

# Another New Family of Binary Sequences with Six or eight-valued Correlations

Sankhadip Roy\*

Department of Basic Science and Humanities, University of Engineering and Management, Kolkata-160, India

In this correspondence, for a positive even integer  $n$ , a new family of binary sequences with  $2^n + 1$  sequences of length  $2^n - 1$  taking six and eight valued correlations is presented. This family can be considered as a new class of Gold-like sequences.

PACS numbers:

## I. INTRODUCTION

Since the late sixties, many families of binary sequences of length  $2^n - 1$  with optimal correlations [2],[3],[4],[6] have been found, where  $n$  is a positive integer. The Gold sequence family [2] is the best known binary sequence family having four-valued correlations. For an odd  $n$ , Boztas and Kumar [1] introduced a family of binary sequences, the so-called Gold-like sequences, whose correlation distribution is identical to that of Gold sequences. For even  $n$ , Udaya [7] introduced families of binary sequences with six-valued correlations. Later, Kim and No further generalized the Gold-like sequences to GKW-like sequences by the quadratic form technique [4]. In this paper, we use the quadratic form technique to get a new family of optimal binary sequences with  $2^n + 1$  sequences of length  $2^n - 1$ .

## II. PRELIMINARIES

Let  $F_{2^n}$  be the finite field with  $2^n$  elements. The trace function from  $F_{2^n}$  to  $F_{2^e}$  is defined by

$$tr_e^n(x) = \sum_{i=0}^{\frac{n}{e}-1} x^{2^{ei}}$$

where  $x \in F_{2^n}$  and  $e|n$  and  $\{v_0, v_1, \dots, v_{2^n-1}\}$  is an enumeration of the elements in  $F_{2^n}$ . We also recall that the symplectic bilinear form of a trace form  $f(x)$  is

$$B(x, z) = f(x) + f(z) + f(x + z) \text{ for } x, z \in F_{2^n}.$$

Let  $f(x)$  be a function from  $F_{2^n}$  to  $F_2$ . The trace transform  $F(\lambda)$  of  $f(x)$  is defined by

$$F(\lambda) = \sum_{x \in F_{2^n}} (-1)^{f(x) + tr_1^n(x\lambda)}.$$

**Lemma 1.** (Helleseth and Kumar [3]) Let  $f(x)$  be a quadratic Boolean function on  $F_{2^n}$ . If the rank of  $f(x)$  is  $2h$ ,  $2 \leq 2h \leq n$ , then the distribution of the trace transform values is given by

$$F(\lambda) = \begin{cases} 2^{n-h}, & 2^{2h-1} + 2^{h-1} \text{ times} \\ 0, & 2^n - 2^{2h} \text{ times} \\ -2^{n-h}, & 2^{2h-1} - 2^{h-1} \text{ times} \end{cases}$$

where rank is the co-dimension of the radical of  $f(x)$ .

All the sequence families considered in this paper are constructed by using the trace function  $a(x) = tr_1^n(x)$  and some quadratic form  $b(x)$  as follows:

$$C = \{f_i(x) | 0 \leq i \leq 2^n, x \in F_{2^n}^*\}$$

where

$$f_i(x) = \begin{cases} a(v_i x) + b(x), & 0 \leq i \leq 2^n - 1 \\ a(x), & i = 2^n. \end{cases}$$

The correlation function between two sequences defined by  $f_i(x)$  and  $f_j(x)$  can be given by the function from  $F_{2^n}$  to the set of integers  $\mathbb{Z}$  as

$$R_{i,j}(\delta) = \sum_{x \in F_{2^n}^*} (-1)^{f_i(x) + f_j(\delta x)}$$

where  $\delta \in F_{2^n}^*$  and it can be expressed as a trace transform

$$\begin{aligned} R_{i,j}(\delta) &= \sum_{x \in F_{2^n}^*} (-1)^{tr_1^n([v_i + v_j]x) + g(x)} \\ &= -1 + \sum_{x \in F_{2^n}} (-1)^{tr_1^n(x\lambda) + g(x)} \\ &= -1 + G(\lambda) \end{aligned}$$

where  $g(x) = b(\delta x) + b(x)$  and  $\lambda = v_i + v_j \in F_{2^n}$ .

