Hence, $(\mathcal{C},\star)$ is a group, which is not Abelian in general; $\mathbf{0}$ is the identity element in $\mathcal{C}$ and $x^{-1}=\pi_x^{-1}(x)$, for all $x\in\mathcal{C}$. Note that $\Pi=\{\pi_x\mid x\in\mathcal{C}\}$ is a subgroup of $\mathcal{S}_n$ with the usual composition of permutations. By $(\mathcal{C},\Pi)$ we shall mean the set of all pairs (x,π_x), where $x\in\mathcal{C}$.

Clearly, the class of propelinear codes is more general than the class of linear codes.

A propelinear code $\mathcal{C}$ is said to be a *translation invariant code* if

$$d(x,y)=d(x\star u,y\star u)\quad\forall x,y\in\mathcal{C}\quad\forall u\in F^n.$$

A propelinear code is not necessarily translation invariant. However, the following different equation is always true:

$$d(u,v)=d(x\star u,x\star v)\quad\forall x\in\mathcal{C}\ \ \forall u,v\in F^n. \tag{1}$$

Using (1) we can prove (see [9]) that a propelinear code $\mathcal{C}$ is translation invariant if and only if

$$\mathrm{wt}(v)=d(x,v\star x)\qquad\forall x\in F^n\quad\forall v\in\mathcal{C}. \tag{2}$$

As can be seen in [9], any translation invariant propelinear code can be viewed as a group isomorphic to a subgroup of $\mathbb{Z}_2^{k_1} \oplus \mathbb{Z}_4^{k_2} \oplus \mathcal{Q}_8^{k_3}$; where $k_1 + 2k_2 + 4k_3 = n$ and $\mathcal{Q}_8$ is the quaternion group on eight elements. We will say these codes are of *type* (k_1, k_2, k_3). Hence, translation invariant propelinear codes include linear codes, of type $(k_1, 0, 0)$, and $\mathbb{Z}_4$-linear codes (see [4]), of type $(0, k_2, 0)$.

Since $\mathcal{Q}_8$ is not Abelian, we deduce that translation invariant propelinear Abelian codes must be of type $(k_1, k_2, 0)$. In [2], it is proved that any 1-perfect translation invariant propelinear code is of type $(k_1, k_2, 0)$, except for the Hamming code of length 7, that has structures of type $(7, 0, 0)$, $(3, 2, 0)$ and $(3, 0, 1)$.

3 1-Perfect Uniform Partitions

Given a 1-perfect partition of F^n ($n = 2^t - 1$, $t \geq 2$), $\Omega = \{C_0, C_1, \ldots, C_n\}$, and a vector $v \in F^n$, such that v is in the class C_k, we denote by $\gamma_i(v)$ ($i \neq k$), the only vector $x \in C_i$ such that $d(v, x) = 1$. We also define $\Gamma_{ij}(v)$ ($i \neq j, i \neq k \neq j$) as the class containing the only vector u such that $d(u, \gamma_i(v)) = 1$, $d(u, \gamma_j(v)) = 1$ and $d(u, v) = 2$.

Definition 2 *A 1-perfect partition $\Omega = \{C_0, C_1, \ldots, C_n\}$ is called* uniform *if the class $\Gamma_{ij}(v)$ does not depend on v, but only on C_k, for all $v \in F^n$, where C_k is the class containing v and i, j, k are all different.*

Note that this is a geometric condition. For instance, given a 1-perfect partition such that for all $i, j = 0, \ldots, n$ we have $C_i = C_j + e_k$ for some $k = \{0, \ldots, n\}$, then the 1-perfect partition is uniform. At the end of this section, we will see that the trivial partition is uniform if and only if the class containing $\mathbf{0}$ is a linear code.

Also, it is clear that if Ω and Ω' are two equivalent 1-perfect partitions of F^n, then Ω is uniform if and only if Ω' is uniform.

Let $\mathcal{C}$ be a propelinear code, we define

$$\Omega(\mathcal{C}) = \{C_0 = \mathcal{C}, C_1, \ldots, C_n\},$$

where $C_i = \mathcal{C} \star e_i$, for all $i = 0, \ldots, n$. We also define the minimum distance of $\Omega(\mathcal{C})$ by

$$\delta = \min_{D \in \Omega(\mathcal{C})} \{d(x, y) | x, y \in D, x \neq y\}.$$

Obviously, if d is the minimum distance between codewords of $\mathcal{C}$, then $\delta \leq d$ and if $\mathcal{C}$ is a translation invariant code, then $\delta = d$.

