Almost Difference Sets and Their Sequences With Optimal Autocorrelation

K. T. Arasu, Cunsheng Ding, *Member, IEEE*, Tor Helleseth, *Fellow, IEEE*, P. Vijay Kumar, *Senior Member, IEEE*, and Halvard M. Martinsen

***Abstract*—Almost difference sets have interesting applications in cryptography and coding theory. In this paper, we give a well-rounded treatment of known families of almost difference sets, establish relations between some difference sets and some almost difference sets, and determine the numerical multiplier group of some families of almost difference sets. We also construct six new classes of almost difference sets, and four classes of binary sequences of period $n \equiv 0 \pmod 4$ with optimal autocorrelation. We have also obtained two classes of relative difference sets and four classes of divisible difference sets (DDSs). We also point out that a result due to Jungnickel can be used to construct almost difference sets and sequences of period $4l$ with optimal autocorrelation.**

***Index Terms*—Almost difference sets, correlation, cyclotomy, difference sets, divisible difference sets (DDSs), relative difference sets, sequence.**

I. Introduction

Let $(A, +)$ be an Abelian group of order n. Let C be a k-subset of A. The set C is an (n, k, λ, t) almost difference set of A if $d_C(w)$ takes on the value λ altogether t times and the value $\lambda + 1$ altogether $n - 1 - t$ times when w ranges over all the nonzero elements of A, where $d_C(w)$ is the *difference function* defined by

$$d_C(w) = |(C + w) \cap C|$$

and

$$C + w = \{x + w | x \in C\}.$$

Let $(G, +)$ be a group of order mn and $(N, +)$ a subgroup of G of order n. If D is a k-subset of G, then D is called an $(m, n, k, \lambda_1, \lambda_2)$ divisible difference set (DDS) provided that the list of differences $\{d_1 - d_2 : d_1, d_2 \in D, d_1 \neq d_2\}$ contain every nonidentity element of N exactly λ_1 times and every element of $G \setminus N$ exactly λ_2 times. If $\lambda_1 = 0$, D is called a *relative difference set*, and N is called the *forbidden subgroup*.

Davis [3] called a DDS D an almost difference set if λ_1 and λ_2 differ by 1. Hence, the almost difference sets defined by Davis are a special class of the (n, k, λ, t) almost difference sets above. Davis defined this special class of almost difference sets due to its relationship to symmetric difference sets [3].

Another kind of almost difference sets were defined by Ding [6]–[8] (see also [2, p. 140]) for the study of cryptographic functions with optimal nonlinearity. Ding, Helleseth, and Lam have considered this special class of almost difference sets for constructing binary sequences with three-level autocorrelation [9]. In fact, the special class of almost difference sets defined by Ding are actually $(n, k, \lambda, \frac{n-1}{2})$ almost difference sets, which are only defined for odd n.

Ding, Helleseth, and Martinsen [10] have generalized the two kinds of almost difference sets by defining the (n, k, λ, t) almost difference sets, for the purpose of obtaining binary sequences with optimal autocorrelation. This broader class of almost difference sets was studied independently by Mertens and Bessenrodt for the Bernasconi model in physics [21]. It is nice that the current (n, k, λ, t) almost difference sets unify the two different kinds of almost difference sets introduced by Davis and Ding, respectively. Clearly, the special class of almost difference sets introduced by Davis are a subclass of DDSs, while there are (n, k, λ, t) almost difference sets that are not DDSs.

Almost difference sets are closely related to cryptography [2], coding theory, and sequences [9], [10]. They can be used to construct cryptographic functions with optimal nonlinearity, sequences with optimal autocorrelation, and good constant-weight codes. So far only a small number of classes of (n, k, λ, t) almost difference sets have been discovered.

In this paper, we give a well-rounded treatment of known families of (n, k, λ, t) almost difference sets, establish relations between some difference sets and some almost difference sets, and determine the numerical multiplier group of some families of almost difference sets. We also construct six new classes of almost difference sets, and four classes of binary sequences of period $n \equiv 0 \pmod 4$ with optimal autocorrelation. We have also obtained two classes of relative difference sets and four classes of DDSs. We also point out that a result due to Jungnickel can be used to construct almost difference sets and sequences of period $4l$ with optimal autocorrelation.

Manuscript received July 6, 2000; revised May 30, 2001. The work of K. T. Arasu was supported in part by the National Science Foundation under Grant CCR-9814106 and by NSA under Grant 904-01-1-0041.

K. T. Arasu is with the Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435 USA (e-mail: karasu@math.wright.edu).

C. Ding is with the Department of Computer Science, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (e-mail: cding@cs.ust.hk).

T. Helleseth and H. M. Martinsen are with the Department of Informatics, University of Bergen, HIB, N-5020 Bergen, Norway (e-mail: torh@ii.uib.no; halvard@ii.uib.no).

P. V. Kumar is with Communication Science Institute, Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089-2565 USA (e-mail: vijay@ceng.usc.edu).

Communicated by A.M. Klapper, Associate Editor for Sequences.

Publisher Item Identifier S 0018-9448(01)08584-4.

II. Known Families and Their Multiplier Groups

We first present two basic properties of almost difference sets. For (n, k, λ, t) almost difference sets of A we have the following basic relation:

$$k(k-1) = t\lambda + (n-1-t)(\lambda+1). \tag{1}$$

Similar to difference sets, we have the following basic result.

Theorem 1: D is an (n, k, λ, t) almost difference set of an Abelian group $(A, +)$ if and only if the complement $D^* = A \setminus D$ is an $(n, n-k, n-2k+\lambda, t)$ almost difference set.

Proof: It can be shown that $d_{D^*}(w) = n - 2k + d_D(w)$. The conclusion then follows. □

We now give a brief summary of known almost difference sets, and determine the numerical multiplier group of some of them. To this end, we need cyclotomy. Let $q = df+1$ be a power of a prime, and let θ be a fixed primitive element of GF (q). Define $D_i^{(d,q)} = \theta^i(\theta^d)$, where (θ^d) denotes the multiplicative group generated by θ^d. The cosets $D_l^{(d,q)}$ are called the *index classes* or *cyclotomic classes* of order d with respect to GF (q). Clearly

$$\text{GF}\,(q) \setminus \{0\} = \bigcup_{i=0}^{d-1} D_i^{(d,q)}.$$

Define

$$(l, m)_d = \left|\left(D_l^{(d,q)} + 1\right) \cap D_m^{(d,q)}\right|.$$

These constants $(l, m)_d$ are called *cyclotomic numbers* of order d with respect to GF (q).

Theorem 2: The known families of cyclotomic almost difference sets are the following:

1) $D_0^{(2,q)}$ with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{2})$, where $q \equiv 1 \pmod 4$. It is also called Paley partial difference set.
2) $D_0^{(4,q)}$ with parameters $(q, \frac{q-1}{4}, \frac{q-13}{16}, \frac{q-1}{2})$, where $q = 25 + 4y^2$ or $q = 9 + 4y^2$ (see Ding [8] and also [2]).
3) $D_0^{(4,q)} \cup \{0\}$ with parameters $(q, \frac{q+3}{4}, \frac{q-5}{16}, \frac{q-1}{2})$, where $q = 1 + 4y^2$ or $q = 49 + 4y^2$ (see Ding, Helleseth, and Lam [9]).
4) $D_0^{(8,q)}$ with parameters $(q, \frac{q-1}{8}, \frac{q-41}{64}, \frac{q-1}{2})$, where $q \equiv 41 \pmod{64}$ and $q = 19^2 + 4y^2 = 1 + 2b^2$ for some integer y and b or $q \equiv 41 \pmod{64}$ and $q = 13^2 + 4y^2 = 1 + 2b^2$ for some integer y and b (see Ding [8] and also [2]).
5) $D_i^{(4,q)} \cup D_{i+1}^{(4,q)}$ for all i with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{2})$, where $q = x^2 + 4$ and $x \equiv 1 \pmod 4$ (see Ding, Helleseth, and Lam [9]).

