This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

Some New Results on Splitter Sets

Zuo Ye, Tao Zhang, Xiande Zhang and Gennian Ge

***Abstract*—Splitter sets have been widely studied due to their applications in flash memories, and their close relations with lattice tilings and conflict avoiding codes. In this paper, we give necessary and sufficient conditions for the existence of nonsingular perfect splitter sets, $B[-k_1,k_2](p)$ sets, where $0 \leq k_1 \leq k_2 = 4$. Meanwhile, constructions of nonsingular perfect splitter sets are given. When perfect splitter sets do not exist, we present four new constructions of quasi-perfect splitter sets. Finally, we give a connection between nonsingular splitter sets and Cayley graphs, and as a byproduct, a general lower bound on the maximum size of nonsingular splitter sets is given.**

***Index Terms*—Splitter set, lattice tiling, flash memory, Cayley graph.**

I. Introduction

Flash memory is a non-volatile, high-density and low-cost memory. There are many fields in which flash memory has found its applications, such as personal computers, digital audio players, digital cameras, mobile phones, embedded systems and so on.

A multilevel flash cell is electrically programmed into one of q threshold states and therefore can be regarded as storing one symbol from the set $\mathbb{Z}_q$. 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 gave a strong motivation for the application of the limited magnitude error model to flash memory [5], [12].

Splitter sets were first studied in [9], [21]–[23], [25]–[27] in the language of lattice tilings. Recently, an important application to the limited magnitude error-correcting codes for flash memories has been found [5], [12]. In this context, a code obtained from a splitter set $B[-k_1,k_2](q)$ can correct a symbol $a \in \{0,1,\cdots,q-1\}$ if it is modified into $(a+e) \pmod{q}$ during transmission, where $-k_1 \leq e \leq k_2$. This new finding has immediately motivated a lot of research on splitter sets (see [4], [7], [12]–[14], [16], [18], [19], [31], [33] and the references therein). Moreover, splitter sets are also useful in the constructions of conflict avoiding codes and k-radius sequences [2], [35].

Some researchers considered the existence of perfect splitter sets. In [13], the authors presented a construction of perfect splitter sets for $k_1 = 0$. The existence of perfect splitter sets for $k_1 = k_2$ has been studied in [14], [23]. Some constructions of perfect splitter sets for $1 \leq k_1 < k_2$ were given in [18], [31], [35]. For the nonexistence results, Woldar [28] obtained some necessary conditions for the existence of purely singular perfect splitter sets for $k_1 = 0$. In [18], [19], Schwartz gave some necessary conditions for the existence of perfect splitter sets for more general $1 \leq k_1 < k_2$. In [33]–[35], the authors 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 integer. In [32], Yuan and Zhao gave a necessary and sufficient condition for the existence of nonsingular perfect $B[-1,3](p)$ sets. For $k_1 = k_2 = 4$, Tamm [27] provided a list of primes p for which a perfect $B[-4,4](p)$ set exists. In [17], Munemasa pointed out that the subgroup $\langle -1,2,3\rangle$ plays a central role in the study of perfect $B[-4,4](p)$ sets.

Since perfect splitter sets only exist for certain parameters, other researchers also studied quasi-perfect splitter sets and optimal splitter sets. In [12], Kløve et al. gave a construction of quasi-perfect splitter sets for $k_1 = 0$. Some constructions of quasi-perfect splitter sets for $k_1 = k_2$ can be found in [14]. The authors of [33] gave a construction of quasi-perfect splitter sets for $1 \leq k_1 < k_2$. The exact size of maximal $B[-k_1,k_2](q)$ sets for $0 \leq k_1 \leq k_2 \leq 4$ and certain q can be found in [12], [14], [29]–[31].

In this work, we continue to derive new results for splitter sets. We give necessary and sufficient conditions for the existence of nonsingular perfect $B[-k_1,k_2](p)$ sets, where $(k_1,k_2) \in \{(0,4),(2,4),(4,4)\}$. We also present four new constructions of quasi-perfect splitter sets. This paper is organized as follows. In Section II, we introduce some notations and terminologies which will be used throughout the paper. In Section III, we give some necessary and sufficient conditions for the existence of nonsingular perfect $B[-k_1,k_2](p)$ sets, where $(k_1,k_2) \in \{(0,4),(2,4),(4,4)\}$. In Section IV, four new constructions of quasi-perfect splitter sets are presented. In Section V, we give a connection between nonsingular splitter sets and Cayley graphs, and by product, a lower bound on the maximum size of nonsingular splitter sets is given. Finally, section VI concludes the paper.

II. Preliminary

In this section, we introduce some useful notations and terminologies, and recall several relevant results which will be used later.

For integers m,n such that $m \leq n$, we denote $[m,n] := \{m,m+1,\ldots,n\}$ and $[m,n]^* := \{m,m+1,\ldots,n\} \setminus \{0\}$.

The research of Z. Ye and X. Zhang were supported by the National Natural Science Foundation of China under grant 11771419.

The research of T. Zhang was supported by the National Natural Science Foundation of China under grant 11801109.

The research of G. Ge was supported by the National Natural Science Foundation of China under Grant Nos. 11431003, 61571310 and 11971325, Beijing Scholars Program, Beijing Hundreds of Leading Talents Training Project of Science and Technology, and Beijing Municipal Natural Science Foundation.

Z. Ye and X. Zhang are with the School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, Anhui, China (e-mails: zyprince@mail.ustc.edu.cn; drzhangx@ustc.edu.cn).

T. Zhang is with the School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China (e-mail: taozhang@gzhu.edu.cn).

G. Ge is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China (Corresponding author, e-mail: gnge@zju.edu.cn).

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

For any integer $q \geq 2$, let $\mathbb{Z}_q$ be the ring of integers modulo q and let $\mathbb{Z}$ be the ring of integers. If a is an element of $\mathbb{Z}_q$ and S is a subset of integers, then aS denotes the set $\{as \pmod q : s \in S\}$.

Definition II.1. *Let $q, k_1, k_2 \in \mathbb{Z}$ with $q \geq 2$ and $0 \leq k_1 \leq k_2$. The set $B \subset \mathbb{Z}_q$ is called a* splitter set *if each of the sets $b\,[-k_1, k_2]^*$, $b \in B$, has $k_1 + k_2$ nonzero elements, and they are pairwise disjoint. We denote such a splitter set by a $B[-k_1, k_2](q)$ set.*

From the definition, if B is a $B[-k_1, k_2](q)$ set, then $|B| \leq \frac{q-1}{k_1+k_2}$. If $|B| = \frac{q-1}{k_1+k_2}$, then we say that B is *perfect*. It is clear that a perfect $B[-k_1, k_2](q)$ set exists only if $q \equiv 1 \pmod{k_1 + k_2}$. If $q \not\equiv 1 \pmod{k_1 + k_2}$ and $|B| = \left\lfloor \frac{q-1}{k_1+k_2} \right\rfloor$, then we say B is *quasi-perfect*. A perfect $B[-k_1, k_2](q)$ set is called *nonsingular* if $\gcd(q, k_2!) = 1$. Otherwise, it is called *singular*. The following theorems can be found in [19], [31].

Theorem II.1. [19, Theorem 14] *Suppose that there exists a perfect $B[-k_1, k_2](q)$ set. Then for any positive integer $d \mid q$ satisfying $\gcd(d, k_2!) = 1$, there is a perfect $B[-k_1, k_2](\frac{q}{d})$ set.*

Theorem II.2. [31, Theorem 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*

$$B_1 \odot B_2 = \{c + rq_1 : \; c \in B_1, r \in [0, q_2 - 1]\} \cup \{q_1 c : \; c \in B_2\}.$$

Then

1) *$B_1 \odot B_2$ is a $B\,[-k_1, k_2]\,(q_1 q_2)$ 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 factor p of q. Therefore, in Section III, when we deal with the existence of nonsingular perfect $B[-k_1, k_2](p)$ sets, we only consider the case when p is a prime. In this case, $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$ is a cyclic multiplicative group, so we don't distinguish between integers and ring elements. The following necessary condition for the existence of perfect splitter sets is quite useful, which will be used frequently later.

Lemma II.1. [33, Lemma 2.4] *Let $k_1, k_2 \in \mathbb{Z}$ with $0 \leq k_1 \leq k_2$, and p be a prime. If B is a perfect $B[-k_1, k_2](p)$ set, then for any $a \in \mathbb{Z}_p^*$, we have $|B \cap a[-k_1, k_2]^*| = 1$.*

The definition of splitter sets is closely related to the following definition from group theory.

Definition II.2. *Let $(G, \cdot)$ be a finite group and A, B be subsets of G. If for any element $g \in G$, there are unique elements $a \in A$ and $b \in B$ such that $g = a \cdot b$, then we say $G = A \cdot B$ is a* factorization *of G, and A (or B) is a* direct factor *of G.*

Remark II.1. *When $p > k_1 + k_2$ is a prime, we can view $[-k_1, k_2]^*$ as a subset of $\mathbb{Z}_p^*$. Then by the definition of perfect splitter sets and factorization, we see that B is a perfect $B[-k_1, k_2](p)$ set if and only if $\mathbb{Z}_p^* = B[-k_1, k_2]^*$ is a factorization.*

For convenience, we introduce more notations before closing this section. For a group G and a subset $S \subseteq G$, $\langle S \rangle$ denotes the subgroup of G generated by S. Suppose g is a generator of $\mathbb{Z}_p^*$, then we say that g is a *primitive root* modulo p. For any element $b \in \mathbb{Z}_p^*$, there exists a unique integer $i \in [0, p-2]$ such that $g^i \equiv b \pmod p$. We say i is the *index of b relative to the base g*, and denote it by $\mathrm{ind}_g(b)$. If $x \in \mathbb{Z}_p^*$, let $\mathrm{ord}_p(x)$ denote the order of x modulo p.

III. Nonsingular perfect $B[-k_1, k_2](p)$ sets for $k_2 = 4$

This section serves to provide complete characterizations of the existence of nonsingular perfect $B[-k_1, k_2](p)$ sets, where $(k_1, k_2) \in \{(0, 4), (2, 4), (4, 4)\}$, and $p \equiv 1 \pmod{k_1 + k_2}$ is a prime. Since there does not exist a nonsingular perfect splitter set when $1 \leq k_1 < k_2$ and $k_1 + k_2$ is an odd integer by [34], we thus completely solve the case when $k_2 = 4$.

A. Complete characterizations

Lemma III.1. *Let $k \geq 1$ be an integer, $p \equiv 1 \pmod{2k + 2}$ be a prime, and let B be a nonsingular perfect $B[-k, k+2](p)$ set. If $i \in B$, then*

$$i \left\langle -\frac{k+1}{k+2} \right\rangle \subseteq B,$$

where $\left\langle -\frac{k+1}{k+2} \right\rangle$ denotes the subgroup of $\mathbb{Z}_p^*$ generated by $-\frac{k+1}{k+2}$. In particular, the order of $-\frac{k+1}{k+2}$ in $\mathbb{Z}_p^*$ is odd.

