New Results in the Theory of Superimposed Codes: Part I

A. D'yachkov[1], A. Macula[2], D. Torney[3], P. Vilenkin[1], S. Yekhanin[1]

Abstract — We introduce and discuss the concept of a binary superimposed (s, ℓ)-code identified by a family of finite sets in which no intersection of ℓ sets is covered by the union of s others. Upper and lower bounds on the rate of these codes are formulated. Their proofs will be given in [7]. Several constructions of these codes are considered in the second part of the present paper [6].

1 Notations and Definitions

In what follows, symbol $\triangleq$ denotes equalities by definition. For any positive integer n, we put $[n] \triangleq \{1, 2, \ldots, n\}$.

Let N and t be positive integers. Consider a set $\mathcal{C} \triangleq \{\mathbf{x}(1), \ldots, \mathbf{x}(t)\}$, composed of t mutually different binary vectors (codewords) of length N; $\mathbf{x}(j) = \big(x_1(j), \ldots, x_N(j)\big)$, $x_i(j) \in \{0, 1\}$, $j \in [t]$.

In what follows, we fix positive integers s and ℓ, such that $s + \ell \leq t$.

Definition 1. A set $\mathcal{C}$ is called a *superimposed* (s, ℓ)*-code* (or, briefly, (s, ℓ)*-code*) if for any two sets $\mathcal{S}, \mathcal{L} \subset [t]$, such that $|\mathcal{S}| = s$, $|\mathcal{L}| = \ell$ and $\mathcal{S} \cap \mathcal{L} = \varnothing$, these exists a position $i \in [N]$, for which $x_i(j) = 1$ for all $j \in \mathcal{L}$, and $x_i(j') = 0$ for all $j' \in \mathcal{S}$.

Integers N and t are called the *length* and *size* of code $\mathcal{C}$, respectively.

For the binary vectors $\mathbf{x} \triangleq (x_1, \ldots, x_N)$ and $\mathbf{y} \triangleq (y_1, \ldots, y_N)$, we consider the *disjunction* operation $\mathbf{x} \bigvee \mathbf{y}$ and *conjunction* operation $\mathbf{x} \bigwedge \mathbf{y}$ defined component-wise, where $0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1$,

[1]A. D'yachkov, P. Vilenkin and S. Yekhanin are with the Department of Probability Theory, Faculty of Mechanics & Mathematics, Moscow State University, Russia (dyachkov@mech.math.msu.su, paul@vilenkin.dnttm.ru, gamov@cityline.ru). Their work is supported by the Russian Foundation of Basic Research, grant 98–01–00241.

[2]A. Macula is with the Department of Mathematics, State University of New York, College at Geneseo, USA (macula@geneseo.edu). His work is supported by NSF Grant DMS–9973252.

[3]D. Torney is with the Theoretical Division T10, Los Alamos National Laboratories, USA (dct@lanl.gov). His work is supported by the US Department of Energy.

$0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0$, $1 \wedge 1 = 1$. We say that vector $\mathbf{x}$ *is covered* by vector $\mathbf{y}$ if $\mathbf{x} \bigvee \mathbf{y} = \mathbf{y}$.

Remark. Obviously, definition 1 is equivalent to the condition:

$$\bigwedge_{j \in \mathcal{L}} \mathbf{x}(j) \text{ is not covered by } \bigvee_{j' \in \mathcal{S}} \mathbf{x}(j').$$

An interpretation of an (s, ℓ)-code as a family of set with certain properties is given in "Part II" of the present paper [6].

Consider the collection $\mathcal{P}(s, \ell, t)$, composed of *supersets* p:

$$\mathcal{P}(s, \ell, t) \triangleq \left\{ \mathsf{p} = \{P_1, \ldots, P_k\} \ : \ 1 \le k \le s, \ \begin{array}{c} P_i \subset [t], \ |P_i| \le \ell, \\ P_i \not\subseteq P_{i'} \text{ for } i \ne i' \end{array} \right\}.$$

We call an element $\mathsf{p} \in \mathcal{P}(s, \ell, t)$ a *positive supersets*, and an element $P \in \mathsf{p}$ — a *positive set* in terms of superset p.