**Definition 1.** Let  $\frac{n}{e} = m$  be even. We define the Boolean functions  $p(x)$  and  $q(x)$  by  $p(x) = \sum_{l=1}^{\frac{n}{2}-1} tr_1^n(x^{2^l+1})$ ,  $q(x) = \sum_{l=1}^{\frac{m}{2}-1} tr_1^n(x^{2^{e^l}+1})$ .

**Definition 2.** (Udaya [7]) For an even integer  $n = 2k \geq 4$ , Udaya introduced the following family  $G$

$$g_i(x) = \begin{cases} tr_1^n(v_i x) + p(x) + tr_1^{\frac{n}{2}}(x^{2^{\frac{n}{2}}+1}), & 0 \leq i \leq 2^n - 1 \\ tr_1^n(x), & i = 2^n. \end{cases}$$

\*Email: sankhadip.roy@uem.edu.in

**Theorem 1.** (Udaya [7]) For the family  $G$ , the distribution of correlation values  $R_{i,j}(\delta)$  are given as follows:

$$\begin{cases} 2^n - 1, & 2^n + 1 \text{ times} \\ -1, & 2^{2n-1}(2^{n-1} + 2^{n-2}) + 2^{2n} - 2 \text{ times} \\ -1 + 2^k, & (2^{2n-1} - 2)(2^{n-1} + 2^{k-1}) \text{ times} \\ -1 - 2^k, & (2^{2n-1} - 2)(2^{n-1} - 2^{k-1}) \text{ times} \\ -1 + 2^{k+1}, & 2^{2n-1}(2^{n-3} + 2^{k-2}) \text{ times} \\ -1 - 2^{k+1}, & 2^{2n-1}(2^{n-3} - 2^{k-2}) \text{ times.} \end{cases}$$

**Definition 3.** (Kim and No [4]) Let  $\frac{n}{e} = m$  be an even integer, where  $m \geq 4$ . Kim and No introduced the following sequences  $S$  with six-valued correlations.

$$s_i(x) = \begin{cases} tr_1^n(v_i x) + q(x) + tr_1^{\frac{n}{2}}(x^{2^{\frac{n}{2}+1}}), & 0 \leq i \leq 2^n - 1 \\ tr_1^n(x), & i = 2^n. \end{cases}$$

**Theorem 2.** (Kim and No [4]) For the family  $S$ , the distribution of correlation values  $R_{i,j}(\delta)$  are given as follows:

$$\begin{cases} 2^n - 1, & 2^n + 1 \text{ times} \\ -1, & 2^{2n-e}(2^n - 2^{n-2e}) + (2^{2n} - 2) \text{ times} \\ -1 + 2^{\frac{n+2e}{2}}, & 2^{2n-e}(2^{n-2e-1} + 2^{\frac{n-2e-2}{2}}) \text{ times} \\ -1 - 2^{\frac{n+2e}{2}}, & 2^{2n-e}(2^{n-2e-1} - 2^{\frac{n-2e-2}{2}}) \\ -1 + 2^{\frac{n}{2}}, & (2^{2n} - 2^{2n-e} - 2)(2^{n-1} + 2^{\frac{n}{2}-1}) \text{ times} \\ -1 - 2^{\frac{n}{2}}, & (2^{2n} - 2^{2n-e} - 2)(2^{n-1} - 2^{\frac{n}{2}-1}) \text{ times.} \end{cases}$$

In this paper we introduce a new family  $U$  which is a combination of  $G$  and  $S$ .

**Definition 4.** Let  $\frac{n}{e} = m \geq 4$  be even. We define the family  $U$  of binary sequences by

$$u_i(x) = \begin{cases} tr_1^n(v_i x) + p(x) + q(x), & 0 \leq i \leq 2^n - 1 \\ tr_1^n(x), & i = 2^n. \end{cases}$$

For the correlation property of the family  $U$ , we have the following main result.

