Publication II

Patric R. J. Östergård and Esa A. Seuranen. 2006. Unidirectional covering codes. IEEE Transactions on Information Theory, volume 52, number 1, pages 336-340.

[15] Y. Tang, T. Kasami, and T. Fujiwara, "On the computation of the search centers and the evaluation of the testing conditions for the h-chase decoding," in *Proc. 23rd Symp. Information Theory and Its Applications*, Aso, Kumamoto, Japan, Oct. 2000, pp. 77–80.

Unidirectional Covering Codes

Patric R. J. Östergård, *Member, IEEE,* and Esa A. Seuranen

***Abstract*—A code $C \subseteq Z_2^n$, where $Z_2 = \{0, 1\}$, has unidirectional covering radius R if R is the smallest integer so that any word in Z_2^n can be obtained from at least one codeword $c \in C$ by replacing either 1s by 0s in at most R coordinates or 0s by 1s in at most R coordinates. The minimum cardinality of such a code is denoted by $E(n, R)$. Upper bounds on this function are here obtained by constructing codes using tabu search; lower bounds, on the other hand, are mainly obtained by integer programming and exhaustive search. Best known bounds on $E(n, R)$ for $n \leq 13$ and $R \leq 6$ are tabulated.**

***Index Terms*—Covering codes, integer programming, tabu search, unidirectional codes.**

I. Introduction

Covering codes have been studied extensively—see [1] and its references—the main motivations being football pools and data compression. Various types of applications have indeed acted as stimulation for bringing forward and studying variants of covering codes, but one can also look at the dual problem of finding packing (that is, error-correcting) codes and via analogies discover unexplored types of coverings.

Two common types of communication channels have inspired the study of asymmetric error-correcting codes [2]–[5], and unidirectional error-correcting codes [2], [4], [6], [7]. Recently, asymmetric covering codes have been considered in several studies [8]–[11], but, to our knowledge, unidirectional covering codes have not received any attention so far. In this correspondence, binary unidirectional covering codes are studied with an emphasis on (bounds on) minimum cardinalities of such codes.

Consider the binary n-dimensional space, Z_2^n, where $Z_2 = \{0, 1\}$. For a prescribed value of R, the set of words obtained by making at most R changes $1 \rightarrow 0$ of the coordinate values to a given word in Z_2^n is called a *downward directed ball*. Analogously, if we allow only changes $0 \rightarrow 1$, we get an *upward directed ball*. Finally the union of a downward and an upward directed ball around a word is called a *unidirectional ball*. A code $C \subseteq Z_2^n$ is said to have unidirectional covering radius R if R is the smallest integer so that any word in Z_2^n is within the unidirectional ball around a codeword $c \in C$. Throughout this correspondence, for given R, we say that a word *covers* (or R-*covers*) the words in its unidirectional ball. The minimum cardinality of such a code is denoted by $E(n, R)$.

Manuscript received October 12, 2004; revised June 10, 2005. This work was supported by the Academy of Finland under Grants 100500, 107493, and 202315. The material in this correspondence was presented in part at the 8th Nordic Combinatorial Conference, Aalborg University, Aalborg, Denmark, October 2004.

The authors are with the Department of Electrical and Communications Engineering, Helsinki University of Technology, 02015 TKK, Finland.

Communicated by K. A. S. Abdel-Ghaffar, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2005.860449

This correspondence is organized as follows. In Section II methods that can be used to obtain lower bounds on $E(n, R)$ are considered; these are mainly based on integer programming and exhaustive computer search. Some constructions for unidirectional covering codes analogous to known constructions for covering codes are discussed in Section III. Many of the best known upper bounds were obtained by finding corresponding codes using tabu search; this approach is described in Section IV. The best known lower and upper bounds on $E(n, R)$ for $n \leq 13$ and $R \leq 6$ are summarized and tabulated in Section V.

II. Lower Bounds

A. Integer Programming Problems

Determination of $E(n, R)$ can be formulated as an integer programming problem, to be discussed in Section II-A1. However, since instances of this problem are computationally feasible only for the very smallest values of n, two relaxations of this problem—which can then be used for determining lower bounds on $E(n, R)$—are presented in Sections II-A2 and II-A3. The program glpk [12] was used to solve instances of these integer programming problems.

