Elementary 2-group character codes

Kohel, David R.; Ding, Cunsheng; Ling, San

2000

Ding, C., Kohel, D. R., & Ling, S. (2000). Elementary 2-group character codes. IEEE Transactions on Information Theory, 46(1), 280-284.

https://hdl.handle.net/10356/96092

https://doi.org/10.1109/18.817529

Elementary 2-Group Character Codes

Cunsheng Ding, *Member, IEEE*, David Kohel, *Member, IEEE*, and San Ling

***Abstract*—In this correspondence we describe a class of codes over GF (q), where q is a power of an odd prime. These codes are analogs of the binary Reed–Muller codes and share several features in common with them. We determine the minimum weight and properties of these codes. For a subclass of codes we find the weight distribution and prove that the minimum nonzero weight codewords give 1-designs.**

***Index Terms*—Group character codes, linear codes, Reed–Muller codes.**

I. Introduction

In this correspondence we describe a class of group character codes $C_q(r, n)$, defined over GF (q), with parameters $[2^n, s_n(r), 2^{n-r}]$, where q is a power of an odd prime and

$$s_n(k) = \sum_{i=0}^{k} \binom{n}{i}.$$

The codes $C_q(r, n)$ are defined in analogy with the binary Reed–Muller codes and have the same parameters [2]. Moreover, as for Reed–Muller codes, $C_q(r, n)$ is generated by minimum-weight codewords, and the dual of $C_q(r, n)$ is equivalent to $C_q(n-r-1, n)$, which is the analog of the equality $R(r, n)^\perp = R(n-r-1, n)$.

The purpose of this correspondence is to describe this class of codes, to determine the dimensions and minimum distances, to characterize the dual codes, and to find the weight distribution and associated 1-designs for the subclass $C_q(1, n)$.

II. Abelian Group Character Codes

Let A be an additive Abelian group of exponent m and order N, with 0 as the identity element. Let K be a finite field whose characteristic does not divide N and which contains the mth roots of unity. Let K^* denote the multiplicative group of nonzero elements of K and let M denote the multiplicative group of characters from A to K^*. The group M is isomorphic noncanonically to A [3, Ch. VI]. In particular, we have $|M| = |A| = N$.

The following lemma is a well-known result, known as the orthogonality relations in character theory [3, Ch. VI, Proposition 4].

Lemma 1. Orthogonality Relations: Let A be a finite additive Abelian group of order N and let M be the group of characters of A. For characters f, g in M and elements x, y in A, we have

$$1) \quad \sum_{x \in A} f(x)g(x) = \begin{cases} N, & \text{if } f = g^{-1} \\ 0, & \text{if } f \neq g^{-1} \end{cases}$$

$$2) \quad \sum_{f \in M} f(x)f(y) = \begin{cases} N, & \text{if } x = -y \\ 0, & \text{if } x \neq -y. \end{cases}$$

Let $M = \{f_0, f_1, \cdots, f_{N-1}\}$, where f_0 is the trivial character. For any subset X of A, we define a linear code C_X over K as

$$C_X = \left\{ (c_0, c_1, \cdots, c_{N-1}) \in K^N : \sum_{i=0}^{N-1} c_i f_i(x) = 0 \text{ for all } x \in X \right\}.$$

Let $X = \{x_0, x_1, \cdots, x_{t-1}\}$ be a subset of A and let X^c be the complement of X in A, indexed such that $A = \{x_0, x_1, \cdots, x_{N-1}\}$.

Proposition 2: Let A and X be as above. For $0 \le i \le N-1$, let $\boldsymbol{v}_i$ denote the vector $(f_0(x_i), f_1(x_i), \cdots, f_{N-1}(x_i))$. Then the set $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{N-1}\}$ is linearly independent. In particular

$$H = [f_{j-1}(x_{i-1})]_{1 \le i \le t, 1 \le j \le N}$$

has rank t and is a parity-check matrix of C_X

$$G = [f_{j-1}(-x_{t-1+i})]_{1 \le i \le N-t, 1 \le j \le N}$$

has rank $N-t$ and is a generator matrix for C_X, so C_X is an $[N, N-t]$ linear code over K. Moreover

$$[f_{j-1}(-x_{i-1})]_{1 \le i \le t, 1 \le j \le N}$$

is a generator matrix for C_{X^c} and $C_X \oplus C_{X^c} = K^N$.

