Сибирский математический журнал
Май—июнь, 2014. Том 55, № 3

УДК 512.54

СЛУЧАЙНЫЕ СИСТЕМЫ УРАВНЕНИЙ В СВОБОДНЫХ АБЕЛЕВЫХ ГРУППАХ

А. В. Меньшов

Аннотация. Исследуется разрешимость случайных систем уравнений в свободной абелевой группе $\mathbb{Z}^m$ конечного ранга m. Пусть $\mathrm{SAT}(\mathbb{Z}^m, k, n)$ и $\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ обозначают множества всех систем из n уравнений от k неизвестных в группе $\mathbb{Z}^m$, разрешимых соответственно в $\mathbb{Z}^m$ и $\mathbb{Q}^m$. Доказано, что асимптотическая плотность $\rho(\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n))$ множества $\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ равна 1 при $n \le k$ и 0 при $n > k$. Для множества $\mathrm{SAT}(\mathbb{Z}^m, k, n)$ при $n < k$ получены оценки для нижней и верхней асимптотических плотностей, показано, что они лежат в интервале от $\Big(\prod\limits_{j=k-n+1}^{k}\zeta(j)\Big)^{-1}$ до $\big(\frac{\zeta(k+m)}{\zeta(k)}\big)^n$, где $\zeta(s)$ — дзета-функция Римана. При $n \le k$ установлена связь между асимптотической плотностью множества $\mathrm{SAT}(\mathbb{Z}^m, k, n)$ и суммами обратных наибольших делителей по матрицам полного ранга. Исходя из этого результата выдвинута гипотеза относительно асимптотической плотности множества $\mathrm{SAT}(\mathbb{Z}^m, n, n)$. Доказано, что $\rho(\mathrm{SAT}(\mathbb{Z}^m, k, n)) = 0$ при $n > k$.

Ключевые слова: свободная абелева группа, уравнение в группах, асимптотическая плотность, квазиполиномы Эрхарта.

1. Введение

Идея генеричности в теории конечных групп идет из работ Эрдеша и Турана [1], а также Диксона [2]. В настоящее время это предмет многочисленных исследований. В геометрической теории групп генерический подход инициирован М. Громовым [3–5]. Он связан со случайными блужданиями на группах.

В последнее время генерический подход все более концентрируется на конкретных группах. Укажем для примера работы [6, 7] о группах с одним соотношением, работы [8, 9] по усредненным функциям Дена.

Р. Гилман, А. Мясников и В. Романьков исследовали асимптотическую плотность разрешимых уравнений в свободных абелевых и конечно порожденных нильпотентных группах [10] и в свободных группах [11]. В [12] рассматривалась асимптотическая плотность разрешимых однородных уравнений в фундаментальных группах компактных поверхностей.

Настоящая работа продолжает исследования асимптотической плотности множества разрешимых уравнений, проведенные в [10] для свободных абелевых групп конечного ранга, но уже для систем уравнений.

Пусть $\mathrm{SAT}(\mathbb{Z}^m, k, n)$ и $\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ обозначают множества всех систем из n уравнений от k неизвестных в группе $\mathbb{Z}^m$, разрешимых соответственно в

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации (проекты 14.B37.21.0359/0859).

$\mathbb{Z}^m$ и $\mathbb{Q}^m$. Исследуется асимптотическая плотность указанных множеств относительно естественной стратификации группы $\mathbb{Z}^m$ шарами, соответствующими норме $\|\cdot\|_\infty$ пространства $\mathbb{R}^m$, определяемой формулой $\|(v_1,\dots,v_m)\|_\infty = \max\{|v_i|\}$. При этом группа $\mathbb{Z}^m$ и ее подгруппы рассматриваются как целочисленные решетки в пространстве $\mathbb{R}^m$.

С привлечением асимптотики для целочисленных матриц фиксированного ранга (см. [13]) в теореме 2 доказано, что асимптотическая плотность множества $\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m,k,n)$ равна 1 при $n \le k$ и 0 при $n > k$. Отсюда получено следствие 1, согласно которому $\rho(\mathrm{SAT}(\mathbb{Z}^m,k,n)) = 0$ при $n > k$.

Для исследования асимптотической плотности множества $\mathrm{SAT}(\mathbb{Z}^m,k,n)$ при $n \le k$ используются методы комбинаторики, оценивающие количества точек решеток в расширениях выпуклых многогранников в $\mathbb{R}^m$ [14, 15]. В теореме 6 получено неравенство на коэффициенты квазиполиномов Эрхарта, являющееся аналогом неравенства из [16, теорема 6]. С помощью полученного неравенства доказан один из основных результатов данной работы — теорема 9, устанавливающая связь между асимптотической плотностью множества $\mathrm{SAT}(\mathbb{Z}^m,k,n)$ и суммами обратных наибольших делителей по матрицам полного ранга. Исходя из этой теоремы выдвинута гипотеза 1 относительно асимптотической плотности множества $\mathrm{SAT}(\mathbb{Z}^m,n,n)$. Вторым основным результатом является теорема 12, в которой получены нетривиальные оценки для нижней и верхней асимптотических плотностей множества $\mathrm{SAT}(\mathbb{Z}^m,k,n)$ при $n < k$, показано, что они лежат в интервале от $\left(\prod\limits_{j=k-n+1}^{k}\zeta(j)\right)^{-1}$ до $\left(\frac{\zeta(k+m)}{\zeta(k)}\right)^n$, где $\zeta(s)$ — дзета-функция Римана.

2. Асимптотическая плотность

Стратификацией счетного множества T называется последовательность $\{T_r\}_{r\in\mathbb{N}}$ непустых конечных подмножеств T_r таких, что $\bigcup\limits_{r\in\mathbb{N}} T_r = T$. Стратификации обычно задаются с помощью функций длины. *Функция длины* на T — это отображение $l : T \to \mathbb{N}$ такое, что для каждого $r \in \mathbb{N}$ множество $\{x \in T \mid l(x) = r\}$ конечно. Стратификации по сферам и шарам образованы соответственно сферами $S_r = \{x \in T \mid l(x) = r\}$ и шарами $B_r = \{x \in T \mid l(x) \le r\}$.