Proof: Since B is a nonsingular perfect $B[-k, k+2](p)$ set, we have that for any $a \in \mathbb{Z}_p^*$, $|B \cap a[-k, k+2]^*| = 1$ by Lemma II.1. For any $i \in B$, taking $a = i$, we have

$$|B \cap i[-k, k+2]^*| = 1. \tag{1}$$

Since $i \in B \cap i[-k, k+2]^*$ and $-i \in i[-k, k+2]^*$, we get $-i \notin B$. Further taking $a = \pm\frac{i}{k+2}$, we have

$$\left| B \bigcap \frac{i}{k+2}[-k, k+2]^* \right| = 1, \tag{2}$$

$$\left| B \bigcap \left(-\frac{i}{k+2} \right) [-k, k+2]^* \right| = 1. \tag{3}$$

By (2) and the fact that $i \in B \bigcap \frac{i}{k+2}[-k, k+2]^*$, we get $B \bigcap \frac{i}{k+2}[-k, k+1]^* = \emptyset$. Observing that $\left(-\frac{i}{k+2}\right)[-k, k+2]^* = \left(\frac{i}{k+2}[-k, k]^*\right) \bigcup \{-\frac{k+1}{k+2}i, -i\}$, we have $-\frac{k+1}{k+2}i \in B$ by (3). Then replacing i in (1), (2) and (3) by $-\frac{k+1}{k+2}i$, and following the same arguments, we can get $i\left(-\frac{k+1}{k+2}\right)^2 \in B$. Repeating this procedure, we deduce that $i\left\langle -\frac{k+1}{k+2} \right\rangle \subseteq B$. If $\mathrm{ord}_p(-\frac{k+1}{k+2})$ is even, then $-1 \in \left\langle -\frac{k+1}{k+2} \right\rangle$, hence $-i \in B$, which is a contradiction. ■

The next lemma can be derived from Lemmas 2.3 and 2.5 of [24]. We sketch the proof here to explain how to get a perfect splitter set.

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

Lemma III.2. *Let $k_2 \geq k_1 \geq 0$ be integers, $p \equiv 1 \pmod{k_1 + k_2}$ be a prime, and $M = [-k_1, k_2]^*$. Then there is a nonsingular perfect $B[-k_1, k_2](p)$ set if and only if M is a direct factor of the subgroup $H = \langle -1, 2, \ldots, k_2 \rangle \subset \mathbb{Z}_p^*$.*

Proof: Suppose B is a nonsingular perfect $B[-k_1, k_2](p)$ set. Let $B' = B \cap H$, then it is easy to verify that $H = MB'$ is a factorization.

Now suppose $H = MB'$ is a factorization. Let $\{b_1, \cdots, b_s\}$ be a complete set of coset representatives of H in $\mathbb{Z}_p^*$. Then $B = \bigcup_{i=1}^{s} b_i B'$ is a perfect $B[-k_1, k_2](p)$ set. ■

We are now ready to present our main results.

Theorem III.1. *Let $p \equiv 1 \pmod 6$ be a prime. Then there is a nonsingular perfect $B[-2, 4](p)$ set if and only if $\operatorname{ord}_p(-\frac{3}{4})$ is odd and $2 \notin \langle 6, 8 \rangle$.*

Proof: The necessity is just a combination of Lemma III.1 and Theorem 5.8 of [33]. Now we consider the other direction. It is easy to check Equation (4) (on the top of next page). The Equation (4) implies that $\langle -1, 2, 3 \rangle \subseteq M\langle 6, -\frac{4}{3} \rangle$, where $M = [-2, 4]^*$. On the other hand, $6^s \left(-\frac{4}{3}\right)^t = (-1)^t 2^{s+2t} 3^{s-t}$ for any $s, t \geq 0$. Therefore, $\langle -1, 2, 3, 4 \rangle = \langle -1, 2, 3 \rangle = M\langle 6, -\frac{4}{3} \rangle$. Hence, by Lemma III.2, we only need to show that $\langle -1, 2, 3 \rangle = MB$ is a factorization, where

$$B = \left\langle 6, -\frac{4}{3} \right\rangle, \text{ if } \operatorname{ord}_p(6) \text{ is odd,}$$

and

$$B = \left\langle 6, -\frac{4}{3} \right\rangle / \{1, -1\}, \text{ if } \operatorname{ord}_p(6) \text{ is even.}$$

Note that if $\operatorname{ord}_p(6)$ is even, then $-1 \in \langle 6, -\frac{4}{3} \rangle$. So by $B = \langle 6, -\frac{4}{3} \rangle / \{1, -1\}$, we mean that B includes exactly one of $-i, i$ for any $i \in \langle 6, -\frac{4}{3} \rangle$.

Since $p \equiv 1 \pmod 6$, we assume that $p = 2^a 3^b c + 1$, where $a, b, c \geq 1$ and $\gcd(c, 6) = 1$. Let g be a primitive root modulo p, suppose that

$$2 \equiv g^{2^{u_1} 3^{v_1} r_1} \pmod p,$$
$$3 \equiv g^{2^{u_2} 3^{v_2} r_2} \pmod p,$$
$$-1 \equiv g^{2^{a-1} 3^b c} \pmod p,$$

where $u_1 u_2, v_1, v_2 \geq 0$, $r_1, r_2 \geq 1$, $2 \nmid r_1 r_2$, $3 \nmid r_1 r_2$, and $2^{u_1} 3^{v_1} r_1, 2^{u_2} 3^{v_2} r_2 < p - 1$.

Note that

$$\operatorname{ind}_g(4) \equiv 2 \times \operatorname{ind}_g(2) \pmod{p-1}$$

and

$$\operatorname{ind}_g(-\frac{3}{4}) \equiv 2^{u_2} 3^{v_2} r_2 - \operatorname{ind}_g(4) + 2^{a-1} 3^b c \pmod{p-1},$$

then $\operatorname{ord}_p(-\frac{3}{4})$ is odd if and only if

$$2^{u_2} 3^{v_2} r_2 - 2^{u_1+1} 3^{v_1} r_1 + 2^{a-1} 3^b c \equiv 0 \pmod{2^a}. \quad (5)$$

By equation (5), if $\min\{u_1 + 1, u_2\} \geq a$, then $2^a \mid 2^{a-1} 3^b c$, which is impossible. Similarly, if $\max\{u_1 + 1, u_2\} \geq a$, then $\min\{u_1 + 1, u_2\} = a - 1$. And if $\max\{u_1 + 1, u_2\} \leq a - 1$, then $u_1 + 1 = u_2 \leq a - 2$. Therefore, there are three cases for the possible values of u_1 and u_2:

$$\begin{cases} u_2 = a - 1, & \text{if } u_1 \geq a - 1; \\ u_2 \geq a, & \text{if } u_1 = a - 2; \\ u_2 = u_1 + 1, & \text{otherwise.} \end{cases} \quad (6)$$

Since $6 = 2 \times 3$ and $8 = 2^3$, we have

$$6 \equiv g^{2^{u_1} 3^{v_1} r_1 + 2^{u_2} 3^{v_2} r_2} \pmod p$$

and

$$8 \equiv g^{2^{u_1} 3^{v_1+1} r_1} \pmod p.$$

Let $d = \gcd\left(2^{u_1} 3^{v_1} r_1 + 2^{u_2} 3^{v_2} r_2, 2^{u_1} 3^{v_1+1} r_1\right)$. So $\langle 6, 8 \rangle = \langle g^{2^{u_1} 3^{v_1} r_1 + 2^{u_2} 3^{v_2} r_2}, g^{2^{u_1} 3^{v_1+1} r_1} \rangle = \langle g^d \rangle$. We will frequently use this fact in the rest of this proof.

Claim 1. $v_1 = v_2$.

Proof of Claim 1: We split the proof into four cases.

If $u_1 \geq u_2$ and $v_1 > v_2$, then

$$d = 2^{u_2} 3^{v_2} \gcd\left(2^{u_1-u_2} 3^{v_1-v_2} r_1 + r_2, 2^{u_1-u_2} 3^{v_1-v_2+1} r_1\right).$$

Let $r = \gcd\left(2^{u_1-u_2} 3^{v_1-v_2} r_1 + r_2, 2^{u_1-u_2} 3^{v_1-v_2+1} r_1\right)$. It is easy to see that $2 \nmid r$ and $3 \nmid r$, so $r \mid r_1$. It follows that $d \mid 2^{u_2} 3^{v_2} r_1$ and thus $d \mid 2^{u_1} 3^{v_1} r_1$. Therefore, $2 \in \langle 6, 8 \rangle$, which is a contradiction.

If $u_1 \geq u_2$ and $v_1 < v_2$, then

$$d = 2^{u_2} 3^{v_1} \gcd\left(2^{u_1-u_2} r_1 + 3^{v_2-v_1} r_2, 2^{u_1-u_2} 3 r_1\right).$$

If $u_1 < u_2$ and $v_1 > v_2$, then

$$d = 2^{u_1} 3^{v_2} \gcd\left(3^{v_1-v_2} r_1 + 2^{u_2-u_1} r_2, 3^{v_1-v_2+1} r_1\right).$$

If $u_1 < u_2$ and $v_1 < v_2$, then

$$d = 2^{u_1} 3^{v_1} \gcd\left(r_1 + 2^{u_2-u_1} 3^{v_2-v_1} r_2, 3 r_1\right).$$

Similar to the first case, each of these three cases implies that $2 \in \langle 6, 8 \rangle$, which is a contradiction. This completes the proof of Claim 1.

Claim 2. $v_1 = v_2 \leq b - 1$.

Proof of Claim 2: By computing, we have

$$|\langle -1, 2, 3 \rangle| = \frac{p-1}{\gcd(\operatorname{ind}_g(-1), \operatorname{ind}_g(2), \operatorname{ind}_g(3), p-1)} = \frac{p-1}{\gcd(2^{u_1} 3^{v_1} r_1, 2^{u_2} 3^{v_2} r_2, 2^{a-1} 3^b c)},$$

and

$$|\langle 6, 8 \rangle| = \frac{p-1}{\gcd(d, p-1)} = \frac{p-1}{\gcd(2^{u_1} 3^{v_1} r_1 + 2^{u_2} 3^{v_2} r_2, 2^{u_1} 3^{v_1+1} r_1, 2^a 3^b c)}.$$

By Claim 1, we have $v_1 = v_2$. We prove the claim by contradiction. If $v = v_1 = v_2 \geq b$. Then

$$\frac{|\langle -1, 2, 3 \rangle|}{|\langle 6, 8 \rangle|} = \frac{\gcd\left(2^{u_1} 3^v r_1 + 2^{u_2} 3^v r_2, 2^{u_1} 3^{v+1} r_1, 2^a 3^b c\right)}{\gcd(2^{u_1} 3^v r_1, 2^{u_2} 3^v r_2, 2^{a-1} 3^b c)} = \frac{\gcd\left(2^{u_1} 3^{v-b} r_1 + 2^{u_2} 3^{v-b} r_2, 2^{u_1} 3^{v-b+1} r_1, 2^a c\right)}{\gcd(2^{u_1} 3^{v-b} r_1, 2^{u_2} 3^{v-b} r_2, 2^{a-1} c)}.$$

