Optimal linear identifying codes

Sanna Ranto

Turku Centre for Computer Science
Lemminkäisenkatu 14 A
FIN-20520 Turku, Finland

Turku Centre for Computer Science
TUCS Technical Report No 443
January, 2002
ISBN 952-12-0953-4
ISSN 1239-1891

Abstract

Identifying codes can be used to locate malfunctioning processors. We determine the cardinalities of optimal linear $(1, \leq l)$-identifying and strongly $(1, \leq l)$-identifying codes in Hamming spaces of any dimension for locating any at most l malfunctioning processors.

Keywords: identifying codes, covering codes, linear codes, Hamming space, code construction

TUCS Research Group
Coding Theory Group

1 Introduction

Identifying codes were introduced in the paper of Karpovsky, Chakrabarty and Levitin [5]. In this paper we are concerned with identifying codes in Hamming spaces. Suppose that there are 2^n processors arranged in the nodes of n-dimensional hypercube. Some of the processors send information to a controller if themselves or any of their neighbours is malfunctioning. The message is YES if problem occurs and otherwise it is NO. The controller should be able to know by the received messages which processor is malfunctioning. We want to minimize the number of processors sending information.

The *Hamming distance* between two words $x = (x_1, \dots, x_n) \in F_2^n$ and $y = (y_0, \dots, y_n) \in F_2^n$, where $F_2 = \{0, 1\}$ is $d(x, y) := |\{i \mid x_i \neq y_i\}|$. The set of non-zero coordinates of a word $x \in F_2^n$ is called a *support* of x. For $x \in F_2^n$ we denote

$$\begin{aligned} B_t(x) &= \{y \in F_2^n \mid d(x, y) \leq t\}, \\ S_t(x) &= \{y \in F_2^n \mid d(x, y) = t\}. \end{aligned}$$

The set $B_t(x)$ is called the *Hamming sphere of radius* t. Let $C \subseteq F_2^n$. For any $X \subseteq F_2^n$ we denote

$$I_t(X) = I_t(C; X) = \bigcup_{x \in X} (B_t(x) \cap C).$$

The set $I_t(X)$ is called the *I-set* of X. If $t = 1$ we denote for short $I(X) = I(C; X)$. We also denote $I(\{x_1, x_2, \dots, x_l\}) = I(x_1, x_2, \dots, x_l)$. We say that x covers y (and vice versa) if $d(x, y) \leq 1$. As usual, the cardinality of a set X is denoted by $|X|$. A binary code $C \subseteq F_2^n$ of cardinality 2^k is linear if it is a k-dimensional subspace of F_2^n.

Definition 1. *Let t and l be non-negative integers. We say that $C \subseteq F_2^n$ is a* $(t, \leq l)$-identifying code *if for all $X, Y \subseteq F_2^n$, $X \neq Y$, such that $|X| \leq l$ and $|Y| \leq l$ we have $I_t(X) \neq I_t(Y)$.*

The smallest cardinality of a $(t, \leq l)$-identifying code of length n is denoted by $M_t^{(\leq l)}(n)$. The smallest cardinality of a binary linear $(t, \leq l)$-identifying code of length n is denoted by $M_t^{(\leq l)}[n]$. A code attaining the smallest cardinality is called *optimal*.

The *direct sum* of codes $C_1 \subseteq F_2^{n_1}$ and $C_2 \subseteq F_2^{n_2}$ is

$$C_1 \oplus C_2 = \{(c_1, c_2) \mid c_1 \in C_1, c_2 \in C_2\} \subseteq F_2^{n_1+n_2}.$$

The next lemma will be often used.

