A New Algorithm for Two-Stage Group Testing

Ilya Vorobyev
Center for Computational and Data-Intensive Science and Engineering,
Skolkovo Institute of Science and Technology
Moscow, Russia 127051
Advanced Combinatorics and Complex Networks Lab,
Moscow Institute of Physics and Technology
Dolgoprudny, Russia 141701
Email: vorobyev.i.v@yandex.ru

Abstract—Group testing is a well-known search problem that consists in detecting of $s$ defective members of a set of $t$ samples by carrying out tests on properly chosen subsets of samples. In classical group testing the goal is to find all defective elements by using the minimal possible number of tests in the worst case. In this work, two-stage group testing is considered. Using the hypergraph approach we design a new search algorithm, which allows improving the known results for fixed $s$ and $t \rightarrow \infty$. For the case $s = 2$ this algorithm achieves information-theoretic lower bound $2 \log_2 t (1 + o(1))$ on the number of tests. Also, the problem of finding $m$ out of $s$ defectives is considered.

I. INTRODUCTION

Group testing problem was introduced by Dorfman in [1]. Suppose that we have a population of $t$ items, some of which are defective. Our task is to find all defective items by performing a minimal number of tests. The test is carried out on a properly chosen subset (pool) of the set of samples. The test outcome is positive if the tested set contains at least one defective element; otherwise, it is negative.

In group testing, two types of algorithms are usually considered. In adaptive group testing, at each step the algorithm decides which group to test by observing the responses of the previous tests. In non-adaptive algorithm, all tests are carried out in parallel. Multistage algorithm is a compromise solution to the group testing problem. In $p$-stage algorithms all tests are divided into $p$ stages. Tests from the $i$th stage may depend on the outcomes of the tests from the previous stages. Define $N_p(t, s)$ to be the minimal worst-case total number of tests needed to find all $s$ defective members of a set of $t$ samples using at most $p$ stages. Also define the optimal rate of $p$-stage search algorithm as

$$R_p(s) = \lim_{t \rightarrow \infty} \frac{\log_2 t}{N_p(t, s)}.$$ 

By the similar way we define the rate $R_{ad}(s)$ of fully adaptive algorithms.

In many applications, it is much cheaper and faster to perform tests in parallel, but non-adaptive algorithms require far more tests than adaptive ones. More precise, for non-adaptive algorithms it is known [2], [3] that $R_1(s) = O(\log_2 s / s^2)$. In contrast, adaptive algorithms allow to achieve the rate $R_{ad} = 1/s$. Rather surprisingly, for 2-stage algorithms it was proved that $O(s \log_2 t)$ tests are already sufficient [4]–[6]. This fact emphasizes the importance of multistage algorithms.

A. Previous results

We refer the reader to the monographs [7], [8] for a survey on group testing and its applications.

For non-adaptive algorithms the best known asymptotic $(s \rightarrow \infty)$ lower bound [6] and upper bounds [9] are as follows

$$\frac{2 \ln 2}{s^2} (1 + o(1)) \leq R_1(s) \leq \frac{4 \log_2 s}{s^2} (1 + o(1)).$$

In addition, we refer to the work [10], where the best lower and upper bounds on $R_1(2)$ were established

$$0.31349 \leq R_1(2) \leq 0.4998.$$ 

For the case of $p$-stage algorithms, $p > 1$, the only known upper bound is information-theoretic one

$$R_p(s) \leq \frac{1}{s}, \quad p > 1. \quad (1)$$

The best asymptotic $(s \rightarrow \infty)$ lower bound for 2-stage algorithms was established in [9]

$$R_2(s) \geq \frac{\log_2 e}{es} (1 + o(1)). \quad (2)$$

The best result for the case $s = 2$ was obtained in [11]

$$R_2(2) \geq 0.4098.$$ 

All of the lower bounds mentioned above were probabilistic. We want to refer to 2 constructive lower bounds for the case $s = 2$. In [12] the authors obtained a 2-stage algorithm with rate 0.4. In [13] an explicit 4-stage testing scheme with rate 0.5 was constructed. This bound matches the information-theoretic upper bound, i.e. the presented 4-stage algorithms allow to achieve the same rate as a fully adaptive algorithm.