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

$$(-1)^x 2^y 3^z = \begin{cases} (-1)^{x+\frac{y-z}{3}} \cdot 6^{\frac{y+2z}{3}} \left(-\frac{4}{3}\right)^{\frac{y-z}{3}}, & \text{if } y \equiv z \pmod 3, \\ (-1)^{x+\frac{y-z-1}{3}} \cdot 2 \cdot 6^{\frac{y+2z-1}{3}} \left(-\frac{4}{3}\right)^{\frac{y-z-1}{3}}, & \text{if } y \equiv z+1 \pmod 3, \\ 3 \cdot 6^{\frac{y+2z-2}{3}} \left(-\frac{4}{3}\right)^{\frac{y-z+1}{3}}, & \text{if } y \equiv z+2 \pmod 3 \text{ and } x + \frac{y-z+1}{3} \text{ is even}, \\ 4 \cdot 6^{\frac{y+2z-2}{3}} \left(-\frac{4}{3}\right)^{\frac{y-z-2}{3}}, & \text{if } y \equiv z+2 \pmod 3 \text{ and } x + \frac{y-z+1}{3} \text{ is odd}. \end{cases} \tag{4}$$

If $u_1 + 1 = u_2 \le a - 2$, then

$$\begin{aligned} &\frac{|\langle -1,2,3\rangle|}{|\langle 6,8\rangle|} \\ =&\frac{\gcd\left(3^{v-b}r_1 + 2\cdot 3^{v-b}r_2, 3^{v-b+1}r_1, 2^{a-u_1}c\right)}{\gcd\left(3^{v-b}r_1, 2\cdot 3^{v-b}r_2, 2^{a-1-u_1}c\right)} \\ =&\frac{\gcd\left(r_1+r_2, r_1, c\right)}{\gcd\left(r_1, r_2, c\right)} = 1. \end{aligned}$$

On the other hand, it is easy to see that $\langle 6,8\rangle \subseteq \langle -1,2,3\rangle$. Hence $\langle 6,8\rangle = \langle -1,2,3\rangle$, which contradicts the fact that $2 \notin \langle 6,8\rangle$.

Similarly, if $u_1 \ge a-1, u_2 = a-1$, then

$$\begin{aligned} &\frac{|\langle -1,2,3\rangle|}{|\langle 6,8\rangle|} \\ =&\frac{\gcd\left(2^{u_1-u_2}3^{v-b}r_1 + 3^{v-b}r_2, 2^{u_1-u_2}3^{v-b+1}r_1, 2c\right)}{\gcd\left(2^{u_1-u_2}3^{v-b}r_1, 3^{v-b}r_2, c\right)} \\ =&1. \end{aligned}$$

If $u_1 = a-2, u_2 \ge a$, then

$$\begin{aligned} &\frac{|\langle -1,2,3\rangle|}{|\langle 6,8\rangle|} \\ =&\frac{\gcd\left(3^{v-b}r_1 + 2^{u_2-u_1}3^{v-b}r_2, 3^{v-b+1}r_1, 4c\right)}{\gcd\left(3^{v-b}r_1, 2^{u_2-u_1}3^{v-b}r_2, 2c\right)} \\ =&1. \end{aligned}$$

Hence for both cases $\langle 6,8\rangle = \langle -1,2,3\rangle$, which contradicts the fact that $2 \notin \langle 6,8\rangle$. This completes the proof of Claim 2.

Hence from now on, we let $v = v_1 = v_2 \le b-1$. Note that

$$\mathrm{ord}_p(6) = \frac{p-1}{\gcd(2^{u_1}3^v r_1 + 2^{u_2}3^v r_2, p-1)},$$

which is odd if and only if $2^{u_1}3^v r_1 + 2^{u_2}3^v r_2 \equiv 0 \pmod{2^a}$. We can also compute to get Equations (7) and (8) (on the top of next page).

Now we divide our proof into two cases.

Case 1: $\mathrm{ord}_p(6)$ is odd.

For this case, we have $2^{u_1}3^v r_1 + 2^{u_2}3^v r_2 \equiv 0 \pmod{2^a}$. So we get that $u_1, u_2 \ge a$ or $u_1 = u_2 \le a-1$. But by (6), it forces that $u_1 = u_2 = a-1$. Thus (8) becomes

$$\begin{aligned} \frac{|\langle -1,2,3\rangle|}{|\langle 6, -\frac{3}{4}\rangle|} &= \frac{\gcd\left(r_1+r_2, r_2+3^{b-v}c-2r_1, 2\times 3^{b-v}c\right)}{\gcd\left(r_1, r_2, 3^{b-v}c\right)} \\ &= \frac{\gcd\left(r_1+r_2, r_2+3^{b-v}c-2r_1, 2\times 3^{b-v}c\right)}{\gcd\left(r_1, r_2, c\right)}. \end{aligned}$$

Since $u_1 = u_2 = a-1$, we have

$$d = 2^{u_2}3^v \gcd\left(r_1+r_2, 3r_1\right).$$

If $3 \nmid \gcd\left(r_1+r_2, 3r_1\right)$, then $d \mid \mathrm{ind}_g(2)$, and hence $2 \in \langle 6,8\rangle$, which is a contradiction. Thus $r_1 + r_2 \equiv 0 \pmod 3$. Now it is easy to see that $2 \mid \gcd\left(r_1+r_2, r_2+3^{b-v}c-2r_1, 2\cdot 3^{b-v}c\right)$ and $3 \mid \gcd\left(r_1+r_2, r_2+3^{b-v}c-2r_1, 2\cdot 3^{b-v}c\right)$. Therefore,

$$\frac{\gcd\left(r_1+r_2, r_2+3^{b-v}q-2r_1, 2\cdot 3^{b-v}c\right)}{\gcd\left(r_1, r_2, c\right)} \ge 6,$$

since $2 \nmid r_1r_2$, $3 \nmid r_1r_2$ and $\gcd(c,6) = 1$. This leads to $\frac{|\langle -1,2,3\rangle|}{|\langle 6,-\frac{3}{4}\rangle|} \ge 6$. On the other hand,

$$|\langle -1,2,3\rangle| = \left|M\left\langle 6, -\frac{3}{4}\right\rangle\right| \le |M|\left|\left\langle 6, -\frac{3}{4}\right\rangle\right| = 6\left|\left\langle 6, -\frac{3}{4}\right\rangle\right|,$$

therefore, $\langle -1,2,3\rangle = MB$ is a factorization.

Case 2: $\mathrm{ord}_p(6)$ is even.

For this case, we only need to prove that

$$\frac{|\langle -1,2,3\rangle|}{|\langle 6,-\frac{3}{4}\rangle|} \ge 3.$$

We divide our proof into three subcases.

Subcase 1: $u_1 \ge a-1$**,** $u_2 = a-1$**.**

For this case, we have

$$d = 2^{u_2}3^v \gcd\left(2^{u_1-u_2}r_1 + r_2, 2^{u_1-u_2}3r_1\right).$$

If $3 \nmid \gcd\left(2^{u_1-u_2}r_1 + r_2, 2^{u_1-u_2}3r_1\right)$, then $2 \in \langle 6,8\rangle$, which is a contradiction. So $r_2 + 2^{u_1-u_2}r_1 \equiv 0 \pmod 3$ and hence $r_2 - 2^{u_1-u_2+1}r_1 \equiv 0 \pmod 3$. Then from (8) we have

$$\frac{|\langle -1,2,3\rangle|}{|\langle 6,-\frac{3}{4}\rangle|} \ge 3.$$

Subcase 2: $u_1 = a-2$**,** $u_2 \ge a$**.**

For this case, we have

$$d = 2^{u_1}3^v \gcd\left(r_1 + 2^{u_2-u_1}r_2, 3r_1\right).$$

If $3 \nmid \gcd\left(r_1 + 2^{u_2-u_1}r_2, 3r_1\right)$, then $2 \in \langle 6,8\rangle$, which is a contradiction. So $r_1 + 2^{u_2-u_1}r_2 \equiv 0 \pmod 3$ and hence $2^{u_2-u_1}r_2 - 2r_1 \equiv 0 \pmod 3$. Then from (8) we have

$$\frac{|\langle -1,2,3\rangle|}{|\langle 6,-\frac{3}{4}\rangle|} \ge 3.$$

Subcase 3: $u_1 + 1 = u_2 \le a-2$**.**

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

$$\frac{|\langle -1,2,3\rangle|}{|\langle 6,-\frac{3}{4}\rangle|} = \frac{\gcd\left(2^{u_1}3^v r_1 + 2^{u_2}3^v r_2, 2^{u_2}3^v r_2 - 2^{u_1+1}3^v r_1 + 2^{a-1}3^b c, 2^a 3^b c\right)}{\gcd\left(2^{u_1}3^v r_1, 2^{u_2}3^v r_2, 2^{a-1}3^b c\right)} \quad (7)$$

$$= \frac{\gcd\left(2^{u_1} r_1 + 2^{u_2} r_2, 2^{u_2} r_2 - 2^{u_1+1} r_1 + 2^{a-1}3^{b-v} c, 2^a 3^{b-v} c\right)}{\gcd\left(2^{u_1} r_1, 2^{u_2} r_2, 2^{a-1}3^{b-v} c\right)}. \quad (8)$$

For this case, we have

$$d = 2^{u_1}3^v \gcd(r_1 + 2r_2, 3r_1).$$

If $3 \nmid \gcd(r_1 + 2r_2, 3r_1)$, then $2 \in \langle 6,8\rangle$, which is a contradiction. So $r_1+2r_2 \equiv 0 \pmod 3$ and hence $r_2-r_1 \equiv 0 \pmod 3$. Then from (8) we have

$$\frac{|\langle -1,2,3\rangle|}{|\langle 6,-\frac{3}{4}\rangle|} \geq 3.$$

■

Theorem III.2. *Let $p \equiv 1 \pmod 8$ be a prime, then there exists a nonsingular perfect $B[-4,4](p)$ set if and only if $\pm 4 \notin \langle 6,16\rangle$.*

Proof: First, suppose B is a nonsingular perfect $B[-4,4](p)$ set. Let $\pm B = B \cup (-B)$, $M = \{\pm 1, \pm 2, \pm 3, \pm 4\}$ and $M' = \{1,2,3,4\}$. Since B is a perfect $B[-4,4](p)$ set, then by Lemma II.1, $|B \cap aM| = 1$ for any $a \in \mathbb{Z}_p^*$. It's easy to verify that $|B \cap aM| = 1$ is equivalent to $|(\pm B) \cap aM'| = 1$. Similarly, $\mathbb{Z}_p^* = MB$ is a factorization if and only if $\mathbb{Z}_p^* = M'(\pm B)$ is a factorization.

Note that if $\mathbb{Z}_p^* = MB$ is a factorization, then $\mathbb{Z}_p^* = MB'$ is also a factorization, where $B' = b^{-1}B$ for some $b \in B$. Hence, without loss of generality, we may assume that $1 \in \pm B$. If $r \in \pm B$, then from $|\pm B \cap rM'| = 1$, we have $2r, 3r, 4r \notin \pm B$; from $|\pm B \cap \frac{1}{2}rM'| = 1$, we have $\frac{3}{2}r \notin \pm B$; and from $|\pm B \cap \frac{1}{3}rM'| = 1$, we have $\frac{2}{3}r, \frac{4}{3}r \notin \pm B$. Note that $6r \in \mathbb{Z}_p^* = M'(\pm B)$, which can be written as $6r = 1\cdot(6r) = 2\cdot(3r) = 3\cdot(2r) = 4\cdot(\frac{3}{2}r)$, but $2r, 3r, \frac{3}{2}r \notin \pm B$, so we have $6r \in \pm B$. Since $|\pm B \cap 2rM'| = 1$, $|\pm B \cap 3rM'| = 1$ and $|\pm B \cap 4rM'| = 1$, then $8r, 9r, 12r \notin \pm B$ and $16r \in \pm B$.