Определение 1. *Асимптотической плотностью* множества $M \subseteq T$ в соответствии со стратификацией $\{T_r\}$ называется предел

$$\rho(M) = \lim_{r\to\infty} \rho_r(M), \quad \text{где } \rho_r(M) = \frac{|M \cap T_r|}{|T_r|},$$

если он существует. В противном случае будем использовать пределы

$$\overline{\rho}(M) = \limsup_{r\to\infty} \rho_r(M), \quad \underline{\rho}(M) = \liminf_{r\to\infty} \rho_r(M),$$

которые будем называть соответственно *верхней и нижней асимптотическими плотностями.*

Множество M называется *генерическим* в соответствии со стратификацией $\{T_r\}$, если $\rho(M) = 1$, и *несущественным*, если $\rho(M) = 0$.

Пусть $\mathbb{Z}^m$ — свободная абелева группа ранга m. Группу $\mathbb{Z}^m$ будем отождествлять со стандартной целочисленной решеткой евклидова пространства $\mathbb{R}^m$.

Считаем, что $\mathbb{R}^m$ снабжено равномерной нормой, определяемой для элемента $v = (v_1, \dots, v_m)$ формулой

$$\|v\|_\infty = \max_i \{|v_i|\}.$$

Эта норма порождает функцию длины $\|\cdot\|_\infty : \mathbb{Z}^m \to \mathbb{N}$ с шарами

$$B_r^m = \{v \in \mathbb{Z}^m \mid \|v\|_\infty \leq r\}.$$

Далее будем вычислять асимптотическую плотность некоторых подмножеств в свободных абелевых группах относительно стратификации по шарам.

3. Уравнения в группах

Уравнение $u = 1$ от k неизвестных в группе G — это выражение вида

$$g_0 x_{i_1}^{m_1} g_1 \dots x_{i_n}^{m_n} g_n = 1,$$

где $g_j \in G$ и $m_j \in \mathbb{Z}$ заданы, а x_{i_j} принадлежит алфавиту неизвестных $X = \{x_1, \dots, x_k\}$. В этом случае *свободное* произведение $G_X = F(X) * G$ — пространство всех уравнений в переменных X с коэффициентами из G. *Решением* уравнения $u = 1$ в G называется отображение $x_j \to h_j \in G$ такое, что $g_0 h_{i_1}^{m_1} g_1 \dots h_{i_n}^{m_n} g_n = 1$. Обозначим через $\mathrm{SAT}(G, k)$ множество всех уравнений из G_X, разрешимых в G (от англ. *satisfiable* — разрешимый).

Так как далее будут рассматриваться уравнения в группе $\mathbb{Z}^m$, будем использовать для них аддитивную запись

$$\gamma_1 \mathbf{x_1} + \dots + \gamma_k \mathbf{x_k} = \mathbf{b}, \tag{1}$$

где $\gamma_j \in \mathbb{Z}$ и $\mathbf{b} \in \mathbb{Z}^m$ заданы, а $\mathbf{x_j} = (x_{j1}, \dots, x_{jm})$ неизвестные.

Систему

$$\begin{cases} \gamma_{11} \mathbf{x_1} + \dots + \gamma_{1k} \mathbf{x_k} = \mathbf{b_1}, \\ \vdots \quad \vdots \\ \gamma_{n1} \mathbf{x_1} + \dots + \gamma_{nk} \mathbf{x_k} = \mathbf{b_n} \end{cases} \tag{2}$$

из n уравнений вида (1) будем записывать в матричном виде

$$AX = B, \tag{3}$$

где

$$A = (\gamma_{ij}) \in \mathbb{Z}^{nk}, \quad B = \begin{pmatrix} \mathbf{b_1} \\ \vdots \\ \mathbf{b_n} \end{pmatrix} \in \mathbb{Z}^{nm} \quad \text{и} \quad X = \begin{pmatrix} \mathbf{x_1} \\ \vdots \\ \mathbf{x_k} \end{pmatrix}.$$

При $G = \mathbb{Z}^m$ в качестве пространства G_X всех уравнений над G в переменных из $X = \{x_1, \dots, x_k\}$ естественно рассматривать *прямое* произведение $A(X) \times \mathbb{Z}^m \simeq \mathbb{Z}^{k+m}$ свободной абелевой группы $A(X)$ с базисом X и группы $\mathbb{Z}^m$. Тогда в качестве пространства $G_{X,n}$ всех систем из n уравнений из G_X естественно рассматривать $\mathbb{Z}^{n(k+m)}$. Через $\mathrm{SAT}(G, k, n)$ обозначим множество всех систем из $G_{X,n}$, разрешимых в G. Для разрешимых в $\mathbb{Q}^m$ систем из $\mathbb{Z}^m_{X,n}$ будем использовать обозначение $\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$.

Заметим, что в системе (3) различные координаты неизвестных попарно независимы, поэтому справедлива следующая очевидная

Лемма 1. *Система уравнений $AX = B$ вида (3) разрешима в $\mathbb{Z}^m(\mathbb{Q}^m)$ тогда и только тогда, когда система $Ax = B_i$ разрешима над $\mathbb{Z}(\mathbb{Q})$ для любого $i = 1, \dots, m$, где B_i — i-й столбец матрицы B.*

Если $X_i = (x_{1i}, \dots, x_{ki})^T$ — решение системы $Ax = B_i$, то матрица $X = (X_1, \dots, X_m)$ — решение системы $AX = B$.

4. Системы, разрешимые в $\mathbb{Q}^m$

Вычислим асимптотическую плотность множества $\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ всех систем вида (3), разрешимых в $\mathbb{Q}^m$.

Рассмотрим систему линейных диофантовых уравнений

$$Ax = b, \quad \text{где } A \in \mathbb{Z}^{nk},\ b \in \mathbb{Z}^n.$$

Согласно теореме Кронекера — Капелли указанная система разрешима над $\mathbb{Q}$ тогда и только тогда, когда $\mathrm{rank}(A) = \mathrm{rank}(A|b)$.