Similar to difference sets, we can define multipliers for almost difference sets. Let D be an almost difference set of an Abelian group A. An automorphism α of A is called a *multiplier* of D, if there is an $a \in A$ with $D^\alpha = a + D$. If α is a multiplier of the form $\alpha: x \mapsto mx$ for some integer $m \in \boldsymbol{Z}_e$, where e is the exponent of A, then α is called a *numerical multiplier*. In this case, we also call m a numerical multiplier.

Theorem 3: Let q be a prime. Consider the almost difference sets of Theorem 2.

a) The numerical multiplier group of the almost difference set $D_0^{(2,q)}$ is itself.
b) The numerical multiplier group of the almost difference set $D_0^{(4,q)}$ is itself.
c) The numerical multiplier group of the almost difference set $D_0^{(4,q)} \cup \{0\}$ is $D_0^{(4,q)}$.
d) The numerical multiplier group of the almost difference set $D_i^{(4,q)} \cup D_{i+1}^{(4,q)}$ is $D_0^{(4,q)}$ for each i if $q > 13$.
e) The numerical multiplier group of the almost difference set $D_0^{(8,q)}$ is itself.

Proof: We first prove a). Note that the set $D_0^{(2,q)}$ of quadratic residues is a multiplicative subgroup of GF $(q) \setminus \{0\}$. By definition, any element of $D_0^{(2,q)}$ is a numerical multiplier. We now prove that any element $a \in D_1^{(2,q)}$ cannot be a multiplier. Suppose that a is a numerical multiplier, then $aD_0^{(2,q)} = D_0^{(2,q)} + b$ for some $b \in$ GF (q). This is equivalent to $D_1^{(2,q)} = D_0^{(2,q)} + b$. Here b cannot be zero. Let b^{-1} be an element of $D_h^{(2,q)}$, where h is 0 or 1. Then $D_1^{(2,q)} = D_0^{(2,q)} + b$ is equivalent to $(h, h+1)_2 = (q-1)/2$. But this is impossible according to the cyclotomic numbers of order 2 given in [26]. This completes the proof of part a).

To prove part b), we need cyclotomic numbers of order 4. Let $q = 4f + 1 = x^2 + 4y^2$ with $x \equiv 1 \pmod 4$. Obviously, we have

$$\begin{aligned} |x| &\le \sqrt{q-4} < \sqrt{q} \\ |y| &\le \sqrt{q-1}/2 < \sqrt{q}/2. \end{aligned} \tag{2}$$

When f is even, there are five possible different cyclotomic numbers [26]; i.e.,

$$\begin{aligned} A &= \frac{q-11-6x}{16} \\ B &= \frac{q-3+2x+8y}{16} \\ C &= \frac{q-3+2x}{16} \\ D &= \frac{q-3+2x-8y}{16} \\ E &= \frac{q+1-2x}{16}. \end{aligned}$$

When f is odd, there are also five possible different cyclotomic numbers [26]; i.e.,

$$\begin{aligned} A &= \frac{q-7+2x}{16} \\ B &= \frac{q+1+2x-8y}{16} \\ C &= \frac{q+1-6x}{16} \\ D &= \frac{q+1+2x+8y}{16} \\ E &= \frac{q-3-2x}{16}. \end{aligned}$$

Note that $D_0^{(4,q)}$ is a subgroup of GF$(q)\backslash\{0\}$. Every element of $D_0^{(4,q)}$ is a numerical multiplier of this almost difference set. We now prove that any element $a \in D_i$ cannot be a numerical multiplier for each i with $1 \le i \le 3$. If a is a multiplier, then there should be an element $b \in$ GF$(q) \setminus \{0\}$ such that

$$aD_0^{(4,q)} = D_i^{(4,q)} = D_0^{(4,q)} + b. \tag{3}$$

Let $b^{-1} \in D_j^{(4,q)}$. Then (3) is true if and only if

$$(j, i+j)_4 = (q-1)/4. \tag{4}$$

Recall that the condition for $D_0^{(4,q)}$ to be an almost difference set is that $q = 25+4y^2$ or $q = 9+4y^2$. Hence $q \ge 13$. With the help of (2), we can prove that each cyclotomic number $(h, k)_4$ of order 4

$$(h, k)_4 < \frac{q+1+2|x|+8|y|}{16} < \frac{q-1}{4}.$$

This shows that (4) cannot be true. Hence the elements of $D_0^{(4,q)}$ are the only numerical multipliers. This completes the proof of part b).

Part c) can be similarly proved as part b). We now prove part d). It is easy to see that $D_i^{(4,q)} \cup D_{i+1}^{(4,q)}$ has the same numerical multiplier group for each i. So we need only to consider the case $i = 0$. Clearly, every element of $D_0^{(4,q)}$ is a numerical multiplier. Let $a \in D_h^{(4,q)}$, where $1 \le h \le 3$. We now prove that a cannot be a numerical multiplier. On the contrary, suppose that a is a numerical multiplier. Then there would exist a b such that

$$D_h^{(4,q)} \cup D_{h+1}^{(4,q)} = D_0^{(4,q)} \cup D_1^{(4,q)} + b. \tag{5}$$

Since $1 \le h \le 3$, b cannot be the zero element of GF(q). So we assume that $b^{-1} \in D_k^{(4,q)}$. It then follows from (5) that

$$D_{h+k}^{(4,q)} \cup D_{h+k+1}^{(4,q)} = D_k^{(4,q)} \cup D_{k+1}^{(4,q)} + 1.$$

Hence

$$\begin{aligned}
\frac{q-1}{2} &= \left|\left[D_k^{(4,q)} \cup D_{k+1}^{(4,q)} + 1\right] \cap \left[D_{h+k}^{(4,q)} \cup D_{h+k+1}^{(4,q)}\right]\right| \\
&= \left|\left(D_k^{(4,q)} + 1\right) \cap D_{h+k}^{(4,q)}\right| \\
&\quad + \left|\left(D_k^{(4,q)} + 1\right) \cap D_{h+k+1}^{(4,q)}\right| \\
&\quad + \left|\left(D_{k+1}^{(4,q)} + 1\right) \cap D_{h+k}^{(4,q)}\right| \\
&\quad + \left|\left(D_{k+1}^{(4,q)} + 1\right) \cap D_{h+k+1}^{(4,q)}\right| \\
&= (k, h+k) + (k, h+k+1) + (k+1, h+k) \\
&\quad + (k+1, h+k+1).
\end{aligned}$$

Define

$$\begin{aligned}
u(h, k) = (k, h+k) + (k, h+k+1) \\
+ (k+1, h+k) + (k+1, h+k+1).
\end{aligned}$$

By making using of cyclotomic numbers of order 4 [26], it can be shown that when h ranges over $\{1, 2, 3\}$ and k ranges over $\{0, 1, 2, 3\}$, $u(h, k)$ takes on only each of the following:

$$\frac{q-x}{4}, \frac{q-2+x}{4}, \frac{q-4-x}{4}, \frac{q+1+2y}{4}, \frac{q+1-2y}{4}, \frac{q-3-2y}{4}, \frac{q-3+2y}{4} \tag{6}$$

