On the Correlation Distribution of Delsarte–Goethals Sequences

Kai-Uwe Schmidt*

29 July 2009 (revised 01 December 2009)

Abstract

For odd integer $m \geq 3$ and $t = 0, 1, \ldots, \frac{m-1}{2}$, we define Family $\mathscr{V}(t)$ to be a set of size $2^{m(t+1)}$ containing binary sequences of period $2^{m+1} - 2$. The nontrivial correlations between sequences in Family $\mathscr{V}(t)$ are bounded in magnitude by $2 + 2^{(m+1)/2+t}$. Families $\mathscr{V}(0)$ and $\mathscr{V}(1)$ compare favourably to the small and large Kasami sets, respectively. So far, the correlation distribution of Family $\mathscr{V}(t)$ is only known for $t = 0$. A general framework for computing the correlation distribution of Family $\mathscr{V}(t)$ is established. The correlation distribution of $\mathscr{V}(1)$ is derived, and a way to obtain the correlation distribution of $\mathscr{V}(2)$ is described.

Keywords

Galois ring, Low correlation, Quadratic Form, Sequence Set

1 Introduction

We consider families of binary sequences for use in code-division multiple access (CDMA) systems (for background see [HK98], for example). The size and the maximum nontrivial correlation are key parameters of such designs. Large family size is required to support a large number of simultaneous users. Small nontrivial correlation is required to ensure message synchronisation and to minimise interference among different users. Knowledge of the distribution of the possible correlation values allows to evaluate the system performance without doing extensive simulations.

For odd integer $m \geq 3$ and $t = 0, 1, \ldots, \frac{m-1}{2}$, Family $\mathscr{V}(t)$, to be defined in Section 4, is a set of binary sequences of period $2^{m+1} - 2$, size $2^{m(t+1)}$, and maximum nontrivial correlation $2 + 2^{\frac{m+1}{2}+t}$ (see Theorem 9). The respective Families $\mathscr{V}(0)$, $\mathscr{V}(1)$, and $\mathscr{V}(2)$ coincide with Families $Q(2)$, $Q(3)$, and $Q(5)$, as defined by Helleseth and Kumar [HK98, p. 1832], and are the largest known designs among all binary sequence families with asymptotically the same period and maximum nontrivial correlation. Table 1 shows that Families $\mathscr{V}(0)$ and $\mathscr{V}(1)$ compare favourably to the small and the large Kasami set, respectively. In general, Family $\mathscr{V}(t)$ is a subset of Family $Q(2^t + 1)$. Following Nechaev's treatment [Nec91] of the Kerdock code, it can be shown that the sequences in $\mathscr{V}(t)$ are codewords of the Delsarte–Goethals code $\mathscr{DG}(m + 1, \frac{m+1}{2} - t)$ [MS77, Ch. 15], punctured in two coordinates.

*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.

Table 1: Comparison of the Kasami Sets with Families $\mathscr{V}(0)$ and $\mathscr{V}(1)$

Family	Period	Family Size	Max. Correlation	m
Kasami (Small set)	$2^{m+1}-1$	$2^{\frac{m+1}{2}}$	$1+2^{\frac{m+1}{2}}$	odd
$\mathscr{V}(0)$	$2^{m+1}-2$	2^m	$2+2^{\frac{m+1}{2}}$	odd
Kasami (Large set)	$2^{m+1}-1$	$2^{\frac{3(m+1)}{2}}+2^{\frac{m+1}{2}}$	$1+2^{\frac{m+3}{2}}$	$1 \pmod 4$
Kasami (Large set)	$2^{m+1}-1$	$2^{\frac{3(m+1)}{2}}+2^{\frac{m+1}{2}}-1$	$1+2^{\frac{m+3}{2}}$	$3 \pmod 4$
$\mathscr{V}(1)$	$2^{m+1}-2$	2^{2m}	$2+2^{\frac{m+3}{2}}$	odd

The distribution of the correlation values of Family $\mathscr{V}(0)$ was recently established by Tang, Helleseth, and Johansen [THJ08]. In the present paper, we pursue a rather different approach and use the theory of $\mathbb{Z}_4$-valued quadratic forms [Sch09]. After giving some background on Galois rings and fields in Section 2, we review $\mathbb{Z}_4$-valued quadratic forms in Section 3. In Section 4, we relate the correlation distribution of Family $\mathscr{V}(t)$ to the distribution of certain exponential sums and prove an upper bound on the magnitude of the nontrivial correlations of Family $\mathscr{V}(t)$. These exponential sums are then analysed in Section 5 for the specific cases of Families $\mathscr{V}(0)$ and $\mathscr{V}(1)$ using the theory of $\mathbb{Z}_4$-valued quadratic forms. In Section 6 we describe how to obtain the correlation distribution of Family $\mathscr{V}(2)$ and comment on the difficulty of extending our technique to $t > 2$.

2 Background on Galois Rings and Fields

In this section, we briefly recall some facts about Galois rings and fields.

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 Nechaev [Nec91] and Helleseth and Kumar [HK98]. Define

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

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

$$z = a + 2b, \quad \text{where } a, b \in L. \tag{1}$$

We define an operation $\oplus$ on L by

$$a \oplus b := a + b + 2\sqrt{ab}. \tag{2}$$

Then $(L, \oplus, \cdot)$ is a *Galois field* of size 2^m [Nec91, Statement 2]. Let K be the prime subfield of L. Note that $K = \{z \in \mathbb{Z}_4 : z^2 = z\}$. Informally, K can be identified with the subset $\{0, 1\}$ of $\mathbb{Z}_4$.

The Frobenius automorphism σ on L is given by $\sigma(x) = x^2$, and the absolute trace function on L is the mapping $\mathrm{tr} : L \to K$ 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 L, as a vector space over K. This last fact can be used to prove the following elementary lemma.

