On the Nonexistence of Perfect Splitter Sets

Tao Zhang and Gennian Ge

***Abstract*— Splitter sets are closely related to lattice tilings, and have applications in flash memories and conflict avoiding codes. In this paper, we prove some nonexistence results for nonsingular perfect splitter sets. We also give some necessary conditions for the existence of purely singular perfect splitter sets. Finally, we apply these results to purely singular perfect $B[-1, k](m)$ and $B[-2, k](m)$ sets for small k. In particular, we solve completely the problems left by Schwartz (European J. Combin., vol. 36, pp.130–142, Feb. 2014).**

***Index Terms*— Splitter set, lattice tiling, flash memory, conflict avoiding code.**

I. Introduction

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

In order to improve the density of flash memories, multi-level (q-level) memory cells are used so that each cell stores $\log_2 q$ bits. 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 [3], [8].

Splitter sets were first studied in [6], [14]–[18], and [20] with connections to lattice tilings. They attracted recent attention again due to an application to error-correcting codes for non-volatile memories (see [2], [4], [8]–[13], [22], [23] 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 $-k_1 \leq e \leq k_2$. Further, splitter sets are also found to be useful in constructing conflict avoiding codes and k-radius sequences [1], [24].

Research works on perfect 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 [9]. Kløve *et al.* [10], gave a construction of perfect splitter sets for $k_1 = k_2$. Constructions of perfect splitter sets for $1 \leq k_1 < k_2$ can be found in [12], [22], and [24]. For the nonexistence results, Woldar [21] gave some necessary conditions for the existence of purely singular perfect splitter sets for $k_1 = 0$. Schwartz [12], [13] presented some general necessary conditions for the existence of perfect splitter sets for $1 \leq k_1 < k_2$. Zhang and Ge [23] showed that there does not exist a nonsingular perfect splitter set when $1 \leq k_1 < k_2$, $(k_1 + 1)k_1 > k_2$ and $k_1 + k_2$ is odd. Later, Zhang *et al.* [24] proved that there does not exist a nonsingular perfect splitter set when $1 \leq k_1 < k_2$ and $k_1 + k_2$ is an odd prime.

The goal of this paper is to continue this investigation and derive new nonexistence results for perfect splitter sets. This paper is organized as follows. In Section II, we provide some notations and results which will be used throughout the paper. In Section III, we provide our main results. Section IV concludes the paper.

II. Preliminaries

In this section we provide notations used throughout this work, and cite specific relevant results which will be used in the following sections. The following notations are fixed throughout this paper.

- Let a, b be integers such that $a \leq b$, denote
$$[a, b] = \{a, a+1, a+2, \ldots, b\} \text{ and}$$
$$[a, b]^* = \{a, a+1, a+2, \ldots, b\} \backslash \{0\}.$$
- 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 $\text{ind}_g(b)$.
- For any positive integer m, let $\mathbb{Z}_m$ be the ring of integers modulo m, $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$ and $\mathbb{Z}_m' = \{a \in \mathbb{Z}_m : \gcd(a, m) = 1\}$.

A. Splitter Sets

Let m, k_1, k_2 be positive integers with $0 \leq k_1 \leq k_2$. The set $B \subseteq \mathbb{Z}_m$ of size n is called a *splitter set* if all the sets

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

Manuscript received April 19, 2017; revised August 19, 2017; accepted August 24, 2017. Date of publication August 30, 2017; date of current version September 13, 2018. G. Ge was supported in part by the National Natural Science Foundation of China under Grant 11431003 and Grant 61571310, in part by Beijing Scholars Program, Beijing Hundreds of Leading Talents Training Project of Science and Technology, and in part by Beijing Municipal Natural Science Foundation.

The authors are with the School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China (e-mail: tzh@zju.edu.cn; gnge@zju.edu.cn).

Communicated by M. Schwartz, Associate Editor for Coding Techniques.
Digital Object Identifier 10.1109/TIT.2017.2746621

have k_1+k_2 nonzero elements, and they are disjoint. We denote such a splitter set by $B[-k_1, k_2](m)$ set. If a $B[-k_1, k_2](m)$ set of size n exists, then we have $n \leq \frac{m-1}{k_1+k_2}$. A $B[-k_1, k_2](m)$ set is called *perfect* if $n = \frac{m-1}{k_1+k_2}$. Clearly, a perfect set can exist only if $m \equiv 1 \pmod{k_1+k_2}$.

A perfect $B[-k_1, k_2](m)$ set is called *nonsingular* if $\gcd(m, k_2!) = 1$. Otherwise, the set is called *singular*. If for any prime $p|m$, there is some k with $0 < k \leq k_2$ such that $p|k$, then the perfect $B[-k_1, k_2](m)$ set is called *purely singular*. As shown in [7], the study of perfect splitter sets can be reduced to the study of nonsingular perfect splitter sets and purely singular perfect splitter sets.

The following theorem can be found in [13].

Theorem 1 [13]: If there is a perfect $B[-k_1, k_2](m)$ set and some positive integer $d|m$, $\gcd(d, k_2!) = 1$, then $(k_1+k_2)d|(m-d)$, and there is a perfect $B[-k_1, k_2](m/d)$ set.

From the above theorem, it is easy to see that if there is a nonsingular perfect $B[-k_1, k_2](m)$ set, then there is a nonsingular perfect $B[-k_1, k_2](p)$ set for each prime p dividing m.

The following lemma is a special case of [7, Th. 1.2.1].

