

On the Automorphism Group of Distinct Weight Codes

Abdelfattah Haily, Driss Harzalla

Department of Mathematics, Faculty of Sciences, University Chouaib Doukkali, El Jadida, Morocco Email: <u>afhaily@yahoo.fr</u>, <u>drissHarzalla@yahoo.ca</u>

Received 15 January 2015; accepted 24 March 2015; published 25 March 2015

Copyright © 2015 by authors and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CC BY). http://creativecommons.org/licenses/by/4.0/

Abstract

In this work, we study binary linear distinct weight codes (DW-code). We give a complete classification of $[n,k]_2$ -DW-codes and enumerate their equivalence classes in terms of the number of solutions of specific Diophantine Equations. We use the Q-extension program to provide examples.

Keywords

Distinct (Constante) Weigth Code, Automorphism Group, Extension Theorem of MacWilliams, Diophantine Equations

1. Preliminaries

One of the main objective of algebraic coding theory is to classify codes up to equivalence by using a list of invariants. The present work is following this way. We study here a class of linear binary codes whose all codewords have distinct weight and will give a classification theorems. Throughout this work all codes are linear binary codes. We call an $[n,k]_2$ -binary code every k dimensional subspace C of \mathbb{F}_2^n . Recall also that the Hamming weight wt(x) of vector x is defined to be the number of nonzero components of x. The minimum of weights where $x \neq 0$ is the minimal distance d of the code.

A Hamming isometry of \mathbb{F}_2^n is a linear application $\sigma: \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $wt(\sigma(x)) = wt(x)$, for every $x \in \mathbb{F}_2^n$. It is well known that in binary case, the isometries are merely the permutations of the coordinates, that is the elements of S_n , the permutation group of $\{1, 2, \dots, n\}$.

Two codes C and C' are said to be equivalent if there exists an isometry σ of \mathbb{F}_2^n such that $\sigma(C) = C'$. An automorphism of C is a Hamming isometry σ such that $\sigma(C) = C$. The automorphisms of C form a subgroup of S_n called the automorphism group of C and we denote it by $\operatorname{Aut}(C)$. Note also that the vector space \mathbb{F}_2^n can be endowed with a product $(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = (x_1y_1, \dots, x_ny_n)$, so that $(\mathbb{F}_2^n, +, \cdot)$ becomes a Boolean ring. Furthermore, wt(x+y) = wt(x) + wt(y) - 2wt(xy), for every $x, y \in \mathbb{F}_2^n$. The code C is said a constant-weight code (CW-code) if all nonzero codewords have the same weight. The dual of binary Hamming codes $H_2(m)$ are simplex codes Σ_m of parameters $[2^m - 1, m]_2$. simplex codes Σ_m are constant weight code (CW-code).

Any permutation of the columns of a k by n binary matrix G which maps the rows of G into rows of the same matrix, is called an automorphism of the binary matrix G [1]. The set of all automorphisms of G is a subgroup of the symmetric group S_n and we denote it by Aut(G). More treatment of linear codes can be found in the book [2].

Ideally, we would like the rate $R = \frac{k}{n}$ to be high, in order to be able to send a large number of errors. The

rate of a DW-code approch zero very quickly when the code length increase: $\frac{k}{n} \le \frac{1}{n} \left[\frac{\ln(n+1)}{\ln(2)} \right] \ge 0$ as shown

in **Figure 1** where $R = \frac{k}{n}$ and $r(k) = \frac{k}{2^k - 1}$, so $R \le r(k)$.

It is more convenient to use the DW-codes in the construction of other codes by using some technic of construction and not to use it alone.

2. Distinct Weight Codes

Definition 1 A linear binary code C of length n is said to be a Distinct Weight Code, (in short: DW-code), if the weight mapping: wt: $C \rightarrow \{0, 1, \dots, n\}$, is one to one, that is x = y whenever wt(x) = wt(y), $\forall x, y \in C$.

The simplest example of such codes are the repetition codes. Later we shall give more nontrivial examples. Let C a DW-code of length n and dimension k. Since the number of element of C is 2^k , then we have $2^k \le n+1$. In the sequel we fix our interest to the extreme case $2^k = n+1$, in which we give a construction.

Proposition 2 Let k such that $2^k \le n+1$. Then every family $u_1, \dots, u_k \in \mathbb{F}_2^n$ of words such that $wt(u_r) = 2^{r-1}$ is linearly independent.

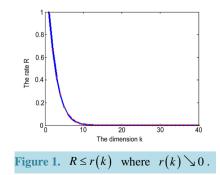
Proof. Suppose on the contrary that u_1, \dots, u_k are not linearly independent, then we have a linear combination $\sum_{i=1}^{k} \alpha_i u_i = 0$, where some α_i is nonzero. Let r be the maximal integer such that $\alpha_r \neq 0$. Then $\alpha_r = 1$, and $u_r = \sum_{i=1}^{r-1} \alpha_i u_i$. Now taking the weights leads to:

$$2^{r-1} = wt(u_r) \le \sum_{i=1}^{r-1} wt(\alpha_i u_i) \le \sum_{i=1}^{r-1} 2^{i-1} = 2^{r-1} - 1$$

a contradiction. \Box

Now we give a construction of a $\begin{bmatrix} 2^k - 1, k \end{bmatrix}$ DW-code.

Let k be a nonzero integer and $n = 2^k - 1$. Take (e_1, \dots, e_n) the canonical basis of \mathbb{F}_2^n . Put $c_r = \sum_{i=2^{r-1}}^{2^r-1} e_i$, then clearly $wt(c_r) = 2^{r-1}$. By the proposition 2, the code-words c_1, c_1, \dots, c_k are linearly independent and generate a [n, k] linear code that we denotes by $\mathcal{D}(k)$. It also seen that $c_i c_i = 0$, whenever $i \neq j$. This



implies that $wt\left(\sum_{i=1}^{k}\alpha_{i}c_{i}\right) = \sum_{i=1}^{k}wt\left(\alpha_{i}c_{i}\right) = \sum_{i=1}^{k}\alpha_{i}2^{i-1}$.

