V. A. Kopytcev, V. G. Mikhailov, On an asymptotical property of spheres in the discrete spaces of large dimension, *Mat. Vopr. Kriptogr.*, 2014, Volume 5, Issue 1, 73–83

DOI: 10.4213/mvk107

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2014 Т. 5 № 1 С. 73–83

УДК: 519.212.2

Об одном асимптотическом свойстве сфер в дискретных пространствах большой размерности

В. А. Копытцев[1], **В. Г. Михайлов**[2]

[1]Академия криптографии Российской Федерации, Москва
[2]Математический институт им. В. А. Стеклова РАН, Москва

Получено 26.XII.2012

Изучается одно асимптотическое (при $m \to \infty$) свойство множеств в m-мерных линейных пространствах K^m над конечным полем K, часто используемое в условиях предельных теорем пуассоновского типа для числа решений систем случайных линейных уравнений и случайных включений над этим полем. Показано, что этим свойством обладают сферы (в метрике Хемминга) в K^m при $m \to \infty$ и любом характере изменения радиусов сфер, обеспечивающем неограниченное возрастание чисел их элементов.

Ключевые слова: линейные пространства над конечными полями, метрика Хемминга, случайные линейные включения

On an asymptotical property of spheres in the discrete spaces of large dimension

V. A. Kopytcev[1], **V. G. Mikhailov**[2]

[1]*Academy of Cryptography of the Russian Federation, Moscow*
[2]*Steklov Mathematical Institute of RAS, Moscow*

Abstract. We study an asymptotic (as $m \to \infty$) property of sets in m-dimensional linear spaces K^m over the finite field K. This property is used in the conditions of Poisson type limit theorems for the number of solutions of systems of random linear equations or random inclusions over finite field. It is shown that the spheres in K^m (with respect to the Hamming distance) possess this property for $m \to \infty$ if the dependence of their radii on m guarantees the unbounded growth of the numbers of their elements.

Key words: linear spaces over finite fields, Hamming distance, random linear inclusions

Citation: *Mathematical Aspects of Cryptography*, 2014, vol. 5, no. 1, pp. 73–83 (Russian).

1. Введение

Рассмотрим систему линейных включений

$$x \in D, \quad Ax \in B \tag{1}$$

над конечным полем K (со случайной матрицей размера $T \times n$). Здесь D и B — некоторые непустые подмножества линейных пространств K^n и K^T над полем K размерностей n и T соответственно. В условиях предельных теорем пуассоновского типа для числа решений системы (1) важными являются предположения об асимптотических свойствах при $n, T \to \infty$ множеств D и B. Эти свойства удобно описывать в терминах некоторой функции $\rho(H)$ множества H в пространстве K^m, $m = n, T$, условием (см. например, [1–3])

$$\rho(D)\rho(B) \to 0, \quad n, T \to \infty.$$

Функция $\rho(H)$ определяется следующим образом. Пусть $N(a_1, a_2, a_3, c, H)$ обозначает число решений системы из m линейных уравнений над полем K, записанной в виде уравнения

$$a_1 u^1 \oplus a_2 u^2 \oplus a_3 u^3 = c \tag{2}$$

относительно тройки векторов $(u^1, u^2, u^3) \in H^3$, где H — некоторое заданное подмножество K^m, $a_1, a_2, a_3 \in K \backslash \{0\}$, $c \in K^m$. Знаки $\oplus$ и $\ominus$ (см. ниже) обозначают сложение и вычитание векторов в линейных пространствах над полем K. Положим

$$N(H) = \max_{a_1, a_2, a_3, c} N(a_1, a_2, a_3, c, H),$$
$$\rho(H) = N(H)/|H|^2,$$

где $|H|$ обозначает число элементов конечного множества H. Естественно рассматривать случай $|H| \geq 2$. Нетрудно проверить, что $|H|^{-1} \leq \rho(H) \leq 1$.

