Some codes correcting single symmetric errors of limited magnitude

Torleiv Kløve, Jinquan Luo, Somaye Yari

Some codes correcting single symmetric errors of limited magnitude

Torleiv Kløve, Jinquan Luo, and Somaye Yari

Department of Informatics, University of Bergen, Norway.
{Torleiv.Klove,Jinquan.Luo,Somaye.Yari}@ii.uib.no

Abstract. An error model with symmetric errors of limited magnitude is considered. Limited magnitude means that the size of any error is limited by a number smaller (usually much smaller) than the alphabet size. Several constructions of codes correcting single error are given. In some cases, the codes are perfect or quasi-perfect.

Keywords: Code, symmetric error, limited magnitude error

1 Introduction

In the symmetric error model, a symbol a over the alphabet

$$\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$$

may be modified during transmission into another symbol $b \in \mathbb{Z}_q$. For some applications, the error magnitude $|b-a|$ is not likely to exceed a certain threshold λ. A model for an asymmetric channel with limited errors was introduced in [1]. A modified model, where wrap-around error are also possible, was considered in [2] and [5]. For this model, a can be changed to $(a+e) \pmod q$, where $0 \le e \le \lambda$ (asymmetric errors) or $0 \le |e| \le \lambda$ (symmetric errors). In [5] and [6], classes of systematic codes correcting single asymmetric errors on this channel are given. The constructions are based on $B[\lambda](q)$ sets. In [3] codes for correcting limited magnitude errors, symmetric and asymmetric, are studied.

In this paper, we consider construction of codes correcting single symmetric limited error. The construction is based on the analogue of $B[\lambda](q)$ sets which we call $C[\lambda](q)$ sets. We first give the definition of $C[\lambda](q)$ sets and the code construction. Then we give several classes of $C[\lambda](q)$ sets.

2 $C[\lambda](q)$ sets and the code construction

For integers a, b, where $a \le b$, we let

$$[a, b] = \{a, a+1, a+2, \ldots, b\}.$$

For an integer $b \in [1, q-1]$, let

$$\Psi(b) = \{ab \bmod q \mid a \in [-\lambda, -1] \cup [1, \lambda]\}. \tag{1}$$

A $C[\lambda](q)$ set of size m is a set of m distinct integers $b_0, b_1, \ldots, b_{m-1} \in [1, q-1]$ such that all the sets $\Psi(b_j)$, $j = 0, 1, \ldots, m-1$ have 2λ nonzero elements, and they are disjoint.

In particular, it is necessary to have

$$q - 1 \geq \left| \bigcup_{j=0}^{m-1} \Psi(b_j) \right| = 2\lambda m.$$

If $\bigcup_{j=0}^{m-1} \Psi(b_j) = [1, q-1]$, then we say that the $C[\lambda](q)$ set is *perfect*. A necessary condition for a perfect $C[\lambda](q)$ set to exist is of course that $q \equiv 1 \pmod{2\lambda}$.

In general, $m \leq (q-1)/(2\lambda)$ and so $m \leq \lfloor (q-1)/(2\lambda) \rfloor$. If $q \not\equiv 1 \pmod{2\lambda}$, then we call a $C[\lambda](q)$ set of maximal size $\lfloor (q-1)/(2\lambda) \rfloor$ *quasi-perfect*.

A $B[\lambda](q)$ set is defined similarly, except that a in (1) is restricted to $a \in [1, \lambda]$.

In [5] it was shown that we can get a code correcting a single limited magnitude symmetric error based on a $C[\lambda](q)$ set as follows: let

$$B = \{b_i \mid 0 \leq i \leq m-1\}$$

be a $C[\lambda](q)$ set. Let H be the $r \times n$ parity check matrix whose columns are all possible vectors over $\mathbb{Z}_q^r$ with the first non-zero element in B and let C be the null space of H^T. Then this code can correct a single symmetric error of magnitude at most λ.

The goal of this paper is to give new constructions of $C[\lambda](q)$ sets, some of them are modifications of the constructions of $B[\lambda](q)$ sets given in [5] and [6].

