REFERENCES

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: North Holland, 1977.

[2] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1982.

[3] V. I. Korzhik, "Bounds on undetected error probability and optimum group codes in a channel with feedback," *Telecommun. Radio Eng.*, vol. 20, no. 1, pt. 2, pp. 87–92, Jan. 1965.

[4] V. K. Leontev, "Error-detecting encoding," *Probl. Inform. Transmission*, vol. 8, pp. 86–92, 1972.

[5] V. I. Levenshtein, "Bounds on the probability of undetected error," *Probl. Inform. Transmission*, vol. 13, pp. 1–12, 1978.

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, "Concerning a bound on undetected error probability," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 2, pp. 235–237, Mar. 1976.

[7] S. K. Leung-Yan-Cheong, E. R. Barnes, and D. U. Friedman, "Some properties of undetected error probability of linear codes," *IEEE Trans. Inform. Theory*, vol. IT-25, no. 1, pp. 110–112, Jan. 1979.

[8] J. K. Wolf, A. M. Michelson, and A. H. Levesque, "On the probability of undetected error for linear block codes," *IEEE Trans. Commun.*, vol. COM-30, no. 2, pp. 317–324, Feb. 1982.

[9] T. Kasami, T. Kløve, and S. Lin, "Linear block codes for error detection," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 1, pp. 131–136, Jan. 1983.

[10] T. Helleseth, T. Kløve, and J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1(q^l - 1)/N$," *Discrete Math.*, vol. 18, pp. 179–211, 1977.

[11] J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, pp. 79–94, Jan. 1963.

[12] R. Padovani and J. K. Wolf, "Data transmission using error detection codes," in *GLOBECOM '82, IEEE Global Telecom. Conf.*, Miami, Nov. 29–Dec. 2, 1982, pp. 626–631.

On an Infinite Series of $[4n, 2n]$ Binary Codes

LÉON M. H. E. DRIESSEN, MEMBER, IEEE

***Abstract*—This correspondence deals with an infinite series of binary, reversible $[4n, 2n, 4]$, $n \geq 2$, unequal error protection codes, which are majority logic decodable. The weight enumerators and automorphism groups are determined completely. For n even the codes are self dual. By pasting together copies of a $[4n, 2n, 4]$ code, binary codes with parameters $[8n, 2n, 8]$ for $n \geq 2$, $[8n, 2n, 12]$ for $n \geq 4$, and $[12n, 2n, 16]$ and $[16n, 2n, 24]$ for $n \geq 3$ are obtained.**

I. INTRODUCTION

The decoder with the best error correction performance for an $[n, k, d]$ binary code to be used on a binary symmetric channel, is a complete nearest neighbor decoder [1, p. 11]. That is, any received word is mapped into a codeword that is nearest in Hamming distance. In many applications not all message bits are equally important and errors in more important bits are more serious than errors in less important bits. The question arises to what extent error patterns of weight greater than $\lfloor (d-1)/2 \rfloor$ can be decoded such that the most important message bits are correctly retrieved. This is the same as asking for an $[n, k, d]$ binary unequal error protection (UEP) code which is optimal [2], [3].

In an experimental digital recorder we have implemented an optimal [12, 6, 4] binary UEP code [4], which guarantees the two most important message bits to be protected against two bit errors in the corresponding codeword. This code is a member of an infinite class of $[4n, 2n, 4]$ binary UEP codes which will be defined and studied in the next section. The [12, 6, 4] UEP code is used as an example throughout the correspondence.

Manuscript received August 13, 1982; revised March 29, 1983.

The author is with Philips Research Laboratories, P.O. Box 80.000, 5600 JA Eindhoven, The Netherlands.

In Section III constructions of $[4nr, 2n]$ binary codes are given for $r = 1, 2, 3$, and 4. These constructions are based on a detailed knowledge of the weight structure of the codes from Section II. Several codes constructed in this correspondence are optimal in the sense that they have the largest minimum distance known for a binary code with the same length and dimension [5].

The notation we use and basic concepts will be explained where necessary. For additional information on coding theory or group theory the reader is referred to [1] and [6], respectively.

II. AN INFINITE SERIES OF $[4n, 2n, 4]$ BINARY CODES

In this section we define and study an infinite class of $[4n, 2n, 4]$, $n \geq 2$, binary codes. As these codes may be considered to be generalizations of the code $\boldsymbol{F}_{16}$ of [7], they are denoted by $\boldsymbol{F}_{4n}$.

Definition: Let I_n be the n by n identity matrix and let J_n be the n-by-n all-one matrix. The code $\boldsymbol{F}_{4n}$ is defined by the generator matrix

$$G_{4n} := \begin{pmatrix} I_n & I_n & 0_n & J_n \\ J_n & 0_n & I_n & I_n \end{pmatrix}.$$

Let $\boldsymbol{g}^{(i)}$ be the ith row of G_{4n} and let the codewords $\boldsymbol{b}^{(i)}$, $1 \leq i \leq 2n$, be defined by

$$\boldsymbol{b}^{(1)} = \boldsymbol{g}^{(1)} \quad \text{and} \quad \boldsymbol{b}^{(2)} = \boldsymbol{g}^{(n+1)},$$
$$\boldsymbol{b}^{(2i-1)} = \boldsymbol{g}^{(1)} + \boldsymbol{g}^{(i)}, \qquad 2 \leq i \leq n,$$
$$\boldsymbol{b}^{(2i)} = \boldsymbol{g}^{(n+1)} + \boldsymbol{g}^{(n+i)}, \qquad 2 \leq i \leq n.$$

The code generated by $\{\boldsymbol{b}^{(i)}: 3 \leq i \leq 2n\}$ is called $\boldsymbol{B}_{4n}$.