Отношение $\rho(H) = N(H)/|H|^2$ является своего рода мерой близости множества H к какому-либо линейному или аффинному подпространству пространства K^m. Для линейных и аффинных подпространств H (и только для них) эта мера принимает максимально возможное значение $\rho(H) = 1$ (см. [4]).

Непосредственно из определения величины $\rho(H)$ вытекают следующие свойства.

А) Пусть $\alpha \in K \backslash \{0\}$, $h \in K^m$ и

$$\alpha H \oplus h = \{y = \alpha x \oplus h \colon x \in H\}.$$

Тогда $\rho(\alpha H \oplus h) = \rho(H)$.

Б) Пусть $H = H(m) \in K^m$ и $m \to \infty$. Из соотношения $\rho(H) \to 0$ вытекает, что $\rho(H \cup H') \to 0$ для любого множества $H' = H'(m) \in K^m$, удовлетворяющего условию $|H'|/|H| \to 0$ при $m \to \infty$.

В) Пусть $H = H(m) \in K^m$ и $\rho(H) \to 0$ при $m \to \infty$. Тогда $|H| \to \infty$.

Покажем, что условие

$$\rho(H) \to 0, \quad m \to \infty,$$

можно трактовать как «асимптотическую свободу множества $H = H(m)$ от линейных комбинаций». Пусть случайные векторы ξ^1, ξ^2 выбраны случайно и независимо из множества H в соответствии с равномерным распределением на нем. Тогда

$$N(a_1, a_2, a_3, c, H) = |H|^2 \mathbf{P}\{a_3^{-1}c \ominus a_3^{-1}a_1\xi^1 \ominus a_3^{-1}a_2\xi^2 \in H\},$$

а условие $\rho(H) \to 0$ эквивалентно соотношению

$$\max_{c \in K^m,\ a_1, a_2 \in K\setminus\{0\}} \mathbf{P}\{c \oplus a_1\xi^1 \oplus a_2\xi^2 \in H\} \to 0. \tag{3}$$

Из (3) следует, что для любого натурального числа $r \geq 3$ и любого набора независимых случайных величин $\xi^1, \ldots, \xi^r$, распределенных равномерно на множестве H, выполнено соотношение

$$\max_{c \in K^m,\ a_1, \ldots, a_r \in K\setminus\{0\}} \mathbf{P}\{c \oplus a_1\xi^1 \oplus \ldots \oplus a_r\xi^r \in H\} \to 0. \tag{4}$$

Чтобы убедиться в этом, достаточно применить к вероятности в левой части (4) формулу полной вероятности относительно значений случайных величин $\xi^3, \ldots, \xi^r$ и воспользоваться соотношением (3).

Соотношение (4) означает, что любая заданная комбинация вида $c \oplus a_1\xi^1 \oplus \ldots \oplus a_r\xi^r$ при больших значениях параметра m, скорее всего, не попадет в множество H.

Замечание 1. Когда множество H замкнуто относительно умножения на ненулевые элементы поля, соотношения (3) и (4) можно упростить, взяв в качестве множителей $a_1, \ldots, a_r$ единицы. Тогда условия (3) и (4) принимают вид

$$\max_{c \in K^m} \mathbf{P}\{c \oplus \xi^1 \oplus \xi^2 \in H\} \to 0, \quad \max_{c \in K^m} \mathbf{P}\{c \oplus \xi^1 \oplus \ldots \oplus \xi^r \in H\} \to 0.$$

Оценка для числа решений системы (2) впервые была получена и использована при изучении асимптотических свойств числа решений конкретного класса случайных линейных включений в [4]. Позднее она использовалась в [5] и [6]. Систематическое использование характеристики $\rho(H)$ в условиях предельных теорем для числа решений случайных линейных и нелинейных включений началось с упомянутых выше работ [1–3] и было продолжено в [7] и [8]. Эти работы показали, что характеристика $\rho(H)$ является удобным и адекватным средством описания достаточных условий в таких теоремах. В связи с этим были предприняты попытки изучения представляющих интерес для приложений классов множеств в пространствах растущей размерности с целью проверки наличия у них свойства «асимптотической свободы» от линейных комбинаций. Так, в работе [1] были рассмотрены последовательности шаров и сфер относительно метрики Хемминга в K^m:

$$S_r(y^0) = \left\{ y \in K^m \colon 1 \le \|y - y^0\| \le r(m) \right\},$$

$$S'_r(y^0) = \left\{ y \in K^m \colon \|y - y^0\| = r(m) \right\}.$$

Здесь $\|x\|$ — число ненулевых элементов в записи вектора $x \in K^m$. Отметим, что значения функции ρ на шарах и сферах не зависят от выбора их центра y^0: $\rho(S_r(y^0)) = \rho(S_r(0^m))$, $\rho(S'_r(y^0)) = \rho(S'_r(0^m))$.

В [1] было доказано следующее утверждение.

Теорема А. *Пусть* $K = GF(q)$,

$$m \to \infty, \quad r = r(m) \ge 1, \ r(m)m^{-1} \le \beta$$

при некотором числе $0 < \beta < (q-1)/q$. *Тогда* $\rho(S_r(y^0)) \to 0$ *и* $\rho(S'_r(y^0)) \to 0$ *при любых* $y^0 = y^0(m) \in K^m$.

В настоящей заметке мы продолжаем эти исследования и даем описание асимптотических свойств величины $\rho(S'_r(y^0))$ при произвольном характере изменения радиуса сферы $S'_r(y^0)$. Получены следующие результаты.

Теорема 1. *Пусть* $K = GF(q)$,

$$m \to \infty, \quad r(m) \to \infty, \ m - r(m) \to \infty.$$

Тогда $\rho(S'_r(y^0)) \to 0$ *при любых* $y^0 = y^0(m) \in K^m$.

Теорема 2. *Пусть* $K = GF(q)$, $q \ge 3$,

$$m \to \infty, \quad m - r(m) = O(1). \tag{5}$$

Тогда $\rho(S'_r(y^0)) \to 0$ *при любых* $y^0 = y^0(m) \in K^m$.

Из теоремы А и теорем 1 и 2 выводится основной результат статьи.

Теорема 3. *Пусть* $K = GF(q)$, $m \to \infty$, $1 \le r = r(m) \le m - 1$ *при* $q = 2$, $1 \le r = r(m) \le m$ *при* $q \ge 3$. *Тогда* $\rho(S'_r(y^0)) \to 0$ *при любых* $y^0 = y^0(m) \in K^m$.

Замечание. Утверждение теоремы 3 было анонсировано в [9]. Оно означает, что свойство «асимптотической свободы от линейных комбинаций» выполнено для сфер относительно метрики Хемминга в K^m при любом характере изменения радиуса сферы, обеспечивающем неограниченное возрастание числа элементов сферы.

Замечание. При изучении асимптотических свойств числа решений систем соотношений $x \in D$, $Ax = b$, где $D = S_r(y^0)$ или $D = S'_r(y^0)$, отвечающих решениям системы случайных линейных уравнений $Ax = b$, попадающим в указанные шары или сферы, в литературе использовались и иные подходы (см. [10, 11]).

2. Доказательства

Доказательство теоремы 1. В силу замечания 1 и свойства А) функции ρ нам достаточно показать, что при $m \to \infty$

$$\max_{c \in K^m} \mathbf{P}\{c \oplus \xi^1 \oplus \xi^2 \in S'_r(0)\} \to 0.$$

Так как распределение случайных величин ξ^i инвариантно относительно перестановок координат, то

$$\begin{aligned} &\mathbf{P}\{c \oplus \xi^1 \oplus \xi^2 \in S'_r(0)\} = \\ &= \sum_{h \in K^m} \mathbf{P}\{h \oplus \xi^2 \in S'_r(0) \mid c \oplus \xi^1 = h\}\mathbf{P}\{c \oplus \xi^1 = h\} = \\ &= \sum_{s=0}^{m} \mathbf{P}\{\|h \oplus \xi^2\| = r \mid \|h\| = s\}\mathbf{P}\{\|c \oplus \xi^1\| = s\}. \end{aligned} \tag{6}$$

