Splitter Sets and k-Radius Sequences

Tao Zhang, Xiande Zhang, and Gennian Ge

***Abstract*—Splitter sets are closely related to lattice tilings, and have applications in flash memories and conflict-avoiding codes. The study of k-radius sequences was motivated by some problems occurring in large data transfer. It is observed that the existence of splitter sets yields k-radius sequences of short length. In this paper, we obtain several new results contributing to splitter sets and k-radius sequences. We give some new constructions of perfect splitter sets, as well as some nonexistence results on them. As a byproduct, we obtain some new results on optimal conflict-avoiding codes. Furthermore, we provide several explicit constructions of short k-radius sequences for certain values of n, by establishing the existence of k-additive sequences. In particular, we show that for any fixed k, there exist infinitely many values of n such that $f_k(n) = \frac{n^2}{2k} + O(n)$, where $f_k(n)$ denotes the shortest length of an n-ary k-radius sequence. This result partially affirms a conjecture posed by Bondy, Lonc, and Rzążewski.**

***Index Terms*—Splitter sets, flash memory, conflict-avoiding codes, lattice tilings, k-radius sequences, k-additive sequences.**

I. Introduction

THE study of splitter sets was motivated by constructing codes correcting single limited magnitude errors used in multilevel cell (MLC) flash memories. The construction of k-radius sequences has recently become the subject of study due to some computing problems occurring in large data transmission. The construction of the splitter sets and k-radius sequences are closely related and so are both studied in this paper.

A. Flash Memories and Splitter Sets

Flash memory is a non-volatile memory technology that is both electrically programmable and erasable. It is currently widely used due to its reliability, high storage density and low cost memories. Many applications of flash memories have been found in personal computers, digital audio players, digital cameras, mobile phones and so on.

To scale the storage density of flash memories, the multilevel memory cell is used to increase the number of stored bits in a cell. Thus, each multilevel memory cell stores $\log_2(q)$ bits regarded as a symbol over a discrete alphabet of size q. The chief disadvantage of flash memories is their inherent asymmetry between cell programming—charge injection into cells, and cell erasure—charge removal from cells. This asymmetry causes significant error sources to change cell levels in one dominant direction. Moreover, many reported common flash error mechanisms induce errors whose magnitudes are small and independent of the alphabet size, which may be significantly larger than the typical error magnitude. Thus, flash errors strongly motivated the application of the limited magnitude error model to flash memory [8], [18].

Splitter sets were first studied in [15] and [28]–[30] with connections to lattice tilings. They attracted recent attention again due to their equivalence to codes correcting single limited magnitude errors in flash memories (see [7], [13], [18]–[20], [24], [25], [32], [33] and the references therein). In this context, a code obtained from a splitter set $B[-k_1, k_2](n)$ can correct a symbol $a \in \{0, 1, \ldots, n-1\}$ if it is modified into $a+e$ during transmission, where $-k_1 \leqslant e \leqslant k_2$. Further, splitter sets are also found to be useful in constructing conflict-avoiding codes [23], [26] and k-radius sequences [3].

Research works on splitter sets involve both existence and nonexistence results. For the existence of such sets, a construction of perfect splitter sets for $k_1 = 0$ can be found in [19]. Kløve *et al.* [20] gave a construction of perfect splitter sets for $k_1 = k_2$. Constructions of splitter sets for $1 \leqslant k_1 < k_2$ can be found in [24], [32], and [33]. For the nonexistence results, Schwartz proved that there does not exist a nonsingular perfect splitter set for $k_1 = k_2 - 1$ in [24]. Later, Zhang and Ge [33] showed that there does not exist a nonsingular perfect splitter set when $(k_1+1)k_1 > k_2$ and $k_1 + k_2$ is odd. Moreover, they proposed the following conjecture.

Conjecture 1 [33]: There does not exist a nonsingular perfect splitter set when $1 \leqslant k_1 \leqslant k_2$ and $k_1 + k_2$ is odd.

One of the primary aims of this paper is to continue this investigation and provide new constructions and nonexistence results for perfect splitter sets. Our contributions to splitter sets are as follows.

Contribution I:

1) We present several constructions of perfect splitter sets, which generalize most of the known constructions;
2) we affirm Conjecture 1 when $k_1 + k_2$ is an odd prime;
3) we solve all the undetermined nonsingular cases left in [25] and [33] for $k_1 = 1$, $k_2 = 3$ and $n \leqslant 1000$;
4) we provide a method of constructing optimal conflict-avoiding codes from splitter sets.

B. k-Radius Sequences

The study of n-ary k-radius sequences was motivated by a problem of fetching huge objects into small memory for

Manuscript received October 12, 2016; revised February 22, 2017; accepted April 10, 2017. Date of publication April 18, 2017; date of current version November 20, 2017. X. Zhang was supported by the National Natural Science Foundation of China under Grant 11301503. G. Ge was supported in part by the National Natural Science Foundation of China under Grant 11431003 and Grant 61571310, in part by the Beijing Hundreds of Leading Talents Training Project of Science and Technology, and in part by the Beijing Municipal Natural Science Foundation.

T. Zhang is with the School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China (e-mail: tzh@zju.edu.cn).

X. Zhang is with the School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China (e-mail: drzhangx@ustc.edu.cn).

G. Ge is with the School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China (e-mail: gnge@zju.edu.cn).

Communicated by M. Schwartz, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2017.2695219

pairwise computations, such as calculating the volume of a tumour from a series of MRI slices. Introduced by Jaromczyk and Lonc [16], n-ary k-radius sequences describe a First-In First-Out caching strategy for computing functions that require computations on all pairs taken from a set of n large objects, where at most $k+1$ objects are cached at any one time. Recently, this problem has been extended to a more general form: k-radius sequences for graphs [12]. In this paper, we focus on the original version of k-radius sequences for complete graphs in [16].

To reduce computing complexity, people are interested in constructing short k-radius sequences. Let $f_k(n)$ be the shortest length of an n-ary k-radius sequence. When k is fixed and n goes to infinity, there are nice asymptotic results on the values of $f_k(n)$. Jaromczyk and Lonc [16] showed that when $k=2$, $f_2(n)=\frac{1}{2}n^2(1+o(1))$. For general k, Blackburn and Mckee [3] first proved that $f_k(n)=\frac{1}{2k}n^2(1+o(1))$ when $k \leqslant 204$ except possibly $k=195$ and when $k+1$ or $2k+1$ is a prime. In the same paper, they revealed nice connections of k-radius sequences to tilings, discrete logarithms, and properties of cyclotomic fields. Blackburn [2] then proved that $f_k(n)=\frac{1}{2k}n^2(1+o(1))$ for every fixed k using a probabilistic argument. The best known estimation was established by Jaromczyk *et al.* [17], who gave a general construction of k-radius sequences by graph decompositions, and improved the asymptotics to $f_k(n)=\frac{1}{2k}n^2+O(n^{1+\varepsilon})$ for every fixed k and every $\varepsilon>0$. Recently, Bondy *et al.* [4] proposed the following conjecture, and proved that it is true for $k=2$.

Conjecture 2: For every fixed positive integer k, $f_k(n)=\frac{n^2}{2k}+O(n)$.

For exact values of $f_k(n)$, in a much earlier paper [14] on the context of database applications, Ghosh studied k-radius sequences and determined all values of $f_k(n)$ when $k=1$. When $k=2$, Jaromczyk and Lonc [16] found exact values of $f_2(n)$ for $n \leqslant 7$. They also proved the following lower bound for the length of k-radius sequences,

$$f_k(n) \geqslant n\lceil\frac{n-1}{2k}\rceil + R_k(n), \tag{1}$$

where

$$R_k(n)=\begin{cases}0, & \text{for } 0<r\leqslant k;\\ r-k, & \text{for } k<r\leqslant 2k,\end{cases} \tag{2}$$

and r is the unique integer such that $n-1 \equiv r \pmod{2k}$. Through a computer search, Chee *et al.* [10] found exact values of $f_2(n)$ for $n=8, 10, 11, 12, 14, 15, 16$ and 18. Later in [17], Jaromczyk *et al.* determined the exact values of $f_2(n)$ whenever $n=2p$ and $p>2$ is a prime. Recently, Bondy *et al.* [4] and [5] gave a general construction of the shortest or close to the shortest k-radius sequences, and determined the values of $f_2(n)$ for all n except when $n \equiv 18, 19, 20, 21 \pmod{24}$ and $n \equiv 7662, 7663, 7664, 7665 \pmod{8760}$. For arbitrary n, they proved that $f_2(n) \leqslant n\lceil\frac{n-1}{4}\rceil+66$, which differs from the lower bound only by a constant. They also determined $f_k(n)$ when k is a power of a prime, and for every n such that $2k^2+1<n\leqslant 2k(k+1)+1$. The exact values of $f_k(n)$ determined in [4] and [17] all meet the lower bound (1) except for $f_2(9)$, which is equal to 21.

For the case when k is not fixed, i.e., k is a function of n, the problem of determining $f_k(n)$ has been considered by Jaromczyk *et al.* [17] and Dębski and Lonc [11]. When $k=\lfloor n^\alpha\rfloor$, where α is a fixed real number such that $0<\alpha<1$, it was shown in [17] that $f_k(n)=\frac{n^2}{2k}+O(n^\beta)$, for some $\beta<2-\alpha$. For some values of $c<1$ and sufficiently large n, the authors in [11] found exact values of $f_{cn}(n)$ by providing direct constructions of optimal sequences.

The novel method to construct short k-radius sequences used in [4] depends on the existence of some other cyclic sequences that they called k-additive sequences. However, the fact that only a few special cases of general constructions of k-additive sequences have been known is a limitation of this method to construct more short k-radius sequences. In this paper, we present some new constructions of k-additive sequences for general k. These constructions are applications of Weil's theorem on multiplicative character sums, see [21].

Contribution II: We give two constructions of k-additive sequences of lengths s such that $n=2ks+1$ is a sufficiently large prime under certain conditions. Consequently, we prove Conjecture 2 in part: for every fixed k, there are infinitely many primes n such that

$$f_k(n)=\frac{n^2}{2k}+O(n).$$

C. Organization

This paper is organized as follows. Section II recalls some basic facts about splitter sets and connections to k-radius sequences. In Section III, we give some constructions of perfect splitter sets based on factorizations of groups, and provide new nonexistence results on perfect splitter sets. Some results on optimal conflict-avoiding codes obtained from splitter sets are also presented in Section III. Section IV gives several direct constructions of k-additive sequences. Finally Section V concludes the paper.

II. Preliminaries

The following notations are fixed throughout this paper.

- For an odd prime p, a primitive root g modulo p, and an integer b not divisible by p, there exists a unique integer $l\in[0,p-2]$ such that $g^l\equiv b \pmod p$. It is known as the index of b relative to the base g, and it is denoted by $\mathrm{ind}_g(b)$.
- For any positive integer q, let $\mathbb{Z}_q$ be the ring of integers modulo q and $\mathbb{Z}_q^*=\mathbb{Z}_q\setminus\{0\}$.
- Let a, b be integers such that $a\leqslant b$, denote
$$[a,b]=\{a,a+1,a+2,\dots,b\} \text{ and}$$
$$[a,b]^*=\{a,a+1,a+2,\dots,b\}\setminus\{0\}.$$
- Unless additionally defined, we assume that $a\cdot T=\{a\cdot t: t\in T\}$ and $T\cdot T'=\{t\cdot t': t\in T, t'\in T'\}$ for any element a and any sets T, T', where $\cdot$ is any binary operator.

