Turkish Journal of Mathematics

Volume 23 | Number 4 Article 2

1-1-1999

The Weight Equations for Binary Linear Codes

ERSAN AKYILDIZ

İSMAİL Ş. GÜLOĞLU

MASATOSHI IKEDA

Turk J Math
23 (1999) , 465 – 483.

THE WEIGHT EQUATIONS FOR BINARY LINEAR CODES*

Ersan Akyıldız, İsmail Ş. Güloğlu & Masatoshi İkeda

Abstract

The system of weight equations for a binary (n, m)-code with respect to its ordered basis is introduced. It connects certain quantities (characteristics) related to the basis with the weights of non-zero words in the code. It is shown that the portion involving the variables does not depend neither on the code nor on the basis. Explicit forms of the matrix of coefficients in the system and its inverse matrix are computed.

1. Introduction

The aim of this note is to introduce the system of weight equations for a binary (n, m)-code $\mathcal{C}$ wiht respect to an ordered basis $\mathcal{B}$ of $\mathcal{C}$. It consists of $2^m - 1$ linear equations involving $2^m - 1$ variables, and connects certain quantities (characteristics) related to the basis with the weights of non-zero words of $\mathcal{C}$. The procedure to obtain the system is in fact elementary but rather tedious, hence it is deliberately prefered to proceed in a clumsy way (see Section 2). It turns out that the portion of the system involving the variables depends only on the dimension m of the code $\mathcal{C}$, but independent from the choice of $\mathcal{C}$, or of the basis $\mathcal{B}$ (Theorem 1). Then explicit forms of the matrix of the coefficients (in the system) and its inverse matrix are calculated (Theorems 2 and 3). As an application a necessary and sufficient condition for a finite sequence of positive integers to be a well-arranged weight pattern of an (n, m)-code is derived.

*This work was carried out at the Marmara Research Center, TÜBİTAK, in the frame of the research project "Coding Theory and Cryptology". The second author was supported by a grant of Turkish Academy of Sciences.

2. Set of Characteristics

First we fix some notations and conventions. As usual $\mathbb{Z}_2^n$ stands for the space consisting of all vectors over $\mathbb{Z}_2$ of length n. For convenience' sake we assume that $\mathbb{Z}_2^n$ is the space of *column vectors* of length n. A portion of a vector v consisting of some consecutive entries of v is called a segment of v. Naturally the empty segment is allowed among the segments of v. A segment S of v is called a 0-segment if S is either the empty segment, or consists only of 0; a 1-segment, on the other hand, means either the empty segment, or a segment containing only 1. Two segments of a vector v are said to be disjoint if they do not contain any entry of v in common. A partition of a vector v is a division of v into mutually disjoint segments of v. The weight of a vector v is denoted by $w(v)$. As usual ${}^t v$ stands for the transposed of the vector v. Now

$$v = \begin{bmatrix} v_1 \\ \vdots \\ v_r \end{bmatrix}$$

being a partition of a column vector v, the horizontal expression for this must, strictly done, be $v = {}^t({}^t v_1, \ldots, {}^t v_r)$. To spare the troublesome t's, however, we write $v = {}^t(v_1, \ldots, v_r)$, in abuse of notation, instead of the above one: ${}^t(v_1, \ldots, v_r)$ stands for ${}^t({}^t v_1, \ldots, {}^t v_r)$. Following the tradition, a vector in a code is called a word of the code.

For a (non-empty) ordered set $\mathcal{U} = \{u_1, \ldots, u_m\}$ in $\mathbb{Z}_2^n$, the $n \times m$ matrix $[u_1, \ldots, u_m]$ is denoted by $[\mathcal{U}]$. Throughout this note, by a *coordinate permutation* we always understand a permutation interchanging some coordinate places of all vectors in $\mathbb{Z}_2^n$. Under these agreements we are going to find a coordinate permutation π such that $[\mathcal{U}^\pi] = [u_1^\pi, \ldots, u_m^\pi]$ takes a very special form which we call the canonical form of $[\mathcal{U}]$. As the matter of fact, our process for this is practically quite simple. To be exact, however, we prefer to proceed in a rather clumsy way.

First we introduce a set of indices for 0- and 1-segments. Let $E = \cup_{i=0}^{m-1} E_i$ where $E_0 = \{\phi\}$, and E_i is the set of all i-tuples $(\epsilon_1, \ldots, \epsilon_i)$ with $\epsilon_\nu \in \{0, 1\}$ $(\nu = 1, \ldots, i)$ for $i = 1, \ldots, m-1$. The number of elements in E_i is 2^i for each i, so that the total number of elements in E is $2^m - 1$. Each E_i with $0 \leq i \leq m-1$ is linearly ordered by the lexicographical order assuming $0 < 1$. Hence, by saying that, for any pair $0 \leq i < j \leq m-1$, every element in E_i is prior to every element in E_j, E is linearly ordered. This ordering on E will be called the semi-lexicographical order. Now, h being $0 \leq h \leq k$,

the element in E_{k-h} obtained by deleting the last h entries from $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_k) \in E_k$ will be called the h-th contraction of $\tilde{\epsilon}$, and will be denoted by $\tilde{\epsilon}^{(h)} : \tilde{\epsilon}^{(h)} = (\epsilon_1, \ldots, \epsilon_{k-h})$. Note that $\tilde{\epsilon}^{(k)} = \phi \in E_0$ for every $\tilde{\epsilon} \in E_k$. Any element $\tilde{\eta} \in E_{k-h}$ is the h-th contraction of a suitable $\tilde{\epsilon} \in E_k$ which will be called an extension of $\tilde{\eta}$ to E_k. Note, in particular, that there are exactly two extensions of $\tilde{\eta} = (\eta_1, \ldots, \eta_{k-1}) \in E_{k-1}$ to E_k : $(\eta_1, \ldots, \eta_{k-1}, 0)$ and $(\eta_1, \ldots, \eta_{k-1}, 1)$. The former will be denoted by $(\tilde{\eta}, 0)$, and the latter by $(\tilde{\eta}, 1)$.

Now, returning to our aim in this section, we first find a coordinate permutation π_1 such that $u_1' = u_1^{\pi_1} = {}^t(S_\phi', S_\phi)$ (see the agreement concerning the transposed of a partition of a column vector at the beginning of this section) is a partition of u_1' with a 0-segment S_ϕ' of length $s_\phi' = n - w(u_1)$, and a 1-segment S_ϕ of length $s_\phi = w(u_1)$. It is clear that we can find such a permutation. Note that S_ϕ' or S_ϕ may be empty. Next, assuming that S_ϕ' and S_ϕ are non-empty, we find a coordinate permutation π_2 such that

(a) π_2 leaves the segments S_ϕ' and S_ϕ (hence u_1' itself) unchanged,

(b) $u_2' = u_2^{\pi_1\pi_2} = {}^t(S_{(0)}', S_{(0)}, S_{(1)}', S_{(1)})$ is a partition of u_2' with 0-segments $S_{(0)}'$ and $S_{(1)}'$ of lengths $s_{(0)}'$ and $s_{(1)}'$ respectively, and with 1-segments $S_{(0)}$ and $S_{(1)}$ of lengths $s_{(0)}$ and $s_{(1)}$ respectively, and finally

(c) the coordinate places involved in the segment ${}^t(S_{(0)}', S_{(0)})$ are exactly those which are involved in S_ϕ', and the same holds for the segment ${}^t(S_{(1)}', S_{(1)})$ and S_ϕ, consequently $s_{(\phi)}' = s_{(0)}' + s_{(0)}$, and $s_\phi = s_{(1)}' + s_{(1)}$ hold.

