V. A. Kopyttsev, A multivariate Poisson theorem for the number of solutions close to given vectors of a system of random linear equations, *Diskr. Mat.*, 2007, Volume 19, Issue 4, 3–22

DOI: 10.4213/dm974

Дискретная математика

том 19 выпуск 4 * 2007

УДК 519.2

Многомерная теорема Пуассона для чисел решений, близких к заданным векторам, у системы случайных линейных уравнений

© 2007 г. В. А. Копытцев

Рассматривается число $\xi(A, b \mid z)$ таких решений системы случайных линейных уравнений $Ax = b$ над конечным полем K, которые принадлежат множеству $X_r(z)$ векторов, отличающихся от некоторого заранее выбранного вектора z в заданном числе r координат (или не более, чем в заданном числе координат). Приведены условия, когда при согласованном росте числа неизвестных, числа уравнений и числа несовпадающих координат в качестве предельного распределения для вектора вида $(\xi(A, b \mid z^{(1)}), \ldots, \xi(A, b \mid z^{(k)}))$ (или для вектора, полученного из указанного после нормирования или сдвига на единицу отдельных компонент) выступает k-мерное пуассоновское распределение. В качестве следствия получены предельные распределения для величины $\xi(A, b \mid z^{(1)}, \ldots, z^{(k)})$, равной числу решений системы, принадлежащих объединению множеств $X_r(z^{(s)})$, $s = 1, \ldots, k$. Работа продолжает исследования, проводившиеся в ряде работ автора и В. Г. Михайлова.

1. Введение

Рассмотрим систему $Ax = b$ из T линейных уравнений над конечным полем K относительно n неизвестных со случайной матрицей $A = (a_{t,i})$ размера $T \times n$, элементы которой независимы в совокупности,

$$\mathbf{P}\{a_{t,i} = \nu\} = \frac{1 + \Delta_{t,i}^{(\nu)}}{q}, \quad \nu \in K, \quad \sum_{\nu \in K} \Delta_{t,i}^{(\nu)} = 0,$$

$q = |K|$ — число элементов поля K.

Относительно вектора $b \in K^T$ будем различать два случая. В первом случае элементы вектора b не зависят от элементов матрицы A, вектор b может быть детерминированным или случайным. Во втором случае $b = Ax^0$, где $x^0 \in K^n$ — заданный вектор.

В каждом из вышеуказанных случаев нас будет интересовать число решений системы $Ax = b$, удовлетворяющих условию

$$x \in X_r(z) = \{x \in K^n : \|x - z\| = r\}, \qquad r \geqslant 1, \tag{1.1}$$

или условию

$$x \in X_r^*(z) = \{x \in K^n : 1 \leqslant \|x - z\| \leqslant r\}, \tag{1.2}$$

где z — заданный вектор, $x-z=(x_1-z_1,\dots,x_n-z_n)$, $\|y\|$ — число ненулевых координат вектора $y\in K^n$.

Обозначим $\xi(A,b\mid z)$ и $\xi^*(A,b\mid z)$ число решений системы $Ax=b$ с независимым от матрицы A вектором b, удовлетворяющих условиям (1.1) и (1.2) соответственно.

Обозначим $\eta(A\mid x^0,z)$ и $\eta^*(A\mid x^0,z)$ число решений системы $Ax=Ax^0$, удовлетворяющих условиям (1.1) и (1.2) соответственно.

Отметим, что число решений системы $Ax=Ax^0$, удовлетворяющих условию (1.1) (условию (1.2)), совпадает с числом решений системы $A((z-x^0)+y)=0^T$ относительно векторов y: $\|y\|=r$ $(1\leqslant\|y\|\leqslant r)$. Поэтому

$$\eta(A\mid x^0,z)=\xi(A,0^T\mid z-x^0), \tag{1.3}$$

$$\eta^*(A\mid x^0,z)=\xi^*(A,0^T\mid z-x^0). \tag{1.4}$$

Таким образом, исследование величин η и η^* сводится к исследованию величин ξ и ξ^* соответственно.

Положим

$$\Delta=\max_{t,i,v}|\Delta_{t,i}^{(v)}|=\max_{t,i,v}|q\mathbf{P}\{a_{t,i}=v\}-1|.$$

Будем использовать запись $\xi\to\Pi(\lambda)$ для обозначения предельных соотношений

$$\mathbf{P}\{\xi=k\}\to\frac{\lambda^k}{k!}e^{\lambda},\qquad k=0,1,\dots$$

В [2] показано (см. в этой работе теорему 1), что если

$$n,T\to\infty,\qquad r=o(n), \tag{1.5}$$

$$\binom{n}{r}(q-1)^rq^{-T}\to\lambda>0, \tag{1.6}$$

$$\Delta\to0,\qquad T\Delta^r\to0, \tag{1.7}$$

то равномерно относительно векторов $b\in K^T\setminus\{0^T\}$

$$\xi(A,b\mid0^n)\to\Pi(\lambda),$$

и в случае $b=0^T$

$$\frac{1}{q-1}\xi(a,0^T\mid0^n)\to\Pi(\lambda/(q-1)).$$

Пусть $z(0)=0^n$, а $z(1),\dots,z(h)\in K^n\setminus\{0^n\}$ — некоторые заданные ненулевые векторы. В настоящей работе показывается, что подход работы [2] можно успешно применить для изучения совместного распределения величин $\xi(A,b\mid z(s))$, $s=0,1,\dots,h$, и совместного распределения величин $\xi^*(A,b\mid z(s))$, $s=0,1,\dots,h$.

Для обозначения предельных соотношений

$$\mathbf{P}\{\xi_0=k_0,\dots,\xi_h=k_h\}\to\frac{\lambda_0^{k_0}e^{-\lambda_0}}{k_0!}\cdots\frac{\lambda_h^{k_h}e^{-\lambda_h}}{k_h!},\qquad k_s=0,1,\dots,$$

будем использовать запись $(\xi_s,\ s=0,1,\dots,h)\to\Pi(\lambda_0)\dots\Pi(\lambda_h)$. В случае, когда $\lambda_s=\lambda$, $s=0,1,\dots,h$, правую часть этой записи будем обозначать $\Pi^{h+1}(\lambda)$, и будем ее обозначать $\Pi(\lambda_0)\Pi^h(\lambda)$, если $\lambda_0\neq\lambda$, $\lambda_s=\lambda$, $s=1,\dots,h$.

Теорема 1. *Пусть $h \geqslant 2$, выполняются условия* (1.5), (1.6) *и $T\Delta \to 0$. Тогда*

(1) *в случае $b \neq 0^T$*

$$(\xi(A, b \mid z(s)),\ s = 0, 1, \ldots, h) \to \Pi^{h+1}(\lambda), \tag{1.8}$$

$$(\xi^*(A, b \mid z(s)),\ s = 0, 1, \ldots, h) \to \Pi^{h+1}(\lambda), \tag{1.9}$$

равномерно относительно векторов $b \in K^T \setminus \{0^T\}$ и линейно независимых векторов $z(1), \ldots, z(h) \in K^n$;

(2) *в случае $b = 0^T$ при любом целом h_1, $1 \leqslant h_1 < h$,*

$$\left(\frac{\xi(A, 0^T \mid 0^n)}{q-1}; \xi(A, 0^T \mid z(s)) - 1,\ s = 1, \ldots, h_1;\right.$$

$$\left.\xi(A, 0^T \mid z(s)),\ s = h_1 + 1, \ldots, h\right) \to \Pi(\lambda/(q-1))\Pi^h(\lambda) \tag{1.10}$$

равномерно относительно векторов $z(1), \ldots, z(h) \in K^n$ таких, что

$$\|z(s)\| = r, \qquad s = 1, \ldots, h_1, \tag{1.11}$$

$$\|z(s)\| \neq r, \qquad s = h_1 + 1, \ldots, h, \tag{1.12}$$

$$\operatorname{rank}(z(1), \ldots, z(h)) = h. \tag{1.13}$$

Пусть $h \geqslant 2$, выполняются условия (1.5), (1.6) *и $T\Delta \to 0$. Тогда справедливо утверждение, полученное из утверждения* 2 *теоремы после замены в соотношении* (1.10) *величин ξ соответствующими величинами ξ^* и после замены условий* (1.11), (1.12) *условиями*

$$\|z(s)\| \leqslant r, \qquad s = 1, \ldots, h_1,$$

$$\|z(s)\| > r, \qquad s = h_1 + 1, \ldots, h.$$

Из равенств (1.3), (1.4) и утверждения 2 теоремы 1 вытекает следующее утверждение.

