$\mathbb{Z}_4$-Valued Quadratic Forms and Quaternary Sequence Families

Kai-Uwe Schmidt

11 January 2009 (revised 30 June 2009)

Abstract

$\mathbb{Z}_4$-valued quadratic forms defined on a vector space over GF(2) are studied. A classification of such forms is established, distinguishing $\mathbb{Z}_4$-valued quadratic forms only by their rank and whether the associated bilinear form is alternating or not. This result is used to compute the distribution of certain exponential sums, which occur frequently in the analysis of quaternary codes and quaternary sequence sets. The concept is applied as follows. When $t = 0$ or m is odd, the correlation distribution of Family $S(t)$, consisting of quaternary sequences of length $2^m - 1$, is established. Then, motivated by practical considerations, a subset $S^*(t)$ of Family $S(t)$ is defined, and the correlation distribution of Family $S^*(t)$ is given for odd and even m.

Keywords

Galois rings, low-correlation sequence sets, quadratic forms, quaternary codes, quaternary sequences

1 Introduction

Quadratic forms taking on values in $\mathbb{Z}_2$ proved to be useful to analyze subcodes of the binary second-order Reed–Muller code $\mathrm{RM}(2, m)$, including Kerdock and Delsarte–Goethals codes, as well as related binary sequence sets, including the Gold and Kasami families (see [14, Ch. 15] and [7, Sec. 6.1], for example). Dickson's classification [5, p. 197] of such forms implies that many of their properties depend only on a single parameter, called the *rank* of the quadratic form. This fact is the key to establish the weight distribution and the correlation distribution of several binary codes and sequence families, respectively.

Kai-Uwe Schmidt is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, BC V5A 1S6, Canada, email: kuschmidt@sfu.ca. He is supported by Deutsche Forschungsgemeinschaft (German Research Foundation) under Research Fellowship SCHM 2609/1-1.

In this paper we revisit $\mathbb{Z}_4$-valued quadratic forms, which have been introduced by Brown [3] and were further studied by Wood [19]. We demonstrate how the theory of $\mathbb{Z}_4$-valued quadratic forms can be used to analyze certain quaternary codes and families of quaternary sequences. More specifically, we establish the distribution of an exponential sum attached to $\mathbb{Z}_4$-valued quadratic forms, which enables us to analyze the correlation distribution of Family $S(t)$. Families $S(0), S(1), S(2), \ldots$ were defined by Kumar et al. [11] and form a nested chain of families of quaternary sequences of length $2^m - 1$ with increasing size and increasing maximum nontrivial correlation. The first member $S(0)$ in this chain is identical to Family A [17], [2]. When m is odd, the sequence families in the chain correspond to shortened $\mathbb{Z}_4$-linear versions of the Delsarte–Goethals codes, as defined by Hammons et al. [6]. We refer to the survey chapter [7] by Helleseth and Kumar for background on sequence families and applications in digital communications systems.

A detailed outline of this paper is given next. In Section 2 we describe a classification of $\mathbb{Z}_4$-valued quadratic forms with respect to their rank and whether the associated bilinear form is alternating or not. This classification is used in Section 3 to compute the distribution of an exponential sum attached to $\mathbb{Z}_4$-valued quadratic forms. This distribution appears to be useful to establish weight distributions and correlation distributions of certain quaternary codes and families of quaternary sequences, respectively.

In Section 4 we study sets of $\mathbb{Z}_4$-valued quadratic forms, which are intimately related to the $\mathbb{Z}_4$-linear Delsarte–Goethals code of length 2^m and to Family $S(t)$ of length $2^m - 1$. The crucial property of such a set is that the difference between distinct elements in the set has rank at least $m - 2t$. Recent results on sets of symmetric bilinear forms [16] are used to determine the rank distribution of these sets.

In Section 5 we combine our results on exponential sums and on the rank distribution of sets of $\mathbb{Z}_4$-valued quadratic forms to determine the correlation distribution of Family $S(t)$ whenever $t = 0$ or m is odd. So far, the correlation distribution of Family $S(t)$ is only known for $t = 0$ [2] and for $t = 1$ [11]. In the latter cases, however, we obtain the results in a much easier way. For even m, it is generally hard to compute the correlation distribution of Family $S(t)$, as even the size of the set is difficult to determine. This motivates the definition of a large subset $S^*(t)$ of Family $S(t)$, for which we establish the correlation distribution for odd and even m. It should be noted that Family $S^*(2)$ of length 255 is used in the IMT-2000 standard [12]. We close this paper with some concluding remarks in Section 6.

2 $\mathbb{Z}_4$-Valued Quadratic Forms

In this section we summarize some basic facts about $\mathbb{Z}_4$-valued quadratic forms. Let

$$K := \{z \in \mathbb{Z}_4 : z^2 = z\}$$

be the set of Teichmuller representatives in $\mathbb{Z}_4$ (informally, K can be identified with the subset $\{0, 1\}$ of $\mathbb{Z}_4$). Then each $z \in \mathbb{Z}_4$ can be uniquely written as

$$z = a + 2b, \text{ where } a, b \in K.$$

We define an operation $\oplus$ on K by $a \oplus b := (a+b)^2$. Then $(K, \oplus, \cdot)$ is the finite field of size 2. Let V be an m-dimensional vector space over K.

A *symmetric bilinear form* on V is a mapping $B : V \times V \to K$ that satisfies symmetry:

$$B(x, y) = B(y, x), \tag{1}$$

and the bilinearity condition:

$$B(\alpha x \oplus \beta y, z) = \alpha\, B(x, z) \oplus \beta\, B(y, z) \quad \text{for } \alpha, \beta \in K. \tag{2}$$

Note that linearity in the second argument follows from symmetry (1). B is called *alternating* if $B(x, x) = 0$ for all $x \in V$. Otherwise it is called *nonalternating*.

Let $\{\lambda_0, \lambda_1, \ldots, \lambda_{m-1}\}$ be a basis for V over K. Then, relative to this basis, B is uniquely determined by its matrix of size $m \times m$ given by

$$\mathbf{B} = (b_{jk})_{0 \le j,k < m}, \quad \text{where} \quad b_{jk} = B(\lambda_j, \lambda_k).$$

The *radical* $\mathrm{rad}(B)$ of B contains all elements $x \in V$ such that $B(x, y) = 0$ for each $y \in V$. The bilinearity condition (2) implies that the radical is a subspace of V. The *rank* of B is defined as

$$\mathrm{rank}(B) := m - \dim_K(\mathrm{rad}(B)).$$

Note that the rank of B is precisely the rank of its matrix.

