Федеральное государственное учреждение «Федеральный научный центр
Научно-исследовательский институт системных исследований Российской академии наук»
(ФГУ ФНЦ НИИСИ РАН)

ТРУДЫ НИИСИ РАН

ТОМ 7 N 3

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ СЛОЖНЫХ СИСТЕМ:

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ АСПЕКТЫ

МОСКВА
2017

Редакционный совет ФГУ ФНЦ НИИСИ РАН:
В.Б. Бетелин (председатель),
Е.П. Велихов, В.А. Галатенко, В.Б. Демидович (отв. секретарь), Б.В. Крыжановский,
А.Г. Кушниренко, А.Г. Мадера, М.В. Михайлюк, В.Я. Панченко, В.П. Платонов,
В.Н. Решетников

Главный редактор журнала:
В.Б. Бетелин

Научный редактор номера:
В.П. Платонов

Тематика номера:
Теоретические основы, алгоритмы и вычисления в алгебре, алгебраической геометрии и теории чисел

Журнал публикует оригинальные статьи по следующим областям исследований: математическое и компьютерное моделирование, обработка изображений, визуализация, системный анализ, методы обработки сигналов, информационная безопасность, информационные технологии, высокопроизводительные вычисления, оптико-нейронные технологии, микро- и наноэлектроника, математические исследования, вопросы численного анализа, история науки и техники

The topic of the issue:

Theoretical foundations, algorithms and computations in algebra, algebraic geometry and number theory

The Journal publishes novel articles on the following research arias: mathematical and computer modeling, image processing, visualization, system analysis, signal processing, information security, information technologies, high-performance computing, optical-neural technologies, micro- and nanoelectronics, mathematical researchs, problems of numerical analysis, history of science and of technique

Заведующий редакцией: Ю.Н. Штейников

Издатель: ФГУ ФНЦ НИИСИ РАН,
117218, Москва, Нахимовский проспект 36, к. 1

© Федеральное государственное учреждение «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук», 2017 г.

СОДЕРЖАНИЕ

I. Алгебра, алгебраическая теория чисел и высокопроизводительные вычисления

В. П. Платонов. Новые алгебраические кривые рода 2 над полем рациональных чисел, якобиево многообразие которых содержит рациональную точку порядка 19 ……..5
М. М. Петрунин. Квазипериодические, но не периодические функциональные непрерывные дроби малых квазипериодов……...…….……...14

II. Аналитическая теория чисел, алгебраическая геометрия и приложения

Г. В. Федоров. Прямая аддитивная задача о распределении целочисленных случайных величин ……..……..21
В. С. Жгун. Свойства фактор-отображения моментов для симплектических многообразий с инвариантными лагранжевыми подмногообразиями ……..…… 39
Ю. Н. Штейников. Об одном неравенстве для положительно определенных функций и множество представителей вычетов по двум модулям ...…… 49
В.С. Жгун. О цепочках вложенных подпространств и многообразиях полных флагов ...… 58
Ю. Н. Штейников. Неполные суммы характеров на сдвинутой геометрической прогрессии…….……62

III. Быстрые алгоритмы в алгебре

Ю.В. Кузнецов, М.М. Петрунин. Об одном быстром алгоритме проверки вырожденности теплицевых матриц …….…….…… 68

Предисловие

Данный номер журнала «Труды НИИСИ РАН» содержит работы сотрудников Отдела теоретической и прикладной алгебры и теории чисел, объединённые в нескольких тематических рубриках. Эти работы охватывают различные направления исследований, ведущихся в Отделе, и демонстрируют естественное соединение глубокой теории, эффективных алгоритмов и супервычислений. Подобный симбиоз будет играть всё большую роль в математике 21-го века.

Научный редактор номера,
академик РАН В.П. ПЛАТОНОВ

Новые алгебраические кривые рода 2 над полем рациональных чисел, якобиево многообразие которых содержит рациональную точку порядка 19

В. П. Платонов[1]

[1] *ФГУ ФНЦ НИИСИ РАН, Москва, Россия, E-mail: platonov@niisi.ras.ru*

Аннотация

В статье строятся новые алгебраические кривые рода 2 над полем рациональных чисел, якобиево многообразие которых содержит рациональную точку порядка 19.

Ключевые слова: фундаментальные единицы, гиперэллиптические поля, якобиевы многообразия, гиперэллиптические кривые, проблема кручения в якобианах, быстрые алгоритмы

Первый пример алгебраической кривой рода 2 над полем рациональных чисел, якобиево многообразие (якобиан) которой содержит рациональную точку порядка 19, был построен Б. Мазуром и Дж. Тейтом в [1]. При этом построенное ими якобиево многообразие не было абсолютно простым и над полем комплексных чисел было изогенно прямому произведению двух эллиптических кривых.

В 2012 году нами были построены кривые рода 2 над полем рациональных чисел, якобиево многообразие которых содержало рациональную точку порядка 19 и было абсолютно простым (см. [2]). Это было сделано с помощью развитого мною принципиально нового подхода к проблеме кручения в якобианах гиперэллиптических кривых над полем рациональных чисел (детали см. в [2]).

В настоящей статье мы находим 11 новых кривых рода 2 над полем $\mathbb{Q}$ рациональных чисел, якобиевы многообразия которых абсолютно просты и содержат рациональные точки порядка 19. Метод построения этих кривых детально изложен в [2]. В основе его лежит принципиально новый подход к вычислению так называемых фундаментальных единиц в гиперэллиптических полях.

Нам понадобится ряд базовых понятий и определений из [2].

Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$ свободный от квадратов многочлен. Обозначим

$$D_f = \mathbb{Q}[x](\sqrt{f}) = \{p + q\sqrt{f} | p, q \in \mathbb{Q}[x]\}$$

Элемент $u \in D_f$ называется единицей, если u обратим в D_f. Если $u \in \mathbb{Q}^*$, то u называется тривиальной единицей в D_f. Проблема существования нетривиальных единиц является трудной и имеет глубокие связи с кручением в якобиевых многообразиях кривых, задаваемых уравнением $y^2 = f(x)$, и непрерывными дробя-

ми в функциональных полях. Для нетривиальной единицы $u = p + q\sqrt{f}$ определим $\deg u = \deg p$. Легко видеть, что $u = p + q\sqrt{f}$ обратим в D_f тогда и только тогда, когда $N(u) = p^2 - q^2 f \in \mathbb{Q}^*$. Отсюда следует, что для существования нетривиальной единицы необходимы следующие условия: 1) $n = 2s$, 2) $a_n = \gamma^2, \gamma \in \mathbb{Q}^*$. Предположим, что D_f обладает нетривиальными единицами. Тогда мультипликативная группа $D_f^* = \mathbb{Q}^* \times \langle u \rangle$, где $\langle u \rangle$ — бесконечная циклическая группа. Элемент u называется фундаментальной единицей кольца D_f или гиперэллиптического поля $\mathbb{Q}(x)(\sqrt{f})$.

Пусть C_f — гладкая проективная модель аффинной кривой, задаваемой уравнением $y^2 = f(x)$. Через J_f обозначим якобиан (якобиево многообразие) гиперэллиптической кривой C_f. Для поля $L = \mathbb{Q}(x)(\sqrt{f})$ обозначим через $\Delta^\circ(L)$ группу классов дивизоров степени 0. Существует естественное вложение $\Delta^\circ(L)$ в группу $\mathbb{Q}$-точек $J_f(\mathbb{Q})$, которое в нашей ситуации является изоморфизмом. Поле L имеет два бесконечных нормирования $w_1(\infty)$, $w_2(\infty)$. Кольцо D_f имеет нетривиальную единицу тогда и только тогда, когда класс дивизора $w_1(\infty) - w_2(\infty)$ в $\Delta^\circ(L)$ имеет конечный порядок. При этом степень фундаментальной единицы в D_f равна порядку класса дивизора $w_1(\infty) - w_2(\infty)$ в $\Delta^\circ(L)$.

1. Фундаментальные единицы и кручение

Мы будем далее концентрироваться на кривых рода 2. Пусть $f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[x]$. Рассмотрим многочлены:

$$
\begin{aligned}
f_1 &= 4\,x^6 + 4\,x^5 + 5\,x^4 - 18\,x^3 - 9\,x^2 + 22\,x - 7,\\
f_2 &= 16\,x^6 + 40\,x^5 + 49\,x^4 + 46\,x^3 + 37\,x^2 + 20\,x + 4,\\
f_3 &= 81\,x^6 + 54\,x^5 + 117\,x^4 - 72\,x^3 - 72\,x^2 - 96\,x - 12,\\
f_4 &= 64\,x^6 + 32\,x^5 - 108\,x^4 + 68\,x^3 + 109\,x^2 - 66\,x + 9,\\
f_5 &= 9\,x^6 + 30\,x^5 + 49\,x^4 - 20\,x^3 - 36\,x^2 + 16\,x + 4,\\
f_6 &= x^6 + 44\,x^5 + 506\,x^4 + 368\,x^3 - 703\,x^2 + 452\,x - 92,\\
f_7 &= 9\,x^6 + 12\,x^5 + 34\,x^4 + 92\,x^3 + 73\,x^2 + 24\,x + 48,\\
f_8 &= 36\,x^6 + 108\,x^5 + 141\,x^4 + 126\,x^3 + 79\,x^2 - 66\,x + 9,\\
f_9 &= 36\,x^6 + 60\,x^5 - 107\,x^4 - 146\,x^3 + 91\,x^2 - 30\,x + 9,\\
f_{10} &= 36\,x^6 + 84\,x^5 + 181\,x^4 + 202\,x^3 + 225\,x^2 + 112\,x + 64,\\
f_{11} &= 36\,x^6 + 12\,x^5 - 35\,x^4 + 162\,x^3 + 37\,x^2 - 12\,x + 124.
\end{aligned}
$$

Теорема 1. *Кольцо $D_i = \mathbb{Q}[x](\sqrt{f_i})$ обладает фундаментальной единицей степени 19, для всех $i = 1, \ldots, 11$.*

Доказательство. Для вычисления фундаментальных единиц используется наш новый метод, изложенный в [2].

Компьютерные вычисления дают следующие явные выражения для фундаментальных единиц u_i колец D_i:

$$u_1 = p_1 + q_1\sqrt{f_1} \in D_1,$$

где многочлен p_1 определяется следующим образом:

$$
\begin{aligned}
p_1 = {} & \frac{128}{85}\,x^{19} + \frac{1344}{85}\,x^{18} + \frac{1568}{17}\,x^{17}\\
& + \frac{30416}{85}\,x^{16} + \frac{85656}{85}\,x^{15} + \frac{178252}{85}\,x^{14}\\
& + \frac{53974}{17}\,x^{13} + \frac{53603}{17}\,x^{12} + \frac{93992}{85}\,x^{11}\\
& - \frac{200601}{85}\,x^{10} - \frac{407774}{85}\,x^{9} - \frac{342306}{85}\,x^{8} - \frac{12992}{17}\,x^{7}\\
& + \frac{162583}{85}\,x^{6} + \frac{34078}{17}\,x^{5} + \frac{52182}{85}\,x^{4}\\
& - \frac{4620}{17}\,x^{3} - \frac{19421}{85}\,x^{2} - 16\,x + \frac{999}{85},
\end{aligned}
$$

а многочлен q_1 следующим:

$$q_1 = \frac{64}{85}\,x^{16} + \frac{128}{17}\,x^{15} + \frac{3568}{85}\,x^{14} + \frac{13264}{85}\,x^{13} + \frac{36012}{85}\,x^{12} + \frac{73152}{85}\,x^{11} + \frac{111337}{85}\,x^{10} + \frac{121297}{85}\,x^{9} + \frac{80471}{85}\,x^{8} + \frac{2518}{85}\,x^{7} - \frac{62563}{85}\,x^{6} - \frac{74297}{85}\,x^{5} - \frac{42219}{85}\,x^{4} - \frac{7834}{85}\,x^{3} + \frac{4231}{85}\,x^{2} + \frac{2417}{85}\,x + 1.$$

Для u_1 выполнено норменное соотношение:

$$N(u_1) = p_1^2 - q_1^2 f_1 = \frac{1048576}{7225},$$

и следовательно, ввиду простоты степени p_1, u_1 — фундаментальная единица степени 19 кольца D_1.

$$u_2 = p_2 + q_2\sqrt{f_2} \in D_2,$$

где многочлен p_2 определяется следующим образом:

$$p_2 = \frac{524288}{1023}\,x^{19} + \frac{262144}{93}\,x^{18} + \frac{2850816}{341}\,x^{17} + \frac{557056}{31}\,x^{16} + \frac{31723520}{1023}\,x^{15} + \frac{45918208}{1023}\,x^{14} + \frac{57151744}{1023}\,x^{13} + \frac{62217728}{1023}\,x^{12} + \frac{19937400}{341}\,x^{11} + \frac{51014860}{1023}\,x^{10} + \frac{77378585}{2046}\,x^{9} + \frac{52134959}{2046}\,x^{8} + \frac{31070593}{2046}\,x^{7} + \frac{5418129}{682}\,x^{6} + \frac{7378859}{2046}\,x^{5} + \frac{2850577}{2046}\,x^{4} + \frac{909907}{2046}\,x^{3} + \frac{228529}{2046}\,x^{2} + 20\,x + \frac{2050}{1023},$$

а многочлен q_2 следующим:

$$q_2 = \frac{131072}{1023}\,x^{16} + \frac{557056}{1023}\,x^{15} + \frac{1343488}{1023}\,x^{14} + \frac{73728}{31}\,x^{13} + \frac{324608}{93}\,x^{12} + \frac{141568}{33}\,x^{11} + \frac{4620928}{1023}\,x^{10} + \frac{1410144}{341}\,x^{9} + \frac{3377554}{1023}\,x^{8} + \frac{1569987}{682}\,x^{7} + \frac{1430776}{1023}\,x^{6} + \frac{1499831}{2046}\,x^{5} + \frac{334049}{1023}\,x^{4} + \frac{246823}{2046}\,x^{3} + \frac{3298}{93}\,x^{2} + \frac{15385}{2046}\,x + 1.$$

Для u_2 выполнено норменное соотношение:

$$N(u_2) = p_2^2 - q_2^2 f_2 = \frac{16384}{1046529},$$

и следовательно, ввиду простоты степени p_2, u_2 — фундаментальная единица степени 19 кольца D_2.

$$u_3 = p_3 + q_3\sqrt{f_3} \in D_3,$$

где многочлен p_3 определяется следующим образом:

$$p_3 = -\frac{19683}{448}\,x^{19} - \frac{6561}{448}\,x^{18} - \frac{19683}{112}\,x^{17} + \frac{9477}{56}\,x^{16} - \frac{20655}{112}\,x^{15} + \frac{74115}{112}\,x^{14} - \frac{10935}{28}\,x^{13} + \frac{37017}{56}\,x^{12} - \frac{27135}{28}\,x^{11} + \frac{13851}{28}\,x^{10} - \frac{21195}{28}\,x^{9} + \frac{18549}{28}\,x^{8} - \frac{8073}{28}\,x^{7} + \frac{1413}{4}\,x^{6} - \frac{1422}{7}\,x^{5} + \frac{423}{7}\,x^{4} - 57\,x^{3} + 21\,x^{2} - \frac{2}{7},$$

