Math-Net.Ru

Общероссийский математический портал

В. И. Круглов, Предельные распределения числа наборов, удовлетворяющих линейному соотношению, *Дискрет. матем.*, 2008, том 20, выпуск 4, 120–135

DOI: <https://doi.org/10.4213/dm1032>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 34.239.49.27

26 апреля 2023 г., 14:13:00

Предельные распределения числа наборов, удовлетворяющих линейному соотношению

© 2008 г. В. И. Круглов

Пусть $X_1, \dots, X_T$ — совокупность независимых случайных элементов конечной абелевой группы G , имеющих на ней равномерное распределение. В работе найдены условия, при которых число упорядоченных наборов $(i_1, \dots, i_k)$ попарно различных чисел из $\{1, \dots, T\}$ таких, что $a_1 X_{i_1} + \dots + a_k X_{i_k} = 0$, где $a_1, \dots, a_k$ — фиксированные целые числа, имеет предельное пуассоновское распределение, когда $T \rightarrow \infty$ и группа G изменяется вместе с T . Приведен также пример последовательности групп G , для которой предельное распределение числа наборов является сложным пуассоновским.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 08–01–00078.

1. Введение

Одна из предложенных Дж. Марсальей статистик, предназначенных для проверки качества датчиков псевдослучайных чисел, строится следующим образом (см., например, [1], с. 110). Пусть $X_1, \dots, X_T$ — порожденные датчиком значения из множества $\{1, \dots, N\}$, а $X_{(1)} \leq X_{(2)} \leq \dots \leq X_{(T)}$ — построенный по ним вариационный ряд. Статистика $\zeta(T, N)$ — это число таких пар (i, j) , $1 \leq i < j \leq T$, что $X_{(i+1)} - X_{(i)} = X_{(j+1)} - X_{(j)}$. Сформулированное в [1] в виде задачи утверждение о том, что распределение $\zeta(T, N)$ сходится к распределению Пуассона с параметром λ при $T, N \rightarrow \infty$, $T^3/(4N) \rightarrow \lambda$, было доказано в работе Н. В. Клыковой [4].

В настоящей работе рассматривается аналогичная задача. Пусть G — конечная абелева группа по сложению и $X_1, \dots, X_T$ — независимые случайные величины, имеющие равномерное распределение на G . В теоремах 1 и 2 указаны условия, при которых число наборов $(i_1, \dots, i_k)$ попарно различных чисел из $\{1, \dots, T\}$ таких, что $a_1 X_{i_1} + \dots + a_k X_{i_k} = 0$, где $a_1, \dots, a_k$ — фиксированные целые числа, имеет предельное пуассоновское распределение, когда $T \rightarrow \infty$ и группа G изменяется вместе с T . В теореме 3 приведен пример последовательности групп G , для которой предельное распределение числа таких наборов является сложным пуассоновским.

2. Комбинаторные свойства линейных соотношений

Пусть k — натуральное число, $a_1, \dots, a_k$ — ненулевые целые числа.

Обозначим через $\mathcal{F}_T$ множество всех упорядоченных наборов из k попарно различных элементов множества $\{1, \dots, T\}$ такого, что

$$|\mathcal{F}_T| = \frac{T!}{(T-k)!} = T^{[k]}.$$

Сопоставим каждому набору $(j_1, \dots, j_k) \in \mathcal{F}_T$ уравнение

$$a_1 y_{j_1} + \dots + a_k y_{j_k} = 0.$$

Будем называть наборы $(j_1^1, \dots, j_k^1) \in \mathcal{F}_T$ и $(j_1^2, \dots, j_k^2) \in \mathcal{F}_T$ эквивалентными (относительно $a_1, \dots, a_k$), если уравнения $a_1 y_{j_1^1} + \dots + a_k y_{j_k^1} = 0$, $a_1 y_{j_1^2} + \dots + a_k y_{j_k^2} = 0$ равносильны над $\mathbf{Z}$, то есть множества их целочисленных решений совпадают. Это отношение эквивалентности разбивает $\mathcal{F}_T$ на классы эквивалентных наборов; обозначим через $\mathcal{F}_T^*$ систему представителей классов эквивалентности, $|\mathcal{F}_T^*| = n$.

Лемма 1. Уравнения $c_1^1 z_1 + \dots + c_t^1 z_t = 0$ и $c_1^2 z_1 + \dots + c_t^2 z_t = 0$, где $c_i^1, c_i^2 \in \mathbf{Z}$, равносильны над $\mathbf{Z}^t$ тогда и только тогда, когда существует такое $\gamma \in \mathbf{Q}$, что $(c_1^1, \dots, c_t^1) = \gamma(c_1^2, \dots, c_t^2)$.

Доказательство. Очевидно, что если $(c_1^1, \dots, c_t^1) = \gamma(c_1^2, \dots, c_t^2)$, то уравнения равносильны.

Обратно, пусть уравнения равносильны. Если существует такое $i \in \{1, \dots, t\}$, что $c_i^1 = 0$ и $c_i^2 \neq 0$, то любой набор $z_1, \dots, z_t$, в котором $z_j = 0 \iff j \neq i$, является решением первого уравнения, но не является решением второго, что противоречит их равносильности. Значит, $c_i^1 \neq 0 \iff c_i^2 \neq 0$ для любого $i = 1, \dots, t$. Если число ненулевых элементов в $(c_1^1, \dots, c_t^1)$ не больше 1, то векторы $(c_1^1, \dots, c_t^1)$ и $(c_1^2, \dots, c_t^2)$ пропорциональны с рациональным коэффициентом пропорциональности γ . Если же оно больше 1 и, для определенности, $c_1^1 \neq 0$, $c_1^2 \neq 0$, то для любого $i > 1$ такого, что $c_i^1 \neq 0$, $c_i^2 \neq 0$, набор переменных $z_{i1} = -c_i^1$, $z_i = c_1^1$, $z_j = 0$ при $j \neq 1, i$, является решением первого уравнения. Следовательно, он является решением второго уравнения, а тогда $-c_i^2 c_1^1 + c_1^2 c_i^1 = 0$, то есть для любого такого i , что $c_i^1 \neq 0$, $c_i^2 \neq 0$,

$$\frac{c_i^1}{c_i^2} = \frac{c_1^1}{c_1^2},$$

будем обозначать это отношение γ .

Лемма 2. Если наборы $(j_1^1, \dots, j_k^1), (j_1^2, \dots, j_k^2) \in \mathcal{F}_T$ эквивалентны относительно набора $a_1, \dots, a_k$, то существует такая перестановка $\sigma \in S_k$, что

$$j_1^1 = j_{\sigma(1)}^2, \dots, j_k^1 = j_{\sigma(k)}^2.$$

Доказательство. Если существует такое $i \in \{1, \dots, k\}$, что $j_i^2 \notin \{j_1^1, \dots, j_k^1\}$, то любой набор $(y_1, \dots, y_T)$, в котором $y_m \neq 0 \iff m = j_i^2$, является решением уравнения $a_1 y_{j_1^1} + \dots + a_k y_{j_k^1} = 0$, но не является решением уравнения $a_1 y_{j_1^2} + \dots + a_k y_{j_k^2} = 0$, что противоречит их равносильности. Следовательно, $\{j_1^2, \dots, j_k^2\} \subseteq \{j_1^1, \dots, j_k^1\}$. Аналогично, $\{j_1^1, \dots, j_k^1\} \subseteq \{j_1^2, \dots, j_k^2\}$, откуда следует, что $\{j_1^1, \dots, j_k^1\} = \{j_1^2, \dots, j_k^2\}$.