**Theorem 3.** The distribution of correlation values of the family  $U$  is given as when  $e$  is odd

Correlation ( $R_{i,j}(\delta)$ )	Number of times it appears
$2^n - 1$	$2^n + 1$
$-1$	$2^{3n} + 2^{2n} - 2^{n+1} + 2^e$ $+ 2^{n+2e-1}(2^{e-1} - 2^{n-1} - 1) - 2$
$-1 + 2^{n-\frac{e-1}{2}}$	$(2^{e-2} + 2^{\frac{e-3}{2}})(2^{n+e} - 2)$
$-1 - 2^{n-\frac{e-1}{2}}$	$(2^{e-2} - 2^{\frac{e-3}{2}})(2^{n+e} - 2)$
$-1 + 2^{n-e+1}$	$(2^{2e-3} + 2^{e-2})(2^{2n} - 2^{n+e})$
$-1 - 2^{n-e+1}$	$(2^{2e-3} - 2^{e-2})(2^{2n} - 2^{n+e})$

and when  $e$  is even

Correlation ( $R_{i,j}(\delta)$ )	Number of times it appears
$2^n - 1$	$2^n + 1$
$-1$	$2^{3n} + 2^{2n} - 2^{n+1} + 2^{e+1}$ $+ 2^{n+e-2}(3 \cdot 2^{e-1} - 2^{n+2} - 3) - 2$
$-1 + 2^{n-\frac{e}{2}}$	$(2^{e-1} + 2^{\frac{e-2}{2}})(2^{n+e-1} + 2^n - 2)$
$-1 - 2^{n-\frac{e}{2}}$	$(2^{e-1} - 2^{\frac{e-2}{2}})(2^{n+e-1} + 2^n - 2)$
$-1 + 2^{n-\frac{e-2}{2}}$	$(2^{e-3} + 2^{\frac{e-4}{2}})(2^{n+e-1} - 2^n)$
$-1 - 2^{n-\frac{e-2}{2}}$	$(2^{e-3} - 2^{\frac{e-4}{2}})(2^{n+e-1} - 2^n)$
$-1 + 2^{n-e}$	$(2^{2e-1} + 2^{e-1})(2^{2n} - 2^{n+e})$
$-1 - 2^{n-e}$	$(2^{2e-1} - 2^{e-1})(2^{2n} - 2^{n+e})$

### III. CORRELATION OF $p(x) + q(x)$

The following theorem describes the correlation of  $p(x) + q(x)$ .

**Theorem 4.** The distribution of the trace transform values (cross-correlation values) of  $p(x) + q(x)$  is given as

$$\begin{cases} 2^{n-\frac{e-1}{2}}, & 2^{e-2} + 2^{\frac{e-3}{2}} \text{ times} \\ 0, & 2^n - 2^{e-1} \text{ times} \\ -2^{n-\frac{e-1}{2}}, & 2^{e-2} - 2^{\frac{e-3}{2}} \text{ times} \end{cases} \text{ when } e \text{ is odd}$$

$$\begin{cases} 2^{n-\frac{e}{2}}, & 2^{e-1} + 2^{\frac{e-2}{2}} \text{ times} \\ 0, & 2^n - 2^e \text{ times} \\ -2^{n-\frac{e}{2}}, & 2^{e-1} - 2^{\frac{e-2}{2}} \text{ times} \end{cases} \text{ when } e \text{ is even.}$$

*Proof.* For the proof we will be using some results from [6] and [7]. We have for  $p'(x) = \sum_{l=1}^{\frac{n}{2}-1} tr_1^n(x^{2^l+1}) + tr_1^{\frac{n}{2}}(x^{2^{\frac{n}{2}+1}})$ ,  $B_{p'}(x, z) = tr_1^n(z(tr_1^n(x) + x))$  and for  $q'(x) = \sum_{l=1}^{\frac{n}{2}-1} tr_1^n(x^{2^{el}+1}) + tr_1^{\frac{n}{2}}(x^{2^{\frac{n}{2}+1}})$ ,  $B_{q'}(x, z) = tr_1^n(z(tr_e^n(x) + x))$ . Then  $B_{p+q}(x, z) = B_{p'+q'}(x, z) = tr_1^n(z[tr_e^n(x) + tr_1^n(x)])$ . So we need to find the number of  $x \in F_{2^n}$  such that  $tr_e^n(x) + tr_1^n(x) = 0$  which implies  $tr_e^n(x) = 0$  or  $1$  when  $e$  is odd.