TABLE I
THE CYCLOTOMIC NUMBERS OF ORDER 8 IN SUBCASE I

	If 2 is a quartic residue
64(0,0)	$q-23-18x-24a$
64(0,1)	$q-7+2x+4a+16y+16b$
64(0,2)	$q-7+6x+16y$
64(0,3)	$q-7+2x+4a-16y+16b$
64(0,4)	$q-7-2x+8a$
64(0,5)	$q-7+2x+4a+16y-16b$
64(0,6)	$q-7+6x-16y$
64(0,7)	$q-7+2x+4a-16y-16b$
64(1,2)	$q+1+2x-4a$
64(1,3)	$q+1-6x+4a$
64(1,4)	$q+1+2x-4a$
64(1,5)	$q+1+2x-4a$
64(1,6)	$q+1-6x+4a$
64(2,4)	$q+1-2x$
64(2,5)	$q+1+2x-4a$
	If 2 is not a quartic residue
64(0,0)	$q-23+6x$
64(0,1)	$q-7+2x+4a$
64(0,2)	$q-7-2x-8a-16y$
64(0,3)	$q-7+2x+4a$
64(0,4)	$q-7-10x$
64(0,5)	$q-7+2x+4a$
64(0,6)	$q-7-2x-8a+16y$
64(0,7)	$q-7+2x+4a$
64(1,2)	$q+1-6x+4a$
64(1,3)	$q+1+2x-4a-16b$
64(1,4)	$q+1+2x-4a+16y$
64(1,5)	$q+1+2x-4a-16y$
64(1,6)	$q+1+2x-4a+16b$
64(2,4)	$q+1+6x+8a$
64(2,5)	$q+1-6x+4a$

if $q \equiv 5 \pmod 8$, and takes on only each of the following:

$$\frac{q-x}{4}, \frac{q-2+x}{4}, \frac{q-4-x}{4}, \frac{q-1+2y}{4}, \frac{q-1-2y}{4} \tag{7}$$

if $q \equiv 1 \pmod 8$. Note that $q = x^2+4$ and $y = \pm 1$ as these are the conditions for $D_0^{(4,q)} \cup D_1^{(4,q)}$ to be an almost difference set, where $x \equiv 1 \pmod 4$. Also as shown above, $u(h, k) = \frac{q-1}{2}$. Since $q > 13$, it can be checked that none of the values in (6) and (7) equals $\frac{q-1}{2}$. This is contrary to $u(h, k) = \frac{q-1}{2}$. This completes the proof of part d).

Finally, we prove part e). For this purpose, we need cyclotomic numbers of order 8. When $q \equiv 1 \pmod 8$ is prime, the 64 cyclotomic numbers have at most 15 different values. These values are expressible in terms of q, x, y, a, and b in

$$q = x^2 + 4y^2 = a^2 + 2b^2, \qquad (x \equiv a \equiv 1 \pmod 4).$$

There are two subcases: the cases $q \equiv 1 \pmod{16}$ and $q \equiv 9 \pmod{16}$. The possible values for the cyclotomic numbers of order 8 are given in Tables I and II [2, pp. 387–388].

Recall that the condition for $D_0^{(8,q)}$ to be an almost difference set is that $q = x^2 + 4y^2 = 1 + 2y^2$, where $(x, b) = (-19, 1)$

TABLE II
THE CYCLOTOMIC NUMBERS OF ORDER 8 IN SUBCASE II

	If 2 is a quartic residue
64(0,0)	$q-15-2x$
64(0,1)	$q+1+2x-4a-16y$
64(0,2)	$q+1+6x+8a-16y$
64(0,3)	$q+1+2x-4a-16y$
64(0,4)	$q+1-18x$
64(0,5)	$q+1+2x-4a+16y$
64(0,6)	$q+1+6x+8a+16y$
64(0,7)	$q+1+2x-4a-16y$
64(1,0)	$q-7+2x+4a$
64(1,1)	$q-7+2x+4a$
64(1,2)	$q+1-6x+4a+16b$
64(1,3)	$q+1+2x-4a$
64(1,7)	$q+1-6x+4a-16b$
64(2,0)	$q-7-2x-8a$
64(2,1)	$q+1+2x-4a$
	If 2 is not a quartic residue
64(0,0)	$q-15-10x-8a$
64(0,1)	$q+1+2x-4a-16b$
64(0,2)	$q+1-2x+16y$
64(0,3)	$q+1+2x-4a-16b$
64(0,4)	$q+1+6x+24a$
64(0,5)	$q+1+2x-4a+16b$
64(0,6)	$q+1-2x-16y$
64(0,7)	$q+1+2x-4a+16b$
64(1,0)	$q-7+2x+4a+16y$
64(1,1)	$q-7+2x+4a-16y$
64(1,2)	$q+1+2x-4a$
64(1,3)	$q+1-6x+4a$
64(1,7)	$q+1+2x-4a$
64(2,0)	$q-7+6x$
64(2,1)	$q+1-6x+4a$

or $(x, b) = (13, 1)$. This means that $q > 269$. It follows from Tables I and II that

$$(i, j)_8 < \frac{q+1+18|x|+16|y|+24|a|+16|b|}{64} = \begin{cases} \frac{q+367+8\sqrt{q-19^2}+8\sqrt{2q-2}}{64}, & (x, a) = (-19, 1) \\ \frac{q+259+8\sqrt{q-13^2}+8\sqrt{2q-2}}{64}, & (x, a) = (13, 1) \end{cases} < \frac{q-1}{8}.$$

Suppose that $a \in D_h^{(8,q)}$ is a numerical multiplier, where $1 \le h \le 7$. Then there is a b such that

$$aD_0^{(8,q)} = D_h^{(8,q)} = D_0^{(8,q)} + b.$$

Since $h \neq 0$, $b \neq 0$. We assume that $b^{-1} \in D_k^{(8,q)}$. Then we obtain that $D_{h+k}^{(8,q)} = D_k^{(8,q)} + 1$. Hence

$$(k, h+k)_8 = \left|\left(D_k^{(8,q)} + 1\right) \cap D_{h+k}^{(8,q)}\right| = \frac{q-1}{8}.$$

This is contrary to the inequality above. Hence a cannot be a numerical multiplier. □

Note that all the almost difference sets above are of an Abelian group A with odd order. There are several classes of almost difference sets of Abelian groups with even order.

Let q be a power of an odd prime, and let α be a primitive element of GF(q) that is used to define the cyclotomic classes $D_i^{(2,q)}$ of order 2. Define a function from $(\boldsymbol{Z}_{q-1}, +)$ to (GF(2), $+$) as

$$f(i) = \begin{cases} 1, & \text{if } \alpha^i \in \left(D_1^{(2,q)} - 1\right) \\ 0, & \text{otherwise.} \end{cases}$$

Let $C_f = \{x \in \boldsymbol{Z}_{q-1} | f(x) = 1\}$ denote the support of f.

Theorem 4: The set C_f is a $(q-1, \frac{q-1}{2}, \frac{q-3}{4}, \frac{3q-5}{4})$ almost difference set if $q \equiv 3 \pmod 4$, and a $(q-1, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ almost difference set if $q \equiv 1 \pmod 4$.

Some binary sequences with optimal autocorrelation give almost difference sets, and *vice versa* [9], [10]. The almost difference sets of Theorem 4 come from two classes of binary sequences with optimal autocorrelation constructed by Lempel, Cohn, and Eastman [19].[1] It is straightforward to prove Theorem 4 by making use of cyclotomic numbers of order 2.

By definition, $C_f = \log_\alpha(D_1^{(2,q)} - 1)$. So a is a numerical multiplier of C_f if and only if there is a $b \in \boldsymbol{Z}_{q-1}$ such that

$$\left(D_1^{(2,q)} - 1\right)^a = \alpha^b \left(D_1^{(2,q)} - 1\right).$$

The determination of the numerical multiplier group of the almost difference set C_f above is still open.

In addition to the almost difference sets derived directly from cyclotomy, there are several other classes of almost difference sets that are related to cyclotomy. Consider the finite field GF(q), where $q \equiv 5 \pmod 8$. It is known that q has a quadratic partition $q = s^2 + 4t^2$, with $s \equiv \pm 1 \pmod 4$ [26]. Let $D_i^{(4,q)}$ be the cyclotomic classes of order 4.

Theorem 5: Let $i, j, l \in \{0, 1, 2, 3\}$ be three pairwise distinct integers, and define

$$C = \left[\{0\} \times \left(D_i^{(4,q)} \cup D_j^{(4,q)}\right)\right] \cup \left[\{1\} \times \left(D_l^{(4,q)} \cup D_j^{(4,q)}\right)\right].$$

Then C is an $(n, \frac{n-2}{2}, \frac{n-6}{4}, \frac{3n-6}{4})$ almost difference set of $A =$ GF$(2) \times$ GF(q) if

1) $t = 1$ and $(i, j, l) = (0, 1, 3)$ or $(0, 2, 1)$, or
2) $s = 1$ and $(i, j, l) = (1, 0, 3)$ or $(0, 1, 2)$.