For a positive superset $\mathsf{p} \in \mathcal{P}(s, \ell, t)$ and a set $\mathcal{C} \triangleq \{\mathbf{x}(1), \ldots, \mathbf{x}(t)\}$ define the *output vector* $\mathbf{o} = \mathbf{o}(\mathsf{p}, \mathcal{C})$ as follows:

$$\mathbf{o}(\mathsf{p}, \mathcal{C}) \triangleq \bigvee_{P \in \mathsf{p}} \bigwedge_{j \in P} \mathbf{x}(j). \tag{1}$$

Definition 2. A set $\mathcal{C}$ is called a *superimposed (s, ℓ)-design* (or, briefly, *(s, ℓ)-design*), if $\mathbf{o}(\mathsf{p}_1, \mathcal{C}) \ne \mathbf{o}(\mathsf{p}_2, \mathcal{C})$ for any $\mathsf{p}_1, \mathsf{p}_2 \in \mathcal{P}(s, \ell, t)$, $\mathsf{p}_1 \ne \mathsf{p}_2$.

Proposition 1. [7] 1) *Any (s, ℓ)-code is an (s, ℓ)-design.* 2) *Any (s, ℓ)-design is an $(s - 1, \ell)$-code and an $(s, \ell - 1)$-code.*

2 Background and Motivations

For the special case $\ell = 1$, a superimposed $(s, 1)$-code ($(s, 1)$-design) is called a superimposed s-code (s-design). They were introduced in [1] and studied in [2, 3, 4]. See also the book [5].

Superimposed (s, ℓ)-codes and designs arise from the problem of group testing for supersets, which can be stated as follows. Assume that we have a set of t objects (we identify them by integers $j \in [t]$), in which several subsets $P_1, \ldots, P_k \subset [t]$ are *positive*. Assume that a number of positive subsets $k \le s$, and the size of each positive subset is not greater then ℓ. Our aim is to determine all positive subsets using a finite number of tests. In each test we take a group $G \subset [t]$ and examine it. The *test result* $r(G) = 1$ (*positive*) if $P_m \subseteq G$ for some $m \in [k]$, and $r(G) = 0$ (*negative*) otherwise.

Let $\mathbf{G} \triangleq (G_1, \ldots, G_N)$ be N testing groups. In the current model we use nonadaptive testing, which means that we select all groups before any test is performed. Let vector $\mathbf{r} = \mathbf{r}(\mathbf{G}) \triangleq (r(G_1), \ldots, r(G_N))$ represent the results of N tests.

Encode the testing groups by the set $\mathcal{C} = \{\mathbf{x}(1), \ldots, \mathbf{x}(t)\}$, where $x_i(j) = 1$ if element $j \in G_i$, and $x_i(j) = 0$ otherwise. Denote by p the superset composed of positive sets $P_1, \ldots, P_k$. Then one can see that the binary output vector $\mathbf{o}(\mathsf{p}, \mathcal{C}) = \mathbf{r}(\mathbf{G})$, see (1).

Our aim can be formulated as follows: construct a set $\mathcal{C}$ so that any *unknown* positive superset $\mathsf{p}^{\mathrm{un}} \in \mathcal{P}(s, \ell, t)$ could be determined (decoded) given the *known* output vector $\mathbf{o}^{\mathrm{kn}} = \mathbf{o}(\mathsf{p}^{\mathrm{un}}, \mathcal{C})$.