а многочлен q_3 следующим:

$$q_3 = -\frac{2187}{448}\,x^{16} - \frac{3645}{224}\,x^{14} + \frac{2349}{112}\,x^{13} - \frac{1053}{56}\,x^{12} + \frac{1539}{28}\,x^{11} - \frac{297}{7}\,x^{10} + \frac{324}{7}\,x^{9} - \frac{1863}{28}\,x^{8} + \frac{270}{7}\,x^{7} - \frac{999}{28}\,x^{6} + \frac{459}{14}\,x^{5} - \frac{375}{28}\,x^{4} + \frac{60}{7}\,x^{3} - \frac{75}{14}\,x^{2} + x.$$

Для u_3 выполнено норменное соотношение:

$$N(u_3) = p_3^2 - q_3^2 f_3 = \frac{4}{49},$$

и следовательно, ввиду простоты степени p_3, u_3 — фундаментальная единица степени 19 кольца D_3.

$$u_4 = p_4 + q_4\sqrt{f_4} \in D_4,$$

где многочлен p_4 определяется следующим образом:

$$\begin{aligned} p_4 = &-\frac{268435456}{14348799}\,x^{19} + \frac{67108864}{4782933}\,x^{18} \\ &+ \frac{520093696}{4782933}\,x^{17} - \frac{2696937472}{14348799}\,x^{16} \\ &- \frac{312475648}{1594311}\,x^{15} + \frac{3451387904}{4782933}\,x^{14} \\ &- \frac{3414556672}{14348799}\,x^{13} - \frac{5533892608}{4782933}\,x^{12} \\ &+ \frac{2218864640}{1594311}\,x^{11} + \frac{5464775680}{14348799}\,x^{10} \\ &- \frac{9057205504}{4782933}\,x^{9} + \frac{5355229376}{4782933}\,x^{8} \\ &+ \frac{9809579008}{14348799}\,x^{7} - \frac{2005958608}{1594311}\,x^{6} \\ &+ \frac{2443605136}{4782933}\,x^{5} + \frac{3116986396}{14348799}\,x^{4} \\ &- \frac{91780360}{281349}\,x^{3} + \frac{4762183}{31261}\,x^{2} - 34\,x \\ &+ \frac{1594335}{531437}, \end{aligned}$$

а многочлен q_4 следующим:

$$\begin{aligned} q_4 = &-\frac{33554432}{14348799}\,x^{16} + \frac{33554432}{14348799}\,x^{15} \\ &+ \frac{52428800}{4782933}\,x^{14} - \frac{321912832}{14348799}\,x^{13} \\ &- \frac{149159936}{14348799}\,x^{12} + \frac{102760448}{1594311}\,x^{11} \\ &- \frac{197705728}{4782933}\,x^{10} - \frac{18276352}{281349}\,x^{9} \\ &+ \frac{175814144}{1594311}\,x^{8} - \frac{307012096}{14348799}\,x^{7} \\ &- \frac{1166032160}{14348799}\,x^{6} + \frac{371474800}{4782933}\,x^{5} \\ &- \frac{131662592}{14348799}\,x^{4} - \frac{25014776}{844047}\,x^{3} \\ &+ \frac{37199270}{1594311}\,x^{2} - \frac{239673}{31261}\,x + 1. \end{aligned}$$

Для u_4 выполнено норменное соотношение:

$$N(u_4) = p_4^2 - q_4^2 f_4 = \frac{76527504}{282425284969},$$

и следовательно, ввиду простоты степени p_4, u_4 — фундаментальная единица степени 19 кольца D_4.

$$u_5 = p_5 + q_5\sqrt{f_5} \in D_5,$$

где многочлен p_5 определяется следующим образом:

$$\begin{aligned} p_5 = &-\frac{59049}{4120456}\,x^{19} - \frac{1043199}{4120456}\,x^{18} \\ &- \frac{9152595}{4120456}\,x^{17} - \frac{51523533}{4120456}\,x^{16} \\ &- \frac{102349413}{2060228}\,x^{15} - \frac{298632663}{2060228}\,x^{14} \\ &- \frac{645825231}{2060228}\,x^{13} - \frac{1012938777}{2060228}\,x^{12} \\ &- \frac{2124910989}{4120456}\,x^{11} - \frac{1056565995}{4120456}\,x^{10} \\ &+ \frac{647672633}{4120456}\,x^{9} + \frac{1505741895}{4120456}\,x^{8} \\ &+ \frac{96858468}{515057}\,x^{7} - \frac{54245229}{515057}\,x^{6} \\ &- \frac{84037329}{515057}\,x^{5} - \frac{13777785}{515057}\,x^{4} \\ &+ \frac{24286602}{515057}\,x^{3} + \frac{8976114}{515057}\,x^{2} - 6\,x \\ &- \frac{1095650}{515057}, \end{aligned}$$

а многочлен q_5 следующим:

$$\begin{aligned} q_5 = &-\frac{19683}{4120456}\,x^{16} - \frac{39366}{515057}\,x^{15} \\ &- \frac{2499741}{4120456}\,x^{14} - \frac{6326991}{2060228}\,x^{13} \\ &- \frac{5600907}{515057}\,x^{12} - \frac{14376609}{515057}\,x^{11} \\ &- \frac{107278587}{2060228}\,x^{10} - \frac{70128099}{1030114}\,x^{9} \\ &- \frac{225962163}{4120456}\,x^{8} - \frac{6048955}{515057}\,x^{7} \\ &+ \frac{114135607}{4120456}\,x^{6} + \frac{61069209}{2060228}\,x^{5} \\ &+ \frac{8588371}{2060228}\,x^{4} - \frac{5685008}{515057}\,x^{3} \\ &- \frac{5913465}{1030114}\,x^{2} + \frac{613361}{515057}\,x + 1. \end{aligned}$$

Для u_5 выполнено норменное соотношение:

$$N(u_5) = p_5^2 - q_5^2 f_5 = \frac{139314069504}{265283713249},$$

и следовательно, ввиду простоты степени p_5, u_5 — фундаментальная единица степени 19 кольца D_5.

$$u_6 = p_6 + q_6\sqrt{f_6} \in D_6,$$

где многочлен p_6 определяется следующим образом:

$$\begin{aligned}
p_6 = {} & \frac{1}{75959752240}\,x^{19} + \frac{11}{3797987612}\,x^{18} \\
& + \frac{21903}{75959752240}\,x^{17} + \frac{650921}{37979876120}\,x^{16} \\
& + \frac{51294169}{75959752240}\,x^{15} + \frac{35148015}{1898993806}\,x^{14} \\
& + \frac{5468727019}{15191950448}\,x^{13} + \frac{2220810367}{446822072}\,x^{12} \\
& + \frac{3637447086099}{75959752240}\,x^{11} \\
& + \frac{346247949267}{1117055180}\,x^{10} \\
& + \frac{95823836472357}{75959752240}\,x^{9} \\
& + \frac{110431833905199}{37979876120}\,x^{8} \\
& + \frac{50350767338783}{15191950448}\,x^{7} \\
& + \frac{63924709591}{55852759}\,x^{6} - \frac{38815029876699}{75959752240}\,x^{5} \\
& + \frac{368253097469}{2234110360}\,x^{4} \\
& + \frac{4128893841631}{9494969030}\,x^{3} - \frac{137939984403}{4747484515}\,x^{2} \\
& - 37\,x + \frac{52711957298}{4747484515},
\end{aligned}$$

а многочлен q_6 следующим:

$$\begin{aligned}
q_6 = {} & \frac{1}{75959752240}\,x^{16} + \frac{99}{37979876120}\,x^{15} \\
& + \frac{1096}{4747484515}\,x^{14} + \frac{91393}{7595975224}\,x^{13} \\
& + \frac{1823849}{4468220720}\,x^{12} + \frac{178653001}{18989938060}\,x^{11} \\
& + \frac{707635791}{4747484515}\,x^{10} + \frac{6092377913}{3797987612}\,x^{9} \\
& + \frac{858159042099}{75959752240}\,x^{8} \\
& + \frac{1843196705831}{37979876120}\,x^{7} \\
& + \frac{216132259605}{1898993806}\,x^{6} \\
& + \frac{5040484280081}{37979876120}\,x^{5} \\
& + \frac{4532675061091}{75959752240}\,x^{4} - \frac{18738125707}{9494969030}\,x^{3} \\
& + \frac{4361867101}{1898993806}\,x^{2} + \frac{32861673048}{4747484515}\,x \\
& + 1.
\end{aligned}$$

Для u_6 выполнено норменное соотношение:

$$N(u_6) = p_6^2 - q_6^2 f_6 = \frac{4852102490441335701504}{22538609220164785225},$$

и следовательно, ввиду простоты степени p_6, u_6 — фундаментальная единица степени 19 кольца D_6.

$$u_7 = p_7 + q_7\sqrt{f_7} \in D_7,$$

где многочлен p_7 определяется следующим образом:

$$\begin{aligned}
p_7 = {} & \frac{27}{5632}\,x^{19} + \frac{9}{1408}\,x^{18} + \frac{195}{2816}\,x^{17} \\
& + \frac{125}{704}\,x^{16} + \frac{8659}{16896}\,x^{15} + \frac{19321}{12672}\,x^{14} \\
& + \frac{117037}{38016}\,x^{13} + \frac{191275}{28512}\,x^{12} \\
& + \frac{17783383}{1368576}\,x^{11} + \frac{6978553}{342144}\,x^{10} \\
& + \frac{837403}{25344}\,x^{9} + \frac{2611025}{57024}\,x^{8} \\
& + \frac{8184125}{152064}\,x^{7} + \frac{2443937}{38016}\,x^{6} \\
& + \frac{393439}{6336}\,x^{5} + \frac{79861}{1584}\,x^{4} + \frac{517}{12}\,x^{3} \\
& + \frac{73}{3}\,x^{2} + 11\,x + \frac{76}{11},
\end{aligned}$$

а многочлен q_7 следующим:

$$q_7 = \frac{9}{5632}\,x^{16} + \frac{3}{2816}\,x^{15} + \frac{111}{5632}\,x^{14} + \frac{5}{132}\,x^{13} + \frac{2749}{25344}\,x^{12} + \frac{3833}{12672}\,x^{11} + \frac{114227}{228096}\,x^{10} + \frac{180523}{171072}\,x^{9} + \frac{812725}{456192}\,x^{8} + \frac{527363}{228096}\,x^{7} + \frac{531337}{152064}\,x^{6} + \frac{24685}{6336}\,x^{5} + \frac{7627}{2112}\,x^{4} + \frac{139}{36}\,x^{3} + \frac{323}{132}\,x^{2} + \frac{4}{3}\,x + 1.$$

Для u_7 выполнено норменное соотношение:

$$N(u_7) = p_7^2 - q_7^2 f_7 = -\frac{32}{121},$$

и следовательно, ввиду простоты степени p_7, u_7 — фундаментальная единица степени 19 кольца D_7.

$$u_8 = p_8 + q_8\sqrt{f_8}, \in D_8$$

где многочлен p_8 определяется следующим образом:

$$p_8 = \frac{93312}{262171}\,x^{19} + \frac{1259712}{262171}\,x^{18} + \frac{645408}{20167}\,x^{17} + \frac{36799920}{262171}\,x^{16} + \frac{9195768}{20167}\,x^{15} + \frac{305961300}{262171}\,x^{14} + \frac{91354338}{37453}\,x^{13} + \frac{1115362953}{262171}\,x^{12} + \frac{1644388524}{262171}\,x^{11} + \frac{2062505457}{262171}\,x^{10} + \frac{2203274838}{262171}\,x^{9} + \frac{1996231122}{262171}\,x^{8} + \frac{216848924}{37453}\,x^{7} + \frac{949786785}{262171}\,x^{6} + \frac{1415099110}{786513}\,x^{5} + \frac{172758842}{262171}\,x^{4} + \frac{341826272}{2359539}\,x^{3} - \frac{260875}{262171}\,x^{2} - 12\,x - \frac{786351}{262171},$$

а многочлен q_8 следующим:

$$q_8 = \frac{15552}{262171}\,x^{16} + \frac{186624}{262171}\,x^{15} + \frac{1105488}{262171}\,x^{14} + \frac{4311792}{262171}\,x^{13} + \frac{12441924}{262171}\,x^{12} + \frac{28205496}{262171}\,x^{11} + \frac{51965379}{262171}\,x^{10} + \frac{11335761}{37453}\,x^{9} + \frac{14499159}{37453}\,x^{8} + \frac{109147266}{262171}\,x^{7} + \frac{98457447}{262171}\,x^{6} + \frac{10549431}{37453}\,x^{5} + \frac{135814345}{786513}\,x^{4} + \frac{46954}{559}\,x^{3} + \frac{10373995}{337077}\,x^{2} + \frac{6029285}{786513}\,x + 1.$$

Для u_8 выполнено норменное соотношение:

$$N(u_8) = p_8^2 - q_8^2 f_8 = -\frac{254803968}{68733633241},$$

и следовательно, ввиду простоты степени p_8, u_8 — фундаментальная единица степени 19 кольца D_8.

$$u_9 = p_9 + q_9\sqrt{f_9} \in D_9,$$

где многочлен p_9 определяется следующим образом:

$$p_9 = -\frac{839808}{255583}\,x^{19} - \frac{5178816}{255583}\,x^{18} - \frac{1423008}{255583}\,x^{17} + \frac{48285072}{255583}\,x^{16} + \frac{65103912}{255583}\,x^{15} - \frac{188201988}{255583}\,x^{14} - \frac{349876494}{255583}\,x^{13} + \frac{416108931}{255583}\,x^{12} + \frac{889921396}{255583}\,x^{11} - \frac{634702249}{255583}\,x^{10} - \frac{1231104042}{255583}\,x^{9} + \frac{774062406}{255583}\,x^{8} + \frac{848619348}{255583}\,x^{7} - \frac{682230129}{255583}\,x^{6} - \frac{106962798}{255583}\,x^{5} + \frac{260816526}{255583}\,x^{4} - \frac{141408408}{255583}\,x^{3} + \frac{46455347}{255583}\,x^{2} - 32\,x + \frac{806115}{255583},$$

а многочлен q_9 следующим:

$$q_9 = -\frac{139968}{255583}\,x^{16} - \frac{746496}{255583}\,x^{15} + \frac{128304}{255583}\,x^{14} + \frac{6502032}{255583}\,x^{13} + \frac{5294268}{255583}\,x^{12} - \frac{23980968}{255583}\,x^{11} - \frac{26211243}{255583}\,x^{10} + \frac{50404985}{255583}\,x^{9} + \frac{52867425}{255583}\,x^{8} - \frac{68424330}{255583}\,x^{7} - \frac{47540067}{255583}\,x^{6} + \frac{59300391}{255583}\,x^{5} + \frac{8593251}{255583}\,x^{4} - \frac{23633130}{255583}\,x^{3} + \frac{9744663}{255583}\,x^{2} - \frac{2440215}{255583}\,x + 1.$$

