Propelinear structure of $\mathbb{Z}_{2k}$-linear codes

J. Borges, C. Fernández-Córdoba and J. Rifà
Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain
(e-mail: \{jborges, cfernandez, jrifa\}@deic.uab.cat)

July 30, 2009

Abstract

Let $C$ be an additive subgroup of $\mathbb{Z}_{2k}^n$ for any $k \geq 1$. We define a Gray map $\Phi: \mathbb{Z}_{2k}^n \rightarrow \mathbb{Z}_2^{kn}$ such that $\Phi(C)$ is a binary propelinear code and, hence, a Hamming-compatible group code. Moreover, $\Phi$ is the unique Gray map such that $\Phi(C)$ is Hamming-compatible group code. Using this Gray map we discuss about the nonexistence of 1-perfect binary mixed group code.

1 Introduction

Since the famous paper [3] on $\mathbb{Z}_4$-linear codes, a large number of articles about $\mathbb{Z}_4$-linear and $\mathbb{Z}_k$-modulo codes have appeared. In more recent papers the Gray map, binary interpretation and concepts introduced in [3] have been generalized, as in [2] for example.

In [4], it is shown that linear and $\mathbb{Z}_4$-linear codes are subclasses of the more general class of translation invariant propelinear codes. In this paper we prove that any $\mathbb{Z}_{2k}$-modulo code is a binary propelinear code, but not translation invariant for $k > 2$.

The paper is organized as follows. In Section 2 we give the preliminary concepts on distance compatibility, propelinear codes and translation invariant propelinear codes. In Section 3 we show the correspondence between $\mathbb{Z}_{2k}$-modulo codes and binary propelinear codes. In section 4 we define mixed group codes and we generalize the above correspondence for these codes to study which of them can be perfect. Finally, in Section 5 we point out some remarks and conclusions.

2 Propelinear codes

Let $\mathbb{F}^n$ be the $n$-dimensional binary vector space. We denote by $0$ the all-zero vector. As usual, the (Hamming) distance between two vectors $x, y \in \mathbb{F}^n$ is the number of coordinates in which they differ and denoted by $d(x, y)$. The weight of a vector $x \in \mathbb{F}^n$ is the number of its nonzero entries $\text{wt}(x) = d(0, x)$.

The concept of (Hamming) distance-compatible operation in $\mathbb{F}^n$ is defined in [3] and [1]. If $*: \mathbb{F}^n \times \mathbb{F}^n \rightarrow \mathbb{F}^n$ is such an operation, then for all $v \in \mathbb{F}^n$ it should verify:
\( (i) \ d(v, v \ast e) = 1 \ \forall e \in \mathbb{F}^n \) with \( \text{wt}(e) = 1; \)

\( (ii) \ v \ast 0 = 0 \ast v = v; \)

\( (iii) \ v \ast e = w \ast e \) if and only if \( v = w, \) for all \( e \in \mathbb{F}^n \) with \( \text{wt}(e) = 1. \)

If \((\mathbb{F}^n, \ast)\) is a group, then the operation \( \ast \) is distance-compatible if and only if \( d(v, v \ast u) = \text{wt}(u) \) for all vectors \( u, v \in \mathbb{F}^n. \) The ‘if’ part is trivial and the ‘only if’ part is shown in [1, Proposition 14]. A binary code \( C \) of length \( n \) is a subset of \( \mathbb{F}^n. \) If this subset is a linear subspace of \( \mathbb{F}^n, \) then \( C \) will be a linear code.

