Contributions to Discrete Mathematics

Volume 16, Number 1, Pages 53–71
ISSN 1715-0868

BOUNDS ON r-IDENTIFYING CODES IN q-ARY LEE SPACE

RAMALINGAM DHANALAKSHMI AND CHINNAPILLAI DURAIRAJAN

Abstract. Identifying codes are used to locate malfunctioning processors in multiprocessor systems. In this paper, we study identifying codes in a q-ary hypercube which is used in parallel processing. Computing upper and lower bounds of $M_{r,q}(n)$, the smallest cardinality among all r-identifying codes in $\mathbb{Z}_q^n$ with respect to the Lee metric, is an important research problem in this area. Using our constructions, we produce tables for upper and lower bounds for $M_{r,q}(n)$. The upper and the lower bounds of $M_{r,4}(n)$ known only when $r = 1$ but using our results, we compute the bounds for $M_{r,4}(n)$ for all $r \geq 1$. Also we improve upon the currently known upper bounds of $M_{1,4}(n)$ due to J. L. Kim and S. J. Kim. Upper bounds of $M_{r,q}(n)$ for $q > 4$ are known previously for some cases of n. We improve some of these bounds and we also compute bounds for all n by using our results.

1. Introduction

Let $\mathbb{Z}_q$ denote the ring of integer residues modulo the positive integer q. For an element $\alpha \in \mathbb{Z}_q$, denote by $\langle \alpha \rangle$ the smallest nonnegative integer m such that $\alpha = m \cdot 1$, where 1 stands for the multiplicative unity in $\mathbb{Z}_q$. The *Lee weight* $w_L(\alpha)$ of an element $\alpha \in \mathbb{Z}_q$, is defined by

$$w_L(\alpha) = \begin{cases} \langle \alpha \rangle & \text{if } 0 \leq \langle \alpha \rangle \leq \frac{q}{2} \\ q - \langle \alpha \rangle & \text{otherwise.} \end{cases}$$

Also the *Lee distance* $d_L(\alpha, \beta)$ between two elements $\alpha, \beta \in \mathbb{Z}_q$ is defined by $d_L(\alpha, \beta) = w_L(\alpha - \beta)$. Note that $d_L(\alpha, \beta) = d_L(\beta, \alpha)$.

The Lee space $\mathbb{Z}_q^n$ is the Cartesian product of $\mathbb{Z}_q$ taken n times. We will

Received by the editors November 9, 2018), and in revised form July 17, 2020.

2010 *Mathematics Subject Classification.* 05C70, 94B65, 94C12.

Key words and phrases. Identifying Codes, q-ary Hypercubes, Code Construction, Fault Tolerance, Direct Sum.

The first author wishes to thank the Department of Science and Technology, Government of India, for their financial support under the DST-(WOS-A) Project No. SR/WOS-A/PM-1025/2014.

use the vector notation $(x_1, \ldots, x_n)$ for words in the ring $\mathbb{Z}_q^n$. For a word $x = (x_1, \ldots, x_n)$ in $\mathbb{Z}_q^n$, the *Lee weight* $w_L(x)$ is defined by

$$w_L(x) = \sum_{i=1}^{n} w_L(x_i),$$

and for $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{Z}_q^n$, the *Lee distance* between x and y is defined by

$$d_L(x, y) = \sum_{i=1}^{n} d_L(x_i, y_i) = \sum_{i=1}^{n} w_L(x_i - y_i).$$

We say that x r-covers y in $\mathbb{Z}_q^n$ if $d_L(x, y) \leq r$. Since the Lee distance function is a metric, y being r-covered by x is equivalent to x being r-covered by y. For $x \in \mathbb{Z}_q^n$, we set

$$B_r(x) = \{y \in \mathbb{Z}_q^n \mid d_L(x, y) \leq r\}$$

as the closed ball in $\mathbb{Z}_q^n$ with center at x and radius r and it is called the Lee ball with radius r centered at x. The cardinality of the Lee ball $B_r(x)$ is known to be independent of the element x and it is denoted by $V_L(n, r, q)$. For a positive integer q, by the theory of Lee codes [1], we have

$$V_L(n, r, q = 2s) = \sum_{i=0}^{\lfloor \frac{r}{s} \rfloor} (-1)^i \binom{n}{i} \sum_{j=0}^{r-si} 2^j \binom{n}{j} \binom{r - si}{j},$$

$$V_L(n, r, q = 2s + 1) = \sum_{i=0}^{r} \binom{n+1}{i} \sum_{j=0}^{\lfloor \frac{r}{s} \rfloor} (-2)^j \binom{n}{j} \binom{n - j}{r - j(s+1) - i}.$$

For more details on Lee metric, see [10].

In 1998, Karpovsky, Chakrabarty, and Levitin [2] introduced identifying codes with respect to various metrics including the Lee metric. The initial application for identifying codes was for fault diagnosis in multiprocessor systems.

Consider a q-ary n-dimensional nonbinary cube. In parallel processing, this cube has a lot of applications. In this model, each processor has two neighbors in each dimension. Therefore each processor is connected to $2n$ neighbors. Similar practical architectures are Intel's Paragon architecture [7] and MIT-Intel J-Machine [4].

While applying identifying codes, testers are positioned in the system so that faults can be localized to a unique processor. It is also applied in environmental monitoring, sensor networks, and location detection in hostile environments. More details of applications of identifying codes are given in [9].

A nonempty subset C of $\mathbb{Z}_q^n$ is called a code of length n. The I-set of a word $x \in \mathbb{Z}_q^n$ with respect to the code C is defined to be

$$I_r(x) = B_r(x) \cap C.$$

A code C is an r*-covering code* in $\mathbb{Z}_q^n$ if $I_r(x) \neq \varnothing$ for all $x \in \mathbb{Z}_q^n$. Equivalently, C is an r-covering code if $\cup_{c \in C} B_r(c) = \mathbb{Z}_q^n$. Code C is said to be an r*-separating code* if $I_r(x) \neq I_r(y)$ for all $x, y \in \mathbb{Z}_q^n$ with $x \neq y$ and an r*-identifying code* if it is both r-covering and r-separating.

The smallest possible cardinality of an r-identifying code of length n is denoted by $M_{r,q}(n)$ whenever such a code exists for these parameters (see Theorem 2.1). Note that such a code C does not exist for all $r \geq n\lfloor q/2 \rfloor$ because $I_r(x) = C$ for all $x \in \mathbb{Z}_q^n$.

Lower and upper bounds for $M_{r,q}(n)$ are given in [2] and [8] for various values of r, q, and n. In this paper, we improve upon the various upper bounds of $M_{r,q}(n)$ which are already known in the literature. Also we compute a lot of new lower and upper bounds for the parameters which were not discussed before in the literature. Using our constructions in Section 2 and Section 4, we produce the tables for upper and lower bounds of $M_{r,q}(n)$ in Section 3 and Section 4, respectively.

2. Upper bounds for r-identifying codes

With respect to the Hamming metric, r-identifying codes of length n exist only when $r < n$. For the Lee metric, we have the following more general result. When $q = 2$, as these two metrics are equivalent, this is the same as the above.

Theorem 2.1. *$\mathbb{Z}_q^n$ is an r-identifying code for all $r \leq n\lfloor q/2 \rfloor - 1$.*

Proof. Let $C = \mathbb{Z}_q^n$ and $x \in \mathbb{Z}_q^n$. Then $I_r(x)$ is nonempty because $x \in I_r(x)$. Let $y \in \mathbb{Z}_q^n$ with $y \neq x$. We have to find $z \in \mathbb{Z}_q^n$ such that $z \in I_r(x) \triangle I_r(y)$ where $\triangle$ stands for the symmetric difference. Let x_k, y_k, and z_k be the kth coordinates of x, y, and z, respectively. Since $x \neq y$, there exists an $i \in \{1, 2, \ldots, n\}$ such that $x_i \neq y_i$. By Euclidean division, there exist two integers s and s' such that $r = s\lfloor q/2 \rfloor + s'$ with either $s' = 0$ or $0 < s' < \lfloor q/2 \rfloor$. We know that $r \leq n\lfloor q/2 \rfloor - 1$. Therefore $s < n$.

Choose z as follows: choose $z_i \in \mathbb{Z}_q$ with $d_L(z_i, x_i) \leq s'$ and $d_L(z_i, y_i) > s'$. Such an element exists because $s' < \lfloor \frac{q}{2} \rfloor$ and choose exactly s coordinates in $\{1, 2, \ldots, n\} \setminus \{i\}$ and set $z_j = y_j + \lfloor \frac{q}{2} \rfloor$ for all j in the above chosen s coordinates and for the remaining coordinates of z, take z_k as x_k. Then $d_L(x, z) \leq s\lfloor \frac{q}{2} \rfloor + d_L(z_i, x_i) \leq s\lfloor \frac{q}{2} \rfloor + s' = r$ and $d_L(y, z) \geq s\lfloor \frac{q}{2} \rfloor + d_L(y_i, z_i) > s\lfloor \frac{q}{2} \rfloor + s' = r$. Hence, the result follows. $\square$

By [3, 6], it is known that deciding whether a code is r-identifying is co-NP-complete and constructing good identifying codes is difficult. Therefore one cannot find an r-identifying code of larger length using computer. So we use Theorems 2.2, 2.7, 2.17, 2.18, and 2.20 to construct an r-identifying code of length $n + k$ starting with an r-identifying code of length n. This is established in Section 3.2 and Tables 3, 4, and 5 of Section 3.5.