1) The Exact IP Problem ($\mathrm{IP}_{\mathrm{exact}}$)*:* An integer programming problem for determining $E(n, R)$ called $\mathrm{IP}_{\mathrm{exact}}$—the solution of which gives an explicit code attaining this value—is as follows:

$$\text{Min } Z = \sum_{i=0}^{2^n-1} b_i$$

Subject to:

$$1 \leq \sum_{j \in S(i)} b_j, \quad \text{where} \quad 0 \leq i < 2^n$$

$$b_i \in \{0, 1\}, \quad \text{where} \quad 0 \leq i < 2^n$$

where b_i tells whether the word i (in decimal form) is in the code or not and $S(i)$ is the set of all words that cover the word i. An analogous integer programming formulation appears in [8] for asymmetric covering codes.

We were able to determine all values of $E(n, R)$ with $n \leq 8$ using this integer programming formulation. We now turn to the formulations utilized for $n > 8$.

2) The Sphere IP Problem ($\mathrm{IP}_{\mathrm{sphere}}$)*:* Since the number of words covered by a codeword depends on the Hamming weight of the codeword, one does not get a volume (sphere covering) bound in a compact form. The volume bound, called $\mathrm{IP}_{\mathrm{sphere}}$, now takes the following form:

$$\text{Min } Z = \sum_{w=0}^{n} s_w$$

Subject to:

$$\binom{n}{w} \leq s_w + \sum_{\substack{r=1 \\ 0 \leq w+r \leq n}}^{R} s_{w+r} \binom{w+r}{r} + \sum_{\substack{r=1 \\ 0 \leq n-w+r \leq n}}^{R} s_{w-r} \binom{n-w+r}{r},$$

where $0 \leq w \leq n$

$$s_w \in \left\{0, 1, 2, \ldots, \binom{n}{w}\right\}, \quad \text{where } 0 \leq w \leq n$$

where s_w denotes the number of codewords of weight w. Instances of this problem are comparatively easy and the number of variables and inequalities grow linearly with n (compared with $\mathrm{IP}_{\mathrm{exact}}$, where these

TABLE I
SOME UPPER BOUNDS ON LAST (w)

			w													
n	R	M	0	1	2	3	4	5	6	7	8	9	10	11	12	13
9	2	20	1	4	7	8	7	7	8	7	4	1				
10	2	31	0	2	5	6	5	2	5	6	5	2	0			
10	3	13	1	4	5	6	2	2	2	6	5	4	1			
11	2	52	0	2	5	16	6	5	5	6	16	5	2	0		
11	3	20	1	4	7	7	5	3	3	5	7	7	4	1		
12	2	90	0	1	7	19	22	8	7	8	22	19	7	1	0	
12	3	31	1	4	9	11	5	4	3	4	5	11	9	4	1	
12	4	13	1	4	6	7	3	2	2	2	3	7	6	4	1	
13	2	156	0	0	9	18	46	13	12	12	13	46	18	9	0	0
13	3	47	1	3	5	17	4	2	2	2	2	4	17	5	3	1
13	4	19	1	4	7	8	5	3	2	2	3	5	8	7	4	1

numbers grow exponentially). Analogous formulations can be found in [13] for covering codes and in [9] for asymmetric covering codes.

3) The Advanced IP Problem ($\mathrm{IP}_{\mathrm{adv}}$)*:* In the volume bound, $\mathrm{IP}_{\mathrm{sphere}}$, one does not take into account that if there are many words of a given weight, then the balls around these words must necessarily overlap. We shall now use this observation to develop an integer programming formulation that improves on the volume bound (and is yet solvable within a reasonable time).