A generator matrix of $\mathcal{D}(k)$ looks like:

	(1	0	0	0	0	0	0	0	0	0	•••	0	0)
	0	1	1	0	0	0	0	0	0	0		0	0
$G_k =$	0	0	0	1	1	1	1	0	0	0		0	0
	÷	÷	÷	÷	÷	÷	÷	÷	÷	÷	÷	÷	:
$G_k =$	0	0	0	0	0	0	0	0	0	1		1	1)

Proposition 3 The $[2^k - 1, k]$ -code $\mathcal{D}(k)$ is a DW-code.

Proof. Since the cardinal of $\mathcal{D}(k)$ is $2^k = n+1$, it suffices to show that wt: $\mathcal{D}(k) \to \{0, 1, \dots, n\}$ is onto. Let $r \in \{0, 1, \dots, n\}$, then r can be written $r = \sum_{i=1}^k \alpha_i 2^{i-1}$ in the base 2, where $\alpha_i \in \{0, 1\}$. Set $x = \sum_{i=1}^k \alpha_i c_i$, then $wt(x) = \sum_{i=1}^k \alpha_i 2^{i-1} = r$. \Box

Up an equivalence we have the following result:

Theorem 4 There exists only one distinct weight $[2^k - 1, k]$ -code, moreover such code is Boolean subring of $(\mathbb{F}_2^n, +, \cdot)$.

Proof. Let C be such a code and take code-words u_1, u_2, \dots, u_k , each u_i has weight 2^{i-1} . These are linearly independent and form a basis of C. Next we show that $u_s u_r = 0$, $\forall s < r$. Otherwise, there exists a least integer r such that $u_s u_r \neq 0$ for some s < r. Since $wt(u_s u_r) \leq wt(u_s)$, one have $u_s u_r = \sum_{i=1}^{r-1} \alpha_i u_i$. Multiplying by u_s yields $u_s u_r = u_s$. Now consider the word $c = u_r + u_s$,

 $wt(c) = wt(u_r) + wt(u_s) - 2wt(u_su_r) = wt(u_r) + wt(u_s) - 2wt(u_s) = 2^{r-1} - 2^{s-1}$ On the other hand, if we consider $h = u_s + u_{s+1} + \dots + u_{r-1}$, then $wt(h) = \sum_{i=s-1}^{r-2} 2^i = 2^{r-1} - 2^{s-1}$. Thus $u_s + u_{s+1} + \dots + u_{r-1} = u_r + u_s$ hence $u_{s+1} + \dots + u_{r-1} + u_r = 0$ a contradition. This means that $u_ru_s = 0$, if $r \neq s$. Since $u_r^2 = u_r$, and u_1, \dots, u_k is a basis of C, then C is a Boolean ring.

Now we define a linear mapping $f: \mathcal{C} \to \mathcal{D}(k)$ by $f(u_i) = c_i$. Then, $f\left(\sum_{i=1}^k \alpha_i u_i\right) = \sum_{i=1}^k \alpha_i c_i$. If $x = \sum_{i=1}^k \alpha_i u_i$, then $wt(f(x)) = wt\left(f\left(\sum_{i=1}^k \alpha_i u_i\right)\right) = wt\left(\sum_{i=1}^k \alpha_i c_i\right) = \sum_{i=1}^k \alpha_i 2^{i-1} = wt(x)$. This implies that f is an isometry between \mathcal{C} and $\mathcal{D}(k)$, and by the extension theorem of MacWilliams, see [3] or [4], there exists a permutation $\sigma \in S_n$, such that $\sigma(\mathcal{C}) = \mathcal{D}(k)$. \Box

Example 5 k = 3 and n = 7 $(2^3 - 1 = 7)$

By using the software Q-extension, see [5] we show, up to equivallence, that among six equivallence classes (0000100)

the unique DW-code C_3 of parametters $\begin{bmatrix} 7,3,1 \end{bmatrix}_2$ is the code of generator matrix $G_3 = \begin{bmatrix} 1110010\\0001001 \end{bmatrix}$. It is clear

that it is equivalent to the code $\mathcal{D}(3)$ of generator matrix $G'_3 = \begin{pmatrix} 1000000\\0110000\\0001111 \end{pmatrix}$. Just swap the second and third

rows and then apply the permutation $\sigma = (1,5)(2,4)(3,7)$.

Theorem 6 Let $2^k = n+1$, Diophantine equations $n = t_1 + t_2 + \dots + t_k$ for which

 $\begin{array}{ll} (1) & t_1 < t_2 < t_3 < \cdots < t_k \\ (2) & t_i \neq \sum_{j \in \left(I \setminus \{i\}\right)} \varepsilon_j t_j \ , \ \forall i = 1, 2, \cdots, k \ , \ \forall I \subseteq \left\{1, 2, \cdots, k\right\}, \ \forall \varepsilon_j = \pm 1 \ , \end{array}$

have a unique solution which is the *k*-uplet $(t_1, t_2, \dots, t_k) = (1, 2, 2^2, 2^3, \dots, 2^{k-1})$.

Proof. $(1, 2, 2^2, 2^3, \dots, 2^{k-1})$ is clearly a solution of the Diophantine equation which satisfies the conditions (1). Assume that $2^i = \sum_{j \in \{I \setminus \{i\}\}} \varepsilon_j 2^j$ for some *i* and *I*, then $2^i + \sum_{i \in K^-} 2^j = \sum_{i \in K^+} 2^j$ (< $2^k - 1$) where $K^+ = \{j \in I \setminus \{i\} / \varepsilon_j = 1\}$ and $K^- = \{j \in I \setminus \{i\} / \varepsilon_j = -1\}$. We can assume without loss of generality that $\{2^j / j \in K^+\} \cap \{2^j / j \in K^-\} = \emptyset$. So by the uniqueness of Development of any integer less than or equal $2^k - 1$ in binary basis, the equality $2^i + \sum_{i \in K^-} 2^j = \sum_{i \in K^+} 2^j$ leads to a contradiction. So the solution $(1, 2, 2^2, 2^3, \dots, 2^{k-1})$ satisfies the conditions (2).