Let $\boldsymbol{V}_n$ be the n-dimensional vector space over GF(2); $\boldsymbol{0}_n$ denotes the all-zero word in $\boldsymbol{V}_n$ and $\boldsymbol{1}_n$ denotes the all-one word in $\boldsymbol{V}_n$. For $\boldsymbol{A} \subset \boldsymbol{V}_n$ and $\boldsymbol{x} \in \boldsymbol{V}_n$ we denote by $\boldsymbol{x} + \boldsymbol{A}$ the coset of $\boldsymbol{A}$ obtained by (componentwise modulo 2) addition of $\boldsymbol{x}$ to each element of $\boldsymbol{A}$.

The cosets $\boldsymbol{B}_{4n}$, $\boldsymbol{b}^{(1)} + \boldsymbol{B}_{4n}$, $\boldsymbol{b}^{(2)} + \boldsymbol{B}_{4n}$, and $\boldsymbol{b}^{(1)} + \boldsymbol{b}^{(2)} + \boldsymbol{B}_{4n}$ are denoted by $\boldsymbol{B}_{4n}^{00}$, $\boldsymbol{B}_{4n}^{10}$, $\boldsymbol{B}_{4n}^{01}$, and $\boldsymbol{B}_{4n}^{11}$, respectively. Clearly $\boldsymbol{F}_{4n} = \boldsymbol{B}_{4n}^{00} \cup \boldsymbol{B}_{4n}^{10} \cup \boldsymbol{B}_{4n}^{01} \cup \boldsymbol{B}_{4n}^{11}$. We shall now derive the weight enumerators of these cosets of $\boldsymbol{B}_{4n}$.

The (Hamming) weight of $\boldsymbol{x} \in \boldsymbol{V}_n$ is denoted by $\mathrm{wt}(\boldsymbol{x})$ and the (Hamming) weight enumerator of $\boldsymbol{A} \subset \boldsymbol{V}_n$ is denoted by $W(\boldsymbol{A}; z)$, where z is an indeterminate.

Lemma: A codeword $\boldsymbol{c} \in \boldsymbol{F}_{4n}$ can be expressed as $\boldsymbol{c} = (\boldsymbol{x}, \boldsymbol{y})G_{4n}$, where $\boldsymbol{x} \in \boldsymbol{V}_n$ and $\boldsymbol{y} \in \boldsymbol{V}_n$. For $0 \leq i, j \leq 1$ it holds that $\boldsymbol{c} \in \boldsymbol{B}_{4n}^{ij}$ if and only if $\mathrm{wt}(\boldsymbol{x}) = i \bmod 2$ and $\mathrm{wt}(\boldsymbol{y}) = j \bmod 2$.

The lemma immediately follows from the observation that

$$\begin{aligned} \boldsymbol{c} &= (\boldsymbol{x}, \boldsymbol{y})G_{4n} \\ &= \sum_{i=1}^{n} x_i \boldsymbol{g}^{(i)} + \sum_{j=1}^{n} y_j \boldsymbol{g}^{(n+j)} \\ &= \sum_{i=2}^{n} x_i \left(\boldsymbol{g}^{(i)} + \boldsymbol{g}^{(1)}\right) + \boldsymbol{g}^{(1)} \sum_{i=1}^{n} x_i \\ &\quad + \sum_{j=2}^{n} y_j \left(\boldsymbol{g}^{(n+j)} + \boldsymbol{g}^{(n+1)}\right) + \boldsymbol{g}^{(n+1)} \sum_{j=1}^{n} y_j. \end{aligned}$$

Theorem 1: The weight enumerators of the cosets of $\boldsymbol{B}_{4n}$ in $\boldsymbol{F}_{4n}$ are

$$W(\boldsymbol{B}_{4n}^{00}; z) = \sum_{i=0}^{\lfloor n/2 \rfloor} \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} \binom{n}{2j} z^{4i+4j},$$

$$W(\boldsymbol{B}_{4n}^{10}; z) = W(\boldsymbol{B}_{4n}^{01}; z) = 2^{n-1} \sum_{i=0}^{\lfloor n-1/2 \rfloor} \binom{n}{2i+1} z^{n+2+4i},$$