Для u_9 выполнено норменное соотношение:

$$N(u_9) = p_9^2 - q_9^2 f_9 = \frac{61917364224}{65322669889},$$

и следовательно, ввиду простоты степени p_9, u_9 — фундаментальная единица степени 19 кольца D_9.

$$u_{10} = p_{10} + q_{10}\sqrt{f_{10}} \in D_{10},$$

где многочлен p_{10} определяется следующим образом:

$$p_{10} = \frac{7558272}{531473}\,x^{19} + \frac{61725888}{531473}\,x^{18} + \frac{292883040}{531473}\,x^{17} + \frac{982050480}{531473}\,x^{16} + \frac{2575183752}{531473}\,x^{15} + \frac{5515290324}{531473}\,x^{14} + \frac{9940303314}{531473}\,x^{13} + \frac{15316688601}{531473}\,x^{12} + \frac{20405847321}{531473}\,x^{11} + \frac{23624328909}{531473}\,x^{10} + \frac{23824919183}{531473}\,x^{9} + \frac{20889691506}{531473}\,x^{8} + \frac{15850960002}{531473}\,x^{7} + \frac{10310110134}{531473}\,x^{6} + \frac{5667550776}{531473}\,x^{5} + \frac{2573395677}{531473}\,x^{4} + \frac{931935165}{531473}\,x^{3} + \frac{253482345}{531473}\,x^{2} + 87\,x + \frac{4251272}{531473},$$

а многочлен q_{10} следующим:

$$q_{10} = \frac{1259712}{531473}\,x^{16} + \frac{8817984}{531473}\,x^{15} + \frac{36216720}{531473}\,x^{14} + \frac{104416128}{531473}\,x^{13} + \frac{234262692}{531473}\,x^{12} + \frac{425015748}{531473}\,x^{11} + \frac{641594439}{531473}\,x^{10} + \frac{815175090}{531473}\,x^{9} + \frac{878692077}{531473}\,x^{8} + \frac{802744928}{531473}\,x^{7} + \frac{618837614}{531473}\,x^{6} + \frac{397336524}{531473}\,x^{5} + \frac{208259470}{531473}\,x^{4} + \frac{85952524}{531473}\,x^{3} + \frac{26308491}{531473}\,x^{2} + \frac{5314034}{531473}\,x + 1.$$

Для u_{10} выполнено норменное соотношение:

$$N(u_{10}) = p_{10}^2 - q_{10}^2 f_{10} = -\frac{4353564672}{282463549729},$$

и следовательно, ввиду простоты степени p_{10}, u_{10} — фундаментальная единица степени 19 кольца D_{10}.

$$u_{11} = p_{11} + q_{11}\sqrt{f_{11}} \in D_{11},$$

где многочлен p_{11} определяется следующим образом:

$$p_{11} = \frac{52488}{563035}\,x^{19} + \frac{122472}{563035}\,x^{18} - \frac{99144}{563035}\,x^{17} + \frac{73872}{112607}\,x^{16} + \frac{1649403}{563035}\,x^{15} - \frac{115803}{112607}\,x^{14} + \frac{897003}{1126070}\,x^{13} + \frac{8347056}{563035}\,x^{12} - \frac{21638543}{18017120}\,x^{11} - \frac{64118231}{18017120}\,x^{10} + \frac{33795239}{900856}\,x^{9} + \frac{11132139}{4504280}\,x^{8} - \frac{50650539}{4504280}\,x^{7} + \frac{232464819}{4504280}\,x^{6} + \frac{60270}{10237}\,x^{5} - \frac{6449781}{563035}\,x^{4} + \frac{42031221}{1126070}\,x^{3} + \frac{3515209}{1126070}\,x^{2} - 4\,x + \frac{6269816}{563035},$$

а многочлен q_{11} следующим:

$$
\begin{aligned}
q_{11} = & \frac{8748}{563035}\,x^{16} + \frac{18954}{563035}\,x^{15} \\
& - \frac{15309}{563035}\,x^{14} + \frac{106353}{1126070}\,x^{13} \\
& + \frac{856629}{2252140}\,x^{12} - \frac{629073}{4504280}\,x^{11} \\
& + \frac{90339}{818960}\,x^{10} + \frac{27940939}{18017120}\,x^{9} \\
& - \frac{1621837}{9008560}\,x^{8} - \frac{1125439}{4504280}\,x^{7} \\
& + \frac{6680567}{2252140}\,x^{6} + \frac{155699}{4504280}\,x^{5} \\
& - \frac{1324069}{2252140}\,x^{4} + \frac{308915}{112607}\,x^{3} + \frac{66029}{563035}\,x^{2} \\
& - \frac{350017}{1126070}\,x + 1.
\end{aligned}
$$

Для u_{11} выполнено норменное соотношение:

$$N(u_{11}) = p_{11}^2 - q_{11}^2 f_{11} = \frac{1549681956}{317008411225},$$

и следовательно, ввиду простоты степени p_{11}, u_{11} — фундаментальная единица степени 19 кольца D_{11}. □

Обозначим через C_i гиперэллиптическую кривую, определяемую уравнением $y^2 = f_i$, а через J_i — якобиан кривой C_i.

Из теоремы 1 непосредственно следует теорема 2.

Теорема 2. *Якобианы J_i имеют $\mathbb{Q}$-точки кручения порядка* 19*, для всех* $i = 1, \ldots, 11$.

2. Простота якобиевых многобразий

В настоящей работе мы будем использовать метод исследования якобиана J на простоту, основанный на изучении его кольца эндоморфизмов над алгебраическим замыканием поля $\mathbb{Q}$, которое мы обозначим через $\mathrm{End}(J)$. Через $\mathrm{End}^0(J)$, мы обозначим $\mathbb{Q}$-алгебру $\mathrm{End}(J) \otimes_{\mathbb{Z}} \mathbb{Q}$. С точностью до изогении якобиан J разлагается над $\overline{\mathbb{Q}}$ в прямое произведение $A_1^{k_1} \times A_2^{k_2} \times \ldots \times A_l^{k_l}$ степеней попарно неизогенных простых абелевых многообразий. Напомним, что для простого абелева многообразия A_i алгебра $D_i = \mathrm{End}^0(A_i)$ является алгеброй с делением. Заметим также, что $\mathrm{End}^0(J)$ — полупростая алгебра над $\mathbb{Q}$, изоморфная прямой сумме матричных алгебр над алгебрами с делением:

$$\mathrm{Mat}(k_1, D_1) \times \mathrm{Mat}(k_2, D_2) \times \ldots \times \mathrm{Mat}(k_l, D_l).$$

Тем самым, чтобы проверить, что якобиан J не прост, достаточно вычислить алгебру эндоморфизмов, а затем, чтобы показать, что она не является алгеброй с делением, надо найти делители нуля в этой алгебре. Алгебра эндоморфизмов над комплексными числами может быть вычислена с помощью системы компьютерной алгебры *Magma*.

Теорема 3. *Якобианы J_i кривых C_i, просты над алгебраическим замыканием поля $\mathbb{Q}$ и содержат $\mathbb{Q}$-точку порядка 19 для* $i = 1, \ldots, 11$.

Доказательство. Во всех случаях кроме случая f_2 алгебра эндоморфизмов оказывается тривиальной, что доказывает абсолютную простоту якобианов.

Алгебра эндоморфизмов $\mathrm{End}^0(J_2)$ порождается матрицей B:

$$B = \begin{pmatrix} 1 & 2 & 0 & -1 \\ 3 & 0 & 1 & 0 \\ 0 & -5 & 1 & 3 \\ 5 & 0 & 2 & 0 \end{pmatrix}.$$

Ее характеристический многочлен $P(x) = \det(B - xE)$ равен $(x^2 - x - 1)^2$.

Отсюда легко видеть, что минимальный многочлен матрицы B это $x^2 - x - 1$. Учитывая что он не имеет корней над $\mathbb{Q}$ заключаем, что алгебра $\mathrm{End}^0(J_2)$ не имеет делителей нуля. Следовательно, якобиан J_2 абсолютно прост.

Наличие $\mathbb{Q}$-точек кручения порядка 19 вытекает из теоремы 2. □

New algebraic curves of genus 2 over the rational number field whose Jacobians have a rational point of order 19

V. P. Platonov

Abstract

In the paper new algebraic curves of genus 2 over the rational number field whose Jacobians have a rational point of order 19 are constructed.

Keywords: fundamental units, hyperelliptic fields, Jacobians, hyperelliptic curves, torsion problem in Jacobians, fast alghorithms

Литература

1. *Mazur B.*, *Tate J.* Points of order 13 on elliptic curves // Inventiones mathematicae. — 1973. — т. 22, № 1. — с. 41—49.
2. *Платонов В. П.* Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // УМН. — 2014. — т. 69:1, № 415. — с. 3—38.

Квазипериодические, но не периодические функциональные непрерывные дроби малых квазипериодов

М. М. Петрунин[1]

[1] *ФГУ ФНЦ НИИСИ РАН, Москва, Россия, E-mail: petrunin@niisi.ras.ru*

Аннотация

Квазипериодические и периодические элементы поля $k(x)(\sqrt{f})$, где f — бесквадратный многочлен нечётной степени, а k — произвольное поле характеристики отличной от 2, играют особую роль. Существует глубокая связь между S-единицами гиперэллиптических полей, точками кручения в якобианах гиперэллиптических кривых и элементами гиперэллиптических полей, разлагающихся в квазипериодические непрерывные дроби. Большинство рассматриваемых в литературе квазипериодических элементов является периодическими, и в литературе практически не встречается явный вид квазипериодических, но не периодических элементов. В настоящей работе мы находим необходимые условия на то, что чистоквазипериодический, но не периодический элемент лежит в соответствующем поле, а также используя непосредственную конструкцию непрерывной дроби, строим элементы, разлагающиеся в чистоквазипериодические, но не периодические функциональные непрерывные дроби малых квазипериодов.

Ключевые слова: фундаментальные единицы, S-единицы, гиперэллиптические поля, якобиевы многообразия, гиперэллиптические кривые, проблема кручения в якобианах, быстрые алгоритмы, непрерывные дроби, $\mathbb{Q}$-точки кручения

Для классического случая гиперэллиптического поля, определяемого многочленом чётной степени, уже более 150 лет известна связь между наличием нетривиальных единиц и периодичностью разложения квадратного корня в непрерывную дробь. А именно, пусть k — поле характеристики отличной от 2, и пусть f — свободный от квадратов многочлен чётной степени из $k[x]$, старший коэффициент которого является квадратом. Тогда элемент $\sqrt{f} \in k((1/x))$ разлагается в $k((1/x))$ в непрерывную дробь. Кольцо $k[x](\sqrt{f})$ обладает нетривиальными единицами в том и только том случае, когда $\sqrt{f}$ разлагается в периодическую непрерывную дробь. Проблема существования нетривиальных единиц, в свою очередь, тесно связана с проблемой кручения в якобианах гиперэллиптических кривых (см. [1], [2], [6]).

Пусть теперь f — свободный от квадратов многочлен нечётной степени $2g+1$, рассмотрим поле $L = k(x)(\sqrt{f})$. Бесконечное нормирование поля $k(x)$ имеет одно продолжение на поле L. В этом случае аналогом нетривиальных единиц, в том числе и в части тесной связи с кручением в якобиане соответствующей гиперэллипти-

ческой кривой, являются нетривиальные S-единицы поля L, где S — множество нормирований, состоящее из одного из двух продолжений конечного нормирования поля $k(x)$, определяемого многочленом $h \in k[x]$, и бесконечного нормирования. В [3] показано, что эффективная связь между нетривиальными S-единицами и разложением $\sqrt{f}$ или связанных с $\sqrt{f}$ элементов в непрерывную дробь в поле формальных степенных рядов $k((h))$ возможна только, когда степень многочлена h равна единице.

В работе [8] показано, что наличие S-единиц в поле L возможно только в случае наличия в L квазипериодических элементов, т.е. элементов периодических с точностью до константы. Кроме того, в работах [4; 5; 8—12] исследована квазипериодичностью элементов специального вида $\frac{\sqrt{f}}{dh^s}$, где d — делитель многочлена f, а $s \in \mathbb{Z}$, и её взаимосвязь с наличием квазипериодических элементов в поле L. В частности, показано квазипериодический элемент такого вида обязательно является периодическим. Отметим, что важность вопроса о периодичности квазипериодического элемента подчёркивает, в частности, то, что произвольно выбранный квазипериодический элемент поля $k((h))$ с четной длиной квазипериода почти наверное будет непериодичным.

Несмотря на то, что каждая непрерывная дробь сходится к некоторому элементу из $k((h))$, в литературе практически не встречается явный вид квазипериодических, но не периодических элементов. Так в теореме 1 работы [7] доказана квазипериодичность класса элементов, связанного с представлением Мамфорда для дивизоров. Элементы $\sqrt{f}/h^s$ для $s = g, g+1$, периодичные, как показано в [8], тогда и только тогда, когда они квазипериодичные, относятся к этому классу, однако, для произвольного элемента этого класса свойство периодичности, вообще говоря, не всегда следует из свойства квазипериодичности. В работе [4] построен пример квазипериодического, но не периодического элемента этого класса.

В настоящей работе мы находим необходимые условия на то, что чистоквазипериодический, но не периодический элемент лежит в поле L для соответствующего f, а также используя непосредственную конструкцию непрерывной дроби, строим элементы, разлагающиеся в чистоквазипериодические, но не периодические функциональные непрерывные дроби малых квазипериодов.

Прежде чем приступить к изложению основных результатов статьи, напомним необходимые понятия.

Пусть $\alpha \in k((h))$ представлен в виде формального степенного ряда

$$\alpha = \sum_{j=e}^{\infty} b_j h^j, \qquad \alpha \in k((h)),\ b_j \in k.$$

Обозначим через $[\alpha]$ — сумму членов с неположительными, а через $\{\alpha\}$ — с положительными показателями степени h разложения α в ряд Лорана:

$$[\alpha] = \begin{cases} \sum\limits_{i=e}^{0} b_j h^j & \text{если } e \le 0, \\ 0 & \text{иначе;} \end{cases}$$

$$\{\alpha\} = \alpha - [\alpha] = \sum_{i=0}^{\infty} b_j h^j.$$

Положим $A_0 = [\alpha]$. Если $\alpha - A_0 \neq 0$, то положим

$$\alpha_1 = \frac{1}{\alpha - A_0} \in k((h)), \quad A_1 = [\alpha_1].$$

Далее по индукции определяем элементы A_i, α_i: если $\alpha_{i-1} - A_{i-1} \neq 0$, то

$$\alpha_i = \frac{1}{\alpha_{i-1} - A_{i-1}} \in k((h)), \quad A_i = [\alpha_i].$$

В результате мы получим *непрерывную дробь*

$$A_0 + \cfrac{1}{A_1 + \cfrac{1}{A_2 + \cfrac{1}{A_3 + \cdots}}}. \tag{1}$$

Будем использовать стандартную сокращенную запись $[A_0, A_1, A_2, \ldots]$ для

непрерывной дроби (1). По построению, $\alpha_n = [A_n, A_{n+1}, \ldots]$.