Lemma 1. *Let E be a subspace of L, and define*

$$E^{\perp} := \{x \in L : \mathrm{tr}(xy) = 0 \text{ for all } y \in E\}.$$

Then

$$\sum_{x \in E} (-1)^{\mathrm{tr}(cx)} = \begin{cases} |E| & \text{for } c \in E^{\perp} \\ 0 & \text{for } c \in L \setminus E^{\perp}. \end{cases}$$

The Frobenius automorphism ϱ on R is given by

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

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

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

We have $\mathrm{Tr}(\varrho(x)) = \mathrm{Tr}(x)$ 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 $x \in L$.

3 $\mathbb{Z}_4$-Valued Quadratic Forms

In this section, we review some facts about $\mathbb{Z}_4$-valued quadratic forms.

A *symmetric bilinear form* on L is a mapping $B : L \times L \to K$ that satisfies symmetry $B(x, y) = B(y, x)$ and the bilinearity condition

$$B(\alpha x \oplus \beta y, z) = \alpha\, B(x, z) \oplus \beta\, B(y, z) \quad \text{for } \alpha, \beta \in K. \tag{3}$$

Moreover, B is called *alternating* if $B(x, x) = 0$ for each $x \in L$. Otherwise, B is called *nonalternating*.

The *radical* $\mathrm{rad}(B)$ of B contains all elements $x \in L$ such that $B(x, y) = 0$ for each $y \in L$. The bilinearity condition (3) implies that this set is a subspace of L. The *rank* of B is defined as

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

A $\mathbb{Z}_4$*-valued quadratic form* Q is a mapping $Q : L \to \mathbb{Z}_4$ that satisfies $Q(0) = 0$ and

$$Q(x \oplus y) = Q(x) + Q(y) + 2B(x, y),$$

where $B : L \times L \to K$ is a symmetric bilinear form. We say that the $\mathbb{Z}_4$-valued quadratic form Q has *rank* r and write $\mathrm{rank}(Q) = r$ 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*. It is readily verified that Q takes values only in $2\mathbb{Z}_2$ (and can therefore be identified with an ordinary

$\mathbb{Z}_2$-valued quadratic form) if and only if Q is alternating. It is well-known [HK98, p. 1800] that the rank of an alternating $\mathbb{Z}_4$-valued quadratic form is always even.

Given a $\mathbb{Z}_4$-valued quadratic form $Q : L \to \mathbb{Z}_4$, we will be interested in the distribution of the values of the exponential sum

$$\chi_Q(c) := \sum_{x \in L} i^{Q(x)} (-1)^{\mathrm{tr}(cx)} \quad \text{for } c \in L \tag{4}$$

(where $i := \sqrt{-1}$). For alternating $\mathbb{Z}_4$-valued quadratic forms we have the following classical result (see [HK98, Thm. 6.2], for example).

Theorem 2 ([HK98, Thm. 6.2]). *Let $Q : L \to \mathbb{Z}_4$ be an alternating $\mathbb{Z}_4$-valued quadratic form of (necessarily even) rank r. Then the distribution of $\{\chi_Q(c) : c \in L\}$ is given by:*

$$\begin{array}{rlrl} 0 & \textit{occurs} & 2^m - 2^r & \textit{times} \\ \pm 2^{m-r/2} & \textit{occurs} & 2^{r-1} \pm 2^{r/2-1} & \textit{times.} \end{array}$$

For nonalternating $\mathbb{Z}_4$-valued quadratic forms the distribution of the values (4) was established by the author in [Sch09]. As an immediate corollary of [Sch09, Thm. 5] we have the following.

Theorem 3 ([Sch09, Thm. 5]). *Let $Q : L \to \mathbb{Z}_4$ be a nonalternating $\mathbb{Z}_4$-valued quadratic form of rank r, and write $s := 2\lceil r/2 \rceil$. The distribution of $\{\mathrm{Re}(\chi_Q(c)) : c \in L\}$ is given by:*

$$\begin{array}{rlrl} 0 & \textit{occurs} & 2^m - 2^{s-1} & \textit{times} \\ \pm 2^{m-s/2} & \textit{occurs} & 2^{s-2} \pm 2^{s/2-1} & \textit{times.} \end{array}$$

The distribution of $\{\mathrm{Im}(\chi_Q(c)) : c \in L\}$ is given by:

$$\begin{array}{rlrl} 0 & \textit{occurs} & 2^m - 2^{s-1} & \textit{times} \\ \pm 2^{m-s/2} & \textit{occurs} & 2^{s-2} & \textit{times (each).} \end{array}$$

In the rest of this section, we consider a particular set of $\mathbb{Z}_4$-valued quadratic forms, which has been studied by the author in [Sch09] following earlier work in [Sch08].

Let $m > 0$ be an odd integer, and let t be an integer satisfying $0 \le t \le \frac{m-1}{2}$. For $a \in L^{t+1}$ write $a = (a_0, a_1, \ldots, a_t)$, and define $Q_a : L \to \mathbb{Z}_4$ by

$$Q_a(x) := \mathrm{Tr}(a_0 x) + 2 \sum_{j=1}^{t} \mathrm{Tr}(a_j x^{2^j+1}). \tag{5}$$

It is straightforward to verify [Sch09] that Q_a is a $\mathbb{Z}_4$-valued quadratic form, and that Q_a is alternating if and only if $a_0 = 0$. The crucial property of Q_a is that, if Q_a is not identically zero, then the rank of Q_a is at least $m - 2t$. More generally, the rank distributions of the forms Q_a and of the forms Q_a that are alternating have been established in [Sch09]. 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 as

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

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

We refer to [MS77, p. 444] for some properties of Gaussian binomial coefficients.