We denote by \((C, \ast)\) a code in \( \mathbb{F}^n \) with a group structure defined by \( \ast. \) This operation could be nondefined in the whole space \( \mathbb{F}^n, \) but it could induce an action \( \ast : C \times \mathbb{F}^n \rightarrow \mathbb{F}^n. \)

**Definition 1** Let \((C, \ast)\) a code in \( \mathbb{F}^n \) and assume the operation \( \ast \) induces an action \( \ast : C \times \mathbb{F}^n \rightarrow \mathbb{F}^n. \) The action \( \ast \) is Hamming-compatible if \( d(x, x \ast v) = \text{wt}(v) \) for all \( x \in C \) and for all \( v \in \mathbb{F}^n. \)

**Definition 2** A binary code \((C, \ast)\) of length \( n \) is a Hamming-compatible group code if \((C, \ast)\) is a group and it is possible to extend \( \ast : C \times \mathbb{F}^n \rightarrow \mathbb{F}^n \) to a Hamming-compatible action.

Of course, given a code \( C \subset \mathbb{F}^n \) among all the different group structures, we are interested in those being Hamming-compatible (assuming we are working with the Hamming metric). A very general class of such codes are the propelinear ones, defined in [6]:

**Definition 3** Let \( S_n \) be the symmetric group of permutations on \( n \) elements. A (binary) code \( C \) of length \( n \) is said to be propelinear if for any codeword \( x \in C \) there is a coordinate permutation \( \pi_x \in S_n \) verifying the properties:

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

Now, we can define the binary operation \( \ast : C \times \mathbb{F}^n \rightarrow \mathbb{F}^n \) such that

\[ x \ast y = x + \pi_x(y) \ \forall x \in C \ \forall y \in \mathbb{F}^n. \]

This operation is clearly associative and closed in \( C. \) Since, for any codeword \( x \in C, \) \( x \ast y = x \ast z \) implies \( y = z, \) we have that \( x \ast y \in C \) if and only if \( y \in C. \) Thus, there must be a codeword \( e \) such that \( x \ast e = x. \) It follows that \( e = 0 \) is a codeword and, from 2, we deduce that \( \pi_0 \) is the identity permutation. Hence, \((C, \ast)\) is a group, which is not Abelian in general; \( 0 \) is the identity element in \( C \) and \( x^{-1} = \pi_x^{-1}(x), \) for all \( x \in C. \) Note that \( \Pi = \{ \pi_x \mid x \in C \} \) is a subgroup of \( S_n \) with the usual composition of permutations.

**Lemma 1** Let \((C, \ast)\) be a propelinear code, then

\[ d(x \ast u, x \ast v) = d(u, v) \ \forall x \in C \ \forall u, v \in \mathbb{F}^n. \]

**Proof:** The claim is trivial and can be found in [6] or [1]. \( \square \)
Lemma 2 A binary propelinear code is a Hamming-compatible group code.

Proof: Let $(C, \star)$ be such a code. We only have to prove that the action $\star : C \times F^n \to F^n$ is Hamming-compatible. But this is clearly true because for any $x \in C$ and any $v \in F^n$ we have
$$d(x, x \star v) = d(x \star 0, x \star v) = d(0, v) = wt(v)$$
applying Lemma 1. □

A propelinear code $(C, \star)$ is said to be a translation invariant code [4] if
$$d(x, y) = d(x \star u, y \star u) \quad \forall x, y \in C \quad \forall u \in F^n.$$ 

As can be seen in [4] the class of translation invariant propelinear codes includes linear and $Z_4$-linear codes. In fact, any translation invariant propelinear code of length $n$ can be viewed as a group isomorphic to a subgroup of $Z_{k_1}^\perp \oplus Z_{k_2}^\perp \oplus Q_{k_3}$; where $k_1 + 2k_2 + 4k_3 = n$ and $Q_8$ is the quaternion group on eight elements. Clearly, the class of propelinear codes is more general than the class of linear codes, being in this case $\pi_x = Id$ for any codeword. We can find other examples of propelinear structure, for instance, in [3] the are examples of $Z_4$-linear codes (Goethals, Preparata like,...) and in [4] we can find the propelinear structure of the standard Preparata code which is not $Z_4$-linear code.

