ISSN 0032-9460, Problems of Information Transmission, 2009, Vol. 45, No. 1, pp. 32–36. © Pleiades Publishing, Inc., 2009.
Original Russian Text © V.M. Sidelnikov, O.Yu. Prikhodov, 2009, published in Problemy Peredachi Informatsii, 2009, Vol. 45, No. 1, pp. 36–40.

CODING THEORY

On the Construction of (w, r) Cover-Free Codes[1]

V. M. Sidelnikov[†2] **and O. Yu. Prikhodov**[†]

Received December 8, 2006

Abstract—We construct a new class of concatenated cover-free codes. We prove that in this class there exists a sequence of (w, r) cover-free codes which has a nonzero limit rate for $w, r = \text{const}$. We consider application of cover-free codes to key distribution systems.

DOI: 10.1134/S0032946009010049

1. INTRODUCTION

We say that a family of sets is (w, r) cover-free if no union of w sets of the family is covered by a union of any other r sets of the same family. Here is a formal definition.

Definition 1. Let $w \geq 1$ and $r \geq 0$ be integers. A collection $A = \{A_1, \ldots, A_T\}$ of subsets of the set $[N] = \{1, \ldots, N\}$ is called a (w, r) *cover-free family* if for any two sets of indices $L, M \subseteq [T]$ such that $L \cap M = \varnothing$, $|L| = w$, and $|M| = r$, we have

$$\bigcap_{\ell \in L} A_\ell \nsubseteq \bigcup_{m \in M} A_m. \tag{1}$$

In particular, for $r = 0$ we have

$$\bigcap_{s=1}^{w} A_{\ell_s} \neq \varnothing \quad \text{for any set} \quad \{\ell_1, \ldots, \ell_w\} \subseteq [T]. \tag{2}$$

It is clear that if a family of sets is (w, r) cover-free, it is also (w', r') cover-free for all $w' \leq w$ and $r' \leq r$.

To a family of sets $\{A_1, \ldots, A_T\}$, we assign an $N \times T$ matrix $\mathcal{A} = (a_{ij})$ whose columns are characteristic vectors of the sets A_j, $j = 1, \ldots, T$. In other words, $a_{ij} = 1$ if $i \in A_j$ and $a_{ij} = 0$ otherwise. Then the above-given definition is equivalent to the fact that for any two disjoint sets of columns $L = \{\ell_1, \ldots, \ell_w\}$ and $M = \{m_1, \ldots, m_r\}$ there exists a row $\boldsymbol{a}_i$ of $\mathcal{A}$ such that $a_{i\ell_1} = \ldots = a_{i\ell_w} = 1$ and $a_{im_1} = \ldots = a_{im_r} = 0$. We refer to the set of columns of such a matrix as a (w, r) cover-free *code*. The parameters N and T are referred to as the code length and cardinality, respectively. This leads to the following definition.

Definition 2. A binary code $\mathcal{C}$ of length n is called a (w, r) *cover-free code* if for any two sets $X, Y \subset \mathcal{C}$ of code vectors such that $X \cap Y = \varnothing$, $|X| = w$, and $|Y| = r$ there exists at least one coordinate i such that

$$x_i = 1 \quad \text{for all} \quad x \in X \qquad \text{and} \qquad y_i = 0 \quad \text{for all} \quad y \in Y. \tag{3}$$

[1] The Editorial Board thanks G.A. Kabatiansky for final preparation of the text.

[2] Supported in part by the Russian Foundation for Basic Research, project nos. 05-01-01018 and 06-07-89170.

The study of (w, r) cover-free codes began in [1], where $(1, r)$ cover-free were introduced and investigated under the name of *superimposed codes* (in Russian literature, *disjunctive codes*). Superimposed codes were extensively studied (see [2, 3]). As areas of possible applications of cover-free codes, we mention construction of experimental designs and key distribution systems (see, e.g., [4, 5]).

Cover-free codes have much in common with separating codes. Recall the definition of separating codes (see the survey [6]).

