New Results on Codes Correcting Single Error of Limited Magnitude for Flash Memory

Tao Zhang and Gennian Ge

Abstract— **Some physical effects that limit the reliability and performance of multilevel flash memories induce errors that have low magnitudes and are dominantly asymmetric. This motivated the application of the asymmetric limited magnitude error model in flash memory. In this paper, we present a new construction of quasi-perfect codes for such errors, and we also study the perfect codes with symmetric errors. Moreover, we show some nonexistence results on perfect codes for correcting single error of limited magnitude.**

Index Terms— **Flash memory, limited magnitude error, splitter set.**

I. Introduction

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

To scale the storage density of flash memories, the multilevel memory cell is used to increase the number of stored bits in a cell. Thus, each multilevel memory cell stores $\log_2(q)$ bits regarded to a symbol over a discrete alphabet of size q. The chief disadvantage of flash memories is their inherent asymmetry between cell programming—charge injection into cells, and cell erasure—charge removal from cells. This asymmetry causes significant error sources to change cell levels in one dominant direction. Moreover, many reported common flash error mechanisms induce errors whose magnitudes are small and independent of the alphabet size, which may be significantly larger than the typical error magnitude. Thus, the flash errors strongly motivated the application of the asymmetric limited magnitude error model to flash memory [2], [5]. In this model, a symbol a over the alphabet $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$ may be changed during transmission into $a + e \in \mathbb{Z}_q$, where $-k_1 \leq e \leq k_2$, and $k_1 \geq 0$, $k_2 \geq 1$ are integers. Codes correcting limited magnitude errors have been studied in a number of papers (see [1], [3], [5]–[9], [13] and the references therein).

For the existence of such codes correcting limited magnitude errors, a construction of perfect codes for $k_1 = 0$ can be found in [6]. In [7], the authors give a construction of perfect and quasi-perfect codes for $k_1 = k_2$. Constructions of codes for $1 \leq k_1 < k_2$ can be found in [7] and [9]. In this paper, we present a new construction of quasi-perfect codes for $1 \leq k_1 < k_2$, which generalizes most of these constructions.

There are also some nonexistence results for perfect codes. In [8], the author proves that there does not exist a nonsingular perfect code for $1 \leq k_1 = k_2 - 1$. In [9], the author shows that for $q \leq 1000$, apart from the known constructions, there is no perfect code with $k_1 = 1,\ k_2 = 3$ except for 13 remaining unresolved cases. In this paper, we show that there is no nonsingular perfect code with $1 \leq k_1 \leq k_2$, $(k_1 + 1)k_1 > k_2$ and $k_1 + k_2$ odd. We also prove that there does not exist a nonsingular perfect code for $k_1 = 1, k_2 = 4$ and $k_1 = 1$, $k_2 = 6$. Moreover, we give a necessary condition for the existence of nonsingular perfect codes with $k_1 = 1, k_2 = 3$ and $k_1 = 2, k_2 = 4$. By applying this result, we rule out 4 of the remaining unsolved cases in [9].

This paper is organized as follows. Section II recalls some definitions and results. Section III gives a new construction of quasi-perfect codes for $1 \leq k_1 \leq k_2$. In Section IV, we give a characterization of nonsingular perfect codes for $k_1 = k_2 \in \{3, 5\}$. In Section V, we show the nonexistence of certain perfect codes. Section VI concludes the paper.

II. Preliminaries

Following Yari et al. [13], let a, b be integers with $a \leq b$, and $\mathbb{Z}_q$ be the ring of integers modulo q. We also let

$$[a, b] = \{a, a+1, a+2, \cdots, b\},$$
$$[a, b]^* = \{a, a+1, a+2, \cdots, b\}\backslash\{0\}.$$

Let k_1, k_2 be integers such that $0 \leq k_1 \leq k_2$. In the (k_1, k_2, q) limited magnitude error channel, an element $a \in \mathbb{Z}_q$ may be changed into any element of the set

$$\{(a+e) \pmod q \mid e \in [-k_1, k_2]\}.$$

For convenience we set $M = [-k_1, k_2]^*$.

For a set $B = \{b_1, b_2, \cdots, b_n\} \subset \mathbb{Z}_q^r$, we define a linear code C_B as

$$C_B = \left\{(x_1, x_2, \cdots, x_n) \in \mathbb{Z}_q^n \mid \sum_{i=1}^{n} x_i b_i \equiv 0 \pmod q\right\}.$$

Manuscript received January 15, 2016; revised April 30, 2016; accepted June 17, 2016. Date of publication June 21, 2016; date of current version July 12, 2016. G. Ge was supported by the National Natural Science Foundation of China under Grant 11431003 and Grant 61571310.

T. Zhang is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China, and also with the School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China (e-mail: tzh@zju.edu.cn).

G. Ge is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China, and also with the Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China (e-mail: gnge@zju.edu.cn).