3 $Z_{2k}$-codes as propelinear codes

There are different ways of giving a generalization of a Gray map. For instance, Carlet gives in [2] a generalization to $Z_{2k}$. In this paper we will give one preserving the basic property that the distance between the images of two consecutive elements is exactly one (see [3]).

Definition 4 The Lee weight of an element $x \in Z_k$, $w_L(x)$, is defined as the minimum absolute value of any representative of its class in $Z_k$. The Lee distance between $x, y \in Z_k$ is $d_L(x, y) = w_L(x - y)$. Clearly, $w_L(x) = d_L(x, 0)$.

Definition 5 A Gray map is an application $\varphi : Z_r \to Z_2^m$ such that

(i) $\varphi$ is one-to-one,

(ii) $d(\varphi(i), \varphi(i + 1)) = 1$, $\forall i \in Z_r$.

Lemma 3 Let $\varphi : Z_r \to Z_2^m$ a Gray map, then $r$ is even.

Proof: Let $\psi : Z_r \to Z_2$ defined as $\psi(i) = \text{wt}(\varphi(i)) \text{ mod } 2$. Clearly, we can write $\psi(i) = \psi(0) + i \text{ mod } 2$. By definition of Gray map we have $d(\varphi(r - 1), \varphi(0)) = 1$ but, if $r$ is odd, $\psi(r - 1) = \psi(0) + r - 1 = \psi(0) \text{ mod } 2$ which is a contradiction. □

Definition 6 Let $\varphi : Z_{2k} \to Z_2^m$ be a Gray map. $\varphi$ is distance-preserving if $d(\varphi(i), \varphi(j)) = d_L(i, j)$ and it is weight-preserving if $\text{wt}(\varphi(i)) = w_L(i)$. 


Definition 7 Let $\varphi : \mathbb{Z}_{2k} \rightarrow \mathbb{Z}_2^n$ a Gray map and let $+$ the usual operation in $\mathbb{Z}_{2k}$. We define the operation $\cdot$ in $\varphi(\mathbb{Z}_{2k})$ as:

$$\varphi(i) \cdot \varphi(j) = \varphi(i + j) \quad (1)$$

for all $i, j \in \mathbb{Z}_{2k}$.

Lemma 4 Let $\varphi : (\mathbb{Z}_{2k}, +) \rightarrow (\mathbb{Z}_2^n, \cdot)$ a Gray map such that $(\varphi(\mathbb{Z}_{2k}), \cdot)$ is a Hamming-compatible code. Then $\varphi$ is distance-preserving if and only if $\varphi$ is weight-preserving.

Proof: Clearly, if $\varphi$ is distance-preserving then is weight-preserving by definition of $\text{wt}$ and $w_L$.

Suppose $\varphi$ is weight-preserving, then

$$d(\varphi(i), \varphi(j)) = d(\varphi(i), \varphi(i) \varphi(j - i)) = \text{wt}(\varphi(j - i)) = w_L(j - i) = d_L(i, j)$$

$\square$

Lemma 5 Let $\varphi : \mathbb{Z}_{2k} \rightarrow \mathbb{Z}_2^n$ be a Gray map such that $(\varphi(\mathbb{Z}_{2k}), \cdot)$ is a Hamming-compatible code, then $\varphi(0) = 0$.

Proof: Let $a \in \mathbb{Z}_{2k}$. We know $(\varphi(\mathbb{Z}_{2k}), \cdot)$ is Hamming-compatible so,

$$0 = d(\varphi(a), \varphi(a + 0)) = d(\varphi(a), \varphi(a) \cdot \varphi(0)) = \text{wt}(\varphi(0))$$

Now, by definition of $\text{wt}()$, we have $\varphi(0) = 0$. $\square$

Theorem 1 Let $\varphi : \mathbb{Z}_{2k} \rightarrow \mathbb{Z}_2^n$ be a Gray map. If $(\varphi(\mathbb{Z}_{2k}), \cdot)$ is a Hamming-compatible code, then $\varphi$ is distance-preserving.