Следствие 1. *Пусть $h \geqslant 2$, выполняются условия* (1.5), (1.6) *и $T\Delta \to 0$. Тогда при любом целом h_1, $1 \leqslant h_1 < h$,*

$$\left(\frac{\eta(A \mid x^0, x^0)}{q-1};\ \eta(A \mid x^0, z(s)) - 1,\ s = 1, \ldots, h_1;\ \eta(A \mid x^0, z(s)),\ s = h_1 + 1, \ldots, h\right)$$

$$\to \Pi(\lambda/(q-1))\Pi^h(\lambda) \tag{1.14}$$

равномерно относительно векторов $x^0, z(1), \ldots, z(h)$ таких, что

$$\|z(s) - x^0\| = r, \qquad s = 1, \ldots, h_1, \tag{1.15}$$

$$\|z(s) - x^0\| \neq r, \qquad s = h_1 + 1, \ldots, h, \tag{1.16}$$

$$\operatorname{rank}(z(1) - x^0, \ldots, z(h) - x^0) = h. \tag{1.17}$$

Пусть $h \geqslant 2$, выполняются условия (1.5), (1.6) *и $T\Delta \to 0$. Тогда справедливо утверждение, полученное из утверждения первой части следствия после замены в соотношении* (1.14) *величин η соответствующими величинами η^* и после замены условий* (1.15), (1.16) *условиями*

$$\|z(s) - x^0\| \leqslant r, \qquad s = 1, \ldots, h_1,$$

$$\|z(s) - x^0\| > r, \qquad s = h_1 + 1, \ldots, h.$$

Пусть $z^{(1)},\dots,z^{(k)}$ — попарно различные векторы. Обозначим $\xi(A,b \mid z^{(1)},\dots,z^{(k)})$ и $\xi^*(A,b \mid z^{(1)},\dots,z^{(k)})$ число решений системы $Ax = b$ с независимым от матрицы A вектором b, удовлетворяющих условию

$$x \in \bigcup_{i=1}^{k} X_r(z^{(i)}) \tag{1.18}$$

и условию

$$x \in \bigcup_{i=1}^{k} X_r^*(z^{(i)}) \tag{1.19}$$

соответственно. Обозначим $\eta(A \mid x^0, z^{(1)},\dots,z^{(k)})$ и $\eta^*(A \mid x^0, z^{(1)},\dots,z^{(k)})$ число решений системы $Ax = Ax^0$, удовлетворяющих условию (1.18) и условию (1.19) соответственно. Несложно проверить, что имеют место соотношения, аналогичные соотношениям (1.3), (1.4):

$$\eta(A \mid x^0, z^{(1)},\dots,z^{(k)}) = \xi(A, 0^T \mid z^{(1)} - x^0, \dots z^{(k)} - x^0), \tag{1.20}$$

$$\eta^*(A \mid x^0, z^{(1)},\dots,z^{(k)}) = \xi^*(A, 0^T \mid z^{(1)} - x^0, \dots z^{(k)} - x^0). \tag{1.21}$$

Пусть $\pi(\lambda)$ — случайная величина, распределенная по закону Пуассона с параметром $\lambda > 0$; k_1, k_2 — заданные действительные числа, $k_1 \neq 0$. Обозначим $k_1\Pi(\lambda) + k_2$ распределение случайной величины $k_1\pi(\lambda) + k_2$; обозначим $P_1 * P_2$ композицию (свертку) дискретных распределений P_1, P_2. Для обозначения сходимости (слабой) распределения величины ξ к распределению $\mathcal{P}$ будем использовать запись $\xi \to \mathcal{P}$.

Как и прежде, будем полагать, что $z(0) = 0^n$, $z(1),\dots,z(h) \in K^n \setminus \{0^n\}$.

Теорема 2. *Пусть $h \geqslant 1$, выполняются условия* (1.5), (1.6) *и $T\Delta \to 0$. Тогда*

(1) *в случае $b \neq 0^T$*

$$(\xi(A,b \mid z(0),\dots,z(h)) \to \Pi(\lambda(h+1)), \tag{1.22}$$

$$(\xi(A,b \mid z(1),\dots,z(h)) \to \Pi(\lambda h) \tag{1.23}$$

равномерно относительно векторов $b \in K^T \setminus \{0^T\}$ и линейно независимых векторов $z(1),\dots,z(h) \in K^n$;

(2) *в случае $b = 0^T$*

$$\xi(A, 0^T \mid z(0), z(1),\dots,z(h)) \to (q-1)\Pi(\lambda/(q-1)) * (\Pi(\lambda h) + 1), \tag{1.24}$$

$$\xi(A, 0^T \mid z(1),\dots,z(h)) \to \Pi(\lambda h) + 1 \tag{1.25}$$

равномерно относительно линейно независимых векторов $z(1),\dots,z(h) \in K^n$, удовлетворяющих условию

$$\exists s \in \{1,\dots,h\}: \quad \|z(s)\| = r; \tag{1.26}$$

(3) *в случае $b = 0^T$*

$$\xi(A, 0^T \mid z(0), z(1),\dots,z(h)) \to (q-1)\Pi(\lambda/(q-1)) * \Pi(\lambda h), \tag{1.27}$$

$$\xi(A, 0^T \mid z(1),\dots,z(h)) \to \Pi(\lambda h) \tag{1.28}$$

равномерно относительно линейно независимых векторов $z(1), \dots, z(h) \in K^n$, *удовлетворяющих условию*

$$\|z(s)\| \neq r, \qquad s = 1, \dots, h. \tag{1.29}$$

Пусть $h \geqslant 1$, *выполняются условия* (1.5), (1.6) *и* $T\Delta \to 0$. *Тогда имеют место утверждения, полученные из утверждений* 1, 2, 3 *теоремы после замены величин* ξ *соответствующими величинами* ξ^* *и после замены условия* (1.26) *условием*

$$\exists s \in \{1, \dots, h\}: \quad \|z(s)\| \leqslant r \tag{1.30}$$

и условия (1.29) — *условием*

$$\|z(s)\| > r, \qquad s = 1, \dots, h. \tag{1.31}$$

Замечание 1. Из многомерных предельных распределений теоремы 1 следуют одномерные предельные распределения, поэтому соотношения (1.22), (1.27) справедливы и при значении $h = 0$.

Замечание 2. Из равенств (1.20), (1.21) и утверждений 2, 3 теоремы 2 можно получить утверждения для величин η, η^*, аналогичные утверждениям следствия 1. Формулировки этих утверждений мы опускаем.

Замечание 3. Отметим, что из следствия 1 вытекают результаты работы [3], полученные В. Г. Михайловым путем исследования самой системы $Ax = Ax^0$.

Замечание 4. В отличие от теоремы 1 работы [2], где используется условие $\Delta \to 0$, $T\Delta^r \to 0$, в теоремах настоящей работы используется более сильное условие $T\Delta \to 0$. Это условие обеспечивает равномерную сходимость (к предельным распределениям) относительно векторов $z(1), \dots, z(h) \in K^n$, $\operatorname{rank}(z(1), \dots, z(h)) = h$, и обеспечивает идентичность (совпадение) предельных распределений для величин ξ и ξ^* (η и η^*).