Let $v(n,k,w,w')$ denote the maximum number of words in Z_2^n that have weight w' and can be covered with k words of weight w. Note that, always assuming $R \geq |w-w'|$, this function does not depend on the unidirectional covering radius R. We now get an integer programming problem, called $\mathrm{IP}_{\mathrm{adv}}$, of the following form:

$$\text{Min } Z = \sum_{w=0}^{n} \sum_{j=1}^{\mathrm{last}(w)} j \cdot s_{w,j}$$

Subject to:

$$\binom{n}{w} \leq \sum_{j=1}^{\mathrm{last}(w)} j \cdot s_{w,j} + \sum_{r=1}^{R} \sum_{j=1}^{\mathrm{last}(w+r)} v(n,j,w+r,w) \cdot s_{w+r,j} + \sum_{r=1}^{R} \sum_{j=1}^{\mathrm{last}(w-r)} v(n,j,w-r,w) \cdot s_{w-r,j},$$

$$\text{where } 0 \leq w \leq n$$

$$\sum_{j=1}^{\mathrm{last}(w)} s_{w,j} \leq 1, \text{ where } 0 \leq w \leq n$$

$$s_{w,j} \in \{0,1\}, \text{ where } 0 \leq w \leq n, 1 \leq j \leq \mathrm{last}(w)$$

where $\mathrm{last}(w)$ is an upper bound on the number of codewords of weight w. Note that $s_{w,j} = 1$ means that there are exactly j codewords of weight w. We shall now see how one can determine exact values of or bounds on $\mathrm{last}(w)$ and $v(n,k,w,w')$.

B. Two Auxiliary Functions

To determine an upper bound on $\mathrm{last}(w)$ for a given problem instance of $\mathrm{IP}_{\mathrm{adv}}$, we solve, for all w' in the interval $0 \leq w' \leq n$, a problem that is a slightly modified version of the volume bound $\mathrm{IP}_{\mathrm{sphere}}$. In this auxiliary integer programming problem, $\mathrm{IP}^*_{\mathrm{sphere}}$, we change the objective function to $\mathrm{Max}\ Z = s_{w'}$ and add the constraint $M = \sum_{w=0}^{n} s_w$ (to fix the number of codewords).

After we have obtained upper bounds on $\mathrm{last}(w)$ using $\mathrm{IP}^*_{\mathrm{sphere}}$ we can make similar modifications to $\mathrm{IP}_{\mathrm{adv}}$, i.e., change the objective function to

$$\mathrm{Max}\ Z = \sum_{j=1}^{\mathrm{last}(w')} j \cdot s_{w',j}$$

and add the constraint

$$M = \sum_{w=0}^{n} \sum_{j=1}^{\mathrm{last}(w)} j \cdot s_{w,j},$$

to form another auxiliary integer programming problem, $\mathrm{IP}^*_{\mathrm{adv}}$. The upper bounds on $\mathrm{last}(w)$ attained by $\mathrm{IP}^*_{\mathrm{adv}}$ are listed in Table I for the instances that lead to best known lower bounds on $E(n,R)$ tabulated at the end of this correspondence.

Before proceeding to discussing the function $v(n,k,w,w')$, we will now present an algorithm that uses integer programming formulations and exhaustive search (to be discussed in Section II-C) in order to improve the lower bound for a given problem instance.

1: $M \leftarrow \mathbf{IP}_{\mathrm{sphere}}(n,R)$
2: Use $\mathbf{IP}^*_{\mathrm{sphere}}(n,R)$ to get upper bounds on $\mathrm{last}(w)$
3: **if** $\mathbf{IP}_{\mathrm{adv}}(n,R) > M$ **then** $M \leftarrow M+1$, **goto** 2
4: Use $\mathbf{IP}^*_{\mathrm{adv}}(n,R)$ to tighten upper bounds on $\mathrm{last}(w)$
5: **switch** perform exhaustive search
6: **case** no solution: $M \leftarrow M+1$, **goto** 2
7: **case** a solution: **exit**
8: **case** search failed: **exit**
9: **end switch**

Once the algorithm has exited, M is a lower bound on (or the exact value of, if the algorithm exited via line 7) $E(n,R)$.

To determine values of $v(n,k,w,w')$, we consider all possible sets of k codewords of weight w. It is obviously necessary to do this only for inequivalent codes, two binary constant weight codes being equivalent if there is a permutation of the coordinates that maps one code onto the other.