Приведем основной результат из [13], где исследуется асимптотика целочисленных матриц фиксированного ранга. Обозначим

$$V_{n,k,s}(\mathbb{Z}) = \{A \in \mathbb{Z}^{nk} \mid \mathrm{rank}(A) = s\}, \quad N(r; n, k, s) = |\{A \in V_{n,k,s}(\mathbb{Z}) \mid \|A\|_2 < r\}|,$$

где $\|A\|_2 = \sqrt{\big(\sum\limits_{i,j} a_{ij}^2\big)}$.

Теорема 1 [13]. *Пусть $k \geq n > s \geq 1$ и $r \to \infty$. Тогда*
(1) $N(r; n, k, s) = \alpha(n, k, s) r^{ks} + O(r^{ks-1})$ при $n < k$,
(2) $N(r; k, k, s) = \beta(k, s) r^{ks} \log r + O(r^{ks})$ при $n = k$.

Заметим, что порядок роста $N(r; n, k, s)$ не изменится при использовании нормы $\|\cdot\|_\infty$ вместо $\|\cdot\|_2$. Пусть

$$N(r; n, k, s)_\infty = |\{A \in V_{n,k,s}(\mathbb{Z}) \mid \|A\|_\infty < r\}|.$$

Очевидно, что

$$\frac{1}{\sqrt{nk}} \|A\|_2 \leq \|A\|_\infty \leq \|A\|_2,$$

$$N(r; n, k, s) \leq N(r; n, k, s)_\infty \leq N(r\sqrt{nk}; n, k, s).$$

Тогда из теоремы 1 получаем, что для любого $s = 1, \ldots, n-1$

$$\rho(V_{n,k,s}(\mathbb{Z})) = \lim_{r \to \infty} \frac{N(r; n, k, s)_\infty}{(2r+1)^{nk}} = 0. \tag{4}$$

Следовательно, $\rho(V_{n,k,n}(\mathbb{Z})) = 1$, т. е. асимптотически почти все матрицы $A \in \mathbb{Z}^{nk} (n \leq k)$ имеют $\mathrm{rank}(A) = n$.

Теорема 2. *Множество $\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ генерическое при $n \leq k$ и несущественное при $n > k$.*

Доказательство. Пусть $B_r = B_r^{n(k+m)}$. Рассмотрим множество

$$S_1 = \{(A|B) \in \mathbb{Z}^{n(k+m)} \mid \mathrm{rank}(A) = n\}$$

систем $AX = B$ вида (3) при $n \leq k$. Все системы в S_1 разрешимы в $\mathbb{Q}^m$, поэтому справедливо включение $S_1 \subset \mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$. Рассмотрим проекцию $\pi_1 : \mathbb{Z}^{n(k+m)} \to \mathbb{Z}^{nk}$, заданную формулой $\pi_1(A|B) = A$. Заметим, что

$$\pi_1(S_1 \cap B_r) = V_{n,k,n}(\mathbb{Z}) \cap \pi_1(B_r)$$

и каждый прообраз содержит ровно $(2r+1)^{nm}$ элементов. Тогда

$$\frac{|\pi_1(S_1 \cap B_r)|}{(2r+1)^{nk}} = \rho_r(V_{n,k,n}(\mathbb{Z})),$$

$$\rho_r(S_1) = \frac{|S_1 \cap B_r|}{|B_r|} = (2r+1)^{nm} \frac{|\pi_1(S_1 \cap B_r)|}{(2r+1)^{n(k+m)}} = \rho_r(V_{n,k,n}(\mathbb{Z})).$$

Следовательно, $\rho(S_1) = \rho(V_{n,k,n}(\mathbb{Z})) = 1$. Отсюда вытекает, что

$$\rho(\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 1 \quad \text{при } n \le k.$$

Рассмотрим множество

$$S_2 = \{(A|B) \in \mathbb{Z}^{n(k+m)} \mid \mathrm{rank}(A|B_1) < k+1\}$$

систем $AX = B$ вида (3) при $n > k$, где B_1 — первый столбец матрицы B. По лемме 1 разрешимость системы $AX = B$ в $\mathbb{Q}^m$ влечет разрешимость системы $Ax = B_1$ над $\mathbb{Q}$, откуда следует, что $\mathrm{rank}(A|B_1) < k+1$, так как $n > k$. Поэтому справедливо включение $\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n) \subset S_2$. Рассмотрим проекцию $\pi_2 : \mathbb{Z}^{n(k+m)} \to \mathbb{Z}^{n(k+1)}$, заданную формулой $\pi_2(A|B) = (A|B_1)$. Заметим, что

$$\pi_2(S_2 \cap B_r) = \pi_2(B_r) \backslash (V_{k+1,n,k+1}(\mathbb{Z}) \cap \pi_2(B_r))$$

и каждый прообраз содержит ровно $(2r+1)^{n(m-1)}$ элементов. Тогда

$$\frac{|\pi_2(S_2 \cap B_r)|}{(2r+1)^{n(k+1)}} = 1 - \rho_r(V_{k+1,n,k+1}(\mathbb{Z})),$$

$$\rho_r(S_2) = \frac{|S_2 \cap B_r|}{|B_r|} = (2r+1)^{n(m-1)} \frac{|\pi_2(S_2 \cap B_r)|}{(2r+1)^{n(k+m)}} = 1 - \rho_r(V_{k+1,n,k+1}(\mathbb{Z})).$$

Следовательно, $\rho(S_2) = 1 - \rho(V_{k+1,n,k+1}(\mathbb{Z})) = 0$. Отсюда

$$\rho(\mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 0 \quad \text{при } n > k. \quad \square$$

Следствие 1. *При $n > k$ множество $\mathrm{SAT}(\mathbb{Z}^m, k, n)$ несущественное.*

Доказательство. Так как $\mathrm{SAT}(\mathbb{Z}^m, k, n) \subset \mathrm{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$, то

$$\rho(\mathrm{SAT}(\mathbb{Z}^m, k, n)) = 0 \quad \text{при } n > k. \quad \square$$

5. Квазиполиномы Эрхарта

При вычислении асимптотической плотности некоторых множеств в свободных абелевых группах полезным оказывается знание характера роста количества точек целочисленной решетки в расширениях выпуклых многогранников (см., например, [17]). Основы изучения этого вопроса заложены в 1960-х гг. французским математиком Эрхартом. Подробное изложение приводимых далее результатов содержится в [14] (см. также [15]).