With the observation above and the fact $1 \in \pm B$, it is easy to see that $\langle 6,16\rangle \subseteq \pm B$ and $\langle 6,16\rangle \cap \{\pm 2, \pm 3, \pm 4, \pm 8, \pm\frac{2}{3}, \pm\frac{4}{3}\} = \emptyset$, which leads to $\pm 4 \notin \langle 6,16\rangle$.

For the other direction, suppose $\pm 4 \notin \langle 6,16\rangle$. Then $2,4,8 \notin \langle 6,16\rangle$ (if $8 \in \langle 6,16\rangle$, then $2 \in \langle 6,16\rangle$) and $16 \in \langle 6,16\rangle$. So the order of $2\langle 6,16\rangle$ in the quotient group $\langle -1,2,3\rangle/\langle 6,16\rangle$ is 4. Since $3\times 16 = 8\times 6$, we have $3\langle 6,16\rangle = 8\langle 6,16\rangle$. Therefore, the subgroup of $\langle -1,2,3\rangle/\langle 6,16\rangle$ generated by $2\langle 6,16\rangle$ is

$$\langle 2\langle 6,16\rangle\rangle = \{\langle 6,16\rangle, 2\langle 6,16\rangle, 3\langle 6,16\rangle, 4\langle 6,16\rangle\}.$$

In particular, $|\langle -1,2,3\rangle| \geq 4|\langle 6,16\rangle|$.

Claim. $-1 \in \langle 6,16\rangle$.

Proof of Claim: Since $p \equiv 1 \pmod 8$, we can assume $p = 2^b c + 1$, where b, c are integers, $b \geq 3$ and $\gcd(c,2) = 1$. Let g be a primitive root modulo p and suppose that

$$2 \equiv g^{2^{u_1} r_1} \pmod p \text{ and } 3 \equiv g^{2^{u_2} r_2} \pmod p,$$

where $u_1, u_2 \geq 0, r_1, r_2 \geq 1$ are integers and $2 \nmid r_1 r_2$. Let $d = \gcd(2^{u_1} r_1 + 2^{u_2} r_2, 2^{u_1+2} r_1)$, then $\langle 6,16\rangle = \langle g^d\rangle$.

If $u_1 > u_2$, then $d = 2^{u_2}\gcd(2^{u_1-u_2} r_1 + r_2, 2^{u_1-u_2+2} r_1) = 2^{u_2}\gcd(r_1, r_2)$. Now it is easy to see that $d \mid 2^{u_1} r_1$, and $2 \in \langle 6,16\rangle$, which is a contradiction. Similarly, if $u_1 < u_2$, we can also get $2 \in \langle 6,16\rangle$. Therefore, we always have $u_1 = u_2$. Now we assume $u = u_1 = u_2$. Then $d = 2^u \gcd(r_1 + r_2, 4r_1)$. If $4 \nmid (r_1 + r_2)$, then $d = 2^{u+1}\gcd(r_1, r_2)$. So $d \mid 2^{u+1} r_1$ and $4 \in \langle 6,16\rangle$, which is a contradiction. Thus, $4 \mid (r_1 + r_2)$. Then $d = 2^{u+2}\gcd(r_1, r_2)$. If $u \geq b-1$, then

$$\begin{aligned}\frac{|\langle -1,2,3\rangle|}{|\langle 6,16\rangle|} &= \frac{\gcd(2^{u+2} r_1, 2^{u+2} r_2, 2^b c)}{\gcd(2^u r_1, 2^u r_2, 2^{b-1} c)} \\ &= \frac{\gcd(2^{u-b+3} r_1, 2^{u-b+3} r_2, 2c)}{\gcd(2^{u-b+1} r_1, 2^{u-b+1} r_2, c)} \\ &= \frac{2\times\gcd(2^{u-b+2} r_1, 2^{u-b+2} r_2, c)}{\gcd(r_1, r_2, c)} \\ &= \frac{2\times\gcd(r_1, r_2, c)}{\gcd(r_1, r_2, c)} = 2,\end{aligned}$$

which contradicts the fact that $|\langle -1,2,3\rangle| \geq 4|\langle 6,16\rangle|$. If $u = b-2$, then $\frac{|\langle -1,2,3\rangle|}{|\langle 6,16\rangle|} = 4$. So $\langle -1,2,3\rangle = \{1,2,3,4\}\langle 6,16\rangle$ is a factorization. This means $-\langle 6,16\rangle = i\langle 6,16\rangle$ for some $i \in \{1,2,3,4\}$, that is to say, $-i \in \langle 6,16\rangle$. Note that $\pm 4 \notin \langle 6,16\rangle$, so $i \neq 2,3,4$. On the other hand, since $u = b-2$, we have

$$|\langle 6,16\rangle| = \frac{p-1}{\gcd(d, p-1)} = \frac{c}{\gcd(r_1, r_2, c)}$$

is an odd number, which means $-1 \notin \langle 6,16\rangle$. Therefore, $u \leq b-3$. Now

$$\begin{aligned}|\langle 6,16\rangle| &= \frac{p-1}{\gcd(2^{u+2} r_1, 2^{u+2} r_2, 2^b c)} \\ &= \frac{2^{b-u-2} c}{\gcd(r_1, r_2, 2^{b-u-2} c)}\end{aligned}$$

is an even number. So $-1 \in \langle 6,16\rangle$. This completes the proof of the claim.

Since $-1 \in \langle 6,16\rangle$, then $\langle -1,2,3\rangle = \langle 2,6,16\rangle = \{1,2,3,4\}\langle 6,16\rangle$ is a factorization. Let $a = \gcd\left(\frac{p-1}{2}, \mathrm{ind}_g(6), \mathrm{ind}_g(16)\right)$, then $\langle 6,16\rangle = \langle g^a\rangle$. Let $u \geq 1$ be the smallest integer such that $2^u a \nmid \frac{p-1}{2}$, then $-1 \notin \left\langle g^{2^u a}\right\rangle$. Let S be a complete set of coset representatives of $\left\langle g^{2^u a}\right\rangle$ in $\langle 6,16\rangle$. Since $-1 \in \langle 6,16\rangle$ and $-1 \notin \left\langle g^{2^u a}\right\rangle$, we can choose S such that if $s \in S$, then $-s \in S$. Let $S' = \left\{s : s \in S \text{ and } 0 \leq \mathrm{ind}_g(s) < \frac{p-1}{2}\right\}$. Then

$$\langle -1,2,3\rangle = \{\pm 1, \pm 2, \pm 3, \pm 4\}\left(\bigcup_{s\in S'} s\left\langle g^{2^u a}\right\rangle\right)$$

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

is a factorization. By Lemma III.2, there exists a perfect $B[-4,4](p)$ set. ■

Remark III.1. *We note that perfect $B[-4,4](p)$ sets have been considered in [17] and [27] before.*

In [17, Lemma 4.3], the author gave an equivalent condition for the existence of a perfect $B[-4,4](p)$ set. But the construction method in the proof of Theorem III.2 is more explicit and simpler than that in the proof of [17, Lemma 4.3].

In [27, Theorem 1], Tamm gave an equivalent condition for the existence of a perfect $B[-4,4](p)$ set and claimed that a perfect $B[-4,4](p)$ set must be of the form

$$x_0 \cdot \mathcal{F} \cup \cdots \cup x_{\rho-1} \cdot \mathcal{F}.$$

However, the calculations of $x_0, \ldots, x_{\rho-1}$ and $\mathcal{F}$ make his construction more complicated than ours.

Similar to Theorem III.2, we show the following result, for which we just sketch the proof.

Theorem III.3. *Let $p \equiv 1 \pmod 4$ be a prime, then there exists a nonsingular perfect $B[0,4](p)$ set if and only if $4 \notin \langle 6, 16\rangle$.*

Proof: First, suppose B is a nonsingular perfect $B[0,4](p)$ set. Let $M = \{1,2,3,4\}$. In the proof of Theorem III.2, taking M' as M, B' as B, respectively, and following the same procedure, we get $\langle 6,16\rangle \subseteq B$ and $4 \notin \langle 6,16\rangle$.

For the other direction, as in the proof of Theorem III.2, the fact $4 \notin \langle 6,16\rangle$ implies that

$$\langle 2\langle 6,16\rangle\rangle = \{\langle 6,16\rangle, 2\langle 6,16\rangle, 3\langle 6,16\rangle, 4\langle 6,16\rangle\}.$$

Therefore, $\langle 1,2,3,4\rangle = \langle 2,6,16\rangle = \{1,2,3,4\}\langle 6,16\rangle$ is a factorization. By Lemma III.2, there exists a perfect $B[0,4](p)$ set. ■

If there exists a nonsingular perfect $B[-2,4](p)$ set ($B[-4,4](p)$ set, or $B[0,4](p)$ set), then we can construct it explicitly from the proofs of Lemma III.2 and Theorem III.1 (Theorem III.2, or Theorem III.3, respectively).

Example III.1. *We give three examples to illustrate how to construct perfect splitter sets by using the above theorems.*

1) *We use the same notations as in the proof of Theorem III.2. Let $p = 97$, then $g = 5$, $\mathrm{ind}_g(6) = 8$, $\mathrm{ind}_g(4) = 68$, $\mathrm{ind}_g(-4) = 20$, $\mathrm{ind}_g(16) = 40$ and $a = 8$. Since $8x \equiv 68 \pmod{96}$ has no solution, then $4 \notin \langle 6,16\rangle$. Similarly, $-4 \notin \langle 6,16\rangle$. So by Theorem III.2, there exists a perfect $B[-4,4](p)$ set. Further,*

$$\langle 6,16\rangle = \{1,6,16,22,35,36,61,62,75,81,91,96\}$$

and (here $u = 2$)

$$\left\langle g^{2^u a}\right\rangle = \langle 5^{32}\rangle = \{1,35,61\}.$$

We can choose $S = \{1,6,91,96\}$ and $S' = \{1,6\}$. Furthermore, $T = \{1,5\}$ is a complete set of coset representatives of $\langle -1,2,3\rangle$ in $\mathbb{Z}_{97}^*$. Thus, the set

$$\bigcup_{t\in T}\bigcup_{s\in S'}\left\{sti \pmod{97} :\ i \in \left\langle g^{2^u a}\right\rangle\right\}$$
$$=\{1,5,6,14,16,30,35,61,75,78,80,84\}$$

is a perfect $B[-4,4](97)$ set. By Theorem III.2 and computation, when $p \le 5000$ is a prime, there is a perfect $B[-4,4](p)$ set if and only if $p = 97, 1873, 2161$ and 3457.

