О системах уравнений в группе $\mathbb{Z}^m$

Антон Меньшов

ОмГУ им. Ф. М. Достоевского, Омск

Апрель, 2013

Введение

- R. Gilman, A. Myasnikov, V. Roman'kov, *Random equations in free groups*, Groups – Complexity – Cryptology 3 (2 2011), pp. 257–284.
- R. Gilman, A. Myasnikov, V. Roman'kov, *Random equations in nilpotent groups*, Journal of Algebra 352 (1 2012), pp. 192–214

Уравнения в группах

Определение

Уравнением $u = 1$ с k неизвестными в группе G будем называть 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 $x_{i_j} \in X = \{x_1, \dots, x_k\}$.

Уравнения в группах

Определение

Уравнением $u = 1$ с k неизвестными в группе G будем называть 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 $x_{i_j} \in X = \{x_1, \dots, x_k\}$.

Свободное произведение $G_X = F(X) * G$ — пространство всех уравнений в переменных X с коэффициентами из G.

Уравнения в группах

Определение

Уравнением $u = 1$ с k неизвестными в группе G будем называть 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 $x_{i_j} \in X = \{x_1, \dots, x_k\}$.

Свободное произведение $G_X = F(X) * G$ — пространство всех уравнений в переменных X с коэффициентами из G.

Определение

Решением уравнения $u = 1$ в G называется отображение $x_j \to h_j \in G$ такое, что $g_0 h_{i_1}^{m_1} g_1 \dots h_{i_n}^{m_n} g_n = 1$.

Уравнения в группе $\mathbb{Z}^m$

В $\mathbb{Z}^m$ будем использовать аддитивную запись и записывать уравнения в виде

$$\gamma_1 x_1 + \ldots + \gamma_k x_k = b, \quad \text{где} \quad \gamma_j \in \mathbb{Z},\ x_j \in \mathbb{Z}^m(\mathbb{Q}^m),\ b \in \mathbb{Z}^m$$

Систему из n уравнений будем записывать в матричном виде

$$AX = B, \quad \text{где} \quad A \in \mathbb{Z}^{n\cdot k},\ X \in \mathbb{Z}^{k\cdot m}(\mathbb{Q}^{k\cdot m}),\ B \in \mathbb{Z}^{n\cdot m}$$

Уравнения в группе $\mathbb{Z}^m$

В $\mathbb{Z}^m$ будем использовать аддитивную запись и записывать уравнения в виде

$$\gamma_1 x_1 + \ldots + \gamma_k x_k = b, \quad \text{где} \quad \gamma_j \in \mathbb{Z},\ x_j \in \mathbb{Z}^m(\mathbb{Q}^m),\ b \in \mathbb{Z}^m$$

Систему из n уравнений будем записывать в матричном виде

$$AX = B, \quad \text{где} \quad A \in \mathbb{Z}^{n\cdot k},\ X \in \mathbb{Z}^{k\cdot m}(\mathbb{Q}^{k\cdot m}),\ B \in \mathbb{Z}^{n\cdot m}$$

- $G_X = A(X) \times \mathbb{Z}^m \simeq \mathbb{Z}^{k+m}$, где $A(X)$ — свободная абелева группа с базисом $X = (x_1, \ldots, x_k)$
- $G_X^n = \mathbb{Z}^{n(k+m)}$ — пространство всех систем из n уравнений из G_X

Уравнения в группе $\mathbb{Z}^m$

Обозначения:

- $SAT(G, k)$ - множество всех уравнений из G_X, разрешимых в G
- $SAT(G, k, n)$ - множество всех систем из G_X^n, разрешимых в G

Если $G \leq H$, то

- $SAT_H(G, k, n)$ - множество всех систем из G_X^n, разрешимых в H

Системы уравнений в $\mathbb{Z}^m$

Пусть $AX = B$ — система из n уравнений в $\mathbb{Z}^m$.
Обозначим $B_1, \ldots, B_m$ — столбцы матрицы $B \in \mathbb{Z}^{nm}$.

Лемма

Система уравнений $AX = B$ разрешима в $\mathbb{Z}^m(\mathbb{Q}^m)$ тогда и только тогда, когда система $Ax = B_i$ разрешима в $\mathbb{Z}(\mathbb{Q})$ для любого $i = 1, \ldots, m$.
Если $X_i = (x_{1i}, \ldots, x_{ki})^T$ — решение системы $Ax = B_i$, то $X = (X_1, \ldots, X_m)$ — решение системы $AX = B$.

Асимптотическая плотность в $\mathbb{Z}^m$

Для $v = (v_1, \ldots, v_m) \in \mathbb{Z}^m$ положим $\|v\|_\infty = \max\{|v_i|\}$.
Обозначим $B_r = \{v \in \mathbb{Z}^m \mid \|v\|_\infty \leq r\}$.

Определение

Асимптотической плотностью множества $M \subseteq \mathbb{Z}^m$ называется предел

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

если он существует. В противном случае будем использовать пределы

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

Системы, разрешимые в $\mathbb{Q}^m$

Рассмотрим систему уравнений

$$Ax = b, \quad \text{где} \quad A \in \mathbb{Z}^{nk},\ b \in \mathbb{Z}^n \tag{1}$$

Теорема (Кронекера-Капелли)

Система (1) разрешима в $\mathbb{Q}$ тогда и только тогда, когда $rank(A) = rank(A|b)$.