Можно показать, что если выполняются условия (1.5), (1.6) и при этом $\Delta \to 0$, $T\Delta^r \to 0$, то

$$(\xi(A, b \mid z(s)),\ s = 0, 1, \dots, h) \to \Pi^{h+1}(\lambda)$$

при любой последовательности векторов $b \neq 0^T$ и векторов

$$z(1), \dots, z(h) \in K^n, \quad \|z(s)\|/r \to \infty, \quad s = 1, \dots, h; \tag{1.32}$$

в тех же условиях

$$\left(\frac{\xi(A, 0^T \mid z(0))}{q-1}; \xi(A, 0^T \mid z(s)),\ s = 1, \dots, h\right) \to \Pi(\lambda/(q-1))\Pi^h(\lambda)$$

при любой последовательности векторов (1.32).

Доказательство вышеуказанных утверждений, а также доказательство аналогичных утверждений для величин ξ^* (при этом может быть использовано некоторое условие, занимающее промежуточное положение между условиями $T\Delta \to 0$ и $\Delta \to 0$, $T\Delta^r \to 0$), выходит за рамки настоящей статьи.

Замечание 5. Из (1.5), (1.6) вытекает оценка

$$T = O(r \ln(n/r)). \tag{1.33}$$

Пользуясь оценкой (1.33), можно оценить скорость убывания величины Δ при условии $T\Delta \to 0$ ($T\Delta^r \to 0$).

Замечание 6. В качестве базового средства для доказательства теоремы 1 настоящей работы использована многомерная теорема Пуассона для сумм индикаторов, доказанная В. Г. Михайловым в [4].

2. Вспомогательные утверждения

Лемма 1. *Пусть* $x^1, \dots, x^m \in K^n$, $1 \leqslant m < n$. *Тогда при любом* $b \in K^T$

$$\mathbf{P}\{Ax^j = b, j = 1, \dots, m\} \leqslant \left(\frac{1+\Delta}{q}\right)^{Tk}, \tag{2.1}$$

если $\operatorname{rank}(x^1, \dots, x^m) = k \leqslant m$, *и*

$$\left(\frac{1-\Delta}{q}\right)^{Tm} \leqslant \mathbf{P}\{Ax^j = b,\ j = 1, \dots, m\} \leqslant \left(\frac{1+\Delta}{q}\right)^{Tm}, \tag{2.2}$$

если $\operatorname{rank}(x^1, \dots, x^m) = m$.

Лемма 1 повторяет лемму 3 работы [2].

Целью приведенных ниже лемм 2–8 является получение оценки ранга $\operatorname{rank}(x^1, \dots, x^m)$ системы векторов $x^1, \dots, x^m$, отличных в заданном числе r координат от векторов из заданного набора $z(0), z(1), \dots, z(h) \in K^n$, $z(0) = 0^n$, $\operatorname{rank}(z(1), \dots, z(h)) = h$.

Положим

$$Y_r = \{y \in K^n : \|y\| = r\}$$

и для векторов $y^1, \dots, y^m \in Y_r$, $r \geqslant 1$, положим

$$M(y^1, \dots, y^m) = \bigcup_{j=1}^{m} M(y^j),$$

где

$$\begin{aligned} M(y) &= \{i : y_i \neq 0\}, \\ \mu(y^1, \dots, y^m) &= |M(y^1, \dots, y^m)|, \\ \rho(y^1, \dots, y^m) &= rm - \mu(y^1, \dots, y^m). \end{aligned} \tag{2.3}$$

Следующие леммы 2 и 3 повторяют с несущественными отличиями в обозначениях и формулировках леммы 4 и 5 работы [2]. С учетом краткости доказательств приведем леммы 2 и 3 вместе с доказательствами.

Лемма 2. *Пусть $r \geqslant 1$, $y^1, \ldots, y^m \in Y_r$, $m \geqslant 2$, и*

$$\alpha_1 y^1 + \ldots + \alpha_m y^m = 0^n \tag{2.4}$$

при некоторых ненулевых $\alpha_1, \ldots, \alpha_m \in K \setminus \{0\}$. Тогда

$$\rho(y^1, \ldots, y^m) \geqslant rm/2. \tag{2.5}$$

Доказательство. Матрица $A(y^1, \ldots, y^m)$, составленная из строк $y^1, \ldots, y^m$, содержит rm ненулевых элементов, а число ненулевых столбцов в ней равно $\mu(y^1, \ldots, y^m)$. В силу (2.4), каждый ненулевой столбец содержит не менее двух ненулевых элементов. Поэтому $2\mu(y^1, \ldots, y^m) \leqslant rm$. Отсюда и из (2.3) следует (2.5). Лемма 2 доказана.

Лемма 3. *Пусть $r \geqslant 1$, $y^1, \ldots, y^m \in Y_r$, $m \geqslant 2$. Тогда*

$$\rho(y^1, \ldots, y^m) \geqslant \rho(y^1, \ldots, y^{m-1}). \tag{2.6}$$

Доказательство. Пусть $\nu_i(y^1, \ldots, y^m)$ — число ненулевых элементов i-го столбца матрицы $A(y^1, \ldots, y^m)$, составленной из строк $y^1, \ldots, y^m$. Положим

$$\rho_i(y^1, \ldots, y^m) = (\nu_i(y^1, \ldots, y^m) - 1) I(\nu_i(y^1, \ldots, y^m) > 0),$$

где $I\{B\}$ — индикатор события B. Нетрудно убедиться, что

$$\rho(y^1, \ldots, y^m) = \sum_{i=1}^{n} \rho_i(y^1, \ldots, y^m), \tag{2.7}$$

при этом

$$\rho_i(y^1, \ldots, y^m) \geqslant \rho_i(y^1, \ldots, y^{m-1}), \tag{2.8}$$

так как $\nu_i(y^1, \ldots, y^m) \geqslant \nu_i(y^1, \ldots, y^{m-1})$. Из (2.7), (2.8) следует (2.6). Лемма 3 доказана.

Пусть при целом $h \geqslant 1$ задано $h+1$ попарно различных векторов $z(0) = 0^n$, $z(s) \in K^n \setminus \{0^n\}$, $s = 1, \ldots, h$, и $h+1$ соответствующих им комплектов векторов

$$y^{1,s}, \ldots, y^{m(s),s} \in Y_r, \qquad s = 0, 1, \ldots, h, \tag{2.9}$$

где $m(s) \geqslant 0$, $\sum_{s=0}^{h} m(s) \geqslant 2$. В случае, когда $m(s) = 0$, будем полагать, что комплект с номером s пуст. Положим

$$\bar{z}(s) = (\bar{z}_1(s), \ldots, \bar{z}_n(s)), \qquad \bar{\bar{z}}(s) = z(s) - \bar{z}(s), \tag{2.10}$$

где

$$\bar{z}_i(s)) = \begin{cases} z_i(s), & i \notin \bigcup_{s=0}^{h} M(y^{1,s}, \ldots, y^{m(s),s}), \\ 0 & \text{в противном случае.} \end{cases}$$

Лемма 4. *Пусть $x^{k,s} = z(s) + y^{k,s}$, $k = 1, \ldots, m(s)$, $s = 0, 1, \ldots, h$, $\sum_{s=0}^{h} m(s) \geqslant 2$ и $r \geqslant 1$, в каждом непустом комплекте $y^{1,s}, \ldots, y^{m(s),s} \in Y_r$ все векторы различны,*

$$\operatorname{rank}(\bar{z}(1), \ldots, \bar{z}(h)) = h. \tag{2.11}$$

Тогда любое равенство вида

$$\sum_{s=0}^{h}(\alpha_{1,s}x^{1,s}+\ldots+\alpha_{m(s),s}x^{m(s),s})=0^n, \tag{2.12}$$

где $\alpha_{k,s}\in K$, *влечет равенство*

$$\sum_{s=0}^{h}(\alpha_{1,s}y^{1,s}+\ldots+\alpha_{m(s),s}y^{m(s),s})=0^n. \tag{2.13}$$