Definition 3. A code $\mathcal{C}$ of length n over an alphabet of q elements is called a (w, r) *separating code* if for any two sets $X, Y \subset \mathcal{C}$ of code vectors such that $X \cap Y = \varnothing$, $|X| = w$, and $|Y| = r$ there exists at least one coordinate i that "separates" them, i.e.,

$$\{x_i : x \in X\} \cap \{y_i : y \in Y\} = \varnothing. \tag{4}$$

It is clear that a (w, r) separating code is also (w', r') separating for all $w' \le w$ and $r' \le r$.

A simple and, in fact, the only known sufficient condition for (w, r) separability is "large enough" code distance, namely,

$$\frac{d}{n} > 1 - \frac{1}{wr}. \tag{5}$$

To prove this condition, it suffices to consider the sum of pairwise distances between elements of two sets of code vectors $X, Y \subset \mathcal{C}$. If these two sets are not separated, then in each coordinate i there is at least one coincidence (intersection) between $\{x_i : x \in X\}$ and $\{y_i : y \in Y\}$, and hence the sum is not greater than $n(wr - 1)$; on the other hand, it is not less than dwr.

It is clear from the definition that for binary codes the separability condition is weaker, since it means existence of a coordinate i such that either $x_i = 1$ for all $x \in X$ and at the same time $y_i = 0$ for all $y \in Y$ or vice versa, $x_i = 1$ and $y_i = 0$ for all $x \in X$ and $y \in Y$, while the "cover-free condition" necessarily requires the first variant, and in the case $w = r$, both variants. Note that already in 1982 Yu.L. Sagalovich [7] considered (w, r) cover-free codes in the case where both parameters are greater than 1. Namely, he considered $(2, 2)$ cover-free codes, which he called completely separating codes, and compared them with binary $(2, 2)$ separating codes. What is especially important for the purposes of the present paper, he also proposed a concatenated construction for $(2, 2)$ cover-free codes based on an outer code with only the property of $(2, 2)$ separability and an inner $(2, 2)$ cover-free code. Later, this construction was many times re-discovered for the general (w, r) case. In the present paper, we propose a modification of the concatenated construction with a new family of inner codes.

2. CONCATENATED CONSTRUCTION

Recall the concatenated construction. Consider a code $\mathcal{C}$ of length n over an alphabet A of q elements and a binary code $\mathcal{A}$ of length N and cardinality q. Let $\psi\colon A \to \mathcal{A}$ be a one-to-one correspondence between the alphabet A and the code $\mathcal{A}$. To a q-ary vector $c \in \mathcal{C}$, assign a binary vector $\Psi(c) = (\psi(c_1), \ldots, \psi(c_n))$ by replacing in the vector $c = (c_1, \ldots, c_n)$ its q-ary coordinates with the corresponding vectors of $\mathcal{A}$. This results in a binary code of length nN and cardinality $|\mathcal{C}|$, called a concatenated code. The codes $\mathcal{C}$ and $\mathcal{A}$ are referred to as the outer and inner code of the concatenated code, respectively. We enumerate coordinates of the concatenated code by ordered pairs (i, j) with $i \in [n]$ and $j \in [N]$.

The following result is well known (see, e.g., [7, 8]). We present a proof since this will help us to explain our modification.

Theorem 1. *A concatenated code with an inner (w, r) cover-free code $\mathcal{A}$ and an outer $|\mathcal{A}|$-ary (w, r) separating code $\mathcal{C}$ is a (w, r) cover-free code.*

Proof. According to the definition, consider two arbitrary disjoint sets of vectors X and Y of the concatenated code with $|X| = w$ and $|Y| = r$, and denote by $X^{(C)}$ and $Y^{(C)}$ the corresponding sets of vectors of the outer code. Since the outer code $\mathcal{C}$ is (w, r) separating, there exists a coordinate i such that $\{x_i : x \in X^{(C)}\} \cap \{y_i : y \in Y^{(C)}\} = \varnothing$. Consider the corresponding *disjoint* sets of vectors of the inner code: $X^{(A)} = \{\psi(x_i) : x \in X^{(C)}\}$ and $Y^{(A)} = \{\psi(y_i) : y \in Y^{(C)}\}$. Since $|X^{(A)}| \le |X^{(C)}| = w$ and $|Y^{(A)}| \le |Y^{(C)}| = r$ and since the code $\mathcal{A}$ is (w, r) cover-free, there exists a coordinate j such that $\psi(x_i)_j = 1$ for all $x \in X$ and $\psi(y_i)_j = 0$ for all $y \in Y$. Hence, (i, j) is the desired coordinate for the concatenated code. $\triangle$