Theorem 4 ([Sch09]). *Let $m > 0$ be an odd integer, write $n := \frac{m-1}{2}$, and let t be an integer satisfying $0 \le t \le n$. For $k = 0, 1, \ldots, t$ define*

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

Let A_j be the number of elements in $\{Q_a : a \in L^{t+1}\}$ having rank j, and let B_j be the number of elements in $\{Q_a : a \in L^{t+1}\}$ that are alternating and have rank j. Then $A_0 = B_0 = 1$, and for $j > 0$ we have $A_j = B_j = 0$ except for

$$\begin{aligned} A_{m-2k} &= \begin{bmatrix} n \\ k \end{bmatrix} S_k && \text{for } k = 0, 1, \ldots, t, \\ A_{m-2k+1} &= 4^{n-k+1} \begin{bmatrix} n \\ k-1 \end{bmatrix} S_k && \text{for } k = 1, 2, \ldots, t, \\ B_{m-2k+1} &= \begin{bmatrix} n \\ k-1 \end{bmatrix} S_k && \text{for } k = 1, 2, \ldots, t. \end{aligned}$$

4 Family $\mathscr{V}(t)$

In this section, we define Family $\mathscr{V}(t)$ and the correlation between two members of this family. We then relate the possible correlation values of Family $\mathscr{V}(t)$ to certain exponential sums. The section will be concluded with a bound on the maximum nontrivial correlations between sequences in Family $\mathscr{V}(t)$.

Let $m \ge 3$ be an odd integer, let t be an integer satisfying $0 \le t \le \frac{m-1}{2}$, and write $q := 2^m$. Let β be a primitive element in L. For $\gamma \in \mathbb{Z}_4$ and $a = (a_0, a_1, \ldots, a_t) \in R \times L^t$ define the quaternary sequence $\{s_{a,\gamma}(k)\}$ of period $q-1$ by

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

Let $\pi : \mathbb{Z}_4 \to \mathbb{Z}_2$ be the mapping defined by

$$\pi(0) = 0, \quad \pi(1) = 0, \quad \pi(2) = 1, \quad \pi(3) = 1.$$

Then the binary sequence $\{\pi(3^k s_{a,\gamma}(k))\}$ has period $2(q-1)$. Define the $(m-1)$-dimensional subspace H of L as

$$H := \{a \in L : \mathrm{tr}(a) = 0\},$$

and let

$$\Gamma(t) := \{(1 + 2c_0, c_1, \ldots, c_t) : c_0 \in H, c_1, \ldots, c_t \in L\}$$

be a subset of $R \times L^t$. *Family* $\mathscr{V}(t)$ is defined to be

$$\mathscr{V}(t) := \{\{\pi(3^k s_{a,\gamma}(k))\} : a \in \Gamma(t), \gamma \in K\}.$$

The size of $\mathscr{V}(t)$ is q^{t+1}.

For $a, b \in R \times L^t$, $\gamma, \delta \in \mathbb{Z}_4$, and integer u, the correlation at displacement u between the sequences $\{\pi(3^k s_{a,\gamma}(k))\}$ and $\{\pi(3^k s_{b,\delta}(k))\}$ is given by

$$C_{(a,\gamma),(b,\delta)}(u) := \sum_{k=0}^{2q-3} (-1)^{\pi(3^{k+u} s_{a,\gamma}(k+u)) + \pi(3^k s_{b,\delta}(k))}.$$

If $(a, \gamma) = (b, \delta)$ and $u \equiv 0 \pmod{2(q-1)}$, then the correlation value $C_{(a,\gamma),(b,\delta)}(u)$ is called *trivial* (in which case it equals $2(q-1)$), otherwise it is called *nontrivial*. The *correlation distribution* of Family $\mathscr{V}(t)$ is the distribution of the values in the multiset

$$\{C_{(a,\gamma),(b,\delta)}(u) : a, b \in \Gamma(t), \gamma, \delta \in K, 0 \le u < 2(q-1)\}.$$

In what follows, we shall establish a relation between the correlation distribution of Family $\mathscr{V}(t)$ and the distribution of certain exponential sums. A key step is the following lemma, which relates the correlation between two binary sequences of the form $\{\pi(3^k s_{a,\gamma}(k))\}$ to the correlation of their quaternary counterparts.

Lemma 5. *For $a, b \in R \times L^t$, $\gamma, \delta \in \mathbb{Z}_4$, and integer u we have*

$$C_{(a,\gamma),(b,\delta)}(u) = 2 \cdot \mathrm{Re}\left(\sum_{k=0}^{q-2} i^{3^u s_{a,\gamma}(k+u) - s_{b,\delta}(k)} \right).$$

Proof. We readily verify the identity

$$(-1)^{\pi(\alpha)+\pi(\beta)} + (-1)^{\pi(-\alpha)+\pi(-\beta)} = 2 \cdot \mathrm{Re}(i^{\alpha-\beta}) \quad \text{for } \alpha, \beta \in \mathbb{Z}_4. \tag{6}$$

Since $\{s_{a,\gamma}(k)\}$ has period $q-1$ and one of 3^{k+q-1} or 3^k is congruent 1 (mod 4) and the other is congruent -1 (mod 4), we have

$$\begin{aligned} C_{(a,\gamma),(b,\delta)}(u) &= \sum_{k=0}^{q-2} \left[(-1)^{\pi(3^u s_{a,\gamma}(k+u)) + \pi(s_{b,\delta}(k))} + (-1)^{\pi(-3^u s_{a,\gamma}(k+u)) + \pi(-s_{b,\delta}(k))} \right] \\ &= \sum_{k=0}^{q-2} 2 \cdot \mathrm{Re}\left(i^{3^u s_{a,\gamma}(k+u) - s_{b,\delta}(k)} \right), \quad \text{by (6)}, \end{aligned}$$

as required. □

We also need the following technical lemma on the number of solutions of a certain equation. Henceforth, let R^* be the following subset of R

$$R^* := \{a + 2b : a \in L \setminus K,\, b \in L\}.$$

Lemma 6. *Let j be an integer. Given $z \in R$, let $N(z)$ be the number of solutions $(a, b, c) \in H \times H \times L \setminus K$ of*

$$3^j(1+2a)c - (1+2b) = z.$$

Then

$$N(z) = \begin{cases} \frac{q}{4} & \text{for } z \in R^* \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Using (2), we find by direct inspection

$$3^j(1+2a)c-(1+2b)=\begin{cases}(c\oplus 1)+2(ac\oplus b\oplus\sqrt{c}\oplus 1) & \text{for even } j\\ (c\oplus 1)+2(ac\oplus b\oplus c\oplus\sqrt{c}\oplus 1) & \text{for odd } j.\end{cases}$$

When c ranges over $L\setminus K$, so does $c\oplus 1$. Therefore, $N(z)=0$ for $z\notin R^*$. It remains to show that, for each $c\in L\setminus K$, the number of solutions $(a,b)\in H\times H$ of $ac\oplus b=y$ is equal to $q/4$ for each $y\in L$.

