Available online at www.sciencedirect.com
ScienceDirect
Discrete Applied Mathematics 156 (2008) 2250–2263
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

New bounds on binary identifying codes[☆]

Geoffrey Exoo[a], Tero Laihonen[b], Sanna Ranto[b,*]

[a] *Department of Mathematics and Computer Science, Indiana State University, Terre Haute, IN 47809, USA*
[b] *Department of Mathematics and Turku Centre for Computer Science TUCS, University of Turku, FIN-20014 Turku, Finland*

Received 13 March 2007; received in revised form 13 September 2007; accepted 20 September 2007
Available online 20 February 2008

Abstract

The original motivation for identifying codes comes from fault diagnosis in multiprocessor systems. Currently, the subject forms a topic of its own with several possible applications, for example, to sensor networks.

In this paper, we concentrate on identification in binary Hamming spaces. We give a new lower bound on the cardinality of r-identifying codes when $r \geq 2$. Moreover, by a computational method, we show that $M_1(6) = 19$. It is also shown, using a non-constructive approach, that there exist asymptotically good $(r, \leq \ell)$-identifying codes for fixed $\ell \geq 2$. In order to construct $(r, \leq \ell)$-identifying codes, we prove that a direct sum of r codes that are $(1, \leq \ell)$-identifying is an $(r, \leq \ell)$-identifying code for $\ell \geq 2$.

Keywords: Identifying code; Hamming space; Lower bound; Asymptotic behaviour; Direct sum

1. Introduction

Let $\mathbb{F} = \{0, 1\}$ be the binary field and denote by $\mathbb{F}^n$ the n-fold Cartesian product of it, i.e. the Hamming space. We denote by $A \triangle B$ the *symmetric difference* $(A \setminus B) \cup (B \setminus A)$ of two sets A and B. The *(Hamming) distance* $d(\mathbf{x}, \mathbf{y})$ between words $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ is the number of coordinate places in which they differ. We say that $\mathbf{x}$ r-*covers* (or *covers*) $\mathbf{y}$ if $d(\mathbf{x}, \mathbf{y}) \leq r$. The *(Hamming) ball* of radius r centered at $\mathbf{x} \in \mathbb{F}^n$ is

$$B_r(\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}^n \mid d(\mathbf{x}, \mathbf{y}) \leq r\}$$

and its cardinality is denoted by $V(n, r)$. For $X \subseteq \mathbb{F}^n$, denote

$$B_r(X) = \bigcup_{\mathbf{x} \in X} B_r(\mathbf{x}).$$

We also use the notation

$$S_r(\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}^n \mid d(\mathbf{x}, \mathbf{y}) = r\}.$$

[☆] Some of the results of this paper have been presented at the International Workshop on Coding and Cryptography, WCC 2007.
* Corresponding author. Fax: +358 23336595.
E-mail addresses: ge@ginger.indstate.edu (G. Exoo), terolai@utu.fi (T. Laihonen), samano@utu.fi (S. Ranto).

0166-218X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2007.09.017

Let C be a code of length n (i.e., a non-empty subset of $\mathbb{F}^n$) and $X \subseteq \mathbb{F}^n$. An *I-set* of the set X (with respect to the code C) is

$$I_r(C; X) = I_r(X) = B_r(X) \cap C.$$

We write for short $I_r(C; \{\mathbf{x}_1, \ldots, \mathbf{x}_k\}) = I_r(C; \mathbf{x}_1, \ldots, \mathbf{x}_k) = I_r(\mathbf{x}_1, \ldots, \mathbf{x}_k)$. If $r = 1$, we omit it from the notation whenever convenient.

Definition 1. Let r and ℓ be non-negative integers. A code $C \subseteq \mathbb{F}^n$ is said to be *$(r, \leq \ell)$-identifying* if for all $X, Y \subseteq \mathbb{F}^n$ such that $|X| \leq \ell$, $|Y| \leq \ell$ and $X \neq Y$ we have

$$I_r(C; X) \neq I_r(C; Y).$$

If $\ell = 1$, we say, for short, that C is *r-identifying*.

Note that a code $C \subseteq \mathbb{F}^n$ is $(r, \leq \ell)$-identifying if and only if

$$I_r(C; X) \triangle I_r(C; Y) \neq \emptyset \tag{1}$$

for any subsets $X, Y \subseteq \mathbb{F}^n$, $X \neq Y$ and $|X| \leq \ell$ and $|Y| \leq \ell$.

A set $X \subseteq \mathbb{F}^n$ that we try to identify (knowing only the set $I_r(X)$) is called a *fault pattern*. Clearly, $I_r(C; \emptyset) = \emptyset$ for any code C, and if C is $(r \leq \ell)$-identifying, then $I_r(C; X) = \emptyset$ implies that there is unique such a set X, namely $X = \emptyset$.

The seminal paper [10] by Karpovsky, Chakrabarty and Levitin initiated research in identifying codes, and it is nowadays a topic of its own; for various papers dealing with identification, see [14]. Originally, identifying codes were designed for finding malfunctioning processors in multiprocessor systems (such as binary hypercubes, i.e., binary Hamming spaces); in this application we want to determine the set of malfunctioning processors X (the fault pattern) of size at most ℓ when the only information available is the set $I_r(C; X)$ provided by the code C. A natural goal there is to use identifying codes which are as small as possible. The theory of identification can also be applied to sensor networks, see [16]. Small identifying codes are needed for energy conservation in [11]. For other applications like environmental monitoring, we refer to [12] and the references therein.

The smallest possible cardinality of an $(r, \leq \ell)$-identifying code of length n is denoted by $M_r^{(\leq \ell)}(n)$ (whenever such a code exists). If $\ell = 1$, we denote $M_r^{(\leq 1)}(n) = M_r(n)$. Moreover, if $r = 1$, we denote $M_1(n) = M(n)$.

This paper is organized as follows. In Section 2 we improve on the known lower bounds on the cardinalities of r-identifying codes by combining a counting argument with partial constructions. On the other hand, by computational methods, we are able to show that $M_1(6) = 19$; thus closing the gap of $18 \leq M_1(6) \leq 19$ in [2]. New 1- and 2-identifying codes are given as well. An averaging method of Section 3 guarantees that good $(r, \leq \ell)$-identifying codes exist. Since the approach is non-constructive, we focus in the last section on constructing $(r, \leq \ell)$-identifying codes for $r \geq 2$ and $\ell \geq 2$. Although $(r, \leq \ell)$-identifying codes are studied in natural grids, see for instance [6,7], in $\mathbb{F}^n$ the problem has not been addressed before when $r \geq 2$ and $\ell \geq 2$.

2. On *r*-identifying codes

2.1. A lower bound

The following theorem improves the lower bound from [10, Theorem 1 (iii) and Theorem 2] for $r \geq 2$.

Theorem 2. *Let $C \subseteq \mathbb{F}^n$ be r-identifying and $m = \max\{|I_r(\mathbf{x})| : \mathbf{x} \in \mathbb{F}^n\}$. Denote*

$$f_r(x) = \frac{(x-2)\left(\binom{2r}{r} - 1\right)}{\binom{2r}{r} + \binom{x}{2} - 1}.$$

We have

$$|C| \geq \frac{2^n (2 + f_r(v))}{V(n, r) + f_r(v) + 1}$$

where $v = m$, if $m \geq 2 + 2\binom{2r}{r}$, and $v = 3$ otherwise.

Proof. Let $C \subseteq \mathbb{F}^n$ be an r-identifying code. Denote by V_i the set of words r-covered by exactly i codewords. There are at most $K = |C|$ words which are r-covered by exactly one codeword. All the other words are r-covered at least by 2 codewords. Let $\mathbf{x} \in \mathbb{F}^n$ be r-covered by exactly two codewords, $I_r(\mathbf{x}) = \{\mathbf{c}_1, \mathbf{c}_2\}$. Now $1 \le d(\mathbf{c}_1, \mathbf{c}_2) \le 2r$. When $d(\mathbf{c}_1, \mathbf{c}_2) = 2r$ there are exactly $\binom{2r}{r}$ words r-covering both of these codewords. If $d(\mathbf{c}_1, \mathbf{c}_2) < 2r$, then by [3, Theorem 2.4.8] we know that there are at least $\binom{2r}{r}$ words r-covering both of these words. Hence, by the definition of identifying codes, for each word $\mathbf{x}$ which is r-covered by two codewords there are at least $\binom{2r}{r} - 1$ words $\mathbf{y}$ such that $I_r(\mathbf{x}) \subseteq I_r(\mathbf{y})$ and hence, words $\mathbf{y}$ are r-covered at least by three codewords. On the other hand, if $\mathbf{y} \in \mathbb{F}^n$ is r-covered by $i \ge 3$ codewords, then there can be at most $\binom{i}{2}$ words $\mathbf{z}$ such that $I_r(\mathbf{z}) \subseteq I_r(\mathbf{y})$ and $|I_r(\mathbf{z})| = 2$. Hence, by counting in two ways the number of pairs $\{\mathbf{x}, \mathbf{y}\}$ such that $\mathbf{x} \in V_2$ and $\mathbf{y} \in V_i$ $(i \ge 3)$ and $I_r(\mathbf{x}) \subseteq I_r(\mathbf{y})$, we have

$$\left(\binom{2r}{r} - 1\right)|V_2| \le \sum_{i=3}^{m} \binom{i}{2} |V_i|. \tag{2}$$