Выпуклым многогранником $\mathscr{P}$ в $\mathbb{R}^d$ называется пересечение конечного числа замкнутых полупространств, т. е. $\mathscr{P} = \{x \in \mathbb{R}^d \mid Ax \le b\}$, где $A \in \mathbb{R}^{md}$, $b \in \mathbb{R}^m$. Далее будут рассматриваться только ограниченные выпуклые многогранники.

Для $t \in \mathbb{Z}^+$ множество $t\mathscr{P} = \{tx \mid x \in \mathscr{P}\}$ — t-расширение многогранника $\mathscr{P}$.

Если все вершины $\mathscr{P}$ являются точками решетки $\mathbb{Z}^d$, то будем называть $\mathscr{P}$ *многогранником решетки*. *Рациональным многогранником* будем называть многогранник, все вершины которого имеют рациональные координаты. В этом случае *знаменателем* $\mathscr{P}$ будем называть наименьшее $p \in \mathbb{Z}^+$, при котором $p\mathscr{P}$ является многогранником решетки $\mathbb{Z}^d$.

Обозначим $L_{\mathscr{P}}(t) = |\{t\mathscr{P} \cap \mathbb{Z}^d\}|$. *Рядом Эрхарта* будем называть ряд

$$\operatorname{Ehr}_{\mathscr{P}}(z) = \sum_{t\geq 0} L_{\mathscr{P}}(t) z^t.$$

При этом условимся считать, что $L_{\mathscr{P}}(0) = 1$.

Далее $\binom{n}{k}$ обозначает *биномиальный коэффициент*, определяемый формулой

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} \quad \text{для } n \in \mathbb{C},\ k \in \mathbb{Z}^+. \tag{5}$$

Следующая теорема суммирует некоторые известные результаты, касающиеся количества точек решетки $\mathbb{Z}^d$ в расширениях многогранников решетки [14, теоремы 3.8, 3.12, леммы 3.13, 3.14].

Теорема 3. *Пусть $\mathscr{P}$ — d-мерный многогранник решетки $\mathbb{Z}^d$. Тогда*

(1) $\operatorname{Ehr}_{\mathscr{P}}(z) = \frac{h_d z^d + \dots + h_1 z + 1}{(1-z)^{d+1}}$, *где* $h_i \in \mathbb{N}$,

(2) $L_{\mathscr{P}}(t) = \binom{t+d}{d} + h_1\binom{t+d-1}{d} + \dots + h_{d-1}\binom{t+1}{d} + h_d\binom{t}{d}$ *— полином от t степени d.*

Полином $L_{\mathscr{P}}(t)$ называют *полиномом Эрхарта для многогранника $\mathscr{P}$*.

Некоторые коэффициенты полинома $L_{\mathscr{P}}(t) = c_d t^d + \dots + c_1 t + c_0$ имеют геометрическую интерпретацию. Так, например, старший коэффициент c_d равен $\operatorname{vol}(\mathscr{P})$ — d-мерному объему $\mathscr{P}$ [14, следствие 3.20], откуда следует

$$\operatorname{vol}(\mathscr{P}) = \frac{1}{d!}(h_d + \dots + h_1 + 1). \tag{6}$$

Также известно, что $c_0 = 1$ [14, следствие 3.15].

Определение 2. *Квазиполиномом степени d* называется функция вида

$$f(n) = c_d(n)n^d + \dots + c_1(n)n + c_0(n),$$

где $c_i(n)$ — периодические функции от n с целым периодом, $c_d(n) \not\equiv 0$.

Если f — квазиполином, то существуют $N \in \mathbb{Z}^+$ и полиномы $f_0, \dots, f_{N-1}$ такие, что

$$f(n) = f_i(n) \quad \text{при } n \equiv i (\operatorname{mod} N).$$

Наименьшее такое N называется *периодом* квазиполинома f.

Теорема 3 допускает обобщение на произвольные рациональные многогранники [14, теорема 3.23, упражнение 3.25].

Теорема 4. *Пусть $\mathscr{P}$ — d-мерный рациональный многогранник в $\mathbb{R}^d$ со знаменателем p. Тогда*

(1) $\operatorname{Ehr}_{\mathscr{P}}(z) = \frac{\sum_{i=0}^{p(d+1)-1} h_i z^i}{(1-z^p)^{d+1}}$, *где* $h_i \in \mathbb{N}$,

(2) *$L_{\mathscr{P}}(t)$ является квазиполиномом от t степени d, период которого делит p.*

Квазиполином $L_{\mathscr{P}}(t)$ называют *квазиполиномом Эрхарта для многогранника $\mathscr{P}$*.

Нам понадобится явное представление для квазиполиномов Эрхарта, как это указано для полиномов Эрхарта в теореме 3.

Лемма 2. *В обозначениях теоремы* 4

$$L_{\mathscr{P}}(t) = f_j(t) \quad \text{при } t \equiv j (\operatorname{mod} p),$$

где

$$f_j(t) = h_j \binom{t+d}{d} + h_{p+j} \binom{t+d-1}{d} + \cdots + h_{dp+j} \binom{t}{d}.$$

Доказательство. Имеем

$$\operatorname{Ehr}_{\mathscr{P}}(z) = \frac{\sum\limits_{i=0}^{d} \sum\limits_{j=0}^{p-1} h_{ip+j} z^{ip+j}}{(1-z^p)^{d+1}} = \left(\sum_{i=0}^{d} \sum_{j=0}^{p-1} h_{ip+j} z^{ip+j} \right) \sum_{t \geq 0} \binom{t+d}{d} z^{tp}$$
$$= \sum_{i=0}^{d} \sum_{j=0}^{p-1} h_{ip+j} \sum_{t \geq 0} \binom{t+d}{d} z^{ip+j+tp} = \sum_{i=0}^{d} \sum_{j=0}^{p-1} h_{ip+j} \sum_{t \geq i} \binom{t+d-i}{d} z^{pt+j}.$$

