Improved bounds on identifying codes in binary Hamming spaces

Geoffrey Exoo\textsuperscript{a}, Ville Junnila\textsuperscript{b}, Tero Laihonen\textsuperscript{c}, Sanna Ranto\textsuperscript{c}

\textsuperscript{a} Department of Mathematics and Computer Science, Indiana State University, Terre Haute, IN 47809, USA
\textsuperscript{b} Turku Centre for Computer Science TUCS, University of Turku, FI-20014 Turku, Finland
\textsuperscript{c} Department of Mathematics, University of Turku, FI-20014 Turku, Finland

\textbf{Abstract}

Let $\ell$, $n$ and $r$ be positive integers. Define $\mathbb{F}^n = \{0, 1\}^n$. The Hamming distance between words $x$ and $y$ of $\mathbb{F}^n$ is denoted by $d(x, y)$. The ball of radius $r$ is defined as $B_r(X) = \{y \in \mathbb{F}^n \mid \exists x \in X : d(x, y) \leq r\}$, where $X$ is a subset of $\mathbb{F}^n$. A code $C \subseteq \mathbb{F}^n$ is called $(r, \leq \ell)$-identifying if for all $X, Y \subseteq \mathbb{F}^n$ such that $|X| \leq \ell$, $|Y| \leq \ell$ and $X \neq Y$, the sets $B_r(X) \cap C$ and $B_r(Y) \cap C$ are different.

The concept of identifying codes was introduced by Karpovsky, Chakrabarty and Levitin in 1998.

In this paper, we present various results concerning $(r, \leq \ell)$-identifying codes in the Hamming space $\mathbb{F}^n$. First we concentrate on improving the lower bounds on $(r, \leq 1)$-identifying codes for $r > 1$. Then we proceed by introducing new lower bounds on $(r, \leq \ell)$-identifying codes with $\ell \geq 2$. We also prove that $(r, \leq \ell)$-identifying codes can be constructed from known ones using a suitable direct sum when $\ell \geq 2$. Constructions for $(r, \leq 2)$-identifying codes with the best known cardinalities are also given.

\textcopyright{} 2009 Elsevier Ltd. All rights reserved.

1. Introduction

The binary Hamming space $\mathbb{F}^n$ is the $n$-fold Cartesian product of the binary field $\mathbb{F} = \{0, 1\}$. A non-empty subset of $\mathbb{F}^n$ is called a code (of length $n$). The Hamming distance $d(x, y)$ between words $x, y \in \mathbb{F}^n$ is the number of coordinate places in which they differ. We say that $x$ $r$-covers $y$ if $d(x, y) \leq r$. The set of non-zero coordinates of a word $x \in \mathbb{F}^n$ is called the support of $x$ and is denoted by $\text{supp}(x)$. The
weight of \( x \) is the cardinality of the support of \( x \) and is denoted by \( w(x) \). For \( x \in \mathbb{F}^n \) we denote

\[
B_r(x) = \{ y \in \mathbb{F}^n \mid d(x, y) \leq r \}, \\
S_r(x) = \{ y \in \mathbb{F}^n \mid d(x, y) = r \}.
\]

The set \( B_r(x) \) is called the Hamming ball of radius \( r \) centred at \( x \). The size of \( B_r(x) \) does not depend on the choice of the word \( x \). Hence, we can denote the number of words in \( B_r(x) \) by

\[
V(n, r) = \sum_{i=0}^{r} \binom{n}{i}.
\]

For \( X \subseteq \mathbb{F}^n \), we denote

\[
B_r(X) = \bigcup_{x \in X} B_r(x).
\]

Let \( C \) be a code of length \( n \) and \( X \subseteq \mathbb{F}^n \). The \( I \)-set of a set \( X \) with respect to the code \( C \) is

\[
I_r(C; X) = I_r(X) = B_r(X) \cap C.
\]

The symmetric difference \((A \setminus B) \cup (B \setminus A)\) of sets \( A \) and \( B \) is denoted by \( A \triangle B \).

**Definition 1.1.** Let \( r \) and \( \ell \) be positive 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 \( \ell = 1 \), then we simply say that \( C \) is \( r \)-identifying.

In other words, a code \( C \subseteq \mathbb{F}^n \) is \((r, \leq \ell)-identifying\) if and only if

\[
I_r(C; X) \triangle I_r(C; Y) \neq \emptyset
\]

for all \( X, Y \subseteq \mathbb{F}^n \) satisfying \( |X| \leq \ell, |Y| \leq \ell \) and \( X \neq Y \). Notice that the definition requires that \( I_r(C; X) \) is non-empty for all non-empty subsets \( X \) of \( \mathbb{F}^n \).

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 exits for these parameters). If \( \ell = 1 \), then we denote the smallest cardinality by \( M_r(n) \). A code attaining the smallest cardinality is called optimal.

Identifying codes were first introduced by Karpovsky, Chakrabarty and Levitin in [14]. Their motivation for identification comes from multiprocessor systems. The problem is to find malfunctioning processors in multiprocessor systems. In other words, the set of malfunctioning processors \( X \) of size at most \( \ell \) is required to be identified when the only available information is the \( I \)-set \( I_r(C; X) \). This \( I \)-set is provided by the processors in the code \( C \) monitoring processors within distance \( r \) and reporting if some are malfunctioning. The theory of identification can also be applied to sensor networks as is discussed in [20]. A natural goal in both cases is to find as small identifying codes as possible (see [15] also for energy conservation in sensor networks).

Since the seminal paper [14], which was published in 1998, the field of identifying codes has been actively studied and forms now a topic of its own — for various papers dealing with identification and closely related topics, see [1], [4,5], [9–11,13], [18,20,21] and for more the web-site [17].

The organization of the paper is as follows. In Section 2 we consider lower bounds for \( r \)-identifying codes using a new approach — for the tables of the best known upper bounds we refer to [4]. Then we proceed in Section 3 by improving lower bounds for \((r, \leq \ell)-identifying\) codes. Finally, in Section 4 we construct some \((r, \leq \ell)-identifying\) codes with the best known cardinalities.
2. Lower bounds for \( r \)-identifying codes

In what follows, we are going to improve the known lower bounds on \( r \)-identifying codes. The main underlying idea in the earlier results presented in [3] and [8] was to find as small values as possible for \( m = \max \{|I_r(x)| : x \in F^n\} \) using partial constructions (besides these results, there is also a bound by Karpovsky et al. [14]; see Theorem 2.5). In this section, we approach the problem in a different manner. Namely, we improve, when \( r > 1 \), the lower bound by concentrating on the function \( P_r(n, i) \) defined below instead of the value \( m \).

Let \( x \in F^n \) and define

\[
P_r(n, i, x) = \max_{C \subseteq F^n} |\{y \in F^n : C \text{ is } r \text{-identifying code satisfying } |I_r(C; x)| = i\}|
\]

In other words, \( P_r(n, i, x) \) denotes the maximum number of words \( y \) such that \( I_r(C; y) \subseteq I_r(C; x) \) and \( |I_r(C; y)| = 2 \), where \( C \) is an \( r \)-identifying code satisfying \( |I_r(C; x)| = i \). Clearly, \( P_r(n, i, \emptyset) = P_r(n, i, x) \) for every \( x \in F^n \) because all the words in \( F^n \) play the same role. Therefore, denote \( P_r(n, i, \emptyset) = P_r(n, i) \).

The definition of \( P_r(n, i) \) may seem somewhat complicated. However, it arises naturally from the proof of the following theorem (see the inequality (1)). We will examine the function more closely after Theorem 2.1.