Definition 1 (Brown [3])**.** A $\mathbb{Z}_4$*-valued quadratic form* is a mapping $Q : V \to \mathbb{Z}_4$ that satisfies

$$Q(\alpha x) = \alpha^2 Q(x) \quad \text{for } \alpha \in K \tag{3}$$

and

$$Q(x \oplus y) = Q(x) + Q(y) + 2B(x, y), \tag{4}$$

where $B : V \times V \to K$ is a symmetric bilinear form.

We say that the $\mathbb{Z}_4$-valued quadratic form $Q : V \to \mathbb{Z}_4$ has *rank* r if its associated bilinear form has rank r. Moreover, Q is called *alternating* if its associated bilinear form is alternating. Otherwise Q is called *nonalternating*.

Since $Q(x \oplus x) = Q(0) = 0$ by (3), we have by (4)

$$2Q(x) = 2B(x, x), \tag{5}$$

and therefore,

$$Q \text{ is } (2\mathbb{Z}_2)\text{-valued} \iff B \text{ is alternating},$$

where B is the bilinear form corresponding to Q. Note that, if Q is $(2\mathbb{Z}_2)$-valued, then Q can be identified with a $\mathbb{Z}_2$-valued quadratic form.

Now let $\mathbf{x} = (x_0, x_1, \ldots, x_{m-1})$ be the K-valued coordinate vector of x relative to the basis $\{\lambda_0, \lambda_1, \ldots, \lambda_{m-1}\}$ for V over K, so that $x = \bigoplus_{j=0}^{m-1} x_j\lambda_j$. Then (2), (3), and (4) give

$$\begin{aligned} Q(x) &= Q\left(\bigoplus_{j=0}^{m-1} x_j\lambda_j\right) \\ &= \sum_{j=0}^{m-1} x_j Q(\lambda_j) + 2\sum_{0\le j<k<m} x_j x_k B(\lambda_j, \lambda_k) \\ &= \sum_{0\le j,k<m} x_j x_k B(\lambda_j, \lambda_k) + \sum_{j=0}^{m-1} x_j(Q(\lambda_j) - B(\lambda_j, \lambda_j)). \end{aligned}$$

Therefore, by (5), there exists $\mathbf{v} \in K^m$ such that

$$Q(x) = \mathbf{x}\mathbf{B}\mathbf{x}^T + 2\mathbf{v}\mathbf{x}^T, \tag{6}$$

where $\mathbf{B}$ is the matrix of B, relative to the basis $\{\lambda_0, \lambda_1, \ldots, \lambda_{m-1}\}$.

Recall that two symmetric matrices A and B over K are *similar* if there exists an invertible matrix P such that $A = PBP^T$. Clearly, two similar matrices have the same rank. The following theorem is well known (see Albert [1, pp. 390–392]).

Result 2. *Let A be a K-valued $m \times m$ symmetric matrix of rank r.*

(i) If A is alternating, then r is even and A is similar to a matrix that has zeros everywhere except on the subdiagonal and the superdiagonal, which are $1010\cdots10100\cdots0$ with $r/2$ ones.

(ii) If A is nonalternating, then A is similar to a diagonal matrix, whose main diagonal is $111\cdots000$ with r ones.

Combination of the representation (6) and Result 2 gives the following.

Corollary 3. *There exists a basis for V over K, determining the coordinates $(x_0, x_1, \ldots, x_{m-1})$ of $x \in V$, such that a $\mathbb{Z}_4$-valued quadratic form $Q : V \to \mathbb{Z}_4$ of rank r can be written as follows. If Q is alternating, we have*

$$Q(x) = 2\sum_{j=0}^{r/2-1} x_{2j}x_{2j+1} + 2\sum_{j=0}^{m-1} v_j x_j,$$

and if Q is nonalternating, we have

$$Q(x) = \sum_{j=0}^{r-1} x_j + 2\sum_{j=0}^{m-1} v_j x_j$$

for some $v_0, v_1, \ldots, v_{m-1} \in K$.

3 Exponential Sums

Let $T : V \times V \to K$ be an inner product in V, that is, T is a symmetric bilinear form of rank m. Let $Q : V \to \mathbb{Z}_4$ be a $\mathbb{Z}_4$-valued quadratic form. In this section we study the exponential sum

$$\chi_Q(u) := \sum_{x \in V} i^{Q(x)} (-1)^{T(u,x)} \quad \text{for } u \in V \tag{7}$$

(where $i := \sqrt{-1}$). It turns out that the distribution of the values in the multiset

$$\{\chi_Q(u) : u \in V\}$$

depends only on the rank of Q and on whether Q is alternating or nonalternating. If Q is alternating, we have the following well-known result (see [7, Thm. 6.2], for example).

Result 4. *Let $Q : V \to \mathbb{Z}_4$ be an alternating $\mathbb{Z}_4$-valued quadratic form of rank r. Then the distribution of the values in the multiset $\{\chi_Q(u) : u \in V\}$ is given by*

value	*frequency*
0	$2^m - 2^r$
$\pm 2^{m-r/2}$	$2^{r-1} \pm 2^{r/2-1}$

An equivalent of Result 4 for nonalternating $\mathbb{Z}_4$-valued quadratic forms is the following.

Theorem 5. *Let $Q : V \to \mathbb{Z}_4$ be a nonalternating $\mathbb{Z}_4$-valued quadratic form of rank r, and write $\omega := (1+i)/\sqrt{2}$. Then the distribution of the values in the multiset $\{\chi_Q(u) : u \in V\}$ is as follows. If r is odd, we have*

value	*frequency*
0	$2^m - 2^r$
$\pm\omega\, 2^{m-r/2}$	$2^{r-2} \pm 2^{(r-3)/2}$
$\pm\omega^3\, 2^{m-r/2}$	$2^{r-2} \mp 2^{(r-3)/2}$

If r is even, we have

value	*frequency*
0	$2^m - 2^r$
$\pm 2^{m-r/2}$	$2^{r-2} \pm 2^{r/2-1}$
$\pm i 2^{m-r/2}$	2^{r-2} *(each)*

Proof. By Corollary 3, there exists a basis $\{\lambda_0, \lambda_1, \ldots, \lambda_{m-1}\}$ for V over K, determining the coordinates $(x_0, x_1, \ldots, x_{m-1})$ of x, such that

$$Q(x) = \sum_{j=0}^{r-1} x_j + 2 \sum_{j=0}^{m-1} v_j x_j \tag{8}$$

for some $v_0, v_1, \ldots, v_{m-1} \in K$.