The aim of this work is a further development of the bounds on the rates $R_2(s)$.
which later will be called the outcome vector $y$

As a result of performed tests we get the outcome vector subset $S$ in the following way. The set of vertexes $X$ at the first stage, some pools are tested in parallel. Tests for the set of samples $X$, $S$, $y$ is from the disjunctive sum of binary columns $s$

possible defective sets of size $X$, $s$, $y$ has a constant number of edges.

In that case, we need to test only the constant amount of non-isolated vertexes individually to find all defective elements. The asymptotic $t \to \infty$ rate of such scheme is equal to the asymptotic rate of the code $X$.

## III. Algorithm for 2 Defectives

We apply the plan described in the previous section to the case $s = 2$. Note that in this case we have graph instead of hypergraph $H$.

**Theorem 1.** $R_2(2) = 0.5$.

As it was mentioned before, this bound matches the bound for a fully adaptive algorithm. In addition, the algorithm from this theorem can be used to find not only 2 defectives but also at most 2 defectives. But to keep things simple, here we consider only the case of exactly 2 defectives.

**Proof of Theorem 1**. Consider a random matrix $X$ of size $N \times t$, each columns of which is chosen independently and uniformly from the set off all columns of weight $wN$, $0 < w < 1$. To keep the notation simple, we ignore the fact that $wN$ may not be an integer. Fix the constant $L$ and consider a graph $G_y = H(X, 2, y)$, where vector $y$ is from $\{0, 1\}^N$.

Call the index $v \in [t]$ a y-bad index of the first type if the degree of the vertex $v \in V$ in the graph $G_y$ is at least $L$. Call the index $v \in [t]$ a y-bad index of the second type if the vertex $v \in V$ is included in some matching of cardinality at least $L$ in the graph $G_y$. Recall that matching is a set of edges without common vertexes. Finally, call the index $v \in [t]$ a bad index if there exists a vector $y \in \{0, 1\}^N$ such that $v$ is a y-bad index of the first or the second type.

The following two propositions imply the theorem.

**Proposition 1.** If the maximum vertex degree and the maximum cardinality of a matching in a graph $G = (V, E)$ don’t exceed $L$, then $|E| \leq 2L^2$.

**Proposition 2.** For any $R < 0.5$ and $w = 1 - \sqrt{2}/2$, there exists an integer $L$ such that for $t = \lfloor 2RN \rfloor$ the mathematical expectation of the number of bad indexes less than 1 for $N$ big enough.

Let us show how the Theorem 1 can be deduced from these two propositions. Indeed, take the parameters $w$, $R$, $L$ from Proposition 2. Thus, for $N$ big enough there exists a $N \times t$ matrix $X$ without bad indexes. Use that matrix $X$ as a testing matrix at the first stage. There is no bad indexes, therefore, for any outcome vector $y = r(X, S_{un})$ graph $G_y$ does not contain a matching of size greater than $L$ or a vertex with a degree greater than $L$. Applying the proposition 1 to the graph $G_y$, we conclude that it has at most $2L^2$ edges. We finish the search procedure by testing all non-isolated vertexes of the graph $G_y$ individually.

Now we prove propositions 1 and 2.

**Proof of Proposition 1**. Fix an arbitrary maximum matching $M \subset E$, $|M| \leq L$, in the graph $G = (V, E)$. Denote the set of endpoints of $M$ as $U \subset V$, $|U| \leq 2L$. Since $M$ is a
maximum matching, every edge $e$ has at least one endpoint in the set $U$. Therefore, the total number of edges is upper bounded by
\[ \sum v \in U \deg(v) \leq 2L^2. \]

**Proof of Proposition 2.** The probability that a fixed index $v$ is a $y$-bad index of the first type for some outcome vector $y$ of weight $qN$ can be upper bounded by $t^L p_1^L$, where $p_1 = \left( \frac{wN}{(q-p)N} \right) / \left( \frac{N}{w} \right)$ is a probability that for some index $u \neq v$ the equation $x(u) \vee x(v) = y$ holds.