Proof: By the lemma, we only must proof that $\varphi$ is weight-preserving. Clearly, $\varphi(0) = 0$, $\varphi(1) = e_{i_1}$ and $\varphi(2) = e_{i_1} + e_{i_2}$ where $e_{i_1}, e_{i_2} \in \mathbb{Z}_2^n$ is the vector with 1 in the coordinate $i_1$ and 0 elsewhere. Let $j \in \mathbb{Z}_{2k}$ such that $\varphi(t) = e_{i_1} + \cdots + e_{i_t} \forall t \leq j$ and $\text{wt}(\varphi(j + 1)) = j - 1$ (j exists because $\varphi(2k - 1) = 1$).

If $j = k$ then $\text{wt}(\varphi(i)) = i = w_L(i) \forall i \leq k$ and $\text{wt}(\varphi(k + i)) = d(\varphi(k), \varphi(2k + i)) = d(\varphi(k), \varphi(i)) = d(\varphi(k), \varphi(k) \cdot \varphi(k - i)) = \text{wt}(\varphi(k - i)) = k - i = w_L(k + i) \forall i \leq k$. So, if $j = k$, the proof is finished.

Suppose $j < k$. There exists $r \geq 1$ such that $\text{wt}(\varphi(j + i)) = \text{wt}(\varphi(j + i - 1)) - 1 \forall i \leq r$ and $\text{wt}(\varphi(j + r + 1)) = \text{wt}(\varphi(j + r)) + 1$. As we know, $d(\varphi(i), \varphi(j + i)) = \text{wt}(\varphi(j)) = j$, therefore $\text{wt}(\varphi(j + i)) = j - i \forall i < r$. If $r = j$ then $\text{wt}(\varphi(j + r)) = 0$ which is not possible because of the one-to-one condition of the Gray map. Then $r < j$ and $\text{wt}(\varphi(j + r)) > 1$.

In the same way, there exists $s \geq 1$ such that $\text{wt}(\varphi(j + r + i)) = \text{wt}(\varphi(j + r + i - 1)) + 1 \forall i \leq s$ and $\text{wt}(\varphi(j + r + s + 1)) = \text{wt}(\varphi(j + r + s)) - 1$. As we know, $d(\varphi(i), \varphi(j + r + i)) = \text{wt}(\varphi(j)) = j - r$, therefore $\text{wt}(\varphi(j + r + i)) = \text{wt}(\varphi(j + r)) + i = j - r + i$. If $s = r$ then $\varphi(j + r + s) = \varphi(j)$ which is not possible, so $s < r$. 

4
We can use the same argument starting from \( j + r + s \) and we always obtain images in \( \mathbb{Z}_2^m \) with weights \( w \) such that \( 1 > w > j \). This is a contradiction with the fact that \( \text{wt}(\varphi(2k - 1)) = 1 \). □

Let \( C \) be a subgroup of \((\mathbb{Z}_2^k, +)\) for some \( k, n \geq 1 \), where + is the usual addition in \( \mathbb{Z}_2^k \) coordinatewisely extended. We say that \( C \) is a \( \mathbb{Z}_2^k \)-modulo code or, briefly, a \( \mathbb{Z}_2^k \)-code. We will see a binary representation of any such code as a propelinear code.

Let \( 0^{(i)} \) be the all-zero vector of length \( i \) and let \( 1^{(j)} \) be the all-one vector of length \( j \). We denote by \( | \) the concatenation, i.e. if \( x = (x_1, \ldots, x_r) \) and \( y = (y_1, \ldots, y_s) \), then \( (x | y) = (x_1, \ldots, x_r, y_1, \ldots, y_s) \).