For any positive real number a we get by counting in two ways the number of pairs $\{\mathbf{x}, \mathbf{c}\}$, where $\mathbf{x} \in \mathbb{F}^n$ and $\mathbf{c} \in C$ such that $d(\mathbf{x}, \mathbf{c}) \le r$, and using (2)

$$\begin{aligned} K \cdot V(n,r) &= \sum_{i=1}^{m} i|V_i| \\ &= (2+a)2^n + \sum_{i=1}^{m}(i-2-a)|V_i| \\ &= (2+a)2^n - (1+a)|V_1| - a|V_2| + \sum_{i=3}^{m}(i-2-a)|V_i| \\ &\ge (2+a)2^n - (1+a)K + \sum_{i=3}^{m}\left(i-2-a-\frac{a}{\binom{2r}{r}-1}\binom{i}{2}\right)|V_i|. \end{aligned}$$

Clearly, $i-2-a-\frac{a}{\binom{2r}{r}-1}\binom{i}{2} \ge 0$ if and only if $a \le f_r(i)$, where

$$f_r(i) := \frac{(i-2)\left(\binom{2r}{r}-1\right)}{\binom{2r}{r}+\binom{i}{2}-1}.$$

The function f_r is decreasing when $i \ge 2 + \sqrt{2\binom{2r}{r}}$, f_r is increasing for $3 \le i \le 2 + \sqrt{2\binom{2r}{r}}$ and $f_r(3) = f_r(2 + 2\binom{2r}{r})$. Thus, when $m \ge 2 + 2\binom{2r}{r}$ we choose $a = f_r(m)$ and otherwise we choose $a = f_r(3)$. In both cases we get the following inequality

$$K \cdot V(n,r) \ge (2 + f_r(v))2^n - (1 + f_r(v))K,$$

from which the claim follows. □

We say that a set A *r-identifies* a set B if for all $\mathbf{x}, \mathbf{y} \in B$, $\mathbf{x} \ne \mathbf{y}$, we have $I_r(A; \mathbf{x}) \ne I_r(A; \mathbf{y})$.

Theorem 3. *Let A be a set of codewords in $B_r(\mathbf{0})$ which r-identifies $B_{2r}(\mathbf{0})$. Suppose $C \subseteq \mathbb{F}^n$ is an r-identifying code. If there is $\mathbf{y} \in \mathbb{F}^n$ such that $|I_r(\mathbf{y})| > |A|$, then the code $C' := (C \setminus I_r(\mathbf{y})) \cup D$, where $D := \{\mathbf{a} + \mathbf{y} \mid \mathbf{a} \in A\}$, is r-identifying and $|C'| < |C|$.*

Proof. It is clear that $|C'| < |C|$. For all $\mathbf{x} \in \mathbb{F}^n \setminus B_{2r}(\mathbf{y})$ we have $I_r(C'; \mathbf{x}) = I_r(C; \mathbf{x})$. Hence whenever $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}^n \setminus B_{2r}(\mathbf{y})$ we have $I_r(C'; \mathbf{x}_1) \ne I_r(C'; \mathbf{x}_2)$. If $\mathbf{x}_1 \in \mathbb{F}^n \setminus B_{2r}(\mathbf{y})$ we have $I_r(C'; \mathbf{x}_1) \cap B_r(\mathbf{y}) = \emptyset$ and if $\mathbf{x}_2 \in B_{2r}(\mathbf{y})$ we have $I_r(C'; \mathbf{x}_2) \cap B_r(\mathbf{y}) \ne \emptyset$. Thus, $I_r(C'; \mathbf{x}_1) \ne I_r(C'; \mathbf{x}_2)$. By the definition of the set A we know that for all $\mathbf{x}_1, \mathbf{x}_2 \in B_{2r}(\mathbf{y})$ we have $I_r(C'; \mathbf{x}_1) \ne I_r(C'; \mathbf{x}_2)$. □

Remark 4. If the code C' in the previous theorem r-covers again some word more than $|A|$ times we continue with the same process. In each step the cardinality of the code is getting smaller and every code is r-identifying. Hence, the process will stop at some point and the result will be an r-identifying code which r-covers each word in $\mathbb{F}^n$ at most $|A|$ times. Consequently, we can use $m \leq |A|$ in the previous theorem. Moreover, if C is r-identifying and attains $M_r(n)$, then we immediately know that $|I_r(\mathbf{x})| \leq |A|$ for any $\mathbf{x} \in \mathbb{F}^n$.

By [10, Theorem 4] we know that $S_1(\mathbf{0})$ 1-identifies $B_2(\mathbf{0})$. By substituting $r = 1$ and $m = |S_1(\mathbf{0})| = n$ to the Theorem 2 we get the following best known lower bound for 1-identifying codes due to Karpovsky, Chakrabarty and Levitin [10] (see also [2]).

Corollary 5 (*Karpovsky et al. [10]*).

$$M(n) \geq \frac{n2^{n+1}}{2+n+n^2} = \frac{n2^n}{V(n,2)}.$$

In [1, Construction 3] it is proven that suitable $\binom{n}{2} - n$ words in $S_2(\mathbf{0})$ 2-identify words in $B_4(\mathbf{0})$ when $n \geq 7$. Taking $m = \binom{n}{2} - n$ in the Theorem 2 one obtains the following.

Corollary 6. *For $n \geq 7$ we have*

$$M_2(n) \geq \frac{2^{n+2}(n^3 - 6n^2 + 17n - 24)}{n^5 - 5n^4 + 5n^3 - 11n^2 + 114n - 56}.$$

In [10, Theorem 5] it is proven that the set $S_r(\mathbf{0})$ r-identifies all the words in $B_{2r}(\mathbf{0})$ provided that $r < n/2$. Choosing $m = \binom{n}{r}$ implies the next result.

Corollary 7. *When $\binom{n}{r} \geq 2 + 2\binom{2r}{r}$ and $r < n/2$, we have*

$$M_r(n) \geq \frac{2^n\left(2 + f_r\left(\binom{n}{r}\right)\right)}{V(n,r) + f_r\left(\binom{n}{r}\right) + 1}.$$

We can apply also other constructions of [1] as the set A in the remark above. Using these results we get the following corollaries.

Corollary 8. *Let*

$$R = 2\binom{\lceil n/2 \rceil}{r-1}\lceil n/2 \rceil + 2\binom{\lceil n/2 \rceil}{r}.$$

When $V(n, r-1) + R \geq 2 + 2\binom{2r}{r}$ we have

$$M_r(n) \geq \frac{2^n(2 + f_r(V(n,r-1) + R))}{V(n,r) + f_r(V(n,r-1) + R) + 1}.$$

Corollary 9. *When $2r - 1$ divides n, $r \geq 3$, and*

$$R = \binom{n}{r} - \binom{2r-1}{r}\left(\frac{n}{2r-1}\right)^r$$

we have

$$M_r(n) \geq \frac{2^n(2 + f_r(V(n,r-1) + R))}{V(n,r) + f_r(V(n,r-1) + R) + 1}.$$

The lower bounds of [10, Theorem 1 (iii)] and [10, Theorem 2], of which the latter one is given below, coincide (see [10]) for every r when n is large enough.

Table 1
New bounds on the cardinalities of 2-identifying codes

n	Previous lower bounds	New lower bounds	Upper bounds
9	26	26	34
10	40	41	62
11	62	67	109
12	103	112	191
13	177	190	496
14	307	326	872
15	538	567	1528
16	950	995	3056
17	1692	1761	6112

New lower bounds come from Corollary 6. The previous lower bounds are due to [10, Theorem 1(iii)]. See Appendix for the code constructions of lengths 9–12. Upper bounds on $13 \leq n \leq 17$ follow from the given smaller codes and [5, Corollary 3].

Theorem 10 (*Karpovsky et al. [10]*).

$$M_r(n) \geq \frac{2^{n+1}}{V(n,r)+1}.$$

It is easy to see that

$$\frac{2^n(2+f_r(x))}{V(n,r)+f_r(x)+1} > \frac{2^{n+1}}{V(n,r)+1}$$

for all $x > 2$ and $n, r \geq 1$. Hence, the lower bound of Theorem 2 is always stronger than the lower bound of Theorem 10. Thus, for every fixed r there exists n_0 such that for all $n \geq n_0$ we improve on the lower bound of [10, Theorem 1 (iii)]. For example, Theorem 2 and the corollaries improve [10, Theorem 1 (iii)] for $r = 2$ when $n \geq 10$, $r = 3$ when $n \geq 20$, $r = 4$ when $n \geq 29$, and $r = 5$ when $n \geq 37$. Some new lower bounds are shown in Table 1.