Now, we look for some necessary conditions such that $\Omega(\mathcal{C})$ becomes a 1-perfect partition.

Lemma 3 *If $\mathcal{C}$ is a 1-perfect propelinear code with $\delta = 3$, then $\Omega(\mathcal{C})$ is a 1-perfect partition.*

Proof. Given two different codewords, $x, y \in \mathcal{C}$, we have that $x \star e_i \neq y \star e_i$, for all $i = 0, \ldots, n$; because $d(z, z \star e_i) \leq 1$, for all $z \in \mathcal{C}$ and for all $i = 0, \ldots, n$ and $d(x, y) \geq 3$. Hence, $|C_i| = |\mathcal{C}|$. Thus, all classes have the correct number of vectors to be a 1-perfect code. Since the minimum distance is always 3, the result holds. ∎

Corollary 4 *If $\mathcal{C}$ is a 1-perfect translation invariant propelinear code, then $\Omega(\mathcal{C})$ is a 1-perfect partition.*

Proof. Since $\mathcal{C}$ is translation invariant, we have that $\delta = 3$. ∎

Now, we will see that 1-perfect propelinear codes give rise to 1-perfect uniform partitions if $\delta = 3$.

Lemma 5 *Let $\mathcal{C}$ be a propelinear code and let $C_i = \mathcal{C} \star e_i$, for all $i = 0, 1, \ldots, n$. Then, for all $i = 0, 1, \ldots, n$*

$$v \star x \in C_i \quad \forall v \in \mathcal{C} \ \ \forall x \in C_i.$$

Proof. If $x \in C_i$, then there is a codeword $u \in \mathcal{C}$ such that $x = u \star e_i$. Hence,

$$\begin{aligned} v \star x &= v \star (u \star e_i) = v \star (u + \pi_u(e_i)) \\ &= v + \pi_v(u) + \pi_v \circ \pi_u(e_i) = v \star u + \pi_{v \star u}(e_i) \\ &= (v \star u) \star e_i. \end{aligned}$$

Since $v \star u$ is a codeword, $(v \star u) \star e_i$ must be in C_i. ∎

Proposition 6 *Let $\mathcal{C}$ be a 1-perfect propelinear code with $\delta = 3$. Then, $\Omega(\mathcal{C})$ is a 1-perfect uniform partition.*

Proof. From Lemma 3, $\Omega(\mathcal{C})$ is a 1-perfect partition.

Let $v \in \mathcal{C}$, then $\gamma_i(v) = v \star e_i$ and $\gamma_j(v) = v \star e_j$. Clearly, the vector $u = v \star (e_i + e_j)$ is at distance one apart from $v \star e_i$ and from $v \star e_j$ and at distance two from v. Thus, $\Gamma_{ij}(v)$ is the class containing u and by Lemma 5, it is the same class that contains $e_i + e_j$. Hence, $\Gamma_{ij}(v)$ does not depend on v.

Now, let $z \in C_k$, where $k \neq 0$. There must be a codeword $v \in \mathcal{C}$ such that $z = v \star e_k$. It is also clear that there is $r \in \{1, \ldots, n\}$ such that $\gamma_i(z) = v \star (e_k + e_r)$, similarly $\gamma_j(z) = v \star (e_k + e_s)$, for some $s \in \{1, \ldots, n\}$. We assume that $i \neq j$ and $i \neq k \neq j$. Then, the vector $u = v \star (e_k + e_r + e_s)$ is at distance one apart from $\gamma_i(z)$ and from $\gamma_j(z)$, and at distance two from z. Hence, $\Gamma_{ij}(z)$ is the class containing u. By Lemma 5, $e_k + e_r \in C_i$, $e_k + e_s \in C_j$ and $e_k + e_r + e_s \in \Gamma_{ij}(z)$. Now, if we take another vector $x \in C_k$, let $u \in \mathcal{C}$ be such that $x = u \star e_k$. By Lemma 5, we have that $u \star (e_k + e_r) \in C_i$, $u \star (e_k + e_s) \in C_j$ and $u \star (e_k + e_r + e_s) \in \Gamma_{ij}(z)$. Consequently, $\gamma_i(x) = u \star (e_k + e_r)$, $\gamma_j(x) = u \star (e_k + e_s)$ and $\Gamma_{ij}(x)$ is the class containing $u \star (e_k + e_r + e_s)$, that is, $\Gamma_{ij}(x) = \Gamma_{ij}(z)$. ∎

Conversely, we will see that the class containing $\mathbf{0}$, in any 1-perfect uniform partition, has a propelinear structure.

