Codes of length two correcting single errors of limited size II

Torleiv Kløve

Department of Informatics,
University of Bergen, N-5020 Bergen, Norway

Abstract. Linear codes of length 2 over the integers modulo some integer q that can correct single errors of limited size are considered. A code can be determined by a check pair of integers. The errors e considered are in the range $-\mu \le e \le \lambda$, such a code can only exist for q sufficiently large. The main content of this note is to make this statement precise, that is, to determine "q sufficiently large" in terms of the integers $-\mu$ and λ.

Keywords: Error correcting code, errors of limited size, integers modulo n.

1 Introduction

We consider linear codes that can correct unbalanced errors i.e. a symbol a over the alphabet $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ may be modified during transmission into another symbol $b \in \mathbb{Z}_q$, where $-\mu \le b - a \le \lambda$, and $\mu \ge 0$ and $\lambda \ge 1$ are integers, see [10]. Without loss of generality, we may assume that $\mu \le \lambda$ (see [11]).

Codes for $\mu = 0$ have been considered e.g. in [3], [4], [7], [8]. Codes for $\mu = \lambda$ have been considered e.g. in [3], [5], [9], [10]. Codes for the general unbalanced case have been considered in [1], [10], [11]. A basic building block for many of these code constructions are sets which we have called $B[-\mu, \lambda](q)$ sets. They correspond to check vectors. In this note, we consider such sets of size two, corresponding to codes of length two.

We let $q_L(-\mu, \lambda)$ be the smallest integer q such that there exists a linear code in $\mathbb{Z}_q^2$ that can correct a single error from $[-\mu, \lambda]$.

In [6] we gave some observations and conjectures based on the values of $q_L(-\mu, \lambda)$ for small values of μ and λ.

In Section 2 we give some some definitions and known results from [6]. In particular, we quote some upper bounds on $q_L(-\mu, \lambda)$ for $\mu < \lambda < 2\mu$.

In Section 3 we give some upper bounds on $q_L(-\mu, \lambda)$ for $\lambda > 2\mu$. This is the main result of this paper.

2 Definitions and known results

Let q be a positive integer. We consider the following channel:

Our alphabet is $\mathbb{Z}_q$. Let λ and μ be integers, where $0 \le \mu \le \lambda < q - \mu$.

Let

$$[-\mu, \lambda] = \{-\mu, -\mu + 1, \ldots, \lambda - 1, \lambda\}$$

and

$$[-\mu, \lambda]^* = \{-\mu, -\mu + 1, \ldots, -1\} \cup \{1, 2, \ldots, \lambda\}.$$

An element $a \in \mathbb{Z}_q$ may be changed into $a + e$, where $e \in [-\mu, \lambda]$.

Let $0 \le \mu \le \lambda$ be integers. A $B[-\mu, \lambda](q)$ set (of size 2) is a set $S = \{a, b\}$ such that all us, where $u \in [-\mu, \lambda]^*$ and $s \in S$, are distinct and non-zero.

The corresponding linear code of length 2 is

$$C_S = \{(x, y) \in \mathbb{Z}_q^2 \mid xa + yb = 0\}.$$

The size of the code is

$$|C_S| = dq \quad \text{where} \quad d = \gcd(a, b, q).$$

The set $B[-\mu, \lambda](q)$ is the set of syndroms of C_S. Hence the code can correct a single error from $[-\mu, \lambda]$.

A number of constructions of $B[-\mu, \lambda](q)$ sets are known, in particular for $\mu = 0$ and for $\mu = \lambda$, see [1]-[10].

We can reformulate the definition of $B[-\mu, \lambda](q)$ sets of size 2 by specifying the conditions to check.