Define the Gray map \( \varphi : \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2^k \) such that:

\[
(i) \quad \varphi(i) = (0^{(k-i)} | 1^{(i)}) \quad \forall i = 0, \ldots, k-1, \text{and}
(ii) \quad \varphi(i + k) = \varphi(i) + 1^{(k)} \quad \forall i = 0, \ldots, k-1. \tag{2}
\]

Define also the associated permutation on \( k \) coordinates

\[
\sigma_j = (1, k, k-1, \ldots, 2)^j \tag{3}
\]

(i.e. \( j \) left shifts) for all vector \( \varphi(j), j = 0, \ldots, 2k - 1 \).

Note that this Gray map \( \varphi \) is distance-preserving and weight-preserving.

**Definition 8** Let \( \varphi \) be the Gray map defined in (2). For any two elements \( \varphi(i), \varphi(j) \in \varphi(\mathbb{Z}_2^k) \) define the product

\[
\varphi(i) \cdot \varphi(j) = \varphi(i) + \sigma_i(\varphi(j)) \tag{4}
\]

We are going to prove that the above product is, in fact, the one defined in (1).

**Lemma 6** Let \( \varphi \) be the Gray map defined in (2). Let \( \varphi(i) \in \varphi(\mathbb{Z}_2^k) \) and the product defined in (4). Then

\[
\varphi(i) = \varphi(1)^i
\]

**Proof:** It is easy to verify that \( \varphi(i) = \varphi(i - 1) \cdot \varphi(1) = \varphi(1) \cdot \varphi(i - 1) \). Applying this repeatedly yields the result. □

**Proposition 1** \((\varphi(\mathbb{Z}_2^k), \cdot)\) is a group, with \( \varphi \) and \( \cdot \) defined in (2) and (4) respectively.

**Proof:** We have that

\[
(\varphi(i) \cdot \varphi(j)) \cdot \varphi(\ell) = (\varphi(1)^i \cdot \varphi(1)^j) \cdot \varphi(1)^\ell = \varphi(1)^{i+j+\ell} = \varphi(i) \cdot (\varphi(j) \cdot \varphi(\ell)),
\]

for all \( i, j, \ell \in \mathbb{Z}_2^k \). Therefore, the operation is associative.

It is clear that \( 0^{(k)} = \varphi(0) \) acts as the identity element. On the other hand, given \( \varphi(i) \in \varphi(\mathbb{Z}_2^k) \), we have that

\[
\varphi(i) \cdot \varphi(k - i) = \varphi(1)^{i+k-i} = \varphi(1)^k = \varphi(k) = \varphi(0) = 0^{(k)}.
\]

□
Corollary 1  Let $\phi$ defined in (2) and $\cdot$ the operation given in (4). The map $\phi : (\mathbb{Z}_{2k}, +) \rightarrow (\phi(\mathbb{Z}_{2k}), \cdot)$ is a group homomorphism and so the operation in (4) and (7) are the same.

Proof:  Given $i, j \in \mathbb{Z}_{2k}$, we have
\[
\phi(i + j) = \phi(1)^{i+j} = \phi(1)^i \cdot \phi(1)^j = \phi(i) \cdot \phi(j).
\]

\qed

Theorem 2 Let $\varphi : \mathbb{Z}_{2k} \rightarrow \mathbb{Z}_2^k$ be a Gray map. If $(\varphi(\mathbb{Z}_{2k}), \cdot)$ is a Hamming-compatible code where $\cdot$ is the operation defined in (4), then $\varphi$ is unique up to coordinate permutation.

Proof:  $(\varphi(\mathbb{Z}_{2k}), \cdot)$ is a Hamming-compatible code and, by Theorem 1, $\varphi$ has the following properties:

\begin{itemize}
  \item $\varphi(j) = e_{i_1} + \cdots + e_{i_j}$, for $j = 1, \ldots, k$.
  \item $\varphi(j + k) = 1^{(k)} + e_{i_1} + \cdots + e_{i_j}$, for $j = 1, \ldots, k$.
\end{itemize}

where $e_{i_1} \in \mathbb{Z}_2^k$ is the vector with 1 in the coordinate $i_1$ and 0 elsewhere.