Lemma 1. *If $C \subseteq F_2^n$ is a linear code and $c \in C$ then for all $x \in F_2^n$*

$$I(x+c) = I(x) + c.$$

Proof. Clearly, $y \in I(x+c)$ if and only if $y \in C$ and $d(x+c, y) \leq 1$. This is equivalent to the fact that $y+c \in C$ (because C is linear) and $d(x, y+c) \leq 1$; that is, $y+c \in I(x)$. This is equivalent to $y \in I(x) + c$. $\square$

The previous lemma implies that each codeword is covered by the same number of codewords in a linear code. Namely, suppose C is a linear code. Then for all $c \in C$ we have $I(\mathbf{0}+c) = I(\mathbf{0})+c$. Thus each codeword is covered by the same number of codewords as $\mathbf{0}$, which is always a codeword. By the lemma we also know that if $x, y \notin C$, $e_i \in S_1(\mathbf{0})$ and both $x+e_i$ and $y+e_i \in C$ then $|I(x)| = |I(y)|$. Indeed, $I(x)+x+e_i = I(x+x+e_i) = I(e_i) = I(y+y+e_i) = I(y)+y+e_i$. In fact, we get more; namely, $|I(x)| = |I(e_i)| = |I(y)|$.

Let us recall the definitions from [2]. The *covering radius* of a code $C \subseteq F_2^n$ is the smallest integer r such that $\cup_{c \in C} B_r(c) = F_2^n$. A code C is a *μ-fold 1-covering* if the codewords of C cover each word of F_2^n at least μ times. We say that such a code is *perfect* if each word in F_2^n is covered exactly μ times. The smallest dimension of a linear μ-fold 1-covering is denoted by $k[n, 1, \mu]$. A code attaining the smallest dimension is called *optimal*.

Denote by $k[n, 1, \mu, \nu]$ the smallest dimension of a binary linear code of length n such that each non-codeword in F_2^n is covered by at least μ codewords and each codeword is covered by at least ν codewords. These covering codes are a generalization of μ-fold 1-coverings, and $k[n, 1, \mu] = k[n, 1, \mu, \mu]$.

Theorem 1. *Suppose μ and ν are positive integers.*

$$2^{k[n,1,\mu,\nu]} \geq 2^l \geq \left\lceil \frac{\mu \cdot 2^n}{n+1+\mu-\nu} \right\rceil,$$

where l is the smallest integer such that the latter inequality holds.

Proof. Denote $K = 2^{k[n,1,\mu,\nu]}$. The claim follows from the direct calculation

$$\nu \cdot K + \mu(2^n - K) \leq K(n+1).$$

$\square$

Theorem 2. *Let μ and ν be positive integers. When $n = (2^r-1)\mu+\nu-1+s$, where $r \geq 0$ and $0 \leq s \leq 2^r\mu - 1$, then*

$$k[n, 1, \mu, \nu] = n - r.$$

Proof. The lower bound comes from Theorem 1.

If $r = 0$ then by Theorem 1, $k[n, 1, \mu, \nu] \geq n$. In F_2^n codewords are covered at least ν times and thus it is the optimal code.

Suppose then that $r \geq 1$. Let H be any $r \times n$ matrix which contains the all-zero column at least $\nu - 1$ times and every non-zero column at least μ times. The matrix H has clearly rank r, and the code which has H as its parity check matrix is as required:

For every $x \in F_2^n$, we call the vector $Hx^T \in F_2^r$ the *syndrome* of x. Here x^T denotes the transpose of x. It is known that a syndrome which informs that a word x is at most at distance one from a code is the sum of at most one column of H. The syndrome of a codeword is the all-zero column. Since we get the zero column ν times as the sum of at most one column we know that codewords are covered ν times. All the non-zero r-tuples occur μ times each as the columns of H, and thus each non-codeword is covered μ times. $\square$

2 On linear $(1, \leq 1)$-identifying codes

Theorem 3.

$$M_1^{(\leq 1)}[n] \geq 2^k \geq \left\lceil \frac{3 \cdot 2^n}{n+3} \right\rceil,$$

where k is the smallest integer such that the latter inequality holds.

Proof. Suppose C is a linear $(1, \leq 1)$-identifying code of length n and cardinality K. We shall show that each word in F_2^n is covered either by one codeword or by at least three codewords. Because C is $(1, \leq 1)$-identifying we have $|I(x)| \geq 1$ for all $x \in F_2^n$, and $|I(x)| = 1$ for at most K words.