Recall that if A and B are subsets of $\mathbb{Z}_q^n$ and $\mathbb{Z}_q^m$ respectively, then $A \oplus B = \{xy : x \in A \text{ and } y \in B\} \subseteq \mathbb{Z}_q^n \oplus \mathbb{Z}_q^m \simeq \mathbb{Z}_q^{n+m}$.

Our next theorem generalizes a result of J. L. Kim and S. J. Kim (See Corollary 2.3).

Theorem 2.2. *Let r and k be any two positive integers with $r \leq k\lfloor q/2 \rfloor - 1$, and let C be an r-identifying code of length n. Then $C \oplus \mathbb{Z}_q^k$ is an r-identifying code of length $n+k$.*

Proof. Let $xa \in \mathbb{Z}_q^n \oplus \mathbb{Z}_q^k \simeq \mathbb{Z}_q^{n+k}$. Since $x \in \mathbb{Z}_q^n$ and C is an r-identifying code in $\mathbb{Z}_q^n$, there exists an element $c \in C$ such that $d_L(x, c) \leq r$. Then $ca \in C \oplus \mathbb{Z}_q^k$ with $d_L(xa, ca) = d_L(x, c) \leq r$. This implies that $ca \in I_r(xa)$. Therefore $I_r(xa) \neq \emptyset$. Next we have to prove that $I_r(xa) \neq I_r(yb)$ for all $xa \neq yb$. Suppose $x \neq y$. As C is an r-identifying code in $\mathbb{Z}_q^n$ and $x, y \in \mathbb{Z}_q^n$ with $x \neq y$, there exists an element $c \in C$ such that $d_L(x, c) \leq r$ and $d_L(y, c) > r$ (or vice versa). This implies that $d_L(xa, ca) = d_L(x, c) \leq r$ and $d_L(yb, ca) = d_L(y, c) + d_L(b, a) \geq d_L(y, c) > r$ (or vice versa). Then $ca \in I_r(xa)$ but $ca \notin I_r(yb)$ (or vice versa). Therefore $I_r(xa) \neq I_r(yb)$ when $x \neq y$.

If $x = y$, then $a \neq b$ because $xa \neq yb$. Since C is an r-identifying code in $\mathbb{Z}_q^n$ and $x \in \mathbb{Z}_q^n$, there exists an element $c \in C$ such that $d_L(x, c) = m \leq r$. Since $r - m \leq r \leq k\lfloor q/2 \rfloor - 1$, by Theorem 2.1, $\mathbb{Z}_q^k$ is an $(r-m)$-identifying code. Since $a, b \in \mathbb{Z}_q^k$ with $a \neq b$, there exists an element $p \in \mathbb{Z}_q^k$ with $d_L(p, a) \leq r - m$ and $d_L(p, b) > r - m$ (or vice versa). This implies that $d_L(xa, cp) = d_L(x, c) + d_L(a, p) \leq m + r - m = r$ and $d_L(xb, cp) = d_L(x, c) + d_L(b, p) > m + r - m = r$ (or vice versa). Therefore $cp \in I_r(xa)$ but $cp \notin I_r(xb)$ (or vice versa). Hence, the result follows. $\square$

Corollary 2.3 (J. L. Kim and S. J. Kim [8])**.** *Let $q \geq 4$. If C is a 1-identifying code in $\mathbb{Z}_q^n$, then so is $C \oplus \mathbb{Z}_q$ in $\mathbb{Z}_q^{n+1}$.*

Proof. Take $k = 1, r = 1$, and $q \geq 4$. Therefore $k\lfloor q/2 \rfloor - 1 \geq 1 \cdot 2 - 1 = 1 = r$. The result follows from Theorem 2.2. $\square$

The following corollary is a direct consequence of Theorem 2.2.

Corollary 2.4. *For $r \leq k\lfloor q/2 \rfloor - 1$,*

$$M_{r,q}(n+k) \leq q^k M_{r,q}(n).$$

The following examples show that r cannot be any larger in Theorem 2.2.

Example 2.5. *For $q = 4, n = 4, k = 1$, and $r = 2$,*

$$C = \{0000, 0002, 2001, 0102, 1111, 0220, 2210, 2003, 1130, 1022, 1013, 1302, 3121, 1222, 0331, 3311, 3203, 2330, 2123, 3232, 3323, 0200\}$$

is a 2-identifying code in $\mathbb{Z}_4^4$ but $C \oplus \mathbb{Z}_4$ is not a 2-identifying code in $\mathbb{Z}_4^5$ because $I_2(22100) = I_2(22103) = \{22100, 22101, 22102, 22103\}$.

Example 2.6. *For $q = 5, n = 3, k = 1,$ and $r = 2$,*

$$C = \{000,001,130,022,311,221,203,\\ 420,402,114,223,142,341,314,433,304\}$$

is a 2-identifying code in $\mathbb{Z}_5^3$ but $C \oplus \mathbb{Z}_5$ is not a 2-identifying code in $\mathbb{Z}_5^4$ because $I_2(1300) = I_2(1304) = \{1300, 1301, 1302, 1303, 1304\}$.

The following theorem is true for all cases of r. When $r < k\lfloor q/2 \rfloor$, this is same as Theorem 2.2 because the condition given in Theorem 2.7 is satisfied by all r-identifying codes in $\mathbb{Z}_q^n$. So here we deal with the missing cases for r, namely $r \geq k\lfloor q/2 \rfloor$ in Theorem 2.2.

Theorem 2.7. *Let $r \geq k\lfloor q/2 \rfloor$ and let $k \geq 1$. Let $C \subseteq \mathbb{Z}_q^n$ be an r-identifying code. Then $C \oplus \mathbb{Z}_q^k$ is an r-identifying code if and only if for every $x \in \mathbb{Z}_q^n$, there exists $c \in C$ with $r - k\lfloor q/2 \rfloor + 1 \leq d_L(x, c) \leq r$.*

Proof. Assume that $C \oplus \mathbb{Z}_q^k$ is an r-identifying code and suppose to the contrary that there exists an element $x \in \mathbb{Z}_q^n$ such that for all $c \in C, d_L(x, c) < r - k\lfloor q/2 \rfloor + 1$ or $r < d_L(x, c)$. This implies that $I_r(x) = I_{r-k\lfloor q/2 \rfloor}(x)$ (If $c \in I_r(x), d_L(x, c) \leq r$. Then by our supposition, $d_L(x, c) \leq r - k\lfloor q/2 \rfloor$. Therefore $c \in I_{r-k\lfloor q/2 \rfloor}(x)$. The other inclusion is trivial). Now we find $I_r(xa)$ for any $a \in \mathbb{Z}_q^k$. For all $y \in \mathbb{Z}_q^k$ and $c \in I_r(x), d_L(xa, cy) = d_L(x, c) + d_L(a, y) \leq r - k\lfloor q/2 \rfloor + k\lfloor q/2 \rfloor = r$ because $I_r(x) = I_{r-k\lfloor q/2 \rfloor}(x)$ and $\forall a \in \mathbb{Z}_q^k, d_L(a, y) \leq k\lfloor q/2 \rfloor$. Therefore

$$I_r(xa) = \{cy : c \in I_{r-k\lfloor \frac{q}{2} \rfloor}(x), y \in \mathbb{Z}_q^k\}.$$

For all $b, d \in \mathbb{Z}_q^k$ with $b \neq d$ we have,

$$I_r(xb) = \{cy : c \in I_{r-k\lfloor \frac{q}{2} \rfloor}(x), y \in \mathbb{Z}_q^k\} = I_r(xd),$$

a contradiction to our assumption that $C \oplus \mathbb{Z}_q^k$ is an r-identifying code.

Now we assume that $\forall x \in \mathbb{Z}_q^n, \exists c \in C$ with $r - k\lfloor q/2 \rfloor + 1 \leq d_L(x, c) \leq r$. We have to prove that $C \oplus \mathbb{Z}_q^k$ is an r-identifying code. Let $xa \in \mathbb{Z}_q^{n+k}$. Since $x \in \mathbb{Z}_q^n$ and C is an r-identifying code, there exists $c \in C$ with $d_L(x, c) \leq r$. Then $d_L(xa, ca) = d_L(x, c) \leq r$. Therefore $ca \in I_r(xa)$. This implies that $I_r(xa) \neq \emptyset$, and therefore $C \oplus \mathbb{Z}_q^k$ is an r-covering in $\mathbb{Z}_q^{n+k}$.

