Kim, Hyun Kwang; **Lebedev, Vladimir**
On optimal superimposed codes. (English) Zbl 1051.94013
J. Comb. Des. 12, No. 2, 79-91 (2004).

A family of subsets of a finite set is called (w, r) cover-free if no intersection of w members of the family is contained in the union of r others [cf. *D. R. Stinson, L. Zhu* and *R. Wei*, J. Comb. Theory, Ser. A 90, 224–234 (2000; Zbl 0948.05055) and *A. D'yachkov, A. Macula, D. Torney* and *P. Vilenkin*, ibid. 99, 195–218 (2002; Zbl 1020.94027)]. Equivalent concepts are that of (binary) (w, r) superimposed codes (they are given by the incidence matrices of (w, r) cover-free families) and of (w, r) key distribution patterns for cryptography.

The authors develop methods of constructing (w, r) superimposed codes using combinatorial designs and 3-covering arrays and prove that some of the $(2, 2)$ and $(2, 3)$ superimposed codes found by their methods are optimal. To get good superimposed codes of large size, they concatenate algebraic-geometric codes with a (w, r) superimposed code; thus they obtain a sequence of (w, r) superimposed codes of positive asymptotic rate.

Reviewer: Ralph-Hardo Schulz (Berlin)

MSC:

94B25 Combinatorial codes
05D05 Extremal set theory
94A60 Cryptography
05B05 Combinatorial aspects of block designs
05B40 Combinatorial aspects of packing and covering

Keywords:

cover-free family; superimposed code; key distribution pattern; super-simple design; covering array; mutually orthogonal latin squares, MOLS; t-design; concatenation; algebraic geometric code

Full Text: DOI

References:

[1] Adams, Aequationes Mathematicae 51 pp 230– (1995)

[2] Alon, Discrete Math 58 pp 191– (1986)

[3] Chateauneuf, J Combin Designs 10 pp 217– (2002)

[4] Chen, J Statistical Planning Infer 51 pp 339– (1996)

[5] Chen, J Combin Math Combin Comput 17 pp 149– (1995)

[6] Chor, IEEE Transactions Inform Theory 46 pp 893– (2000)

[7] Cohen, IEEE Transactions Infor Theory 40 pp 1872– (1994)

[8] and Intersecting codes and identifying codes, Proc Intern Workshop Coding Cryptography, January 8-12, 2001, Paris (France), pp. 139-147.

[9] and CRC Handbook Combin Designs CRC Press, Inc., 1996.· doi:10.1201/9781420049954

[10] and Combinatorial group testing and its applications, World Scientific, Singapore, New Jersey, London, Hong Kong, 1993. · Zbl 0867.90060

[11] D'yachkov, Problemy Peredachi Informatsii 18 pp 7– (1982)

[12] D'yachkov, Problems Control Inform Theory 12 pp 229– (1983)

[13] D'yachkov, Problems Control Inform Theory 18 pp 237– (1989)

[14] D'yachkov, IEEE Trans Inform Theory 46 (2000)

[15] and New applications and results of superimposed code theory arising from the potentialities of molecular biology, Numbers, Inform Complexity, Kluwer Academic Publishers, 2000, pp. 265-282. · Zbl 1034.94015

[16] and New results in the theory of superimposed codes, Seventh International Workshop Algebraic Combin Coding Theory, June 18-24, 2000, Bansko (Bulgaria), pp. 126-136.

[17] D'yachkov, J Combin Theory, Series A 99 pp 195– (2002)

[18] Dyer, J Cryptol 8 pp 189– (1995)

[19] Erdos, J Combin Theory 33 pp 158– (1982)

[20] Erdos, Israel J Math 51 pp 75– (1985)

[21] Gronau, J Combin Math Combin Comput 11 pp 113– (1992)

[22] Kautz, IEEE Trans Inform Theory IT-10 pp 363– (1964)

[23] Korner, J Combin Theory, Series A 71 pp 112– (1995)

[24] and The Theory of error-correcting codes, North Holland, 1983.

[25] Mago, IEEE Trans Comput 22 pp 928– (1973)

[26] Mitchell, Discrete Applied Math 21 pp 215– (1988)

[27] O'Keefe, Designs Codes Cryptography 5 pp 261– (1995)

[28] Quinn, Designs, Codes Cryptography 4 pp 177– (1994)

[29] Quinn, J Cryptology 12 pp 227– (1999)

[30] Sagalovich, Probl Inform Transmission 30 pp 105– (1994)

[31] Sagalovich, Problemy Peredachi Informatsii 18 pp 74– (1982)

[32] Sloane, J Combin Designs 1 pp 51– (1993)

[33] Stinson, Designs, Codes Cryptography 12 pp 215– (1997)

[34] Stinson, J Combin Designs 8 pp 189– (2000)

[35] Stinson, J Combin Theory Ser A 90 pp 224– (2000)

[36] Stinson, key distribution patterns, group testing algorithms and related structures, J Stat Planning Infer 86 pp 595– (2000) · Zbl 1054.94013

[37] Tsfasmann, Discrete Applied Math 33 pp 241– (1991)

[38] Wang, J Combin Theory Ser A 93 pp 112– (2001)