Suppose that for some $y \in F_2^n$ we have $|I(y)| \geq 2$. Then $\{y + e_1, y + e_2\} \subseteq I(y)$ where $e_1, e_2 \in B_1(\mathbf{0})$. Now $\{y + e_1, y + e_2\} \subseteq I(y + e_1 + e_2)$. In order to distinguish between $I(y)$ and $I(y + e_1 + e_2)$ we must have *i)* some $e_3 \in B_1(0)$ such that $e_1 \neq e_3 \neq e_2$ and $y + e_3 \in I(y)$ which implies that $y + e_1 + e_2 + e_3 \in I(y + e_1 + e_2)$, or *ii)* $|I(y + e_1 + e_2)| \geq 3$ and this similarly implies $|I(y)| \geq 3$. Since y was chosen arbitrarily we know that for all $y \in F_2^n$ such that $|I(y)| > 1$ we have $|I(y)| \geq 3$. Now we can calculate

$$K + 3(2^n - K) \leq K(n + 1)$$

from which the claim follows. $\square$

For linear $(1, \leq 1)$-identifying codes we get the next nice result which is not known for $(1, \leq 1)$-identifying codes in general.

Theorem 4.

$$M_1^{(\leq 1)}[n] \leq 2M_1^{(\leq 1)}[n-1].$$

Proof. Let D be a linear $(1, \leq 1)$-identifying code of length $n-1$ and cardinality $M_1^{(\leq 1)}[n-1]$. If each codeword is covered by more than one codeword then by [1, Theorem 1] the direct sum $\{0,1\} \oplus D$ is a $(1, \leq 1)$-identifying code of length n. Clearly, the code $\{0,1\} \oplus D$ is linear.

Suppose then that in D each codeword is covered only by itself. Then as noticed in the proof of Theorem 3 each non-codeword is covered by at least three codewords. Denote by $C(0) = \{(0,0),(1,1)\} \subseteq F_2^2$ and $C(1) = \{(0,1),(1,0)\} \subseteq F_2^2$. We shall show that the code

$$C = \bigcup_{(x_1,x_2,\dots,x_{n-1}) \in D} (x_1, x_2, \dots, x_{n-2}) \oplus C(x_{n-1})$$

is a linear $(1, \leq 1)$-identifying code of length n. The code C is linear because D is and $C(0) \cup C(1) = F_2^2$. If G_D is a generator matrix for D then the matrix

$$G_C = \begin{pmatrix} & & & & 0 \\ & G_D & & & \vdots \\ & & & & 0 \\ 0 & \dots & 0 & 1 & 1 \end{pmatrix}$$

is a generator matrix for C. The requirement that in D each codeword is covered only by itself is equivalent with the condition that the minimum distance of D is at least two. From the generator matrix G_C we easily see that this holds for C, too.

Suppose $x = (x', a) \in F_2^n$, where $x' \in F_2^{n-2}$ and $a \in F_2^2$, is a non-codeword. Assume that $a \in C(z)$, where $z \in F_2$. Now $(x', z) \notin D$ and we know that $|I(D; (x', z))| \geq 3$. In particular,

$$I(D; (x', z)) = \{(c, z) \in D \mid d(x', c) \leq 1\} \cup A,$$

where $A = \{(x', z+1)\}$ if $(x', z+1) \in D$ and otherwise A is empty. Now

$$I(C; x) = \{(c, a) \in F_2^n \mid d(x', c) \leq 1, (c, z) \in D\} \cup B,$$

where $B = \{(x', b) \in F_2^n \mid b \in C(z+1)\}$ if $(x', z+1) \in D$ and otherwise B is empty. This means that also in C each non-codeword is covered by at least three codewords. Since in the intersection of three Hamming spheres of radius one there is at most one word, we know that each non-codeword is distinguishable. Now we know that each word in F_2^n has a unique I-set. Thus C is a linear $(1, \leq 1)$-identifying code of length n and cardinality $2M_1^{(\leq 1)}[n-1]$. $\square$