Let $\{\mu_0, \mu_1, \ldots, \mu_{m-1}\}$ be another basis for V over K that is dual to $\{\lambda_0, \lambda_1, \ldots, \lambda_{m-1}\}$ with respect to the inner product T, that is,

$$T(\lambda_j, \mu_k) = \delta_{jk} \quad \text{for } 0 \le j, k < m, \tag{9}$$

where δ_{jk} is the Kronecker delta. Let $(u_0, u_1, \ldots, u_{m-1})$ be the coordinate vector of $u \in V$ relative to $\{\mu_0, \mu_1, \ldots, \mu_{m-1}\}$ and write $v = v_0\mu_0 \oplus v_1\mu_1 \oplus \cdots \oplus v_{m-1}\mu_{m-1}$. Then we have from (7), (8), and (9)

$$\chi_Q(u \oplus v) = \sum_{x \in V} i^{\sum_{j=0}^{r-1} x_j + 2\sum_{j=0}^{m-1} u_j x_j}.$$

Clearly, when u ranges over V, so does $u \oplus v$. Applying further manipulations, we obtain

$$\begin{aligned}
\chi_Q(u \oplus v) &= \sum_{x \in V} \prod_{j=0}^{r-1} i^{(1+2u_j)x_j} \prod_{j=r}^{m-1} (-1)^{u_j x_j} \\
&= \prod_{j=0}^{r-1} \sum_{x_j \in K} i^{(1+2u_j)x_j} \prod_{j=r}^{m-1} \sum_{x_j \in K} (-1)^{u_j x_j} \\
&= \prod_{j=0}^{r-1} (1 + i(-1)^{u_j}) \prod_{j=r}^{m-1} (1 + (-1)^{u_j}).
\end{aligned}$$

If $u_j = 1$ for some j satisfying $r \le j < m$, then $\chi_Q(u \oplus v) = 0$. This can happen in $2^m - 2^r$ cases. Now let $u_j = 0$ for $r \le j < m$. Then we have

$$\begin{aligned}
\chi_Q(u \oplus v) &= 2^{m-r} \prod_{j=0}^{r-1} (1 + i(-1)^{u_j}) \\
&= 2^{m-r} \cdot 2^{r/2} \prod_{j=0}^{r-1} \omega^{(-1)^{u_j}} \\
&= 2^{m-r/2}\, \omega^{r - 2\,\mathrm{wt}(u_0, u_1, \ldots, u_{r-1})} \\
&= 2^{m-r/2}\, \omega^{r \pmod 2}\, i^{\lfloor r/2 \rfloor - \mathrm{wt}(u_0, u_1, \ldots, u_{r-1})},
\end{aligned}$$

where wt(.) denotes the Hamming weight. For integer j, let $A_j(r)$ be the number of words $z \in K^r$ with $\mathrm{wt}(z) = \lfloor r/2 \rfloor - j \pmod 4$. Then, the value

$$2^{m-r/2}\, \omega^{r \pmod 2}\, i^j$$

occurs $A_j(r)$ times in the multiset $\{\chi_Q(u) : u \in V\}$. It remains to determine the numbers $A_j(r)$ for $j = 0, 1, 2, 3$.

Since half of the words in K^r have odd weight, we have

$$A_0(r) + A_2(r) = A_1(r) + A_3(r) = 2^{r-1}. \tag{10}$$

It is straightforward to obtain the recurrence

$$A_j(r) = A_{j-1}(r-2) + A_{j+1}(r-2) + 2A_j(r-2) \quad \text{for } r \geq 3.$$

Substituting (10) gives

$$A_j(r) = 2^{r-3} + 2A_j(r-2) \quad \text{for } r \geq 3. \tag{11}$$

Using (11) together with the initial values

$$A_0(1) = 1, \quad A_1(1) = 0, \quad A_2(1) = 0, \quad A_3(1) = 1$$

we readily verify that for odd r we have

$$A_j(r) = \begin{cases} 2^{r-2} + 2^{(r-3)/2} & \text{for } j = 0 \\ 2^{r-2} - 2^{(r-3)/2} & \text{for } j = 1 \\ 2^{r-2} - 2^{(r-3)/2} & \text{for } j = 2 \\ 2^{r-2} + 2^{(r-3)/2} & \text{for } j = 3. \end{cases}$$

Similarly, (11) and the initial values

$$A_0(2) = 2, \quad A_1(2) = 1, \quad A_2(2) = 0, \quad A_3(2) = 1$$

can be used to verify that we have for even r

$$A_j(r) = \begin{cases} 2^{r-2} + 2^{r/2-1} & \text{for } j = 0 \\ 2^{r-2} & \text{for } j = 1 \\ 2^{r-2} - 2^{r/2-1} & \text{for } j = 2 \\ 2^{r-2} & \text{for } j = 3. \end{cases}$$

This completes the proof. □

4 Sets of $\mathbb{Z}_4$-Valued Quadratic Forms

In this section we study sets of $\mathbb{Z}_4$-valued quadratic forms on V having the property that the difference between distinct elements in such a set has rank at least $m - 2t$ for integer t satisfying $0 \leq t \leq \frac{m-1}{2}$.

We shall first recall some facts about Galois fields and rings. Let R be a Galois extension of $\mathbb{Z}_4$ of degree m. Then $(R, +, \cdot)$ is a *Galois ring* of characteristic 4 and cardinality 4^m. For details on Galois rings we refer to [13], [15], and [7]. Define

$$F := \{z \in R : z^{2^m} = z\}$$

to be the set of Teichmuller representatives in R. Then each $z \in R$ can be uniquely written as

$$z = a + 2b, \quad \text{where } a, b \in F.$$

For $a, b \in F$ we define

$$a \oplus b := (a + b)^{2^m}.$$

Elementary manipulation gives

$$a \oplus b = a + b + 2(ab)^{2^{m-1}}.$$

It is straightforward to verify [15, Statement 2] that $(F, \oplus, \cdot)$ is a *Galois field* of size 2^m. By the definition of K, the prime subfield of F is equal to K.