Lemma 2 [7]: If $m|n$ and there exist both a perfect $B[-k_1, k_2](m)$ set and a perfect $B[-k_1, k_2](n)$ set, then there exists a perfect $B[-k_1, k_2](n/m)$ set.

B. 1-Fold Factorization of Group

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.

A subset $A \subseteq \mathbb{Z}_m$ is said to be *periodic* if its stabilizer $N(A) = \{g \in \mathbb{Z}_m : A + g = A\}$ is a nontrivial subgroup of $\mathbb{Z}_m$. The following two lemmas can be found in [19].

Lemma 3 ([19, Th. 3.17]): If $G = A + B$ is a 1-fold factorization and $\gcd(k, |A|) = 1$, then $G = kA + B$ is a 1-fold factorization.

Lemma 4 ([19, Th. 4.4]): Assume that $\mathbb{Z}_m = A + B$ is a 1-fold factorization. If $|A|$ is a prime power, then A or B is periodic.

Then we have the following lemma.

Lemma 5: Assume that $\mathbb{Z}_m = A + B$ is a 1-fold factorization. If $|A| = q$ is a prime power, then $A \pmod{lq}$ is a periodic subset of size q in $\mathbb{Z}_{lq}$ for some $l|\frac{m}{q}$.

Proof: Let $n = \frac{m}{q}$, the proof is by induction on factors of n. If A is periodic in $\mathbb{Z}_{nq}$, then we are done. If not, since $|A|$ is a prime power, by Lemma 4, B is periodic in $\mathbb{Z}_{nq}$. Then there exists an element $e \in \mathbb{Z}_{nq}^*$ such that $B + e = B$, hence B is the union of some cosets of $\langle e \rangle$, where $\langle e \rangle$ is the subgroup of $\mathbb{Z}_{nq}$ generated by e. We can write B as $B = \langle e \rangle + C$, where C is the set of representatives of the cosets. Then $\mathbb{Z}_{nq} = A + \langle e \rangle + C$. Assume $|\langle e \rangle| = s$, we have $s|n$ since $s|C| = n$. Then $\mathbb{Z}_{\frac{n}{s}q} = A + C$, where the sets A and C are modulo $\frac{n}{s}q$. If A is periodic in $\mathbb{Z}_{\frac{n}{s}q}$, then we are done by taking $l = \frac{n}{s}$. If not, we repeat the above step until it stops. Since n is finite, there exists an $l|n$ such that $A \pmod{lq}$ is a periodic subset of size q in $\mathbb{Z}_{lq}$. ∎

III. Nonexistence of Perfect Splitter Sets

This section serves to provide new nonexistence results for nonsingular perfect splitter sets and purely singular perfect splitter sets.

A. Nonsingular Perfect Splitter Sets

In this subsection, we first prove a conjecture which is raised in [23].

Theorem 6: There does not exist a nonsingular perfect splitter set when $1 \leq k_1 < k_2$ and $k_1 + k_2$ is odd.

Proof: By Theorem 1, 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. If there exists a perfect $B[-k_1, k_2](p)$ set B, let $A = \{\mathrm{ind}_g(i) : i \in [-k_1, k_2]^*\}$, $C = \{\mathrm{ind}_g(i) : i \in B\}$, then $\mathbb{Z}_{p-1} = A + C$. Since $|A| = k_1 + k_2$ is odd, by Lemma 3, we have $\mathbb{Z}_{p-1} = 2A + C$. Then $|2A| = |A|$. Note that $0, \frac{p-1}{2} \in A$, we have $|2A| < |A|$, which is a contradiction. ∎

For the case $k_1 = 0$ or $1 \leq k_1 \leq k_2$ and $k_1 + k_2$ is even, it seems that there always exists a nonsingular perfect $B[-k_1, k_2](n)$ set for certain n [9], [10], [12], [22], [24]. In the remainder of this subsection, we give some necessary and sufficient conditions for the existence of a nonsingular perfect $B[-k_1, k_2](n)$ set for certain k_1 and k_2. The following theorem partially affirms Conjecture 11 of [23].

Theorem 7: Let p, k be odd primes, g be a primitive root modulo p and $\mu = gcd\{ind_g(j) : j \in [-1, k]^*\}$. Then there exists a perfect $B[-k, k](p)$ set if and only if

$$p \equiv 1 \pmod{2\mu k} \text{ and } |\{\frac{ind_g(j)}{\mu} \pmod{k} : j \in [1, k]\}| = k.$$

Proof: If $p \equiv 1 \pmod{2\mu k}$ and $|\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod{k} : j \in [1, k]\}| = k$, then the existence result follows from [10, Th. 2].

Suppose B is a perfect $B[-k, k](p)$ set. Let $A = \{\mathrm{ind}_g(j) : j \in [-k, k]^*\}$, $A' = \{\mathrm{ind}_g(j) : j \in [1, k]\}$ and $C = \{\mathrm{ind}_g(j) : j \in B\}$. Then $\mathbb{Z}_{p-1} = A + C$ and $A = A' + \{0, \frac{p-1}{2}\}$. Hence $\mathbb{Z}_{p-1} = A' + \{0, \frac{p-1}{2}\} + C$. Therefore $\mathbb{Z}_{\frac{p-1}{2}} = A' + C$. Note that $|A'| = k$ is an odd prime, by Lemma 5, there exists an integer l such that $kl|\frac{p-1}{2}$ and A' is periodic in $\mathbb{Z}_{kl}$. Then there exists an element $e \in \mathbb{Z}_{kl}^*$ such that $A' + e = A'$, hence A' is the union of some cosets of $\langle e \rangle$, where $\langle e \rangle$ is the subgroup of $\mathbb{Z}_{kl}$ generated by e. We can write A' as $A' = \langle e \rangle + D$, where D is the set of representatives of the cosets. Then $|A'| = |\langle e \rangle| \cdot |D| = k$ is an odd prime. Note that $e \in \mathbb{Z}_{kl}^*$, then $|\langle e \rangle| = k$ and D has only one element. Since $\mathrm{ind}_g(1) = 0$, we have $A' \pmod{kl} = \{il : i \in [0, k-1]\}$. Then $l = \mu$ and

$$p \equiv 1 \pmod{2\mu k} \text{ and } |\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod{k} : j \in [1, k]\}| = k.$$