Доказательство. Действительно, из (2.12) получаем, что

$$\sum_{s=1}^{h}(\alpha_{1,s}+\ldots+\alpha_{m(s),s})\bar{z}(s)+\sum_{s=1}^{h}(\alpha_{1,s}+\ldots+\alpha_{m(s),s})\bar{\bar{z}}(s) + \sum_{s=0}^{h}(\alpha_{1,s}y^{1,s}+\ldots+\alpha_{m(s),s}y^{m(s),s})=0^n. \tag{2.14}$$

Согласно определению (2.10) векторов $\bar{z}(s)$, $s=0,1,\ldots,h$, из (2.14) следует, что

$$\sum_{s=1}^{h}(\alpha_{1,s}+\ldots+\alpha_{m(s),s})\bar{z}(s)=0^n. \tag{2.15}$$

Соотношение (2.15) вместе с условием (2.11) приводит к равенствам

$$\alpha_{1,s}+\ldots+\alpha_{m(s),s}=0, \qquad s=1,\ldots,h. \tag{2.16}$$

Из (2.14) и (2.16) получаем (2.13). Лемма 4 доказана.

Лемма 5. *Пусть выполнены условия леммы* 4 *и, если* $m(0)\geqslant 2$, *нулевой комплект* $y^{1,0},\ldots,y^{m(0),0}$ *не содержит пар коллинеарных векторов. Тогда*

$$x^{k,s}\neq 0^n, \quad k=1,\ldots,m(s), \quad s=0,1,\ldots,h, \tag{2.17}$$

и любые два вектора x^{k_1,s_1}, x^{k_2,s_2} *как при* $s_1\neq s_2$, *так и при* $s_1=s_2$, $k_1\neq k_2$ *линейно независимы.*

Доказательство. Действительно, $x^{k,0}\neq 0^n$, $r=1,\ldots,m(0)$, так как $x^{k,0}=y^{k,0}$, $r\geqslant 1$. Вместе с этим, $x^{k,s}\neq 0^n$, $k=1,\ldots,m(s)$, $s=1,\ldots,h$, так как в силу (2.11) $\bar{z}(s)\neq 0^n$, $s=1,\ldots,h$.

Докажем второе утверждение леммы. Пусть $\alpha_1x^{k_1,s_1}+\alpha_2x^{k_2,s_2}=0^n$. Если $s_1\neq s_2$ и $s_1,s_2\in\{1,\ldots,h\}$, то в силу (2.11) $\alpha_1=\alpha_2=0$. Если $s_1=0, s_2\in\{1,\ldots,h\}$, то по определению $\bar{z}(0)=0^n$, и в силу (2.11) $\bar{z}(s_2)\neq 0^n$, поэтому $\alpha_2=0$, $\alpha_1x^{k_1,0}=0^n$, и согласно (2.17) $\alpha_1=0$.

Пусть $\alpha_1x^{k_1,s}+\alpha_2x^{k_2,s}=0^n$, $k_1\neq k_2$, $s\in\{0,1,\ldots,h\}$. Отсюда последовательно получаем, что

$$\alpha_1y^{k_1,s}+\alpha_2y^{k_2,s}+(\alpha_1+\alpha_2)\bar{\bar{z}}(s)+(\alpha_1+\alpha_2)\bar{z}(s)=0^n, \tag{2.18}$$

$$(\alpha_1+\alpha_2)\bar{z}(s)=0^n. \tag{2.19}$$

Если $s = 0$, то по определению $\bar{z}(0) = \bar{\bar{z}}(0) = 0^n$, поэтому из (2.18) следует равенство $\alpha_1 y^{k_1,0} + \alpha_2 y^{k_2,0} = 0^n$, из которого по условию леммы (нулевой комплект не содержит пар коллинеарных векторов) следуют равенства $\alpha_1 = \alpha_2 = 0$.

Если $s \in \{1, \ldots, h\}$, то $\bar{z}(s) \neq 0^n$, поэтому из (2.18) и затем из (2.19) получаем, что $\alpha_1 + \alpha_2 = 0$, $\alpha_1(y^{k_1,s} - y^{k_2,s}) = 0^n$.

По условию леммы (в одном комплекте все векторы различны) $y^{k_1,s} - y^{k_2,s} \neq 0^n$, следовательно, $\alpha_1 = \alpha_2 = 0$. Лемма 5 доказана.

Занумеруем элементы в объединении комплектов $y^{1,s}, \ldots, y^{m(s),s}$, $s = 0, 1, \ldots, h$. Пусть

$$\bigcup_{s=0}^{h} \{y^{1,s}, \ldots, y^{m(s),s}\} = \{y^1, \ldots, y^m\}, \tag{2.20}$$

при этом полагаем, что $m = m(0) + m(1) + \ldots + m(h)$ и $y^k = y^{k,0}$, если $1 \leqslant k \leqslant m(0)$, и $y^k = y^{k-(m(0)+\ldots+m(s-1)),s}$, если $m(0) + \ldots + m(s-1) < k < m(0) + \ldots + m(s)$, $s = 1, \ldots, h$.

Точно так же занумеруем элементы в объединении комплектов $x^{1,s}, \ldots, x^{m(s),s}$, $s = 0, 1, \ldots, h$, где $x^{k,s} = z(s) + y^{k,s}$:

$$\bigcup_{s=0}^{h} \{x^{1,s}, \ldots, x^{m(s),s}\} = \{x^1, \ldots, x^m\}. \tag{2.21}$$

Лемма 6. *Пусть выполнены условия леммы 5, при этом*

$$\mu(y^1, \ldots, y^m) > r(m-1) - r/2. \tag{2.22}$$

Тогда

$$\operatorname{rank}(x^1, \ldots, x^m) = m. \tag{2.23}$$

Доказательство. В случаях $m = 1$ и $m = 2$ это утверждение вытекает из леммы 5. Пусть $m \geqslant 3$, выполнено неравенство (2.22), и $\operatorname{rank}(x^1, \ldots, x^m) < m$. Тогда имеет место равенство вида

$$\alpha_1 x^1 + \ldots + \alpha_m x^m = 0^n, \tag{2.24}$$

и согласно лемме 4 выполнено равенство

$$\alpha_1 y^1 + \ldots + \alpha_m y^m = 0^n. \tag{2.25}$$

Согласно лемме 5, число ненулевых коэффициентов в левых частях равенств (2.24) и (2.25) равно

$$d = |\{i \in \{1, \ldots, m\} : \alpha \neq 0\}| \geqslant 3. \tag{2.26}$$

Используя леммы 2, 3 и неравенство (2.26), получаем, что

$$\mu(y^1, \ldots, y^m) = rm - \rho(y^1, \ldots, y^m) \leqslant rm - \frac{dr}{2} \leqslant rm - \frac{3r}{2} = r(m-1) - \frac{r}{2},$$

что противоречит условию (2.22). Лемма 6 доказана.

Лемма 7. *Пусть выполнены условия леммы* 5, $\operatorname{rank}(x^1, \ldots, x^m) < m$ *и*

$$x^m = \alpha_1 x^1 + \ldots + \alpha_{m-1} x^{m-1}. \tag{2.27}$$

Тогда

$$\mu(y^1, \ldots, y^{m-1}) = \mu(y^1, \ldots, y^m), \tag{2.28}$$

$$\operatorname{rank}(x^1, \ldots, x^{m-1}) = \operatorname{rank}(x^1, \ldots, x^m). \tag{2.29}$$

Доказательство. Согласно лемме 4, из (2.27) следует равенство

$$y^m = \alpha_1 y^1 + \ldots + \alpha_{m-1} y^{m-1}. \tag{2.30}$$

Из (2.30) следует, что в матрице $A(y^1, \ldots, y^m)$, составленной из строк $y^1, \ldots, y^m$, любой столбец, соответствующий ненулевому элементу вектора y^m, содержит не менее двух ненулевых элементов. Поэтому вычеркивание строки y^m из матрицы $A(y^1, \ldots, y^m)$ не меняет общего числа ненулевых столбцов. Отсюда следует (2.28). Из (2.27) следует (2.29). Лемма 7 доказана.