В соответствии с определением (5) во всех бесконечных суммах можно начать суммирование с $t = 0$, не изменяя самой суммы. Тогда

$$\operatorname{Ehr}_{\mathscr{P}}(z) = \sum_{i=0}^{d} \sum_{j=0}^{p-1} h_{ip+j} \sum_{t \geq 0} \binom{t+d-i}{d} z^{pt+j}$$
$$= \sum_{j=0}^{p-1} \sum_{t \geq 0} \left(\sum_{i=0}^{d} h_{ip+j} \binom{t+d-i}{d} \right) z^{pt+j} = \sum_{j=0}^{p-1} \sum_{t \geq 0} f_j(t) z^{pt+j}. \qquad \square$$

Для квазиполиномов Эрхарта $L_{\mathscr{P}}(t) = c_d(t)t^d + \cdots + c_1(t)t + c_0(t)$, как и для полиномов, старший коэффициент $c_d(t)$ равен d-мерному объему $\mathscr{P}$, а $c_0(t) = 1$ [14, упражнения 3.27, 3.29]. Таким образом, c_d и c_0 — константы. Отсюда следует аналогичная (6) формула

$$\operatorname{vol}(\mathscr{P}) = \frac{1}{d!}(h_j + h_{p+j} + \cdots + h_{dp+j}), \quad \text{где } j = 0, \ldots, p-1. \tag{7}$$

Не всякий полином может являться полиномом Эрхарта, так как последние довольно специфичны. Их коэффициенты, а также корни, удовлетворяют определенным соотношениям (см., например, [18]). Обратимся к неравенству, полученному в [16].

Напомним, что *числа Стирлинга первого рода* $s(n,k)$ определяются как коэффициенты при последовательных степенях переменной x в многочлене $[x]_n$:

$$[x]_n = x(x-1)\ldots(x-n+1) = \sum_{k=0}^{n} s(n,k) x^k. \tag{8}$$

Теорема 5 [16]. *Пусть $\mathscr{P}$ — d-мерный многогранник решетки $\mathbb{Z}^d$ с полиномом Эрхарта $L_{\mathscr{P}}(t) = c_d t^d + \cdots + c_1 t + 1$. Тогда*

$$c_r \leq (-1)^{d-r} s(d,r) c_d + (-1)^{d-r-1} \frac{s(d,r+1)}{(d-1)!} \quad \text{для } r = 1, \ldots, d-1.$$

Установим аналогичное неравенство для коэффициентов квазиполиномов Эрхарта.

Теорема 6. *Пусть $\mathscr{P}$ — d-мерный рациональный многогранник в $\mathbb{R}^d$ со знаменателем p и квазиполиномом Эрхарта $L_{\mathscr{P}}(t) = c_d t^d + c_{d-1}(t)t^{d-1} + \dots + c_1(t)t + 1$. Тогда*

$$|c_r(t)| \le |s(d+1, r+1)|c_d \quad \text{для } r = 1, \dots, d-1,\ t \in \mathbb{Z}^+.$$

Доказательство. Далее для произвольного полинома $g(x)$ коэффициент при x^i будем обозначать через $g(x)|_i$.

Согласно лемме 2 $L_{\mathscr{P}}(t) = f_j(t)$ при $t \equiv j \pmod p$, где

$$f_j(t) = \sum_{i=0}^{d} h_{ip+j}\binom{t+d-i}{d}.$$

Тогда

$$c_r(j) = f_j(t)|_r = \left(\sum_{i=0}^{d} h_{ip+j}\binom{t+d-i}{d}\right)\Bigg|_r = \sum_{i=0}^{d} h_{ip+j}\binom{t+d-i}{d}\Bigg|_r.$$

Нетрудно убедиться, что при $i = 1, \dots, d$

$$\left|\binom{t+d-i}{d}\Bigg|_r\right| \le \binom{t+d}{d}\Bigg|_r.$$

Отсюда с учетом $h_i \in \mathbb{N}$ и формулы (7) следует, что для $j = 0, \dots, p-1$

$$|c_r(j)| = |f_j(t)|_r| \le \sum_{i=0}^{d} h_{ip+j}\left|\binom{t+d-i}{d}\Bigg|_r\right| \le \sum_{i=0}^{d} h_{ip+j}\binom{t+d}{d}\Bigg|_r$$

$$= \binom{t+d}{d}\Bigg|_r (h_j + h_{p+j} + \dots + h_{dp+j}) = \binom{t+d}{d}\Bigg|_r d!\operatorname{vol}(\mathscr{P}) = |s(d+1, r+1)|c_d. \quad \square$$

Пусть $w_1, \dots, w_d$ — линейно независимые векторы в $\mathbb{R}^d$. Множество

$$\Lambda = \Lambda(w_1, \dots, w_d) = \{x_1 w_1 + \dots + x_d w_d \mid x_i \in \mathbb{Z}\}$$

называется *решеткой* с базисом $\{w_1, \dots, w_d\}$, число $d(\Lambda) = |\det(w_1, \dots, w_d)|$ — *определителем решетки* Λ.

Заметим, что результаты данного раздела остаются справедливыми и для произвольной решетки $\Lambda(w_1, \dots, w_d)$. Действительно, пусть A — матрица, столбцами которой являются векторы $(w_1, \dots, w_d)$, и ψ — линейное преобразование, заданное матрицей A. Тогда $\Lambda = \psi(\mathbb{Z}^d)$ и $\mathbb{Z}^d = \psi^{-1}(\Lambda)$. Если $\mathscr{P}$ — d-мерный многогранник такой, что некоторое его расширение $t\mathscr{P}$ является многогранником решетки Λ, то $\psi^{-1}(\mathscr{P})$ — d-мерный рациональный многогранник и

$$L_{\mathscr{P},\Lambda}(t) = |\{t\mathscr{P} \cap \Lambda\}| = |\{t\psi^{-1}(\mathscr{P}) \cap \mathbb{Z}^d\}|.$$

Учитывая, что $\operatorname{vol}(\mathscr{P}) = |\det(A)|\operatorname{vol}(\psi^{-1}(\mathscr{P}))$, получаем, что старший коэффициент $L_{\mathscr{P},\Lambda}(t)$ равен $\frac{\operatorname{vol}(\mathscr{P})}{d(\Lambda)}$.