Now  $tr_e^n : F_{2^n} \xrightarrow{onto} F_{2^e}$ . So  $|Ker(tr_e^n)| = \frac{2^n}{2^e} = 2^{n-e}$ . Therefore  $|\{x \in F_{2^n} : tr_e^n(x) = 0 \text{ or } 1\}| = 2|Ker(tr_e^n)| = 2^{n-e+1}$ . Hence the rank of  $p+q$  is  $n - (n - e + 1) = e - 1$  and we get the first case using the Lemma 1.

When  $e$  is even, if  $tr_e^n(x) = 1, tr_1^n(x) = tr_1^e(tr_e^n(x)) = tr_1^e(1) = 0$ . So  $tr_e^n(x) + tr_1^n(x) \neq 0$ . So when  $e$  is even  $tr_e^n(x) = 0$  and in that case rank of  $p+q$  is equal to  $e$  and we get the second case.  $\square$

### IV. PROOF OF THEOREM 8

The proof can be divided into the following five cases.

**Case 1:**  $\delta = 1, i = j$  :

It is a trivial case and thus

$$R_{i,j}(\delta) = \sum_{x \in F_{2^n}^*} (-1)^{f_i(x)+f_j(x)} = 2^n - 1, 2^n + 1 \text{ times.}$$

**Case 2:**  $\delta \neq 1, i = j = 2^n :$

$$R_{i,j}(\delta) = \sum_{x \in F_{2^n}^*} (-1)^{tr_1^n(x)+tr_1^n(\delta x)} = \sum_{x \in F_{2^n}^*} (-1)^{tr_1^n(1+\delta x)} = -1, 2^n - 2 \text{ times (number of choices for } \delta \neq 0, 1).$$

**Case 3:**  $\delta = 1, i \neq j, 0 \leq i, j \leq 2^n - 1 :$

$$R_{i,j}(\delta) = \sum_{x \in F_{2^n}^*} (-1)^{u_i(x)+u_j(x)} = \sum_{x \in F_{2^n}^*} (-1)^{tr_1^n((v_i+v_j)x)} = -1, \quad 2^n(2^n - 1) \text{ times}$$

**Case 4:**  $i = 2^n, j \neq 2^n$  (or  $j = 2^n, i \neq 2^n$ ):

For fixed  $\delta$

$$R_{2^n,j}(\delta) = \sum_{x \in F_{2^n}^*} (-1)^{tr_1^n([\delta+v_j]x)+p(x)+q(x)} = -1 + \sum_{x \in F_{2^n}^*} (-1)^{tr_1^n(\lambda x)+p(x)+q(x)}$$

for  $\lambda = \delta + v_j$ .

The distribution of the trace transform of  $p(x) + q(x)$  is already given in Theorem 9. Therefore, the distribution of correlation function for a fixed  $\delta$  is given as

$$\begin{cases} -1 + 2^{n-\frac{e-1}{2}}, & 2^{e-2} + 2^{\frac{e-3}{2}} \text{ times} \\ -1, & 2^n - 2^{e-1} \text{ times} \\ -1 - 2^{n-\frac{e-1}{2}}, & 2^{e-2} - 2^{\frac{e-3}{2}} \text{ times} \end{cases} \quad \text{when } e \text{ is odd}$$

$$\begin{cases} -1 + 2^{n-\frac{e}{2}}, & 2^{e-1} + 2^{\frac{e-2}{2}} \text{ times} \\ -1, & 2^n - 2^e \text{ times} \\ -1 - 2^{n-\frac{e}{2}}, & 2^{e-1} - 2^{\frac{e-2}{2}} \text{ times} \end{cases} \quad \text{when } e \text{ is even.}$$