Лемма 8. *Пусть выполнены условия леммы* 5 *и при некотором целом* $2 \leqslant k \leqslant m$

$$\mu(y^1, \ldots, y^m) > r(k-1) - r/2. \tag{2.31}$$

Тогда

$$\operatorname{rank}(x^1, \ldots, x^m) \geqslant k. \tag{2.32}$$

Доказательство. При $k = m$ это утверждение вытекает из леммы 6, а при $k = 2$ из леммы 5. Пусть $2 < k < m$ и

$$\operatorname{rank}(x^1, \ldots, x^m) < k. \tag{2.33}$$

Применяя лемму 7, нетрудно установить, что найдутся векторы $y^1, \ldots, y^k$ (не ограничивая общности, будем считать, что они первые) такие, что

$$\mu(y^1, \ldots, y^k) = \mu(y^1, \ldots, y^m), \tag{2.34}$$

$$\operatorname{rank}(x^1, \ldots, x^k) = \operatorname{rank}(x^1, \ldots, x^m). \tag{2.35}$$

Из (2.31), (2.34) следует, что $\mu(y^1, \ldots, y^k) > r(k-1) - r/2$. Поэтому согласно лемме 6 и равенству (2.35) $\operatorname{rank}(x^1, \ldots, x^m) = k$, что противоречит неравенству (2.33). Лемма 8 доказана.

Лемма 9. *Пусть выполнены условия леммы* 4 *и при некотором целом* $2 \leqslant k \leqslant m$,

$$r(k-1) - r/2 < \mu(y^1, \ldots, y^m) \leqslant rk - r/2. \tag{2.36}$$

Тогда

$$\mathbf{P}\{Ax^j = b,\ j = 1, \ldots, m\} \leqslant ((1+\Delta)/q)^{kT} \tag{2.37}$$

при любом $b \in K^T \setminus \{0^T\}$.

Пусть выполнены условия леммы 5 *и при некотором целом* k, $2 \leqslant k \leqslant m$, *выполнены неравенства* (2.36). *Тогда при* $b = 0^T$

$$\mathbf{P}\{Ax^j = 0^T,\ j = 1, \dots, m\} \leqslant ((1+\Delta)/q)^{kT}. \tag{2.38}$$

Пусть выполнены условия леммы 4 *и*

$$rm - r/2 < \mu(y^1, \dots, y^m). \tag{2.39}$$

Тогда

$$((1-\Delta)/q)^{mT} \leqslant \mathbf{P}\{Ax^j = b,\ j = 1, \dots, m\} \leqslant ((1+\Delta)/q)^{mT} \tag{2.40}$$

при любом $b \in K^T$.

Доказательство. Если выполнены условия леммы 4, $m(0) \geqslant 2$ и нулевой комплект $y^{1,0}, \dots, y^{m(0),0}$ содержит пару коллинеарных векторов, то выполнено и неравенство (2.37), так как $\mathbf{P}\{Ax^j = b,\ j = 1, \dots, m\} = 0$ при $b \neq 0^T$. Если выполнены условия леммы 4 и нулевой комплект $y^{1,0}, \dots, y^{m(0),0}$ не содержит коллинеарных векторов, то выполнены условия леммы 5, и, согласно леммам 1 и 8, из (2.36) следует (2.37) и (2.38).

При условии (2.39) набор $y^1, \dots, y^m$ не содержит коллинеарных векторов, так как при их наличии $\mu(y^1, \dots, y^m) < r(m-1) = rm - r$. Поэтому, если выполнены условия леммы 4 и условия (2.39), то выполнены условия леммы 5 и согласно леммам 1 и 8 имеют место равенства (2.40). Лемма 9 доказана.

Положим

$$R_m^{(k)} = rq^{-kT} \binom{n}{rk - \omega(r)} \binom{rk - \omega(r)}{r}^m (q-1)^{rm} (h+1)^m, \tag{2.41}$$

где $\omega(r) = [r/2]$ при $r \geqslant 2$ и $\omega(r) = 1$ при $r = 1$, $[a]$ — целая часть числа a.

Лемма 10. *Найдется такая константа* $C < \infty$, *что при всех* $n, T, r \geqslant 1$, $h \geqslant 1$, $m \geqslant 2$, $rm \leqslant n/2$, $2 \leqslant k \leqslant m$ *выполнено неравенство*

$$R_m^{(k)} \leqslant \Lambda^k \exp\{-\omega(r) \ln(n/r) + rm(\ln m + C)\},$$

где

$$\Lambda = \binom{n}{r} (q-1)^r q^{-T}.$$

Лемма 10 вытекает из леммы 10 работы [2].

3. Доказательство теоремы 1

Пусть $\operatorname{rank}(z(1), \dots, z(h)) = h$ и $A(z(1), \dots, z(h))$ — матрица размера $h \times n$, составленная из строк $z(1), \dots, z(h)$. Согласно условиям теоремы можно полагать, что $n > h$. Выберем в матрице $A(z(1), \dots, z(h))$ произвольные h линейно независимых столбцов. Пусть $i_1, \dots, i_h$ — номера выбранных линейно независимых столбцов. Положим

$$Y_r = \{y \in K^n : \|y\| = r\}, \qquad M(y) = \{i : y_i \neq 0\}, \tag{3.1}$$

$$Y_r' = \{y \in Y_r : i_1, \dots, i_h \notin M(y)\}, \tag{3.2}$$

$$Y_r'' = Y_r \setminus Y_r'. \tag{3.3}$$

Ясно, что

$$\xi(A,b \mid z(s)) = \xi'(Ab \mid z(s)) + \xi''(Ab \mid z(s)), \qquad s = 0,1,\ldots,h, \tag{3.4}$$

где $\xi'(A,b \mid z(s))$ — число решений системы $Ax = b$, удовлетворяющих условию $x - z(s) \in Y_r'$ и $\xi''(A,b \mid z(s))$ — число решений системы, удовлетворяющих условию $x - z(s) \in Y_r''$.

Покажем, что

$$(\xi'(A,b \mid z(s)),\ s = 0,1,\ldots,h) \to \Pi^{h+1}(\lambda) \tag{3.5}$$

и вместе с этим

$$\mathbf{P}\{\xi''(A,b \mid z(s)) = 0,\ s = 0,1,\ldots,h\} \to 1 \tag{3.6}$$

равномерно относительно векторов, указанных в первой части теоремы 1. Из (3.4), (3.5), (3.6) будет следовать (1.8).

Занумеруем элементы множества Y_r'. Пусть

$$Y_r' = \{y^k,\ k = 0,1,\ldots,N-1\}, \qquad N = \binom{n-h}{r}(q-1)^r.$$

С учетом данной нумерации занумеруем все векторы x, удовлетворяющие условиям $x - z(s) \in Y_r'$, $s = 0,1,\ldots,h$. Положим

$$x^j = z([j/N]) + y^j, \qquad j = 0,1,\ldots,N(h+1)-1,$$

где $y^j = y^{j \bmod N} = y^{j - N[j/N]}$. При этом получаем, что

$$\xi'(A,b \mid z(s)) = \sum_{j=Ns}^{N(s+1)-1} \zeta(x^j),$$

где

$$\zeta(x^j) = \begin{cases} 1, & Ax^j = b, \\ 0, & Ax^j \neq b. \end{cases}$$

Согласно теореме 1 из работы [4], для доказательства соотношения (3.5) достаточно убедиться в том, что

$$\sum_{j=Ns}^{N(s+1)-1} \mathbf{P}\{Ax^j = b\} \to \lambda, \qquad s = 0,1,\ldots,h, \tag{3.7}$$

$$\max_{0 \leqslant j \leqslant N(h+1)-1} \mathbf{P}\{Ax^j = b\} \to 0, \tag{3.8}$$

и при всех $m = 2,3,\ldots$

$$\sum_{0 \leqslant j_1 < \ldots < j_m \leqslant N(h+1)-1} |\mathbf{P}\{Ax^{j_1} = b,\ldots,Ax^{j_m} = b\} - \mathbf{P}\{Ax^{j_1} = b\}\ldots\mathbf{P}\{Ax^{j_m} = b\}| \to 0 \tag{3.9}$$

равномерно относительно указанных в первой части теоремы векторов.