6. Системы, разрешимые в $\mathbb{Z}^m$

Оценим асимптотическую плотность множества $\mathrm{SAT}(\mathbb{Z}^m, k, n)$.

Для начала упомянем классические критерии разрешимости в целых числах для систем линейных диофантовых уравнений вида

$$Ax = b, \quad \text{где } A \in \mathbb{Z}^{nk},\ b \in \mathbb{Z}^n. \tag{9}$$

Пусть $M \in \mathbb{Z}^{nk}$ $(n \le k)$ и $\operatorname{rank}(M) = n$. Тогда $\gcd(M)$ обозначает *наибольший делитель матрицы* M, который определяется как наибольший общий делитель ее миноров порядка n.

Теорема 7 [19]. *Пусть $Ax = b$ — система вида (9) и $\operatorname{rank}(A) = n$. Система имеет целочисленное решение тогда и только тогда, когда наибольший делитель матрицы системы совпадает с наибольшим делителем ее расширенной матрицы.*

Также можно упомянуть критерий, который, по-видимому, принадлежит Ван дер Вардену, но автор не нашел подходящей ссылки.

Теорема 8 (Ван дер Варден). *Система $Ax = b$ вида (9) имеет целочисленное решение тогда и только тогда, когда*

$$\forall v \in \mathbb{Q}^n \quad vA \in \mathbb{Z}^k \Longrightarrow (v, b) \in \mathbb{Z}.$$

Воспользуемся другим критерием, который позволит нам применить теорию Эрхарта. Рассмотрим при $n \le k$ систему уравнений из $\mathbb{Z}^m_{X,n}$ вида

$$AX = B, \quad \text{где } A \in \mathbb{Z}^{nk},\ B \in \mathbb{Z}^{nm}. \tag{10}$$

Обозначим через A_i и B_j столбцы матриц A и B соответственно, и пусть $H_A = \langle A_1, \dots, A_k \rangle$ — подгруппа в $\mathbb{Z}^n$, порожденная столбцами матрицы A.

Справедлива следующая очевидная

Лемма 3. *Система $AX = B$ вида (10) разрешима в $\mathbb{Z}^m$ тогда и только тогда, когда $B_i \in H_A$ для любого $i = 1, \dots, m$.*

Пусть $\operatorname{rank}(A) = n$. Тогда H_A — подгруппа конечного индекса в $\mathbb{Z}^n$, а следовательно, является n-мерной решеткой в $\mathbb{R}^n$ с определителем $d(H_A) = |\mathbb{Z}^n : H_A| = \gcd(A)$, а B_1^n — n–мерный рациональный многогранник. Таким образом,

$$\left|\left\{B_r^n \cap H_A\right\}\right| = \left|\left\{rB_1^n \cap H_A\right\}\right| = L_{B_1^n, H_A}(r)$$

— квазиполином Эрхарта, который далее будем обозначать просто через $L_A(r)$. Рассмотрим сумму

$$S_{m,k,n}(r) = \sum_{\substack{A \in B_r^{nk},\\ \operatorname{rank}(A)=n}} L_A^m(r). \tag{11}$$

В соответствии с леммой 3 эта сумма описывает количество разрешимых систем вида (10) из $\mathbb{Z}^m_{X,n}$ в шаре $B_r^{n(k+m)}$, для которых $\operatorname{rank}(A) = n$. Пусть

$$L_A(t) = c_{A,n}t^n + c_{A,n-1}(t)t^{n-1} + \dots + c_{A,1}(t)t + 1,$$

$$L_A^m(r) = \sum_{i=0}^{mn} \alpha_{A,i} r^i.$$

Тогда $S_{m,k,n}(r)$ можно представить в виде

$$S_{m,k,n}(r) = \sum_{\substack{A \in B_r^{nk},\\ \operatorname{rank}(A)=n}} \sum_{i=0}^{mn} \alpha_{A,i} r^i = \sum_{i=0}^{mn} \Big(\sum_{\substack{A \in B_r^{nk},\\ \operatorname{rank}(A)=n}} \alpha_{A,i} \Big) r^i = \sum_{i=0}^{mn} s_{m,k,n,i}(r) r^i.$$

Легко видеть, что $\alpha_{A,0} = 1$ и

$$\alpha_{A,mn} = c_{A,n}^m = \left(\frac{\operatorname{vol}(B_1^n)}{d(H_A)} \right)^m = 2^{mn} \gcd(A)^{-m}.$$

Тогда

$$s_{m,k,n,mn}(r) = \sum_{\substack{A \in B_r^{nk},\\ \operatorname{rank}(A)=n}} \alpha_{A,mn} = 2^{mn} \sum_{\substack{A \in B_r^{nk},\\ \operatorname{rank}(A)=n}} \gcd(A)^{-m}.$$

Лемма 4. $s_{m,k,n,mn}(r) = O(r^{nk})$ *при* $r \to \infty$.

Доказательство. Имеем

$$s_{m,k,n,mn}(r) = 2^{mn} \sum_{\substack{A\in B_r^{nk},\\ \operatorname{rank}(A)=n}} \gcd(A)^{-m} \le 2^{mn} \sum_{\substack{A\in B_r^{nk},\\ \operatorname{rank}(A)=n}} 1$$
$$\le 2^{mn}\left|B_r^{nk}\right| = 2^{mn}(2r+1)^{nk}. \quad \square$$

Покажем, что слагаемое $r^{mn}s_{m,k,n,mn}(r)$ вносит основной вклад в сумму $S_{m,k,n}(r)$ с точки зрения асимптотической плотности.

Лемма 5. $\lim\limits_{r\to\infty} \frac{s_{m,k,n,i}(r)r^i}{r^{n(k+m)}} = 0$ *при* $i = 0, \dots, mn-1$.