Now to obtain such a permutation, look at first the segment, say T_ϕ', of $u_2^{\phi_1}$ corresponding to S_ϕ', and find a coordinate permutation $\pi_2^{(0)}$ permuting only the coordinate places involved in S_ϕ' among themselves, and transforming T_ϕ' into the form ${}^t(0, \ldots, 0, 1, \ldots, 1)$ consisting of a 0-segment lying above a 1-segment. Then set the 0-segment equal to $S_{(0)}'$, and the 1-segment equal to $S_{(0)}$. Next look at the segment, say T_ϕ, of $u_2^{\pi_1}$ corresponding to S_ϕ, and find a coordinate permutation $\pi_2^{(1)}$ interchanging only the coordinate places involved in S_ϕ, and transforming T_ϕ into a vector consisting of a 0-segment above a 1-segment. Then call the 0-segment $S_{(1)}'$, and the 1-segment $S_{(1)}$. Setting $\pi_2 = \pi_2^{(0)}\pi_2^{(1)}$, we readily see that π_2 satisfies all conditions required. Now if $S_\phi' = \phi$, then $S_{(0)}'$ and $S_{(0)}$ are simply put equal to the empty set, similarly if $S_\phi = \phi, S_{(1)}'$ and $S_{(1)}$ are defined to

be empty. The coordinate permutation $\pi_2^{(0)}$ or $\pi_2^{(1)}$ then is understood to be the identity permutation accordingly. Note that, under these definitions for $S'_{(0)}, S_{(0)}, S'_{(1)}$ and $S_{(1)}$ in these special circumstances, the conditions (a), (b) and (c) still hold. It is now almost clear how we proceed further. Before doing this, however, it is in place to mention that

(d) the segments ${}^t(S'_{(0)}, S_{(0)})$ and ${}^t(S'_{(1)}, S_{(1)})$ constructed above are arranged in the lexicographical order on $E_1 = \{(0), (1)\}$, namely the former is located above the latter.

Now take any r satisfying $2 \leq r < m$, and assume that there are already found a sequence of coordinate permutations $\pi_1, \ldots, \pi_r$ satisfying the following conditions: For each i with $2 \leq i \leq r$,

(1) $u'_i = u_i^{\pi_1 \cdots \pi_i}$ is partitioned into the form ${}^t(\ldots, S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}}, \ldots)$ with 0-segments $S'_{\tilde{\epsilon}}$ and 1-segments $S_{\tilde{\epsilon}}$ where $\tilde{\epsilon}$ runs through E_{i-1};

(2) the coordinate places involved in the segment ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ are either exactly those involved in $S'_{\tilde{\epsilon}(1)}$, or exactly those involved in $S_{\tilde{\epsilon}(1)}$ according as the last entry ϵ_{i-1} of $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_{i-1})$ is 0 or 1 for every $\tilde{\epsilon} \in E_{i-1}$, consequently, $s'_{\tilde{\epsilon}}$ and $s_{\tilde{\epsilon}}$ being the lengths of $S'_{\tilde{\epsilon}}$ and $S_{\tilde{\epsilon}}$ respectively, $s'_{\tilde{\epsilon}} + s_{\tilde{\epsilon}} = s'_{\tilde{\epsilon}(1)}$ or $s_{\tilde{\epsilon}(1)}$ according as the last entry of $\tilde{\epsilon}$ is 0 or 1;

(3) the segments ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ $(\tilde{\epsilon} \in E_{i-1})$ appearing in the partition of u'_i are arranged in the lexicographical order on E_{i-1};

(4) π_i leaves each of the segments $S'_{\tilde{\eta}}$ and $S_{\tilde{\eta}}$ unchanged for every $\tilde{\eta} \in E_{i-2}$.

Before showing that we can go one-step further, note that the condition (2) together with (4) implies that π_i leaves all segments $S'_{\tilde{\lambda}}$ and $S_{\tilde{\lambda}}$ with $\tilde{\lambda} \in E_j$ unchanged for $j \leq i-2$, hence it leaves every u'_j with $j \leq i-1$ unchanged. Further note that the conditions above are actually satisfied in the case $r = 2$ (compare with (a), (b), (c) and (d)). Now the construction of a coordinate permutation π_{r+1} satisfying the equivalents of the conditions above is completely parallel to that for the case $r = 2$. For the sake of completeness, however, we repeat the process. For this end, take any $\tilde{\epsilon} \in E_{r-1}$, and the segments $S'_{\tilde{\epsilon}}$ and $S_{\tilde{\epsilon}}$. First, assuming that $S'_{\tilde{\epsilon}}$ and $S_{\tilde{\epsilon}}$ are both non-empty, let the segment in $u_{r+1}^{\pi_1 \cdots \pi_r}$ corresponding to $S'_{\tilde{\epsilon}}$ be $T'_{\tilde{\epsilon}}$, and let the segment corresponding to $S_{\tilde{\epsilon}}$ be $T_{\tilde{\epsilon}}$. Further find a coordinate permutation $\rho_{r+1}^{(\tilde{\epsilon})}$ permuting only the coordinate places involved in $S'_{\tilde{\epsilon}}$ among

themselves, and transforming $T'_{\tilde{\epsilon}}$ into a vector of the form "a 0-segment lying above a 1-segment". Then furnish the 0-segment and the 1-segment of $(T'_{\tilde{\epsilon}})^{\rho^{(\tilde{\epsilon})}_{r+1}}$ with indices by setting them equal to $S'_{(\tilde{\epsilon},0)}$ and $S_{(\tilde{\epsilon},0)}$ respectively. Do the same thing for $T_{\tilde{\epsilon}}$. Namely find a coordinate permutation $\pi^{(\tilde{\epsilon})}_{r+1}$ interchanging only the coordinate places involved in $S_{\tilde{\epsilon}}$, and transforming $T_{\tilde{\epsilon}}$ into a vector of the form "a 0-segment above a 1-segment". Then call the 0-segment and the 1-segment of $T_{\tilde{\epsilon}}^{\pi^{(\tilde{\epsilon})}_{r+1}}$ $S'_{(\tilde{\epsilon},\ell)}$ and $S_{(\tilde{\epsilon},\ell)}$ respectively. So far for the case where $S'_{\tilde{\epsilon}}$ and $S_{\tilde{\epsilon}}$ are both non-empty. If, on the contrary, $S'_{\tilde{\epsilon}}$ or $S_{\tilde{\epsilon}}$ is empty, then the corresponding (formal) 0-segment and 1-segment in $u_{r+1}^{\pi_1\cdots\pi_r}$ are both defined to be empty, i.e. if $S'_{\tilde{\epsilon}} = \phi$, then we set $S'_{(\tilde{\epsilon},0)} = S_{(\tilde{\epsilon},0)} = \phi$, and if $S_{\tilde{\epsilon}} = \phi$, then $S'_{(\tilde{\epsilon},1)} = S_{(\tilde{\epsilon},1)} = \phi$. Furthermore the coordinate permutation $\rho^{(\tilde{\epsilon})}_{r+1}$ or $\pi^{(\tilde{\epsilon})}_{r+1}$ in question is understood to be the identity permutation accordingly. In this way, we obtain a pair of coordinate permutations $\{\rho^{(\tilde{\epsilon})}_{r+1}, \pi^{(\tilde{\epsilon})}_{r+1}\}$ and a quadruple of segments

$$\{S'_{(\tilde{\epsilon},0)}, S_{(\tilde{\epsilon},0)}, S'_{(\tilde{\epsilon},1)}, S_{(\tilde{\epsilon},1)}\}$$

for each $\tilde{\epsilon} \in E_{r-1}$. Note that, if $\tilde{\epsilon}$ runs through $E_{r-1}, (\tilde{\epsilon}, 0)$ and $(\tilde{\epsilon}, 1)$ range over all elements in E_r. Setting

$$\pi_{r+1} = \prod_{\tilde{\epsilon}\in E_{r-1}} \left(\rho^{(\tilde{\epsilon})}_{r+1}\ \pi^{(\tilde{(}\epsilon)}_{r+1}\right),$$

we then readily see that π_{r+1} together with $S'_{\tilde{\delta}}$ and $S_{\tilde{\delta}}(\tilde{\delta} \in E_r)$ constructed above satisfies the equivalents of (1)-(4) above. Note here that the permutations appearing on the right in the definition of π_{r+1} are pair-wise commutative. Thus completing the induction, we see the existence of m coordinate permutations $\pi_1, \ldots, \pi_m$ subject to the conditions above. Then, setting $\pi = \pi_1 \cdots \pi_m$, we obtain the following

