Restrictions on the Weight Distribution of Binary Linear Codes Imposed by the Structure of Reed–Muller Codes

Juriaan Simonis

***Abstract*—The words of a binary linear $[n, k]$ code $\mathcal{C}$ whose weights belong to a given subset $I \subset \{0, 1, \cdots, n\}$ constitute a word in a certain Reed–Muller code $\mathfrak{RM}(r, k)$. Appropriate choices of I result in low values of the order r and thus yield restrictions on the weight distribution of $\mathcal{C}$.**

***Index Terms*— Binary linear code, affine code, weight distribution, Reed–Muller code.**

I. Introduction

The even words in a binary linear code $\mathcal{C}$ fill either half or all of $\mathcal{C}$. This simple fact has recently been generalized by Brouwer [1], who proved the following three theorems.

Theorem 1: Let $\mathcal{C}$ be a binary linear code with parameters $[n, k, d]$ all of whose words have even weight, and suppose that the maximum dimension of a doubly even subcode of $\mathcal{C}$ is t. Let $\mathcal{D}$ be the set of words in $\mathcal{C}$ with weight divisible by 4. Then

$$|\mathcal{D}| \in \{2^{k-1} - 2^t, 2^{k-1}, 2^{k-1} + 2^{t-1}\}.$$

Theorem 2: Let $a \geq 1$ be an integer, and let $\mathcal{C}$ be a binary linear code all of whose words have weight divisible by 2^{a-1}. Let $\mathcal{D}$ be the set of words in $\mathcal{C}$ with weight divisible by 2^a. Then

$$|\mathcal{D}| \geq \frac{1}{2^a}|\mathcal{C}|$$

and if equality holds, $\mathcal{D}$ is a subspace of $\mathcal{C}$.

Theorem 3: Let $a \geq 1$ be an integer, and let $\mathcal{C}$ be a binary linear code all of whose words have weight divisible by 2^{a-1}. Let $\mathcal{E}$ be the set of words in $\mathcal{C}$ with weight not divisible by 2^a. If $\mathcal{E} \neq \phi$, then

$$|\mathcal{E}| \geq \frac{1}{2^a}|\mathcal{C}|,$$

and if equality holds then $\mathcal{E}$ is a coset of a subspace of $\mathcal{C}$.

Several elements in these theorems suggest Reed–Muller codes.

i) The nonzero weights in the second order Reed–Muller code $\mathfrak{RM}(2, k)$ are of the form 2^{k-1} or $2^{k-1} \pm 2^t$.

ii) The minimum weight of the ath order Reed–Muller code $\mathfrak{RM}(a, k)$ is equal to 2^{k-a}.

iii) The words of minimum weight in $\mathfrak{RM}(a, k)$ are the $(k - a)$ flats in the affine space $\mathbf{F}_2^k$.

The purpose of this paper is to show that these similarities are no coincidence. The main idea is as follows.

Consider the set $\mathcal{S}_I \subset \mathbf{F}_2^n$ consisting of the words whose weight belongs to a given subset $I \subset \{0, 1, \cdots, n\}$. Let $\deg(\mathcal{S}_I)$ be the degree of $\mathcal{S}_I$, i.e., the degree of its characteristic function as a subset of $\mathbf{F}_2^n$. Then any binary linear $[n, k]$ code $\mathcal{C}$ intersects $\mathcal{S}_I$ in a subset of degree $r \leq \deg(\mathcal{S}_I)$, and $\mathcal{C} \cap \mathcal{S}_I$ can be viewed as a word in the Reed–Muller code $\mathcal{RM}(r, k)$. Hence the number $\sum_{i \in I} A_i(\mathcal{C})$ of words in $\mathcal{C}$ with weight $\in I$ must be a weight in $\mathfrak{RM}(r, k)$, which, especially for small values of r, puts a severe restriction on the weight distribution of $\mathcal{C}$.

Manuscript received June 30, 1992; revised March 29, 1993.

The author is with the Faculty of Technical Mathematics and Informatics, Delft University of Technology, 2600 GA, Delft, Holland.

IEEE Log Number 9215118.

After a short section on Reed–Muller codes, we shall discuss the following two questions.

i) For what subsets $I \subset \{0, 1, \cdots, n\}$ is $\deg(\mathcal{S}_I)$ small?

ii) What conditions on the code $\mathcal{C}$ guarantee that the degree of $\mathcal{C} \cap \mathcal{S}_I$ is small compared to $\deg(\mathcal{S}_I)$?

