Tr. J. of Mathematics
21 (1997) , 1 – 14.


# WEIGHT EQUATIONS FOR BINARY LINEAR CODES AND THEIR APPLICATIONS*

*Ersan Akyıldız, İsmail Ş. Güloğlu & Masatoshi İkeda*

**Abstract**

Some combinatorial problems concerning binary vector spaces are solved by applying the techniques developed in [1]. These illustrate that they are effective tools for such purposes.

## 1. Introduction

In the previous paper [1], we have introduced certain invariants characterizing binary linear codes. The aim of this note is to illustrate how they can be applied to some combinatorial problems concerning partitions of the binary vector space. We first resume some facts from [1], then, after introducing the linear code determined by a given binary vector space, we transform the formulae given in the previous section into simplier forms more adequate for our purpose.

Throughout the paper we keep the notations as: $V$ stands for a finite dimensional binary vector space (i.e. a finite dimensional vector space over $\mathbb{Z}_2$), and for any subset $X$ of $V, X'$ and $|X|$ denote complementary set of $X$ in $V$ and the number of elements of $X$ respectively. In the last two sections, we prove the following

**Theorem 1.** *Let $V$ be a binary vector space of dimension $n \neq 2$. Then there is no subset $A$ of $V$ satisfying the condition that, for any hyperplane $H$ of $V$ (i.e. any subspace of codimension 1), $|A \cap H| = |A' \cap H|$ holds.*

**Theorem 2.** *Let $V$ be a binary vector space of dimension $n \geq 2$. If there is a subset $A$ of $V$ such that, for any hyperplane $H$ of $V$, either $|A \cap H| = |A' \cap H|$, or $|A \cap H'| = |A' \cap H'|$ holds, then the dimension $n$ of $V$ is necessarily even, and the characteristic function of $A$ is a bent function on $V$. The converse of the statement above is also true.*

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

## 2. Facts Borrowed From [1]

Our proof of the theorem above heavily relies on the facts obtained in [1], so, for reader's convenience, some of these facts are summarized in this section.

Throughout this note we always work in $V = Z_2^n$ with $n > 1$ which is assumed to be the space of all row vectors of length $n$. In accord with the discussions in the following sections, we assume that every linear code of block length $N$ coming up in our discussion is a subspace of ${}^t(Z_2^N)$, the space of all column vectors of length $N$. In order to distinguish the coodinate places of the row vector from that of the column vector, we temporarily call the former the ordinate place, and the latter the coordinate place. Accordingly we call a permutation interchanging the ordinate places of all row vectors in $Z_2^n$ an ordinate permutation, while a permutation acting on the coordinate places of all vectors in ${}^t(Z_2^N)$ a coordinate permutation.

*A* portion of a (column) vector $v$ consisting of some consecutive entries of $v$ is called a segment of $v$, where the empty segment is allowed. *A* segment $S$ of a (column) vector $v$ is said to be a 0-segment if it is either empty, or consists only of 0's; $S$ is called a 1-segment if it is either empty, or consists only of 1's. Two segments of $v$ are said to be disjoint if they do not contain any entry of $v$ in common. *A* division of $v$ into mutually disjoint segments is called a partition of $v$. Now let $\{v_1, \cdots, v_r\}$ be a collection of column vectors not necessarily of the same length. Then, in abuse of notation, ${}^t(v_1, \cdots, v_r)$ stands for the column vector

$$\begin{bmatrix} v_1 \\ \vdots \\ v_r \end{bmatrix}.$$

As usual the weight of a vector $v$ is denoted by $w(v)$.

Here are the facts taken from [1] which will be used in the following sections.

**Fact 1.** *(Lemma 1, [1]. Let $\{u_1, \cdots, u_m\}$ be an ordered set of (not necessarily linearly independent) vectors chosen from ${}^t(Z_2^N)$ for some $N$. Then there is a coordinate permutation $\pi$ such that the matrix $[u_1^\pi, \cdots, u_m^\pi]$ satisfies the following conditions: For each $i(= 1, \cdots, m)$,*

*(1) the $i-th$ column $u_i^\pi$ is partitions into the form ${}^t(\cdots, S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}}, \cdots)$ with 0-segments $S'_{\tilde{\epsilon}}$ and 1-segments $S_{\tilde{\epsilon}}$ where $\tilde{\epsilon}$ ranges over all elements in $E_{i-1}$ which is, by definition, the set of all $(0,1)$-sequences of length $i-1$ if $i \geq 2$, and $E_0 = \{\phi\}$;*

*(2) if $i \geq 2$, then, for every $\tilde{\epsilon} \in E_{i-1}$ the coordinate places involved in the segment ${}^t(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ of the $i-th$ column $u_i^\pi$ are either exactly those involved in the segment $S'_{\tilde{\epsilon}(1)}$ or exactly those involved in $S_{\tilde{\epsilon}(1)}$ of the $(i-1)-th$ column $u_{i-1}^\pi$, according as the last entry of $\tilde{\epsilon}$ is 0 or 1, where $\tilde{\epsilon}(1)$ denotes the element in $E_{i-1}$ obtained from $\tilde{\epsilon}$ by deleting its last entry (consequently, $s'_{\tilde{\epsilon}}$ and $s_{\tilde{\epsilon}}$ being the lengths of $S'_{\tilde{\epsilon}}$ and $S_{\tilde{\epsilon}}$ respectively, if $i \geq 2$. either*

$$s'_{\tilde{\epsilon}} + s_{\tilde{\epsilon}} = s'_{\tilde{\epsilon}(1)}, \quad or \quad s'_{\tilde{\epsilon}} + s_{\tilde{\epsilon}} = s_{\tilde{\epsilon}(1)}$$

*according as the last entry of* $\tilde{\epsilon}$ *is* $0$ *or* $1$, *while, for* $i = 1$, $s'_{\phi} + s_{\phi} = N$, *and* $s_{\phi} = w(u_1)$;

*(3) the segments* ${}^{t}(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ *with* $\tilde{\epsilon} \in E_{i-1}$ *appearing in the partition of the* $i-th$ *column* $u_i^{\pi}$ *are arranged in the lexicographical order on* $E_{i-1}$ *assuming* $0 < 1$.