2.2. Computational results

Let $\mathbf{x}_1, \mathbf{x}_2, \mathbf{w} \in \mathbb{F}^n$. We say that $\mathbf{w}$ *r-distinguishes* $\mathbf{x}_1$ and $\mathbf{x}_2$ if $d(\mathbf{w}, \mathbf{x}_i) \leq r$ for exactly one value of $i \in \{1, 2\}$. Fix an ordering of $\{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \neq \mathbf{y}, \mathbf{x}, \mathbf{y} \in \mathbb{F}^n\}$, the set of unordered pairs of elements from $\mathbb{F}^n$. Let $\sigma(\mathbf{x}, \mathbf{y})$ denote that the index of the pair $(\mathbf{x}, \mathbf{y})$ is that ordering. For each $\mathbf{w} \in \mathbb{F}^n$ define a binary sequence $\{b_i^{\mathbf{w}}\}$, $1 \leq i \leq \binom{2^n}{2}$, such that $b^{\mathbf{w}}_{\sigma(\mathbf{x},\mathbf{y})} = 1$ if $\mathbf{w}$ r-distinguishes $\mathbf{x}$ and $\mathbf{y}$, and $b^{\mathbf{w}}_{\sigma(\mathbf{x},\mathbf{y})} = 0$, otherwise. Then an r-identifying code $C = \{\mathbf{w}_k\}$ is a subset of $\mathbb{F}^n$ such that for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$, $\mathbf{x} \neq \mathbf{y}$, we have $\bigvee_k b^{\mathbf{w}_k}_{\sigma(\mathbf{x},\mathbf{y})} = 1$. i.e., every pair of elements from $\mathbb{F}^n$ is r-distinguished by at least one codeword.

2.2.1. Construction techniques

With the above notation, we can describe a series of greedy algorithms for constructing identifying codes.

1. For each $\mathbf{w} \in \mathbb{F}^n$, construct a bitstring corresponding to the sequence $\{b_i^{\mathbf{w}}\}$, $1 \leq i \leq \binom{2^n}{2}$.
2. Mark each such bitstring as unused.
3. Mark each unordered pair of $\mathbb{F}^n$ elements as undistinguished.
4. While there are undistinguished pairs:
   (a) Pick an element that distinguishes the maximum number of undistinguished pairs.
   (b) Mark the element as used.
   (c) Mark the pairs it distinguishes as distinguished.

One issue is left unresolved in the above outline: the method used to break ties in step 4(a). Several possibilities arise: choosing according to some fixed ordering, choosing randomly, or choosing according to a secondary computation.

Neither of the first two possibilities seems capable of producing new results, but will come within one or two of the current upper bounds for the values of $n \leq 12$ and $r \leq 2$. To get new results, we need to refine the tie breaking criterion. We have three essentially different methods that can be used in step 4(a) which yield new upper bounds:

- Choose the word whose mean Hamming distance from current codewords is as small as possible.
- Choose the word according to some predetermined Hamming weight distribution for the code.
- Choose the word so as equalize the number of 1-bits in each bit position.

A further word of explanation is in order for the second of these. By looking at known examples for good codes, one can speculate how an ideal weight distribution for a small identifying code should look like. Then one can choose codewords in step 4(a) that help achieve this distribution.

A number of other ideas were tried, but those listed above seem to be the most effective. However, this is a somewhat subjective evaluation, and is probably limited to the particular cases given in the theorem below.

Using these methods, we have determined new upper bounds for the cases given in the following theorem. The first of the three methods listed above produced all of the values, except for that of $M_2(12)$, which was produced by using method two as the secondary decision factor, and method three as a tertiary decision factor.

Theorem 11. *$M_1(9) \leq 114$, $M_1(10) \leq 214$, $M_2(9) \leq 34$, $M_2(10) \leq 62$, $M_2(11) \leq 109$, and $M_2(12) \leq 191$.*

The codes attaining these values are given in Appendix. From [2,10] we know that $M_1(2) = 3$, $M_1(3) = 4$, $M_1(4) = 7$, $M_1(5) = 10$, $M_1(7) = 32$, and by [1] we know $M_2(3) = 7$, $M_2(4) = 6$, $M_2(5) = 6$, $M_2(6) = 8$. Moreover, in [5] is given $M_2(7) = 14$.

2.2.2. *Lower bound proofs*

We outline a computational technique used to prove that certain codes do not exist. We focus on the case of $M_1(6)$, where it was previously established that the correct value was either 18 or 19 [2]. We show that no code of size 18 exists, thereby establishing 19 as the correct value.

Our proof makes use of a *canonical form* for a code, which we now define. Two sets of codewords are called *equivalent* if there is an automorphism of the n-cube taking one set to the other. There are $n!2^n$ automorphisms of the n-cube. These can be viewed as consisting of a permutation of the bit positions (coordinates), composed with a translation. So there are potentially $n!2^n$ representations of a code. Our canonical form will give us an unambiguous choice of one of these representations.

Let S be a set of codewords from $\mathbb{F}^n$, with $|S| = k$. It will be convenient to identify the codewords with the integers from 0 to $2^n - 1$. This gives us a natural ordering of $\mathbb{F}^n$. Our canonical form will then be an ordered list of codewords. The elements of the list will be a set of words equivalent to S with the following properties.

- The list is in increasing order.
- Among all possible lists with the first property, the canonical list is the one which is lexicographically first.

Such a canonical form, for a set of k codewords, will be called a *k-form*.

A naive approach for determining the canonical form for S requires considering 2^n translations, each combined with $n!$ coordinate permutations. It is, however, possible to speed things up considerably[1] by making a few observations. For example, the first word in a canonical form must be zero. In addition, the second word will have the minimum number of 1-bits (among the non-zero words in all representation of the code). Finally, observe that the canonical form can be generated in order by adding the word with the minimum number of bits that are not set in any of the previously included codewords. Ties can be broken by examining the bits which are set in previously included codewords.

Now we can outline the three stage proof. First, we generate an ordered list of codewords of some specified size. In the case of showing that $M_1(6) \neq 18$, we generated all 12-forms. The number of canonical forms for sets of codewords in $\mathbb{F}^6$ for sizes 1–12 are 1, 6, 16, 103, 497, 3253, 19735, 120843, 681474, 3561696, 16938566, and 73500514, respectively.

Once we have this ordered list, we generate, for each 12-form, the set of codewords that we need to examine to see if the 12-form extends to a solution (i.e., an identifying code of size 18), assuming that none of the previous forms gave us a solution. For the first 12-form on our list, we need to look at all 52 words not in the form. But if we know

[1] The final version of our canonicalization procedure was more than 100 times faster than our initial version.

that the first form does not extend to a solution, we can eliminate from consideration, in the course of processing the second form, any codeword which, when added to the second form, yields a subcode equivalent to the first.

In the third and final step in the proof, we take each of the 12-forms generated in step one, and the corresponding list of candidate additions to the form generated in step 2, and do an exhaustive search to see if it can be completed to a solution. We found that the number of words that we had to consider decreased quickly. In the course of processing the first 100,000 12-forms, the mean number of codewords we were able to eliminate exceeded 40, leaving a mean of less than 12 codewords to consider when trying to extend the form to an identifying code. For the last 100,000 12-forms, the mean number of codewords left to consider was less than one.

So in summary we have the following method.

- Generate a list of all 12-forms.
- For each 12 form, generate a list of codewords that can be added to the form without creating subcodes equivalent to forms earlier in the list.
- Do an exhaustive search using the results from the first two steps.

It should be noted that the choice of 12-forms was empirical. We ran the procedure to completion for both 11-forms and for 12-forms. Using 12-forms required about 2/3 of the time that 11-forms used. For 13-forms and larger, the quantity of data files generated was so large, we were unable to run either the second or the third step. As it was, for 12-forms, the second step required 8 GB of memory; 13-forms would have required at least 24 GB. We had no such computers available. The situation for 14-forms and larger would have been much worse.

Of these steps, the first step is the only step that we ran on a single CPU. The other two steps can be conveniently split into cases and run on multiple CPUs. They were run using over 200 CPUs in two student PC labs, one Beowulf cluster, and few faculty office machines. Over 90% of the CPU time consumed by this process was spent doing the second step.

The total elapsed time for the entire run was roughly 36 h. It may be of interest to compare this with the time that would have been taken had all $\binom{64}{18}$ possible codes been checked. Our best estimate is this would have taken using the same set of machines approximately 75,000 years.

Theorem 12. $M_1(6) = 19$.

3. An averaging method and existence of asymptotically good identifying codes

The next theorem is inspired by Delsarte and Piret [4]. Let $m(r, \ell)$ stand for the minimum of $|B_r(X) \triangle B_r(Y)|$ over any subsets $X, Y \subseteq \mathbb{F}^n$, $X \neq Y$ and $1 \leq |X| \leq \ell$ and $1 \leq |Y| \leq \ell$. If $m(r, \ell) = 0$, then no $(r, \leq \ell)$-identifying code exists in $\mathbb{F}^n$ and if $m(r, \ell) \geq 1$, then $C = \mathbb{F}^n$ is trivially $(r, \leq \ell)$-identifying. Denote further by N_ℓ the number of (unordered) pairs $\{X, Y\}$ of subsets of $\mathbb{F}^n$ such that $X \neq Y$ and $1 \leq |X| \leq \ell$ and $1 \leq |Y| \leq \ell$.