The obtained results, extensions of Brouwer's theorems, may be useful in nonexistence proofs for binary linear codes with given parameters.

II. Reed–Muller Codes

The standard reference is [6, chap. 13, 14, and 15]. A more geometric description can be found in [7].

Let $\mathcal{E}$ be a k-dimensional $\mathbf{F}_2$-affine space. The power set $\mathfrak{P}(\mathcal{E})$ of $\mathcal{E}$ is a 2^k-dimensional $\mathbf{F}_2$-vector space under the usual addition $\mathcal{X} + \mathcal{Y} := (\mathcal{X} \cup \mathcal{Y}) \backslash (\mathcal{X} \cap \mathcal{Y})$.

Definition 1: For $0 \leq r \leq k$, the rth order Reed–Muller code $\mathfrak{RM}(r, \mathcal{E})$ over $\mathcal{E}$ is the linear subspace of $\mathfrak{P}(\mathcal{E})$ generated by the $(k - r)$-flats (r-codimensional affine subspaces) of the space $\mathcal{E}$. Set $\mathfrak{RM}(r, \mathcal{E}) := \{\phi\}$ for $r < 0$ and $\mathfrak{RM}(r, \mathcal{E}) := \mathfrak{P}(\mathcal{E})$ for $r > k$. If $\mathcal{E} := \mathbf{F}_2^k$, the standard $\mathbf{F}_2$-affine space, we write $\mathfrak{RM}(r, k)$ for $\mathfrak{RM}(r, \mathcal{E})$.

Examples: i) $\mathfrak{RM}(0, \mathcal{E}) = \{\phi, \mathcal{E}\}$.

ii) $\mathfrak{RM}(1, \mathcal{E}) = \{\phi, \mathcal{E}, \text{the affine hyperplanes}\}$. (It is the dual of an extended Hamming code with parameters $[2^k, 2^k - k - 1, 4]$.)

iii) $\mathfrak{RM}(k, \mathcal{E}) = \mathfrak{P}(\mathcal{E})$.

iv) $\mathfrak{RM}(k - 1, \mathcal{E}) = \{\mathcal{X} \subset \mathcal{E} \,|\, |\mathcal{X}| \equiv 0 \pmod 2\}$.

v) $\mathfrak{RM}(k - 2, \mathcal{E}) = \{\mathcal{X} \in \mathfrak{RM}(k - 1, k) \,|\, \sum_{X \in \mathcal{X}} X = o\}$. [$\mathfrak{RM}(k-2, \mathcal{E})$ is the extended Hamming code mentioned under ii)].

Basic Properties: i) If $r < s$, then $\mathfrak{RM}(r, \mathcal{E}) \subset \mathfrak{RM}(s, \mathcal{E})$.

ii) If $\mathcal{X} \in \mathfrak{RM}(r, \mathcal{E})$, $\mathcal{Y} \in \mathfrak{RM}(s, \mathcal{E})$, then $\mathcal{X} \cap \mathcal{Y} \in \mathfrak{RM}(r + s, \mathcal{E})$.

iii) If $\dim(\mathcal{E}) = \dim(\mathcal{E}')$, then the codes $\mathfrak{RM}(r, \mathcal{E})$ and $\mathfrak{RM}(r, \mathcal{E}')$ are equivalent.

A. Degree

Definition 2: The degree $\deg(\mathcal{X}) = \deg_{\mathcal{E}}(\mathcal{X})$ of a subset $\mathcal{X} \subset \mathcal{E}$ is the minimum of $\{r \,|\, \mathcal{X} \in \mathfrak{RM}(r, \mathcal{E})\}$.

Note:

i) $\deg(\mathcal{X} + \mathcal{Y}) \leq \max\{\deg(\mathcal{X}), \deg(\mathcal{Y})\}$.

ii) $\deg(\mathcal{X} \cap \mathcal{Y}) \leq \deg(\mathcal{X}) + \deg(\mathcal{Y})$.

iii) If $\mathcal{C} \in \mathcal{E}$ is an affine subspace, then $\deg_{\mathcal{C}}(\mathcal{X} \cap \mathcal{C}) \leq \deg_{\mathcal{E}}(\mathcal{X})$.

B. Some Properties of $\mathfrak{RM}(r, \mathcal{E})$

Proposition 1:

i) $\dim \mathfrak{RM}(r, \mathcal{E}) = \sum_{i=0}^{r} \binom{k}{i}$.

ii) $\mathfrak{RM}(r, \mathcal{E})^{\perp} = \mathfrak{RM}(k - r - 1, \mathcal{E})$.

iii) Hence $\deg(\mathcal{X}) \leq r$ if and only if $|\mathcal{X} \cap \mathcal{Z}| \equiv 0 \pmod 2$ for a generating set of elements $\mathcal{Z} \in \mathfrak{RM}(k - r - 1, \mathcal{E})$.