Conversely, Let (t_1, t_2, \dots, t_k) a solution of the equation $n = t_1 + t_2 + \dots + t_k$ satisfying (1)-(2). We can take d_i , $i = 1, 2, \dots, k$ elements of F_2^n such that $wt(d_i) = t_i$ and $d_1 = \left(\underbrace{1 \dots 1}_{t_1} 0 \dots 0\right)$,

$$d_2 = \left(\underbrace{0\cdots 0}_{i_1}\underbrace{1\cdots 1}_{i_2}\underbrace{0\cdots 0}_{i_2}\right), \quad \cdots, \quad d_k = \left(\underbrace{0\cdots 0}_{i_1}\underbrace{0\cdots 0}_{i_2}\underbrace{0\cdots 0}_{i_2}\underbrace{1\cdots 1}_{i_k}\right), \quad d_i, \quad i = 1, 2, \cdots, k \text{ are linearly independent. The}$$

condition (2) means that the code of generator matrix $G = \begin{pmatrix} a_1 \\ \vdots \\ d_k \end{pmatrix}$ is a dw-code. On after Theorem 1.3, the

condition (1) implies that there exists an invertible k by k matrix $A = (a_{i,j})_{i,j}$ and a permutation matrix

is the generator matrix of the code $\mathcal{D}(k)$. It is clear that G is of the form:

where $a_{i,j} = 0$ or 1, $\forall i, j$ and $\forall j = 1, 2, 3, \dots, k$ we have $t_j = \sum_{i=1}^{i=k} 2^{i-1} a_{j,\sigma(i)}$. So we have

 $2^{k} - 1 = \sum_{j=1}^{j=k} t_{j} = \sum_{j=1}^{j=k} \left(\sum_{i=1}^{i=k} 2^{i-1} a_{j,\sigma(i)} \right) = \sum_{i=1}^{i=k} 2^{i-1} \left(\sum_{j=1}^{j=k} a_{j,\sigma(i)} \right), \text{ and then we have } \sum_{j=1}^{j=k} a_{j,\sigma(i)} = 1, \forall i = 1, 2, \dots, k \text{ by the uniqueness of development of } 2^{k} - 1 \text{ in binary basis. By (1) we have}$

$$\sum_{i=1}^{i=k} 2^{i-1} a_{1,\sigma(i)} < \sum_{i=1}^{i=k} 2^{i-1} a_{2,\sigma(i)} < \dots < \sum_{i=1}^{i=k} 2^{i-1} a_{k,\sigma(i)}, \text{ then we have: } \forall i, j, a_{i,\sigma(j)} = \delta_i^j \quad (\text{Kronecker symbol}).$$
Since $t_j = \sum_{i=1}^{i=k} 2^{i-1} a_{j,\sigma(i)}, \text{ we have } \forall j = 1, 2, \dots, k$, $t_j = 2^{j-1}$ and finally we have $(t_1, t_2, t_3, \dots, t_k) = (1, 2, 2^2, 2^3, \dots, 2^{k-1}).$

Remark 7 Without the conditions (1) and (2), Diophantine equations have $C_{2^{k-2}}^{k-1}$ different solutions. For all

 $k \ge 3$ note that there is no DW-self-dual code. Indeed, if not, we will have $2^k - 1 \le n = 2k$, wich is impossible.

3. Classification and Automorphism Group of DW-Codes

3.1. Automorphism Group: The General Case

We consider, without loss of generality, that a generator matrix of a DW-code has no zero columns. Indeed, if this is the case, the zero columns are omitted and we consider the obtained DW-code. This assumption is made in the entier paper. We study the automorphism group of DW-codes. We first notice the following:

Proposition 8 Let (u_1, u_2, \dots, u_k) any basis of an [n, k] DW-code. Then

Aut $(\mathcal{C}) = \{ \sigma \in \mathcal{S}_n | \sigma(u_i) = u_i, \forall i = 1, \cdots, k \}.$

Moreover, if G any generator matrix of C, then σ is an automorphism of C, if and only if, σ is an automorphism of the binary matrix G.

Proof. Clear.

Proposition 9 The automorphism group of any DW-code is nontrivial of even order.

Proof. Let G be a generator matrix of a DW [n,k]-code C. We may suppose that all columns of G are nonzero. The n columns of G are taken among a set of $2^k - 1$ columns. Suppose that all columns of G are distincts, since $n \ge 2^k - 1$, then the columns of G are the $n = 2^k - 1$ distinct nonzero vectors of \mathbb{F}_2^k and C will be the simplex code, which is clearly not DW. This contradiction shows that at least 2 columns of G are identical. Now the transposition of these two columns gives an automorphism of C. \Box

We deduce that the dual code C^{\perp} of a DW-code has a non-trivial automorphism group and has minimum distance $d^{\perp} = 2$.