Definition 1. *A set $\mathcal{B} = \{a, b\} \subseteq \mathbb{Z}_q$ is a $B[-\mu, \lambda](q)$ set if and only if*

$$\begin{aligned} & xa \not\equiv 0 \textit{ (mod } q) \textit{ for all } x \in [-\mu, \lambda]^*, & (1)\\ & xa \not\equiv ya \textit{ (mod } q) \textit{ for all } x, y \in [-\mu, \lambda]^*, x < y, & (2)\\ & xb \not\equiv 0 \textit{ (mod } q) \textit{ for all } x \in [-\mu, \lambda]^*, & (3)\\ & xb \not\equiv yb \textit{ (mod } q) \textit{ for all } x, y \in [-\mu, \lambda]^*, x < y, & (4)\\ \textit{and} \quad & xa \not\equiv yb \textit{ (mod } q) \textit{ for all } x, y \in [-\mu, \lambda]^*. & (5) \end{aligned}$$

Definition 2. *Given μ and λ, $q_L(-\mu, \lambda)$ is the smallest q for which a $B[-\mu, \lambda](q)$ set of size two exists.*

In [8] we showed that $q_L(0, \lambda) = 2\lambda + 1$ and a corresponding $B[0, \lambda](q)$ set is $\{1, q - 1\}$. In [9], we showed that $q_L(-\lambda, \lambda) = (\lambda + 1)^2 + 1$ and a corresponding $B[-\lambda, \lambda](q)$ set is $\{1, \lambda + 1\}$.

Let

$$p_{-\mu,\lambda} = (\lambda + 1)^2 - (\lambda - \mu)^2 = (\mu + 1)(2\lambda + 1 - \mu).$$

We have shown the following results:

Theorem 1. *a) [6, Theorem 1]: $q_L(-\mu, \lambda) \geq p_{-\mu,\lambda}$ for all μ, λ.*
b) [6, Theorem 2]: $q_L(-\mu, \lambda) = p_{-\mu,\lambda}$ if $\gcd(\lambda + 1, \lambda - \mu) = 1$.

We have computed $q_L(-\mu, \lambda)$ by complete search for $0 \leq \mu < \lambda \leq 20$. For these values, we gave the following observations in [6]:

1. If $\gcd(\lambda + 1, \lambda - \mu) > 1$ and $\mu < \lambda < 2\mu$, then $q_L(-\mu, \lambda) = p_{-\mu,\lambda} + \lambda - \mu$.
2. If $\gcd(\lambda + 1, \lambda - \mu) > 1$ and $\lambda > 2\mu$, then $q_L(-\mu, \lambda) = p_{-\mu,\lambda} + \mu + 1$.

Possibly these expressions are true for all μ, λ.

Upper bounds are obtained by explicit constructions. For $\mu + 1 < \lambda < 2\mu$ we gave the following result.

Theorem 2. *[6, Theorem 3]: For all μ, λ such that $\mu + 1 < \lambda < 2\mu$, we have $q_L(-\mu, \lambda) \leq p_{-\mu,\lambda} + \lambda - \mu$. If $\gcd(\lambda + 1, \lambda - \mu) > 1$, then one $B[-\mu, \lambda](p_{-\mu,\lambda} + \lambda - \mu)$ set is $\{2\lambda - \mu, 2\lambda - \mu + 1\}$.*

The goal of the following paper is to give a similar result for $\lambda > 2\mu$.

Remark. We have a related channel for the integers: any $a \in [0, q - 1]$ can be changed to $b \in [0, q - 1$ where $-\mu \leq b - a \leq \lambda$. Error in flash memories can be modeled by this channel, see e.g. [2], [10]. We see that codes correcting single errors over the channel defined over $\mathbb{Z}_q$ in particular corrects errors from $[0, q - 1]$ in the corresponding channels over the integers.

3 Upper bounds on $q_L(-\mu, \lambda)$ for $\lambda > 2\mu$.

The main result in the present paper is the following upper bound:

Theorem 3. *If $\mu \geq 1$ and $\lambda > 2\mu$, then we have*

$$q_L(-\mu, \lambda) \leq p_{-\mu,\lambda} + \mu + 1 = (\mu + 1)(2\lambda + 2 - \mu).$$

In [6, Theorem 4] we proved this in a special case, namely when $\lambda+1$ is multiple of $\mu + 1$. In that case, $\{1, 2\lambda + 1 - \mu\}$ is a $B[\mu, \lambda]((\mu + 1)(2\lambda + 2 - \mu))$ set.