Theorem 5. *Let $n = 3(2^r - 1) + s$ for $r \geq 1$ and $0 \leq s \leq 3 \cdot 2^r - 1$. Then*

$$M_1^{(\leq 1)}[n] = 2^{n-r}.$$

Proof. Let $n = 3(2^r - 1)$. By Theorem 2 there exists a code such that each non-codeword is covered by exactly three codewords and each codeword is covered only by itself. Thus this code is $(1, \leq 1)$-identifying. The cardinality of the code is 2^{n-r}. The upper bounds for $1 \leq s \leq 3 \cdot 2^r - 1$ follow from Theorem 4. The lower bounds follow from Theorem 3 since, $2^{n-r-1} < 3 \cdot 2^n/(n+3) \leq 2^{n-r}$. □

The linear $(1, \leq 1)$-identifying codes constructed in the proofs of Theorem 5 and Theorem 4 are not unique for all lengths. Let $n = 2^r - 1 = 3(2^{r-2} - 1) + 2^{r-2} + 2$ for $r \geq 3$ and $\mathcal{H}$ denote a Hamming code of length n. Then the code $C = \mathcal{H} \cup (\mathcal{H} + 10^{n-1}) \cup (\mathcal{H} + 010^{n-2}) \cup (\mathcal{H} + 110^{n-2})$ is a linear code and each word in F_2^n is covered by four codewords, and thus it is also $(1, \leq 1)$-identifying. The code C is optimal and by repeatedly taking the direct sum with $\{0, 1\}$ we get optimal codes up to the length $3(2^{r-1} - 1) - 1$. These codes and the codes of Theorem 5 are not equivalent, since in the codes of Theorem 5 all codewords are covered only by themselves.

3 On linear $(1, \leq l)$-identifying codes

Theorem 6. *A linear code $C \subseteq F_2^n$ is $(1, \leq 2)$-identifying if and only if it is a 5-fold 1-covering. In particular, $M_1^{(\leq 2)}[n] = 2^{k[n,1,5]}$.*

Proof. Suppose first that $|I(C; x)| \geq 5$ for all $x \in F_2^n$. Then no set of size at most two where x does not belong to can cover the whole I-set of x. Namely, the set of size at most two can cover at most four of codewords covering x. Thus C is $(1, \leq 2)$-identifying.

Let C be a linear $(1, \leq 2)$-identifying code realizing $M_1^{(\leq 2)}[n]$. By [4] (it is also easy to see) we know that $|I(x)| \geq 3$ for all $x \in F_2^n$. Let us first consider codewords. Suppose $c \in C$. Since C is linear, $\mathbf{0} \in C$. Suppose first that $|I(c)| = 3$. Then by Lemma 1, $I(\mathbf{0}) = \{\mathbf{0}, c_1, c_2\}$ for some codewords $c_1, c_2 \in S_1(\mathbf{0})$. By linearity, $c_1 + c_2 \in C$. Again by Lemma 1, $I(c_1) = \{\mathbf{0}, c_1, c_1 + c_2\}$ and $I(c_1 + c_2) = \{c_1, c_2, c_1 + c_2\}$, and thus $I(\mathbf{0}, c_1) = I(\mathbf{0}, c_1 + c_2) = \{\mathbf{0}, c_1, c_2, c_1 + c_2\}$, which is impossible. Hence $|I(c)| \geq 4$ for all $c \in C$.

If $|I(c)| = 4$ then $I(\mathbf{0}) = \{x, y, z, \mathbf{0}\}$ where the supports of x, y and z are i, j and k respectively. By linearity there exist codewords c_1, c_2, c_3 and c_4 with supports $\{i, j\}, \{i, k\}, \{j, k\}$ and $\{i, j, k\}$ respectively. But now

$I(\mathbf{0}, c_4) = I(y, c_2) = \{\mathbf{0}, x, y, z, c_1, c_2, c_3, c_4\}$. Thus each codeword is covered by at least five codewords.