Stein et al. [4], [7], [8] studied $C[\lambda](q)$ sets, which they called packings of crosses in Z_q. In particular, [7] considers perfect $C[\lambda](q)$ sets, and it is mainly shown that perfect sets do not exist in some cases. But also some existence results are given. In our notations, [4] and [8] consider asymptotic expressions when $l \to \infty$ for the smallest q such that there exists a $C[\lambda](q)$ set of size m.

3 On perfect $C[\lambda](p)$ sets for primes p

Stein [7] showed (Corollary 5.3) that if q is a prime, then a perfect $C[2](q)$ set exists if and only if 4 divides the order of 2 modulo q. Here, we will consider explicit constructions of perfect $C[\lambda](q)$ sets for general λ.

For an odd prime p, a primitive root g modulo p, and an integer a not divisible by p, there exists a unique integer $\iota \in [0, p-2]$ such that $g^\iota \equiv a \pmod{p}$. It is known as the index of a relative to the base g, and it is denoted by $\mathrm{ind}_g(a)$. In particular, $\mathrm{ind}_g(-1) = (p-1)/2$. Let

$$\mu = \mu_{\lambda,p} = \gcd\left(\mathrm{ind}_g(-1), \mathrm{ind}_g(2), \mathrm{ind}_g(3), \ldots, \mathrm{ind}_g(\lambda)\right).$$

We see that μ divides $\mathrm{ind}_g(-1) + \mathrm{ind}_g(i) \equiv \mathrm{ind}_g(-i) \pmod{p-1}$ for $i \in [1, \lambda]$. Thus the set

$$H = \{g^{i\mu} \bmod p \mid i \geq 0\}$$

is the multiplicative subgroup of $\mathbb{Z}_p^*$ generated by the integers $-1, 2, 3, \ldots, \lambda$. The size of H is $n = (p-1)/\mu$. In particular, μ does not depend on g.

Theorem 1. *Let $\lambda \geq 2$ and let $p > \lambda$ be a prime. If a perfect $C[\lambda](p)$ set exists, then 2λ divides $(p-1)/\mu$, that is*

$$p \equiv 1 \pmod{2\mu\lambda}.$$

Proof. Let S be a perfect $C[\lambda](q)$ set. We decompose $\mathbb{Z}_p^*$ into the μ cosets of H. For any coset aH and any $x \in aH$, we have $ix \bmod p \in aH$ for $i \in [1, \lambda] \cup [-\lambda, -1]$. Therefore $|S \cap aH| \leq \lfloor n/(2\lambda) \rfloor$. In total we get

$$\frac{p-1}{2\lambda} = |S| \leq \left\lfloor \frac{n}{2\lambda} \right\rfloor \mu = \left\lfloor \frac{n}{2\lambda} \right\rfloor \cdot \frac{p-1}{n} \leq \frac{n}{2\lambda} \cdot \frac{p-1}{n} = \frac{p-1}{2\lambda}$$

which implies that 2λ divides n. □

Theorem 2. *Let $\lambda \geq 2$. Let p be a prime such that $p \equiv 1 \pmod{2\mu\lambda}$, where $\mu = \mu_{\lambda,p}$. Let g be a primitive root modulo p. If*

$$\left\{ \frac{\mathrm{ind}_g(j)}{\mu} \bmod \lambda \mid j \in [1, \lambda] \right\} = [0, \lambda - 1],$$

and ν is a positive integer such that $\nu | \mu$ and $\gcd(\mu/\nu, \lambda) = 1$, then

$$X = \left\{ g^{\nu\lambda i + j} \bmod p \mid i \in \left[0, \frac{p-1}{2\nu\lambda} - 1\right], j \in [0, \nu - 1] \right\}$$

is a perfect $C[\lambda](p)$ set.