Proof: The linear independence of the set $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{N-1}\}$ follows from Lemma 1. The other conclusions of the proposition then follow from this linear independence. □

III. Elementary 2-Group Character Codes

Hereafter we let A be the elementary 2-Abelian group $(\boldsymbol{Z}/2\boldsymbol{Z})^n$, for which we prescribe a basis $\{e_1, \cdots, e_n\}$ of generators. Moreover, we denote the neutral element of A by e_0. For the field K we take a finite field GF (q) for q odd. Since $\{\pm 1\}$ is contained in GF (q), the character group M of A is defined. Relative to the basis for A we can define characters by $f_j(e_i) = (-1)^{j_{i-1}}$, where

$$j = \sum_{k=0}^{n-1} j_k 2^k, \qquad \text{for } 0 \le j < 2^n.$$

One easily verifies that this gives an indexing $M = \{f_0, \cdots, f_{2^n-1}\}$ on the group of characters from A to GF $(q)^*$, where GF $(q)^*$ is defined to be GF $(q) \backslash \{0\}$.

Theorem 3: For any subset X of A, let $X^c = A \backslash X$. Then the dual code $C_X^\perp$ equals C_{X^c}.

Proof: This follows from the orthogonality relations of Lemma 1, the description of a generator matrix for C_{X^c} of Proposition 2, and from the fact that every element of A is its own inverse. □

The classes of codes over GF (q) described in this section have many subclasses of codes. Different choices of the set X give different subclasses of codes over GF (q). We now describe a subclass of codes over GF (q) which have the same parameters as the binary Reed–Muller codes.

Manuscript received February 10, 1999; revised June 12, 1999. The work of C. Ding and S. Ling was supported in part under Grant RP 960668/M.

C. Ding is with the Department of Computer Science, National University of Singapore, Lower Kent Ridge Road, Singapore 119260 (e-mail: dingcs@comp.nus.edu.sg).

D. Kohel was with the Department of Mathematics, National University of Singapore, Lower Kent Ridge Road, Singapore 119260 . He is now with the School of Mathematics and Statistics, Carslaw Building, F07, University of Sydney, Sydney, NSW 2006, Australia (e-mail: kohel@maths.usvd.edu.au).

S. Ling is with the Department of Mathematics, National University of Singapore, Lower Kent Ridge Road, Singapore 119260 (e-mail: matlings@math.nus.edu.sg).

Communicated by I. F. Blake, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(00)00075-4.

Definitions: The Hamming weight $\|a\|$ of an element $a = a_1e_1 + \cdots + a_ne_n$ of A is defined to be the number of nonzero a_k. For $-1 \le r \le n$, let

$$X(r, n) = \{a \in A: \|a\| > r\}$$

and let $C_q(r, n)$ denote the code $C_{X(r,n)}$ over GF (q). For a word $\boldsymbol{c} = (c_0, \cdots, c_{2^n-1})$ in K^{2^n}, let the support of $\boldsymbol{c}$ be defined as

$$\mathrm{Supp}\,(\boldsymbol{c}) = \{i: 0 \le i < 2^n, \text{ and } c_i \ne 0\}$$

and let its weight wt $(\boldsymbol{c})$ be defined as $|\mathrm{Supp}\,(\boldsymbol{c})|$. By convention we define the minimum distance of the zero code to be ∞, which we represent by any integer larger than the block length of the code.

We use $|$ to denote concatenation of codewords, and for two sets U and V of codewords define $U\|V$ to be the set

$$\{\boldsymbol{u}|(\boldsymbol{u}+\boldsymbol{v}): \boldsymbol{u} \in U, \boldsymbol{v} \in V\}.$$

Lemma 4: The dimension of the code $C_q(r, n)$ is

$$s_n(r) = \sum_{j=0}^{r} \binom{n}{j}.$$

Proof: This follows from Proposition 2 and the definition of $X(r, n)$. □

Lemma 5: The code $C_q(r+1, n+1)$ decomposes as the direct sum

$$C_q(r+1, n)\|C_q(r, n) = (C_q(r+1, n)\|\{\boldsymbol{0}\}) \oplus (\{\boldsymbol{0}\}\|C_q(r, n))$$

where $\{\boldsymbol{0}\}$ is the zero code in K^{2^n}.