Так как $j_l^1 \neq j_m^1$ и $j_l^2 \neq j_m^2$ при $l \neq m$, множество $\{j_1^2, \dots, j_k^2\}$ является перестановкой множества $\{j_1^1, \dots, j_k^1\}$, что и требовалось доказать.

Пусть S — множество всех перестановок $\sigma \in S_k$ таких, что уравнение

$$a_1 y_1 + \dots + a_k y_k = 0$$

равносильно уравнению

$$a_{\sigma(1)} y_1 + \dots + a_{\sigma(k)} y_k = 0,$$

и $w = w(a_1, \dots, a_k) = |S|$. Очевидно, множество S равномощно любому классу эквивалентности множества $\mathcal{F}_T$ относительно набора $(a_1, \dots, a_k)$.

Лемма 3. Пусть уравнение имеет вид

$$a'_1 y_1 + \dots + a'_1 y_{k_1} + a'_2 y_{k_1+1} + \dots + a'_2 y_{k_1+k_2} + \dots + a'_l y_{k_1+\dots+k_l} = 0,$$

где $k_1 + \dots + k_l = k$ и $a'_u \neq a'_v$ при $u \neq v$. Если существует такая перестановка $\sigma_0 \in S_k$, что $(-a_1, \dots, -a_k) = (a_{\sigma_0(1)}, \dots, a_{\sigma_0(k)})$, то $w = 2k_1! \dots k_l!$, в противном случае $w = k_1! \dots k_l!$.

Доказательство. Если $\sigma \in S$, то согласно лемме 1 существует такое рациональное число γ , что $(a_{\sigma(1)}, \dots, a_{\sigma(k)}) = \gamma(a_1, \dots, a_k)$. Так как $\max |a_{\sigma(j)}| = \max |a_j|$, справедливо равенство $|\gamma| = 1$, то есть $\gamma = \pm 1$.

Пусть

$$\begin{aligned} S^1 &= \{\sigma \in S_k : (a_{\sigma(1)}, \dots, a_{\sigma(k)}) = (a_1, \dots, a_k), \\ S^2 &= \{\sigma \in S_k : (a_{\sigma(1)}, \dots, a_{\sigma(k)}) = (-a_1, \dots, -a_k)\}. \end{aligned}$$

Тогда $S = S^1 \sqcup S^2$ и в силу условия леммы $|S^1| = k_1! \dots k_l!$. Множество S^2 либо пусто, либо равномощно S^1 . Тем самым лемма доказана.

Из леммы 3 следует, что все классы эквивалентности имеют одну и ту же мощность w . Таким образом,

$$n = |\mathcal{F}_T^*| = \frac{|\mathcal{F}_T|}{|K_1|} = \frac{k!}{w} \binom{k}{T}.$$

3. Вероятностные свойства линейных соотношений

Любую конечную абелеву группу можно представить в виде произведения примарных циклических групп: $G = G_1 \times \dots \times G_m$; для всех таких представлений совокупности значений $\{|G_1|, \dots, |G_m|\}$ совпадают с точностью до перестановки (см., например, [7], гл. I, §10). Положим

$$f(G) = f(a_1, \dots, a_k, G) = \frac{\gcd(a_1, \dots, a_k, |G_1|) \dots \gcd(a_1, \dots, a_k, |G_m|)}{|G_1| \dots |G_l|}.$$

Если наибольший общий делитель $\gcd(a_1, \dots, a_k, |G|) = 1$, то $f(G) = 1/|G|$, а если группа G циклическая и $\gcd(a_1, \dots, a_k, |G|) = q$, то $f(G) = q \cdot |G|$.

Лемма 4. Если G —конечная абелева группа по сложению, случайные величины $X_1, \dots, X_k$ независимы и равномерно распределены на G , то

$$\mathbf{P}(a_1 X_1 + \dots + a_k X_k = 0) = f(a_1, \dots, a_k, G).$$

Доказательство. Пусть G — примарная циклическая группа порядка p^s , где p — простое число. Очевидно, $\gcd(a_1, \dots, a_k, p^s) = p^t$ для некоторого целого $t \in \{0, 1, \dots, s\}$. Если $t = s$, то $f(G) = 1$ и a_i кратно p^s для любого $i = 1, \dots, k$. Следовательно,

$$\mathbf{P}(a_1 X_1 + \dots + a_k X_k = 0) = 1 = f(a_1, \dots, a_k, G).$$

Пусть $t < s$. Положим $a'_i = a_i / p^t$, тогда

$$a_1 X_1 + \dots + a_k X_k = p^t (a'_1 X_1 + \dots + a'_k X_k).$$

Хотя бы одно число из $a'_1, \dots, a'_k$ не делится на p , поэтому для какого-то $i \in \{1, \dots, k\}$ число a'_i обратимо по модулю p^s . Без ограничения общности будем считать, что $i = 1$.

Для любого $g \in G$ по формуле полной вероятности

$$\begin{aligned} \mathbf{P}(a'_1 X_1 + \dots + a'_k X_k = g) &= \mathbf{P}(X_1 = (a'_1)^{-1}(g - a'_2 X_2 - \dots - a'_k X_k)) \\ &= \sum_{h \in G} \mathbf{P}(g - a'_2 X_2 - \dots - a'_k X_k = h) \\ &\quad \times \mathbf{P}(X_1 = (a'_1)^{-1}h \mid g - a'_2 X_2 - \dots - a'_k X_k = h) \\ &= \sum_{h \in G} \frac{1}{|G|} \mathbf{P}(g - a'_2 X_2 - \dots - a'_k X_k = h) = \frac{1}{|G|}, \end{aligned}$$

следовательно,

$$\begin{aligned} \mathbf{P}(a_1 X_1 + \dots + a_k X_k = 0) &= \mathbf{P}(p^t (a'_1 X_1 + \dots + a'_k X_k) = 0) \\ &= \mathbf{P}(a'_1 X_1 + \dots + a'_k X_k \text{ делится на } p^{s-t}) \\ &= \frac{|\{g \in G \mid g \text{ делится на } p^{s-t}\}|}{|G|} = \frac{p^t}{|G|} \\ &= \frac{\gcd(a_1, \dots, a_k, |G|)}{|G|} = f(G). \end{aligned}$$

Пусть G — абелева группа. Тогда найдутся примарные циклические группы $G_1, \dots, G_m$ такие, что $G = G_1 \times \dots \times G_m$, и любой элемент $g \in G$ однозначно представим в виде $g = (g_1, \dots, g_m)$. Так как $X_1, \dots, X_k$ независимы и равномерно распределены на G , представления $X_j = (X_{j,1}, \dots, X_{j,m})$ независимы и компоненты $X_{j,i}$ этих представлений независимы и равномерно распределены на соответствующих группах G_i . Поэтому

$$\mathbf{P}(a_1 X_1 + \dots + a_k X_k = 0) = \prod_{i=1}^m \mathbf{P}(a_1 X_{1,i} + \dots + a_k X_{k,i} = 0) = f(a_1, \dots, a_k, G),$$

так как из доказанного выше следует, что

$$\mathbf{P}(a_1 X_{1,i} + \dots + a_k X_{k,i} = 0) = \frac{\gcd(a_1, \dots, a_k, |G_i|)}{|G_i|}, \quad i = 1, \dots, m.$$