As  $\delta$  varies over  $F_{2^n}^*$ , the distribution is for  $e$  odd

$$\begin{cases} -1 + 2^{n-\frac{e-1}{2}}, & (2^{e-2} + 2^{\frac{e-3}{2}})(2^n - 1) \text{ times} \\ -1, & (2^n - 2^{e-1})(2^n - 1) \text{ times} \\ -1 - 2^{n-\frac{e-1}{2}}, & (2^{e-2} - 2^{\frac{e-3}{2}})(2^n - 1) \text{ times} \end{cases}$$

and for  $e$  even

$$\begin{cases} -1 + 2^{n-\frac{e}{2}}, & (2^{e-1} + 2^{\frac{e-2}{2}})(2^n - 1) \text{ times} \\ -1, & (2^n - 2^e)(2^n - 1) \text{ times} \\ -1 - 2^{n-\frac{e}{2}}, & (2^{e-1} - 2^{\frac{e-2}{2}})(2^n - 1) \text{ times} \end{cases}$$

**Case 5:**  $\delta \in F_{2^n} \setminus \{0, 1\}$  and  $0 \leq i, j \leq 2^n - 1 :$

In this case, we have

$$u_i(x) + u_j(\delta x) = p(x) + q(x) + p(\delta x) + q(\delta x) + tr_1^n([v_i + \delta v_j]x).$$

Actually, the correlation function is equivalent to the trace transform of a function  $r(x)$  which is given as

$$r(x) = p(x) + q(x) + p(\delta x) + q(\delta x).$$

In order to compute the distribution of the correlation values, the rank of the symplectic form associated with  $r(x)$  must be found and it is enough to count the number of  $x$  in  $F_{2^n}$  satisfying

$$B_r(x, z) = 0, \text{ for all } z \in F_{2^n}$$

where

$$B_r(x, z) = r(x) + r(z) + r(x + z).$$

Plugging  $p(x)$  and  $q(x)$  into  $B_r(x, z)$ , we have

$$B_r(x, z) = tr_1^n(z[tr_1^n(x) + tr_e^n(x)] + \delta z[tr_1^n(\delta x) + tr_e^n(\delta x)]) = tr_1^n(z[\delta tr_1^n(\delta x) + \delta tr_e^n(\delta x) + tr_1^n(x) + tr_e^n(x)]).$$

So the rank can be computed by determining the number of solutions to

$$\delta tr_1^n(\delta x) + \delta tr_e^n(\delta x) + tr_1^n(x) + tr_e^n(x) = 0. \quad (1)$$

Let  $tr_e^n(x) = a$  and  $tr_e^n(\delta x) = b$ , where  $a, b \in F_{2^e}$ . Then (1) can be written as

$$\delta tr_1^e(b) + tr_1^e(a) + \delta b + a = 0. \quad (2)$$

**SubCase 1:**  $\delta \in F_{2^e}$ . Then from equation (1), we get

$$\delta^2 a + \delta tr_1^n(\delta x) + tr_1^n(x) + a = 0 \quad (3)$$

as  $tr_e^n(\delta x) = \delta tr_e^n(x) = \delta a$  because  $\delta \in F_{2^e}$ .

Now we have the following four cases depending on the values of  $tr_1^n(\delta x)$  and  $tr_1^n(x)$

1.  $tr_1^n(\delta x) = 1$  and  $tr_1^n(x) = 1$ , which implies  $\delta^2 a + \delta + 1 + a = 0$ .
2.  $tr_1^n(\delta x) = 1$  and  $tr_1^n(x) = 0$ , which gives  $\delta^2 a + \delta + a = 0$ .
3.  $tr_1^n(\delta x) = 0$  and  $tr_1^n(x) = 1$ , which implies  $\delta^2 a + 1 + a = 0$ .
4.  $tr_1^n(\delta x) = 0$  and  $tr_1^n(x) = 0$ , which gives  $\delta^2 a + a = 0$ .