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

Digital Object Identifier 10.1109/TIT.2016.2582759

If an error e occurs in position j, that is, $(x_1, x_2, \cdots, x_n)$ is changed into $(y_1, y_2, \cdots, y_n)$ where $y_j = x_j + e$ and $y_i = x_i$ for $i \neq j$, then

$$\sum_{i=1}^{n} y_i b_i \equiv eb_j + \sum_{i=1}^{n} x_i b_i \equiv eb_j \pmod{q}.$$

This sum is called the syndrome of the error. Then the set of syndromes for a single error is

$$MB = \{eb \in \mathbb{Z}_q^r \mid e \in M, b \in B\}.$$

If all these syndromes are distinct and non-zero, that is, $MB \subset \mathbb{Z}_q^r \backslash \{0\}$ and $|MB| = (k_1 + k_2)|B|$, then C_B can correct any single limited magnitude error and we call B an (r, q, k_1, k_2) splitter set. In [13], the authors give a construction of (r, q, k_1, k_2) splitter set from $(1, q, k_1, k_2)$ splitter set. In this paper, we focus on $(1, q, k_1, k_2)$ splitter set.

Following the terminology of [13], a $(1, q, k_1, k_2)$ splitter set is called a $B[-k_1, k_2](q)$ set. Therefore, a $B[-k_1, k_2](q)$ set of size n is a set B such that all the sets

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

have $k_1 + k_2$ nonzero elements, and they are disjoint. In particular, we have

$$q \geq (k_1 + k_2)n + 1$$

and so

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

A $B[-k_1, k_2](q)$ set is called perfect if $n = \frac{q-1}{k_1+k_2}$. Clearly, a perfect set can exist only if $q \equiv 1 \pmod{k_1 + k_2}$. If $q \not\equiv 1 \pmod{k_1+k_2}$ and $n = \lfloor \frac{q-1}{k_1+k_2} \rfloor$, then B is called quasi-perfect. The reader can also find the research of perfect $B[-k_1, k_2](q)$ sets in [4] and [10]–[12], which are not in a coding theoretic context.

The paper [8] suggests that we distinguish two types of perfect $B[-k_1, k_2](q)$ sets.

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

We also have the following two useful theorems.

Theorem 2 [9]: If there is a perfect $B[-k_1, k_2](q)$ set and some positive integer $d|q$, $\gcd(d, k_2!) = 1$, then $(k_1+k_2)d|(q-d)$, and there is a perfect $B[-k_1, k_2](q/d)$ set.

Theorem 3 [13]: 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

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

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 p dividing q. The following lemma is a powerful tool to derive some necessary conditions for the existence of a perfect $B[-k_1, k_2](p)$ set.

Lemma 4: Let p be a prime, k_1, k_2 be integers such that $1 \leq k_1 \leq k_2$, set $M = [-k_1, k_2]^*$. If B is a perfect $B[-k_1, k_2](p)$ set, then B satisfies the following conditions:

1) *for any $a \in \mathbb{Z}_p^*$, $|B \cap aM| = 1$;*
2) *If $i \in B$, then $-i, \pm 2i, \cdots, \pm k_2 i \notin B$.*

Proof: Note that B is perfect if and only if the $|B|(k_1+k_2) = p-1$ products $bm,\ b \in B, m \in M$ are distinct and nonzero.

(i) We only need to show that for each $a \in \mathbb{Z}_p^*$ there is a unique pair of (b, m) with $b \in B$ and $m \in M$ such that $b = am$.

If there exist $b_1, b_2 \in B$, $m_1, m_2 \in M$ 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 B is perfect, we conclude that $b_1 = b_2$ and $m_1 = m_2$. Hence we have shown the uniqueness.

For any $b \in B$, $m \in M$, there exists a unique $a \in \mathbb{Z}_p^*$ such that $b = am$. Since $|B|(k_1+k_2) = p-1$, this now shows that for any $a \in \mathbb{Z}_p^*$ there is a unique pair of (b, m) with $b \in B$ and $m \in M$ such that $b = am$.

(ii) Let $i \in B$ and $m \in [2, k_2]$, then $m \cdot i = 1 \cdot (mi)$. By the uniqueness of product for perfect B, we can conclude that $mi \notin B$. Similarly, for $i \in B$ and $m \in [1, k_2]$, we have $m \cdot i = (-1) \cdot (-mi)$ and so $-mi \notin B$. ■

III. A Construction of Quasi-Perfect $B[-k_1, k_2](q)$ Sets

The following construction is a generalization of [13, Th. 4] and the proof is similar. For the sake of completeness, we give the proof. We first give some notations. For an odd prime p, a primitive root g modulo p, and an integer b not divisible by p, there exists a unique integer $l \in [0, p-2]$ such that $g^l \equiv b \pmod{p}$. It is known as the index of b relative to the base g, and it is denoted by $\mathrm{ind}_g(b)$.

Theorem 5: Let p be a prime, k_1, k_2, t be integers such that $0 \leq k_1 \leq k_2$, $t|\gcd(k_1, k_2)$ and $\frac{k_1+k_2}{t}|(p-1)$. For $0 \leq i \leq t-1$, let $T_i = \{x | x \equiv i \pmod{t},\ x \in [-k_1, k_2]^*\}$, then $|T_i| = \frac{k_1+k_2}{t}$. Let g be a primitive root modulo p such that $g \equiv 1 \pmod{t}$, and let $\theta = \gcd\{\mathrm{ind}_g(k) \mid k \in [-k_1, k_2]^*\}$. If

$$|\{\frac{\mathrm{ind}_g(k)}{\theta} \pmod{\frac{k_1+k_2}{t}} \mid k \in T_i\}| = \frac{k_1+k_2}{t}$$

for $0 \leq i \leq t-1$ and v is a positive integer such that $v|\theta$, $\frac{v(k_1+k_2)}{t}|(p-1)$ and $\gcd(\frac{\theta}{v}, \frac{k_1+k_2}{t}) = 1$, then

$$\left\{ g^{\frac{v(k_1+k_2)}{t}i+j} \pmod{tp} \mid i \in [0, \frac{t(p-1)}{v(k_1+k_2)} - 1],\ j \in [0, v-1] \right\}$$

is a quasi-perfect $B[-k_1, k_2](tp)$ set. In particular, if $t = 1$, then the above set is a perfect $B[-k_1, k_2](p)$ set.