We consider the general case $2^k < n+1$. The action of automorphism group $\operatorname{Aut}(\mathcal{C})$ on the set $\Omega = \{c_1, c_2, \dots, c_n\}$ of columns of a generator matrix G defined by: $\sigma(c_i) = c_{\sigma(i)}$ for all σ in $\operatorname{Aut}(\mathcal{C})$ and c_i in Ω , splits all the columns of G into disjoint orbits. The orbits O_1, O_2, \dots, O_f each formed of a single column, they are the columns fixed by the group $\operatorname{Aut}(\mathcal{C})$. We set f = 0 if no orbit is formed of a single column and then it is clear that $0 \le f < 2^k - 1$ since since $\operatorname{Aut}(\mathcal{C})$ can not be trivial. The $r(\ge 1)$ other orbits are $O_{i_1}, O_{i_2}, \dots, O_{i_r}, |O_{i_i}| \ge 2, i = 1, 2, \dots, r$. We set $O_i = \{c_i\}, i = 1, 2, \dots, f$ if $f \ge 1$ and

 $O_{t_i} = \left\{ c_i^{(1)}, c_i^{(2)}, \cdots, c_i^{(t_i)} \right\}, \quad i = 1, 2, \cdots, r \text{ , therefore, we have precisely } 0 \le f \le 2^k - 1 - r \text{ .}$

Up to equivalence, we can consider that the code C is of generator matrix

$$G = \left(\underbrace{c_1^{(1)}, c_1^{(2)}, \cdots, c_1^{(t_1)}}_{O_{t_1}}, \cdots, \underbrace{c_r^{(1)}, c_r^{(2)}, \cdots, c_r^{(t_r)}}_{O_{t_r}}, \underbrace{c_1}_{O_1}, \underbrace{c_2}_{O_2}, \cdots, \underbrace{c_f}_{O_f}\right) = \begin{pmatrix}d_1\\ \vdots\\ d_k\end{pmatrix}$$

 $d_j = \left(d_j^{(i)}\right)_i \text{ rows of } G \text{ , such that } 2 \le t_1 \le t_2 \le \cdots \le t_r.$

Since C is a DW-code, then for each $j = 1, 2, \dots, k$ for each $\sigma \in \operatorname{Aut}(C)$ we have $\sigma(d_j) = d_j$ $\forall j = 1, 2, \dots, k$. So $\forall i = 1, 2, \dots, n$ we have $d_j^{(\sigma(i))} = d_j^{(i)}$. We therefore deduce that: $\forall i = 1, 2, \dots, r$, $c_i^{(1)} = c_i^{(2)} = \dots = c_i^{(t_i)}$. So each orbit O_{t_i} consists of $t_i \ge 2$ equal columns.

The following theorem legitimate the idea of giving a definition to the 3-tuple

 $(f, k, (t_1, t_2, \dots, t_r))$ which we call signature of the DW-code and we denote $\operatorname{sign}(\mathcal{C}) = (f, k, (t_1, t_2, \dots, t_r))$. We give here the full classification of such a code in several cases.

Theorem 10 If two DW-codes C and C' are equivalent then they have the same signatures: sign(C) = sign(C').

Proof. Let \mathcal{C} and \mathcal{C}' two equivalent DW-codes of parameters [n,k]. So $\exists \sigma \in S_n$ such as $\sigma(\mathcal{C}) = \mathcal{C}'$.

We have $\operatorname{Aut}(\mathcal{C}') = \sigma \operatorname{Aut}(\mathcal{C}) \sigma^{-1}$. Let G be a generator matrix of the code \mathcal{C} . Under the action of the automorphism group $\operatorname{Aut}(\mathcal{C})$ we can assume that G is of the form $G = (O_{t_1}, \dots, O_{t_r}, O_1, O_2, \dots, O_f)$ where $O_{t_i} = \{c_{s_{i-1}+1}, \dots, c_{s_i}\}, \quad s_i = \sum_{j=1}^{j=i} t_j \quad \forall i = 1, 2, \dots, t_r \text{ and } O_i = \{c_{s_r+i}\} \quad \forall i = 1, 2, \dots, f$.

So we have $O_{t_i} = \left\{ c_{s_{i-1}+1}, \cdots, c_{s_i} \right\} = \left\{ c_{\sigma(s_i)} / \sigma \in \operatorname{Aut}(\mathcal{C}) \right\} = \left\{ c_{\sigma^{-1}\rho\sigma(s_i)} / \rho \in \operatorname{Aut}(\mathcal{C}') \right\}$ and then

 $\sigma(O_{t_i}) = \left\{ c_{\rho\sigma(s_i)} \middle/ \rho \in \operatorname{Aut}(\mathcal{C}') \right\} = O'_{t_i} \text{ which is an orbit of the column } c_{\sigma(s_i)} \text{ under the action of } \operatorname{Aut}(\mathcal{C}') \text{ on the generator matrix } G' = \sigma(G) \text{ of the code } \mathcal{C}'. \text{ similarly we have } \sigma(O_i) = \left\{ c_{\rho\sigma(s_r+i)} \middle/ \rho \in \operatorname{Aut}(\mathcal{C}') \right\} = O'_i \text{ which is an orbit of the column } c_{\sigma(s_r+i)} \text{ under the action of } \operatorname{Aut}(\mathcal{C}') \text{ on the generator matrix } G'. \text{ Thus } G$ and G' have the same number of ponctual orbits, the same number of non-ponctual orbits and the two orbits O_{t_i} and O'_{t_i} on the one hand and O_i and O'_i on the other hand have the same number of columns. we conclude that the two codes C and C' have the same Signature. \Box

3.2. Classification

 C_k .

