Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 177-180*

Colored superimposed codes[1]

Vladimir Lebedev lebed37@iitp.ru
Institute for Information Transmission Problems, Moscow, RUSSIA

1 Introduction

One of the most important applications of (w, r) superimposed codes (see, [1] - [3]) is the following cryptography problem. There are T users and N secret keys. Each user has his own set of keys, and a group of users can communicate if there exists a common secret key for the whole group. It is required that, for any group of w users and any group of other r users, there should exist a key such that all users of the first group have this key and thus can communicate, while neither of the r users of the second group possess this key. Thus, users of the first group can exchange information "secretly" from users of the second group.

Now assume that all users have the same set of keys, but any key has several states. Let all keys have the same numbers of the states. A user can not change key's state and the user can communicate with users who have the key with this state. There are several groups of users (the number of the groups is not more then the number of the key's states). We want that there is a key such that for any group of users the key has the same state (and for different groups - different states) and so the users from any group can communicate secretly from users of other groups.

This situation can naturally be thought of as a q-ary $N \times T$ matrix $C = \|c_{ij}\|$, where $c_{ij} = k$ if the jth user possesses the ith secret key with the state k. Then the property described above means that, for any subsets $R_0, R_1, \ldots, R_{q-1} \subset [T]$ of cardinalities $|R_s| = r_s$, there exists a row i in C such that $c_{ij} = s$ for all j from R_s, where $s = 0, 1, \ldots, q-1$. We will refer to the matrix as $(r_0, r_1, \ldots, r_{q-1})$ superimposed code or colored superimposed code.

Of course, we would like to minimize the number of secret keys with a fixed number of users, or, equivalently, maximize the number of users with a fixed number of keys. Thus, the problem consists in finding a matrix C that obeys this property, with the number of columns as large as possible (rows are of length N). We will often refer to columns of C as codewords and refer to the

[1]Supported in part by the Russian Foundation for Basic Research, project no. 06-01-00226.

matrix C itself as a q-ary code. Furthermore, in what follows, we use the term "code of size $N \times T$" rather than the more commonly used "code of length N and cardinality T."

Denote by $N(T, r_0, r_1, \ldots, r_{q-1})$ the minimum possible length of a $(r_0, r_1, \ldots, r_{q-1})$ superimposed code of a given cardinality T. A colored code is optimal if $N = N(T, r_0, r_1, \ldots, r_{q-1})$. The rate of a q-ary code of length N and cardinality T is, as usual, $R = (\log T)/N$. We are interested in the asymptotic behavior of the rate

$$R(r_0, r_1, \ldots, r_{q-1}) = \limsup_{T \to \infty} \frac{\log_q T}{N(T, r_0, r_1, \ldots, r_{q-1})}$$

of such (optimal) codes.

2 Some results

Let us start with the formal definition of $(r_0, r_1, \ldots, r_{q-1})$ superimposed codes.

Definition 1. *A q-ary $N \times T$ matrix $C = \|c_{ij}\|$ is called a $(r_0, r_1, \ldots, r_{q-1})$* superimposed code of size $N \times T$ *if, for any disjoint subsets $R_0, R_1, \ldots, R_{q-1} \subset [T]$ of cardinalities $|R_s| = r_s$, there exists a coordinate $i \in [N]$ such that $c_{ij} = s$ for all $j \in R_s$, where $s = 0, 1, \ldots, q-1$.*

Theorem 1. *For colored superimposed codes we have*

$$R(r_0, r_1, \ldots, r_{q-1}) \geq 1/(S-1) \log_q \frac{S^S}{S^S - r_0^{r_0} r_1^{r_1} \ldots r_{q-1}^{r_{q-1}}},$$

where $S = (r_0 + r_1 + \ldots + r_{q-1})$.

The next important parameter will be defined for an arbitrary q-ary code C of size $N \times T$. Consider positive integers $(x_0, x_1, \ldots, x_{q-1})$. Fix a collection I consisting of $X = x_0 + x_1 + \ldots + x_{q-1}$ codewords and denote by $C_X(I)$ the submatrix of C formed by these codewords. Thus, the matrix $C_X(I)$ is of size $N \times X$. By the "X-distance" for the collection I, we call the number of rows of $C_X(I)$ such that each row has x_s elements with value s for all s, where $s = 0, 1, \ldots, q-1$. We denote this number by $d(C_X(I))$.