В слагаемом правой части (6) считается, что векторы ξ^2 и $h \oplus \xi^2$ содержат по r ненулевых элементов каждый, а вектор h содержит s ненулевых элементов. Пусть j — число общих ненулевых координат у векторов ξ^2 и h. Тогда, очевидно, среди последних имеется ровно $r - (r - j) - (s - j) = 2j - s \ge 0$ координат, которые в векторе $h \oplus \xi^2$ отличны от нуля. Используя этот факт, а также

записи $h = (h_1, \ldots, h_m)$, $\xi^2 = (\xi_1^2, \ldots, \xi_m^2)$ и формулу полной вероятности, получаем:

$$\begin{aligned}
&\mathbf{P}\left\{\|h \oplus \xi^2\| = r \mid \|h\| = s\right\} = \\
&= \sum_{j=0}^{\min\{r,s\}} \mathbf{P}\left\{\|h \oplus \xi^2\| = r, |\{i\colon h_i\xi_i^2 \neq 0\}| = j \mid \|h\| = s\right\} = \\
&= \frac{1}{C_m^r (q-1)^r} \sum_{s/2 \le j \le \min\{r,s\}} C_s^j C_{m-s}^{r-j} (q-1)^{r-j} C_j^{2j-s} (q-2)^{2j-s}.
\end{aligned} \tag{7}$$

Рассмотрим случай $q \geq 3$. Из (7) получаем

$$\begin{aligned}
&\mathbf{P}\left\{\|h \oplus \xi^2\| = r \mid \|h\| = s\right\} = \\
&= \sum_{s/2 \le j \le \min\{r,s\}} \frac{C_s^j C_{m-s}^{r-j}}{C_m^r} C_j^{s-j} \left(\frac{q-2}{q-1}\right)^j \left(\frac{1}{q-2}\right)^{s-j} \le \\
&\le \max_{s/2 \le j \le s} C_j^{s-j} \left(\frac{q-2}{q-1}\right)^j \left(\frac{1}{q-2}\right)^{s-j}.
\end{aligned}$$

Значение j^* параметра j, при котором достигается указанный максимум, равно

$$j^* = \frac{s(q-1)}{q}.$$

Поэтому

$$\begin{aligned}
&\max_{s/2 \le j \le s} C_j^{s-j} \left(\frac{q-2}{q-1}\right)^j \left(\frac{1}{q-2}\right)^{s-j} = \\
&= \max_{\alpha \in \{0,1\}} \left\{ C_{[j^*]+\alpha}^{s-[j^*]-\alpha} \left(\frac{q-2}{q-1}\right)^{[j^*]+\alpha} \left(\frac{1}{q-2}\right)^{s-[j^*]-\alpha} \right\}.
\end{aligned}$$

Непосредственные вычисления показывают, что найдется константа $C_1 < \infty$, при которой выражение в правой части этого равенства не превосходит

$$C_1 C_{[j^*]}^{s-[j^*]} \left(\frac{q-2}{q-1}\right)^{j^*} \left(\frac{1}{q-2}\right)^{s-j^*}$$

Используя формулу Стирлинга $k! = \sqrt{2\pi k}(k/e)^k(1 + o(1))$ при $k \to \infty$, получаем также, что найдется константа $C_2 < \infty$, при которой

$$C_{[j^*]}^{s-[j^*]} \le C_2 \sqrt{\frac{q(q-1)}{s(q-2)}} \frac{(q-1)^{s(q-1)/q}}{(q-2)^{s(q-2)/q}}.$$

Следовательно,

$$\begin{gathered}\max_{s/2\le j\le s} C_j^{s-j}\left(\frac{q-2}{q-1}\right)^j\left(\frac{1}{q-2}\right)^{s-j}\le\\ \le C_1 C_{[j^*]}^{s-[j^*]}\left(\frac{q-2}{q-1}\right)^{j^*}\left(\frac{1}{q-2}\right)^{s-j^*}\le\\ \le C_1C_2\sqrt{\frac{q(q-1)}{s(q-2)}}\frac{(q-1)^{s(q-1)/q}}{(q-2)^{s(q-2)/q}}\cdot\left(\frac{q-2}{q-1}\right)^{s(q-1)/q}\left(\frac{1}{q-2}\right)^{s/q}=\\ =C_1C_2\sqrt{\frac{q(q-1)}{s(q-2)}}.\end{gathered}\tag{8}$$