Now let $c\in L\setminus K$ be arbitrary, but fixed. Application of Lemma 1 with $E=H$ (and therefore $E^\perp=K$) shows that the number of solutions $a\in H$ of

$$\mathrm{tr}(ac)=\epsilon$$

is equal to $q/4$ for each $\epsilon\in K$. Hence, as a ranges over H, the set $\{ac\oplus b : b\in H\}$ is either H or $L\setminus H$, and each of these cases occurs $q/4$ times. We conclude that, for each $y\in L$, the number of solutions $(a,b)\in H\times H$ of $ac\oplus b=y$ is $q/4$, which completes the proof. □

We are now in a position to prove the following result, which relates the correlation distribution of Family $\mathscr{V}(t)$ to the distribution of certain exponential sums.

Theorem 7. *For $a\in R\times L^t$ and $\gamma\in\mathbb{Z}_4$ define*

$$\zeta(a,\gamma):=2\cdot\mathrm{Re}\Big(\sum_{k=0}^{q-2}i^{s_{a,\gamma}(x)}\Big).$$

(a) The distribution of the correlation values

$$\{C_{(a,\gamma),(b,\delta)}(u) : a,b\in\Gamma(t),\gamma,\delta\in K, 0\le u<2(q-1), u\notin\{0,q-1\}\}$$

is as follows:

$$\begin{array}{llllll}\zeta(a,0) & (a\in R^*\times L^t) & \textit{occurs} & \frac{3}{4}q^{t+1} & \textit{times},\\ \zeta(a,1) & (a\in R^*\times L^t) & \textit{occurs} & \frac{1}{4}q^{t+1} & \textit{times},\\ \zeta(a,2) & (a\in R^*\times L^t) & \textit{occurs} & \frac{1}{4}q^{t+1} & \textit{times},\\ \zeta(a,3) & (a\in R^*\times L^t) & \textit{occurs} & \frac{3}{4}q^{t+1} & \textit{times}.\end{array}$$

(b) The distribution of the correlation values

$$\{C_{(a,\gamma),(b,\delta)}(u) : a,b\in\Gamma(t),\gamma,\delta\in K, u\in\{0,q-1\}\}$$

is as follows:

$$\begin{array}{llllll}0 & & \textit{occurs} & q^{2(t+1)} & \textit{times},\\ \zeta(a,0) & (a\in 2H\times L^t) & \textit{occurs} & q^{t+1} & \textit{times},\\ \zeta(a,0) & (a\in 2(L\setminus H)\times L^t) & \textit{occurs} & \frac{1}{2}q^{t+1} & \textit{times},\\ \zeta(a,2) & (a\in 2(L\setminus H)\times L^t) & \textit{occurs} & \frac{1}{2}q^{t+1} & \textit{times}.\end{array}$$

Proof. For $a, a' \in R \times L^t$ and integer u we have

$$\{s_{a,\gamma}(k+u)\} = \{s_{a',\gamma}(k)\},$$

where, writing $a = (a_0, a_1, \ldots, a_t)$ and $a' = (a'_0, a'_1, \ldots, a'_t)$,

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

Since β has order $q-1$ and $\gcd(2, q-1) = 1$, we then have for fixed $b \in R \times L^t$ and $\gamma, \delta \in \mathbb{Z}_4$

$$\begin{aligned} &\{\{3^u s_{a,\gamma}(k+u)\} - \{s_{b,\delta}(k)\} : a \in \Gamma(t), 0 \le u < 2(q-1), u \ne 0 \text{ even}\} \\ &= \{\{s_{a,\gamma}(k)\} - \{s_{b,\delta}(k)\} : a \in \Gamma'(t)\} \\ &= \{\{s_{a-b,\gamma-\delta}(k)\} : a \in \Gamma'(t)\}, \end{aligned} \tag{7}$$

where

$$\Gamma'(t) = \{((1+2c_0)d, c_1, \ldots, c_t) : c_0 \in H, c_1, \ldots, c_t \in L, d \in L \setminus K\}.$$

Similarly, since $\beta^{q-1} = 1$,

$$\begin{aligned} &\{\{3^u s_{a,\gamma}(k+u)\} - \{s_{b,\delta}(k)\} : a \in \Gamma(t), 0 \le u < 2(q-1), u \ne q-1 \text{ odd}\} \\ &= \{\{3s_{a,\gamma}(k)\} - \{s_{b,\delta}(k)\} : a \in \Gamma'(t)\} \\ &= \{\{s_{3a-b,3\gamma-\delta}(k)\} : a \in \Gamma'(t)\}. \end{aligned} \tag{8}$$

Then (7), (8), and application of Lemma 5 give

$$\begin{aligned} &\left\{C_{(a,\gamma),(b,\delta)}(u) : a, b \in \Gamma(t), \gamma, \delta \in K, 0 \le u < 2(q-1), u \notin \{0, q-1\}\right\} \\ &\qquad = \left\{\zeta(3^j a - b, 3^j\gamma - \delta) : a \in \Gamma'(t), b \in \Gamma(t), \gamma, \delta \in K, j \in \{0,1\}\right\}. \end{aligned} \tag{9}$$

Now, for $a, b, z \in R \times L^t$, write

$$\begin{aligned} a &= (a_0, a_1, \ldots, a_t) \\ b &= (b_0, b_1, \ldots, b_t) \\ z &= (z_0, z_1, \ldots, z_t). \end{aligned}$$

Given $j \in \{0, 1\}$ and $z \in R \times L^t$, let $N_j(z)$ be the number of solutions $(a, b) \in \Gamma'(t) \times \Gamma(t)$ of

$$3^j(a_0, 2a_1, \ldots, 2a_t) - (b_0, 2b_1, \ldots, 2b_t) = (z_0, 2z_1, \ldots, 2z_t). \tag{10}$$

Then we have by application of Lemma 6

$$N_j(z) = \begin{cases} \frac{1}{4}q^{t+1} & \text{for } z \in R^* \times L^t \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

for either j. For $j \in \{0, 1\}$ and $y \in \mathbb{Z}_4$, let $S_j(y)$ be the number of solutions $(\gamma, \delta) \in K \times K$ of $3^j\gamma - \delta = y$. Then

$$\begin{aligned} &S_0(0) = 2, \quad S_0(1) = 1, \quad S_0(2) = 0, \quad S_0(3) = 1, \\ &S_1(0) = 1, \quad S_1(1) = 0, \quad S_1(2) = 1, \quad S_1(3) = 2. \end{aligned} \tag{12}$$

Now (a) follows by combining (9), (11), and (12).