The probability that a fixed index $v$ is a $y$-bad index of the second type for some outcome vector $y$ of weight $qN$ can be upper bounded by $t^{2L+1} p_1 p_2 \leq t^{2L+1} p_2^L$, where $p_2 = \left( \frac{qN}{w} \right) \left( \frac{wN}{(q-w)N} \right)$ is a probability that for some indexes $u_1, u_2$ the equation $x(u_1) \vee x(u_2) = y$ holds.

Therefore, the mathematical expectation of the number of bad indexes can be upper bounded as follows
\[ t^{2L} p_1^L + t^{2L+1} p_2 \leq 2^N \sup_{q \in \{w, \min(2w, 1)\}} \left( t^L p_1^L + t^{2L+1} p_2^L \right) \leq 2^N \sup_{q \in \{w, \min(2w, 1)\}} \left( q^{RN(L+1)} p_1^L + 2^{RN(2L+2)} p_2^L \right). \]

Take $L$ such that $R(L+1) - 0.5L = -1 + \varepsilon$, $\varepsilon > 0$. Then the mathematical expectation of the number of bad indexes is less than
\[ 2^{-\varepsilon N} \sup_{q \in \{w, \min(2w, 1)\}} \left( 2^{0.5N} p_1^L + 2^N p_2^L \right). \]

To finish the proof of the proposition it is sufficient to show that $p_1 < 2^{-0.5N(1+\varepsilon(1))}$ and $p_2 < 2^{-N(1+\varepsilon(1))}$ for all $q$. It is easy to see that $p_2^q \leq p_2$, hence it is enough to verify the inequality $p_2 < 2^{-N(1+\varepsilon(1))}$.

Taking the logarithm and dividing by $N$, we obtain
\[ \sup_{q \in \{w, \min(2w, 1)\}} qh(w/q) + wh((q-w)/w) - 2h(w) < -1 + o(1). \]

For $w = 1 - \sqrt{2}/2$ the maximal value of the left-hand side is equal to $-1$, therefore, the inequality holds.

The theorem is proved.

**IV. Algorithm for $s$ Defectives.** To describe an algorithm for finding $s$ defectives we must introduce some new notions. Fix an integer $L$ and consider a $s$-uniform hypergraph $H$. Call the set of edges $e_1, e_2, \ldots, e_L$ a $(s, L, k)$-bad configuration if $e_i \cap e_j = U$, $|U| = k$, for any $i$ and $j$. In other words, $(s, L, k)$-bad configuration consists of $L$ edges such that the intersection of every two edges is the same set of size $k$. Call a code $X$ a $(s, L, K)$-good code, $K \subset \{0, 1, \ldots, s-1\}$, if the hypergraph $H(X, s, y)$ doesn’t contain a $(s, L, k)$-bad configuration for any outcome vector $y$ and integer $k \in K$. Let $N(t, s, L, K)$ be the minimal length of $(s, L, K)$-good code of size $t$. The asymptotic rate $R(s, L, K)$ of $(s, L, K)$-good code is defined as follows
\[ R(s, L, K) = \lim_{t \to \infty} \frac{\log_2 t}{N(t, s, L, K)}. \]

Denote the limit $\lim_{t \to \infty} R(s, L, K)$ by $R(s, \infty, K)$.

The following lemma demonstrates the connection between $(s, L, K)$-good codes and two-stage group testing problem.

**Lemma 2.**
\[ R_2(s) \geq R(s, \infty, \{0, 1, \ldots, s-1\}). \]

**Proof of Lemma 2.** Use $(s, L, \{0, 1, \ldots, s-1\})$-good code $X$ of size $t$ as a test matrix at the first stage. Then for any outcome vector $y$ hypergraph $H(X, s, y)$ doesn’t contain $(s, L, k)$-bad configurations for $k = 0, 1, \ldots, s-1$.