Theorem 13. *Let $r \geq 1$, $\ell \geq 1$ and $n \geq 1$. Provided that $m(r, \ell) > 0$, there exists an $(r, \leq \ell)$-identifying code of size K in $\mathbb{F}^n$ such that*

$$K \leq \left\lceil \frac{2^n}{m(r, \ell)} \ln N_\ell \right\rceil + 1.$$

Proof. Let $C \subseteq \mathbb{F}^n$. Denote by $P_r^{(\ell)}(C)$ the number of pairs $\{X, Y\}$, where $X, Y \subseteq \mathbb{F}^n$, $X \neq Y$, $1 \leq |X| \leq \ell$ and $1 \leq |Y| \leq \ell$, such that

$$I_r(C; X) \triangle I_r(C; Y) = \emptyset.$$

We denote by $\mathcal{C}_K$ the set of all codes of size K. Clearly, $|\mathcal{C}_K| = \binom{2^n}{K}$. We get

$$\begin{aligned}\sum_{C \in \mathcal{C}_K} P_r^{(\ell)}(C) &= \sum_{C \in \mathcal{C}_K} \sum_{1 \leq |X| \leq \ell} \sum_{\substack{1 \leq |Y| \leq \ell, Y \neq X \\ I_r(C;X) \triangle I_r(C;Y) = \emptyset}} 1 \\ &= \sum_{1 \leq |X| \leq \ell} \sum_{\substack{Y \neq X \\ 1 \leq |Y| \leq \ell}} \sum_{\substack{C \in \mathcal{C}_K \\ I_r(C;X) \triangle I_r(C;Y) = \emptyset}} 1\end{aligned}$$

$$= \sum_{1\le|X|\le\ell} \sum_{\substack{Y\neq X\\ 1\le|Y|\le\ell}} \binom{2^n - |B_r(X) \triangle B_r(Y)|}{K}$$
$$\le \sum_{1\le|X|\le\ell} \sum_{\substack{Y\neq X\\ 1\le|Y|\le\ell}} \binom{2^n - m(r,\ell)}{K}$$
$$\le N_\ell \binom{2^n - m(r,\ell)}{K}.$$

Let $m(r,\ell) \ge 1$ and

$$K = \left\lceil \frac{2^n}{m(r,\ell)} \ln N_\ell \right\rceil.$$

We can assume that $K \le 2^n$, because otherwise the assertion is trivial.

Now the average

$$\frac{\sum_{C\in\mathcal{C}_K} P_r^{(\ell)}(C)}{\binom{2^n}{K}} \le \frac{N_\ell \binom{2^n - m(r,\ell)}{K}}{\binom{2^n}{K}}$$
$$\le N_\ell \left(\frac{2^n - m(r,\ell)}{2^n}\right)^K$$
$$\le N_\ell \left(1 - \frac{m(r,\ell)}{2^n}\right)^K$$
$$< 1.$$

The last inequality follows from the fact that $(1-1/x)^x < 1/e$ for $x \ge 1$.

Consequently, there exists $C' \in \mathcal{C}_K$ such that $P_r^{(\ell)}(C') = 0$, that is, C' satisfies (1) for any subsets $X, Y \subseteq \mathbb{F}^n$, $X \neq Y$ and $1 \le |X| \le \ell$ and $1 \le |Y| \le \ell$. To guarantee that we can construct with C' an $(r, \le \ell)$-identifying code, we need to make sure that (1) also holds when $X = \emptyset$, that is, $I_r(C;Y) \neq \emptyset$ for any $Y \subseteq \mathbb{F}^n$, $1 \le |Y| \le \ell$. Obviously, this is satisfied if $I_r(C;\mathbf{y}) \neq \emptyset$ for all $\mathbf{y} \in \mathbb{F}^n$. If $\ell \ge 2$, then this holds for C'; if $I_r(C';\mathbf{w}) = \emptyset$, then $I_r(C';\mathbf{w}') \triangle I_r(C';\mathbf{w}',\mathbf{w}) = \emptyset$ for any $\mathbf{w} \neq \mathbf{w}'$ and this contradicts $P_r^{(\ell)}(C') = 0$. If $\ell = 1$ we must modify our code C' accordingly. There can be at most one word, say $\mathbf{w}$, such that $I_r(C';\mathbf{w}) = \emptyset$; indeed, if $I_r(C';\mathbf{w}) = I_r(C';\mathbf{w}') = \emptyset$ for $\mathbf{w} \neq \mathbf{w}'$, then we obtain $I_r(\mathbf{w}) \triangle I_r(\mathbf{w}') = \emptyset$ which contradicts the fact that $P_r^{(1)}(C') = 0$. Consequently, the code $C' \cup \{\mathbf{w}\}$ is $(r, \le \ell)$-identifying and the size equals $K+1$. □

Corollary 14. *Let $2r+1 \le n$. There exists an $(r, \le 1)$-identifying code in $\mathbb{F}^n$ of cardinality*

$$K \le \left\lceil \frac{2^n}{\binom{n-1}{r}} n \ln 2 \right\rceil + 1.$$

Proof. By [3, Theorem 2.4.8], we know that $m(r,1) = 2\binom{n-1}{r}$. Obviously, $N_1 = \binom{2^n}{2} \le 2^{2n}$. The claim now follows from the previous theorem. □

This result improves on the upper bound in [9, Corollary 2.3]. Here we apply directly the averaging method to identifying codes instead of using covering codes. Moreover, this approach has the advantage that it works also in the cases $\ell \ge 2$. It is shown in [9] that

$$\lim_{n\to\infty} \frac{1}{n} \log_2 M_r(n) = 1 - H(\rho)$$

where $r = \lfloor \rho n \rfloor$ and $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. An analogous asymptotic result is not known for $\ell > 1$. The next two corollaries give us a result which is close to the best possible when ρ is small and ℓ is fixed (see Fig. 1).

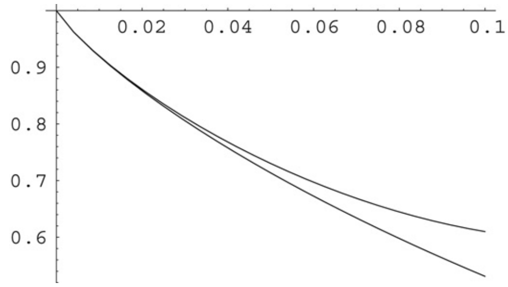

Fig. 1. For $\ell = 2$ the lower bound $1 - H(\rho)$ and the upper bound $1 - (1 - 2\ell\rho)H(\frac{\rho}{1-2\ell\rho})$.

Corollary 15. *Let $\ell \geq 2$ and $n \geq (2\ell + 1)r$. There exists an $(r, \leq \ell)$-identifying code in $\mathbb{F}^n$ of size*

$$K \leq \left\lceil \frac{2^n}{\binom{n-2\ell r}{r}} 2 \ln \sum_{i=1}^{\ell} \binom{2^n}{i} \right\rceil .$$

Proof. First we estimate $m(r, \ell)$. Let X be the larger one of the two subsets (in the definition of $m(r, \ell)$) if they are of different sizes. There exists $\mathbf{x} \in X \setminus Y$ and, without loss of generality, we can assume that $\mathbf{x}$ is the all-zero word. Denote by S the set of coordinates where at least one element of $Y \cap B_{2r}(\mathbf{0})$ has 1. The size of S is at most $2\ell r$. Now those words of weight r whose all 1's are outside S belong to $B_r(\mathbf{x}) \subseteq B_r(X)$ but not to $B_r(Y)$ by the definition of S. Thus,

$$m(r, \ell) \geq \binom{n - 2\ell r}{r}.$$

The assertion follows from the previous theorem by observing that

$$N_\ell \leq \left(\sum_{i=1}^{\ell} \binom{2^n}{i} \right)^2 . \quad \square$$

Using standard estimates for binomial coefficients, see [3, p. 33], we conclude the following.

Corollary 16. *Let $\ell \geq 2$ and $r = \lfloor \rho n \rfloor$ where $0 \leq \rho \leq 1/(2\ell + 1)$. Then*

$$1 - H(\rho) \leq \lim_{n \to \infty} \frac{1}{n} \log_2 M_r^{(\leq \ell)}(n) \leq 1 - (1 - 2\ell\rho) H\left(\frac{\rho}{1 - 2\ell\rho} \right).$$

4. On $(r, \leq \ell)$-identifying codes

In the previous section we saw that there exist (without any constructions) $(r, \leq \ell)$-identifying codes of small sizes. In this section we construct $(r, \leq \ell)$-identifying codes by a direct sum method. Although $(r, \leq \ell)$-identifying codes are studied in the square grid, the triangular grid, the king grid and the hexagonal mesh [7,6], no results concerning these codes (when $r \geq 2$ and $\ell \geq 2$) in Hamming spaces are known. Before the direct sum method, we give a lower estimate.

Theorem 17. *For $r \geq 2$ and $\ell \geq 2$ we have*

$$M_r^{(\leq \ell)}(n) \geq \left\lceil \frac{(2\ell - 1)2^n}{\binom{n}{r} + \binom{n}{r-1}} \right\rceil .$$

Proof. Suppose $C \subseteq \mathbb{F}^n$ is an $(r, \leq \ell)$-identifying code. We shall show that for every $\mathbf{x} \in \mathbb{F}^n$ we have $|I_r(\mathbf{x}) \cap (S_r(\mathbf{x}) \cup S_{r-1}(\mathbf{x}))| \geq 2\ell - 1$. Without loss of generality we can prove that the claim holds for $\mathbf{x} = \mathbf{0}$ and clearly, it then holds for every $\mathbf{x} \in \mathbb{F}^n$. For any two words $\mathbf{c}_1, \mathbf{c}_2$ of weight $1 \le w(\mathbf{c}_1) \le r$ and $1 \le w(\mathbf{c}_2) \le r$ there is a word $\mathbf{y}_1$ of weight two which r-covers both of these words. Clearly, $I_{r-2}(\mathbf{0}) \subseteq I_r(\mathbf{y}_1)$. If $|I_r(\mathbf{0}) \cap (S_r(\mathbf{0}) \cup S_{r-1}(\mathbf{0}))| \le 2\ell - 2$, then there is a collection of words of weight two, $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_{\ell-1}$, which r-cover the whole set $I_r(\mathbf{0})$. This is not possible because otherwise we have $I_r(\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_{\ell-1}) = I_r(\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_{\ell-1}, \mathbf{0})$. We get the claim by counting in two ways the number of pairs $\{\mathbf{x}, \mathbf{c}\}$ where $\mathbf{x} \in \mathbb{F}^n$, $\mathbf{c} \in C$, and $r - 1 \le d(\mathbf{c}, \mathbf{x}) \le r$:

$$|C|\left(\binom{n}{r} + \binom{n}{r-1}\right) \ge (2\ell - 1)2^n. \quad \square$$

A direct sum of codes $C_1 \subseteq \mathbb{F}^n$ and $C_2 \subseteq \mathbb{F}^m$ is

$$C_1 \oplus C_2 = \{(\mathbf{c}_1, \mathbf{c}_2) \in \mathbb{F}^{n+m} \mid \mathbf{c}_1 \in C_1, \mathbf{c}_2 \in C_2\}.$$

In [5] it is proved that we can get an r-identifying code as a direct sum of r 1-identifying codes. In this section we generalize this result for $(r, \le \ell)$-identifying codes. We separate two cases $\ell = 2$ and $\ell \ge 3$.