$$W(\boldsymbol{B}_{4n}^{11}; z) = 2^{2n-2} z^{2n}.$$

0018-9448/84/0300-0392$01.00 ©1984 IEEE

Proof: From the Lemma we deduce that

$\boldsymbol{c} \in \boldsymbol{B}_{4n}^{00}$ if and only if $\mathrm{wt}(\boldsymbol{x})$ and $\mathrm{wt}(\boldsymbol{y})$ are even, in which case $\boldsymbol{c} = (\boldsymbol{x}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{y})$ and $\mathrm{wt}(\boldsymbol{c}) = 2(\mathrm{wt}(\boldsymbol{x}) + \mathrm{wt}(\boldsymbol{y}))$,
$\boldsymbol{c} \in \boldsymbol{B}_{4n}^{10}$ if and only if $\mathrm{wt}(\boldsymbol{x})$ is odd and $\mathrm{wt}(\boldsymbol{y})$ is even, in which case $\boldsymbol{c} = (\boldsymbol{x}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{y} + \mathbf{1}_n)$ and $\mathrm{wt}(\boldsymbol{c}) = n + 2\,\mathrm{wt}(\boldsymbol{x})$,
$\boldsymbol{c} \in \boldsymbol{B}_{4n}^{01}$ if and only if $\mathrm{wt}(\boldsymbol{x})$ is even and $\mathrm{wt}(\boldsymbol{y})$ is odd, in which case $\boldsymbol{c} = (\boldsymbol{x} + \mathbf{1}_n, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{y})$ and $\mathrm{wt}(\boldsymbol{c}) = n + 2\,\mathrm{wt}(\boldsymbol{y})$,
$\boldsymbol{c} \in \boldsymbol{B}_{4n}^{11}$ if and only if $\mathrm{wt}(\boldsymbol{x})$ and $\mathrm{wt}(\boldsymbol{y})$ are odd, in which case $\boldsymbol{c} = (\boldsymbol{x} + \mathbf{1}_n, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{y} + \mathbf{1}_n)$ and $\mathrm{wt}(\boldsymbol{c}) = 2n$.

The expressions for the weight enumerators are now easily found. Q.E.D.

From Theorem 1 we know that $\boldsymbol{F}_{4n}$, $n \geq 2$, has minimum distance 4. There is a generalization of the concept of minimum distance, called separation vector, the value of which strongly depends on the encoding procedure [2], [3]. Let $\boldsymbol{h}^{(1)}, \boldsymbol{h}^{(2)}, \cdots, \boldsymbol{h}^{(k)}$ be k basis codewords according to which the encoding takes place. That is, if $\boldsymbol{m} \in \boldsymbol{V}_k$, the corresponding codeword is $\boldsymbol{c}(\boldsymbol{m}) = m_1\boldsymbol{h}^{(1)} + m_2\boldsymbol{h}^{(2)} + \cdots + m_k\boldsymbol{h}^{(k)}$. The separation vector $\boldsymbol{s} = (s_1, s_2, \cdots, s_k)$ is defined by $s_i := \min\{\mathrm{wt}(\boldsymbol{c}(\boldsymbol{m})): \boldsymbol{m} \in \boldsymbol{V}_k, m_i = 1\}$ for $1 \leq i \leq k$. A separation vector $\boldsymbol{s}$ guarantees the correct retrieval of message bit m_i if the number of errors in the code word $\boldsymbol{c}(\boldsymbol{m})$ is at most $\lfloor (s_i - 1)/2 \rfloor$, [2], [3]. If not all s_i are equal to the minimum distance, the code is said to have the unequal error protection property. For $n \geq 3$, the code $\boldsymbol{F}_{4n}$ has the UEP property. We state this in Theorem 2.

Theorem 2: The code $\boldsymbol{F}_{4n}$, $n \geq 2$, has the following properties:

a) $\boldsymbol{F}_{4n}$ is reversible.
b) $\boldsymbol{F}_{4n}$ is equivalent to its dual code.
c) $\boldsymbol{F}_{4n}$ is self dual if and only if n is even.
d) $\boldsymbol{F}_{4n}$ is equivalent to a double circulant code.
e) If the message word $\boldsymbol{m} \in \boldsymbol{V}_{2n}$ is encoded as $\boldsymbol{c}(\boldsymbol{m}) = m_1\boldsymbol{b}^{(1)} + m_2\boldsymbol{b}^{(2)} + \cdots + m_{2n}\boldsymbol{b}^{(2n)}$, then $\boldsymbol{F}_{4n}$, $n \geq 3$, has the UEP property with separation vector $\boldsymbol{s}$, $s_1 = s_2 = n + 2$, and $s_i = 4$ for $3 \leq i \leq 2n$.
f) $\boldsymbol{F}_{4n}$ is majority logic decodable.

Proof:

a) The reversibility follows immediately from the generator matrix G_{4n}.

b) The matrix obtained from G_{4n} by interchanging the columns i and $n + i$ for $1 \leq i \leq n$ and $2n + 1 \leq i \leq 3n$ is a parity check matrix for $\boldsymbol{F}_{4n}$.

c) $\boldsymbol{F}_{4n}$ is self dual if and only if $G_{4n}G_{4n}^T = 0_{2n}$, thus if and only if n is even.

d) The matrix formed by taking the columns of G_{4n} in the order $n + i, i, 2n + i, 3n + i$ for $i = 1, 2, \cdots, n$, is the generator matrix of a quasi-cyclic code with shift 2.

e) If $\boldsymbol{m} \in \boldsymbol{V}_{2n}$, then $\boldsymbol{c}(\boldsymbol{m}) \in \boldsymbol{B}_{4n}^{m_1 m_2}$.

The separation vector is $\boldsymbol{s} = (s_1, s_2, \cdots, s_{2n})$:

$$s_1 = \min\{\mathrm{wt}(\boldsymbol{c}): \boldsymbol{c} \in \boldsymbol{B}_{4n}^{11} \cup \boldsymbol{B}_{4n}^{10}\} = n + 2,$$

$$s_2 = \min\{\mathrm{wt}(\boldsymbol{c}): \boldsymbol{c} \in \boldsymbol{B}_{4n}^{11} \cup \boldsymbol{B}_{4n}^{01}\} = n + 2, \quad \text{and}$$

$$s_i = \mathrm{wt}(\boldsymbol{b}^{(i)}) = 4 = \min\{\mathrm{wt}(\boldsymbol{c}): \boldsymbol{c} \in \boldsymbol{F}_{4n}\} \qquad \text{for } 3 \leq i \leq 2n.$$