Obviously, it is possible if and only if the output vectors are different for any positive sets, i.e., if $\mathcal{C}$ is an (s, ℓ)-design (see definition 2). The decoding algorithm in general case has the following form: look over all supersets $\mathsf{p} \in \mathcal{P}(s, \ell, t)$, for each of them calculate the output vector $\mathbf{o}(\mathsf{p}', \mathcal{C})$ and compare it with the given vector $\mathbf{o}^{\mathrm{kn}}$. The decoding complexity of this algorithm is proportional to the size $|\mathcal{P}(s, \ell, t)| \sim t^{s\ell}/s!(\ell!)^s$, when $t \to \infty$, while s and ℓ are fixed.

Since any (s, ℓ)-code $\mathcal{C}$ is also an (s, ℓ)-design (proposition 1), it also can be used for decoding supersets. Moreover, in this case the following decoding algorithm can be used:

1. Look over all sets $P \subset [t]$, $|\mathcal{P}| \le \ell$, using increasing order of sizes, except those, which contain any positive set $P_m \in \mathsf{p}^{\mathrm{un}}$ of smaller size found before.

2. For each such set P calculate the output vector $\mathbf{o}(\{P\}, \mathcal{C})$.

3. P is positive set ($P \in \mathsf{p}^{\mathrm{un}}$) if and only if $\mathbf{o}(\{P\}, \mathcal{C})$ is covered by the given vector $\mathbf{o}^{\mathrm{kn}}$.

The decoding complexity of this algorithm is proportional to the number of such sets P, which is $\sim t^s/s!$, when $t \to \infty$, s and ℓ are fixed.

If $\ell = 1$, then each positive set P contains exactly one element, which is called the *positive element*. See [5] for the more detailed investigation of the group testing and its applications.

3 Properties of (s,ℓ)-codes

Denote by $N(t,s,\ell)$ and $N'(t,s,\ell)$ the minimum possible length of (s,ℓ)-code and (s,ℓ)-design of size t, respectively. Denote by $t(N,s,\ell)$ and $t'(N,s,\ell)$ the maximum possible size of (s,ℓ)-code and (s,ℓ)-design of length N, respectively.

Proposition 1 yields the inequalities

$$\begin{aligned} \max\big\{N(t,s-1,\ell), N(t,s,\ell-1)\big\} \le N'(t,s,\ell) \le N(t,s,\ell), \\ \min\big\{t(N,s-1,\ell), t(N,s,\ell-1)\big\} \ge t'(N,s,\ell) \ge t(N,s,\ell). \end{aligned}$$

Proposition 2. (Trivial (s,ℓ)-code). *Take an integer w, such that $\ell \le w \le t-s$. Put $N \triangleq \binom{t}{w}$ and consider a set of codewords $\mathcal{C}$, for which $\mathbf{x}_i \triangleq \big(x_i(1),\ldots,x_i(t)\big)$, $i \in [N]$, are all possible binary vectors of weight w. Then $\mathcal{C}$ is an (s,ℓ)-code and, therefore,*

$$N(t,s,\ell) \le \min\left\{\binom{t}{s},\binom{t}{\ell}\right\} = \binom{t}{\min\{s,\ell\}}. \tag{2}$$

If $t = s+\ell$, then this condition holds with the sign of equality.

Inequality (2) can be generalized as follows:

$$N(t,s,\ell) \le \min\left\{\binom{N(t,\ell,1)}{s},\binom{N(t,s,1)}{\ell}\right\}. \tag{3}$$

Inequality (2) follows from (3) and the trivial bound on the length of superimposed s-codes $N(t,s,1) \le t$. It also gives the way to construct (s,ℓ)-codes based on the s-codes, see “Part II” of the present paper [6].