Proof: For vector subspaces U and V of K^{2^n} it is clear from the definitions that $U\|V = U\|\{\boldsymbol{0}\} \oplus \{\boldsymbol{0}\}\|V$. Moreover, by the combinatorial equality

$$s_n(r) + s_n(r+1) = s_{n+1}(r+1)$$

Lemma 4 and the linear independence of $C_q(r+1, n)\|\{\boldsymbol{0}\}$ and $\{\boldsymbol{0}\}\|C_q(r, n)$ imply the result provided that both are contained in $C_q(r+1, n+1)$.

Let A_n be the elementary 2-Abelian group generated by $\{e_1, \cdots, e_n\}$, identified as a subgroup of $A_{n+1} = A_n \oplus \boldsymbol{Z}/2\boldsymbol{Z}\ e_{n+1}$. The character f_j on A_n identifies with the character f_j on A_{n+1} by setting $f_j(e_{n+1}) = 1$ for all $0 \le j \le 2^n - 1$. Then by definition $f_{j+2^n} = f_j f_{2^n}$, where

$$f_{2^n}(e_i) = \begin{cases} -1, & \text{if } i = n+1 \\ 1, & \text{otherwise.} \end{cases}$$

The words in $C_q(r+1, n)\|\{\boldsymbol{0}\}$ are of the form $\boldsymbol{c}|\boldsymbol{c}$ such that $\boldsymbol{c} = (c_0, \cdots, c_{2^n-1})$ and

$$\sum_{j=0}^{2^n-1} c_j f_j(a) = 0$$

for all a in $X(r+1, n)$. One readily verifies that $C_q(r+1, n)\|\{\boldsymbol{0}\} = C_{X_1}$, where

$$X_1 = X(r+1, n) \cup (A_n + e_{n+1}).$$

Similarly, $\{\boldsymbol{0}\}\|C_q(r, n) \subseteq C_{X_2}$, where

$$X_2 = X(r, n) \cup (X(r, n) + e_{n+1}).$$

Since X_1 and X_2 contain $X(r+1, n+1)$, both C_{X_1} and C_{X_2} are contained in $C_q(r+1, n+1)$ and the result holds. □

Theorem 6: $C_q(r, n)$ is a $[2^n, s_n(r), 2^{n-r}]$ code over GF (q).

Proof: It only remains to prove the correctness of the minimum distance. Since $X(0, n) = A\backslash\{e_0\}$, a generator matrix for $C_q(0, n)$ is

$$[f_0(e_0)\, f_1(e_0) \cdots f_{2^n-1}(e_0)] = [1 \cdots 1].$$

Therefore, $C_q(0, n)$ has minimum weight 2^n.

At the other extreme, $X(n, n)$ is empty, so $C_q(n, n) = K^{2^n}$ and $C_q(n, n)$ has minimum weight 1. In particular, it follows that the minimum weight is correct for $n = 1$ and $0 \le r \le 1$.

Suppose now that Theorem 6 gives the correct minimum distance for some $n \ge 1$ and all $0 \le r \le n$. By Lemma 5, a word $\boldsymbol{c}$ in $C_q(r+1, n+1)$ is of the form

$$\boldsymbol{c} = \boldsymbol{u}|(\boldsymbol{u}+\boldsymbol{v})$$

where $\boldsymbol{u}$ and $\boldsymbol{v}$ are codewords in $C_q(r+1, n)$ and $C_q(r, n)$, respectively. Then

$$\mathrm{wt}(\boldsymbol{c}) \ge 2\mathrm{wt}(\boldsymbol{u}) + \mathrm{wt}(\boldsymbol{v}) - 2|\mathrm{Supp}(\boldsymbol{u}) \cap \mathrm{Supp}(\boldsymbol{v})| \ge \mathrm{wt}(\boldsymbol{v}) \ge 2^{n-r}.$$

Conversely, $\{\boldsymbol{0}\}\|C_q(r, n)$ is a subcode of $C_q(r+1, n+1)$ with minimum distance 2^{n-r}, so the minimum distance of $C_q(r+1, n+1)$ is 2^{n-r}. □

Theorem 7: The minimum nonzero weight codewords generate $C_q(r, n)$.