By [13,8] we have the following frequently used lemma.

Lemma 18. *Let $C \subseteq \mathbb{F}^n$ be a $(1, \le \ell)$-identifying code. For all $\mathbf{x} \in \mathbb{F}^n$ we have $|I_r(\mathbf{x})| \ge 2\ell - 1$.*

The following lemma is easy to check.

Lemma 19. *For all $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ we have*

$$|B_1(\mathbf{x}) \cap B_1(\mathbf{y})| = \begin{cases} n+1 & \text{if } \mathbf{x} = \mathbf{y} \\ 2 & \text{if } 1 \le d(\mathbf{x}, \mathbf{y}) \le 2 \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 20. *Let $C \subseteq \mathbb{F}^n$ be a $(1, \le 2)$-identifying code. There does not exist a* square *of codewords such that $\mathbf{x}, \mathbf{y} \in C$, $d(\mathbf{x}, \mathbf{y}) = 2$, $|I(\mathbf{x})| = |I(\mathbf{y})| = 3$ and $|I(\mathbf{x}) \cap I(\mathbf{y})| = 2$.*

Proof. Suppose to the contrary that for $\mathbf{x}, \mathbf{y} \in C$ we have $d(\mathbf{x}, \mathbf{y}) = 2$, $|I(\mathbf{x})| = |I(\mathbf{y})| = 3$ and $|I(\mathbf{x}) \cap I(\mathbf{y})| = 2$. For $\mathbf{c} \in I(\mathbf{x}) \cap I(\mathbf{y})$ we have $I(\mathbf{x}, \mathbf{c}) = I(\mathbf{y}, \mathbf{c})$, which is a contradiction. $\square$

Let n_i be positive integers for $i = 1, \ldots, r$. Denote $N = \sum_{i=1}^{r} n_i$ and $N^* = N - n_r$.

Theorem 21. *Suppose $r \ge 1$. Let $C_i \subseteq \mathbb{F}^{n_i}$ for $1 \le i \le r$ be $(1, \le 2)$-identifying codes. Then $C = C_1 \oplus \cdots \oplus C_r$ is an $(r, \le 2)$-identifying code.*

Proof. Let $X = \{\mathbf{x}, \mathbf{y}\}$, $Y = \{\mathbf{z}, \mathbf{w}\} \subseteq \mathbb{F}^N$, $X \ne Y$ and $|X|, |Y| \le 2$. Denote $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_r)$, $\mathbf{y} = (\mathbf{y}_1, \ldots, \mathbf{y}_r)$, $\mathbf{z} = (\mathbf{z}_1, \ldots, \mathbf{z}_r)$ and $\mathbf{w} = (\mathbf{w}_1, \ldots, \mathbf{w}_r)$. If for some k there is $\{\mathbf{x}_k, \mathbf{y}_k\} \ne \{\mathbf{z}_k, \mathbf{w}_k\}$, then because C_k is $(1, \le 2)$-identifying there is $\mathbf{c}_k \in I_1(C_k; \mathbf{x}_k, \mathbf{y}_k) \triangle I_1(C_k; \mathbf{z}_k, \mathbf{w}_k)$. Without loss of generality we may assume $\mathbf{c}_k \in I_1(C_k; \mathbf{x}_k) \setminus I_1(C_k; \mathbf{z}_k, \mathbf{w}_k)$. By Lemma 18, for all $1 \le h \le k$, $h \ne k$, we have $|I_1(C_h; \mathbf{x}_h)| \ge 3 > |\{\mathbf{z}_h, \mathbf{w}_h\}|$. Thus, there is a codeword $\mathbf{c}_h \in I_1(C_h; \mathbf{x}_h)$ such that $d(\mathbf{c}_h, \{\mathbf{z}_h, \mathbf{w}_h\}) \ge 1$. Hence $(\mathbf{c}_1, \ldots, \mathbf{c}_{k-1}, \mathbf{c}_k, \mathbf{c}_{k+1}, \ldots, \mathbf{c}_r) \in I_r(C; \mathbf{x}) \setminus I_r(C; Y)$.

Suppose that for all $1 \le k \le r$ we have $\{\mathbf{x}_k, \mathbf{y}_k\} = \{\mathbf{z}_k, \mathbf{w}_k\}$. This is possible only if $|X| = |Y| = 2$. Because $X \ne Y$ we may assume

$$\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_r) \qquad \mathbf{z} = (\mathbf{x}_1, \mathbf{y}_2, \mathbf{z}_3, \ldots, \mathbf{z}_r)$$
$$\mathbf{y} = (\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3, \ldots, \mathbf{y}_r) \qquad \mathbf{w} = (\mathbf{y}_1, \mathbf{x}_2, \mathbf{w}_3, \ldots, \mathbf{w}_r)$$

where $\mathbf{x}_1 \ne \mathbf{y}_1$, $\mathbf{x}_2 \ne \mathbf{y}_2$ and $\{\mathbf{x}_k, \mathbf{y}_k\} = \{\mathbf{z}_k, \mathbf{w}_k\}$ for $k \ge 3$. Because $\mathbf{x}_h \in \{\mathbf{z}_h, \mathbf{w}_h\}$ for all $3 \le h \le r$, then by Lemma 18, $|I_1(C_h; \mathbf{x}_h) \setminus \{\mathbf{x}_h\}| \ge 2 > |\{\mathbf{z}_h, \mathbf{w}_h\} \setminus \{\mathbf{x}_h\}|$. Thus, for all $3 \le h \le r$ there are $\mathbf{c}_h \in I_1(C_h; \mathbf{x}_h)$ such that $d(\mathbf{c}_h, \{\mathbf{z}_h, \mathbf{w}_h\}) \ge 1$. Similarly, we find corresponding codewords for $\mathbf{y}_3, \ldots, \mathbf{y}_r$.

Lemmata 18 and 19 imply that there is $\mathbf{c}_i \in I_1(C_i; \mathbf{x}_i) \setminus I_1(C_i; \mathbf{y}_i)$ for $i = 1, 2$. For both i's there are two possible cases

(A) $d(\mathbf{x}_i, \mathbf{c}_i) = 1$
(B) $d(\mathbf{x}_i, \mathbf{c}_i) = 0$, if there is no codeword $\mathbf{c}_j$ such that the case A would hold.

In the case (B) we must have by Lemma 19, $d(\mathbf{x}_i, \mathbf{y}_i) = 2$ and $|I_1(C_i; \mathbf{x}_i) \cap I_1(C_i; \mathbf{y}_i)| = 2$. Lemma 20 implies that there is $\mathbf{c}_{\mathbf{y}_i} \in I_1(C_i; \mathbf{y}_i) \setminus I_1(C_i; \mathbf{x}_i)$ such that $d(\mathbf{x}_i, \mathbf{c}_{\mathbf{y}_i}) = 3$ and $d(\mathbf{y}_i, \mathbf{c}_{\mathbf{y}_i}) = 1$. If both $\mathbf{x}_1$ and $\mathbf{x}_2$ belong to the case (A), then $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_r) \in I_r(C; X) \setminus I_r(C; Y)$. If $\mathbf{x}_1$ belongs to the case (A) and $\mathbf{x}_2$ belongs to the case (B), then $(\mathbf{c}_1, \mathbf{c}_{\mathbf{y}_2}, \mathbf{c}_3, \ldots, \mathbf{c}_r) \in I_r(C; Y) \setminus I_r(C; X)$. The cases $\mathbf{x}_1$ in (B) and $\mathbf{x}_2$ in (A) proceed similarly. If both $\mathbf{x}_1$ and $\mathbf{x}_2$ belong to the case (B), then $(\mathbf{x}_1, \mathbf{c}_{\mathbf{y}_2}, \mathbf{c}_3, \ldots, \mathbf{c}_r) \in I_r(C; Y) \setminus I_r(C; X)$. □

When proving the corresponding result for $\ell \geq 3$ the following lemmata are used.