A. Splitter Sets

Let q be a positive integer and k_1, k_2 be non-negative integers with $0\leqslant k_1\leqslant k_2$. The set $B\subseteq\mathbb{Z}_q$ of size n is called a *splitter set* if all the sets

$$\{ab \pmod q : a\in[-k_1,k_2]^*\},\quad b\in B,$$

have k_1+k_2 nonzero elements, and they are disjoint. We denote such a splitter set by $B[-k_1,k_2](q)$ set.

If a $B[-k_1,k_2](q)$ set of size n exists, then we have

$$q \geqslant (k_1+k_2)n+1,$$

and so

$$n \leqslant \frac{q-1}{k_1+k_2}.$$

A $B[-k_1,k_2](q)$ set is called *perfect* if $n=\frac{q-1}{k_1+k_2}$. Clearly, a perfect set can exist only if $q \equiv 1 \pmod{k_1+k_2}$.

The paper [24] suggests that we distinguish two types of perfect $B[-k_1,k_2](q)$ sets.

Definition 3: Let k_1,k_2 be integers such that $0 \leqslant k_1 \leqslant k_2$, and let q be a positive integer. The perfect $B[-k_1,k_2](q)$ set is nonsingular *if* $\gcd(q,k_2!)=1$. *Otherwise, the set is called* singular. *If for any prime $p|q$, there is some k with $0<k\leqslant k_2$ such that $p|k$, then the perfect $B[-k_1,k_2](q)$ set is called* purely singular.

The following two constructions are useful for perfect splitter sets.

Theorem 4 [25, Th. 14]: If there is a perfect $B[-k_1,k_2](q)$ set and some positive integer $d|q$, $\gcd(d,k_2!)=1$, *then $(k_1+k_2)d|(q-d)$, and there is a perfect $B[-k_1,k_2](q/d)$ set.*

Theorem 5 [32, Th. 5]: Let B_1 be a $B[-k_1,k_2](q_1)$ set and B_2 be a $B[-k_1,k_2](q_2)$ set where $\gcd(q_2,k_2!)=1$. *Let*

$$B_1\odot B_2=\{c+rq_1 : c\in B_1, r\in[0,q_2-1]\}\cup\{q_1c : c\in B_2\}.$$

Then,

1) *$B_1\odot B_2$ is a $B[-k_1,k_2](q_1q_2)$ set;*
2) *$|B_1\odot B_2|=q_2|B_1|+|B_2|$;*
3) *If both B_1 and B_2 are perfect, then $B_1\odot B_2$ is perfect.*

From the above two theorems, it is easy to see that there is a perfect nonsingular $B[-k_1,k_2](q)$ set if and only if there is a perfect nonsingular $B[-k_1,k_2](p)$ set for each prime p dividing q.

B. k-Radius Sequences From Splitter Sets

Let Σ be an n-element alphabet. An n-ary *k-radius sequence* over Σ is a finite sequence $s_0,s_1,\ldots,s_{m-1}$ of elements taken from Σ such that, for all distinct $x,y\in\Sigma$, there exist $i,j\in[0,m-1]$ such that $s_i=x$, $s_j=y$ and $|i-j|\leqslant k$. In other words, any two distinct elements of Σ are at distance of at most k somewhere in the sequence. For example,

$$3,6,2,7,0,5,6,4,1,0,7,3,4,2,5,1,3$$

is an 8-ary 2-radius sequence of length 17 over $\mathbb{Z}_8$.

To reduce the computational complexity, Jaromczyk and Lonc [16] were interested in constructing short k-radius sequences, which is also interesting in pure combinatorics. The example above shows that $f_2(8)\leqslant 17$, and in fact $f_2(8)=17$ by [10].

The following construction of short n-ary k-radius sequences can be found in [3, Th. 3.1] by Blackburn and Mckee.

Theorem 6 [3, Th. 3.1]: Let n be a prime number. If there exists a perfect $B[-k,k](n)$ set, then there exists an n-ary k-radius sequence of length $\frac{n-1}{2k}(n+k-1)+1$.

In fact, this result can be easily extended to a general perfect $B[-k_1,k_2](n)$ set as follows.

Theorem 7: Let n be a prime number. If there exists a perfect $B[-k_1,k_2](n)$ set, then there exists an n-ary k_2-radius sequence of length $\frac{n-1}{k_1+k_2}(n+k_2-1)+1$.

Proof: If there exists a perfect $B[-k_1,k_2](n)$ set $D=\{d_1,d_2,\cdots,d_{\frac{n-1}{k_1+k_2}}\}$, let $T(d)=\{-k_1d,-(k_1-1)d,\cdots,-2d,-d,d,2d,\cdots,k_2d\}$. Then $\bigcup_{d\in D}T(d)$ covers $\mathbb{Z}_n^*$.

For each $d\in D$, let s_d be the periodic sequence $0,d,2d,\ldots,(n-1)d,0,d,\ldots$ of period n. Let $\overline{s}_d$ be a finite sequence of length $n+k_2$ consisting of $n+k_2$ consecutive terms of the periodic sequence s_d. Note that the sequence $\overline{s}_d$ contains all pairs (x,y) with $y-x\in T(d)$. For $i\geqslant 2$, we choose the first element of $\overline{s}_{d_i}$ to be equal to the final element of $\overline{s}_{d_{i-1}}$. Then the concatenation of sequences $\overline{s}_{d_i}$, $1\leqslant i\leqslant\frac{n-1}{k_1+k_2}$ is an n-ary k_2-radius sequence of length $\frac{n-1}{k_1+k_2}(n+k_2-1)+1$. ■

Note that Theorems 6 and 7 are based on perfect splitter sets, which yield n-ary sequences with prime n. Now we combine a method given in [33] and the idea in Theorem 6 to construct short k-radius sequences over $\mathbb{Z}_n$, where n may not be a prime. For an element $d\in\mathbb{Z}_n$, we define the set $T_{k,n}(d)$ by

$$\begin{aligned}&T_{k,n}(d)\\&=d\{\pm1,\pm2,\ldots,\pm k\}\\&=\{-kd,-(k-1)d,\ldots,-2d,-d,d,2d,\ldots,(k-1)d,kd\}.\end{aligned}$$

Theorem 8: Let p be a prime, $t<k<p$ be integers such that $t|k$ and $\frac{2k}{t}|(p-1)$. For $0\leqslant i\leqslant t-1$, let $T_i=\{x|x\equiv i \pmod t, x\in[-k,k]^*\}$, then $|T_i|=\frac{2k}{t}$. Let g be a primitive root modulo p such that $g\equiv 1 \pmod t$, and let $\theta=\gcd\{\mathrm{ind}_g(a)|a\in[-k,k]^*\}$. If

$$|\{\frac{\mathrm{ind}_g(a)}{\theta} \pmod{\frac{2k}{t}}|a\in T_i\}|=\frac{2k}{t}$$

for $0\leqslant i\leqslant t-1$ and υ is a positive integer such that $\upsilon|\theta$, $\frac{2\upsilon k}{t}|(p-1)$ and $\gcd(\frac{\theta}{\upsilon},\frac{2k}{t})=1$, then there exists a (tp)-ary k-radius sequence of length $\frac{t(p-1)\cdot(tp-1)}{2k}+\frac{t(3p-1)}{2}$.

Proof: Let

$$D=\{g^{\frac{2k\upsilon}{t}i+j} \pmod{tp}|i\in[0,\frac{t(p-1)}{2k\upsilon}-1],\\ j\in[0,\upsilon-1]\}.$$

Note that $|D|=\frac{t(p-1)}{2k}$. It has been proved in [33, Th. 5] that $T_{k,tp}(d)$, where $d\in D$, are pairwise disjoint in $\mathbb{Z}_{tp}\setminus\{0\}$ with each set being of size $2k$. We claim that $T_{k,tp}(d)$, $d\in D$ cover each element in $\mathbb{Z}_{tp}\setminus\{0,p,2p,\ldots,(t-1)p\}$ exactly once. In fact, since g is a primitive root modulo p, g^l is nonzero in $\mathbb{Z}_p$ for any l, which means $p\nmid d$ for any $d\in D$. Noting that $k<p$, we have $p\nmid kd$ since p is a prime.

For each $d\in D$, let s_d be the periodic sequence $0,d,2d,\ldots,(tp-1)d,0,d,\ldots$ of period tp. Since $\gcd(d,t)=1$ and $\gcd(d,p)=1$, we have $\gcd(d,tp)=1$. Then distinct elements $x,y\in\mathbb{Z}_{tp}$ appear at distance k or less somewhere within s_d if and only if $y - x \in T_{k,tp}(d)$. Let $\overline{s}_d$ be a finite sequence of length $tp + k$ consisting of $tp + k$ consecutive terms of the periodic sequence s_d. Order elements of D as $\{d_1, d_2, \ldots, d_{\frac{t(p-1)}{2k}}\}$. For each $i \geqslant 2$, we choose the first term of $\overline{s}_{d_i}$ to be equal to the final term of $\overline{s}_{d_{i-1}}$. Let s_p be the reverse of the sequence

$$\begin{aligned}&0, p, 2p, \ldots, (t-1)p, 1, p+1, 2p+1, \ldots,\\ &\qquad (t-1)p+1, \ldots, p-1, 2p-1, \ldots, tp-1.\end{aligned}$$

Then the concatenation of the sequences s_p, and $\overline{s}_{d_i}$, $1 \leqslant i \leqslant \frac{t(p-1)}{2k}$ is a (tp)-ary k-radius sequence of length $tp + \frac{t(p-1)}{2k} \cdot (tp + k - 1) = \frac{t(p-1)\cdot(tp-1)}{2k} + \frac{t(3p-1)}{2}$. ■

For $t \geqslant 2$, several parameters for which the conditions of Theorem 8 hold can be found in [33, Table I]. We give one example to illustrate this construction.

Example 9: Let $p = 29$, $k = 4$ and $t = 2$. Then $g = 3$ is a primitive root modulo p. We have $\mathrm{ind}_g(1) = 0$, $\mathrm{ind}_g(2) = 17$, $\mathrm{ind}_g(3) = 1$, $\mathrm{ind}_g(4) = 6$, $\mathrm{ind}_g(-1) = 14$, $\mathrm{ind}_g(-2) = 3$, $\mathrm{ind}_g(-3) = 15$, $\mathrm{ind}_g(-4) = 20$. *Hence $\theta = 1$ and we have*

$$\begin{aligned}\mathrm{ind}_g(-1) &\equiv 2 \pmod 4, & \mathrm{ind}_g(1) &\equiv 0 \pmod 4,\\ \mathrm{ind}_g(-3) &\equiv 3 \pmod 4, & \mathrm{ind}_g(3) &\equiv 1 \pmod 4,\end{aligned}$$

and

$$\begin{aligned}\mathrm{ind}_g(-2) &\equiv 3 \pmod 4, & \mathrm{ind}_g(2) &\equiv 1 \pmod 4,\\ \mathrm{ind}_g(-4) &\equiv 0 \pmod 4, & \mathrm{ind}_g(4) &\equiv 2 \pmod 4.\end{aligned}$$

Taking $v = 1$ gives

$$D = \{3^{4i} \pmod{58} | 0 \leqslant i \leqslant 6\} = \{1, 23, 7, 45, 49, 25, 53\}.$$

Then it is routine to check that $T_{4,58}(d)$, $d \in D$ cover each element of $\mathbb{Z}_{58} \setminus \{0, 29\}$ exactly once. Therefore, by Theorem 8, there exists a 58-ary 4-radius sequence of length 486. Combining the lower bound in (1), we have $464 \leqslant f_4(58) \leqslant 486$.