C. Polynomial Functions on $\mathbf{F}_2^k$

From the coordinate functions

$$x_i \colon \mathbf{F}_2^k \to \mathbf{F}_2, \quad (a_1, a_2, \cdots, a_k) \mapsto a_i,$$

we form the monomial functions

$$x^I := \prod_{i \in I} x_i \quad (I \subset \{1, 2, \cdots, k\}).$$

Since $x_i x_i = x_i$, all polynomial functions are linear combinations of the x^I. There is a one–one correspondence between the subsets $\mathcal{X} \subset \mathbb{F}_2^k$ and the functions $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$: to a subset $\mathcal{X}$ corresponds its characteristic function $\chi_{\mathcal{X}}$, and, conversely, to a function f corresponds its support $\mathrm{supp}(f)$. A simple counting argument shows that all functions $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ are polynomial. If we define the degree of a function $f := \sum_I a_I x^I$ in the obvious way, we have

$$\deg(f) = \deg(\mathrm{supp}(F)),$$

so $\mathfrak{RM}(r, k) = \{\mathcal{X} \subset \mathbb{F}_2^k \mid \deg(\chi_{\mathcal{X}}) \leq r\}$. (This is the usual definition of Reed–Muller codes.)

D. The Weights of Reed–Muller Codes

We list a few known facts:

Proposition 2: i) The weight of all elements $\mathcal{X} \in \mathfrak{RM}(r, \mathcal{E})$ is divisible by $2^{\lfloor (k-1)/r \rfloor}$. Hence, the occurring weights in $\mathfrak{RM}(1, \mathcal{E})$ are 0, 2^{k-1} and 2^k.

ii) The minimum weight of $\mathfrak{RM}(r, \mathcal{E})$ is equal to 2^{k-r}.

iii) The words of minimum weight in $\mathfrak{RM}(r, \mathcal{E})$ are the $(k-r)$ flats.

iv) If $\mathcal{X} \in \mathfrak{RM}(r, \mathcal{E})$ and $|\mathcal{X}| < 2^{k-r+1}$, then

$$|\mathcal{X}| = 2^{k-r+1} - 2^{k-r+1-\nu}$$

for some integer ν.

v) The occurring weights in $\mathfrak{RM}(2, \mathcal{E})$ are 0, 2^k, 2^{k-1}, and $2^k(1 \equiv 2^{-s})$ where s is the rank of the quadratic form $\chi_{\mathcal{X}}$ determined by the word $\mathcal{X}$. (Cf. Dieudonné [2, p. 33].) Explicit formulas for the weight distribution of $\mathfrak{RM}(2, \mathcal{E})$ can be found in [6].

vi) In [3], the authors claim a classification of all $\mathcal{X} \subset \mathbb{F}_2^k$ with $|\mathcal{X}| < 5 \cdot 2^{k-r-1}$. The results are stated without proof, and the reader is referred to the report [4]. Apart from this result, not very much more is known.

III. The Degree of Symmetric Subsets of $\mathbb{F}_2^n$

We consider subsets of $\mathbb{F}_2^n$ that are invariant under all coordinate permutations. These sets form a $(n+1)$-dimensional linear subspace $\mathfrak{S} \subset \mathfrak{P}(\mathbb{F}_2^n)$, and the constant weight sets

$$\mathcal{S}_i := \{X \in \mathbb{F}_2^n \mid |X| = i\}$$

constitute a basis of $\mathfrak{S}$. Thus, any element of $\mathfrak{S}$ can be represented in the form

$$\mathcal{S}_I := \sum_{i \in I} \mathcal{S}_i$$

where I is a subset of $\{0, 1, \cdots, n\}$. The subsets

$$\mathcal{B}_i := \mathrm{supp}\left(\sum_{|I|=i} x^I\right)$$

of degree i form another basis of $\mathfrak{S}$. These two bases are related as follows.

Proposition 3:

$$\mathcal{B}_j = \sum \binom{i}{j}_2 \mathcal{S}_i \quad \text{and} \quad \mathcal{S}_j = \sum \binom{i}{j}_2 \mathcal{B}_i$$

where $\binom{i}{j}_2 := \binom{i}{j} \pmod 2$.