For $n \geq 3$ this proves the UEP property of $\boldsymbol{F}_{4n}$.

f) For $\boldsymbol{m} \in \boldsymbol{V}_{2n}$ we define $\boldsymbol{x}(\boldsymbol{m})$ and $\boldsymbol{y}(\boldsymbol{m})$ as

$$\boldsymbol{x}(\boldsymbol{m}) := \left(\sum_{i=1}^{n} m_{2i-1}, m_3, m_5, \cdots, m_{2n-1} \right)$$

and

$$\boldsymbol{y}(\boldsymbol{m}) := \left(\sum_{i=1}^{n} m_{2i}, m_4, m_6, \cdots, m_{2n} \right).$$

Then we have

$$\begin{aligned} \boldsymbol{c}(\boldsymbol{m}) &= (\boldsymbol{x}(\boldsymbol{m}), \boldsymbol{y}(\boldsymbol{m}))G_{4n} \\ &= (\boldsymbol{x}(\boldsymbol{m}) + m_2\mathbf{1}_n, \boldsymbol{x}(\boldsymbol{m}), \boldsymbol{y}(\boldsymbol{m}), \boldsymbol{y}(\boldsymbol{m}) + m_1\mathbf{1}_n). \end{aligned}$$

Let $\hat{\boldsymbol{c}}$ be the received word. We have to find a number of checks on each message bit m_i such that with majority logic decoding the error protection as specified by e) is achieved. For $j = 1, 2, 3, 4$ we define $p_j := \sum_{i=1}^{n} \hat{c}_{(j-1)n+i}$. Consider m_1 first.

If n is even, then it is easy to find $n + 2$ orthogonal checks [3] on m_1, namely p_1, p_2, and $\hat{c}_{2n+i} + \hat{c}_{3n+i}$ for $1 \leq i \leq n$. If n is odd we again have the n orthogonal checks $\hat{c}_{2n+i} + \hat{c}_{3n+i}$ for $1 \leq i \leq n$ but the other checks, although orthogonal to the previous ones, will not be mutually orthogonal. Note that p_2, $\hat{c}_1 + \hat{c}_{n+1} + p_1$, and $\hat{c}_2 + \hat{c}_{n+2} + p_1$ are three checks on m_1 which only involve the bits $\hat{c}_1, \cdots, \hat{c}_{2n}$. If these checks are mutually equal, which happens to be so if there are no errors among $\hat{c}_1, \cdots, \hat{c}_{2n}$, then p_2 is considered as a double check on m_1. If the three checks are not mutually equal, which happens to be so if exactly one error occurs among $\hat{c}_1, \cdots, \hat{c}_{2n}$, then p_2 and $p_2 + 1$ are considered as checks on m_1 (or no check is considered).

It is easily seen that a majority vote on the $n + 2$ checks on m_1, found as explained above, guarantees m_1 to be correctly retrieved if at most $\lfloor (n + 1)/2 \rfloor$ errors occur in $\hat{\boldsymbol{c}}$. In a similar way $n + 2$ checks on m_2 are found.

Once we have m_1 and m_2, four orthogonal checks on m_{2i-1} for $2 \leq i \leq n$ are $\hat{c}_i + m_2$, $\hat{c}_{n+i}$, $p_1 + \hat{c}_i + m_1 + (m_2$ if n is even), and $p_2 + \hat{c}_{n+i} + m_1$. In a similar way four orthogonal checks on m_{2i} for $2 \leq i \leq n$ are found. Q.E.D.

Example: Let $n = 3$. The code $\boldsymbol{F}_{12}$ is generated by

$$\left.\begin{aligned} \boldsymbol{b}^{(1)} &= \boldsymbol{g}^{(1)} = (1,0,0,1,0,0,0,0,0,1,1,1) \\ \boldsymbol{b}^{(2)} &= \boldsymbol{g}^{(4)} = (1,1,1,0,0,0,1,0,0,1,0,0) \\ \boldsymbol{b}^{(3)} &= \boldsymbol{g}^{(1)} + \boldsymbol{g}^{(2)} = (1,1,0,1,1,0,0,0,0,0,0,0) \\ \boldsymbol{b}^{(4)} &= \boldsymbol{g}^{(4)} + \boldsymbol{g}^{(5)} = (0,0,0,0,0,0,1,1,0,1,1,0) \\ \boldsymbol{b}^{(5)} &= \boldsymbol{g}^{(1)} + \boldsymbol{g}^{(3)} = (1,0,1,1,0,1,0,0,0,0,0,0) \\ \boldsymbol{b}^{(6)} &= \boldsymbol{g}^{(4)} + \boldsymbol{g}^{(6)} = (0,0,0,0,0,0,1,0,1,1,0,1) \end{aligned}\right\} \text{ generate } \boldsymbol{B}_{12}.$$

The weight enumerators of the cosets of $\boldsymbol{B}_{12}$ in $\boldsymbol{F}_{12}$ are

$$\begin{aligned} W(\boldsymbol{B}_{12}^{00}; z) &= 1 + 6z^4 + 9z^8, \\ W(\boldsymbol{B}_{12}^{10}; z) = W(\boldsymbol{B}_{12}^{01}; z) &= 12z^5 + 4z^9, \\ W(\boldsymbol{B}_{12}^{11}; z) &= 16z^6. \end{aligned}$$

$\boldsymbol{F}_{12}$ is equivalent to the double circulant code with the circulants (100000) and (110101).