Proposition 3. (Symmetry). *If $\mathcal{C}$ an (s,ℓ)-code, then a set $\overline{\mathcal{C}}$, which is obtained by replacing $0 \longleftrightarrow 1$ in $\mathcal{C}$, is an (ℓ,s)-code. Hence,*

$$N(t,s,\ell) = N(t,\ell,s), \quad t(N,s,\ell) = t(N,\ell,s).$$

4 Bounds on the Rate

For fixed $1 \le \ell \le s$, we define a *rate* of a superimposed (s,ℓ)-code

$$R(s,\ell) \triangleq \varlimsup_{N\to\infty} \frac{\log_2 t(N,s,\ell)}{N} = \varlimsup_{t\to\infty} \frac{\log_2 t}{N(t,s,\ell)}.$$

Proposition 3 yields the symmetry property of the rate: $R(s,\ell) = R(\ell, s)$. Taking this into account, in what follows we assume that $s \geq \ell$.

One can prove the following *trivial upper bound* on the rate:

$$R(s,\ell) \leq \frac{1}{s\ell}.$$

The better bound is obtained by the method which was used in [2] for the case $\ell = 1$. Consider the functions

$$h(p) \triangleq -p\log_2 p - (1-p)\log_2(1-p), \quad 0 < p < 1,$$
$$f_s(v) \triangleq h(v/s) - vh(1/s), \quad 0 < v < 1, \quad s > 1.$$

Proposition 4. [7] *For $s \geq \ell \geq 1$ the rate*

$$R(s,\ell) \leq \overline{R}(s,\ell) \triangleq \frac{1}{d(s,\ell)},$$

where $d(s,\ell)$ for $s \geq \ell \geq 1$ is defined recurrently:

- *if $\ell = 1$, then $d(1,1) \triangleq 1$, $d(2,1)$ has the form*

$$d(2,1) \triangleq \left[\max_{0 \leq v \leq 1} f_2(v)\right]^{-1} = f_2(0.4)^{-1} \approx 3.106,$$

  and for $s \geq 3$ the number $d(s,1)$ is the unique solution of the equation

$$d(s,1) = \left[f_s\left(1 - \frac{d(s-1,1)}{d(s,1)}\right)\right]^{-1}, \quad d(s,1) \geq d(s-1,1);$$

- *if $\ell \geq 2$, then for $s \geq \ell$*

$$d(s,\ell) \triangleq \sum_{k=1}^{s-\ell+1} d(s-k+1, \ell-1) + d(\ell, \ell-1).$$

The lower bound is obtained by the random coding method.

Proposition 5. [7] *For $s \geq \ell \geq 1$ the rate*

$$R(s,\ell) \geq \underline{R}(s,\ell) \triangleq \frac{\max\{E_1(s,\ell), E_2(s,\ell)\}}{s+\ell-1} > 0,$$

where

$$E_1(s,\ell) \triangleq -\log_2\left(1 - \frac{s^s \ell^\ell}{(s+\ell)^{s+\ell}}\right),$$

$$E_2(s,\ell) \triangleq \max_{q=2,3,\ldots} -\log_2\left(1 - \left(\frac{1}{q}\right)^{\ell-1}\left(1-\frac{1}{q}\right)^s\right) \Big/ q.$$

The asymptotic properties of the lower bound is given by

Proposition 6. *Let $s \to \infty$ and $\ell \geq 2$ be fixed. Then the lower bound*

$$\underline{R}(s,\ell) \sim \frac{\ell^\ell e^{-\ell}\log_2 e}{s^{\ell+1}}.$$

References

[1] W.H. Kautz, R.C. Singleton, "Nonrandom Binary Superimposed Codes," *IEEE Trans. Inform. Theory*, **4** (1964), 363–377.

[2] A. D'yachkov, V. Rykov, "Bounds on the Length of Disjunct Codes," *Problemy Peredachi Informatsii*, **3** (1982), 7–13, (in Russian).

[3] P. Erdos, P. Frankl, Z. Furedi, "Families of Finite Sets in which No Set Is Covered by the Union of r Others," *Israel Journal of Math.*, **1–2** (1985), 75–89.

[4] A. D'yachkov, V. Rykov, A.M. Rashad, "Superimposed Distance Codes," *Problems of Control and Inform. Theory*, **4** (1989), 237–250.