Соотношения (3.7), (3.8) проверяются несложно: при любом $b \in K^n \setminus \{0^n\}$ и любом $s = 1, \dots, h$ получаем, что

$$\sum_{j=Ns}^{N(s+1)-1} \mathbf{P}\{Ax^j = b\} = N((1+O(\Delta))/q)^T = \binom{n-h}{r}(q-1)^r((1+O(\Delta))/q)^T$$
$$= (1+o(1))\binom{n}{r}(q-1)^r q^{-T} \to \lambda,$$
$$\max_{0 \leqslant j \leqslant N(h+1)-1} \mathbf{P}\{Ax^j = b\} \leqslant ((1+\Delta)/q)^T \to 0.$$

Осталось проверить (3.9). Для этого воспользуемся леммами 4 и 9. Отметим, что при любом наборе номеров $(j_1, \dots, j_m)\colon 0 \leqslant j_1 < \dots < j_m \leqslant N(h+1)-1$, векторы y^j: $j \in \{j_1, \dots, j_m\} \cap \{Ns, \dots, N(s+1)-1\}$, $s = 0, 1, \dots, h$, составляют комплекты вида (2.9). В каждом непустом комплекте все векторы различны. Векторы $\bar{z}(1), \dots, \bar{z}(h)$, заданные формулой (2.10), составляют систему максимального ранга, $\operatorname{rank}(\bar{z}(1), \dots, \bar{z}(h)) = h$, так как матрица $A(\bar{z}(1), \dots, \bar{z}(h))$, составленная из строк $\bar{z}(1), \dots, \bar{z}(h)$, по определению (3.2) множества Y'_r содержит линейно независимые столбцы с номерами (3.7). Следовательно, для векторов $y^{j_1}, \dots, y^{j_m}$ и $x^{j_1}, \dots, x^{j_m}$ выполнены условия леммы 4 и справедливы первое и третье утверждения леммы 9.

Пусть

$$S_m = \{(j_1, \dots, j_m)\colon 0 \leqslant j_1 < \dots < j_m \leqslant N(s+1)-1,\ \mu(y^{j_1}, \dots, y^{j_m}) \leqslant rm - r/2\},$$

Разобьем сумму из условия (3.9) на две суммы, полагая (в сокращенной записи), что

$$\sum_{0 \leqslant j_1 < \dots < j_m \leqslant N(h+1)-1} = \sum_{(j_1,\dots,j_m) \in S_m} + \sum_{(j_1,\dots,j_m) \notin S_m}. \tag{3.10}$$

При произвольном наборе индексов $(j_1, \dots, j_m) \notin S_m$ выполняется неравенство $\mu(y^{j_1}, \dots, y^{j_m}) > rm - r/2$, и согласно третьему утверждению леммы 9

$$|\mathbf{P}\{Ax^{j_1} = b, \dots, Ax^{j_m} = b\} - \mathbf{P}\{Ax^{j_1} = b\} \dots \mathbf{P}\{Ax^{j_m} = b\}| = q^{-mT} O(T\Delta).$$

Поэтому

$$\sum_{(j_1,\dots,j_m) \notin S_m} = \lambda O(T\Delta) \to 0. \tag{3.11}$$

Для первой суммы в разбиении (3.10) справедлива оценка

$$\sum_{(j_1,\dots,j_m) \in S_m} \leqslant \Sigma_1 + \Sigma_2, \tag{3.12}$$

где

$$\Sigma_1 = \sum_{(j_1,\dots,j_m) \in S_m} \mathbf{P}\{Ax^{j_1} = b, \dots, Ax^{j_m} = b\}, \tag{3.13}$$
$$\Sigma_2 = \sum_{(j_1,\dots,j_m) \in S_m} \mathbf{P}\{Ax^{j_1} = b\} \dots \mathbf{P}\{Ax^{j_m} = b\}. \tag{3.14}$$

Оценим суммы (3.13), (3.14). Положим

$$W_m(l) = |\{(j_1, \ldots, j_m): 0 \leqslant j_1 < \ldots < j_m \leqslant N(h+1)-1, \mu(x^{j_1}, \ldots, x^{j_m}) = l\}|.$$

Несложно установить, что

$$W_m(l) \leqslant \binom{n}{l}\binom{l}{r}^m (q-1)^{rm}(h+1)^m. \tag{3.15}$$

Используя первое утверждение леммы 9 и оценку (3.15), получаем, что

$$\Sigma_1 \leqslant \sum_{k=2}^{m} q^{-kT}(1+\Delta)^{kT} \sum_{r(k-1)-r/2<l\leqslant rk-r/2} W_m(l) \leqslant (1+\Delta)^{mT} \sum_{k=2}^{m} R_m^{(k)}, \tag{3.16}$$

при этом

$$R_m^{(k)} = rq^{-kT}\binom{n}{rk-\omega(r)}\binom{rk-\omega(r)}{r}^m (q-1)^{rm}(h+1)^m, \tag{3.17}$$

где $\omega(r) = [r/2]$ при $r \geqslant 2$ и $\omega(r) = 1$ при $r = 1$, $[a]$ — целая часть числа a. Отсюда, используя лемму 10, получаем, что

$$\Sigma_1 \leqslant (1+\Delta)^{mT}\frac{\Lambda^m - 1}{\Lambda - 1}\exp\{-\omega(r)\ln(n/r) + rm(\ln m + C)\}, \tag{3.18}$$

где

$$\Lambda = \binom{n}{r}(q-1)^r q^{-T}.$$

В силу неравенства (3.18) и условий теоремы,

$$\Sigma_1 \to 0. \tag{3.19}$$

Для суммы (3.14) выполняется оценка, аналогичная оценке (3.16):

$$\Sigma_2 = q^{-mT}(1+\Delta)^{mT}\sum_{k=2}^{m}\sum_{r(k-1)-r/2<l\leqslant rk-r/2} W_m(l) \leqslant (1+\Delta)^{mT}\sum_{k=2}^{m} R_m^{(k)}.$$

Следовательно,

$$\Sigma_2 \to 0. \tag{3.20}$$

Из (3.10)–(3.14), (3.19) и (3.20) получаем (3.9). Таким образом, (3.5) доказано.

Для завершения доказательства (1.8) осталось доказать (3.6). При $b \neq 0^T$

$$\begin{aligned}\mathbf{E}\xi''(A, b \mid z(s)) &\leqslant \sum_{i=1}^{\min(r,h)}\binom{h}{i}\binom{n-h}{r-i}(q-1)^r q^{-T}(1+\Delta)^T \\ &\leqslant (hr/n)\binom{n}{r}(q-1)^r q^{-T}(1+\Delta)^T = o(1).\end{aligned} \tag{3.21}$$

Из (3.21) получаем, что

$$\mathbf{E}\sum_{s=0}^{h}\xi''(A,b\mid z(s))\to 0.$$

Отсюда следует (3.6). Соотношение (1.8) доказано.

