Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Journal of Combinatorial Theory, Series A 104 (2003) 365–370

Journal of Combinatorial Theory Series A

http://www.elsevier.com/locate/jcta

Note

$K_5(7,3) \leqslant 100$

Guillaume Gommard and Alain Plagne

LIX, École polytechnique, F-91128 Palaiseau Cedex, France

Received 14 July 2003

Communicated by Jacobus van Lint

Abstract

One of the main aims in the theory of covering codes is to obtain good estimates on $K_q(n,R)$, the minimal cardinality of an R-covering code over the nth power of an alphabet with q elements. This paper reports on the new bound $K_5(7,3) \leqslant 100$, obtained by an improved computer search based on Östergård and Weakley's method. In particular, the code leading to this bound has a group of automorphisms quite different from the one Östergård and Weakley used. This new upper bound significantly improves the former record (which was 125).

MSC: primary 94B60

Keywords: Covering code; Group of automorphisms; Simulated annealing

1. Introduction

In the field of covering codes, one of the main questions is the determination of $K_q(n,R)$ which is defined as the minimal cardinality of an R-covering code over the nth power of an alphabet with cardinality q.

More formally, let us consider an alphabet with q elements, that we denote by $\mathbb{Z}_q$ (and that we sometimes see as the cyclic group with q elements, for convenience). If n is a positive integer, we define the Hamming distance between two elements in $\mathbb{Z}_q^n$, $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$, as

$$\mathrm{d}(\mathbf{x},\mathbf{y}) = |\{i \in \mathbb{N}, 1 \leqslant i \leqslant n : x_i \neq y_i\}|.$$

E-mail addresses: guillaume.gommard@polytechnique.org (G. Gommard), plagne@lix.polytechnique.fr (A. Plagne).

0097-3165/$ - see front matter
doi:10.1016/j.jcta.2003.08.004

In this metric space, the ball with center $\mathbf{x}$ and radius r is classically defined as $\{\mathbf{y}\in\mathbb{Z}_q^n : \mathrm{d}(\mathbf{x},\mathbf{y})\leqslant r\}$. Let now R be a positive integer. A subset $\mathscr{C}$ of $\mathbb{Z}_q^n$ is said to be an R-covering code if the union of the balls centered at the elements of $\mathscr{C}$ covers the whole space. Equivalently, $\mathscr{C}$ is an R-covering code if for any element in $\mathbb{Z}_q^n$, there exists an element in $\mathscr{C}$ at a distance less than or equal to R. With these notations, $K_q(n,R)$ is the minimal cardinality of any R-covering code in $\mathbb{Z}_q^n$.

Computing exactly $K_q(n,R)$ is, in general, a difficult problem. Except in the case when the parameters (q, n and R) of the code are all very small and some special cases (perfect codes), we only know lower and upper bounds. While lower bounds are usually obtained using theoretical arguments based on improved versions of the so-called sphere covering bound, upper bounds are obtained by constructions.

Some powerful construction methods are based on computer local search methods like simulated annealing, tabu search or genetic algorithms [1]. All these methods which exist in a more general context have been successfully applied in the context of covering codes. To be more precise, simulated annealing (which is the more popular method) has been used for instance in [5,7,9,10,13–15], to quote a few; tabu search in [8,10]; genetic algorithms in [12].

The most studied (main) cases correspond to small values of the parameters, namely $q\leqslant 5, n\leqslant 33, R\leqslant 10$. Any improved method for obtaining bounds on $K_q(n,R)$ is usually tested on these very cases which have thus been widely investigated. However, larger q can also be of interest (see [4]). The book [3], which is the most complete reference on covering codes, concentrates on the above-mentioned main cases: the tables it contains on bounds for $K_q(n,R)$ (at the end of Chapter 6) are limited to $q=2$, $n\leqslant 33, R\leqslant 10$, $q=3$, $n\leqslant 14, R\leqslant 8$, $q=4$, $n\leqslant 10, R\leqslant 6$ and $q=5$, $n\leqslant 9, R\leqslant 6$. Note that several bounds have already been improved with respect to the tables given in [3].

In the case $q=5$, $n=7$, $R=3$, it is currently known that

$$30\leqslant K_5(7,3)\leqslant 125.$$

The lower bound follows from the sphere-covering bound while the upper bound follows from $K_5(7,3)\leqslant 5K_5(6,3)$ and $K_5(6,3)\leqslant 25$ (proved in [6]).

In this paper, we improve the upper bound $K_5(7,3)\leqslant 125$.

Theorem 1. *One has*

$$K_5(7,3)\leqslant 100.$$

This result has been obtained by an improved local search, based on an idea of Östergård and Weakley. Basically, this idea consists in imposing some additional structural properties to the code we are looking for.

In Section 2, we give the list of codewords establishing Theorem 1. In Section 3, we recall Östergård and Weakley's method and explain how we started from it to get our new bound.

2. The proof

To prove our theorem, it is enough to give a list of 100 codewords which 3-cover the whole space. In this section, for simplicity, the word $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ will be simply denoted by $x_1\ x_2\ \cdots\ x_n$.