2) *Let $p = 139$, then $g = 2$, $\mathrm{ind}_g(2) = 1$, $\mathrm{ind}_g(6) = 42$ and $\mathrm{ind}_g(8) = 3$, so $2 \notin \langle 6,8\rangle$. It is easy to see that $-\frac{4}{3} = 45$ in $\mathbb{Z}_{139}$ and $\mathrm{ord}_p(45) = 23$. Therefore, there exists a perfect $B[-2,4](139)$ set. In this case, $\mathrm{ord}_p(6) = 23$ is odd, $\mathrm{ind}_g(45) = 30$ and $\gcd(\mathrm{ind}_g(6), \mathrm{ind}_g(45)) = 6$. By the proof of Theorem III.1, the set*

$$\langle 6,45\rangle = \{2^{6i} \pmod{139} :\ 0 \le i \le 22\}$$

is a perfect $B[-2,4](139)$ set.

3) *Let $p = 181$, then $g = 2$, $\mathrm{ind}_g(2) = 1$, $\mathrm{ind}_g(6) = 57$ and $\mathrm{ind}_g(8) = 3$, so $2 \notin \langle 6,8\rangle$. It is easy to see that $-\frac{4}{3} = 59$ and $\mathrm{ord}_p(59) = 5$. Therefore, there exists a perfect $B[-2,4](181)$ set. In this case, $\mathrm{ord}_p(6) = 60$ is even, $\mathrm{ind}_g(59) = 36$ and $\gcd(\mathrm{ind}_g(6), \mathrm{ind}_g(59)) = 3$. Then $\langle 6,59\rangle = \{2^{3i} \pmod{181} :\ 0 \le i \le 59\}$. By the proof of Theorem III.1, the set*

$$\{2^{3i} \pmod{181} :\ 0 \le i \le 29\}$$

is a perfect $B[-2,4](181)$ set. By Theorem III.1, for primes $p \le 1000$, apart from the 10 constructions in [31], perfect $B[-2,4](p)$ sets exist only when $p = 181, 313, 421, 541, 919$ and 937.

B. Simpler characterizations for special cases

When $\gcd\left(\frac{p-1}{k_1+k_2}, k_1+k_2\right) = 1$, we are able to give a much simpler characterization for the existence of perfect splitter sets. Before stating our results, we need some useful lemmas.

Lemma III.3. [24, Theorem 7.1] *Let m and n be relatively prime positive integers. If $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$ are sets of integers such that their sum set*

$$A + B := \{a_i + b_j :\ 1 \le i \le m, 1 \le j \le n\}$$

is a complete set of representatives modulo mn, then A is a complete set of residues modulo m and B is a complete set of residues modulo n.

Lemma III.4. *Let $k_2 \ge k_1 \ge 0$ be integers, and let p be a prime such that $p \equiv 1 \pmod{k_1 + k_2}$ and $\gcd\left(k_1+k_2, \frac{p-1}{k_1+k_2}\right) = 1$. Suppose g is a primitive root modulo p, and denote $N = \{\mathrm{ind}_g(j) :\ j \in [-k_1,k_2]^*\}$. Then there exists a nonsingular perfect $B[-k_1,k_2](p)$ set if and only if N is a complete set of residues modulo k_1+k_2.*

Proof: Let B be a nonsingular perfect $B[-k_1,k_2](p)$ set, and $A = \{\mathrm{ind}_g(b) :\ b \in B\}$. Then $\mathbb{Z}_{p-1} = N + A$ is a factorization. Since $\gcd\left(k_1+k_2, \frac{p-1}{k_1+k_2}\right) = 1$, it follows from Lemma III.3 that N is a complete set of residues modulo k_1+k_2.

The other direction follows from [31, Theorem 3]. ■

We will apply Lemma III.4 to the cases when $(k_1,k_2) \in \{(2,4),(0,4),(4,4)\}$. Note that $p \equiv 1 \pmod 6$ and

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

$\gcd\left(6, \frac{p-1}{6}\right) = 1$ if and only if $p \equiv 7, 31 \pmod{36}$; $\gcd\left(4, \frac{p-1}{4}\right) = 1$ is equivalent to that $p \equiv 5 \pmod 8$; and $\gcd\left(8, \frac{p-1}{8}\right) = 1$ is equivalent to that $p \equiv 9 \pmod{16}$.

Theorem III.4. 1) *Let $p \equiv 7, 31 \pmod{36}$ be a prime. Then there exists a nonsingular perfect $B[-2,4](p)$ set if and only if 6 is a cubic residue in $\mathbb{Z}_p$ and $2, 3$ are not cubic residues.*

2) *Let $p \equiv 5 \pmod 8$ be a prime. Then there exists a nonsingular perfect $B[0,4](p)$ set if and only if 6 is a quartic residue modulo p.*

3) *Let $p \equiv 9 \pmod{16}$ be a prime. Then there does not exist a nonsingular perfect $B[-4,4](p)$ set.*

Proof: Assume that g is a primitive root modulo p.

1). Suppose there exists a nonsingular perfect $B[-2,4](p)$ set. By Lemma III.4, $N = \{\mathrm{ind}_g(j) \pmod 6 : j \in [-2,4]^*\} = \mathbb{Z}_6$. Since $\mathrm{ind}_g(-j) \equiv \mathrm{ind}_g(j) + \frac{p-1}{2} \pmod{p-1}$, we have $\mathrm{ind}_g(-j) \equiv \mathrm{ind}_g(j) + 3 \pmod 6$. The possible values of $\mathrm{ind}_g(j)$ modulo 6 are listed below.

	case 1	case 2	case 3	case 4
$\mathrm{ind}_g(1) \pmod 6$	0	0	0	0
$\mathrm{ind}_g(-1) \pmod 6$	3	3	3	3
$\mathrm{ind}_g(2) \pmod 6$	1	2	4	5
$\mathrm{ind}_g(-2) \pmod 6$	4	5	1	2
$\mathrm{ind}_g(3) \pmod 6$	5	1	5	1
$\mathrm{ind}_g(4) \pmod 6$	2	4	2	4

Therefore integers 2 and 3 can not be cubic residues modulo p, and 6 must be a cubic residue whichever the case is.

For the other direction, suppose $\mathrm{ind}_g(2) = x$ and $\mathrm{ind}_g(3) = y$. Then $\mathrm{ind}_g(6) \equiv x + y \pmod{p-1}$. The fact that 6 is a cubic residue implies that $x + y \equiv 0 \pmod 3$. Further, the fact that 2 and 3 are not cubic residues implies that $\{x, y\} \equiv \{1,2\}$ or $\{1,5\}$ or $\{2,4\}$ or $\{4,5\} \pmod 6$. Since $p \equiv 7, 31 \pmod{36}$, 3 is not a quadratic residue in $\mathbb{Z}_p$ [11, page 55]. Combining all these observations, we have the only four cases for the values of x and y. For any case, it is easy to see that $\{\mathrm{ind}_g(j) \pmod 6 : j \in [-2,4]^*\} = \mathbb{Z}_6$. The proof is complete by Lemma III.4.

	case 1	case 2	case 3	case 4
$x \pmod 6$	2	1	5	4
$y \pmod 6$	1	5	1	5

2). Suppose there exists a nonsingular perfect $B[0,4](p)$ set. Then $\{\mathrm{ind}_g(j) \pmod 4 : j \in [0,4]^*\} = \mathbb{Z}_4$ by Lemma III.4. Since $p \equiv 5 \pmod 8$, then 2 is not a quadratic residue modulo p [11, Proposition 5.1.3]. Note also that $\mathrm{ind}_g(4) \equiv 2 \times \mathrm{ind}_g(2) \pmod 4$. Therefore, there are only two case: $\mathrm{ind}_g(2) \equiv 1 \pmod 4$, $\mathrm{ind}_g(3) \equiv 3 \pmod 4$, $\mathrm{ind}_g(4) \equiv 2 \pmod 4$ or $\mathrm{ind}_g(2) \equiv 3 \pmod 4$, $\mathrm{ind}_g(3) \equiv 1 \pmod 4$, $\mathrm{ind}_g(4) \equiv 2 \pmod 4$. In both cases, we have $\mathrm{ind}_g(6) \equiv \mathrm{ind}_g(2) + \mathrm{ind}_g(3) \equiv 0 \pmod 4$, that is, 6 is a quartic residue modulo p.

For the other direction, suppose $\mathrm{ind}_g(2) = x$ and $\mathrm{ind}_g(3) = y$. Then the fact that 6 is a quartic residue modulo p implies that $\mathrm{ind}_g(6) \equiv x + y \equiv 0 \pmod 4$. We also have $x \equiv 1$ or $3 \pmod 4$ since 2 is not a quadratic residue modulo p. Thus, we have two cases.

	case 1	case 2
$\mathrm{ind}_g(1) \pmod 4$	0	0
$\mathrm{ind}_g(2) \pmod 4$	1	3
$\mathrm{ind}_g(3) \pmod 4$	3	1
$\mathrm{ind}_g(4) \pmod 4$	2	2

For any case, it is easy to see that $\{\mathrm{ind}_g(j) \pmod 4 : j \in [0,4]^*\} = \mathbb{Z}_4$. The proof is complete.

3). Since $\frac{p-1}{2} \equiv 4 \pmod 8$, we always have $\mathrm{ind}_g(1) \equiv 0 \pmod 8$ and $\mathrm{ind}_g(-1) \equiv 4 \pmod 8$. Since $p \equiv 1 \pmod 8$, 2 is a quadratic residue modulo p. There are four cases for $\mathrm{ind}_g(2)$:

- $\mathrm{ind}_g(2) \equiv 0 \pmod 8$;
- $\mathrm{ind}_g(2) \equiv 2 \pmod 8$, then $\mathrm{ind}_g(4) \equiv 4 \pmod 8$;
- $\mathrm{ind}_g(2) \equiv 4 \pmod 8$, then $\mathrm{ind}_g(-2) \equiv 0 \pmod 8$; and
- $\mathrm{ind}_g(2) \equiv 6 \pmod 8$, then $\mathrm{ind}_g(4) \equiv 4 \pmod 8$.

For any case, it is impossible to have $\{\mathrm{ind}_g(j) \pmod 8 : j \in [-4,4]^*\} = \mathbb{Z}_8$. Hence there does not exist a perfect $B[-4,4](p)$ set. ■

For the existence of nonsingular perfect $B[-2,4](p)$ sets, we can give another characterization from number theory. In the following discussion, all the undefined terminologies can be found in [11].

Let $\omega = \frac{-1+\sqrt{-3}}{2}$. Suppose $p \equiv 1 \pmod 6$, then we can assume $p = \pi\bar{\pi}$, where $\pi = 3m - 1 + 3n\omega$ is a primary prime in the ring $\mathbb{Z}[\omega]$, and $\bar{\pi}$ is the complex conjugate of π. By the cubic reciprocity and [11, Chapter 9, Exercise 5], we have

$$\chi_\pi(2) = \chi_2(\pi) \equiv \pi \pmod 2 \quad \text{and} \quad \chi_\pi(3) = \omega^{2n}.$$

Notice that $\chi_\pi(2), \chi_\pi(3) \neq 1$, as that 2 and 3 are not cubic residues modulo p (and therefore modulo π). Thus, 6 is a cubic residue modulo p if and only if

$$\begin{cases} \chi_\pi(2) = \omega \\ \chi_\pi(3) = \omega^2 \end{cases} \text{or} \begin{cases} \chi_\pi(2) = \omega^2 \\ \chi_\pi(3) = \omega, \end{cases}$$

and hence if and only if

$$\begin{cases} m \text{ is odd, } n \text{ is odd} \\ n \equiv 1 \pmod 3 \end{cases} \text{or} \begin{cases} m \text{ is even, } n \text{ is odd} \\ n \equiv 2 \pmod 3. \end{cases} \tag{9}$$

For the first condition in (9), let $m = 2k + 1$ for some integer k. Since n is odd and $n \equiv 1 \pmod 3$, then n can only be of the form $6l + 1$ for some integer l. In this case, $p = \pi\bar{\pi} = 36k^2 - 108kl + 324l^2 + 6k + 72l + 7$, then $\frac{p-1}{6} \equiv k + 1 \pmod 6$. So $\gcd(\frac{p-1}{6}, 6) = 1$ if and only if $k \equiv 0$ or $4 \pmod 6$, that is $m \equiv 1$ or $9 \pmod{12}$.