Suppose that Ω is a 1-perfect partition. Let $\mathcal{C}$ be the code, i.e. the class containing $\mathbf{0}$, and let C_i be the class containing e_i, for all $i = 1, \ldots, n$. For every codeword $v \in \mathcal{C}$ and for every $i \in \{1, \ldots, n\}$, we define $v \star e_i$ as the only vector $x \in C_i$ such that $d(v, x) = 1$. Clearly, there exists a unique permutation π_v, such that $v \star e_i = v + \pi_v(e_i)$, for all $i = 1, \ldots, n$. Now, for any vector $u \in F^n$, we can define $v \star u = v + \pi_v(u)$. We shall prove that $(\mathcal{C}, \star)$ is a propelinear code if Ω is uniform.

Lemma 7 *Let Ω be a 1-perfect uniform partition and $\star$ as defined above. If $x \in C_l$, then for all $v \in C$ we have $v \star x \in C_l$.*

Proof. We proceed by induction on the weight of x.

If $\mathrm{wt}(x) = 0$ or $\mathrm{wt}(x) = 1$ the result is certainly satisfied.

If $\mathrm{wt}(x) = 2$ then $x = e_i + e_j$ for $i, j \in \{1, \ldots, n\}$, $i \neq j$. Since $e_i + e_j$ is in the class $\Gamma_{ij}(\mathbf{0})$, we have that $C_l = \Gamma_{ij}(\mathbf{0})$. Clearly, $v \star (e_i + e_j) \in \Gamma_{ij}(v)$. As Ω is uniform, we obtain

$$C_l = \Gamma_{ij}(\mathbf{0}) = \Gamma_{ij}(v) \Longrightarrow v \star x = v \star (e_i + e_j) \in C_l.$$

Now, we assume $\mathrm{wt}(x) > 2$. Then, there is a vector y such that $x = y+e_i+e_j$, where $i \neq j$ and $\mathrm{wt}(y) = \mathrm{wt}(x) - 2$. Let $p, q, r \in \{0, \ldots, n\}$ be such that $y \in C_p$, $y+e_i \in C_q$, and $y+e_j \in C_r$. Since $\mathrm{wt}(y), \mathrm{wt}(y+e_i), \mathrm{wt}(y+e_j) < \mathrm{wt}(x)$ we can apply the hypothesis of induction and obtain $v \star y \in C_p$, $v \star (y+e_i) \in C_q$ and $v \star (y + e_j) \in C_r$. Thus,

$$v \star x = v \star (y + e_i + e_j) \in \Gamma_{qr}(v \star y) = \Gamma_{qr}(y) = C_l.$$

∎

Lemma 8 *Let Ω be a 1-perfect uniform partition. Then, for all $u, v \in \mathcal{C}$, and $x \in F^n$, $u \star (v \star x) = (u \star v) \star x$.*

Proof. First of all, we remark that $u \star (v \star x)$ and $(u \star v) \star x$ belong to the same class in $\Omega(\mathcal{C})$, (the class of x).

If $x = e_i$, $(i \in \{1, \ldots, n\})$, then

$$u \star (v \star e_i) = u \star (v + \pi_v(e_i)) = u \star v + \pi_u \circ \pi_v(e_i)$$

and

$$(u \star v) \star e_i = u \star v + \pi_{u \star v}(e_i),$$

hence, $d(u \star (v \star x), (u \star v) \star x) \leq 2$. Since $u \star (v \star x)$ and $(u \star v) \star x$ belong to the same class and each class is a 1-perfect code then $d(u \star (v \star x), (u \star v) \star x) = 0$. Therefore, $(u \star v) \star e_i = u \star (v \star e_i)$ for all $i = 1, \ldots, n$

For $x \in F^n$ with $\mathrm{wt}(x) > 1$, we can write $x = \sum_{i=1}^{n} \lambda_i e_i$ (for some $\lambda_1, \ldots, \lambda_n \in \{0, 1\}$) and

$$\begin{aligned} (u \star v) \star x &= (u \star v) \star \sum_{i=1}^{n} \lambda_i e_i = \sum_{i=1}^{n} \lambda_i (u \star v) \star e_i \\ &= \sum_{i=1}^{n} \lambda_i u \star (v \star e_i) = u \star (v \star \sum_{i=1}^{n} \lambda_i e_i) = u \star (v \star x). \end{aligned}$$

∎

Proposition 9 *Let Ω be a 1-perfect uniform partition. Then, the code $\mathcal{C}$ has a propelinear structure and, moreover, $\Omega = \Omega(\mathcal{C})$.*

Proof. If Ω is a 1-perfect uniform partition, then for all $x \in F^n$ and for all $v \in \mathcal{C}$ we can define $v \star x$. From Lemma 7, $x \in C_i$ if and only if $v \star x \in C_i$ for every class $C_i \in \Omega$. Therefore, $v \star \mathcal{C} = \mathcal{C}$ for all $v \in \mathcal{C}$.