Proof. First we note that since

$$\frac{\mathrm{ind}_g(j)}{\nu} = \frac{\mu}{\nu} \cdot \frac{\mathrm{ind}_g(j)}{\mu}$$

and $\gcd(\mu/\nu, \lambda) = 1$, we get

$$\left\{ \frac{\mathrm{ind}_g(j)}{\nu} \bmod \lambda \mid j \in [1, \lambda] \right\} = [0, \lambda - 1]. \tag{2}$$

Clearly, $rg^{\nu\lambda i + j} \not\equiv 0 \pmod{p}$ for any $r \in [1, \lambda]$. Suppose that

$$rg^{\nu\lambda i + j} \equiv sg^{\nu\lambda i' + j'} \pmod{p}$$

where $r, s \in [-\lambda, -1] \cup [1, \lambda]$, $i, i' \in \left[0, \frac{p-1}{2\nu\lambda} - 1\right]$, and $j, j' \in [0, \nu - 1]$. Then

$$\mathrm{ind}_g(r) + \nu\lambda i + j \equiv \mathrm{ind}_g(s) + \nu\lambda i' + j' \pmod{p-1}. \tag{3}$$

Modulo ν we get

$$j \equiv j' \pmod{\nu}$$

which implies that $j = j'$ since $j, j' \in [0, \nu - 1]$. Therefore, from (3) we obtain

$$\mathrm{ind}_g(r) \equiv \mathrm{ind}_g(s) \pmod{\nu\lambda}$$

and so

$$\frac{\mathrm{ind}_g(r)}{\nu} \bmod \lambda = \frac{\mathrm{ind}_g(s)}{\nu} \bmod \lambda.$$

Combined with (2), this implies that $r = s$ or $r = -s$.

If $r = s$, (3) implies that $i \equiv i' \pmod{\frac{p-1}{\nu\lambda}}$ and so $i = i'$. Otherwise $r = -s \neq 0$. Therefore

$$\nu\lambda i \equiv \frac{p-1}{2} + \nu\lambda i' \pmod{p-1}$$

which implies $\frac{p-1}{2} \mid \nu\lambda(i - i')$. Since $0 < |i - i'| \leq \frac{p-1}{2\nu\lambda} - 1$ and $0 < |\nu\lambda(i - i')| < \frac{p-1}{2}$, then we have $i = i'$ which is a contradiction. □

Example 1. Let $\lambda = 3$ and $p = 37$. Then $g = 2$ is a primitive root and $\mu = 1$. Hence $B = \{2^{3i} \bmod 37 \mid 0 \leq i \leq 5\}$ is a $C[3](37)$ set.

4 A construction of $C[\lambda](q)$ sets

For $\lambda \geq 2$, let

$$\Pi_\lambda = \{p \mid p \text{ is a prime and } p \leq \lambda\},$$

and

$$P_\lambda = \prod_{p \in \Pi_\lambda} p.$$

Theorem 3. *If $\mu = \nu P_\lambda + 1$ or $\mu = \nu P_\lambda - 1$, and $q = (2\lambda + 1)\mu$, then the set*

$$C = \{(2\lambda + 1)i + 1 \mid i \in [0, \mu - 1]\}$$

is a $C[\lambda](q)$ set.

Proof. Let $\mu = \nu P_\lambda + \omega$, where $\omega \in \{1, -1\}$. Suppose that

$$r((2\lambda + 1)i + 1) \equiv s((2\lambda + 1)j + 1) \pmod{(2\lambda + 1)\mu}, \tag{4}$$

where $r, s \in [-\lambda, \lambda]$, $(r, s) \neq (0, 0)$. Then

$$r \equiv s \pmod{2\lambda + 1}$$

and so $r = s \neq 0$. Then (4) implies that

$$ri \equiv rj \pmod{\mu}.$$

Since $\gcd(r, \mu) = 1$, we get

$$i \equiv j \pmod{\mu}$$

which implies that $i = j$. □

5 On maximal $C[2](p)$ sets

Define $N_2(q)$ to be the maximal size of a $C[2](q)$ set. In this section, we will construct maximal size $C[2](q)$ sets for all q and determine $N_2(q)$ meanwhile. Denote by

$$\mathbb{Z}_q^* = \{a \mid (a,q) = 1, 1 \le a \le q-1\}.$$

We have the following disjoint union decomposition.