To prove Theorem 3, we treat μ even and μ odd separately. For both cases, we let

$$t = 2\lambda + 2 - \mu \text{ and } q = (\mu + 1)t.$$

Lemma 1. *If μ is even, $\lambda > 2\mu$, $a = 2\lambda + 1 - \mu$, and $b = a + 2$, then $\{a, b\}$ is a $B[\mu, \lambda](q)$ set for $q = (\mu + 1)(2\lambda + 2 - \mu)$.*

Proof: We check (1)-(5) in Definition 1. We have

$$a = t - 1 \text{ and } b = t + 1.$$

Hence, we clearly get the following relations:

$$\begin{array}{lll} \text{If } x \in [-\mu, -1], & \text{then } xb \pmod t = t + x & \text{and } xa \pmod t = -x. \\ \text{If } x \in [1, \lambda], & \text{then } xb \pmod t = x & \text{and } xa \pmod t = t - x. \end{array}$$

We see that $xa \pmod t \neq 0$. In particular, $xa \pmod q \neq 0$. Hence (1) is satisfied.

Since $\lambda + \mu < t$, we see that if $x, y \in [-\mu, \lambda]$ and $x < y$, then $xa \not\equiv ya \pmod t$. In particular, $xa \not\equiv ya \pmod q$, that is, (2) is satisfied.

Similarly, (3) and (4) are satisfied.

Finally, suppose that $x, y \in [-\mu, \lambda]$ and $yb \equiv xa \pmod q$. Then $y \equiv -x \pmod t$ and so $y = -x$ and so

$$x, y \in [-\mu, \mu]^*. \tag{6}$$

Hence

$$2xt = x(a + b) = xa - yb \equiv 0 \pmod{(\mu + 1)t}$$

and so

$$2x \equiv 0 \pmod{(\mu + 1)}.$$

Since $\mu + 1$ is odd, this implies that $x \equiv 0 \pmod{(\mu + 1)}$, but this contradicts (6). Hence, (5) is satisfied.
QED

Example 1. Let $\mu = 2$ and $\lambda = 5$. We have $\gcd(\lambda + 1, \lambda - \mu) = 3$. Consider the construction in Lemma 1. We have $a = 9$, $b = 11$, $q = 30$. The code is

$$C = \{(x, y) \in \mathbb{Z}_{30}^2 \mid 9x + 11y = 0\} = \{(x, 21x) \mid x \in \mathbb{Z}_{30}\}.$$

The simplest corresponding encoding is, of course, $z \mapsto (z, 21z)$.

For $(x, y) \in \mathbb{Z}_{30}^2$, the corresponding syndrom is $9x + 11y$. For $(x, y) \in C$ and $e \in [-2, 5]$, the syndrom corresponding to the error $(e, 0)$ is

$$9(x + e) + 11y = 9x + 11y + 9e = 9e$$

and the syndrom corresponding to the error $(0, e)$ is $11e$. We give the values the syndroms in the following table.

e	-2	-1	1	2	3	4	5
$9e$	12	21	9	18	27	6	15
$11e$	8	19	11	22	3	14	25

They are all distinct, that is, the set $\{9, 11\}$ is indeed a $B[-2, 5](30)$ set.

For μ odd we find a similar, but more complicated, construction.

Lemma 2. *If $\mu = 2\nu+1$ is odd, $\lambda > 2\mu$, $a = \mu\lambda - \theta$ where $\theta = 2\nu^2$, and $b = a+1$, then $\{a, b\}$ is a $B[\mu,\lambda](q)$ set.*

Proof: First we note that

$$2a = 2\mu\lambda - (\mu-1)^2 = \mu(2\lambda - \mu + 2) - 1 = \mu t - 1, \tag{7}$$
$$2b = 2a + 2 = \mu t + 1. \tag{8}$$