Proof: Suppose that

$$rg^{\frac{v(k_1+k_2)}{t}i_1+j_1} \equiv sg^{\frac{v(k_1+k_2)}{t}i_2+j_2} \pmod{tp},$$

TABLE I

EXAMPLES OF QUASI-PERFECT $B[-k_1,k_2](tp)$ SETS FROM THEOREM 5 WITH $t \geq 2$

k_1	k_2	t	p
2	2	2	7, 11, 19, 23, 31, 43, 47, 59, 67, 71
2	6	2	557, 653, 677, 1373, 1733, 1877, 1997, 2237, 2693, 3413
4	4	2	5, 29, 53, 101, 149, 173, 197, 269, 293, 317
4	8	2	1171, 3511, 4003, 9319, 12907, 15031, 17851, 21787, 22051, 24223
3	3	3	23, 31, 47, 71, 79, 103, 127, 151, 167, 191
3	9	3	941, 5981, 6221, 12941, 18749, 19421, 26669, 27509, 28901, 29021

where $r,s \in [-k_1,k_2]^*$, $i_1,i_2 \in [0, \frac{t(p-1)}{\upsilon(k_1+k_2)}-1]$ and j_1, $j_2 \in [0,\upsilon-1]$. Noting that $g \equiv 1 \pmod{t}$, we have $r \equiv s \pmod{t}$, hence $r,s \in T_l$ for some $0 \leq l \leq t-1$.

Since

$$rg^{\frac{\upsilon(k_1+k_2)}{t}i_1+j_1} \equiv sg^{\frac{\upsilon(k_1+k_2)}{t}i_2+j_2} \pmod{p},$$

we have

$$\begin{aligned}&\mathrm{ind}_g(r)+\frac{\upsilon(k_1+k_2)}{t}i_1+j_1\\ &\quad\equiv \mathrm{ind}_g(s)+\frac{\upsilon(k_1+k_2)}{t}i_2+j_2 \pmod{p-1}.\end{aligned}$$

Reducing this modulo υ, we get

$$j_1 \equiv j_2 \pmod{\upsilon},$$

which implies $j_1=j_2$ since $j_1,j_2 \in [0,\upsilon-1]$. Therefore, we obtain

$$\mathrm{ind}_g(r) \equiv \mathrm{ind}_g(s) \pmod{\frac{\upsilon(k_1+k_2)}{t}}$$

and so

$$\frac{\mathrm{ind}_g(r)}{\upsilon} \equiv \frac{\mathrm{ind}_g(s)}{\upsilon} \pmod{\frac{(k_1+k_2)}{t}}.$$

Noting that $\gcd(\frac{\theta}{\upsilon},\frac{k_1+k_2}{t})=1$, we obtain $r=s$, and then $i_1=i_2$. ■

We give some examples to illustrate our construction.

Example 6: Let $p=73$, $k_1=2$, $k_2=2$ and $t=2$. Then $g=5$ is a primitive root modulo p. We also have $\mathrm{ind}_g(1)=0$, $\mathrm{ind}_g(2)=8$, $\mathrm{ind}_g(-1)=36$, *and* $\mathrm{ind}_g(-2)=44$. *Hence $\theta=4$ and we have*

$$\frac{\mathrm{ind}_g(-1)}{4} \equiv 1 \pmod{2},\quad \frac{\mathrm{ind}_g(1)}{4} \equiv 0 \pmod{2},$$

and

$$\frac{\mathrm{ind}_g(-2)}{4} \equiv 1 \pmod{2},\quad \frac{\mathrm{ind}_g(2)}{4} \equiv 0 \pmod{2}.$$

Then taking $\upsilon=4$ in Theorem 5 gives that

$$\{5^{8i+j} \pmod{146} \mid i \in [0,8],\ j \in [0,3]\}$$

is a quasi-perfect $B[-2,2](146)$ set.

Example 7: Let $p=557$, $k_1=2$, $k_2=6$ and $t=2$. Then $g=3$ is a primitive root modulo p. We also have $\mathrm{ind}_g(1)=0$, $\mathrm{ind}_g(2)=363$, $\mathrm{ind}_g(3)=1$, $\mathrm{ind}_g(4)=170$, $\mathrm{ind}_g(5)=207$, $\mathrm{ind}_g(6)=364$, $\mathrm{ind}_g(-1)=278$ *and* $\mathrm{ind}_g(-2)=85$. *Hence $\theta=1$ and we have*

$$\begin{aligned}\mathrm{ind}_g(-1)\equiv 2 \pmod{4},\ \mathrm{ind}_g(1)\equiv 0 \pmod{4},\\ \mathrm{ind}_g(3)\equiv 1 \pmod{4},\ \mathrm{ind}_g(5)\equiv 3 \pmod{4},\end{aligned}$$

and

$$\begin{aligned}\mathrm{ind}_g(-2)\equiv 1 \pmod{4},\ \mathrm{ind}_g(2)\equiv 3 \pmod{4},\\ \mathrm{ind}_g(4)\equiv 2 \pmod{4},\ \mathrm{ind}_g(6)\equiv 0 \pmod{4}.\end{aligned}$$

Then taking $\upsilon=1$ in Theorem 5 gives that

$$\{3^{4i} \pmod{1114} \mid i \in [0,138]\}$$

is a quasi-perfect $B[-2,6](1114)$ set.