Theorem 6: Let $i, j, l \in \{0, 1, 2, 3\}$ be three pairwise distinct integers and define

$$C = \left[\{0\} \times \left(D_i^{(4,q)} \cup D_j^{(4,q)}\right)\right] \cup \left[\{1\} \times \left(D_l^{(4,q)} \cup D_j^{(4,q)}\right)\right] \cup \{0, 0\}.$$

Then C is an $(n, \frac{n}{2}, \frac{n-2}{4}, \frac{3n-2}{4})$ almost difference set of $A =$ GF$(2) \times$ GF(q) if

1) $t = 1$ and
$(i, j, l) \in \{(0, 1, 3), (0, 2, 3), (1, 2, 0), (1, 3, 0)\}$
or
2) $s = 1$ and
$(i, j, l) \in \{(0, 1, 2), (0, 3, 2), (1, 0, 3), (1, 2, 3)\}$.

The classes of almost difference sets described in Theorems 5 and 6 are due to Ding, Helleseth, and Martinsen [10]. They were

[1]One of the referees pointed out that the sequences of [19] were already described in [24] by Sidelnikov. However, we have been unable to get a copy of [24].

used to construct binary sequences with optimal autocorrelation when q is prime [10].

Theorem 7: All the almost difference sets given in Theorem 5 have the numerical multiplier group $\phi^{-1}(\{1\}\times D_0^{(4,q)})$ when q is prime, where ϕ: $x \to (x \bmod 2, x \bmod q)$ is the isomorphism from $\boldsymbol{Z}_{2q}$ to $\boldsymbol{Z}_2 \times \boldsymbol{Z}_q$.

Proof: Clearly, each element of $\{1\}\times D_0^{(4,q)}$ is a numerical multiplier. On the other hand, if (a, b) is a numerical multiplier, then $a = 1$ and there is a c such that

$$b\left(D_i^{(4,q)} \cup D_j^{(4,q)}\right) = \left(D_i^{(4,q)} \cup D_j^{(4,q)}\right) + c$$
$$b\left(D_l^{(4,q)} \cup D_j^{(4,q)}\right) = \left(D_l^{(4,q)} \cup D_j^{(4,q)}\right) + c \qquad (8)$$

where $b \in D_h^{(4,q)}$ for some $1 \le h \le 3$. Similar to the proof of Theorem 3, we can prove that there are no b and c such that (8) holds. This completes the proof of this theorem. □

Theorem 8: All the almost difference sets given in Theorem 6 have the numerical multiplier group $\phi^{-1}(\{1\}\times D_0^{(4,q)})$ when q is prime, where ϕ: $x \to (x \bmod 2, x \bmod q)$ is the isomorphism from $\boldsymbol{Z}_{2q}$ to $\boldsymbol{Z}_2 \times \boldsymbol{Z}_q$.

Proof: This can be proved similarly as Theorem 7. □

There are two classes of binary sequences of period $p^m - 1$ with optimal autocorrelation constructed by No, Chung, Song, Yang, Lee, and Helleseth [22]. These sequences give two classes of cyclic almost difference sets.

Some DDSs are almost difference sets. Davis has given several classes of such almost difference sets. As it takes much space to describe them, we only summarize the parameters of these almost difference sets in the following theorem.

Theorem 9 (Davis [3]): There are almost difference sets with the following parameters:

1) $(4\cdot 3^{2a}, 2(3^{2a}-3^a), 3^{2a}-2\cdot 3^a, 3^{2a}-1)$ in $H \times \boldsymbol{Z}_{3^a}^2$, where H is a group of order 4;
2) $((q+1)q^2, q(q+1), q, q^2-1)$ in $H \times EA(q^2)$, where $EA(q^2)$ denotes the additive group $(\mathrm{GF}(q^2), +)$ and H is a group of order $q+1$.

There are also other almost difference sets that are also DDSs. We shall deal with them in later sections.

III. Difference Sets and Almost Difference Sets

Let D be a k-subset of an Abelian group $(A, +)$ of order n. If the difference function $d_D(w)$ equals λ for all nonzero elements w of A, then D is called an (n, k, λ) difference set. In this section, we establish some connections between some difference sets and almost difference sets. We shall show that it is possible to construct almost difference sets from difference sets and *vice versa*. Throughout this section, we assume that $n \equiv 1 \pmod 4$, and let A be an Abelian group of order n.

Lemma 1: Let D be an (n, k, λ) difference set of A and let $d \in D$. If $D\setminus\{d\}$ is an $(n, k-1, \lambda-1, \frac{n-1}{2})$ almost difference set of A, then

$$k = \frac{n+3}{4} \qquad \lambda = \frac{n+3}{16}.$$

Proof: This is similarly proved as Lemma 2. □

Theorem 10: Let D be an $(n, \frac{n+3}{4}, \frac{n+3}{16})$ difference set of A, and let d be an element of D. If $2d$ cannot be written as the sum of two distinct elements of D, then $D \setminus \{d\}$ is an $(n, \frac{n-1}{4}, \frac{n-13}{16}, \frac{n-1}{2})$ almost difference set of A.

Proof: Let $D = \{d, d_1, d_2, \ldots, d_{(n-1)/4}\}$. If $2d$ cannot be written as a sum of two distinct elements of D, then

$$d-d_1, d-d_2, \ldots, d-d_{(n-1)/4}$$
$$d_1-d, d_2-d, \ldots, d_{(n-1)/4}-d$$

are $(n-1)/2$ pairwise distinct elements. Since D is an $(n, \frac{n+3}{4}, \frac{n+3}{16})$ difference set, $D\setminus\{d\}$ is an $(n, \frac{n-1}{4}, \frac{n-13}{16}, \frac{n-1}{2})$ almost difference set of A. □

Theorem 10 shows how to construct an almost difference set from a difference set by removing one element.

Theorem 11: Let $D = \{d_1, d_2, \ldots, d_{(n-1)/4}\}$ be an $(n, \frac{n-1}{4}, \frac{n-13}{16}, \frac{n-1}{2})$ almost difference set of A. Let A_1 and A_2 be two subsets of A such that $A_1 \cup A_2 = A \setminus \{0\}$ and $x-y$ takes on each element of A_1 $\frac{n-13}{16}$ times and each element of A_2 $\frac{n+3}{16}$ times when (x, y) ranges over $D \times D$ with $x \ne y$. Let $d \in A \setminus D$. If

1) $2d$ is not a sum of any two distinct elements of D
2) $d - d_i \in A_1$ and $d_i - d \in A_1$ for all i

then $D \cup \{d\}$ is an $(n, \frac{n+3}{4}, \frac{n+3}{16})$ difference set of A.

Proof: If $2d$ cannot be written as the sum of two distinct elements of D, then

$$d-d_1, d-d_2, \ldots, d-d_{(n-1)/4}$$
$$d_1-d, d_2-d, \ldots, d_{(n-1)/4}-d$$

are $(n-1)/2$ pairwise distinct elements, and form A_1 by the second condition. Since D is an $(n, \frac{n-1}{4}, \frac{n-13}{16}, \frac{n-1}{2})$ almost difference set, by the definition of A_1 and A_2, $D \cup \{d\}$ is an $(n, \frac{n+3}{4}, \frac{n+3}{16})$ difference set of G. □

Theorem 11 shows how to construct a difference set from an almost difference set by adding one element.

Example 1: The set $\{5, 6, 9, 11\}$ is a $(13, 4, 1)$ difference set of $\boldsymbol{Z}_{13}$, while $\{5, 6, 9\}$ is a $(13, 3, 0, 6)$ almost difference set of $\boldsymbol{Z}_{13}$. This example shows the two constructions described in Theorems 10 and 11.