$\boldsymbol{F}_{12}$ is a [12, 6, 4] code with separation vector (5, 5, 4, 4, 4 4). This is optimal [3], [4]. The check sets on $m_1, m_2, \cdots, m_6$ are

$$\begin{aligned} m_1 &= \hat{c}_7 + \hat{c}_{10}, \\ m_1 &= \hat{c}_8 + \hat{c}_{11}, \\ m_1 &= \hat{c}_9 + \hat{c}_{12}, \\ m_1 &= \hat{c}_4 + \hat{c}_5 + \hat{c}_6 = p_2, \\ m_1 &= p_2 \text{ if } \hat{c}_4 + \hat{c}_5 + \hat{c}_6 = \hat{c}_2 + \hat{c}_3 + \hat{c}_4 = \hat{c}_1 + \hat{c}_3 + \hat{c}_5, \\ &\qquad \text{else } p_2 + 1. \end{aligned}$$

$$\begin{aligned} m_2 &= \hat{c}_1 + \hat{c}_4, \\ m_2 &= \hat{c}_2 + \hat{c}_5, \\ m_2 &= \hat{c}_3 + \hat{c}_6, \\ m_2 &= \hat{c}_7 + \hat{c}_8 + \hat{c}_9 = p_3, \\ m_2 &= p_3 \text{ if } \hat{c}_7 + \hat{c}_8 + \hat{c}_9 = \hat{c}_{11} + \hat{c}_{12} + \hat{c}_7 = \hat{c}_{10} + \hat{c}_{12} + \hat{c}_8 \\ &\qquad \text{else } p_3 + 1. \end{aligned}$$

$$\begin{aligned} m_3 &= \hat{c}_2 + m_2, & m_4 &= \hat{c}_8, \\ m_3 &= \hat{c}_5, & m_4 &= \hat{c}_{11} + m_1, \\ m_3 &= \hat{c}_1 + \hat{c}_3 + m_1, & m_4 &= \hat{c}_7 + \hat{c}_9 + m_2, \\ m_3 &= \hat{c}_4 + \hat{c}_6 + m_1. & m_4 &= \hat{c}_{10} + \hat{c}_{12} + m_2. \end{aligned}$$

$$\begin{aligned} m_5 &= \hat{c}_3 + m_2, & m_6 &= \hat{c}_9, \\ m_5 &= \hat{c}_6, & m_6 &= \hat{c}_{12} + m_1, \\ m_5 &= \hat{c}_1 + \hat{c}_2 + m_1, & m_6 &= \hat{c}_7 + \hat{c}_8 + m_2, \\ m_5 &= \hat{c}_4 + \hat{c}_5 + m_1. & m_6 &= \hat{c}_{10} + \hat{c}_{11} + m_2. \end{aligned}$$

The code F_8 is an [8,4,4] code with weight enumerator $W(F_8; z) = 1 + 14z^4 + z^8$ and hence F_8 is the nearly perfect and self dual [8,4,4] extended Hamming code or, equivalently, the first-order Reed–Muller code of length 8 [1, p. 28]. Consequently the automorphism group of F_8 is the general affine group GA(3) [1, p. 376] of order 1344. The automorphism group of F_{4n}, $n \geq 3$, is given by Theorem 3.

If π is a permutation of $\{1,2,\cdots,n\}$, then π induces a mapping of V_n onto V_n as follows: the word $x \in V_n$ is mapped onto $\pi(x) = (x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, \cdots, x_{\pi^{-1}(n)})$.

The automorphism group of $A \subset V_n$ is denoted by $\mathrm{Aut}(A)$.

Theorem 3: Let the permutations τ, λ_i, and ρ_i, $1 \leq i \leq n$, of $\{1,2,\cdots,4n\}$ be given by

$$\tau = (1,4n)(2,4n-1)(3,4n-2)\cdots(2n,2n+1),$$
$$\lambda_i = (i, n+i),$$
$$\rho_i = (2n+i, 3n+i).$$

Let T_n, L_n, $\bar{L}_n$, R_n, and $\bar{R}_n$ be the groups generated by τ, $\{\lambda_i: 1 \leq i \leq n\}$, $\{\lambda_i\lambda_j: 1 \leq i < j \leq n\}$, $\{\rho_i: 1 \leq i \leq n\}$, and $\{\rho_i\rho_j: 1 \leq i < j \leq n\}$, respectively. Let S_n^l be the symmetric group on n points acting on $\{1,2,\cdots,n\}$ and $\{n+1, n+2,\cdots,n+n\}$ simultaneously. Let S_n^r be the symmetric group on n points acting on $\{2n+1, 2n+2,\cdots,2n+n\}$ and $\{3n+1, 3n+2,\cdots,3n+n\}$ simultaneously. The automorphism groups of B_{4n} and F_{4n}, $n \geq 3$, respectively, are

$$\mathrm{Aut}(B_{4n}) = T_n \times L_n \times R_n \times S_n^l \times S_n^r$$
$$\mathrm{Aut}(F_{4n}) = T_n \times \bar{L}_n \times \bar{R}_n \times S_n^l \times S_n^r.$$

Both groups are 1-transitive groups acting on $4n$ points and have order $2^{2n+1}(n!)^2$ and $2^{2n-1}(n!)^2$, respectively.

Proof: A permutation of the coordinate set acting on words is weight-preserving. From theorem 1 it follows that for $n \geq 3$ any codeword of F_{4n} having weight 4 is in B_{4n}. Since B_{4n} is generated by codewords of weight 4, we have that for $n \geq 3$ $\mathrm{Aut}(F_{4n})$ is a subgroup of $\mathrm{Aut}(B_{4n})$.