Lemma 22. *Let $\ell \geq 3$ and $C \subseteq \mathbb{F}^n$ be an $(1, \leq \ell)$-identifying code. For all $\mathbf{x} \in \mathbb{F}^n$ and $Y \subseteq \mathbb{F}^n$, $|Y| \leq \ell$, there exists $\mathbf{c} \in I_1(\mathbf{x}) \setminus \{\mathbf{x}\}$ such that $d(\mathbf{c}, Y) \geq 1$.*

Proof. By [13] we know that for all $\mathbf{x} \in \mathbb{F}^n$ we have $|I_1(\mathbf{x})| \geq 2\ell - 1$. Thus, $|I_1(\mathbf{x}) \setminus \{\mathbf{x}\}| \geq 2\ell - 2 > \ell \geq |Y|$, which implies the claim. □

Lemma 23. *Suppose $r \geq 1$ and $\ell \geq 2$. Let $C \subseteq \mathbb{F}^n$ be an $(r, \leq \ell)$-identifying code. Then for all $\mathbf{x} \in \mathbb{F}^n$ and for every $\mathbf{e} \in S_1(\mathbf{x})$ it holds that the set $(C \cap S_r(\mathbf{x})) \setminus B_r(\mathbf{e})$ is such that there is no set of size at most $\ell - 2$ that r-covers it.*

Proof. Assume that for some $\mathbf{x} \in \mathbb{F}^n$ and $\mathbf{e} \in S_1(\mathbf{x})$ there is a set $Y \subseteq \mathbb{F}^n$ such that $|Y| \leq \ell - 2$ and Y r-covers a set $(I_r(\mathbf{x}) \cap S_r(\mathbf{x})) \setminus (S_r(\mathbf{x}) \cap B_r(\mathbf{e}))$. Then $I_r(Y \cup \{\mathbf{x}, \mathbf{e}\}) = I_r(Y \cup \{\mathbf{e}\})$, which is impossible. □

Theorem 24. *Suppose $\ell \geq 3$. Let $C_i \subseteq \mathbb{F}^{n_i}$ for $1 \leq i \leq r$ be $(1, \leq \ell)$-identifying codes. Then $C = C_1 \oplus \cdots \oplus C_r \subseteq \mathbb{F}^N$ is an $(r, \leq \ell)$-identifying code.*

Proof. We prove by induction on r that $C = C_1 \oplus \cdots \oplus C_r$ is an $(r, \leq \ell)$-identifying code and, moreover, for every $X, Y \subseteq \mathbb{F}^N$, $1 \leq |X|, |Y| \leq \ell$ and $X \neq Y$, there is $\mathbf{c} \in I_r(C; \mathbf{x}) \setminus I_r(C; Y)$ such that $r - 1 \leq d(\mathbf{c}, \mathbf{x}) \leq r$ for some $\mathbf{x} \in X$ or $\mathbf{c} \in I_r(C; \mathbf{y}) \setminus I_r(C; X)$ such that $r - 1 \leq d(\mathbf{c}, \mathbf{y}) \leq r$ for some $\mathbf{y} \in Y$. The first step of induction, $r = 1$, is trivial. The induction hypothesis is that the claim holds for $C^* = C_1 \oplus \cdots \oplus C_{r-1}$.

Let $X, Y \subseteq \mathbb{F}^N$, $1 \leq |X|, |Y| \leq \ell$, $X \neq Y$, $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_{\ell_1}\}$ and $Y = \{\mathbf{y}_1, \ldots, \mathbf{y}_{\ell_2}\}$ and denote

$$\mathbf{x}_i = (\mathbf{x}_{i,1}, \ldots, \mathbf{x}_{i,r-1}, \mathbf{x}_{i,r}) = (\mathbf{x}_i^*, \mathbf{x}_{i,r}), \qquad \mathbf{y}_j = (\mathbf{y}_{j,1}, \ldots, \mathbf{y}_{j,r-1}, \mathbf{y}_{j,r}) = (\mathbf{y}_j^*, \mathbf{y}_{j,r})$$

for $1 \leq i \leq \ell_1$ and $1 \leq j \leq \ell_2$. Denote $X^* = \{\mathbf{x}_1^*, \ldots, \mathbf{x}_{\ell_1}^*\}$ and $Y^* = \{\mathbf{y}_1^*, \ldots, \mathbf{y}_{\ell_2}^*\}$, $X_i = \{\mathbf{x}_{1,i}, \ldots \mathbf{x}_{\ell_1,i}\}$ and $Y_i = \{\mathbf{y}_{1,i}, \ldots, \mathbf{y}_{\ell_2,i}\}$, for $1 \leq i \leq r$.

If $X^* \neq Y^*$, then the induction hypothesis implies that there is a codeword $\mathbf{c}^* \in I_{r-1}(C^*; X^*) \triangle I_{r-1}(C^*; Y^*)$. Without loss of generality we may assume $\mathbf{c}^* \in I_{r-1}(C^*; \mathbf{x}_1^*) \setminus I_{r-1}(C^*; Y^*)$. The induction hypothesis also implies, that $r - 2 \leq d(\mathbf{c}^*, \mathbf{x}_1^*) \leq r - 1$. By Lemma 22 we know that there is $\mathbf{c}_r \in I_1(C_r; \mathbf{x}_{1,r}) \setminus \{\mathbf{x}_{1,r}\}$ such that $d(\mathbf{c}_r, Y_r) \geq 1$. Hence $(\mathbf{c}^*, \mathbf{c}_r) \in I_r(C; X) \setminus I_r(C; Y)$. Moreover, $r - 1 \leq d((\mathbf{c}^*, \mathbf{c}_r), \mathbf{x}_1) \leq r$.

Suppose next $X^* = Y^*$ and $X_r \neq Y_r$. Because C_r is $(1, \leq \ell)$-identifying there is $\mathbf{c}_r \in I_1(C_r; X_r) \triangle I_1(C_r; Y_r)$. Without loss of generality we may assume $\mathbf{c}_r \in I_1(C_r; \mathbf{x}_{1,r}) \setminus I_1(C_r; Y_r)$. By Lemma 22, for every $1 \leq k \leq r - 1$ there is $\mathbf{c}_k \in I_1(C_k; \mathbf{x}_{1,k}) \setminus \{\mathbf{x}_{1,k}\}$ such that $d(\mathbf{c}_k, Y_k) \geq 1$. Hence, $(\mathbf{c}_1, \ldots, \mathbf{c}_{r-1}, \mathbf{c}_r) \in I_r(C; X) \setminus I_r(C; Y)$. Moreover, $(\mathbf{c}_1, \ldots, \mathbf{c}_{r-1}, \mathbf{c}_r) \in S_{r-1}(\mathbf{x}_1) \cup S_r(\mathbf{x}_1)$.

Suppose then $X^* = Y^*$ and $X_r = Y_r$. There is for some k, $\mathbf{x}_{k,r} \neq \mathbf{y}_{h,r}$ for all h for which $\mathbf{x}_k^* = \mathbf{y}_h^*$, otherwise $X = Y$.

- Suppose $|Y^* \setminus \{\mathbf{x}_k^*\}| \leq \ell - 2$, then by Lemma 23 there is a codeword $\mathbf{c}^* \in (C^* \cap S_{r-1}(\mathbf{x}_k^*)) \setminus I_{r-1}(Y^* \setminus \{\mathbf{x}_k^*\})$. There is $\mathbf{c}_r \in I_1(C_r; \mathbf{x}_{k,r}) \setminus I_1(C_r; Y_r \setminus \{\mathbf{x}_{k,r}\})$. If $d(\mathbf{c}_r, \mathbf{x}_{k,r}) = 1$, then $(\mathbf{c}^*, \mathbf{c}_r) \in I_r(C; X) \setminus I_r(C; Y)$.

  Suppose $\mathbf{c}_r = \mathbf{x}_{k,r}$ is the only codeword in $I_1(C_r; \mathbf{x}_{k,r}) \setminus I_1(C_r; Y_r \setminus \{\mathbf{x}_{k,r}\})$. This implies $|I_1(C_r; \mathbf{x}_{k,r}) \setminus \{\mathbf{x}_{k,r}\}| = 2\ell - 2$, $|Y_r \setminus \{\mathbf{x}_{k,r}\}| = \ell - 1$, for all $\mathbf{y}_{h,r} \in Y_r \setminus \{\mathbf{x}_{k,r}\}$ we have $d(\mathbf{x}_{k,r}, \mathbf{y}_{h,r}) = 2$ and $|I_1(C_r; \mathbf{x}_{k,r}) \cap I_1(C_r; \mathbf{y}_{h,r})| = 2$. Moreover, we have $d(\mathbf{y}_{h_1,r}, \mathbf{y}_{h_2,r}) = 4$, for $h_1 \neq h_2$. There is $\mathbf{x}_t^* \in X^* = Y^*$ such that $\mathbf{x}_k^* \neq \mathbf{x}_t^*$. Otherwise, $X^* = \{\mathbf{x}_k^*\} = Y^*$ and $X_r = Y_r$ imply that $X = Y$. Suppose there is $\mathbf{y}_{t,r}$ such that $(\mathbf{x}_t^*, \mathbf{y}_{t,r}) \in Y$ and $(\mathbf{x}_k^*, \mathbf{y}_{t,r}) \notin Y$. Let us choose $\mathbf{c}_r' \in I_1(C_r; \mathbf{x}_{k,r}) \cap I_1(C_r; \mathbf{y}_{t,r})$. As mentioned above $d(\mathbf{c}_r', \mathbf{x}_{k,r}) = d(\mathbf{c}_r', \mathbf{y}_{t,r}) = 1$

and $d(\mathbf{c}'_r, \mathbf{y}_{h,r}) = 3$ for all $\mathbf{y}_{h,r} \neq \mathbf{x}_{k,r}$ and $\mathbf{y}_{h,r} \neq \mathbf{y}_{t,r}$. We get $(\mathbf{c}^*, \mathbf{c}'_r) \in I_r(C; X) \setminus I_r(C; Y)$, moreover $d((\mathbf{c}^*, \mathbf{c}'_r), (\mathbf{x}^*_k, \mathbf{x}_{k,r})) = r$.