4. Предельная теорема

Пусть случайные величины $X_1, \dots, X_T$ независимы в совокупности и имеют равномерное распределение на конечной абелевой группе G , пусть заданы ненулевые целые числа

$a_1, \dots, a_k$ и $\mathcal{J}_T, \mathcal{J}_T^*$, w те же, что были введены в разделе 1. Положим

$$\begin{aligned}\xi &= \frac{1}{w} \sum_{(j_1, \dots, j_k) \in \mathcal{J}_T} I(a_1 X_{j_1} + \dots + a_k X_{j_k} = 0) \\ &= \sum_{(j_1, \dots, j_k) \in \mathcal{J}_T^*} I(a_1 X_{j_1} + \dots + a_k X_{j_k} = 0).\end{aligned}$$

Теорема 1. Пусть ненулевые целые числа $a_1, \dots, a_k$ фиксированы, $T \rightarrow \infty$ и группа G изменяется так, что $|G| = N \rightarrow \infty$,

$$\mathbf{E}\xi = \frac{T^{[k]} f(a_1, \dots, a_k, G)}{w} \rightarrow \lambda, \quad 0 < \lambda < \infty,$$

и для любых фиксированных $\delta \in \mathbf{N}$, $\varepsilon > 0$ выполняется соотношение

$$\mathbf{P}(\delta Y = 0) = o(N^{-1+\varepsilon}),$$

где Y — случайная величина, имеющая равномерное распределение на G . Тогда

$$\lim_{N, T \rightarrow \infty} \mathbf{P}(\xi = m) = \frac{\lambda^m}{m!} e^{-\lambda}, \quad m = 0, 1, 2, \dots$$

Доказательство. Пусть

$$\mathcal{J}_T^* = \{(j_1^i, \dots, j_k^i) \mid i = 1, \dots, n\},$$

где

$$n = |\mathcal{J}_T^*| = \frac{T^{[k]}}{w}, \quad \eta_i = I(a_1 X_{j_1^i} + \dots + a_k X_{j_k^i} = 0), \quad i = 1, \dots, n.$$

Для любого неупорядоченного набора попарно различных индексов $(i_1, \dots, i_r)$, $1 \leq i_j \leq n$, введем обозначение

$$b_{i_1 \dots i_r} = \mathbf{P}(\eta_{i_1} = \dots = \eta_{i_r} = 1).$$

Согласно теореме Б. А. Севастьянова (см. [8] и [5], с. 117), распределения сумм случайных индикаторов сходятся к распределению Пуассона с параметром λ , если выполняются следующие условия:

$$\lim_{N, T \rightarrow \infty} \max_{1 \leq i \leq n} b_i = 0, \quad \lim_{N, T \rightarrow \infty} \sum_{i=1}^n b_i = \lambda, \quad (\text{A})$$

и для любого $r = 2, 3, \dots$ найдутся такие множества $I_r(n)$ наборов индексов $(i_1, \dots, i_r)$, что справедливы предельные соотношения

$$\lim_{N, T \rightarrow \infty} \sum_{(i_1, \dots, i_r) \in I_r(n)} b_{i_1 \dots i_r} = 0, \quad \lim_{N, T \rightarrow \infty} \sum_{(i_1, \dots, i_r) \in I_r(n)} b_{i_1} \dots b_{i_r} = 0, \quad (\text{B})$$

$$\lim_{N, T \rightarrow \infty} \max_{(i_1, \dots, i_r) \notin I_r(n)} \left| \frac{b_{i_1 \dots i_r}}{b_{i_1} \dots b_{i_r}} - 1 \right| = 0. \quad (\text{C})$$

В силу леммы 4, индикаторы η_i одинаково распределены и $\mathbf{P}(\eta_i = 1) = b_i = f(G)$ (здесь и далее $f(G) = f(a_1, \dots, a_k, G)$), поэтому выполнение условий (A) следует из условий теоремы:

$$\mathbf{E}\xi = \sum_{i=1}^n b_i = nb_1 = \frac{T^{[k]}}{w} f(G) \rightarrow \lambda,$$

$$\max_{1 \leq i \leq n} b_i = f(G) = O\left(\frac{1}{T^k}\right) = o(1).$$

Каждому $i = 1, \dots, n$ соответствуют набор $j_1^i, \dots, j_k^i$ и уравнение

$$a_1 X_{j_1^i} + \dots + a_k X_{j_k^i} = 0.$$

Будем говорить, что совокупность попарно различных чисел $(i_1, \dots, i_r)$, $r \geq 2$, $1 \leq i_j \leq n$, принадлежит исключительному множеству $I_r(n)$, если для некоторых s и t , $1 \leq s < t \leq r$, соответствующие i_s и i_t наборы $j_1^{i_s}, \dots, j_k^{i_s}$ и $j_1^{i_t}, \dots, j_k^{i_t}$ пересекаются. Отметим, что при $(i_1, \dots, i_r) \notin I_r(n)$ индикаторы $\eta_{i_1}, \dots, \eta_{i_r}$ независимы и поэтому выполняется условие (C).

Для совокупности $(i_1, \dots, i_r)$ (при заданных r и T) обозначим через $A_{i_1, \dots, i_r}$ матрицу системы линейных уравнений относительно $x_1, \dots, x_T$

$$\begin{aligned} a_1 x_{j_1^{i_1}} + \dots + a_k x_{j_k^{i_1}} &= 0, \\ &\dots \\ a_1 x_{j_1^{i_r}} + \dots + a_k x_{j_k^{i_r}} &= 0. \end{aligned} \tag{1}$$

Под рангом матрицы будем понимать ее ранг над кольцом целых чисел.

Так как матрица $A_{i_1, \dots, i_r}$ имеет r строк и T столбцов, $r < T$, для ее ранга справедливо неравенство $\text{rank}(A_{i_1, \dots, i_r}) \leq r$. В то же время по построению множества $\mathcal{J}_T^*$ первые два уравнения системы (1) не равносильны, поэтому (см. лемму 1) первые две строки $A_{i_1, \dots, i_r}$ не пропорциональны и $2 \leq \text{rank}(A_{i_1, \dots, i_r}) \leq r$.

Разобьем $I_r(n)$ на непересекающиеся множества

$$I_r^v(n) = \{(i_1, \dots, i_r) \in I_r(n) \mid \text{rank}(A_{i_1, \dots, i_r}) = v\}, \quad v = 2, \dots, r.$$

Лемма 5. При $T \rightarrow \infty$ для любого v , $2 \leq v \leq r$,

$$|I_r^v(n)| = O(T^{kv-1}).$$

Доказательство. Пусть сначала $v = r$. Тогда число ненулевых элементов в матрице $A_{i_1, \dots, i_r}$ равно kr , и если $(i_1, \dots, i_r) \in I_r(n)$, то матрица $A_{i_1, \dots, i_r}$ имеет не более $kr - 1$ столбцов, содержащих ненулевые элементы.