Lemma 1. *There is a coordinate permutation π such that the matrix $[\mathcal{U}^\pi] = [u_1^\pi, \ldots, u_m^\pi]$ satisfies the conditions: For each i $(= 1, \ldots, m)$*

(1) the i-th column $u'_i = u_i^\pi$ is partitioned into the form ${}^t(\ldots, S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}}, \ldots)$ with 0-segments $S'_{\tilde{\epsilon}}$ and 1-segments $S_{\tilde{\epsilon}}$, where $\tilde{\epsilon}$ ranges over all elements in E_{i-1};

(2) if $i \geq 2$, the coordinate places involved in the segment ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ of the i-th column are either exactly those involved in the segment $S'_{\tilde{\epsilon}^{(1)}}$ of the $(i-1)$-th column, or exactly those involved in the segment $S_{\tilde{\epsilon}^{(1)}}$ of the $(i-1)$-th column according as the

last entry of $\tilde{\epsilon}$ is 0 or 1 for every $\tilde{\epsilon} \in E_{i-1}$, consequently, $s'_{\tilde{\epsilon}}$ and $s_{\tilde{\epsilon}}$ being the lengths of $S'_{\tilde{\epsilon}}$ and $S_{\tilde{\epsilon}}$ respectively, if $i \geq 2$, $s'_{\tilde{\epsilon}} + s_{\tilde{\epsilon}} = s'_{\tilde{\epsilon}(1)}$ or $s_{\tilde{\epsilon}(1)}$ according as the last entry of $\tilde{\epsilon}$ is 0 or 1, while, if $i = 1$, $s'_{\phi} + s_{\phi} = n$, and $s_{\phi} = w(u_1) = w(u'_1)$;

(3) the segments ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ $(\tilde{\epsilon} \in E_{i-1})$ in the partition of the i-th column u'_i are arranged in the lexicographical order on E_{i-1}.

The set of the segments $S'_{\tilde{\epsilon}}$ and $S_{\tilde{\epsilon}}$ $(\tilde{\epsilon} \in E)$ satisfying the conditions (1), (2) and (3) in Lemma 1 will be caled the canonical tableau for $[\mathcal{U}]$, and the matrix $[\mathcal{U}^{\pi}]$ the canonical form for $[\mathcal{U}]$. The latter will be denoted by $\mathcal{X}_{\mathcal{U}}$. Its shape does not depend on the specific choice of the permutations π used in its construction (see Corollary to Lemma 2, and Remark 2 below).

Remark 1. By (2) in Lemma 1, $s'_{\tilde{\epsilon}} = s'_{\tilde{\epsilon}(1)} - s_{\tilde{\epsilon}}$ or $s_{\tilde{\epsilon}(1)} - s_{\tilde{\epsilon}}$ according as the last entry of $\tilde{\epsilon}$ is 0 or 1 for every $\tilde{\epsilon} \in E_{i-1}$ with $i \geq 2$, and $s'_{\phi} = n - s_{\phi}$. Hence, by induction, we have the following: If, for $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_{i-1}) \in E_{i-1}$ with $i \geq 2$, the last non-zero entry in it has the index h (≥ 1), then

$$s'_{\tilde{\epsilon}} = s_{\tilde{\epsilon}(i-h)} - s_{\tilde{\epsilon}(i-h-1)} - \cdots - s_{\tilde{\epsilon}};$$

if $i \geq 2$, and if all entries in $\tilde{\epsilon}$ are zero, then $s'_{\tilde{\epsilon}} = n - s_{\tilde{\epsilon}(i-1)} - \cdots - s_{\tilde{\epsilon}}$; if $i = 1$, i.e. if $\tilde{\epsilon} = \phi$, then $s'_{\phi} = n - s_{\phi}$. Note that these relations still hold even if $s'_{\tilde{\epsilon}}$ or $s_{\tilde{\epsilon}}$ is zero, i.e. if the segment $S'_{\tilde{\epsilon}}$ or the segment $S_{\tilde{\epsilon}}$ is empty.

Lemma 2. *Keeping the same notations as in Lemma 1, let ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ be a segment in u'_i with $i \geq 2$, where $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_{i-1}) \in E_{i-1}$. If the segment is non-empty, then, for any entry x in the segment, the entries in the canonical form $\mathcal{X}_{\mathcal{U}}$ located on the row (of $\mathcal{X}_{\mathcal{U}}$) through x, and to the left of x are exactly $\{\epsilon_1, \ldots, \epsilon_{i-1}\}$ including the order. Conversely if, for an entry x in $\mathcal{X}_{\mathcal{U}}$, the entries on the row through x, and to the left of x are $\{\epsilon_1, \ldots, \epsilon_{i-1}\}$ in this order, then x is in the segment ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ of u'_i, where $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_{i-1})$. Thus the property stated above characterizes the entries in the segments among the entries of $\mathcal{X}_{\mathcal{U}}$.*

Proof. The first assertion is easily verified for the second column u'_2. So assume that it has already been proved for all u'_j with $2 \leq j < i$, and take an entry x from a non-empty segment ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ of u'_i with the index $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_{i-1})$. Then, from the way of indexing the segments in u'_{r+1} using the indices of the segments in u'_r employed in the proof of

Lemma 1, we see that the entry x' in $\mathcal{X}_{\mathcal{U}}$ found on the row through x, to the left of x, and next to x is ϵ_{i-1}, the last entry of $\tilde{\epsilon}$. Since x' is an entry of $S'_{\tilde{\epsilon}(1)}$ or of $S_{\tilde{\epsilon}(1)}$ according as ϵ_{i-1} is 0 or 1, where $S'_{\tilde{\epsilon}(1)}$ and $S_{\tilde{\epsilon}(1)}$ are both segments of u'_{i-1}, we can apply induction to deduce that the entries of $\mathcal{X}_{\mathcal{U}}$ found on the row through x' (hence through x), and to the left of x' are exactly $\{\epsilon_1, \ldots, \epsilon_{i-2}\}$ in this order. So we see that our assertion still holds for u'_i. This proves the first half of the lemma. To prove the second half, assume that, for an entry x in $\mathcal{X}_{\mathcal{U}}$, the entries in $\mathcal{X}_{\mathcal{U}}$ on the row through x, and to the left of x are $\{\epsilon_1, \ldots, \epsilon_{i-1}\}$ including the order. Then x must be in some segment, say ${}^t(S'_{\tilde{\delta}}, S_{\tilde{\delta}})$ with $\tilde{\delta} \in E_{i-1}$, of u'_i. Since this segment is non-empty, by the first half, $\tilde{\delta}$ must coincide with $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_{i-1})$. Hence $x \in {}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$. □