3.2.1. Case 1: f = 0 and k = rWe have

$$G = \left(\underbrace{c_1^{(1)}, c_1^{(2)}, \cdots, c_1^{(t_1)}}_{O_{t_1}}, \cdots, \underbrace{c_k^{(1)}, c_k^{(2)}, \cdots, c_k^{(t_k)}}_{O_{t_k}}\right) = \begin{pmatrix} d_1 \\ \vdots \\ d_k \end{pmatrix}$$

Theorem 11 If C is an $[n,k]_2$ DW-code without punctual orbits (f=0) and if the number of non punctual orbits is equal to the dimension of the DW-code (r=k) then the code C is equivalent to a DW-code of generator matrix

 $G = G_k \left(t_1, t_2, \dots, t_k \right) = \begin{pmatrix} \underbrace{1 \dots 1}_{t_1} 000 \dots 0 \dots 0\\ 0 \dots 0 \underbrace{1 \dots 1}_{t_2} \dots 0 \dots 0\\ \vdots\\ 000000 \dots 00 \underbrace{1 \dots 1}_{t_k} \end{pmatrix} \text{ whith } 2 \le t_1 < t_2 < \dots < t_k \text{ and } t_1 = d \text{ is the minimal distance of }$

Proof. After a series of permutations and elementary operations on rows of G we can make the first line of a_{i_1}

the first orbit formed only by ones and all other rows are null
$$\begin{array}{c} 00 \cdots 0 \\ \vdots \\ 00 \cdots 0 \end{array}$$
 all other bits of the first row of the $00 \cdots 0$

generator matrix are zero. Otherwise the first line of another orbit O_{t_s} will be formed only by 1 s. And a series of permutations and elementary row operations can make null all the other rows of this orbit so $O_{t_1} \cap O_{t_s} \neq \emptyset$. This is a contradiction since two orbits are disjoint. We obtain a generator matrix of an equivalent code denoted

by the same sign $G_k = \begin{bmatrix} 0 & | \\ \vdots & | & G_k^0 \\ 0 & | \end{bmatrix}$. It is easy to see that G_k^0 is a generator matrix of a DW-code

without punctual orbits $(f_{G_k^0} = 0)$ and the number of orbits is equal to the dimension of this DW-code $(r_{G^0} = k - 1)$ and This allows for reasoning by induction. We obtain a generator matrix of an equivalent code

$$G_{k}(t_{1},t_{2},\cdots,t_{k}) = \begin{pmatrix} \underbrace{1\cdots1}_{t_{1}}000\cdots0\cdots0\\0\cdots0\underbrace{1\cdots1}_{t_{2}}\cdots0\cdots0\\\vdots\\000000\cdots00\underbrace{1\cdots1}_{t_{k}} \end{pmatrix}$$

It is clear that we have $wt(d_1) = t_1 = d$, $wt(d_2) = t_2$, \cdots , $wt(d_k) = t_k$ and $2 \le t_1 < t_2 < \cdots < t_k$, $(t_1 \ge 2)$ since $t_1 = 1$ implies the existence of a punctual orbit). \Box

Remark 12 In this case, up to equivallence, each $[n,k]_2$ DW-code admits the system $\{d_1, d_2, \dots, d_k\}$ as

orthogonal basis:
$$d_1 = \left(\underbrace{1\cdots 1}_{t_1} 0\cdots 0\right), \quad d_2 = \left(\underbrace{0\cdots 0}_{t_1} \underbrace{1\cdots 1}_{t_2} 0\cdots 0\right), \quad \cdots, \quad d_2 = \left(\underbrace{0\cdots 0}_{t_1} \underbrace{0\cdots 0}_{t_2} 0\cdots 0\underbrace{1\cdots 1}_{t_k}\right) \quad such as$$

 $wt(d_1) = t_1 = d, wt(d_2) = t_2, \cdots, \quad wt(d_k) = t_k \quad and \quad 2 \le t_1 < t_2 < \cdots < t_k.$

Example 13 Consider the [15,3,2], DW-code of generator matrix

10000000000100		(110000000000000)	1
011111111000010	. It is equivallente to the code of generator matrix	001111000000000	
00000000111001		000000111111111)

 $t_1=2\,,\ t_2=4\,,\ t_3=9\,,\ f=0\,,\ r=k=3$

Corollary 14 Let two $[n,k]_2$ DW-codes C and C' without punctual orbits and the number of their orbits is equal to their dimension. Then the codes C and C' are equivalent if and only if sign(C) = sign(C'). \Box

The converse of Theorem 11 is true under an additional condition.

Theorem 15 Let C an $[n,k]_2$ code of generator matrix $G_k(t_1,t_2,\dots,t_k)$ (as in the last remark). If: (1) $2 \le t_1 < t_2 < \dots < t_k$

(2) $\forall I \subseteq \{1, 2, \dots, k\}, \forall i = 1, 2, \dots, k, \forall \varepsilon_j = \pm 1 \text{ we have } t_i \neq \sum_{j \in \{I \setminus \{i\}\}} \varepsilon_j t_j$

then C is a DW-code of minimum distance $d = t_1$ for which f = 0 and r = k. **Proof.** Clear.

Corollary 16 The number of equivalence classes of $[n,k,d]_2$ DW-codes such as f = 0, k = r and $2^k < n+1$ equals the number of solutions (t_1,t_2,t_3,\dots,t_k) of the Diophantine equations $n = t_1 + t_2 + t_3 + \dots + t_k$ satisfying the following conditions

(1)
$$d = t_1 < t_2 < t_3 < \dots < t_k$$

(2) $t_i \neq \sum_{j \in (I \setminus \{i\})} \varepsilon_j t_j, \forall i = 1, 2, \dots, k, \forall \varepsilon_j = \pm 1, \forall I \subseteq \{1, 2, \dots, k\}.$

Proof. Let the application that maps each equivalence class represented by the matrix $G_k(t_1, t_2, \dots, t_k)$ to the *t*-tuple (t_1, t_2, \dots, t_k) solution of the Diophantine equation as described in Theorem 11. This application is clearly a bijection between the set of equivalence classes and the set of solutions of the Diophantine equation satisfying conditions (1) and (2). \Box

3.2.2. Case 2: $f \neq 0$ and k = r

Theorem 17 If C is an $[n,k]_2$ DW-code with f punctual orbits $(f \neq 0)$ and if the number of non punctual orbits is equal to the dimension of the DW-code (r = k) then the code C is equivalent to the