**Proposition 3.** If a $s$-uniform hypergraph $H = (V, E)$ doesn’t contain $(s, L, k)$-bad configurations for $k = 0, 1, \ldots, s-1$, then the number of edges $|E|$ is at most $c(s, L)$, where $c(s, L)$ doesn’t depend on $|V|$.

**Proof of Proposition 3.** Suppose, seeking a contradiction, that a hypergraph $H = (V, E)$ without bad configurations contains more than $c(s, L)$ edges. Exact formula for $c(s, L)$ will be specified later. Construct a complete graph $\tilde{G} = K_{|E|}$, which vertex set $V = \{e_1, \ldots, e_{|E|}\}$ corresponds to the edges of hypergraph $H$. Color the edge $f = (e_1, e_2)$ of the graph $\tilde{G}$ in color $i+1$, if the cardinality of the intersection $e_1 \cap e_2$ is equal to $i$, $i = 0, 1, \ldots, s-1$.

Recall that Ramsey number $R(c_1, \ldots, c_l)$ is a minimal integer $n$ such that if the edges of a complete graph $K_n$ are colored with $l$ different colors, then for some $i$ between 1 and $c$, the graph must contain a complete subgraph of size $c_i$ whose edges are all color $i$. Here we need only the fact that the number $R(c_1, \ldots, c_l)$ exists.

Take $c(s, L) = R(c_0(s, L), \ldots, c_0(s, L))$. Then for some $k$ there exists a set $E_0$ of edges $e_i, \ldots, e_{c_0(s, L)}$ from the hypergraph $H$ such that $e_i \cap e_j = k$ for any $1 \leq i < j \leq c_0(s, L)$.

Consider an edge $e_1$. Any other edge from the set $E_0$ has $k$ common vertexes with $e_1$. Taking $c_0(s, L) > \binom{k}{2} / (L-1)$, we obtain that some $k$ vertexes $v_1, \ldots, v_k$ belong to another $L-1$ edges $w_1, \ldots, w_{L-1}$ from the set $E_0$. But then the set of edges $e_1, w_1, \ldots, w_{L-1}$ forms bad configuration of type $k$.

This contradiction proves the proposition. ∎
Using Proposition 3 we conclude that the hypergraph $H(X, s, y)$ has at most $c(s, L)$ edges. Thus, we can find all defectives by testing all non-isolated vertices individually at the second stage. The number of tests at the second stage doesn’t depend on the number of elements $t$, therefore, taking limits $t \to \infty$ and $L \to \infty$ we obtain the inequality 6.

To obtain a lower bound on the rate $R(s, \infty, K)$ we use a random coding method.

**Lemma 3.** Define a function $A(s, w, q)$

$$A(s, w, q) = (1 - q) \log_2(1 - q) + q \log_2 \left( \frac{wy^s}{1 - y} \right) + sw \log_2 \frac{1 - y^s}{y} + sh(w), \hspace{0.5cm} w < q < \min(1, sw), \hspace{0.5cm} (7)$$

where $y \in (0, 1)$ is a unique root of the equation

$$q = w \frac{1 - y^s}{1 - y}, \hspace{0.5cm} (8)$$

Define $R(s, k, w)$ as follows.

$$R(s, k, w) = \min \left\{ R_1(s, k, w), R_2(s, k, w) \right\}, \hspace{0.5cm} (9)$$

where

$$R_1(s, k, w) = \inf_{\max(w, kw/2) \leq q \leq \min((s - k)w, 1)} \frac{A(s - k, w, q) - kw + h(q)}{s - k}, \hspace{0.5cm} (10)$$

$$R_2(s, k, w) = \inf_{\frac{kw}{1} \leq q \leq \frac{k(s - k)w}{w}} \frac{A(s - k, w, q) - kw \left( \frac{w}{kw} \right) + h(q)}{s - k}, \hspace{0.5cm} (11)$$