Corollary. *For any i with $2 \leq i \leq m$, and for any $\tilde{\epsilon} = (\epsilon_1, \ldots \epsilon_{i-1}) \in E_{i-1}, s'_{\tilde{\epsilon}}$ is the number of 0 's in u_i for which the entries in $[\mathcal{U}]$, located on the row (of $[\mathcal{U}]$), through it, and on the left of it are exactly $\{\epsilon_1, \ldots, \epsilon_{i-1}\}$ including the order. Similarly $s_{\tilde{\epsilon}}$ is the number of 1's in u_i satisfying the same condition as above. In particular, $s'_{\tilde{\epsilon}}$ (or $s_{\tilde{\epsilon}}$) is zero, i.e. $S'_{\tilde{\epsilon}}$ (or $S_{\tilde{\epsilon}}$) is empty, if and only if there is no 0 (or 1) satisfying the condition formulated for $\tilde{\epsilon}$.*

Remark 2. Because the characterization of the number $s'_{\tilde{\epsilon}}$ and $s_{\tilde{\epsilon}}$ for $\tilde{\epsilon} \in E$ given above has nothing to do with coordinate permutations, we see that the canonical form for $[\mathcal{U}]$ does not depend on the coordinate permutation used for its construction. It is completely determined by the set of integers $\{s'_{\tilde{\epsilon}}, s_{\tilde{\epsilon}} \,|\, \tilde{\epsilon} \in E\}$. Further, by Remark 1, each $s'_{\tilde{\epsilon}}$ can be expressed in terms of $s_{\tilde{\eta}}$ ($\tilde{\eta} \in E$) by a formula solely depending on the form $\tilde{\epsilon}$. Hence the set above, in turn, is completely characterized by the set of non-negative integers $\{s_{\tilde{\epsilon}} \,|\, \tilde{\epsilon} \in E\}$ which will be called *the set of characteristics of the ordered set* $\mathcal{U} = \{u_1, \ldots, u_m\}$.

Before concluding this section, we return to our original aim. Let $\mathcal{C}$ be a binary (n, m)-code, i.e. an m-dimensional subspace of $\mathbb{Z}_2^n$, and $\mathcal{B} = \{b_1, \ldots, b_m\}$ an ordered basis of $\mathcal{C}$. The discussion above can apply to the ordered basis $\mathcal{B}$, hence one can talk about the canonical form for $[\mathcal{B}]$ and the set of characteristics of $\mathcal{B}$. The former is denoted by $\mathcal{X}_{\mathcal{B}}$.

3. Weight Equations

We first work with an arbitrary ordered set $\mathcal{U} = \{u_1, u_2, \ldots, u_m\}$, then, after proving

Lemma 3 below, we return to our (n, m)-code with an ordered basis $\mathcal{B}$. We keep all notations used in the previous section, in particular, $\mathcal{X}_{\mathcal{U}} = [u'_1, u'_2, \ldots, u'_m]$ stands for the canonical form for $[\mathcal{U}]$. As was said in the introduction, our next aim is to express the weight of the sum $u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}$ for various choices of the indices, subject to the condition $1 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_k \leq m$, in terms of the characterstics of the set $\mathcal{U}$. Before stating our results it is appropriate to introduce some notation:

Let $A = \cup_{j=0}^{m} A_j$, where $A_0 = \{\phi\}$, and A_j is the set of all j-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_j)$ of integers subject to the condition $1 \leq \alpha_1 < \cdots < \alpha_j \leq m$, for $j = 1, 2, \ldots, m$. The total number of elements in A is then 2^m. One can define a linear order on A by saying:

(i) $\phi < a$ for any $a \in A \setminus A_0$;

(ii) $(1) < (2) < \cdots < (m)$;

(iii) $(\alpha_1, \ldots, \alpha_j) < (\beta_1, \beta_2, \ldots, \beta_i)$ if and only if $(\alpha_j) < (\beta_i)$ or $\alpha_j = \beta_i$ and $(\alpha_1, \ldots, \alpha_{j-1}) < (\beta_1, \ldots, \beta_{i-1})$.

This ordering will be called the reversed lexicographical order. Let $A^0 = A \setminus A_0$. For an element $\tilde{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_j) \in A_j$ and for a positive integer h with $h \leq j$, the h-th contraction $\tilde{\alpha}^{(h)}$ of $\tilde{\alpha}$ is the element of A obtained by deleting the last h entries of $\tilde{\alpha}$, $\tilde{\alpha}^{(h)} := (\alpha_1, \ldots, \alpha_{j-h})$ if $h < j$ and $\tilde{\alpha}^{(j)} = \emptyset$. In this case $\tilde{\alpha}$ is called an extension of $\tilde{\alpha}^{(h)}$ to A_j. There is another way of partitioning A^0 which will be used later. For $1 \leq r \leq m$, let $A^{(r)}$ be the subset of all elements in A^0 with the last entry equal to r. Then clearly $A^0 = \cup_{r=1}^{m} A^{(r)}$. Any element in $A^{(r)}$ is either of the form (r), or of the form $(\alpha_1, \ldots, \alpha_i, r)$ subject to the condition $1 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_i < r$. We simply write $(\tilde{\alpha}, r)$, instead of these expressions, where

$$\tilde{\alpha} \in A_0 \cup \bigcup_{s<r} A^{(s)}.$$

Note that for $(\tilde{\alpha}, r), (\tilde{\beta}, r) \in A^{(r)}$ with $r > 1$ we have $(\tilde{\alpha}, r) < (\tilde{\beta}, r)$ if and only if $\tilde{\alpha} < \tilde{\beta}$. Furthermore every element in $A^{(s)}$ is prior to every element in $A^{(r)}$ if $s < r$. We shall use the following abbreviations: Assume that $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_j) \in A_j$ with $1 \leq j$ is given. Then for any $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_i) \in E_i$ with $i \geq j$, the sum $\Sigma_{v=1}^{j} \epsilon_{\alpha_v}$ will be denoted by $(\tilde{\epsilon} \,|\, \tilde{\alpha})$. As for $A_0 = \{\phi\}$ we set $(\tilde{\epsilon} \,|\, \phi) = \emptyset$. Under the same assumption, if $j \geq 1$ the subset of E_i consisting of all $\tilde{\epsilon}$ satisfying $(\tilde{\epsilon} \,|\, \tilde{\alpha}) \equiv 0 (\mathrm{mod}\ 2)$ will be denoted by $E_i^{(0)}(\tilde{\alpha})$ and the

subset of all $\tilde{\epsilon} \in E_i$ satisfying $(\tilde{\epsilon} \,|\, \tilde{\alpha}) \equiv 1 (\mathrm{mod}\ 2)$ by $E_i^{(1)}(\tilde{\alpha})$. As for $A_0 = \{\phi\}$ we set $E_i^{(0)}(\phi) = E_i$ and $E_i^{(1)}(\phi) = \emptyset$.

Before stating our main lemma, it will be in place to point out that any coordinate permutation is an injective, linear map from $\mathbb{Z}_2^n$ to itself preserving the weight of every vector in $\mathbb{Z}_2^n$. Hence we have $w(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}) = w(u'_{\alpha_1} \oplus \cdots \oplus u'_{\alpha_k})$ for every $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. This justifies our working with $\{u'_1, u'_2, \ldots, u'_m\}$ instead of $\{u_1, \ldots, u_m\}$ in the proof of the following

Lemma 3. *With the notation above, for any $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_k) \in A^0$ we have*

$$(A)\ w(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}) = \sum_{\tilde{\epsilon} \in E^{(0)}_{\alpha_k - 1}(\tilde{\alpha}^{(1)})} s_{\tilde{\epsilon}} + \sum_{\tilde{\epsilon} \in E^{(1)}_{\alpha_k - 1}(\tilde{\alpha}^{(1)})} (s_{\tilde{\epsilon}^{(\alpha_k - h)}} - s_{\tilde{\epsilon}^{(\alpha_k - h + 1}} - \cdots - s_{\tilde{\epsilon}})$$

where in the second sum $h = h_{\tilde{\epsilon}}$ is the index of the last non-zero entry of $\tilde{\epsilon}$ (observe that for $\tilde{\epsilon} \in E_i^{(1)}(\tilde{\alpha})$ there exists a non-zero entry);

$$(B)\ w(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}) - w(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_{k-1}}) = \sum_{\tilde{\epsilon} \in E^{(0)}_{\alpha_k - 1}(\tilde{\alpha}^{(1)})} s_{\tilde{\epsilon}} - \sum_{\tilde{\epsilon} \in E^{(1)}_{\alpha_k - 1}(\tilde{\alpha}^{(1)})} s_{\tilde{\epsilon}}$$

for $k \geq 2$, and

(C) the coefficient of $s_{\tilde{\epsilon}}$ with $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_{\alpha_k - 1}) \in E_{\alpha_k - 1}$ in (A) is equal to $(-1)^{(\tilde{\epsilon} \,|\, \tilde{\alpha}^{(1)})}$, where the agreement $(-1)^{\phi} = 1$ is taken into account for the case $k = 1$.