\textbf{Theorem 2.1.} Let \( C \subseteq F^n \) be an \( r \)-identifying code. Define

\[
a = \min_{i = 3, \ldots, V(n, r)} \left\{ 2 + \frac{(i - 2)(\frac{2r}{r} - 1)}{\left(\frac{2r}{r}\right) + P_r(n, i) - 1} \right\}
\]

Then we have

\[
|C| \geq M_r(n) \geq \frac{a \cdot 2^n}{V(n, r) + a - 1}.
\]

\textbf{Proof.} Denote by \( V_i \) the words which are \( r \)-covered by exactly \( i \) codewords. Let \( x \in F^n \) be a word \( r \)-covered by exactly two codewords (if any such words \( x \) exist). By Theorem 2.4.8 in [6] we know that there are at least \( \left(\frac{2r}{r}\right) \) words in \( F^n \) covering both of these codewords (and one of them is \( x \)).

Therefore, for each word which is \( r \)-covered by exactly two codewords there are at least \( \left(\frac{2r}{r}\right) - 1 \) words which are \( r \)-covered by at least three codewords, since the code \( C \) is \( r \)-identifying. On the other hand, if \( y \in F^n \) is \( r \)-covered by \( i \geq 3 \) codewords, then there are at most \( P_r(n, i) \) words \( z \in F^n \) such that \( I_r(z) \subseteq I_r(y) \) and \( |I_r(z)| = 2 \). Hence, by counting in two ways the number of pairs \( \{x, y\} \) such that \( x \in V_2, y \in V_i (i \geq 3) \) and \( I_r(x) \subseteq I_r(y) \), we have

\[
\left(\frac{2r}{r}\right) - 1|V_2| \leq \sum_{i = 3}^{V(n, r)} P_r(n, i)|V_i|.
\]

Notice also that there are clearly at most \( K = |C| \) words \( r \)-covered by a single codeword, i.e., \( |V_1| \leq K \).

Now, by counting in two ways the number of pairs \( \{x, c\} \), where \( x \in F^n \) and \( c \in C \) is \( r \)-covered by \( x \), and by using the inequality (1), we have

\[
K \cdot V(n, r) = \sum_{i = 1}^{V(n, r)} i|V_i| = a \cdot 2^n - (a - 1)|V_1| - (a - 2)|V_2| + \sum_{i = 3}^{V(n, r)} (i - a)|V_i|.
\]
Theorem 2.2. Clearly, for any \( r \)-identifying code, we immediately have that \( P_r(n, i) \leq \binom{i}{2} \). This estimate provides useful upper bound for small \( i \). On the other hand it is also clear that \( P_r(n, i) \leq V(n, 2r) \), since only words in \( B_{2r}(0) \) are able to \( r \)-cover codewords in \( B_r(0) \). (Actually, we can further say that \( P_r(n, i) \leq V(n, 2r) - 1 \), since the word \( 0 \) is always \( r \)-covered by \( i \geq 3 \) codewords.) This upper bound works better with bigger \( i \). Together these two estimates imply that

\[
P_r(n, i) \leq \min \left\{ \binom{i}{2}, V(n, 2r) \right\}.
\]

In what follows, we present two ways to improve the bound \( V(n, 2r) \) for \( P_r(n, i) \). The first approach, which is based on Theorem 2.2, concentrates on bounding the number of words of weight \( 2r - 1 \) and \( 2r \) that contribute to the value \( P_r(n, i) \). For the second method, assume that \( w \) is an integer such that \( r \leq w \leq 2r \). Theorem 2.4 provides us then an upper bound for the number of words in \( B_{w}(0) \) that are \( r \)-covered by at most two codewords in \( B_r(0) \) when there are exactly \( i \) codewords in \( B_r(0) \). These two approaches will then be combined (as is presented later).

In the following, we define two auxiliary functions, namely \( F_r(n, w) \) and \( f_r(n, w) \). The relation between these functions and the considered function \( P_r(n, i) \) is examined after Theorem 2.2. Let now \( C \subseteq \mathbb{F}^n \) be an \( r \)-identifying code and \( w \) an integer such that \( 2r - 1 \leq w \leq 2r \). Then define

\[
F_r(n, w) = F_r(C; n, w) = \{a \in S_w(0) \subseteq \mathbb{F}^n \mid I_r(a) \subseteq I_r(0), |I_r(a)| = 2\}.
\]

Define also

\[
f_r(n, w) = \max_{D \subseteq B_r(0)} |\{I_r(D; x) \mid x \in S_w(0) \subseteq \mathbb{F}^n, I_r(D; x) \subseteq I_r(0), |I_r(D; x)| = 2\}|.
\]

Clearly, for any \( r \)-identifying code \( C \subseteq \mathbb{F}^n \) we have \( |F_r(n, w)| \leq f_r(n, w) \). (Notice also that the value \( f_r(n, w) \) remains unchanged if the word \( 0 \) is replaced by an arbitrary word \( y \in \mathbb{F}^n \).)

**Theorem 2.2.** Let \( C \subseteq \mathbb{F}^n \) be an \( r \)-identifying code. If \( k \) and \( w \) are integers such that \( 2r - 1 \leq w \leq 2r \), then

\[
|F_r(n, w)| \leq \frac{f_r(k, w)}{\binom{k}{w}} \binom{n}{w}.
\]

**Proof.** Let \( y \in \mathbb{F}^n \) be a word of weight \( k \). Define

\[
H(y) = \{x \in \mathbb{F}^n \mid \text{supp}(x) \subseteq \text{supp}(y)\}.
\]

Let us now consider pairs \( \{y, x\} \), where \( y \) is a word of weight \( k \) and \( x \in H(y) \cap F_r(n, w) \). Since \( 2r - 1 \leq w \leq 2r \), each word in \( B_r(0) \) that is \( r \)-covered by a word in \( S_w(0) \cap H(y) \) belongs to \( H(y) \). Therefore, for each word \( y \) of weight \( k \), there exists at most \( f_r(k, w) \) different words in \( H(y) \cap F_r(n, w) \). Thus, by counting in two ways the number of pairs \( \{y, x\} \), we have

\[
\binom{n - w}{k - w} |F_r(n, w)| \leq \binom{n}{k} f_r(k, w).
\]
Furthermore, we have

\[ |F_r(n, w)| \leq f_r(k, w) \left( \binom{n}{k} \right) \left( \binom{n-w}{k-w} \right) = f_r(k, w) \left( \binom{n}{k} \right) \left( \binom{n-w}{k-w} \right) \]

\[ = f_r(k, w) \left( \binom{n}{w} \binom{n-w}{k-w} \right) = f_r(k, w) \left( \binom{n}{w} \right) \left( \binom{k}{w} \right). \quad \square \]

**Theorem 2.2** tells us that the ratio of \(|F_r(n, w)|\) to \(|S_w(\emptyset)| = \binom{n}{w}\) is always at most \(f_r(k, w)/\binom{k}{w}\) when \(n \geq k\) and \(2r - 1 \leq w \leq 2r\). Therefore, the value \(f_r(k, w)\) for small \(k(n)\), provides us an upper bound for the number of words in \(F_r(n, w)\). Furthermore, the number of words of weight \(w\) that contribute to the value \(P_r(n, i)\) is at most

\[ \max_{C \subseteq \mathbb{F}_2^n} |\{F_r(C; n, w) \mid C \text{ is } r\text{-identifying}\}| \]

and, therefore, is bounded from above by \((f_r(k, w)/\binom{k}{w}) \left( \binom{n}{w} \right)\). Thus, if we know the values \(f_r(k_1, 2r - 1)\) and \(f_r(k_2, 2r)\) with \(k_1\) and \(k_2\) being positive integers, then we have for \(n \geq \max\{k_1, k_2\}\) that

\[ P_r(n, i) \leq \sum_{j=0}^{2r-2} \binom{n}{j} + f_r(k_1, 2r - 1) \left( \binom{n}{2r-1} \right) + f_r(k_2, 2r) \left( \binom{n}{2r} \right). \quad (4) \]

The following theorem provides us an easy upper bound for \(f_r(2r + 1, 2r)\).