For the second condition in (9), let $m = 2k$ for some integer k. Since n is odd and $n \equiv 2 \pmod 3$, then n can only be of the form $6l + 5$ for some integer l. In this case, $p = \pi\bar{\pi} = 36k^2 - 108kl + 324l^2 - 102k + 558l + 241$, then $\frac{p-1}{6} \equiv k + 3l + 4 \pmod 6$. So $\gcd(\frac{p-1}{6}, 6) = 1$ if and only if $k + 3l \equiv 1$ or $3 \pmod 6$.

Thus, we have the following corollary.

Corollary III.1. *Let $p \equiv 1 \pmod 6$ be a prime and $\gcd(\frac{p-1}{6}, 6) = 1$. Then there exists a nonsingular perfect $B[-2,4](p)$ set if and only if there exist $k, l \in \mathbb{Z}$, such that one of the following three conditions holds:*

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

1) $p = 1296k^2 - 648kl + 324l^2 + 36k + 72l + 7$. *This case corresponds to the first condition in (9) and* $m \equiv 1 \pmod{12}$.
2) $p = 1296k^2 - 648kl + 324l^2 + 1764k - 360l + 607$. *This case corresponds to the first condition in (9) and* $m \equiv 9 \pmod{12}$.
3) $p = 36k^2 - 108kl + 324l^2 - 102k + 558l + 241$ *and* $k + 3l \equiv 1$ *or* $3 \pmod 6$. *This case corresponds to the second condition in (9).*

Example III.2. *We give some examples from Corollary III.1.*

1) *Let* k, l *range from* -100 *to* 100. *The eight smallest primes of the form* $p = 1296k^2 - 648kl + 324l^2 + 36k + 72l + 7$ *are listed in Table I. In particular, if we let* $l = 0$, *then* $p = 1296k^2 + 36k + 7$. *Bunyakovsky's conjecture [6], which has not been proved yet, suggests that there are infinitely many such primes.*

TABLE I

p	7	1087	1123	1447	1483	2239	2311	2707
k	0	1	−1	0	1	1	−1	0
l	0	1	−2	2	2	−1	1	−3

2) *Let* k, l *range from* -100 *to* 100. *The eight smallest primes of the form* $p = 1296k^2 - 648kl + 324l^2 + 1764k - 360l + 607$ *are listed in Table II.*

TABLE II

p	139	571	607	751	859	1291	2011	2371
k	−1	0	0	−1	−1	0	−1	−2
l	0	1	0	1	−2	−1	2	−3

IV. Constructions of quasi-perfect splitter sets

In this section, we provide four new constructions of quasi-perfect splitter sets.

A. Quasi-perfect $B[0, k](m)$ sets

Theorem IV.1. *Let* k, m *be positive integers such that* $\gcd(m, k!) = 1$. *Let* $a = (-k)^{-1} \pmod m$. *Then*

$$B = \{ik + 1 : \ i \in [0, m-1] \text{ and } i \neq a\}$$

is a quasi-perfect $B[0, k](km)$ *set.*

Proof: Suppose $r(ik + 1) \equiv 0 \pmod{km}$, where $r \in [1, k]$ and $i \in [0, m-1] \setminus \{a\}$. Since $ik + 1 \not\equiv 0 \pmod k$, then $r \equiv 0 \pmod k$, and hence $r = k$. This implies that $ik + 1 \equiv 0 \pmod m$, which contradicts the fact that $i \not\equiv (-k)^{-1} \pmod m$.

Suppose $r(ik + 1) \equiv s(jk + 1) \pmod{km}$, where $r, s \in [1, k]$ and $i, j \in [0, m-1] \setminus \{a\}$. Then $r \equiv s \pmod k$, and so $r = s$. This implies that $rik \equiv rjk \pmod{km}$, and so $ri \equiv rj \pmod m$. Note that $\gcd(m, k!) = 1$, then $i \equiv j \pmod m$, and so $i = j$.

Combing the above analysis, we see that B is a $B[0, k](km)$ set of size $m - 1 = \lfloor \frac{km-1}{k} \rfloor$. ■

Example IV.1. 1) *Let* $k = 5$ *and* $m = 7$. *By Theorem IV.1, the set*

$$\{1, 6, 11, 16, 26, 31\}$$

is a quasi-perfect $B[0, 5](35)$ *set.*

2) *Let* $k = 6$ *and* $m = 7$. *By Theorem IV.1, the set*

$$\{1, 13, 19, 25, 31, 37\}$$

is a quasi-perfect $B[0, 6](42)$ *set.*

Remark IV.1. *It is easy to see that Theorem IV.1 is a generalization of [12, Theorem 1], and the above examples cannot be obtained by Theorem 1 of [12]. Moreover, Theorem IV.1 shows that, for any integer k, there exists a quasi-perfect* $B[0, k](km)$ *set for all positive integers* m *whose prime factors are all greater than k.*

B. Quasi-perfect $B[-k, k](m)$ sets

Theorem IV.2. *Let* $k > 0$ *be an integer, and* p *be a prime such that* $k < p < 2k$. *Then*

$$B = \{k + 1\} \cup \{1 + (2k + 2)i : \ i \in [0, p-1]\}$$

is a quasi-perfect $B[-k, k](p(2k + 2))$ *set.*

Proof: Suppose $r(k+1) \equiv s(k+1) \pmod{p(2k+2)}$, where $r, s \in [-k, k]^*$. Then $r \equiv s \pmod{2p}$, and so $r = s$.

Suppose $r(k+1) \equiv s(1+(2k+2)i) \pmod{p(2k+2)}$, where $r, s \in [-k, k]^*$ and $i \in [0, p-1]$. Then $s \equiv 0 \pmod{k+1}$, which is a contradiction.

Suppose $r(1 + (2k+2)i) \equiv s(1 + (2k+2)j) \pmod{p(2k+2)}$, where $r, s \in [-k, k]^*$ and $i, j \in [0, p-1]$. Then $r \equiv s \pmod{2k+2}$, and so $r = s$. This implies $r(2k+2)i \equiv r(2k+2)j \pmod{p(2k+2)}$, and so $ri \equiv rj \pmod p$. Note that $p > k$ is a prime, we have $\gcd(r, p) = 1$. Then $i \equiv j \pmod p$, and so $i = j$.

Combing the above analysis, we see that B is a $B[-k, k](p(2k+2))$ set of size $p + 1 = \left\lfloor \frac{p(2k+2)-1}{2k} \right\rfloor$. ■

Example IV.2. 1) *Let* $k = 3$ *and* $p = 5$. *By Theorem IV.2, the set*

$$\{1, 4, 9, 17, 25, 33\}$$

is a quasi-perfect $B[-3, 3](40)$ *set.*

2) *Let* $k = 4$ *and* $p = 7$. *By Theorem IV.2, the set*

$$\{1, 5, 11, 21, 31, 41, 51, 61\}$$

is a quasi-perfect $B[-4, 4](70)$ *set.*

Theorem IV.3. *Let* k *be an even integer and* $m \geq 1$. *For* $i = 0, 1$, *let* $T_i = \{x : \ x \equiv i \pmod 2, x \in [1, k]\}$, *then* $|T_i| = \frac{k}{2}$. *Suppose that* $p \equiv 1 \pmod{2^m k}$ *is a prime. Let* g *be a primitive root modulo* p *such that* $g \equiv 1 \pmod 2$. *Denote* $v := 2^{m-1}k$. *If there exists a* 2^m*-subset* $A \subset \mathbb{Z}_v$ *such that* $\mathbb{Z}_v = A + \{\text{ind}_g(x) \pmod v : \ x \in T_i\}$ *is a factorization for each* $i = 0, 1$, *then there exists a quasi-perfect* $B[-k, k](2p)$ *set.*

Proof: Let $p = 2^m kn + 1 = 2vn + 1$ be a prime for some $n \geq 1$. We claim that the set $\{g^{i+jv} : \ i \in A, j \in [0, n-1]\}$ is a quasi-perfect $B[-k, k](2p)$ set of size $2^m n$.

Suppose that

$$sg^{i_1+j_1v} \equiv lg^{i_2+j_2v} \pmod{2p}, \tag{10}$$

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

where $s, l \in [-k, k]^*, i_1, i_2 \in A$ and $j_1, j_2 \in [0, n-1]$. Then

$$sg^{i_1+j_1 v} \equiv lg^{i_2+j_2 v} \pmod p,$$

and hence

$$\mathrm{ind}_g(s) + i_1 + j_1 v \equiv \mathrm{ind}_g(l) + i_2 + j_2 v \pmod{p-1}.$$

Reducing this to the residue modulo $v = 2^{m-1}k$, we get

$$\mathrm{ind}_g(s) + i_1 \equiv \mathrm{ind}_g(l) + i_2 \pmod v.$$

Since $g \equiv 1 \pmod 2$, then $s \equiv l \pmod 2$ by (10). Hence $s, l \in T_i \cup (-T_i)$. However, the two values $\mathrm{ind}_g(s) \pmod v$ and $\mathrm{ind}_g(l) \pmod v$ always belong to $\{\mathrm{ind}_g(x) \pmod v : x \in T_i\}$ even when $s \in -T_i$ or $l \in -T_i$, due to the fact that $\mathrm{ind}_g(-1) \equiv \frac{p-1}{2} \pmod v \equiv 0 \pmod v$. Then by the definition of A, we have $i_1 = i_2$ as well as $s = l$ or $s = -l$.

If $s = l$, then $j_1 = j_2$.