 $DW\text{-}code \ of \ generator \ matrix \ G = \begin{pmatrix} t_1 & 0 \cdots 0 & \cdots & 0 \cdots 0 & | & c_1c_2 \cdots c_f \\ 0 \cdots 0 & 1 \cdots 1 & \cdots & 0 \cdots 0 & | & \vdots \\ 0 \cdots 0 & 0 \cdots 0 & \cdots & 0 \cdots 0 & | & \vdots \\ \vdots & \vdots & \vdots & \vdots & | & \vdots \\ 0 \cdots 0 & 0 \cdots 0 & \cdots & 0 \cdots 0 & | & \vdots \\ 0 \cdots 0 & 0 \cdots 0 & \cdots & 0 \cdots 0 & | & \vdots \\ 0 \cdots 0 & 0 \cdots 0 & \cdots & 0 \cdots 0 & | & \vdots \\ 0 \cdots 0 & 0 \cdots 0 & \cdots & 1 \cdots 1 & | & \vdots \end{pmatrix}$ with $1 \le f \le 2^k - 1 - k$ and $2 \le t_1 \le t_2 \le \cdots \le t_k . \square$ Example 18 Consider the $[15, 3, 4]_2$ DW-code C_1 of generator matrix $G_1 = \begin{pmatrix} 111 & 0000000 & 000 & 10 \\ 111 & 1111111 & 000 & 01 \\ 111 & 0000000 & 111 & 01 \end{pmatrix}$. It is equivalente to the code C_2 of generator matrix $G_2 = \begin{pmatrix} 111 & 000 & 0000000 & \frac{F}{10} \\ 000 & 111 & 0000000 & 11 \\ 000 & 000 & 11111111 & 11 \end{pmatrix}$ $t_1 = 3, \ t_2 = 3, \ t_3 = 7, \ f = 2, \ r = k = 3$

We have $\operatorname{sign}(\mathcal{C}_1) = \operatorname{sign}(\mathcal{C}_2)$ since \mathcal{C}_1 and \mathcal{C}_2 are equivallente.

The converse of this theorem is true under an additional condition. Let C an $[n,k]_2$ of generator matrix

$$\begin{pmatrix} \underbrace{1\cdots 1}_{i_1} & | & c_1c_2\cdots c_f \\ & \ddots & | & \vdots \\ & & \underbrace{1\cdots 1}_{i_k} & | & \vdots \end{pmatrix}$$
 with: $1 \le f \le 2^k - 1 - k$ and $2 \le t_1 \le t_2 \le \cdots \le t_k$. c_1, c_2, \cdots, c_f are f different

columns which are also different from all unitary columns $(1,0,\dots,0)^{T}$, $(0,1,0,\dots,0)^{T}$, \dots , $(0,\dots,0,1)^{T}$.

For each $I \subseteq \{1, 2, \dots, k\}$, denote by $\omega_{I,\epsilon}$ the weight of the sum of all the jth rows where $j \in I \setminus \{i\}$ of the $k \times f$ matrix

$$A = \begin{pmatrix} \varepsilon_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \varepsilon_2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \varepsilon_3 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \varepsilon_k \end{pmatrix} \begin{pmatrix} c_1, & c_2, & \cdots & , c_f \end{pmatrix} \quad \varepsilon_j = \pm 1, \quad \varepsilon = (\varepsilon_j)_j$$

For all $i = 1, 2, \dots, k$ denote by α_i the weight of the *i*th row of the $k \times f$ matrix (c_1, c_2, \dots, c_f) . So by setting the numbers $\rho_{I,i,\epsilon} = \omega_{I,\epsilon} - \alpha_i$ we have the following result, let C an [n,k] code of generator matrix G as described in theorem 17 we have:

Theorem 19 If for all $I \subseteq \{1, 2, \dots, k\}$, for all $i \in I$ and for all $\epsilon = (\varepsilon_j)_j$, $\varepsilon_j = \pm 1$ we have

$$t_i \neq \left(\sum_{j \in (I \setminus \{i\})} \varepsilon_j t_j\right) + \rho_{I,i,\epsilon} \quad then \ the \ code \quad \mathcal{C}_k \quad is \ a \ DW\text{-}code. \ \Box$$

Let C_k an $[n,k]_2$ DW-code such as $2^k < n+1$, r = k and $1 \le f \le 2^k - 1 - k$. We have $n(f) = C_{2^k - 1 - k}^f$ different way to the choice of f fixed columns. For each value of f and for the s_f -th choice of f fixed

columns we denote by $N(f, s_f)$, $1 \le s_f \le C_{2^k - 1 - k}^f$ the number of solutions of the Diophantine equations $n - f = t_1 + t_2 + t_3 + \dots + t_k$ which satisfy the following conditions

$$\begin{array}{ll} (1) & 2 \leq t_1 \leq t_2 \leq t_3 \leq \cdots \leq t_k \\ (2) & t_i \neq \left(\sum_{j \in \{I \setminus \{i\}\}} \varepsilon_j t_j\right) + \rho_{I,i,\epsilon} \quad \forall i = 1, 2, \cdots, k \ , \forall I \subseteq \{1, 2, \cdots, k\} \ , \ \forall \epsilon = \left(\varepsilon_j\right)_j, \ \varepsilon_j = \pm 1 \end{array}$$

So we have the following result.

Theorem 20

1) The number of equivalence classes of [n,k] DW-codes with $2^k < n+1$ and a given f such that $1 \le f \le 2^k - 1 - k$ and k = r equals the number $\sum_{s_f=1}^{s_f=n(f)} N(f,s_f)$.

