Superimposed Codes and ALOHA system

Arkady G. D'yachkov, Vyacheslav V. Rykov

Moscow State University, Faculty of Mechanics and Mathematics,
Department of Probability Theory, Moscow, 119899, Russia,
Email: dyachkov@nw.math.msu.su

Abstract–**We study an application of superimposed codes [1, 2, 3] to the ALOHA-system [4] with a central station. These codes increase the transmission rate [4].**

1 Statement of the problem

Let a system contain M terminal *stations* and let a *multiple-access channel* (MAC) [5] connect these M stations to the *central station* (CS). Each terminal station has a source. The sources can generate binary sequences called *information packets*. Each information packet has the same length K, and these packets should be transmitted. The CS is interested in the *contents* of the packet. The CS is not interested in a terminal station transmitted this packet. For instance, such situation can occur in a *reference communication system* (RCS) (see **Fig. 1**) which contains a *feedback broadcast channel* (FBC) [5]. If the CS receives a *request*, then it uses the FBC to transmit the *answer* to this request to all M stations simultaneously.

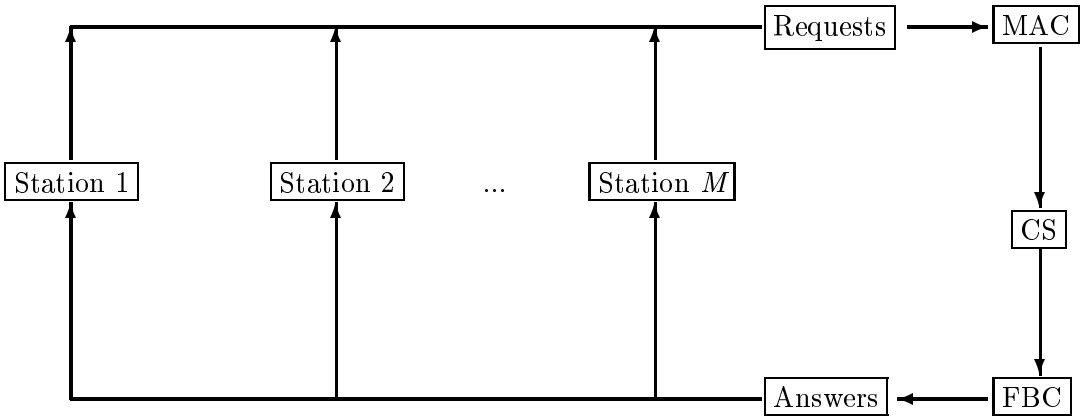

Fig.1. A block-scheme of the RCS.

2 Notations and definitions

Introduce $t = 2^K$ and enumerate all 2^K possible information packets by integers from 1 to t. Let an integer $N \geq K$ and let $X = \|x_i(u)\|,\ i = 1, 2, \ldots, N,\ u = 1, 2, \ldots, t$, be a binary $(N \times t)$-matrix (*code*). The column $\mathbf{x}(u) = (x_1(u), x_2(u), \ldots, x_N(u)) \in \{0,1\}^N,\ u = 1, 2, \ldots, t$ is called a *code packet*, corresponding to the information packet (request) with the number u. Suppose that the time is divided into the *windows* of equal lengths. For all M stations (*synchro*), each window is divided into N units. Within every window each station has one of two possibilities:

- the station can *be silent*,

- the station can send *one* of t code packets, transmitting *one binary symbol for the time unit*.

Let $\mu > 0$ be a fixed parameter. Put $p = \mu/M$, $0 < p < 1$. Suppose that the sources are independent. During the time of a given window, the source of the m-th station $m = 1, 2, \ldots, M$ randomly chooses between two possibilities:

- with probability $p = \mu/M$, the source generates one information packet which will be sent by the m-th station during the next window using the corresponding code packet,
- with probability $1 - p$, the source does not generate any packet, and the m-th station is silent during the next window.