[5] D.-Z. Du, F.K. Hwang, *Combinatorial Group Testing and Its Applications,* World Scientific, Singapore-New Jersey-London-Hong Kong, 1993.

[6] A. D'yachkov, A. Macula, D. Torney, P. Vilenkin, S. Yekhanin, "New Results in the Theory of Superimposed Codes: Part II," *present volume.*

[7] A. D'yachkov, A. Macula, D. Torney, P. Vilenkin, "Families of Finite Sets in which No Intersection of ℓ Sets is Covered by the Union of s Others," *submitted for publication.*

New Results in the Theory of Superimposed Codes: Part II

A. D'yachkov[1], A. Macula[2], D. Torney[3], P. Vilenkin[1], S. Yekhanin[1]

Abstract — In the second part of the paper, we work out a constructive method for (s, ℓ)-codes [8] based on concatenated codes and MDS-codes [2, 3]. The method is a generalization of the constructive method for $(s, 1)$-codes [1, 6]. In addition, we discuss the constructions of the list-decoding superimposed codes [4, 7], identified by a family of finite sets in which no union of L sets is covered by the union of s others.

1 Notations and Definitions

We use notations and definitions from "Part I" of the present paper [8]. Let t and N be positive integers, and $\mathcal{C}$ be a set of t binary codewords of length N:

$$\mathcal{C} \triangleq \{\mathbf{x}(1), \ldots, \mathbf{x}(t)\}, \quad \mathbf{x}(j) \triangleq \big(x_1(j), \ldots, x_N(j)\big) \in \{0,1\}^N. \tag{4}$$

For any subset $\tau \subset [t]$ consider the disjunction and conjunction

$$\mathrm{V}(\tau) \triangleq \bigvee_{j \in \tau} \mathbf{x}(j), \quad \Lambda(\tau) \triangleq \bigwedge_{j \in \tau} \mathbf{x}(j). \tag{5}$$

For positive integers s and ℓ, such that $t \geq s + \ell$, put

$$\pi(s, \ell, t) \triangleq \big\{(\mathcal{S}, \mathcal{L}) \,:\, \mathcal{S}, \mathcal{L} \subset [t],\, |\mathcal{S}| = s,\, |\mathcal{L}| = \ell,\, \mathcal{S} \cap \mathcal{L} = \varnothing\big\}. \tag{6}$$

Definition 1 [8]. A *superimposed binary* (s, ℓ)*-code* of *length* N and *size* t is a set $\mathcal{C}$ (4), such that for any pair $(\mathcal{S}, \mathcal{L}) \in \pi(s, \ell, t)$ the vector $\Lambda(\mathcal{L})$ is not covered by $\mathrm{V}(\mathcal{S})$.

Definition 2. A *superimposed list-decoding code* of *strength* s and *list-size* L is a set $\mathcal{C}$ (4), such that for any pair $(\mathcal{S}, \mathcal{L}) \in \pi(s, L, t)$ the vector $\mathrm{V}(\mathcal{L})$ is not covered by $\mathrm{V}(\mathcal{S})$.

---

[1]A. D'yachkov, P. Vilenkin and S. Yekhanin are with the Department of Probability Theory, Faculty of Mechanics & Mathematics, Moscow State University, Russia (dyachkov@mech.math.msu.su, paul@vilenkin.dnttm.ru, gamov@cityline.ru). Their work is supported by the Russian Foundation of Basic Research, grant 98–01–00241.

[2]A. Macula is with the Department of Mathematics, State University of New York, College at Geneseo, USA (macula@geneseo.edu). His work is supported by NSF Grant DMS–9973252.

[3]D. Torney is with the Theoretical Division T10, Los Alamos National Laboratories, USA (dct@lanl.gov). His work is supported by the US Department of Energy.

