Publication III

Esa A. Seuranen and Patric R. J. Östergård. 2006. New lower bounds for asymmetric covering codes. Congressus Numerantium, volume 178, pages 57-63.

New Lower Bounds for Asymmetric Covering Codes

Esa A. Seuranen and Patric R. J. Östergård
Department of Electrical and Communications Engineering
Helsinki University of Technology
P.O. Box 3000, 02015 TKK, Finland
E-mail: {esa.seuranen,patric.ostergard}@tkk.fi

Abstract

A code $C \subseteq Z_2^n$, where $Z_2 = \{0, 1\}$, has asymmetric covering radius R if R is the smallest integer such that any word $v \in Z_2^n$ can be obtained from at least one codeword $c \in C$ by replacing 1s by 0s in at most R coordinates. The minimum cardinality of such a code is denoted by $D(n, R)$. In this paper we apply exhaustive search and integer programming to obtain several new lower bounds on $D(n, R)$. The best known lower bounds on $D(n, R)$ for $n \leq 13$ and $R \leq 10$ are tabulated.

1 Introduction

Covering codes have been studied extensively—see [4] and its references—the main motivations being football pools and data compression. Recently a variant of covering codes, *asymmetric covering codes*, has received some attention [2,5,6,8,11]. A code $C \subseteq Z_2^n$, where $Z_2 = \{0, 1\}$, has asymmetric covering radius R if R is the smallest integer such that for every *word* $v \in Z_2^n$ there is a *codeword* $c \in C$, so that c can be transformed into v by changing at most R 1s into 0s (we say that c *covers* v). The minimum cardinality of such a code is denoted by $D(n, R)$.

In this paper we mainly use techniques presented in [12]—integer programming and exhaustive search—with minor modifications to obtain new lower bounds on $D(n, R)$.

Integer programming problems discussed in this paper were solved with GLPK [7] and isomorphism computations were carried out using *nauty* [10].

2 Applied Techniques

Determining the minimum cardinality of asymmetric covering codes can be formulated directly as an integer programming problem [2]:

$$\begin{aligned} \text{Min } Z &= \sum_{i=0}^{2^n-1} b_i \\ \text{Subject To:} & \\ 1 &\leq \sum_{j \in S(i)} b_j, \text{ where } 0 \leq i < 2^n \\ b_i &\in \{0,1\}, \text{ where } 0 \leq i < 2^n, \end{aligned}$$

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.

We need some results from [12] (see the reference for the proofs). 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 that $0 \leq w - w' \leq R$, this function does not depend on the asymmetric covering radius R. Let $A(n,d,w)$ denote the maximum number of codewords in a code with length n, minimum distance d, and constant weight w; see [1,3,9] for extensive results on this function.

Theorem 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* $v(n,k,w,w') < k \cdot v(n,1,w,w')$.

Theorem 2 $v(n,k+1,w,w') \leq \frac{k+1}{k} \cdot v(n,k,w,w')$ *for* $0 \leq w' \leq w \leq n$ *and* $k \geq 1$.

Theorem 3 *For* $0 \leq w' \leq w \leq n$, *let* $k = A(n, 2(w-w'+1), w) + i$ *with* $i \geq 1$. *Then* $v(n,k,w,w') \leq k \cdot v(n,1,w,w') - i$.

Exhaustive search, analogous to the search in [12], can be used both to determine values of $v(n,k,w,w')$ and to improve lower bounds on $D(n,R)$, providing the necessary computation is feasible.

Upper bounds on $v(n,k,w,w')$ can be obtained by Theorems 1–3. Exact values for small parameters can be determined by generating all possible constant weight codes with k codewords of weight w by adding one codeword at a time—i.e., the codes with j codewords are generated from the codes with $j-1$ codewords—and pruning isomorphic codes.