**Remark to Fact 1.** (Remark 1, [1]). By (2) in Fact 1 above,

$$s'_{\tilde{\epsilon}} = s'_{\tilde{\epsilon}(1)} - s_{\tilde{\epsilon}}, \quad or \quad s'_{\tilde{\epsilon}} = s_{\tilde{\epsilon}(1)} - s_{\tilde{\epsilon}}$$

according as the last entry of $\tilde{\epsilon}$ is $0$ or $1$, for every $\tilde{\epsilon} \in E_{i-1}$ with $i \geq 2$. Hence, by induction, we obtain the following: If

$$\tilde{\epsilon} = (\epsilon_1, \cdots, \epsilon_{i-1}) \in E_{i-1}$$

with $i \geq 2$ has the last non-zero entry at the $h-th$ position with $h \geq 1$, then

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

where $\tilde{\epsilon}(v)$ is the $(0,1)$ - sequence obtained from $\tilde{\epsilon}$ by deleting its last $v$ entries.

The matrix $u^{\pi} = [u_1^{\pi}, \cdots, u_m^{\pi}]$ satisfying the conditions (1) through (3) in Fact 1 is called the canonical from of the matrix $U = [u_1, \cdots, u_m]$. Its shape does not depend on the choice of the coordinate permutation $\pi$ used for its construction. This is seen from the following fact characterizing the indices of the segments.

**Fact 2.** *(Lemma 2, [1]). Keeping the same notations as in Fact* 1, *let* ${}^{t}(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ *be a segment in the* $i-th$ *column of the canonical from with* $i \geq 2$, *where* $\tilde{\epsilon} = (\epsilon_1, \cdots, \epsilon_{i-1}) \in E_{i-1}$. *If the segment is not empty, then, for any entry* $x$ *in the segment, the entries in the canonical from located on the row through* $x$, *and to the left of* $x$ *are exactly* $\{\epsilon_1, \cdots, \epsilon_{i-1}\}$ *including the order. Conversely, for any entry* $x$ *in the canonical from, if the entries on the row through* $x$, *and to the left of* $x$ *are* $\{\epsilon_1, \cdots, \epsilon_{i-1}\}$ *in this order, then* $x$ *is in the segment* ${}^{t}(S'_{\tilde{\epsilon}}, S_{\tilde{\epsilon}})$ *of the* $i-th$ *column of the canonical from, where* $\tilde{\epsilon} = (\epsilon_1, \cdots, \epsilon_{i-1})$.

The set

$$\left\{ s_{\tilde{\epsilon}} | \tilde{\epsilon} \in \bigcup_{i=1}^{m} E_{i-1} \right\}$$

is called the set of characteristics of the matrix $U$ (or of the ordered set $\{u_1, \cdots, u_m\}$), likewise the set

$$\left\{ s'_{\tilde{\epsilon}} | \tilde{\epsilon} \in \bigcup_{i=1}^{m} E_{i-1} \right\}$$

the set of co-characteristics of $U$, or of the ordered set $\{u_1, \cdots, u_m\}$. In most applications, however, we use the subset consisting of characteristics with indices in $E_{m-1}$. This will be called the set of characteristics belonging to the last column of $U$. Similarly the set of co-characteristics with indices in $E_{m-1}$ will be called the set of co-characteristics belonging to the last column of $U$.

Next let

$$A = \bigcup_{j=0}^{m} A_j,$$

where $A_0 = \{\phi\}$, and, for $j \geq 1, A_j$ is the set of all $j-$tuples $(\alpha_1, \cdots, \alpha_j)$ of integers subject to the condition $1 \leq \alpha_1 < \cdots < \alpha_j \leq m$. For any $\tilde{\alpha} = (\alpha_1, \cdots, \alpha_j)$ with $j \geq 1, \tilde{\alpha}^{(1)}$ denotes the element in $A_{j-1}$ obtained from $\tilde{\alpha}$ by omitting its last entry.

For any $\tilde{\alpha} = (\alpha_1, \cdots, \alpha_j) \in A_j$, let $(\tilde{\epsilon}|\tilde{\alpha})$ denote the sum $\sum_{v=1}^{i} \epsilon_{\alpha_v}$, where $\tilde{\epsilon} = (\epsilon_1, \cdots, \epsilon_i) \in E_i$ with $i \geq j \geq 1$. As for the case $j = 0, (\tilde{\epsilon}|\phi)$ is understood to be 0 for every $\tilde{\epsilon}$. Using the notations introduced above, the main formulae we need are given in the following:

**Fact 3.** *(Lemma3, (A) and (B), [1]). Keeping the notations above, for any* $\tilde{\alpha} = (\alpha_1, \cdots, \alpha_k) \in \bigcup_{j=1}^{m} A_j$, *we have*

$$(A)\ w(u_{\alpha 1} \oplus \cdots \oplus u_{\alpha k}) = \sum_{\substack{\tilde{\epsilon} \in E_{\alpha_k - 1} \\ (\tilde{\epsilon}|\tilde{\alpha}(1)) \equiv 0(2)}} s_{\tilde{\epsilon}} + \sum_{\substack{\tilde{\epsilon} \in E_{\alpha_k - 1} \\ (\tilde{\epsilon}|\tilde{\alpha}(1)) \equiv 1(2)}} (s_{\tilde{\epsilon}(\alpha_k - h)} - s_{\tilde{\epsilon}(\alpha_k - h - 1)} - \cdots - s_{\tilde{\alpha})}$$

where in the second sun $h = h_{\tilde{\epsilon}}$ denotes the index of the last non-zero entry of $\tilde{\epsilon}$ (observe that, if $(\tilde{\epsilon}|\tilde{\alpha}(1)) \equiv 1 \mod 2$ for an $\tilde{\alpha}(1) \neq \phi$, there is non-zero entry in $\tilde{\epsilon}$, while, if $\tilde{\alpha}(1) = \phi (i.e.\, \text{if}\, k = 1)$, then the second sum is the empty sum, because $(\tilde{\epsilon}|\phi) = 0$ by definition) ;

$$(B)\ w(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}) - \omega(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_{k-1}}) = \sum_{\substack{\tilde{\epsilon} \in E_{\alpha_k - 1} \\ (\tilde{\epsilon}|\tilde{\alpha}(1)) \equiv 0(2)}} s_{\tilde{\epsilon}} - \sum_{\substack{\tilde{\epsilon} \in E_{\alpha_k - 1} \\ (\tilde{\epsilon}|\tilde{\alpha}(1)) \equiv 1(2)}} s_{\tilde{\epsilon}}$$

*(observe that, if* $k = 1$, *then* $\tilde{\alpha}(1) = \phi$, *hence* $(\tilde{\epsilon}|\tilde{\alpha}(1)) = 0$ *by definition, so that the second sum is empty).*

As one can see directly from the proof of $(A)$ in [1], or from the remark to Fact 1 on the foregoing page, the formula $(A)$ can be rewritten into the following form.

**Fact 4.** *Under the same assumptions as above, for every* $\tilde{\alpha} = (\alpha_1, \cdots, \alpha_k) \in \bigcup_{j=1}^{m} A_j$, *we have*

$$(A')\ w(u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}) = \sum_{\substack{\tilde{\epsilon} \in E_{\alpha_k - 1} \\ (\tilde{\epsilon}|\tilde{\alpha}(1)) \equiv 0(2)}} s_{\tilde{\epsilon}} + \sum_{\substack{\tilde{\epsilon} \in E_{\alpha_k - 1} \\ (\tilde{\epsilon}|\tilde{\alpha}(1)) \equiv 1(2)}} s'_{\tilde{\epsilon}}.$$

**Remark to Fact 4.** In particular, if $\alpha_k = m$, $s_{\tilde{\epsilon}}$ and $s'_{\tilde{\epsilon}}$ appering in $(A')$ range over all characteristics and co-characteristics belonging to the last column of $U$.

Before concluding this section ve just mention the following ([1]).

**Fact 5.** *Let* $C$ *be a binary* $(n, m)$*-code. Then an injective linear map* $\rho : C \to \mathbb{Z}_2^n$ *is induced by a coordinate permutation if and omly if* $\rho$ *preserves the weight of every code-word in* $C$.

## 3. Linear Code Determined by a Binary Vector Space

Let $V$ be a binary vector space of dimension $n$, and $S$ a non-empty subset of $V$, where the vectors in $V$ are assumed to be row vectors of length $n$. Look at the array having vectors in $S$ as rows to obtain an $|S| \times n$ matrix $M_S$. $M_S$ is uniquely determined up to coordinate permutations. Further, if necessary, $M_S$ may be assumed to be in its cononical from. Now let $\{u_1, ..., u_n\}$ be the columns of the matrix $M_S$, then they span a linear code $\mathcal{L}(S)$ of block length $|S|$. If furthermore $S$ contains $n$ linearly independent vectors, $\mathcal{L}(S)$ is an $(|S|, n)$-code. The linear code $\mathcal{L}(S)$ is uniquely determined by $S$ up to equivalence, because $M_S$ is unique up to coordinate permutations. The code $\mathcal{L}(S)$ will be called the linear code determined by the set $S$.

Now let $A$ be a subset of $V$, and $B$ its complementary set in $V$, and let $\{u_1, \cdots, u_n\}$ and $\{u'_1, \cdots, u'_n\}$ be the columns of $M_A$ and $M_B$ respectively. We further assume that $A$ contains a basis of $V$. The linear codes $\mathcal{L}(A)$ and $\mathcal{L}(B)$ will be denoted by $\mathcal{A}_n$ and $\mathcal{B}_n$ respectively. Now, for any increasing sequence $1 \leq \alpha_1 < \cdots < \alpha_k \leq n$, $v = u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}$ is a code-word in $\mathcal{A}_n$, where, for the empty sequence, the resulting code-word is understood to be the zero of $\mathcal{A}_n$. Corresponding to the code-word $v$, there is a well-defined code-word

$$v' = u'_{\alpha_1} \oplus \cdots \oplus u'_{\alpha_k} \in \mathcal{B}_n,$$

and the map $h_{A,B} : v \mapsto v'$ for $v \in \mathcal{A}_n$ gives rise to homomorphisms from $\mathcal{A}_n$ to $\mathcal{B}_n$.