III. Splitter Sets

This section serves to provide new general constructions and prove new nonexistence results of perfect splitter sets based on 1-fold factorizations of groups. Further, we observe the equivalence between splitter sets and a subclass of conflict-avoiding codes, which enables us to determine optimal sizes of the latter codes for new infinitely many parameters.

Let G be a finite group and let A and B be subsets of G. If for each element h of G, there are unique elements $a \in A$ and $b \in B$ such that $h = a + b$, then we say $G = A + B$ is a 1*-fold factorization* of group G. There have been some research works concerning 1-fold factorization of groups. For a survey of recent progress in this topic we refer the reader to [31].

A. Constructions of Perfect Splitter Sets

We first give two general simple constructions.

Theorem 10: Let $p = (k_1 + k_2)nm + 1$ be a prime and g be a primitive root modulo p. Let

$$A = \{\mathrm{ind}_g(i) \pmod{(k_1 + k_2)n} : i \in [-k_1, k_2]^*\}.$$

If there exists a subset $A' \subseteq \mathbb{Z}_{(k_1+k_2)n}$ of size n such that $\mathbb{Z}_{(k_1+k_2)n} = A + A'$ is a 1*-fold factorization, then there exists a perfect $B[-k_1, k_2](p)$ set.*

Proof: Let

$$B = \{g^{b+(k_1+k_2)ni} : b \in A', \ i \in [0, m-1]\}.$$

Then $|B| = mn$ and it is easy to see that $B \cdot [-k_1, k_2]^* = \mathbb{Z}_p^*$. Hence B is a perfect $B[-k_1, k_2](p)$ set. ■

Theorem 11: Let $p = 2knm + 1$ be a prime and g be a primitive root modulo p. Let

$$A = \{\mathrm{ind}_g(i) \pmod{kn} : i \in [1, k]\}.$$

If there exists a subset $A' \subseteq \mathbb{Z}_{kn}$ of size n such that $\mathbb{Z}_{kn} = A + A'$ is a 1*-fold factorization, then there exists a perfect $B[-k, k](p)$ set.*

Proof: Let

$$B = \{g^{b+kni} : b \in A', \ i \in [0, m-1]\}.$$

We claim that B is a perfect $B[-k, k](p)$ set.

Suppose that

$$rg^{kni_1+j_1} \equiv sg^{kni_2+j_2} \pmod p,$$

where $r, s \in [-k, k]^*$, $i_1, i_2 \in [0, m-1]$ and $j_1, j_2 \in A'$. Then we have

$$\mathrm{ind}_g(r) + kni_1 + j_1 \equiv \mathrm{ind}_g(s) + kni_2 + j_2 \pmod{p-1}.$$

Reducing this modulo kn, we get

$$\mathrm{ind}_g(r) + j_1 \equiv \mathrm{ind}_g(s) + j_2 \pmod{kn}.$$

Since $kn | \frac{p-1}{2}$, $j_1, j_2 \in A'$ and $\mathbb{Z}_{kn} = A + A'$ is a 1-fold factorization, we have $j_1 = j_2$ and $r = s$ or $r = -s$.

If $r = s$, then $i_1 \equiv i_2 \pmod{2m}$ and so $i_1 = i_2$. Otherwise, $r = -s$, then $kni_1 \equiv kni_2 + \frac{p-1}{2} \pmod{p-1}$, which implies $\frac{p-1}{2} | kn(i_1 - i_2)$ and $i_1 \neq i_2$. That is $m | (i_1 - i_2)$ and $i_1 \neq i_2$, which is a contradiction. ■

Remark 12: In Theorem 10, if $A = \{0, n, 2n, \ldots, (k_1+k_2-1)n\}$, then we can take $A' = [0, n-1]$ to satisfy the 1*-fold factorization condition. This is exactly the case appeared in [19] and [32]. The same phenomenon appears in Theorem 11.*

In order to give new existence results of perfect splitter sets, we define the set

$$\begin{aligned}&S(2k, 2^{m+1}k)\\ &\quad = \{\{0, 2j, 4j, \ldots, 2(k-1)j, 2^m kj, (2^m k + 2)j, \ldots,\\ &\qquad (2^m k + 2(k-1))j\} : j \in [1, 2^m k], \ \gcd(j, 2^{m+1}k) = 1\}.\end{aligned}$$

Lemma 13: Let $m \geqslant 1$, then for any set $A \in S(2k, 2^{m+1}k)$, there exists a set $A' \subset \mathbb{Z}_{2^{m+1}k}$ of size 2^m such that $A + A' = \mathbb{Z}_{2^{m+1}k}$ is a 1*-fold factorization.*

Proof: Let $A = \{0, 2j, 4j, \ldots, 2(k-1)j, 2^m kj, (2^m k + 2)j, \ldots, (2^m k + 2(k-1))j\}$ for some $j \in [1, 2^m k]$

TABLE I

EXAMPLES OF PERFECT $B[-k_1, k_2](p)$ SETS FROM COROLLARY 14

k_1	k_2	m	p
1	3	2	241, 1489, 3793, 17041, 22993, 26161, 33457, 35569, 39313, 45553
1	3	3	19681, 29473, 34273, 79777, 88609, 88801, 96097, 97441, 142369, 155809
1	3	4	577, 13249, 20161
1	5	2	34729
2	4	2	313, 6073, 11497, 12889, 23497, 34057, 36313, 42409, 46633, 49081
2	4	3	38449, 77041, 79633
3	5	2	78241
2	6	3	307009

TABLE II

EXAMPLES OF PERFECT $B[-k, k](p)$ SETS FROM COROLLARY 15

k	m	p
6	2	134161, 189169
6	3	86689

and $\gcd(j, 2^{m+1}k) = 1$. Then the result follows by taking $A' = \{2kji_1 + i_2 : \ i_1 \in [0, 2^{m-1} - 1],\ i_2 \in [0, 1]\}$. ■

Combining Theorems 10, 11 and Lemma 13, we have the following two corollaries.

Corollary 14: Let $m \geqslant 1$, $p = 2^m(k_1+k_2)n+1$ be a prime, k_1+k_2 be even and g be a primitive root modulo p. If $\{\mathrm{ind}_g(i) \pmod{(k_1 + k_2)2^m} : i \in [-k_1, k_2]^*\}$ *is contained in* $S(k_1 + k_2, (k_1+k_2)2^m)$*, then there exists a perfect* $B[-k_1, k_2](p)$ *set.*

Corollary 15: Let $m \geqslant 1$, $p = 2^{m+1}kn + 1$ be a prime, k be an even integer and g be a primitive root modulo p. If $\{\mathrm{ind}_g(i) \pmod{2^m k} : i \in [1, k]\}$ *is contained in* $S(k, 2^m k)$*, then there exists a perfect* $B[-k, k](p)$ *set.*

Tables I and II list some parameters for which the conditions of Corollaries 14 and 15 are satisfied, respectively. Combining Theorem 5, Tables I and II, we can obtain infinitely many new perfect splitter sets.

B. Nonexistence of Perfect Splitter Sets

In this section, we give some nonexistence results of perfect splitter sets by 1-fold factorizations of groups. A subset $A \subseteq \mathbb{Z}_n$ is said to be *periodic* if its stabilizer $N(A) = \{g \in \mathbb{Z}_n : A + g = A\}$ is a nontrivial subgroup of $\mathbb{Z}_n$. The following result of periodic sets of cyclic groups can be found in [31].

Lemma 16 [31, Ths. 4.4, 4.5, and 4.6]: Assume that $\mathbb{Z}_n = A + B$ is a 1-fold factorization. If

1) *$|A|$ is a prime power, or*
2) *n is a divisor of one of the numbers: $u^e v$, u^2v^2, u^2vw, $uvwz$, where u, v, w, z are primes and e is a positive integer,*

then A or B is periodic.

Now we have the following necessary condition for perfect splitter sets.

Theorem 17: Let $p = (k_1 + k_2)m + 1$ be a prime number and g be a primitive element modulo p. Assume that

1) *$k_1 + k_2$ is a prime power, or*
2) *$p - 1$ is a divisor of one of the numbers: $u^e v$, u^2v^2, u^2vw, $uvwz$, where u, v, w, z are primes and e is a positive integer.*

Let $A = \{\mathrm{ind}_g(i) : \ i \in [-k_1, k_2]^*\}$. If there exists a perfect $B[-k_1, k_2](p)$ set, then $A \pmod{(k_1 + k_2)l}$ is a periodic subset of size $(k_1 + k_2)$ in $\mathbb{Z}_{(k_1+k_2)l}$ for some $l|m$.

Proof: The proof is by induction on factors of m.

If A is periodic in $\mathbb{Z}_{(k_1+k_2)m}$, then we are done. If not, since there exists a perfect $B[-k_1, k_2](p)$ set, there exists a set C of size m such that $A + C = \mathbb{Z}_{p-1}$. Note that $|A| = k_1 + k_2$ is a prime power or $p-1$ is a divisor of one of the numbers: $u^e v$, u^2v^2, u^2vw, $uvwz$, where u, v, w, z are primes and e is a positive integer. Then by Lemma 16, C is periodic in $\mathbb{Z}_{(k_1+k_2)m}$. So there exists an element $e \in \mathbb{Z}^*_{(k_1+k_2)m}$ such that $C+e = C$, hence C is the union of some cosets of $\langle e\rangle$, where $\langle e\rangle$ is the subgroup of $\mathbb{Z}_{(k_1+k_2)m}$ generated by e. We can write C as $C = \langle e\rangle + D$, where D is the set of representatives of the cosets. Then $\mathbb{Z}_{(k_1+k_2)m} = A + \langle e\rangle + D$. Assume $|\langle e\rangle| = s$, we have $s|m$ since $s|D| = m$. Then $\mathbb{Z}_{(k_1+k_2)\frac{m}{s}} = A + D$, where the sets A and D are modulo $(k_1 + k_2)\frac{m}{s}$. If A is periodic in $\mathbb{Z}_{(k_1+k_2)\frac{m}{s}}$, then we are done by taking $l = \frac{m}{s}$. If not, we repeat the above step until it stops. Since m is finite, there exists an $l|m$ such that $A \pmod{(k_1 + k_2)l}$ is a periodic subset of size $(k_1 + k_2)$ in $\mathbb{Z}_{(k_1+k_2)l}$. ■

Theorem 18: Suppose that $k_1 + k_2$ is an odd prime, $1 \leqslant k_1 < k_2$, then there does not exist a nonsingular perfect $B[-k_1, k_2](n)$ set.