Оценим теперь вероятность $\mathbf{P}\{\|c\oplus\xi^1\|\le t\}$. Имеем

$$\begin{gathered}\mathbf{P}\{\|c\oplus\xi^1\|\le t\}=\frac{|\{y\colon \|y\|=r,\ \|c\oplus y\|\le t\}|}{|\{y\colon \|y\|=r\}|}\le\\ \le\frac{|\{y\colon \|c\oplus y\|\le t\}|}{|\{y\colon \|y\|=r\}|}=\frac{\sum_{s=0}^t C_m^s(q-1)^s}{C_m^r(q-1)^r}.\end{gathered}\tag{9}$$

Выбрав $t=\ln r$, из (6), (8) и (9) получаем:

$$\begin{gathered}\mathbf{P}\{c\oplus\xi^1\oplus\xi^2\in S_r'(0)\}=\\ =\sum_{s=0}^m\mathbf{P}\{\|h\oplus\xi^2\|=r\mid\|h\|=s\}\mathbf{P}\{\|c\oplus\xi^1\|=s\}\le\\ \le\sum_{t+1\le s\le m}\mathbf{P}\{\|h\oplus\xi^2\|=r\mid\|h\|=s\}\mathbf{P}\{\|c\oplus\xi^1\|=s\}+\\ +\mathbf{P}\{\|c\oplus\xi^1\|\le t\}\le\\ \le C_1C_2\sqrt{\frac{q(q-1)}{s(q-2)}}+\frac{\sum_{s=0}^t C_m^s(q-1)^s}{C_m^r(q-1)^r}\to 0.\end{gathered}\tag{10}$$

В случае $q\ge 3$ утверждение теоремы доказано.

Пусть теперь $q=2$. Так как в этом случае $S_r'(y)=S_{m-r}'(z(y))$, где $z(y)=(1,\dots,1)\oplus y$, то можно считать, что $r\le m/2$.

Положив в (7) $q=2$, получим

$$\mathbf{P}\left\{\|h\oplus\xi^2\|=r\mid\|h\|=s\right\}=0,$$

если $s > 2r$ или число s нечетно, а при четных $s \leq 2r \leq m$

$$\mathbf{P}\left\{\|h \oplus \xi^2\| = r \mid \|h\| = s\right\} = \frac{C_s^{s/2} C_{m-s}^{r-s/2}}{C_m^r}. \tag{11}$$

Покажем, что выражение в правой части (11) монотонно возрастает по r, $s/2 + 1 \leq r \leq m/2$. Действительно,

$$\frac{\frac{C_s^{s/2} C_{m-s}^{r-s/2}}{C_m^r}}{\frac{C_s^{s/2} C_{m-s}^{r-s/2-1}}{C_m^{r-1}}} = \frac{C_{m-s}^{r-s/2} C_m^{r-1}}{C_{m-s}^{r-s/2-1} C_m^r} =$$

$$= \frac{(r - s/2 - 1)!(m - s - r + s/2 + 1)!}{(r - s/2)!(m - s - r + s/2)!} \cdot \frac{r!(m-r)!}{(r-1)!(m - r + 1)!} =$$

$$= \frac{m - r + 1 - s/2}{m - r + 1} \cdot \frac{r}{r - s/2}.$$

При $r = s/2 + 1$ это отношение больше единицы, и оно убывает с ростом r при $r \geq s/2 + 1$. Обозначим через r^* наибольшее значение r, при котором это отношение больше 1. Будем искать его как решение (не обязательно целочисленное) уравнения

$$(m - r^* + 1 - s/2)r^* = (m - r^* + 1)(r^* - s/2).$$

Оно имеет единственное решение $(m + 1)/2$. Значит,

$$r^* \in \left\{\left[\frac{m+1}{2}\right], \left[\frac{m+1}{2}\right] + 1\right\}.$$