Recursively, the codes with $i+1$ codewords are constructed from a complete set of codes with i codewords by adding one codeword in all possible ways. Equivalence of the constructed constant weight codes is tested using the standard approach of mapping the codes into bipartite graphs—with vertices for codewords and coordinates, joining a codeword vertex to a coordinate vertex exactly when the corresponding codeword has a 1 in that coordinate—and testing graph isomorphism using *nauty* [14]. See Fig. 1, where the graphs of all inequivalent codes of length 5, size 2, and weight 3 are displayed.

Using the above-mentioned computational method for determining $v(n,k,w,w')$ is too demanding for all but the smallest values of k,

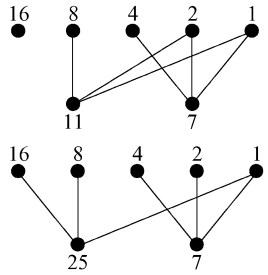

Fig. 1. Graphs of inequivalent codes.

accentuating the need for other approaches for determining values of (or bounds on) this function.

The maximum number of codewords without overlapping unidirectional balls follows from the size of certain constant weight error-correcting codes (also called packing designs in the literature). The maximum number of codewords in a code with length n, minimum distance d, and constant weight w is denoted by $A(n,d,w)$; see [15]–[17] for extensive results on this function.

Lemma 2.1: For $0 \leq k \leq A(n, 2(|w-w'|+1), w)$, we have $v(n,k,w,w') = k \cdot v(n,1,w,w')$; and for $k = A(n, 2(|w-w'|+1), w) + 1$, we have $v(n,k,w,w') < k \cdot v(n,1,w,w')$.

Proof: By the definition of $A(n,d,w)$ there is a (maximal) set of codewords $C \in Z_2^n$ of size $A(n,d,w)$ and weight w, so that a cut of unidirectional balls of covering radius $d/2-1$ around any two codewords in C is empty. For $d = 2(|w-w'|+1)$ we get that $d/2 - 1 = |w-w'|$, so $v(n,k,w,w') = k \cdot v(n,1,w,w')$ for $0 \leq k \leq A(n, 2(|w-w'|+1), w)$ and $v(n,k,w,w') < k \cdot v(n,1,w,w')$ for $k > A(n, 2(|w-w'|+1), w)$. □

Next we present an inequality that can be used to obtain upper bounds on $v(n,k,w,w')$.

Theorem 2.2: $v(n,k+1,w,w') \leq \frac{k+1}{k} \cdot v(n,k,w,w')$ for $0 \leq w, w' \leq n$ and $k \geq 1$.

Proof: Let C be a code that attains $v(n,k+1,w,w')$. By the pigeonhole principle, there exists a codeword $c \in C$ whose removal uncovers at most $\frac{1}{k+1} v(n,k+1,w,w')$ words. Then $C \backslash \{c\}$ covers at least $\frac{k}{k+1} v(n,k+1,w,w')$ words so $v(n,k,w,w') \geq \frac{k}{k+1} \cdot v(n,k+1,w,w')$.

When the number of codewords exceeds $A(n, 2(|w-w'|+1), w)$ we get the following result for upper bounds on $v(n,k,w,w')$. □

Corollary 2.3: For $0 \leq w, w' \leq n$, let $k = A(n, 2(|w-w'|+1), w) + i$ with $i \geq 1$. Then $v(n,k,w,w') \leq k \cdot v(n,1,w,w') - i$.

Proof: For $i = 1$ the corollary follows from Lemma 2.1. For $i > 1$ apply Theorem 2.2 iteratively. □

By complementing a code attaining $v(n,k,w,w')$ one gets a code that attains $v(n,k,n-w,n-w')$.

Proposition 2.4: $v(n,k,w,w') = v(n,k,n-w,n-w')$ for $0 \leq w, w' \leq n$ and $k \geq 0$.

As an example, we tabulate in Table II the values of $v(10,k,w,w')$ used in the processing of $E(10,3) > 13$. Since $R = 3$ we need consider only sets of parameters that fulfill $|w-w'| \leq 3$, and by Proposition 2.4 we may restrict the value of w to $w \leq 5$. (Similar tables for other problem instances are omitted.)