Число вариантов выбора столбцов, содержащих ненулевые элементы, не превосходит

$$\sum_{m=k}^{kr-1} \binom{T}{m} = O\left(\binom{T}{kr-1}\right),$$

а число способов составить матрицы вида $A_{i_1, \dots, i_r}$, расставив числа $a_1, \dots, a_k$ в выбранных столбцах, конечно и не зависит от N и T . Поэтому число таких матриц есть $O\left(\binom{T}{kr-1}\right)$. Следовательно, при фиксированных k, r и $T \rightarrow \infty$

$$|I_r^r(n)| \leq |I_r(n)| = O(T^{kr-1}).$$

Пусть теперь $2 \leq v \leq r - 1$. Если $(i_1, \dots, i_r) \in I_r^v(n)$, то в матрице $A_{i_1, \dots, i_r}$ можно выбрать v линейно независимых строк. Будем называть эти строки базисными, остальные небазисными; v базисных строк содержат kv ненулевых элементов, которые покрываются не более чем kv столбцами. Допустим, что эти элементы содержатся ровно в kv столбцах. Рассмотрим небазисную строку, которая является линейной комбинацией v базисных строк. Она отлична от каждой из первых v строк, поэтому по крайней мере два коэффициента в этой линейной комбинации не равны нулю. Так как по предположению все ненулевые элементы базисных строк расположены в разных столбцах, небазисная строка содержит не меньше $2k$ ненулевых элементов, а это противоречит тому, что их ровно k .

Таким образом, все ненулевые элементы v базисных строк покрываются не более чем $kv - 1$ столбцами. Эти столбцы можно выбрать не более чем

$$\sum_{m=k}^{kv-1} \binom{T}{m} = O\left(\binom{T}{kv-1}\right)$$

способами. Учитывая, что число возможных расположений строк в матрице, число возможных размещений ненулевых элементов базисных строк в выбранных столбцах, а также число способов выбора коэффициентов в выражениях небазисных строк через базисные строки ограничены константой, зависящей лишь от k и v , получаем, что при фиксированных r, k, v , $2 \leq v \leq r - 1$, и $T \rightarrow \infty$

$$|I_r^v(n)| = O\left(\binom{T}{kv-1}\right) = O(T^{kv-1}).$$

Из леммы 5 и условий теоремы следует выполнение второго из условий (B):

$$\sum_{(i_1, \dots, i_r) \in I_r(n)} b_{i_1} \dots b_{i_r} = f(G)^r |I_r(n)| = f(G)^r O(T^{kr-1}) \rightarrow 0.$$

Лемма 6. Для любого v , $2 \leq v \leq r$, величина $\sup_{(i_1, \dots, i_r) \in I_r^v(n)} b_{i_1, \dots, i_r}$ не зависит от T и при $N \rightarrow \infty$

$$\sup_{(i_1, \dots, i_r) \in I_r^v(n)} b_{i_1, \dots, i_r} = o(\sqrt[k]{N}/N^v).$$

Доказательство. Введем обозначение $\vec{X} = (X_1, \dots, X_T)^\top$. Тогда

$$\eta_{i_1} = \dots = \eta_{i_r} = 1 \iff A_{i_1, \dots, i_r} \vec{X} = 0.$$

Под матрицей $\text{diag}(d_1, \dots, d_t)_{m \times n}$, где $t \leq \min(m, n)$, будем понимать матрицу D размера $m \times n$ такую, что

$$d_{ij} = \begin{cases} d_s, & \text{если } i = j = s, 1 \leq s \leq t, \\ 0 & \text{в противном случае.} \end{cases}$$

Предложение 1 ([3]). Для любой матрицы A над $\mathbf{Z}$ размера $r \times T$ существуют обратимые над $\mathbf{Z}$ матрицы U и V такие, что

$$UAV = A^1 = \text{diag}(\delta_1, \dots, \delta_t),$$

где $\delta_1, \dots, \delta_t \in \mathbf{N}_0$ и δ_{i+1} кратно δ_i для всех $i = 1, \dots, t - 1$, причем матрица A^1 определена единственным образом.

Будем для любой матрицы $A_{i_1, \dots, i_r}$ обозначать через $A_{i_1, \dots, i_r}^1 = UA_{i_1, \dots, i_r}V$ диагональную матрицу $A_{i_1, \dots, i_r}^1$ из предложения 1.

Если $(i_1, \dots, i_r) \in I_r^v(n)$, то число ненулевых элементов матрицы $A_{i_1, \dots, i_r}^1$ равно v , так как $\text{rank}(A_{i_1, \dots, i_r}^1) = \text{rank}(UA_{i_1, \dots, i_r}V) = \text{rank}(A_{i_1, \dots, i_r}) = v$ в силу невырожденности матриц U и V .

Преобразуем систему уравнений $A_{i_1, \dots, i_r} \vec{X} = 0$ следующим образом:

$$A_{i_1, \dots, i_r} \vec{X} = 0 \iff UA_{i_1, \dots, i_r}V(V^{-1}\vec{X}) = 0 \iff A_{i_1, \dots, i_r}^1(V^{-1}\vec{X}) = 0.$$

Лемма 7. Пусть $\alpha_1, \dots, \alpha_m$ — независимые случайные величины, равномерно распределенные на G , C и C^{-1} — невырожденные целочисленные матрицы размера $m \times m$. Пусть $\vec{\beta} = C^{-1}\vec{\alpha}$, где $\vec{\alpha} = (\alpha_1, \dots, \alpha_m)^\top$, $\vec{\beta} = (\beta_1, \dots, \beta_m)^\top$. Тогда $\beta_1, \dots, \beta_m$ — независимые случайные величины, равномерно распределенные на G .

Доказательство. Ясно, что $\vec{\beta} = \vec{g} \iff \vec{\alpha} = C\vec{g}$ для любого $\vec{g} \in G^m$. Так как случайный вектор $\vec{\alpha}$ имеет равномерное распределение на множестве G^m ,

$$\mathbf{P}(\vec{\beta} = \vec{g}) = \mathbf{P}(\vec{\alpha} = C\vec{g}) = \frac{1}{|G^m|},$$

то есть $\vec{\beta}$ имеет равномерное распределение на множестве G^m , из чего следует независимость $\beta_1, \dots, \beta_m$.

Введем обозначение $\vec{Y} = (Y_1, \dots, Y_T)^\top = V^{-1}\vec{X}$. Так как матрица V обратима над кольцом $\mathbf{Z}$, матрица V^{-1} также является целочисленной матрицей. Из того, что случайные величины $X_1, \dots, X_T$ независимы, имеют равномерное распределение на G , из леммы 7 следует, что $Y_1, \dots, Y_T$ — независимые случайные величины, равномерно распределенные на G .

Так как вектор $\vec{X}$ равномерно распределен на G^T , для любой совокупности $(i_1, \dots, i_r) \in I_r^v(n)$

$$b_{i_1, \dots, i_r} = \mathbf{P}(A_{i_1, \dots, i_r} \vec{X} = 0) = \mathbf{P}(A_{i_1, \dots, i_r}^1 \vec{Y} = 0),$$

где $A_{i_1, \dots, i_r}^1 = \text{diag}(\delta_1, \dots, \delta_v)$ и вектор $\vec{Y}$ равномерно распределен на G^T . Поэтому в силу последнего условия теоремы с $\varepsilon = 1/(2vk)$

$$\begin{aligned} b_{i_1, \dots, i_r} &= \mathbf{P}(\delta_1 Y_1 = 0, \dots, \delta_v Y_v = 0) = \mathbf{P}(\delta_1 Y_1 = 0) \dots \mathbf{P}(\delta_v Y_v = 0) \\ &= \left(o \left(\frac{2vk\sqrt{N}}{N} \right) \right)^v = o \left(\frac{2k\sqrt{N}}{N^v} \right). \end{aligned}$$

Заметим, что вероятность $b_{i_1, \dots, i_r}$ зависит лишь от вида матрицы $A_{i_1, \dots, i_r}^1$, то есть не зависит от T . Следовательно,

$$\sup_{(i_1, \dots, i_r) \in I_r^v(n)} b_{i_1, \dots, i_r} = o \left(\frac{2k\sqrt{N}}{N^v} \right)$$

и не зависит от T . Лемма 6 доказана.