Lemma 2: Let D be an (n, k, λ) difference set of A and let $d \in A\setminus D$. If $D\cup\{d\}$ is an $(n, k+1, \lambda, \frac{n-1}{2})$ almost different set, then

$$k = \frac{n-1}{4} \qquad \lambda = \frac{n-5}{16}.$$

Proof: By the necessary conditions of difference sets and almost difference sets, we have, respectively

$$\begin{cases} k(k-1) = \lambda(n-1) \\ (k+1)k = (2\lambda+1)(n-1)/2. \end{cases}$$

The conclusion above is proved by solving this set of equations. □

Theorem 12: Let D be an $(n, \frac{n-1}{4}, \frac{n-5}{16})$ difference set of A, and let $d \in A \setminus D$. If $2d$ cannot be written as the sum of two distinct elements of D, then $D\cup\{d\}$ is an $(n, \frac{n+3}{4}, \frac{n-5}{16}, \frac{n-1}{2})$ almost difference set of A.

Proof: This can be proved similarly as Theorem 10. □

Theorem 12 shows how to construct an almost difference set from a difference set by adding one element.

Theorem 13: Let $D = \{d, d_1, \ldots, d_{(n-1)/4}\}$ be an $(n, \frac{n+3}{4}, \frac{n-5}{16}, \frac{n-1}{2})$ almost difference set of A. Let A_1 and A_2 be two subsets of A such that $A_1 \cup A_2 = A \setminus \{0\}$ and $x-y$ takes on each element of A_1 $\frac{n-5}{16}$ times and each element of A_2 $\frac{n+11}{16}$ times when (x, y) ranges over $D \times D$ with $x \neq y$. If

1) $2d$ is not the sum of any two distinct elements of D,
2) $d - d_i \in A_1$ and $d_i - d \in A_1$ for all i,

then $D \setminus \{d\}$ is an $(n, \frac{n-1}{4}, \frac{n-5}{16})$ difference set of A.

Proof: This can be proved similarly as Theorem 11. □

Theorem 13 shows how to construct a difference set from an almost difference set by removing one element.

Example 2: The set $\{0, 1, 3, 13, 16, 17\}$ is a $(21, 6, 1, 10)$ almost difference set of $\boldsymbol{Z}_{21}$. By removing 0 we obtain $\{1, 3, 13, 16, 17\}$ that is a $(21, 5, 1)$ difference set of $\boldsymbol{Z}_{21}$. This example illustrates the constructions of Theorems 12 and 13.

IV. Two New Families of Almost Difference Sets

Let $(A, +)$ and $(B, +)$ be Abelian groups of order n and m, respectively, and let f be a function from A to B. One measure of nonlinearity of f is defined by

$$P_f = \max_{0 \neq a \in A} \max_{b \in B} \Pr(f(x+a) - f(x) = b) \tag{9}$$

where $\Pr(E)$ denotes the probability of the occurrence of even E. Functions with high nonlinearity have important applications in cryptography and coding theory [2].

Lemma 3: Let f be a function from $(A, +)$ to $(B, +)$. Then

$$P_f = \max_{0 \neq a \in A} \max_{b \in B} \left(\frac{\sum_{y \in B} |C_y \cap (C_{y+b} - a)|}{|A|} \right).$$

Proof: Note that

$$\begin{aligned}
&|\{x \in A | f(x+a) - f(x) = b\}| \\
&\quad = \left| \bigcup_{y \in B} \{x \in A | f(x) = y \text{ and } f(x+a) = y + b\} \right| \\
&\quad = \left| \bigcup_{y \in B} \left(C_y \bigcap (C_{y+b} - a) \right) \right| \\
&\quad = \sum_{y \in B} |C_y \cap (C_{y+b} - a)|.
\end{aligned}$$

The conclusion then follows. □

It is easy to see that

$$\sum_{b \in B} \sum_{y \in B} |C_y \cap (C_{y+b} - a)| = |A|.$$

It then follows from Lemma 3 and the equation above that

$$P_f \geq \frac{1}{|B|}. \tag{10}$$

This is the lower bound for the nonlinearity of a function from A to B. The smaller the value of P_f, the higher the nonlinearity of f. For applications in coding theory and cryptography we wish to find functions with the smallest possible P_f. We say that f has perfect nonlinearity if $P_f = \frac{1}{m}$.

Lemma 4 [1], [15]: The power function x^s from GF (p^m) to GF (p^m), where p is odd, has perfect nonlinearity $P_f = \frac{1}{p^m}$ for the following s:

- $s = 2$.
- $s = p^k + 1$, where $m/\gcd(m, k)$ is odd.
- $s = (3^k+1)/2$, where $p = 3$, k is odd, and $\gcd(m, k) = 1$.

We now use functions with perfect nonlinearity to construct almost difference sets.

Theorem 14: Let f be a function from an Abelian group $(A, +)$ of order n to another Abelian group $(B, +)$ of order n with perfect nonlinearity $P_f = \frac{1}{n}$. Define

$$C_b = \{x \in A | f(x) = b\}$$

and

$$C = \bigcup_{b \in B} \{b\} \times C_b \subseteq B \times A.$$

Then C is an $(n^2, n, 0, n-1)$ almost difference set of $B \times A$.

Proof: Recall the difference function $d_C(x)$. Since f has perfect nonlinearity $P_f = \frac{1}{n}$, it follows from Lemma 3 that

$$\begin{aligned}
&d_C(w_1, w_2) \\
&\quad = |(C + (w_1, w_2)) \cap C| \\
&\quad = \left| \left[\bigcup_{b_1 \in B} \{b_1 + w_1\} \times (C_{b_1} + w_2) \right] \bigcap \left[\bigcup_{b_2 \in B} \{b_2\} \times C_{b_2} \right] \right| \\
&\quad = \sum_{b_1 \in B} \sum_{b_2 \in B} |\{b_1 + w_1\} \cap \{b_2\}| \cdot \left| (C_{b_1} + w_2) \bigcap C_{b_2} \right| \\
&\quad = \sum_{b_1 \in B} \left| (C_{b_1} + w_2) \bigcap C_{b_1 + w_1} \right| \\
&\quad = \sum_{y \in B} \left| C_y \bigcap (C_{y + w_1} - w_2) \right| \\
&\quad = \begin{cases} n, & \text{if } (w_1, w_2) = (0, 0) \\ 0, & \text{if } w_1 \neq 0,\ w_2 = 0 \\ 1, & \text{otherwise} \end{cases}
\end{aligned}$$

where $w_1 \in B$ and $w_2 \in A$. Hence C is an $(n^2, n, 0, n-1)$ almost difference set of $B \times A$. □

Theorem 15: Let $f(x) = x^s$ be a function from GF (p^m) to GF (p^m), where p is odd. Define $C_b = \{x \in \text{GF}(p^m) | f(x) = b\}$ for each $b \in \text{GF}(p^m)$ and

$$C = \bigcup_{b \in \text{GF}(p^m)} \{b\} \times C_b \subseteq \text{GF}(p^m) \times \text{GF}(p^m).$$

If

- $s = 2$, or
- $s = p^k + 1$, where $m/\gcd(m, k)$ is odd, or
- $s = (3^k+1)/2$, where $p = 3$, k is odd, and $\gcd(m, k) = 1$.

Then C is a $(p^{2m}, p^m, 0, p^m - 1)$ almost difference set of GF$(p^m) \times$ GF(p^m).

Proof: This follows from Lemma 4 and Theorem 14. □

Theorem 15 gives three classes of almost difference sets of GF$(q)\times$GF(q), which are not cyclic. The first class given by the perfect nonlinear function x^2 is not new (see Pott [23, Theorem 2.2.9]. The remaining two classes of almost difference sets given by the other two perfect nonlinear functions are new.

The three classes of almost difference sets are also relative difference sets with parameters $(p^m, p^m, p^m, 0, 1)$, with forbidden set $\{0\} \times$ GF(p^m).