Используя вытекающее из локальной предельной теоремы Муавра–Лапласа (см. формулу (3.9) на стр. 198 книги [12]), соотношение

$$C_{2k}^{k+\delta} = \frac{1}{\sqrt{\pi k}} 2^{2k}(1 + o(1)), \quad \delta \in \{-1, 0, 1\} \quad \text{при } k \to \infty,$$

получаем, что при некотором $C < \infty$ и достаточно больших m

$$\frac{C_s^{s/2} C_{m-s}^{r-s/2}}{C_m^r} \leq \frac{C_s^{s/2} C_{m-s}^{r^*-s/2}}{C_m^{r^*}} \leq C\sqrt{\frac{m}{s(m-s)}}. \tag{12}$$

Напомним, что здесь s — четное число.

Вероятность $\mathbf{P}\{\|c \oplus \xi^1\| \le t\}$ оценивается по формуле (9). Имеем

$$\mathbf{P}\{\|c \oplus \xi^1\| \le t\} \le \frac{1}{C_m^r} \sum_{s=0}^{t} C_m^s.$$

Аналогично,

$$\mathbf{P}\{\|c \oplus \xi^1\| \ge m - t\} = \frac{1}{C_m^r} \sum_{s=0}^{t} C_m^s. \tag{13}$$

Из (6), (11), (12)–(13) аналогично (10) получаем:

$$\begin{gathered}\mathbf{P}\{c \oplus \xi^1 \oplus \xi^2 \in S_r'(0)\} \le \\ \le \sum_{t+1 \le 2l \le m-t} \mathbf{P}\{\|h \oplus \xi^2\| = r \mid \|h\| = 2l\}\mathbf{P}\{\|c \oplus \xi^1\| = 2l\} + \\ + \mathbf{P}\{\|c \oplus \xi^1\| \le t\} + \mathbf{P}\{\|c \oplus \xi^1\| \ge m - t\} \le \\ \le C\sqrt{\frac{m}{t(m-t)}} + 2\frac{\sum_{s=0}^{t} C_m^s}{C_m^r}\end{gathered}$$

при любом $1 \le t < m/2$. Взяв $t = \ln r$, придем к соотношению

$$\mathbf{P}\{c \oplus \xi^1 \oplus \xi^2 \in S_r'(0)\} \to 0$$

при $m,\ r,\ m - r \to \infty$. Этим доказательство теоремы 1 завершено.

Доказательство теоремы 2. Согласно свойству А) достаточно рассмотреть случай, когда $y^0 = 0^m$. Здесь и далее 0^m и 1^m — m-мерные векторы, составленные только из нулей и только из единиц соответственно.

Разобьем множество $S_r'(0^m)$ на не пересекающиеся подмножества:

$$S_r'(0^m) = \bigcup_{U \subset \{1,\dots,m\}:\ |U|=r} S(U), \tag{14}$$

где $S(U) = \{(x_1, \dots, x_m) \in K^m : x_j \ne 0\ \forall j \in U\}$. Тогда

$$N(S_r'(0^m)) \le \bigcup_{U_1,U_2,U_3 \subset \{1,\dots,m\}} N(S(U_1), S(U_2), S(U_3)). \tag{15}$$

При заданных множествах U_1, U_2, U_3 в системе (2) имеются по крайней мере $m-3(m-r)$ уравнений над полем K относительно $u_1^t, u_2^t, u_3^t \in K\backslash\{0\}$ (t — номер такого уравнения). Согласно теореме 1 каждое такое уравнение имеет