Proof. By the remark above we may observe $w(u'_{\alpha_1} \oplus \cdots \oplus u'_{\alpha_k})$ instead of $w(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k})$. We first prove the assertions for the case $k = 1$. In this case the sum inside w in (A) is u'_j for some j $(1 \leq j \leq m)$ and the righthand side is $\Sigma_{\tilde{\epsilon} \in E_{j-1}} s_{\tilde{\epsilon}}$, which being the sum of the lengths of the 1-segments in u'_j is equal to the weight $w(u'_j)$. This proves (A) for this case. (C) is also true, because of the agreement $(-1)^{\phi} = 1$. Next, assuming $k > 1$, to prove (A) (and (B)) we compute the contribution to weight $w(u'_{\alpha_1} \oplus \cdots \oplus u'_{\alpha_k})$ (or weight difference $w(u'_{\alpha_1} \oplus \cdots \oplus u'_{\alpha_k}) - w(u'_{\alpha_1} \oplus \cdots \oplus u'_{\alpha_{k-1}})$ respectively) done by the segment ${}^t(s'_{\tilde{\epsilon}}, s_{\tilde{\epsilon}})$ in u'_{α}, under the assumption $\tilde{\epsilon} = (\epsilon_1, \ldots, \epsilon_{\alpha_k - 1}) \in E_{\alpha_k - 1}$. Now by Lemma 2 the entries in the canonical form for $[\mathcal{U}]$, found on the row through any entry, say x, in the segment ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$, and to the left of x are exactly $\epsilon_1, \epsilon_2, \ldots, \epsilon_{\alpha_k - 1}$ appearing in this order. Hence the entries $\epsilon_{\alpha_1}, \ldots, \epsilon_{\alpha_{k-1}}$ are on the same row as x does and they are also in $u'_{\alpha_1}, \ldots, u'_{\alpha_{k-1}}$ respectively. Now if $\tilde{\epsilon} \in E^{(0)}_{\alpha_k - 1}(\tilde{\alpha}^{(1)})$, then the entry x makes a contribution of amount 1 to both weight and weight difference if $x = 1$, but none if $x = 0$. Thus in this case the total amount of the contribution to the weight and also

weight difference from the segment ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ is $s_{\tilde{\epsilon}}$. If, on the other hand $\tilde{\epsilon} \in E^{(0)}_{\alpha_k-1}(\tilde{\alpha}^{(1)})$, then the entry x makes a contribution of amount 1 to the weight and no contribution to the weight difference if $x = 0$, but none to the weight and -1 to the weight difference if $x = 1$. Hence, in this case, the total amount of contribution to the weight and the weight difference from the segment ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ is $s'_{\tilde{\epsilon}}$ and $(-s_{\tilde{\epsilon}})$, respectively. By Remark 2,

$$s'_{\tilde{\epsilon}} = s_{\tilde{\epsilon}^{(\alpha_k-h)}} - s_{\tilde{\epsilon}^{(\alpha_k-h-1)}} - \cdots - s_{\tilde{\epsilon}},$$

where h is the index of the last non-zero entry in $\tilde{\epsilon}$. Finally, summing up the contributions over all $\tilde{\epsilon} \in E_{\alpha_k-1}$ we obtain the formulas (A) and (B). To prove (C) it suffices just to look at the sign of each $s_{\tilde{\epsilon}}$ with $\tilde{\epsilon} \in E_{\alpha_k-1}$ in (A). □

Up to now we have always worked with an arbitrary ordered set in $\mathbb{Z}_2^n$. Now we return to our original aim, and assume that $\mathcal{B} = \{b_1, b_2, \ldots, b_m\}$ is an ordered basis of a binary (n, m)-code $\mathcal{C}$. In this circumstance all non-zero words in $\mathcal{C}$ can be indexed by the set A^0 by associating $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_j) \in A^0$ with the word $b_{\alpha_1} \oplus \cdots \oplus b_{\alpha_j} \in \mathcal{C}$, this association is bijective, since $\mathcal{B}$ is a basis for $\mathcal{C}$.

Now, we set up a system of linear equations which we call the system of weight equations for the binary code $\mathcal{C}$ with respect to the ordered basis $\mathcal{B}$. For this, we first apply Lemma 3 to the basis $\mathcal{B}$, and, using the same symbols $\{s_{\tilde{\epsilon}} \mid \tilde{\epsilon} \in E\}$ for the characteristics of $\mathcal{B}$, we obtain the relations (A) for $\mathcal{B}$, where the right sides must be replaced by $w(b_{\alpha_1} \oplus \cdots \oplus b_{\alpha_k})$ in accordance with the indices $(\alpha_1, \ldots, \alpha_k)$. Then, introducing the variable $X_{\tilde{\epsilon}}$ for each $\tilde{\epsilon} \in E$, and substituting $X_{\tilde{\epsilon}}$ in place of $s_{\tilde{\epsilon}}$ for every $\tilde{\epsilon} \in E$, we establish a system linear equations of the form:

$$\text{(D)} \quad \sum^{(1)} X_{\tilde{\epsilon}} + \sum^{(2)} \left(X_{\tilde{\epsilon}^{(\alpha_k-h)}} - \sum_{v=0}^{\alpha_k-h-1} X_{\epsilon^{(v)}} \right) = w(b_{\alpha_1} \oplus \cdots \oplus b_{\alpha_k}),$$

where, $\tilde{\alpha}$ being $(\alpha_1, \ldots, \alpha_k)$, the first sum $\Sigma^{(1)}$ is taken over all $\tilde{\epsilon} \in E^{(0)}_{\alpha_k-1}(\tilde{\alpha}^{(1)})$, and the second sum $\Sigma^{(2)}$ over all $\tilde{\epsilon} \in E^{(1)}_{\alpha_k-1}(\tilde{\alpha}^{(1)})$, and h denotes the index of the last non-zero entry of $\tilde{\epsilon} \in E^{(1)}_{\alpha_k-1}(\tilde{\alpha}^{(1)})$. Further we arrange the variables $X_{\tilde{\epsilon}}$ according to the semi-lexicographical order for the indices $\tilde{\epsilon} \in E$, and the equations by the reversed lexicographical order for the indices $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_k) \in A^0$. The system of $2^m - 1$ linear equations involving $2^m - 1$ variables thus obtained is called *the system of weight equations for the binary code $\mathcal{C}$ with respect to the ordered basis $\mathcal{B}$*. Putting the system in the form

$$\text{(E)} \qquad MX = W_{\mathcal{C}}$$

with the matrix of coefficients M, the vector X of variables $X_{\tilde{\epsilon}}$ (arranged by the semi-lexicographical order for the indices $\tilde{\epsilon} \in E$), and the vector $W_{\mathcal{C}}$ of the weights of non-zero words in $\mathcal{C}$ (arranged by the reversed lexicographical order for the indices $\tilde{\alpha} \in A^0$), we now examine the matrix of coefficients M.