Наконец, докажем, что выполняется первое из условий (В).

Так как

$$f(a_1, \dots, a_k, G) \geq \frac{1}{|G_1| \dots |G_m|} = \frac{1}{N}$$

и по условию

$$\frac{1}{w} T^{[k]} f(a_1, \dots, a_k, G) \rightarrow \lambda,$$

при достаточно больших N и T

$$\frac{T^k}{wN} \leq \frac{T^k f(a_1, \dots, a_k, G)}{w} \leq 2\lambda,$$

то есть $T^k/N \leq 2\lambda w$. Используя оценки лемм 5 и 6, получаем, что

$$\begin{aligned} \sum_{(i_1, \dots, i_r) \in I_r(n)} b_{i_1, \dots, i_r} &= \sum_{v=2}^r \sum_{(i_1, \dots, i_r) \in I_r^v(n)} b_{i_1, \dots, i_r} \leq \sum_{v=2}^r |I_r^v(n)| \sup_{(i_1, \dots, i_r) \in I_r^v(n)} b_{i_1, \dots, i_r} \\ &= o\left(\sum_{v=2}^r \frac{2^k \sqrt[k]{N}}{N^v} T^{kv-1}\right) = o\left(\sum_{v=2}^r \left(\frac{T^k}{N}\right)^v \frac{2^k \sqrt[k]{N}}{T}\right) = o\left(\frac{2^k \sqrt[k]{N}}{T}\right). \end{aligned}$$

Таким образом, осталось доказать, что $2^k \sqrt[k]{N}/T \rightarrow 0$. Пусть $\delta_0 = \gcd(a_1, \dots, a_k)$ и случайная величина Y имеет равномерное распределение на группе G . Тогда

$$\mathbf{P}(\delta_0 Y = 0) = \frac{\gcd(\delta_0, |G_1|) \dots \gcd(\delta_0, |G_m|)}{|G_1| \dots |G_m|} = f(G).$$

Из последнего условия теоремы 1 следует, что для всех $\varepsilon > 0$

$$f(G) = \mathbf{P}(\delta_0 Y = 0) = o\left(\frac{N^\varepsilon}{N}\right).$$

Поскольку $T^{[k]} f(a_1, \dots, a_k, G) \rightarrow \lambda w$, при достаточно больших N и T справедливо неравенство $T^k f(G) \geq \lambda w/2$, откуда следует, что для всех $\varepsilon > 0$

$$\frac{1}{T} = o(N^{-1/k+\varepsilon}).$$

Таким образом,

$$\frac{2^k \sqrt[k]{N}}{T} = o(N^{-1/(2k)+\varepsilon}) = o(1),$$

поскольку здесь можно выбрать $\varepsilon < 1/(2k)$. Теорема 1 доказана.

5. Пример

Рассмотрим две последовательности абелевых групп $G_1(d) = \mathbf{Z}_2^d$, $G_2(d) = \mathbf{Z}_4 \times (\mathbf{Z}_2)^{d-2}$, $d = 1, 2, \dots$, для которых последнее условие теоремы 1 не выполняется. Покажем, что в первом случае предельное распределение ξ пуассоновское, а во втором может быть сложным пуассоновским.

Теорема 2. Пусть случайные величины $X_1, \dots, X_T$ независимы и равномерно распределены на $G = \mathbf{Z}_2^d$,

$$\xi = \sum_{(j_1, \dots, j_k) \in \mathcal{J}_T^*} I(X_{j_1} + \dots + X_{j_k} = 0).$$

Если $d, T \rightarrow \infty$ так, что $\mathbf{E}\xi \rightarrow \lambda$, где $0 < \lambda < \infty$, то распределение случайной величины ξ сходится к распределению Пуассона с параметром λ .

Теорема 3. Пусть случайные величины $X_1, \dots, X_T$ независимы и равномерно распределены на $G = \mathbf{Z}_4 \times (\mathbf{Z}_2)^{d-2}$,

$$\xi = \sum_{(j_1, j_2, j_3) \in \mathcal{J}_T^*} I(-X_{j_1} + X_{j_2} + X_{j_3} = 0).$$

Если $d, T \rightarrow \infty$ так, что $\mathbf{E}\xi \rightarrow \lambda$, где $0 < \lambda < \infty$, то распределение ξ сходится к сложному пуассоновскому распределению:

$$\mathbf{E}s^\xi \rightarrow \exp\left(\frac{\lambda(s^3 + 3s^2 + 3s - 7)}{12}\right).$$

Доказательство теоремы 2. Для любого $(j_1, \dots, j_k) \in \mathcal{J}_T^*$ согласно лемме 4

$$\mathbf{P}(X_{j_1} + \dots + X_{j_k} = 0) = f(1, \dots, 1, \mathbf{Z}_2^d) = \frac{1}{2^d} = \frac{1}{|G|},$$

значит,

$$\mathbf{E}\xi = |\mathcal{J}_T^*| \frac{1}{2^d} = \frac{T^{[k]}}{w(1, \dots, 1)} \frac{1}{2^d} = \frac{T^{[k]}}{2^d k!} = \frac{T^k (1 + o(1))}{2^d k!} = \frac{T^k}{2^d k!} (1 + o(1)),$$

так как $w(1, \dots, 1) = k!$ по лемме 3.

Используем метод Чена–Стейна (см. [2]).

Лемма 8. Пусть $\xi = \sum_{i \in \Gamma} \eta_i$, где случайные индикаторы η_i одинаково распределены, $p = \mathbf{P}\{\eta_1 = 1\}$. Пусть для каждого $i \in \Gamma$ множество $\Gamma \setminus \{i\}$ разбито на непересекающиеся подмножества Γ_i^s и Γ_i^w , и $\gamma = \sup_{i \in \Gamma} |\Gamma_i^s|$, $Z_i = \sum_{j \in \Gamma_i^s} \eta_j$, $W_i = \sum_{j \in \Gamma_i^w} \eta_j$.