We claim that also each non-codeword is covered by at least five codewords. First we show that $|I(x)| \geq 4$ for all $x \notin C$. Assume on the contrary that $x \notin C$ and $|I(x)| = 3$. Without loss of generality (by Lemma 1) we can assume that $x \in S_1(\mathbf{0})$. There exist two non-codewords y and z in $S_1(\mathbf{0})$ such that $x + y$ and $x + z$ belong to the code, and by linearity also $y + z \in C$. Now by Lemma 1, $I(x, y) = \{\mathbf{0}, x + y, x + z, y + z\} = I(x, z)$, which is a contradiction. Hence $|I(x)| \geq 4$ for all $x \notin C$.

Assume now that $x \notin C$ and $I(x) = \{x + e_1, x + e_2, x + e_3, x + e_4\}$ where $e_i \in S_1(\mathbf{0})$, for $i = 1, \dots, 4$ are different non-codewords. Take

$$\begin{aligned} y &= x + e_1 + e_2, \\ z &= x + e_3 + e_4, \\ v &= y + e_3 + e_4. \end{aligned}$$

Using Lemma 1 we get

$$\begin{aligned} I(y) &= \{y + e_1 = x + e_2, y + e_2 = x + e_1, y + e_3, y + e_4\}, \\ I(z) &= \{z + e_1, z + e_2, z + e_3 = x + e_4, z + e_4 = x + e_3\}, \\ I(v) &= \{v + e_1, v + e_2, v + e_3 = y + e_4, v + e_4 = y + e_3\}. \end{aligned}$$

Now $z + e_1 = x + e_3 + e_4 + e_1 = y + e_3 + e_4 + e_2 = v + e_2$ and similarly $z + e_2 = v + e_1$. Thus we have $I(x, v) = I(y, z)$ which is a contradiction, and hence $|I(x)| \geq 5$ for all $x \in F_2^n$. □

Let $l \geq 3$. It is proved in [7, Theorem 2] that $C \subseteq F_2^n$ is $(1, \leq l)$-identifying if and only if it is a $(2l - 1)$-fold 1-covering. Thus we have the next theorem.

Theorem 7. *For all $l \geq 3$*

$$M_1^{(\leq l)}[n] = 2^{k[n,1,2l-1]}.$$

When $l = 2$ and $l = 3$ we want in both cases that each word is covered by at least five codewords, and thus in these two cases the optimal codes are the same.

Let $l \geq 3$. Now [7, Corollary 1] says that $M_1^{(\leq l)}(n) = (2l - 1)2^n/(n + 1)$ if and only if there are integers $i \geq 0$, $\mu_0 > 0$ such that $\mu_0 \mid (2l - 1)$ and $2l - 1 \leq 2^i \mu_0$ and $n = \mu_0 2^i - 1$. When $n = 2^r(2l - 1) - 1$ for $r \geq 0$ the above requirements are true and $(2l - 1)2^n/(n + 1) = 2^{n-r}$, and thus the linear codes constructed above for lengths $n = 2^r(2l - 1) - 1$ where $r \geq 0$ are optimal also in the case where linearity is not required.

n	$M_1^{(\leq 1)}[n]$	$M_1^{(\leq 2)}[n] = M_1^{(\leq 3)}[n]$	$M_1^{(\leq 4)}[n]$
2	4	-	-
3	4	-	-
4	8	16	-
5	16	32	-
6	32	64	64
7	64	128	128
8	128	256	256
9	128	256	512
10	256	512	1024
11	512	1024	2048
12	1024	2048	4096
13	2048	4096	4096
14	4096	8192	8192

Table 1: The values of $M_1^{(\leq 1)}[n]$, $M_1^{(\leq 2)}[n] = M_1^{(\leq 3)}[n]$ and $M_1^{(\leq 4)}[n]$ for short lengths.