Доказательство. Для $i = 0$ утверждение очевидно, так как $\alpha_{A,0} = 1$. Согласно теореме 6 для $r = 1, \dots, n-1$

$$|c_{A,r}(t)| \le \max_i \{|s(n+1,i)|\} c_{A,n},$$

тогда для любой суммы вида

$$\Omega(r) = \sum_{\substack{A\in B_r^{nk},\\ \operatorname{rank}(A)=n}} c_{A,i_1}(r)\dots c_{A,i_s}(r), \quad \text{где } i_j \in \{1,\dots,n\}, \tag{12}$$

справедливо $|\Omega(r)| \le \beta s_{s,k,n,sn}(r)$ для некоторой константы β, не зависящей от r. Значит, $\Omega(r) = O(r^{nk})$. Любая сумма

$$s_{m,k,n,i}(r) = \sum_{\substack{A\in B_r^{nk},\\ \operatorname{rank}(A)=n}} \alpha_{A,i}$$

может быть представлена в виде суммы конечного числа сумм вида (12), а значит, также есть $O(r^{nk})$.

Утверждение леммы следует из того факта, что для любой функции $f(r) = O(r^{nk})$

$$\lim_{r\to\infty} \frac{f(r)r^i}{r^{n(k+m)}} = 0 \quad \text{при } i < mn. \qquad \square$$

Пусть

$$F_{m,k,n}(r) = \frac{s_{m,k,n,mn}(r)}{2^{mn}} = \sum_{\substack{A\in B_r^{nk},\\ \operatorname{rank}(A)=n}} \gcd(A)^{-m}.$$

Установим связь между асимптотической плотностью множества $\mathrm{SAT}(\mathbb{Z}^m,k,n)$ и суммой $F_{m,k,n}(r)$.

Теорема 9. *Существует* $\rho(\mathrm{SAT}(\mathbb{Z}^m,k,n)) = \rho$ *тогда и только тогда, когда существует*

$$\lim_{r\to\infty} \frac{F_{m,k,n}(r)}{(2r)^{nk}} = \rho.$$

Доказательство. Пусть существует $\rho(\mathrm{SAT}(\mathbb{Z}^m,k,n)) = \rho$. Тогда в силу (4) системы с матрицами ранга меньше n не вносят вклад в асимптотическую плотность и

$$\lim_{r\to\infty} \frac{S_{m,k,n}(r)}{\left|B_r^{n(k+m)}\right|} = \rho.$$

Далее, по лемме 5 только старшее слагаемое $S_{m,k,n}(r)$ вносит вклад в последний предел, тогда

$$\lim_{r\to\infty} \frac{s_{m,k,n,mn}(r)r^{mn}}{\left|B_r^{n(k+m)}\right|} = \rho = \lim_{r\to\infty} \frac{s_{m,k,n,mn}(r)r^{mn}}{(2r)^{n(k+m)}} = \lim_{r\to\infty} \frac{F_{m,k,n}(r)}{(2r)^{nk}}.$$

Обратное аналогично. $\square$

Рассмотрим случай, когда $n = k$ и $m = 1$. Тогда

$$F_{1,n,n}(r) = \sum_{\substack{A\in B_r^{nn},\\ \operatorname{rank}(A)=n}} \frac{1}{|\det(A)|}. \tag{13}$$

В [20] приводится асимптотика целочисленных матриц с заданным значением определителя. Пусть

$$V_{n,k} = \{M \in \mathbb{Z}^{nn} \mid \det(M) = k\}, \quad N(r, V_{n,k}) = |\{M \in V_{n,k} \mid \|M\|_2 \le r\}|,$$

тогда согласно [20, пример 1.6]

$$N(r, V_{n,k}) \sim c_{n,k} r^{n^2-n}.$$

В предположении, что каждое значение определителя принимается примерно одинаковое количество раз, получаем, что

$$F_{1,n,n}(r) = O(r^{n^2-n}\ln(r)),$$

тогда

$$\lim_{r\to\infty} \frac{F_{1,n,n}(r)}{(2r)^{nn}} = 0$$

и, значит, $\rho(\mathrm{SAT}(\mathbb{Z}, n, n)) = 0$. Далее, так как

$$\rho(\mathrm{SAT}(\mathbb{Z}^{m+1}, n, n)) \le \rho(\mathrm{SAT}(\mathbb{Z}^m, n, n)),$$

то $\rho(\mathrm{SAT}(\mathbb{Z}^m, n, n)) = 0$ для произвольного m.

Это дает основания выдвинуть следующую гипотезу.

Гипотеза 1. $F_{1,n,n}(r) = O(r^{n^2-n}\ln(r))$ *и* $\rho(\mathrm{SAT}(\mathbb{Z}^m, n, n)) = 0$.

Далее установим оценки для нижней и верхней асимптотических плотностей множества $\mathrm{SAT}(\mathbb{Z}^m, k, n)$.

Матрицу $A \in \mathbb{Z}^{nk} (n \le k)$ будем называть *унимодулярной*, если она может быть дополнена до матрицы $\bar{A} \in GL_n(\mathbb{Z})$. Известно, что A унимодулярная тогда и только тогда, когда наибольший делитель A равен единице. Из теоремы 7 следует, что любая система $AX = B$ из $\mathbb{Z}^m_{X,n}$ с унимодулярной матрицей A разрешима в $\mathbb{Z}^m$. Обозначим

$$U_{n,k} = \{A \in \mathbb{Z}^{nk} \mid A \text{ унимодулярная}\}.$$

Далее $\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ — дзета-функция Римана.

Асимптотическая плотность унимодулярных матриц известна из следующего результата.

Теорема 10 [21]. (1) $\rho(U_{n,k}) = \left(\prod\limits_{j=k-n+1}^{k} \zeta(j)\right)^{-1}$ *при* $k > n \geq 1$,
(2) $\rho(U_{n,n}) = 0$ *при* $n \geq 1$.

Заметим, что в [21] используется немного другое определение плотности в $\mathbb{Z}^{nk}$, которое тем не менее эквивалентно нашему определению асимптотической плотности относительно стратификации $\mathbb{Z}^{nk}$ шарами в норме $\|\cdot\|_\infty$.

Теорема 10 позволяет получить оценку нижней асимптотической плотности множества $\mathrm{SAT}(\mathbb{Z}^m, k, n)$. Для получения оценки верхней плотности необходим результат, устанавливающий асимптотическую плотность разрешимых уравнений в Z^m.

Теорема 11 [10]. (1) $\rho(\mathrm{SAT}(\mathbb{Z}^m, k)) = \frac{\zeta(k+m)}{\zeta(k)}$ *при* $k \geq 2$,
(2) $\rho(\mathrm{SAT}(\mathbb{Z}^m, 1)) = 0$.