Table I lists some parameters for which the conditions of Theorem 5 are satisfied. It seems that when $\frac{k_1+k_2}{t}$ is even, there are infinitely many primes p satisfying the conditions of Theorem 5.

We have computed to check the conditions of Theorem 5 when $0<k_1\leq k_2$, $k_1+k_2\leq 12$, $t|\gcd(k_1,k_2)$ and $\frac{k_1+k_2}{t}$ is odd, but we do not find any $p \leq 5000$ satisfying the conditions. Hence, we pose the following conjecture.

Conjecture 8: Let p be a prime, k_1,k_2,t be integers such that $0<k_1\leq k_2$, $t|\gcd(k_1,k_2)$ and $\frac{k_1+k_2}{t}|(p-1)$. For $0\leq i\leq t-1$, let $T_i=\{x|x\equiv i \pmod{t},\ x\in[-k_1,k_2]^*\}$. Let g be a primitive root modulo p such that $g\equiv 1 \pmod{t}$, and let $\theta=\gcd\{\mathrm{ind}_g(k) \mid k\in[-k_1,k_2]^*\}$. If $|\{\frac{\mathrm{ind}_g(k)}{\theta} \pmod{\frac{k_1+k_2}{t}} \mid k\in T_i\}|=\frac{k_1+k_2}{t}$ for $0\leq i\leq t-1$, then $\frac{k_1+k_2}{t}$ is even.

IV. A CHARACTERIZATION OF PERFECT $B[-k,k](q)$ SETS WITH SMALL k

As we have pointed out that, in order to classify nonsingular perfect $B[-k,k](q)$ sets, we only need to determine nonsingular perfect $B[-k,k](p)$ sets for all primes p. In [7], the authors have completely determined the maximal $B[-2,2](q)$ sets. In this section, we consider nonsingular perfect $B[-k,k](q)$ sets with $k=3,5$. In the following sections of this paper, we always use $\langle a,b,\cdots,c\rangle$ to denote the subgroup of $\mathbb{Z}_p^*$ generated by a, b, $\cdots$, and c.

Theorem 9: Let p be a prime of the form $p=6l+1$, where l is an odd number. Let g be a primitive root modulo p and $\theta=\gcd\{\mathrm{ind}_g(\lambda) \mid \lambda\in[-3,3]^*\}$. Then there exists a perfect $B[-3,3](p)$ set if and only if

$|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod 6 \mid \lambda \in [-3,3]^*\}| = 6$. *Moreover, if* $|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod 6 \mid \lambda \in [-3,3]^*\}| = 6$, *let* v *be a positive integer such that* $v|\theta$, $6v|(p-1)$ *and* $\gcd(\frac{\theta}{v}, 6) = 1$, *then*

$$\left\{ g^{6vi+j} \pmod p \mid i \in [0, \frac{(p-1)}{6v} - 1],\ \ j \in [0, v-1] \right\}$$

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

Proof: If $|\{\frac{\mathrm{ind}_g(k)}{\theta} \pmod 6 \mid k \in [-3,3]^*\}| = 6$, then the existence result follows from Theorem 5 (or [7, Th. 2]).

If B is a perfect $B[-3,3](p)$ set, let $M = \{\pm1, \pm2, \pm3\}$, $M' = \{1,2,3\}$ and $\pm B = B \cup (-B)$. By Lemma 4, for any $a \in \mathbb{Z}_p^*$, $|B \bigcap aM| = 1$. It is easy to see that $|B \cap aM| = 1$ is equivalent to $|\pm B \cap aM'| = 1$.

Assume $1 \in \pm B$, if $r \in \pm B$, then $2r, 3r \notin \pm B$. Since $6r = 1 \cdot (6r) = 2 \cdot (3r) = 3 \cdot (2r)$, then $6r \in \pm B$. Note that $|\pm B \cap 2rM'| = 1$ and $|\pm B \cap 6rM'| = 1$, which implies $4r, 12r \notin \pm B$. Then $8r \in \pm B$ since $|\pm B \cap 4rM'| = 1$. As a consequence $\langle 6, 8 \rangle \subseteq \pm B$. Since $1 \in \pm B$, we have $\pm2, \pm3 \notin \pm B$ and then $\pm2, \pm3 \notin \langle 6,8 \rangle$. Note that $2 \notin \langle 6,8\rangle$ and $2^3 \in \langle 6,8 \rangle$, so we have $2\langle 6,8\rangle$ has order 3 in the quotient group $\mathbb{Z}_p^*/\langle 6,8\rangle$. We can also compute to obtain that $4\langle 6,8\rangle = 3\langle 6,8\rangle$, hence $\langle 2\langle 6,8\rangle\rangle = \{\langle 6,8\rangle, 2\langle 6,8\rangle, 3\langle 6,8\rangle\}$.