Before proving the next theorem we put stress on the following

Remark 3. The left side of the system (E) depends only on the sets E and A^0, hence only on the dimension m, but does not depend on neither $\mathcal{C}$, nor $\mathcal{B}$. The only part in the system depending on these latter is $W_{\mathcal{C}}$ on the right side of (E) which yields the complete pattern of the weights of non-zero words in $\mathcal{C}$, and is arranged in the reversed lexicographical order depending on the order of the basis words in $\mathcal{B}$.

Theorem 1. *The matrix M of the coefficients in the system (E) for a binary (n, m)-code with respect to its ordered basis is independent from the choice of the code, or of the ordered basis. Furthermore it is of the form:*

$$M = \begin{bmatrix} H_1 & & & & \\ & \ddots & & & \bigcirc \\ & & H_{2^{r-1}} & & \\ & * & & \ddots & \\ & & & & H_{2^{m-1}} \end{bmatrix},$$

where $H_{2^{r-1}}$ $(r = 1, \ldots, m)$ is a normalized Hadamard matrix (see [2], p.204) of size 2^{r-1} whose $(\tilde{\alpha}, \tilde{\epsilon})$-entry is $(-1)^{(\tilde{\epsilon} \,|\, \tilde{\alpha}^{(1)})}$ for every pair $\tilde{\alpha} \in A^{(r)}$ and $\tilde{\epsilon} \in E_{r-1}$. Hence M is non-singular, so that the system (E) for a binary (n, m)-code $\mathcal{C}$ with respect to an ordered basis $\mathcal{B}$ has a unique solution $\{X_{\tilde{\epsilon}} = s_{\tilde{\epsilon}} \,|\, \tilde{\epsilon} \in E\}$ where $\{s_{\tilde{\epsilon}} \,|\, \tilde{\epsilon} \in E\}$ is the set of characteristics of $\mathcal{B}$.

Proof. The explicit form (D) for the equations in the system together with the ordering

of the variables $X_{\tilde{\epsilon}}$ ($\tilde{\epsilon} \in E$) implies that M is of the form

$$M = \begin{bmatrix} M_1 & & & & \\ & \ddots & & & \bigcirc \\ & & M_r & & \\ & * & & \ddots & \\ & & & & M_m \end{bmatrix}$$

where M_r is the matrix of the coefficients of $X_{\tilde{\epsilon}}$ with $\tilde{\epsilon} \in E_{r-1}$ in the equations indexed by $\tilde{\alpha} \in A^{(r)}$ for $r = 1, \ldots, m$. Hence to prove our assertion, it suffices to show that

(i) M_r is an Hadamard matrix of size 2^{r-1}, and

(ii) the $(\tilde{\alpha}, \tilde{\epsilon})$-entry of M_r is $(-1)^{(\tilde{\epsilon}\,|\,\tilde{\alpha}^{(1)})}$ for every pair $\tilde{\alpha} \in A^{(r)}$ and $\tilde{\epsilon} \in E_{r-1}$ for each r $(= 1, \ldots, m)$.

The size of M_r is 2^{r-1}, because the number of elements in E_{r-1} as well as that of elements in $A^{(r)}$ is 2^{r-1}. (ii) follows from Lemma 3 (C). So it only remains to show that M_r is an Hadamard matrix. Now the first row of M_r consists of the coefficients of $X_{\tilde{\epsilon}}$ ($\tilde{\epsilon} \in E_{r-1}$) in the equation indexed by the first element in $A^{(r)}$ which is (r). Since $(r)^{(1)}$, the first contraction of (r), is empty, we have

$$(-1)^{(\tilde{\epsilon}\,|\,(r)^{(1)})} = (-1)^{(\tilde{\epsilon}\,|\,\phi)} = (-1)^{\phi} = 1$$

for every $\tilde{\epsilon} \in E_{r-1}$. This shows that the first row of M_r consists only of 1. Next the first element in E_{r-1} is $\tilde{\epsilon}_0 = (0, \ldots, 0)$ of length $r-1$. Hence $(-1)^{(\tilde{\epsilon}_0\,|\,\tilde{\alpha}^{(1)})} = 1$ for every $\tilde{\alpha} \in A^{(r)}$. Thus the first column of M_r also consists only of 1. Because every entry in M_r is of the form $(-1)^{(\tilde{\epsilon}\,|\,\tilde{\alpha})}$, it is ± 1. Finally take any pair of elements $\tilde{\alpha}, \tilde{\beta} \in A^{(r)}$, and look at the $\tilde{\alpha}$-th and the $\tilde{\beta}$-th rows of M_r. Recalling that they are of the forms $\tilde{\alpha} = (\tilde{\alpha}^{(1)}, r)$ and $\tilde{\beta} = (\tilde{\beta}^{(1)}, r)$, compute the dot product of these rows. Then we see that it is equal to

$$\sum_{\tilde{\epsilon} \in E_{r-1}} (-1)^{(\tilde{\epsilon}\,|\,\tilde{\gamma})}$$

where $\tilde{\gamma} = (\gamma_1, \ldots, \gamma_k)$ stands for the symmetric difference of the sets $\tilde{\alpha}^{(1)}$ and $\tilde{\beta}^{(1)}$. If the symmetric difference $\tilde{\gamma}$ is not empty, i.e. if $\tilde{\alpha}^{(1)}$ and $\tilde{\beta}^{(1)}$ do not coincide with each

other, then the last sum is zero, because, in E_{r-1}, there are as many $\tilde{\epsilon}$ making

$$\sum_{v=1}^{k} \epsilon_{\gamma_v}$$

even as $\tilde{\epsilon}$ making it odd.

Note that this argument equally applies for the case where one of $\tilde{\alpha}^{(1)}$ and $\tilde{\beta}^{(1)}$ is empty. If, on the contrary, the symmetric difference $\tilde{\gamma}$ is empty, i.e. if $\tilde{\alpha} = \tilde{\beta}$, then the dot product is equal to 2^{r-1}. This completes the proof of the theorem. □

As an example of the application of Theorem 1 we have

Corollary. *(MacWilliams-Sloane [3], Exercise 33, pp.231-232). Let $\mathcal{C}$ be a binary (n, m)-code. Then an injective, linear map $\rho : \mathcal{C} \to \mathbb{Z}_2^n$ is induced by a coordinate permutation if and only if ρ preserves the weight of every word in $\mathcal{C}$.*

Proof. Assume that ρ is an injective, linear map from $\mathcal{C}$ into $\mathbb{Z}_2^n$ preserving the weight. Further let $\mathcal{B} = \{b_1, \ldots, b_m\}$ be an ordered basis of $\mathcal{C}$. Then $\mathcal{B}^\rho = \{b_1^\rho, \ldots, b_m^\rho\}$ is an ordered basis of the (n, m)-code $\mathcal{C}^\rho$. Since further ρ preserves the weight, we have

$$w(b_{\alpha_1}^\rho \oplus \cdots \oplus b_{\alpha_k}^\rho) = w(b_{\alpha_1} \oplus \cdots \oplus b_{\alpha_k})$$

for every $(\alpha_1, \ldots, \alpha_k) \in A^0$. Hence the system of weight equations for $\mathcal{C}^\rho$ with respect to $\mathcal{B}^\rho$ coincides with that for $\mathcal{C}$ with respect to $\mathcal{B}$. Then, by the uniqueness of the solution of the system, we see that $\mathcal{B}$ and $\mathcal{B}^\rho$ have the same canonical form. Hence there is a coordinate permutation π satisfying $b_i^\pi = b_i^\rho$ for $i = 1, \ldots, m$, so that $x^\pi = x^\rho$ for every $x \in \mathcal{C}$. The converse is trivial. □

Remark 4. By the same argument we can show the following: Binary (n, m)-codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent via coordinate permutations if and only if they have ordered basis $\mathcal{B}_1$ and $\mathcal{B}_2$ respectively such that the system of weight equations for $\mathcal{C}_1$ with respect to $\mathcal{B}_1$ coincides with that for $\mathcal{C}_2$ with respect to $\mathcal{B}_2$.