If $|\tau| = 1$, then $\mathrm{V}(\tau) = \Lambda(\tau)$. For this reason, for $\ell = L = 1$ definitions 1 and 2 are equivalent, and a set $\mathcal{C}$ in this case is called a *binary superimposed code* of *strength* s (or, briefly, s*-code*).

A codeword $\mathbf{x}(j)$ can be interpreted as a subset of the set $[N]$. Then $\mathrm{V}(\tau)$ is the union, and $\Lambda(\tau)$ is the intersection of corresponding sets. Taking this into account, a superimposed s-code can be identified by a family of sets in which no set is covered by a union of s others; a superimposed (s, ℓ)-code is identified by a family of sets in which no intersection of ℓ sets is covered by a union of s others; and a superimposed s-code with list-size L is identified by a family of sets in which no union of L sets is covered by a union of s others.

The applications of s-codes and (s, ℓ)-codes to the problem of identifying positive elements and positive sets in the group testing model are discussed in "Part I" of the present paper [8, Sec. 2]. Superimposed s-codes with list-size L can also be used in this model as follows: if $\mathsf{p} \subset [t]$ is a set of positive elements, $|\mathsf{p}| \le s$, and testing groups form an s-code with list-size L, then given the test results one can construct a set $\mathsf{p}' \subset [t]$, such that $\mathsf{p} \subseteq \mathsf{p}'$ and $|\mathsf{p}' \backslash \mathsf{p}| \le L - 1$. If $L = 1$, then one can decode an unknown set p exactly.

2 Constructions of (s, ℓ)-codes

Trivial construction. Let $\mathcal{C}'$ be an $(s, 1)$-code of length N' and size t. Put $N \triangleq \binom{N'}{\ell}$ and let $\sigma_1, \dots, \sigma_N$ be all ℓ-subsets of the set $[N']$. Construct a new code $\mathcal{C} \triangleq \{\mathbf{x}(1), \dots, \mathbf{x}(t)\}$ of length N, for which

$$x_i(j) \triangleq \bigvee_{m \in \sigma_i} x'_m(j), \quad i \in [N], \quad j \in [t].$$

Then $\mathcal{C}$ is an (s, ℓ)-code. This yields the bound [8, (3)].

Concatenated construction. Consider an integer $q \ge 2$ and a set $\mathcal{C}$ (4), in which elements $x_i(j)$ are taken from the q-ary alphabet $[q] = \{1, \dots, q\}$.

Definition 3. A q-ary set $\mathcal{C}$ defined above is called a *superimposed q-ary (s, ℓ)-code*, if for any pair $(\mathcal{S}, \mathcal{L}) \in \pi(s, \ell, t)$ there exists a coordinate $i \in [n]$ for which the *coordinate sets*

$$\mathcal{L}_i \triangleq \{x_i(j) \,:\, j \in \mathcal{L}\} \subseteq [q] \quad \text{and} \quad \mathcal{S}_i \triangleq \{x_i(j') \,:\, j' \in \mathcal{S}\} \subseteq [q]$$

are disjoint, i.e., $\mathcal{S}_i \cap \mathcal{L}_i = \varnothing$. Integers t and n are called the *size* and *length* of code $\mathcal{C}$, respectively.

Proposition 7. (Concatenated construction) *Let $s \ge 1$, $\ell \ge 1$, $t \ge s + \ell$ and $q \ge s + \ell$ be integers. Assume that there exists a q-ary (s, ℓ)-code $\mathcal{C}^{(q)} = \|x_i^{(q)}(j)\|$ of size $t^{(q)}$ and length $n^{(q)}$ and an (s, ℓ)-code $\mathcal{C}' = \|x'_i(j)\|$ of size*

$t' \geq q$ and length n'. Then there exists a superimposed (s, ℓ)-code $\mathcal{C}$ of size $t = t^{(q)}$ and length $N = n^{(q)} n'$.