∎

Similarly, we have the following result.

Theorem 8: Let p, k be odd primes, g be a primitive root modulo p and $\mu = gcd\{ind_g(j) : j \in [1, k]\}$. Then there exists a perfect $B[1, k](p)$ set if and only if

$$p \equiv 1 \pmod{\mu k} \text{ and } |\{\frac{ind_g(j)}{\mu} \pmod{k} : j \in [1, k]\}| = k.$$

Proof: If $p \equiv 1 \pmod{\mu k}$ and $|\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod k : j \in [1,k]\}| = k$, then the existence result follows from [9, Th. 4].

Suppose B is a perfect $B[1,k](p)$ set. Let $A = \{\mathrm{ind}_g(j) : j \in [1,k]\}$ and $C = \{\mathrm{ind}_g(j) : j \in B\}$. Then $\mathbb{Z}_{p-1} = A + C$. Note that $|A| = k$ is an odd prime, by Lemma 5, there exists an integer l such that $kl|(p-1)$ and A is periodic in $\mathbb{Z}_{kl}$. Then there exists an element $e \in \mathbb{Z}_{kl}^*$ such that $A + e = A$, hence A is the union of some cosets of $\langle e\rangle$, where $\langle e\rangle$ is the subgroup of $\mathbb{Z}_{kl}$ generated by e. We can write A as $A = \langle e\rangle + D$, where D is the set of representatives of the cosets. Then $|A| = |\langle e\rangle| \cdot |D| = k$ is an odd prime. Note that $e \in \mathbb{Z}_{kl}^*$, then $|\langle e\rangle| = k$ and D has only one element. Since $\mathrm{ind}_g(1) = 0$, we have $A \pmod{kl} = \{il : i \in [0, k-1]\}$. Then $l = \mu$ and

$$p \equiv 1 \pmod{\mu k} \text{ and } |\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod k : j \in [1,k]\}| = k.$$

■

Remark 9: In Theorems 7 and 8, the number μ does not depend on the choice of g [9], [10].

The following theorem is a general result which works for any k_1, k_2.

Theorem 10: Let p be an odd prime, $1 \le k_1 \le k_2$ be integers such that $\gcd(k_1+k_2, \frac{p-1}{k_1+k_2}) = 1$. Let g be a primitive root modulo p and $\mu = \gcd\{\mathrm{ind}_g(j) : j \in [-1,k_2]^*\}$. Then there exists a perfect $B[-k_1,k_2](p)$ set if and only if

$$p \equiv 1 \pmod{\mu(k_1+k_2)} \text{ and}$$
$$|\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod{k_1+k_2} : j \in [-k_1,k_2]^*\}| = k_1 + k_2.$$

Proof: If $p \equiv 1 \pmod{\mu(k_1+k_2)}$ and $|\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod{k_1+k_2} : j \in [-k_1,k_2]^*\}| = k_1 + k_2$, then the existence result follows from [9], [10], [22].

Suppose B is a perfect $B[-k_1,k_2](p)$ set. Let $A = \{\mathrm{ind}_g(j) : j \in [-k_1,k_2]^*\}$ and $C = \{\mathrm{ind}_g(j) : j \in B\}$. Then $\mathbb{Z}_{p-1} = A + C$. Since $\gcd(k_1+k_2, \frac{p-1}{k_1+k_2}) = 1$, by Lemma 3, we have $\mathbb{Z}_{p-1} = \frac{p-1}{k_1+k_2}A + C$. Then $|A| = |\frac{p-1}{k_1+k_2}A|$. If $\gcd(\mu, k_1+k_2) > 1$, then each of the elements in $\frac{p-1}{k_1+k_2}A$ is a multiple of $\frac{p-1}{k_1+k_2}\gcd(\mu, k_1+k_2)$. And so

$$\begin{aligned}|\frac{p-1}{k_1+k_2}A| &\le \frac{p-1}{\frac{p-1}{k_1+k_2}\gcd(\mu,k_1+k_2)}\\ &= \frac{k_1+k_2}{\gcd(\mu,k_1+k_2)}\\ &< k_1+k_2\\ &= |A|,\end{aligned}$$

which is a contradiction. Hence $\gcd(\mu, k_1+k_2) = 1$. Noting that $\mu|(p-1)$, we have $p \equiv 1 \pmod{\mu(k_1+k_2)}$.