Further
$$a + b = 2a + 1 = \mu t \equiv 0 \pmod{t}. \tag{9}$$

Hence,

$$2a \equiv t - 1 = 2\lambda + 2 - \mu - 1 = 2\lambda + 2 - 2\nu - 1 - 1 = 2(\lambda - \nu) \pmod{t}$$

and so, since t is odd, we get

$$a \equiv \lambda - \nu \pmod{t}. \tag{10}$$

Let $\ell = \lfloor \lambda/2 \rfloor$. From (7) and (10) we get the following relations:

$$\begin{array}{lll}
\text{If } x \in [-\nu, -1], & \text{then } 2xa \pmod{t} & = -x. \\
\text{If } x \in [-\nu-1, -1], & \text{then } (2x+1)a \pmod{t} & = \lambda - \nu - x. \\
\text{If } x \in [1, \ell], & \text{then } 2xa \pmod{t} & = t - x. \\
\text{If } x \in [0, \ell], & \text{then } (2x+1)a \pmod{t} & = \lambda - \nu - x.
\end{array}$$

Hence, (1) is satisfied.
Further,

$$\begin{array}{ll}
\{2xa \pmod{t} \mid x \in [-\nu, -1]\} & = [1, \nu] \\
\{(2x+1)a \pmod{t} \mid x \in [0, \ell]\} & = [\lambda - \nu - \ell, \lambda - \nu] \\
\{(2x+1)a \pmod{t} \mid x \in [-\nu-1, -1]\} & = [\lambda - \nu + 1, \lambda + 1] \\
\{2xa \pmod{t} \mid x \in [1, \ell]\} & = [t - \ell, t - 1]
\end{array}$$

We have
$$(t - \ell) - (\lambda + 1) = (\lambda - \nu - \ell) - \nu = \lambda - \ell - 2\nu,$$

and

$$\begin{aligned}
2(\lambda - \ell - 2\nu) &= 2\lambda - 2\ell - 2(\mu - 1) \\
&= (\lambda - 2\ell) + (\lambda - 2\mu - 1) + 3 \\
&\geq 1 + 0 + 3 > 0.
\end{aligned}$$

Hence, we see that if $x, y \in [-\mu, \lambda]$ and $x < y$, then $xa \not\equiv ya \pmod{t}$. In particular, $xa \not\equiv ya \pmod{q}$. Hence (2) is satisfied.

From (9) we get $b \equiv -a \pmod{t}$. Hence, (3) is satisfied. Further we see that if $x, y \in [-\mu, \lambda]$ and $x < y$, then $xb \not\equiv yb \pmod{t}$. In particular, $xb \not\equiv yb \pmod{q}$. Hence (4) is satisfied.

Finally, if $x, y \in [-\mu, \lambda]$ and $xa \equiv yb \pmod{q}$, then $xa \equiv yb \equiv -ya \pmod{t}$. Since t is odd, we have

$$\gcd(a, t) = \gcd(2a, t) = \gcd(2\mu t - 1, t) = 1.$$

Hence $x \equiv -y \pmod{t}$ and so $x = -y$. Therefore,

$$x, y \in [-\mu, \mu]^*. \tag{11}$$

Further, we get $xa \equiv -xb \pmod q$ and so $x(a+b) \equiv 0 \pmod q$. Hence

$$x\mu t \equiv 0 \ (\mathrm{mod}\ (\mu+1)t).$$

Therefore,

$$x\mu \equiv 0 \ (\mathrm{mod}\ \mu+1)$$

and so

$$x \equiv 0 \ (\mathrm{mod}\ \mu+1)$$

which is impossible by (11). Hence (5) is satisfied.
QED

Example 2. Let $\mu = 1$ and $\lambda = 3$. We have $\gcd(\lambda+1, \lambda-\mu) = 2$. Consider the construction in Lemma 2. Then $\nu = 0$, $\theta = 0$, $a = 3$, $b = 4$, $q = 14$. The code is

$$\begin{aligned} C =& \{(x,y) \in \mathbb{Z}_{14}^2 \mid 3x+4y=0\} \\ =& \{(2\alpha, 2\alpha+7\beta) \mid \alpha \in [0,6], \beta \in [0,1]\} \\ =& \{(0,0),(2,2),(4,4),(6,6),(8,8),(10,10),(12,12)\} \\ & \cup \{(0,7),(2,9),(4,11),(6,13),(8,1),(10,3),(12,5)\} \end{aligned}$$

We note that there is no γ such that $C = \{(x,\gamma x) \mid x \in [0,13]\}$ in this case.