The Frobenius automorphism σ on F is given by $\sigma(x) = x^2$, and the absolute trace function on F is the mapping $\mathrm{tr} : F \to K$ given by

$$\mathrm{tr}(x) := \bigoplus_{j=0}^{m-1} \sigma^j(x).$$

It is easy to check that $\mathrm{tr}(\sigma(x)) = \mathrm{tr}(x)$ and $\mathrm{tr}(\alpha x \oplus \beta y) = \alpha\,\mathrm{tr}(x) \oplus \beta\,\mathrm{tr}(y)$ for $\alpha, \beta \in K$. Another useful property is that the mapping $(x, y) \mapsto \mathrm{tr}(xy)$ is an inner product in F, as a vector space over K. The Frobenius automorphism π on R is given by

$$\pi(a + 2b) := \sigma(a) + 2\sigma(b), \quad \text{where } a, b \in F,$$

and the absolute trace function on R is defined to be the mapping $\mathrm{Tr} : R \to \mathbb{Z}_4$ given by

$$\mathrm{Tr}(x) := \sum_{j=0}^{m-1} \pi^j(x).$$

We have $\mathrm{Tr}(\pi(x)) = \mathrm{Tr}(x)$ and $\mathrm{Tr}(\alpha x + \beta y) = \alpha\,\mathrm{Tr}(x) + \beta\,\mathrm{Tr}(y)$ for $\alpha, \beta \in \mathbb{Z}_4$. Moreover, the identity $2\,\mathrm{Tr}(x) = 2\,\mathrm{tr}(x)$ holds for each $x \in F$.

In what follows, we shall make use of the fact that F is an m-dimensional vector space over K and consider $\mathbb{Z}_4$-valued quadratic forms defined on F. For $a \in F^{t+1}$ write $a = (a_0, a_1, \ldots, a_t)$, and define $Q_a : F \to \mathbb{Z}_4$ by

$$Q_a(x) := \mathrm{Tr}(a_0 x) + 2 \sum_{j=1}^{t} \mathrm{Tr}(a_j x^{2^j+1}).$$

Straightforward manipulation yields

$$Q_a(x \oplus y) = Q_a(x) + Q_a(y) + 2B_a(x, y),$$

where $B_a : F \times F \to K$ is given by

$$B_a(x,y) := \mathrm{tr}(a_0^2 xy) \oplus \bigoplus_{j=1}^{t} \mathrm{tr}\left(a_j \left[x^{2^j} y \oplus x y^{2^j}\right]\right).$$

It is readily verified that $Q(\alpha x) = \alpha^2 Q(x)$ for each $\alpha \in K$ and that B_a is a symmetric bilinear form on F. Therefore, Q_a is a $\mathbb{Z}_4$-valued quadratic form by Definition 1.

We define the following two sets of $\mathbb{Z}_4$-valued quadratic forms

$$\mathcal{Q}(t) := \{Q_a : a \in F^{t+1}\}$$
$$\mathcal{Q}^*(t) := \{Q_a : a \in F^{t+1}, a_0 = 0\}.$$

Notice that $\mathcal{Q}^*(t)$ is the subset of $\mathcal{Q}(t)$ that contains precisely the alternating $\mathbb{Z}_4$-valued quadratic forms in $\mathcal{Q}(t)$.

In [16] the corresponding sets of bilinear forms

$$\mathcal{B}(t) := \{B_a : a \in F^{t+1}\}$$
$$\mathcal{B}^*(t) := \{B_a : a \in F^{t+1}, a_0 = 0\}$$

have been studied. The crucial property of $\mathcal{B}(t)$ is that the difference between distinct elements in $\mathcal{B}(t)$ has rank at least $m - 2t$, and when m is odd, $\mathcal{B}(t)$ is the largest possible set with this property. The rank distribution of $\mathcal{B}^*(t)$ and $\mathcal{B}(t)$ has been determined in [16, Thm. 8 and Thm. 9], respectively. By the definition of the rank of $\mathbb{Z}_4$-valued quadratic forms, we immediately deduce the rank distributions of $\mathcal{Q}^*(t)$ and $\mathcal{Q}(t)$. In order to state the results, we recall that for real x and nonnegative integer k the 4-*ary Gaussian binomial coefficient* $\begin{bmatrix} x \\ k \end{bmatrix}$ is defined to be

$$\begin{bmatrix} x \\ 0 \end{bmatrix} := 1$$

$$\begin{bmatrix} x \\ k \end{bmatrix} := \frac{(4^x - 1)(4^{x-1} - 1)\cdots(4^{x-k+1} - 1)}{(4^k - 1)(4^{k-1} - 1)\cdots(4 - 1)} \quad \text{for } k > 0.$$

We refer to [14, p. 444] for some properties of Gaussian binomial coefficients.

Result 6. *Let $0 \le t \le \frac{m-1}{2}$, and write $n := \lfloor \frac{m}{2} \rfloor$. Let B_j be the number of elements in $\mathcal{Q}^*(t)$ having rank j. If m is odd, we have*

$$B_{m-2k-1} = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k}^{t-1} (-1)^{j-k} 4^{\binom{j-k}{2}} \begin{bmatrix} n-k \\ n-j \end{bmatrix} \left(2^{m(t-j)} - 1\right)$$

for $k = 0, 1, \ldots, \frac{m-3}{2}$. If m is even, we have

$$B_{m-2k} = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k}^{t} (-1)^{j-k} 4^{\binom{j-k}{2}} \begin{bmatrix} n-k \\ n-j \end{bmatrix} \left(2^{m(t-j)+j} - 1\right)$$

for $k = 0, 1, \ldots, \frac{m-2}{2}$. Moreover, $B_0 = 1$ and $B_j = 0$ if j is odd.

Result 7. *Let $0 \le t \le \frac{m-1}{2}$, and write $n := \lfloor \frac{m}{2} \rfloor$. Let A_j be the number of elements in $\mathcal{Q}(t)$ having rank j. If m is odd, we have*

$$A_{m-2k} = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k}^{t} (-1)^{j-k} 4^{\binom{j-k}{2}} \begin{bmatrix} n+1-k \\ n+1-j \end{bmatrix} \left(2^{m(t-j+1)} - 1\right)$$

for $k = 0, 1, \ldots, \frac{m-1}{2}$ and

$$A_{m-2k-1} = 4^{n-k} \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k}^{t-1} (-1)^{j-k} 4^{\binom{j-k}{2}} \begin{bmatrix} n-k \\ n-j \end{bmatrix} \left(2^{m(t-j)} - 1\right)$$

for $k = 0, 1, \ldots, \frac{m-3}{2}$. If m is even, we have

$$A_{m-2k} = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k}^{t} (-1)^{j-k} 4^{\binom{j-k}{2}} \begin{bmatrix} n-k \\ n-j \end{bmatrix} \left(2^{m(t-j+1)+j-2k} - 1\right)$$

for $k = 0, 1, \ldots, \frac{m-2}{2}$ and

$$A_{m-2k-1} = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k+1}^{t} (-1)^{j-k} 4^{\binom{j-k}{2}} \begin{bmatrix} n-k \\ n-j \end{bmatrix} 2^{m(t-j+1)-j} (1 - 4^{j-k})$$

for $k = 0, 1, \ldots, \frac{m-2}{2}$. Moreover, $A_0 = 1$.