Let $xa, x'b \in \mathbb{Z}_q^{n+k}$ with $xa \neq x'b$. We have to prove that $I_r(xa) \neq I_r(x'b)$. If $x \neq x'$, since C is an r-identifying code in $\mathbb{Z}_q^n$ and $x, x' \in \mathbb{Z}_q^n$, there exists an element $c \in C$ with $d_L(x, c) \leq r$ and $d_L(x', c) > r$ (or vice versa). Then $d_L(xa, ca) = d_L(x, c) \leq r$ and $d_L(x'b, ca) = d_L(x', c) + d_L(b, a) \geq d_L(x', c) > r$. Therefore $ca \in I_r(xa)$ but $ca \notin I_r(x'b)$ (or vice versa).

Next, consider the case when $x = x'$. As $xa \neq x'b$, $a \neq b$. By our assumption, there exists an element $c \in C$ with $r - k\lfloor q/2 \rfloor + 1 \leq d_L(x, c) = d \leq r$. This implies that $r - d \leq k\lfloor q/2 \rfloor - 1$. By Theorem 2.1, $\mathbb{Z}_q^k$ is an $(r - d)$-identifying code. This implies that there exists an element $y \in \mathbb{Z}_q^k$ such that $d_L(y, a) \leq r - d$ and $d_L(y, b) > r - d$ (or vice versa). Then

$d_L(xa, cy) = d_L(x, c) + d_L(a, y) \leq d + r - d = r$ and $d_L(x'b, cy) = d_L(x', c) + d_L(b, y) > d + r - d = r$. Therefore, $cy \in I_r(xa)$ but $cy \notin I_r(x'b)$ (or vice versa). This completes the proof. □

The next three lemmas are related to the cardinality of the intersection of Lee balls. These are used later to find r-identifying codes in Lee spaces.

Lemma 2.8. *Let $q = 2s$ be any positive even integer and r any positive integer. Let $x_0 = 000\cdots 0$ and $y_0 = 100\cdots 0$ be elements of $\mathbb{Z}_q^n$. Then*

$$|B_r(x_0) \cap B_r(y_0)| = 2\sum_{k=1}^{\min\{r,s\}} \sum_{i=0}^{\lfloor \frac{r-k}{s} \rfloor} (-1)^i \binom{n-1}{i} \sum_{j=0}^{r-k-si} 2^j \binom{n-1}{j} \binom{r-k-si}{j}.$$

Proof. To find the cardinality of $B_r(x_0) \cap B_r(y_0)$, we divide the elements of $B_r(x_0) \cap B_r(y_0)$ into $2\min\{r, s\}$ disjoint classes with respect to the first coordinate and compute the number of elements in each of these classes. The sum of the cardinalities of these classes gives the cardinality of $B_r(x_0) \cap B_r(y_0)$. Since $d_L(x_0, y_0) = 1$, both x_0 and y_0 belong to $B_r(x_0) \cap B_r(y_0)$. Therefore $B_r(x_0) \cap B_r(y_0)$ is nonempty.

Suppose z is an element of $B_r(x_0) \cap B_r(y_0)$ and the first coordinate of z is $-(k-1)$ or k. Here k varies from 1 to $\min\{r, s\}$ because $d_L(z, x_0) \leq r$ and distance between any two elements in $\mathbb{Z}_q = \mathbb{Z}_{2s}$ is less than or equal to s. Then the first coordinate of z has distance k either with the first coordinate of x_0 or with the first coordinate of y_0 because $d_L(0, k) = k$, $d_L(1, k) \leq k$, $d_L(0, -(k-1)) \leq k$, and $d_L(1, -(k-1)) = k$. Since the remaining coordinates of x_0 and y_0 are the same and z is an element of $B_r(x_0) \cap B_r(y_0)$, the remaining coordinates of z have at most $r-k$ distance with the remaining $n-1$ coordinates of x_0. Therefore there are $V_L(n-1, r-k, q)$ (See Section 1 for the definition of $V_L(n-1, r-k, q)$) elements in $B_r(x_0) \cap B_r(y_0)$ with first coordinate as $-(k-1)$ and there are $V_L(n-1, r-k, q)$ elements with first coordinate as k. Therefore we have

$$\begin{aligned} |B_r(x_0) \cap B_r(y_0)| &= 2\sum_{k=1}^{\min\{r,s\}} V_L(n-1, r-k, q) \\ &= 2\sum_{k=1}^{\min\{r,s\}} \sum_{i=0}^{\lfloor \frac{r-k}{s} \rfloor} (-1)^i \binom{n-1}{i} \sum_{j=0}^{r-k-si} 2^j \binom{n-1}{j} \binom{r-k-si}{j}. \end{aligned}$$

Hence, the result follows. □

Lemma 2.9. *For both even and odd integer q and for any distinct elements x, y of $\mathbb{Z}_q^n$, $|B_r(x) \cap B_r(y)| \leq |B_r(x_0) \cap B_r(y_0)|$ (where x_0 and y_0 are as in Lemma 2.8).*

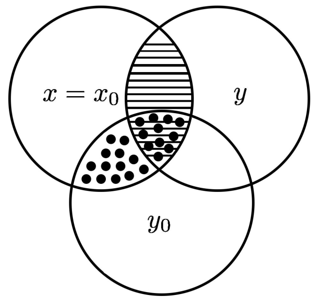

FIGURE 1.

Proof. Let $d_L(x, y) = i \geq 1$. Then without loss of generality, we can take $x = 000\cdots 0$. Clearly $\underbrace{11\cdots 1}_{i\,\text{times}}00\cdots 0$ has a larger intersection with x than $\underbrace{22\cdots 2}_{k\text{ times}}\ \underbrace{11\cdots 1}_{i-2k\text{ times}}\ 00\cdots 0$. So it is enough to take $y = \underbrace{11\cdots 1}_{i\,\text{times}}00\cdots 0$. From Figure 1 it is clear that for proving $|B_r(x)\cap B_r(y)| \leq |B_r(x_0)\cap B_r(y_0)|$, it is enough to prove that $|(B_r(x)\cap B_r(y))\setminus B_r(y_0)| \leq |(B_r(x_0)\cap B_r(y_0))\setminus B_r(y)|$. Since $B_r(x) \cap B_r(y) \subseteq B_r(x)$, we have $(B_r(x) \cap B_r(y)) \setminus B_r(y_0) \subseteq B_r(x) \setminus B_r(y_0)$. Therefore $|(B_r(x)\cap B_r(y))\setminus B_r(y_0)| \leq |B_r(x)\setminus B_r(y_0)|$. This implies that for proving $|(B_r(x)\cap B_r(y))\setminus B_r(y_0)| \leq |(B_r(x_0)\cap B_r(y_0))\setminus B_r(y)|$, it is enough to prove that $|B_r(x)\setminus B_r(y_0)| \leq |(B_r(x_0)\cap B_r(y_0))\setminus B_r(y)|$. Therefore we need to prove that there exists a one-to-one map ϕ from $B_r(x) \setminus B_r(y_0)$ to $(B_r(x_0) \cap B_r(y_0)) \setminus B_r(y)$. We define the map ϕ as follows: for $c \in B_r(x) \setminus B_r(y_0)$, set $\phi(c) = c' = c'_1c'_2\cdots c'_n$ where

$$c'_k = \begin{cases} -(c_k - 1) \text{ if } k \in \{2, 3, \ldots, i+1\} \\ c_k \text{ otherwise.} \end{cases} \tag{2.1}$$

We first prove that $c' \in (B_r(x_0)\cap B_r(y_0))\setminus B_r(y)$. Since $c \in B_r(x),\ d_L(c, x) = m \leq r$. Therefore

$$\begin{aligned} d_L(c', x) &= \sum_{k\notin\{2,\ldots,i+1\}} d_L(c'_k, x_k) + \sum_{k\in\{2,\ldots,i+1\}} d_L(c'_k, x_k) \\ &= \sum_{k\notin\{2,\ldots,i+1\}} d_L(c_k, x_k) + \sum_{k\in\{2,\ldots,i+1\}} (d_L(c_k, x_k) - 1) \\ &= \sum_{k=1}^{n} d_L(c_k, x_k) - i \\ &= d_L(c, x) - i \\ &= m - i \leq r. \end{aligned}$$

Now as $x = x_0,\ d_L(c', x_0) = d_L(c', x) = m - i \leq r$. Therefore $c' \in B_r(x_0)$. Also by the triangle inequality, $d_L(c', y_0) \leq d_L(c', x_0) + d_L(x_0, y_0) = (m -$

$i) + 1 \leq m \leq r$. Then $c' \in B_r(y_0)$. This implies that $c' \in B_r(x_0) \cap B_r(y_0)$. Now if $d_L(c_k, y_k) = j$, then $d_L(c'_k, y_k) = j + 1$ for all $k \in \{2, 3, \ldots, i+1\}$. Therefore

$$\begin{aligned} d_L(c', y) &= \sum_{k \notin \{2,\ldots,i+1\}} d_L(c'_k, y_k) + \sum_{k \in \{2,\ldots,i+1\}} d_L(c'_k, y_k) \\ &= \sum_{k=1}^{n} d_L(c_k, y_k) + i \\ &= d_L(c, y) + i. \end{aligned}$$

By the choice of c, $c \notin B_r(y_0)$, and hence $r < d_L(c, y_0) \leq d_L(c, y) + d_L(y, y_0)$ $= d_L(c, y) + i - 1 = d_L(c', y) - 1$. This implies that $d_L(c', y) > r$. Therefore $c' \in (B_r(x_0) \cap B_r(y_0)) \setminus B_r(y)$.