Proof: If there exists a nonsingular perfect $B[-k_1, k_2](n)$ set, then $\gcd(n, k_2!) = 1$. By Theorem 4, for any prime $p|n$, there exists a perfect $B[-k_1, k_2](p)$ set. Hence we only need to show that there does not exist a perfect $B[-k_1, k_2](p)$ set for any prime $p \equiv 1 \pmod{k_1 + k_2}$. Let g be a primitive root modulo p and $a = k_1 + k_2$. If there exists a perfect $B[-k_1, k_2](p)$ set, then $A = \{\mathrm{ind}_g(i) : \ i \in [-k_1, k_2]^*\}$ is periodic in $\mathbb{Z}_{al}$ for some l satisfying $al|(p - 1)$. Since $|A| = a$ is a prime number and $\mathrm{ind}_g(1) = 0 \in A$, we have $A \pmod{al} = \{il : \ i \in [0, a - 1]\}$.

Assume $p-1 = alr$. Note that $\mathrm{ind}_g(-1) = \frac{p-1}{2} = \frac{alr}{2} \in A$. Then $\frac{alr}{2} \equiv sl \pmod{al}$ for some $0 < s \leqslant a - 1$. Hence $al|(\frac{alr}{2} - sl)$, therefore $a|(\frac{ar}{2} - s)$. Since a is odd, then $2|r$ and $a|s$, which is a contradiction. ■

By Theorem 17 and computer search, we also have the following result.

Theorem 19: 1) *There does not exist a perfect $B[-1,3](n)$ set for $n = 97, 457$ and 485.*

2) *There does not exist a perfect $B[-2,4](n)$ set for $n = 37, 349$ and 877.*

For $B[-1,3](n)$ set, combining Table I and Theorem 19, we have completely solved the undetermined nonsingular cases left in [33, Corollary 19].

C. Applications to Conflict-Avoiding Codes

Conflict-avoiding codes are used in the multiple-access collision channel without feedback. A codeword here is a subset I of $\mathbb{Z}_n$, and the weight of I is the size $|I|$. For a codeword I, let

$$d(I) = \{a - b \pmod{n} : \ a, b \in I\}$$

denote the set of differences between any two elements in I. Note that $0 \in d(I)$. Let $d^*(I)$ be the set of nonzero differences in $d(I)$, that is

$$d^*(I) = d(I) \backslash \{0\},$$

which is the set of differences between any two distinct elements of I. A collection of M codewords

$$C = \{I_1, I_2, \ldots, I_M\}$$

is called a *conflict-avoiding code* (CAC) of length n and weight ω if

$$d^*(I_j) \cap d^*(I_k) = \emptyset$$

for all $j \neq k$ and $|I_j| = \omega$ for all $j \in [1, M]$. We denote such a code by (n, ω)-CAC.

Example 20: Let $n = 15$, $\omega = 3$. The four codewords $\{0,5,10\}$, $\{0,1,2\}$, $\{0,7,11\}$, $\{0,6,12\}$ constitute a $(15,3)$-CAC. We can verify that the sets of nonzero differences

$$\begin{aligned} d^*(\{0,5,10\}) &= \{5,10\}, \\ d^*(\{0,1,2\}) &= \{1,2,13,14\}, \\ d^*(\{0,7,11\}) &= \{4,7,8,11\}, \\ d^*(\{0,6,12\}) &= \{3,6,9,12\}, \end{aligned}$$

are disjoint.

Given positive integers n and ω, consider the class of all CACs with length n and weight ω. A CAC in this class with maximum number of codewords is called *optimal*, and the maximal number of codewords is denoted by $M(n, \omega)$. The main problem in CAC is to determine $M(n, \omega)$ for all n and ω. Example 20 shows that $M(15, 3) \geqslant 4$.

A codeword I is called *equidifference* if the elements in I form an arithmetic progression in $\mathbb{Z}_n$, i.e.

$$I = \{0, i, 2i, \ldots, (\omega - 1)i\}$$

for some $i \in \mathbb{Z}_n$. The element i is called a *generator* of this codeword. For an equidifference codeword I generated by i, the set of differences is

$$d(I) = \{0, \pm i, \pm 2i, \ldots, \pm(\omega - 1)i\}.$$

The elements $\pm i, \pm 2i, \ldots, \pm(\omega - 1)i$ may not be distinct in $\mathbb{Z}_n$. Hence $|d^*(I)| \leqslant 2\omega - 2$, with equality holds if $\pm i, \pm 2i, \ldots, \pm(\omega - 1)i$ are all distinct. A codeword I of weight ω is *exceptional* if $|d^*(I)| < 2\omega - 2$. If all codewords in a CAC C are equidifference, then we say that C is equidifference, and the set of generators is denoted by $\Gamma(C)$.

If C is an equidifference CAC of length n and weight ω with no exceptional codeword, then the set of generators of C forms a $B[-(\omega - 1), \omega - 1](n)$ set. Conversely, if there exists a $B[-k, k](n)$ set, which is taken as the set of generators of some code C, then the corresponding code C is an equidifference CAC of length n and weight $k + 1$ with no exceptional codeword. Therefore, we have the following result.

Theorem 21: If there exists a $B[-k, k](n)$ set with size m, then $M(n, k + 1) \geqslant m$.

The following result is similar to Theorem 5, which is a recursive construction for CACs.

Theorem 22 [23, Th. 6.1]: Let $\omega \geqslant 3$, and n_1, n_2 and s be positive integers such that n_1 is divisible by s and $gcd(l, n_2) = 1$ for all $l \in [2, \omega - 1]$. Let C_1 be an equidifference (n_1, ω)-CAC consisting of m_1 nonexceptional codewords $I_1, \ldots, I_{m_1}$ so that

$$\mathbb{Z}_{n_1} \backslash \cup_{j=1}^{m_1} d^*(I_j) \supseteq \frac{n_1}{s} \mathbb{Z}_{n_1}.$$

Let C_2 be an equidifference (sn_2, ω)-CAC with m_2 codewords. The code C of length $n_1 n_2$ generated by

$$\begin{aligned} \Gamma(C) = \{&i + jn_1 : i \in \Gamma(C_1), \ \ j \in [0, n_2 - 1]\} \\ &\cup \{(n_1/s)k : k \in \Gamma(C_2)\} \end{aligned}$$

is an equidifference $(n_1 n_2, \omega)$-CAC with $m_1 n_2 + m_2$ codewords.

Given a subset $I \subseteq \mathbb{Z}_n$, recall that the stabilizer $N(I) = \{g \in \mathbb{Z}_n : I + g = I\}$ is a subgroup of $\mathbb{Z}_n$. The authors in [26] showed that $d(I) \supseteq N(d(I))$ for any subset $I \subseteq \mathbb{Z}_n$. In the same paper, they gave a general upper bound on $M(n, \omega)$.

Theorem 23: [26, Corollary 5] *Let C be an (n, ω)-CAC. If there are E exceptional codewords $I_1, I_2, \ldots, I_E$ in C, then*

$$|C| \leqslant \frac{n - 1 + \sum_{j=1}^{E} (|N(d(I_j))| - 1)}{2\omega - 2}.$$

Moreover, they determined many new values of $M(n, \omega)$. Using a similar idea, we obtain the following theorem. For the sake of completeness, we give the proof.

Theorem 24: Let $\omega \geqslant 3$. Suppose n is an integer such that $n - 1$ is divisible by $2\omega - 2$ and $gcd(n, (2\omega - 2)!) = 1$. If there is a perfect $B[-(\omega - 1), \omega - 1](n)$ set and an integer t such that $\omega \leqslant t \leqslant 2\omega - 2$, and $gcd(t, (\omega - 1)!) = 1$, then $M(tn, \omega) = t\frac{n-1}{2\omega-2} + 1$.

Proof: If there exists a perfect $B[-(\omega - 1), \omega - 1](n)$ set, then there exists an equidifference (n, ω)-CAC C_1 with $\frac{n-1}{2\omega-2}$ nonexceptional codewords. Let C_2 be a trivial (t, ω)-CAC consisting of only one codeword generated by 1. Applying Theorem 22 with $s = 1$, $n_1 = n$, $n_2 = t$ to C_1 and C_2, we have a (tn, ω)-CAC with $t\frac{n-1}{2\omega-2} + 1$ codewords.

It suffices to show that any (tn, ω)-CAC contains at most $t\frac{n-1}{2\omega-2}+1$ codewords. Let C be a (tn, ω)-CAC. Suppose that there are E exceptional codewords I_j, $j \in [1, E]$, in C. For each j, let N_j be the stabilizer of $d(I_j)$. Then the size of N_j is strictly less than $2\omega-1$ since $|N_j| \leqslant |d(I_j)| \leqslant 2\omega-2$.

We claim that any subgroup G of $\mathbb{Z}_{tn}$ of size less than $2\omega-1$ is a subgroup of

$$\langle n\rangle = \{0, n, 2n, \ldots, (t-1)n\}.$$

Suppose on the contrary that there exists an element $a \in G$ which is not divisible by n. Then the order of a in $\mathbb{Z}_{tn}$ is bigger than $2\omega-2$ since $\gcd(n, (2\omega-2)!) = 1$, which contradicts to the fact that $|G| < 2\omega-1$.

Hence we have $N_j \subset \langle n\rangle$ for each j. By Theorem 23, we obtain

$$\begin{aligned}|C| &\leqslant \frac{tn-1+\sum_{j=1}^{E}(|N_j|-1)}{2\omega-2}\\ &\leqslant \frac{tn-1+t-1}{2\omega-2}\\ &\leqslant t\frac{n-1}{2\omega-2}+\frac{t-1}{\omega-1}.\end{aligned}$$

Since $\omega \leqslant t \leqslant 2\omega-2$, we conclude that $M(tn, \omega) = t\frac{n-1}{2\omega-2}+1$. ■

Since we have obtained infinitely many new perfect splitter sets in Section III-A, infinitely many new values of $M(n, \omega)$ can be determined by Theorem 24.

IV. Short k-Radius Sequences

In this section, we investigate short k-radius sequences by constructing new infinite families of k-additive sequences. We begin by reviewing some necessary techniques used in [11].

Assume that the terms of a sequence $s_0, s_1, \ldots, s_{m-1}$ are arranged in a "cyclic way", i.e. s_0 is the successor of s_{m-1}. By the *cyclic distance* between any two indices i and j, we mean the Lee metric for $\mathbb{Z}_m$, that is, $d_L(i, j) = \min(|i-j|, m-|i-j|)$. A cyclic sequence over A is a *cyclic k-radius sequence*, if every two different elements in Σ have indices of cyclic distance at most k somewhere in the sequence. We denote by $g_k(n)$ the length of the shortest cyclic k-radius sequence over an n-element alphabet. Observe that if $s_0, s_1, \ldots, s_{m-1}$ is a cyclic k-radius sequence, then $s_0, s_1, \ldots, s_{m-1}, s_0, s_1, \ldots, s_{k-1}$ is a noncyclic k-radius sequence. Hence, $g_k(n) \leqslant f_k(n) \leqslant g_k(n)+k$.

By counting the occurrences of a random element of Σ in a cyclic k-radius sequence, Bondy *et al.* [4] showed that

$$g_k(n) \geqslant n\lceil\frac{n-1}{2k}\rceil. \tag{3}$$

Bondy *et al.* [4] also showed the importance of the case $n \equiv 1 \pmod{2k}$ when constructing the shortest (cyclic) k-radius sequences.