Now we must show that if $w = u \star v \in \mathcal{C}$, then $\pi_w = \pi_u \circ \pi_v$. But, from Lemma 8 and for all e_i, $i = 1, \ldots, n$, $w \star e_i = (u \star v) \star e_i = u \star (v \star e_i)$ and hence, $w + \pi_w(e_i) = u \star v + \pi_u \circ \pi_v(e_i) = w + \pi_u \circ \pi_v(e_i)$ for all $i = 1, \ldots, n$. Therefore π_w and $\pi_u \circ \pi_v$ are isometries of F^n coinciding over each e_i, $i = 1, \ldots, n$ and they must be equal.

For all $e_i \in F^n$ such that $\mathrm{wt}(e_i) = 1$, there exists a class $D \in \Omega$ such that $e_i \in D$. By Lemma 7, $\mathcal{C} \star e_i \subseteq D$ and, since $|\mathcal{C} \star e_i| = |\mathcal{C}| = |D|$, we have $\mathcal{C} \star e_i = D$ and $\Omega = \Omega(\mathcal{C})$. ∎

Propositions 6 and 9 show that there exists a correspondence between 1-perfect propelinear codes and 1-perfect uniform partitions:

Theorem 10 *Let Ω be a 1-perfect partition of F^n and let $\mathcal{C}$ be the class which contains the vector $\mathbf{0}$. $\mathcal{C}$ is a propelinear code with $\delta = 3$ and $\Omega = \Omega(\mathcal{C})$ if and only if Ω is a 1-perfect uniform partition.*

Note that if $\mathcal{C}$ is a Hamming code of length n, then it has a very simple propelinear structure (π_x is the identity for all codeword x) and hence $\{\mathcal{C} + e_i\}_{i=0}^n$ is a 1-perfect uniform partition. Conversely, if $\{\mathcal{C} + e_i\}_{i=0}^n$ is a 1-perfect uniform partition, then we define $\star$ as the addition and we obtain that $(\mathcal{C}, +)$ is a group, that is, a Hamming code.

4 1-Perfect Distance Invariant Uniform Partitions

Definition 11 *A 1-perfect partition $\Omega = \{C_0, C_1, \ldots, C_n\}$ is called* distance invariant *if for all $k \in \{0, 1, \ldots, n\}$ and for all $x, y \in C_k$, we have*

$$d(x, y) = d(\gamma_i(x), \gamma_i(y)) \quad \forall i = 0, \ldots, n \ \ (i \neq k).$$

Lemma 12 *Let Ω and Ω' be two equivalent 1-perfect partitions of F^n. Then, Ω is distance invariant if and only if Ω' is distance invariant.*

Proof. The result is straightforward because permutations and translations are distance-preserving. ∎

1-Perfect partitions generated by 1-perfect linear codes or by 1-perfect translation invariant propelinear codes have the important property that they are distance invariant, as we will see. We will prove that there also exists a correspondence between 1-perfect translation invariant propelinear codes and 1-perfect distance invariant uniform partitions.

Proposition 13 *Let $\mathcal{C}$ be a 1-perfect translation invariant propelinear code. Then, $\Omega(\mathcal{C})$ is a 1-perfect distance invariant uniform partition.*

Proof. $\Omega(\mathcal{C})$ is a 1-perfect uniform partition by Proposition 6. We need to show that it is distance invariant. Let $x, y \in C_i$ and $x', y' \in C_j$ at distance 1 apart from x and y, respectively. If C_i or C_j is equal to $\mathcal{C}$, then the assertion is obvious. Hence, we can assume that C_i and C_j are not equal to $\mathcal{C}$.