5 Correlation Distribution of Family $S(t)$

In this section we recall the definition of Family $S(t)$ from [11] and define the related Family $S^*(t)$. We then study the correlation distribution of these families.

Let $q := 2^m$, $0 \le t \le \frac{m-1}{2}$, and $m \ge 3$. Let β be a primitive element in F. For $a \in R \times F^t$ write $a = (a_0, a_1, \ldots, a_t)$, and define the quaternary sequence $\{s_a(k)\}$ by

$$s_a(k) := \mathrm{Tr}(a_0 \beta^k) + 2 \sum_{j=1}^{t} \mathrm{Tr}(a_j \beta^{(2^j+1)k}).$$

Given a sequence $\{s(k)\}$, the *least period* of $\{s(k)\}$ is by definition the smallest positive integer u such that

$$\{s(k+u)\} = \{s(k)\}.$$

Since β has order $q-1$, the least period of the sequence $\{s_a(k)\}$ is at most $q-1$. Define a subset $P(t)$ of $R \times F^t$ by

$$P(t) := \{a \in R \times F^t : \{s_a(k)\} \text{ has least period } q-1\}.$$

We record the following lemma for later use.

Lemma 8. *We have*

$$|P(t)| = q^{t+2} - 1 \tag{12}$$

if and only if $t = 0$ *or* m *is odd.*

Proof. The identity (12) holds if and only if $\{s_a(k)\}$ has least period $q-1$ for each nonzero $a \in R \times F^t$. Since β has order $q-1$, (12) holds for $t = 0$. When m is odd, we have $\gcd(2^j + 1, q-1) = 1$ for $j = 1, 2, \ldots, \frac{m-1}{2}$ [14, p. 449], and therefore, β^{2^j+1} has order $q-1$ for $j = 1, 2, \ldots, \frac{m-1}{2}$. We conclude that (12) holds for odd m and all t. When m is even, we have $\gcd(3, q-1) = 3$, and therefore, for $t > 0$ there exist nonzero $a \in R \times F^t$ such that $\{s_a(k)\}$ has least period less than $q-1$. □

We say that two sequences $\{s_a(k)\}$ and $\{s_b(k)\}$ are *cyclically equivalent* if there exists an integer u such that

$$\{s_a(k+u)\} = \{s_b(k)\}.$$

This equivalence relation partitions

$$\{\{s_a(k)\} : a \in P(t)\}$$

into equivalence classes, each consisting of $q-1$ cyclically equivalent sequences. Let $P_{cd}(t)$ be a subset of $P(t)$ corresponding to picking precisely one sequence in each equivalence class. *Family* $S(t)$ is defined in [11] to be the set

$$S(t) := \{\{s_a(k)\} : a \in P_{cd}(t)\}.$$

Family $S(0)$ is also known as Family A [17], [2].

From Lemma 8 we have

$$|S(t)| = \frac{q^{t+2} - 1}{q-1} \quad \text{for } t = 0 \text{ or odd } m.$$

When m is even, it is generally difficult to identify the full set $S(t)$. It is therefore preferable in practise to work with a subset of $S(t)$, which we define now. Let

$$P^*_{cd}(t) := \{(1 + 2b_0, b_1, \ldots, b_t) : b_0, b_1, \ldots, b_t \in F\}$$

be a subset of $R \times F^t$. For each $a \in P^*_{cd}(t)$, the sequence $\{s_a(k)\}$ has least period $q-1$, and for distinct $a, b \in P^*_{cd}(t)$ the sequences $\{s_a(k)\}$ and $\{s_b(k)\}$ are not cyclically equivalent. We define *Family* $S^*(t)$ to be the set

$$S^*(t) := \{\{s_a(k)\} : a \in P^*_{cd}(t)\}.$$

By virtue of definition, $S^*(t)$ is a subset of $S(t)$ of size q^{t+1}. Family $S^*(2)$ of length 255 is used as an uplink scrambling code in the IMT-2000 standard [12].

For integer u we define the *correlation* between the sequences $\{s_a(k)\}$ and $\{s_b(k)\}$ to be

$$C_{a,b}(u) := \sum_{k=0}^{q-2} i^{s_a(k+u) - s_b(k)}.$$

If $a = b$ and $u \equiv 0 \pmod{q-1}$, we say that $C_{a,b}(u)$ is a *trivial correlation value*, otherwise $C_{a,b}(u)$ is called a *nontrivial correlation value*. It was established in [11, Thm. 1] that for $\{s_a(k)\}, \{s_b(k)\} \in S(t)$ all nontrivial correlation values $C_{a,b}(u)$ are at most $1 + 2^{m/2+t}$ in magnitude. In what follows, we determine the distribution of the correlation values of Family $S(t)$ whenever $|S(t)| = (q^{t+2}-1)/(q-1)$ and the distribution of the correlation values of Family $S^*(t)$.

Theorem 9. *Let $t = 0$ or m be odd, and write $\omega := (1+i)/\sqrt{2}$. For $j = 0, 1, \ldots, m$, let A_j be the number of elements of rank j in $\mathcal{Q}(t)$, and let B_j be the number of elements of rank j in $\mathcal{Q}^*(t)$. Then the distribution of the correlation values*

$$\{C_{a,b}(u) : a, b \in P_{cd}(t), 0 \le u \le q-2\}$$

is as given in Table 1.

Theorem 10. *Write $\omega := (1+i)/\sqrt{2}$. For $j = 0, 1, \ldots, m$, let A_j be the number of elements of rank j in $\mathcal{Q}(t)$, and let B_j be the number of elements of rank j in $\mathcal{Q}^*(t)$. Then the distribution of the correlation values*

$$\{C_{a,b}(u) : a, b \in P^*_{cd}(t), 0 \le u \le q-2\}$$

is given in Table 2.