2) The number of equivalence classes of $[n,k]_2$ DW-codes with $2^k < n+1$, $f \neq 0$ and k = r equals the number $\sum_{f=1}^{f=2^k-1-k} \left(\sum_{s_f=1}^{s_f=n(f)} N(f,s_f)\right)$. \Box

Example 21 By using the result of the last theorem and the Q-extension software, We show that there exist Only 4 $[11,3]_2$ DW-code up to equivalence verifying r = k = 3. Indeed $1 \le f \le 2^3 - 1 - 3 = 4$ and we have:

• For f = 1 the set of possible columns taken in the following order are:

So the number of DW-codes with $2^k < n+1$, f = 1 and k = r is $\sum_{i=1}^{i=4} N(1,i) = 3$.

• For f = 2 the set of possible columns taken in the following order are:

So there is no DW-codes with $2^k < n+1$, f = 2 and k = r since $\sum_{i=1}^{i=6} N(2,i) = 0$.

• For f = 3 the set of possible columns taken in the following order are:

$$\begin{array}{c|c} 1\text{th} & 2\text{th} & 3\text{th} & 4\text{th} \\ \hline [c_1c_2c_3] & [c_1c_2c_4] & [c_1c_3c_4] & [c_2c_3c_4] \\ 110 & 111 & 101 & 101 \\ 101 & 101 & 111 & 011 \\ 011 & 011 & 011 & 111 \\ N(3,1) = N(3,2) = N(3,3) = N(3,4) = 0 \end{array}$$

So there is no DW-codes avec $2^k < n+1$, f = 3 and k = r since $\sum_{i=1}^{i=4} N(3,i) = 0$.

• For f = 4 the set of possible columns taken in the following order are:

$$\frac{\frac{1\text{th}}{\left[c_{1}c_{2}c_{3}c_{4}\right]}}{1101} \\
1011 \\
0111 \\
N(4,1) = 0, \quad N(4,2) = 0, \quad N(4,3) = 1, \quad N(4,4) = 0.$$

So there is one DW-codes such as $2^k < n+1$, f = 3 and k = r since $\sum_{i=1}^{i=1} N(4,i) = 1$.

We deduce that there is only four $[11,3]_2$ DW-codes, among 98 equivalence classes, satisfying r = k = 3 since

$$\sum_{f=1}^{f=4} \left(\sum_{i=1}^{i=n(f)} N(f,i) \right) = \sum_{i=1}^{i=4} N(1,i) + \sum_{i=1}^{i=6} N(2,i) + \sum_{i=1}^{i=4} N(3,i) + \sum_{i=1}^{i=1} N(4,i) = 4$$

3.2.3. Case 3: f = 0 and $k \neq r$

We have necessarily k < r.

Theorem 22 If C is an $[n,k]_2$ DW-code without punctual orbits (f = 0) and if the number of non punctual orbits is different from the dimension of the DW-code $(r \neq k)$ then

k < r and the code C is equivalent to the DW-code of generator matrix

$$\begin{pmatrix} \underbrace{1\cdots 1}_{t_1} & | & \underbrace{*\cdots *}_{k\cdots *} & \cdots & \underbrace{*\cdots *}_{t_k} \\ & \ddots & | & \vdots & \ddots & \vdots \\ & & \underbrace{1\cdots 1}_{t_k} & | & \vdots & \cdots & \vdots \\ & & & & & \end{pmatrix}$$

with $2 \le t_1 \le t_2 \le \dots \le t_k$. \square

of generator matrix $\begin{pmatrix} 1100000000 & 1111 \\ 00111100000 & 0000 \\ 00000011111 & 1111 \end{pmatrix}$ $f = 0, \ k = 3, \ r = 4, \ t_1 = 2, \ t_2 = 4, \ t_3 = 5, \ t_4 = 4. \square$

In this case two DW-codes with the same signature are not necessarily equivalent as shown in the following example:

Example 24 Let C_1 the DW-code of generator matrix G_1 and C_2 the DW-code of generator matrix G_2 such as C_1 and C_2 are not equivalent and

We have $sign(C_1) = sign(C_2) = (1, 3, (2, 4, 8))$.

3.2.4. Case 4: $f \neq 0$ and $k \neq r$

We can have two cases k < r or r < k

Theorem 25 If C is an $[n,k]_2$ DW-code with f punctual orbits $(f \neq 0)$ and if the number of non punctual orbits is greater than the dimension of the DW-code (r > k) then the code C is equivalent to the

$$DW\text{-}code \ of \ generator \ matrix \left(\begin{array}{cccc} 1 & \cdots & 1 & \cdots & 1 \\ \hline 1 & \cdots & 1 & \hline c_1 & \cdots & c_f & \hline s & \cdots & s \\ \hline & \ddots & & \vdots & \vdots & \ddots & \vdots \\ & 1 & \cdots & 1 & \vdots & \vdots & \cdots & \vdots \end{array} \right) \ with \ 2 \le t_1 \le t_2 \le \cdots \le t_k \ \Box$$

$$\mathbf{Example \ 26 \ The \ [15,3,4]_2 \ DW\text{-}code \ of \ generator \ matrix \ \begin{pmatrix} 111000000000100 \\ 11111110010 \\ 11111110000001001 \end{pmatrix} \ is \ equivallent \ to \ the \ code$$

$$of \ generator \ matrix \ \begin{pmatrix} 1100000 \ 1111111 \ 0 \\ 0011000 \ 1111111 \ 1 \\ 0000111 \ 0000000 \ 0 \end{pmatrix} \ t_1 = 2 \ , \ t_2 = 2 \ , \ t_3 = 3 \ , \ t_4 = 7 \ , \ f = 1 \ , \ k = 3 \ , \ r = 4$$

Theorem 27 If C is an $[n,k]_2$ DW-code with f punctual orbits $(f \neq 0)$ and if the number of non punctual orbits is lower than the dimension of the DW-code (r < k) then the code C is equivalent to the DW-code of generator matrix

$$\begin{pmatrix} \underbrace{1\cdots 1}_{t_1} & \overbrace{c_1c_2\cdots c_f}^{\text{fixed columns}} \\ & \ddots & \vdots \\ & \underbrace{1\cdots 1}_{t_r} & \vdots \\ 000 & \cdots & 000 & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 000 & \cdots & 000 & \vdots \end{pmatrix}$$

with $2 \le t_1 \le t_2 \le \dots \le t_r$. \square

Example 28 The $[15,3,4]_2$ DW-code of generator matrix $\begin{pmatrix} 11000000000100\\11111110000010\\10000001111001 \end{pmatrix}$ is equivalent to the code

Remark 29 Self-orthogonality.