V. New Classes of Binary Sequences With Optimal Autocorrelation and Almost Difference Sets

Given a binary sequence $\{s(t)\}$ of period n, the autocorrelation of the sequence at shift w is defined by

$$\boldsymbol{C}_s(w) = \sum_{t=0}^{n-1} (-1)^{s(t+w)-s(t)}.$$

An important problem in sequence design is to find sequences with optimal autocorrelation, i.e., where

1) $\boldsymbol{C}_s(w) = -1$ for all $w \not\equiv 0 \pmod n$ if $n \equiv 3 \pmod 4$;
2) $\boldsymbol{C}_s(w) \in \{1, -3\}$ for all $w \not\equiv 0 \pmod n$ if $n \equiv 1 \pmod 4$;
3) $\boldsymbol{C}_s(w) \in \{2, -2\}$ for all $w \not\equiv 0 \pmod n$ if $n \equiv 2 \pmod 4$;
4) $\boldsymbol{C}_s(w) \in \{0, -4\}$ or $\boldsymbol{C}_s(w) \in \{0, 4\}$ for all $w \not\equiv 0 \pmod n$ if $n \equiv 0 \pmod 4$.

A sequence $\{s(t)\}$ of period n is said to have *ideal* autocorrelation if $\boldsymbol{C}_s(w) = -1$ for all $w \not\equiv 0 \pmod n$, where $n \equiv 3 \pmod 4$. For applications of sequences with good correlation, we refer to [2], [12], [14], and [25].

There are only two known constructions of binary sequences of period $n \equiv 0 \pmod 4$ with optimal autocorrelation values $0, -4$. The first construction was given by Lempel, Cohn, and Eastman [19]. The second one was given by No, Chung, Song, Yang, Lee, and Helleseth [22]. In this section, we shall present a construction that gives several classes of binary sequences of period $n \equiv 0 \pmod 4$ with optimal autocorrelation values $0, -4$. These binary sequences with optimal autocorrelation give several classes of cyclic almost difference sets with parameters $(4l, 2l-1, l-2, l-1)$ or $(4l, 2l-1, l-2, l-1)$. We also point out that a result due to Jungnickel gives similar binary sequences and almost difference sets.

The following result is well known and straightforward to prove.

Lemma 5 [2, p. 143]: Let $\{s(t)\}$ be a binary sequence of period n. Then

$$\boldsymbol{C}_s(w) = n - 4(k - d_C(w))$$

where $C = \{i \in \boldsymbol{Z}_n | s(i) = 1\}$ is the *support* or *characteristic set* of $\{s(t)\}$, $k = |C|$, and $d_C(x)$ is the difference function defined earlier.

The following theorem follows from Lemma 5.

Theorem 16: Let $\{s(t)\}$ be a binary sequence of period n, and let C be its support with k elements. Then C is an (n, k, λ, t) almost difference set of $\boldsymbol{Z}_n$ if and only if the autocorrelation function $\boldsymbol{C}_s(w)$ takes on $n - 4(k - \lambda)$ altogether t times and $n - 4(k - \lambda - 1)$ altogether $n - 1 - t$ times when w ranges over all nonzero elements of $\boldsymbol{Z}_n$.

Theorem 16 serves as a bridge between some binary sequences with three-level autocorrelation and cyclic almost difference sets. We shall make use of this bridge in the sequel.

Let $\{s(t)\}$ be a sequence of period l. Define the matrix $M = (m_{j,i})$, $0 \le j \le 3$, $0 \le i \le l-1$, as

$$M = \begin{pmatrix} s(0) & s(1) & \cdots & s(l-1) \\ \overline{s}(0+\delta) & \overline{s}(1+\delta) & \cdots & \overline{s}(l-1+\delta) \\ \overline{s}(0) & \overline{s}(1) & \cdots & \overline{s}(l-1) \\ \overline{s}(0+\delta) & \overline{s}(1+\delta) & \cdots & \overline{s}(l-1+\delta) \end{pmatrix} \tag{11}$$

where $\overline{s}(i) = 1 + s(i)$ is the complement of $s(i)$, and $0 \le \delta \le l-1$ is any fixed integer.

The following theorem describes our construction of binary sequences of period $4l$ with optimal autocorrelation.

Theorem 17: Let $\{s(t)\}$ be of period l with ideal autocorrelation and let M be defined as in (11). Let $\{u(t)\}$ be a sequence of period $4l$ defined by

$$u(t) = m_{j,i}$$

where

$$\begin{cases} t \equiv j \pmod 4 \\ t \equiv i \pmod l. \end{cases} \tag{12}$$

Then $\{u(t)\}$ has optimal autocorrelation, given by

$$\boldsymbol{C}_u(\tau) = \begin{cases} -4, & 3l \text{ times} \\ 0, & l-1 \text{ times} \\ 4l, & \text{once.} \end{cases}$$

Proof: The proof is divided into two parts by considering the values of $\boldsymbol{C}_s(\tau)$, when $\tau \equiv 0 \pmod 4$, and when $\tau \not\equiv 0 \pmod 4$. For $\tau \equiv 0 \pmod 4$, we have the following general situations of the comparison in the autocorrelation:

$$\begin{array}{lll} s(t) & \text{compare} & s(t+\tau) \\ \overline{s}(t+\delta) & \text{compare} & \overline{s}(t+\tau+\delta) \\ \overline{s}(t) & \text{compare} & \overline{s}(t+\tau) \\ \overline{s}(t+\delta) & \text{compare} & \overline{s}(t+\tau+\delta). \end{array}$$

For all t, $0 \le t \le l-1$, each row will have correlation values -1, such that

$$\boldsymbol{C}_s(\tau) = -4, \qquad \text{for all } \tau \equiv 0 \pmod 4.$$

For $\tau \not\equiv 0 \pmod 4$, we typically have for one shift

$$\begin{array}{lll} s(t) & \text{compare} & \overline{s}(t+\tau+\delta+1) \\ \overline{s}(t+\delta) & \text{compare} & s(t) \\ \overline{s}(t) & \text{compare} & \overline{s}(t+\delta) \\ \overline{s}(t+\delta) & \text{compare} & \overline{s}(t). \end{array}$$

It is easy to see that two of the comparisons, the two on the top, give value 1, and the other two give value -1, such that

$$\boldsymbol{C}_s(\tau) = 0, \qquad \text{for all } \tau \neq 0 \pmod 4.$$

For other $\tau \neq 0 \pmod 4$ it will be similar. From this, the correlation distribution follows. □

Theorem 18: Let U be the support (also called characteristic set) of the sequence $\{u(t)\}$ of Theorem 17, and let C be the support of the underlying sequence $\{s(t)\}$. Then

$$\begin{aligned} U = &[(l+1)C \bmod 4l] \\ &\cup [(l+1)(C-\delta)^* + 3l \bmod 4l] \\ &\cup [(l+1)C^* + 2l \bmod 4l] \\ &\cup [(l+1)(C-\delta)^* + 3l \bmod 4l] \end{aligned} \tag{13}$$

where C^* and $(C-\delta)^*$ denote the complement of C and $C-\delta$ in $\boldsymbol{Z}_l$, respectively. Furthermore,

$$\begin{aligned} \phi(U) = &\{0\} \times C \cup \{1\} \times (C-\delta)^* \\ &\cup \{2\} \times C^* \cup \{3\} \times (C-\delta)^* \end{aligned} \tag{14}$$

where $\phi(x) = (x \bmod 4, x \bmod l)$ is the isomorphism from $\boldsymbol{Z}_{4l}$ to $\boldsymbol{Z}_4 \times \boldsymbol{Z}_l$.

Proof: It is well known that $\{s(t)\}$ has ideal autocorrelation if and only if its support C is an $(l, \frac{l-1}{2}, \frac{l-3}{4})$ or $(l, \frac{l+1}{2}, \frac{l+1}{4})$ difference set of $\boldsymbol{Z}_l$, where $l \equiv 3 \pmod 4$. So we assume that $l = 4h-1$ for some integer h. Note that $4h + (-1)l = 1$. By the Chinese remainder algorithm [11], (12) holds if and only if

$$\begin{aligned} t &\equiv (4hi - lj) \pmod{4l} \\ &\equiv (i(l+1) - lj) \pmod{4l}. \end{aligned}$$

The conclusions then follow from the definition of the matrix M of (11) and the definition of the sequence $\{u(t)\}$. □

The following result follows from Theorem 18.