In the foregoing section we have introduced a sort of pairing $(\tilde{\epsilon}|\tilde{\alpha})$ for $\tilde{\epsilon} \in E_{i-1}$ and $\tilde{\alpha} \in A_j$ under the assumption $i - 1 \geq j \geq 0$. In particular, for $\tilde{\epsilon} \in E_{n-1}$, the pairing is defined for all

$$\tilde{\alpha} \in \bigcup_{j=0}^{n-1} A_j.$$

Let $\mathcal{A}_{n-1}$ be the subcode of $\mathcal{A}_n$ spanned by $\{u_i| = 1, \cdots, n-1\}$. Then, since the set is linearly independent, the code-words in $\mathcal{A}_{n-1}$ bijectively correspond to the elements in

$$\bigcup_{j=0}^{n-1} A_j : \tilde{\alpha} = (\alpha_1, \cdots, \alpha_k) \mapsto v = u_{\alpha_1} \oplus \cdots \oplus u_{\alpha_k}.$$

Note here that $\phi \mapsto 0$ by the remark above. Hence we may use the symbol $(\tilde{\epsilon}|v)$ instead of $(\tilde{\epsilon}|\tilde{\alpha})$ provided that $\tilde{\alpha}$ and $v$ correspond to each other under the map above. Note here that $(\tilde{\epsilon}|0) = (\tilde{\epsilon}|\phi) = 0$ according to the definition of the second symbol. Now it is easy to check that

$$(\tilde{\epsilon}|v_1 \oplus v_2) = (\tilde{\epsilon}|v_1) + (\tilde{\epsilon}|v_2)(\mathrm{mod}2),$$

so that $(-1)^{(\tilde{\epsilon}|v)}$ is a character of the additive group $\mathcal{A}_{n-1}$. Furthermore, under the correspondence $\tilde{\epsilon} \mapsto (-1)^{(\tilde{\epsilon}|*)}$, $E_{n-1}$ may be viewed as the character group of $\mathcal{A}_{n-1}$. In particular, note that the element $\tilde{0} = (0, \cdots, 0)(= (n-1) -$ times $0)$ of $E_{n-1}$, and only this corresponds to the unit character of $\mathcal{A}_{n-1}$.

Now let $\{s_{\tilde{\epsilon}}|\tilde{\epsilon} \in E_{n-1}\}$ and $\{s'_{\tilde{\eta}}|\tilde{\eta} \in E_{n-1}\}$ be the sets of characteristics and of co-characteristics belonging to the last column of $M_A$, further let

$$\{t_{\tilde{\epsilon}'}|\tilde{\epsilon}' \in E_{n-1}\} \text{ and } \{t'_{\tilde{\eta}'}|\tilde{\eta}' \in E_{n-1}\}$$

be those for the last column of $M_B$.

**Lemma 3.** *$s_{\tilde{\epsilon}}$ is either 1, or 0 for each $\tilde{\epsilon} \in E_{n-1}$. The same holds for $s'\tilde{\eta}', t_{\tilde{\epsilon}'}$, and $t'_{\tilde{\eta}'}$ with $\tilde{\eta}, \tilde{\epsilon}' \in E_{n-1}$.*

**Proof.** The proof of the assertion is essentially the same for every case. Hence only the first one will be proved. Assume that $s_{\tilde{\epsilon}} > 1$ for an $\tilde{\epsilon} \in E_{n-1}$, and let $x$ and $x'$ be the entries of the segment $S_{\tilde{\epsilon}}$ at two distinct coordinate places in it. First note that $x$ and $x'$ are both 1. Furthermore, by fact 2 in the foregoing section, the entries of $M_A$ located on the row throgh $x$ (or $x'$), and to the left of $x$ (or of $x'$) are exactly $\{\epsilon_1 \cdots \epsilon_{n-1}\}$ in this order, where $\tilde{\epsilon} = (\epsilon_1, \cdots, \epsilon_{n-1})$. Hence the rows of $M_A$ through $x$ and $x'$ respectively coincide with each other. This, however, is impossible, because otherwise the set $A$ would contain the same vector twice. This completes the proof. □

Let

$$\Gamma = \{\tilde{\epsilon} \in E_{n-1}|s_{\tilde{\epsilon}} = 1\}, \Delta = \{\tilde{\eta} \in E_{n-1} s'_{\tilde{\eta}} = 1\}, \Gamma' = \{\tilde{\epsilon}' \in E_{n-1}|t_{\tilde{\epsilon}'} = 1\},$$

and

$$\Delta' = \{\tilde{\eta}' \in E_{n-1} | t'_{\tilde{\eta}'} = 1\}.$$

Then

**Lemma 4.** *$\Gamma$ and $\Gamma'$ are pairwise disjoint, and $\Gamma \cup \Gamma' = E_{n-1}$. Furthermore $|\Gamma| + |\Delta| = |A|$ and $|\Gamma'| + |\Delta'| = |B|$.*

**Proof.** If $\tilde{\epsilon} \in \Gamma \cap \Gamma'$, then the segment $S_{\tilde{\epsilon}}$ in the last column of $M_A$ and the segment $T_{\tilde{\epsilon}}$ in the last column of $M_B$ are both non-empty. Let $x$ be an entry in $S_{\tilde{\epsilon}}$, and $y$ that in $T_{\tilde{\epsilon}}$. First note that $x$ and $y$ both are 1. Then, applying the same argument as in the proof of Lemma 3, we come to the conclusion that the sets $A$ and $B$ contain a vector in common. This contradiction proves the disjointness of $\Gamma$ and $\Gamma'$. The same argument can apply for $\Delta, \Delta'$. Now $|\Gamma|$ is the number of the rows of $M_A$ with tail-end 1 (i.e. with the last coordinate 1), and $|\Delta|$ is that of rows in $M_A$ with tail-end 0. Hence $|\Gamma| + |\Delta| = |A|$. The same reasoning proves $|\Gamma'| + |\Delta'| = |B|$. Clearly $\Gamma \cup \Gamma' \subseteq E_{n-1}$, and $\Delta \cup \Delta' \subseteq E_{n-1}$. On the other hand, we have $|\Gamma| + |\Delta| + |\Gamma'| + |\Delta'| = |A| + |B| = 2^n$. Hence the equalities $\Gamma \cup \Gamma' = E_{n-1}$ and $\Delta \cup \Delta' = E_{n-1}$ follow. □

Now, using the new notation for the pairing $(\tilde{\epsilon}|\tilde{\alpha})$ introduced just before Lemma 3, we can rewrite the formula $(A')$ in Fact 4 for the case we are interested in.