The fourth equation is true only if  $a = 0$ , otherwise  $(\delta^2 + 1)a = 0 \Rightarrow \delta = 1$  but  $\delta \neq 0$  or  $1$ . Also if  $a = tr_e^n(x) = 0$ , we get  $tr_1^n(x) = tr_1^e(a) = tr_1^e(0) = 0$  and  $tr_1^n(\delta x) = tr_1^e(\delta a) = tr_1^e(0) = 0$ . So all the  $x \in F_{2^n}$  for which  $tr_e^n(x) = 0$  are solutions to the equation (3) and that actually gives us  $2^{n-e}$  solutions so far. Before we start discussing the other two equations we need the following simple but interesting observation.

$$\begin{aligned} tr_1^e\left(\frac{\delta}{1+\delta^2}\right) &= tr_1^e\left(\frac{\delta+1}{\delta^2+1} + \frac{1}{\delta^2+1}\right) \\ &= tr_1^e\left(\frac{\delta+1}{\delta^2+1}\right) + tr_1^e\left(\frac{1}{\delta^2+1}\right) \\ &= tr_1^e\left(\frac{\delta+1}{(\delta+1)^2}\right) + tr_1^e\left(\left(\frac{1}{\delta+1}\right)^2\right) \\ &= tr_1^e\left(\frac{1}{\delta+1}\right) + tr_1^e\left(\frac{1}{\delta+1}\right) \\ &= 0. \end{aligned}$$

First, we consider  $e$  is odd. Then  $tr_1^e(1) = 1$ .

(1) gives  $a = \frac{1}{1+\delta}$  which implies

$$\begin{aligned} tr_1^n(\delta x) &= tr_1^e(a\delta) \\ &= tr_1^e\left(\frac{\delta}{1+\delta}\right) \\ &= tr_1^e\left(1 + \frac{1}{\delta+1}\right) \\ &= tr_1^e(1) + tr_1^e\left(\frac{1}{\delta+1}\right) \\ &= 1 + tr_1^e\left(\frac{1}{\delta+1}\right) \end{aligned}$$

and  $tr_1^n(x) = tr_1^e(a) = tr_1^e\left(\frac{1}{\delta+1}\right)$ .

(2) gives  $a = \frac{\delta}{1+\delta^2}$  which implies

$$\begin{aligned} tr_1^n(\delta x) &= tr_1^e\left(\frac{\delta^2}{1+\delta^2}\right) \\ &= tr_1^e\left(\frac{\delta}{1+\delta}\right) \\ &= 1 + tr_1^e\left(\frac{1}{\delta+1}\right) \end{aligned}$$

and  $tr_1^n(x) = tr_1^e\left(\frac{\delta}{1+\delta^2}\right) = 0$ .

(3) gives  $a = \frac{1}{1+\delta^2}$  which implies

$$tr_1^n(\delta x) = tr_1^e\left(\frac{\delta}{1+\delta^2}\right) = 0, tr_1^n(x) = tr_1^e\left(\frac{1}{1+\delta}\right).$$

Now if  $tr_1^e\left(\frac{1}{1+\delta}\right) = 0$ , then (2) works. If  $tr_1^e\left(\frac{1}{1+\delta}\right) = 1$ , then (3) works. So in any case we have all together  $2 \cdot 2^{n-e} = 2^{n-e+1}$  solutions.

Now we consider the case when  $e$  is even. Then  $tr_1^e(1) = 0$  and  $tr_1^e\left(\frac{\delta}{1+\delta}\right) = tr_1^e\left(\frac{1}{1+\delta}\right)$ .

(1) gives  $a = \frac{1}{1+\delta}$  which implies

$$\begin{aligned} tr_1^n(\delta x) &= tr_1^e\left(\frac{\delta}{1+\delta}\right) \\ &= tr_1^e\left(\frac{1}{\delta+1}\right) \\ &= tr_1^n(x). \end{aligned}$$

(2) gives  $a = \frac{\delta}{1+\delta^2}$  which implies

$$\begin{aligned} tr_1^n(\delta x) &= tr_1^e\left(\frac{\delta^2}{1+\delta^2}\right) \\ &= tr_1^e\left(\frac{\delta}{1+\delta}\right) \\ &= tr_1^e\left(\frac{1}{\delta+1}\right) \end{aligned}$$

and  $tr_1^n(x) = tr_1^e\left(\frac{\delta}{1+\delta^2}\right) = 0$ .