Exploiting the formula (B) in Lemma 3 we can complete now the description of the matrix M of coefficients in (E). For this purpose we first recall a well-known term of Linear Algebra: X being any square matrix of size N, by the t-th principal minor matrix of X for $1 \leq t \leq N$ we understand the $t \times t$ matrix obtained by deleting all rows and columns with indices $> t$ from X, and we use the notation X_t for it. The following theorem then inductively yields the shape of the matrix M.

Theorem 2. *For the matrix M of the coefficients in (E) the $(2^r - 1)$-th principal minor M_{2^r-1} is of the following form: $M_1 = [1]$ for $r = 1$, and*

$$M_{2^r-1} = \left[\begin{array}{c|c} M_{2^{r-1}-1} & \\ 0 \cdots 0 & \bigcirc \\ M_{2^{r-1}-1} & H_{2^{r-1}} \end{array}\right] \quad \textit{for} \quad r = 2, \ldots, m,$$

where $H_{2^{r-1}}$ is the Hadamard matrix of size 2^{r-1} described in Theorem 1, and the $(0, \ldots, 0)$ inserted between two $M_{2^{r-1}-1}$ denotes the row 0-vector of length $2^{r-1} - 1$.

Proof. First $M_1 = [1]$ for $r = 1$, because the first equation in the system is $\mathcal{X}_\phi = w(b_1)$ where b_1 is the first basis ward in the ordered basis $\mathcal{B} = \{b_1, \ldots, b_m\}$ of the (n, m)-code $\mathcal{C}$ in question. Next, assume that $r \geq 2$. Observe that M_{2^r-1} is the matrix of coefficients of

$$X_{\tilde{\epsilon}} \quad \left(\tilde{\epsilon} \in \bigcup_{i=0}^{r-1} E_i\right)$$

in the equations indexed by

$$\tilde{\alpha} \in \bigcup_{s \leq r} A^{(s)}.$$

Looking at an equation indexed by $\tilde{\beta} \in A^{(s)}$ with $s \leq r - 1$, from the explicit form (D) we see that this equation does not contain any variables with index in E_{r-1}, which shows that the submatrix of M_{2^r-1} consisting of the first $2^{r-1} - 1$ rows is of the form $[M_{2^{r-1}-1}, 0]$ where 0 denotes the $(2^{r-1} - 1) \times 2^{r-1}$ zero matrix: The next row of the matrix corresponds to $\tilde{\alpha} = (r)$ and hence to the equation

$$w(b_r) = \sum_{\tilde{\epsilon} \in E_{r-1}} X_{\tilde{\epsilon}}$$

which is in the desired form. The remaining rows are indexed by $\tilde{\alpha} = (\tilde{\beta}, v)$ with

$$\tilde{\beta} \in \bigcup_{s \leq r-1} A^{(s)}.$$

Since the ordering of these indices is exactly the same as the corresponding $\tilde{\beta} = \tilde{\alpha}^{(1)}$'s, the formula (B) of Lemma 3 can be used to see that the coefficient of $\mathcal{X}_{\tilde{\epsilon}}$ with

$$\tilde{\epsilon} \in \bigcup_{i=0}^{r-2} E_i$$

in the equation indexed by $\tilde{\alpha}$ is equal to its coefficient in the equation indexed by $\tilde{\alpha}^{(1)}$. On the other hand we have seen already in Theorem 1, that the submatrix of M_{2^r-1} corresponding to the rows indexed by $A^{(r)}$ and columns indexed by E_{r-1} is the Hadamard matrix $H_{2^{r-1}}$. This completes the proof. □

From the explicit form of M_{2^r-1} we can compute its inverse.

Corollary. *For $r = 1, \ldots, m$, the inverse $M^{-1}_{2^r-1}$ of M_{2^r-1} is given by: $M_1^{-1} = [1]$ for $r = 1$, and*

$$M^{-1}_{2^r-1} = \begin{bmatrix} M^{-1}_{2^{r-1}-1} & 0 \\ -(1/2^{r-1})({}^tH_{2^{r-1}})^- & (1/2^{r-1})\,{}^tH_{2^{r-1}} \end{bmatrix}$$

for $r = 2, \ldots, m$, where $({}^tH_{2^{r-1}})^-$ denotes the $2^{r-1} \times (2^{r-1} - 1)$ matrix obtained by deleting the first column from ${}^tH_{2^{r-1}}$.

Remark 5. Using M^{-1} we can express each of the characteristics of an ordered basis of an (n, m)-code $\mathcal{C}$ in terms of the weights of non-zero words in $\mathcal{C}$. This is formulated in a somewhat different form in the next section.

4. Application

In this section we take up a question closely related to the facts obtained in the previous sections. We namely ask the following: Under what (numerical) conditions on

a sequence Ω of $2^m - 1$ positive integers, does Ω become the complete pattern of the weights of non-zero words in a binary (n, m)-code? In order to give a partial answer to this question, we introduce the following concept: A sequence $\{w_{\tilde{\alpha}} \mid \tilde{\alpha} \in A^0\}$ of positive integers indexed by the set A^0 is called a *well-arranged weight pattern of a binary (n, m)-code* if there is a binary (n, m)-code with an ordered basis $\{b_1, \ldots, b_m\}$ satisfying

$$w_{\tilde{\alpha}} = w(b_{\alpha_1} \oplus \cdots \oplus b_{\alpha_k}) \quad \text{for every} \quad \tilde{\alpha} = (\alpha_1, \ldots, \alpha_k) \in A^0.$$

Theorem 3. *Let $\Omega = \{w_{\tilde{\alpha}} \mid \tilde{\alpha} \in A^0\}$ be a sequence of positive integers indexed by the set A^0. Then Ω is a well-arranged weight pattern of a binary (n, m)-code if and only if the following conditions are satisfied:*

(A′) For $r = 1, \ldots, m$, and for every $\tilde{\epsilon} \in E_{r-1}$, the sum

$$w_{(r)} + \sum_{\tilde{\alpha} \in A^{(r)^-}} (-1)^{(\tilde{\epsilon} \mid \tilde{\alpha})} (w_{(\tilde{\alpha}, r)} - w_{\tilde{\alpha}})$$

is $2^{r-1} t_{\tilde{\epsilon}}$ with a non-negative integer $t_{\tilde{\epsilon}}$ not exceeding n, where

$$A^{(r)^-} = \bigcup_{s<r} A(s)$$

(note that if $r = 1$, then $\tilde{\epsilon} = \phi$, and the inside of the summation is empty);

(B′) (i) $\sum_{v=0}^{m-1} t_{\tilde{\epsilon}^{(v)}} \leq n$, if $\tilde{\epsilon} = (0, \ldots, 0) \in E_{m-1}$ consists only of 0's, and

(ii) $t_{\tilde{\epsilon}^{(r-h)}} - \sum_{v=0}^{r-h-1} t_{\tilde{\epsilon}^{(v)}} \geq 0$, if $\tilde{\epsilon} \in E_{r-1}$ has the last non-zero entry at the h-th position.