Если $\gamma \rightarrow \infty$ и выполняются следующие условия:

- (1) случайные величины η_i и W_i независимы для любого $i \in \Gamma$,
- (2) существует равномерная по всем $i \in \Gamma$, $j \in \Gamma_i^s$ оценка $\mathbf{E}\eta_i \eta_j = O(p^2)$,

а случайная величина $\pi(\lambda)$ имеет распределение Пуассона с параметром λ , то для расстояния полной вариации между ξ и $\pi(\mathbf{E}\xi)$ справедлива оценка

$$\rho(\xi, \pi(\mathbf{E}\xi)) = \sup_{A \subset \mathbf{Z}_+} |\mathbf{P}(\xi \in A) - \mathbf{P}(\pi(\mathbf{E}\xi) \in A)| = O(|\Gamma| p^2 \gamma).$$

Доказательство. Согласно [2] (с. 66, формула (2.2); с. 70, теорема 2.5),

$$\rho(\xi, \pi(\mathbf{E}\xi)) \leq k_2 \sum_{i \in \Gamma} (p \mathbf{E}(\eta_i + Z_i) + \mathbf{E}\eta_i Z_i) + k_1 \sum_{i \in \Gamma} \mathbf{E}|p - \mathbf{E}(\eta_i | W_i)|,$$

где

$$k_1 = k_1(\mathbf{E}\xi) = 1 \wedge \sqrt{\frac{2}{e\mathbf{E}\xi}}, \quad k_2 = k_2(\mathbf{E}\xi) = \frac{1 - \exp(-\mathbf{E}\xi)}{\mathbf{E}\xi}.$$

Так как для любого $i \in \Gamma$ по условию леммы случайная величина W_i не зависит от η_i , при всех $i \in \Gamma$

$$\mathbf{E}|p - \mathbf{E}(\eta_i | W_i)| \equiv 0.$$

Далее,

$$\mathbf{E}(\eta_i + Z_i) = \mathbf{E}\left(\eta_i + \sum_{j \in \Gamma_i^s} \eta_j\right) = p(1 + |\Gamma_i^s|) \leq p(1 + \gamma) = O(p\gamma),$$

и в силу второго условия леммы

$$\mathbf{E}\eta_i Z_i = \mathbf{E}\left(\eta_i \sum_{j \in \Gamma_i^s} \eta_j\right) = \sum_{j \in \Gamma_i^s} \mathbf{E}\eta_i \eta_j = O(p^2)|\Gamma_i^s| = O(p^2\gamma),$$

следовательно,

$$\rho(\xi, \pi(\mathbf{E}\xi)) \leq k_2 \sum_{i \in \Gamma} (p\mathbf{E}(\eta_i + Z_i) + \mathbf{E}\eta_i Z_i) \leq k_2 \sum_{i \in \Gamma} O(p^2\gamma) = O(|\Gamma|p^2\gamma),$$

и лемма 8 доказана.

Положим $\Gamma = \mathcal{J}_T^*$ и для всех $i \in \Gamma$ разобьем множество $\Gamma \setminus \{i\}$ на Γ_i^s и Γ_i^w следующим образом: будем считать, что $l \in \Gamma_i^s$, если множества переменных в уравнениях $X_{j_1^i} + \dots + X_{j_k^i} = 0$ и $X_{j_1^l} + \dots + X_{j_k^l} = 0$ пересекаются, и будем считать, что $l \in \Gamma_i^w$ в противном случае.

Из независимости $X_1, \dots, X_T$ следует, что для любых двух различных наборов $(j_1^i, \dots, j_k^i)$ и $(j_1^l, \dots, j_k^l)$ соответствующие им индикаторы независимы, следовательно, выполняется второе условие леммы 8. Первое условие выполняется, поскольку ни одна из переменных $X_{j_1^i}, \dots, X_{j_k^i}$ не входит в запись случайной величины W_i .

Заметим, что для любого $l \in \Gamma_i^s$ хотя бы одна переменная из $X_{j_1^i}, \dots, X_{j_k^i}$ входит в набор $X_{j_1^l}, \dots, X_{j_k^l}$, поэтому $|\Gamma_i^s| \leq kT^{k-1}$. Следовательно, $\gamma \leq k^2T^{k-1} = O(|\Gamma|T^{-1})$ и, если

$$\mathbf{E}\xi = |\Gamma|p = \frac{T^k}{2^d k!}(1 + o(1)) \rightarrow \lambda \in (0, \infty),$$

то

$$\rho(\xi, \pi(\mathbf{E}\xi)) \leq O(|\Gamma|p^2|\Gamma|T^{-1}) = O(T^{-1}|\Gamma|^2p^2) = O(T^{-1}(\mathbf{E}\xi)^2) = O(T^{-1}).$$

Теорема 2 доказана.

Доказательство теоремы 3. Преобразуем запись случайной величины ξ :

$$\begin{aligned} \xi &= \sum_{(j_1, j_2, j_3) \in \mathcal{J}_T^*} I(-X_{j_1} + X_{j_2} + X_{j_3} = 0) \\ &= \sum_{1 \leq j_1 < j_2 < j_3 \leq T} (\eta_{j_1, j_2, j_3}^1 + \eta_{j_1, j_2, j_3}^2 + \eta_{j_1, j_2, j_3}^3) = \sum_{1 \leq j_1 < j_2 < j_3 \leq T} \eta_{j_1, j_2, j_3}, \end{aligned}$$

где $\eta_{j_1, j_2, j_3}^k = I(X_{j_1} + X_{j_2} + X_{j_3} - 2X_{j_k} = 0)$, $k = 1, 2, 3$, $\eta_{j_1, j_2, j_3} = \sum_{k=1}^3 \eta_{j_1, j_2, j_3}^k$.

Лемма 9. Для любых $1 \leq j_1 < j_2 < j_3 \leq T$

$$\begin{aligned} \mathbf{P}\{\eta_{j_1, j_2, j_3} = 0\} &= 1 - \frac{7}{4|G|}, & \mathbf{P}\{\eta_{j_1, j_2, j_3} = 1\} &= \frac{3}{4|G|}, \\ \mathbf{P}\{\eta_{j_1, j_2, j_3} = 2\} &= \frac{3}{4|G|}, & \mathbf{P}\{\eta_{j_1, j_2, j_3} = 3\} &= \frac{1}{4|G|}. \end{aligned}$$

Доказательство. Распределение случайной величины $\eta_{j_1, j_2, j_3}^1 + \eta_{j_1, j_2, j_3}^2 + \eta_{j_1, j_2, j_3}^3$ не зависит от конкретных значений j_1, j_2, j_3 , поэтому будем опускать эти индексы для упрощения формул.

Из леммы 4 следует, что если случайные величины X_1, X_2, X_3 независимы и имеют равномерное распределение на группе G , то

$$\mathbf{P}\{\eta^k = 1\} = \mathbf{P}\{-X_1 + X_2 + X_3 = 0\} = \frac{1}{|G|}, \quad k = 1, 2, 3.$$

При этом же предположении для любых $1 \leq l < k \leq 3$

$$\begin{aligned} \mathbf{P}\{\eta^l = \eta^k = 1\} &= \mathbf{P}\{-X_1 + X_2 + X_3 = 0, X_1 - X_2 + X_3 = 0\} \\ &= \mathbf{P}\{-X_1 + X_2 + X_3 = 0, 2X_3 = 0\} \\ &= \mathbf{P}\{2X_3 = 0\} \mathbf{P}\{-X_1 + X_2 + X_3 = 0 \mid 2X_3 = 0\} = \frac{1}{2|G|}, \end{aligned}$$

и аналогично

$$\begin{aligned} \mathbf{P}\{\eta^1 = \eta^2 = \eta^3 = 1\} \\ &= \mathbf{P}\{-X_1 + X_2 + X_3 = 0, X_1 - X_2 + X_3 = 0, X_1 + X_2 - X_3 = 0\} \\ &= \mathbf{P}\{-X_1 + X_2 + X_3 = 0, 2X_2 = 0, 2X_3 = 0\} = \frac{1}{4|G|}. \end{aligned}$$

Отсюда и из формул включения–исключения следует справедливость леммы 9.