Then

$$R(s, \infty, K) \geq \sup_{0 < w < 1} \min_{0 < k \leq K} R(s, k, w) \hspace{0.5cm} (12)$$

The proof of this lemma can be found in the Appendix. Lemma 9 and Lemma 2 give us

**Theorem 4.**

$$R_2(s) \geq \sup_{0 < w < 1} \min_{0 < k < s} R(s, k, w) \hspace{0.5cm} (13)$$

The best lower bounds for the case $s > 2$ are given by disjunctive list-decoding codes with the length of the list $L \to \infty$ 9. In Table 1 we compare bounds given by Theorem 4 with the best previously known lower bounds.

| $s$  | 3   | 4   | 5   | 6   |
|------|-----|-----|-----|-----|
| old  | 0.199 | 0.145 | 0.114 | 0.094 |
| new  | 0.3219 | 0.199 | 0.145 | 0.114 |

Note that the new lower bound for $s + 1$ defective elements coincides with the old lower bound for $s$ defective elements.

Putting $k = s - 1$ into the condition (11) we obtain the expression $R(s, s - 1, w) < h(w) - (s - 1)wh(1/(s - 1))$. The same expression appears in the derivations of the old lower bound. It means that new algorithm doesn’t improve the previous best known bound for $s \to \infty$.

**V. Finding $m$ Out of $s$ Defectives**

The technique developed in the previous sections can be used to find only part of the defectives. Suppose that we want to find only $m$ out of $s$ defectives. Define $N_p(t, s, m)$ to be the minimal worst-case total number of tests needed to find $m$ out of $s$ defective members in a set of $t$ samples using at most $p$ stages. Also define the optimal rate of $p$-stage search algorithm as

$$R_p(s, m) = \lim_{t \to \infty} \frac{\log_2 t}{N_p(t, s, m)}$$

The problem of finding $m$ out of $s$ defectives with the help of non-adaptive algorithms was formulated in (14) for $m = 1$ and in (15) for the general case. The best results were obtained in (16), (17), where the following bound was proved

$$R(s, m) \geq \min \left( \frac{c_1}{s}, \frac{c_2}{m^2} \right)$$

for some constants $c_1$ and $c_2$.

For two-stage algorithms, we don’t know if it is possible to find all defectives with the rate $1/2$. But it turns out that we can find at least half of the defectives with this rate.

**Theorem 5.**

$$R_2(s, [s/2] + 1) \geq \frac{1}{s} \hspace{0.5cm} (14)$$

**Proof of Theorem 5** This proof is based on the following technical lemma.

**Lemma 6.**

$$R(s, \infty, \{0, 1, \ldots, [s/2]\}) \geq \frac{1}{s} \hspace{0.5cm} (15)$$

The proof of this lemma is postponed to the Appendix. Let us show how it implies the theorem. Use $(s, L, \{0, 1, \ldots, [s/2]\})$-good code $X$ of size $t$ as a test matrix at the first stage. Then for any outcome vector $y$ hypergraph $H(X, s, y) = (V, E)$ doesn’t contain $(s, L, k)$-bad configurations for $k = 0, 1, \ldots, [s/2]$. Form subset of edges $E_1 \subset E$ such that for every $e_1, e_2 \in E_1$ the intersection $e_1 \cap e_2$ has at most $[s/2]$ vertices, and for every $e_1 \in E_1, e_2 \in E \setminus E_1$ the intersection $e_1 \cap e_2$ has at least $[s/2] + 1$ vertices. Such subset can be constructed greedily by adding edges one by one while it is possible. At the second stage we test all non-isolated vertices of the hypergraph $H_1 = (V, E_1)$. At least $[s/2] + 1$ vertices of every edge $e \in E$ will be tested by construction of $E_1$, thus, we will find at least $[s/2] + 1$ defectives. The number of tests at the second stage is upper bounded by $s ||E_1||$. The hypergraph $H_1 = (V, E_1)$ doesn’t contain any $(s, L, k)$-bad configurations for $k = 0, 1, \ldots, s - 1$. Using proposition 3 we conclude that $|E_1| \leq c(s, L)$. Therefore, the number of tests at the second stage doesn’t depend on the total number of elements $t$. Taking limits $t \to \infty$ and $L \to \infty$ and using lemma 6 we obtain the desired inequality 14.
VI. Conclusion

A new algorithm for two-stage group testing was proposed, which improves previously known results. For the case of 2 defectives, this algorithm has the optimal rate of 0.5. Also, a two-stage algorithm which finds at least half of the defectives with the rate $1/s$ was constructed.