**Lemma 5.** *For any $v \in \mathcal{A}_{n-1}$ we have*

$$(A''_1) \quad w(v \oplus u_n) = \sum_{\substack{\tilde{\epsilon} \in E_{n-1} \\ (\tilde{\epsilon}|v) \equiv 0(2)}} s_{\tilde{\epsilon}} + \sum_{\substack{\tilde{\eta} \in E_{n-1} \\ (\tilde{\eta}|v) \equiv 1(2)}} s'_{\tilde{\eta}} \quad \textit{and}$$

$$(A''_2) \quad w(v' \oplus u'_n) = \sum_{\substack{\tilde{\epsilon}' \in E_{n-1} \\ (\tilde{\epsilon}'|v') \equiv 0(2)}} t_{\tilde{\epsilon}'} + \sum_{\substack{\tilde{\eta}' \in E_{n-1} \\ (\tilde{\eta}'|v') \equiv 1(2)}} t'_{\tilde{\eta}'} \quad \textit{and}$$

*where $v'$ stands for the code-word in $\mathcal{B}_{n-1} (= \langle u'_1, \cdots, u'_{n-1} \rangle)$ corresponding to $v$.*

Using Lemma 3, the formulae above can further be put in a more practical forms.

**Lemma 6.** *For any $v \in \mathcal{A}_{n-1}$, we have*

$$(A'''_1) \quad w(v \oplus u_n) = (1/2)|A| + (1/2) \left( \sum_{\tilde{\epsilon} \in \Gamma} (-1)^{(\tilde{\epsilon}|v)} - \sum_{\tilde{\eta} \in \Delta} (-1)^{(\tilde{\eta}|v)} \right), \textit{and}$$

$$(A_2''') \quad w(v' \oplus u'_n) = (1/2)|B| + (1/2)\left(\sum_{\tilde{\epsilon}' \in \Gamma'} (-1)^{(\tilde{\epsilon}'|v')} - \sum_{\tilde{\eta}' \in \Delta'} (-1)^{(\tilde{\eta}'|v')}\right),$$

*where $v'$ stands for the code-word in $\mathcal{B}_{n-1}$ corresponding to $v$.*

**Proof.** The proof is completely parallel for each case, so only $(A_1''')$ will be derived from $(A_1'')$ in Lemma 5. Since $s_{\tilde{\epsilon}}$ (or $s'_{\tilde{\eta}}$) is either 1, or 0 according as $\tilde{\epsilon} \in \Gamma$, or not ($\tilde{\eta} \in \Delta$, or not), $(A_1'')$ can be rewritten into

$$w(v \oplus u_n) = \sum_{\substack{\tilde{\epsilon} \in \Gamma \\ (\tilde{\eta}|v) \equiv 0(2)}} 1 + \sum_{\substack{\tilde{\eta} \in \Delta \\ (\tilde{\eta}|v) \equiv 1(2)}} 1,$$

where the first sum above is equal to

$$(1/2)\left(|\Delta| - \sum_{\tilde{\epsilon} \in \Delta} (-1)^{(\tilde{\epsilon}|v)}\right),$$

and the second one to

$$(1/2)\left(|\Gamma| + \sum_{\tilde{\eta} \in \Gamma} (-1)^{(\tilde{\eta}|v)}\right).$$

Hence, putting them in the corresponding places in the equality above, we obtain the formula $(A_1''')$. □

**Lemma 7.** *For every $v \in \mathcal{A}_{n-1}$, we have*

$$(A_1^{iv}) \quad w(v) = (1/2)|A| - (1/2)\left(\sum_{\tilde{\epsilon} \in \Gamma} (-1)^{(\tilde{\epsilon}|v)} + \sum_{\tilde{\eta} \in \Delta} (-1)^{(\tilde{\eta}|v)}\right), \text{ and}$$

$$(A_2^{iv}) \quad w(v') = (1/2)|B| - (1/2)\left(\sum_{\tilde{\epsilon}' \in \Gamma'} (-1)^{(\tilde{\epsilon}'|v')} + \sum_{\tilde{\eta}' \in \Delta'} (-1)^{(\tilde{\eta}'|v')}\right),$$

*where $v'$ stands for the code-words in $\mathcal{B}_{n-1}$ corresponding to $v$.*

**Proof.** The formula $(B)$ in Fact 3, Section 2, applied to $v \oplus u_n$ with $v \in \mathcal{A}_{n-1}$, can be rewritten into the from:

$$w(v \oplus u_n) - w(v) = \sum_{\tilde{\epsilon} \in \Gamma} (-1)^{(\tilde{\epsilon}|v)} \text{for any } v \in \mathcal{A}_{n-1}.$$

Note here that the formula $(B)$ is valid even when $v = 0$. Then, by Lemma 6,

$$w(v) = w(v \oplus u_n) - \sum_{\tilde{\epsilon} \in \Gamma} (-1)^{(\tilde{\epsilon}|v)} = (1/2)|A| - (1/2) \left( \sum_{\tilde{\epsilon} \in \Gamma} (-1)^{(\tilde{\epsilon}|v)} + \sum_{\tilde{\eta} \in \Delta} (-1)^{(\tilde{\eta}|v)} \right),$$

as desired. Doing the same thing for $w(v' \oplus u'_n) - w(v')$, we obtain $(A_1^{iv})$ and $(A_2^{iv})$. □

Before concluding this section we prove a lemma which will be used repeatedly.