(3) gives  $a = \frac{1}{1+\delta^2}$  which implies just like before

$$tr_1^n(\delta x) = 0 \text{ and } tr_1^n(x) = tr_1^e\left(\frac{1}{1+\delta}\right).$$

Now if  $tr_1^e\left(\frac{1}{1+\delta}\right) = 0$ , then (1),(2) and (3) do not work, only (4) works and that gives us  $2^{n-e}$  solutions. If  $tr_1^e\left(\frac{1}{1+\delta}\right) = 1$ , then each of (1),(2),(3) and (4) works and in that case we have  $4 \cdot 2^{n-e} = 2^{n-e+2}$  many solutions. So actually, in half of the cases we have  $2^{n-e}$  many solutions and the other half gives us  $2^{n-e+2}$  many solutions.

As  $\delta$  varies over  $F_{2^e} \setminus \{0, 1\}$  and  $0 \leq i, j \leq 2^n - 1$ , the distribution of correlation function is

$$\begin{cases} -1 + 2^{n-\frac{e-1}{2}}, & (2^{e-2} + 2^{\frac{e-3}{2}})2^n(2^e - 2) \text{ times} \\ -1, & (2^n - 2^{e-1})2^n(2^e - 2) \text{ times} \\ -1 - 2^{n-\frac{e-1}{2}}, & (2^{e-2} - 2^{\frac{e-3}{2}})2^n(2^e - 2) \text{ times} \end{cases}$$

and when  $e$  is even

$$\begin{cases} -1 + 2^{n-\frac{e}{2}}, & (2^{e-1} + 2^{\frac{e-2}{2}})2^n(2^{e-1} - 1) \text{ times} \\ -1 + 2^{n-\frac{e-2}{2}}, & (2^{e-3} + 2^{\frac{e-4}{2}})2^n(2^{e-1} - 1) \text{ times} \\ -1, & (2^n - 2^e)2^n(2^{e-1} - 1) \\ & + (2^n - 2^{e-2})2^n(2^{e-1} - 1) \text{ times} \\ -1 - 2^{n-\frac{e}{2}}, & (2^{e-1} - 2^{\frac{e-2}{2}})2^n(2^{e-1} - 1) \text{ times} \\ -1 - 2^{n-\frac{e-2}{2}}, & (2^{e-3} - 2^{\frac{e-4}{2}})2^n(2^{e-1} - 1) \text{ times} \end{cases}$$

**SubCase 2:**  $\delta \notin F_{2^e}$ . This case is little complicated. Say  $n = se$  and pick  $\delta \in F_{2^n}$ . Consider the map  $\phi : F_{2^n} \rightarrow F_{2^e} \times F_{2^e}$  by  $\phi(x) = (tr_e^n(x), tr_e^n(\delta x))$ .

We claim: If  $\delta \notin F_{2^e}$ , then  $\phi$  is onto.

**proof:** Set  $q = 2^e$ . Write  $\delta = \epsilon^q$ . Set  $\delta' = \epsilon^q + \epsilon$ .  $\delta \notin F_q \Rightarrow \delta' \neq 0$ , since  $\delta' = 0 \Rightarrow \epsilon^q = \epsilon \Rightarrow \epsilon \in F_q \Rightarrow \delta \in F_q$ . Pick any  $z \in F_q$ .  $tr_e^n$  is onto, so  $\exists \gamma \in F_{q^s}$  with  $tr_e^n(\gamma) = z$ .