Из леммы 9 следует, что $\mathbf{E}\eta_{j_1, j_2, j_3} \equiv 3/|G|$ и поэтому

$$\mathbf{E}\xi = \binom{T}{3} \mathbf{E}\eta_{j_1, j_2, j_3} = \frac{3\binom{T}{3}}{|G|} = \frac{T^3}{2|G|}(1 + o(1)) = \frac{T^3}{2^{d+1}}(1 + o(1)) \rightarrow \lambda \in (0, \infty).$$

Воспользуемся результатами из [2] (с. 84, §3.1; с. 88, формула (3.7); с. 91, теорема 3.6).

Предложение 2. Пусть

$$\xi = \sum_{i \in \Gamma} \eta_i,$$

где η_i — целочисленные неотрицательные случайные величины, для каждого $i \in \Gamma$ множество $\Gamma \setminus \{i\}$ разбито на непересекающиеся подмножества $\Gamma_i^{vs}, \Gamma_i^w, \Gamma_i^b, u$

$$Z_i = \sum_{j \in \Gamma_i^{vs}} \eta_j, \quad W_i = \sum_{j \in \Gamma_i^w} \eta_j, \quad U_i = \sum_{j \in \Gamma_i^b} \eta_j.$$

Если

$$\pi = \sum_{k=1}^{\infty} k \zeta_k,$$

где ξ_k независимы и случайная величина ξ_k имеет пуассоновское распределение с параметром

$$\lambda_k = \frac{1}{k} \sum_{i \in \Gamma} \mathbf{E}(\eta_i I(\eta_i + Z_i = k)),$$

то для расстояния полной вариации между ξ и π справедлива оценка

$$\begin{aligned} \rho(\xi, \pi) &\leq \sum_{i \in \Gamma} (\mathbf{E}\eta_i \mathbf{E}(\eta_i + Z_i + U_i) + \mathbf{E}\eta_i U_i) \\ &\quad + \sum_{i \in \Gamma} \sum_{j=1}^{\infty} \sum_{m=1}^{\infty} j \mathbf{E} |\mathbf{P}\{\eta_i = j, \eta_i + Z_i = m\} - \mathbf{P}(\eta_i = j, \eta_i + Z_i = m \mid W_i)|. \end{aligned}$$

В нашем случае $\Gamma = \{(j_1, j_2, j_3), 1 \leq j_1 < j_2 < j_3 \leq T\}$. Для каждого $i \in \Gamma$ разобьем множество $\Gamma \setminus \{i\}$ на Γ_i^{vs} , Γ_i^w и Γ_i^b следующим образом: будем считать, что $l \in \Gamma_i^b$, если наборы индексов (j_1^i, j_2^i, j_3^i) и (j_1^l, j_2^l, j_3^l) пересекаются, и будем считать, что $l \in \Gamma_i^w$ в противном случае.

Таким образом, $\Gamma_i^{vs} = \emptyset$ и $Z_i \equiv 0$. Отметим, что для любого $i \in \Gamma$ в сумму, определяющую W_i , не входят $X_{j_1^i}, X_{j_2^i}, X_{j_3^i}$, поэтому η_i , являющаяся функцией от $X_{j_1^i}, X_{j_2^i}, X_{j_3^i}$, и W_i независимы, следовательно,

$$\mathbf{E} |\mathbf{P}\{\eta_i = j, \eta_i + Z_i = m\} - \mathbf{P}(\eta_i = j, \eta_i + Z_i = m \mid W_i)| \equiv 0,$$

то есть

$$\rho(\xi, \pi) \leq \sum_{i \in \Gamma} (\mathbf{E}\eta_i \mathbf{E}(\eta_i + U_i) + \mathbf{E}\eta_i U_i).$$

Для любых различных s и t множества $\{X_{j_1^s}, X_{j_2^s}, X_{j_3^s}\}$ и $\{X_{j_1^t}, X_{j_2^t}, X_{j_3^t}\}$ не совпадают, поэтому из независимости $X_1, \dots, X_T$ следует, что случайные величины $\eta_{j_1^s, j_2^s, j_3^s}^k$ и $\eta_{j_1^t, j_2^t, j_3^t}^l$ независимы для любых различных $k, l = 1, 2, 3$. Далее, в силу леммы 4

$$\mathbf{E}\eta_{j_1^s, j_2^s, j_3^s}^k = \mathbf{E}\eta_{j_1^t, j_2^t, j_3^t}^l = \frac{1}{|G|},$$

следовательно,

$$\mathbf{E}\eta_s \eta_t = \mathbf{E} \sum_{k=1}^3 \eta_{j_1^s, j_2^s, j_3^s}^k \sum_{l=1}^3 \eta_{j_1^t, j_2^t, j_3^t}^l = \sum_{k=1}^3 \sum_{l=1}^3 \mathbf{E}\eta_{j_1^s, j_2^s, j_3^s}^k \eta_{j_1^t, j_2^t, j_3^t}^l = \frac{9}{|G|^2}.$$

Таким образом, с учетом того, что распределение η_i не зависит от $i \in \Gamma$ и $\mathbf{E}\eta_i \equiv 3/|G|$, получаем, что

$$\begin{aligned} \rho(\xi, \pi) &\leq \sum_{i \in \Gamma} (\mathbf{E}\eta_i \mathbf{E}(\eta_i + U_i) + \mathbf{E}\eta_i U_i) = \sum_{i \in \Gamma} \left(\mathbf{E}\eta_i \left(\mathbf{E}\eta_i + \sum_{j \in \Gamma_i^b} \mathbf{E}\eta_j \right) + \sum_{j \in \Gamma_i^b} \mathbf{E}\eta_i \eta_j \right) \\ &= \frac{9}{|G|^2} \sum_{i \in \Gamma} (2|\Gamma_i^b| + 1) = \frac{18|\Gamma||\Gamma_1^b|}{|G|^2} (1 + o(1)) \\ &= \frac{2}{3T} \left(\frac{3\binom{T}{3}}{|G|} \right)^2 (1 + o(1)) = \frac{2\lambda^2}{3T} (1 + o(1)), \end{aligned}$$

так как

$$|\Gamma_i^b| = \binom{T}{2} + \binom{T}{1} = \frac{3}{T} \binom{T}{3} (1 + o(1))$$

для любого $i \in \Gamma$ и

$$\frac{3}{|G|} \binom{T}{3} = \lambda(1 + o(1)).$$

Итак, при условии $\mathbf{E}\xi \rightarrow \lambda$ распределение случайной величины ξ сходится к сложному пуассоновскому распределению суммы $\sum_{k=1}^3 k\zeta_k$, где ζ_k независимы и для любого $k = 1, 2, 3$ случайная величина ζ_k имеет распределение Пуассона с параметром

$$\begin{aligned} \lambda_k &= \lim_{d, T \rightarrow \infty} \frac{1}{k} \sum_{i \in \Gamma} \mathbf{E}(\eta_i I(\eta_i + Z_i = k)) \\ &= \lim_{d, T \rightarrow \infty} \frac{1}{k} \sum_{i \in \Gamma} k \mathbf{P}\{\eta_i = k\} = \lim_{d, T \rightarrow \infty} \binom{T}{3} \mathbf{P}\{\eta_i = k\}, \end{aligned}$$

то есть

$$\lambda_1 = \lambda_2 = \lim_{d, T \rightarrow \infty} \frac{3 \binom{T}{3}}{4|G|} = \frac{\lambda}{4}, \quad \lambda_3 = \lim_{d, T \rightarrow \infty} \frac{\binom{T}{3}}{4|G|} = \frac{\lambda}{12}.$$

Поэтому производящая функция распределения ξ имеет вид

$$\begin{aligned} \mathbf{E}_S \xi &= \mathbf{E}_S \xi_1 + 2\xi_2 + 3\xi_3 = \mathbf{E}_S \xi_1 \mathbf{E}_S 2\xi_2 \mathbf{E}_S 3\xi_3 \\ &= \exp\left(\frac{\lambda}{4}(s-1) + \frac{\lambda}{4}(s^2-1) + \frac{\lambda}{12}(s^3-1)\right) \\ &= \exp\left(\frac{\lambda}{12}(s^3 + 3s^2 + 3s - 7)\right). \end{aligned}$$

Теорема 3 доказана.