The simplest corresponding encoding is $2\alpha+\beta \mapsto (2\alpha, 2\alpha+7\beta)$.

For $(x,y) \in \mathbb{Z}_{14}^2$, the corresponding syndrom is $3x+4y$. For $(x,y) \in C$ and $e \in [-1,3]$, the syndrom corresponding to the error $(e,0)$ is $3e$ and the syndrom corresponding to the error $(0,e)$ is $4e$. We give the values of the syndroms in the following table.

e	-1	1	2	3
$3e$	11	3	6	9
$4e$	10	4	8	12

As an example of decoding, suppose that $(6,11)$ received, The corresponding syndrom is $3\cdot 6+4\cdot 11 \equiv 6 \pmod{14}$. From the table we see that is corresponds to the error $(2,0)$ and so the corrected codeword is $(6,11)-(2.0) = (4,11)$. Hence $\alpha = 2$ and $\beta = 1$ and $(4,11)$ is the encoding of $2\cdot 2+1 = 5$.

We give one more example where the encoding is more complicated.

Example 3. Let $\mu = 5$ and $\lambda = 14$. We have $\gcd(\lambda+1, \lambda-\mu) = 3$. Consider the construction in Lemma 2. Then $\nu = 2$, $\theta = 8$, $a = 62$, $b = 63$, $q = 150$. We see that if (x,y) is a codeword, then $x \equiv 0 \pmod 3$ and y is even. Let $x = 3x_1$ and $y = 2y_1$. Then

$$62\cdot 3x_1 + 63\cdot 2y_1 \equiv 0 \pmod{150}$$

and so

$$31x_1 + 21y_1 \equiv 0 \pmod{25}$$

which implies that $y_1 \equiv 14x_1 \pmod{25}$. Hence the code is

$$C = \{(6\alpha+75\beta, 28\alpha+50\gamma) \mid \alpha \in [0,24], \beta \in [0,1], \gamma \in [0,2]\}$$

The simplest corresponding encoding is $6\alpha+3\beta+\gamma \mapsto (6\alpha+75\beta, 28\alpha+50\gamma)$.

References

1. Battaglioni, M., Chiaraluce, F., Kløve, T.: On non-linear codes correcting errors of limited size, Proc. Globecom, Singapore, 4-8 December 2017, 1–7. Published in IEEE Xplore.
2. Dolecek, L and Cassuto, Y, Channel coding for nonvolatile memory technologies: theoretical advances and practical considerations, Proc. of the IEEE, 105 (9), 1705-1724, 2017.
3. Elarief N., Bose, B.: Optimal, systematic, q-ary codes correcting all asymmetric and symmetric errors of limited magnitude, IEEE T Inform Theory 56, 979–983 (2010)
4. Jiang, Mateescu, R., Schwartz, M., Bruck, J.: Rank modulation for flash memories, IEEE T Inform Theory 55, 2659–2673 (2009)
5. Kløve, T.: Codes of length 2 correcting single errors of limited size, Springer LNCS 9496, 190—201 (2015)
6. Kløve, T.: Codes of length two correcting single errors of limited size, Cryptography and Communications, to appear.
7. Kløve, T., Elarief N., Bose, B.: Systematic, single limited magnitude error correcting codes for Flash Memories, IEEE T Inform Theory 57, 4477–4487 (2011)
8. Kløve, T., Luo, J., Naydenova, I., Yari, S.: Some codes correcting asymmetric errors of limited magnitude, IEEE T Inform Theory 57, 7459–7472 (2011)
9. Kløve, T., Luo, J., Yari, S.: Codes correcting single errors of limited magnitude, IEEE T Inform Theory 58, 2206–2219 (2012)
10. Schwartz, M.: Quasi-cross lattice tilings with applications to flash memory, IEEE T Inform Theory 58, 2397–2405 (2012)
11. Yari, S., Kløve, T., Bose, B.: Some linear codes correcting single errors of limited magnitude for flash memories, IEEE T Inform Theory 59, 7278–7287 (2013)