Proof: A word $X \in \mathbb{F}_2^n$ of weight i is contained in $\mathcal{B}_j$ if and only if an odd number of monomials x^J with $|J| = j$ take the value 1 in X. But this number is equal to $\binom{i}{j}$. The second equality follows from the fact that the binary $(n+1) \times (n+1)$-matrix $\left[\binom{i}{j}_2\right]$ is equal to its inverse. (Use the standard binomial identity $\sum_j \binom{i}{j}\binom{j}{k} = 2^{i-k}\binom{i}{k}$.) □

The following result of Lucas permits us to describe the sets $\mathcal{S}_I$ with $\deg(\mathcal{S}_I) < 2^m$ more explicitly.

Theorem 4: (Lucas [5]). If $\sum_a i_a 2^a$, $\sum_a j_a 2^a$ are the binary expansions of the nonnegative integers i, j, then

$$\binom{i}{j}_2 = \prod_a \binom{i_a}{j_a}.$$

Corollary 1: The degree of $\mathcal{S}_I$ is smaller than 2^m if and only if the subset $I \subset \{0, 1, \cdots, n\}$ is periodic, with period 2^m.

Both $\mathfrak{X} := \{\mathcal{X} \in \mathfrak{S} \mid \deg(\mathcal{X}) < 2^m\}$ and $\mathfrak{Y} := \{\mathcal{S}_I \mid I \text{ is periodic with period } 2^m\}$ are 2^m-dimensional linear subspaces of $\mathfrak{S}$. So we only have to show that the basis $\{\mathcal{B}_0, \mathcal{B}_1, \cdots, \mathcal{B}_{2^m-1}\}$ of $\mathfrak{X}$ is contained in $\mathfrak{Y}$. By Proposition 3, we have

$$\mathfrak{B}_j = \mathcal{S}_I, \quad \text{with } I := \left\{i \middle| \binom{i}{j}_2 \neq 0\right\}.$$

Suppose that $j < 2^m$. Then Lucas' theorem implies that $\binom{i}{j}_2 = \binom{i+2^m}{j}_2$ for all nonnegative integers i. Hence, I is periodic with period 2^m. □

Another useful consequence of Lucas' theorem is the following.

Proposition 4: If $\sum_{a=0}^{m-1} j_a 2^a$ is the binary expansion of the nonnegative integer $j \leq n$, then

$$\sum_{i \equiv j (2^m)} \mathcal{S}_i = \bigcap_{a=0}^{m-1} (\mathcal{B}_{2^a} + (1 - j_a)\mathbb{F}_2^n).$$

Hence, $\deg(\sum_{i \equiv j(2^m)} \mathcal{S}_i) = \text{minimum}\{2^m - 1, n\}$.

Proof: Proposition 3 and Lucas' theorem imply that

$$\sum_{i_a = 1} \mathcal{S}_i = \sum_i \binom{i_a}{1} \mathcal{S}_i = \sum_i \binom{i}{2^a}_2 \mathcal{S}_i = \mathcal{B}_{2^a}.$$

Obviously, we have

$$\sum_{i_a = 0} \mathcal{S}_i = \mathcal{B}_{2^a} + \mathbb{F}_2^n \quad \text{(the complement of } \mathcal{B}_{2^a}).$$

Substitute these two expressions in the right-hand side of the equality

$$\sum_{i \equiv j(2^m)} \mathcal{S}_i = \bigcap_{a=0}^{m-1} \sum_{i_a = j_a} \mathcal{S}_i. \qquad \square$$

IV. The Degree of $\mathcal{C} \cap \mathcal{S}_I$ for Affine Codes $\mathcal{C}$

Let $\mathcal{C} \subset \mathbb{F}_2^n$ be a k-dimensional affine code, i.e., a coset in $\mathbb{F}_2^n$ of a k-dimensional linear code. The intersection $\mathcal{A}_I := \mathcal{C} \cap \mathcal{S}_I$ obviously consists of the words in $\mathcal{C}$ whose weight belongs to the index set I. The mere fact that $\deg_{\mathcal{C}}(\mathcal{A}_I) \leq \deg(\mathcal{S}_I)$ allows us to draw all kinds of conclusions, for instance:

Proposition 5: A linear code $\mathcal{C}$ of dimension ≥ 4 has at least one nonzero word whose weight is divisible by 4.