**Theorem 2.3.** We have

\[ f_r(2r + 1, 2r) \leq 2r. \]

**Proof.** Assume to the contrary that \(f_r(2r + 1, 2r) \geq 2r + 1\), i.e. \(f_r(2r + 1, 2r) = 2r + 1\) since \(f_r(2r + 1, 2r) \leq \left( \frac{2r+1}{2r} \right) = 2r + 1\). Let \(D \subseteq B_r(\emptyset)\) be a set such that it attains this value. Now there exist at least three codewords in \(S_r(\emptyset)\) (or we are done). Therefore, there exist two codewords \(c_1, c_2 \in S_r(\emptyset)\) such that \(\text{supp}(c_1) \cap \text{supp}(c_2)\) is non-empty, i.e. \(|\text{supp}(c_1) \cup \text{supp}(c_2)| < 2r\). Hence, there exist words \(x_1, x_2 \in S_{2r}(\emptyset)\) such that \(\{c_1, c_2\}\) is included in \(I_r(D; x_1)\) and \(I_r(D; x_2)\). This is a contradiction, since we assumed that each word in \(S_{2r}(\emptyset)\) is \(r\)-covered by a different set of codewords of size two. \(\square\)

It should be remarked that the upper bound for \(f_r(2r + 1, 2r)\) in the previous theorem can be attained. For example when \(r = 2\), it is easy to see that the set \(D = \{00101, 00110, 01001, 01010\}\) attains the value \(f_r(5, 4) = \left( \frac{5}{2} \right) - 1 = 4\).

Notice that (when \(n\) grows) most of the words in \(B_{2r}(\emptyset)\) belong to \(S_{2r}(\emptyset)\). Hence, it is natural to concentrate on the values \(f_r(n, 2r)\) needed in applying **Theorem 2.2**. The following values provide us significant improvements over **Theorem 2.3**:

\[ f_2(9, 4) = 60, \quad f_3(9, 6) = 42 \quad \text{and} \quad f_4(10, 8) = 24. \quad (5) \]

These values were obtained by extensive computations using computers. The method uses our notion of a canonical form for a set of codewords, also used in [8], which we now describe.

A set \(S\) of \(k\) codewords of length \(n\) is isomorphic to any set obtained from \(S\) by applying some permutation to the bit positions (coordinates) of all codewords. \(S\) is also isomorphic to any set obtained from \(S\) by translating each codeword in \(S\) by a fixed word. One obtains our canonical representation for \(S\) of codewords by considering each of the \((\text{up to}) \, !n!2^n\) isomorphic representations of \(S\) so obtained, listing the codewords of each in increasing order (the codewords can be viewed as \(n\)-bit binary numbers), and taking the representation that is lexicographically least.
For small sets of codewords, we were able to evaluate \( f \) by counting the number of \( I \)-sets of size two in each canonical form. For larger sets, there are two phases. For code sizes not too much larger (perhaps up to 10 or 12 more codewords, depending on \( n \)) than the size of the canonical forms, one can do a simple exhaustive search using some straightforward tree pruning. It is for such code sizes that the maximum number of \( I \)-sets of size two is reached. For example, in establishing \( f_2(9, 4) = 60 \), we found it feasible to generate all canonical forms of size 11, and found that the maximum occurs for sets of codewords of size 16.

The time-consuming cases occur when the size of the code is much larger than the size of the canonical forms. It turns out that in these cases the maximum number of \( I \)-sets of size two that can be obtained is much smaller than the maximum. Intuitively, the codewords are too densely packed in the Hamming space for there to be a large number of \( I \)-sets of size two. Again referring to the example of \( f_2(9, 4) = 60 \), we found that for sets of codewords of size 26 and larger, the maximum number of \( I \)-sets of size two was only 15. Since we were only interested in whether the maximum value of 60 could be improved, significant tree pruning could be done. However, searching through all possibilities is still extremely time consuming. To assist in the search, we create a list of all pairs of codewords that might possibly be \( I \)-sets of size two, as words are added to the code in the search process, certain of these pairs are eliminated as candidates. When there are not enough candidates left to improve on our previous best, we can prune the search. Some refinements of this process were used for the case of \( f_4(10, 8) \).

Using the values in (5), we are able to significantly decrease the last term in the equation (4). When \( r = 2 \), it is also straightforward to check that \( f_2(5, 3) \leq 9 \). Thus, when \( r = 2 \) and \( n \geq 9 \), we have by the equation (4) that \((k_1 = 5, k_2 = 9)\)

\[
P_2(n, i) \leq \min \left\{ \binom{i}{2}, \frac{2}{9} \sum_{j=0}^{2} \binom{n}{j} + \frac{9}{10} \binom{n}{3} + \frac{60}{126} \binom{n}{4} \right\}.
\]

Actually, this inequality together with Theorem 2.1 provides the best known lower bounds for \( M_\nu(n) \) when \( r = 2 \) and \( n \geq 9 \).

The consideration above provided an efficient way to estimate the number of words of weight \( 2r - 1 \) and \( 2r \) contributing to the value \( P_r(n, i) \). The following theorem, on the other hand, gives us an upper bound for the number of words in \( B_w(0) \) (\( r \leq w \leq 2r \)) that are \( r \)-covered by at most two codewords in \( B_r(0) \) when there are exactly \( i \) codewords in \( B_r(0) \).

**Theorem 2.4.** Let \( w \) be an integer such that \( r \leq w \leq 2r \) and \( i \) be the number of codewords in the ball \( B_r(0) \). Define

\[
f_{r, b}(n, i) = \min \left\{ \sum_{k=b}^{r} \sum_{j=0}^{\lfloor \frac{k-b}{2} \rfloor} (r+b) \binom{n-r-b}{j}, i \right\}
\]

and

\[
D_{n, r, w}(i_1, \ldots, i_r) = V(n, w) - \sum_{b=1}^{w-r} \left( \sum_{k=b}^{r} \binom{i_k}{k} \sum_{j=0}^{\lfloor \frac{(k-b)/2} \rfloor} \binom{k-n-k}{n-k} \binom{n-k}{r+b-k+j} \right) - 2 \frac{r}{r+b} \binom{n}{r+b} + \sum_{b=1}^{w-r} \frac{2}{r+b} \binom{n}{r+b} - 2.
\]

Then the number of words in \( B_w(0) \) that are \( r \)-covered by at most two codewords in \( B_r(0) \) is at most

\[
\max\{D_{n, r, w}(i_1, \ldots, i_r) \mid i_1 + \cdots + i_r = i \text{ and } 0 \leq i_j \leq \binom{n}{j} \text{ for } 1 \leq j \leq r \}.
\]

**Proof.** Let \( C \subseteq \mathbb{F}^n \) be an \( r \)-identifying code. Let \( k \) and \( b \) be integers such that \( 1 \leq k \leq r \) and \( 1 \leq b \leq k \). Let us then count the number of words of weight \( r + b \) that a word of weight \( k \) \( r \)-covers. If a word
\( \mathbf{x} \in \mathbb{F}_n \) of weight \( k \) \( r \)-covers a word \( \mathbf{y} \in \mathbb{F}_n \) of weight \( r + b \), then there are at most \( \left\lfloor \frac{k-b}{2} \right\rfloor \) positions such that the bits in \( \mathbf{x} \) and \( \mathbf{y} \) in the corresponding positions are 1 and 0, respectively. Thus, each word of weight \( k \) now \( r \)-covers

\[
\sum_{j=0}^{\left\lfloor \frac{k-b}{2} \right\rfloor} \binom{k}{j} \binom{n-k}{r+b-k+j}
\]

words of weight \( r + b \). In a similar way, it can be showed that each word of weight \( r + b \) \( r \)-covers

\[
\sum_{j=0}^{\left\lfloor \frac{k-b}{2} \right\rfloor} \binom{r+b}{k-j} \binom{n-r-b}{j}
\]

words of weight \( k \). Therefore, each word of weight \( r + b \) \( r \)-covers

\[f_{r,b}(n) = \sum_{k=b}^{r} \sum_{j=0}^{\left\lfloor \frac{k-b}{2} \right\rfloor} \binom{r+b}{k-j} \binom{n-r-b}{j}\]

words in \( B_r(0) \).