TABLE II
SOME VALUES OF $v(10,k,w,w')$ WHEN $R = 3$

		w'										
w	k	0	1	2	3	4	5	6	7	8	9	10
0	1	1	10	45	120							
1	1	1	1	9	36	84						
1	2	1	2	17	64	140						
1	3	1	3	24	85	175						
1	4	1	4	30	100	195						
2	1	1	2	1	8	28	56					
2	2	1	4	2	16	55	106					
2	3	1	6	3	24	81	150					
2	4	1	8	4	32	106	188					
2	5	1	10	5	40	130	220					
3	1	1	3	3	1	7	21	35				
3	2	1	6	6	2	14	42	69				
3	3	1	9	9	3	21	63	102				
3	4	1	10	12	4	28	82	126				
3	5	1	10	15	5	35	100	147				
3	6	1	10	18	6	42	118	165				
4	1		4	6	4	1	6	15	20			
4	2		8	12	8	2	12	30	40			
5	1			10	10	5	1	5	10	10		
5	2			20	20	10	2	10	20	20		

C. Exhaustive Search

The instances of the IP problems discussed so far possess a large symmetry group, which has a significant impact on the computing time of any optimization software used. A tailored backtrack algorithm can be developed to make a further improvement of some of the lower bounds possible. The main idea is to try to construct codes one codeword at a time, and solve instances of versions of the IP problems discussed earlier, slightly modified to be able to handle fixed codewords. We now discuss one possible such algorithm.

We fix the number of codewords, M, and aim at proving that no such code exists. Moreover, we fix the weight distribution of the code within the boundary of $\mathrm{last}(w)$ (cf. Table I; also notice that complementing a code does not affect its covering properties, so having checked a given weight distribution, its reverse may be ignored). Each possible weight distribution is now handled separately, and the code is built up one codeword at a time, rejecting equivalent codes (essentially in the same way as described in Section II-B). The codewords are added in order of either increasing or decreasing weight.

Bounding takes place by solving IP problems for partial codes. If the coverage of the fixed codewords plus the maximal coverage of the unassigned codewords—cf. $\mathrm{IP}_{\mathrm{adv}}$—could not produce a desired code, then the partial code is discarded.

III. CONSTRUCTIONS AND UPPER BOUNDS

Attempts were made to carry over known constructions of covering codes [1] to the case of unidirectional covering codes, but with limited success. For example, the direct sum, defined as $C_1 \oplus C_2 = \{(c_1, c_2) : c_1 \in C_1, c_2 \in C_2)\}$, is not generally a good construction. As an example, the binary codes $C_1 = \{0\}$ and $C_2 = \{1\}$ have unidirectional covering radius 1, whereas the direct sum $C_1 \oplus C_2$ is not a unidirectional covering code for any positive R. However, when either C_1 or C_2 contains all words of the ambient space, we get the following result.

Theorem 3.1: If $C \subseteq Z_2^n$ has unidirectional covering radius R, then $C \oplus Z_2^m$ has unidirectional covering radius R.

Proof: Consider an arbitrary word $x = (x_1, x_2)$, where $x_1 \in Z_2^n$ and $x_2 \in Z_2^m$. Then there exists a codeword $c \in C$ that covers x_1 with unidirectional covering radius R, so $(c, x_2) \in C \oplus Z_2^m$ covers (x_1, x_2) with unidirectional covering radius R. □

Corollary 3.2: $E(n+1,R) \leq 2E(n,R)$.

The following results for small codes are straightforward.

Proposition 3.3: The code $C = \{00\ldots0\}$ attains $E(n,R) = 1, n \leq R$. The code $C = \{00\ldots0, 11\ldots1\}$ attains $E(n,R) = 2, \lfloor \frac{n}{2} \rfloor \leq R < n$.

By Proposition 3.3 and Corollary 3.2, we have $E(2R+3,R) \leq 8$. In fact, it turns out that $E(2R+3,R) = 8$ for $R > 1$; the rest of this section is devoted to proving this bound. Before proceeding, we need the following definition. A code $C \subseteq Z_2^n$ is said to be s-surjective if for any set of s coordinates $a_1, a_2, \ldots, a_s$ of C and any s-tuple $(b_1, b_2, \ldots, b_s) \in Z_2^s$ there is a codeword $(c_1, c_2, \ldots, c_n) \in C$ such that $c_{a_i} = b_i$ for $1 \leq i \leq s$. The proof of the following theorem is analogous to that of [18, Theorem 5].

