Cover-Free Families and Superimposed Codes: Constructions, Bounds, and Applications to Cryptography and Group Testing

Arkadii D'yachkov Vladimir Lebedev Pavel Vilenkin Sergei Yekhanin

Abstract — **This paper deals with (s,ℓ)-*cover-free families* or *superimposed* (s,ℓ)*-codes*. They generalize the concept of superimposed s-codes and have several applications for cryptography and group testing. We present a new asymptotic bound on the rate of optimal codes and develop some constructions.**

I. Definitions

Let $X = \|x_i(j)\|$ be a binary matrix with N rows and t columns, $i = 1,\dots,N$, $j = 1,\dots,t$. We consider X as a binary code of length N and size t with columns as codewords. Let s and ℓ be positive integers, $s+\ell \le t$. A matrix X is called a *superimposed* (s,ℓ)*-code* if for any two sets of columns $S, L \subset [t] = \{1,2,\dots,t\}$ such that $|S| = s$, $|L| = \ell$, and $S \cap L = \emptyset$, there exists a row $i \in [N]$ such that $x_i(j) = 1$ for all $j \in L$ and $x_i(j') = 0$ for all $j' \in S$.

For the special case $\ell = 1$ superimposed codes were introduced in [1] and studied in many papers [2, 4, 8, 9, 13]. Superimposed (s,ℓ)-codes are the natural generalization of this concept which is closely connected with cover-free families.

Superimposed codes have several applications: the problem of nonadaptive search for positive supersets [9, 10, 12, 13], the problem of key storage in secure networks [3, 6, 12, 13], ets.

Denote by $N(t,s,\ell)$ the smallest length of a superimposed (s,ℓ)-code having size t. Let $R(s,\ell)$ be the rate function of these codes, i.e., $R(s,\ell) = \limsup_{t\to\infty} (\log_2 t)/N(t,s,\ell)$.

II. Asymptotic Bounds on $R(s,\ell)$

Theorem 1 [10, 13]. *If $s \to \infty$ and $\ell = \text{const}$ then the following asymptotic inequalities hold*

$$\frac{\ell^\ell e^{-\ell}\log_2 e}{s^{\ell+1}}(1+\bar{o}(1)) \le R(s,\ell) \le \frac{(\ell+1)!\log_2 s}{s^{\ell+1}}(1+\bar{o}(1)).$$

For the case $\ell = 1$, these bounds coincide with the best known bounds which can be found in [2, 4]. Some upper bounds are also proved in [6, 7, 11]. Some of them are non-asymptotic, i.e., true for all values of s and ℓ. In [7] one can find an upper bound that is better then our bound when $s \approx \ell$. In [11] one can find a non-asymptotic upper bound in a simple form. The asymptotic form of this bound looks like our bound but contains $2\ell \cdot \ell!$ instead of $(\ell+1)!$.

III. Constructions of Superimposed (s,ℓ)-codes

A simple construction of superimposed codes is based on concatenated codes. It was considered in [5, 8, 9, 10, 13]. To apply it, we need *large* q-ary separating codes [5, 10, 13] and *small* (having size q) binary superimposed codes. Some q-ary separating codes can be obtained from MDS-codes [5, 10, 13]. Using Reed-Solomon codes we can obtain the following constructive result which is formulated in terms of upper bound on $N(t,s,\ell)$.

Theorem [5, 10, 13]. *Let s, ℓ, and λ be positive integers and $q \ge s\ell\lambda$ be a prime power. Then* $N(q^{\lambda+1},s,\ell) \le N(q,s,\ell)[s\ell\lambda+1]$.

Finally, we need to have a number of small (having size q) superimposed codes. For the special case $s = \ell = 2$ the table of such codes can be found in [5]. In [10, 13] and the present work we improve this table. Our method is based on the difference sets and cyclic constructions.

[1]A. D'yachkov, P. Vilenkin, and S. Yekhanin are with the Moscow State University, Moscow, Russia (dyachkov@mech.math.msu.su, paul@vilenkin.dnttm.ru, gamov@cityline.ru). V. Lebedev is with the Institute of Information Transmission Problems, Moscow, Russia (lebed@iitp.ru).

[2]This work was partly supported by the Russian RFBR grant N. 01-01-00495 and the INTAS-00-738 grant.

References

[1] W.H. Kautz, R.C. Singleton, "Nonrandom Binary Superimposed Codes," *IEEE Trans. Inform. Theory*, vol IT-10, no. 3, pp. 363-377, 1964.

[2] A. G. D'yachkov, V. V. Rykov, "Bounds on the Length of Disjunct Codes," *Problemy Peredachi Informatsii*, vol. 18, no. 3, pp. 7–13, 1982 (in Russian).

[3] C. J. Mitchel, F. C. Piper, "Key Storage in Secure Networks," *Discrete Appl. Math.* vol. 21, pp. 215–228, 1988.

[4] A. G. D'yachkov, V. V. Rykov, A. M. Rashad, "Superimposed Distance Codes," *Problems of Control and Inform. Theory*, vol. 18, no. 4, pp. 237–250, 1989.

[5] Yu. L. Sagalovich, "Separating Systems," *Problemy Peredachi Informatsii*, vol. 30, no. 2, pp. 14–35, 1994 (in Russian).

[6] M. Dyer, T. Fenner, A. Frieze, A. Thomason, "On key storage in secure networks," *J. Cryptology*, vol. 8, pp. 189–200, 1995.

[7] K. Engel, "Interval packing and covering in the boolean lattice," *Combin. Probab. Comput.*, vol. 5, pp. 373–384, 1996.

[8] A. G. D'yachkov, A. J. Macula, V. V. Rykov, "New Constructions of Superimposed Codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 284–290, 2000.

[9] A. G. D'yachkov, A. J. Macula, V. V. Rykov, New Applications and Results of Superimposed Code Theory Arising from the Potentialities of Molecular Biology. In the book: Numbers, Information and Complexity, pp. 265–282, Kluwer Academic Publishers, 2000.

[10] A. G. D'yachkov, A. J. Macula, D. C. Torney, P. A. Vilenkin, S. M. Yekhanin, "New Results in the Theory of Superimposed Codes," *Proceedings of ACCT-7*, Bansko, Bulgaria, 2000, pp. 126–136.

[11] D. R. Stinson, R. Wei, L. Zhu, "Some New Bounds for Cover-Free Families," *J. Combin. Theory Ser. A*, vol. 90, pp. 224–234, 2000.

[12] D. R. Stinson, Tran van Trung, R. Wei, "Secure Frameproof Codes, Key Distribution Patterns, Group Testing Algorithms and Related Structures," available at http://cacr.math.uwaterloo.ca/ dstinson.

[13] P. A. Vilenkin, Asymptotic Problems of Combinatorial Coding Theory and Information Theory. Ph.D. dissertation, Moscow State University, 2001.