Proof: By Proposition 4, the set $\sum_{i \equiv 0(4)} \mathcal{S}_i$ has degree 3. So, by Proposition 2 ii), the set $\sum_{i \equiv 0(4)} \mathcal{A}_i$ consists of an even number of codewords. (One of the referees pointed out that we obtain another proof by applying Theorem 1 to the even weight subcode of $\mathcal{C}$.) □

We can say more if we have additional information on the code $\mathcal{C}$. The following proposition, for instance, is a straightforward consequence of Proposition 4.

Proposition 6: Let $m \geq p$ and j arbitrary. If all weights in $\mathcal{C}$ are divisible by 2^p, then the degree of the set $\sum_{i\equiv j(2^m)} \mathcal{A}_i$ does not exceed $2^m - 2^p$.

Proof: If the set $\sum_{i\equiv j(2^m)} \mathcal{A}_i$ is empty, the proposition is trivial. If $\sum_{i\equiv j(2^m)} \mathcal{A}_i$ is nonempty, then j must be divisible by 2^p. Hence, the set $\sum_{i\equiv j(2^m)} \mathcal{S}_i$ of degree $2^m - 1$ is contained in the set $\sum_{i\equiv 0(2^p)} \mathcal{S}_i$ of degree $2^p - 1$. By assumption, the latter set contains the code $\mathcal{C}$, so $\deg_{\mathcal{C}} (\mathcal{C} \cap \sum_{i\equiv 0(2^p)} \mathcal{S}_i) = 0$. Hence,

$$\deg_{\mathcal{C}} \left(\mathcal{C} \cap \sum_{i\equiv j(2^m)} \mathcal{S}_i \right) = \deg \left(\sum_{i=j(2^m)} \mathcal{A}_i \right) \leq (2^m - 1) - (2^p - 1) = 2^m - 2^p. \quad \square$$

Note that Brouwer's theorem 1 corresponds to the case $p = 1$, $m = 2$, and $j = 0$. It directly follows from known facts about the structure of second order Reed–Muller codes. Much more can be said if $p = m - 1$.

Proposition 7: If all weights in the linear code $\mathcal{C}$ are divisible by 2^{m-1}, then the degree of $\sum_{i\equiv 0(2^m)} \mathcal{A}_i$ does not exceed m.

Proof: (Based on Brouwer's proofs of Theorems 2 and 3.) In virtue of Proposition 1, part iii), we have to show that an $(m + 1)$-dimensional linear code $\mathcal{C}$ all of whose words have weight divisible by 2^{m-1} must have an even number of codewords whose weight is divisible by 2^m. We proceed by induction on m. The case $m = 1$ is trivial. Take $m \geq 2$ and choose a minimal codeword $X \in \mathcal{C}$ such that $|X| \equiv 2^{m-1}(2^m)$. (We are done if X does not exist.) The formula

$$|X + Y| - |Y| = |X| - 2|X \cap Y|$$

implies that $|X \cap Y| \equiv 0(2^{m-2})$ for all $Y \in \mathcal{C}$. The punctured code $\mathcal{C}_{\overline{X}} := \{Y \backslash X \mid Y \in \mathcal{C}\}$ satisfies the induction hypothesis for $m - 1$, so it contains an even number of words with $|Y \backslash X| \equiv 0(2^{m-1})$. Now from

$$|X + Y| \equiv |Y|(2^m) \Leftrightarrow 2|X \cap Y| \equiv 2^{m-1}(2^m) \Leftrightarrow |Y \backslash X| \equiv 2^{m-2}(2^{m-1})$$

we infer that an even number of cosets of $\{\phi, X\}$ in $\mathcal{C}$ contains exactly one word whose weights is divisible by 2^m and each of the remaining cosets contains an even number of words whose weight is divisible by 2^m. $\square$

Open Problem: Does a result comparable to Proposition 7 exist for $p \leq m-2$? The first nontrivial case is $m = 4$, $p = 2$. Proposition 6 implies that in all doubly even codes the words whose weight is divisible by 16 constitute a set of degree ≤ 12. On the other hand, the direct sum of three [7, 3, 4] simplex codes is 9-dimensional code for which the zero vector is the only word whose weight is divisible by 16. Does a doubly even code with $\deg (\sum_{i\equiv 0(16)} \mathcal{A}_i) = 10$ exist? The following proposition may be of some value.

Proposition 8: Let $\mathcal{C}$ be a binary linear $[n, k]$ code, and let $\mathcal{X} \subset \mathcal{C}$ be any subset. Then $\deg_{\mathcal{C}} (\mathcal{X}) < k - r$ if and only if all shortened codes $\mathcal{C}^{\overline{T}}$ with respect to coordinate sets T of cardinality $\leq r$ intersect $\mathcal{X}$ in an even number of codewords.