Теорема 4. Пусть случайные величины $X_1, \dots, X_T$ независимы и имеют равномерное распределение на $G = \mathbf{Z}_N$, а

$$\xi = \sum_{(j_1, \dots, j_k) \in \mathcal{J}_T^*} I(a_1 X_{j_1} + \dots + a_k X_{j_k} = 0).$$

Если $N, T \rightarrow \infty$ так, что

$$\mathbf{E}\xi = \frac{T^{[k]} \gcd(a_1, \dots, a_k, N)}{wN} \rightarrow \lambda,$$

где $0 < \lambda < \infty$, то распределение случайной величины ξ сходится к распределению Пуассона с параметром λ ; расстояние по вариации между распределением ξ и распределением Пуассона с параметром λ убывает как $O(T^{-1})$.

Доказательство. Согласно лемме 4

$$\mathbf{P}(a_1 X_1 + \dots + a_k X_k = 0) = \frac{q}{N} = f(a_1, \dots, a_k, G),$$

где $q = \gcd(a_1, \dots, a_k, N)$. Отсюда следует формула для $\mathbf{E}\xi$. Покажем, что выполняется последнее условие теоремы 1. Представим N в виде произведения простых множителей: $N = p_1^{\alpha_1} \dots p_m^{\alpha_m}$, где $p_i \neq p_j$ при $i \neq j$, тогда $\mathbf{Z}_N = \mathbf{Z}_{p_1^{\alpha_1}} \times \dots \times \mathbf{Z}_{p_m^{\alpha_m}}$ и для любого фиксированного $r \in \mathbf{N}$, для равномерно распределенной на G случайной величины Y , для любого $\varepsilon > 0$ при $N \rightarrow \infty$

$$\begin{aligned} \mathbf{P}(rY = 0) &= \frac{\gcd(r, p_1^{\alpha_1})}{p_1^{\alpha_1}} \dots \frac{\gcd(r, p_m^{\alpha_m})}{p_m^{\alpha_m}} \\ &= \frac{\gcd(r, N)}{N} \leq \frac{r}{N} = o\left(\frac{N^\varepsilon}{N}\right). \end{aligned}$$

Следовательно, если

$$\mathbf{E}\xi = T^k \gcd(a_1, \dots, a_k, N)/(wN) \rightarrow \lambda,$$

то распределение ξ сходится к распределению Пуассона с параметром λ .

Получим оценку скорости сходимости. Из условий теоремы следует, что $T^k/N \leq 2\lambda w$ при достаточно больших T, N , то есть $T^k = O(N)$.

Для любого набора $(i_1, i_2) \in I_2(n)$ рассмотрим матрицу A_{i_1, i_2} и соответствующую ей матрицу

$$A_{i_1, i_2}^1 = \begin{pmatrix} rr\delta_{i_1, i_2}^1 & 0 \\ 0 & \delta_{i_1, i_2}^2 \end{pmatrix}.$$

Поскольку матрица A_{i_1, i_2}^1 зависит лишь от взаимного расположения строк матрицы A_{i_1, i_2} и не зависит от T , существует такое конечное множество Δ , что $\delta_{i_1, i_2}^1, \delta_{i_1, i_2}^2 \in \Delta$.

Далее, в ходе доказательства леммы 6 было показано, что

$$b_{i_1, i_2} = \mathbf{P}\{\delta_{i_1, i_2}^1 y_1 = 0, \delta_{i_1, i_2}^2 y_2 = 0\} = \frac{\gcd(\delta_{i_1, i_2}^1, N)}{N} \frac{\gcd(\delta_{i_1, i_2}^2, N)}{N},$$

следовательно,

$$\sup_{(i_1, i_2) \in I_2(n)} b_{i_1, i_2} \leq \left(\sup_{\delta \in \Delta} \frac{\gcd(\delta, N)}{N} \right)^2 = \frac{1}{N^2} (\sup_{\delta \in \Delta} \gcd(\delta, N))^2 = O(p^2),$$

поскольку, как было показано ранее,

$$p = \frac{1}{N} \gcd(a_1, \dots, a_k, N) = O\left(\frac{1}{N}\right).$$

Положим $\Gamma = \mathcal{G}_T^*$ и для каждого $i \in \Gamma$ разобьем множество $\Gamma \setminus \{i\}$ на Γ_i^s и Γ_i^w следующим образом: будем считать, что $l \in \Gamma_i^s$, если множества переменных в уравнениях $X_{j_1}^i + \dots + X_{j_k}^i = 0$ и $X_{j_1}^l + \dots + X_{j_k}^l = 0$ пересекаются, и что $l \in \Gamma_i^w$ в противном случае. Заметим, что $|\Gamma_i^s|$ не зависит от i и, поскольку хотя бы одна переменная из $X_{j_1}^i, \dots, X_{j_k}^i$ содержится в множестве $\{X_{j_1}^i, \dots, X_{j_k}^i\}$, постольку $|\Gamma_i^s| \leq kT^{k-1} = O(T^{k-1})$.

Первое условие леммы 8 выполняется, так как ни одна из переменных $X_{j_1}^i, \dots, X_{j_k}^i$ не входит в запись случайной величины W_i , второе условие выполняется, поскольку $\sup_{(i_1, i_2) \in I_2(n)} b_{i_1, i_2} = O(p^2)$. Следовательно, в силу леммы 8

$$\rho(\zeta, \pi(\mathbf{E}\zeta)) = O(|\Gamma|p^2\gamma) = O(T^k p^2 T^{k-1}) = O(T^{-1}).$$

Автор признателен А. М. Зубкову за постановку задачи и внимание.

Список литературы

1. Aldous D. J., *Probability approximations via the Poisson clumping heuristics*. Springer, New York, 1989.
2. Barbour A. D., Chen L. H. Y., *An introduction to Stein's method*. World Scientific, New York, 2005.
3. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра, I*. Гелиос АРВ, Москва, 2003.
4. Клыкова Н. В., Предельное распределение числа совпадающих промежутков. *Теория вероятностей и ее применения* (2002) **47**, №1, 147–152.
5. Колчин В. Ф., Севастьянов Б. А., Чистяков В. П., *Случайные размещения*. Наука, Москва, 1976.
6. Кострикин А. И., *Введение в алгебру. I. Основы алгебры*. Физматлит, Москва, 2000.
7. Ленг С., *Алгебра*. Мир, Москва, 1968.
8. Севастьянов Б. А., Предельный закон Пуассона в схеме сумм зависимых случайных величин. *Теория вероятностей и ее применения* (1972) **17**, №4, 733–738.

Статья поступила 26.12.2007.