Let the random variable ξ_μ be the number of code packets, which were transmitted during a given window. If M is sufficiently large, then ξ_μ has the Poisson distribution with parameter μ:

$$\Pr\{\xi_\mu = n\} = \frac{\mu^n e^{-\mu}}{n!}, \quad n = 0, 1, 2, \ldots. \tag{1}$$

3 Mathematical models of MAC

For the RCS, the deterministic MAC [5] (with n inputs and one output) is described by the function

$$f_n = f_n(a_1, a_2, \ldots, a_n), \ a_i \in \{0, 1\}.$$

If the MAC's inputs (signals of n transmitting stations) are binary symbols $a_1, a_2, \ldots, a_n$, then the MAC's output (signal received by CS) is denoted by $f_n(a_1, a_2, \ldots, a_n)$. We consider two models of MAC corresponding to two types of *modulation* for transmission of binary symbols. Let $\sum_{i=1}^n a_i$ denote the arithmetic sum, i.e., the number of 1's in the sequence $a_1, a_2, \ldots, a_n$. The *disjunct model* (D–model)

$$f_n(a_1, a_2, \ldots, a_n) = \begin{cases} 1, & \sum_{i=1}^n a_i \neq 0, \\ 0, & \sum_{i=1}^n a_i = 0, \end{cases} \tag{2}$$

corresponds to the *impulse modulation* (IM), and the *symmetrical disjunct model* (SD–model)

$$f_n(a_1, a_2, \ldots, a_n) = \begin{cases} 1, & \sum_{i=1}^n a_i = n, \\ 0, & \sum_{i=1}^n a_i = 0, \\ *, & 1 \leq \sum_{i=1}^n a_i \leq n-1, \end{cases} \tag{3}$$

where the symbol " $*$ " denotes an *erasure*, describes the *frequency modulation* (FM). The adequacy of these models is evident. Function (2) is called the *Boolean sum* of binary symbols $a_1, a_2, \ldots, a_n$. By analogy, function (3) will be called *symmetrical Boolean sum* of $a_1, a_2, \ldots, a_n$.

4 Superimposed (s,L,N)-codes

We say that column $\mathbf{z}$ *covers* column $\mathbf{x}$ (or $\mathbf{x}$ is covered by $\mathbf{z}$) if the component-wise Boolean sum of $\mathbf{z}$ and $\mathbf{x}$ is equal $\mathbf{z}$. Let $1 \leq s < t$, $1 \leq L \leq t - s$ be integers.

Definition [2]. An $(N \times 2^K)$-matrix X is called a *list-decoding superimposed code* (LDSC) for the D–model of *length* N, *size* $t = 2^K$, *strength* s and *list-size* L if the Boolean sum of any s-subset of columns (codewords) X can cover not more than $L - 1$ columns that are not

components of the s-subset. This code also will be called a *superimposed* (s, L, N)-*code* of size $t = 2^K$. The ratio K/N is called the *rate* of code X.

By analogy with this definition, we define list-decoding superimposed code (or superimposed (s, L, N)-code) for SD–model. One can easily understand that any superimposed (s, L, N)-code for D–model is also the superimposed (s, L, N)-code for SD–model.

Kautz-Singleton [1] obtained a family of superimposed $(s, 1, N)$-codes for D–model with the following parameters. Let $k \geq 2$ be an integer and $q \geq k - 1$ be a prime or prime power. Then

$$K = \lfloor k \log_2 q \rfloor, \quad N = q[1 + (k-1)s], \quad s = \left\lfloor \frac{q}{k-1} \right\rfloor, \tag{4}$$

where symbol $\lfloor b \rfloor$ denotes the largest integer $\leq b$.