Finally we prove that the mapping ϕ is one-to-one. Let $c, \tilde{c} \in B_r(x) \setminus B_r(y_0)$ with $c \neq \tilde{c}$. For proving ϕ is one-to-one, we need to prove that $\phi(c) \neq \phi(\tilde{c})$ i.e., $c' \neq \tilde{c}'$. For proving this, we need to prove that for at least one $k \in \{1, 2, \ldots, n\}, c'_k \neq \tilde{c_k}'$. Since $c \neq \tilde{c}$, there exists $k \in \{1, 2, \ldots, n\}$ such that $c_k \neq \tilde{c_k}$. If $k \in \{2, \ldots, i+1\}$, then by equation (2.1), $c'_k = -(c_k - 1)$ and $\tilde{c_k}' = -(\tilde{c_k} - 1)$. Since $c_k \neq \tilde{c_k}$, then $c'_k \neq \tilde{c_k}'$. Otherwise, $k \notin \{2, \ldots, i+1\}$. Then by equation (2.1), $c'_k = c_k$ and $\tilde{c_k}' = \tilde{c_k}$. Therefore $c'_k \neq \tilde{c_k}'$. In both of the two cases, $c' \neq \tilde{c}'$. Hence, the result follows. □

Lemma 2.10. *Let $q = 2s$ be any positive even integer and r, any positive integer. Let*

$$m = 1 + 2 \sum_{k=1}^{\min\{r,s\}} \sum_{i=0}^{\lfloor \frac{r-k}{s} \rfloor} (-1)^i \binom{n-1}{i} \sum_{j=0}^{r-k-si} 2^j \binom{n-1}{j} \binom{r-k-si}{j}.$$

Then in $\mathbb{Z}_q^n$, the intersection of any m distinct Lee balls of radius r is either empty or consists of a single word.

Proof. Let $c_1, c_2, \ldots, c_m$ be any m words in $\mathbb{Z}_q^n$ with $\bigcap_{i=1}^m B_r(c_i) \neq \varnothing$. Then there exists an element $x \in \mathbb{Z}_q^n$ with $x \in \bigcap_{i=1}^m B_r(c_i)$. Suppose there exists $y \in \mathbb{Z}_q^n$ such that $y \in \bigcap_{i=1}^m B_r(c_i)$ with $y \neq x$. Then $x, y \in B_r(c_i)$ for all i and hence $c_i \in B_r(x) \cap B_r(y)$ for all i with $1 \leq i \leq m$. This implies that $|B_r(x) \cap B_r(y)| \geq m$. This is a contradiction since by Lemmas 2.8 and 2.9, we have

$$|B_r(x) \cap B_r(y)| < m.$$

Therefore, our assumption is wrong and we conclude that $\bigcap_{i=1}^m B_r(c_i)$ consists of a single word. □

The following two examples show the sharpness of the above lemma.

Example 2.11. *For $q = 4, r = 3$, and $n = 3$, let us take*

$$X = \{010, 200, 110, 020, 300, 210, 120, 030, 021, 310, 220, 211, 130, 121, 320, 311, 230, 221, 023, 330, 321, 231, 222, 213, 123, 331, 322, 313, 223, 323, 233, 333\}.$$

Here the number of Lee balls, namely, $|X| = 32$ while $m = 33$. We find that $\bigcap_{x \in X} B_3(x) = \{220, 320\}$ consisting of more than one point.

Example 2.12. *For $q = 6, r = 4$, and $n = 2$, let us take*

$$Y = \mathbb{Z}_6^2 \setminus \{32, 42, 23, 33, 43, 53, 34, 44\}.$$

Here the number of Lee balls, namely, $|Y| = 28$ while $m = 29$. We find that $\bigcap_{y \in Y} B_4(y) = \{00, 10\}$ consisting of more than one point.

In our next theorem, we provide a sufficient condition for a subset in $\mathbb{Z}_q^n$ to be an r-identifying code.

Theorem 2.13. *Let $q = 2s$ be any positive even integer and r, any positive integer. Let*

$$m = 1 + 2 \sum_{k=1}^{\min\{r,s\}} \sum_{i=0}^{\lfloor \frac{r-k}{s} \rfloor} (-1)^i \binom{n-1}{i} \sum_{j=0}^{r-k-si} 2^j \binom{n-1}{j} \binom{r-k-si}{j}.$$

Let $C \subseteq \mathbb{Z}_q^n$ be such that $|I_r(x)| \geq m$ for all $x \in \mathbb{Z}_q^n$. Then C is an r-identifying code.

Proof. Let $x \in \mathbb{Z}_q^n$. Since $|I_r(x)| \geq m, I_r(x) \neq \varnothing$ and hence $I_r(x)$ contains at least m codewords, say, $c_1, c_2, \ldots, c_m$. Then $x \in \cap_{i=1}^m B_r(c_i)$. Therefore, by Lemma 2.10, $\cap_{i=1}^m B_r(c_i) = \{x\}$. Suppose that there exists $y \neq x$ in $\mathbb{Z}_q^n$ such that $I_r(y) = I_r(x)$. Then $\{x, y\} \subset \cap_{i=1}^m B_r(c_i)$, a contradiction to Lemma 2.10. Therefore, $I_r(y) \neq I_r(x)$ for any two distinct x, y in $\mathbb{Z}_q^n$. Hence C is an r-identifying code. □

We will see the importance of the above theorem in Corollary 2.14 and Corollary 2.16 given below. Specifically, Corollary 2.16 provides the subsets in $\mathbb{Z}_q^n$ which are all r-identifying codes for all $r \in \{1, \ldots, n\lfloor q/2 \rfloor - 2\}$. Corollary 2.14 provides a sufficient condition on a subset X of $\mathbb{Z}_q^n$ so that its complement is an r-identifying code.

Corollary 2.14. *Let $q = 2s$ be any even positive integer and r, any positive integer. If $X \subseteq \mathbb{Z}_q^n$ with $|X| \leq k = V_L(n, r, q) - m$, where m is as in Theorem 2.13, then $\mathbb{Z}_q^n \setminus X$ is an r-identifying code.*

Proof. By assumption, $X \subseteq \mathbb{Z}_q^n$ with $|X| \leq k$. Let $C = \mathbb{Z}_q^n \setminus X$ and $x \in \mathbb{Z}_q^n$. Recall that $I_r(x) = B_r(x) \cap C$. If $X \subseteq B_r(x)$ then $|B_r(x) \cap C| \geq V_L(n, r, q) - k = m$. Otherwise $|B_r(x) \cap C| > V_L(n, r, q) - k = m$. In any case, $|I_r(x)| \geq m$. By Theorem 2.13, C is an r-identifying code. □

$s \backslash r$	3	4	5	6
2	$\frac{4}{3}n^3 - 4n^2 + \frac{11}{3}n - 2$	$\frac{2}{3}n^4 - \frac{10}{3}n^3 + \frac{35}{6}n^2 - \frac{25}{6}n$	$\frac{4}{15}n^5 - 2n^4 + \frac{17}{3}n^3 - \frac{15}{2}n^2 + \frac{137}{30}n - 2$	$\frac{4}{45}n^6 - \frac{14}{15}n^5 + \frac{35}{9}n^4 - \frac{49}{6}n^3 + \frac{406}{45}n^2 - \frac{49}{10}n$
3	$\frac{4}{3}n^3 - 2n^2 + \frac{5}{3}n - 2$	$\frac{2}{3}n^4 - \frac{4}{3}n^3 + \frac{4}{3}n^2 - \frac{5}{3}n$	$\frac{4}{15}n^5 - \frac{2}{3}n^4 + \frac{2}{3}n^3 - \frac{4}{3}n^2 + \frac{31}{15}n - 2$	$\frac{4}{45}n^6 - \frac{4}{15}n^5 + \frac{2}{9}n^4 - \frac{2}{3}n^3 + \frac{197}{90}n^2 - \frac{77}{30}n$
4	$\frac{4}{3}n^3 - 2n^2 + \frac{8}{3}n - 2$	$\frac{2}{3}n^4 - \frac{4}{3}n^3 + \frac{10}{3}n^2 - \frac{11}{3}n$	$\frac{4}{15}n^5 - \frac{2}{3}n^4 + \frac{8}{3}n^3 - \frac{16}{3}n^2 + \frac{61}{15}n - 2$	$\frac{4}{45}n^6 - \frac{4}{15}n^5 + \frac{14}{9}n^4 - \frac{14}{3}n^3 + \frac{286}{45}n^2 - \frac{61}{15}n$

TABLE 1. $V_L(n,r,q) - m$ given in Corollary 2.14

For small values of s and r, the values of $V_L(n,r,q=2s) - m$ are given in Table 1.