Докажем один из основных результатов данной работы.

Теорема 12. *Справедливы следующие оценки:*
(1) $\rho(U_{n,k}) \leq \underline{\rho}(\mathrm{SAT}(\mathbb{Z}^m, k, n))$ *при* $k > n > 1$,
(2) $\overline{\rho}(\mathrm{SAT}(\mathbb{Z}^m, k, n)) \leq \rho(\mathrm{SAT}(\mathbb{Z}^m, k))^n$ *при* $k \geq n > 1$.

Доказательство. Рассмотрим при $k > n > 1$ множество

$$S_1 = \{(A|B) \in \mathbb{Z}^{n(k+m)} \mid A \text{ унимодулярная}\} \subset \mathrm{SAT}(\mathbb{Z}^m, k, n).$$

Нетрудно показать, что $\rho(S_1) = \rho(U_{n,k})$. Тогда

$$\rho(U_{n,k}) \leq \underline{\rho}(\mathrm{SAT}(\mathbb{Z}^m, k, n)).$$

Рассмотрим множество S_2 систем из $\mathbb{Z}^m_{X,n}$, в которых каждое из n уравнений разрешимо в отдельности. Очевидно, что $\mathrm{SAT}(\mathbb{Z}^m, k, n) \subset S_2$. Заметим, что

$$\rho_r(S_2) = \rho_r(\mathrm{SAT}(\mathbb{Z}^m, k))^n,$$

$$\rho(S_2) = \lim_{r\to\infty} \rho_r(S_2) = (\lim_{r\to\infty} \rho_r(\mathrm{SAT}(\mathbb{Z}^m, k)))^n = \rho(\mathrm{SAT}(\mathbb{Z}^m, k))^n.$$

Тогда

$$\overline{\rho}(\mathrm{SAT}(\mathbb{Z}^m, k, n)) \leq \rho(\mathrm{SAT}(\mathbb{Z}^m, k))^n. \qquad \square$$

В заключение автор благодарит своего научного руководителя В. А. Романькова за поставленную задачу и полезные советы и замечания.

ЛИТЕРАТУРА

1. *Erdos P., Turan P.* On some problems of statistical group theory. I // Z. Wahrscheinlichkeitstheorie verw. Geb. 1965. V. 4. P. 175–186.
2. *Dixon J.* The probability of generating the symmetric group // Math. Z. 1969. Bd 110, Heft 3. S. 199–205.
3. *Gromov M.* Hyperbolic groups // Essays in group theory. MSRI publ. New York; Berlin: Springer-Verl., 1987. V. 8. P. 75–263.
4. *Gromov M.* Asymptotic invariants of infinite groups // Geometric group theory (Sussex, 1991). Cambridge: Cambridge Univ. Press, 1993 V. 2. P. 1–295. London Math. Soc. Lect. Notes Ser.; V. 182).
5. *Gromov M.* Random walks in random groups // Geom. Funct. Anal. 2003. V. 13. P. 73–146.
6. *Kapovich I., Schupp P.* Genericity, the Arzhantseva–Olshanskii method and the isomorphism problem for one-relator groups // Math. Ann. 2005. V. 331, N 1. P. 1–19.
7. *Kapovich I., Schupp P.* Delzant's T-invariant, one-relator groups and Kolmogorov complexity // Comment. Math. Helv. 2005. V. 80. P. 911–933.

8. *Кукина Е. Г., Романьков В. А.* Субквадратичность усредненной функции Дена для свободных абелевых групп // Сиб. мат. журн. 2003. Т. 44, № 4. С. 772–778.

9. *Романьков В. А.* Об асимптотическом росте усредненной функции Дена для нильпотентных групп // Алгебра и логика. 2007. Т. 46, № 1. С. 60–74.

10. *Gilman R., Myasnikov A., Roman'kov V.* Random equations in nilpotent groups // J. Algebra. 2012. V. 352. P. 192–214.

11. *Gilman R., Myasnikov A., Roman'kov V.* Random equations in free groups // Groups, Complexity, Cryptol. 2011. V. 3. P. 257–284.

12. *Antolin Y., Ciobanu L., Viles N.* On the asymptotics of visible elements and homogeneous equations in surface groups // Groups Geom. Dyn. 2012. V. 6. P. 619–638.

13. *Katznelson Y.* Integral matrices of fixed rank // Proc. Amer. Math. Soc. 1994. V. 120, N 3. P. 667–675.

14. *Beck M., Robins S.* Computing the continuous discretely. New York: Springer-Verl., 2007.

15. *Stanley R.* Enumerative combinatorics.. Cambridge: Cambridge Univ. Press, 1997. V. 1.

16. *Betke U., McMullen P.* Lattice points in lattice polytopes // Monatsh. Math. 1985. V. 99, N 4. P. 253–265.

17. *Меньшов А.* Асимптотическая плотность рациональных множеств в $\mathbb{Z}^n$ // Вестн. Омск. ун-та. 2013. № 2. С. 37–40.

18. *Beck M., De Loera J., Develin M., Pfeifle J., Stanley R.* Coefficients and roots of Ehrhart polynomials // Integer points in polyhedra. Geometry, number theory, algebra, optimization. Providence, RI: Amer. Math. Soc., 2005. P. 15–36. (Contemp. Math.; V. 374). arXiv:math.CO/0402148.

19. *Smith H. J. S.* On systems of linear indeterminate equations and congruences // Philos. Trans. R. Soc. Lond. 1861. V. 151. P. 293–326.

20. *Duke W., Rudnick Z., Sarnak P.* Density of integer points on affine homogeneous varieties // Duke Math. J. 1993. V. 71, N 1. P. 143–179.

21. *Maze G., Rosenthal J., Wagner U.* Natural density of rectangular unimodular integer matrices // Linear Algebra Appl. 2011. V. 434, N 5. P. 1319–1324.

Статья поступила 18 сентября 2013 г.

Меньшов Антон Владимирович
Омский гос. университет им. Ф. М. Достоевского,
пр. Мира, 55 А, Омск 644077
`menshov.a.v@gmail.com`