Let us define $\mathscr{C}_1$ to be the code

1304200 4103121 2142302 2034133 1402434 0130420
2410311 0214232 3203413 3140244 2013040 1241031
3021422 1320343 4314024 4201300 3124101 2302142
4132033 2431404 0420130 0312411 4230212 3413203
0243144 3042010 1031241 1423022 0341323 4024314,

$\mathscr{C}_2$ to be

4223000 3341101 4022142 1332003 4431124 0422300
0334111 4402212 0133203 2443114 0042230 1033411
1440222 0013323 1244314 3004220 1103341 2144022
2001333 1124434 2300420 4110331 2214402 3200133
3112444 2230040 3411031 0221442 3320013 4311244,

$\mathscr{C}_3$ to be

2434310 0404231 0103412 2140213 2013234 1243430
3040421 1010342 1214023 3201324 3124340 2304041
4101032 2121403 2320134 4312430 4230401 3410102
0212143 3232014 3431240 0423041 0341012 4021213
1323204 4343120 4042301 1034102 1402123 0132324,

$\mathscr{C}_4$ to be

1111110 2222221 3333332 4444443 0000004,

and finally $\mathscr{C}_5$ to be

0000000 1111111 2222222 3333333 4444444.

If $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2 \cup \mathscr{C}_3 \cup \mathscr{C}_4 \cup \mathscr{C}_5$, then it is easily checked that $\mathscr{C}$ is a 3-covering code on $\mathbb{Z}_5^7$ and that $|\mathscr{C}| = |\mathscr{C}_1| + |\mathscr{C}_2| + |\mathscr{C}_3| + |\mathscr{C}_4| + |\mathscr{C}_5| = 30 + 30 + 30 + 5 + 5 = 100$. This proves Theorem 1.

As we will see later, the partition of $\mathscr{C}$ into the five subsets $(\mathscr{C}_i)_{1 \leqslant i \leqslant 5}$ corresponds in fact to a structure of $\mathscr{C}$. The $(\mathscr{C}_i)_{1 \leqslant i \leqslant 5}$ are five orbits under the action of the group of automorphisms we used.

3. Where does the proof come from?

Let us start by exposing Östergård and Weakley's work [11] on searching for good covering codes. These authors noticed that classical computer search could be improved if one imposes some kind of structure to the code.

They only considered codes which are sent into themselves under the action of a given group of automorphisms G. Once G is fixed, the method consists of partitioning the ambient space into orbits under the action of G. It proceeds with constructing a graph whose vertices are the orbits, and where two vertices $\mathscr{O}_1$ and $\mathscr{O}_2$ are adjacent if there are elements $\mathbf{o_1} \in \mathscr{O}_1, \mathbf{o}_2 \in \mathscr{O}_2$ such that $\mathrm{d}(\mathbf{o_1}, \mathbf{o}_2) \leqslant R$. This construction has an interesting property: if $\mathscr{S}$ is a subset of orbits such that any orbit not in $\mathscr{S}$ is adjacent to $\mathscr{S}$ (such an $\mathscr{S}$ is called a covering of the graph), then $\bigcup_{\mathscr{O} \in \mathscr{S}} \mathscr{O}$ is an R-covering code on $\mathbb{Z}_q^n$. Therefore, if the orbits' cardinalities are large, it considerably reduces the algorithmical complexity of the problem. The method ends by approaching the solutions of the reduced problem. In [11], a computer search using tabu is used to select a good set of orbits.

A basic feature in Östergård and Weakley's method is to fix the group G according to what seems to be (and even sometimes is) the best choice in small dimensions. In this work, we first tried to improve the method of these authors by trying several different groups G: we actually only imposed that G is generated by *one* or *two* elements. This seems to be the most reasonable choice because we need G not too large (to obtain a number of orbits not too small). With this restriction, the computer randomly chose automorphisms. Then, the method explained in the next paragraph was applied with corresponding groups G.

Once G was fixed, we tried to completely solve the reduced problem, when it was possible. To do so, we used either a basic branch and bound algorithm, or CPLEX (a combinatorial optimization solver). Branch and bound can be used when the tree to explore is not too deep; in particular, a way of restricting the research is to backtrack when the code's cardinality becomes greater than the best known upper bound of $K_q(n, R)$.

When it was not possible to find the exact solution, we used a simulated annealing algorithm. Just like Östergård and Weakley, we first fix how many orbits of each cardinality we want to select; this repartition is chosen so that the cardinalities' sum is less than the best known upper bound of $K_q(n, R)$. The simulated annealing begins with a given temperature T. At each program's step, we consider a neighbor of the orbits' set by replacing an orbit with an adjacent one of the same cardinality. If this neighbor covers more orbits than the former set, it is automatically accepted. If it covers p orbits less, it is accepted with probability $\exp(-p/T)$. To end the step, the temperature is multiplied by a constant $\chi \in]0, 1[$. Moreover, we *repeat* the simulated annealing: when T gets under a given bound, we change χ into $2 - \chi$ in order to warm the system; this warming ends when T becomes high enough, we then begin the simulated annealing again. It leads to a repetition of cooling and warming steps, which very often gives good results.