Let $t(s, L, N) = 2^{K(s,L,N)}$ be the maximal possible size of LDSC. For fixed L and s, define the *asymptotic rate* of LDSC

$$R(s, L) = \overline{\lim_{N \to \infty}} \frac{K(s, L, N)}{N}. \tag{5}$$

For the D–model, Dyachkov-Rykov-Antonov [6] (see also [7, 8]) obtained a *random coding bound* on the asymptotic rate of LDSC

$$R(s, L) \geq \frac{L \log_2 e}{(s + L - 1)\lceil es \rceil}. \tag{6}$$

where symbol $\lceil b \rceil$ denotes the least integer $\geq b$.

5 Performance of the RCS

Suppose that in a given window $\xi_\mu = n$ and code packets $\mathbf{x}(u_1), \mathbf{x}(u_2), \ldots, \mathbf{x}(u_n)$, where $1 \leq u_1 \leq u_2 \leq \ldots \leq u_n \leq t$, are transmitted. Denote by $\mathbf{z} = \mathbf{z}(X, u_1, u_2, \ldots, u_n)$ the packet, which is received by the CS. From (2) and (3) it follows that for the D–model (SD–model), the output packet $\mathbf{z}$ is the Boolean sum (symmetrical Boolean sum) of the transmitted code packets.

Let $1 \leq s \leq T < t = 2^K$ be integers. If the CS has a *threshold* T and uses a superimposed $(s, T-s+1, N)$-code X, then the performance of the RCS is going on as follows. Having received $\mathbf{z}$, the CS selects all $n' \geq n$ columns of X which are covered by $\mathbf{z}$. There are two possibilities:

- if $n' \leq T$, then the CS answers (over a FBC) all the requests corresponding to the selected code packets (*successful transmission of requests*);
- if $n' \geq T+1$, then the CS does not answer any request received in a given window (*refusal*).

For applications, the maximal possible number of answers is $T \ll t = 2^K$. The number T is interpreted as a *capacity* of the CS. Note that the CS transmits over a FBC not more than $T - s$ unnecessary answers. According to the definition of a superimposed $(s, T - s + 1, N)$–code, the refusal means that $\xi_\mu \geq s + 1$ and

$$A_s(\mu) = \sum_{n=0}^{s} \frac{n\mu^n e^{-\mu}}{n!} = \mu \sum_{n=0}^{s-1} \frac{\mu^n e^{-\mu}}{n!}. \tag{7}$$

is a lower bound on the *average number of successfully transmitted requests in a given window of length* N. In addition,

$$r_s(\mu) = \Pr\{\xi_\mu \geq s + 1\} = \sum_{n=s+1}^{\infty} \frac{\mu^n e^{-\mu}}{n!}. \tag{8}$$

is an upper bound on the *probability of refusal.*

6 Characteristics of the RCS

For a superimposed $(s, T-s+1, N)$-code X of size $t = 2^K$, denote by $E(\mu, X)$ an *average number of successfully transmitted information bits in the time unit of the RCS performance.* By definition, each request contains K information bits. Hence, by virtue of (7), we have

$$E(\mu, X) \geq \frac{K}{N} A_s(\mu) = \frac{K\mu}{N} \sum_{n=0}^{s-1} \frac{\mu^n e^{-\mu}}{n!}, \tag{9}$$

The quantity $E(\mu, X)$ is also called a *rate* of the superimposed $(s, T-s+1, N)$-code X of size $t = 2^K$ for the RCS.

Let $\epsilon,\ 0 < \epsilon < 1$, be fixed. Following [4], define the *maximal rate* $\mathcal{R}(\epsilon, X)$ of a superimposed $(s, T-s+1, N)$-code X of size $t = 2^K$ provided that the refusal probability $\leq \epsilon$. With the help of (8) and (9), we obtain

$$\mathcal{R}(\epsilon, X) \geq \max_{\mu: r_s(\mu) \leq \epsilon} E(\mu, X) \geq \frac{K}{N} \mathcal{A}_s(\epsilon), \tag{10}$$