From the lemma we know that

$$B_{4n} = \{(x,x,y,y): x \in V_n, \mathrm{wt}(x) \text{ is even}; y \in V_n, \mathrm{wt}(y) \text{ is even}\}.$$

Due to the special form of the elements of B_{4n} we define the pairs of coordinates $\{i, n+i\}$, $1 \leq i \leq n$, to be left pairs and the pairs $\{2n+i, 3n+i\}$, $1 \leq i \leq n$, to be right pairs.

A word is equivalently represented by the set of its nonzero coordinates. So $c \in B_{4n}$ if and only if c is the union of an even number of left pairs and an even number of right pairs. For $n \geq 3$, an automorphism of B_{4n} must send pairs into pairs. Moreover, if an automorphism of B_{4n} sends a left pair into a left pair, then all left pairs are sent into left pairs and all right pairs into right pairs; if an automorphism sends a left pair into a right pair, then all left pairs are sent into right pairs and vice versa. From Theorem 2 a) we know that τ is an automorphism of F_{4n}; τ has order 2 and sends left pairs into right pairs and vice versa. Any automorphism of B_{4n} leaving the coordinates $2n+1, 2n+2,\cdots,4n$ fixed is the product of a permutation leaving every left pair fixed and a permutation of the left pairs and hence is an element of $L_n \times S_n^l$. Any element of $L_n \times S_n^l$ is an automorphism of B_{4n}. Similarly any element of $R_n \times S_n^r$ is an automorphism of B_{4n}.

We have proved that $\mathrm{Aut}(B_{4n}) = T_n \times L_n \times R_n \times S_n^l \times S_n^r$. As we saw above, $\mathrm{Aut}(F_{4n})$ is a subgroup of $\mathrm{Aut}(B_{4n})$. An automorphism of B_{4n} is an automorphism of F_{4n} if and only if $b^{(1)}$ and $b^{(2)}$ are sent into codewords of F_{4n}. For $\pi \in S_n^l$ we have $\pi(b^{(2)}) = b^{(2)}$ and $\pi(b^{(1)}) = g^{(\pi(1))}$. Hence $S_n^l \subset \mathrm{Aut}(F_{4n})$. Analogously $S_n^r \subset \mathrm{Aut}(F_{4n})$. For $\pi \in R_n$ we have $\pi(b^{(2)}) = b^{(2)}$, but $\pi(b^{(1)}) = (10\cdots0, 10\cdots0, y, y+1_n)$ for some $y \in V_n$, which according to the lemma is a codeword of F_{4n} if and only if $\mathrm{wt}(y)$ is even. So $\pi(b^{(1)}) \in F_{4n}$ if and only if $\pi \in \bar{R}_n$. Analogously for $\pi \in L_n$ we have $\pi \in \mathrm{Aut}(F_{4n})$ if and only if $\pi \in \bar{L}_n$.

We have proved that $\mathrm{Aut}(F_{4n}) = T_n \times \bar{L}_n \times \bar{R}_n \times S_n^l \times S_n^r$. Q.E.D.

Example: Let $n = 3$.

$$T_3 = \{(1),(1,12)(2,11)(3,10)(4,9)(5,8)(6,7)\}.$$
$$L_3 = \{(1),(1,4),(2,5),(3,6),(1,4)(2,5),(1,4)(3,6),(2,5)(3,6),(1,4)(2,5)(3,6)\}.$$
$$\bar{L}_3 = \{(1),(1,4)(2,5),(1,4)(3,6),(2,5)(3,6)\}.$$
$$R_3 = \{(1),(7,10),(8,11),(9,12),(7,10)(8,11),(7,10)(9,12),(8,11)(9,12),(7,10)(8,11)(9,12)\}.$$
$$\bar{R}_3 = \{(1),(7,10)(8,11),(7,10)(9,12),(8,11)(9,12)\}.$$
$$S_3^l = \{(1),(1,2)(4,5),(1,3)(4,6),(2,3)(5,6),(1,2,3)(4,5,6),(1,3,2)(4,6,5)\}.$$
$$S_3^r = \{(1),(7,8)(10,11),(7,9)(10,12),(8,9)(11,12),(7,8,9)(10,11,12),(7,9,8)(10,12,11)\}.$$

$|\mathrm{Aut}(B_{12})| = 4608$ and $|\mathrm{Aut}(F_{12})| = 1152$.

III. Combining Codes

In this section we use the structure of the codes F_{4n}, defined and studied in Section II, to obtain linear codes with other parameters. Some of these codes are good in the sense that they have the largest minimum distance known [5].

Concatenating or "pasting" two words x and y of length n and m, respectively, to form a new word $|x|y|$, gives a word of length $n+m$:

$$|x|y| = (x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m).$$

Let $x^{(1)}, x^{(2)},\cdots,x^{(k)}$ and $y^{(1)}, y^{(2)},\cdots,y^{(k)}$ be k basis codewords for an $[n_1, k, d_1]$ and an $[n_2, k, d_2]$ code, respectively. A pasting of these codes may be the $[n_1+n_2, k, d]$ code with $|x^{(1)}|y^{(1)}|,\cdots,|x^{(k)}|y^{(k)}|$ as k basis codewords, where $d \geq d_1 + d_2$.