$$\mathbb{Z}_q = \{0\} \bigcup_{d>1, d|q} \mathbb{Z}_q(d) \text{ with } \mathbb{Z}_q(d) = \{aq/d \,|\, a \in \mathbb{Z}_d^*\}. \tag{5}$$

5.1 The case q is odd

In this subsection we assume that q is odd. Let d be any divisor of q. Then d is odd and let $\mathrm{ord}_d(2)$ be the order of 2 in $\mathbb{Z}_d^*$, that is,

$$\mathrm{ord}_d(2) = \min\{n |\, 2^n \equiv 1 \pmod d, n > 0\}.$$

For any positive integer n, the 2-adic exponent valuation of n, denoted by $v_2(n)$, is the exact power of 2 dividing n, that is, $n = 2^{v_2(n)}n'$ with n' odd. Suppose q has the prime factorization $q = \prod_{i=0}^{t} q_i$ where

$$q_i = \prod_{j=1}^{r_i} p_{i,j}^{e_{i,j}} \tag{6}$$

such that $p_{i,j}$ are distinct primes, $e_{i,j} \ge 1$, and $v_2(\mathrm{ord}_{p_{i,j}}(2)) = i$ for $1 \le j \le r_i$.

In [6] we showed the following result.

Lemma 1. *(i) For odd $d = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$, with p_i distinct odd primes, we have*

$$\mathrm{ord}_d(2) = \mathrm{lcm}(\mathrm{ord}_{p_1^{e_1}}(2), \mathrm{ord}_{p_2^{e_2}}(2), \cdots, \mathrm{ord}_{p_s^{e_s}}(2)).$$

In particular, $v_2(\mathrm{ord}_d(2)) = i$ if and only if $\max\limits_{1\le j\le s} v_2(\mathrm{ord}_{p_j^{e_j}}(2)) = i$.

(ii) For any odd prime p, suppose $2^{\mathrm{ord}_p(2)} = 1 + p^{u_p}s_p$ with $p \nmid s_p$. Then

$$\mathrm{ord}_{p^k}(2) = \begin{cases} \mathrm{ord}_p(2), & \text{if } k \le u_p \\ p^{k-u_p}\,\mathrm{ord}_p(2), & \text{if } k > u_p. \end{cases}$$

For an odd integer d, define $\langle 2\rangle_d$ to be the cyclic subgroup of $\mathbb{Z}_d^*$ generated by 2. In order to construct maximal size $C[2](q)$ sets, we need to determine if $-1 \in \langle 2\rangle_d$ or not for each d with $d|q$. The following result provides an easy criterion.

Lemma 2. *Suppose that $d = \prod\limits_{i=1}^{n} p_i^{e_i}$ is odd, where $p_1, p_2, \ldots, p_n$ are distinct primes, and $e_i \ge 1$ for $1 \le i \le n$. Then $-1 \in \langle 2\rangle_d$ if and only if*

$$v_2(\mathrm{ord}_{p_1}(2)) = v_2(\mathrm{ord}_{p_2}(2)) = \cdots = v_2(\mathrm{ord}_{p_n}(2)) \ge 1.$$

Proof. If $-1 \in \langle 2 \rangle_d$, then $2^h \equiv -1 \pmod{d}$ for some h which implies $2^h \equiv -1 \pmod{p_i}$ and $2^{2h} \equiv 1 \pmod{p_i}$. Hence $\mathrm{ord}_{p_i}(2) \mid 2h$. Also, $\mathrm{ord}_{p_i}(2) \nmid h$ (otherwise $2^h \equiv 1 \pmod{p_i}$). Therefore $v_2(\mathrm{ord}_{p_i}(2)) = v_2(2h) = 1 + v_2(h) \geq 1$ which is independent of i.