For $j = 1, \ldots, k$, let $\mu_j$ be the transposition such that $\mu_j(e_{i_1}) = e_{i_{k-j+1}}$. Let $\mu$ be the permutation whose decomposition in product of transpositions is $\mu_1 \cdots \mu_k$.

Now it is easy to check that $\varphi = \mu \circ \varphi$, where $\varphi$ is the map defined in (2).

\qed

Remark:  If $\varphi : \mathbb{Z}_{2k} \rightarrow \mathbb{Z}_2^l$ is a Gray map, we have $l \geq k$ and, by the last theorem, if $l > k$ there are useless coordinates. Thus we can assume $l = k$.

Definition 9  We define the extended map $\Phi : \mathbb{Z}_{2k}^n \rightarrow \mathbb{Z}_2^{kn}$ such that $\Phi(j_1, \ldots, j_n) = (\phi(j_1), \ldots, \phi(j_n))$, where $\phi$ is defined in (2). Finally, we define the permutations $\pi_x = (\sigma_{j_1} \cdots | \sigma_{j_n})$, for $x = \Phi(j_1, \ldots, j_n)$, where $\sigma_i$ is defined in (3).

Next theorem will prove that given a $\mathbb{Z}_{2k}$-code of length $n$, there exists a propelinear code of length $kn$ such that both codes are isomorphic. The isomorphism between them extends the usual structure in $\mathbb{Z}_{2k}$ $(\cdot)$ to the propelinear structure in $\mathbb{Z}_2^k$.

Theorem 3  If $C$ is a $\mathbb{Z}_{2k}$-code, then $\Phi(C)$ is a propelinear code with associated permutation $\pi_x$ for all codeword $x \in \Phi(C)$.

Proof:  Let $x = \Phi(j_1, \ldots, j_n) = (\phi(j_1), \ldots, \phi(j_n))$ and $y = \Phi(i_1, \ldots, i_n) = (\phi(i_1), \ldots, \phi(i_n))$ be two codewords. Then,
\[
x + \pi_x(y) = (\phi(j_1) + \sigma_{j_1}(\phi(i_1)), \ldots, \phi(j_n) + \sigma_{j_n}(\phi(i_n)).
\]

For any coordinate, say $r$, we have that
\[
\phi(j_r) + \sigma_{j_r}(\phi(i_r)) = \phi(1)^{i_r} \phi(1)^{r} = \phi(1)^{i_r} = \phi(j_r + i_r).
\]

Thus,
\[
x + \pi_x(y) = (\phi(j_1 + i_1), \ldots, \phi(j_n + i_n)) = \Phi((j_1, \ldots, j_n) + (i_1, \ldots, i_n)).
\]
Therefore, it is clear that $x + \pi_x(y) \in \Phi(C)$.

On the other hand, the associated permutation of $\phi(j_r + i_r)$ is

$$\sigma_{j_r + i_r} = (1, k, k - 1, \ldots, 2)^{j_r + i_r} = \sigma_{j_r} \circ \sigma_{i_r},$$

hence, if $z = x + \pi_x(y)$, then $\pi_z = \pi_x \circ \pi_y$. \hfill \Box

**Corollary 2** The map $\Phi : (C, +) \rightarrow (\Phi(C), \star)$ is a group isomorphism, where $x \star y = x + \pi_x(y)$ for all $x, y \in \Phi(C)$.

**Proof:** As we have seen in the previous proof, $x \star y = \Phi(\Phi^{-1}(x) + \Phi^{-1}(y))$ and, clearly, $\Phi$ is bijective. \hfill \Box

In [4] it is shown that linear and $\mathbb{Z}_4$-linear codes are translation invariant. Now, we show that for $k > 2$ any $\mathbb{Z}_{2k}$-code, viewed as a binary propelinear code, is not translation invariant according to the classification given in [4].