Proof: The codes $\mathcal{C}^{\overline{T}}$ with $|T| \leq r$ generate the Reed–Muller code $\mathfrak{RM}(r, \mathcal{C})$. Now apply part iii) of Proposition 1. $\square$

Example: Let $\mathcal{C}$ be the extended binary Golay code, and let $I := \{0, 16\}$. Using the fact that the words of fixed weight in $\mathcal{C}$ form a five-design, we calculate the number of codewords in $\mathcal{C} \cap \mathcal{A}_I$. For $|T| = 0, 1, 2, 3, 4, 5$, this number is 760, 254, 78, 22, 6, 2, respectively, but for $|T| = 6$, odd intersections must occur. Hence, $\deg (\mathcal{A}_I) = 6$.

REFERENCES

[1] A. E. Brouwer, "The linear programming bound for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 677–680, 1993.

[2] J. Dieudonné, *La géométrie des groupes classiques.* Berlin: Springer, 1971.

[3] T. Kasami, N. Tokura, and S. Azumi, "On the weight enumeration of weights less than 2.5d of Reed–Muller codes," *Inform. Contr.*, vol. 30, pp. 380–395, 1976.

[4] ——, "On the weight enumeration of weights less than 2.5d of Reed–Muller Codes," Faculty of Eng. Sci., Rep. Osaka Univ., Japan, 1974.

[5] M. E. Lucas, "Sur les congruences des nombres Euleriennes, et des coefficients différentials des fonctions trigonométriques, suivant un-module premier," *Bull. Soc. Math. France*, vol. 6, pp. 49–54, 1878.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* New York: North-Holland, 1983.

[7] J. Simonis, "Reed-Muller codes," Faculty of Mathemat. Inform., Rep. 87-23, ISSN 0920-8577, Delft Univ. of Technol., 1987.

On a Class of Optimal Nonbinary Linear Unequal-Error-Protection Codes for Two Sets of Messages

Robert H. Morelos-Zaragoza and Shu Lin

***Abstract*— Several authors have addressed the problem of designing good linear unequal error protection (LUEP) codes. However, very little is known about good *nonbinary* LUEP codes. We present a class of *optimal nonbinary* LUEP codes for two different sets of messages. By combining t-error-correcting Reed–Solomon (RS) codes and shortened nonbinary Hamming codes, we obtain nonbinary LUEP codes that protect one set of messages against any t or fewer symbol errors and the remaining set of messages against any single symbol error. For $t \geq 2$, we show that these codes are optimal in the sense of achieving the Hamming lower bound on the number of redundant symbols of a nonbinary LUEP code with the same parameters.**

***Index Term*—Unequal error protection codes.**

I. INTRODUCTION

Let C be a linear (n, k) block code over $\mathrm{GF}(q)$ with generator matrix G. Let message vectors $\overline{u} \in \mathrm{GF}(q)^k$ consist of 2 parts $\overline{u}_1$, $\overline{u}_2$ where $\overline{u}_i$ is a k_i-symbol component message, for $i = 1, 2$, $k = k_1 + k_2$, i.e.,

$$\overline{u} = (\overline{u}_1, \overline{u}_2), \quad \overline{u}_1 \in \mathrm{GF}(q)^{k_1}, \quad \overline{u}_2 \in \mathrm{GF}(q)^{k_2}.$$

Define the *separation vector* of C as

$$\overline{s}(G) = (s_1(G), s_2(G))$$

with

$$s_i(G) = \min \{\mathrm{wt}(\overline{u}G) | \overline{u}_j \in \mathrm{GF}(q)^{k_j}, \ j = 1, 2, \ \overline{u}_i \neq 0\}$$

where $i = 1, 2$, $k = k_1 + k_2$, and $\mathrm{wt}(\overline{x})$ is the Hamming weight of $\overline{x} \in \mathrm{GF}(q)^n$. The parameter

$$t_i(G) \triangleq \lfloor (s_i(G) - 1)/2 \rfloor,$$

Manuscript received June 9, 1992; revised October 23, 1993. This work was supported by the NSF under Grants NCR-88813480, NCR-9115400, and by NASA under Grant NAG 5-931. This paper was presented in part at the International Symposium on Information Theory and Its Applications, Honolulu, HI, November 27–30, 1990.

The authors are with the Department of Electrical Engineering, University of Hawaii at Manoa, Honolulu, HI 96822.

IEEE Log Number 9215117.