Напомним, что разложение в непрерывную дробь элемента α называется квазипериодическим, если существуют такие $i, j \in \mathbb{Z}$, $i > j \geq 0$ и $c \in k^\times$, что $\alpha_i = c\alpha_j$, где α_k – полное частное с номером k к $\alpha = \alpha_0$. Наименьшее такое $i - j$ называется длиной квазипериода. Мы будем называть элемент квазипериодичным (периодичным), если его разложение квазипериодично (периодично). За более полным изложением основных фактов, связанных с теорией непрерывных дробей для данного случая, мы отсылаем читателя к [3].

Мы будем писать

$$\alpha = [B_0, B_1, \ldots, B_{i-1}, \overline{A_1, A_2, \ldots, A_n}^c],$$

если $c\alpha_i = \alpha_{i+n}$.

Обозначим для $B = b_0 + b_{-1}h^{-1} + \cdots + b_{-n}h^{-n} \in k[h^{-1}]$ значение свободного коэффициента за $fc(B) = b_0$.

Теорема 1. *Квазипериодический, но не периодический, элемент $\alpha = [\overline{A_0, A_1}^c], c \neq 1 \in k^\times, A_i \in k[h^{-1}]$ лежит в $k(x)(\sqrt{f})$ для некоторого многочлена f нечётной степени только, если $fc(A_0)fc(A_1) = \frac{-(1+c)\pm 2\sqrt{c}}{c}$, где $t_i = v_h(A_i)$.*

Доказательство. Рассмотрим непрерывную дробь элемента $\alpha = [\overline{A_0, A_1}^c]$, $c \neq 1 \in k^\times$:

$$\alpha = A_0 + \cfrac{1}{A_1 + \cfrac{1}{c\alpha}} = A_0 + \frac{c\alpha}{c\alpha A_1 + 1} = \frac{c\alpha A_1 A_0 + c\alpha + A_0}{c\alpha A_1 + 1}.$$

Откуда получаем квадратичную зависимость на α:

$$\alpha^2 c A_1 + \alpha(1 - cA_0A_1 - c) - A_0 = 0,$$

где $A_0, A_1 \in k[h^{-1}]$. Пусть $s_i = v_h(A_i)$, для $i = 0,\ 1$. Тогда перепишем зависимость в виде многочленов из $k[h]$.

$$\alpha^2 c a_1 h^{s_0} + \alpha(h^{s_0+s_1}(1-c) - ca_0a_1) - a_0h^{s_1} = 0,$$

где $a_i = A_i h^{s_i} \in k[h] \sim k[x]$. Дискриминант для этого уравнения равен

$$D = (h^{s_0+s_1}(1-c) - ca_0a_1)^2 + 4ca_0a_1h^{s_0+s_1}.$$

Ясно, что если $\deg a_i < s_i$ для некоторого i, то $\deg D$ будет чётным числом. Наша задача выбрать такие A_i, чтобы итоговый D имел нечетную степень. Раскроем дискриминант:

$$\begin{aligned} D &= h^{2(s_0+s_1)}(1-c)^2 - 2c(1-c)a_0a_1h^{s_0+s_1} \\ &+ c^2a_0^2a_1^2 + 4ca_0a_1h^{s_0+s_1} = \\ &= (h^{s_0+s_1})^2(1-c)^2 + 2(c+1)(ca_0a_1)h^{s_0+s_1} \\ &+ (ca_0a_1)^2. \end{aligned}$$

Напомним, что многочлены записаны как степени h. Мы хотим, чтобы старшие коэффициенты сократились. Положим $z = c\,\mathrm{lc}(a_0)\,\mathrm{lc}(a_1)$ и запишем желаемое:

$$(1-c)^2 + 2(1+c)z + z^2 = 0.$$

Это уравнение имеет решения вида

$$\begin{aligned} z &= \frac{1}{2}(-2(1+c) \pm \sqrt{4(1+c)^2 - 4(1-c)^2}) \\ &= -(1+c) \pm 2\sqrt{c}. \end{aligned}$$

Теорема доказана. □

Из доказательства теоремы 1 ясен алгоритм построения квазипериодического не не периодического элемента. Воспользуемся им для построения примера.

Пример 1. *Пусть $c = 4$. Тогда $z = -5 \pm 4$. Пусть $z = -1$. Зафиксируем $lc(a_0) = 1$, тогда $lc(a_1) = -1/4$.*

Пусть $s_0 = 2$, а $s_1 = 1$. Тогда $a_0 = d_0 + d_1x + x^2$, а $a_1 = e_0 - 1/4x$.

И для $d_0 = 1,\ d_1 = 0, e_0 = 1$ дискриминант будет следующего вида:

$$D = 32\,x^5 + 8\,x^4 + 24\,x^3 + 33\,x^2 - 8\,x + 16.$$

А квазипериодический элемент α следующего:

$$\alpha = \frac{-3\,x^3 + (x^2+1)(x-4) - \sqrt{D}}{2(x-4)x^2} = [\overline{x^{-2}+1, x^{-1} - 1/4}^{4}].$$

Для обобщения теоремы 1 нам потребуется напомнить несколько фактов и понятий.

Определим по индукции элементы $P_n, Q_n \in k(x)$. Положим

$$P_{-2} = 0,\ P_{-1} = 1,\ Q_{-2} = 1,\ Q_{-1} = 0$$

и если $n \geq 0$, то

$$P_n = A_n P_{n-1} + P_{n-2},$$
$$Q_n = A_n Q_{n-1} + Q_{n-2}.$$

Дробь P_n/Q_n называется подходящей дробью к α. По индукции нетрудно показать, что выполнено:

$$\begin{aligned} v_h(P_n) =& v_h(A_n) + v_h(P_{n-1}) = \\ & \sum_{j=0}^{n} v_h(A_j), \\ v_h(Q_n) =& v_h(A_n) + v_h(Q_{n-1}) = \\ & \sum_{j=1}^{n} v_h(A_j). \end{aligned} \tag{2}$$

Элементы α, α_m и подходящие дроби связывается следующее соотношение (см. [3]):

$$Q_n P_{n-1} - P_n Q_{n-1} = (-1)^n, \tag{3}$$

$$Q_n \alpha - P_n = \frac{(-1)^n}{Q_n \alpha_{n+1} + Q_{n-1}}, \tag{4}$$

$$\alpha = \frac{P_n \alpha_{n+1} + P_{n-1}}{Q_n \alpha_{n+1} + Q_{n-1}}. \tag{5}$$

Теорема 2. *Квазипериодический, но не периодический, элемент $\alpha = [\overline{A_0, A_i, \ldots, A_{2m}}^{c}], c \neq 1 \in k^{\times}, A_i \in k[h^{-1}]$ лежит в $k(x)(\sqrt{f})$ для некоторого многочлена f нечётной степени только, если $fc(Q_{n-2}) + cfc(P_{n-1}) = \pm 2\sqrt{c}$, где $n = 2m$.*

Доказательство. Имеем $c\alpha = \alpha_{2m}$. Откуда

$$\alpha = \frac{c\alpha P_{n-1} + P_{n-2}}{c\alpha Q_{n-1} + Q_{n-2}}. \tag{6}$$

Откуда

$$cQ_{n-1}\alpha^2 + (Q_{n-2} - cP_{n-1})\alpha - P_{n-2} = 0.$$

Рассмотрим $v_h(P_n) = v_h(Q_n) + v_h(A_0) = \sum_{i=0}^{n} v_h(A_i) = \sum_{i=0}^{n} t_i$, где $t_i = v_h(A_i)$. Обозначим $s_n = \sum_{i=0}^{n} t_i$.

Рассмотрим значения нормирований у коэффициентов при степени α:

$$\begin{aligned} & v_h(cQ_{n-1}) = s_{n-1} - t_0, \\ & v_h(Q_{n-2} - cP_{n-1}) = v_h(P_{n-1}) = s_{n-1}, \\ & v_h(P_{n-2}) = s_{n-2}. \end{aligned}$$

Наименьшее значение нормирование получается равно s_{n-1}. Перепишем (6) так, чтобы получилось выражение от α с коэффициентами из $k[h^{-1}]$:

$$\begin{aligned} & cQ_{n-1}h^{s_{n-1}}\alpha^2 + (Q_{n-2} - cP_{n-1})h^{s_{n-1}}\alpha - \\ & - P_{n-2}h^{s_{n-1}} = 0. \end{aligned}$$

Откуда дискриминант $D = h^{2s_{n-1}}D'$, где $D' = (Q_{n-2} - cP_{n-1})^2 + 4cQ_{n-1}P_{n-2} = Q_{n-2}^2 - 2cQ_{n-2}P_{n-1} + c^2P_{n-1}^2 + 4cQ_{n-1}P_{n-2}$.

Воспользуемся соотношением 3 и тем, что $n = 2m$:

$$D' = Q_{n-2}^2 + c^2P_{n-1}^2 + 2cQ_{n-2}P_{n-1} - 4c.$$

Перепишем условие:

$$D' = (Q_{n-2} + cP_{n-1})^2 - 4c. \tag{7}$$

Откуда получаем условия зануления свободного коэффициента и, соответственно, утверждение теоремы. □

Замечание. *Условие $fc(Q_{n-2}) + cfc(P_{n-1})$ можно переписать следующим образом:*

$$\begin{aligned} & fc(Q_{n-2}) - 1 + c(fc(P_{n-1}) - 1) = \\ & - (c+1) \pm 2\sqrt{c}, \end{aligned} \tag{8}$$

что для $n = 2$ совпадает с условием теоремы 1.

Для случая $n = 2$ мы видели, что достаточно проверять только выражение, зависящее от произведения $fc(A_0)fc(A_1)$, однако в более общем случае, ситуация несколько усложняется.

Пример 2. *Построим* P_1, P_2, P_3 *и* Q_1, Q_2, Q_3*:*

$$P_0 = A_0,\ Q_0 = 1,$$
$$P_1 = A_1A_0 + 1,\ Q_1 = A_1,$$
$$P_2 = A_2A_1A_0 + A_2 + A_0,$$
$$Q_2 = A_2A_1 + 1,$$
$$P_3 = A_3A_2A_1A_0 + A_3A_2 + A_3A_0 + A_1A_0 + 1,$$
$$Q_3 = A_3A_2A_1 + A_3 + A_1$$

Выражение (8) *приобретает следующий вид:*

$$c(A_0A_1A_2A_3 + A_0A_1 + A_0A_3 + A_2A_3) + \\ + A_1A_2 = -(c+1) \pm 2\sqrt{c},$$

Для того, чтобы дискриминант имел нечётную степень, мы должны требовать равенство 0 *уже более сложного выражения, чем в случае* $n = 2$.

Пусть $c = 4$. *Тогда* $z = -5 \pm 4$. *Пусть* $z = -1$. *Зафиксируем* $fc(A_0) = fc(A_1) = fc(A_3) = 1$, *тогда* $fc(A_2) = -1$.

Пусть $s_i = 1$, *для* $i = 0, \ldots, 3$. *Выбор коэффициентов при* x^{-1} *свободный, пусть это будут* 1. *Тогда* $A_2 = -1 + x^{-1}$, *а* $A_i = 1 + x$, $i = 0, 1, 3$.

Тогда дискриминант имеет следующий вид:

$$D = 64\,x^7 + 168\,x^6 + 272\,x^5 + 329\,x^4 + \\ + 272\,x^3 + 168\,x^2 + 64\,x + 16,$$

А квазипериодический элемент α *имеет вид:*

$$\alpha = \frac{4\,x^4 + 8\,x^3 + 11\,x^2 + 8\,x + 4 - \sqrt{D}}{8\,x^4 + 8\,x^3 + 8\,x^2 + 8\,x} \\ = \left[\overline{\frac{1}{x} + 1, \frac{1}{x} + 1, \frac{1}{x} - 1, \frac{1}{x} + 1}^{4}\right].$$

Работа выполнена при поддержке Российского Научного Фонда (грант 16-11-10111).

Quasiperiodic, but not periodic, functional continued fractions of small quasiperiods

M. M. Petrunin

Abstract

Quasiperiodic and periodic elements of the field $k(x)(\sqrt{f})$, where f is a square-free polynomial of odd degree, and k is an arbitrary field of characteristic different from 2, play a special role. There is a deep connection between S-units of hyperelliptic fields, torsion points in Jacobians of hyperelliptic curves, and elements of hyperelliptic fields that expand into quasiperiodic continued fractions. Most of the quasi-periodic elements considered in the literature are periodic, and there is practically no explicit form of quasi-periodic, but not periodic, elements in the literature. In this paper we find the necessary conditions for the fact that a purequasiperiodic but not a periodic element lies in the corresponding field, and also using the direct construction of a continued fraction, we construct elements that expands into pure quasiperiodic but not periodic functional continued fractions of small quasiperiods.

Keywords: fundamental units, S-units, hyperelliptic fields, Jacobians, hyperelliptic curves, torsion problem in Jacobians, fast alghorithms, continued fractions, $\mathbb{Q}$-torsion points

Литература

1. *Abel N.* Ueber die Integration der Differential-Formel $\rho dx/\sqrt{R}$ wenn R und ρ ganze Functionen sind // Journal für die reine und angewandte Mathematik. — 1826. — т. 1. — с. 185—221.
2. *Adams W. W.*, *Razar M. J.* Multiples of point on elliptic curves and continued fractions // Proc. London Math. Soc. (3). — 1980. — т. 41, № 3. — с. 481—498.
3. *Беняш-Кривец В. В.*, *Платонов В. П.* Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Математический сборник. — 2009. — т. 200, № 11. — с. 15—44.
4. *Петрунин М. М.* S-единицы и периодичность квадратного корня в гиперэллиптических полях // Доклады Академии наук. — 2017. — т. 474, № 2. — с. 155—158.
5. *Петрунин М. М.* Вычисление фундаментальных S-единиц в гиперэллиптических полях рода 2 и проблема кручения в якобианах гиперэллиптических кривых // Чебышевский Сборник. — 2015. — т. 16, № 4. — с. 250—284.
6. *Платонов В. П.* Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // УМН. — 2014. — т. 69:1, № 415. — с. 3—38.

7. *Платонов В. П.*, *Жгун В. С.*, *Федоров Г. В.* Непрерывные дроби в гиперэллиптических полях и представление Мамфорда // Доклады РАН. — 2016. — т. 471, № 6. — с. 640—644.

8. *Платонов В. П.*, *Петрунин М. М.* S-единицы в гиперэллиптических полях и периодичность непрерывных дробей // Доклады РАН. — 2016. — т. 470, № 3. — с. 260—265.

9. *Платонов В. П.*, *Петрунин М. М.* S-единицы и периодичность в квадратичных функциональных полях // УМН. — 2016. — т. 71, № 5. — с. 181—182.

10. *Платонов В. П.*, *Федоров Г. В.* S-единицы и периодичность непрерывных дробей в гиперэллиптических полях // Доклады РАН. — 2015. — т. 465, № 5. — с. 537—541.

11. *Платонов В. П.*, *Федоров Г. В.* О периодичности непрерывных дробей в гиперэллиптических полях // Доклады Академии наук. — 2017. — т. 474, № 5. — с. 540—544.

12. *Платонов В. П.*, *Федоров Г. В.* О периодичности непрерывных дробей в эллиптических полях // Доклады Академии наук. — 2017. — т. 475, № 2. — с. 133—136.