**Proposition 2** If $k > 2$ and $C \in \mathbb{Z}_{2k}^n$, then $\Phi(C)$ is a propelinear but not translation invariant code.

**Proof:** Consider the vector $z = (1, 0, \ldots, 0, 1) \in \mathbb{F}^k$. Then it is easy to check that $d(0^k \star z, \phi(1) \star z) = 3 \neq d(0^k, \phi(1)) = 1$. \hfill \Box

We have seen that starting from a $\mathbb{Z}_{2k}$-code $C$, of length $n$, the code $\Phi(C)$ with $\Phi$ (see Definition 9) is a propelinear code of length $kn$ and both codes are isomorphic (Theorem 3). As we defined $\Phi$, the minimum Hamming distance in $\Phi(C)$ is exactly the minimum Lee distance in $C$ but it is at least the minimum Hamming distance in $C$.

Let $N$ be the number of codewords of $C$; clearly, it is also the codewords number of $\Phi(C)$. Let $R = \frac{\log_2 N}{n} = \frac{\log_2 N}{n \cdot \log_2 2k} = \frac{\log_2 N}{n(1 + \log_2 k)}$ be the information rate of $C$, and let $R'$ the information rate of $\Phi(C)$. We can express $R'$ as

$$R' = \frac{\log_2 N}{kn} = \frac{1 + \log_2 k}{k} R$$

therefore $R'$ is getting smaller than $R$ while the value of $k$ is raising; in fact, if $k \geq 3$ we obtain $R' < R$.

In this section we have seen that $\mathbb{Z}_{2k}$-codes can be represented as binary codes. We will use this representation in the next section to give some results about codes in $\mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$, where $\times$ denotes the direct product, and some necessary conditions to be 1-perfect codes.

### 4 Perfect propelinear codes

**Definition 10** A general mixed group code $C$ is an additive subgroup of $G_1 \times \cdots \times G_r$, where $G_1, \ldots, G_r$ are finite groups. We say that a binary code $C$ of length $n$ is a mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$ if $C = \Phi(C)$, where $i_1, \ldots, i_r$ are the minimum value such that $C$ is a subgroup of $\mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$, and $\sum_{j=1}^r i_j k_j = n$. We denote $C \leq \mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$. 

7
Remark: If $C \leq \mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$ then $C = C_1 \times \cdots \times C_r$, with $C_j \leq \mathbb{Z}_{2i_j}^{k_j}$. We can write $\Phi(C)$ as $(\Phi_1(C_1), \cdots, \Phi_r(C_r))$ with $\Phi_j : \mathbb{Z}_{2i_j}^{k_j} \rightarrow \mathbb{Z}_2^{i_j k_j}$ as in Definition [9]. We will denote $x \in \mathcal{C}$ as $(x_1 \cdots x_r)$ where $x_j \in \Phi_j(C_j)$. □

Theorem 4 Let $\mathcal{C}$ be a binary mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$ and length $n$. If $\mathcal{C}$ is 1-perfect, then $\mathcal{C}$ is of type $(\mathbb{Z}_2^k, \mathbb{Z}_4^{(n-k)/2})$ for some $k \in \mathbb{N}$.

Proof: Let $\mathcal{C}$ be a binary mixed group code of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$. Suppose there exists $j \in \{1, \ldots, r\}$ such that $i_j > 2$. Without loss of generality we will assume $j = 1$ and $k_1 = 1$.