If $-1 \notin \langle 6,8\rangle$, assume $\langle 6,8\rangle = \langle g^a\rangle$ for some integer a. We have $-1\langle 6,8\rangle$ has order 2 in the quotient group $\mathbb{Z}_p^*/\langle 6,8\rangle$. Then $\langle -1,2,6,8\rangle = \{\pm1,\pm2,\pm3\}\langle 6,8\rangle = \langle g^{\frac{a}{6}}\rangle$ since $[\langle -1,2,6,8\rangle : \langle 6,8\rangle] = 6$. Therefore $|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod 6 \mid \lambda \in [-3,3]^*\}| = 6$, where $\theta = a/6$.

If $-1 \in \langle 6,8\rangle$, assume $\langle 6,8\rangle = \langle g^a\rangle$ for some integer a. Then $a|3l$ since $-1 \in \langle 6,8\rangle$ and $-1 = g^{3l}$. Note that $2a \nmid 3l$, hence $-1 \notin \langle g^{2a}\rangle$, then $\langle -1\rangle \cap \langle g^{2a}\rangle = \{1\}$. Since $\gcd(3l, 2a) = a$, we have $\langle 6,8\rangle = \langle g^a\rangle = \langle g^{3r}, g^{2a}\rangle = \langle -1\rangle \times \langle g^{2a}\rangle = \{\pm1\}\langle g^{2a}\rangle$. Then $\langle 2,6,8\rangle = \{\pm1,\pm2,\pm3\}\langle g^{2a}\rangle = \langle g^{\frac{a}{3}}\rangle$ since $[\langle 2,6,8\rangle : \langle 6,8\rangle] = 3$. Therefore $|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod 6 \mid \lambda \in [-3,3]^*\}| = 6$, where $\theta = a/3$. ■

Theorem 10: Let p *be a prime of the form* $p = 10l + 1$, *where* l *is and odd number. Let* g *be a primitive root modulo* p *and* $\theta = \gcd\{\mathrm{ind}_g(\lambda) \mid \lambda \in [-5,5]^*\}$. *Then there exists a perfect* $B[-5,5](p)$ *set if and only if* $|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod{10} \mid \lambda \in [-5,5]^*\}| = 10$. *Moreover, if* $|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod{10} \mid \lambda \in [-5,5]^*\}| = 10$, *let* v *be a positive integer such that* $v|\theta$, $10v|(p-1)$ *and* $\gcd(\frac{\theta}{v}, 10) = 1$, *then*

$$\left\{ g^{10vi+j} \pmod p \mid i \in [0, \frac{(p-1)}{10v} - 1],\ \ j \in [0, v-1] \right\}$$

is a perfect $B[-5,5](p)$ *set.*

Proof: If $|\{\frac{\mathrm{ind}_g(k)}{\theta} \pmod{10} \mid k \in [-5,5]^*\}| = 10$, then the existence result follows from Theorem 5 (or [7, Th. 2]).

If B is a perfect $B[-5,5](p)$ set, let $M = \{\pm1, \pm2, \pm3, \pm4, \pm5\}$, $M' = \{1,2,3,4,5\}$ and $\pm B = B \cup (-B)$. A lengthy routine discussion deduces that $\langle 6,20,32\rangle \subseteq \pm B$ or $\langle 10,12,32\rangle \subseteq \pm B$.

We first assume that $\langle 6,20,32\rangle \subseteq \pm B$. Since $1 \in \pm B$, we have $\pm2,\pm3,\pm4,\pm5 \notin \pm B$ and then $\pm2,\pm3,\pm4,\pm5 \notin \langle 6,20,32\rangle$. Note that $2 \notin \langle 6,20,32\rangle$ and $2^5 \in \langle 6,20,32\rangle$, so we have $2\langle 6,20,32\rangle$ has order 5 in the quotient group $\mathbb{Z}_p^*/\langle 6,20,32\rangle$. We can also compute to obtain that $8\langle 6,20,32\rangle = 5\langle 6,20,32\rangle$ and $16\langle 6,20,32\rangle = 3\langle 6,20,32\rangle$, hence $\langle 2\langle 6,20,32\rangle\rangle = \{\langle 6,20,32\rangle, 2\langle 6,20,32\rangle, 3\langle 6,20,32\rangle, 4\langle 6,20,32\rangle, 5\langle 6,20,32\rangle\}$.

If $-1 \notin \langle 6,20,32\rangle$, assume $\langle 6,20,32\rangle = \langle g^a\rangle$ for some integer a. We have $-1\langle 6,20,32\rangle$ has order 2 in the quotient group $\mathbb{Z}_p^*/\langle 6,20,32\rangle$. Then $\langle -1,2,6,20,32\rangle = \{\pm1,\pm2,\pm3,\pm4,\pm5\}\langle 6,20,32\rangle = \langle g^{\frac{a}{10}}\rangle$ since $[\langle -1,2,6,20,32\rangle : \langle 6,20,32\rangle] = 10$. Therefore $|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod{10} \mid \lambda \in [-5,5]^*\}| = 10$, where $\theta = a/10$.