Theorem 3.4: If there exists a code attaining $E(n+2, R+1)$ that is not 2-surjective, then $E(n,R) \leq E(n+2, R+1)$.

Proof: Let C be a code attaining $E(n+2, R+1)$ that is not 2-surjective. Without loss of generality, assume that C is not 2-surjective in the last two coordinates and that $b \in Z_2^2$ does not occur in those coordinates. Removing the last two coordinates of C gives a code C'. If C' would have unidirectional covering radius $R+1$, with $a \in Z_2^n$ being a word that is not R-covered by any $c' \in C'$, then $(a,b) \in Z_2^{n+2}$ would not be $(R+1)$-covered by any $c \in C$. Hence C' has unidirectional covering radius at most R. □

Theorem 3.5: $E(2R+3,R) = 8$ for $R > 1$.

Proof: By Proposition 3.3 and Corollary 3.2, we have $E(2R+3,R) \leq 8$ for all R. The result $E(7,2) = 8$ can be settled via the corresponding instance of IP_{exact}.

Assume that there is an $R > 2$ such that $E(2R+3,R) < 8$, and consider the smallest such value of R. Obviously, the corresponding code must be 2-surjective, because otherwise we can use Theorem 3.4 to arrive at an even smaller value of R. By a well-known result by Kleitman and Spencer [19, Theorem 1], which implies that binary 2-surjective codes with length greater than $\binom{M-1}{\lfloor M/2 \rfloor - 1}$ do not exist for size M, it follows that such codes of size 7 do not exist for lengths $n > 15$, that is, $R > 6$. The covering radii of small binary 2-surjective codes of size 7 are investigated in [20]. Since the unidirectional covering radius of a code is at least as big as its covering radius, it follows from the results in [20, Table I] that there are no binary 2-surjective codes of size 7, length $2R+3$, and unidirectional covering radius R for $3 \leq R \leq 6$. Hence we have a contradiction. □

IV. Upper Bounds Using Tabu Search

The promising results in [10], [21] inspired us to apply tabu search in the search for good unidirectional covering codes. Tabu search is a local search method for combinatorial optimization, in which all the solutions in the neighborhood of the current solution are inspected and the most promising one is selected, even if it is worse than the current solution. The search continues until a good enough solution is found or the search has taken too long. A so-called tabu list is used to prevent the search from re-inspecting solutions that have already been tried (recently). For more information on tabu search the reader is referred to [22].

We let the cost of a solution be the number of words in the space that are not covered, so a unidirectional covering code corresponds to zero cost. The search starts from a—random or specified—initial solution, and the number of codewords is kept constant during the search. It turned out that the initial solution often had a substantial impact on the success of the search. In one approach a (suboptimal) code was constructed by Theorem 3.1 and then a random codeword was removed to get the initial solution. When the search was completed successfully, a codeword was removed randomly from the solution and the search was performed again.

TABLE III
Bounds on $E(n,R)$ for $n \leq 13, R \leq 6$

$n \backslash R$	1	2	3	4	5	6
1	1					
2	2	1				
3	2	2	1			
4	4	2	2	1		
5	7	2	2	2	1	
6	12	4	2	2	2	1
7	16	$_o$8	2	2	2	2
8	32	$_o$14*	4	2	2	2
9	62	$_e$21–24*	$_t$8	2	2	2
10	107–120	$_e$32–36*	$_e$14–15*	4	2	2
11	180–192	$_e$53–68*	$_e$21–26*	$_t$8	2	2
12	342–380	$_e$91–126*	$_e$32–44*	$_e$14–15*	4	2
13	598–704	$_e$157–240*	$_e$48–74*	$_e$20–26*	$_t$8	2

Many details of the algorithm used are analogous to those in [21]. The neighborhood is constructed with respect to a fixed uncovered word (to find this uncovered word, one goes through the words in lexicographic order, starting from the word considered in the previous step of the algorithm). Any alteration of a codeword $c \in C$ to a word $c' \notin C$ is in the neighborhood if c' covers the uncovered word. If the codeword c was altered during the last T iterations, it cannot be altered, that is, it is in the tabu list, unless the result would be a unidirectional covering code.