Let $x = (10 \cdots 01|0 \cdots 0| \cdots |0 \cdots 0) \in \mathbb{F}^n$. If $\mathcal{C}$ is 1-perfect, then there exists $y \in \mathcal{C}$ such that $d(x, \Phi(y)) \leq 1$. As the minimum weight in $\mathcal{C}$ is 3 and the distance of $x$ must be at most 1, the only possibility is $i_1 = 3$ and $\Phi(y) = (111|0 \cdots 0| \cdots |0 \cdots 0)$, therefore $\mathcal{C} = G_1 \times \cdots \times G_r$ where $G_1$ is a subgroup of $\mathbb{Z}_6$ and $3 \in G_1$. The only subgroups of $\mathbb{Z}_6$ that contain 3 are $\{0, 3\}$ and $\mathbb{Z}_6$. We assume $G_1 = \mathbb{Z}_6$; otherwise, $G_1 = \{0, 3\}$ would be isomorphic to $\mathbb{Z}_2$. Let $u = (101100 \cdots 0)$, $v = (101010 \cdots 0) \in \mathbb{F}^n$ (where customary commas have been deleted); $u, v \notin \mathcal{C}$. The only codewords at distance 1 of $u$ and $v$ are, respectively, $(111100 \cdots 0)$ and $(110110 \cdots 0)$ but the distance betwen them is 2 which is not possible if $\mathcal{C}$ is 1-perfect. □

1-perfect binary mixed codes of type $(\mathbb{Z}_2^k, \mathbb{Z}_4^{(n-k)/2})$ are called 1-perfect additive codes and they are studied in [1].

5 Conclusions

It is well known the usual Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^3$ (see [2], [3] and [7]) but there are different ways of giving a generalization from $\mathbb{Z}_r$ to $\mathbb{Z}_2^m$. The generalization given in this paper has the property to be distance-preserving, considering the Lee distance in $\mathbb{Z}_r$ and the Hamming distance in $\mathbb{Z}_2^m$. However there could be other kind of generalizations, perhaps the most important to be considered are those where the distance in $\mathbb{Z}_r$ is different to the Lee distance or, merely, where the distance between 0 and $r-1$ is not 1.

Let $\phi : \mathbb{Z}_r \rightarrow \mathbb{Z}_2^m$ be the Gray map, and let $(\phi(\mathbb{Z}_r), \cdot)$ (defined in [11]) be a Hamming-compatible code. We know that $r$ is even ($r = 2k$) and, without useless coordinates, $m$ is exactly $k$. We have proved that such a Gray map is, in fact, unique up to coordinate permutation and we have used this to give some results on $\mathbb{Z}_{2k}$-codes.

Given a $\mathbb{Z}_{2k}$-code of length $n$, there exists a binary propelinear code of length $kn$ such that both codes are isomorphic. In this way codes in $\mathbb{Z}_{2i_1}^{k_1} \times \cdots \times \mathbb{Z}_{2i_r}^{k_r}$ (or mixed groups of type $(\mathbb{Z}_{2i_1}^{k_1}, \ldots, \mathbb{Z}_{2i_r}^{k_r})$) could be represented as binary codes. Finally we have seen that if such a code is 1-perfect then, necessarily, it is a code of type $(\mathbb{Z}_2^k, \mathbb{Z}_4^{k})$.

As we have seen at the end of the Section 3, the representation of a $\mathbb{Z}_{2k}$-code as a binary code is not efficient enough because the information rate which is $R$ in the first code, become $\frac{1 + \log_2 k}{k} R$ in the second one, that is lower. From this point of view, as we have seen that the representation of a $\mathbb{Z}_{2k}$-code is unique,
we should look for other alternatives, apart from Gray maps, to represent a $\mathbb{Z}_{2^k}$-code as a binary code.

References

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

[2] C. Carlet, “$\mathbb{Z}_{2^k}$-Linear codes,” *IEEE Trans. on Information Theory*, vol. 44, pp. 1543-1547, 1998.

[3] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, “The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes,” *IEEE Trans. on Information Theory*, vol. 40, pp. 301-319, 1994.

[4] J. Pujol and J. Rifà, “Translation invariant propelinear codes,” *IEEE Trans. Information Theory*, vol. 43, pp. 590-598, 1997.

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

[6] 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, pp. 341-355, Springer-Verlag.

[7] Zhe-Xiam Wan, “Quaternary Codes,” World Scientific, 1997.