4 Strongly identifying codes

Strongly identifying codes were defined in [3]. In this variant processors that belong to a code either send right information of themselves or then not. In order to identify at most l malfunctioning processors using a code C we must be able to distinguish between all the sets $I(X) \setminus S$ where $X \subseteq F_2^n$, $|X| \leq l$ and $S \subseteq C \cap X$.

Definition 2. *Let t and l be positive integers. Suppose $C \subseteq F_2^n$. For all $X \subseteq F_2^n$ we define*

$$\mathcal{I}_t(X) = \{U \mid I_t(X) \setminus (X \cap C) \subseteq U \subseteq I_t(X)\}.$$

If for all $X, Y \subseteq F_2^n$, such that $X \neq Y$, $|X|, |Y| \leq l$, we have $\mathcal{I}_t(X) \cap \mathcal{I}_t(Y) = \emptyset$, then we say that C is a strongly $(t, \leq l)$-identifying code.

The smallest cardinality of a strongly $(t, \leq l)$-identifying code is denoted by $M_t^{(\leq l)SID}(n)$. The smallest cardinality of linear strongly $(t, \leq l)$-identifying code is denoted by $M_t^{(\leq l)SID}[n]$. Clearly, a strongly $(t, \leq l)$-identifying code is $(t, \leq l)$-identifying. We denote $I'(y) = I(y) \setminus \{y\}$ for $y \in F_2^n$.

Theorem 8.

$$M_1^{(\leq 1)SID}[n] \geq 2^k \geq \left\lceil \frac{3 \cdot 2^n}{n+2} \right\rceil,$$

where k is the smallest integer such that the latter inequality holds.

Proof. Let C be an optimal linear strongly $(1, \leq 1)$-identifying code, and denote $K = |C|$. There are at most K words which are covered exactly by one codeword. From the proof of Theorem 3 we know that all the other words are covered by at least three codewords. For all $c \in C$, $|I(c)| > 1$ since otherwise $I'(c) = \emptyset$, which is impossible. In fact, codewords are covered by at least four codewords. Assume on the contrary that $|I(c)| = 3$ for $c \in C$. Then by Lemma 1, $|I(\mathbf{0})| = 3$. In particular, $I(\mathbf{0}) = \{\mathbf{0}, c_1, c_2\}$, where $c_1, c_2 \in S_1(\mathbf{0})$ are codewords. By linearity $c_1 + c_2 \in C$ and using again Lemma 1 we get $I'(\mathbf{0}) = I'(c_1 + c_2) = \{c_1, c_2\}$, which is a contradiction.

Thus we can calculate

$$4K + K + 3(2^n - 2K) \leq K(n + 1)$$

from which the claim follows. □

Theorem 9. *Let $n = 3(2^r - 1) + 1 + s$, where $r \geq 1$ and $0 \leq s \leq 3 \cdot 2^r - 1$. Then*

$$M_1^{(\leq 1)SID}[n] = 2^{n-r}.$$

Proof. Let H be an $r \times n$ matrix such that there is at most one non-zero binary r-tuple which occurs only once as the columns of H and all the other r-tuples (including the all-zero tuple) occur at least three times. As in the proof of Theorem 2 we know that the code which has H as its parity check matrix has the following properties. Each codeword is covered at least four times. There are 2^{n-r} or 0 non-codewords which are covered by exactly one codeword. All the other non-codewords are covered by at least three codewords.

The I-sets $I(x)$ for all $x \in F_2^n$ are unique since at distance one from each codeword there is at most one non-codeword which is covered only by this one codeword, and all the other words of F_2^n are covered by at least three codewords. Three codewords is enough to make an I-set unique since in the intersection of three Hamming spheres of radius one there is at most one word. Also the sets $I'(x)$ for all codewords are different, since again there are at least three words in $I'(x)$.