Define

\[T_r(j, w) = |\{ \mathbf{x} \in S_w(0) \mid I_r(\mathbf{x}) \subseteq I_r(0), |I_r(\mathbf{x})| = j \}|,\]

and denote

\[i_k = |I_r(0) \cap S_k(0)|, \quad \text{where} \ 1 \leq k \leq r.\]

Notice that \( i = i_1 + \cdots + i_r \). Now denote \( f_{r,b}(n, i) = \min\{f_{r,b}(n, i)\} \). Notice that the value \( f_{r,b}(n, i) \) now tells us the maximum number of codewords in \( B_r(0) \) that each word of weight \( r + b \) \( r \)-covers. (Actually, here the integer \( i \) could be replaced by the sum \( i_b + \cdots + i_r \), but it would complicate the analysis of the function \( D_{n,r,w}(i_1, \ldots, i_r) \) and did not provide any improvements in the numerical cases we considered.)

By counting in two ways the number of pairs \( \{\mathbf{x}, \mathbf{c}\} \) with \( \mathbf{x} \in S_{r+b}(0) \) and \( \mathbf{c} \in I_r(\mathbf{x}) \cap B_r(0) \), we have

\[
\sum_{k=b}^{r} \left( \sum_{j=0}^{\left\lfloor \frac{k-b}{2} \right\rfloor} \binom{k}{j} \binom{n-k}{r+b-k+j} \right) = \sum_{j=0}^{r} jT_r(j, r+b)
\]

\[
\leq 2 \sum_{j=0}^{r} T_r(j, r+b) + \sum_{j=3}^{r} f_{r,b}(n, i) T_r(j, r+b) + \sum_{j=3}^{r} f_{r,b}(n, i) T_r(j, r+b)
\]

\[
= 2 \left( \binom{n}{r+b} - \sum_{j=3}^{r} T_r(j, r+b) \right) + \sum_{j=3}^{r} f_{r,b}(n, i) T_r(j, r+b)
\]

Consequently, we have

\[
\sum_{j=3}^{r} T_r(j, r+b) = \frac{r \left( \sum_{k=b}^{r} \left( \sum_{j=0}^{\left\lfloor \frac{k-b}{2} \right\rfloor} \binom{k}{j} \binom{n-k}{r+b-k+j} \right) \right) - 2 \binom{n}{r+b}}{f_{r,b}(n, i) - 2}.
\]
Now we have
\[
V(n, 2r) - \sum_{b=1}^{w-r} \sum_{j=3}^{n} T_r(j, r + b) 
\leq V(n, 2r) - \sum_{b=1}^{w-r} \left( \sum_{k=b}^{r} \left( \sum_{j=0}^{(k-b)/2} \binom{k}{j} \binom{n-k}{r+b-k-j} - 2 \binom{n}{r+b} \right) \right) 
\leq D_{n,r,w}(i_1, \ldots, i_r).
\]

For given \(i_1, \ldots, i_r\) the above inequality provides us an upper bound for the number of words in \(B_w(\emptyset)\) which are \(r\)-covered by at most two codewords. Hence, when we maximize the function \(D_{n,r}(i_1, \ldots, i_r)\) over all different choices of \(i_1, \ldots, i_r\) such that \(i_1 + \cdots + i_r = i\) and \(i_j \leq \binom{n}{j}\), the claim immediately follows.

In applying Theorem 2.4, we have to be able to solve the following optimization problem for fixed \(i (3 \leq i \leq V(n, r))\):
\[
\max\{D_{n,r,w}(i_1, \ldots, i_r) \mid i_1 + \cdots + i_r = i \text{ and } i_j \leq \binom{n}{j} \text{ for } j = 1, \ldots, r\}.
\]

Indeed, this problem can be solved quite easily as follows:

1. Calculate the coefficients of \(i_k\) in \(D_{n,r,w}(i_1, \ldots, i_r)\). (Notice that the sum \(i_1 + \cdots + i_r\) is equal to the fixed constant \(i\).)
2. Sort \(i_k\) in decreasing order regarding the coefficients of \(i_k\). Let the sorted list be \(i_{j_1}, \ldots, i_{j_s}\).
3. Let \(s\) be the largest integer such that
\[
\sum_{k=1}^{s-1} \binom{n}{j_k} \leq i.
\]

Now the function \(D_{n,r,w}(i_1, \ldots, i_r)\) is maximized by choosing \(i_{j_k} = \min\{i - \sum_{k=1}^{s-1} \binom{n}{j_k} \leq \binom{n}{j_k}\}\),
\(i_k = \binom{n}{i_{j_k}}\) for \(k = 1, \ldots, s - 1\) and \(i_{j_{s+1}} = \cdots = i_r = 0\).

We have now presented two ways (Theorems 2.2 and 2.4) to improve the upper bound (3) for \(P_r(n, i)\). When \(r = 2\), the best known lower bounds are obtained by using only Theorem 2.2 (see the equation (6)). However, when \(r > 2\), to obtain the best known lower bounds we need to combine the two methods explained above. For example when \(r = 3\), we obtain the following inequality by combining Theorems 2.2 and 2.4:
\[
P_3(n, i) \leq \min \left\{ \binom{i}{2}, \frac{1}{\binom{n}{i}}, \frac{1}{\binom{n}{i_1 + \cdots + i_r}} = D_{n,3,5}(i_1, \ldots, i_r) + \frac{42}{84} \binom{n}{6} \right\},
\] where \(0 \leq i_j \leq \binom{n}{j} \text{ for all } j = 1, \ldots, r\). This inequality improves the known lower bounds, when \(n \geq 19\).

When \(r = 4\) and \(r = 5\), the known lower bounds are improved in a similar way to the inequality (7), i.e., we use Theorem 2.2 to estimate the number of words of weight \(2r\) contributing to the value \(P_r(n, i)\) and Theorem 2.4 for smaller weights. This method improves the known lower bounds for \(r = 4\) when \(n \geq 28\) and for \(r = 5\) when \(n \geq 37\). (Notice that when \(r = 4\) we have the value \(f_4(10, 8) = 24\) obtained by computers and when \(r = 5\) we have the estimate \(f_5(11, 10) \leq 10\) by Theorem 2.3.) In particular, we have \(M_5(37) \geq 542868\) (the best previously known bound is 539088).

As we have seen, Theorem 2.1 improves lower bounds when \(r \geq 2\) and \(n\) is large enough. With small \(n\) the best known lower bounds are provided by the third part of Theorem 1 in [14] (by Karpovsky
et al.). For completeness and to cover efficiently also the case \( r \geq \frac{n}{2} \) (see [2]) this result is rephrased in the following theorem.