Definition 2. *The* minimum "X-distance" *for a q-ary code C is the value $d_X = \min_{|I|=X} d(C_X(I))$. Denote by $R^{(N)}(d_X)$ the rate of a q-ary code of length N with minimum "X-distance" d_X.*

Theorem 2. *For q-ary code C of length N with minimum "X-distance" d_X we have the following asymptotic bound:*

$$R^{(N)}(d_X) \le (1 - \frac{X^X x_0! x_1! \dots x_{q-1}!}{x_0^{x_0} x_1^{x_1} \dots x_{q-1}^{x_{q-1}} X!} \frac{d_X}{N})(1 - \log_q(q-1)).$$

The following lemma explains the relation between the parameter d_X and $(r_0, r_1, \dots, r_{q-1})$ superimposed codes.

Lemma. *If a $(r_0, r_1, \dots, r_{q-1})$ superimposed code C of size $N \times T$ exists, then a $(r_0 - x_0, r_1 - x_1, \dots, r_{q-1} - x_{q-1})$ superimposed code of size*

$$\lfloor d_X x_0! x_1! \dots x_{q-1}! / X! \rfloor \times (T - X).$$

exists.

Corollary. *If there exists a $(r_0, r_1, \dots, r_{q-1})$ superimposed code C of cardinality T with minimum "X-distance" d_X, then, for positive integers x_s ($x_s < r_s$), we have*

$$N(T - X, r_0 - x_0, r_1 - x_1, \dots, r_{q-1} - x_{q-1}) \le \frac{d_X x_0! x_1! \dots x_{q-1}!}{X!}.$$

Theorem 3. *For the rate of $(r_0, r_1, \dots, r_{q-1})$ superimposed codes, we have the asymptotic bound:*

$$R(r_0, r_1, \dots, r_{q-1}) \le \frac{R(r_0 - x_0, r_1 - x_1, \dots, r_{q-1} - x_{q-1})}{R(r_0 - x_0, \dots, r_{q-1} - x_{q-1})/(1 - \log_q(q-1)) + X^X/(x_0^{x_0} \dots x_{q-1}^{x_{q-1}})}.$$

Proof. Consider an optimal $(r_0, r_1, \dots, r_{q-1})$ superimposed code of cardinality T, length $N(T, r_0, r_1, \dots, r_{q-1})$, and rate $R_T(r_0, r_1, \dots, r_{q-1})$. Theorem 2 implies that, as $T \to \infty$

$$R_T(r_0, r_1, \dots, r_{q-1}) \le 1 - \frac{X^X d_X x_0! x_1! \dots x_{q-1}!}{x_0^{x_0} x_1^{x_1} \dots x_{q-1}^{x_{q-1}} X! N(T, r_0, r_1, \dots, r_{q-1})})(1 - \log_q(q-1)) + o(1)$$

Using the corollary of the lemma, we get

$$R_T(r_0, r_1, \ldots, r_{q-1}) \leq$$
$$(1 - \frac{X^X N(T - X, r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1})}{x_0^{x_0} x_1^{x_1} \ldots x_{q-1}^{x_{q-1}} N(T, r_0, r_1, \ldots, r_{q-1})})(1 - \log_q(q-1)) + o(1).$$

Let us apply Definition 2 of $R_{T-X}(r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1})$ and pass to the limit as $T \to \infty$ on both sides of the above inequality. As a result, we get a recurrence inequality for the rate $R(r_0, r_1, \ldots, r_{q-1})$, which can be written as

$$R(r_0, r_1, \ldots, r_{q-1})(1 + \frac{X^X(1 - \log_q(q-1))}{x_0^{x_0} x_1^{x_1} \ldots x_{q-1}^{x_{q-1}} R(r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1})})$$
$$\leq 1 - \log_q(q-1).$$

From this inequality, the statement of the theorem follows.

References

[1] C. J. Mitchell, F. C. Piper, Key storage in secure networks, *Discr. Appl. Math.* 21, 1988, 215-228.

[2] H. K. Kim, V. Lebedev, On optimal superimposed codes, *J. Combin. Des.* 12, 2004, 79-91.

[3] A. D'yachkov, A. Macula, V. Torney, P. Vilenkin, Families of finite sets in which no intersection of l sets is covered by the union of s others, *J. Combin. Theory* Ser. A. 99, 2002, 195-218.

[4] D. R. Stinson, R. Wei, L. Zhu, Some new bounds for cover-free families, *J. Combin. Theory* Ser. A. 90, 2000, 224-234.

[5] A. D'yachkov, P. Vilenkin, S. Yekhanin, Upper bounds on the rate of superimposed (s, l)-codes based on Engel's inequality, *Proc. Eighth Intern. Workshop ACCT*, Tsarskoe Selo, Russia, 2002, 95-99.

[6] V. S. Lebedev, Some tables for (w, r) superimposed codes, *Proc. Eighth Intern. Workshop ACCT*, Tsarskoe Selo, Russia, 2002, 185-189.

[7] V. S. Lebedev, New asymptotic upper bound on the rate of (w, r) cover free codes, *Probl. Inform. Transm.* 39, 2003, 317-323.