We make a simple but important remark on the proof of Theorem 1. It is clear that the sum of cardinalities of the disjoint subsets $X^{(A)}$ and $Y^{(A)}$ is not greater than the cardinality of the inner code. Therefore, the theorem remains valid if we replace the requirement that the binary inner code $\mathcal{A}$ is (w, r) cover-free with the following:

For any set of code vectors $X \subset \mathcal{A}$ with $|X| \le w$ there exists at least one coordinate i such that

$$x_i = 1 \quad \textit{for all} \quad x \in X \qquad \textit{and} \qquad y_i = 0 \quad \textit{for all} \quad y \in \mathcal{A} \setminus X. \tag{6}$$

We say, somewhat informally, that such a code is (w, ∞) *cover-free*.

Consider a code matrix $\mathcal{A}_{q,w}$ of size $N_{q,w} \times q$, where $N_{q,w} = \binom{q}{1} + \binom{q}{2} + \ldots + \binom{q}{w}$, whose rows are all the $N_{q,w}$ nonzero q-dimensional binary vectors of weight at most w. Obviously, it possesses this property (and in fact there are no other codes). Indeed, for an arbitrary set of code vector columns $X \subset \mathcal{A}_{q,w}$ such that $|X| \le w$, as a coordinate i we should take the coordinate for which the ith row is the characteristic vector of the set X. Here are two examples of such code matrices for the case of $w = 2$:

$$A_{2,2} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad A_{3,2} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{7}$$

Thus, we have the following theorem.

Theorem 2. *A concatenated code with the inner code $\mathcal{A}_{q,w}$ and an outer q-ary (w, r) separating code $\mathcal{C}$ is a (w, r) cover-free code.*

In particular, Theorem 2 yields explicit constructions of cover-free codes with an asymptotically nonzero rate R. For instance, one can take q-ary algebraic geometry (n, k) codes asymptotically meeting the TVZ bound (see [9])

$$\frac{d}{n} \ge 1 - \frac{k}{n} - \left(\sqrt{q} - 1\right)^{-1} + o(1) \tag{8}$$

as outer codes and choose q and k/n so that, first, $q \ge 49$, to satisfy the conditions of the TVZ bound, and second, $dn^{-1} > 1 - (wr)^{-1}$, to have an outer (w, r) separating code. Direct computation for the case of $w = 2$, which is most interesting for applications (see Section 3), leads to the following result.

Corollary. *For $q > \max\{48, (2r + 1)^2\}$, a concatenated code with the inner code $\mathcal{A}_{q,2}$ and an outer q-ary algebraic geometry code $\mathcal{C}$ meeting the TVZ bound* (8) *is a $(2, r)$ cover-free code with rate*

$$R \ge \left(\frac{1}{2r} - \frac{1}{\sqrt{q} - 1}\right) \frac{2 \log_2 q}{q(q + 1)} + o(1). \tag{9}$$

If one does not need to construct codes explicitly, it is possible to increase the final rate of (w, r) cover-free concatenated codes by taking random outer codes and using the corresponding existence bounds for (w, r) separating codes [10].

3. KEY DISTRIBUTION AND COVER-FREE CODES

Here we describe the well-known equivalence between cover-free families of sets (codes) and compromise-resistant key distribution systems (see [4, 5]). We confine ourselves to the case of $w = 2$, since the general case is considered similarly.