Development of the algorithm, which will achieve the optimal rate for the number of defectives greater than 2, is a natural open problem. Another interesting task is to obtain an upper bound on the rate $R_p(s), p > 1$, which is stronger than information-theoretic bound $1/s$.

We note that the technique used in this paper could be also applied to another group testing models, such as, for example, symmetric or threshold group testing.

VII. Acknowledgement

I. Vorobyev was supported in part by RFBR through grant nos. 18-07-01427 A, 18-31-00361 MOL_A.

References

[1] R. Dorfman, “The detection of defective members of large populations,” The Annals of Mathematical Statistics, vol. 14, no. 4, pp. 436–440, 1943.

[2] A. G. D’yachkov and V. V. Rykov, “Bounds on the length of disjunctive codes,” Problemy Peredachi Informatsii, vol. 18, no. 3, pp. 7–13, 1982.

[3] M. Ruszinkó, “On the upper bound of the size of the r-cover-free families,” Journal of Combinatorial Theory, Series A, vol. 66, no. 2, pp. 302–310, 1994.

[4] A. De Bonis, L. Gasieniec, and U. Vaccaro, “Optimal two-stage algorithms for group testing problems,” SIAM Journal on Computing, vol. 34, no. 5, pp. 1253–1270, 2005.

[5] A. Rashad, “Random coding bounds on the rate for list-decoding superimposed codes,” Problems of Control and Information Theory, vol. 19, no. 2, pp. 141–149, 1990.

[6] A. G. D’yachkov, “Lectures on designing screening experiments,” arXiv preprint arXiv:1401.7505, 2014.

[7] D. Du, F. K. Hwang, and F. Hwang, Combinatorial group testing and its applications. World Scientific, 2000, vol. 12.

[8] F. Cicalese, Fault-Tolerant Search Algorithms, ser. Monographs in Theoretical Computer Science. An EATCS Series. Springer Berlin Heidelberg, 2013.

[9] A. G. D’yachkov, I. V. Vorob’ev, N. Polyansky, and V. Y. Shchukin, “Bounds on the rate of disjunctive codes,” Problems of Information Transmission, vol. 50, no. 1, pp. 27–56, 2014.

[10] D. Coppersmith and J. B. Shearer, “New bounds for union-free families of sets,” the electronic journal of combinatorics, vol. 5, no. 1, p. 39, 1998.

[11] P. Damaschke, A. S. Muhammad, and G. Wiener, “Strict group testing and the set basis problem,” Journal of Combinatorial Theory, Series A, vol. 126, pp. 70–91, 2014.

[12] P. Damaschke and A. S. Muhammad, “A toolbox for provably optimal multistage group testing strategies,” in International Computing and Combinatorics Conference. Springer, 2013, pp. 446–457.

[13] A. G. D’yachkov, I. V. Vorobyev, N. Polyanskiy, and V. Y. Shchukin, “On a hypergraph approach to multistage group testing problems,” in Information Theory (ISIT), 2016 IEEE International Symposium on. IEEE, 2016, pp. 1183–1191.

[14] M. Csorsz and M. Ruszinkó, “Single-user tracing and disjointly superimposed codes,” IEEE transactions on information theory, vol. 51, no. 4, pp. 1606–1611, 2005.

[15] B. Lazczay and M. Ruszinkó, “Multiple user tracing codes,” in Information Theory, 2006 IEEE International Symposium on. IEEE, 2006, pp. 1900–1904.