Since $|A| = |\frac{p-1}{k_1+k_2}A|$, then for any $a, b \in A$, $\frac{p-1}{k_1+k_2}a \not\equiv \frac{p-1}{k_1+k_2}b \pmod{p-1}$, that is $a \not\equiv b \pmod{k_1+k_2}$. Since $\gcd(\mu, k_1+k_2) = 1$, then $\frac{a}{\mu} \not\equiv \frac{b}{\mu} \pmod{k_1+k_2}$. Hence we have $|\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod{k_1+k_2} : j \in [-k_1,k_2]^*\}| = k_1+k_2$. ■

B. Singular Perfect Splitter Sets

The following lemma is a generalization of [5, Th. 2.1] and the proof is similar. For the sake of completeness, we give the proof.

Lemma 11: Let k_1, k_2 be integers, $1 \le k_1 < k_2$, $k_2 \ge 3$, $n = k_1 + k_2 + 1$. If n is not a prime, then there does not exist a perfect $B[-k_1,k_2](n^2)$ set.

Proof: Assume that $\mathbb{Z}_{n^2}^* = [-k_1,k_2]^*B$. Note that the number of elements in $[-k_1,k_2]^*$ relatively prime to n is $\varphi(n)$, then the number of elements in B relatively prime to n is $\varphi(n^2)/\varphi(n) = n$. Thus $B = \{x, a_1, a_2, \cdots, a_n\}$, where $\gcd(x,n) > 1$ and $\gcd(a_i,n) = 1$ for $i = 1, \cdots, n$.

If $jn \in \mathbb{Z}_{n^2}^*$, $1 \le j \le n-1$ has the form ia_k, where $i \in [-k_1,k_2]^*$, then $jn \equiv ia_k \pmod{n^2}$. Thus $n|i$, contradicting the fact that $|i| \le k_2 < n$. Consequently $n, 2n, \cdots, (n-1)n$ are a permutation of $-k_1x \pmod{n^2}, \cdots, -x \pmod{n^2}, x \pmod{n^2}, \cdots, k_2x \pmod{n^2}$. Thus $x = in$ for some integer $1 \le i \le n-1$. Without loss of generality, we assume that $x = n$, and then $B = \{n, a_1, a_2, \cdots, a_n\}$. We divide the proof into three cases.

Case 1 ($n = pqm$, Where p and q Are Distinct Primes, $p < q$, and $m \in \mathbb{Z}$): Let $d = q^2m$. Observe that $n < d < n^2$, $d|n^2$ while $n \nmid d$. It is easy to see that $d \not\equiv in \pmod{n^2}$. Thus assume $d \equiv ia_j \pmod{n^2}$ for some $i \in [-k_1,k_2]^*$. Let $l = \frac{n^2}{d}$, clearly $l < n$. Then we have $0 \equiv ld \equiv lia_j \pmod{n^2}$. Since $\gcd(a_j,n) = 1$, then $li \equiv 0 \pmod{n^2}$, contradicting the fact that $|i|, l < n$.

Case 2 ($n = 2^k$, Where $k \ge 3$): Assume that $[-k_1,k_2]^*\{2^k, a_1, \cdots, a_{2^k}\} = \mathbb{Z}_{2^{2k}}^*$. Then $[-k_1,k_2]^*\{a_1, \cdots, a_{2^k}\} = S$, where $S = \mathbb{Z}_{2^{2k}}\backslash(2^k\{0,1,\cdots,2^k-1\})$, the elements in $\mathbb{Z}_{2^{2k}}$ that are not multiples of 2^k. Let $T = \{a_1, \cdots, a_{2^k}\}$.

Let $p = t2^{k-1} \in S$, then t is odd. Note that there are $\varphi(2^{k+1}) = 2^k$ choices of t. Write $p = ma$, where $m \in [-k_1,k_2]^*$ and $a \in T$. Since a is odd, then m is a multiple of 2^{k-1}. Note that $|m| \le k_2 < 2^k$, then $m = 2^{k-1}$. Thus, for t odd, there exists $a \in T$ such that $t2^{k-1} \equiv 2^{k-1}a \pmod{2^{2k}}$, that is $t \equiv a \pmod{2^{k+1}}$. Since there are exactly 2^k choices of t and $|T| = 2^k$, each odd residue class mod 2^{k+1} contains exactly one element of T.

Let $q = u2^{k-2} \in S$, where u is odd. Write $q = u2^{k-2} = ma$, where $m \in [-k_1,k_2]^*$ and $a \in T$. One concludes that m is an odd multiple of 2^{k-2}, hence either $m = 2^{k-2}$ or $m = 3\cdot 2^{k-2}$ as $5 \cdot 2^{k-2} > 2^k$.

Let a_0 be an arbitrary element of T. Consider the element $9 \cdot 2^{k-2}a_0 \in S$. This element has the form $2^{k-2}a_1$ or $3 \cdot 2^{k-2}a_1$ for some $a_1 \in T$. In the second case $9 \cdot 2^{k-2}a_0 \equiv 3 \cdot 2^{k-2}a_1 \pmod{2^{2k}}$, hence $3a_0 \equiv a_1 \pmod{2^{k+2}}$. Thus the element $2^{k-2}a_1$ has two representations.

For the first case, we have $9 \cdot 2^{k-2}a_0 \equiv 2^{k-2}a_1 \pmod{2^{2k}}$, which implies $9a_0 \equiv a_1 \pmod{2^{k+2}}$. We repeat the argument with a_1 replacing a_0. We have for each positive integer r, there exists an element $a_r \in T$ such that $9^r a_0 \equiv a_r \pmod{2^{k+2}}$.