Lemma 25 [4, Lemma 2.1]: If $g_k(n) = n\lceil\frac{n-1}{2k}\rceil$ for some $n \equiv 1 \pmod{2k}$, then

(i) $f_k(n') = n'\lceil\frac{n'-1}{2k}\rceil + R_k(n')$,

(ii) $g_k(n') = n'\lceil\frac{n'-1}{2k}\rceil$

for every n' such that $n-2k < n' \leqslant n$, where $R_k(n')$ is defined in (2).

By Lemma 25, it is reasonable to focus on constructing short k-radius sequences over an alphabet of size $n \equiv 1 \pmod{2k}$. Let $s > k$ be a positive integer and $n = 2ks+1$. A cyclic sequence $a_0, a_1, \ldots, a_{s-1}$ of elements of the cyclic group $\mathbb{Z}_n$ is called *k-additive* if for every nonzero element $a \in \mathbb{Z}_n$ the set

$$\{a_i, a_i+a_{i+1}, \ldots, a_i+a_{i+1}+\cdots+a_{i+k-1} : i \in [0, s-1]\}$$

contains exactly one of the elements a and $-a = n-a$. Note that the indices in this definition are computed modulo s. Let $\sigma := \sum_{i=0}^{s-1} a_i$. The construction of cyclic k-radius sequences from k-additive sequences was shown in the following lemma.

Lemma 26: [4, Lemma 4.1] *Let k and s be positive integers such that $k < s$ and let $n = 2ks+1$. If there exists a k-additive sequence $a_0, a_1, \ldots, a_{s-1}$ over $\mathbb{Z}_n$ such that $\gcd(\sigma, n) = d$, then there are d cyclic sequences $x^0, x^1, \ldots, x^{d-1}$ over $\mathbb{Z}_n$, each of them of length $\frac{ns}{d}$, such that every two elements of $\mathbb{Z}_n$ are at distance at most k in exactly one of these sequences and exactly once in the sequence.*

Applying Lemma 26 with $d = 1$, Lemma 25 and the lower bounds (1) and (3), it is immediate to get the following result.

Theorem 27 [4, Th. 4.2]: If there exists a k-additive sequence $a_0, a_1, \ldots, a_{s-1}$ such that $\gcd(\sigma, 2ks+1) = 1$, then

$$f_k(n) = n\lceil\frac{n-1}{2k}\rceil + R_k(n) \text{ and } g_k(n) = n\lceil\frac{n-1}{2k}\rceil$$

for every n such that $2k(s-1)+1 < n \leqslant 2ks+1$.

For every cyclic sequence x^t appearing in Lemma 26, $0 \leqslant t < d$, let $\overline{x}^t$ be the noncyclic sequence obtained from x^t by adjoining its k initial terms at the end of x^t. The length of each sequence $\overline{x}^t$ is $\frac{ns}{d}+k$. Clearly, the concatenation of the sequences $\overline{x}^t$, $t = 0, 1, \ldots, d-1$ is a noncyclic k-radius sequence of length $ns+dk$.

Theorem 28 [4, Th. 4.3]: If there exists a k-additive sequence $a_0, a_1, \ldots, a_{s-1}$ such that $\gcd(\sigma, n) = d$ and $n = 2ks+1$, then

$$g_k(n) \leqslant f_k(n) \leqslant ns+dk = n\cdot\frac{n-1}{2k}+dk.$$

By Theorems 27 and 28, the existence of a k-additive sequence of length s implies that of a (cyclic) n-ary k-radius sequence of the shortest possible or close to the shortest possible length, for certain values of n. However, there are very limited results on the existence of k-additive sequences, especially the ones satisfying Theorem 27. We summarize them in the following lemma.

Lemma 29 [1], [4], [5], [27]:

(i) *There exists a 2-additive sequence of length s for all $s \geqslant 3$. If $s \not\equiv 5 \pmod 6$ and $s \not\equiv 1916 \pmod{2190}$, then there exists a 2-additive sequence of length s such that $\gcd(\sigma, 4s+1) = 1$.*

(ii) *If k is a power of a prime, then there exists a k-additive sequence of length $k+1$ such that $\gcd(\sigma, 2k(k+1)+1) = 1$.*

(iii) *There is no 3-additive sequence of length five. There exists a 3-additive sequence of length $s \in \{4, 12, 13, 16\}$ such that $\gcd(\sigma, 6s+1) = 1$.*

By computer search, we show that there exists a k-additive sequence of length s such that $\gcd(\sigma, 2ks+1) = 1$, for $k = 2$ and $s \in \{5, 11, 17, 23, 29\}$, $k = 3$ and $6 \leqslant s \leqslant 17$, and $k = 4$ and $s \in \{5, 6, 8, 9\}$. These sequences are available upon request.

In the remainder of this section, we provide several general constructions of k-additive sequences over $\mathbb{Z}_n$, where n is a prime. The first two constructions are applications of Weil's Theorem. Given a prime $p \equiv 1 \pmod{r}$ and a primitive element $g \in \mathbb{Z}_p$, we use C_0^r to denote the multiplicative subgroup $\{g^{ir} : 0 \leqslant i < (p-1)/r\}$ of the r-th powers modulo p, and C_j^r to denote the coset of C_0^r in $\mathbb{Z}_p$, i.e., $C_j^r = g^j \cdot C_0^r$, $0 \leqslant j < r$. Here is an application of Weil's theorem on multiplicative character sums, which can be found in [6], [9], and [34].

Theorem 30 [9, Th. 3.2]: Let $p \equiv 1 \pmod{r}$ *be a prime satisfying the inequality*

$$p - \left[\sum_{i=0}^{l-2} \binom{l}{i} (l-i-1)(r-1)^{l-i}\right] \sqrt{p} - lr^{l-1} > 0.$$

Then, for any given l-tuple $(j_1, j_2, \ldots, j_l) \in [0, r-1]^l$ and any given l-tuple $(c_1, c_2, \ldots, c_l)$ of pairwise distinct elements of $\mathbb{Z}_p$, there exists an element $x \in \mathbb{Z}_p$ such that $x + c_i \in C_{j_i}^r$ for each $i \in [1, l]$.

From Theorem 30, it is immediate to have the following consequence.

Corollary 31: For any integers l and r, there exists $p \equiv 1 \pmod{r}$ large enough such that for any given l-tuple $(j_1, j_2, \ldots, j_l) \in [0, r-1]^l$ and any given l-tuple $(c_1, c_2, \ldots, c_l)$ of pairwise distinct elements of $\mathbb{Z}_p$, $x + c_i \in C_{j_i}^r$, $i \in [1, l]$ have a solution in $\mathbb{Z}_p$.

Now, we describe our constructions of k-additive sequences in the following subsections according to their lengths.

A. Lengths mk With Odd m

Before giving the general construction, we illustrate our main idea by constructing 3-additive sequences.

Let $n = 36t + 19 = 6(6t+3) + 1$ be a prime for some integer t, and let g be a primitive element of $\mathbb{Z}_n$. We would like to construct a 3-additive sequence of length $6t + 3$ of the form

$$1, x, y, h, hx, hy, \ldots, h^{2t}, h^{2t}x, h^{2t}y,$$

where $h = g^{18}$ for some $x, y \in \mathbb{Z}_n$. By the definition of 3-additive sequences, we need the union M of the multisets

$$\{1, x, y, h, hx, hy, \ldots, h^{2t}, h^{2t}x, h^{2t}y\},$$
$$\{1+x, x+y, y+h, h+hx, hx+hy, \ldots, h^{2t} + h^{2t}x, h^{2t}x + h^{2t}y, h^{2t}y + 1\} \text{ and}$$
$$\{1+x+y, x+y+h, y+h+hx, h+hx+hy, \ldots, h^{2t} + h^{2t}x + h^{2t}y, h^{2t}x + h^{2t}y + 1, h^{2t}y + 1 + x\}$$

to contain exactly one of the elements $\pm a$. Let $R = \{1, x, y, x+1, x+y, y+h, 1+x+y, x+y+h, y+h+hx\}$, then $M = R \cdot C_0^{18}$. Since $-1 = g^{18t+9} \notin C_0^{18}$, if R is a representative system for the coset classes in $\{C_i^9 : i \in [0, 8]\}$, then M contains exactly one of the elements $\pm a$. We apply Corollary 31 separately to find elements x and y, which are combined to satisfy this required condition of R. Since 0 and 1 are distinct elements in $\mathbb{Z}_n$, by Corollary 31, there exists an element $x \in \mathbb{Z}_n$ such that $x \in C_1^9$ and $x + 1 \in C_2^9$ if n is sufficiently large. Next, we need to find the element y such that $\{y, y+x, y+h, y+x+1, y+x+h, y+h+hx\}$ is a representative system for the coset classes in $\{C_i^9 : i \in [3, 8]\}$. Since $x \in C_1^9$, $x + 1 \in C_2^9$ and $h \in C_0^9$, it is easy to check that elements in $\{0, x, h, x+1, x+h, h+hx\}$ are all distinct. Then by Corollary 31, the desired element $y \in \mathbb{Z}_n$ also exists when n is sufficiently large.

Now we give our first general construction of k-additive sequences.

Theorem 32: Let k and t be positive integers, and let $n = 2k(2kt + k) + 1 = 4k^2t + 2k^2 + 1$. If n is a sufficiently large prime, then there exist $x_i \in \mathbb{Z}_n$, $i = 2, \ldots, k$, such that

$$1, x_2, x_3, \ldots, x_k, h, hx_2, \ldots, hx_k, \ldots, h^{2t}, h^{2t}x_2, \ldots, h^{2t}x_k$$

is a k-additive sequence of length $(2t+1)k$, where $h = g^{2k^2}$ and g is a primitive element of $\mathbb{Z}_n$.

Proof: Let M be the collection of sums of at most k consecutive elements in the given cyclic sequence. For convenience, let $x_1 = 1$. Then $M = R \cdot C_0^{2k^2}$, where R is the union of the following three sets:

$$\Phi_1 = \{\sum_{i=l}^{j} x_i : 1 \leqslant j \leqslant k, 1 \leqslant l \leqslant j\},$$

$$\Phi_2 = \{x_k + h\sum_{i=1}^{j} x_i : 1 \leqslant j \leqslant k-1\}, \text{ and}$$

$$\Phi_3 = \{h\sum_{i=1}^{j} x_i + \sum_{i=l}^{k} x_i : 1 \leqslant j \leqslant k-2, j+1 \leqslant l \leqslant k-1\}.$$

Note that $|\Phi_1| = \sum_{j=1}^{k} j$, $|\Phi_2| = k - 1$, $|\Phi_3| = \sum_{j=1}^{k-2}(k-1-j)$, and hence $|R| = k^2$. We need to find elements x_j, $j \in [2, k]$, such that R is a representative system for the coset classes in $C = \{C_j^{k^2} : j \in [0, k^2-1]\}$.