If $s = -l$, then $\frac{p-1}{2} + j_1 v \equiv j_2 v \pmod{p-1}$. Hence $\frac{p-1}{2} \mid v(j_1 - j_2)$, that is $n \mid (j_1 - j_2)$, which implies $j_1 = j_2$. ■

Remark IV.2. *It is not easy to generalize the construction in Theorem IV.3 to quasi-perfect $B[-k, k](tp)$ sets with $t > 2$. To see this, let k be a multiple of t, and we partition $[1, k]$ into t residue classes modulo t. By the same arguments, we can deduce that $s \equiv l \pmod t$. Then $s, l \in T_i \cup (-T_{t-i})$, from which we can not obtain the key conditions that $\mathrm{ind}_g(s) \pmod v$ and $\mathrm{ind}_g(l) \pmod v$ always belong to $\{\mathrm{ind}_g(x) \pmod v : x \in T_i\}$.*

Example IV.3. *We give an example to compare the construction from Theorem IV.3 and that from [33, Theorem 5]. Let $p = 13729$, $k = 8$, $m = 1$. Then $g = 23$ is a primitive root modulo p. We also have*

$$\begin{array}{lll} \mathrm{ind}_g(-8) = 6654, & \mathrm{ind}_g(-7) = 11084, & \mathrm{ind}_g(-6) = 6376, \\ \mathrm{ind}_g(-5) = 9594, & \mathrm{ind}_g(-4) = 11300, & \mathrm{ind}_g(-3) = 11022, \\ \mathrm{ind}_g(-2) = 2218, & \mathrm{ind}_g(-1) = 6864, & \mathrm{ind}_g(1) = 0, \\ \mathrm{ind}_g(2) = 9082, & \mathrm{ind}_g(3) = 4158, & \mathrm{ind}_g(4) = 4436, \\ \mathrm{ind}_g(5) = 2730, & \mathrm{ind}_g(6) = 13240, & \mathrm{ind}_g(7) = 4220, \\ \mathrm{ind}_g(8) = 13518. & & \end{array}$$

It is easy to see that

$$\begin{aligned} &\{\mathrm{ind}_g(i) \pmod 8 : \ i = 1, 3, 5, 7\} \\ =&\{\mathrm{ind}_g(i) \pmod 8 : \ i = 2, 4, 6, 8\} = \{0, 2, 4, 6\}. \end{aligned}$$

Then by Theorem IV.3, $\{23^{i+8j} \pmod{27458} : \ i \in [0, 1], j \in [0, 857]\}$ is a quasi-perfect $B[-8, 8](27458)$ set.

Applying [33, Theorem 5] with $t = 2$ and $\theta = \gcd\{\mathrm{ind}_g(k) \mid k \in [-8, 8]^*\}$, we get

$$\left\{ \frac{\mathrm{ind}_g(i)}{2} \pmod 8 : \ i = \pm 1, \pm 3, \pm 5, \pm 7 \right\} = \{0, 5, 6, 7\}$$

and

$$\left\{ \frac{\mathrm{ind}_g(i)}{2} \pmod 8 : \ i = \pm 2, \pm 4, \pm 6, \pm 8 \right\} = \{2, 4, 5, 7\}.$$

However, both sets have size $4 \neq \frac{k_1+k_2}{t} = 8$, hence we cannot get a quasi-perfect $B[-8, 8](27458)$ set from [33, Theorem 5].

TABLE III
EXAMPLES OF QUASI-PERFECT $B[-k, k](2p)$ SETS FROM THEOREM IV.3

k	m	p
4	1	97, 241, 409, 457, 1009, 1129, 1489, 1873, 2017, 2161
4	2	577, 1201, 4801, 5233, 7393, 10513, 14401, 14449, 14593
4	3	13441, 49633, 122497, 136993, 147457, 149377
8	1	12721, 13729, 33889, 65809

C. Quasi-perfect $B[-(k-1), k](m)$ sets

Theorem IV.4. *Let $k > 0$ be an integer, and p be a prime such that $k < p < \frac{4k-1}{3}$. Then*

$$B = \{k+1\} \cup \{1 + (2k+2)i : \ i \in [0, p-1]\}$$

is a quasi-perfect $B[-(k-1), k](p(2k+2))$ set.

Proof: Suppose $r(k+1) \equiv s(k+1) \pmod{p(2k+2)}$, where $r, s \in [-(k-1), k]^*$. Then $r \equiv s \pmod{2p}$, and so $r = s$.

Suppose $r(k+1) \equiv s(1 + (2k+2)i) \pmod{p(2k+2)}$, where $r, s \in [-(k-1), k]^*$ and $i \in [0, p-1]$. Then $s \equiv 0 \pmod{k+1}$, which is a contradiction.

Suppose $r(1+(2k+2)i) \equiv s(1+(2k+2)j) \pmod{p(2k+2)}$, where $r, s \in [-(k-1), k]^*$ and $i, j \in [0, p-1]$. Then $r \equiv s \pmod{2k+2}$, and so $r = s$. This implies $r(2k+2)i \equiv r(2k+2)j \pmod{p(2k+2)}$, and so $ri \equiv rj \pmod p$. Note that $p > k$ is a prime, we have $\gcd(r, p) = 1$. Then $i \equiv j \pmod p$, and so $i = j$.

Combining all pieces, we see that B is a $B[-(k-1), k](p(2k+2))$ set of size $p + 1 = \left\lfloor \frac{p(2k+2)-1}{2k-1} \right\rfloor$. ■

Example IV.4. 1) *Let $k = 6$ and $m = 7$. By Theorem IV.4, the set*

$$\{1, 7, 15, 29, 43, 57, 71, 85\}$$

is a quasi-perfect $B[-5, 6](98)$ set.

2) *Let $k = 9$ and $m = 11$. By Theorem IV.4, the set*

$$\{1, 10, 21, 41, 61, 81, 101, 121, 141, 161, 181, 201\}$$

is a quasi-perfect $B[-8, 9](220)$ set.

V. SPLITTER SETS AND CAYLEY GRAPHS

In this section, we give a connection between splitter sets and Cayley graphs. All the terminologies relevant to graph theory can be found in [3], [8]. For the convenience of readers, we introduce some of them briefly.

Suppose H is a finite abelian group. Let S be a subset of H such that the identity $e \notin S$, and $s \in S$ implies that $s^{-1} \in S$. A *Cayley graph* defined by H and S is an undirected graph $G = (V(G), E(G))$ with vertex set $V = H$ and edge set $E(G)$, such that $\{x, y\} \in E(G)$ if and only if $xy^{-1} \in S$. We denote it by $G = Cay(H, S)$. This kind of graph has been widely studied in the literature, such as [1], [10], [20].

Given a graph $G = (V(G), E(G))$, a subset $I \subseteq V(G)$ is an *independent* set if for any two distinct elements $x, y \in I$, $\{x, y\} \notin E(G)$. The maximum size of an independent set is called the *independence number*, denoted as $\alpha(G)$. We say G is *d-regular*, if for each $x \in V(G)$, there exist exactly d vertices $y \in V(G)$ such that $\{x, y\} \in E(G)$. We say a sequence of pairwise-distinct vertices $P = x_0 x_1 \cdots x_{n-1} x_n$

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

($n \geq 1$) is a *path* connecting x_0 and x_n, if $\{x_i, x_{i+1}\} \in E(G)$ for any $i = 0, \ldots, n-1$. If for any distinct $x, y \in V(G)$, there is a path connecting x and y, we say G is *connected*. A maximal connected subgraph of G is called a *connected component*. A 2-regular connected graph is called a *cycle*. We say two graphs $G_1 = (V_1, E_1)$ and $G_1 = (V_2, E_2)$ are *isomorphic*, if there exists a bijection $f : V_1 \longrightarrow V_2$ such that $\{x, y\} \in E_1$ if and only if $\{f(x), f(y)\} \in E_2$.

In the rest of this section, we let $k_2 \geq k_1 \geq 0$ be integers and $M = [-k_1, k_2]^*$. Since perfect $B[0,1](p)$ sets and perfect $B[-1,1](p)$ sets are trivial, and maximal $B[-k_1, 2](q)$ sets have been completely determined for any q in [12], [14], [31], we assume $k_2 \geq 3$ in this section. For any prime $p > k_1 + k_2$, M can be seen as a subset of $\mathbb{Z}_p^*$. Let $S = \{xy^{-1} : x, y \in M \text{ and } x \neq y\}$, $G = Cay(\mathbb{Z}_p^*, S)$ and $G' = Cay(\langle M \rangle, S)$. Note that $\langle S \rangle = \langle M \rangle$, so G' is a connected component of G [20] and each connected component of G is isomorphic to G'.

First, we have the following observation.

Proposition V.1. *A subset $B \subset \mathbb{Z}_p^*$ is a $B[-k_1, k_2](p)$ set if and only if B is an independent set in G.*

Proof: First, suppose B is a $B[-k_1, k_2](p)$ set. If there exist two different $b_1, b_2 \in B$ such that $\{b_1, b_2\} \in E(G)$, then there exist two different $x, y \in M$ such that $b_1 b_2^{-1} = xy^{-1}$, i.e. $xb_2 = yb_1$. Since B is a $B[-k_1, k_2](p)$ set, we have $x = y$ and $b_1 = b_2$, which is a contradiction. So B is an independent set in G.

On the other hand, suppose B is an independent set in G. If there exist $b_1, b_2 \in B$ and $x, y \in M$ such that $xb_1 = yb_2$, then $b_1 b_2^{-1} = yx^{-1}$. If $b_1 \neq b_2$, then by the definition of G, $\{b_1, b_2\} \in E(G)$, which contradicts the assumption that B is an independent set in G. So $b_1 = b_2$ and $x = y$. Thus B is a $B[-k_1, k_2](p)$ set. ∎

By Proposition V.1, a $B[-k_1, k_2](p)$ set of maximum size is equivalent to a maximum independent set in the graph G. The next lemma is a corollary of Brooks' theorem [15]. It can be used to give a nontrivial lower bound on the size of a maximum $B[-k_1, k_2](p)$ set for any prime $p > k_1 + k_2 + 1$ and any $0 \leq k_1 \leq k_2$ with $k_2 \geq 3$. To the best of our knowledge, there was no general lower bound before. Recall that a complete graph is a graph Γ in which $\{x, y\} \in E(\Gamma)$ for each pair of distinct $x, y \in V(\Gamma)$, and an odd cycle is a cycle with odd vertices.

Lemma V.1. *Let Γ be a d-regular graph. If each connected component of Γ is not a complete graph or an odd cycle, then*

$$\alpha(\Gamma) \geq \frac{|V(\Gamma)|}{d}.$$

Otherwise,

$$\alpha(\Gamma) \geq \frac{|V(\Gamma)|}{d+1}.$$

From the definition, we can easily check that G and G' are both $|S|$-regular. If $p > k_1 + k_2 + 2$ and $k_2 \geq 3$, then $|S| > 2$ and therefore G' is not an odd cycle. Since G' is $|S|$-regular, we have $|\langle M \rangle| \geq |S| + 1$. Furthermore, if $|\langle M \rangle| \geq |S| + 2$, G' cannot be a complete graph. Thus, we have the following corollary.

Corollary V.1. *Let B be a $B[-k_1, k_2](p)$ set of maximum size. If $p > k_1 + k_2 + 1$ and $k_2 \geq 3$, then*

$$|B| \geq \left\lceil \frac{p-1}{|S|+1} \right\rceil.$$

Further, if $|\langle M \rangle| \geq |S| + 2$ and $p > k_1 + k_2 + 2$, then

$$|B| \geq \left\lceil \frac{p-1}{|S|} \right\rceil.$$

There is another advantage by connecting splitter sets with Cayley graphs: we can use some mathematical softwares such as Maple to get a maximum independent set of graphs (and thus a splitter set of maximum size).