If $-1 \in \langle 6,20,32\rangle$, assume $\langle 6,20,32\rangle = \langle g^a\rangle$ for some integer a. Then $a|5l$ since $-1 \in \langle 6,20,32\rangle$ and $-1 = g^{5l}$. Note that $2a \nmid 5l$, hence $-1 \notin \langle g^{2a}\rangle$, then $\langle -1\rangle \cap \langle g^{2a}\rangle = \{1\}$. Since $\gcd(5l, 2a) = a$, we have $\langle 6,20,32\rangle = \langle -1\rangle \times \langle g^{2a}\rangle = \{\pm1\}\langle g^{2a}\rangle$. Then $\langle 2,6,20,32\rangle = \{\pm1,\pm2,\pm3,\pm4,\pm5\}\langle g^{2a}\rangle = \langle g^{\frac{a}{5}}\rangle$ since $[\langle 2,6,20,32\rangle : \langle 6,20,32\rangle] = 5$. Therefore $|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod{10} \mid \lambda \in [-5,5]^*\}| = 10$, where $\theta = a/5$.

For the case $\langle 10,12,32\rangle \subseteq \pm B$, the discussions are similar. ■

Based on the above two theorems, we propose the following conjecture.

Conjecture 11: Let p *be a prime of the form* $p = 2kl + 1$, *where* k *and* l *are odd numbers. Let* g *be a primitive root modulo* p *and* $\theta = \gcd\{\mathrm{ind}_g(\lambda) \mid \lambda \in [-k,k]^*\}$. *Then there exists a perfect* $B[-k,k](p)$ *set if and only if* $|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod{2k} \mid \lambda \in [-k,k]^*\}| = 2k$. *Moreover, if* $|\{\frac{\mathrm{ind}_g(\lambda)}{\theta} \pmod{2k} \mid \lambda \in [-k,k]^*\}| = 2k$, *let* v *be a positive integer such that* $v|\theta$, $2kv|(p-1)$ *and* $\gcd(\frac{\theta}{v}, 2k) = 1$, *then*

$$\left\{ g^{2kvi+j} \pmod p \mid i \in [0, \frac{(p-1)}{2kv} - 1],\ \ j \in [0, v-1] \right\}$$

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

V. Nonexistence of Certain Perfect $B[-k_1,k_2](q)$ Sets

Note that there exists a nonsingular perfect $B[-k_1,k_2](q)$ set if and only if there exists a nonsingular perfect $B[-k_1,k_2](p)$ set for each prime $p|q$. In this section, we show that there does not exist a nonsingular perfect $B[-k_1,k_2](q)$ set with $1 \le k_1 \le k_2$, $(k_1+1)k_1 > k_2$ and $k_1 + k_2$ odd. We also prove that there is no nonsingular perfect $B[-1,4](q)$ and $B[-1,6](q)$ set. Moreover, we give a necessary condition for the existence of perfect $B[-1,3](q)$ and $B[-2,4](q)$ sets.

Theorem 12: Let p *be a prime and* k_1, k_2 *be integers such that* $1 \le k_1 \le k_2$. *If* $(k_1+1)k_1 > k_2$ *and* $k_1 + k_2$ *is an odd integer, then there does not exist a perfect* $B[-k_1,k_2](p)$ *set.*

Proof: Let B be a perfect $B[-k_1,k_2](p)$ set. Without loss of generality, assume $1 \in B$. If $M = [-k_1,k_2]^*$, then by Lemma 4, for any $a \in \mathbb{Z}_p^*$, $|B \bigcap aM| = 1$, and $-1, \pm2, \cdots, \pm k_2 \notin B$.

Taking $a = 2, -2, \cdots, k_2, -k_2$, we have:

there exists exactly one of $\{\pm2(\lfloor\frac{k_2}{2}\rfloor + 1), \cdots, \pm2k_1, 2(k_1+1), \cdots, 2k_2\}$ contained in B,

there exists exactly one of $\{\pm2(\lfloor\frac{k_2}{2}\rfloor + 1), \cdots, \pm2k_1, -2(k_1+1), \cdots, -2k_2\}$ contained in B,

$\cdots$

there exists exactly one of $\{\pm(k_1+1)(\lfloor\frac{k_2}{k_1+1}\rfloor+1),\cdots,\pm(k_1+1)k_1,(k_1+1)^2,\cdots,(k_1+1)k_2\}$ contained in B,

there exists exactly one of $\{\pm(k_1+1)(\lfloor\frac{k_2}{k_1+1}\rfloor+1),\cdots,\pm(k_1+1)k_1,-(k_1+1)^2,\cdots,-(k_1+1)k_2\}$ contained in B,

$\dots$

there exists exactly one of $\{\pm k_2\cdot 2,\cdots,\pm k_2k_1,k_2(k_1+1),\cdots,k_2^2\}$ contained in B,

there exists exactly one of $\{\pm k_2\cdot 2,\cdots,\pm k_2k_1,-k_2(k_1+1),\cdots,-k_2^2\}$ contained in B.

For any $2\le i\le k_1$ and $(k_1+1)\le j\le k_2$, if $ij\in B$, then $\pm i(\lfloor\frac{k_2}{i}\rfloor+1),\cdots,\pm ik_1\notin B$, hence there exists $(k_1+1)\le l\le k_2$ such that $-il\in B$. Therefore there are an even number of elements having the form $\pm ij$ with $2\le i\le k_1$, $(k_1+1)\le j\le k_2$ contained in B.