On the other hand, if

$$t := v_2(\mathrm{ord}_{p_1}(2)) = v_2(\mathrm{ord}_{p_2}(2)) = \cdots = v_2(\mathrm{ord}_{p_n}(2)) \geq 1,$$

then we have $t = v_2(\mathrm{ord}_{p_i^{e_i}}(2))$ for $1 \leq i \leq n$ by Lemma 1 (ii) and $t = v_2(\mathrm{ord}_d(2))$ by Lemma 1 (i). Since the multiplicative group $\mathbb{Z}^*_{p_i^{e_i}}$ is cyclic, we have $2^{\mathrm{ord}_{p_i^{e_i}}(2)/2} \equiv -1 \pmod{p_i^{e_i}}$ which implies that

$$2^{\mathrm{ord}_d(2)/2} = \left(2^{\mathrm{ord}_{p_i^{e_i}}(2)/2}\right)^{\mathrm{ord}_d(2)/\mathrm{ord}_{p_i^{e_i}}(2)} \equiv (-1)^{\mathrm{ord}_d(2)/\mathrm{ord}_{p_i^{e_i}}(2)} = -1 \pmod{p_i^{e_i}}.$$

By the Chinese Remainder Theorem, it follows that $2^{\mathrm{ord}_d(2)/2} \equiv -1 \pmod{d}$. □

Now we can present the main result of this subsection (the proof is not included in this abstract).

Theorem 4. *For q odd, we have*

$$N_2(q) = \frac{q-1}{4} - \frac{1}{4}\left(\sum_{d \mid q_0} \frac{\varphi(d)}{\mathrm{ord}_d(2)} + 2\sum_{d \mid q_1} \frac{\varphi(d)}{\mathrm{ord}_d(2)}\right)$$

where q_0 is defined in (6).

Corollary 1. *A $C[2](q)$ perfect set exists if and only if $v_2(\mathrm{ord}_p(2)) \geq 2$ for any prime p dividing q.*

5.2 The case q is even

In the following we consider the case when q is even. For the case $q \equiv 2 \pmod{4}$, an easy observation shows the following result.

Theorem 5. *The set $S = \{1, 3, \cdots, 2m-1\}$ is a $C[2](4m+2)$-set and*

$$N_2(4m+2) = m.$$

For the case $4 \mid q$, we have a similar result as [5, Theorem 5].

Theorem 6. *For $m > 1$, we have $N_2(4m) = \lfloor \frac{m}{2} \rfloor + N_2(m)$.*

Proof. (Sketch) Let S_m be a $C[2](m)$ set of size $N_2(m)$ and

$$T_m = \{1, 3, \cdots, 2 \cdot \lfloor m/2 \rfloor - 1\}.$$

We claim that the set

$$T_m \bigcup \{4c \mid c \in S_m\}$$

is a $C[2](4m)$ set of size $\lfloor m/2 \rfloor + N_2(m)$.

First we have $N_2(4m) \geq \lfloor \frac{m}{2} \rfloor + N_2(m)$. Next, let S be a $C[2](4m)$ set and c be an element of S such that $c \equiv 2 \pmod 4$. Then there exists a unique $d \in T_m$ such that $2d \equiv c \pmod{4m}$ or $-2d \equiv c \pmod{4m}$ (but not both). Replacing c by d, we get a new $C[2](4m)$ set. Repeating this procedure, we can get a $C[2](4m)$-set S' without elements congruent to 2 modulo 4. It is easy to verify that the set

$$\{c/4 \mid c \in S' \backslash T_m\}$$

is a $C[2](m)$ set. Hence $N_2(4m) \leq \lfloor \frac{m}{2} \rfloor + N_2(m)$ and the result follows. □

Combining Theorems 4, 5, and 6, we have a satisfactory answer on construction of maximal size $C[2](q)$ sets for all q.

6 On quasi-perfect $C[\lambda](\lambda p)$ sets for primes p

An example of a construction of a quasi-perfect set is given by the following theorem.

Theorem 7. *Let $p \equiv 3 \pmod 4$ be a prime and $a \equiv 1 \pmod \lambda$ be a positive integer. If*

(i) $\mathrm{ord}_p(a) = \frac{p-1}{2}$,
(ii) for any i, $1 \leq i < \lambda/2$, $i(\lambda - i)$ is quadratic residue mod p,

then the set

$$\left\{a^i \mid 0 \leq i < (p-1)/2\right\}$$

is a quasi-perfect $C[\lambda](\lambda p)$ set.