Theorem 19: Let $\{u(t)\}$ be the sequence in Theorem 17. If the support C of the underlying sequence $\{s(t)\}$ has cardinality $\frac{l+1}{2}$, then

$$|U| = |\{u(t) = 1 \,|\, 0 \leq t \leq 4l-1\}| = 2l \pm 1$$

where U is the support of the sequence $\{u(t)\}$.

From now on, we will call the sequence $s(t)$ the *base sequence* of this construction. By Theorem 19, the sequence $\{u(t)\}$ is almost balanced.

Theorem 20: Let $\{u(t)\}$ be the sequence in Theorem 17, and let U be its support. Then U is a $(4l, 2l-1, l-2, l-1)$ or $(4l, 2l+1, l, l-1)$ almost difference set of $\boldsymbol{Z}_{4l}$.

Proof: This follows from Theorems 19, 17, and 16. □

The construction of binary sequences of period $4l$ with optimal autocorrelation of Theorem 17 and the construction of almost difference sets of $\boldsymbol{Z}_{4l}$ in Theorem 20 are quite general and flexible, as different classes of base sequences give different classes of sequences with optimal autocorrelation and almost difference sets.

As made clear earlier, a binary sequence of period $l \equiv 3 \pmod 4$ has ideal autocorrelation if and only if its support C is an $(l, \frac{l-1}{2}, \frac{l-3}{4})$ or $(l, \frac{l+1}{2}, \frac{l+1}{4})$ difference set of $\boldsymbol{Z}_l$. Difference sets of this type are called *Paley–Hadamard difference sets*.

Cyclic Paley–Hadamard difference sets include the following classes:

A) with parameters $(p, \frac{p-1}{2}, \frac{p-3}{4})$, where $p \equiv 3 \pmod 4$ is prime, and the difference set just consists of all the quadratic residues in $\boldsymbol{Z}_p$;

B) with parameters $(2^t-1, 2^{t-1}-1, 2^{t-2}-1)$, for description of difference sets with these parameters see Dillon [4], Dillon and Dobbertin [5], Gordon, Mills, and Welch [13], Pott [23], Xiang [27];

C) with parameters $(l, \frac{l-1}{2}, \frac{l-3}{4})$, where $l = p(p+2)$ and both p and $p+2$ are primes. These are the twin-prime difference sets, and may be defined as

$$\begin{aligned} &\{(g, h) \in \boldsymbol{Z}_p \times \boldsymbol{Z}_{p+2} : g, h \neq 0 \text{ and } \chi(g)\chi(h) = 1\} \\ &\qquad \cup \{(g, 0) : g \in \boldsymbol{Z}_p\} \end{aligned}$$

where $\chi(x) = +1$ if x is a nonzero square in the corresponding field, and $\chi(x) = -1$ otherwise [18];

D) with parameters $(p, \frac{p-1}{2}, \frac{p-3}{4})$, where p is a prime of the form $p = 4s^2 + 27$. They are cyclotomic difference sets and can be described as [17]

$$D = D_0^{(6,p)} \cup D_1^{(6,p)} \cup D_3^{(6,p)}$$

where $D_0^{(6,p)}$ denotes the multiplicative group generated by α^6, $D_i^{(6,p)} = \alpha^i D_0^{(6,p)}$ denotes the cosets, and α is a primitive element of $\boldsymbol{Z}_q$.

Theorem 21: The construction of Theorem 17 gives the following families of binary sequences of period n with optimal autocorrelation for the following n:

1) $n = 4p$, where $p \equiv 3 \pmod 4$ is any prime;
2) $n = 4(2^t - 1)$, for any integer $t \geq 1$;
3) $n = 4p(p+2)$, where p and $p+2$ are any twin primes;
4) $n = 4p$, where $p = 4s^2 + 27$ is any prime.

Proof: Note that the sequences with support being the difference sets with parameters of A), B), C), and D) have ideal autocorrelation. With these base sequences, the construction of Theorem 17 gives the four classes of binary sequences of period n described above. □

Theorem 22: The support U of (13) of the four classes of binary sequences with optimal autocorrelation in Theorem 21 gives four families of cyclic almost difference sets with the following parameters:

1) $(4p, 2p-1, p-2, p-1)$, where $p \equiv 3 \pmod 4$ is any prime;
2) $(4(2^t-1), 2^{t+1}-3, 2^t-3, 2^t-2)$, for any integer $t \geq 1$;
3) $(4p(p+2), 2p(p+2)-1, p(p+2)-2, p(p+2)-1)$, where p and $p+2$ are any twin primes;

4) $(4p, 2p-1, p-2, p-1)$, where $p = 4s^2 + 27$ is any prime.

Proof: This follows from Theorems 21 and 20. □

The construction of Theorem 17 is based on interleaving four closely related sequences with ideal autocorrelation. It is quite general, and gives more classes of binary sequences of period $n \equiv 0 \pmod 4$ with optimal autocorrelation if new families of binary sequences with ideal autocorrelation are discovered. The expression of (13) shows clearly that the four classes of almost difference sets with parameters of Theorem 22 are based on Paley–Hadamard difference sets. When $\delta = 0$, the construction of Theorem 17 is equivalent to the so-called product method [20]. The sequence constructed is the EXCLUSIVE–OR of a binary sequence of period l with ideal autocorrelation and the binary sequence $01110111\ldots$. Hence, the construction of Theorem 17 is a generalization of the product method.

In the remainder of this section, we show that a result due to Jungnickel can also be used to construct almost difference sets with the same parameters as those of Theorem 22 and thus binary sequences of period $4l$ with optimal autocorrelation.

Theorem 23 (Jungnickel [16]): Let D_1 be an ordinary (v, a, λ) difference set in a group A, and let D_2 be an difference set with parameters $(4u^2, 2u^2-u, u^2-u)$ in a group B. Then

$$D := (D_2 \times D_1^*) \cup (D_2^* \times D_1)$$

is a DDS in $B \times A$ relative to $\{1\} \times A$, with parameters $(4u^2, v, 2u^2v + 2au - uv, \lambda_1, \lambda_2)$, where

$$\lambda_1 = (2u^2 - u)(v - 2a) + 4u^2\lambda$$
$$\lambda_2 = u^2v - uv + 2au,$$

and D_2^* denotes the complement of D_2.

As a corollary of Theorem 23, we have the following conclusion.

Corollary 1: Let D_1 be an ordinary $(l, \frac{l-1}{2}, \frac{l-3}{4})$ (respectively, $(l, \frac{l+1}{2}, \frac{l+1}{4})$) difference set in $\boldsymbol{Z}_l$, let D_2 be a trivial difference set in $\boldsymbol{Z}_4$ with parameters $(4, 1, 0)$. Then

$$D := (D_2 \times D_1^*) \cup (D_2^* \times D_1)$$

is $(4l, 2l-1, l-2, l-1)$ (respectively, $(4l, 2l+1, l, l-1)$) almost difference set of $\boldsymbol{Z}_4 \times \boldsymbol{Z}_l$. Thus, the binary sequence with support $\phi^{-1}(D)$ has period $4l$ and optimal autocorrelation.

By choosing D_1 to be any Paley–Hadamard difference set, Corollary 1 gives an almost difference set and binary sequence with optimal autocorrelation. This is similar to the construction given by Theorem 17. Now one basic question is whether the two constructions are the same or "equivalent," as the parameters of the almost difference sets obtained with the two constructions are the same.

To answer the above question, we introduce equivalences for sequences and almost difference sets. Two binary sequences $\{s(i)\}$ and $\{t(i)\}$ of period n are said to be equivalent if and only if there are two integers a and b in $\boldsymbol{Z}_n$ such that $\gcd(n, a) = 1$ and

$$s(i) = t(ai + b)$$

for all i. Similarly, two almost difference sets D_1 and D_2 of $\boldsymbol{Z}_{4l}$ with the same parameters are said to be equivalent if and only if there are two integers a and b in $\boldsymbol{Z}_{4l}$ such that $\gcd(a, 4l) = 1$ and

$$aD_1 + b = D_2.$$

Theorem 24: The binary sequences and almost difference sets obtained by Theorem 17 and Corollary 1 are not equivalent.