Remark 2.15. *In Table 1, the first box shows that if $s = 2$ so that $q = 2s = 4$, and $r = 3$, $\mathbb{Z}_4^n \setminus X$ is a 3-identifying code if $|X| \le (4/3)n^3 - 4n^2 + (11/3)n - 2$. Table 2 shows that for $q = 4, n = 4$, $\mathbb{Z}_4^4 \setminus X$ is a 3-identifying code if $|X| \le 34$.*

n	$s=2$			$s=3$		
	$r=3$	$r=4$	$r=5$	$r=3$	$r=4$	$r=5$
4	34	34	20	58	100	130
5	83	125	125	123	275	475
6	164	329	461	224	614	1316
7	285	714	1286	369	1197	3057

TABLE 2. The integer k given in Corollary 2.14

Corollary 2.16. *Let $q = 2s$ be any even positive integer. Then $\mathbb{Z}_q^n \setminus X$ is an r-identifying code for all $r \in \{1, \ldots, n(q/2) - 2\}$ where X is a subset of $\mathbb{Z}_q^n$ with $|X| \le \min_{r=1,\ldots,n(q/2)-2}\{V_L(n,r,q) - m\}$ and m is as in Theorem 2.13.*

Proof. Direct consequence of Corollary 2.14. $\square$

If an r-identifying code C satisfies the condition in Theorem 2.7, then by using that code, we can find r-identifying codes of greater lengths. But then even if C fails to satisfy the condition in Theorem 2.7, we can still find r-identifying codes of greater lengths. This is motivated by Theorem 3 of [3] for the Hamming metric.

In [3], the authors proved their theorem by using the fact that $\mathbb{F}_2^n \setminus \{00\cdots 0\}$ is an r-separating code for all $r \in \{0, 1, \ldots, n-1\}$. Now in our case, we obtain larger r-identifying codes for all $r \in \{1, \ldots, n(q/2) - 2\}$ by using Corollary 2.16.

Theorem 2.17. *Let q be an even positive integer. Let $r_1 \ge k \cdot (q/2) \ge r_2 \ge 0$ with $k \cdot (q/2) \ge 3$ and let C be an r_1-identifying code of length n*

and $X_{k,r_2} = \{x \in \mathbb{Z}_q^n \mid d_L(x,c) \le r_1 - k \cdot (q/2) + r_2$ *or* $d_L(x,c) > r_1 + r_2$ *for all* $c \in C\}$*. Choose* $Y_{k,r_2} \subseteq \mathbb{Z}_q^n$ *such that for every* $x \in X_{k,r_2}$*, there exists* $y \in Y_{k,r_2}$ *with* $r_1 + r_2 - k \cdot (q/2) + 2 \le d_L(x,y) \le r_1 + r_2 - 1$*. Then* $C' = (C \oplus \mathbb{Z}_q^k) \cup (Y_{k,r_2} \oplus (\mathbb{Z}_q^k \setminus X))$ *is an* $(r_1 + r_2)$*-identifying code of length* $n + k$ *where* $X \subseteq \mathbb{Z}_q^k$ *with* $|X| = \min_{r=1,\ldots,k(q/2)-2}\{V_L(k,r,q) - m\}$ *and* m *is as in Theorem 2.13.*

Proof. The proof that C' is an $(r_1 + r_2)$-covering code is similar to that of Theorem 3 of [3]. Now we have to prove that C' is an $(r_1 + r_2)$-separating code. Take $x, y \in \mathbb{Z}_q^{n+k} (x \neq y)$. Here $x = x_1x_2, y = y_1y_2$ with $x_1, y_1 \in \mathbb{Z}_q^n, x_2, y_2 \in \mathbb{Z}_q^k$. We have four cases to consider:

CASE 1: $x_1 \neq y_1$ and $x_2 \neq y_2$.

Because C is an r_1-identifying code in $\mathbb{Z}_q^n$ and $x_1, y_1 \in \mathbb{Z}_q^n$ with $x_1 \neq y_1$, there exists $c \in C$ with $d_L(x_1, c) \le r_1$ and $d_L(y_1, c) > r_1$. If $r_2 \le k \cdot (q/2) - 1$, look at the proof of Theorem 2.1 where it is shown that $\mathbb{Z}_q^n$ is an r-separating code. In that proof x and y are taken as arbitary elements. By applying that proof, we can produce an element in $\mathbb{Z}_q^k$ which has distance less than or equal to r_2 from x_2 and distance strictly greater than r_2 from y_2 and vice versa. Therefore we can have $v \in \mathbb{Z}_q^k$ with $d_L(x_2, v) \le r_2$ and $d_L(y_2, v) > r_2$.

If $r_2 = k \cdot (q/2)$ then set

$$v = y_2 + \underbrace{\frac{q}{2}\frac{q}{2}\cdots\frac{q}{2}}_{k \text{ times}}$$

so that $d_L(v, y_2) = k \cdot (q/2) = r_2$ and $d_L(v, x_2) \le r_2$. In both of the above two subcases, $d_L(x, cv) = d_L(x_1x_2, cv) = d_L(x_1, c) + d_L(x_2, v) \le r_1 + r_2$, and $d_L(y, cv) = d_L(y_1y_2, cv) = d_L(y_1, c) + d_L(y_2, v) > r_1 + r_2$. Therefore $cv \in I_{r_1+r_2}(x)$ but $cv \notin I_{r_1+r_2}(y)$.

CASE 2: $x_1 \neq y_1, x_2 = y_2$.

Again, C is an r_1-identifying code in $\mathbb{Z}_q^n$ and $x_1, y_1 \in \mathbb{Z}_q^n$ with $x_1 \neq y_1$. There exists $c \in C$ with $d_L(x_1, c) \le r_1$ and $d_L(y_1, c) > r_1$. Now we have to find $v \in \mathbb{Z}_q^k$ with $d_L(x_2, v) = r_2$. By Euclidean division on integers, there exist m and r such that $r_2 = m(q/2) + r$ with $0 \le r < (q/2)$. Since $r_2, q/2$, and r are nonnegative, m is nonnegative. Also $m \le k$ because $r_2 \le k \cdot (q/2)$. If $m = k$ then $r = 0$ and $r_2 = k \cdot (q/2)$. Then set

$$v = x_2 + \underbrace{\frac{q}{2}\frac{q}{2}\cdots\frac{q}{2}}_{k \text{ times}}.$$

Therefore $d_L(v, x_2) = k \cdot (q/2) = r_2$. If $m < k$, set

$$v = x_2 + \underbrace{\frac{q}{2}\cdots\frac{q}{2}}_{m}\underbrace{r}_{1}\underbrace{00\cdots0}_{k-m-1}.$$

Then $d_L(v,x_2) = m \cdot (q/2) + r = r_2$. In both of the above two subcases, $d_L(v,x_2) = r_2$. Then $d_L(x,cv) = d_L(x_1x_2,cv) = d_L(x_1,c) + d_L(x_2,v) \le r_1 + r_2$, and $d_L(y,cv) = d_L(y_1y_2,cv) = d_L(y_1,c) + d_L(y_2,v) > r_1 + r_2$. Therefore $cv \in I_{r_1+r_2}(x)$ but $cv \notin I_{r_1+r_2}(y)$.

CASE 3: $x_2 \neq y_2$ and $x_1 = y_1 \notin X_{k,r_2}$.

Apply a similar argument as in the proof of Theorem 3 of [3].

CASE 4: $x_2 \neq y_2$ and $x_1 = y_1 \in X_{k,r_2}$.

By the construction of Y_{k,r_2}, there is a vector $z \in Y_{k,r_2}$ such that $r_1+r_2-k\cdot(q/2)+2 \le d_L(z,x_1) \le r_1+r_2-1$. Let $r = r_1+r_2-d_L(z,x_1)$. Then $d_L(z,x_1) = r_1+r_2-r$. Therefore $r_1+r_2-k\cdot(q/2)+2 \le r_1+r_2-r \le r_1+r_2-1$. This implies that $1 \le r \le k\cdot(q/2)-2$. By Corollary 2.16, $\mathbb{Z}_q^k \setminus X$ is an r-identifying code. Therefore there is a vector $v \in \mathbb{Z}_q^k \setminus X$ which is within distance r from x_2 but not from y_2, or vice versa. Then $d_L(zv,x_1x_2) = d_L(z,x_1) + d_L(v,x_2) \le d_L(z,x_1) + r = r_1 + r_2$, and $d_L(zv,x_1y_2) = d_L(z,x_1)+d_L(v,y_2) > d_L(z,x_1)+r = r_1+r_2$ or vice versa, with $zv \in Y_{k,r_2} \oplus (\mathbb{Z}_q^k \setminus X) \subseteq C'$. In both the cases, $I_{r_1+r_2}(x) \neq I_{r_1+r_2}(y)$. Hence, the result follows.