Прямая аддитивная задача о распределении целочисленных случайных величин

Г.В. Федоров[1]

[1] *ФГУ ФНЦ НИИСИ РАН, Москва, Россия,*
E-mail: fedorov@mech.math.msu.su

Аннотация

Предметом нашего внимания в данной статье являются прямые аддитивные задачи с растущим количеством слагаемых. Такие задачи обычно формулируются на языке теории вероятностей, при этом говорят о нарастающих суммах случайных величин. Продолжая исследования В.П. Маслова и В.Е. Назайкинского мы рассматриваем более общую постановку задачи, чем в [5], а именно, в каждой размерности системы мы допускаем растущее число степеней свободы. Для этой системы с одним линейным неравенством мы находим асимптотическое распределение случайной величины и асимптотику для энтропии. Физическая интерпретация рассматриваемых задач обсуждается в [4]-[3].

Ключевые слова: прямые аддитивные задачи, распределение случайных величин, энтропия, многомерная функция делителей

1. Прямые аддитивные задачи

Пусть заданы две конечные или бесконечные последовательности вещественных чисел, расположенных в порядке возрастания:

$$\{\lambda_j\} = \{\lambda_1, \lambda_2, \lambda_3, \ldots\},$$
$$\{\mu_j\} = \{\mu_1, \mu_2, \mu_3, \ldots\}.$$

Образуем множество попарных сумм

$$\{\tau_j\} = \{\lambda_i + \mu_j\}.$$

Значению $\tau \in \{\tau_j\}$ можно приписывать кратность, равную количеству представлений числа τ в указанном виде. Одна из задач состоит в том, чтобы из свойства последовательностей $\{\lambda_j\}$ и $\{\mu_j\}$ вывести свойства их попарных сумм. В это направление включается много задач, среди которых А.Г. Постников [8] выделяет две серии:

1. Задачи о распределении крайностей. Эти задачи будем называть *локальными*. Здесь речь идет об изучении величины
$$p(\tau) = \sum_{\tau=\lambda_i+\mu_j} 1,$$
где суммирование ведется по всем парам (λ_i, μ_j).

2. Обозначим через $n_1(u)$ и через $n_2(u)$ количество чисел соответственно по-

следовательностей $\{\lambda_j\}$ и $\{\mu_j\}$, не превосходящих границы u (u является асимптотически возрастающим параметром). Обозначим через $q(u)$ количество решений неравенства $\lambda_i + \mu_j \leq u$. Задача состоит в изучении величины $q(u)$ при заданных функциях $n_1(u)$ и $n_2(u)$. Такие задачи будем называть *интегральными*. Очевидно, что

$$q(u) = \sum_{\lambda_i \leq u} n_2(u - \lambda_i) = \sum_{\mu_j \leq u} n_1(u - \mu_j).$$

Коснемся постановки аддитивных задач с неограниченным количеством слагаемых. Пусть задана неубывающая последовательность положительных чисел $\{\lambda_j\} = \{\lambda_1, \lambda_2, \lambda_3, \ldots\}$. Последовательность $\{\lambda_j\}$ бесконечно раз сложенная сама с собой, состоит по определению из чисел вида

$$\{\tau_j\} = \{n_1\lambda_1 + n_2\lambda_2 + \ldots + n_s\lambda_s + \ldots\},$$

где n_j — целые неотрицательные числа, причем только конечное количество чисел n_j не равны нулю. Для $\tau \in \{\tau_j\}$ и границы u можно также рассматривать локальные и интегральные прямые аддитивные задачи.

В качестве примера локальной задачи с бесконечным количеством слагаемых укажем на классическую задачу Харди и Рамануджана. В ней предметом внимания является функция натурального аргумента $p(n)$, определенная как количество представлений числа n виде суммы натуральных слагаемых. В этой задаче исходной последовательностью является натуральный ряд, который счетное количество раз складывается сам с собой. Функция $p(n)$ является быстро возрастающей (см. [1])

$$\ln p(n) \sim \pi\sqrt{\frac{2}{3}}\sqrt{n}.$$

Более точная асимптотическая формула имеет вид (см. [9])

$$p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{2n/3}}.$$

Функцию $p(n)$ в задаче Харди и Рамануджана можно определить как количество решений уравнения

$$n = 1 \cdot x_1 + 2 \cdot x_2 + \ldots + j \cdot x_j + \ldots$$

в неотрицательных целых числах x_j. В самом деле, последнее равенство означает, что в разбиении n в сумму натуральных слагаемых число j встречается x_j раз, причем $x_j = 0$ при $j > n$. Такая постановка задачи естественным образом обобщается. Пусть задана монотонно возрастающая последовательность натуральных чисел $a_1, a_2, \ldots, a_r, \ldots$. Обозначим для данного натурального n через $\tilde{p}(n)$ количество решений в целых неотрицательных числах x_j уравнения

$$n = a_1x_1 + a_2x_2 + \ldots + a_rx_r + \ldots.$$

Асимптотическое поведение функции $\tilde{p}(n)$ исследовалось с помощью трех методов:

1. элементарный метод;
2. метод, основанный на тауберовых теоремах для преобразования Лапласа быстро растущих функций;
3. аналитический метод, основанный на формулах обращения для производящих функций.

В прямых аддитивных задачах исследователь идет от величины $n(u)$ к величине $q(u)$. В обратных аддитивных задачах исследование ведется в противоположном направлении.

Предметом нашего внимания в данной статье будут прямые аддитивные задачи с растущим количеством слагаемых. Такие задачи обычно формулируются на языке теории вероятностей, при этом говорят о нарастающих суммах случайных величин. Продолжая исследования В.П. Маслова и В.Е. Назайкинского [5] в данной статье мы рассматриваем более общую постановку задачи, а именно, в каждой размерности системы мы допускаем растущее число степеней свободы. Для этой системы с одним линейным неравенством мы находим асимптотическое распределение случайной величины и асимптотику для энтропии, которая будет определена далее.

Физическая интерпретация рассматриваемых задач обсуждается в [4]-[3].

2. Прямые аддитивные задачи с растущим количеством слагаемых

Рассмотрим задачи, а также некоторые результаты, полученные в цикле работ В.П. Маслова и В.Е. Назайкинского [5]-[2]. Мы будем использовать наши обозначения для того, чтобы далее можно было корректно сравнивать наши результаты с результатами [5]-[2].

1. *Системы целой положительной размерности с одним линейным неравенством.*

Определим $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Пусть задана последовательность $R_j \in \mathbb{N}_0$, $j \in \mathbb{N}$. Рассмотрим множество

$$\mathcal{F}_d = \big\{ f : \mathbb{N}_0^d \to \mathbb{N}_0,\ f(0,\dots,0) = 0, \\ f(j_1,\dots,j_d) \le R_{j_1+\dots+j_d} \big\}.$$

Для заданного $M \in \mathbb{N}$ определим

$$\mathcal{F}_d(M) = \Big\{ f \in \mathcal{F}_d : \\ \sum (j_1 + \dots + j_d) f(j_1,\dots,j_d) \le M \Big\},$$

где суммирование берется по всем наборам $(j_1,\dots,j_d) \in \mathbb{N}_0^d$. Ясно, что $\mathcal{N}(M) = \#\mathcal{F}_d(M)$ конечно. Считая, что все $f \in \mathcal{F}_d(M)$ равновероятны, рассматриваются следующие задачи:

- вычислить значение $N = N(M)$, при котором достигается минимум

  $$\min \sum_{f \in \mathcal{F}_d(M)} \Big| \sum f(j_1,\dots,j_d) - N \Big|,$$

  то есть наиболее вероятное значение суммы $\sum f(j_1,\dots,j_d)$.

- найти асимптотическую формулу для энропии $S = \ln \mathcal{N}(M)$.

2. *Системы произвольной положительной размерности с одним линейным неравенством.*

Для $f \in \mathcal{F}_d(M)$ перенумеруем все значения $f(j_1,\dots,j_d)$, лежащие на одном и том же уровне энергии $j = j_1 + \dots + j_d$, в произволном фиксированном порядке от 1 до $q_j = \binom{j+d-1}{j}$, и обозначим их через f_{jk}, $k = 1,\dots,q_j$. Обозначим

$$f_j = \sum_{k=1}^{q_j} f_{jk}, \qquad f_{jk} \le R_j.$$

Теперь по аналогии обобщим задачу для нецелой размерности d. Для этого определим

$$q_j = \left[\frac{\Gamma(j+d)}{\Gamma(d)\Gamma(j+1)} \right],$$

и рассмотрим всевозможные наборы целых неотрицательных чисел f_{jk}, $j = 1, 2, \dots$, $k = 1,\dots,q_j$, таких, что

$$f_j = \sum_{k=1}^{q_j} f_{jk}, \qquad \sum_{j=1}^{\infty} j f_j \le M,$$

как прежде считая, что все $f \in \mathcal{F}_d(M)$ равновероятны.

Определим число $b = b(M)$ как положительное решение уравнения

$$M = \sum_{j=1}^{\infty} \frac{j q_j}{e^{bj} - 1}, \tag{1}$$

и положим

$$N_j = \frac{q_j}{e^{bj} - 1}, \qquad N = \sum_{j=1}^{\infty} N_j.$$

В статье [5] доказано, что при $M \to \infty$ справедливы асимптотические соотношения

$$M \simeq b^{-d-1}, \quad d \ge 1;$$
$$N \simeq b^{-d}, \quad d > 1;$$
$$N \simeq b^{-1} |\ln b|, \quad d = 1;$$

$$S = \ln \mathcal{N}(M) = \\ = bM + \sum_{j=1}^{\infty} q_j \ln \frac{1 - e^{-(R_j+1)bj}}{1 - e^{-bj}} + O(\ln N).$$

Выражения для величин M и N могут быть выписаны более точно в виде рядов

по степеням b с явно выписанными коэффициентами и остатками. При $d \in [1;2)$ можно доказывать теоремы о концентрации, в которых ширина окресности будет не сликом велика (сравнима с шириной окрестности при $d \geq 2$), но при этом приходится рассматривать не все, а лишь достаточно высокие уровни энергии, начиная с некоторого $j = j_0$.

3. *Системы отрицательной размерности с одним линейным неравенством.*

Будем рассматривать уровни энергии, не превышающие достаточно большого фиксированного j_1 и не меньших $j_0 \geq 1 + [-d]$. Опредлим кратности

$$q_j = \left[\frac{\Gamma(j+d)\Gamma(j_1+1)}{\Gamma(j+1)\Gamma(j_1+d)}\right].$$

По формуле Стирлинга для дальнейшего будет достаточно асимптотического соотношения

$$q_j \asymp \left(\frac{j}{j_1}\right)^{d-1}.$$

При фиксированных $j_0 < j_1$ уравнение (1) имеет единственное решение $b = b(M) > 0$ для любого $M > 0$. Функция $b(M)$ монотонно убывает и стремится к нулю при $M \to \infty$. Для некоторой абсолютной положительной постоянной C будем считать, что

$$bj_1 \geq C, \quad 0 \leq d < 1; \qquad \frac{j_1}{j_0} \ll 1, \quad d < 1.$$

Тогда при $b \to 0$ справедливы асимптотические соотношения (см. [6])

$$N \asymp \left(\frac{j_1}{j_0}\right)^{1-d} b^{-1}, \quad d < 1;$$

$$M \asymp j_1^{1-d} b^{-d-1}, \quad 0 < d < 1;$$

$$M \asymp j_1 b^{-1} |\ln(bj_0)|, \quad d = 0;$$

$$M \asymp \left(\frac{j_1}{j_0}\right)^{1-d} b^{-1} j_0, \quad d < 0.$$

4. *Общие системы произвольной размерности с одним линейным неравенством.*

Пусть $q_j = j^{d-1} + r_j$, $|r_j| < 1$, $j = 1, 2, \ldots$, $1 < d < 2$, а суммы $R_j = \sum_{s=1}^{j} r_j$ равномерно ограничены. При $M \to \infty$ число N оказывается для "большинства" наборов $\{f_{jk}\}$ близким к числу

$$N_0 = M^{d/(d+1)} \frac{\Gamma(d)\zeta(d)}{\big(\Gamma(d+1)\zeta(d+1)\big)^{d/(d+1)}}$$

в следующем смысле. Если $\mathcal{N}(M, \Delta)$ — число наборов $\{f_{jk}\}$, удовлетворяющих неравенству $|N - N_0| > \Delta$, то при $\Delta = N_0^{1/d}\sqrt{\ln N_0 \xi(N_0)}$, где $\xi(N_0)$ — произвольно выбранная положительная функция, растущая (сколь угодно медленно) на бесконечности, то выполнены оценки

$$\frac{\mathcal{N}(M, \Delta)}{\mathcal{N}(M)} \leq C_m N_0^{-m},$$

для $m \in \mathbb{N}_0$ с некоторыми постоянными C_m. Справедливы аналогичные оценки для ограниченных интервалов $j_1 \leq j \leq j_2$

$$\frac{\mathcal{N}'\left(M, [j_1,\ j_2]\right)}{\mathcal{N}(M)} \leq C_m N_0^{-m}, \qquad (2)$$

где $m \in \mathbb{N}_0$, и $\mathcal{N}'\left(M, [j_1,\ j_2]\right)$ — число наборов $\{f_{jk}\}$, удовлетворяющих неравенству

$$\left|\sum_{j=j_1}^{j_2} N_j - b^{-d} \int\limits_{bj_1}^{bj_2} \frac{x_{d-1}\mathrm{dx}}{e^x - 1}\right| > N_0^{\alpha}\sqrt{\ln N_0 \xi(N_0)},$$

и параметр b связан с M соотношением

$$M = b^{-d-1}\Gamma(d+1)\zeta(d+1).$$

В работе [7] при дополнительных условиях на интервал $[j_1, j_2]$ (он не должен быть слишком узким) доказано, что оценки вида (2) являются точными в том смысле, что показатель $\alpha = \frac{\gamma}{2} + \frac{(1-\gamma)}{d}$ в формуле для $\Delta = N_0^{\alpha}$ неулучшаем.

5. *Системы произвольной размерности с двумя линейным неравенствами.*

Если $M, N \to \infty$ и скорости роста этих параметров связаны определенным (для разных значений d по-разному зависящих от d) соотношением, то в пределе "большинство" наборов (относительно упомянутой меры) концентрируется вблизи предельного распределения, описываемого бозе-эйнштейновскими формулами.