**Lemma 8.** *Let $A$ and $B$ be as above, and $\{u_1, \cdots, u_n\}$ the columns of the matrix $M_A$. Then, for any non-zero code-word $u = u_{i_1} \oplus \cdots \oplus u_{i_k}$ with $1 \leq i_1 < \cdots < i_k \leq n$ in $\mathcal{A}_n$, the weight $w(u)$ is equal to $|A \cap H'_u|$, where $H_u$ is the hyperplane in $V$ defined by the equateon $x_{i_1} \oplus \cdots \oplus x_{i_k} = 0$, and $H'_u$ its complementray set. Similarly, for $u'(= h_{A,B}(u))$ in $\mathcal{B}_n$, $w(u') = |B \cap H'_u|$.*

**Proof.** Clearly $|A \cap H|$ ( or $|B \cap H|$) is the number of zeros appearing in the coordinates of the code-word $u$ (or in $u'$), hence $|A \cap H'| = |A| - |A \cap H|$ ( or$|B \cap H'| = |B| - |B \cap H|$) is equal to the weight $w(u)$ ( or to $w(u')$). □

## 4. Proof of Theorem 1.

If $n = 1$, obviously there is no subset satisfying the condition in Theorem 1. If $n = 2$, however, there actually exists such a subset: $A = \{(0, 0)\}$. Hence we prove the theorem assuming that $n \geq 3$. Let $A$ be a subset satisfying the condition. Clearly $A$ is non-empty. Further let $B$ be the complementary set of $A$ in $V$. We may further assume that $|A| \geq |B|$. First we show that $|A| = |B|$. For this end, assuming $|A| > |B|$, set $d = |A| - |B|$. Then $A$ contains a basis of $V$, because then $|A| > 2^{n-1}$. Hence the linear code $\mathcal{A}_n$ determined by $A$ is of dimension $n$, and the discussions in the foregoing section can apply. As before let $\{u_1, \cdots, u_n\}$ be the columns of the matrix $M_A$, and $\{u'_1, \cdots, u'_n\}$ that of $M_B$. Then, by Lemma 8, for any non-zero code-word $u = u_{i_1} \oplus \cdots \oplus u_{i_k}$ with $1 \leq i_1 < \cdots i_k \leq n$ in $\mathcal{A}_n$, we have $w(u) = |A \cap H'_u|$ where $H_u$ is the hyperplane defined by $x_{i_1} \oplus \cdots \oplus x_{i_k} = 0$. Similarly, for

$$u'(= h_{A,B}(u)), w(u') = |B \cap H'_u|.$$

Hence the condition in Theorem 1 implies that $w(u) = w(u') + d$ for every non zero $u \in \mathcal{A}_n$. In particular, $w(v) = w(v') + d$ for all non-zero $v \in \mathcal{A}_{n-1}$, where $\mathcal{A}_{n-1}$ denotes

the subcode of $A_n$ spanned by $\{u_1, \cdots, u_{n-1}\}$. Now, by the formula $(A_1^{iv})$ and $(A_2^{(iv)})$ in Section 3, we have

$$w(v) = (1/2)|A| - (1/2)\left(\sum_{\Gamma} + \sum_{\Delta}\right)$$

and

$$w(v') = (1/2)|B| - (1/2)\left(\sum_{\Gamma'} + \sum_{\Delta'}\right)$$

where $\Gamma, \Gamma', \Delta$ and $\Delta'$ denote the sets of indices of the non-zero characteristics and the non-zero co-characteristics belonging to the last columns of $M_A$ and $M_B$ respectively. Note that $\Gamma \cap \Gamma' = \Delta \cap \Delta' = \phi$, and $\Gamma \cup \Gamma' = \Delta \cup \Delta' = E_{n-1}$. Hence we further obtain

$$w(v) - w(v') = (1/2)d - (1/2)\left(\sum_{\Gamma} + \sum_{\Delta} - \sum_{\Gamma'} - \sum_{\Delta'}\right) = \begin{cases} d, & \text{if } v \neq 0, \\ 0, & \text{if } v = 0. \end{cases}$$

Now, summing up the both sides over all $v \in \mathcal{A}_{n-1}$, and, taking the orthogonality relations into account, we obtain

$$d(2^{n-1}-1) = \begin{cases} 2^{n-2}d + 2^{n-1} \text{ or } 2^{n-2}d - 2^{n-1} & \text{according as } \tilde{0} \in \Gamma' \cap \Delta', \text{ or } \tilde{0} \in \Gamma' \cup \Delta, \\ 2^{n-2}d, & \text{if } \tilde{0} \notin \Gamma \cup \Delta', \text{ and } \tilde{0} \notin \Delta \cap \Gamma'. \end{cases}$$

Of course the second case is impossible, because $n > 2$ by assumption. In the first case, $d(2^{n-2}-1) = 2^{n-1}$, which is only possible if $n = 3$, and $\tilde{0} \in \Gamma' \cap \Delta'$. Furthermore, $d$ must be 4, and $|A| = 6$, and $|B| = 2$. Now, since $\tilde{0} \in \Gamma' \cap \Delta'$, these data completely determine the set $B$ : $B = \{(0,0,0),(0,0,1)\}$. Then, for the hyperplane defined by $x_3 = 0$, the condition in Theorem 1 is not satisfied, as is easily checked. This contradiction proves our assertion that $|A| = |B|$. Now this further implies that $w(u) = w(u')$ for all $u \in \mathcal{A}_n$, because $w(u) = |A| - |A \cap H_u|$, and $w(u') = |B| - |B \cap H_u|$ for the hyperplane $H_u$, as was explained before. This then says that the homomorphism $h_{A,B}$ is injective, weight-preserving one. Hence, by Fact 5 in Section 2, $h_{A,B}$ is induced by a coordinate permutation. This, however, is impossible, because then the sets $A$ and $B$ would coincide with each other. This completes the Proof of Theorem 1.