We partition C into k parts C_j, $j \in [1, k]$, such that $|C_j| = j$, $j \leqslant k-1$ and $|C_k| = 2k - 1 + \frac{(k-1)(k-2)}{2}$. In particular, let $C_1 = \{C_0^{k^2}\}$. We also partition R into k sets R_j, $j \in [1, k]$, such that R_j consists of all elements of R in which the largest index of unknowns is j. That is,

$$R_j = \{\sum_{i=l}^{j} x_i : 1 \leqslant l \leqslant j\}, j \in [1, k-1], \text{ and}$$
$$R_k = \{\sum_{i=l}^{k} x_i : 1 \leqslant l \leqslant k\} \cup \Phi_2 \cup \Phi_3.$$

Note that $|R_j| = |C_j|$ for all j. Further, $R_{j+1} = x_{j+1} + (R_j \cup \{0\})$ when $j < k-1$. We will find x_j one by one by Corollary 31 such that R_j is a representative system for the coset classes in C_j, $2 \leqslant j \leqslant k$, and consequently R is a representative system for those in C.

When $j = 2$, it is easy to show that there exists an element x_2 such that $x_2, x_2 + 1$ in R_2 represent coset classes

TABLE III
ELEMENTS IN R_i WHEN $k = 3$

R_1	R_2	R_3	
1	x	y	$y+g$
g	$x+1$	$y+x$	$y+g+x$
	gx	$y+x+1$	$y+g+gx$
	$g(x+1)$	gy	$g(y+g^{35})$
		$g(y+x)$	$g(y+g^{35}+x)$
		$g(y+x+1)$	$g(y+g^{35}+g^{35}x)$

in C_2 if n is sufficiently large. When $j = 3$, since $0, x_2, x_2+1$ are distinct elements, there exists an element x_3 such that x_3, x_3+x_2, x_3+x_2+1 in R_3 represent coset classes in C_3 if n is sufficiently large. Suppose that there exists an element x_j $(j < k-1)$ such that R_j is a representative system of the coset classes in C_j. Then elements in $R_j \cup \{0\}$ are all distinct, so there exists an element x_{j+1} such that elements in R_{j+1} represent coset classes in C_{j+1}. Finally, we need to find x_k such that elements in R_k represent those in C_k. Since

$$R_k = x_k + (R_{k-1} \cup \{0\} \cup (\Phi_2 - x_k) \cup (\Phi_3 - x_k)),$$

we need to show that elements in $R_k - x_k$ are all distinct. Note that the difference of any two elements in $R_k - x_k$ must have one of the forms

$$\sum_{i=j_1}^{j_2} x_i,\ h\sum_{i=j_1}^{j_2} x_i \text{ or } h\sum_{i=j_1}^{j_2} x_i \pm \sum_{i=l_1}^{l_2} x_i,$$

where $1 \leqslant j_1 \leqslant j_2 \leqslant k-1$, and $1 \leqslant l_1 \leqslant l_2 \leqslant k-1$. For any $1 \leqslant j_1 \leqslant j_2 \leqslant k-1$, we know that $\sum_{i=j_1}^{j_2} x_i$ appears in some R_j, $j < k$. So $\sum_{i=j_1}^{j_2} x_i$ and $\sum_{i=l_1}^{l_2} x_i$ are either in different coset classes or $\sum_{i=j_1}^{j_2} x_i = \pm \sum_{i=l_1}^{l_2} x_i$. But in both cases, the difference with any of the four forms can not be zero. This completes the proof. ■

B. Lengths mk With Even m

Note that the k-additive sequences constructed in Lemma 32 are of lengths which are odd multiples of k. This subsection gives a similar construction but the lengths of sequences are even multiples of k. We again begin with examples of $k = 3$ and 4.

Let $n = 72t+37 = 6(12t+6)+1$ be a prime. We construct a 3-additive sequence of length $12t+6$ of the form

$$1, x, y, g, gx, gy, g^{36}, g^{36}x, g^{36}y, g^{37}, g^{37}x, g^{37}y, \ldots, g^{72t}, g^{72t}x, g^{72t}y, g^{72t+1}, g^{72t+1}x, g^{72t+1}y,$$

where g is a primitive element of $\mathbb{Z}_n$. Let M be the collection of sums of at most three consecutive elements. Let $R = R_1 \cup R_2 \cup R_3$ which are listed in Table III. Then $M = R \cdot C_0^{36}$. We need R to be a representative system for the coset classes in $\{C_i^{18} : i \in [0, 17]\}$ as before so that M covers exactly one of the elements $\pm a$. This could be satisfied if

$$\begin{array}{l|ll} x \in C_2^{18}, & y \in C_6^{18}, & y+g \in C_{12}^{18}, \\ x+1 \in C_4^{18}, & y+x \in C_8^{18}, & y+g+x \in C_{13}^{18}, \\ & y+x+1 \in C_{10}^{18}, & y+g+gx \in C_{14}^{18}, \\ & & y+g^{35} \in C_{14}^{18}, \\ & & y+g^{35}+x \in C_{15}^{18}, \\ & & y+g^{35}+g^{35}x \in C_{16}^{18}. \end{array}$$

It is easy to show that there exists an element x such that $x \in C_2^{18}$, $x+1 \in C_4^{18}$ when n is sufficiently large by Corollary 31. To apply Corollary 31 to y, we need to prove that elements in $\{0, x, x+1, g, g+x, g+gx, g^{35}, g^{35}+x, g^{35}+g^{35}x\}$ are all distinct. Note that $x, x+1, g, g+gx, g^{35}, g^{35}+g^{35}x$ represent coset classes C_i^{18}, $i \in \{2, 4, 1, 5, 17, 3\}$. If the element x also satisfies $x+g \in C_a^{18}$ and $x+g^{35} \in C_b^{18}$, where $0 \leqslant a \neq b \leqslant 17$ and $\{a, b\} \cap \{2, 4, 1, 5, 17, 3\} = \emptyset$, then we are done. Fortunately, we could add these extra conditions when we find the element x. Since elements in $\{0, 1, g, g^{35}\}$ are distinct, there exists an element x such that $x \in C_2^{18}$, $x+1 \in C_4^{18}$, $x+g \in C_a^{18}$ and $x+g^{35} \in C_b^{18}$ when n is sufficiently large. Consequently, the desired element y exists by Corollary 31.

Note that in the above example when $k = 3$, we need extra constraints on x for the convenience to apply Corollary 31 to y. This phenomenon occurs more often in the next example and is essential in the proof of the final general construction.

Let $n = 128t+65 = 8(16t+8)+1$ be a prime. We would like to construct a 4-additive sequence of length $s = 16t+8$ of the form

$$1, x, y, z, g, gx, gy, gz, g^{64}, g^{64}x, g^{64}y, g^{64}z, g^{65}, g^{65}x, g^{65}y, g^{65}z, \ldots, g^{128t}, g^{128t}x, g^{128t}y, g^{128t}z, g^{128t+1}, g^{128t+1}x, g^{128t+1}y, g^{128t+1}z,$$

where g is a primitive element of $\mathbb{Z}_n$. Let M be the collection of sums of at most four consecutive elements in the sequence. Let $R = R_1 \cup R_2 \cup R_3 \cup R_4$ which are listed in Table IV.

Then $M = R \cdot C_0^{64}$. Now we need to find elements x, y and z such that R is a representative system of the coset classes in $\{C_i^{32} : i \in [0, 31]\}$. One of the patterns of sufficient constraints on elements in R is listed in Table V.

Now we solve x, y and z of these constraints in the following steps by Corollary 31, provided that n is sufficiently large.

(S1) There exists an element x such that $x \in C_2^{32}$ and $x+1 \in C_4^{32}$.

(S2) There exists an element y such that $y \in C_6^{32}$, $y+x \in C_8^{32}$ and $y+x+1 \in C_{10}^{32}$ since $0, x, x+1$ are distinct elements.

(S3) Finally, we need to find z to satisfy the remaining conditions in Table V. By Corollary 31, we need to show that all elements c in the form $z+c$ in Table V are distinct. We list these elements and the distribution of some of them in Table VI.

There are six elements c in Table VI that we do not know the coset classes they represent. If they form a representative system of the coset classes $C_{b_i}^{32}$, $i \in [1, 6]$, where b_i are distinct numbers in $[0, 31] \setminus \{6, 8, 10, 1, 5, 11, 31, 3, 9\}$, then elements

TABLE IV

ELEMENTS IN R_i WHEN $k = 4$

R_1	R_2	R_3	R_4		
1	x	y	z	$z+g$	$gz+g^{64}$
g	$x+1$	$y+x$	$z+y$	$z+g+y$	$wz+g^{64}+gy$
	gx	$y+x+1$	$z+y+x$	$z+g+y+x$	$gz+g^{64}+gy+gx$
	$g(x+1)$	gy	$z+y+x+1$	$z+g+gx$	$gz+g^{64}+g^{64}x$
		$g(y+x)$	gz	$z+g+gx+y$	$gz+g^{64}+g^{64}x+gy$
		$g(y+x+1)$	$g(z+y)$	$z+g+gx+gy$	$gz+g^{64}+g^{64}x+g^{64}y$
			$g(z+y+x)$		
			$g(z+y+x+1)$		

TABLE V

SUFFICIENT CONDITIONS OF ELEMENTS IN R WHEN $k = 4$

$x \in C_2^{32}$	$z \in C_{12}^{32}$	$z+g \in C_{20}^{32}$	$z+g^{63} \in C_{25}^{32}$
$x+1 \in C_4^{32}$	$z+y \in C_{14}^{32}$	$z+g+y \in C_{21}^{32}$	$z+g^{63}+y \in C_{26}^{32}$
	$z+y+x \in C_{16}^{32}$	$z+g+y+x \in C_{22}^{32}$	$z+g^{63}+y+x \in C_{27}^{32}$
$y \in C_6^{32}$	$z+y+x+1 \in C_{18}^{32}$	$z+g+gx \in C_{23}^{32}$	$z+g^{63}+g^{63}x \in C_{28}^{32}$
$y+x \in C_8^{32}$		$z+g+gx+y \in C_{24}^{32}$	$z+g^{63}+g^{63}x+y \in C_{29}^{32}$
$y+x+1 \in C_{10}^{32}$		$z+g+gx+gy \in C_{25}^{32}$	$z+g^{63}+g^{63}x+g^{63}y \in C_{30}^{32}$

TABLE VI

DISTRIBUTION OF ELEMENTS c WHEN $k = 4$

0	$g \in C_1^{32}$	$g^{63} \in C_{31}^{32}$
$y \in C_6^{32}$	$g+y \in ?$	$g^{63}+y \in ?$
$y+x \in C_8^{32}$	$g+y+x \in ?$	$g^{63}+y+x \in ?$
$y+x+1 \in C_{10}^{32}$	$g+gx \in C_5^{32}$	$g^{63}+g^{63}x \in C_3^{32}$
	$g+gx+y \in ?$	$g^{63}+g^{63}x+y \in ?$
	$g+gx+gy \in C_{11}^{32}$	$g^{63}+g^{63}x+g^{63}y \in C_9^{32}$

in Table VI are all distinct. To satisfy this, we modify (S2) as follows.

(S2') Find y such that $y \in C_6^{32}$, $y+x \in C_8^{32}$, $y+x+1 \in C_{10}^{32}$, and $y+\{g, g+x, g(1+x), g^{63}, g^{63}+x, g^{63}(1+x)\}$ represent $C_{b_i}^{32}$, $i \in [1, 6]$.

By Corollary 31, such an element y exists if elements in $\{0, x, x+1, g, g+x, g(1+x), g^{63}, g^{63}+x, g^{63}(1+x)\}$ are all distinct. This could be obtained if we go back further to (S1) and modify it as follows.