Proof: Let $M_q(r, n)$ denote the set of minimum nonzero weight codewords of $C_q(r, n)$. The result is clear for $n = 1$ and all r, and likewise for $r = -1$ and all n. Moreover, $C_q(r+1, n+1)$ is generated by

$$M_q(r+1, n)\|\{\boldsymbol{0}\} \cup \{\boldsymbol{0}\}\|M_q(r, n)$$

by the direct sum of Lemma 5. This set is contained in $M_q(r+1, n+1)$, from which the result holds by induction. □

Let $\mathcal{G}$ be defined as the subgroup in the group of linear automorphisms of K^{2^n} generated by permutations of coordinates and by multiplications of coordinates by elements of K^*. Two codes C and C' are called equivalent if and only if $C' = \phi(C)$ for some $\phi \in \mathcal{G}$.

Theorem 8: The dual code $C_q(r, n)^\perp$ is equivalent to $C_q(n-r-1, n)$.

Proof: The theorem clearly holds for $r = n$, so we assume henceforth that $0 \le r < n$. Let $\mu = e_1 + \cdots + e_n$. Then the equality

$$X(r, n)^c = \mu + X(n-r-1, n)$$

follows immediately from the definitions. By Theorem 3 and the definitions of the codes, one easily verifies that the map

$$K^{2^n} \to K^{2^n}$$

$$(c_0, \cdots, c_{2^n-1}) \mapsto (f_0(\mu)c_0, \cdots, f_{2^n-1}(\mu)c_{2^n-1})$$

is an automorphism of K^{2^n} of order two, which induces an equivalence of $C_q(r, n)^\perp$ and $C_q(n-r-1, n)$ and vice versa. □

Corollary 9: $C_q(r, n)^\perp$ is a $[2^n, s_n(n-r-1), 2^{r+1}]$ code which is generated by its minimum nonzero weight codewords.

Proof: The conclusions follow from Theorems 6–8. □

Remark: The Reed–Muller codes $R(r, n)$ are well-known to have the same parameters $[2^n, s_n(r), 2^{n-r}]$ as the codes $C_q(r, n)$, so the latter can be viewed as analogs over GF (q) of the corresponding binary Reed–Muller codes. Moreover, we have

$$R(r,\, n)^{\perp} = R(n-r-1,\, n)$$

of which Theorem 8 is its analog. While strict equality of $C_q(r,\, n)^{\perp}$ and $C_q(n-r-1,\, n)$ does not hold, the proof shows that the equivalence *is* a simple coordinate twist. Stated formally, this says that $C_q(n-r-1,\, n)$ is the dual of $C_q(r,\, n)$ with respect to the twisted inner product

$$\langle \boldsymbol{u},\, \boldsymbol{v}\rangle = \sum_{j=0}^{2^n-1} f_j(\mu)\, u_j\, v_j$$

on vectors $\boldsymbol{u} = (u_0,\, \cdots,\, u_{2^n-1})$ and $\boldsymbol{v} = (v_0,\, \cdots,\, v_{2^n-1})$ in K^{2^n}.

Example 1: Consider $n = 3$. Then $C_3(1,\, 3)$ is a [8, 4, 4] ternary code with generator matrix

$$\begin{bmatrix} 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \end{bmatrix}$$

and weight enumerator polynomial $1 + 24x^4 + 16x^5 + 32x^6 + 8x^8$. In Theorem 17, we show that the support of the codewords of minimum nonzero weight form a 1-(8, 4, 6) design. □

Example 2: Consider $n = 4$. Then $C_3(2,\, 4)$ is a [16, 5, 8] ternary code with generator matrix as seen in the matrix at the bottom of this page and weight enumerator polynomial

$$1 + 40x^8 + 80x^{10} + 32x^{11} + 80x^{12} + 10x^{16}.$$

Its dual code $C_3(2,\, 4)^{\perp}$ is a [16, 11, 4] code with weight enumerator polynomial

$$\begin{aligned} &1 + 200x^4 + 352x^5 + 2544x^6 + 5600x^7 + 13740x^8 \\ &+ 23840x^9 + 34272x^{10} + 36480x^{11} + 30840x^{12} \\ &+ 18400x^{13} + 8720x^{14} + 1824x^{15} + 334x^{16}. \end{aligned}$$ □

IV. The Weight Distribution in $C_q(1,\, n)$

Let the characters f_j be as defined previously for $0 \le j < 2^n$ and define vectors $\boldsymbol{v}_i = (f_0(e_i),\, \cdots,\, f_{2^n-1}(e_i))$ for $0 \le i \le n$. In particular, $\boldsymbol{v}_0$ is the vector $(1,\, \cdots,\, 1)$ and $\{\boldsymbol{v}_0,\, \boldsymbol{v}_1,\, \cdots,\, \boldsymbol{v}_n\}$ is a basis for the code $C_q(1,\, n)$.