There is a set of users $\boldsymbol{T}$, $|\boldsymbol{T}| = T$, and a trusted center, which generates a set of independent secret keys $\boldsymbol{K} = \{k_1, \ldots, k_N\}$. The trusted center chooses a public (i.e., non-secret) family $\mathcal{A} = \{A_1, \ldots, A_T\}$ of subsets of $[N]$ and provides each user $j \in \boldsymbol{T}$ with a corresponding set of secret keys

$$\boldsymbol{K}_j = \{k_s \mid s \in A_j\} \subset \boldsymbol{K}, \tag{10}$$

which is used by user j to communicate with other users. Users i and j may use any common key $k \in \boldsymbol{K}_i \cap \boldsymbol{K}_j$ for communication with each other. A key distribution is said to be r-compromise-resistant if for any coalition M of at most r abusers, any (legal) pair i, j has at least one common key that is not contained in the union of keys of the abusers from this coalition. It is easily seen that this distribution is nothing else but the definition of a $(2, r)$ cover-free family of sets (code) $\mathcal{A}$.

Thus, the corollary of Theorem 2 yields an explicit construction of r-compromise-resistant key distribution systems with the number of keys of the order of the logarithm of the number of users. Another important parameter of a key distribution system is $\chi = \max\limits_{j \in \boldsymbol{T}} |\boldsymbol{K}_j|$, the maximum number of secret keys stored by users in their electronic memory; we call this number the complexity of a system (or of the corresponding code). Thus, the complexity (in our terms) of the code $\mathcal{A}_{q,w}$ is $\sum\limits_{i=0}^{w-1} \binom{q-1}{i} = 1 + N_{q-1,w-1}$, and the complexity of a concatenated code from Theorem 2 with the inner code $\mathcal{A}_{q,w}$ is not greater than $n(1 + N_{q-1,w-1})$, where n is the length of the outer (w, r) separating q-ary code. For applications of this type, it is natural to maximize the number of users T for a given χ.

REFERENCES

1. Kautz, W.H. and Singleton, R.C., Nonrandom Binary Superimposed Codes, *IEEE Trans. Inform. Theory*, 1964, vol. 10, no. 4, pp. 363–377.

2. D'yachkov, A.G. and Rykov, V.V., Bounds on the Length of Disjunctive Codes, *Probl. Peredachi Inf.*, 1982, vol. 18, no. 3, pp. 7–13 [*Probl. Inf. Trans.* (Engl. Transl.), 1982, vol. 18, no. 3, pp. 166–171].

3. Erdős, P., Frankl, F., and Füredi, F., Families of Finite Sets in Which No Set Is Covered by the Union of r Others, *Israel J. Math.*, 1985, vol. 51, no. 1–2, pp. 79–89.

4. Mitchell, C.J. and Piper, F.C., Key Storage in Secure Networks, *Discrete Appl. Math.*, 1988, vol. 21, no. 3, pp. 215–228.

5. Stinson, D.R., On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption, *Des. Codes Cryptogr.*, 1997, vol. 12, no. 3, pp. 215–243.

6. Sagalovich, Yu.L., Separating Systems, *Probl. Peredachi Inf.*, 1994, vol. 30, no. 2, pp. 14–35 [*Probl. Inf. Trans.* (Engl. Transl.), 1994, vol. 30, no. 2, pp. 105–123].

7. Sagalovich, Yu.L., Completely Separating Systems, *Probl. Peredachi Inf.*, 1982, vol. 18, no. 2, pp. 74–82 [*Probl. Inf. Trans.* (Engl. Transl.), 1982, vol. 18, no. 2, pp. 140–146].

8. Kim, H.K. and Lebedev, V.S., On Optimal Superimposed Codes, *J. Combin. Des.*, 2004, vol. 12, no. 2, pp. 79–91.

9. Vlăduţ, S.G., Nogin, D.Yu., and Tsfasman, M.A., *Algebrogeometricheskie kody. Osnovnye ponyatiya*, Moscow: MCCME, 2003. Translated under the title *Algebraic Geometry Codes. Basic Notions*, Providence: Amer. Math. Soc., 2007.

10. Cohen, G.D. and Schaathun, H.G., Separating Codes: Constructions and Bounds, *Proc. 6th Latin American Sympos. on Theoretical Informatics (LATIN 2004), Buenos Aires, Argentina, 2004*, Farach-Colton, M., Ed., Lect. Notes Comp. Sci., vol. 2976, Berlin: Springer, 2004, pp. 322–328.