Proof. The code $\mathcal{C}$ is constructed by the concatenation of codes $\mathcal{C}^{(q)}$ and $\mathcal{C}'$, i.e., each q-ary symbol $\theta \in [q]$ in the code $\mathcal{C}^{(q)}$ is replaced with the codeword $\mathbf{x}'(\theta)$ from the code $\mathcal{C}'$. The j-th codeword of the new code $\mathcal{C}$ has the form

$$\mathbf{x}(j) \triangleq \left(\mathbf{x}'\left(x_1^{(q)}(j)\right), \dots, \mathbf{x}'\left(x_{n'}^{(q)}(j)\right)\right).$$

One can easily prove that this code $\mathcal{C}$ is really an (s, ℓ)-code.

Proposition 8. *Let $s = \ell = 2$. Then the minimum length $N(t, 2, 2)$ for $4 \leq t \leq 8$ has the form*

$$N(4, 2, 2) = \tbinom{4}{2} = 6, \quad N(5, 2, 2) = \tbinom{5}{2} = 10,$$
$$N(6, 2, 2) = N(7, 2, 2) = N(8, 2, 2) = 14.$$

Proof. For $t = s + \ell = 4$ the optimal (s, ℓ)-code is trivial [8, Prop. 2]. For $t = 5, 6$ we used a computer exhaustive search: for $t = 5$ the optimal $(2, 2)$-code is trivial, and for $t = 6$ the optimal code has length $N = 14$ (the trivial length for this case is $\binom{6}{2} = 15$).

Consider the following 3×8 quaternary matrix

$$C^{(4)} = \begin{pmatrix} 4 & 2 & 3 & 1 & 2 & 4 & 1 & 3 \\ 1 & 1 & 2 & 2 & 3 & 3 & 4 & 4 \\ 2 & 4 & 1 & 3 & 2 & 4 & 1 & 3 \end{pmatrix}.$$

One can check that the columns of $C^{(4)}$ form a superimposed quaternary $(2, 2)$-code of size 8 and length 3. The concatenation of this code with the trivial $(2, 2)$-code of size 4 and length $\binom{4}{2} = 6$ leads to the binary $(2, 2)$-code of size $t = 8$ and length $N = 6 \cdot 3 = 18$. Examining this code, one can see that there is a pair of rows, which are repeated three times in the given code. Obviously, we can remove two copies of each row, and get the binary $(2, 2)$-code of size $t = 8$ and length $N = 14$. Since $N(6, 2, 2) = 14$, we have that $N(8, 2, 2) = N(7, 2, 2) = 14$.

Definition 4. The *Maximum Distance Separable code* (*MDS-code*) with parameters (q, k, n) is a q-ary code of size $t = q^k$, length n and the Hamming distance $d = n - k + 1$ [3].

Proposition 9. *If $q^k \geq s + \ell$ and $n \geq s\ell(k - 1) + 1$, then any MDS-code with parameters (q, k, n) is a superimposed q-ary (s, ℓ)-code.*

For any integer $\lambda \geq 1$ and a prime power $q \geq \lambda$ there exists an MDS-code with parameters $(q, \lambda + 1, q + 1)$ (*Reed–Solomon code*). The concatenation of this code with the optimal binary superimposed code of size q leads to the following

Proposition 10. *Let $s \geq 1$, $\ell \geq 1$ and $\lambda \geq 1$ be integers and $q \geq s\ell\lambda$ be a prime power. Then*

$$N(q^{\lambda+1}, s, \ell) \leq N(q, s, \ell)\left[s\ell\lambda + 1\right].$$

Table 1 gives several numerical values of upper bounds on $N(t, 2, 2)$ calculated with the help of propositions 8 and 10. For instance,