To prove (b), observe that we have by Lemma 5

$$\begin{aligned}\big\{C_{(a,\gamma),(b,\delta)}(u) : a,b \in \Gamma(t), \gamma,\delta \in K, u \in \{0,q-1\}\big\}& \\ = \big\{\zeta(3^j a - b, 3^j\gamma - \delta) : a,b \in \Gamma(t), \gamma,\delta \in K, j \in \{0,1\}\big\}&, \quad (13)\end{aligned}$$

where we used that $\{s_{a,\gamma}(k)\}$ has period $q-1$ and $3^{q-1} \equiv 3 \pmod 4$.

Given $j \in \{0,1\}$ and $z \in R \times L^t$, let $M_j(z)$ be the number of solutions $(a,b) \in \Gamma(t) \times \Gamma(t)$ satisfying (10). Since m is odd, we have $\mathrm{tr}(1) = 1$, and therefore,

$$c \in H \Longleftrightarrow (1 \oplus c) \in L \setminus H.$$

By direct inspection, we then find that

$$M_0(z) = \begin{cases} \frac{1}{2}q^{t+1} & \text{for } z \in 2H \times L^t \\ 0 & \text{otherwise} \end{cases} \quad (14)$$

and

$$M_1(z) = \begin{cases} \frac{1}{2}q^{t+1} & \text{for } z \in 2(L \setminus H) \times L^t \\ 0 & \text{otherwise.} \end{cases} \quad (15)$$

Now (b) follows by combining (13), (14), (15) and (12). In particular, the correlation value 0 occurs

$$\big(S_0(1) + S_0(3) + S_1(1) + S_1(3)\big) \cdot \big(\tfrac{1}{2}q^{t+1}\big)^2 = q^{2(t+1)}$$

times, since for $a \in 2L \times L^t$ and $2\gamma \neq 0$, the sequence $\{i^{s_{a,\gamma}(k)}\}$ is imaginary, hence $\zeta(a,\gamma) = 0$. $\square$

It will be convenient to rephrase Theorem 7. To this end, let $a = (a_0, a_1, \ldots, a_t) \in L^{t+1}$, $c \in L$, and $\gamma \in \mathbb{Z}_4$, and observe that we have by (1)

$$s_{(a_0+2c,a_1,\ldots,a_t),\gamma}(k) = Q_a(\beta^k) + 2\,\mathrm{Tr}(c\beta^k) + \gamma \quad \text{for each integer } k,$$

where Q_a is the $\mathbb{Z}_4$-valued quadratic form defined in (5). Hence

$$\begin{aligned}\zeta((a_0+2c,a_1,\ldots,a_t),\gamma) &= 2 \cdot \mathrm{Re}\bigg(i^\gamma \sum_{k=0}^{q-2} i^{Q_a(\beta^k)+2\,\mathrm{Tr}(c\beta^k)}\bigg) \\ &= 2 \cdot \mathrm{Re}\bigg(i^\gamma\Big[-1 + \sum_{x\in L} i^{Q_a(x)}(-1)^{\mathrm{tr}(cx)}\Big]\bigg).\end{aligned}$$

We therefore deduce the following.

Corollary 8. *Let $a \in L^{t+1}$, write $a = (a_0, a_1, \ldots, a_t)$, and let $Q_a : L \to \mathbb{Z}_4$ be as defined in (5). For $\gamma \in \mathbb{Z}_4$ write*

$$\xi(a,c,\gamma) := 2 \cdot \mathrm{Re}\bigg(i^\gamma\Big[-1 + \sum_{x\in L} i^{Q_a(x)}(-1)^{\mathrm{tr}(cx)}\Big]\bigg).$$

(a) The distribution of the correlation values

$$\{C_{(a,\gamma),(b,\delta)}(u) : a, b \in \Gamma(t), \gamma, \delta \in K, 0 \le u < 2(q-1), u \notin \{0, q-1\}\}$$

is as follows:

$$\begin{array}{llll} \xi(a,c,0) & (a \in (L \setminus K) \times L^t,\, c \in L) & \textit{occurs} & \frac{3}{4}q^{t+1} \quad \textit{times}, \\ \xi(a,c,1) & (a \in (L \setminus K) \times L^t,\, c \in L) & \textit{occurs} & \frac{1}{4}q^{t+1} \quad \textit{times}, \\ \xi(a,c,2) & (a \in (L \setminus K) \times L^t,\, c \in L) & \textit{occurs} & \frac{1}{4}q^{t+1} \quad \textit{times}, \\ \xi(a,c,3) & (a \in (L \setminus K) \times L^t,\, c \in L) & \textit{occurs} & \frac{3}{4}q^{t+1} \quad \textit{times}. \end{array}$$

(b) The distribution of the correlation values

$$\{C_{(a,\gamma),(b,\delta)}(u) : a, b \in \Gamma(t), \gamma, \delta \in K, u \in \{0, q-1\}\}$$

is as follows:

$$\begin{array}{llll} 0 & & \textit{occurs} & q^{2(t+1)} \quad \textit{times}, \\ \xi(a,c,0) & (a \in L^{t+1},\, a_0 = 0,\, c \in H) & \textit{occurs} & q^{t+1} \quad \textit{times}, \\ \xi(a,c,0) & (a \in L^{t+1},\, a_0 = 0,\, c \in L \setminus H) & \textit{occurs} & \frac{1}{2}q^{t+1} \quad \textit{times}, \\ \xi(a,c,2) & (a \in L^{t+1},\, a_0 = 0,\, c \in L \setminus H) & \textit{occurs} & \frac{1}{2}q^{t+1} \quad \textit{times}. \end{array}$$

Using Corollary 8, we can easily bound the magnitude of the nontrivial correlations between sequences in Family $\mathscr{V}(t)$ as follows.