If such a $\mathbf{y}_{t,r}$ does not exist, then $X^* = Y^* = \{\mathbf{x}^*_k, \mathbf{x}^*_t\}$ and $\mathbf{x}^*_k$ appears $\ell - 1$ times in Y^*. Now $(\mathbf{x}^*_t, \mathbf{x}_{k,r}) \in Y \setminus X$ and $(\mathbf{x}^*_t, \mathbf{x}_{t,r}) \in X \setminus Y$. Moreover, $|Y^* \setminus \{\mathbf{x}^*_t\}| = 1 \leq \ell - 2$, as above we have $\mathbf{c}^*_t \in (C^* \cap S_{r-1}(\mathbf{x}^*_t)) \setminus I_{r-1}(C^*; Y^* \setminus \{\mathbf{x}^*_t\})$. Because $|I_1(C_r; \mathbf{x}_{t,r})| \geq 2\ell - 1 > 3 \geq |(I_1(\mathbf{x}_{t,r}) \cap I_1(\mathbf{x}_{k,r})) \cup \{\mathbf{x}_{t,r}\}|$ there is $\mathbf{c}_{t,r} \in I_1(C_r; \mathbf{x}_{t,r}) \setminus (\{\mathbf{x}_{t,r}\} \cup I_1(C_r; \mathbf{x}_{k,r}))$. As above it is proved, we know that $d(\mathbf{c}_{t,r}, \mathbf{y}_{h,r}) \geq 3$ for all $\mathbf{y}_{h,r} \in Y_r$, $\mathbf{y}_{h,r} \neq \mathbf{x}_{t,r}$. Hence, $(\mathbf{c}_t, \mathbf{c}_{t,r}) \in I_r(C; (\mathbf{x}^*_t, \mathbf{x}_{t,r})) \setminus I_r(C; Y)$. Moreover, $d((\mathbf{x}^*_t, \mathbf{x}_{t,r}), (\mathbf{c}_t, \mathbf{c}_{t,r})) = r$.

- Suppose then that $|Y^* \setminus \{\mathbf{x}^*_k\}| = \ell - 1$. This implies $|Y^*| = \ell$ and every word in Y^* appears there only once. Because $X^* = Y^*$ the same holds for X^*, as well. Hence, there is $(\mathbf{x}^*_k, \mathbf{x}_{k,r}) \in X \setminus Y$ and $(\mathbf{x}^*_k, \mathbf{y}_{h,r}) \in Y \setminus X$, for some h. By the induction hypothesis there is $\mathbf{c}^* \in I_{r-1}(C^*; X^*) \triangle I_{r-1}(C^*; X^* \setminus \{\mathbf{x}^*_k\})$. This implies $\mathbf{c}^* \in I_{r-1}(C^*; \mathbf{x}^*_k)$ and $r - 2 \leq d(\mathbf{c}^*, \mathbf{x}^*_k) \leq r - 1$.
  - Suppose $d(\mathbf{c}^*, \mathbf{x}^*_k) = r - 1$. Because
  $$|(I_1(C_r; \mathbf{x}_{k,r}) \setminus \{\mathbf{x}_{k,r}\}) \setminus I_1(C_r; \mathbf{y}_{h,r})| \geq 2\ell - 4 > \ell - 2 = |Y_r \setminus \{\mathbf{x}_{k,r}, \mathbf{y}_{h,r}\}|$$
  we know that there is $\mathbf{c}_r \in I_1(C_r; \mathbf{x}_{k,r}) \setminus \{\mathbf{x}_{k,r}\}$ such that $d(\mathbf{c}_r, \mathbf{y}_{h,r}) \geq 2$ and $d(\mathbf{c}_r, \mathbf{y}_{j,r}) \geq 1$ for $j \neq h$. Thus, $(\mathbf{c}^*, \mathbf{c}_r) \in I_r(C; X) \setminus I_r(C; Y)$ and $d((\mathbf{c}^*, \mathbf{c}_r), (\mathbf{x}^*_k, \mathbf{x}_{k,r})) = r$.
  - Suppose $d(\mathbf{c}^*, \mathbf{x}^*_k) = r - 2$. We separate cases depending on the distance between $\mathbf{x}_{k,r}$ and $\mathbf{y}_{h,r}$. In every case, we will find a codeword $\mathbf{c}_r$ such that $1 \leq d(\mathbf{x}_{k,r}, \mathbf{c}_r) \leq 2$, $d(\mathbf{y}_{h,r}, \mathbf{c}_r) \geq 3$ and $d(\mathbf{c}_r, \mathbf{y}_{j,r}) \geq 1$, for $j \neq h$. Then $(\mathbf{c}^*, \mathbf{c}_r) \in I_r(C; X) \setminus I_r(C; Y)$ and it satisfies the wanted distance properties. If $d(\mathbf{x}_{k,r}, \mathbf{y}_{h,r}) \geq 4$, then clearly there is $\mathbf{c}_r \in I_1(C_r; \mathbf{x}_{k,r}) \setminus \{\mathbf{x}_{k,r}\}$, which satisfies the conditions.

    If $d(\mathbf{x}_{k,r}, \mathbf{y}_{h,r}) = 3$, then $|S_1(\mathbf{x}_{k,r}) \cap B_2(\mathbf{y}_{h,r})| = 3$. Because always $n_i \geq 4$ (otherwise no $(1, \leq \ell)$-identifying code exists), there is $\mathbf{z} \in S_1(\mathbf{x}_{k,r}) \setminus B_2(\mathbf{y}_{h,r})$. Now $|I_1(C_r; \mathbf{z}) \setminus \{\mathbf{x}_{k,r}, \mathbf{z}\}| \geq 2\ell - 3 > \ell - 2 \geq |Y_r \setminus \{\mathbf{x}_{k,r}, \mathbf{y}_{h,r}\}|$ implies that there is $\mathbf{c}_r \in I_1(C_r; \mathbf{z})$ which satisfies the conditions.

    If $d(\mathbf{x}_{k,r}, \mathbf{y}_{h,r}) = 2$, then $|(I_1(C_r; \mathbf{x}_{k,r}) \setminus \{\mathbf{x}_{k,r}\}) \setminus B_2(\mathbf{y}_{h,r})| \geq 2\ell - 4 > \ell - 2 = |Y_r \setminus \{\mathbf{x}_{k,r}, \mathbf{y}_{h,r}\}|$. Thus, we find $\mathbf{c}_r \in I_1(C_r; \mathbf{x}_{k,r})$ which satisfies the conditions.

    If $d(\mathbf{x}_{k,r}, \mathbf{y}_{h,r}) = 1$, then there is $\mathbf{z} \in S_1(\mathbf{x}_{k,r})$, $\mathbf{z} \neq \mathbf{y}_{h,r}$ and
    $$\begin{aligned}|I_1(C_r; \mathbf{z}) \setminus (\{\mathbf{x}_{k,r}, \mathbf{z}\} \cup (I_1(\mathbf{y}_{h,r}) \cap I_1(\mathbf{z})))| &\geq 2\ell - 4 > \ell - 2 \\ &\geq |Y_r \setminus \{\mathbf{x}_{k,r}, \mathbf{y}_{h,r}\}|.\end{aligned}$$
    Thus, there is $\mathbf{c}_r \in I_1(C_r; \mathbf{z}) \cap S_2(\mathbf{x}_{k,r})$, which satisfies the conditions. □

Combining the results of Theorems 21 and 24 and [5, Theorem 3], we get the next corollary.

Corollary 25. *For $r \geq 1$ and $\ell \geq 1$ we have*

$$M_r^{(\leq \ell)}\left(\sum_{i=1}^{r} n_i\right) \leq \prod_{i=1}^{r} M_1^{(\leq \ell)}(n_i).$$

Cardinalities for $(1, \leq 2)$-identifying codes can be found from [8,15], for example $M_1^{(\leq 2)}(4) = 11$, $M_1^{(\leq 2)}(5) = 16$, $30 \leq M_1^{(\leq 2)}(6) \leq 32$ and $M_1^{(\leq 2)}(7) = 48$. For $\ell \geq 3$, $(1, \leq \ell)$-identifying codes are considered in [13].

Acknowledgements

We wish to thank Iiro Honkala for fruitful discussions and, in particular, for helping us with Remark 4 and Theorem 3. We would also like to thank anonymous reviewers for valuable comments. Moreover S. Ranto wishes to thank Antoine Lobstein for useful comments. The second author's research was supported by the Academy of Finland under grant 111940. The third author's research was supported in part by the Nokia Foundation and the Academy of Finland under grant 210280.

Appendix

In this section we list the 1- and 2-identifying codes of Theorem 11. Codewords are represented as hexadecimal numbers.