3. Постановка задачи с растущим числом степеней свободы

Перейдем к описанию системы, которую будем рассматривать в данной статье. Пусть $t \in \mathbb{N}$ и дан свободный моноид G с множеством образующих $P = \{\omega_1, \ldots, \omega_t\}$. Нейтральный элемент будем обозначать 1. Фиксируем $k \in \mathbb{N}$ и рассмотрим целочисленную решетку вида

$$\mathbb{N}_0^{tk} = \{\bar{\nu} = ((\nu_{1,1}, \ldots, \nu_{t,1}), \ldots, (\nu_{1,k}, \ldots, \nu_{t,k}))\},$$

где $\nu_{ij} \in \mathbb{N}_0$. Зададим функции $\theta, \theta_j : \mathbb{N}_0^{tk} \to G$ следующим образом:

$$\theta_j = \prod_{m=1}^{t} \omega_m^{\nu_{mj}},\ j = 1, \ldots, k, \quad \theta(\bar{\nu}) = \prod_{j=1}^{k} \theta_j.$$

Для данной функции $R : G \to \mathbb{N}_0 \cup \{+\infty\}$ определим множество

$$\mathcal{F}_{t,k} = \{f : \mathbb{N}_0^{tk} \to \mathbb{N}_0,\ f(\bar{0}) = 0, f(\bar{\nu}) \le R(\theta(\bar{\nu}))\}.$$

Для $\beta \in G$ и $f \in \mathcal{F}_{t,k}$ положим

$$f^*(\beta) = \sum_{\bar{\nu}:\theta(\bar{\nu})=\beta} f(\bar{\nu}) = \sum_{\bar{\nu}\in\theta^{-1}(\beta)} f(\bar{\nu}). \quad (3)$$

Для $\beta \in G$ единственным образом определено разложение $\beta = \prod_{\omega\in P} \omega^{k_\omega}$. Положим $v_\omega(\beta) = k_\omega$ для каждого $\omega \in P$. Положим $\Omega(\beta) = \sum_{\omega\in P} v_\omega(\beta)$.

Для $f \in \mathcal{F}_{t,k}$ и некоторого числа $Q \ge 1$ определим

$$N_Q(f) = \sum_{\beta:\Omega(\beta)\le Q} f^*(\beta).$$

Для $M \in \mathbb{N}$ обозначим

$$\mathcal{M}(M,Q) = \Big\{f \in \mathcal{F}_{t,k} : \sum\nolimits_{\beta:\Omega(\beta)\le Q} \Omega(\beta) f^*(\beta) \le M\Big\},$$

$$\mathcal{M}_0(M,Q) = \Big\{f \in \mathcal{F}_{t,k} : \sum\nolimits_{\beta:\Omega(\beta)\le Q} \Omega(\beta) f^*(\beta) = M\Big\}.$$

Количество элементов в $\mathcal{M}(M,Q)$ и $\mathcal{M}_0(M,Q)$ обозначим

$$\mathcal{N}(M,Q) = \#\mathcal{M}(M,Q),$$
$$\mathcal{N}_0(M,Q) = \#\mathcal{M}_0(M,Q).$$

Для чисел N и $\Delta = \Delta(M,Q,N)$ определим

$$\mathcal{N}(M,Q,N,\Delta) = \#\Big\{f \in \mathcal{F}_{t,k} : |N_Q(f) - N| > \Delta, \sum_{\beta:\Omega(\beta)\le Q} \Omega(\beta) f^*(\beta) \le M\Big\}.$$

Нашей целью является при различных условиях на число Q (например, $Q = Q(M) \to \infty$ при $M \to \infty$) определить такое число $N = N(M,Q)$ (если оно существует), для которого найдется $\Delta = \Delta(M,Q,N) = o(N)$, что вероятность

$$\mathrm{P}(M,Q,N,\Delta) = \frac{\mathcal{N}(M,Q,N,\Delta)}{\mathcal{N}(M,Q)} \to 0$$

при $M \to \infty$.

Заметим, что при $t = 1$ наша постановка становится в точности такой же, как в [5].

4. Асимптотическая формула для энтропии

Запишем количество наборов $\mathcal{N}_0(M,Q)$ через сумму символов Кронекера

$$\mathcal{N}_0(M,Q) = \sum_{f\in\mathcal{F}_{t,k}} \delta\left(M, \sum_{\beta:\Omega(\beta)\le Q} \Omega(\beta) f^*(\beta)\right) = \sum_{f\in\mathcal{F}_{t,k}} \delta\left(M, \sum_{\beta:\Omega(\beta)\le Q} \Omega(\beta) f^*(\beta)(f)\right) \times \times \exp\left(bM - b\sum_{\beta:\Omega(\beta)\le Q} \Omega(\beta) f^*(\beta)\right),$$

где $b > 0$ — некоторый вещественный параметр, условия на кторого мы получим далее. Воспользуемся известным тождеством

$$\delta(m,n) = \frac{b}{2\pi}\int_{-\pi/b}^{\pi/b} e^{ib\phi(m-n)}\mathrm{d}\phi,$$

тогда

$$\mathcal{N}_0(M,Q) = \tfrac{be^{bM}}{2\pi} \int\limits_{-\pi/b}^{\pi/b} e^{ib\phi M} \times \times \sum_{f\in\mathcal{F}_{t,k}} \exp\left(-b\sum_{\beta:\Omega(\beta)\le Q} \Omega(\beta) f^*(\beta)(1+i\phi)\right)\mathrm{d}\phi.$$

Подставим выражение (3) в подынтегральную сумму

$$\sum_{f\in\mathcal{F}_{t,k}} \exp\left(-b(1+i\phi)\sum_{\beta:\Omega(\beta)\le Q}\Omega(\beta)f^*(\beta)\right)=$$
$$=\prod_{\beta:\Omega(\beta)\le Q}\ \prod_{\beta=\theta_1\cdot\ldots\cdot\theta_k}\left(\sum_{n=0}^{R(\beta)} e^{-b(1+i\phi)\Omega(\beta)n}\right)=$$
$$=\prod_{\beta:\Omega(\beta)\le Q}\ \prod_{\beta=\theta_1\cdot\ldots\cdot\theta_k}\frac{1-\exp\Big(-b(1+i\phi)\Omega(\beta)(R(\beta)+1)\Big)}{1-\exp\Big(-b(1+i\phi)\Omega(\beta)\Big)}=$$
$$=\prod_{\beta:\Omega(\beta)\le Q}\left(\frac{1-\exp\Big(-b(1+i\phi)\Omega(\beta)(R(\beta)+1)\Big)}{1-\exp\Big(-b(1+i\phi)\Omega(\beta)\Big)}\right)^{\tau_k(\beta)},$$

где $\tau_k(\beta)$ — многомерная функция делителей, равная количеству решений уравнения $\alpha_1\cdot\ldots\cdot\alpha_k=\beta$ в переменных $\alpha_1,\ldots,\alpha_k\in G$.

Если $R(\beta)=+\infty$ для всех β, удовлетворяющих условию $\Omega(\beta)\le Q$, то

$$\sum_{f\in\mathcal{F}_{t,k}} \exp\left(-b(1+i\phi)\sum_{\beta:\Omega(\beta)\le Q}\Omega(\beta)f^*(\beta)\right)=$$
$$\prod_{\beta:\Omega(\beta)\le Q}\Big(1-\exp\Big(-b(1+i\phi)\Omega(\beta)\Big)\Big)^{-\tau_k(\beta)}.$$

Возвращаясь к интегралу, имеем

$$\mathcal{N}_0(M,Q)=\frac{be^{bM}}{2\pi}\int\limits_{-\pi/b}^{\pi/b}\exp\left(b^{-k}\Phi(\phi)\right)\mathrm{d}\phi,$$

$$\Phi(\phi)=ib^{k+1}\phi M+b^k\sum_{\beta:\Omega(\beta)\le Q}\tau_k(\beta)\times$$
$$\times\ln\left(\frac{1-\exp\Big(-b(1+i\phi)\Omega(\beta)(R(\beta)+1)\Big)}{1-\exp\Big(-b(1+i\phi)\Omega(\beta)\Big)}\right).$$

Аргумент экспоненты в интеграле $2\pi/b$ - периодичен. Далее действуем по методу Лапласа, считая $h=b^{-k}$ малым параметром. В итоге получаем

$$\mathcal{N}(M,Q)\ge\mathcal{N}_0(M,Q)\ge$$
$$\ge Cb^{1+k/2}\exp\left(bM+\sum_{\beta:\Omega(\beta)\le Q}\tau_k(\beta)\times\right.$$
$$\left.\times\ln\frac{1-\exp\Big(-b\Omega(\beta)(R(\beta)+1)\Big)}{1-\exp\Big(-b\Omega(\beta)\Big)}\right).$$

Оценка сверху имеет вид

$$\mathcal{N}(M,Q)=\sum_{f\in\mathcal{M}(M,Q)}1\le$$
$$\le\sum_{f\in\mathcal{M}(M,Q)}\exp\left(bM-b\sum_{\beta:\Omega(\beta)\le Q}\Omega(\beta)f^*(\beta)\right)=$$
$$=e^{bM}\prod_{\beta:\Omega(\beta)\le Q}\ \prod_{\beta=\theta_1\cdot\ldots\cdot\theta_k}\left(\sum_{n=0}^{R(\beta)}\exp\Big(-b\Omega(\beta)n\Big)\right)=$$
$$=\exp\left(bM+\sum_{\beta:\Omega(\beta)\le Q}\tau_k(\beta)\times\right.$$
$$\left.\times\ln\frac{1-\exp\Big(-b\Omega(\beta)(R(\beta)+1)\Big)}{1-\exp\Big(-b\Omega(\beta)\Big)}\right).$$

Написанные выше неравенства выполнены для любого $b>0$. Наиболее точные оценки достигаются, когда параметр b удовлетворяет экстремальному условию (локального максимума)

$$M+\sum_{\beta:\Omega(\beta)\le Q}\frac{\tau_k(\beta)\Omega(\beta)(R(\beta)+1)}{\exp\Big(b\Omega(\beta)(R(\beta)+1)\Big)-1}-$$
$$-\sum_{\beta:\Omega(\beta)\le Q}\frac{\tau_k(\beta)\Omega(\beta)}{\exp\Big(b\Omega(\beta)\Big)-1}=0.$$

Если $R(\beta)=+\infty$ для всех β, удовлетворяющих условию $\Omega(\beta)\le Q$, то последнее условие принимает вид

$$M=\sum_{\beta:\Omega(\beta)\le Q}\frac{\Omega(\beta)\cdot\tau_k(\beta)}{e^{b\Omega(\beta)}-1}.$$

Сформулируем только что доказанный результат.

Теорема 1. *При $M\to\infty$ справедлива асимптотическая формула*

$$S=\sum_{\beta:\Omega(\beta)\le Q}\tau_k(\beta)\cdot\ln\frac{1-\exp\Big(-b\Omega(\beta)(R(\beta)+1)\Big)}{1-\exp\Big(-b\Omega(\beta)\Big)}+$$
$$+bM+O(\ln b).$$

5. Концентрация вариантов вблизи предельного распределения

Выберем произвольные действительные числа $f_\beta^{(l)}$, $l=1,\ldots,L$, удовлетворяющие

условию

$$\sum_{l=1}^{L} |f_\beta^{(l)}| \le C_0\Omega(\beta) < b\Omega(\beta) \qquad (4)$$

для всех β таких, что $\Omega(\beta) < Q$. Пусть $\mathcal{N}(\Delta) = \mathcal{N}(M, Q, N, \Delta)$ — количество наборов $\{n_{\theta_1\ldots\theta_k}\}$ удовлетворяющих условиям

$$\sum_{\beta:\Omega(\beta)\le Q} \Omega(\beta) f^*(\beta) \le M,$$

$$\sum_{l=1}^{L} \left| \sum_{\beta:\Omega(\beta)\le Q} f_\beta^{(l)} (f^*(\beta) - \bar{n}_\beta) \right| > \Delta,$$

где

$$\bar{n}_\beta = \tau_k(\beta) \left[\tfrac{1}{e^{b\Omega(\beta)}-1} - \tfrac{(R(\beta)+1)}{e^{b\Omega(\beta)(R(\beta)+1)}-1} \right],$$

$$\bar{n}_{\theta_1\ldots\theta_k} = \tfrac{\bar{n}_\beta}{\tau_k(\beta)}.$$

Множество самих таких наборов $\{n_{\theta_1\ldots\theta_k}\}$ обозначим $\mathcal{A}$. Докажем, что для некоторых постоянных C_q справедливы неравенства

$$\frac{\mathcal{N}(\Delta)}{\mathcal{N}(M,Q)} \le \frac{C_q}{N^q}, \qquad q = 1, 2, \ldots,$$

где

$$N = \sum_{\beta:\Omega(\beta)\le Q} \bar{n}_\beta.$$

Существует набор $\kappa = (\kappa_1, \ldots, \kappa_L) \in \{0,1\}^L$ такой, что для наборов $\{n_{\theta_1\ldots\theta_k}\}$ из множества $\mathcal{A}$ выполняется неравенство

$$\sum_{\beta:\Omega(\beta)\le Q} \sum_{\beta=\theta_1\cdot\ldots\cdot\theta_k} \left(\sum_{l=1}^{L} (-1)^{\kappa_l} f_\beta^{(l)} \right) (f^*(\beta) - \bar{n}_\beta) \ge \Delta.$$

Обозначим

$$f(\beta,\kappa) = \sum_{l=1}^{L} (-1)^{\kappa_l} f_\beta^{(l)}.$$

Пусть $c > 0$ — некоторый вещественный параметр, который мы определим ниже, тогда зададим

$$G(\kappa) = b\left(M - \sum_{\beta:\Omega(\beta)\le Q} \Omega(\beta) \sum_{\beta=\theta_1\cdot\ldots\cdot\theta_k} n_{\theta_1\ldots\theta_k} \right) +$$
$$+c \sum_{\beta:\Omega(\beta)\le Q} \sum_{\beta=\theta_1\cdot\ldots\cdot\theta_k} f(\beta,\kappa)(n_{\theta_1\ldots\theta_k} - \bar{n}_{\theta_1\ldots\theta_k}) \ge c\Delta.$$

Для некоторого набора κ (возможно, что таких наборов несколько) $G(\kappa) \ge 0$, следовательно, для суммы экспонент по всем наборам κ имеем

$$\sum_\kappa \exp\bigl(G(\kappa)\bigr) \ge 1.$$

По определению

$$\mathcal{N}(\Delta) = \sum_{n_{\theta_1\ldots\theta_k}\in\mathcal{A}} 1 \le$$
$$\le \sum_{n_{\theta_1\ldots\theta_k}\in\mathcal{A}} \textstyle\sum_\kappa \exp\bigl(G(\kappa)\bigr) = e^{bM-c\Delta} \sum_\kappa g(\kappa),$$

где

$$g(\kappa) = \sum_{n_{\theta_1\ldots\theta_k}\in\mathcal{A}} \prod_{\beta:\Omega(\beta)\le Q} \prod_{\beta=\theta_1\cdot\ldots\cdot\theta_k} e^{-b\Omega(\beta)n_{\theta_1\ldots\theta_k}} \times$$
$$\times \exp\{cf(\beta,\kappa)(n_{\theta_1\ldots\theta_k} - \bar{n}_{\theta_1\ldots\theta_k})\} =$$
$$= \prod_{\beta:\Omega(\beta)\le Q} \exp\{-c\tau_k(\beta) f(\beta,\kappa)\bar{n}_\beta\} \times$$
$$\times \left(\tfrac{1-\exp\{(cf(\beta,\kappa)-b\Omega(\beta))(R_\beta+1)\}}{1-\exp\{(cf(\beta,\kappa)-b\Omega(\beta))\}} \right)^{\tau_k(\beta)} =$$
$$= \exp\left\{ \sum_{\beta:\Omega(\beta)\le Q} \tau_k(\beta) \Bigl(\ln \tfrac{1-e^{(cf(\beta,\kappa)-b\Omega(\beta))(R_\beta+1)}}{1-e^{(cf(\beta,\kappa)-b\Omega(\beta))}} - \right.$$
$$\left. -cf(\beta,\kappa)\bar{n}_\beta \Bigr) \right\}.$$

Для сходимости геометрической прогрессии в случае $R(\beta) = +\infty$ необходимо потребовать, чтобы для всех β таких, что $\Omega(\beta) < Q$, было выполнено неравенство

$$b\Omega(\beta) - c\sum_{l=1}^{L} (-1)^{\kappa_l} f_\beta^{(l)} > 0,$$

то есть с учетом (4) потребуем, чтобы было выполнено условие $c < \frac{b}{2C_0}$ на параметр c.