From Results 6 and 7 we have $A_j = B_j = 0$ for $j = 1, 2, \ldots, m-2t-1$, which implies that the maximum modulus of the nontrivial correlation values of Family $S^*(t)$ is $1+2^{m/2+t}$. Since $S^*(t)$ is a subset of $S(t)$, this shows that the upper bound on the maximum modulus of the nontrivial correlation values of Family $S(t)$, given in [11, Thm. 1], is tight. Moreover, we conclude that the number of different correlation values in the correlation distributions given in Theorems 9 and 10 equals $8t + 6$.

We note that the statement in Theorem 9 in connection with Results 6 and 7 was proved using different techniques in [2, Thm. 6] for $t = 0$ and in [11, Thm. 2] for $t = 1$. For even m the correlation distribution of Family $S(1)$ was established in [11, Thm. 3]. The correlation distribution of Family $S^*(2)$ of length 255 was obtained numerically in [12] (though, unfortunately, there is a mistake in the first two rows of [12, Table 2]).

Proof of Theorem 9. By the definition of Family $S(t)$, for fixed $b \in R \times F^t$, we have the following multiset equality

$$\begin{aligned}
&\{\{s_a(k+u)\} - \{s_b(k)\} : a \in P_{cd}(t), 0 \le u \le q-2\} \\
&= \{\{s_a(k)\} - \{s_b(k)\} : a \in P(t)\} \\
&= \{\{s_{a-b}(k)\} : a \in P(t)\}.
\end{aligned}$$

Therefore,

$$\{C_{a,b}(u) : a, b \in P_{cd}(t), 0 \le u \le q-2\} = \left\{ \sum_{k=0}^{q-2} i^{s_{a-b}(k)} : a \in P(t), b \in P_{cd}(t) \right\}. \tag{13}$$

Table 1: Correlation Distribution of Family $S(t)$ for $t = 0$ or m odd ($j \in \{1, 2, \ldots, m\}$)

value	frequency
$-1 + q$	$\frac{q^{t+2}-1}{q-1}$
-1	$\frac{q^{t+2}-2}{q-1} \sum_{\ell=0}^{m-1} A_\ell (q - 2^\ell)$
$-1 \pm 2^{m-j/2}$ (j even)	$\frac{q^{t+2}-2}{q-1} \left((A_j + B_j) 2^{j-2} \pm A_j 2^{j/2-1} \right)$
$-1 \pm i2^{m-j/2}$ (j even)	$\frac{q^{t+2}-2}{q-1} (A_j - B_j) 2^{j-2}$ (each)
$-1 \pm \omega 2^{m-j/2}$ (j odd)	$\frac{q^{t+2}-2}{q-1} A_j (2^{j-2} \pm 2^{(j-3)/2})$
$-1 \pm \omega^3 2^{m-j/2}$ (j odd)	$\frac{q^{t+2}-2}{q-1} A_j (2^{j-2} \mp 2^{(j-3)/2})$

Table 2: Correlation Distribution of Family $S^*(t)$ ($j \in \{1, 2, \ldots, m\}$)

value	frequency
$-1 + q$	q^{t+1}
-1	$\frac{q^{t+1}}{q-1} \sum_{\ell=0}^{m-1} ((q-2)A_\ell + B_\ell)(q - 2^\ell)$
$-1 \pm 2^{m-j/2}$ (j even)	$\frac{q^{t+1}}{q-1} ((q-2)A_j + qB_j) 2^{j-2}$ $\pm \frac{q^{t+1}}{q-1} ((q-2)A_j + B_j) 2^{j/2-1}$
$-1 \pm i2^{m-j/2}$ (j even)	$\frac{q^{t+1}(q-2)}{q-1} (A_j - B_j) 2^{j-2}$ (each)
$-1 \pm \omega 2^{m-j/2}$ (j odd)	$\frac{q^{t+1}(q-2)}{q-1} A_j (2^{j-2} \pm 2^{(j-3)/2})$
$-1 \pm \omega^3 2^{m-j/2}$ (j odd)	$\frac{q^{t+1}(q-2)}{q-1} A_j (2^{j-2} \mp 2^{(j-3)/2})$

Given $z \in R \times F^t$, let $N(z)$ be the number of solutions $(a, b) \in P(t) \times P_{cd}(t)$ of $a - b = z$. If $t = 0$ or m is odd, we have by Lemma 8

$$P(t) = \{a \in R \times F^t : a \neq (0, 0, \ldots, 0)\},$$

and therefore using $|P_{cd}(t)| = (q^{t+2} - 1)/(q - 1)$,

$$N(z) = \begin{cases} \dfrac{q^{t+2} - 1}{q - 1} - 1 & \text{for } -z \in P_{cd}(t) \\ \dfrac{q^{t+2} - 1}{q - 1} & \text{otherwise.} \end{cases} \tag{14}$$

Since $P_{cd}(t)$ does not contain $(0, 0, \ldots, 0)$, we conclude that the trivial correlation value $q-1$ occurs $(q^{t+2} - 1)/(q - 1)$ times in the multiset (13). Writing

$$S_z := \sum_{k=0}^{q-2} i^{s_z(k)},$$

then by (14), the nontrivial correlation values in the multiset (13) are distributed as follows

$$\begin{aligned} &S_{-z}, \quad z \in P_{cd}(t) && \text{occurs} \quad \frac{q^{t+2} - 1}{q - 1} - 1 \quad \text{times} \\ &S_{-z}, \quad z \in P(t) \setminus P_{cd}(t) && \text{occurs} \quad \frac{q^{t+2} - 1}{q - 1} \quad \text{times.} \end{aligned}$$

For $a \in P_{cd}(t)$ define

$$E_a(t) := \{z \in P(t) : \{s_z(k)\} \text{ is cyclically equivalent to } \{s_a(k)\}\}.$$

Then, for each $a \in P_{cd}(t)$, the set $E_a(t)$ is an equivalence class in the sense that $\{\{s_z(k)\} : z \in E_a(t)\}$ contains exactly $q - 1$ cyclically equivalent sequences. By definition, $P_{cd}(t)$ contains exactly one member of each equivalence class, and we have the partition

$$P(t) = \bigcup_{a \in P_{cd}(t)} E_a(t).$$

Therefore, the set $P(t) \setminus P_{cd}(t)$ contains exactly $q - 2$ members of each equivalence class. Note that S_z is constant for all z belonging to one equivalence class. Hence the distribution of the nontrivial correlation values in the multiset (13) can be expressed as follows. For each $z \in P(t)$ the value S_{-z} occurs

$$\left(\frac{q^{t+2} - 1}{q - 1} - 1\right) \frac{1}{q - 1} + \frac{q^{t+2} - 1}{q - 1} \frac{q - 2}{q - 1} = \frac{q^{t+2} - 2}{q - 1}$$

times. When z runs through $P(t)$, so does $-z$. It therefore remains to establish the distribution of S_z when z ranges over $P(t)$.