(S1') Find x such that $x \in C_2^{32}$, $x+1 \in C_4^{32}$, $x+g \in C_{a_1}^{32}$ and $x+g^{63} \in C_{a_2}^{32}$, where a_1, a_2 are different numbers in $[0, 31] \setminus \{2, 4, 1, 5, 31, 3\}$.

Since $\{0, 1, g, g^{63}\}$ are all distinct, such an element x exists by Corollary 31. Consequently, we could solve y and z by (S2') and (S3).

Now we give our second general construction of k-additive sequences.

Theorem 33: Let k and t be positive integers. Let $n = 2k(4kt+2k)+1 = 8k^2t+4k^2+1$ be a prime. If n is sufficiently large, then there exist elements $x_2, x_3, \ldots, x_k$ in $\mathbb{Z}_n$ such that the following sequence

$$1, x_2, x_3, \ldots, x_k, g, gx_2, gx_3, \ldots, gx_k,$$
$$g^{4k^2}, g^{4k^2}x_2, \ldots, g^{4k^2}x_k, g^{4k^2+1}, g^{4k^2+1}x_2, \ldots, g^{4k^2+1}x_k,$$
$$\ldots,$$
$$g^{8k^2t}, g^{8k^2t}x_2, \ldots, g^{8k^2t}x_k, g^{8k^2t+1}, g^{8k^2t+1}x_2, \ldots, g^{8k^2t+1}x_k$$

is a k-additive sequence of length $2(2t+1)k$, where g is a primitive element of $\mathbb{Z}_n$.

Proof: By the definition of k-additive sequences, we need the set M of sums of at most k consecutive elements in the sequence contains exactly one of the elements $\pm a$, for each $a \in \mathbb{Z}_n^*$. Denote $x_1 = 1$. For each $j \in [1, k]$, let

$$\Upsilon_j = \{x_j + g\sum_{i=1}^{m} x_i : 1 \leqslant m \leqslant j-1\},$$

$$\Phi_j = \{g\sum_{i=1}^{m} x_i + \sum_{i=l}^{j} x_i : 1 \leqslant m \leqslant j-2,$$
$$m+1 \leqslant l \leqslant j-1\},$$

$$\Psi_j = \{x_j + g^{4k^2-1}\sum_{i=1}^{m} x_i : 1 \leqslant m \leqslant j-1\}, \text{ and}$$

$$\Omega_j = \{g^{4k^2-1}\sum_{i=1}^{m} x_i + \sum_{i=l}^{j} x_i : 1 \leqslant m \leqslant j-2,$$
$$m+1 \leqslant l \leqslant j-1\}.$$

Define

$$R_j = \{1, g\} \times \{\sum_{i=l}^{j} x_i : 1 \leqslant l \leqslant j\}, j \in [1, k-1] \text{ and}$$

$$R_k = \{1, g\} \times \{\sum_{i=l}^{k} x_i : 1 \leqslant l \leqslant k\} \cup \Upsilon_k \cup \Phi_k \cup g\Psi_k \cup g\Omega_k.$$

Let R be the union of R_j, then $M = R \cdot C_0^{4k^2}$. Since $-1 = g^{4k^2t+2k^2} \notin C_0^{4k^2}$, we need to show that there exist elements $x_2, x_3, \ldots, x_k$ such that R is a representative system for the coset classes in $C = \{C_j^{2k^2} : j \in [0, 2k^2-1]\}$. It is easy to check that the pattern (4) (on the top of next page) of constraints on elements in R is sufficient.

Now we claim that (4) has solutions when n is sufficiently large. Let $R'_j = \{\sum_{i=l}^{j} x_i : 1 \leqslant l \leqslant j\} \cup \Upsilon_j \cup \Phi_j \cup \Psi_j \cup \Omega_j$, for each $j \leqslant k$. It is routine to check the following facts hold

$$\begin{cases}\sum_{i=l}^{j} x_i \in C_{j(j+1)-2l}^{2k^2}, & \text{for } 1\leqslant l\leqslant j,\ 1\leqslant j\leqslant k,\\ \text{elements in } \Upsilon_k\cup\Phi_k \text{ represent } C_r^{2k^2}, & k(k+1)\leqslant r\leqslant k(k+1)+\frac{k(k-1)}{2}-1, \text{ and}\\ \text{elements in } \Psi_k\cup\Omega_k \text{ represent } C_r^{2k^2}, & k(k+1)+\frac{k(k-1)}{2}-1\leqslant r\leqslant 2k^2-2.\end{cases} \tag{4}$$

$$\begin{cases}\sum_{i=l}^{j} x_i \in C_{j(j+1)-2l}^{2k^2}, \text{ for } 1\leqslant l\leqslant j, \text{ and}\\ \text{elements in } \Upsilon_j\cup\Phi_j\cup\Psi_j\cup\Omega_j \text{ represent coset classes in } C_j.\end{cases} \tag{5}$$

for all $j < k$.

$$\Upsilon_{j+1} = x_{j+1} + g\{\sum_{i=1}^{m} x_i : 1\leqslant m\leqslant j\},$$
$$\Phi_{j+1} = x_{j+1} + (\Upsilon_j\cup\Phi_j),$$
$$\Psi_{j+1} = x_{j+1} + g^{4k^2-1}\{\sum_{i=1}^{m} x_i : 1\leqslant m\leqslant j\} \text{ and}$$
$$\Omega_{j+1} = x_{j+1} + (\Psi_j\cup\Omega_j).$$

Then for each $j < k$, we have

$$R'_{j+1} = x_{j+1} + (R'_j \cup \{0\} \cup (\{g, g^{4k^2-1}\} \times\{\sum_{i=1}^{m} x_i : 1\leqslant m\leqslant j\})). \tag{6}$$

Note that $|\Upsilon_j\cup\Phi_j\cup\Psi_j\cup\Omega_j| = j(j-1)$. For each $j < k$, let

$$C_j \subset [0, 2k^2-1] \setminus (\{j(j+1)-2l : 1\leqslant l\leqslant j\} \cup \{m(m+1)-1, m(m+1)-3 : 1\leqslant m\leqslant j\})$$

such that $|C_j| = j(j-1)$. Now we will find x_j, for each $2\leqslant j\leqslant k-1$, such that elements in R'_j satisfy the constraints (5) on the top of this page.

We prove that elements x_j, $2\leqslant j < k-1$, exist by induction. When $j = 2$, $R'_2 = \{x_2, x_2+1, x_2+g, x_2+g^{4k^2-1}\}$, then there exists an element x_2 satisfying (5) by Corollary 31. Suppose that there exists an element x_j such that (5) is satisfied. By the definition of C_j, we know that elements in

$$R'_j \cup \{0\} \cup (\{g, g^{4k^2-1}\} \times \{\sum_{i=1}^{m} x_i : 1\leqslant m\leqslant j\})$$

are all distinct. Hence, by Eq. (6) and Corollary 31, there exists an element x_{j+1} such that (5) holds for $j+1$.

In particular, there exists an element x_{k-1} such that (5) holds, which means that elements in

$$R'_{k-1} \cup \{0\} \cup (\{g, g^{4k^2-1}\} \times \{\sum_{i=1}^{m} x_i : 1\leqslant m\leqslant k-1\})$$

are all distinct. Hence, by Corollary 31, there exists an element x_k such that elements in R'_k satisfy the corresponding constraints in (4).

Combining all pieces, we prove that there exist elements x_j, $2\leqslant j\leqslant k$ such that (4) holds, that is, R forms a representative system of the coset classes $C_j^{2k^2}$, $j\in[0, 2k^2-1]$. This completes the proof. ■

C. Lengths Independent of k

In the previous two subsections, we give constructions of k-additive sequences of lengths which are multiples of k. In this subsection, we provide two constructions where the lengths are independent of k.

Theorem 34: Let k and t be positive integers. Let $n = 2k(2t+1)+1 = 4kt+2k+1$ be a prime. If there exists a primitive root $g\in\mathbb{Z}_n$ such that $\{1, 1+g^{2k}, 1+g^{2k}+g^{4k}, \ldots, 1+g^{2k}+g^{4k}+\cdots+g^{2k(k-1)}\}$ is a representative system of the coset classes C_i^k, $i\in[0, k-1]$, then

$$1, g^{2k}, g^{4k}, \ldots, g^{4kt}$$

is a k-additive sequence of length $(2t+1)$.

Proof: We prove it by definition. Let $R = \{1, 1+g^{2k}, 1+g^{2k}+g^{4k}, \ldots, 1+g^{2k}+g^{4k}+\cdots+g^{2k(k-1)}\}$ and M be the collection of sums of at most k consecutive elements in the given cyclic sequence. Then $M = R\cdot C_0^{2k}$. Since $-1 = g^{2kt+k}\notin C_0^{2k}$, the fact that R is a representative system of the coset classes in $\{C_i^k : i\in[0, k-1]\}$ implies that M covers exactly one of elements $\pm a$ for each $a\in\mathbb{Z}_n^*$. ■

A slightly different version of Theorem 34 is given below, which yields sequences of even length.

Theorem 35: Let k and t be positive integers. Let $n = 2k(4t+2)+1 = 8kt+4k+1$ be a prime. If there exists a primitive root $g\in\mathbb{Z}_n$ such that $\{1, g\}\times R$ forms a representative system of the coset classes in $\{C_i^{2k} : i\in[0, 2k-1]\}$, then

$$1, g, g^{4k}, g^{4k+1}, g^{8k}, g^{8k+1}, \ldots, g^{8kt}, g^{8kt+1}$$

is a k-additive sequence of length $(4t+2)$, where R is the collection of sums of the first j terms in the sequence, $1\leqslant j\leqslant k$.

Proof: We prove it by definition. Let M be the collection of sums of at most k consecutive elements in the given cyclic sequence. Then $M = \{1, g\}\cdot R\cdot C_0^{4k}$. Since $-1 = g^{4kt+2k}\notin C_0^{4k}$, the fact that $\{1, g\}\cdot R$ is a representative system of the coset classes in $\{C_i^{2k} : i\in[0, 2k-1]\}$ implies that M covers exactly one of elements $\pm a$ for each $a\in\mathbb{Z}_n^*$. ■

Although we give two constructions of k-additive sequences in Theorems 34 and 35 based on a special primitive root of $\mathbb{Z}_n$, the proof of the existence of this special root may be beyond the authors' present knowledge in number theory. We list in Tables VII and VIII, the thirteen smallest primes n for each case, for which there exists a primitive root satisfying the corresponding conditions. In fact, for Theorem 34, we find the required primitive root of $\mathbb{Z}_n$ for all primes of n between 67 and 5000 when $k = 3$, between 521 and 5000 when $k = 4$, and between 2591 and 10000 when $k = 5$. For Theorem 35,

TABLE VII

GIVEN k, THE SMALLEST PRIMES n AND CORRESPONDING g^{2k} SATISFYING CONDITIONS OF LEMMA 34

$k=3$	n	67	79	103	127	139	151	163	199	211	223	271	283	307
	g^6	22	46	34	47	6	20	6	8	5	4	31	61	4
$k=4$	n	73	137	233	313	409	521	569	601	617	761	809	857	937
	g^8	2	38	32	256	77	143	16	9	83	34	256	62	16
$k=5$	n	211	311	431	571	751	911	971	1031	1091	1151	1171	1231	1471
	g^{10}	73	13	32	309	32	450	167	211	5	397	208	339	475

TABLE VIII

GIVEN k, THE SMALLEST PRIMES n AND CORRESPONDING g SATISFYING CONDITIONS OF LEMMA 35

$k=3$	n	229	349	373	397	541	613	661	709	733	757	829	853	877
	g	28	212	99	18	383	5	195	17	84	152	445	526	735
$k=4$	n	401	1361	1489	1553	1777	1873	2129	2161	2417	2609	2801	2833	2897
	g	132	159	359	243	566	499	311	336	119	207	279	442	281
$k=5$	n	1621	2621	2741	3061	4621	5101	5621	5821	5861	5981	6101	6301	6661
	g	219	1213	1872	2139	1641	2278	1328	4351	4383	918	431	2639	739

the required primitive root of $\mathbb{Z}_n$ exists for all primes of n between 541 and 10000 when $k = 3$, and between 3697 and 20000 when $k = 4$. Our experimental results may suggest positive answers for both cases when n is a sufficiently large prime.