Системы, разрешимые в $\mathbb{Q}^m$

Yonatan R. Katznelson, *Integral Matrices of Fixed Rank*, Proceedings of the American Mathematical Society 120.3 (1994), pp. 667–675

Обозначим

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

Теорема (Y. R. Katznelson)

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 $n = k$.

Системы, разрешимые в $\mathbb{Q}^m$

Обозначим

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

Теорема (Y. R. Katznelson)

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 $n = k$.

Следствие

- $\rho(V_{n,k,s}(\mathbb{Z})) = 0$, при $s = 1, \ldots, n-1$
- $\rho(V_{n,k,n}(\mathbb{Z})) = 1$

Системы, разрешимые в $\mathbb{Q}^m$

Теорема

(1) $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 1$ при $n \leq k$,

(2) $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 0$ при $n > k$.

Системы, разрешимые в $\mathbb{Q}^m$

Теорема

(1) $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 1$ при $n \leq k$,

(2) $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 0$ при $n > k$.

Рассмотрим множество

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

систем вида $AX = B$ при $n \leq k$. Справедливо влючение

$$S_1 \subset SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n).$$

Так как $\rho(S_1) = 1$ при $n \leq k$, то $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 1$.

Системы, разрешимые в $\mathbb{Q}^m$

Теорема

(1) $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 1$ при $n \leq k$,

(2) $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 0$ при $n > k$.

Рассмотрим множество

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

систем вида $AX = B$ при $n > k$. Справедливо влючение

$$SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n) \subset S_2.$$

Так как $\rho(S_2) = 0$ при $n > k$, то $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 0$.

Системы, разрешимые в $\mathbb{Q}^m$

Теорема

(1) $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 1$ при $n \leq k$,

(2) $\rho(SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 0$ при $n > k$.

Так как $SAT(\mathbb{Z}^m, k, n) \subset SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$, то получаем

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

Следствие

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

Системы, разрешимые в $\mathbb{Z}^m$

Рассмотрим систему уравнений

$$Ax = b, \quad \text{где} \quad A \in \mathbb{Z}^{nk},\ b \in \mathbb{Z}^n,\ n \leq k \tag{2}$$

Наибольшим делителем матрицы A будем называть наибольший общий делитель ее миноров порядка n.

Теорема (Smith)

Пусть $Ax = b$ система вида (2) и $rank(A) = n$. Система разрешима в $\mathbb{Z}$ тогда и только тогда, когда наибольший делитель матрицы системы совпадает с наибольшим делителем ее расширенной матрицы.

Системы, разрешимые в $\mathbb{Z}^m$

Матрицу $A \in \mathbb{Z}^{nk}(n \leq k)$ 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.

Системы, разрешимые в $\mathbb{Z}^m$

G. Maze, J. Rosenthal, U. Wagner *Natural density of rectangular unimodular integer matrices*, Linear Algebra and Its Applications 434.5 (2011), pp. 1319–1324

Обозначим

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

Теорема (G. Maze, J. Rosenthal, U. Wagner)

(1) $\rho(U_{n,k}) = \left(\prod_{j=k-n+1}^{k} \zeta(j) \right)^{-1}$ при $k > n \geq 1$,

(2) $\rho(U_{n,n}) = 0$ при $n \geq 1$.

Системы, разрешимые в $\mathbb{Z}^m$

R. Gilman, A. Myasnikov, V. Roman'kov, *Random equations in nilpotent groups*, Journal of Algebra 352 (1 2012), pp. 192–214

Теорема (R. Gilman, A. Myasnikov, V. Roman'kov)

(1) $\rho(SAT(\mathbb{Z}^m, k)) = \dfrac{\zeta(k+m)}{\zeta(k)}$ при $k \geq 2$,

(2) $\rho(SAT(\mathbb{Z}^m, 1)) = 0$.

Системы, разрешимые в $\mathbb{Z}^m$

Теорема

Справедливы следующие оценки

(1) $\rho(U_{n,k}) \leq \underline{\rho}(SAT(\mathbb{Z}^m, k, n))$ при $k > n > 1$,

Системы, разрешимые в $\mathbb{Z}^m$

Теорема

Справедливы следующие оценки

(1) $\rho(U_{n,k}) \leq \underline{\rho}(SAT(\mathbb{Z}^m, k, n))$ при $k > n > 1$,

(2) $\overline{\rho}(SAT(\mathbb{Z}^m, k, n)) \leq \rho(SAT(\mathbb{Z}^m, k))^n$ при $k \geq n > 1$,

Системы, разрешимые в $\mathbb{Z}^m$

Теорема

Справедливы следующие оценки

(1) $\rho(U_{n,k}) \leq \underline{\rho}(SAT(\mathbb{Z}^m, k, n))$ при $k > n > 1$,

(2) $\overline{\rho}(SAT(\mathbb{Z}^m, k, n)) \leq \rho(SAT(\mathbb{Z}^m, k))^n$ при $k \geq n > 1$,

(3) $\rho(SAT(\mathbb{Z}^m, k, n)) = 0$ при $n > k \geq 1$;

Спасибо за внимание