The algorithm terminates when a unidirectional covering code is encountered or when the algorithm has proceeded L steps without improving the best solution (that is, which has the least number of uncovered words) found so far.

V. Results

Exact values of and best known lower and upper bounds on $E(n,R)$ for $n \leq 13$ are listed in Table III. The values for $R \geq 7$ follow from Proposition 3.3 and are omitted. Note that the entries for $R = 1$ coincide with those of covering codes [23]. The other unmarked entities follow from Proposition 3.3 and Corollary 3.2. The subscripts for the lower bound are as follows: "o" for IPexact, "e" for exhaustive search, and "t" for Theorem 3.5. The unidirectional covering codes found by tabu search and corresponding to the starred bounds in Table III are distributed electronically at http://users.tkk.fi/~eseurane/papers/ucc/. The computations were carried out on a 1-GHz PC, and the total computing time for all results was less than two weeks.

Acknowledgment

The authors are grateful to the anonymous referees for their helpful comments and suggestions for improving the proofs.

References

[1] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North-Holland, 1997.

[2] T. Etzion, "New lower bounds for asymmetric and unidirectional codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 6, pp. 1696–1704, Nov. 1991. Correction in *IEEE Trans. Inf. Theory*, vol.38, no. 3, pp. 1183–1184, May 1992.

[3] T. Etzion and P. R. J. Östergård, "Greedy and heuristic algorithms for codes and colorings," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 382–388, Jan. 1998.

[4] G. Fang and H. C. A. van Tilborg, "Bounds and constructions of asymmetric or unidirectional error-correcting codes," *Appl. Algebra Eng. Comm. Comput.*, vol. 3, pp. 269–300, 1992.

[5] J. H. Weber, C. de Vroedt, and D. E. Boekee, "Bounds and constructions for binary codes of length less than 24 and asymmetric distance less than 6," *IEEE Trans. Inf. Theory*, vol. 34, no. 5, pp. 1321–1331, Sep. 1988.

[6] D. K. Ray-Chaudhuri, N. M. Singhi, S. Sanyal, and P. S. Subramanian, "Theory and design of t-unidirectional error-correcting and d-unidirectional error-detecting code," *IEEE Trans. Comput.*, vol. 43, no. 10, pp. 1221–1226, Oct. 1994.
[7] J. H. Weber, C. de Vroedt, and D. E. Boekee, "Bounds and constructions for codes correcting unidirectional errors," *IEEE Trans. Inf. Theory*, vol. 35, no. 4, pp. 797–810, Jul. 1989.
[8] D. Applegate, E. M. Rains, and N. J. A. Sloane, "On asymmetric coverings and covering numbers," *J. Combin. Des.*, vol. 11, pp. 218–228, 2003.
[9] J. N. Cooper, R. B. Ellis, and A. B. Kahng, "Asymmetric binary covering codes," *J. Combin. Theory Ser. A*, vol. 100, pp. 232–249, 2002.
[10] P. R. J. Östergård and E. A. Seuranen, "Constructing asymmetric covering codes by tabu search," *J. Combin. Math. Combin. Comput.*, vol. 51, pp. 165–173, 2004.
[11] M. Krivelevich, B. Sudakov, and V. H. Vu, "Covering codes with improved density," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1812–1815, Jul. 2003.
[12] GLPK (GNU Linear Programming Kit). [Online]. Available: http://www.gnu.org/software/glpk
[13] R. G. Stanton and J. G. Kalbfleisch, "Covering problems for dichotomized matchings," *Aequationes Math.*, vol. 1, pp. 94–103, 1968.
[14] B. D. McKay, "nauty User's Guide (Version 1.5)," Comp. Sci. Depat., Australian Nat. Univ., Canberra, Tech. Rep. TR-CS-90-02, 1990.
[15] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2373–2395, Nov. 2000.
[16] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1334–1380, Nov. 1990.
[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[18] G. Cohen, A. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inf. Theory*, vol. IT-32, no. 5, pp. 680–694, Sep. 1986.
[19] D. J. Kleitman and J. Spencer, "Families of k-independent sets," *Discr. Math.*, vol. 6, pp. 255–262, 1973.
[20] G. Kéri and P. R. J. Östergård, "Further Results on the covering Radius of Small Codes," Labo. Operations Res. and Decision Syst., Computer and Automation Inst., Hungarian Acad. Sciences, Budapest, Hungary, Rep. WP 2004-1, 2004.
[21] P. R. J. Östergård, "Constructing covering codes by tabu search," *J. Combin. Des.*, vol. 5, pp. 71–80, 1997.
[22] A. Hertz, E. Taillard, and D. de Werra, "Tabu search," in *Local Search in Combinatorial Optimization*, E. Aarts and J. K. Lenstra, Eds. Chichester, U.K.: Wiley, 1997, pp. 121–136.
[23] R. Bertolo, P. R. J. Östergård, and W. D. Weakley, "An updated table of binary/ternary mixed covering codes," *J. Combin. Des.*, vol. 12, pp. 157–176, 2004.