$$\mathcal{A}_s(\epsilon) = \max_{\mu: r_s(\mu) \leq \epsilon} A_s(\mu), \tag{11}$$

where the maximum in the right-hand sides of (10) and (11) is taken over all $\mu,\ \mu > 0$, for which $r_s(\mu) \leq \epsilon$. For a fixed threshold $T = 1, 2, \ldots$, we introduce the *capacity* of RCS:

$$\mathcal{C}_T(\epsilon) = \sup_{K \geq 1} \max_X \mathcal{R}(\epsilon, X), \tag{12}$$

where $\max_X$ denotes the maximization over all superimposed $(s, T-s+1, N)$-codes X of size $t = 2^K$. Let the asymptotic rate $R(s, L)$ of (s, L, N)-codes be defined by (5). From (10) it follows that

$$\mathcal{C}_T(\epsilon) \geq \max_{1 \leq s \leq T} \left\{ R(s, T-s+1) \cdot \mathcal{A}_s(\epsilon) \right\}. \tag{13}$$

Evidently, for any fixed $\epsilon,\ 0 < \epsilon < 1$, the capacity $\mathcal{C}_1(\epsilon) < \mathcal{C}_2(\epsilon) < \cdots$. If $T = 1$, then the RCS is the ALOHA-system without feedback [4], i.e., $N = K$ and the coding is not used. One can easily understand that:

- if $0 \leq \epsilon \leq 1 - 2/e = 0.264$, then the capacity $\mathcal{C}_1(\epsilon) = \mathcal{A}_1(\epsilon)$ could be given in the parametric form
$$\mathcal{C}_1(\epsilon) = \mu e^{-\mu}, \quad \epsilon = 1 - e^{-\mu}(1+\mu), \qquad 0 \leq \mu \leq 1;$$
- if $\epsilon \geq 1 - 2/e = 0.264$, then $\mathcal{C}_1(\epsilon) = e^{-1} = 0.368$.

7 Lower bounds on the capacity

Let $T \geq 2$. Let $s = 1, 2, \ldots, T$ be fixed and functions $A_s(\mu)$,$r_s(\mu)$ and $\mathcal{A}_s(\epsilon)$ be defined by (7), (8) and (11). Denote by $\mu = \mu_s$ the unique value of parameter $\mu > 0$ for which $A_s(\mu)$ achieves its maximum, i.e.,

$$A_s(\mu_s) = \max_{\mu > 0} A_s(\mu) = \max_{\mu > 0} \left\{ \mu \sum_{n=0}^{s-1} \frac{\mu^n e^{-\mu}}{n!} \right\}.$$

Obviously, $r_s(\mu)$ is a monotonically increasing function of the parameter $\mu > 0$ and there exists the *inverse* function $r_s^{(-1)}(\epsilon)$, $0 < \epsilon < 1$. Therefore, $\mathcal{A}_s(\epsilon)$ could be written as follows

$$\mathcal{A}_s(\epsilon) = \begin{cases} A_s(r_s^{(-1)}(\epsilon)), & \text{if } 0 < \epsilon \le r_s(\mu_s), \\ A_s(\mu_s), & \text{if } r_s(\mu_s) \le \epsilon < 1. \end{cases} \tag{14}$$

For the case $0 < \epsilon \le r_s(\mu_s)$, the function $\mathcal{A}_s(\epsilon)$ *monotonically increases* and formula (14) could be given in the parametric form

$$\mathcal{A}_s(\epsilon) = A_s(\mu) = \mu \sum_{n=0}^{s-1} \frac{\mu^n e^{-\mu}}{n!},$$

$$\epsilon = r_s(\mu) = \sum_{n=s+1}^{\infty} \frac{\mu^n e^{-\mu}}{n!} = 1 - \sum_{n=0}^{s} \frac{\mu^n e^{-\mu}}{n!}, \quad 0 < \mu \le \mu_s. \tag{15}$$