Let $S=\{j\mid(k_1+1)\le j\le k_2, ij\in B$ for some $i\in[-k_2,k_2]^*\}$, and $S'=\{j\mid(k_1+1)\le j\le k_2, ij\in B$ for some $i\in[-k_1,k_1]^*\}$. Then $S=\{j\mid(k_1+1)\le j\le k_2\}$ and $S'\subsetneqq S$ since $|S'|$ is even.

Let $T\supseteq S'$ be a subset of S with size k_2-k_1-1. Assume $S\backslash T=\{t\}$ and $T=\{t_1,\cdots,t_{k_2-k_1-1}\}$. Since $T\subset S$, then $\pm tt_l\notin B$ for $1\le l\le k_2-k_1-1$ and $\pm ti\notin B$ for $1\le i\le k_1$. Note that there exists exactly one of $\{\pm t(\lfloor\frac{k_2}{t}\rfloor+1),\cdots,\pm tk_1,t(k_1+1),\cdots,tk_2\}$ contained in B and there exists exactly one of $\{\pm t(\lfloor\frac{k_2}{t}\rfloor+1),\cdots,\pm tk_1,-t(k_1+1),\cdots,-tk_2\}$ contained in B. Hence $\pm t^2\in B$, which contradicts Lemma 4. ■

From Theorem 12, we can immediately get the following corollary, which can also be found in [8].

Corollary 13: There does not exist a nonsingular perfect $B[-(k-1),k](q)$ set for $k\ge 2$.

Theorem 14: Let p be a prime, then there does not exist a perfect $B[-1,4](p)$ set.

Proof: Let p be a prime, $M=\{-1,1,2,3,4\}$. Suppose B is a perfect $B[-1,4](p)$ set. Without loss of generality, assume $1\in B$, then $-1,\pm2,\pm3,\pm4\notin B$. From Lemma 4, for any $a\in\mathbb{Z}_p^*$, $|B\cap aM|=1$. Taking $a=2,-2,3,-3,4,-4$, 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 $|B\cap -8M|=1$. ■

By combining Theorems 12 and 14, we can get the following result.

Corollary 15: There does not exist a nonsingular perfect $B[-(k-3),k](q)$ set for $k\ge 4$.

Theorem 16: Let p be a prime, then there does not exist a perfect $B[-1,6](p)$ set.

Proof: Let p be a prime, $M=\{-1,1,2,3,4,5,6\}$ and B be a perfect $B[-1,6](p)$ set. Without loss of generality, assume $1\in B$, then $-1,\pm2,\pm3,\pm4,\pm5,\pm6\notin B$. By Lemma 4, for any $a\in\mathbb{Z}_p^*$, $|B\cap aM|=1$. Taking $a=2,-2,3,-3,4,-4,5,-5,6,-6$, we have:

there exists exactly one of $\{8,10,12\}$ contained in B,

there exists exactly one of $\{-8,-10,-12\}$ contained in B,

there exists exactly one of $\{9,12,15,18\}$ contained in B,

there exists exactly one of $\{-9,-12,-15,-18\}$ contained in B,

there exists exactly one of $\{8,12,16,20,24\}$ contained in B,

there exists exactly one of $\{-8,-12,-16,-20,-24\}$ contained in B,

there exists exactly one of $\{10,15,20,25,30\}$ contained in B,

there exists exactly one of $\{-10,-15,-20,-25,-30\}$ contained in B,

there exists exactly one of $\{12,18,24,30,36\}$ contained in B,

there exists exactly one of $\{-12,-18,-24,-30,-36\}$ contained in B.

Then there exist exactly two of $\{\pm8,\pm10,\pm12\}$ contained in B, and for any i $(i=8,10,12)$, at most one of i and $-i$ is contained in B. Below, we split our discussion into six cases.

Case 1: $8,-10\in B$.

Then we can deduce that $-8,10,\pm12,\pm16,\pm24,-15,-25,\pm20,\pm30\notin B$. Hence there exists exactly one of $\{18,36\}$ contained in B and there exists exactly one of $\{-18,-36\}$ contained in B, which contradicts the fact $|B\cap 18M|=1$ and $|B\cap -18M|=1$.

Case 2: $8,-12\in B$.

Then we can compute to obtain that $8,9,-12,-25,30\in B$ and $\pm10,-20,-30,-40,-50,-60\notin B$, which contradicts the fact that $|B\cap -10M|=1$.

Case 3: $10,-12\in B$.

Then we can compute to obtain that $10,-12,16,18,-25\in B$ and $\pm8,-16,-24,-32,-40,-48\notin B$, which contradicts the fact that $|B\cap -8M|=1$.

For the cases $-8,10\in B$, $-8,12\in B$ and $-10,12\in B$, the discussions are similar. ■

Note that Theorems 12, 14 and 16 partially confirm Conjecture 8. Based on these theorems, we also have the following conjecture.

Conjecture 17: There does not exist a nonsingular perfect $B[-k_1,k_2](q)$ set with $1\le k_1\le k_2$ and k_1+k_2 odd.

The following two theorems give a necessary condition for the existence of perfect $B[-1,3](q)$ and $B[-2,4](q)$ sets.