There exist $u, v \in \mathcal{C}$ such that $x = u \star e_i$ and $y = v \star e_i$ with $d(x, y) = d(u, v)$ since $\mathcal{C}$ is translation invariant. Moreover, $d(x', u) = d(y', v) = 2$. Then, there will be vectors e_r and e_s such that $x' = u \star (e_i + e_r)$ and $y' = v \star (e_i + e_s)$, by Lemma 5, $e_i + e_r, e_i + e_s \in C_j$. But

$$d(e_i + e_r, e_i + e_s) = \mathrm{wt}(e_r + e_s) < 3,$$

thus the only possibility is $r = s$. Therefore,

$$d(x', y') = d(u \star (e_i + e_r), v \star (e_i + e_r)) =$$

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

∎

We will see that this correspondence is reciprocal:

Proposition 14 *Let Ω be a 1-perfect distance invariant uniform partition. Then the class $\mathcal{C} \in \Omega$ which contains the vector $\mathbf{0}$ is a 1-perfect translation invariant propelinear code.*

Proof. By Theorem 10, we only need to see that $\mathcal{C}$ is a translation invariant code. Let $x \in F^n$. From (2), it suffices to show that, for all $v \in \mathcal{C}$, $\mathrm{wt}(v) = d(x, v \star x)$.

We use induction on $\mathrm{wt}(x)$. If $\mathrm{wt}(x) = 0$, the statement is clear. Assume that $\mathrm{wt}(x) > 0$ and that we know that the equation holds for all vectors of weight smaller than $\mathrm{wt}(x)$. Write $x = x' + e_i$ for any $i \in \mathit{supp}(x)$. Then $d(x, x') = 1$ and $d(v \star x, v \star x') = 1$. Since the partition is distance invariant,

$d(x, v\star x) = d(x', v\star x')$ and by the induction hypothesis $d(x', v\star x') = \mathrm{wt}(v)$, because $\mathrm{wt}(x') < \mathrm{wt}(x)$. ∎

From Theorem 10 and from Propositions 13 and 14, we obtain the next classification theorem:

Theorem 15 *Let Ω be a 1-perfect partition of F^n and let $\mathcal{C}$ be the class which contains the vector $\mathbf{0}$. $\mathcal{C}$ is a 1-perfect translation invariant propelinear code and $\Omega = \Omega(\mathcal{C})$ if and only if Ω is a 1-perfect distance invariant uniform partition.*

Theorems 10 and 15 characterize 1-perfect codes from 1-perfect partitions. The first one characterizes 1-perfect codes from 1-perfect uniform partitions. The second one characterizes 1-perfect codes from 1-perfect distance invariant uniform partitions.

As can be seen in [2], given a 1-perfect translation invariant propelinear code $\mathcal{C}$ of length $n > 7$, its translation invariant propelinear structure is unique. Thus, $\Omega(\mathcal{C})$ is the unique 1-perfect distance invariant uniform partition containing $\mathcal{C}$ as a class, up to equivalence.

5 1-Perfect Uniform Not Distance Invariant Partitions

The 1-perfect partitions $\Omega(\mathcal{C})$ obtained when $\mathcal{C}$ is a 1-perfect translation invariant propelinear code are always distance invariant partitions. In order to find an initial example of 1-perfect uniform but not distance invariant partition, we need to find a 1-perfect propelinear and not translation invariant code. In this section, we will prove that any Hamming code of length greater than 7 has a propelinear structure which is neither translation invariant, nor Abelian. We will also find a not translation invariant propelinear structure for any 1-perfect translation invariant propelinear code of length greater than 15.

First of all, we recall the well-known construction of Vasil'ev codes:

Theorem 16 *Let C_n be a 1-perfect code of length n. Define the code*

$$C_{2n+1} = \{(v \mid v + c \mid p(v) + f(c)) : v \in F^n, c \in C_n\},$$

where p is the binary parity map and f is any map from H_n to $\mathbb{Z}_2$, such that $f(\mathbf{0}) = 0$.

Then, C_{2n+1} is a 1-perfect code of length $2n+1$.

Proof. The interested reader can find the proof in [11]. ∎

We remark that if C_n is linear, then C_{2n+1} is linear if and only if f is a linear morphism.

If $(\mathcal{C}, \star)$ is a propelinear code, then a map $f : \mathcal{C} \longrightarrow \mathbb{Z}_2$ is a *propelinear morphism* if $f(x \star y) = f(x) + f(y)$, for all $x, y \in \mathcal{C}$.

Theorem 17 *Let C_n be a 1-perfect propelinear code of length n. Let p and f be as defined in Theorem 16, such that f is a propelinear morphism. Then, the code C_{2n+1} defined as*

$$C_{2n+1} = \{(v \mid v + c \mid p(v) + f(c)) : v \in F^n, c \in C_n\}$$

is a 1-perfect propelinear code.