Set  $\beta = (\delta')^{-1}\gamma$  (possible as  $\delta' \neq 0$ ). Let  $x = \beta^q + \beta$ . Then  $tr_e^n(x) = 0$  and

$$\begin{aligned} tr_e^n(\delta x) &= tr_e^n(\epsilon^q \beta^q + \epsilon^q \beta) \\ &= tr_e^n(\epsilon^q \beta^q + \epsilon \beta + \delta' \beta) \\ &= tr_e^n(\delta' \beta) \\ &= tr_e^n(\gamma) = z. \end{aligned}$$

So  $(0, z) \in \text{Im}(\phi)$  and since  $z$  is arbitrary  $0 \times F_q \subset \text{Im}(\phi)$ . Similarly,  $F_q \times 0 \subset \text{Im}(\phi)$ . As  $\phi$  is additive,  $\phi$  is onto.

Hence the number of solutions to  $(tr_e^n(x), tr_e^n(\delta x)) = (\epsilon_1, \epsilon_2)$ , where  $\epsilon_i \in F_{2^e}$  is  $2^{n-2e}$ . Now when  $\delta \notin F_{2^e}$  from equation(2) we get  $b = tr_1^e(b)$  and  $a = tr_1^e(a)$ .

Suppose,  $e$  is odd. Then  $(b, a) = (1, 0), (0, 1), (1, 1)$  and  $(0, 0)$  give us solutions to equation( 2). So we have all together  $4 \cdot 2^{n-2e} = 2^{n-2e+2}$  solutions. If  $e$  is even, none of  $(b, a) = (1, 0), (0, 1), (1, 1)$  is a solution to equation(2). Consider  $b = 1, a = 0$ . Then  $tr_1^e(b) = 0 \neq b$ . Similarly, we can show that the other two do not work either. So only  $(b, a) = (0, 0)$  gives us solution to equation (2) and we have  $2^{n-2e}$  solutions. As  $\delta$  varies over  $F_{2^n} \setminus F_{2^e}$ , the distribution of correlation function is

$$\begin{cases} -1 + 2^{n-e+1}, & (2^{2e-3} + 2^{e-2})2^n(2^n - 2^e) \text{ times} \\ -1, & (2^n - 2^{2e-2})2^n(2^n - 2^e) \text{ times} \\ -1 - 2^{n-e+1}, & (2^{2e-3} - 2^{e-2})2^n(2^n - 2^e) \text{ times} \end{cases}$$

$$\begin{cases} -1 + 2^{n-e}, & (2^{2e-1} + 2^{e-1})2^n(2^n - 2^e) \text{ times} \\ -1, & (2^n - 2^{2e})2^n(2^n - 2^e) \text{ times} \\ -1 - 2^{n-e}, & (2^{2e-1} - 2^{e-1})2^n(2^n - 2^e) \text{ times} \end{cases}$$

Combining the results of the above five cases, the distribution of the correlation values for the sequence family  $U$  can be obtained.

- 
- [1] Boztas, S., Kumar, P.V., *Binary sequences with Gold-like correlation but larger linear span*, IEEE Trans. Inform. Theory, **40** (1994),532-537.
- [2] Gold, R., *Maximal recursive sequences with 3-valued recursive cross-correlation functions* , IEEE Trans. Inform. Theory, **14** (1968), 154-156.
- [3] Hellesteth, T. and Kumar, P.V., "*Sequences with low correlation*,"in *Handbook of Coding Theory* , V.S. Pless and W.C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier (1998).
- [4] Kim, S.H., and No, J.S., *New families of Binary Sequences with low correlation* , IEEE Trans. Inform. Theory, **49**,No.11 (2003), 3059-3065.
- [5] Lidl, R. and Niederreiter ,W., *Finite Fields, Encyclopedia of Mathematics and its Application*,Vol 20, Cambridge University Press , Cambridge , 1997.
- [6] Tang, X., Hellesteth,T., Hu,L., Jiang,W., *A new family of Gold-like sequences*, S.W.Golomb et al.(Eds.):SSC 2007.LNCS 4893,(2007), 62-69.
- [7] Udaya, P., "*Polyphase and frequency hopping sequences obtained from finite rings*", Ph.D. dissertation, Dept. Elec. Eng.,Indian Inst. Technol., Kanpur, 1992.