## 5. Proof of Theorem 2

Let $A$ be a subset of $V$ satisfying the condition in Theorem 2, and $B$ its complementary set in $V$. Without loss of generality, we may assume that $|A| \geq |B|$.

**Lemma 1.** *The subset $A$ contains a basis of $V$.*

**Proof.** Assume that $A \subseteq H$ for a hyperplane of $V$. Then $|A| = |A \cap H| \geq |B| \geq |B \cap H|$, so that the equatilty $|A \cap H| = |B \cap H|$ holds only if $|B| = |B \cap H|$, hence $B \subseteq H$. If, on the other hand, the equality $|A \cap H'| = |B \cap H'|$ holds, then $0 = |A \cap H'| = |B \cap H'|$ implies that $B \subseteq H$. Thus in either case, $B$ is contained in $H$. But this is absurd, because $|A| + |B| = 2^n$, and $A \cap B = \phi$.

As before, $\{u_1, \cdots, u_n\}$ being the columns of the matrix $M_A$, and $\{u'_1, \cdots, u'_n\}$ that of the matrix $M_B$, let $\Gamma, \Delta, \Gamma'$ and $\Delta'$ be the sets of characteristics and co-characteristics of the last columns of $M_A$ and $M_B$ respectively. Note that $\Gamma \cap \Gamma' = \Delta \cap \Delta' = \phi$, and $\Gamma \cup \Gamma' = \Delta \cup \Delta' = E_{n-1}$. □

**Lemma 2.** *For any $u \in \mathcal{A}_n, w(u) - w(u')$ is either $|A| - |B|$, or $0$, where $u'$ denotes $h_{A,B}(u)$.*

**Proof.** By Lemma 8 in Section 3, for any non-zero $u \in \mathcal{A}_n, w(u) = |A \cap H'_u|$, and $w(u') = |B \cap H'_u|$, where $H_u$ with $u = u_{i_1} \oplus \cdots \oplus u_{i_k} (1 \leq i_1 < \cdots < i_k \leq n)$ is the hyperplane of $V$ defined by $x_{i_1} \oplus \cdots \oplus x_{i_k} = 0$. Hence, by the condition in Theorem 2, we have our assertion. □

**Corollary** $|A| > |B|$.

**Proof.** If $|A| = |B|$, then the block lengths of $\mathcal{A}_n$ and $\mathcal{B}_n$ are the same. Furthermore, by lemma above, $w(u) = w(u')$ for all $u \in \mathcal{A}_n$. Hence $h_{A,B}$ is an injective, weight preserving one, so that it is induced by a coordinate permutation by Fact 5 in Section 2. But this is absurd, because then the sets $A$ and $B$ coincide with each other. □

**Lemma 3.** $|A| - |B| = 2^r$ *,with* $r \geq 1$.

**Proof.** Let $d = |A| - |B| (> 0)$, and let $X = \{v \in \mathcal{A}_{n-1} | w(v) - w(v') = d\}$.
Then

$$\sum_{v \in \mathcal{A}_{n-1}} (w(v) - w(v')) = d|X|.$$

On the other hand, the sum is also equal to

$$2^{n-2}d - \frac{1}{2} \sum_{v \in \mathcal{A}n-1} \left( \sum_{\Gamma} + \sum_{\Delta} - \sum_{\Gamma'} - \sum_{\Delta'} \right)$$

by formulae in Lemma 7. The last expression above is equal to either $2^{n-2}d - 2^{n-1}$, or $2^{n-2}d + 2^{n-1}$ or $2^{n-2}d$ according as $\tilde{O} \in \Gamma \cap \Delta$, or $\tilde{O} \in \Gamma' \cap \Delta'$, or $\tilde{O}$ is either in

$\Gamma \cap \Delta'$, or in $\Delta \cap \Gamma'$. In the first case, $d(|X| - 2^{n-2}) = 2^{n-1}$, so that $d$ is a power of 2. Similarly, in either of the other cases, we conclude that $d$ is a power of 2, say $2^r$. Note that $r \geq 1$, because $d(= |A| - |B|) = 1$ is in consistent with $|A| + |B| = 2^n$ with $n \geq 2$. This completes the proof of the lemma. □

**Lemma 4.** *$2r = n$, hence the dimension of $V$ is even.*

**Proof.** Observe the sum

$$\sum_{v \in \mathcal{A}_{n-1}} \{(w(v) - (1/2)|A|) - (w(v') - (1/2)|B|)\}^2.$$

First note that the inside of the bracket takes the values $2^{r-1}$ or $-2^{r-1}$, so that the sum is equal to $2^{2r-2} \cdot 2^{n-1}$. On the other hand, by formulae in Lemma 7, the sum is equal to

$$\sum_{v \in \mathcal{A}_{n-1}} \frac{1}{4} \left( \sum_{\Gamma} + \sum_{\Delta} - \sum_{\Gamma'} - \sum_{\Delta'} \right)^2 = 2^{n-1}(|\Gamma \cap \Delta| + |\Gamma' \cap \Delta'|).$$