Proof. Assign the permutation $\pi_x = (\pi_c \mid \pi_c \mid Id)$ to each codeword $x \in C_{2n+1}$, such that

$$x = (v \mid v + c \mid p(v) + f(c)); \text{ where } v \in F^n, c \in C_n.$$

Then, let

$$y = (u \mid u + d \mid p(u) + f(d)) \in C_{2n+1}, \quad (u \in F^n, d \in C_n).$$

First, we will show that $x \star y \in C_{2n+1}$.

$$\begin{aligned} x \star y &= (v \mid (v + c) \mid p(v) + f(c)) + (\pi_c(u) \mid \pi_c(u) + \pi_c(d) \mid p(u) + f(d)) \\ &= (v + \pi_c(u) \mid v + \pi_c(u) + c + \pi_c(d) \mid p(v) + p(u) + f(c) + f(d)) \\ &= (v + u' \mid v + u' + c \star d \mid p(v + u) + f(c \star d)), \end{aligned}$$

where $u' = \pi_c(u)$. Now, let $z = v + u' \in F^n$. Since $c \star d \in C_n$ we can write

$$x \star y = (z \mid z + w \mid p(z) + f(w)),$$

where $w = c \star d$. Since $z \in F^n$ and $w \in C_n$, we have that $x \star y \in C_{2n+1}$.

On the other hand, $\pi_{x \star y} = (\pi_w \mid \pi_w \mid Id)$. Since $\pi_w = \pi_{c \star d} = \pi_c \circ \pi_d$, we have that

$$\pi_{x \star y} = (\pi_c \circ \pi_d \mid \pi_c \circ \pi_d \mid Id) = \pi_x \circ \pi_y.$$

∎

Now, we start from $G_7 = H_7$ with the propelinear structure of type $(3, 2, 0)$. Define

$$G_{2n+1} = \{(v \mid v + c \mid p(v + c)) : v \in F^n, c \in G_n\},$$

where $n = 2^t - 1$, $t \geq 3$.

Theorem 18 *For all $n = 2^t - 1$ where $t \geq 3$, the code G_{2n+1} is a 1-perfect linear (Hamming) code of length $2n + 1$ and, moreover, G_{2n+1} has a propelinear structure that is neither Abelian, nor translation invariant.*

Proof. By Theorem 17, G_{2n+1} is a 1-perfect linear and propelinear code, since the binary parity map is a linear and propelinear morphism. A propelinear structure of G_{2n+1} can be obtained by assigning the permutation $\pi_x = (\pi_c \mid \pi_c \mid Id)$ to each $x \in G_{2n+1}$ such that

$$x = (v \mid v + c \mid p(v + c)); \text{ where } v \in F^n, c \in G_n.$$

In G_7, any π_w ($w \in G_7$) is a product of disjoint transpositions (see [9] or [2]). Then, π_c and π_x are also a product of disjoint transpositions. Hence π_x is an order 2 permutation for all $x \in G_{2n+1}$. Let $c \in G_n$ such that $\pi_c \neq Id$, and let $v = \mathbf{1}$ be the all-one vector. Define

$$x = (v \mid v + c \mid p(v + c)) \in G_{2n+1}.$$

Let (i, j) be a transposition factor of π_c ($i < j \leq n$). Now, let $u \in F^n$ such that $u_i \neq u_j$, and let

$$y = (u \mid u + c \mid p(u + c)) \in G_{2n+1}.$$

Put $z = x \star y$ and $z' = y \star x$. Then, it is easy to verify that $z_i \neq z'_i$ and $z_j \neq z'_j$. Thus $x \star y \neq y \star x$.

Now, consider $x \star e_i = x + e_j$. We have that

$$d(e_i, x \star e_i) = \mathrm{wt}(e_i + (x \star e_i)) = \mathrm{wt}(x + e_i + e_j) = \mathrm{wt}(x) - 2.$$

Since $d(e_i, x \star e_i) \neq \mathrm{wt}(x)$, we conclude that G_{2n+1} is not translation invariant, by (2). ∎

Note that for all $n = 2^t - 1$ ($t \geq 3$), the elements of G_n have order 2 or 4, since the associated permutations have order 2.

Corollary 19 $\Omega(G_n) = \{G_n \star e_i\}_{i=0}^n$ *is a 1-perfect uniform partition, which is not distance invariant and, hence, is not equivalent to the trivial partition.*

Proof. If $\Omega(G_n)$ is a 1-perfect partition, it must be uniform and not distance invariant by Theorems 10 and 15. Hence, it will not be equivalent to $\{G_n + e_i\}_{i=0}^n$, which is distance invariant. We have to show that $\Omega(G_n)$ is a 1-perfect partition.