Let $V = \mathrm{GF}(q)^n$ and for $\boldsymbol{a}$ in V let $\|\boldsymbol{a}\|$ denote its Hamming weight. For $\boldsymbol{a} = (a_1,\, \cdots,\, a_n)$ in V, set $\boldsymbol{a} \cdot (\boldsymbol{v}_1,\, \cdots,\, \boldsymbol{v}_n)$ equal to the dot product $\sum_{i=1}^{n} a_i \boldsymbol{v}_i$. The collection of vectors of the form $\sum_{i=1}^{n} a_i \boldsymbol{v}_i$ constitute a subcode $C_q^0(1,\, n)$ of codimension 1. We first describe the weight distribution in $C_q^0(1,\, n)$ then treat the nontrivial cosets $a_0\boldsymbol{v}_0 + C_q^0(1,\, n)$.

We begin with a series of lemmas which reduce the analysis of the weight distribution to the weights of codewords in subsets of $C_q^0(1,\, n)$.

Lemma 10: Let $\boldsymbol{a}$ have Hamming weight m in V. Then the vector $\boldsymbol{v} = \boldsymbol{a} \cdot (\boldsymbol{v}_1,\, \cdots,\, \boldsymbol{v}_n)$ has Hamming weight $2^n - 2^{n-m}|W|$, where

$$W = \left\{ \boldsymbol{b} = (b_1,\, \cdots,\, b_n) \in V\colon b_i = \pm a_i \text{ for all } i \text{ and } \sum_{i=1}^{n} b_i = 0 \right\}.$$

Proof: Clearly $\boldsymbol{a} \cdot (\boldsymbol{v}_1,\, \cdots,\, \boldsymbol{v}_n)$ has weight 2^n less the number of j for which

$$\sum_{i=1}^{n} a_i f_j(e_i) = 0. \tag{1}$$

For any such j we associate the vector $\boldsymbol{b} = (a_1 f_j(e_1),\, \cdots,\, a_n f_j(e_n))$ in W. But for any $\boldsymbol{b}$ in W there are 2^{n-m} indices j for which (1) holds and has associated vector $\boldsymbol{b}$. Namely, if we let $j = \sum_{i=0}^{n-1} j_i 2^i$ be one such value, then $k = \sum_{i=0}^{n-1} k_i 2^i$ is another if and only if $k_{i-1} = j_{i-1}$ whenever $a_i \ne 0$. □

Let $s = (q-1)/2$ and let $\{\alpha_1,\, \cdots,\, \alpha_{q-1}\}$ be an indexing of the elements of $\mathrm{GF}(q)^*$ such that $\alpha_{i+s} = -\alpha_i$. For an element $\boldsymbol{a} = (a_1,\, a_2,\, \cdots,\, a_m)$ of V, define for each i

$$n_i(\boldsymbol{a}) = |\{k\colon 1 \le k \le n \text{ and } a_k = \pm\alpha_i\}|.$$

Lemma 11: For $\boldsymbol{a}$ in V, let $n_1 = n_1(\boldsymbol{a}),\, \cdots,\, n_s = n_s(\boldsymbol{a})$ be the associated multiplicities. Then the weight of the vector $\boldsymbol{v} = \boldsymbol{a} \cdot (\boldsymbol{v}_1,\, \cdots,\, \boldsymbol{v}_n)$ is

$$2^n - 2^{n-m} \sum_{\substack{-n_i \le m_i \le n_i \\ m_i \equiv n_i \bmod 2 \\ \sum_{i=1}^{s} m_i\alpha_i = 0}} \prod_{i=1}^{s} \binom{n_i}{\frac{n_i + m_i}{2}}.$$

In particular, the weight of $\boldsymbol{v}$ depends only on the multiplicities $n_1,\, \cdots,\, n_s$, and not on the ordering of the coordinates of $\boldsymbol{a}$.