Convolutional Goppa Codes

J. M. Muñoz Porras, *Member, IEEE*, J. A. Domínguez Pérez, J. I. Iglesias Curto, and G. Serrano Sotelo

***Abstract*—In this correspondence, we define convolutional Goppa codes over algebraic curves and construct their corresponding dual codes. Examples over the projective line and over elliptic curves are described, obtaining in particular some maximum-distance separable (MDS) convolutional codes.**

***Index Terms*—Algebraic curves, convolutional codes, finite fields, Goppa codes, maximum-distance separable (MDS) codes.**

I. Introduction

Goppa codes are evaluation codes for linear series over smooth curves over a finite field $\mathbb{F}_q$. Using Forney's algebraic theory of convolutional codes [1] (see also [2, Ch. 2] and [3]), in [4], we proposed a new construction of convolutional codes, which we called convolutional Goppa codes (CGC), in terms of evaluation along sections of a family of algebraic curves.

The aim of this correspondence is to reformulate the results of [4] in a straightforward language. In Section II, we define CGC as Goppa codes for smooth curves defined over the field $\mathbb{F}_q(z)$ of rational functions in one variable z over the finite field $\mathbb{F}_q$. These CGC are in fact more general than the codes defined in [4], since there are smooth curves over $\mathbb{F}_q(z)$ that do not extend to a family of smooth curves over the affine line $\mathbb{A}^1_{\mathbb{F}_q}$. With this definition, one has another advantage: the techniques of algebraic geometry required are easier than those used in [4]: we use exactly the same language as is usual in the literature on Goppa codes. Section III is devoted to define the dual CGC.

Section IV contains the definition of free distance for a convolutional code together with some remarks about the geometric interpretation of the Hamming weight for Goppa codes and the weight for CGC.

The last two sections of the correspondence are devoted to illustrating the general construction with some examples. In Section V we construct several CGC of genus zero; that is, defined in terms of the projective line $\mathbb{P}^1_k$ over the field $\mathbb{F}_q(z)$. Some of these examples are MDS-convolutional codes and are very easy to handle.

In Section VI, we give examples of CGC of genus one; that is, defined in terms of elliptic curves over $\mathbb{F}_q(z)$. These examples are not so easy to study. In fact, a consequence of this preliminary study of CGC of genus one is that a deeper understanding of the arithmetic properties of elliptic fibrations (see, for instance, [5]) and of the translation of these properties into the language of convolutional codes is necessary.

In the Appendix, we propose a way to obtain a geometric interpretation of the weight for CGC.

II. Convolutional Goppa Codes

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_q(z)$ the (infinite) field of rational functions of one variable. Let $(X, \mathcal{O}_X)$ be a smooth projective curve over $\mathbb{F}_q(z)$ of genus g.

Manuscript received October 14, 2003; revised November 12, 2004. This work was supported in part by the Spanish DGESYC through research Project BMF2000-1327 and by the "Junta de Castilla y León" through research Projects SA009/01 and SA032/02.

The authors are with the Department of Mathematics, University of Salamanca, 37008 Salamanca, Spain (e-mail: jmp@usal.es; jadoming@usal.es; joseig@usal.es; laina@usal.es).

Communicated by K. A. S. Abdel-Ghaffar, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2005.860447