Proof. Assume first that Ω is well-arranged. Then there is a binary (n, m)-code $\mathcal{C}$ with an ordered basis $\mathcal{B} = \{b_1, \ldots, b_m\}$ satisfying $w_{\tilde{\alpha}} = w(b_{\alpha_1} \oplus \cdots \oplus b_{\alpha_k})$ for every $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_k) \in A^0$. The unique solution of the system $MX = W_{\mathcal{C}} = {}^t(\ldots, w_{\tilde{\alpha}}, \ldots)$ is the set of characteristics $\{s_{\tilde{\epsilon}} \mid \tilde{\epsilon} \in E\}$ of $\mathcal{B}$. Using the explicit form of M^{-1} we can write down each of the characteristics, in fact we find $s_{\tilde{\epsilon}} = t_{\tilde{\epsilon}}$ for every $\tilde{\epsilon} \in E$. Hence the condition (A′) must be satisfied. The conditions listed in (B′) say nothing but the non-negativeness of $s'_{\tilde{\epsilon}}$ ($\tilde{\epsilon} \in E$) expressed by the formulae in Remark 1. If conversely

Ω satisfies the conditions (A′) and (B′), then the system $MX = {}^t(\ldots, w_{\tilde{\alpha}}, \ldots)$ has the unique solution $\{t_{\tilde{\epsilon}} \mid \tilde{\epsilon} \in E\}$, because

$$ {}^t(\ldots, t_{\tilde{\epsilon}}, \ldots) = M^{-1}[\ {}^t(\ldots, w_{\tilde{\alpha}}, \ldots)]. $$

Now, for each $\tilde{\epsilon} \in E_{i-1}$ $(i = 1, \ldots, m)$, we define $t'_{\tilde{\epsilon}}$ as follows: If $\tilde{\epsilon} = (0, \ldots, 0)$ consists only of 0's,

$$ t'_{\tilde{\epsilon}} = n - \sum_{v=0}^{i-1} t_{\tilde{\epsilon}^{(v)}}, $$

hence, in particular, for $i = 1$, $t'_{\phi} = n - t_{\phi} = n - w_{(1)}$; if $\tilde{\epsilon}$ has the last non-zero entry at the h-th position, then

$$ t'_{\tilde{\epsilon}} = t_{\tilde{\epsilon}^{(i-h)-}} \sum_{v=0}^{i-h-1} t_{\tilde{\epsilon}^{(v)}}. $$

Then (i) and (ii) in (B′) ensure that $t'_{\tilde{\epsilon}}$ is non-negative for each $\tilde{\epsilon} \in E$. Furthermore it is easy to check that $t'_{\tilde{\epsilon}} + t_{\tilde{\epsilon}} = t'_{\tilde{\epsilon}^{(1)}}$, or $= t_{\tilde{\epsilon}^{(1)}}$ according as the last entry of $\tilde{\epsilon}$ is 0 or 1. Now taking a (column) 0-vector $T'_{\tilde{\epsilon}}$ of length $t'_{\tilde{\epsilon}}$ and a (column) 1-vector $T_{\tilde{\epsilon}}$ of length $t_{\tilde{\epsilon}}$ for each $\tilde{\epsilon} \in E_{i-1}$, further putting $T'_{\tilde{\epsilon}}$ above $T_{\tilde{\epsilon}}$ to obtain the (column) vector ${}^t(T'_{\tilde{\epsilon}}, T_{\tilde{\epsilon}})$, and finally arranging these vectors vertically in the lexicographical order on E_{i-1}, we set up a (column) vector u_i for each i $(= 1, \ldots, m)$. The relation satisfied by $t'_{\tilde{\epsilon}}$ and $t_{\tilde{\epsilon}}$ mentioned above then implies firstly that the segment ${}^t(T'_{\tilde{\epsilon}}, T_{\tilde{\epsilon}})$ (in u_i) exactly involves either the coordinate places involved in $T'_{\tilde{\epsilon}}$ (in u_{i-1}), or those involved in $T_{\tilde{\epsilon}}$ (in u_{i-1}) according as the last non-zero entry of $\tilde{\epsilon}$ is 0 or 1, secondly that the length of each u_i $(i = 1, \ldots, m)$ is n. This shows that $\{t_{\tilde{\epsilon}} \mid \tilde{\epsilon} \in E\}$ is the set of characteristics of the ordered set $\{u_1, \ldots, u_m\}$ in $\mathbb{Z}_2^n$ (see Lemma 1). Then, by Lemma 3, we have

$$ M[\ {}^t(\ldots, t_{\tilde{\epsilon}}, \ldots)] = {}^t(\ldots, w(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}), \ldots). $$

Now comparing this with

$$ M[\ {}^t(\ldots, t_{\tilde{\epsilon}}, \ldots)] = {}^t(\ldots, w_{\tilde{\epsilon}}, \ldots) $$

above, we obtain

$$ w_{\tilde{\alpha}} = w(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}) \quad \text{for every} \quad \tilde{\alpha} = (\alpha_1, \ldots, \alpha_k) \in A^0. $$

Since each $w_{\tilde{\alpha}}$ is positive by assumption, we conclude that $\{u_1, \ldots, u_m\}$ is linearly independent. Thus we have shown that Ω is a well-arranged weight pattern for the (n, m)-code

spanned by $\{u_1, \ldots, u_m\}$. □

Remark 6. Although the facts obtained above seem rather clumsy and inpractical, yet they turn out to be useful for some special cases. As an example, they are applied to classify the binary codes admitting two distinct values for the weights of non-zero words (see [1]).

5. Appendix

In this note we have always been stuck in the case of a fixed ordered basis of a binary code. Some facts about the connection between data for two ordered basis, however, can be easily derived. For example, the connection between the sets of characteristics of two ordered basis $\mathcal{B}$ and $\mathcal{B}'$ in a binary (n, m)-code $\mathcal{C}$ is obtained in the following way. Being $\mathcal{B} = \{b_1, \ldots, b_m\}$ and $\mathcal{B}' = \{b'_1, \ldots, b'_m\}$, the map $b_i \mapsto b'_i \quad (i = 1, \ldots, m)$ induces a permutation ρ on the weight pattern W_C. Let P be a permutation matrix of size $2^m - 1$ affording this permutation on $W_C := PW_C = W_C^\rho$. Then the set of characteristics $\{t_{\tilde{\epsilon}} \,|\, \tilde{\epsilon} \in E\}$ of $\mathcal{B}'$ is obtained from ${}^t(\ldots, t_{\tilde{\epsilon}}, \ldots) = (M^{-1}PM)\ {}^t(\ldots, s_{\tilde{\epsilon}}, \ldots)$ where $\{s_{\tilde{\epsilon}} \,|\, \tilde{\epsilon} \in E\}$ is the set of characteristics of $\mathcal{B}$.

After the authors had finished this note, Haluk Oral, Boğaziçi University, has kindly drawn authors' attention to the lecture note [4] in which there are some arguments similar to, yet rather different from ours. The difference is essentially based on the choices of the orderings on the index sets. The authors thank H. Oral for his assistance during their preparation of this note.

References

[1] E. Akyıldız, İ.Ş. Güloğlu and M. İkeda: Bent Functions and Related Linear Codes, Preprint, Marmara Research Center, TÜBİTAK, 1994.

[2] M. Hall: Combinatorial Theory, John Wiley, 1967.

[3] F.J. MacWilliams and N.J. Sloane: The Theory of Error-correcting Codes, North-Holland, 1977.

[4] P.C. van Oorschot and S.A. Vanstone: An Introduction to Error-Correcting Codes with Applications, University of Waterloo, 1989.

Ersan AKYILDIZ & İsmail Ş. GÜLOĞLU
Department of Mathematics
Middle East Technical University
06531 Ankara - TURKEY
Masatoshi İKEDA
Department of Mathematics
Marmara Research Center
Gebze, Kocaeli - TURKEY

Received 03.01.1997