Now for each k, $9^{2^{k-2}} \equiv 2^{k+1} + 1 \pmod{2^{k+2}}$. Thus for $r = 2^{k-2}$, we have $9^r a_0 \equiv a_r \pmod{2^{k+2}}$ and then $a_0 \equiv a_r \pmod{2^{k+1}}$. Since distinct elements of T are incongruent

mod 2^{k+1}, we have $a_0 = a_r$, then $9^r a_0 \equiv a_0 \pmod{2^{k+2}}$, contradicting $q^r \equiv 2^{k+1}+1 \pmod{2^{k+2}}$.

Case 3 ($n = p^k$, Where p Is an Odd Prime and $k \geq 2$): For this case, the result follows from [18, Th. 3.2]. ∎

Lemma 12: Suppose there exists a perfect $B[-1,k](m)$ set. Suppose also there exist an integer $a > 0$ and a prime p such that $p|m$, $p|a(k+1)+1$ and $a|p-1$. Then $a(k+1)+1|m$.

Proof: Let $B = \{s_1, \cdots, s_n\}$ be a perfect $B[-1,k](m)$ set, and suppose $p|s_i$ for $1 \leq i \leq t$ and $p \nmid s_i$ for $t+1 \leq i \leq n$. We claim that for $t+1 \leq i \leq n$, $|\{j : p|js_i, j \in [-1,k]^*\}| = \frac{a(k+1)-(p-1)}{ap}$. This amounts to showing that $\alpha = \frac{a(k+1)-(p-1)}{a}$ is the largest integer less than or equal to k which is divisible by p. α is an integer follows from $a|p-1$. We have $p|\alpha$ by $p|a(1+k)+1$ and $\gcd(a,p)=1$. It is easy to see that $\alpha < k$ and the next largest integer divisible by p is $\alpha + p > k$. Hence $\langle p\rangle = \{0\} \cup \{js_i : j \in [-1,k]^*, i \in [1,t]\} \cup \{(hp)s_i : h \in [1, \frac{a(k+1)-(p-1)}{ap}], i \in [t+1,n]\}$, which gives

$$\frac{n(k+1)+1}{p} = |\langle p\rangle| = 1 + (k+1)t + \frac{a(k+1)-(p-1)}{ap}(n-t).$$

Then $(a + a(k+1)t + t - n)(1-p) = 0$. Hence $n - t = a + a(k+1)t$. Therefore $m = 1 + n(k+1) = (a(k+1)+1)(t(k+1)+1)$. ∎

Similarly, we have the following lemma.

Lemma 13: Suppose there exists a perfect $B[-2,k](m)$ set. Suppose also there exist an integer $a > 0$ and an odd prime p such that $p|m$, $p|a(k+2)+1$, $a|p-1$ and $a < p-1$. Then $a(k+2)+1|m$.

Proof: Let $B = \{s_1, \cdots, s_n\}$ be a perfect $B[-2,k](m)$ set, and suppose $p|s_i$ for $1 \leq i \leq t$ and $p \nmid s_i$ for $t+1 \leq i \leq n$. We claim that for $t+1 \leq i \leq n$, $|\{j : p|js_i, j \in [-2,k]^*\}| = \frac{a(k+2)-(p-1)}{ap}$. This amounts to showing that $\alpha = \frac{a(k+2)-(p-1)}{a}$ is the largest integer less than or equal to k which is divisible by p. α is an integer follows from $a|p-1$. We have $p|\alpha$ by $p|a(2+k)+1$ and $\gcd(a,p)=1$. It is easy to see that $\alpha < k$ and the next largest integer divisible by p is $\alpha + p > k$. Hence $\langle p\rangle = \{0\} \cup \{js_i : j \in [-2,k]^*, i \in [1,t]\} \cup \{(hp)s_i : h \in [1, \frac{a(k+2)-(p-1)}{ap}], i \in [t+1,n]\}$, which gives

$$\frac{n(k+2)+1}{p} = |\langle p\rangle| = 1 + (k+2)t + \frac{a(k+2)-(p-1)}{ap}(n-t).$$

Then $(a + a(k+2)t + t - n)(1-p) = 0$. Hence $n - t = a + a(k+2)t$. Therefore $m = 1 + n(k+2) = (a(k+2)+1)(t(k+2)+1)$. ∎

Now we have the following result.

Lemma 14: Let $k \geq 3$. If there exists a perfect $B[-1,k](m)$ set with $k+2$ composite, then either

- *$gcd(k+2, m) = 1$, or*
- *$k+2|m$ and $gcd(k+2, \frac{m}{k+2}) = 1$.*

Proof: Assume $\gcd(k+2,m) > 1$. Applying Lemma 12 with $a = 1$ and p being any prime divisor of $\gcd(k+2,m)$, we see that $k+2|m$. Since there exist both a perfect $B[-1,k](m)$ set and a perfect $B[-1,k](k+2)$ set, then there exists a perfect $B[-1,k](\frac{m}{k+2})$ set by Lemma 2. If $\gcd(k+2, \frac{m}{k+2}) > 1$, we can repeat the above argument and get a perfect $B[-1,k](\frac{m}{(k+2)^2})$ set. Then by Lemma 2, we have a perfect $B[-1,k]((k+2)^2)$ set, which contradicts Lemma 11. ∎

The following lemma is the singular version of [23, Lemma 4].