For $c \in F^{t+1}$ write $c = (c_0, c_1, \ldots, c_t)$ and let $f_c : F \to \mathbb{Z}_4$ be given by

$$f_c(x) := \mathrm{Tr}(c_0 x) + 2\sum_{j=1}^{t} \mathrm{Tr}(c_j x^{2^j+1}),$$

so that for $d \in F$ we have $s_{(c_0+2d,c_1,\ldots,c_t)}(k) = f_c(\beta^k) + \mathrm{Tr}(2d\beta^k)$, where β is a primitive element in F. Define

$$\zeta(c, d) := -1 + \sum_{x \in F} i^{f_c(x)}(-1)^{\mathrm{tr}(dx)}.$$

Then $\zeta(c, d) = S_{(c_0+2d,c_1,\ldots,c_t)}$, which leaves to establish the distribution of $\zeta(c, d)$ when (c, d) ranges over $F^{t+2} \setminus \{(0, 0, \ldots, 0)\}$.

Notice that f_c is a $\mathbb{Z}_4$-valued quadratic form and that we have

$$\begin{aligned} \mathcal{Q}(t) &= \{f_c : c \in F^{t+1}\} \\ \mathcal{Q}^*(t) &= \{f_c : c \in F^{t+1}, c_0 = 0\}. \end{aligned}$$

By assumption, as c ranges over F^{t+1}, f_c is alternating and has rank j in B_j cases, and f_c is nonalternating and has rank j in $A_j - B_j$ cases for $j = 0, 1, \ldots, m$. Note that $B_j = 0$ for odd j. Combination with Result 4 and Theorem 5 gives the distribution of $\zeta(c, d)$ when (c, d) ranges over F^{t+2}. The proof is completed by noting that $\zeta(0, 0, \ldots, 0) = q - 1$. □

Proof of Theorem 10. First observe that, by writing $a = (a_0, \ldots, a_t)$ and $a' = (a'_0, \ldots, a'_t)$ for $a, a' \in R \times F^t$, we have

$$\{s_a(k + u)\} = \{s_{a'}(k)\} \quad \text{for integer } u,$$

where

$$\begin{aligned} a'_0 &= a_0\beta^u \\ a'_j &= a_j\beta^{(2^j+1)u} \quad \text{for } j = 1, 2, \ldots, t. \end{aligned}$$

Therefore, for fixed $b \in R \times F^t$, we have the following multiset equality

$$\begin{aligned} &\{\{s_a(k + u)\} - \{s_b(k)\} : a \in P^*_{cd}(t), 0 \le u \le q - 2\} \\ &= \{\{s_a(k)\} - \{s_b(k)\} : a \in R^* \times F^t\} \\ &= \{\{s_{a-b}(k)\} : a \in R^* \times F^t\}, \end{aligned}$$

where $R^* := R \setminus 2R$ is the group of units in R. Therefore,

$$\{C_{a,b}(u) : a, b \in P^*_{cd}(t), 0 \le u \le q - 2\} = \left\{\sum_{k=0}^{q-2} i^{s_{a-b}(k)} : a \in R^* \times F^t, b \in P^*_{cd}(t)\right\}. \quad (15)$$

Given $z \in R \times F^t$, let $N(z)$ be the number of solutions $(a, b) \in (R^* \times F^t) \times P^*_{cd}(t)$ of $a - b = z$. Writing $z = (z_0, z_1, \ldots, z_t)$, we have from the definition of $P^*_{cd}(t)$

$$N(z) = \begin{cases} 0 & \text{for } z_0^2 = 1 \\ q^{t+1} & \text{otherwise.} \end{cases} \tag{16}$$

For $\lambda \in F$ and $c = (c_1, c_2, \ldots, c_t) \in F^t$, let $f_{\lambda,c} : F \to \mathbb{Z}_4$ be given by

$$f_{\lambda,c}(x) := \mathrm{Tr}(\lambda x) + 2 \sum_{j=1}^{t} \mathrm{Tr}(c_j x^{2^j+1}),$$

so that for $d \in F$ we have $s_{(\lambda+2d,c_1,\ldots,c_t)}(k) = f_{\lambda,c}(\beta^k) + \mathrm{Tr}(2d\beta^k)$, where β is a primitive element in F. Define

$$\zeta(\lambda, c, d) := -1 + \sum_{x \in F} i^{f_{\lambda,c}(x)} (-1)^{\mathrm{tr}(dx)}.$$

Then, by (16), for each $\lambda \in F \setminus \{1\}$ and each $(c, d) \in F^{t+1}$, the value $\zeta(\lambda, c, d)$ occurs q^{t+1} times in the multiset (15). Notice that $f_{\lambda,c}$ is a $\mathbb{Z}_4$-valued quadratic form. Therefore, in view of Result 4 and Theorem 5, for $\lambda \in F \setminus \{1\}$ and $c \in F^t$, it remains to classify $f_{\lambda,c}$ with respect to its rank and whether it is alternating or nonalternating.

The $\mathbb{Z}_4$-valued quadratic forms $f_{0,c}$ are alternating, and we have

$$\mathcal{Q}^*(t) = \{f_{0,c} : c \in F^t\}.$$

Therefore, for $c \in F^t$, $f_{0,c}$ has rank equal to j in B_j cases, where $j = 0, 1, \ldots, m$. Note that $B_j = 0$ for odd j. For $\lambda \neq 0$, the $\mathbb{Z}_4$-valued quadratic forms $f_{\lambda,c}$ are nonalternating and we have

$$\mathcal{Q}(t) = \{f_{\lambda,c} : (\lambda, c) \in F^{t+1}\}.$$

By applying variable substitution $x \mapsto x/\lambda$, we see that, if $\lambda \neq 0$, then the distribution of the rank of the values in the multiset $\{f_{\lambda,c} : c \in F^t\}$ is independent of λ. Therefore, for $\lambda \in F \setminus \{0, 1\}$ and $c \in F^t$, the $\mathbb{Z}_4$-valued quadratic form $f_{\lambda,c}$ has rank j in $\frac{q-2}{q-1}(A_j - B_j)$ cases, where $j = 0, 1, \ldots, m$. This completes the proof. □

We close this section with a specific example for the application of Theorems 9 and 10. Take $m = 5$ and $t = 1$ and use the notation of Theorems 9 and 10. From Result 6 we find that the nonzero B's are given by

$$B_0 = 1$$
$$B_4 = 31,$$

and by Result 7 the nonzero A's are given by

$$A_0 = 1$$
$$A_3 = 155$$
$$A_4 = 496$$
$$A_5 = 372.$$

For $m = 5$ the correlation distributions of Families $S(1)$ and $S^*(1)$ are shown in Table 3.