[16] N. Alon and V. Asodi, “Tracing a single user,” European Journal of Combinatorics, vol. 27, no. 8, pp. 1227–1234, 2006.

[17] ———, “Tracing many users with almost no rate penalty,” IEEE transactions on information theory, vol. 53, no. 1, pp. 437–439, 2007.

[18] A. G. D’yachkov, I. V. Vorob’ev, N. Polyansky, and V. Y. Shchukin, “Almost disjoint list-decoding codes,” Problems of Information Transmission, vol. 51, no. 2, pp. 110–131, 2015.

Appendix

Proof of Lemma 3 Consider a random matrix $X$ of size $N \times t$, $t = 2^{\lceil R_p(s) \rceil}$, each column of which is chosen independently and uniformly from the set of all columns of weight $wN$, $0 < w < 1$. To keep the notation simple we ignore the fact that $wN$ may not be an integer. We want to prove that with a positive probability hypergraph $H(X, s, y)$ does not contain bad configurations for any outcome vector $y \in \{0, 1\}^N$.

Estimate the mathematical expectation of the number of bad configurations $\xi_k$ for $k = 0, \ldots, s - 1$. Fix outcome vector $y$ of weight $qN$. Denote the weight of the union of $k$ common vertexes of configuration as $q_0N$, the weight of the union of additional $s - k$ vertexes as $q_1N$. Let $P(l, q, Q)$ be equal to the probability that the weight of the union of $l$ random columns equals $Q$, where each column is chosen independently and uniformly from the set of all columns of weight $q$. Then the following inequality holds true.

$$E\xi_k \leq 2^N \max_{1(k > 0)w \leq q_0 \leq kw} t^k N \left( \frac{P(k, wN, q_0N)}{P(wN, q_0N)} \right)^L \times \max_{q_0 < q < sw} \left( \frac{q_0N}{(q - q_1)N} \right)^L \frac{P(s - k, wN, q_1N)}{P(s - k, wN, q_1N)} \left( \frac{q}{q_0} \right)^L,$$

where $P(lwN, q_0N) = p$ is a probability that the union of $l$ columns gives a specific column of weight $q_1N$, $t^k \times t^{(s-k)L}$ is an upper bound for the number of ways to choose indexes of columns, $2^N \times N^{q_0N} N^{(q - q_1)N}$ is an upper bound for the number of ways to choose an outcome vector $y$, a weight $q_0N$, a vector of weight $q_0N$, a weight $q_1N$ and a vector of weight $q_1N$ such that disjunctive union of this vector with a fixed vector of weight $q_0N$ gives a fixed vector of weight $qN$.

Let the function $A(l, q, Q)$ be defined by

$$A(l, q, Q) = -\lim_{N \to \infty} \frac{\log_2 P(l, q, Q)}{N}.$$

We use the representation (7) of the function $A(l, q, Q)$, which was established in Theorem 4 of paper [18].

We want to prove that $E\xi_k < 1/s$. Taking the logarithm and dividing both parts by $NL$, then taking a limit $\lim_{N \to \infty} \frac{\log_2 P(l, q, Q)}{N}$, we obtain a sufficient condition for the inequality $E\xi_k < 1/s$.

$$\sup_{(s - k)w \leq q_0 \leq kw} \left( q \right) \log_2 P(l, q, Q) = \log_2 \left( \frac{q}{q_0} \right)$$

$$* = I(k > 0)w \leq q_0 \leq kw, \max(q_0, q_1) \leq q \leq \min(sw, 1)$$

$$= l(1 - k)w, \leq q_1 \leq (s - k)w, \leq q_0 \leq kw.$$
1) If \( q_0 = kw \), then we obtain the condition
\[
\sup_{\ast} (s - k)R - A(s - k, w, q_1) + kwh \left( \frac{q - q_1}{kw} \right) - h(q_1) \leq o(1), \tag{18}
\]
\[\ast = \max(kw, q_1) \leq q \leq \min(sw, 1)w \leq q_1 \leq (s - k)w.\]

We have to consider two more cases.

a) Case \( q_1 \leq kw/2 \). Maximum is attained at \( q = kw \).