Lower bounds on $D(n,R)$ can be improved as follows: for a given cardinality of the code, all possible weight distributions are checked one by

one to see whether asymmetric covering codes corresponding to the weight distributions exist. The cardinality is assumed to be the best known lower bound on $D(n, R)$, and hence the objective is to improve the bound by one. The construction of codes is done again by adding one codeword at a time according to the weight distribution under inspection. The search tree is pruned if a generated code is isomorphic to a code generated earlier or if it cannot lead—$v(n, k, w, w')$ can be used to get an upper bound on the coverage of the unfixed codewords—to a desired asymmetric covering code.

An upper bound on the number of codewords with weight w' in an asymmetric covering code with cardinality M, assuming that such a code exists, can be obtained with the following integer programming problem (analogous to $\mathrm{IP}^*_{\mathrm{sphere}}$ in [12]):

$$\begin{aligned}
\text{Max } Z &= s_{w'} \\
\text{Subject To:} & \\
\binom{n}{w} &\leq \sum_{\substack{r=0 \\ 0 \leq w+r \leq n}}^{R} s_{w+r} \binom{w+r}{r}, \text{ where } 0 \leq w \leq n \\
s_w &\in \left\{0, 1, 2, \ldots, \binom{n}{w}\right\}, \text{ where } 0 \leq w \leq n \\
M &= \sum_{w=0}^{n} s_w,
\end{aligned}$$

where s_w represents the number of codewords with weight w. We shall use the notation last(w') for $s_{w'}$ in what follows.

A bound for asymmetric covering codes was obtained in [5, Proposition 16.1], which we restate here. Let $\phi(n, R)$ denote the maximum total number of zeroes the codewords of a code attaining $D(n, R)$ can contain.

Theorem 4 $D(n, R) \geq D(n-1, R) + \lceil \phi(n, R)/n \rceil$.

We can use the following integer programming problem for obtaining a lower bound on the total number of zeros of the codewords with the further assumption that M is the cardinality of the code:

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

Subject To:

$$\binom{n}{w} \leq \sum_{r=0}^{R} \sum_{k=1}^{\text{last}(w+r)} v(n,k,w+r,w) \cdot s_{w+k,j}, \text{ where } 0 \leq w \leq n$$

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

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

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

where $s_{w,k} = 1$ if there are exactly k codewords of weight w, and $s_{w,k} = 0$ otherwise.

We introduce the notation $\phi(n, R, M)$ for the maximum total number of zeroes the codewords of a code with length n, asymmetric covering radius R, and cardinality M can contain. If $M < D(n, R)$, then we let $\phi(n, R, M) = \infty$. Obviously, $\phi(n, R, D(n, R)) = \phi(n, R)$. The proof of the following theorem follows that of [5, Proposition 16.1] (Theorem 4 here).

Theorem 5 *If* $D(n-1, R) + \lfloor \phi(n, R, M)/n \rfloor > M$, *then* $D(n, R) > M$.

For given values of n and R, we solve the integer programming problem above with M being the best known lower bound on $D(n, R)$. The result is a lower bound on $\phi(n, R, M)$, which is applied to Theorem 5 to see if we can improve the lower bound on $D(n, R)$ by 1. If that is the case, we repeat the process once again with M increased by 1. It is tempting to conjecture that the result of the integer programming problem could be used to improve the lower bound on $D(n, R)$ by more than 1—with Theorem 5 in a form similar to that of 4—but monotonicity of the solutions of the integer programming problem above with respect to the value of M is an open problem.

In the column New of Table 1, we list the lower bounds on $\lceil \phi(n, R, M)/n \rceil$ obtained that can be used to get new lower bounds on $D(n, R)$ by Theorem 5. For comparison, the lower bounds on $\lceil \phi(n, R)/n \rceil$ obtained by [5, Proposition 17] are shown in the column Old. As previously discussed, in some cases the result builds on calculating lower bounds on $\lceil \phi(n, R, M)/n \rceil$ for several consecutive values of M; only the entry for the last M in this sequence is listed in the table.