**Theorem 2.5.** Let \( C \subseteq \mathbb{F}^n \) be an \( r \)-identifying code. Then we have

\[
|C| \cdot V(n, r) \geq \sum_{i=1}^{s} i \left( \frac{|C|}{i} \right) + (s + 1) \left( 2^n - \sum_{i=0}^{s} \left( \frac{|C|}{i} \right) \right)
\]

where \( s \) is the largest integer such that

\[
\sum_{i=0}^{s} \left( \frac{|C|}{i} \right) \leq 2^n.
\]

If \( n/2 \leq r \leq n - 1 \), then instead of equation (8) we use

\[
|C| \cdot V(n, n - r - 1) \geq \sum_{i=1}^{s} i \left( \frac{|C|}{i} \right) + (s + 1) \left( 2^n - \sum_{i=0}^{s} \left( \frac{|C|}{i} \right) \right)
\]

where \( s \) is the largest integer such that

\[
\sum_{i=0}^{s} \left( \frac{|C|}{i} \right) \leq 2^n.
\]

**Proof.** Denote again by \( V_i \) the words which are \( r \)-covered by exactly \( i \) codewords. Let \( C \subseteq \mathbb{F}^n \) be an \( r \)-identifying code. Counting the number of pairs \( \{x, c\} \) where \( x \in \mathbb{F}^n \), \( c \in C \) and \( d(x, c) \leq r \), we get

\[
|C| \cdot V(n, r) = \sum_{i=0}^{V(n,r)} i |V_i|.
\]

Clearly, \( |V_0| = 0 \). To bound from below the right-hand side of the equation, we make for small \( i = 1, 2, \ldots \) the cardinalities \( |V_i| \) as large as possible. Trivially, \( |V_i| \leq \left( \frac{|C|}{i} \right) \). But up to which \( i \) can we do this? Clearly, up to \( s \) defined in (9). The rest of the words (i.e., in \( V_i \) where \( i \geq s + 1 \)) are covered by at least \( s + 1 \) times. This yields (8).

Suppose then \( n/2 \leq r \leq n - 1 \). By [2], we know that an \( r \)-identifying code has the property that also the sets \( I_{n-r-1}(x) \) are different, but (exactly) one can be empty. Hence, for the radius \( n - r - 1 \), we can count exactly as above, but now \( |V_0| \leq 1 \) and we have to use \( s \) as defined in (11).

The previous theorem tells us when it is possible to have an \( r \)-identifying code of given size. It can be used to compute a lower bound for an \( r \)-identifying code in the following way: we start our computation from a known lower bound and then increase the size of the code until the equation (8) is satisfied.

In particular, Theorem 2.5 gives us that \( M_3(5) \geq 9 \). On the other hand, we know by [12] that \( M_3(5) \leq 10 \). The following theorem shows that, indeed, \( M_3(5) = 10 \).

**Theorem 2.6.** \( M_3(5) = 10 \).

**Proof.** By the considerations above, we know that \( 9 \leq M_3(5) \leq 10 \). Assume then to the contrary that there exists a 3-identifying code \( C \subseteq \mathbb{F}^5 \) of size 9. By [2], the code \( C \) has the property that also the sets \( I_1(C; x) \) are different for all \( x \in \mathbb{F}^5 \) (although one of these sets can be empty). As before, let \( V_i \) denote the set of words which are 1-covered by exactly \( i \) codewords of \( C \).

If \( |V_j| \geq 1 \) for some \( j = 4, \ldots, V(5, 1) \), then as in (10) we get

\[
54 = |C| \cdot V(5, 1) \geq 1 \cdot 0 + 9 \cdot 1 + 21 \cdot 2 + 1 \cdot 4 = 55,
\]

which is a contradiction. Hence, \( |V_j| = 0 \) for every \( j = 4, \ldots, V(5, 1) \).
Table 1
Lower bounds (the best previously known bounds in the parentheses) on the cardinalities of \( r \)-identifying codes for \( r = 2 \) and \( r = 3 \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( M_2(n) )</th>
<th>( M_3(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>(^a) 7</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>(^a) 6</td>
<td>(^f) 15</td>
</tr>
<tr>
<td>5</td>
<td>(^a) 6</td>
<td>(^d) 10</td>
</tr>
<tr>
<td>6</td>
<td>(^a) 8</td>
<td>(^a) 7</td>
</tr>
<tr>
<td>7</td>
<td>(^a) 14</td>
<td>(^a) 8</td>
</tr>
<tr>
<td>8</td>
<td>(^a) 17</td>
<td>(^a) 10</td>
</tr>
<tr>
<td>9</td>
<td>(^b) 27 ((^i) 26)</td>
<td>(^a) 13</td>
</tr>
<tr>
<td>10</td>
<td>(^b) 43 ((^i) 41)</td>
<td>(^a) 18</td>
</tr>
<tr>
<td>11</td>
<td>(^b) 71 ((^i) 67)</td>
<td>(^a) 25</td>
</tr>
<tr>
<td>12</td>
<td>(^b) 118 ((^i) 112)</td>
<td>(^a) 39</td>
</tr>
<tr>
<td>13</td>
<td>(^b) 199 ((^i) 190)</td>
<td>(^a) 61</td>
</tr>
<tr>
<td>14</td>
<td>(^b) 341 ((^i) 326)</td>
<td>(^a) 95</td>
</tr>
<tr>
<td>15</td>
<td>(^b) 590 ((^i) 567)</td>
<td>(^a) 151</td>
</tr>
<tr>
<td>16</td>
<td>(^b) 1033 ((^i) 995)</td>
<td>(^a) 241</td>
</tr>
<tr>
<td>17</td>
<td>(^b) 1824 ((^i) 1761)</td>
<td>(^a) 383</td>
</tr>
<tr>
<td>18</td>
<td>(^b) 3244 ((^i) 3141)</td>
<td>(^a) 608</td>
</tr>
<tr>
<td>19</td>
<td>(^b) 5809 ((^i) 5638)</td>
<td>(^b) 974 ((^i) 959)</td>
</tr>
<tr>
<td>20</td>
<td>(^b) 10465 ((^i) 10179)</td>
<td>(^b) 1656 ((^i) 1593)</td>
</tr>
<tr>
<td>21</td>
<td>(^b) 18949 ((^i) 18471)</td>
<td>(^b) 2839 ((^i) 2722)</td>
</tr>
<tr>
<td>22</td>
<td>(^b) 34467 ((^i) 33674)</td>
<td>(^b) 4909 ((^i) 4731)</td>
</tr>
<tr>
<td>23</td>
<td>(^b) 63029 ((^i) 61647)</td>
<td>(^b) 8549 ((^i) 8276)</td>
</tr>
<tr>
<td>24</td>
<td>(^b) 115664 ((^i) 113288)</td>
<td>(^b) 14985 ((^i) 14562)</td>
</tr>
<tr>
<td>25</td>
<td>(^b) 213004 ((^i) 208921)</td>
<td>(^b) 26420 ((^i) 25899)</td>
</tr>
<tr>
<td>26</td>
<td>(^b) 393602 ((^i) 386520)</td>
<td>(^b) 46833 ((^i) 45784)</td>
</tr>
<tr>
<td>27</td>
<td>(^b) 729602 ((^i) 717218)</td>
<td>(^b) 83425 ((^i) 81749)</td>
</tr>
<tr>
<td>28</td>
<td>(^b) 1356002 ((^i) 1334510)</td>
<td>(^b) 149271 ((^i) 146575)</td>
</tr>
<tr>
<td>29</td>
<td>(^b) 2526996 ((^i) 2489423)</td>
<td>(^b) 268200 ((^i) 263829)</td>
</tr>
<tr>
<td>30</td>
<td>(^b) 4721086 ((^i) 4654848)</td>
<td>(^b) 483728 ((^i) 478179)</td>
</tr>
</tbody>
</table>

\(^a\) Theorem 2.5 by Karpovsky et al. [14].
\(^b\) Theorem 2.1.
\(^c\) Theorem 2 in [8].
\(^d\) Theorem 2.6.
\(^e\) By computer search in [7].
\(^f\) Blass et al. in [2].