не более $(q-1)^2-1$ решений. В свою очередь, подсистема из остальных уравнений имеет не более $q^{2\cdot 3(m-r)}$ решений (по q^2 решений на каждое ее уравнение). Поэтому

$$N(S(U_1),S(U_2),S(U_3)) \le q^{6(m-r)}\left((q-1)^2-1\right)^{m-3(m-r)}.$$

Используя (5), (14), (15) и равенства $S'_r(0^m)=C_m^r(q-1)^r$, получаем

$$\rho(S'_r(0^m)) = \frac{N(S'_r(0^m))}{(C_m^r(q-1)^r)^2} \le C_m^r\left(\frac{q^2}{(q-1)^2-1}\right)^{3(m-r)}\frac{\left((q-1)^2-1\right)^m}{(q-1)^{2r}} =$$
$$= C_m^{m-r}\left(\frac{q^6(q-1)^2}{((q-1)^2-1)^3}\right)^{m-r}\left(1-\frac{1}{(q-1)^2}\right)^m =$$
$$= \exp\left\{m\left(\ln\left(1-\frac{1}{(q-1)^2}\right)+o(1)\right)\right\} = o(1).$$

Поэтому $\rho(S'_r(y^0)) = \rho(S'_r(0^m)) \to 0$. Теорема 2 доказана.

Доказательство теоремы 3. В случае $q \ge 3$ утверждение теоремы 3 следует из теорем А, 1 и 2. В случае $q=2$, $r \le m-1$ оно следует из теорем А и 1 и равенств $\rho(S'_{m-r}(y^0)) = \rho(S'_{m-r}(0^m)) = \rho(S'_r(1^m)) = \rho(S'_r(0^m))$. Теорема 3 доказана.

Авторы признательны А. В. Лапшину за полезные замечания.

Список литературы

1. *Копытцев В. А., Михайлов В. Г.* Теоремы пуассоновского типа для числа специальных решений случайного линейного включения // Дискретная математика. — 2010. — Т. 22. Вып. 2. — С. 3–21.
2. *Копытцев В. А., Михайлов В. Г.* Теоремы пуассоновского типа для числа решений случайных включений // Математические вопросы криптографии. — 2010. — Т. 1. Вып. 4. — С. 63–84.
3. *Копытцев В. А., Михайлов В. Г.* О распределении чисел решений случайных включений // Математические вопросы криптографии. — 2011. — Т. 2. Вып. 2. — С. 55–80.
4. *Михайлов В. Г.* Предельная теорема для числа неколлинеарных решений системы случайных уравнений специального вида // Дискретная математика. — 2001. — Т. 13. Вып. 3. — С. 81–90.

5. *Михайлов В. Г.* Предельные теоремы для числа точек случайного линейного подпространства, попавших в заданное множество // Дискретная математика. — 2003. — Т. 15. Вып. 2. — С. 128–157.
6. *Михайлов В. Г.* Предельные теоремы для числа решений системы случайных линейных уравнений, попавших в заданное множество // Дискретная математика. — 2007. — Т. 19. Вып. 1. — С. 17–26.
7. *Копытцев В. А., Михайлов В. Г.* Условия сходимости к распределению Пуассона для чисел решений случайных включений // Математические вопросы криптографии. — 2012. — Т. 3. Вып. 3. — С.35–55.
8. *Копытцев В. А., Михайлов В. Г.* Предельные теоремы пуассоновского типа для обобщенного линейного включения // Дискретная математика. — 2012. — Т. 24. Вып. 3. — С. 108–121.
9. *Копытцев В. А., Михайлов В. Г.* Об одном асимптотическом свойстве сфер в дискретных пространствах большой размерности // Обозр. прикл. и промышл. матем. — 2011. — Т. 18. Вып. 5. — С. 786.
10. *Копытцев В. А.* О числе решений систем линейных булевых уравнений в множестве векторов, обладающих заданным числом единиц // Дискретная математика. — 2002. — Т. 14. Вып. 4. — С. 87–109.
11. *Копытцев В. А.* О числе решений системы случайных линейных уравнений // Дискретная математика. — 2006. — Т. 18. Вып. 1. — С. 40–62.
12. *Феллер В.* Введение в теорию вероятностей и ее приложения. Т. 1. — М.: Мир, 1984, 528 с.