Table 3: Correlation Distributions of Families $S(1)$ and $S^*(1)$ for $m = 5$

value	frequency	
	for $S(t)$	for $S^*(t)$
31	1057	1024
-1	12352782	11598848
$+3 + 4i$	3931920	3686400
$-5 - 4i$	2359152	2211840
$-5 + 4i$	2359152	2211840
$+3 - 4i$	3931920	3686400
$+7$	3276600	3082240
-9	1179576	1112064
$-1 + 8i$	1965960	1843200
$-1 - 8i$	1965960	1843200
$+7 + 8i$	491490	460800
$-9 - 8i$	163830	153600
$-9 + 8i$	163830	153600
$+7 - 8i$	491490	460800

6 Concluding Remarks

The theory of quadratic forms is a natural tool to analyze subcodes of the binary second-order Reed–Muller code $\mathrm{RM}(2, m)$, including Kerdock and Delsarte–Goethals codes, as well as related binary sequence sets, including Gold and Kasami families. We have shown that, by allowing quadratic forms to take values in $\mathbb{Z}_4$, we obtain a natural tool to analyze certain sets of quaternary sequence families. We have used this relationship to study the correlation distribution of Family $S(t)$, which includes Family A.

The theory of $\mathbb{Z}_4$-valued quadratic forms, in particular Result 4 and Theorem 5, can also be used to establish the correlation distribution of other sets of quaternary sequences of length $2^m - 1$, such as the quaternary Kasami set [8] and Family A with large linear span [9]. Moreover, the concept can be adapted to handle sets of quaternary sequences of length $2(2^m - 1)$, such as Family D [10], and sets of related binary sequences of length $2(2^m - 1)$, such as the Kerdock sequences [18].

Since the real part of the exponential sum (7) can be related to the Lee weight of the word obtained by evaluating the corresponding $\mathbb{Z}_4$-valued quadratic form on V (see [6, Sec. II.C], for example), the theory of $\mathbb{Z}_4$-valued quadratic forms can be used analyze the Lee weight distribution of subcodes of the quaternary second-order Reed–Muller code $\mathrm{ZRM}(2, m)$, such as the quaternary Kerdock and Delsarte–Goethals codes [6]. We remark that the relation between the quaternary Kerdock code and $\mathbb{Z}_4$-valued quadratic forms has been first reported by Calderbank et al. [4].

References

[1] A. A. Albert. Symmetric and alternate matrices in an arbitrary field. *Trans. Amer. Math. Soc.*, 43:386–436, 1938.

[2] S. Boztaş, R. Hammons, and P. V. Kumar. 4-phase sequences with near-optimum correlation properties. *IEEE Trans. Inf. Theory*, 38(3):1101–1113, May 1992.

[3] E. H. Brown, Jr. Generalizations of the Kervaire invariant. *Annals Math.*, 95(2):368–383, Mar. 1972.

[4] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line sets. *J. London Math. Soc.*, 75:436–480, 1997.

[5] L. E. Dickson. *Linear Groups with an Exposition of the Galois Field Theory.* New York: Dover Publications Inc., 1958.

[6] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Trans. Inf. Theory*, 40(2):301–319, Mar. 1994.

[7] T. Helleseth and P. V. Kumar. Sequences with low correlation. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory.* Amsterdam, The Netherlands: Elsevier, 1998.

[8] T. Helleseth, P. V. Kumar, H. M. Martinsen, and O. N. Vassbakk. Correlation distribution of the quaternary Kasami sequences. In *Sequences and Their Applications*, Discrete Mathematics and Theoretical Computer Science, pages 240–253. Springer, 1998.

[9] W. Jiang, L. Hu, X. Tang, and X. Zeng. New optimal quadriphase sequences with larger linear span. *IEEE Trans. Inf. Theory*, 55(1):458–470, Jan. 2009.

[10] A. Johansen, T. Helleseth, and X. Tang. The correlation distribution of quaternary sequences of period $2(2^n - 1)$. *IEEE Trans. Inf. Theory*, 54(7):3130–3139, Jul. 2008.

[11] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons, Jr. Large families of quaternary sequences with low correlation. *IEEE Trans. Inf. Theory*, 42(2):579–592, Mar. 1996.

[12] P. V. Kumar, H. F. F. Lu, T. Helleseth, and D.-J. Shin. On large family of low correlation quaternary sequences $S(2)$. *IEEE Int. Conf. Personal Wireless Commun.*, pages 33–37, Dec. 2000.

[13] B. R. MacDonald. *Finite Rings with Identity*. Marcel Dekker, New York, 1974.

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

[15] A. A. Nechaev. Kerdock code in a cyclic form. *Discrete Math. Appl.*, 1(4):365–384, 1991. Originally published in Russian in *Diskretnaya Matematika*, vol. 1, no. 4, pp. 123–139, 1989.

[16] K.-U. Schmidt. Symmetric bilinear forms over finite fields of even characteristic. *Submitted for publication*, 2008.

[17] P. Solé. *A Quartenary Cyclic Code, and a Family of Quadriphase Sequences with Low Correlation Properties*, volume 388 of *Lecture Notes in Computer Science*, pages 193–201. New York: Springer Verlag, 1989.

[18] X. Tang, T. Helleseth, and A. Johansen. *On the Correlation Distribution of Kerdock Sequences*, volume 5203 of *Lecture Notes in Computer Science*, pages 121–129. New York: Springer Verlag, 2008.

[19] J. A. Wood. Witt's extension theorem for mod four valued quadratic forms. *Trans. Amer. Math. Soc.*, 336(1):445–461, Mar. 1993.