Finally, once we have a solution (or *the* solution) for the reduced problem, we consider the result-code and delete one of its points; then we start a simulated annealing from the obtained code. We continue reducing the code while the simulated annealing finds covering codes. This last step allows to find smaller covering codes, starting from codes stable for automorphisms.

Due to the enormous computational means needed by such a research program, we decided to restrict ourselves to "small" codes i.e. those with small parameters. In several cases that we experimented, this method led to the same upper bound as the one which was known to be the best. The main case on which we worked was the case $q = 5$, $n = 7$ and $R = 3$ for which we could prove the improvement given by Theorem 1.

We first tried Östergård and Weakley's group of automorphisms which led us to the bound 105.

The bound 100 that we finally could prove was obtained with a group of automorphisms *not* of the form used by Östergård and Weakley. In the case under study, the computer could find a group which gave a better result. Indeed, the bound 100 was computed with the group G generated by one element, namely (recall that $\mathbb{Z}_5$ can be seen as the cyclic group with five elements)

$$\sigma : \left| \begin{array}{ccc} \mathbb{Z}_5^7 & \to & \mathbb{Z}_5^7 \\ (x_1, x_2, \ldots, x_6, x_7) & \mapsto & (x_2 + 1, x_3 + 1, \ldots, x_6 + 1, x_1 + 1, x_7 + 1). \end{array} \right.$$

In other words, σ can be seen as the composition of a cyclic permutation of the six first coordinates and the translation $x \to x + 1$ (where 1 is the all-one word). Under the action of G, the space $\mathbb{Z}_5^7$ is partitioned into 2635 orbits, namely 2580 with cardinality 30, 40 with cardinality 15, 10 with cardinality 10 and 5 with cardinality 5. Therefore, we decided to look for a code of size 100, with 3 orbits with cardinality 30 and 2 with cardinality 5. Our computer search revealed that such a choice was possible with the orbits $\mathscr{C}_1, \mathscr{C}_2, \mathscr{C}_3, \mathscr{C}_4$ and $\mathscr{C}_5$ given in Section 2.

We finish with two remarks on G, the group generated by σ, which were pointed out by the referee. First, we may notice that this group (which, again, was found randomly) differs only slightly from that of [11]: in that paper, (a conjugate of) the group of use is also generated by one single element of the same form as σ, but with a different length for the cycle in the permutation. Secondly, similar groups have been prescribed in [2] for the dual problem of finding good 5-ary error-correcting codes.

Acknowledgments

We are grateful to the UMS Medicis, École polytechnique, for providing us with powerful computational resources. We used a free version of CPLEX for which we thank ILOG. Finally, we thank Patric Östergård for providing us with several papers and preprints and the referee for useful remarks.

References

[1] E.H.L. Aarts, P.J.M. van Laarhoven, Local search in coding theory, Discrete Math. 106/107 (1992) 11–18.
[2] G.T. Bogdanova, P.R.J. Östergård, Bounds on codes over an alphabet of five elements, Discrete Math. 240 (2001) 13–19.
[3] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, Covering Codes, Elsevier, Amsterdam, 1997.
[4] G. Kéri, P.R.J. Östergård, Bounds for covering codes over large alphabets, preprint, 2003.
[5] P.J.M. van Laarhoven, E.H.L. Aarts, J.H. van Lint, L.T. Wille, New upper bounds for the football pool problem for 6, 7, and 8 matches, J. Combin. Theory Ser. A 52 (1989) 304–312.
[6] P.R.J. Östergård, Upper bounds for q-ary covering codes, IEEE Trans. Inform. Theory 37 (1991) 660–664.
[7] P.R.J. Östergård, New upper bounds for the football pool problem for 11 and 12 matches, J. Combin. Theory Ser. A 67 (1994) 161–168.
[8] P.R.J. Östergård, Constructing covering codes by tabu search, J. Combin. Des. 5 (1997) 71–80.
[9] P.R.J. Östergård, New constructions for q-ary covering codes, Ars Combin. 52 (1999) 51–63.
[10] P.R.J. Östergård, M.K. Kaikkonen, New upper bounds for binary covering codes, Discrete Math. 178 (1998) 165–179.
[11] P.R.J. Östergård, W.D. Weakley, Constructing covering codes with given automorphisms, Des. Codes Cryptogr. 16 (1999) 65–73.
[12] R.J.M. Vaessens, E.H.L. Aarts, J.H. van Lint, Genetic algorithms in coding theory—a table for $A_3(n,d)$, Discrete Appl. Math. 45 (1993) 71–87.
[13] L.T. Wille, The football pool problem for 6 matches: a new upper bound obtained by simulated annealing, J. Combin. Theory Ser. A 45 (1987) 171–177.
[14] L.T. Wille, Improved binary code coverings by simulated annealing, Congr. Numer. 73 (1990) 53–58.
[15] L.T. Wille, New binary covering codes obtained by simulated annealing, IEEE Trans. Inform. Theory 42 (1996) 300–302.