□

In particular, if $r_2 = 0$, we have the following theorem.

Theorem 2.18. *Let q be an even positive integer. Let $r_1 \ge k\cdot(q/2) \ge 3$ and let C be an r_1-identifying code of length n and $X_k = \{x \in \mathbb{Z}_q^n \mid d_L(x,c) \le r_1 - k\cdot(q/2)$ or $d_L(x,c) > r_1$ for all $c \in C\}$. Choose $Y_k \subseteq \mathbb{Z}_q^n$ such that for every $x \in X_k$, there exists $y \in Y_k$ with $r_1 - k\cdot(q/2)+2 \le d_L(x,y) \le r_1 - 1$. Then $C' = (C \oplus \mathbb{Z}_q^k) \cup (Y_k \oplus (\mathbb{Z}_q^k \setminus X))$ is an r_1-identifying code of length $n+k$ where $X \subset \mathbb{Z}_q^k$ with $|X| = \min_{r=1,\ldots,k\cdot(q/2)-2}\{V_L(k,r,q) - m\}$ and m as in Theorem 2.13.*

The following corollary is a direct consequence of the last two theorems.

Corollary 2.19. *Let q be an even positive integer. Let $r_1 \ge k\cdot(q/2) \ge r_2 \ge 0$ and $k\cdot(q/2) \ge 3$. We then have*

(1) $M_{r_1,q}(n+k) \le q^k M_{r_1,q}(n) + (q^k - \min_{r=1,\ldots,k(q/2)-2}\{V_L(k,r,q) - m\})|Y_k|$

(2) $M_{r_1+r_2,q}(n+k) \le q^k M_{r_1,q}(n) + (q^k - \min_{r=1,\ldots,k(q/2)-2}\{V_L(k,r,q) - m\})|Y_{k,r_2}|$

where m is as in Theorem 2.13, Y_k comes from Theorem 2.18, Y_{k,r_2} from 2.17.

If q is an even integer greater than or equal to 6, then $k\cdot(q/2) \ge 3$. Therefore we can find codes of greater length using Theorem 2.18 for these parameters. This is established in (1) of Section 3.2.

In the cases when $q = 4$ and $q = 5$, we can use the following theorem for finding codes of greater length. This is established in Section 3.2 and Table 3 and Table 4 of Section 3.5.

Using the fact that $\mathbb{Z}_4 \setminus \{0\}$ and $\mathbb{Z}_5 \setminus \{0\}$ are both 0-separating codes and

1-separating codes, one can prove the following theorem, in a way similar to that of Theorem 2.18.

Theorem 2.20. *Let $q \in \{4,5\}$. Let $r_1 \geq \lfloor q/2 \rfloor = 2$ and let C be an r_1-identifying code of length n and $X_1 = \{x \in \mathbb{Z}_q^n \mid d_L(x,c) \leq r_1 - \lfloor q/2 \rfloor$ or $d_L(x,c) > r_1$ for all $c \in C\}$. Choose $Y_1' \subseteq \mathbb{Z}_q^n$ such that for every $x \in X_1$, there exists $y \in Y_1'$ with $r_1 - \lfloor q/2 \rfloor + 1 \leq d_L(x,y) \leq r_1$. Then $C' = (C \oplus \mathbb{Z}_q) \cup (Y_1' \oplus (\mathbb{Z}_q \setminus \{0\}))$ is an r_1-identifying code of length $n+1$.*

Corollary 2.21. *Let $q \in \{4,5\}$. Let $r_1 \geq \lfloor q/2 \rfloor = 2$. We then have*

$$M_{r_1,q}(n+1) \leq qM_{r_1,q}(n) + (q-1)|Y_1'|.$$

3. Tables for upper bounds of $M_{r,q}(n)$

Using our constructions in Section 2, we produce tables for upper bounds of $M_{r,q}(n)$ for $1 \leq r \leq 5, 2 \leq n \leq 7$, and $q \in \{4,5,6\}$ (see Tables 3, 4, and 5 in Section 3.5). The upper bounds obtained by using the results in [2] and [8] are written in bold letters in the tables. We improve some of these bounds using our results. This can be viewed in the tables. The bounds are produced by using our results of previous section (see Section 3.2). The bounds for these new parameters have not been considered earlier. For small lengths, we can compute the codes by using the following Greedy algorithm.

3.1. Greedy Algorithm.

For a subset C of $\mathbb{Z}_q^n$, we define $NC_L(C)$ and $NS_L(C)$ as the number of vectors which are not r-covered and not r-separated by C, respectively, and the evaluation function $f_L(C)$ as $NC_L(C)$ $+NS_L(C)$. The Greedy algorithm is as follows.

(1) Start with $C = \emptyset$.
(2) Compute $f_L(C) - f_L(C \cup \{m\})$ for all $m \in \mathbb{Z}_q^n$.
(3) Choose m which maximizes $f_L(C) - f_L(C \cup \{m\})$.
(4) Replace C by $C \cup \{m\}$.
(5) Continue the process until $f_L(C) = 0$.

The upper bounds obtained using the above Greedy algorithm are marked as ‘a’ in Tables 3, 4, and 5 of Section 3.5.

3.2. Applications of the Theorems in Section 2.

After getting codes of small length up to 4 by using the Greedy algorithm, we apply the theorems in Section 2 for finding codes of greater length using a computer. The upper bounds obtained by Theorem 2.2, Theorem 2.7, and Theorem 2.20 are marked as ‘b’,‘c’, and ‘d’, respectively, in Tables 3, 4, and 5 of Section 3.5.

We then produce X_1, Y_1 of Theorem 2.18 and Y_1' of Theorem 2.20 with the aid of a computer. For all computations in this section, $k = 1$. Here elements of $\mathbb{Z}_q^n$ are represented by the corresponding decimal numbers, for example 0231 in $\mathbb{Z}_5^4$ is represented by $66 = 0 \times 5^3 + 2 \times 5^2 + 3 \times 5^1 + 1 \times 5^0$.

In $\mathbb{Z}_8^3$,

$$\{0,6, 34, 89, 123, 136, 148, 152, 175, 256, 258, 263, 289, 299, 343, 359, 387, 403, 424, 425, 436, 449, 486\}$$

is a 4-identifying code of cardinality 23 with $X_1 = \{224\}$ and $Y_1 = \{221\}$. Here

$$M_{4,8}(4) \leq 8 \cdot 23 + 8 \cdot 1 = 192. \tag{3.1}$$

In $\mathbb{Z}_4^4$, there is a 2-identifying code of cardinality 22 with $X_1 = \{1111, 2210, 1130, 3121, 0331, 3311, 2330, 2123, 3323\}$ and $Y_1' = \{0001, 2120, 3320, 1100\}$.

$$\text{Here } M_{2,4}(5) \leq 4 \cdot 22 + 3 \cdot 4 = 100. \tag{3.2}$$

In $\mathbb{Z}_4^4$, there is a 3-identifying code of cardinality 14 with $X_1 = \{1022, 1333, 3332\}$ and $Y_1' = \{0032\}$. Here

$$M_{3,4}(5) \leq 4 \cdot 14 + 3 \cdot 1 = 59. \tag{3.3}$$

In $\mathbb{Z}_4^5$, there is a 4-identifying code of cardinality 24 with $X_1 = \{20023\}$ and $Y_1' = \{10000\}$. Here

$$M_{4,4}(6) \leq 4 \cdot 24 + 3 \cdot 1 = 99. \tag{3.4}$$

In $\mathbb{Z}_5^3$, there is a 2-identifying code of cardinality 16 with $X_1 = \{130, 022, 420, 142, 433\}$ and $Y_1' = \{020, 032\}$. Here

$$M_{2,5}(4) \leq 5 \cdot 16 + 4 \cdot 2 = 88. \tag{3.5}$$

In $\mathbb{Z}_5^3$, there is a 3-identifying code of cardinality 11 with $X_1 = \{422\}$ and $Y_1' = \{020\}$. Here

$$M_{3,5}(4) \leq 5 \cdot 11 + 4 \cdot 1 = 59. \tag{3.6}$$

3.3. **Removing Codewords.** For several codes, the cardinality can be further reduced by simply removing some of the codewords which are superfluous. These are marked in the tables as '*'. The codewords are identified by actual verification of the fact that if m is such a codeword, then the code $C \setminus \{m\}$ is also an r-identifying code.

3.4. **Applications of Theorem 9 of Karpovsky et al.** [2]**.** After getting codes of small length by using Sections 3.1, 3.2, and 3.3, we apply Theorem 9 of [2] for finding codes of greater length. The upper bounds obtained in this section are marked as '**' in Tables 3, 4, and 5 of Section 3.5. The following are the bounds obtained by using Sections 3.1, 3.2, 3.3, and Theorem 9 of [2].