Assume now that \( |V_3| \leq 1 \). Then, as in the proof of Theorem 2.1, we have

\[
|V_2| \leq \sum_{i=3}^{\sigma(5,1)} p_i(5, i) |V_i| \leq p_1(5, 3) \leq \left( \frac{3}{2} \right) = 3.
\]

Since \( |V_3| \leq 1 \), the number of words in \( V_2 \) is at least 21. This observation together with the previous inequality leads to a contradiction. Therefore, \( |V_3| \geq 2 \). However, this implies that

\[ 54 = |C| \cdot V(5, 1) \geq 1 \cdot 0 + 9 \cdot 1 + 20 \cdot 1 + 2 \cdot 3 \geq 55, \]

which is a contradiction. Thus, there does not exist a 3-identifying code of length 5 with 9 codewords. Therefore, \( M_3(5) = 10 \). \( \Box \)

In Table 1 we have listed the best known lower bounds for \( r = 2, 3 \) and \( 2 \leq n \leq 30 \). For the best known lower bounds, we refer to [4].

3. Lower bounds for \((r, \leq \ell)\)-identifying codes

Let \( r \) and \( \ell \) be integers such that \( r \geq 2 \) and \( \ell \geq 2 \). In this section, we show that it is beneficial to concentrate on the sets \( S_r(x) \cap C \) instead of the usual \( I \)-sets \( B_r(x) \cap C \), when we are bounding the cardinality of \((r, \leq \ell)\)-identifying codes from below.
Let $C$ be an $(r, \leq \ell)$-identifying code. Define
\[ D_r(x) = S_r(x) \cap C \]
and
\[ D_r(X) = \bigcup_{y \in X} D_r(y), \]
where $x \in \mathbb{F}^n$ and $X \subseteq \mathbb{F}^n$. The following preliminary results are needed in the proofs of Theorems 3.4 and 3.5, which provide us new lower bounds for $(r, \leq \ell)$-identifying codes.

**Lemma 3.1.** Let $C \subseteq \mathbb{F}^n$ be an $(r, \leq \ell)$-identifying code and $x_1, x_2, \ldots, x_i \in \mathbb{F}^n$, where $1 \leq i \leq \ell - 1$ and $x_i \not\in \{x_1, \ldots, x_{i-1}\}$. Then we have
\[ |D_r(x_i) \setminus \left( \bigcup_{j=1}^{i-1} I_r(x_j) \right) | \geq 2\ell - 2i. \]

**Proof.** Assume to the contrary that
\[ |D_r(x_i) \setminus \left( \bigcup_{j=1}^{i-1} I_r(x_j) \right) | \leq 2\ell - 2i - 1 = 2(\ell - i - 1) + 1. \]
Now there exist words $y_1, \ldots, y_{\ell-i}$ such that $d(x_i, y_j) = 2$ for all $j = 1, \ldots, \ell-i-1$ and $d(x_i, y_{\ell-i}) = 1$ such that $D_r(x_i) \subseteq I_r(y_1) \cup \cdots \cup I_r(y_{\ell-i})$. Since $I_{\ell-i}(x_i) \subseteq I_r(y_{\ell-i})$, we have
\[ I_r(y_1, \ldots, y_{\ell-i}, x_1, \ldots, x_{i-1}) = I_r(y_1, \ldots, y_{\ell-i}, x_1, \ldots, x_{i-1}, x_i), \]
which is a contradiction with the fact that $C$ is an $(r, \leq \ell)$-identifying code. Thus, the claim holds. \qed

**Corollary 3.2.** Let $C \subseteq \mathbb{F}^n$ be an $(r, \leq \ell)$-identifying code and $X, Y \subseteq \mathbb{F}^n$ be two distinct sets such that $|X| \leq \ell - 2$ or $|Y| \leq \ell - 2$. Then we have
\[ \bigcup_{x \in X} D_r(x) \neq \bigcup_{y \in Y} D_r(y). \]

**Proof.** Without loss of generality, we may assume that $|Y| \geq |X|$. Let $y$ be a word in $Y \setminus X$. Then, as $|X| \leq \ell - 2$, by Lemma 3.1, we have
\[ D_r(y) \setminus \left( \bigcup_{x \in X} I_r(x) \right) \neq \emptyset. \]
Hence, the claim follows. \qed

**Corollary 3.3.** Let $C \subseteq \mathbb{F}^n$ be an $(r, \leq \ell)$-identifying code and $X = \{x_1, x_2, \ldots, x_i\} \subseteq \mathbb{F}^n$ a set with $1 \leq i \leq \ell - 1$. Then we have
\[ \left| \bigcup_{k=1}^{i} D_r(x_k) \right| \geq i(2\ell - i - 1). \]

**Proof.** By Lemma 3.1, we have
\[ \left| \bigcup_{k=1}^{i} D_r(x_k) \right| = \left| \bigcup_{k=1}^{i} (D_r(x_k) \setminus (D_r(x_1) \cup \cdots \cup D_r(x_{k-1}))) \right| = \sum_{k=1}^{i} |D_r(x_k) \setminus (D_r(x_1) \cup \cdots \cup D_r(x_{k-1}))| \]
Lemma 3.1 can be applied to find lower bounds in a way similar to Corollary 3.3. Let $$g_j = \sum_{k=1}^{j}(2\ell - 2k) = j(2\ell - j - 1)$$. The following theorem provides us a new lower bound for $$(r, \leq \ell)$$-identifying codes.

**Theorem 3.4.** Let $$C \subseteq \mathbb{F}^n$$ be an $$(r, \leq \ell)$$-identifying code with $$r \geq 2$$ and $$\ell \geq 3$$. Then we have

$$|C| \sum_{j=1}^{\ell-2} \sum_{i=1}^{j} \left( \begin{array}{c} n \\ i \end{array} \right) \left( 2^n - \left( \begin{array}{c} n \\ j-i \end{array} \right) \right) \geq \sum_{i=1}^{\ell-2} \left( \sum_{j=1}^{s_i} \left( \begin{array}{c} |C| \\ i \end{array} \right) + \left( \begin{array}{c} 2^n \\ j \end{array} \right) - \sum_{j=1}^{s_i} \left( \begin{array}{c} |C| \\ i \end{array} \right) \right)(s_j + 1),$$

where, for $$j = 1, \ldots, \ell - 2$$, $$s_j$$ is the integer such that

$$\sum_{i=g_j}^{s_j} \left( \begin{array}{c} |C| \\ i \end{array} \right) \leq \left( \begin{array}{c} 2^n \\ j \end{array} \right) < \sum_{i=g_j}^{s_j+1} \left( \begin{array}{c} |C| \\ i \end{array} \right).$$

**Proof.** Let $$j$$ be an integer such that $$1 \leq j \leq \ell - 2$$ and define $$X_j = \{X \mid X \subseteq \mathbb{F}^n, |X| = j\}$$. Let us now consider pairs $$(X, c)$$, where $$X \in X_j$$ and $$c$$ is covered exactly at distance $$r$$ by a word in X. It is easy to see that there exist

$$\sum_{i=1}^{j} \left( \begin{array}{c} n \\ i \end{array} \right) \left( 2^n - \left( \begin{array}{c} n \\ r \end{array} \right) \right)$$

different sets in $$X_j$$ corresponding to each codeword $$c$$. On the other hand, by Corollary 3.3, for each $$X \in X_j$$ we have $$D_r(X) \geq g_j$$ and, by Corollary 3.2, we know that $$D_r(X)$$ is unique for each $$X \in X_j$$. Thus, by counting in two ways the number of pairs $$(X, c)$$ with $$X \in X_j$$ and $$c \in C$$ such that $$d(X, c) = r$$, we have

$$|C| \sum_{i=1}^{j} \left( \begin{array}{c} n \\ i \end{array} \right) \left( 2^n - \left( \begin{array}{c} n \\ r \end{array} \right) \right) \geq \sum_{i=g_j}^{s_j} \left( \begin{array}{c} |C| \\ i \end{array} \right) + \left( \begin{array}{c} 2^n \\ j \end{array} \right) - \sum_{i=g_j}^{s_j} \left( \begin{array}{c} |C| \\ i \end{array} \right)(s_j + 1),$$

where $$s_j$$ is such that $$\sum_{i=g_j}^{s_j} \left( \begin{array}{c} |C| \\ i \end{array} \right) \leq \left( \begin{array}{c} 2^n \\ j \end{array} \right) < \sum_{i=g_j}^{s_j+1} \left( \begin{array}{c} |C| \\ i \end{array} \right)$$. Now, by combining the inequality above for all $$j$$, the claim follows. □

Theorem 3.4 can be applied to find lower bounds in a way similar to Theorem 2.5. For example, the previous theorem provides us the best known lower bound 197 when $$r = 13, l = 5$$ and $$n = 35$$. Previously the best known lower bound for these values was 169 by Karpovsky et al. in [14].