Example V.1. *Take $k_1 = 0, k_2 = 3$, we compute some values listed in Table IV on the top of next page. The third row is a lower bound from Corollary V.1. The fourth row is computed via the command* IndependenceNumber *in Maple and the last row is a maximum independent set (i.e. a splitter set of maximum size) computed via the command* MaximumIndependentSet *in Maple.*

VI. Conclusion

In this paper, we consider the existence of splitter sets. We give some necessary and sufficient conditions for the existence of a nonsingular perfect $B[-k_1, k_2](p)$ set, where $(k_1, k_2) \in \{(0,4), (2,4), (4,4)\}$. For easy reference, we summarize the equivalent conditions obtained in this paper and related known results in Table V, where p is a prime, g is a primitive root modulo p and $\mu = \gcd\{\text{ind}_g(j) : j \in [-1, k]^*\}$ (for $B[-k, k](p)$ sets), or $\mu = \gcd\{\text{ind}_g(j) : j \in \{2, \ldots, k, p-1\}\}$ (for $B[0, k](p)$ sets), or $\mu = \gcd\{\text{ind}_g(j) : j \in [-1, k_2]^*\}$ (for $B[-k_1, k_2](p)$ sets).

We also present four new constructions of quasi-perfect splitter sets. Finally, we give a general lower bound on the maximum size of a $B[-k_1, k_2](p)$ set for any prime $p > k_1 + k_2 + 1$ and any $k_2 \geq k_1 \geq 0$, by connecting splitter sets with independent sets of Cayley graphs.

For future work, we suggest the following questions.

1) Prove the nonexistence conjectures for purely *singular* perfect splitter sets proposed in [28], [34].
2) Determine the maximum size of $B[-k_1, k_2](n)$ sets. This problem has been completely solved for $0 \leq k_1 \leq k_2 \leq 2$ [13], [14], [31].
3) Give a characterization of nonsingular perfect $B[-k_1, k_2](p)$ sets. In [34], the authors proved that there does not exist a nonsingular perfect $B[-k_1, k_2](p)$ set when $1 \leq k_1 < k_2$ and $k_1 + k_2$ is odd. The other results are listed in Table V. In this paper, we completely determine the condition for the existence of a nonsingular perfect $B[-k_1, k_2](p)$ set, where $(k_1, k_2) \in \{(0,4), (2,4), (4,4)\}$. The next case is $(k_1, k_2) = (1, 5)$.
4) Give more constructions of perfect or quasi-perfect splitter sets. In [14, Table V], the authors listed $B[-3,3](q)$ sets of maximum size for all $q \leq 70$. Among these, there are eight nontrivial perfect or quasi-perfect $B[-3,3](q)$ sets, six of which are examples obtained from general

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

TABLE IV
THE CASE $k_1 = 0, k_2 = 3$

p	7	11	13	17	19	23	29	31	37
$\|S\|$	4	6	6	6	6	6	6	6	6
Corollary V.1	2	2	2	3	3	4	5	5	6
$\alpha(G)$	2	2	3	4	5	5	8	8	12
a maximum independent set (maximum splitter set)	{1,6}	{1,5}	{1,4,11}	{1,4,13,16}	{1,6,8,14,15}	{1,4,5,6,7}	{1,5,6,7,8, 11,19,26}	$\{1,4,9,10,14,23,25,26\}$	$\{1,6,8,10,11,14,23,26,27,29,31,36\}$

TABLE V
EXISTENCE OF NONSINGULAR PERFECT SPLITTER SETS

Nonsingular perfect splitter sets	Necessary and sufficient conditions	Remarks
$B[-k,k](p)$, where k is an odd prime	$p \equiv 1 \pmod{2\mu k}$ and $\left\|\left\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod{k} : j \in [1,k]\right\}\right\| = k$	Theorem 3.2 of [34]
$B[0,k](p)$, where k is an odd prime	$p \equiv 1 \pmod{\mu k}$ and $\left\|\left\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod{k} : j \in [1,k]\right\}\right\| = k$	Theorem 3.3 of [34]
$B[-k_1,k_2](p)$, $\gcd(\frac{p-1}{k_1+k_2}, k_1+k_2) = 1$	$p \equiv 1 \pmod{\mu(k_1+k_2)}$ and $\left\|\left\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod{k} : j \in [-k_1,k_2]^*\right\}\right\| = k_1+k_2$	Theorem 3.5 of [34]
$B[0,2](p)$	$p \equiv 1 \pmod{2}$ and $\mathrm{ord}_p(2)$ is even	Theorem 2 of [13]
$B[-2,2](p)$	$p \equiv 1 \pmod{4}$ and $v_2(\mathrm{ord}_p(2)) \geq 2$	Corollary 3 of [14]
$B[-1,3](p)$	$p \equiv 5 \pmod{8}$, 6 is a quartic residue modulo p	Theorem 4.4 of [32]
	$p \equiv 1 \pmod{8}$, $\mathrm{ord}_p(-\frac{3}{2})$ is odd and $4 \mid \mathrm{ord}_p(2)$	Theorem 4.5 of [32]
$B[-2,4](p)$	$p \equiv 1 \pmod{6}$, $\mathrm{ord}_p(-\frac{3}{4})$ is odd and $2 \notin \langle 6,8\rangle$	Theorem III.1
$B[-4,4](p)$	$p \equiv 1 \pmod{8}$ and $\pm 4 \notin \langle 6,16\rangle$	Theorem III.2
$B[0,4](p)$	$p \equiv 1 \pmod{4}$ and $4 \notin \langle 6,16\rangle$	Theorem III.3

theorems in the same paper. In this paper, we give a construction of quasi-perfect $B[-k,k](p(2k+2))$ sets in Theorem IV.2, where $p \in [k+1, 2k-1]$ is a prime. This gives a quasi-perfect $B[-3,3](40)$ set $\{1,4,9,17,25,33\}$ as in Example 1, which is different from the one $\{1,4,5,7,9,17\}$ given in [14, Table V]. There is still one more quasi-perfect splitter set given in [14, Table V], that is, $B[-3,3](18) = \{1,4\}$. We wonder whether this example could be generalized to an infinite family.

5) Find more constructions of splitter sets of maximum size. One may try to generalize the splitter sets listed in Table V of [14].

ACKNOWLEDGEMENT

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. In particular, we thank one of the reviewers for introducing us the reference [17]. The authors would also like to thank Prof. Moshe Schwartz, the associate editor, for his excellent editorial job.

REFERENCES

[1] L. Babai, "Spectra of Cayley graphs," *Journal of Combinatorial Theory. Series B*, vol. 27, no. 2, pp. 180–189, 1979.

[2] S. R. Blackburn and J. F. McKee, "Constructing k-radius sequences," *Mathematics of Computation*, vol. 81, no. 280, pp. 2439–2459, 2012.

[3] A. Bondy and M. Murty, *Graph Theory*, 1st ed., ser. Graduate Texts in Mathematics. Springer-Verlag London, 2008, vol. 244.

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

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

[6] W. contributors, "Bunyakovsky conjecture," https://en.wikipedia.org/w/index.php?title=Bunyakovsky_conjecture&oldid=898182463, date of last revision: 21 May 2019 22:43 UTC.

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

[8] C. Godsil and G. Royle, *Algebraic Graph Theory*, 1st ed., ser. Graduate Texts in Mathematics. Springer-Verlag New York, 2001, vol. 207.

[9] D. Hickerson and S. Stein, "Abelian groups and packing by semicrosses," *Pacific Journal of Mathematics*, vol. 122, no. 1, pp. 95–109, 1986.

[10] W. Imrich, "On the connectivity of Cayley graphs," *Journal of Combinatorial Theory. Series B*, vol. 26, no. 3, pp. 323–326, 1979.

[11] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., ser. Graduate Texts in Mathematics. Springer-Verlag New York, 1990, vol. 84.

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

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

[14] T. Klove, J. Luo, and S. Yari, "Codes correcting single errors of limited magnitude," *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2206–2219, 2012.

[15] L. Lovász, "Three short proofs in graph theory," *Journal of Combinatorial Theory, Series B*, vol. 19, no. 3, pp. 269–271, 1975.

[16] S. Martirossian, "Single-error correcting close packed and perfect codes," in *Proceedings of 1st INTAS International Seminar on Coding Theory and Combinatorics*, 1996, pp. 90–115.

[17] A. Munemasa, "On perfect t-shift codes in abelian groups," *Des. Codes Cryptogr.*, vol. 5, no. 3, pp. 253–259, 1995.

[18] M. Schwartz, "Quasi-cross lattice tilings with applications to flash memory," *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2397–2405, 2012.

[19] ——, "On the non-existence of lattice tilings by quasi-crosses," *European Journal of Combinatorics*, vol. 36, pp. 130–142, 2014.

[20] M. Shahzamanian, M. Shirmohammadi, and B. Davvaz, "Roughness in cayley graphs," *Information Sciences*, vol. 180, no. 17, pp. 3362–3372, 2010.

[21] S. Stein, "Factoring by subsets," *Pacific Journal of Mathematics*, vol. 22, no. 3, pp. 523–541, 1967.

[22] ——, "Packings of $\mathbb{R}^n$ by certain error spheres," *IEEE Transactions on Information Theory*, vol. 30, no. 2, pp. 356–363, 1984.

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2952370, IEEE Transactions on Information Theory

[23] S. Stein and S. Szabó, *Algebra and Tiling: Homomorphisms in the Service of Geometry*, ser. Carus Mathematical Monographs. Mathematical Association of America, 1994, vol. 25.
[24] S. Szabó and A. Sands, *Factoring Groups into Subsets*, ser. Lecture Notes in Pure and Applied Mathematics. Boca Raton, FL, USA: CRC Press, 2009, vol. 257.
[25] S. Szabó, "Some problems on splittings of groups," *Aequationes Mathematicae*, vol. 30, no. 1, pp. 70–79, Dec 1986.
[26] ——, "Some problems on splittings of groups II," *Proceedings of the American Mathematical Society*, vol. 101, no. 4, pp. 585–591, 1987.
[27] U. Tamm, "Splittings of cyclic groups and perfect shift codes," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 2003–2009, 1998.
[28] A. J. Woldar, "A reduction theorem on purely singular splittings of cyclic groups," *Proceedings of the American Mathematical Society*, vol. 123, no. 10, pp. 2955–2959, 1995.
[29] D. Xie and J. Luo, "Asymmetric single magnitude four error correcting codes," *CoRR*, vol. abs/1903.01148, 2019.
[30] ——, "Correcting codes for asymmetric single magnitude four error," *CoRR*, vol. abs/1905.02570, 2019.
[31] S. Yari, T. Kløve, and B. Bose, "Some codes correcting unbalanced errors of limited magnitude for flash memories," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7278–7287, 2013.
[32] P. Yuan and K. Zhao, "On the existence of perfect splitter sets," *CoRR*, vol. abs/1903.00118, 2019.
[33] T. Zhang and G. Ge, "New results on codes correcting single error of limited magnitude for flash memory," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4494–4500, 2016.
[34] ——, "On the nonexistence of perfect splitter sets," *IEEE Transactions on Information Theory*, vol. 64, no. 10, pp. 6561–6566, 2018.
[35] T. Zhang, X. Zhang, and G. Ge, "Splitter sets and k-radius sequences," *IEEE Transactions on Information Theory*, vol. 63, no. 12, pp. 7633–7645, 2017.

Zuo Ye is currently a Ph.D. student at University of Science and Technology of China, Hefei, Anhui, P. R. China. His research interests include combinatorics, coding theory, and their interactions.

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.

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, quantum information theory, and their interactions. She is on the Editorial Board of *Journal of Combinatorial Designs*. 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 combinatorics, coding theory, information security, and their interactions.

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.

0018-9448 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.