Proof: By Lemma 10, it suffices to determine $|W|$. Let $\boldsymbol{b}$ be in W, and for each i let u_i be the number of occurrences of α_i in the coordinates of $\boldsymbol{b}$. Then the number of occurrences of $-\alpha_i$ in this vector is $n_i - u_i$. It follows that

$$\sum_{i=1}^{n} b_i = \sum_{i=1}^{s} (u_i\alpha_i - (n_i - u_i)\alpha_i) = \sum_{i=1}^{s} (2u_i - n_i)\alpha_i$$

and we set $m_i = 2u_i - n_i$. Since there are $\prod_{i=1}^{s} \binom{n_i}{u_i}$ vectors $\boldsymbol{b}$ in W with associated multiplicities $n_1,\, \cdots,\, n_s$, we obtain

$$|W| = \sum_{\substack{0 \le u_i \le n_i \\ \sum_{i=1}^{s} m_i\alpha_i = 0}} \prod_{i=1}^{s} \binom{n_i}{u_i}$$

$$\begin{bmatrix} 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \end{bmatrix}$$

from which the lemma follows. $\square$

The following lemma gives the weight of vectors in the nontrivial coset of $C_q^0(1, n)$ in $C_q(1, n)$, and is proved similarly.

Lemma 12: For $\boldsymbol{a}$ in V, let $n_1 = n_1(\boldsymbol{a}), \cdots, n_s = n_s(\boldsymbol{a})$ be the associated multiplicities. Then the weight of a vector $\boldsymbol{v} = a_0\boldsymbol{v}_0 + \boldsymbol{a} \cdot (\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n)$, with $a_0 \neq 0$, is

$$2^n - 2^{n-m} \sum_{\substack{-n_i \le m_i \le n_i \\ m_i \equiv n_i \bmod 2 \\ \sum_{i=1}^{s} m_i \alpha_i = -1}} \prod_{i=1}^{s} \binom{n_i}{\frac{n_i+m_i}{2}}.$$

In particular, the weight of $\boldsymbol{v}$ depends only on the multiplicities $n_1, \cdots, n_s$, and not on the ordering of the coordinates of $\boldsymbol{a}$.

When $q = 3$ the product in Lemmas 11 and 12 consists of one term. In this case, we obtain a precise formula for the weight distribution in $C_3^0(1, n)$ and $C_3(1, n)$. First we prove a result concerning sums of binomial coefficients in progressions.

Lemma 13: Let m be a positive integer. Define

$$a = \sum_{\substack{0 \le j \le m \\ j \equiv 0 \bmod 3}} \binom{m}{j} \qquad b = \sum_{\substack{0 \le j \le m \\ j \equiv 1 \bmod 3}} \binom{m}{j} \qquad c = \sum_{\substack{0 \le j \le m \\ j \equiv 2 \bmod 3}} \binom{m}{j}.$$

1) If $m = 3k$, then

$$a = \frac{2^m + (-1)^k 2}{3} \qquad b = c = \frac{2^m - (-1)^k}{3}.$$

2) If $m = 3k + 1$, then

$$a = b = \frac{2^m + (-1)^k}{3} \qquad c = \frac{2^m - (-1)^k 2}{3}.$$

3) If $m = 3k + 2$, then

$$b = \frac{2^m + (-1)^k 2}{3} \qquad a = c = \frac{2^m - (-1)^k}{3}.$$

Proof: Let m be of the form $3k + i$, with $0 \le i \le 2$, and let ϵ be a primitive third root of unity. We note that ϵ has trace -1 and that $\epsilon + 1$ is a cube root of -1 whose square is ϵ. Expanding the binomial expression we obtain

$$(\epsilon + 1)^m = \sum_{j=0}^{m} \binom{m}{j} \epsilon^{m-j}.$$

In the three cases $i = 0, 1$, and 2, respectively, we obtain

$$\begin{aligned} (-1)^k &= a + c\epsilon + b\epsilon^2 \\ (-1)^k(\epsilon + 1) &= b + a\epsilon + c\epsilon^2 \\ (-1)^k \epsilon &= c + b\epsilon + a\epsilon^2. \end{aligned}$$