Lemma 15: Let n, k_1, k_2 be integers such that $1 \leq k_1 < k_2$. Suppose B is a perfect $B[-k_1,k_2](n)$ set. Set $\mathbb{Z}_n' = \{i : i \in \mathbb{Z}_n, gcd(i,n) = 1\}$, $M(n) = \{i : i \in [-k_1,k_2]^*, gcd(i,n) = 1\}$ and $B(n) = \{i : i \in B, gcd(i,n) = 1\}$. Then $\mathbb{Z}_n' = M(n) \cdot B(n)$ and for any $a \in \mathbb{Z}_n'$, $|B(n) \cap aM(n)| = 1$.

Proof: It is easy to see that $\mathbb{Z}_n' = M(n) \cdot B(n)$ and $\varphi(n) = |M(n)||B(n)|$. We only need to show that for each $a \in \mathbb{Z}_n'$ there is a unique pair of (b,m) with $b \in B(n)$ and $m \in M(n)$ such that $b = am$.

If there exist $b_1, b_2 \in B(n)$, $m_1, m_2 \in M(n)$ such that $b_1 = am_1$ and $b_2 = am_2$, then $m_2 b_1 = m_2 a m_1 = m_1 b_2$. Since $\mathbb{Z}_n' = M(n) \cdot B(n)$, we conclude that $b_1 = b_2$ and $m_1 = m_2$. Hence we have shown the uniqueness.

For any $b \in B(n)$, $m \in M(n)$, there exists a unique $a \in \mathbb{Z}_n'$ such that $b = am$. Since $|M(n)||B(n)| = \varphi(n)$, this means that for any $a \in \mathbb{Z}_n'$ there is a unique pair of (b,m) with $b \in B(n)$ and $m \in M(n)$ such that $b = am$. ∎

Now we apply the above general methods to purely singular perfect $B[-1,k](m)$ and $B[-2,k](m)$ sets for small k.

Theorem 16: If $k = 3, 4, 5, 6, 8, 9, 10$, then there does not exist any purely singular perfect $B[-1,k](m)$ set except for $m = 1$ and except possibly for $m = k+2$.

Proof: We prove the theorem case by case.

- $k = 3$. For this case, the result can be found in [7, Th. 2.0.5].
- $k = 4$. For this case, $m = 2^u 3^v$ for certain nonnegative integers u and v. As $k+2 = 6$, Lemma 14 tells us that $m = 1$ or 6.
- $k = 5$. For this case, $m = 5^u$ for certain nonnegative integer u since $m \equiv 1 \pmod 6$. If $u \geq 1$, by Lemma 15, there exists $B \subseteq \mathbb{Z}_{5^u}'$ such that $\mathbb{Z}_{5^u}' = B \cdot M$ and $|B \cap M| = 1$, where $\mathbb{Z}_{5^u}' = \{i : i \in \mathbb{Z}_{5^u}, \gcd(i,5) = 1\}$ and $M = \{-1, 1, 2, 3, 4\}$. Without loss of generality, assume $1 \in B$, then $-1, \pm 2, \pm 3, \pm 4 \notin B$. Taking $a = 2, -2, 3, -3, 4, -4$ in Lemma 15, we have:

  there exists exactly one of $\{6, 8\}$ contained in B,
  there exists exactly one of $\{-6, -8\}$ contained in B,
  there exists exactly one of $\{6, 9, 12\}$ contained in B,
  there exists exactly one of $\{-6, -9, -12\}$ contained in B,
  there exists exactly one of $\{8, 12, 16\}$ contained in B,
  there exists exactly one of $\{-8, -12, -16\}$ contained in B.

  If $6 \in B$, then $-6, 8, 9, 12 \notin B$, hence $-8, 16 \in B$, which contradicts $|B \cap 8M| = 1$. Similarly, if $8 \in B$, then $6, -8, 12, 16 \notin B$, hence $-6 \in B$. Then $-12 \notin B$, therefore $-16 \in B$, which contradicts $|B \cap -8M| = 1$.

Thus there does not exist any purely singular perfect $B[-1,5](m)$ set except for $m=1$.