Trivially, $\Omega(G_n)$ is a partition of F^n, where each class has the same number of vectors. Thus, we only need to prove that the minimum distance in every class is 3. Suppose that there exist $x, y \in G_n$ and e_i such that $d(x \star e_i, y \star e_i) < 3$, where $x \neq y$. Then, we have $d(e_i, x^{-1} \star y \star e_i) < 3$, i.e. we have a codeword $z = x^{-1} \star y$ such that $d(e_i, z \star e_i) = 1$ or $d(e_i, z \star e_i) = 2$.

In the first case, we would have $\mathrm{wt}(z) = 3$ and $\mathrm{wt}(z + \pi_z(e_i) + e_i) = 1$. In the second case, we would have $\mathrm{wt}(z) = 4$ and $\mathrm{wt}(z + \pi_z(e_i) + e_i) = 2$. In any case, we would have that $\pi_z(e_i) = e_j \neq e_i$, and $i, j \in supp(z)$.

Let $\nu = (n-1)/2$, then we know that

$$z = (v \mid v + c \mid p(v + c)) \text{ for some } v \in F^\nu \text{ and } c \in G_\nu.$$

We also know that $\pi_z = (\pi_c \mid \pi_c \mid Id)$. Since $\pi_z \neq Id$, we have that $\pi_c \neq Id$ and, hence, $c \neq \mathbf{0}$. Now, suppose that $supp(v)$ is not included in $supp(c)$. Let α and β be the pair of vectors such that $\alpha + \beta = v$ and $supp(\alpha) \cap supp(c) = \emptyset$, $supp(\beta) \subset supp(c)$.

Then, we have

$$\begin{aligned} \mathrm{wt}(z) &\geq \mathrm{wt}(v) + \mathrm{wt}(v + c) \\ &= \mathrm{wt}(\alpha) + \mathrm{wt}(\beta) + \mathrm{wt}(\alpha) + \mathrm{wt}(c) - \mathrm{wt}(\beta) \\ &= 2\mathrm{wt}(\alpha) + \mathrm{wt}(c) \geq \mathrm{wt}(c) + 2 \geq 5, \end{aligned}$$

which is a contradiction. Therefore, the support of v must be included in the support of c. Since $e_j = \pi_z(e_i)$ and $\pi_z = (\pi_c \mid \pi_c \mid Id)$ we have that either i and j or $i - \nu$ and $j - \nu$ are in the support of c. Let $(i', j') = (i, j)$ if $i, j \leq \nu$ and $(i', j') = (i - \nu, j - \nu)$ if $i, j > \nu$. Then (i', j') is a transposition factor of π_c. On the other hand,

$$\mathrm{wt}(c) = \mathrm{wt}(v) + \mathrm{wt}(v + c) \leq \mathrm{wt}(z) \leq 4.$$

The conclusion is that there is a codeword c of weight less than 5 in G_ν and there is a coordinate position i' such that i' and $\pi_c(i')$ are in the support of

c. Repeating this argument, we would have that one such codeword would also be in G_7. Hence, if we let $x \in G_7$ be such a codeword, we would have that $d(e_k, x \star e_k) \neq \mathrm{wt}(x)$ for some $k \leq 7$. This is not possible, however, since we started with the propelinear structure of type $(3, 2, 0)$ in G_7 and, thereby, G_7 is translation invariant. ∎

We can use the same construction to get 1-perfect uniform and not distance invariant partitions with nonlinear (but, obviously propelinear) codes. Let G_n be a 1-perfect translation invariant propelinear, but not linear, code of length $n \geq 15$. As before, define

$$G_{2n+1} = \{(v \mid v + c \mid p(v + c)) : v \in F^n, c \in G_n\}$$

and assign the permutation $\pi_x = (\pi_c \mid \pi_c \mid Id)$ to each $x \in G_{2n+1}$ such that

$$x = (v \mid v + c \mid p(v + c)); \text{ where } v \in F^n, c \in G_n.$$

It can be easily verified that G_{2n+1} has a not translation invariant propelinear structure by using the same arguments as in Theorem 18. Hence, by the arguments of the proof of Corollary 19, $\Omega(G_n)$ will be a 1-perfect uniform and not distance invariant partition for all $n = 2^t - 1$, where $t > 4$. We remark that, in this case, G_n is not a linear code:

Proposition 20 *With the above construction, G_n is not a linear code, for all $n = 2^t - 1$, where $t \geq 4$.*

Proof. We already know that G_{15} is not a linear code. Inductively, suppose that G_n is not a linear code, we want to prove that G_{2n+1} cannot be linear.