Theorem 9. *The nontrivial correlation values of Family $\mathscr{V}(t)$ are bounded in magnitude by $2 + 2^t\sqrt{2q}$.*

Proof. Let $\xi(a, c, \gamma)$ be as defined in Corollary 8. By Corollary 8, in the correlation distribution of Family $\mathscr{V}(t)$ the trivial correlation value $\xi(0, 0, 0) = 2(q-1)$ occurs exactly $|\mathscr{V}(t)| = q^{t+1}$ times, and the value $\xi(0, 0, 2)$ never occurs. Therefore, the nontrivial correlation values of Family $\mathscr{V}(t)$ are contained in the set

$$\{\xi(a, c, \gamma) : a \in L^{t+1}, c \in L, \gamma \in \mathbb{Z}_4, (a, c, 2\gamma) \text{ nonzero}\}. \tag{16}$$

We have $\xi(0, 0, \gamma) = 0$ for $2\gamma \neq 0$, and from Lemma 1, applied with $E = L$, we conclude that $\xi(0, c, \gamma) = -2\mathrm{Re}(i^\gamma)$ for $c \neq 0$. Theorem 4 asserts that the rank of Q_a is at least $m - 2t$ for nonzero a. We then conclude from Theorems 2 and 3 that the values in the set (16) are bounded in magnitude by $2 + 2^{\frac{m+1}{2}+t}$. □

Theorem 9 was proved by Helleseth and Kumar [HK98, p. 1833] for $t \in \{0, 1\}$. In general, Family $\mathscr{V}(t)$ is a subset of Family $Q(2^t + 1)$, as defined by Helleseth and Kumar in [HK98]. In [HK98, p. 1832] it was proved that all nontrivial correlation values of Family $Q(2^t+1)$ are at most $2+2^{t+1}\sqrt{q}$ in magnitude, which differs from the bound in Theorem 9 approximately by a factor $\sqrt{2}$.

Table 2: Correlation Distribution of Family $\mathscr{V}(0)$.

value	frequency
$2(q-1)$	q
0	q^2
2	$\frac{q^2}{4}$
-2	$\frac{3q^2}{4}-q$
$\pm\sqrt{2q}$	$\frac{q^2}{2}(q-2)$ (each)
$2\pm\sqrt{2q}$	$\frac{q}{4}(q-2)(\frac{q}{2}\mp\sqrt{\frac{q}{2}})$
$-2\pm\sqrt{2q}$	$\frac{3q}{4}(q-2)(\frac{q}{2}\pm\sqrt{\frac{q}{2}})$

5 Correlation Distribution of Families $\mathscr{V}(0)$ and $\mathscr{V}(1)$

In this section, we use Corollary 8 to establish the correlation distribution of Families $\mathscr{V}(0)$ and $\mathscr{V}(1)$. The correlation distribution of Family $\mathscr{V}(0)$ has been derived in [THJ08]. Based on Corollary 8, we give a short alternative proof for this result.

Theorem 10. *The distribution of the correlation values*

$$\{C_{(a,\gamma),(b,\delta)}(u) : a,b \in \Gamma(0), \gamma,\delta \in K, 0 \le u < 2(q-1)\} \tag{17}$$

is given in Table 2.

Proof. Let $\xi(a,c,\gamma)$ be as defined in Corollary 8. The $\mathbb{Z}_4$-valued quadratic form $Q_a(x) = \mathrm{Tr}(ax)$ is nonalternating and has rank m for each $a \in L \setminus K$. (Alternatively, the last fact can be deduced from Theorem 4 with $t = 0$.) Application of Theorem 3 then gives the number of occurrences of the correlation values $\pm\sqrt{2q}$ and $\pm 2 \pm \sqrt{2q}$, identified in Corollary 8 (a). The number of occurrences of the correlation values $2(q-1)$, 0, and ± 2, identified in Corollary 8 (b), are easily established using the fact

$$\sum_{x\in L}(-1)^{\mathrm{tr}(cx)} = \begin{cases} 0 & \text{for } c \in L \setminus \{0\} \\ q & \text{for } c = 0 \end{cases}$$

(see Lemma 1) and that $0 \in H$. □

In what follows, we establish the correlation distribution of Family $\mathscr{V}(1)$. We treat the respective exponential sums arising in Corollary 8 (a) and in Corollary 8 (b) in Lemmas 11 and 12 below.

Lemma 11. *The distribution of the correlation values*

$$\{C_{(a,\gamma),(b,\delta)}(u) : a,b \in \Gamma(1), \gamma,\delta \in K, 0 \le u < 2(q-1), u \notin \{0, q-1\}\} \tag{18}$$

is given in Table 3.