Для доказательства соотношения (1.9) достаточно показать, что

$$\mathbf{E}\sum_{s=0}^{h}(\xi^*(A,b\mid z(s))-\xi(A,b\mid z(s)))\to 0 \tag{3.22}$$

равномерно относительно указанных в первой части теоремы 1 векторов. С учетом (1.6) находим, что для любых векторов $b\in K^T\setminus\{0^T\}$ и $z(s)\in K^n$

$$\mathbf{E}(\xi^*(A,b\mid z(s))-\xi(A,b\mid z(s)))\leqslant q^{-T}(1+\Delta)^T\sum_{k=0}^{r-1}|Y_k|=o\left(\binom{n}{r}(q-1)^r q^{-T}\right)\to 0. \tag{3.23}$$

Из (3.23) следует (3.22), что вместе с (1.8) влечет (1.9).

Осталось доказать второе утверждение теоремы 1. Воспользуемся разбиением множества Y_r на подмножества (3.2), (3.3) с соответствующими разложениями

$$\xi(A,0^T\mid z(s))=\xi'(A,0^T\mid z(s))+\xi''(A,0^T\mid z(s)),\qquad s=0,1,\ldots,h. \tag{3.24}$$

Покажем, что

$$((1/(q-1))\xi'(A,0^T\mid 0^n);\xi'(A,0^T\mid z(s)),s=1,\ldots,h)\to\Pi(\lambda/(q-1))\Pi^h(\lambda) \tag{3.25}$$

и вместе с этим

$$\mathbf{P}\{\xi''(A,0^T\mid 0^n)=0;\xi''(A,0^T\mid z(s))-1=0,\ s=0,1,\ldots,h_1;\\ \xi''(A,0^T\mid z(s))=0,\ s=h_1+1,\ldots,h\}\to 1 \tag{3.26}$$

равномерно относительно указанных во второй части теоремы векторов. Из (3.24), (3.25) и (3.26) будет следовать (1.10).

Доказательство (3.25) аналогично доказательству (3.5), где $b\neq 0^T$. Сначала отметим, что $\xi(A,0^T\mid 0^n,r)$ принимает значения, кратные числу $q-1=|K\setminus\{0\}|$, так как все элементы из любого класса

$$\{\alpha y:\alpha\in K\setminus\{0\}\},\qquad y\in Y_r, \tag{3.27}$$

одновременно удовлетворяют или не удовлетворяют системе $Ax=0^T$. Пусть множество

$$\widehat{Y}'_r=\{\hat{y}^k,\ k=0,\ldots,\widehat{N}-1\},\qquad \widehat{N}=N/(q-1)=\binom{n-h}{r}(q-1)^{r-1}, \tag{3.28}$$

составлено из представителей классов (3.27), содержащихся в множестве

$$Y'_r=\{y^k,\ k=0,1,\ldots,N-1\},\qquad N=N/\binom{n-h}{r}(q-1)^r. \tag{3.29}$$

Используя данную нумерацию векторов в множествах (3.28), (3.29), занумеруем все векторы x, удовлетворяющие условию $x-z(0) \in \hat{Y}'_r$ и условиям $x-z(s) \in Y'_r$, $s = 1, \ldots, h$. Положим

$$x^j = z(0) + y^j, \qquad j = 0, 1, \ldots, \hat{N} - 1,$$

где $y^j = \hat{y}^j$, и положим

$$x^j = z([(j - \hat{N})/N] + 1) + y^j, \qquad j = \hat{N}, \ldots, \hat{N} + Nh - 1,$$

где $y^j = y^{(j-\hat{N}) \bmod N}$.

При этой нумерации получаем, что

$$(1/(q-1))\xi'(A, 0^T \mid 0^n) = \sum_{j=0}^{\hat{N}-1} \zeta(x^j),$$

$$\xi'(A, 0^T \mid z(s)) = \sum_{j=\hat{N}+N(s-1)}^{\hat{N}+Ns-1} \zeta(x^j), \qquad s = 1, \ldots, h,$$

где $\zeta(x^j) = 1$ при $Ax^j = 0^T$ и $\zeta(x^j) = 0$ при $Ax^j \neq 0^T$.

Так же, как при доказательстве первой части теоремы, воспользуемся теоремой 1 работы [4] и покажем, что

$$\sum_{j=0}^{\hat{N}-1} \mathbf{P}\{Ax^j = 0^T\} \to (\lambda/(q-1)), \tag{3.30}$$

$$\sum_{j=\hat{N}+N(s-1)}^{\hat{N}+Ns-1} \mathbf{P}\{Ax^j = 0^T\} \to \lambda, \qquad s = 1, \ldots, h, \tag{3.31}$$

$$\max_{0 \leqslant j \leqslant \hat{N}+Nh-1} \mathbf{P}\{Ax^j = 0^T\} \to 0, \tag{3.32}$$

и при всех $m = 2, 3, \ldots$

$$\sum_{0 \leqslant j_1 < \ldots < j_m \leqslant \hat{N}+Nh-1} |\mathbf{P}\{Ax_1^j = 0^T, \ldots, Ax^{j_m} = 0^T\} - \mathbf{P}\{Ax^{j_1} = 0^T\} \ldots \mathbf{P}\{Ax^{j_m} = 0^T\}| \to 0 \tag{3.33}$$

равномерно относительно указанных во второй части теоремы векторов.

Легко проверяется, что соотношения (3.30), (3.31), (3.32) следуют из условий теоремы 1.

Для проверки (3.33) воспользуемся леммами 5 и 9. Учтем, что при любом наборе $(j_1, \ldots, j_m) : 0 \leqslant j_1 < \ldots < j_m \leqslant \hat{N} + Nh - 1$ векторы

$$y^j : j \in \{j_1, \ldots, j_m\} \cap \{0, \ldots, \hat{N} - 1\} \tag{3.34}$$

и векторы

$$y^j : j \in \{j_1, \ldots, j_m\} \cap \{\hat{N} + N(s-1), \ldots, \hat{N} + Ns - 1\}, \qquad s = 1, \ldots, h, \tag{3.35}$$

составляют комплекты вида (2.9) и нулевой комплект, составленный из векторов (3.34), не содержит пар коллинеарных векторов. Очевидно, условие (2.11) тоже выполнено.

Значит, для векторов $y^{j_1}, \dots, y^{j_m}$ и $x^{j_1}, \dots, x^{j_m}$ выполнены условия леммы 5 (следовательно, и леммы 4) и справедливы второе и третье утверждения леммы 9. Поэтому для проверки (3.33) можно повторить выкладки (3.10)–(3.20), использованные для проверки (3.9) (где $b \neq 0^T$), положив $b = 0^T$ и заменив число $N(h+1)-1$, ограничивающее сверху номера векторов y^j и x^j, числом $\widehat{N} + Nh - 1$. Таким образом докажем соотношение (3.33) и вместе с ним соотношение (3.25).

Для доказательства (1.10) осталось проверить (3.26). С этой целью отметим, что если выполнены условия (1.11), то (в силу определений (3.2), (3.3) множеств Y_r', Y_r'') выполнены включения $z(s) \in Y_r''$, $s = 1, \dots, h_1$, при этом вектор $x = 0^n$ удовлетворяет условиям $x - z(s) \in Y_r''$, $s = 1, \dots h_1$, и является решением системы $Ax = 0^T$ с вероятностью, равной единице; все остальные (ненулевые) векторы $x\colon x - z(s) \in Y_r''$, $s = 1, \dots, h_1$ (при выполнении включений (1.11)) являются решениями с вероятностью, меньшей или равной $q^{-T}(1+\Delta)^T$. Все векторы $x\colon x - x(s) \in Y_r''$, $s = h_1 + 1, \dots, h$, при выполнении условий (1.12), а также все векторы $x\colon x - x(0) \in Y_r''$ ненулевые, и для этих векторов

$$\mathbf{P}\{Ax = 0^T\} \leqslant q^{-T}(1+\Delta)^T.$$

поэтому имеет место оценка, аналогичная оценке (3.21):

$$\mathbf{E}\xi''(A, 0^T \mid 0^n) + \sum_{s=1}^{h_1} \mathbf{E}(\xi''(A, 0^T \mid z(s)) - 1) + \sum_{s=h_1+1}^{h_1} \mathbf{E}(\xi''(A, 0^T \mid z(s)) \leqslant (h+1) \sum_{i=1}^{\min(r,h)} \binom{h}{i}\binom{n-h}{r-i}(q-1)^r q^{-T}(1+\Delta)^T = o(1).$$

Отсюда следует (3.26). Соотношение (1.10) доказано.