Обозначим

$$\phi_\beta = \ln \tfrac{1-e^{(cf(\beta,\kappa)-b\Omega(\beta))(R_\beta+1)}}{1-e^{(cf(\beta,\kappa)-b\Omega(\beta))}} - cf(\beta,\kappa)\bar{n}_\beta.$$

Разложим в ряд Тейлора в точке $x_0 = b\Omega(\beta)$ функцию

$$F(x) = \ln \tfrac{1-e^{-x(R_\beta+1)}}{1-e^{-x}},$$
$$x = b\Omega(\beta) - cf(\beta,\kappa),$$

тогда

$$F\bigl(b\Omega(\beta) - cf(\beta,\kappa)\bigr) = F\bigl(b\Omega(\beta)\bigr) -$$
$$-F'\bigl(b\Omega(\beta)\bigr) \cdot cf(\beta,\kappa) +$$
$$+\tfrac{1}{2}F''\bigl(b\Omega(\beta) - \Theta cf(\beta,\kappa)\bigr) \cdot c^2 f(\beta,\kappa)^2,$$

где число $\Theta = \Theta(\beta) \in [0,1]$. Имеем

$$F'(x) = \frac{(R_\beta+1)e^{-x(R_\beta+1)}}{1-e^{-x(R_\beta+1)}} - \frac{e^{-x}}{1-e^{-x}} = \\ = \frac{R_\beta+1}{e^{x(R_\beta+1)}-1} - \frac{1}{e^x-1},$$

так что при выборе

$$\bar{n}_\beta = -F'\big(b\Omega(\beta)\big) = \\ = \frac{1}{e^{b\Omega(\beta)}-1} - \frac{R_\beta+1}{e^{b\Omega(\beta)(R_\beta+1)}-1}$$

получаем

$$\frac{c^2 f(\beta,\kappa)^2}{2} \min_{0.5\le t\le 1.5} F''(b\Omega(\beta)t) \le \\ \le \phi_\beta - \ln\frac{1-e^{-b\Omega(\beta)(R_\beta+1)}}{1-e^{-b\Omega(\beta)}} \le \\ \le \frac{c^2 f(\beta,\kappa)^2}{2} \max_{0.5\le t\le 1.5} F''(b\Omega(\beta)t).$$

Прямое вычисление дает

$$F''(x) = \frac{e^x}{(e^x-1)^2} - \frac{(R_\beta+1)^2 e^{x(R_\beta+1)}}{(e^{x(R_\beta+1)}-1)^2},$$

так что

$$\max_{0.5\le t\le 1.5} F''(b\Omega(\beta)t) \le \\ \le \max_{0.5\le t\le 1.5} \frac{e^{b\Omega(\beta)t}}{(e^{b\Omega(\beta)t}-1)^2} = \frac{e^{b\Omega(\beta)/2}}{(e^{b\Omega(\beta)/2}-1)^2}, \\ \min_{0.5\le t\le 1.5} F''(b\Omega(\beta)t) \ge 0.$$

Собирая вычисления, получаем

$$\mathcal{N}(\Delta) \le e^{bM-c\Delta} 2^L \times \\ \times \exp\left\{ \sum_{\beta:\Omega(\beta)\le Q} \tau_k(\beta) \ln\frac{1-e^{-b\Omega(\beta)(R_\beta+1)}}{1-e^{-b\Omega(\beta)}} + \right. \\ \left. + C_1 c^2 \sum_{\beta:\Omega(\beta)\le Q} \tau_k(\beta)\Omega(\beta)^2 \frac{e^{b\Omega(\beta)/2}}{(e^{b\Omega(\beta)/2}-1)^2} \right\},$$

где C_1 — некоторая константа, $0 < C_1 < C_0^2$. Отдельно оценим

$$B(Q) = \sum_{\beta:\Omega(\beta)\le Q} \tau_k(\beta)\Omega(\beta)^2 \frac{e^{b\Omega(\beta)/2}}{(e^{b\Omega(\beta)/2}-1)^2} = \\ = \sum_{m=1}^{Q} \binom{m+kt-1}{kt-1} \frac{m^2\cdot e^{bm/2}}{(e^{bm/2}-1)^2} \ll \\ \ll \left(\frac{2}{b}\right)^{kt+2} \int_{b/2}^{bQ/2} \frac{u^{kt+1}e^u}{(e^u-1)^2}\mathrm{d}u = \\ = -\left(\frac{2}{b}\right)^{kt+2} \int_{b/2}^{bQ/2} u^{kt+1}\mathrm{d}\frac{1}{e^u-1} = \\ = \left(\frac{2}{b}\right)^{kt+2} \int_{a_1}^{a_2} \ln^{kt+1}\left(1+\frac{1}{t}\right)\mathrm{d}t,$$

где

$$t = \frac{1}{e^u-1}, \quad a_1 = \frac{1}{e^{bQ/2}-1}, \quad a_2 = \frac{1}{e^{b/2}-1}.$$

Если $0 < bQ < 2\ln 2$, то

$$\int_{a_1}^{a_2} \ln^{kt+1}\left(1+\frac{1}{t}\right)\mathrm{d}t \ll \\ \ll \int_{a_1}^{a_2} \frac{1}{t^{kt+1}}\mathrm{d}t \ll kt(bQ/2)^{kt}.$$

Если $bQ \ge 2\ln 2$, то

$$\int_{a_1}^{a_2} \ln^{kt+1}\left(1+\frac{1}{t}\right)\mathrm{d}t \ll \\ \ll \int_{a_1}^{1} (-\ln t)^{kt+1}\mathrm{d}t + \int_1^{a_2} \frac{1}{t^{kt+1}}\mathrm{d}t \ll \\ \ll \frac{(bQ/2)^{kt+1}}{e^{bQ/2}-1} + kt.$$

Итак,

$$B(Q) \ll \begin{cases} \frac{kt\cdot Q^{kt}}{b^2}, & 0 < bQ < 2\ln 2, \\ \frac{Q^{kt+1}}{b\cdot e^{bQ/2}} + kt\left(\frac{2}{b}\right)^{kt+2}, & bQ \ge 2\ln 2. \end{cases}$$

Таким образом,

$$\mathcal{N}(\Delta) \le \\ \le \exp\left\{ \sum_{\beta:\Omega(\beta)\le Q} \tau_k(\beta) \ln\frac{1-e^{-b\Omega(\beta)(R_\beta+1)}}{1-e^{-b\Omega(\beta)}} + \right. \\ \left. + bM + L\ln 2 - c\Delta + C_2 B(Q) c^2 \right\}.$$

Теперь необходимо, чтобы выражение $L\ln 2 - c\Delta + C_2\cdot B(Q)c^2$ принимало минимальное значение, откуда

$$c = C_2\frac{\Delta}{B(Q)},$$

причем для L возникает ограничение

$$L < C_3\frac{\Delta^2}{B(Q)}.$$

Здесь под $B(Q)$ мы имеем ввиду его оценку. Тогда в выражении для $\mathcal{N}(\Delta)$ возникает понижающим множитель порядка

$$\exp\left\{-C_4\frac{\Delta}{B(Q)}\right\}.$$

6. Элементарные оценки с целыми параметрами

Предложение 1. *Пусть* $Q = Q(n) \to +\infty$, *при* $n \to +\infty$, $q = q(n) > 0$, $y > 0$ *— вещественный параметр. Если* $\frac{q \ln y}{Qy} \to -\infty$ *при* $n \to +\infty$, *то*

$$\sum_{m=1}^{\infty} \frac{\tau_q(\omega^m)}{|Q-m|e^{ym}} \ll \frac{1}{q-1} \frac{1}{(1-e^{-y})^{q-1}}.$$

Если $y < 1$ *и* $\frac{Qy}{q \ln y} \to -\infty$ *при* $n \to +\infty$ *или* $y \geq 1$, *то*

$$\sum_{m=1}^{\infty} \frac{\tau_q(\omega^m)}{|Q-m|e^{ym}} \ll \frac{1}{Q} \frac{1}{(1-e^{-y})^{q}}.$$

Если $\frac{q \ln y}{Qy} \asymp -1$, *то*

$$\sum_{m=1}^{\infty} \frac{\tau_q(\omega^m)}{|Q-m|e^{ym}} \ll \frac{1}{(1-e^{-y})^{q}}.$$

Константа в знаке Виноградова во всех случаях не зависит от значений Q, q *и* y.

Доказательство. Приведем основную идею и краткие рассуждения для обоснования леммы.

Основной вклад суммы

$$\Sigma_0 = \sum_{m=1}^{\infty} \frac{\tau_q(\omega^m)}{e^{ym}}$$

сосредоточен в окрестности точки m такой, что

$$\tau_q(\omega^m) = \binom{m+q-1}{q-1} \asymp e^{ym},$$

то есть при $y < 1$ в окрестности точки

$$m \asymp m_0 = \frac{q \ln \frac{1}{y}}{y},$$

а при $y \geq 1$ в окрестности точки $m_0 = 1$.

Если $Q \prec m_0$, то ввиду преобразования

$$\binom{m+q-1}{q-1} = \frac{m+1}{q-1}\binom{m+q-1}{q-2}$$

имеем

$$\Sigma = \sum_{m=1}^{\infty} \tfrac{\tau_q(\omega^m)}{|Q-m|e^{ym}} \asymp$$
$$\asymp \tfrac{1}{q-1} \sum_{m=m_0-m_1}^{m_0+m_1} \tfrac{m+1}{|Q-m|e^{ym}} \tbinom{m+q-1}{q-2} \asymp$$
$$\asymp \tfrac{1}{q-1} \sum_{m=2}^{\infty} \tfrac{\tau_{q-1}(\omega^m)}{e^{ym}} \asymp \tfrac{1}{q-1} \tfrac{1}{(1-e^{-y})^{q-1}}.$$

Если $Q \succ m_0$, то

$$\Sigma \asymp \sum_{m=1}^{m_0+m_1} \tfrac{1}{|Q-m|e^{ym}} \tbinom{m+q-1}{q-1} \asymp \tfrac{1}{Q} \tfrac{1}{(1-e^{-y})^{q}}.$$

Наконец, если $\frac{q \ln y}{Qy} \asymp -1$, то $Q \asymp m_0$, поэтому

$$\Sigma < \sum_{m=1}^{\infty} \frac{1}{e^{ym}} \binom{m+q-1}{q-1} = \frac{1}{(1-e^{-y})^{q}}.$$

Предложение доказано. □

Лемма 1. *Пусть* $x > 0$ *— некторое вещественное число и* n *— натуральное число, тогда*

$$\sum_{q=n}^{\infty} \frac{x^q}{q!} \ll \begin{cases} \frac{x^n}{n!}, & \text{при} \quad 0 < xe < n, \\ e^x, & \text{при} \quad xe \geq n. \end{cases}$$

Доказательство. Если $0 < xe < n$, то

$$\sum_{q=n}^{\infty} \tfrac{x^q}{q!} \ll \int_n^{\infty} \tfrac{(ex)^u}{u^{u+1/2}} \mathrm{d}u =$$
$$= \int_n^{\infty} \exp\left((1+\ln x)u - \left(u+\tfrac{1}{2}\right)\ln u\right) \mathrm{d}u \ll$$
$$\ll \int_{\infty}^{n} \exp\left((1+\ln x)u - \left(u+\tfrac{1}{2}\right)\ln n\right) \mathrm{d}u \ll \tfrac{x^n}{n!}.$$

Если $xe \geq n$, то очевидно

$$\sum_{q=n}^{\infty} \frac{x^q}{q!} < e^x.$$

Лемма доказана. □

Лемма 2. *Пусть* Q *— достаточно большое натуральное число,* $b > 0$ *— вещественный параметр,* n *—фиксированное натуральное число. Тогда для произвольного целого* Q_0 *такого, что* $1 \leq Q_0 \leq Q$, *справедлива оценка*

$$\sum_{m \leq Q} \frac{m^n}{e^{bm}-1} \ll \begin{cases} \frac{Q^n}{bn}, & \text{при } 0 < bQ < 1, \\ \frac{Q^n}{be^{bQ}}, & \text{при } bQ \geq 1. \end{cases}$$

Доказательство. Перейдем к интегралу и разобьем его на две части:

$$B = \sum_{m\le Q} \frac{m^n}{e^{bm}-1} \ll \int\limits_1^Q \frac{u^n \mathrm{d}u}{e^{bu}-1} = \frac{1}{b^{n+1}} \int\limits_b^{bQ} \frac{u^n \mathrm{d}u}{e^u-1} =$$

$$= \frac{1}{b^{n+1}} \left(\int\limits_b^{bQ_0} \frac{u^n \mathrm{d}u}{e^u-1} + \int\limits_{bQ_0}^{bQ} \frac{u^n \mathrm{d}u}{e^u-1} \right) = \frac{B_1+B_2}{b^{n+1}}.$$

Оценим каждый интеграл. Если $1 < bQ_0 < n$, то

$$B_1 = \int\limits_b^1 + \int\limits_1^{bQ_0} \ll \int\limits_b^1 u^{n-1}\mathrm{d}u + \int\limits_1^{bQ_0} \frac{u^n \mathrm{d}u}{e^u} \ll$$

$$\ll \frac{1}{n} + \sum_{q=0}^{n} \frac{n!}{q!} \frac{u^q}{e^u} \Bigg|_1^{bQ_0}.$$

$$\sum_{q=0}^{n} \frac{n!}{q!} \frac{u^q}{e^u} \Bigg|_1^{bQ_0} =$$

$$= \sum_{q=0}^{\infty} \frac{n!}{q!} \frac{u^q}{e^u} \Bigg|_1^{bQ_0} + O\left(\frac{n!}{e^{bQ_0}} \frac{(bQ_0)^n}{n!} \right) + O\left(\frac{n!}{e} \frac{1}{n!} \right) =$$

$$= \frac{n!}{e^{bQ_0}} e^{bQ_0} - \frac{n!}{e} e + O\left(\frac{(bQ_0)^n}{e^{bQ_0}} \right) = O\left(\frac{(bQ_0)^n}{e^{bQ_0}} \right).$$

Следовательно,

$$B_1 \ll \frac{1}{n} + \frac{(bQ_0)^n}{e^{bQ_0}} \ll \frac{(bQ_0)^n}{e^{bQ_0}}.$$