Table 3: Correlation Distribution of Family $\mathscr{V}(t)$ at Shifts not in $\{0, q-1\}$.

value	frequency
0	$\frac{q^3}{2}(q-2)^2$
2	$\frac{q^3}{8}(q-2)^2$
-2	$\frac{3q^3}{8}(q-2)^2$
$\pm\sqrt{2q}$	$\frac{q^3}{6}(q-2)(q+4)$ (each)
$2 \pm \sqrt{2q}$	$\frac{q^2}{12}(q-2)(q+4)(\frac{q}{2} \mp \sqrt{\frac{q}{2}})$
$-2 \pm \sqrt{2q}$	$\frac{q^2}{4}(q-2)(q+4)(\frac{q}{2} \pm \sqrt{\frac{q}{2}})$
$\pm 2\sqrt{2q}$	$\frac{q^3}{12}(q-2)^2$ (each)
$2 \pm 2\sqrt{2q}$	$\frac{q^2}{6}(q-2)^2(\frac{q}{8} \mp \sqrt{\frac{q}{8}})$
$-2 \pm 2\sqrt{2q}$	$\frac{q^2}{2}(q-2)^2(\frac{q}{8} \pm \sqrt{\frac{q}{8}})$

Proof. We adopt the notation of Corollary 8. The $\mathbb{Z}_4$-valued quadratic form Q_a is nonalternating for each $a \in (L \setminus K) \times L$. Therefore, in view of Theorem 3, in order to establish the distribution of the values in (18), it is sufficient to determine the numbers

$$C_{2j} := \big|\{Q_a : a \in (L \setminus K) \times L, \text{ rank}(Q_a) = 2j \text{ or } 2j-1\}\big|$$

for $j = 0, 1, \ldots, \frac{m+1}{2}$. Let A_j be the number of elements in $\{Q_a : a \in L \times L\}$ having rank j, and let B_j be the number of elements in $\{Q_a : a \in L \times L\}$ that are alternating and have rank j. Since Q_a is alternating if and only if $a_0 = 0$ and for $a_0 \neq 0$ we have $\text{rank}(Q_{(a_0,a_1)}) = \text{rank}(Q_{(1,a_1/a_0^3)})$, we readily verify that

$$C_{2j} = \tfrac{q-2}{q-1}(A_{2j} + A_{2j-1} - B_{2j}) \quad \text{for } j = 0, 1, \ldots, \tfrac{m+1}{2}.$$

From Theorem 4, $A_0 = B_0 = 1$, and for $j > 0$, we have $A_j = B_j = 0$ except for

$$\begin{aligned} A_m &= \tfrac{1}{3}(q-1)(q+4), \\ A_{m-1} &= \tfrac{q}{2}(q-1), \\ A_{m-2} &= \tfrac{1}{3}(q-1)(\tfrac{q}{2}-1), \\ B_{m-1} &= q-1. \end{aligned}$$

Therefore, C_{2j} is equal to zero, except for

$$\begin{aligned} C_{m+1} &= \tfrac{1}{3}(q-2)(q+4), \\ C_{m-1} &= \tfrac{2}{3}(q-2)^2. \end{aligned}$$

Now the lemma follows from Theorem 3 and Corollary 8 (a). □

Table 4: Correlation Distribution of Family $\mathscr{V}(t)$ at Shifts in $\{0, q-1\}$.

value	frequency
$2(q-1)$	q^2
0	q^4
2	$\frac{q^4}{8}$
-2	$q^2(\frac{3q^2}{8}+\frac{q}{2}-1)$
$2\pm 2\sqrt{2q}$	$\frac{q^3}{4}(\frac{q}{4}\mp\sqrt{\frac{q}{8}})$
$-2\pm 2\sqrt{2q}$	$q^2(\frac{3q}{4}-1)(\frac{q}{4}\pm\sqrt{\frac{q}{8}})$

Lemma 12. *The distribution of the correlation values*

$$\{C_{(a,\gamma),(b,\delta)}(u) : a, b \in \Gamma(1), \gamma, \delta \in K, u \in \{0, q-1\}\}$$

is given in Table 4.

Proof. We use the notation of Corollary 8. Note that for $a_0 = 0$ we have $Q_a(x) = 2\,\mathrm{Tr}(a_1x^3) = 2\,\mathrm{tr}(a_1x^3)$. For $b, c \in L$ define

$$\tau(b,c) := \sum_{x\in L}(-1)^{\mathrm{tr}(bx^3)+\mathrm{tr}(cx)},$$

so that $\xi((0,b),c,\gamma) = 2\cdot\mathrm{Re}(i^\gamma[-1+\tau(b,c)])$ for all $b, c \in L$ and all $\gamma \in \mathbb{Z}_4$. In view of Corollary 8 (b), to prove the lemma, it is sufficient to determine the distribution of

$$\{\tau(b,c) : b \in L,\, c \in H\} \tag{19}$$

and the distribution of

$$\{\tau(b,c) : b \in L,\, c \in L \setminus H\}\,. \tag{20}$$

For $a_0 = 0$ the $\mathbb{Z}_4$-valued quadratic form $Q_a(x) = 2\,\mathrm{tr}(a_1x^3)$ is alternating, and Theorem 4 can be used to verify that its rank equals $m-1$ for $a_1 \neq 0$ and equals zero for $a_1 = 0$. Therefore, by Theorem 2, the distribution of

$$\{\tau(b,c) : b, c \in L\} \tag{21}$$

is given by:

$$\begin{array}{rlrl} q & \text{occurs} & 1 & \text{time} \\ 0 & \text{occurs} & (q-1)(\frac{q}{2}+1) & \text{times} \\ \pm\sqrt{2q} & \text{occurs} & (q-1)(\frac{q}{4}\pm\sqrt{\frac{q}{8}}) & \text{times.} \end{array}$$

For $c \neq 0$ we have $\tau(b,c) = \tau(b/c^3, 1)$ for each $b \in L$. Therefore, for fixed $c \in L$, the distribution of $\{\tau(b,c) : b \in L\}$ depends only on whether $c = 0$ or $c \neq 0$. Since we know the distribution of (21), in order to obtain the distributions of (19) and (20), it is sufficient to know $\tau(b,0)$ for all $b \in L$. Clearly, $\tau(0,0) = q$. When m is odd, $\gcd(3, q-1) = 1$, hence for $b \neq 0$, the mapping $x \mapsto bx^3$ is a permutation on L. By Lemma 1, applied with $E = L$, we then have

$$\tau(b,0) = \begin{cases} q & \text{for } b = 0 \\ 0 & \text{for } b \neq 0. \end{cases}$$

Since $0 \in L$ is contained in H, the distribution of (19) is given by:

$$\begin{array}{rlrl} q & \text{occurs} & 1 & \text{time} \\ 0 & \text{occurs} & (\frac{q}{2}-1)\frac{q}{2} + q - 1 & \text{times} \\ \pm\sqrt{2q} & \text{occurs} & (\frac{q}{2}-1)(\frac{q}{4} \pm \sqrt{\frac{q}{8}}) & \text{times,} \end{array}$$

and the distribution of (20) is given by:

$$\begin{array}{rlrl} 0 & \text{occurs} & \frac{q^2}{4} & \text{times} \\ \pm\sqrt{2q} & \text{occurs} & \frac{q}{2}(\frac{q}{4} \pm \sqrt{\frac{q}{8}}) & \text{times.} \end{array}$$

Now the lemma is a straightforward consequence of Corollary 8 (b). □

Combination of Lemmas 11 and 12 gives the correlation distribution of Family $\mathscr{V}(1)$.