n	R	M	New	Old	n	R	M	New	Old
9	1	100	43	41	12	1	584	264	257
9	2	34	13	12	12	2	155	63	61
9	3	17	6	5	12	3	62	22	20
10	1	178	78	75	12	5	16	5	4
10	2	56	22	20	13	1	1078	494	483
10	3	26	9	8	13	2	265	110	106
11	1	320	142	138	13	3	97	35	33
11	2	92	36	35					
11	3	40	14	12					
11	4	19	6	5					

Table 1: Results for the auxiliary function

3 Results

The best known lower bounds on $D(n, R)$ for $1 \leq n \leq 13$, $1 \leq R \leq 10$ are tabulated in Table 2. An entry marked with a period is an exact value. Unmarked entries were established in [5]—either directly or by Theorem 4 with [5, Proposition 17]. The subscripts have the following meanings: *a*) the bound was obtained in [2]; *b*) the bound was obtained in this study by solving the integer programming problem in the beginning of Section 2; *c*) the bound was shown in this study by exhaustive search (Section 2); and *d*) the bound follows from Theorem 5 and the results in Table 1.

As a conclusion, in total 26 new lower bounds on $D(n, R)$ were obtained with six of them being exact values.

Acknowledgements

This research was supported by the Academy of Finland under Grants No. 100500, No. 107493 and No. 110196.

References

[1] E. Agrell, A. Vardy, and K. Zeger, Upper bounds for constant-weight codes, *IEEE Trans. Inform. Theory* **46** (2000), 2373–2395.

[2] D. Applegate, E. M. Rains, and N. J. A. Sloane, On asymmetric coverings and covering numbers, *J. Combin. Des.* **11** (2003), 218–228.

$n\backslash R$	1	2	3	4	5	6	7	8	9	10
1	1.									
2	2.	1.								
3	3.	2.	1.							
4	6.	3.	2.	1.						
5	10.	5.	3.	2.	1.					
6	18.	8.	4.	3.	2.	1.				
7	$_a$31.	$_b$14.	$_b$7.	4.	3.	2.	1.			
8	$_a$58.	$_c$22	$_c$12.	6.	4.	3.	2.	1.		
9	$_d$101	$_d$35	$_d$18	$_c$10.	6.	4.	3.	2.	1.	
10	$_d$179	$_d$57	$_d$27	14	$_c$8.	5.	4.	3.	2.	1.
11	$_d$321	$_d$93	$_d$41	$_d$20	$_c$12	$_c$8.	5.	4.	3.	2.
12	$_d$585	$_d$156	$_d$63	29	$_d$17	11	7.	5.	4.	3.
13	$_d$1079	$_d$266	$_d$98	43	24	15	$_c$10	7.	5.	4.

Table 2: Best known lower bounds on $D(n, R)$

[3] A. E. Brouwer, J.B. Shearer, N. J. A. Sloane, and W. D. Smith, A new table of constant weight codes, *IEEE Trans. Inform. Theory* **36** (1990), 1334–1380.

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

[5] J. N. Cooper, R. B. Ellis, and A. B. Kahng, Asymmetric binary covering codes, *J. Combin. Theory Ser. A* **100** (2002), 232–249.

[6] G. Exoo. Upper bounds for optimal asymmetric covering codes [electronic], available at (originally published 2003) <URL:`http://isu.indstate.edu/ge/COMBIN/ACODES/`>.

[7] GLPK (GNU Linear Programming Kit) [electronic], available at <UTL:`http://www.gnu.org/software/glpk/`>.

[8] M. Krivelevich, B. Sudakov, and V. H. Vu, Covering codes with improved density, *IEEE Trans. Inform. Theory* **49** (2003), 1812–1815.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[10] B. D. McKay, *nauty* user's guide (version 1.5), Computer Science Department, Australian National University, Tech. Report TR-CS-90-02, 1990.

[11] P. R. J. Östergård and E. A. Seuranen, Constructing asymmetric covering codes by tabu search, *J. Combin. Math. Combin. Comput.* **51** (2004), 165–173.

[12] P. R. J. Östergård and E. A. Seuranen, Unidirectional covering codes, *IEEE Trans. Inform. Theory* **52** (2006), 336–340.