A code which is equivalent to a self-orthogonal code is also self-orthogonal. The property of self- orthogonality is then an invariant of the equivalence of codes. We then have the following points:

• If $f \neq 0$ or $(f = 0 \text{ and } r \neq k)$ then, up to equivalence, a generator matrix of the code is of the form G = [TD] where D is not an empty submatrix. If the code is self-othogonal then $GG^{T} = 0$. So $[TD][TD]^{T} = 0$ and then we have:

•
$$f \neq 0$$
 and $r > k$ and then $DD^{\mathrm{T}} = \mathrm{diag}(t_1[2], t_2[2], \dots, t_k[2])$

- $f \neq 0$ and r < k then $DD^{\mathrm{T}} = \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix}$ where $B = \mathrm{diag}(t_1[2], t_2[2], \dots, t_r[2])$.
- $f \neq 0$ and r = k then $DD^{T} = \text{diag}(t_{1}[2], t_{2}[2], \dots, t_{k}[2])$
- finally f = 0 and $r \neq k$ and then $DD^{T} = \text{diag}(t_1[2], t_2[2], \dots, t_k[2])$
- If f = 0 and r = k the code C is self-orthogonal if and only if $t_i \equiv 0 \mod 2$ for all $i = 1, 2, \dots, k$.

3.3. Determination of the Automorphism Group

Theorem 30 The automorphism group of a [n,k] DW-code of signature $(f,k,(t_1,t_2,\dots,t_r))$ is isomorphic to the group direct product $\prod_{i=1}^r S_{t_i}$.

Proof. Let G be a generator matrix of the code C. We can assume that G is of the form

 $G = (O_{t_1}, \dots, O_{t_r}, O_1, O_2, \dots, O_f) \text{ where } O_{t_i} = \{c_{s_{i-1}+1}, \dots, c_{s_i}\}, \quad s_i = \sum_{j=1}^{j=i} f_j \quad \forall i = 1, 2, \dots, t_r \text{ and } O_i = \{c_{s_r+i}\} \\ \forall i = 1, 2, \dots, f \text{ .}$

For $i = 1, \dots, r$, let $E_i = \{s_{i-1} + 1, \dots, s_i\}$, let $E_{s_r+i} = \{s_r + i\}$ for all $i = 1, 2, \dots, f$. Clearly, the subsets E_1, \dots, E_n form a partition of $\{1, 2, \dots, n\}$. Now let $G_i = \{\sigma \in S_n / \sigma(E_i) \subset E_i \text{ and } \forall j \neq i, \sigma(x) = x, \forall x \in E_j\}$.

Clearly the G_i are subgroups of S_n and each is isomorphic to S_{t_i} and $G_i = \{id\}$ for all

 $i = s_r + 1, \dots, s_r + f = n$. Since forall $\sigma \in G_i$, $\sigma(c_j) = c_j$, it follows that the G_i are subgroups of $\operatorname{Aut}(\mathcal{C})$. Now we are going to show that $\operatorname{Aut}(\mathcal{C})$ is the inner direct product $G_1G_2\cdots G_k$

If $i \neq j$, and $\sigma \in G_i$, $\tau \in G_j$, then $\sigma \tau = \tau \sigma$.

Let $\sigma_1 \sigma_1 \cdots \sigma_k = I$, then applying this equality to each E_i yields $\sigma_i = I$, $\forall i$.

Now let $\sigma \in \operatorname{Aut}(\mathcal{C})$. Since $\sigma(c_i) = c_i$, the E_i are globally invariant under σ . Let σ_i the permutation defined by $\sigma_i(x) = \sigma(x)$, if $x \in E_i$, and $\sigma_i(x) = x$ elswhere. Then it is clear that $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$, and this finishes the proof. \Box

Example 31

of generator matrix
$$\begin{pmatrix} 11100000000 & 110\\ 000111000000 & 111\\ 000000111111 & \underline{101}\\ fixed \end{pmatrix} t_1 = 3, t_2 = 3, t_3 = 6, f = 3, r = k = 3$$

Aut $(\mathcal{C}) = S_2 \cdot S_4 \cdot S_9$ and $|\operatorname{Aut}(\mathcal{C})| = (2!) \times (4!) \times (9!)$

Acknowledgements

The authors would like to thank the refrees for their helpful suggestions and remarks.

References

- [1] Bouyukliev, I. (2007) About the Code Equivalence, Advances in Coding Theory and Cryptology. In: Shaska, T., Huffman, W.C., Joyner, D. and Ustimenko, V., Eds., *Series in Coding Theory and Cryptology*, World Scientific Publishing, Vol. 3, 126-151.
- [2] MacWilliams, F.J. and Sloane, N.J.A. (1977) The Theory of Error-Correcting Codes. Elsevier-North-Holland, Amsterdam.
- [3] MacWilliams, F.J. (1962) Combinatorial Problems of Elementary Abellan Groups. Ph.D. Dissertation, Harvard University, Cambridge.
- [4] Bogart, K., Goldberg, D. and Gordon, J. (1978) An Elementary Proof of the MacWilliams Theorem on Equivalence of Codes. *Information and Control*, 37, 19-22. <u>http://dx.doi.org/10.1016/S0019-9958(78)90389-3</u>
- [5] Bouyukliev, I.G. (2007) What Is Q-Extension? Serdica Journal of Computing, 1, 115-130.