Theorem 13. *The distribution of the correlation values*

$$\{C_{(a,\gamma),(b,\delta)}(u) : a, b \in \Gamma(1), \gamma, \delta \in K, 0 \leq u < 2(q-1)\}$$

is given in Table 5.

6 Remarks on the Case When $t > 1$

This paper grew out in an attempt to establish the correlation distribution of Family $\mathscr{V}(t)$ for all t satisfying $0 \leq t \leq \frac{m-1}{2}$. However, it turned out to be difficult to handle the cases when $t > 1$. In this section, we comment on this issue.

It is not hard to establish, for general t, the distribution of the correlation values between sequences in Family $\mathscr{V}(t)$ for shifts u not in $\{0, q-1\}$. This can be done by adapting the proof of Lemma 11. The difficulty arises in the analysis of the distribution of the remaining correlation values

$$\{C_{(a,\gamma),(b,\delta)}(u) : a, b \in \Gamma(t), \gamma, \delta \in K, u \in \{0, q-1\}\}. \tag{22}$$

Given $b \in L^t$, write $b = (b_1, b_2, \ldots, b_t)$. For $b \in L^t$ and $c \in L$ define

$$f_b(x) := \sum_{j=1}^{t} \mathrm{tr}(b_j x^{2^j+1})$$

Table 5: Correlation Distribution of Family $\mathscr{V}(1)$.

value	frequency
$2(q-1)$	q^2
0	$\frac{q^3}{2}(q-2)^2+q^4$
2	$\frac{q^3}{8}(q-2)^2+\frac{q^4}{8}$
-2	$\frac{3q^3}{8}(q-2)^2+q^2(\frac{3q^2}{8}+\frac{q}{2}-1)$
$\pm\sqrt{2q}$	$\frac{q^3}{6}(q-2)(q+4)$ (each)
$2\pm\sqrt{2q}$	$\frac{q^2}{12}(q-2)(q+4)(\frac{q}{2}\mp\sqrt{\frac{q}{2}})$
$-2\pm\sqrt{2q}$	$\frac{q^2}{4}(q-2)(q+4)(\frac{q}{2}\pm\sqrt{\frac{q}{2}})$
$\pm2\sqrt{2q}$	$\frac{q^3}{12}(q-2)^2$ (each)
$2\pm2\sqrt{2q}$	$\frac{q^2}{6}(q-2)^2(\frac{q}{8}\mp\sqrt{\frac{q}{8}})+\frac{q^3}{4}(\frac{q}{4}\mp\sqrt{\frac{q}{8}})$
$-2\pm2\sqrt{2q}$	$\frac{q^2}{2}(q-2)^2(\frac{q}{8}\pm\sqrt{\frac{q}{8}})+q^2(\frac{3q}{4}-1)(\frac{q}{4}\pm\sqrt{\frac{q}{8}})$

and

$$\tau(b,c) := \sum_{x\in L}(-1)^{f_b(x)+\mathrm{tr}(cx)}.$$

By Corollary 8 (b), in order to compute the distribution of the values in (22), we need to determine the distribution of $\tau(b,c)$ when (b,c) ranges over $L^t\times H$ and when (b,c) ranges over $L^t\times L\setminus H$. Using Theorems 4 and 2, we can establish the distribution of $\tau(b,c)$ when (b,c) ranges over $L^t\times L$. For $c\neq 0$ the variable substitution $x\mapsto \frac{x}{c}$ gives $\tau(b,c)=\tau(b',1)$, where $b'=(b'_1,b'_2,\ldots,b'_t)$ and

$$b'_j=\frac{b_j}{c^{2^j+1}} \quad \text{for } j=1,2,\ldots,t.$$

It is therefore sufficient to determine the distribution of $\tau(b,0)$ when b ranges over L^t.

For $t=2$ we have $f_b(x)=\mathrm{tr}(b_1x^3)+\mathrm{tr}(b_2x^5)$. In this case, one can deduce the distribution of $\{\tau(b,0):b\in L^t\}$ from a recent result by Johansen and Helleseth [JH09] on the crosscorrelation between the two m-sequences $\{\mathrm{tr}(\beta^{3k})\}$ and $\{\mathrm{tr}(\beta^{5k})\}$, where β is a primitive element in L. In this way, the correlation distribution of Family $\mathscr{V}(2)$ can be established. The result however is quite complex and is omitted.

In the general case, the computation of the distribution of the values in the multiset $\{\tau(b,0):b\in L^t\}$ is left as a challenging open problem.

References

[HK98] 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.

[JH09] A. Johansen and T. Helleseth. A family of m-sequences with five-valued cross correlation. *IEEE Trans. Inf. Theory*, 55(2):880–887, Feb. 2009.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[Nec91] A. A. Nechaev. Kerdock code in a cyclic form. *Discrete Math. Appl.*, 1(4):365–384, 1991.

[Sch08] K.-U. Schmidt. Symmetric bilinear forms over finite fields of even characteristic. *Submitted for publication*, 2008.

[Sch09] K.-U. Schmidt. $\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families. *IEEE Trans. Inf. Theory*, 55(12):5803–5810, Dec. 2009.

[THJ08] X. Tang, T. Helleseth, and A. Johansen. On the correlation distribution of Kerdock sequences. In *Proc. of Sequences and Their Applications (SETA)*, volume 5203 of *Lecture Notes in Computer Science*, pages 121–129. New York: Springer Verlag, 2008.