1. $N(16, 2, 2) = N(4^2, 2, 2) \leq N(4, 2, 2) \cdot [4 \cdot 1 + 1] \leq 6 \cdot 5 = 30$;
2. $N(512, 2, 2) = N(8^3, 2, 2) \leq N(8, 2, 2) \cdot [4 \cdot 2 + 1] \leq 14 \cdot 9 = 126$;

t	4	8	16	25	64	512	625	2^{12}	2^{16}	2^{20}
N	6	14	30	50	70	126	250	270	390	510

Table 1. Parameters of superimposed $(2, 2)$-codes

3 On Constructions of List-Decoding Codes

For a set of codewords $\mathcal{C}$ (4) and a subset $\tau \subset [t]$ denote by $L(\tau, \mathcal{C}) \geq 0$ the number of indices $j \in [t]\backslash\tau$, such that the vector $\mathbf{x}(j)$ is not covered by $\mathrm{V}(\tau)$. Let $L_s(\mathcal{C})$ denote the maximum value of $L(\tau, \mathcal{C})$ over all $\tau \subset [t]$, $|\tau| = s$. The number $L_s(\mathcal{C})$ is the maximum list-size of the list-decoding superimposed code of strength s (see definition 2).

Along with $L_s(\mathcal{C})$ we study the number $L_s^*(\mathcal{C})$, which is the *average number* of codewords covered by a random s-subset $\tau \subset [t]$:

$$L_s^*(\mathcal{C}) \triangleq \sum_{\substack{\tau\subset[t]\\ |\tau\|=s}} L(\tau, \mathcal{C}) \Bigg/ \binom{t}{s}. \tag{7}$$

Further we claculate value of L_s^* and give the upper bound on L_s, for binary superimposed codes, that are obtained from q-nary MDS codes by trival concatenation. Those codes were studied in [1, 6, 7]

We say that the concatenation is trival if q-nary symbols are replaced with the columns of the $(q \times q)$ identity matrix.

Theorem 1: For a binary superimposed code, obtained from (q, k, n) MDS code by trival concatenation,

$$L_p^* = q^k \frac{(\binom{q^k-1}{p} - C(p))}{\binom{q^k}{p}} \tag{8}$$

$$C(p) = \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} D(p, i)$$

$$D(p,v) = \begin{cases} \binom{q^{k-v}(q-1)^v}{p}, & \text{if } v \le k; \\ \binom{A_v(v)}{p}, & \text{if } v > k. \end{cases}$$

$$A_v(v) = (q-1)\sum_{j=0}^{k-1}(-1)^j \binom{v-1}{j} q^{k-j-1}$$

Theorem 2: For a binary superimposed code, obtained from (q,k,n) MDS code by trival concatenation,

$$L(s) \le min\{s^k - s, q^k - \frac{n*(q-s)*q^{k-1}}{w} - s\}, \tag{9}$$

where w is the greatest solution of the equatation

$$\prod_{i=1}^{k-1}(w-i) = (n-1)(n-k+1)\left(\frac{q-s}{q}\right)^{k-1}$$

Another construction of list-decoding superimposed codes based on the incidence of the finite sets was studied in [5].

References

[1] W.H. Kautz, R.C. Singleton, "Nonrandom Binary Superimposed Codes," *IEEE Trans. Inform. Theory*, **4** (1964), 363-377.

[2] R.S. Singleton, "Maximum Distance Q-Nary Codes," *IEEE Trans. Inform. Theory*, **2** (1964), 116-118.

[3] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, 1983.

[4] A. D'yachkov, V. Rykov, "A Survey of Superimposed Code Theory," *Problems of Control and Inform. Theory*, **4** (1983), 229–242.

[5] P. Vilenkin, "On Constructions of List–Decoding Superimposed Codes," *Proc. of ACCT-6*, Pskov, Russia, 1998, 228–231.

[6] A. D'yachkov, A. Macula, V. Rykov, "New Constructions of Superimposed Codes," *IEEE Trans. Inform. Theory*, **1** (2000), 284–290.

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

[8] A. D'yachkov, A. Macula, D. Torney, P. Vilenkin, S. Yekhanin, "New Results in the Theory of Superimposed Codes: Part I," *present volume.*