This leads to
\[
\sup_{w \leq q_1 \leq \min((s-k)w, kw/2)} (s - k)R - A(s - k, w, q_1) + kwh \left( \frac{q_1}{kw} \right) - h(q_1) \leq o(1), \tag{19}
\]
which is equivalent to \( R \leq R_2(s, k, w) \), where \( R_2(s, k, w) \) is defined in \((11)\).

b) Case \( q_1 \geq kw/2 \). In this case optimal \( q \) is equal to \( q_1 + kw/2 \). Then condition \((13)\) transforms into
\[
\sup_{\ast} (s - k)R - A(s - k, w, q_1) + kwh \left( \frac{q_1}{kw} \right) - h(q_1) \leq o(1), \tag{20}
\]
\[\ast = \max(w, kw/2) \leq q_1 \leq (s - k)w,
\]
which is equivalent to \( R \leq R_3(s, k, w) \), where \( R_3(s, k, w) \) is defined in \((11)\).

2) If \( q_0 = q \), then we obtain
\[
\sup_{\ast} (s - k)R - A(s - k, w, q_1) + qh \left( \frac{q_1}{q} \right) - h(q_1) \leq o(1), \tag{21}
\]
\[\ast = q_1 \leq q \leq kw, w \leq q_1 \leq (s - k)w.
\]

The left-hand side of \((21)\) is an increasing function of \( q \), thus we put \( q = kw \). This leads to
\[
\sup_{w \leq q_1 \leq \min(kw,(s-k)w)} (s - k)R - A(s - k, w, q_1) + kwh \left( \frac{q_1}{kw} \right) - h(q_1) \leq o(1). \tag{22}
\]

Note that condition \((22)\) is weaker than condition \((20)\)
for \( q_1 \geq kw/2 \); for \( q_1 \leq kw/2 \) it coincides with condition \((19)\).
Therefore, it can be omitted.

**Proof of Lemma 6** Consider function \( f(q) = A(s, w, q) + h(q) \) as a function of \( q \), \( w \leq q \leq \min(sw, 1) \).

**Proposition 4.** Functions \( f(q) \) attains its minimal value at the point \( q_{\min} = \frac{w}{2(1 - 2^{-s})} \).

**Proof of Proposition 4** Using the representation \((7)-(8)\) we represent \( f(q) \) as a function of \( y \). Taking derivative we find that it attains its minimal value at the point \( y = 2^{-1/s} \). Since there is a bijection between \( q \) and \( y \), we conclude that \( f(q) \) attains its minimal value at the corresponding point \( q_{\min} \).  

Let \( K \) be a set \( \{0, 1, \ldots, [s/2]\} \). The following chain of inequalities holds.
\[
R(s, \infty, K) \geq \sup_{0 < w < 1} \min_{k \in K} \min(R_1(s, k, w), R_2(s, k, w)) \geq \sup_{0 < w < 1} \min_{k \in K} \frac{A(s - k, w, q_{\min}) - kw + h(q_{\min})}{s - k} \geq \sup_{0 < w < 1} \min_{k \in K} h(w) + w \left( \log_2 \left( 2^{1/(s-k)} - 1 \right) - \frac{k}{s - k} \right). \tag{23}
\]

Function \( \log_2 \left( 2^{1/(s-k)} - 1 \right) - \frac{k}{s - k} \) is a concave function of \( k \), therefore, its minimum is achieved either at \( k = 0 \) or \( k = [s/2] \). It is easy to check that the minimum is attained at \( k = 0 \). Thus,
\[
R(s, \infty, K) \geq \sup_{0 < w < 1} h(w) + w \left( \log_2 \left( 2^{1/s} - 1 \right) \right), \tag{24}
\]
which leads to
\[
R(s, \infty, K) \geq \frac{1}{s}
\]
for \( w = 1 - 2^{-1/s} \).