- $k=6$. For this case, $m=2^u3^v5^w$ for certain nonnegative integers u,v,w. As $k+2=8$, Lemma 14 tells us that $2^u=1$ or 8. By Lemma 2, there exists a perfect $B[-1,6](3^v5^w)$ set. If $v\geq 1$, then there are $2\cdot 3^{v-1}5^w$ elements coprime to 3 in $\mathbb{Z}_{3^v5^w}$ while there are 5 elements coprime to 3 in $[-1,6]^*$, so $w\geq 1$. If $w\geq 1$, then there are $4\cdot 3^v5^{w-1}$ elements coprime to 5 in $\mathbb{Z}_{3^v5^w}$ while there are 6 elements coprime to 5 in $[-1,6]^*$, so $v\geq 1$. Hence $v=w=0$ or $v,w\geq 1$. If $v,w\geq 1$, then by Lemma 15, there exists $B\subseteq \mathbb{Z}'_{3^v5^w}$ such that $\mathbb{Z}'_{3^v5^w}=B\cdot M$ and $|B\cap M|=1$, where $\mathbb{Z}'_{3^v5^w}=\{i:i\in \mathbb{Z}_{3^v5^w},\gcd(i,15)=1\}$ and $M=\{-1,1,2,4\}$. Without loss of generality, assume $1\in B$, then $-1,\pm 2,\pm 4\notin B$. Since $|B\cap 2M|=1$, then $8\in B$. Similarly $-8\in B$ from $|B\cap(-2)M|=1$. This contradicts the fact that $|B\cap 8M|=1$. Thus there does not exist any purely singular perfect $B[-1,6](m)$ set except for $m=1,8$.
- $k=8$. For this case, $m=2^u5^v7^w$ for certain nonnegative integers u,v,w since $m\equiv 1 \pmod 9$. As $k+2=10$, Lemma 14 tells us that $2^u5^v=1$ or 10. By Lemma 2, there exists a perfect $B[-1,8](7^w)$ set. If $w\geq 1$, then there are $6\cdot 7^{w-1}$ elements coprime to 7 in $\mathbb{Z}_{7^w}$ while there are 8 elements coprime to 7 in $[-1,8]^*$, then $8|6\cdot 7^{w-1}$, which is a contradiction. Hence there does not exist any purely singular perfect $B[-1,8](m)$ set except for $m=1,10$.
- $k=9$. For this case, $m=3^u7^v$ for certain nonnegative integers u,v since $m\equiv 1 \pmod{10}$. If $u\geq 1$, then there are $2\cdot 3^{u-1}7^v$ elements coprime to 3 in $\mathbb{Z}_{3^u7^v}$ while there are 7 elements coprime to 3 in $[-1,9]^*$, so $v\geq 1$. If $v\geq 1$, then there are $6\cdot 3^u7^{v-1}$ elements coprime to 7 in $\mathbb{Z}_{3^u7^v}$ while there are 9 elements coprime to 7 in $[-1,9]^*$, so $u\geq 1$. Hence $u=v=0$ or $u,v\geq 1$. If $u,v\geq 1$, by Lemma 15, there exists $B\subseteq \mathbb{Z}'_{3^u7^v}$ such that $\mathbb{Z}'_{3^u7^v}=B\cdot M$ and $|B\cap M|=1$, where $\mathbb{Z}'_{3^u7^v}=\{i:i\in \mathbb{Z}_{3^u7^v},\gcd(i,21)=1\}$ and $M=\{-1,1,2,4,5,8\}$. Without loss of generality, assume $1\in B$, then $-1,\pm 2,\pm 4,\pm 5,\pm 8\notin B$. Taking $a=2,-2,4,-4$ in Lemma 15, we have:

  there exists exactly one of $\{10,16\}$ contained in B,
  there exists exactly one of $\{-10,-16\}$ contained in B,
  there exists exactly one of $\{16,20,32\}$ contained in B,
  there exists exactly one of $\{-16,-20,-32\}$ contained in B.

  If $10\in B$, then $-10,16\notin B$, hence $-16\in B$. Then $-20,32,-32\notin B$, this forces $20\in B$, which contradicts $|B\cap 10M|=1$. We can similarly do for the case $16\in B$. Thus there does not exist any purely singular perfect $B[-1,9](m)$ set except for $m=1$.
- $k=10$. For this case, $m=2^u3^v5^w7^x$ for certain nonnegative integers u,v,w,x. As $k+2=12$, Lemma 14 tells us that $2^u3^v=1$ or 12. By Lemma 2, there exists a perfect $B[-1,10](5^w7^x)$ set. If $w\geq 1$, then there are $4\cdot 5^{w-1}7^x$ elements coprime to 5 in $\mathbb{Z}_{5^w7^x}$ while there are 9 elements coprime to 5 in $[-1,10]^*$, then $9|4\cdot 5^{w-1}7^x$, which is a contradiction. Hence $w=0$. If $x\geq 1$, then there are $6\cdot 7^{x-1}$ elements coprime to 7 in $\mathbb{Z}_{7^x}$ while there are 10 elements coprime to 7 in $[-1,10]^*$, then $10|6\cdot 7^{x-1}$, which is also a contradiction. Hence there does not exist any purely singular perfect $B[-1,10](m)$ set except for $m=1,12$. ■

Theorem 17: If $k=3,4,6$, then there does not exist any purely singular perfect $B[-2,k](m)$ set except for $m=1$ and except possibly for $m=k+3$.

Proof: We prove the theorem case by case.

- $k=3$. If there exists a purely singular perfect $B[-2,3](m)$ set, then $m=2^u3^v$. If $v\geq 1$, applying Lemma 13 with $a=1$ and $p=3$, we have $6|m$. By a similar discussion as Lemma 14, we have $u\geq v$ and $v=0$ or 1. If $u>v$, by Lemma 2, there exists a purely singular perfect $B[-2,3](2^{u-v})$ set. Note that there are 2^{u-v-1} elements coprime to 2 in $\mathbb{Z}_{2^{u-v}}$ while there are 3 elements coprime to 2 in $[-2,3]^*$. We must have $3|2^{u-v-1}$, which is a contradiction. Thus there does not exist any purely singular perfect $B[-2,3](m)$ set except for $m=1,6$.
- $k=4$. Since $m\equiv 1 \pmod 6$, then it is easy to see that there does not exist any purely singular perfect $B[-2,k](m)$ set except for $m=1$.
- $k=6$. If there exists a purely singular perfect $B[-2,6](m)$ set, then $m=3^u5^v$. If $u\geq 1$, applying Lemma 13 with $a=1$ and $p=3$, we have $9|m$. By a similar discussion as Lemma 14, we have $u=0$ or 2. If $v\geq 1$, by Lemma 2, there exists a purely singular perfect $B[-2,6](5^v)$ set. Note that there are $4\cdot 5^{v-1}$ elements coprime to 5 in $\mathbb{Z}_{5^v}$ while there are 7 elements coprime to 5 in $[-2,6]^*$. We must have $7|4\cdot 5^{v-1}$, which is a contradiction. Thus there does not exist any purely singular perfect $B[-2,6](m)$ set except for $m=1,9$. ■

Remark 18: In [13], the author determined all the perfect $B[-1,3](n)$ sets for $n\leq 1001$ and perfect $B[-2,3](n)$ sets for $n\leq 1251$ except for a few cases. Note that Zhang et al. [24] have solved all the undetermined nonsingular cases left in [13] for the perfect $B[-1,3](n)$ sets with $n\leq 1001$. Combining Theorems 6, 16 and 17, we have proved that there does not exist any purely singular perfect $B[-1,3](n)$ set and there does not exist any perfect $B[-2,3](n)$ set except for $n=1,6$. Hence we have completely solved the problems left in [13].