Let integers $2 \le s \le T$ be fixed and let there exist a superimposed $(s, T-s+1, N)$-code X of size $t = 2^K$. Definition (12) and inequality (10) imply that the capacity

$$\mathcal{C}_T(\epsilon) \ge \frac{K}{N} \mathcal{A}_s(\epsilon), \tag{16}$$

where the function $\mathcal{A}_s(\epsilon)$ is defined by (14) or (15). Using the Kautz-Singleton parameters (4), one can easily obtain the numerical values of the lower bound (16). As an example, we consider two superimposed $(s, 1, N)$-codes of size $t = 2^K$ from family (4):

1. $(k = 5,\ q = 16) \implies (T = s = 4,\ K = 20,\ N = 272)$;
2. $(k = 3,\ q = 16) \implies (T = s = 8,\ K = 12,\ N = 272)$.

Fig. 2 shows lower bounds (16) for these two codes (see $s = T = 4$ and $s = T = 8$) as well as the capacity of the ALOHA-system $\mathcal{C}_1(\epsilon) = \mathcal{A}_1(\epsilon)$ (see $s = T = 1$).

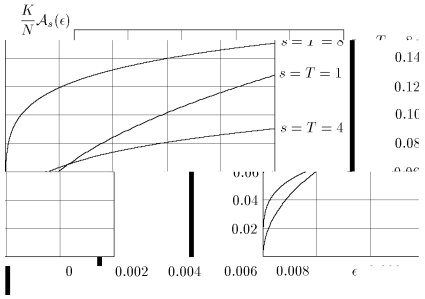

Fig. 2.

Inequalities (6) and (13) yield the *lower random coding bound* on $\mathcal{C}_T(\epsilon)$:

$$\mathcal{C}_T(\epsilon) \geq \max_{1 \leq s \leq T} \left\{ \frac{(T-s+1)\log_2 e}{T\lceil es \rceil} \cdot \mathcal{A}_s(\epsilon) \right\}. \tag{17}$$

Let an arbitrary ϵ, $0 < \epsilon < 1$, be fixed and $s \to \infty$. Applying normal approximation [9] to the Poisson distribution, one can easily understand that $\mathcal{A}_s(\epsilon) = s(1+o(1))$. Hence, inequality (17) implies that the following theorem is true.

Theorem. *For any fixed* ϵ, $0 < \epsilon < 1$,

$$\overline{\lim_{T \to \infty}} \mathcal{C}_T(\epsilon) \geq \frac{\log_2 e}{e} = 0.5307.$$

References

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

[2] A.G. D'yachkov, V.V. Rykov, "A Survey of Superimposed Code Theory," *Problems of Control and Inform. Theory*, vol. 12, no. 4, pp. 229-242, 1983.

[3] D.-Z. Du, F.K. Hwang, "Combinatorial group testing and its applications," World Scientific, Singapore-New Jersey-London-Hong Kong, 1993.

[4] L. Kleinroch, "Queueing Systems. Vol.II; Computer Applications," J.Wiley, New York, 1976.

[5] T.M. Cover, J.A. Thomas, "Elements of Information Theory," J.Wiley, New York, 1991.

[6] A.G. D'yachkov, V.V. Rykov, M.A. Antonov, "List-decoding superimposed codes", *10-th Simposium po probleme izbytochnosti v informatsionnyx sistemax*, doklady, v.1, Leningrad, 1989, pp. 116-119, (in Russian).

[7] A.M. Rashad, "Random coding bounds on the rate for list-decoding superimposed codes", *Problems of Control and Information Theory*, v.19, No 2, 1990, pp. 141-149.

[8] A.G. D'yachkov, V.V. Rykov, "On superimposed codes," *Fourth International Workshop "Algebraic and Combinatorial Coding Theory"*, Novgorod, Russia, September 1994, pp. 83-85.

[9] W. Feller, "Introduction to Probability Theory and Its Applications", J.Wiley, New York, 1968.