1-identifying codes

n	|*C*|	*C*
9	114	4, E, F, 10, 1E, 24, 25, 2B, 30, 31, 36, 39, 3E, 41, 42, 46, 48, 4A, 53, 55, 57, 5E, 62, 68, 6F, 75, 7B, 7C, 83, 87, 89, 95, 98, 9C, 9D, E1, EA, ED, EF, A2, A3, AB, AC, B5, B8, BF, CA, CC, CD, D0, D7, D8, DB, F1, F2, F4, F6, 101, 103, 107, 114, 11A, 11B, 11C, 11F, 122, 128, 12D, 12F, 130, 133, 13D, 145, 148, 14E, 153, 154, 159, 15B, 161, 165, 16E, 176, 177, 178, 17B, 17C, 180, 188, 189, 192, 193, 196, 19D, 1E0, 1E3, 1E9, 1A4, 1A5, 1A6, 1AC, 1B9, 1BE, 1BA, 1C2, 1C5, 1CE, 1CF, 1D4, 1DB, 1DD, 1F1, 1F7, 1FE
10	214	0, 4, F, 12, 16, 1B, 23, 2D, 36, 38, 39, 3D, 43, 46, 53, 55, 58, 62, 65, 68, 6A, 6F, 74, 75, 7B, 80, 87, 8E, 8F, 91, 95, 99, E9, A0, A3, A5, AE, B3, B8, BA, BC, C0, C1, CA, CD, CF, D3, DE, DC, DF, F1, F6, FE, 103, 105, 108, 109, 110, 111, 116, 126, 12E, 12B, 137, 138, 13D, 144, 145, 14C, 14F, 157, 159, 15A, 15C, 165, 16A, 170, 172, 179, 17E, 183, 188, 18C, 195, 196, 19B, 19F, 1E0, 1E3, 1E4, 1E7, 1EB, 1EC, 1A0, 1A6, 1A9, 1B3, 1BA, 1BF, 1C2, 1CE, 1D5, 1DC, 1F0, 1F4, 1F9, 1FD, 201, 20A, 20B, 20C, 216, 217, 21C, 21D, 222, 223, 227, 22B, 235, 238, 246, 249, 24E, 24D, 250, 254, 256, 258, 260, 261, 26D, 271, 27E, 27B, 280, 287, 289, 29E, 29C, 2E7, 2E8, 2EA, 2A5, 2A6, 2AB, 2AD, 2B0, 2BB, 2BF, 2C3, 2C4, 2D2, 2D4, 2D5, 2DB, 2F2, 2F7, 2F8, 2FB, 2FD, 304, 305, 30E, 311, 315, 31A, 321, 324, 327, 329, 32E, 334, 33A, 33B, 342, 345, 348, 34B, 352, 35F, 361, 366, 373, 37E, 37C, 37D, 37F, 383, 384, 38A, 393, 399, 39C, 39F, 3E4, 3EB, 3EC, 3A2, 3AA, 3AD, 3B0, 3B1, 3B6, 3BC, 3C8, 3C9, 3CD, 3CF, 3D1, 3D2, 3D6, 3DA, 3F7

2-identifying codes

n	|*C*|	*C*
9	34	17, 1A, 34, 39, 45, 48, 60, 63, 6E, 84, AA, AD, B3, CF, D2, D9, FC, 102, 109, 11C, 127, 15F, 164, 171, 17A, 18E, 190, 193, 1A1, 1BF, 1C3, 1D5, 1E8, 1F6
10	62	27, 3E, 5D, 5F, 62, 70, 85, 89, 8E, 95, A8, B3, D2, E4, EB, FD, 106, 110, 138, 143, 14A, 154, 15A, 169, 171, 18B, 19D, 1A1, 1B6, 1CC, 1ff, 203, 208, 216, 219, 23B, 241, 26A, 26D, 277, 282, 297, 2AC, 2B4, 2C6, 2Cf, 2DC, 2F1, 30F, 313, 31C, 325, 33C, 360, 37E, 388, 3AA, 3B9, 3C5, 3D0, 3DB, 3E6
11	109	40, 4D, 5D, 74, 82, 8C, 99, EF, A0, B0, C6, F7, FA, 101, 108, 124, 12F, 156, 173, 17A, 181, 197, 19A, 1A3, 1BD, 1CE, 1D5, 20C, 217, 21B, 226,239, 23E, 23B, 243, 26A, 275, 28F, 2A5, 2DB, 2DC, 332, 34D, 358, 368, 37F, 390, 3E2, 3E4, 3E9, 3BE, 3C7, 3D3, 41F, 42B, 430, 438, 44A, 465, 47E, 482, 497, 4E3, 4CC, 4D1, 502, 50E, 50D, 514, 535, 54A, 557, 569, 58D, 59B, 5E4, 5B2, 5DB, 5F8, 604, 607, 611, 654, 66C, 672, 692, 69C, 6E0, 6EF, 6A9, 6AE, 6BD, 6C0, 6F8, 707, 733, 738, 741, 753, 75E, 75D, 76E, 775, 78A, 78B, 79C, 7A1, 7F6, 7F9
12	191	19, 55, 64, 80, 84, 93, EB, B1, CC, F7, FE, 106, 123, 137, 15B, 168, 176, 17E, 18B, 19C, 1ED, 1A4, 1C6, 210, 218, 225, 23E, 246, 272, 29F, 2B2, 2BC, 2C9, 2D5, 2D8, 30A, 30D, 341, 351, 367, 373, 399, 3EE, 3A8, 3AF, 3B2, 3F0, 40D, 41E, 41B, 42E, 438, 447, 452, 455, 487, 48F, 4F7, 4F9, 500, 529, 558, 561, 57E, 5E3, 5E4, 5B5, 5BA, 5D7, 5DD, 607, 620, 64A, 66F, 67B, 67C, 68C, 690, 6E1, 6AA, 6CA, 6F7, 6FC, 712, 716, 71B, 731, 74B, 75C, 76D, 791, 7A6, 7BB, 7C4, 7D2, 80E, 829, 835, 85E, 86F, 893, 898, 8E8, 8A2, 8DD, 8FE, 90E, 932, 93C, 940, 94E, 963, 98C, 991, 9EF, 9C5, 9D2, 9F5, 9F9, E23, E26, E3B, E3F, E41, E5D, E76, E8F, E94, E99, EE9, EA1, EDA, EF8, A0B, A0C, A16, A57, A69, A74, A7A, A83, AEA, AC3, AC4, ADD, B07, B10, B22, B39, B52, B96, BA5, BBF, BDF, BF5, C03, C24, C48, C62, C71, C9B, CE7, CAD, CB6, CCE, CD0, D05, D1F, D2B, D30, D44, D4D, D5F, D74, D81, D89, D8A, DB3, DB6, F08, F1C, F48, F51, F66, F8A, FE0, FEC, FAC, FBD, FD3, FFA

References

[1] U. Blass, I. Honkala, S. Litsyn, On binary codes for identification, J. Combin. Des. 8 (2) (2000) 151–156.
[2] U. Blass, I. Honkala, S. Litsyn, Bounds on identifying codes, Discrete Math. 241 (1–3) (2001) 119–128.
[3] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, Covering Codes, Elsevier, Amsterdam, 1997.

[4] P. Delsarte, P. Piret, Do most binary linear codes achieve the Goblick bound on the covering radius? IEEE Trans. Inform. Theory 32 (6) (1986) 826–828.

[5] G. Exoo, T. Laihonen, S. Ranto, Improved upper bounds on binary identifying codes, IEEE Trans. Inform. Theory 53 (11) (2007) 4255–4260.

[6] I. Honkala, T. Laihonen, On identifying codes in the hexagonal mesh, Inform. Process. Lett. 89 (1) (2004) 9–14.

[7] I. Honkala, T. Laihonen, On identifying codes in the triangular and square grids, SIAM J. Comput. 33 (2) (2004) 304–312.

[8] I. Honkala, T. Laihonen, S. Ranto, On codes identifying sets of vertices in Hamming spaces, Des. Codes Cryptogr. 24 (2) (2001) 193–204.

[9] I. Honkala, A. Lobstein, On the density of identifying codes in the square lattice, J. Combin. Theory Ser. B 85 (2) (2002) 297–306.

[10] M.G. Karpovsky, K. Chakrabarty, L.B. Levitin, On a new class of codes for identifying vertices in graphs, IEEE Trans. Inform. Theory 44 (2) (1998) 599–611.

[11] M. Laifenfeld, A. Trachtenberg, Disjoint identifying-codes for arbitrary graphs, in: Proceedings of International Symposium on Information Theory, ISIT 2005, 2005, pp. 244–248.

[12] M. Laifenfeld, A. Trachtenberg, T.Y. Berger-Wolf, Identifying codes and the set cover problem, in: Proceedings of the 44th Annual Allerton Conf. on Communication, Control and Computing, Monticello, USA, 2006.

[13] T. Laihonen, Sequences of optimal identifying codes, IEEE Trans. Inform. Theory 48 (3) (2002) 774–776.

[14] A. Lobstein, Identifying and locating-dominating codes in graphs, a bibliography, published electronically at: http://perso.enst.fr/~lobstein/debutBIBidetlocdom.pdf.

[15] S.M. Ranto, I.S. Honkala, T.K. Laihonen, Two families of optimal identifying codes in binary Hamming spaces, IEEE Trans. Inform. Theory 48 (5) (2002) 1200–1203.

[16] S. Ray, D. Starobinski, A. Trachtenberg, R. Ungrangsi, Robust location detection with sensor networks, in: Fundamental Performance Limits of Wireless Sensor Networks, IEEE J. Sel. Areas Commun. 22 (2004) (special issue).