- $M_{2,4}(7) \leq M_{1,4}(4) \cdot M_{1,4}(3) = 67 \times 21 = 1407$
- $M_{3,4}(6) \leq M_{1,4}(2) \cdot M_{2,4}(4) = 7 \times 22 = 154$
- $M_{3,4}(7) \leq M_{1,4}(3) \cdot M_{2,4}(4) = 21 \times 22 = 462$
- $M_{4,4}(6) \leq M_{2,4}(3) \cdot M_{2,4}(3) = 8 \times 8 = 64$
- $M_{4,4}(7) \leq M_{2,4}(3) \cdot M_{2,4}(4) = 8 \times 22 = 176$

TABLE 3. Upper bounds for $M_{r,4}(n)$

n	$M_{1,4}(n)$	$M_{2,4}(n)$	$M_{3,4}(n)$	$M_{4,4}(n)$	$M_{5,4}(n)$
2	$7^a\mathbf{7^{e,i}}$(optimal)	7^a	15^a	-	-
3	$21^a\mathbf{28^e}$	8^a	7^a	20^a	63^a
4	$67^*68^a\mathbf{112^e}$	22^a	14^a	14^a	22^a
5	$266^*268^b\mathbf{448^e}$	92^*100^d	51^*59^d	24^*56^c	28^*88^c
6	$1064^b\mathbf{1792^e}$	352^b	154^{**}	64^{**}	46^*112^c
7	$4256^b\mathbf{7168^e}$	1407^{**}	462^{**}	176^{**}	112^{**}

- $M_{5,4}(7) \leq M_{2,4}(3) \cdot M_{3,4}(4) = 8 \times 14 = 112$
- $M_{2,5}(6) \leq M_{1,5}(3) \cdot M_{1,5}(3) = 39 \times 39 = 1521$
- $M_{2,5}(7) \leq M_{1,5}(4) \cdot M_{1,5}(3) = 195 \times 39 = 7605$
- $M_{3,5}(5) \leq M_{1,5}(2) \cdot M_{2,5}(3) = 10 \times 16 = 160$
- $M_{3,5}(6) \leq M_{1,5}(3) \cdot M_{2,5}(3) = 39 \times 16 = 624$
- $M_{3,5}(7) \leq M_{1,5}(3) \cdot M_{2,5}(4) = 39 \times 73 = 2847$
- $M_{4,5}(6) \leq M_{2,5}(3) \cdot M_{2,5}(3) = 16 \times 16 = 256$
- $M_{4,5}(7) \leq M_{2,5}(3) \cdot M_{2,5}(4) = 16 \times 73 = 1168$
- $M_{5,5}(6) \leq M_{2,5}(3) \cdot M_{3,5}(3) = 16 \times 11 = 176$
- $M_{5,5}(7) \leq M_{1,5}(2) \cdot M_{4,5}(5) = 10 \times 52 = 520$
- $M_{2,6}(5) \leq M_{1,6}(2) \cdot M_{1,6}(3) = 14 \times 54 = 756$
- $M_{2,6}(6) \leq M_{1,6}(3) \cdot M_{1,6}(3) = 54 \times 54 = 2916$
- $M_{2,6}(7) \leq M_{1,6}(4) \cdot M_{1,6}(3) = 324 \times 54 = 17496$
- $M_{3,6}(5) \leq M_{1,6}(2) \cdot M_{2,6}(3) = 14 \times 27 = 378$
- $M_{3,6}(6) \leq M_{1,6}(3) \cdot M_{2,6}(3) = 54 \times 27 = 1458$
- $M_{3,6}(7) \leq M_{1,6}(3) \cdot M_{2,6}(4) = 54 \times 149 = 8046$
- $M_{4,6}(5) \leq M_{1,6}(2) \cdot M_{3,6}(3) = 14 \times 16 = 224$
- $M_{4,6}(6) \leq M_{2,6}(3) \cdot M_{2,6}(3) = 27 \times 27 = 729$
- $M_{4,6}(7) \leq M_{2,6}(3) \cdot M_{2,6}(4) = 27 \times 149 = 4023$
- $M_{5,6}(6) \leq M_{2,6}(3) \cdot M_{3,6}(3) = 27 \times 16 = 432$
- $M_{5,6}(7) \leq M_{2,6}(3) \cdot M_{3,6}(4) = 27 \times 75 = 2025$

3.5. **Tables.** We give our results for $1 \leq r \leq 5$ and $2 \leq n \leq 7$ in the Lee Spaces $\mathbb{Z}_4^n$, $\mathbb{Z}_5^n$, and $\mathbb{Z}_6^n$. For some parameters, give two upper bounds, the first one is from Section 3.2 and the second from Section 3.3. The upper bounds computed by us (resp. others) are written in normal (resp. bold) fonts. In the tables below, we write optimal when the exact value is known. The superscripts denote the sections whose results have been employed to determine the values. The description of the superscript are given at the end of Table 5.

4. Lower bounds for r-identifying codes

Lower bounds for r-identifying codes with respect to the Lee metric are given in [2, 8]. In [2], it is shown that $M_{1,q}(n) \geq q^n/(n+1)$ for $q > 4$ and the lower bounds for $M_{1,3}(n)$ and $M_{1,4}(n)$ are given in [8]. But for $r \geq 2$,

n	$M_{1,5}(n)$	$M_{2,5}(n)$	$M_{3,5}(n)$	$M_{4,5}(n)$	$M_{5,5}(n)$
2	$\mathbf{10}^{\mathbf{f}}$	6^a	11^a	-	-
3	39^a	16^a	11^a	15^a	33^*35^a
4	195^b	$73^*88^d\mathbf{100}^{\mathbf{f}}$	42^*59^d	18^a	20^a
5	975^b	365^c	160^{**}	52^*90^c	38^*100^c
6	4875^b	1521^{**}	$624^{**}\mathbf{1000}^{\mathbf{f}}$	256^{**}	176^{**}
7	24375^b	7605^{**}	2847^{**}	1168^{**}	520^{**}

TABLE 4. Upper bounds for $M_{r,5}(n)$

n	$M_{1,6}(n)$	$M_{2,6}(n)$
2	$14^a\mathbf{16}^{\mathbf{k}}$	$9^a\mathbf{9}^{\mathbf{g}}$
3	$\mathbf{54}^{\mathbf{g,j}}$(optimal)	27^a
4	$\mathbf{324}^{\mathbf{h}}$	$149^*162^b\mathbf{324}^{\mathbf{g}}$
5	$\mathbf{1701}^{\mathbf{l}}$	756^{**}
6	$\mathbf{8748}^{\mathbf{l}}$	2916^{**}
7	$\mathbf{34992}^{\mathbf{g,j}}$(optimal)	17496^{**}

n	$M_{3,6}(n)$	$M_{4,6}(n)$	$M_{5,6}(n)$
2	9^a	14^a	35^a
3	$16^a\mathbf{27}^{\mathbf{g}}$	13^a	16^a
4	75^*96^c	$48^*78^c\mathbf{81}^{\mathbf{g}}$	29^*96^c
5	378^{**}	224^{**}	$117^*174^c\mathbf{243}^{\mathbf{g}}$
6	$1458^{**}\mathbf{5832}^{\mathbf{g}}$	729^{**}	432^{**}
7	8046^{**}	4023^{**}	2025^{**}

TABLE 5. Upper bounds for $M_{r,6}(n)$

*-Section 3.3	**-Section 3.4	a-Section 3.1
b-Theorem 2.2	c-Theorem 2.7	d-Theorem 2.20
e-(iii) of [8, Theorem 3.7]	f-(1) [2, Corollary 9]	g-(3) [2, Corollary 9]
h-[2, Corollary 5]	i-[8, Theorem 3.6]	j-[2, Theorem 6]
k-[8, Corollary 3.9]	l-[2, Theorem 7]	

the lower bounds for $M_{r,4}(n)$ are not known previously in the literature. In this section, we compute lower bounds for $M_{r,4}(n)$ for all r by using the idea in Theorem 2.1 of [5] for the Hamming metric. For this we need to prove the following two lemmas, Lemma 4.2 and Lemma 4.3. First we define some notation similar to those given in [5].

For $x \in \mathbb{Z}_q^n$, define

$$P_{r,n}(x,i) = \max_{C\subseteq\mathbb{Z}_q^n} |\{y \in \mathbb{Z}_q^n | C \text{ is an r-identifying code satisfying } |I_r(x)| = i \text{ and } I_r(y) \subseteq I_r(x), |I_r(y)| = 2\}|.$$

Since each word of $\mathbb{Z}_q^n$ plays the same role, $P_{r,n}(\mathbf{0},i) = P_{r,n}(x,i)$ for all $x \in \mathbb{Z}_q^n$ where $\mathbf{0}$ is the all-zero vector. Therefore we can set $P_{r,n}(\mathbf{0},i) = P_{r,n}(i)$.

Remark 4.1.

$$P_{r,n}(i) \leq \min\left\{\binom{i}{2}, V_L(n, 2r, 4)\right\}.$$

Lemma 4.2. *In $\mathbb{Z}_4^n$, with respect to the Lee metric,*

$$|B_r(x) \cap B_r(y)| = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \binom{r - \frac{k}{2}}{i} \left(\sum_{l=0}^{r-2i} \binom{r - \frac{k}{2} - i}{l} 2^l \binom{k}{r - 2i - l} \right)$$

for all $x, y \in \mathbb{Z}_4^n$ with $d_L(x, y) = 2r$ and x and y differ in $r + (k/2)$ coordinate places such that in each of $r - (k/2)$ of these places, they differ by 2 while in each of the remaining k places, they differ by 1.