Before closing this section, we note that for all the k-additive sequences constructed in this section, $\gcd(\sigma, n) = n$. Hence, by Lemma 28, an upper bound $f_k(n) \leqslant \frac{n(n-1)}{2k} + nk$ is obtained for these values of n. Other more complicated schemata have produced more k-additive sequences that are not worth mentioning here.

V. CONCLUDING REMARKS

In this paper, we are devoted to the constructions of splitter sets and k-radius sequences. They are connected by a construction of short k-radius sequences from splitter sets. For splitter sets, we present some new constructions of perfect splitter sets, as well as some nonexistence results on them. It should be noted that we have given a necessary condition for perfect splitter sets $B[-k_1, k_2](p)$ (p is a prime) with certain parameters in Theorem 17. That is, the set $A = \{\text{ind}_g(i) : i \in [-k_1, k_2]^*\}$ (g is a primitive element modulo p) is a periodic set of size $|A|$ when restricted in some subgroup $\mathbb{Z}_{(k_1+k_2)l}$ of $\mathbb{Z}_{p-1}$. To the best of our knowledge, this property is satisfied for all the known constructions of nonsingular perfect splitter sets. Hence we put forward the following problem.

Problem 36: Let p be a prime number and $1 \leqslant k_1 \leqslant k_2$, if there exists a perfect splitter set $B[-k_1, k_2](p)$, then it is not clear whether the following conclusion holds or not. That is, there exists an integer l with $(k_1 + k_2)l|(p - 1)$ and a primitive element g modulo p, such that the set $A = \{\text{ind}_g(i) : i \in [-k_1, k_2]^*\}$ is a periodic set of size $|A|$ in the subgroup $\mathbb{Z}_{(k_1+k_2)l}$.

For k-radius sequences, we give two constructions of k-additive sequences by applying Weil's theorem, which shows that for any fixed k, there exist infinitely many values of n such that $f_k(n) = \frac{n^2}{2k} + O(n)$. This result partially answers a conjecture recently proposed by Bondy, Lonc and Rzążewski. Note that a recent paper [22] by Lonc shows a similar result from the existence of difference families. We also present some constructions based on the existence of special primitive roots modulo some prime under certain conditions. Our experimental results may suggest that when the prime is sufficiently large, there always exist such primitive roots satisfying conditions especially in Theorems 34 and 35.

ACKNOWLEDGMENTS

The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of the presentation of this paper, and to Prof. Moshe Schwartz, the associate editor, for his excellent editorial job.

REFERENCES

[1] D. W. Bange and A. E. Barkauskas, "Sequentially additive graphs," *Discrete Math.*, vol. 44, no. 3, pp. 235–241, 1983.

[2] S. R. Blackburn, "The existence of k-radius sequences," *J. Combinat. Theory Ser. A*, vol. 119, no. 1, pp. 212–217, 2012.

[3] S. R. Blackburn and J. F. McKee, "Constructing k-radius sequences," *Math. Comput.*, vol. 81, no. 280, pp. 2439–2459, 2012.

[4] A. Bondy, Z. Lonc, and P. Rzazzewski, "Constructing optimal k-radius sequences," *SIAM J. Discrete Math.*, vol. 30, no. 1, pp. 452–464, 2016.

[5] A. Bondy, Z. Lonc, and P. Rzazzewski, "Erratum: Constructing optimal k-radius sequences," *SIAM J. Discrete Math.*, vol. 31, no. 1, pp. 645–646, 2017.

[6] M. Buratti, "Cyclic designs with block size 4 and related optimal optical orthogonal codes," *Designs Codes Cryptogr.*, vol. 26, no. 1, pp. 111–125, 2002.

[7] S. Buzaglo and T. Etzion, "Tilings with n-dimensional chairs and their applications to asymmetric codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1573–1582, Mar. 2013.

[8] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes for asymmetric limited-magnitude errors with application to multilevel flash memories," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1582–1595, Apr. 2010.

[9] Y. Chang and L. Ji, "Optimal $(4up, 5, 1)$ optical orthogonal codes," *J. Combinat. Des.*, vol. 12, no. 5, pp. 346–361, 2004.

[10] Y. M. Chee, S. Ling, Y. Tan, and X. Zhang, "Universal cycles for minimum coverings of pairs by triples, with application to 2-radius sequences," *Math. Comp.*, vol. 81, no. 277, pp. 585–603, 2012.

[11] M. Debski and Z. Lonc, "Sequences of large radius," *Eur. J. Combin.*, vol. 41, pp. 197–204, Oct. 2014.

[12] M. Debski, Z. Lonc, and P. Rzazewski, "Sequences of radius k for complete bipartite graphs," in *International Workshop on Graph-Theoretic Concepts in Computer Science*. Heidelberg, Germany: Springer, 2016, pp. 1–12.

[13] N. Elarief and B. Bose, "Optimal, systematic, q-ary codes correcting all asymmetric and symmetric errors of limited magnitude," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 979–983, Mar. 2010.

[14] S. P. Ghosh, "Consecutive storage of relevant records with redundancy," *Commun. ACM*, vol. 18, no. 8, pp. 464–471, 1975.

[15] D. Hickerson and S. Stein, "Abelian groups and packing by semicrosses," *Pacific J. Math.*, vol. 122, no. 1, pp. 95–109, 1986.

[16] J. W. Jaromczyk and Z. Lonc, "Sequences of radius k: How to fetch many huge objects into small memory for pairwise computations," in *Algorithms Computer* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2004, pp. 594–605.

[17] J. W. Jaromczyk, Z. Lonc, and M. Truszczyński, "Constructions of asymptotically shortest k-radius sequences," *J. Combinat. Theory Ser. A*, vol. 119, no. 3, pp. 731–746, 2012.

[18] T. Kløve, B. Bose, and N. Elarief, "Systematic, single limited magnitude error correcting codes for flash memories," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4477–4487, Jul. 2011.

[19] T. Kløve, J. Luo, I. Naydenova, and S. Yari, "Some codes correcting asymmetric errors of limited magnitude," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7459–7472, Nov. 2011.

[20] T. Kløve, J. Luo, and S. Yari, "Codes correcting single errors of limited magnitude," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2206–2219, Apr. 2012.

[21] R. Lidl and H. Niederreiter, *Finite Fields* (Encyclopedia of Mathematics and its Applications), 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[22] Z. Lonc, "Note on a construction of short k-radius sequences," *Discrete Math.*, vol. 340, no. 3, pp. 504–507, 2017.

[23] K. Momihara, M. Müller, J. Satoh, and M. Jimbo, "Constant weight conflict-avoiding codes," *SIAM J. Discrete Math.*, vol. 21, no. 4, pp. 959–979, 2007.

[24] M. Schwartz, "Quasi-cross lattice tilings with applications to flash memory," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2397–2405, Apr. 2012.

[25] M. Schwartz, "On the non-existence of lattice tilings by quasi-crosses," *Eur. J. Combinat.*, vol. 36, pp. 130–142, Feb. 2014.

[26] K. W. Shum, W. S. Wong, and C. S. Chen, "A general upper bound on the size of constant-weight conflict-avoiding codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3265–3276, 2010.

[27] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, vol. 43, no. 3, pp. 377–385, 1938.

[28] S. K. Stein, "Factoring by subsets," *Pacific J. Math.*, vol. 22, no. 3, pp. 523–541, 1967.

[29] S. K. Stein, "Packings of R^n by certain error spheres," *IEEE Trans. Inf. Theory*, vol. 30, no. 2, pp. 356–363, Mar. 1984.

[30] S. Stein and S. Szabo, "Algebra and tiling," in *Carus Mathematical Monographs* (Mathematical Association of America). Washington, DC, USA: The Mathematical Association of America, 1994.

[31] S. Szabo and A. D. Sands, *Factoring Groups Into Subsets* (Lecture Notes in Pure and Applied Mathematics). Boca Raton, FL, USA: CRC Press, 2009.

[32] S. Yari, T. Kløve, and B. Bose, "Some codes correcting unbalanced errors of limited magnitude for flash memories," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7278–7287, Nov. 2013.

[33] T. Zhang and G. Ge, "New results on codes correcting single error of limited magnitude for flash memory," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4494–4500, Aug. 2016.

[34] X. Zhang and G. Ge, "Existence of Z-cyclic 3PDTWh(p) for prime p ≡ 1 (mod 4)," *Designs, Codes Cryptogr.*, vol. 45, no. 1, pp. 139–155, 2007.

Tao Zhang is currently a Ph.D. student at Zhejiang University, Hangzhou, Zhejiang, P. R. China. His research interests include combinatorial design theory, coding theory, algebraic combinatorics, and their interactions.

Xiande Zhang received the Ph.D. degree in mathematics from Zhejiang University, Hangzhou, Zhejiang, P. R. China in 2009. From 2009 to 2015, she held postdoctoral positions in Nanyang Technological University and Monash University. Currently, she is a Research Professor at School of Mathematical Sciences, University of Science and Technology of China. Her research interests include combinatorial design theory, coding theory, cryptography, and their interactions. She received the 2012 Kirkman Medal from the Institute of Combinatorics and its Applications.

Gennian Ge received the M.S. and Ph.D. degrees in mathematics from Suzhou University, Suzhou, Jiangsu, P. R. China, in 1993 and 1996, respectively. After that, he became a member of Suzhou University. He was a postdoctoral fellow in the Department of Computer Science at Concordia University, Montreal, QC, Canada, from September 2001 to August 2002, and a visiting assistant professor in the Department of Computer Science at the University of Vermont, Burlington, Vermont, USA, from September 2002 to February 2004. He was a full professor in the Department of Mathematics at Zhejiang University, Hangzhou, Zhejiang, P. R. China, from March 2004 to February 2013. Currently, he is a full professor in the School of Mathematical Sciences at Capital Normal University, Beijing, P. R. China. He is also an adjunct professor in the School of Mathematics and Information Science at Guangzhou University, Guangzhou, P. R. China. His research interests include the constructions of combinatorial designs and their applications to codes and crypts.

Dr. Ge is on the Editorial Board of Journal of Combinatorial Designs, Science China Mathematics, Applied Mathematics–A Journal of Chinese Universities. He received the 2006 Hall Medal from the Institute of Combinatorics and its Applications.