Proof. Suppose

$$ra^u \equiv sa^v \pmod{\lambda p} \tag{7}$$

for some $r, s \in [-\lambda, \lambda]$, $(r, s) \neq (0, 0)$ and $u, v \in [0, (p-1)/2 - 1]$. Without loss of generality, we may assume that $r \geq s$ and $r \geq 0$. From (7) we get

$$r \equiv s \pmod \lambda$$

which implies $r = s$, $(r, s) = (\lambda, -\lambda)$, or $r = s + \lambda$.
Case I: $r = s \neq 0$. In this case (7) gives us

$$a^u \equiv a^v \pmod p$$

which implies $u = v$ since $\mathrm{ord}_p(a) = (p-1)/2$ and $u, v \in [0, (p-1)/2 - 1]$.
Case II: $(r, s) = (\lambda, -\lambda)$. In this case we have

$$a^{v-u} \equiv -1 \pmod p$$

which implies that -1 is a quadratic residue. This is impossible since $p \equiv 3 \pmod 4$.
Case III: $(r, s) = (\lambda, 0)$. In this case we have

$$a^u \equiv 0 \pmod p$$

which is impossible. The case $(r, s) = (0, -\lambda)$ is similar.
Case IV: $r = s + \lambda$ with $s = -\sigma$, where $\sigma, r \in [1, \lambda - 1]$. Then

$$(\lambda - \sigma) \equiv -a^{v-u}\sigma \pmod p$$

which leads to a contradiction since $\sigma(\lambda - \sigma)$ is a quadratic residue and $-a^{v-u}$ is quadratic non-residue.

The condition (ii) and the quadratic reciprocity law give necessary congruences for p. These can be combined with the condition $p \equiv 3 \pmod 4$. Numerical result indicates that if these conditions are satisfied, then we can always find $a \equiv 1 \pmod \lambda$ satisfying (i).

For $\lambda = 3, 4, 5$ we get the following results:

- If $\lambda = 3$ we must have $p \equiv 7 \pmod 8$. In particular, $C[3](3p)$ sets exist for the primes $p = 7, 23, 31, 47, 71, 79, 103, 127$.
- If $\lambda = 4$ we must have $p \equiv 11 \pmod{12}$. In particular, $C[4](4p)$ sets exist for the primes $p = 11, 23, 47, 59, 71, 83$.
- If $\lambda = 5$ we must have $p \equiv 19, 23 \pmod{24}$. In particular, $C[5](5p)$ sets exist for the primes $p = 19, 23, 43, 47, 67, 71$.

7 Minimal q for which there exists a $C[\lambda](q)$ set of size 2

Theorem 8. *The minimal q for which a $C[\lambda](q)$ set of size 2 exists is*

$$q = (\lambda + 1)^2 + 1 \ .$$

Proof. If $\{a, b\}$ is a $C_1[\lambda](q)$ set, then for all $x, y \in [0, \lambda]$, the positive residues

$$ax + by \pmod q$$

are different. Indeed, if

$$ax + by \equiv ax' + by' \pmod q$$

for $x, y, x', y' \in [0, \lambda]$ with $(x, y) \neq (x', y')$, then

$$a(x - x') \equiv b(y' - y) \pmod q$$

with $x - x', y' - y \in [-\lambda, \lambda]$ and $(x - x', y' - y) \neq (0, 0)$. Since there are $(\lambda + 1)^2$ distinct choices for $x, y \in [0, \lambda]$, we have $q \geq (\lambda + 1)^2$.