Proof. Without loss of generality we take

$$x = \underbrace{00\cdots0}_{r-\frac{k}{2}}\underbrace{00\cdots0}_{k}\underbrace{00\cdots0}_{n-r-\frac{k}{2}},$$

$$y = \underbrace{22\cdots2}_{r-\frac{k}{2}}\underbrace{11\cdots1}_{k}\underbrace{00\cdots0}_{n-r-\frac{k}{2}}.$$

We have to find the number of elements of $\mathbb{Z}_4^n$ belonging to $B_r(x) \cap B_r(y)$. Suppose z is such an element. Then $d_L(x, z) \leq r$ and $d_L(z, y) \leq r$. If $d_L(x, z) < r$, then by triangle inequality $d_L(x, y) < 2r$, a contradiction. Therefore $d_L(z, x) = r$. If $d_L(z, y) < r$, again by the triangle inequality $d_L(x, y) < 2r$, a contradiction. Therefore $d_L(z, y) = r$ and $d_L(z, x) = r$. As

$$z,\, y \in \mathbb{Z}_4^{r-\frac{k}{2}} \oplus \mathbb{Z}_4^k \oplus \mathbb{Z}_4^{n-r-\frac{k}{2}}, \text{ set } z = z'z''z''' \text{ and } y = y'y''y''',$$

where $z',\ y' \in \mathbb{Z}_4^{r-\frac{k}{2}}$, $z'', y'' \in \mathbb{Z}_4^k$, and $z''', y''' \in \mathbb{Z}_4^{n-r-\frac{k}{2}}$.

If $w_L(z''') = m \geq 1$, then either $d_L(z, x) \neq r$ or $d_L(z, y) \neq r$ (if $d_L(z, x) = r$, then we have $w_L(z') + w_L(z'') = r - m$ because $w_L(z) = w_L(z - x) = d_L(z, x) = r$. Also $w_L(y') + w_L(y'') = 2r$. Therefore $d_L(z, y) > r$), a contradiction to the fact that $d_L(z, x) = r$ and $d_L(z, y) = r$. Therefore $m = 0$. This implies that z''' is the all-zero word.

Suppose z' has i coordinates as 2 where $0 \leq i \leq \lfloor r/2 \rfloor$. The reason for the upper bound of i is $d_L(z, x) = r$. Now $d_L(z, x) \geq 2i$. Consider the remaining coordinates of z' and the coordinates belonging to z''. From these coordinates, we can choose at most $r - 2i$ coordinate positions and fill them with weight one words and leave the remaining coordinates as zero because we already have $w_L(z) \geq 2i$.

Suppose l coordinates from the remaining $r - (k/2) - i$ coordinates of z' with $0 \leq l \leq r - 2i$ are filled with either 1 or 3. In these l coordinates, 1 may occur in any of the p-coordinates where $0 \leq p \leq l$. Therefore we have $\sum_{p=0}^{l} \binom{l}{p} = 2^l$ choices. Suppose $r - 2i - l$ coordinates from the k

coordinates of z'' are filled with 1. The remaining coordinates of z are zero because $w_L(z) = r$. Therefore we have

$$|B_r(x) \cap B_r(y)| = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \binom{r-\frac{k}{2}}{i} \left(\sum_{l=0}^{r-2i} \binom{r-\frac{k}{2}-i}{l} 2^l \binom{k}{r-2i-l} \right).$$

□

Lemma 4.3. *For each nonnegative even integer k and nonnegative integer r,*

$$\sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \binom{r-\frac{k}{2}}{i} \left(\sum_{l=0}^{r-2i} \binom{r-\frac{k}{2}-i}{l} 2^l \binom{k}{r-2i-l} \right) = \binom{2r}{r}.$$

Proof. See the following: `https://math.stackexchange.com/questions/2303893`. □

We thank Markus Scheuer (`https://math.stackexchange.com/users/1320\07/markus-scheuer`) and Marko Riedel (`http://pnp.mathematik.uni-stuttga\rt.de/iadm/Riedel/`) for their help proving Lemma 4.3.

By using Lemma 4.2 and Lemma 4.3, we can prove the following theorem in a similar way to the proof of Theorem 2.1 of [5].

Theorem 4.4. *Let $C \subseteq \mathbb{Z}_4^n$ be an r-identifying code. Let*

$$a = \min_{i=3,\ldots,V_L(n,r,4)} \left\{ 2 + \frac{(i-2)(\binom{2r}{r}-1)}{\binom{2r}{r} + P_{r,n}(i) - 1} \right\}.$$

Then

$$|C| \geq M_{r,4}(n) \geq \frac{a \cdot 4^n}{V_L(n,r,4) + a - 1}.$$

In Table 6, we use the upper bounds of $P_{r,n}(i)$ from Remark 4.1 to find the lower bounds for $M_{r,4}(n)$ by using Theorem 4.4.

From Tables 3 and 6, we have

$$M_{2,4}(3) = 8, \quad M_{1,4}(2) = 7, \quad 18 \leq M_{1,4}(3) \leq 21,$$
$$4 \leq M_{2,4}(2) \leq 7, \quad 17 \leq M_{2,4}(4) \leq 22, \quad 5 \leq M_{3,4}(3) \leq 7.$$

Remark 4.5: By Theorem 4.4, we can find the lower bounds of $M_{r,4}(n)$ for all r. These bounds were not previously known for $r \geq 2$. For small values of r, lower bounds are given in Table 6. When $r = 1$, our lower bounds are the same as the lower bounds obtained in [8]. But if there is any improvement in the upper bound of $P_{r,n}(i)$, it will simultaneously improve, by Theorem 4.4, the lower bound of $M_{r,4}(n)$. Therefore improving the upper bound of $P_{r,n}(i)$ is to be considered as an important open problem in this area.

Acknowledgement

The authors thank Prof. R. Balakrishnan, Adjunct Professor of our department for his valuable suggestions and review of this paper.

n	$M_{1,4}(n)$	$M_{2,4}(n)$	$M_{3,4}(n)$	$M_{4,4}(n)$	$M_{5,4}(n)$
2	6	4	3	-	-
3	18	8	5	4	3
4	56	17	8	5	4
5	183	42	17	8	5
6	623	115	35	16	8
7	2164	334	81	32	15
8	7654	1015	209	65	29
9	27434	3195	571	149	59
10	99392	10327	1636	371	119
11	363287	34096	4862	979	269
12	1337719	114512	14869	2703	656
13	4956905	390142	46539	7727	1690
14	18467305	1345475	148497	22718	4541
15	69125011	4688575	481632	68377	12611

TABLE 6. Lower bounds for $M_{r,4}(n)$ by using Theorem 4.4

REFERENCES

1. J. Astola, *The theory of lee codes*, Lappeenranta University of Technology, 1982.
2. K. Chakrabarty, M. G. Karpovsky, and L. B. Levitin, *On a new class of codes for identifying vertices in graphs*, IEEE Trans. Inform. Theory **44** (1998), 599–611.
3. I. Charon, G. Cohen, O. Hudry, and A. Lobstein, *New identifying codes in the binary hamming space*, Eur. J. Combin. **31** (2010), 491–501.
4. W. J. Dally, *The message-driven processor: A multicomputer processing node with efficient mechanisms*, IEEE Micro **12** (1992), 23–39.
5. G. Exoo, V. Junnila, T. Laihonen, and S. Ranto, *Improved bounds on identifying codes in binary hamming spaces*, Eur. J. Combin. **31** (2010), 813–827.
6. I. Honkala and A. Lobstein, *On the complexity of the identification problem in hamming spaces*, Acta Informatica **38** (2002), 839–845.
7. R. M. Hord, *Parallel supercomputing in mimd architectures*, CRC Press, 1993.
8. J. L. Kim and S. J. Kim, *Identifying codes in q-ary hypercubes*, Bull. Inst. Combin. Appl. **59** (2010), 93–102.
9. M. Laifenfeld and A. Trachtenberg, *Identifying codes and covering problems*, IEEE Trans. Inform. Theory **54** (2008), 3929–3950.
10. R. M. Roth, *Introduction to coding theory*, Cambridge University Press, 2006.

DEPARTMENT OF MATHEMATICS, SCHOOL OF MATHEMATICAL SCIENCES, BHARATHIDASAN UNIVERSITY, TIRUCHIRAPPALLI, TAMIL NADU-620024, INDIA
E-mail address: `mathlakshmi10@gmail.com`

DEPARTMENT OF MATHEMATICS, SCHOOL OF MATHEMATICAL SCIENCES, BHARATHIDASAN UNIVERSITY, TIRUCHIRAPPALLI, TAMIL NADU-620024, INDIA
E-mail address: `cdurai66@rediffmail.com`