Proof: Let D_1 be an ordinary $(l, \frac{l-1}{2}, \frac{l-3}{4})$ (respectively, $(l, \frac{l+1}{2}, \frac{l+1}{4})$) difference set of $\boldsymbol{Z}_l$. Then the almost difference set obtained in Corollary 1 is of the form

$$D = \{i\} \times D_1^* \cup \{i+1, i+2, i+3\} \times D_1$$

where $i \in \boldsymbol{Z}_4$. Let (a_1, b_1) and (a_2, b_2) be two elements of $\boldsymbol{Z}_4 \times \boldsymbol{Z}_l$ with $\gcd(a_1, 4) = 1$ and $\gcd(b_1, l) = 1$. Then we have

$$\begin{aligned}(a_1, b_1)D + (a_2, b_2) &= \{a_1 i + a_2\} \times C_1^* \\ &\quad \cup \{(i+1)a_1 + a_2, (i+2)a_1 + a_2, (i+3)a_1 + a_2\} \times C_1 \end{aligned} \tag{15}$$

where $C_1 = b_1 D_1 + b_2$ is a difference set with the same parameters as D_1. Hence the expression of (15) cannot be of the form of (14), as in (14) the list

$$\{C, (C-\delta)^*, C^*, (C-\delta)^*\}$$

no three elements are identical while in (15) three elements in the list

$$\{C_1^*, C_1, C_1, C_1\}$$

are the same. This proves the conclusion of this theorem. □

The discussions above proves the following.

Theorem 25: The set $\phi(U)$ of (14) is a DDS of $\boldsymbol{Z}_4 \times \boldsymbol{Z}_l$ with parameters

$$(4, l, 2l+1, l, l+1) \quad \text{or} \quad (4, l, 2l-1, l-2, l-1)$$

relative to $\{0\} \times \boldsymbol{Z}_l$.

Theorem 24 means that the DDSs $\phi(U)$ in Theorem 25 are not equivalent to those of Theorem 23. Hence we have also described several classes of DDSs in this paper.

VI. Concluding Remarks

Our contribution of this paper includes the determination of the numerical multiplier group for several classes of almost difference sets given in Section II, the establishment of some relations between some almost difference sets and some difference sets in Section III, the construction of six new classes of almost difference sets in Sections IV and V, and the four classes of binary sequences of period $n \equiv 0 \pmod 4$ with optimal autocorrelation in Section V. Some of the new almost difference sets obtained in this paper are also DDSs.

It is interesting to note that most of the families of almost difference sets known so far are related to cyclotomy. So far only a small number of classes of almost difference sets are found.

Numerical results show that there should be more families of almost difference sets that remain to be discovered. For example, the set

$$\{0, 1, 2, 3, 4, 5, 6, 7, 9, 11, 12, 15, 16, 19, 23, 24, 29, 30, 32, 35, 37, 39\}$$

is a $(45, 22, 10, 22)$ almost difference set of $\boldsymbol{Z}_{45}$, which does not belong to any known class of almost difference sets. Another example is the following almost difference set of $\boldsymbol{Z}_{33}$ with parameters $(33, 16, 7, 16)$:

$$\{0, 1, 2, 3, 4, 5, 6, 8, 13, 14, 18, 20, 22, 25, 28, 29\}.$$

It is an open question whether $(v, \frac{v-1}{2}, \lambda, t)$ almost difference sets exist for all odd v. It is very likely that the answer is positive.

ACKNOWLEDGMENT

The authors wish to thank both referees for their comments that improved this paper, and for pointing out references [20], [21], and [24] to them.

REFERENCES

[1] R. S. Coulter and R. Matthews, "Planar functions and planes of the Lenz–Barlotti class II," *Des., Codes Cryptogr.*, vol. 10, pp. 165–195, 1997.

[2] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Amsterdam, The Netherlands: North-Holland/Elsevier, 1998, North-Holland Mathematical Library 55.

[3] J. A. Davis, "Almost difference sets and reversible difference sets," *Arch. Math.*, vol. 59, pp. 595–602, 1992.

[4] J. F. Dillon, "Multiplicative difference sets via additive characters," *Des., Codes Cryptogr.*, vol. 17, pp. 225–235, 1999.

[5] J. F. Dillon and H. Dobbertin, "Cyclic difference sets with singer parameters," manuscript, 1999.

[6] C. Ding, "The differential cryptanalysis and design of the natural stream ciphers," in *Fast Software Encryption (Lecture Notes in Computer Science)*, R. Anderson, Ed. Heidelberg, Germany: Springer-Verlag, 1994, vol. 809, pp. 101–115.

[7] ——, "Binary cyclotomic generators," in *Fast Software Encryption (Lecture Notes in Computer Science)*, B. Preneel, Ed. New York: Springer-Verlag, 1995, vol. 1008, pp. 29–60.

[8] ——, "Cryptographic counter generators," TUCS Series in Dissertation 4, Turku Centre for Computer Science, ISBN 951-650-929-0, 1997.

[9] C. Ding, T. Helleseth, and K. Y. Lam, "Several classes of sequences with three-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2606–2612, Nov. 1999.

[10] C. Ding, T. Helleseth, and H. M. Martinsen, "New families of binary sequences with optimal three-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 47, pp. 428–433, Jan. 2001.

[11] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. Singapore: World Scientific, 1996.

[12] S. W. Golomb, *Shift Register Sequences*. Laguna Hills, CA: Aegean Park, 1982.

[13] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.*, vol. 14, pp. 614–625, 1962.

[14] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, vol. II, pp. 1765–1854.

[15] T. Helleseth and D. Sandberg, "Some power mappings with low differential uniformity," *Applic. Alg. Eng., Commun. Comput.*, vol. 8, pp. 363–370, 1997.

[16] D. Jungnickel, "On automorphism groups of divisible designs," *Can. J. Math*, vol. 34, pp. 257–297, 1982.

[17] ——, "Difference sets," in *Contemporary Design Theory: A Collection of Surveys*, J. Dinitz and D. R. Stinson, Eds. New York: Wiley, 1992.

[18] D. Jungnickel and A. Pott, "Difference sets: An introduction," in *Difference Sets, Sequences and their Correlation Properties*, A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds. Amsterdam, The Netherlands: Kluwer, 1999, pp. 259–295.

[19] A. Lempel, M. Cohn, and W. L. Eastman, "A class of binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 38–42, Jan. 1977.

[20] H. D. Lüke, "Sequences and arrays with perfect periodic correlation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 24, no. 3, pp. 287–294, 1988.

[21] S. Mertens and C. Bessenrodt, "On the ground states of the Bernasconi model," *J. Phys. A: Math. Gen.*, vol. 31, pp. 3731–3749, 1998.

[22] J.-S. No, H. Chung, H.-Y. Song, K. Yang, J.-D. Lee, and T. Helleseth, "New construction for binary sequences of period $p^m - 1$ with optimal autocorrelation using $(z+1)^d + az^d + b$," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1638–1644, May 2001.

[23] A. Pott, *Finite Geometry and Character Theory (Lecture Notes in Mathematics)*. Berlin, Germany: Springer-Verlag, 1995, vol. 1601.

[24] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inform. Transm.*, vol. 5, no. 1, pp. 12–16, 1969.

[25] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, revised ed. Rockville, MD: McGraw-Hill, 1994, vol. 1, Computer Science, 1985.

[26] T. Storer, *Cyclotomy and Difference Sets*. Chicago, IL: Marham, 1967.

[27] Q. Xiang, "Recent results on difference sets with classical parameters," in *Difference Sets, Sequences and Their Correlation Properties*, A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds. Amsterdam, The Netherlands: Kluwer, 1999, pp. 419–434.