If $q = (\lambda+1)^2$ and $\{a, b\}$ is a $C[\lambda](q)$ set. Then

$$\{ax + by \pmod q \mid x, y \in [0, \lambda]\} = [0, q-1].$$

In particular,

$$\gcd(a, b, (\lambda+1)^2) = 1. \tag{8}$$

Hence there exist $x, y \in [0, \lambda]$ such that

$$(\lambda+1)a \equiv ax + by \pmod{(\lambda+1)^2}.$$

If $x > 0$, then $(\lambda+1-x)a = yb \pmod{(\lambda+1)^2}$ with $\lambda+1-x, y \in [-\lambda, \lambda]$ and $\lambda+1-x \neq 0$ which is a contradiction. Therefore, $x = 0$ which implies that

$$(\lambda+1)a \equiv by \pmod{(\lambda+1)^2}. \tag{9}$$

Similarly, there exists an $x \in [0, \lambda]$ such that

$$(\lambda+1)b \equiv ax \pmod{(\lambda+1)^2}. \tag{10}$$

By (9) and (10) we have

$$axy \equiv b(\lambda+1)y \equiv a(\lambda+1)^2 \equiv 0 \pmod{(\lambda+1)^2}$$

which implies that

$$\frac{(\lambda+1)^2}{\gcd(a, (\lambda+1)^2)} \mid xy.$$

In the same way, we have

$$\frac{(\lambda+1)^2}{\gcd(b, (\lambda+1)^2)} \mid xy.$$

From (8) we conclude that $(\lambda+1)^2 \mid xy$. Since $x, y \in [0, \lambda]$, this implies that $xy = 0$. Hence $x = 0$ or $y = 0$. If $x = 0$, then from (10) we obtain $(\lambda+1) | b$. Therefore

$$\lambda \cdot b \equiv (-1) \cdot b \pmod{(\lambda+1)^2}$$

which leads to a contradiction. Similarly, $y = 0$ also leads to a contradiction.

As a consequence, for $q = (\lambda+1)^2$, $C[\lambda](q)$ sets of size 2 do not exist. Therefore, we must have $q \geq (\lambda+1)^2 + 1$. For $q = (\lambda+1)^2 + 1$, it is easy to see that $\{1, \lambda+1\}$ is a $C[\lambda](q)$ set:

$$\begin{aligned}
&\{x \cdot 1 \mid 1 \leq |x| \leq \lambda\} \cup \{x \cdot (\lambda+1) \mid 1 \leq |x| \leq \lambda\} \\
=\,&[1, \lambda] \cup [\lambda^2 + \lambda + 2, \lambda^2 + 2\lambda + 1] \\
&\cup \{\lambda+1, 2\lambda+2, \ldots, \lambda^2+\lambda\} \cup \{\lambda+2, 2\lambda+3, \ldots, \lambda^2+\lambda+1\}.
\end{aligned}$$

□

Acknowledgement

This work is supported by the Norwegian Research Council under the grant 191104/V30. The research of Jinquan Luo is also supported by NSF of China under grant 60903036, NSF of Jiangsu Province under grant 2009182 and the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2010D12).

References

1. R. Ahlswede, H. Aydinian, L. H. Khachatrian, and L. M. G. M. Tolhuizen, "On q-ary codes correcting all unidirectional errors of a limited magnitude", Proceedings of Ninth International Workshop on Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria, pp. 20–26, June 2004.
2. Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes for asymmetric limited-magnitude errors with application to multi-level flash memories", *IEEE Trans. Information Theory*, vol. 56, pp. 1582–1595, April 2010.
3. N. Elarief and B. Bose, "Optimal, systematic, q-ary codes correcting all asymmetric and symmetric errors of limited magnitude", *IEEE Trans. Information Theory*, vol. 56, pp. 979–983, March 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, N. Elarief and B. Bose, "Systematic, single limited magnitude error correcting codes for Flash Memories", *IEEE Trans. Information Theory*, vol. 57, 2011, to appear.
6. T. Kløve, J. Luo, I. Naydenova, and S. Yari, " Some codes correcting asymmetric errors of limited magnitude", submitted manuscript.
7. S. Stein, "Factoring by subsets", *Pacific J. Math*, vol. 22, no. 3, pp. 523–541, 1967.
8. S. Stein, "Packings of R^n by certain error spheres", *IEEE Trans. Information Theory*, vol. 30, pp. 356–363, March 1984.