The following theorem is a slightly modified version of Theorem 16 in [8]. However, it enables us to improve some lower bounds.

**Theorem 3.5.** For $$r \geq 2$$ and $$\ell \geq 2$$ we have

$$M_j^{(r, \leq \ell)}(n) \geq \left\lceil \frac{(2\ell - 2)2^n}{\left( \begin{array}{c} n \\ r \end{array} \right)} \right\rceil.$$

**Proof.** Let $$C \subseteq \mathbb{F}^n$$ be an $$(r, \leq \ell)$$-identifying code. By Lemma 3.1, we have that $$D_r(x) \geq 2\ell - 2$$ for every $$x \in \mathbb{F}^n$$. Now, by counting in two ways the number of pairs $$(x, c)$$, where $$x \in \mathbb{F}^n$$ and $$c \in D_r(x)$$, we have
\[ |C| \left( \frac{n}{r} \right) \geq (2\ell - 2)2^n. \]

Hence, the claim follows directly from this inequality. \( \square \)

The previous theorem gives us, for example, the best known lower bound 37 for \((2, \leq 3)\)-identifying code of length \(n = 8\). The best previously known bound for these values was 36 by Theorem 16 in [8].

4. Constructions for \((r, \leq \ell)\)-identifying codes

In the previous section we presented results concerning the lower bounds of \((r, \leq \ell)\)-identifying codes. In what follows, we consider direct sum methods to construct new \((r, \leq \ell)\)-identifying codes from known ones. The results presented in this section are mainly based on [19, Chapter 4]. The direct sum methods have been previously used, for example, in [3] and [7] (to construct new identifying codes from known ones). The direct sum of codes \(C_1 \subseteq \mathbb{F}^{n_1}\) and \(C_2 \subseteq \mathbb{F}^{n_2}\), where \(n_1\) and \(n_2\) are positive integers, is defined as

\[ C_1 \oplus C_2 = \{(x_1, x_2) \mid x_1 \in C_1, x_2 \in C_2\}. \]

Let us then start by presenting a preliminary lemma used in the following proofs.

**Lemma 4.1.** Suppose \(r \geq 1\) and \(\ell \geq 2\). Let \(C \subseteq \mathbb{F}^n\) be an \((r, \leq \ell)\)-identifying code. Then for every word \(y \in \mathbb{F}^n\) and set \(X \subseteq \mathbb{F}^n\) such that \(|X| \leq \ell - 2\) and \(y \notin X\), we have

\[ D_r(y) \setminus \left( \bigcup_{x \in X} I_r(x) \right) \neq \emptyset. \]

**Proof.** The result immediately follows from the proof of Corollary 3.2. \( \square \)

The next theorem considers \(r = 2\) for all \(\ell \geq 2\). Because of Theorem 4.4 and Example 4.5, we have kept a general radius \(r\) in the following proof as long as possible.

**Theorem 4.2.** Let \(r = 2\) and \(\ell \geq 2\). If \(C \subseteq \mathbb{F}^n\) is an \((r, \leq \ell)\)-identifying code, then \(D := C \oplus \mathbb{F}^r \subseteq \mathbb{F}^{n+r}\) is \((r, \leq \ell)\)-identifying.

**Proof.** Let \(X, Y \subseteq \mathbb{F}^{n+r}, X \neq Y, X = \{x_1, \ldots, x_{\ell}\}, Y = \{y_1, \ldots, y_{\ell}\}, 1 \leq \ell_1 \leq \ell \) and \(1 \leq \ell_2 \leq \ell\). Let us denote \(x_i = (x_i^*, x_i^t)\) and \(y_j = (y_j^*, y_j^t)\), where \(x_i^*, y_j^* \in \mathbb{F}^n\) and \(x_i^t, y_j^t \in \mathbb{F}^r\) for \(1 \leq i \leq \ell_1\) and \(1 \leq j \leq \ell_2\). Denote \(X^* = \{x_1^*, \ldots, x_{\ell_1}^*\}\) and \(Y^* = \{y_1^*, \ldots, y_{\ell_2}^*\}\).

If \(X^* \neq Y^*\), then there exists \(c^* \in I_r(C; X^*) \cap I_r(C; Y^*)\). Without loss of generality we can assume \(c^* \in I_r(C; x_1^*); Y)\). Now \(c^*, x_1^* \in I_r(D; X) \setminus I_r(D; Y)\).

Suppose \(X^* = Y^*\). Assume to the contrary that \(I_r(D; X) = I_r(D; Y)\). Because \(X \neq Y\), for some \(i\) there is \(x_i^* \neq y_i^*\) for all \(h\) for which \(y_h^* = x_i^*\). Without loss of generality we can assume \(i = 1\). Now \(x_1 \notin Y\) and the words \((x_1^*, y_{h_1}^*), \ldots, (x_1^*, y_{h_{\ell_2}}^*)\) \(\in Y\) do not \(r\)-cover codewords that are at distance \(r\) from \(x_1\) and end with \(x_1^t\). By Lemma 4.1 we know that such a codeword exists and in \(Y\) there must be \(\ell - 1\) words which \(r\)-cover these codewords. This implies that every word in \(Y^*\) appear only once. This also holds for \(X^*\) since \(X^* = Y^*\).

There is a codeword \(c^* \in I_r(C; x_1^*; Y)\), because otherwise \(I_r(C; X^* \setminus \{x_1^*\}) = I_r(C; X^*)\). If \(d(c^*, x_1^*) \geq 1\), then because \(d(x_1^*, y_{h_1}^*) \geq 1\), there is a word \(f \in \mathbb{F}^n\) such that \(d(f, x_1^*) \leq r - d(c^*, x_1^*)\) and \(d(f, y_{h_1}^*) > r - d(c^*, x_1^*)\). Thus, \((c^*, f) \in I_r(D; X) \setminus I_r(D; Y)\), which is a contradiction.

Suppose therefore that \(d(c^*, x_1^*) = 0\) and \(c^*\) is the only word in \(I_r(C; x_1^*) \setminus I_r(C; X^* \setminus \{x_1^*\})\). In particular,

\[ 2r \geq d(x_1^*, X^* \setminus \{x_1^*\}) \geq r + 1. \] (12)

Next we show that \(X \setminus \{x_1\} = Y \setminus \{y_{h_1}\}\). Assume there is a word \(x_k \in X \setminus \{x_1\}\) such that \(x_k \notin Y \setminus \{y_{h_1}\}\), that is \(x_k^* \neq y_{h_1}^*\), when \(x_k^* = y_{h_1}^*\). As above we get a contradiction unless \(x_k^*\) is the only codeword in \(I_r(C; x_k^*; Y)\). Because \(d(x_1^*, x_k^*) \leq 2r\) there is \(w \in B_r(x_1^*) \cap B_r(x_k^*)\),
now $I_r(C; (X^* \setminus \{x^*_1\}) \cup \{w\}) = I_r(C; (X^* \setminus \{x^*_k\}) \cup \{w\})$, which is impossible. This means that $X \setminus \{x_1\} = Y \setminus \{y_1\}$.