Let $c, d \in G_n$ such that $c + d \notin G_n$. Now, consider the codewords $x = (\mathbf{0} \mid c \mid p(c))$ and $y = (\mathbf{0} \mid d \mid p(d))$ in G_{2n+1}. Then,

$$x + y = (\mathbf{0} \mid c + d \mid p(c + d)),$$

which is not a codeword in G_{2n+1} because $c + d \notin G_n$. ∎

6 1-Perfect Distance Invariant Nonuniform Partitions

We have only eight examples of 1-perfect distance invariant nonuniform partitions. As can be seen in [6], there are 11 nonequivalent partitions of length

7, three of them are uniform partitions corresponding to the 3 different translation invariant propelinear structures (see [9] or [2]) of the Hamming code of length 7. However, all 11 partitions must be distance invariant:

Theorem 21 *Any 1-perfect partition of length 7 is distance invariant.*

Proof. Recall that any 1-perfect code of length 7 is equivalent to the Hamming code and the distance (or weight) distribution is $\{0, 3, 4, 7\}$. Let x and y be two vectors in the same class, and let x' and y' be two vectors in any other class such that $d(x, x') = d(y, y') = 1$. If $d(x, y) \neq d(x', y')$, then $d(x, y) = d(x', y') \pm 2$. However, this is not possible because $d(x, y), d(x', y') \in \{3, 4, 7\}$. ∎

Therefore, we have 8 1-perfect partitions of length 7 that are distance invariant and nonuniform.

7 Conclusions

Given a 1-perfect code $\mathcal{C}$ we can always construct several nonequivalent 1-perfect partitions containing $\mathcal{C}$ as a class (see [10]). The classes of these partitions can be obtained by means of translations or other techniques. If $\mathcal{C}$ is linear, then the translations always give the trivial partition. However, these Hamming codes always have a propelinear (nonlinear) structure which allows us to construct other 1-perfect partitions.

We have characterized the 1-perfect partitions obtained from propelinear codes, namely, 1-perfect uniform partitions, and vice versa. Also, we have shown the equivalence between 1-perfect distance invariant uniform partitions and 1-perfect translation invariant propelinear codes.

We have shown that any Hamming code of length $n \geq 15$ has a non-Abelian propelinear structure. The use of this algebraic structure allows to construct 1-perfect uniform but not distance invariant partitions.

Finally, we have found eight examples of 1-perfect distance invariant nonuniform partitions. All these examples are 1-perfect partitions of length 7. Thus, it remains an open question the existence of such partitions of length greater than 7.

Acknowledgment

The authors would like to thank Josep M. Arqués for his assistance with several computer verifications. We also thank the anonymous referees for their helpful comments and suggestions in an earlier version which have greatly improved the presentation and correctness of this paper.

References

[1] E.F. Assmus Jr. and J.D. Key: Designs and Codes. Cambridge Univ. Press, 1992.

[2] J. Borges and J. Rifà: A characterization of 1-perfect additive codes. IEEE Trans. Information Theory, **45**(5):1688-1697 (1999).

[3] T. Etzion and A. Vardy: On perfect codes and tilings: problems and solutions. SIAM J. Discrete Math., **11**:205-223 (1998).

[4] 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. on Information Theory, **40**:301-319 (1994).

[5] F.J. MacWilliams and N.J.A. Sloane: The Theory of Error-Correcting Codes. North-Holland Publishing Company, 1977.

[6] K.T. Phelps: An enumeration of 1-perfect binary codes of length 15. Australasian Journal of Combinatorics, **21**:287-298 (2000).

[7] J. Rifà: Well-ordered Steiner triple systems and 1-perfect partitions of the n-cube. SIAM J. Discrete Mathematics, **12**(1):35-47 (1999).

[8] J. Rifà, J.M. Basart and L. Huguet: On completely regular propelinear codes. In Proc. 6th International Conference, AAECC-6. 1989, number 357 in LNCS: 341-355, Springer-Verlag.

[9] J. Rifà and J. Pujol: Translation invariant propelinear codes. IEEE Trans. Information Theory, **43**:590-598 (1997).

[10] J. Rifà and A. Vardy: On partitions of space into perfect codes. III French-Israeli Workshop on Coding and Information Integrity. Ein Boqeq, Dead Sea, October 1997.

[11] J.L. Vasil'ev: On nongroup close-packed codes. Probl. Kibernet., **8**:375-378 (1962, in Russian).