The lower bound follows from Theorem 8 since $2^{n-r-1} < 3 \cdot 2^n/(n+2) \leq 2^{n-r}$. □

There is a linear strongly $(1, \leq 1)$-identifying code for length $n = 3$, too (Theorem 9 does not give this). We have $M_1^{(\leq 1)SID}[3] = 8$ since F_2^3 covers each codeword four times and there are no non-codewords. Theorem 8 gives the lower bound.

Theorem 10. *For $l \geq 3$,*

$$M_1^{(\leq l)SID}[n] = 2^{k[n,1,2l-1,2l]}.$$

Proof. By [6] we know that C is a strongly $(1 \leq l)$-identifying if and only if C covers each word at least $2l-1$ times and each codeword at least $2l$ times. Thus we have the claim. □

Theorem 11.

$$M_1^{(\leq 2)SID}[n] = 2^{k[n,1,5,6]}.$$

Proof. Lower bound: Suppose C is an optimal linear strongly $(1, \leq 2)$-identifying code. By Theorem 6 we know that each word in F_2^n must be covered by at least five codewords, because otherwise C cannot be a linear $(1, \leq 2)$-identifying code. If codewords were covered by five codewords, then $I(\mathbf{0}) = \{c_1, c_2, c_3, c_4, \mathbf{0}\}$ for some $c_1, c_2, c_3, c_4 \in C$ of weight one. By linearity and Lemma 1 it would be $I'(\mathbf{0}) \cup I'(c_1 + c_2 + c_3 + c_4) = \{c_1, c_2, c_3, c_4, c_1 + c_2 + c_3, c_1 + c_2 + c_4, c_1 + c_3 + c_4, c_2 + c_3 + c_4\} = I'(c_1 + c_2) \cup I'(c_3 + c_4)$. Thus all codewords must be covered by at least six codewords.

Upper bound: By the proof of Theorem 10 we know that a code attaining the dimension $k[n, 1, 5, 6]$ is strongly $(1, \leq 3)$-identifying. This implies that such a code is also a linear strongly $(1, \leq 2)$-identifying code. □

The optimal linear strongly $(1, \leq l)$-identifying codes are the same for the values $l = 2$ and $l = 3$.

Acknowledgement: The author wishes to thank Iiro Honkala for many inspiring discussions and helpful comments.

References

[1] U. Blass, I. Honkala, and S. Litsyn. Bounds on identifying codes. *Discrete Mathematics*, 241(1-3):119–128, 2001.

[2] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein. *Covering Codes.* Elsevier, Amsterdam, 1997.

[3] I. Honkala, T. Laihonen, and S. Ranto. On strongly identifying codes. *Discrete Mathematics.* to appear.

[4] I. Honkala, T. Laihonen, and S. Ranto. On codes identifying sets of vertices in Hamming spaces. *Designs, Codes and Cryptography*, 24:193–204, 2001.

n	$M_1^{(\leq 1)SID}[n]$	$M_1^{(\leq 2)SID}[n] = M_1^{(\leq 3)SID}[n]$	$M_1^{(\leq 4)SID}[n]$
3	8	-	-
4	8	-	-
5	16	32	-
6	32	64	-
7	64	128	128
8	128	256	256
9	256	512	512
10	256	512	1024
11	512	1024	2048
12	1024	2048	4096
13	2048	4096	8192
14	4096	8192	8192

Table 2: The values of $M_1^{(\leq 1)SID}[n]$, $M_1^{(\leq 2)SID}[n] = M_1^{(\leq 3)SID}[n]$ and $M_1^{(\leq 4)SID}[n]$ for short lengths.

[5] M. G. Karpovsky, K. Chakrabarty, and L. B. Levitin. On a new class of codes for identifying vertices in graphs. *IEEE Transactions on Information Theory*, 44(2):599–611, 1998.

[6] T. Laihonen. Optimal codes for strong identification. *European Journal of Combinatorics*. to appear.

[7] T. Laihonen. Sequences of optimal identifying codes. *IEEE Transactions on Information Theory*. to appear.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**