Theorem 4: Let the code G_{8n}, $n \geq 2$, of length $8n$ be generated by

$$|b^{(i)}|b^{(i)} + 1_{4n}|, \quad i = 1,2,$$
$$|b^{(i)}|b^{(i)}\quad|, \quad 3 \leq i \leq 2n.$$

The code G_{8n} is an $[8n, 2n, 8]$ code and for $n \geq 3$ it has the UEP property with separation vector s, $s_1 = s_2 = 4n$ and $s_i = 8$, $3 \leq i \leq 2n$.

The weight enumerator of G_{8n} is

$$W(G_{8n}; z) = \sum_{i=0}^{\lfloor n/2 \rfloor} \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2i}\binom{n}{2j} z^{2(4i+4j)} + 3 \cdot 2^{2n-2} z^{4n}.$$

Proof: Obviously G_{8n} has dimension $2n$. Let $|x|y|$ be any codeword of G_{8n}. If $x \in B_{4n}^{00}$, then $y = x$ and, according to Theorem 1, $\mathrm{wt}(y) = \mathrm{wt}(x) = 4r$ for some r, $0 \leq r \leq 2\lfloor n/2 \rfloor$. If $x \in B_{4n}^{11}$, then $y = x$ and $\mathrm{wt}(x) = 2n$. If $x \in B_{4n}^{01} \cup B_{4n}^{10}$, then $y = x + 1_{4n}$ and $\mathrm{wt}(y) = 4n - \mathrm{wt}(x)$. The separation vector and the weight enumerator are now easily found. Q.E.D.

Theorem 5: Let the code H_{8n}, $n \geq 2$, of length $8n$ be generated by

$$|b^{(i)}\ |b^{(i)}\quad\quad|, \quad i = 1,2,$$
$$|b^{(i)}\ |b^{(i)} + b^{(i+1)}\quad|, \quad 3 \leq i \leq 2n-1,$$
$$|b^{(2n)}|b^{(2n)} + b^{(3)} + b^{(4)}|.$$

The code H_{8n} is an $[8n, 2n, d]$ code where $d = 2(n+2)$ if $n = 2$, 3 and $d = 12$ otherwise. For $n \geq 5$, H_{8n} has the UEP property with separation vector s, $s_1 = s_2 = 2(n+2)$ and $s_i = 12$ for $3 \leq i \leq 2n$.

Proof: Obviously H_{8n} has dimension $2n$. Let $|x|y|$ be any codeword of H_{8n}. If $x \in B_{4n}^{01} \cup B_{4n}^{10}$, then also $y \in B_{4n}^{01} \cup B_{4n}^{10}$ and so, according to Theorem 1, $\mathrm{wt}(|x|y|) = 2(n+2) + 4r$ for some r, $0 \le r \le 2\lfloor (n-1)/2 \rfloor$. If $x \in B_{4n}^{11}$, then also $y \in B_{4n}^{11}$ and hence $\mathrm{wt}(x) = \mathrm{wt}(y) = 2n$. If $x \in B_{4n}^{00}$, then also $y \in B_{4n}^{00}$. Clearly $\mathrm{wt}(x) = 0$ if and only if $\mathrm{wt}(y) = 0$. If $\mathrm{wt}(x) = 4$, then either $x = b^{(i)}$ for some i, $3 \le i \le 2n$ or $x = b^{(i)} + b^{(i+2r)}$ for some r and i, $0 < r < n$ and $3 \le i \le 2n - 2r$. In both cases $\mathrm{wt}(y) \ge 8$. From this we deduce that if $\mathrm{wt}(y) = 4$, then $\mathrm{wt}(x) \ge 8$. The separation vector is now easily derived. Q.E.D.

Example: Let $n = 3$. The code G_{24} is a $[24, 6, 8]$ code with weight enumerator $1 + 6z^8 + 48z^{12} + 9z^{16}$. The separation vector of G_{24} is $(12, 12, 8, 8, 8, 8)$.

The code H_{24} is a $[24, 6, 10]$ code. The weight enumerator, determined by inspection, is

$$W(H_{24}; z) = 1 + 18z^{10} + 28z^{12} + 12z^{14} + 3z^{16} + 2z^{18}.$$

The proofs of the following theorems are omitted since they are similar to the proofs of Theorem 4 and Theorem 5.

Theorem 6: Let the code I_{12n}, $n \ge 2$, of length $12n$ be generated by

$$\begin{aligned}
&|b^{(i)}\ |b^{(i)} + \mathbf{1}_{4n}|b^{(i)}\ &&|, && i = 1, 2,\\
&|b^{(i)}\ |b^{(i)}\ |b^{(i)} + b^{(i+1)}\ &&|, && 3 \le i \le 2n - 1,\\
&|b^{(2n)}|b^{(2n)}\ |b^{(2n)} + b^{(3)} + b^{(4)}|.
\end{aligned}$$

The code I_{12n} is a $[12n, 2n, d]$ code where $d = 12$ if $n = 2$ and $d = 16$ otherwise. For $n \ge 3$, I_{12n} has the UEP property with separation vector s, $s_1 = s_2 = 5n + 2$, and $s_i = 16$ for $3 \le i \le 2n$.