Without loss of generality $h = 1$, and we have $X = \{x_1, x_2, \ldots, x_t\}$ and $Y = \{y_1, x_2, \ldots, x_t\}$ where $x_t \neq y_1, x^*_t = y^*_1$ and $x^*_t \neq y_1$. Moreover, the set $\{x^*_2, \ldots, x^*_r\}$ r-covers $I_r(C; x^*_1) \setminus \{x^*_1\}$.

The assumption $I_r(D; X) = I_r(D; Y)$ implies that the set $\{x^*_2, \ldots, x^*_r\}$ r-covers $I_r(D; x^*_1) \triangle I_r(D; y^*_1)$. Suppose $x^*_t \in X^* \setminus \{x^*_1\}$ r-covers a codeword $c^*_t \in (I_r(C; x^*_1) \setminus I_r-D(x^*_1, y^*_1)(C; x^*_1)) \setminus I_r(C; X^* \setminus \{x^*_1\})$ (such words $x^*_t$ and $c^*_t$ always exist). Hence, the word $x_t = (x_t^*, x^*_t) \in X \cap Y$ r-covers the codewords $(c^*_t, x^*_t) \in I_r(D; x^*_1)$ and $(c^*_t, y^*_t) \in I_r(D; y^*_1)$ (since $d((x^*_t, x^*_1), (c^*_t, y^*_1)) \geq r - d(x^*_t, y^*_1) + 1 + d(x^*_t, y^*_1) \geq r + 1$).

We have

$$2r \geq d(x_t, (c_t^*, x_t^*)) + d(x_t, (c_t^*, y_t^*))$$

$$= d(x_t^*, c_t^*) + d(x_t, x_t^*) + d(x_t^*, c_t^*) + d(x_t^*, y_t^*)$$

$$\geq 2d(x_t^*, c_t^*) + d(x_t^*, y_t^*).$$

Hence, $d(x_t^*, c_t^*) \leq r - \frac{1}{2}d(x_t^*, y_t^*)$, which implies

$$\forall c_t^* \in (I_r(C; x_t^*) \cap B_r(x_t^*) \setminus B_r-(d(x_t^*, y_t^*))(x_t^*)) \setminus I_r(X^* \setminus \{x^*_1, x^*_t\}) : d(x_t^*, c_t^*) \leq r - 1. \quad (13)$$

This and (12) imply $r + 1 \leq d(x_t^*, x_t^*) \leq 2r - 1$. From now on $r = 2$ and $d(x_t^*, x_t^*) = 3$.

- If $d(x_t^*, y_t^*) = 2$, then by (13) we have $I_r(C; x_t^*) \cap I_r(C; x_t^*) \subseteq I_1(C; x_t^*) \cap I_2(C; x_t^*)$. Hence, for every $y^* \in S_2(x_t^*)$ such that $d(y^*, x_t^*) = 1$ we have

$$I_2(C; (X^* \setminus \{x_t^*, x_t^*\}) \cup \{y^*\}) = I_2(C; (X^* \setminus \{x_t^*\}) \cup \{y^*\})$$

which is a contradiction.

- Suppose then $d(x_t^*, y_t^*) = 1$. If $(S_1(x_t^*) \cap I_2(C; x_t^*) \setminus I_2(X^* \setminus \{x_t^*, x_t^*\}) = \emptyset$, then we are done as in the previous case. If there is $c_t^* \in (S_1(x_t^*) \cap I_2(C; x_t^*) \setminus I_2(X^* \setminus \{x_t^*, x_t^*\})$, then $(c_t^*, y_t^* + 11) \in I_2(D; x_t^*) \setminus I_2(D; Y)$. (Recall that by the sum of vectors $y_t^* + 11$ of length 2, we mean the usual addition of vectors.) Namely, $y_t^* + 11 \neq x_t^*$ otherwise $x_t^*$ could not cover any codeword at $S_2(y_t^*)$ ending with $y_t^*$. \hfill \Box

For $r = 1$ the previous result is known to be true when $\ell \geq 3$ [16].

**Corollary 4.3.** For $\ell \geq 2$ we have:

$$M_1^{\leq \ell} (n + 1) \leq 2M_1^{\leq \ell} (n).$$

$$M_2^{\leq \ell} (n + 2) \leq 4M_2^{\leq \ell} (n).$$

For general $r$ (in particular, when $\ell \geq 3$) we have the following slightly weaker result.

**Theorem 4.4.** Let $r \geq 1$ and $\ell \geq 2$. If $C \subseteq \mathbb{F}^n$ is an $(r, \leq \ell)$-identifying code, then $D := C \oplus \mathbb{F}^{r+1} \subseteq \mathbb{F}^{n+r+1}$ is $(r, \leq \ell)$-identifying.

**Proof.** The first three paragraphs of the proof of Theorem 4.2 go similarly. Using the same notations we can continue slightly differently. Now we only have the case $d(x_t^*, c_t^*) \geq 0$. Because $d(x_t^*, y_t^*) \geq 1$ there is a word $f \in \mathbb{F}^{r+1}$ such that $d(f, x_t^*) \leq r - d(c_t^*, x_t^*)$ and $d(f, y_t^*) > r - d(c_t^*, x_t^*)$. Thus, $(c_t^*, f) \in I_r(D; X) \setminus I_r(D; Y)$. \hfill \Box

The next example shows that Theorem 4.2 cannot be generalized for $(3, \leq 2)$-identifying codes.

**Example 4.5.** By a computer it can be shown that the code

$$C = \{0\} \cup (S_3(0) \cap S_2(111110000)) \cup (\mathbb{F}^8 \setminus B_4(0)) \subseteq \mathbb{F}^8$$

is $(3, \leq 2)$-identifying code of length 8. The code $C \oplus \mathbb{F}^3$ is not $(3, \leq 2)$-identifying since

$$I_3(0000000000, 1111100000) = I_3(0000000001, 1111100000).$$

This code is chosen in such a way that it satisfies the conditions of the seventh paragraph in the proof of Theorem 4.2.
Theorems 4.2 and 4.4 together with known \((r, \leq \ell)\)-identifying codes provide us a method to construct new \((r, \leq \ell)\)-identifying codes. By computer search, we have found that the binary representation of the numbers 1, 2, 5, 10, 25, 28, 30, 36, 41, 47, 50, 51, 52, 57, 63, 65, 70, 75, 77, 82, 87, 91, 99, 102, 104, 110, 117, 120, 125, and 126 form a \((2, \leq 2)\)-identifying code of length 7 and cardinality 30. Therefore, using Theorem 4.2 and this code, we can construct a \((2, \leq 2)\)-identifying code of length 9 with cardinality 120. The cardinalities of both of these codes are current records.

Using computers, we have also been able to find other \((r, \leq \ell)\)-identifying codes with the smallest known cardinality. These codes are presented in the following.

The binary representation of the numbers 4, 7, 11, 12, 15, 16, 18, 23, 24, 25, 26, 34, 35, 40, 41, 43, 45, 49, 53, 55, 60, and 62 form a \((2, \leq 2)\)-identifying code of length 6 and cardinality 22.

The binary representation of the numbers 1, 5, 17, 22, 39, 41, 48, 52, 63, 66, 72, 75, 90, 91, 93, 102, 108, 113, 115, 122, 131, 132, 140, 154, 157, 169, 174, 178, 201, 208, 215, 224, 239, 247, and 252 form a \((3, \leq 2)\)-identifying code of length 8 and cardinality 37. Observe that applying now Theorem 4.4 gives us the best known code of size 592 and length 12.


Acknowledgements

The second author’s research was supported by the Academy of Finland under grant 210280. The third author’s research was supported by the Academy of Finland under grant 111940. The fourth author’s research was supported in part by the Nokia Foundation.

References