Note here that

$$\Gamma = (\Gamma \cap \Delta) \cup (\Gamma \cap \Delta'), \Delta = (\Gamma \cap \Delta) \cup (\Gamma' \cap \Delta), \Gamma' = (\Gamma' \cap \Delta') \cup (\Gamma' \cap \Delta),$$

and $\Delta' = (\Gamma' \cap \Delta') \cup (\Gamma \cap \Delta')$. From the above equality we obtain $|\Gamma \cap \Delta| + |\Gamma' \cap \Delta'| = 2^{2r-2}$. Next observe the sum

$$\sum_{v \in \mathcal{A}_{n-1}} \{(w(v \oplus u_n) - (1/2)|A|) - (w(v' \oplus u'_n) - (1/2)|B|)\}^2.$$

Again the inside of the bracket takes the values of $2^{r-1}$ or $-2^{r-1}$, so that the sum is equal to $2^{2r-2} \cdot 2^{n-1}$. On the other hand, it is equal to

$$\sum_{v \in \mathcal{A}_{n-1}} (1/4) \left( \sum_{\Gamma} - \sum_{\Delta} - \sum_{\Gamma'} + \sum_{\Delta'} \right)^2 = 2^{n-1}(|\Gamma \cap \Delta'| + |\Gamma' \cap \Delta|).$$

Hence $|\Gamma \cap \Delta'| + |\Gamma' \cap \Delta| = 2^{2r-2}$. Since

$$|\Gamma| + |\Gamma'| = |\Gamma \cap \Delta| + |\Gamma \cap \Delta' + |\Gamma' \cap \Delta'| + |\Gamma' \cap \Delta| = 2^{2r-2} + 2^{2r-2} = 2^{2r-1},$$

comparing with $|\Gamma| + \Gamma'| = |E_{n-1}|$, we arrive at the equality $2r = n$. This completes the proof of the lemma. □

Now we can prove the rest of the assertions in Theorem 2.

As we have seen above, the dimension of $V$ is even, say $2m$ with $m \geq 1$, and $|A| - |B| = 2^m$, so that $|A| = 2^{2m-1} + 2^{m-1}$, and $|B| = 2^{2m-1} - 2^{m-1}$.

By a bent function on $V = Z_2^{2m}$, we understand a function $f : Z_2^{2m} \to Z_2$ such that

$$\left| \sum_{\underline{x} \in V} (-1)^{f(\underline{x}) \oplus \underline{x}.\underline{y}} \right| = 2^m \quad \text{for every} \quad \underline{y} \in V.$$

Now if $f$ is bent, by setting $\underline{y} = \underline{O}$, we see that the set $B(f)$ of zeros of $f$ is either of size $2^{2m-1} + 2^{m-1}$, or of size $2^{2m-1} - 2^{m-1}$. Furthermore, applying the relation above for the hyperplane defined by $\underline{x}.\underline{y}_0 = 0$ with any non-zero $\underline{y}_0 \in V$, we see that $|B(f) \cap H| + |B(f)' \cap H'|$ is either equal to $|B(f)|$, or to $|B(f)'|$ for any hyperplane $H$ in $V$. Here, as usual $H'$ and $B(f)'$ stand for the respective complementary sets. Conversely if $B$ is any subset of $V$ satisfying the conditions mentioned above, then it is easy to see that the characteristic function of $B$ is bent. So for our purpose, it suffices to show that $|A \cap H| + |A' \cap H'|$ is either equal to $|A|$, or to $|A'|$ for our set $A$, and for any hyperplane $H$ in $V$. Since $B = A'$, the relation in question is nothing but $|A \cap H| + |B \cap H'| = |A|$, or $|B|$. Now if $|A \cap H| = |B \cap H|$ for a hyperplane $H$, then $|B \cap H'| = |B| - |B \cap H|$, so that $|A \cap H| + |B \cap H'| = |B|$. If on the other hand, $|A \cap H'| = |B \cap H'|$, then $|A \cap H| + |B \cap H'| = |A \cap H| + |A \cap H'| = |A|$. Thus we have verified that our set $A$ actually satisfies the condition in question, *i.e.*$A$ is the set of zeros of a bent function, say $f$. Then clearly $B$ is the set of zeros of the bent function $1 \oplus f$. This completes the proof of the "only if" part of Theorem 2. The "if part" of the theorem can be proved by following the proof above in the reversed order.

By using Stirling formula we obtain the following

**Corollary.** *For sufficiently large $n$, the number of bent functions on $\mathbb{Z}_n^{2n}$ is less than one $2^{n-1}$ -th of the total numbers functions on $\mathbb{Z}_2^{2n}$.*

## References

[1] İ.Ş. Güloğlu and M. İkeda: The weight equations for binary linear codes, *No.*6, Preprint series in Pure and Applied Mathematics, Marmara Research Center, TÜBİTAK (1994)

# $\mathbb{Z}_2$-LİNEER KODLARIN AĞIRLIK DENKLEMLERİ VE UYGULAMALARI

**Özet**

[1]' de geliştirilmiş teknikler yardımıyla 2 elemanlı cisim üzerindeki vektör uzaylarında kombinatorik bazı problemler çözüldü. Bu da, [1]' de tekniklerin böyle gayeler için ne kadar geçerli olduğuna bir örnek teşkil etmektedir.

Ersan AKYILDIZ, İsmail Ş. GÜLOĞLU
Department of Mathematics
Middle East Technical University
06531 Ankara-TURKEY

Masatoshi İKEDA
TÜBİTAK
Marmara Resarch Center
Gebze-KOCAELİ

Received 12.2.1995
Revised 9.12.1996