Theorem 18: Let p be a prime of the form $4n+1$, and let $\langle 4,6\rangle$ be the subgroup of $\mathbb{Z}_p^*$ generated by 4 and 6. If $\langle 4,6\rangle \bigcap \{\pm 2,\pm 3\} \neq \emptyset$, then there does not exist a perfect $B[-1,3](p)$ set.

Proof: Let p be a prime of the form $4n+1$, B be a perfect $B[-1,3](p)$ set and $M=\{-1,1,2,3\}$. Set $\pm B = B \cup -B$. Assume $1 \in B$, then $-1, \pm 2, \pm 3 \notin B$, which yields that $\pm 2, \pm 3 \notin \pm B$. If $r \in B$ then $-r, \pm 2r, \pm 3r \notin B$. Hence $6r \in B$ or $-6r \in B$.

If $6r \in B$, we can compute to obtain that $-4r, -9r \in B$. Similarly, if $-6r \in B$, then $4r, 9r \in B$. As a consequence, $\langle 6,4,9\rangle = \langle 6,4\rangle \subseteq \pm B$. Therefore $\langle 4,6\rangle \cap \{\pm 2,\pm 3\} \subseteq \pm B \cap \{\pm 2, \pm 3\} = \emptyset$, which contradicts our assumption. ■

In [9], the author shows that, for $q \leq 1000$, apart from the known constructions [13], there is no perfect $B[-1,3](q)$ set, except possibly for

$$q = 81, 89, 97, 241, 405, 445, 457, 485, 577, 729, 881, 937, 941.$$

For $q = 941$, we can construct a perfect $B[-1,3](q)$ set from Theorem 5. For the remaining 12 cases, we can rule out 4 of them by Theorem 18. That is, we have the following corollary.

Corollary 19: For $q \leq 1000$, apart from the known constructions [13], there is no perfect $B[-1,3](q)$ set, except possibly for

$$q = 81, 97, 241, 405, 457, 485, 577, 729.$$

Proof: We only need to show that there is no perfect $B[-1,3](q)$ set for $q = 89, 445, 881, 937$.

For $q = 89, 881, 937$, the result follows from Theorem 18, and for the case $q = 445 = 5 \times 89$, the result follows from Theorems 18 and 2. ■

Theorem 20: Let p be a prime of the form $6n+1$, and let $\langle 6,8\rangle$ be the subgroup of $\mathbb{Z}_p^*$ generated by 6 and 8. If $\langle 6,8\rangle \bigcap \{\pm 2,\pm 3,\pm 4\} \neq \emptyset$, then there does not exist a perfect $B[-2,4](p)$ set.

Proof: Let p be a prime of the form $6n+1$, B be a perfect $B[-2,4](p)$ set and $M=\{-2,-1,1,2,3,4\}$. Set $\pm B = B \cup -B$. Assume $1 \in B$, then $-1, \pm 2, \pm 3, \pm 4 \notin B$, and $\pm 2, \pm 3, \pm 4 \notin \pm B$. If $r \in B$ then $-r, \pm 2r, \pm 3r, \pm 4r \notin B$. By Lemma 4, there exists exactly one of $\{6r, 8r\}$ contained in B and there exists exactly one of $\{-6r, -8r\}$ contained in B. Then we get that $\langle 6,8\rangle \subseteq \pm B$. As a consequence $\langle 6,8\rangle \bigcap \{\pm 2,\pm 3,\pm 4\} \subseteq \pm B \cap \{\pm 2,\pm 3,\pm 4\} = \emptyset$, which contradicts our assumption. ■

By Theorem 20, for primes p of the form $6n+1$ and $p \leq 1000$, apart from the known constructions [13], there is no perfect $B[-2,4](p)$ set, except possibly for

$$p = 37, 181, 241, 313, 337, 349, 409, 421, 541, 877, 919, 937.$$

VI. Conclusion

In this paper, we consider the $B[-k_1,k_2](q)$ sets which can be used to construct codes correcting single error of limited magnitude.

Not much has been known about quasi-perfect $B[-k_1,k_2](q)$ sets. We give a new construction of quasi-perfect $B[-k_1,k_2](q)$ sets. For the case $k_1 = k_2$, we give a characterization of nonsingular perfect $B[-k,k](q)$ sets when $k = 3,5$ for certain q. We conjecture that this is also true for general k. In Section V, we show that there does not exist a nonsingular perfect $B[-k_1,k_2](q)$ set with $1 \leq k_1 \leq k_2$, $(k_1+1)k_1 > k_2$ and k_1+k_2 odd. We also prove that there does not exist a nonsingular perfect $B[-1,4](q)$ and $B[-1,6](q)$ set. We conjecture that there does not exist nonsingular perfect $B[-k_1,k_2](q)$ set with k_1+k_2 odd. It should be noted that we can prove these conjectures for small k (or k_1,k_2) by using similar methods, but it is difficult to get the general result.

Finally, we give a necessary condition for the existence of perfect $B[-1,3](q)$ and $B[-2,4](q)$ sets. By applying this result, we solve 4 of the 13 undetermined cases remaining in [9].

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. 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.

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

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

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

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

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

[12] S. Stein and S. Szabó, *Algebra and Tiling* (Carus Mathematical Monographs), vol. 25. Washington, DC, USA: MAA, 1994.

[13] 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.

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

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. His research interests include the constructions of combinatorial designs and their applications to codes and crypts.

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