TABLE I
THE WEIGHT DISTRIBUTION IN $C_3^0(1, n)$

$0 \le m \le n$	Weight	Frequency
$m = 3k$	$2^n - 2^{n-m}(2^m + (-1)^k 2)/3$	$\binom{n}{m}2^m$
$m = 3k+1$	$2^n - 2^{n-m}(2^m - (-1)^k 2)/3$	$\binom{n}{m}2^m$
$m = 3k+2$	$2^n - 2^{n-m}(2^m + (-1)^k 2)/3$	$\binom{n}{m}2^m$

TABLE II
THE WEIGHT DISTRIBUTION IN $C_3(1, n)\backslash C_3^0(1, n)$

$0 \le m \le n$	Weight	Frequency
$m = 3k$	$2^n - 2^{n-m}(2^m - (-1)^k)/3$	$\binom{n}{m}2^{m+1}$
$m = 3k+1$	$2^n - 2^{n-m}(2^m + (-1)^k)/3$	$\binom{n}{m}2^{m+1}$
$m = 3k+2$	$2^n - 2^{n-m}(2^m - (-1)^k)/3$	$\binom{n}{m}2^{m+1}$

Taking the trace of 1 and ϵ times the corresponding equation, together with the equation $2^m = a + b + c$, gives the asserted result. $\square$

Theorem 14: The weight distribution in the code $C_3^0(1, n)$ is given by Table I and in $C_3(1, n)\backslash C_3^0(1, n)$ by Table II.

Proof: The weights follow by applying Lemma 13 to the weight formulas of Lemmas 11 and 12. The frequency of a given weight is determined by counting the number of $\boldsymbol{a}$ in V with Hamming weight m. $\square$

Corollary 15: The weight distribution of the dual code $C_3(n - 2, n)^{\perp}$ is given in Tables I and II.

Proof: This follows from the equivalence with $C_3(1, n)$ of Theorem 8. $\square$

Having determined the weight distribution in $C_3(1, n)$, we now determine the minimum nonzero weight codewords.

Theorem 16: The minimum nonzero weight codewords in $C_3(1, n)$ are precisely the distinct words $a\boldsymbol{v}_i + b\boldsymbol{v}_j$, for a, b in GF$(3)^*$ and $0 \le i < j \le n$. In particular, they are $2n(n + 1)$ in number, and two words have the same support if and only if one is a multiple of the other.

Proof: By Theorem 6, the minimum nonzero weight is 2^{n-1}. By Theorem 14, the weight 2^{n-1} codewords are those of the form $a\boldsymbol{v}_i + b\boldsymbol{v}_j$, of which there are $2n(n - 1)$. The final statement is an immediate consequence. $\square$

Corollary 17: The set of supports of the minimum nonzero weight codewords of $C_3(1, n)$ is a 1-$(2^n, 2^{n-1}, n(n + 1)/2)$ design.

Proof: By Theorem 6, the minimum nonzero weight supports are subsets of the 2^n coordinate positions of size 2^{n-1}, and by Theorem 16 are $n(n + 1)$ in number. Since kth coordinate of $\boldsymbol{v}_i$ is $f_{k-1}(e_i)$, it is clear that exactly one of the pair $\{a\boldsymbol{v}_i \pm b\boldsymbol{v}_j\}$ has nonzero kth coordinate. Thus exactly half of the supports of minimum nonzero weight codewords contains a given k, and the result follows. $\square$

V. CONCLUDING REMARKS

We have described a class $C_q(r, n)$ of group character codes over GF(q) and determined their dimensions and minimum weights. For each n and r, the length, dimension, and minimum weight of $C_q(r, n)$ agrees with that of the binary Reed–Muller code $R(r, n)$. For the codes $C_q(1, n)$ we have explicitly determined the weight distribution and proved that the minimum nonzero weight codewords give 1-designs. It remains an open problem for the class of codes $C_q(r, n)$ described here to determine the weight distribution for r greater than 1.

Acknowledgment

The authors wish to thank I. F. Blake for his encouragement and the referees for their constructive comments and suggestions that considerably improved this correspondence.

References

[1] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*. New York, NY: Academic, 1975.

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[3] J.-P. Serre, *A Course in Arithmetic, Graduate Texts in Mathematics 7*. New York, NY: Springer-Verlag, 1973.