Theorem 7: Let the code J_{16n}, $n \ge 2$, of length $16n$ be generated by

$$\begin{aligned}
&|b^{(i)}\ |b^{(i)} + \mathbf{1}_{4n}|b^{(i)}\ &&|b^{(i)} + \mathbf{1}_{4n}\ &&|, && i = 1, 2,\\
&|b^{(i)}\ |b^{(i)}\ |b^{(i)} + b^{(i+1)}\ &&|b^{(i)} + b^{(i+1)}\ &&|, && 3 \le i \le 2n - 1,\\
&|b^{(2n)}|b^{(2n)}\ |b^{(2n)} + b^{(3)} + b^{(4)}|b^{(2n)} + b^{(3)} + b^{(4)}|.
\end{aligned}$$

The code J_{16n} is a $[16n, 2n, d]$ code where $d = 16$ if $n = 2$ and $d = 24$ otherwise. For $n \ge 4$, J_{16n} has the UEP property with separation vector s, $s_1 = s_2 = 8n$, and $s_i = 24$ for $3 \le i \le 2n$.

Example: Let $n = 3$. The code I_{36} is a $[36, 6, 16]$ code with separation vector $(17, 17, 16, 16, 16, 16)$, and the code J_{48} is a $[48, 6, 24]$ code. The weight enumerators of both codes can be determined without writing out all codewords,

$$W(I_{36}; z) = 1 + 6z^{16} + 24z^{17} + 16z^{18} + 6z^{20} + 8z^{21} + 3z^{24}$$

and

$$W(J_{48}; z) = 1 + 60z^{24} + 3z^{32}.$$

Copies of F_{4n} may be combined in many other ways, yielding codes again with other parameters or codes with the same parameters but with another weight enumerator. As an example of this latter statement we give the following theorem.

Theorem 8: Let the code K_{12n}, $n \ge 2$, of length $12n$ be generated by

$$\begin{aligned}
&|b^{(1)}\ |b^{(1)}\ &&|b^{(1)} + b^{(2)}\ &&|,\\
&|b^{(2)}\ |b^{(1)} + b^{(2)}\ &&|b^{(2)}\ &&|,\\
&|b^{(3)}\ |b^{(3)} + b^{(4)}\ &&|b^{(3)}\ &&|,\\
&|b^{(i)}\ |b^{(i)} + b^{(i+1)}|b^{(i)} + b^{(i-1)}\ &&|, && 4 \le i \le 2n - 1,\\
&|b^{(2n)}|b^{(2n)}\ &&|b^{(2n)} + b^{(2n-1)}|.
\end{aligned}$$

The code K_{12n} is a $[12n, 2n, d]$ code where $d = 12$ if $n = 2$ and $d = 16$ otherwise. All weights are divisible by 4. For $n \ge 4$, K_{12n} has the UEP property with separation vector s, $s_1 = s_2 = 4n + 4$, and $s_i = 16$ for $3 \le i \le 2n$.

Example: Let $n = 3$. The code K_{36} is a $[36, 6, 16]$ code. The weight enumerator is determined by inspection (compare with I_{36}), $W(K_{36}; z) = 1 + 38z^{16} + 14z^{20} + 11z^{24}$.

Summary

In this correspondence an infinite class of $[4n, 2n, 4]$, $n \ge 2$, binary codes has been studied in some detail. In particular the weight enumerators and automorphism groups have been determined. The detailed knowledge of the weight structure of these codes has led to several other infinite series of binary codes.

References

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North-Holland, 1977.
[2] L. A. Dunning and W. E. Robbins, "Optimal encoding of linear block codes for unequal error protection," *Inform. Contr.*, vol. 37, pp. 150–177, May 1978.
[3] W. J. van Gils, "Two topics on linear unequal error protection codes: Bounds on their length and cyclic code classes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 866–876, Nov. 1983.
[4] L. M. H. E. Driessen, Dutch Patent Nr. 8105799, Dec. 1981.
[5] H. J. Helgert and R. D. Stinaff, "Minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 344–356, May 1973.
[6] M. Hall, *The Theory of Groups*. New York: McMillan, 1964.
[7] V. Pless, "A classification of self-orthogonal codes over GF(2)," *Discrete Math.*, vol. 3, pp. 209–246, 1972.

Further Classifications of Codes Meeting the Griesmer Bound

TOR HELLESETH

***Abstract*—For any (n, k, d) binary linear code, the Griesmer bound says that $n \ge \sum_{i=0}^{k-1} \lceil d/2^i \rceil$, where $\lceil x \rceil$ denotes the smallest integer $\ge x$. We consider codes meeting the Griesmer bound with equality. These codes have parameters**

$$\left(s(2^k - 1) - \sum_{i=1}^{p} (2^{u_i} - 1),\ k,\ s2^{k-1} - \sum_{i=1}^{p} 2^{u_i - 1} \right),$$

where $k > u_1 > \cdots > u_p \ge 1$. We characterize all such codes when $p = 2$ or $u_{i-1} - u_i \ge 2$ for $2 \le i \le p$.

I. Introduction

We let an (n, k, d) code be a binary linear code of length n, dimension k, and minimum distance of at least d. We let $n(k, d)$ be the smallest integer n such that an (n, k, d) code exists. Many efforts have been made to find codes with parameters $(n(k, d), k, d)$. For an extensive list of bounds on $n(k, d)$ the reader should consult the tables of Helgert and Stinaff [1].

A general lower bound on $n(k, d)$, due to Griesmer [2], says

$$n(k, d) \ge \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil, \tag{1.1}$$

Manuscript received September 27, 1982; revised March 7, 1983. This work was presented in part at the IEEE International Symposium on Information Theory, Les Arcs, France, June 21–25, 1982.

The author is with CHOD Norway/SEC, Oslo Mil/Akershus, Oslo 1, Norway.

0018-9448/84/0300-0395$01.00 ©1984 IEEE