Доказательство последнего утверждения теоремы аналогично приведенному выше доказательству соотношения (1.9) при установленном соотношении (1.8).

Теорема 1 доказана.

4. Доказательство теоремы 2

Теорема 2 выводится из теоремы 1 с помощью простых вспомогательных оценок. Получим эти оценки. Ясно, что

$$\xi(A, b \mid z(0), z(1), \dots, z(h)) \leqslant \sum_{s=0}^{h} \xi(A, b \mid z(s)). \tag{4.1}$$

При этом, если $b \neq 0^T$, то согласно равенствам

$$\mathbf{P}\{Ax = b\} = \begin{cases} q^{-T}, & x \neq 0^T, \\ 0, & x = 0^T \end{cases}$$

имеет место оценка

$$\mathbf{E}\left(\sum_{s=0}^{h}\xi(A,b\mid z(s))-\xi(A,b\mid z(0),z(1),\ldots,z(h))\right)$$
$$\leqslant q^{-T}(1+\Delta)^{T}\sum_{0\leqslant s_1<s_2\leqslant h}|X_r(z(s_1))\cap X_r(z(s_2))|, \quad (4.2)$$

где

$$X_r(z(s))=\{x\colon \|x-z(s)\|=r\}.$$

Пусть $b=0^T$. Для этого случая введем индикатор

$$I(z(0),z(1),\ldots,z(h))=\begin{cases}1, & \exists s\in\{1,\ldots,h\}\colon \|z(s)\|=r,\\ 0, & \|z(s)\|\neq r,\ s=1,\ldots,h.\end{cases} \quad (4.3)$$

Величина (4.3) является индикатором наличия нулевого решения: вектор $x=0^n$ при $\|z(s)\|=r$ удовлетворяет условию $\|x-z(s)\|=r$ и заведомо удовлетворяет системе $Ax=0^T$; если $\|z(s)\|\neq r$, то вектор $x=0^n$ не удовлетворяет условию $\|x-z(s)\|=r$.

Для чисел ненулевых решений справедливо неравенство

$$\xi(A,0^T\mid z(0),z(1),\ldots,z(h))-I(z(0),z(1),\ldots,z(h))\leqslant\sum_{s=0}^{h}[\xi(A,0^T\mid z(s))-I(z(s))], \quad (4.4)$$

где

$$I(z(s))=\begin{cases}1, & \|z(s)\|=r,\\ 0, & \|z(s)\|\neq r.\end{cases}$$

Вместе с (4.4) имеет место неравенство, аналогичное неравенству (4.2):

$$\mathbf{E}\left(\sum_{s=0}^{h}(\xi(A,0^T\mid z(s))-I(z(s)))-(\xi(A,0^T\mid z(0),z(1),\ldots,z(h))\right.$$
$$\left.-I(z(0),z(1),\ldots,z(h)))\right)\leqslant q^{-T}(1+\Delta)^{T}\sum_{0\leqslant s_1<s_2\leqslant h}|X_r(z(s_1))\cap X_r(z(s_2))|. \quad (4.5)$$

С учетом (4.2), (4.5) оценим числа векторов в пересечениях $X_r(z(s_1))\cap X_r(z(s_2))$, $0\leqslant s_1<s_2\leqslant h$.

Векторы $z(0),z(1)\ldots,z(h)$ попарно различны. Выберем произвольную пару $z(s_1)=(z_1(s_1),\ldots,z_n(s_1))$, $z(s_2)=(z_1(s_2),\ldots,z_n(s_2))$, и для нее выберем произвольный индекс

$$i\in\{1,\ldots,n\}\colon\quad z_i(s_1)\neq z_i(s_2). \quad (4.6)$$

Положим

$$X_r^{(1,i)}(z(s))=\{x\colon \|x-z(s)\|=r,\ x_i=z_i(s)\}, \quad (4.7)$$
$$X_r^{(2,i)}(z(s))=\{x\colon \|x-z(s)\|=r,\ x_i\neq z_i(s)\}, \quad (4.8)$$

Ясно, что

$$X_r(z(s)) = X_r^{(1,i)}(z(s)) \cup X_r^{(2,i)}(z(s)), \tag{4.9}$$

$$X_r^{(1,i)}(z(s)) \cap X_r^{(2,i)}(z(s)) = \varnothing. \tag{4.10}$$

С учетом (4.9), (4.10) получаем, что

$$|X_r(z(s_1)) \cap X_r(z(s_2))| = \sum_{j=1}^{2}\sum_{l=1}^{2} |X_r^{(j,i)}(z(s_1)) \cap X_r^{(l,i)}(z(s_2))|.$$

Из (4.6) и (4.7) следует, что

$$X_r^{(1,i)}(z(s_1)) \cap X_r^{(2,i)}(z(s_2)) = \varnothing.$$

Поэтому

$$|X_r(z(s_1)) \cap X_r(z(s_2))| \leqslant |X_r^{(2,i)}(z(s_1))| + |X_r^{(2,i)}(z(s_2))| + |X_r^{(2,i)}(z(s_1)) \cap X_r^{(2,i)}(z(s_2))|. \tag{4.11}$$

Осталось отметить, что

$$|X_r^{(2,i)}(z(s_1))| = |X_r^{(2,i)}(z(s_2))| = \binom{n-1}{r-1}(q-1)r = (r/n)\binom{n}{r}(q-1)^r. \tag{4.12}$$

Из (4.1), (4.2), (4.11), (4.12) и условий (1.5), (1.6) вытекает, что

$$\mathbf{P}\{\xi(A, b \mid z(0), z(1), \ldots, z(h)) = \sum_{s=0}^{h} \xi(A, b \mid z(s))\} \to 1 \tag{4.13}$$

равномерно относительно векторов $b \in K^T \setminus \{0^T\}$ и попарно различных векторов $z(s) \in K^n$, $s = 0, 1, \ldots, h$. Вместе с этим из (4.4), (4.5), (4.11), (4.12) и условий (1.5), (1.6) вытекает, что

$$\mathbf{P}\left\{(\xi(A, b \mid z(0), z(1), \ldots, z(h)) - I(z(0), z(1) \ldots, z(h))) = \sum_{s=0}^{h}(\xi(A, b \mid z(s)) - I(z(s)))\right\} \to 1 \tag{4.14}$$

равномерно относительно попарно различных векторов $z(s) \in K^n$, $s = 0, 1, \ldots, h$.

Из соотношений (4.13), (4.14), а также из подобных соотношений, связанных с векторами $z(1), \ldots, z(h)$ (и не связанных с вектором $z(0) = 0^n$), и утверждений теоремы 1 следуют утверждения 1, 2, 3 теоремы 2, сформулированные для величин ξ.

Доказательство утверждений 1, 2, 3 для величин ξ^* проводится совершенно аналогично.

Теорема 2 доказана.

Список литературы

1. Копытцев В. А., О числе решений систем линейных булевых уравнений в множестве векторов, обладающих заданным числом единиц. *Дискретная математика* (2002) **14**, №4, 87–109.
2. Копытцев В. А., О числе решений системы случайных линейных уравнений в множестве векторов специального вида. *Дискретная математика* (2006) **18**, №1, 40–62.
3. Михайлов В. Г., О числе решений, близких к заданному вектору. *Обозрение прикладной и промышленной математики* (2005) **12**, №2, 435–436.
4. Михайлов В. Г., Сходимость к процессу с независимыми приращениями в схеме нарастающих сумм зависимых случайных величин. *Матем. сб.* (1974) **94**, 283–299.

Статья поступила 1.09.2006.
Переработанный вариант поступил 21.11.2006.