Note that Schwartz [12] has constructed an infinite family of purely singular perfect $B[-1,2](4^l)$ sets. Based on the above results, we propose the following conjecture.

Conjecture 19: Let k_1,k_2 be integers with $1\leq k_1<k_2$ and $k_1+k_2\geq 4$, then there does not exist any purely singular perfect $B[-k_1,k_2](m)$ set except for $m=1$ and except possibly for $m=k_1+k_2+1$.

IV. Conclusion

In this paper, we are devoted to proving some nonexistence results for perfect splitter sets. The study of perfect splitter

sets can be reduced to the study of nonsingular perfect splitter sets and purely singular perfect splitter sets. For nonsingular perfect splitter sets, we show that there does not exist a nonsingular perfect $B[-k_1, k_2](m)$ set when $1 \leq k_1 < k_2$ and $k_1 + k_2$ is odd, which affirms a conjecture raised in [23]. We also give some necessary and sufficient conditions for the existence of a perfect $B[-k_1, k_2](n)$ set for $k_1 = 0$ or $1 \leq k_1 \leq k_2$ and $k_1 + k_2$ is even. For purely singular perfect splitter sets, we provide some general necessary conditions for the existence of a purely singular perfect splitter set. As an application, we apply these results to purely singular perfect $B[-1, k](m)$ and $B[-2, k](m)$ sets for small k. These results suggest that for $1 \leq k_1 < k_2$ and $k_1 + k_2 \geq 4$, there does not exist any purely singular perfect $B[-k_1, k_2](m)$ set except for $m = 1$ and except possibly for $m = k_1 + k_2 + 1$.

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] S. R. Blackburn and J. F. McKee, "Constructing k-radius sequences," *Math. Comput.*, vol. 81, no. 280, pp. 2439–2459, 2012.
[2] 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.
[3] 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.
[4] 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.
[5] S. Galovich and S. Stein, "Splittings of abelian groups by integers," *Aequationes Math.*, vol. 22, nos. 2–3, pp. 249–267, 1981.
[6] D. Hickerson and S. Stein, "Abelian groups and packing by semicrosses," *Pacific J. Math.*, vol. 122, no. 1, pp. 95–109, 1986.
[7] D. R. Hickerson, "Splittings of finite groups," *Pacific J. Math.*, vol. 107, no. 1, pp. 141–171, 1983.
[8] 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.
[9] 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.
[10] 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.
[11] S. Martirosyan, "Single-error correcting close packed and perfect codes," in *Proc. 1st INTAS Int. Seminar Coding Theory Combinat.*, 1996, pp. 90–115.
[12] M. Schwartz, "Quasi-cross lattice tilings with applications to flash memory," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2397–2405, Apr. 2012.
[13] M. Schwartz, "On the non-existence of lattice tilings by quasi-crosses," *Eur. J. Combinat.*, vol. 36, pp. 130–142, Feb. 2014.
[14] S. K. Stein, "Factoring by subsets," *Pacific J. Math.*, vol. 22, no. 3, pp. 523–541, 1967.
[15] S. K. Stein, "Packings of R^n by certain error spheres," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 2, pp. 356–363, Mar. 1984.
[16] S. Stein and S. Szabó, *Algebra and Tiling* (Carus Mathematical Monographs), vol. 25. Washington, DC, USA: MAA, 1994.
[17] S. Szabó, "Some problems on splittings of groups," *Aequationes Math.*, vol. 30, no. 1, pp. 70–79, 1986.
[18] S. Szabó, "Some problems on splittings of groups. II," *Proc. Amer. Math. Soc.*, vol. 101, no. 4, pp. 585–591, 1987.
[19] S. Szabó and A. D. Sands, *Factoring Groups into Subsets* (Lecture Notes in Pure and Applied Mathematics), vol. 257. Boca Raton, FL, USA: CRC Press, 2009.
[20] U. Tamm, "Splittings of cyclic groups and perfect shift codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 2003–2009, Sep. 1998.
[21] A. J. Woldar, "A reduction theorem on purely singular splittings of cyclic groups," *Proc. Amer. Math. Soc.*, vol. 123, no. 10, pp. 2955–2959, 1995.
[22] 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.
[23] 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.
[24] T. Zhang, X. Zhang, and G. Ge, "Splitter sets and k-radius sequences," *IEEE Trans. Inf. Theory*, to be published, doi: 10.1109/TIT.2017.2695219.

Tao Zhang received his Ph.D. degree in mathematics from Zhejiang University, Hangzhou, Zhejiang, P. R. China, in 2017. He is currently an associate professor in the School of Mathematics and Information Science at Guangzhou University, Guangzhou, P. R. China. His research interests include combinatorial design theory, coding theory, algebraic combinatorics, and their interactions.

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 combinatorics, coding theory, information security, and their interactions.

Dr. Ge is on the Editorial Board of the *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.