Если $bQ_0 \le 1$, то

$$B_1 \ll \int\limits_b^{bQ_0} u^{n-1}\mathrm{d}u \ll \frac{(bQ_0)^n}{n} - \frac{b^n}{n} \ll \frac{(bQ_0)^n}{n}.$$

Если $bQ_0 \ge n$, то

$$B_1 \ll \int\limits_b^1 u^{n-1}\mathrm{d}u + \int\limits_1^{bQ_0} \frac{u^n \mathrm{d}u}{e^u} \ll$$

$$\ll \frac{1}{n} + \frac{(bQ_0)^n}{e^{bQ_0}} - n! \ll \frac{(bQ_0)^n}{e^{bQ_0}}.$$

Аналогично получаем

$$B_2 \ll \begin{cases} \frac{(bQ)^n}{n}, & \text{при} \quad 0 < bQ < 1, \\ \frac{(bQ)^n}{e^{bQ}}, & \text{при} \quad bQ \ge 1. \end{cases}$$

Лемма доказана. □

Лемма 3. *Пусть $0 < b < 1$ — некторое вещественное число и n — натуральное число, тогда*

$$B = \sum_{m=1}^{\infty} \frac{m}{e^{bm}-1} \binom{m+n-1}{n-1} \ll \frac{n!}{b^{n+1}}.$$

Доказательство. Запишем

$$B_\infty = \sum_{m=Q}^{\infty} \frac{m}{e^{bm}-1} \binom{m+n-1}{n-1} \ll$$

$$\ll \frac{1}{b^{n+1}} \int_{bQ}^{\infty} \frac{u^n}{e^u-1} \mathrm{d}u.$$

Если $bQ > n$, то

$$B_\infty \ll \frac{1}{b^{n+1}} \left(\int\limits_{bQ}^{\infty} \frac{u^n}{e^u} \mathrm{d}u + \int\limits_{bQ}^{\infty} \frac{u^n}{e^u(e^u-1)} \mathrm{d}u \right) =$$

$$= \frac{1}{b^{n+1}} \sum_{q=0}^{n} \frac{n!}{q!} \frac{(bQ)^q}{e^{bQ}} + O\left(\frac{1}{b^{n+1}} \frac{n!}{e^{bQ}} \right) \ll \frac{Q^n}{be^{bQ}}.$$

Если $1 < bQ < n$, то

$$B_\infty \ll \frac{n!}{b^{n+1}}.$$

Если $0 < bQ < 1$, то справедлива оценка

$$B_\infty \ll \frac{1}{b^{n+1}} \int\limits_{bQ}^{1} u^{n-1}\mathrm{d}u +$$

$$+ \frac{1}{b^{n+1}} \left(\int\limits_1^{\infty} \frac{u^n}{e^u} \mathrm{d}u + \int\limits_1^{\infty} \frac{u^n}{e^u(e^u-1)} \mathrm{d}u \right) \ll \frac{n!}{b^{n+1}}.$$

Следовательно, для некоторого $1 \le Q$ справедлива оценка

$$B \ll \begin{cases} \frac{Q^n}{bn} + \frac{n!}{b^{n+1}}, & \text{при} \quad 0 < bQ < 1, \\ \frac{Q^n}{be^{bQ}} + \frac{n!}{b^{n+1}}, & \text{при} \quad 1 \le bQ < n, \\ \frac{Q^n}{be^{bQ}}, & \text{при} \quad bQ \ge n. \end{cases}$$

Из анализа этих возможностей следует, что

$$B \ll \begin{cases} \frac{n!}{b^{n+1}}, & \text{при} \quad 0 < bQ < n, \\ \frac{Q^n}{be^{bQ}}, & \text{при} \quad bQ \ge n. \end{cases}$$

Таким образом, при $Q = \alpha \frac{n}{b}$ с подходящим значением α мы получаем утверждение леммы.

Лемма доказана. □

Предложение 2. *Пусть Q — натуральное число, $b > 0$ — вещественный параметр, такой, что $b = b(Q) = o(1/Q)$ при $Q \to \infty$, k и t — натуральные числа. Тогда справедлива асимптотическая формула*

$$\sum_{m\le Q} \frac{m}{e^{bm}-1} \binom{m+kt-1}{kt-1} = \frac{1}{b} \binom{Q+kt}{kt} \big(1 + O(bQ)\big).$$

Доказательство. Заметим, что при достаточно малом b и целом m, $1 \le m \le Q$ справедлива оценка

$$\frac{1}{b} < \frac{m}{e^{bm}-1} < \frac{1}{b(1+bm)} = \frac{1}{b}\big(1+O(bQ)\big).$$

Теперь утверждение леммы следует из известной формулы

$$\sum_{m=0}^{Q}\binom{m+kt-1}{kt-1} = \binom{Q+kt}{kt}.$$

Предложение доказано. □

7. Обобщение оценок на случай действительных параметров

Нам понадобится обобщение известной формулы

$$\sum_{m=0}^{Q}\binom{m+kt-1}{kt-1} = \binom{Q+kt}{kt}.$$

Лемма 4. *Пусть n — натуральное число, $0 < a < b$ - действительные числа. Тогда при $b \to \infty$ справедлива асимптотическая формула*

$$\int\limits_a^b \binom{x}{n} dx = \binom{b}{n+1} - \binom{a}{n+1} + O\binom{b}{n},$$

где

$$\binom{x}{n} = \frac{x(x-1)\cdot\ldots\cdot(x-n-1)}{n!}.$$

Доказательство. При некотором z, $0 < \Re z < 1$, справедливо соотношение

$$(1+z)^x = \sum_{n=0}^{\infty}\binom{x}{n}z^n.$$

Если m — целое число, то

$$\int\limits_0^1 e^{2\pi i\alpha m}\mathrm{d}\alpha = \begin{cases}1, & \text{если} \quad m=0,\\ 0, & \text{иначе.}\end{cases}$$

Таким образом, при некотором t, $0 < t < 1$

$$\binom{x}{n} = \frac{1}{t^n}\int\limits_0^1 e^{2\pi i\alpha n}(1+te^{-2\pi i\alpha})^x\mathrm{d}\alpha.$$

Следовательно,

$$\int\limits_a^b \tbinom{x}{n}\mathrm{d}x = \tfrac{1}{t^n}\int\limits_0^1 e^{2\pi i\alpha n}\int\limits_a^b(1+te^{-2\pi i\alpha})^x\mathrm{d}x\,\mathrm{d}\alpha,$$

При вычислении внутреннего интеграла возникает логарифм, у которого мы рассматриваем ту ветвь, для которой $\mathrm{Ln}\,1 = 0$. Тогда

$$\ln(1+te^{-2\pi i\alpha}) = \\ = te^{-2\pi i\alpha}\left(1-\tfrac{1}{2}te^{-2\pi i\alpha}+O(t^2)\right) = \\ = \tfrac{te^{-2\pi i\alpha}}{1+\frac{1}{2}te^{-2\pi i\alpha}+O(t^2)}.$$

Значит,

$$\int\limits_a^b \tbinom{x}{n}\mathrm{d}x = \\ = \tfrac{1}{t^{n+1}}\int\limits_0^1 e^{2\pi i\alpha(n+1)}\Big((1+te^{-2\pi i\alpha})^b - \\ -(1+te^{-2\pi i\alpha})^a\Big)\mathrm{d}\alpha + \\ +O\Bigg(\tfrac{1}{t^n}\int\limits_0^1 e^{2\pi i\alpha n}\Big((1+te^{-2\pi i\alpha})^b - \\ -(1+te^{-2\pi i\alpha})^a\Big)\mathrm{d}\alpha\Bigg).$$

Снова разлагая в ряд, получаем

$$\int_a^b\binom{x}{n}\mathrm{d}x = \binom{b}{n+1} - \binom{a}{n+1} + O\binom{b}{n}.$$

Лемма доказана. □

Более точно утверждение леммы можно записать следующим образом:

$$\int\limits_a^b \tbinom{x}{n}\mathrm{d}x = \tbinom{b}{n+1} - \tbinom{a}{n+1} + \\ +\tfrac{1}{2}\tbinom{b}{n} - \tfrac{1}{2}\tbinom{a}{n} + O\tbinom{b}{n-1}.$$

Сформулируем обобщение леммы 2 для положительных действительных значений параметров Q, k, t. Для вещественных $x \ge 0$ и $y \ge 1$ определим

$$\binom{x+y-1}{y-1} = \frac{1}{xB(x,y)}.$$

Предложение 3. *Пусть $0 < Q_1 < Q_2$ — вещественные числа, $b > 0$ — вещественный параметр, такой, что $b = o(1/Q_2)$ при $Q_2 \to \infty$, $k \geq 1$ и $t \geq 1$ — вещественные числа. Тогда справедлива асимптотическая формула*

$$\int\limits_{Q_1}^{Q_2} \tfrac{u}{e^{bu}-1}\tbinom{u+kt-1}{kt-1}\,du =$$
$$= \tfrac{1}{b}\Bigg(\tbinom{Q_2+kt}{kt} - \tbinom{Q_1+kt}{kt} +$$
$$+\tfrac{1}{2}\tbinom{Q_2+kt}{kt-1} - \tfrac{1}{2}\tbinom{Q_1+kt}{kt-1}\Bigg)\times$$
$$\times\left(1 + O(bQ) + O\left(\tfrac{(kt)^2}{(Q_2+kt)^2}\right)\right).$$

Доказательство. Заметим, что при достаточно малом b и некотором u, $0 < Q_1 \leq u \leq Q_2$ справедлива оценка

$$\frac{1}{b} < \frac{u}{e^{bu}-1} < \frac{1}{b(1+bu)} = \frac{1}{b}\big(1 + O(bQ_2)\big).$$

Теперь утверждение леммы следует из леммы 4 при $n = [kt]$.

Предложение доказано. □

Таким образом, если $b = b(Q) = o(1/Q)$ и $R(\beta) = +\infty$ для всех β, удовлетворяющих условию $\Omega(\beta) \leq Q$, то

$$M = \frac{1}{b}\binom{Q+kt}{kt}\big(1 + O(bQ)\big).$$

Это означает, что при условии

$$M \prec \frac{1}{Q}\binom{Q+kt}{kt}$$

для оптимальной оценки энтропии мы должны выбрать

$$b = M\binom{Q+kt}{kt}^{-1}.$$

Тогда

$$S = bM\big(1 + O(bQ)\big) + b^{1-kt}\big(1 + O(b)\big).$$

8. Асимптотические формулы

В этом параграфе мы приводим ряд асимптотических результатов необходимых для исследования поставленных в этой работе задачи, а также имеющих собственный интерес.

Лемма 5. *Пусть*

$$f(z) = \begin{cases} \ln\frac{z}{e^z-1}, & z \neq 0 \\ 0, & z = 0, \end{cases}$$

однозначная функция, заданная главной ветвью логарифма. Тогда

$$\left|\ln\frac{1}{e-1} - \sum_{n=1}^{N} b_n\right| \leq 5C_0\left(\frac{4}{5}\right)^{N+1},$$

где

$$b_n = \tfrac{f^{(n)}(0)}{n!}, \quad n = 1, \ldots, N,$$

$$C_0 = \max_{|z|=5/4}|f(z)| \approx 1.75194.$$

Доказательство. Так как

$$\ln\frac{z}{e^z-1} = -\ln\frac{e^z-1}{z},$$

то в силу разложения

$$\frac{e^z-1}{z} = 1 + \sum_{n=2}^{\infty}\frac{z^{n-1}}{n!}$$

замечаем, что функция $f(z)$ является аналитичной в области

$$G = \left\{z : \left|\frac{e^z-1}{z} - 1\right| < 1\right\}.$$

Обозначим $a = |z|$, тогда

$$\frac{e^a-1}{a} - 1 > 0$$

для любого значения $a \neq 0$. Оценивая,

$$\left|\tfrac{e^z-1}{z} - 1\right| = \left|\textstyle\sum_{n=2}^{\infty}\tfrac{z^{n-1}}{n!}\right| \leq$$
$$\leq \textstyle\sum_{n=2}^{\infty}\tfrac{a^{n-1}}{n!} = \tfrac{e^a-1}{a} - 1 < 1,$$

получаем, что

$$G = \{z : \ |z| < a_0\},$$

где $a_0 \approx 1.25643$ — ненулевое решение уравнения $e^a - 2a - 1 = 0$.

Рассмотрим контур γ_0 в форме окружности с центром в точке $z_0 = 0$ и радиуса

$\frac{5}{4} < a_0$. Тогда имеет место разложение в ряд Тейлора

$$f(z) = \sum_{n=1}^{\infty} b_n z^n, \qquad b_n = \frac{f^{(n)}(0)}{n!},$$

который сходится в круге $I(\gamma_0)$. По неравенству Коши, имеем

$$|b_n| = \left|\frac{f^{(n)}(0)}{n!}\right| \le \frac{M(5/4)}{(5/4)^n} = C_0 \left(\frac{4}{5}\right)^n,$$
$$M(\rho) = \max_{|z|=\rho} |f(z)|\}.$$

Таким образом, для точки $z_1 = 1$ имеем

$$\left|\frac{1}{e-1} - \sum_{n=1}^{N} b_n\right| = \left|\frac{1}{e-1} - \sum_{n=N+1}^{\infty} b_n\right| \le$$
$$\le C_0 \sum_{n=N+1}^{\infty} \left(\frac{4}{5}\right)^n = 5C_0 \left(\frac{4}{5}\right)^{N+1}.$$

Лемма доказана. □

Пусть функция $\theta_0 : \mathbb{N}_0^t \to G$ задана следующим образом

$$\theta_0(\bar{\nu}) = \prod_{m=1}^{t} \omega_m^{\nu_m}.$$

Предложение 4. *Справедливо тождество*

$$\sum_{\beta:\Omega(\beta)=Q} \tau_k(\beta) = \binom{Q+kt-1}{kt-1}.$$

Доказательство. Запишем

$$\sum_{\beta:\Omega(\beta)=Q} \tau_k(\beta) = \sum_{\bar{\nu}:\nu_1+\ldots+\nu_t=Q} \tau_k(\theta_0(\bar{\nu})) =$$
$$= \sum_{\bar{\nu}:\nu_1+\ldots+\nu_t=Q} \sum_{\theta_1\ldots\theta_k=\theta_0(\bar{\nu})} 1,$$

Для каждого θ_m, $m = 1, \ldots, t$, имеем разложение

$$\theta_j = \prod_{m=1}^{t} \omega_j^{\nu_{mj}}, \quad \sum_{j=1}^{k} \nu_{mj} = \nu_m.$$

Следовательно, двойную сумму можно записать в одну сумму по всем наборам $\{\nu_{mj}\}$ с условием

$$\mathcal{A}: \qquad \sum_{m=1}^{t} \sum_{j=1}^{k} \nu_{mj} = Q.$$

Таким образом,

$$\sum_{\beta:\Omega(\beta)=Q} \tau_k(\beta) = \sum_{\mathcal{A}} 1 = \tau_{kt}(\omega^Q) = \binom{Q+kt-1}{kt-1}.$$

Предложение доказано. □

При достаточно больших значениях Q имеем асимптотику

$$\binom{Q+kt-1}{kt-1} = \frac{Q^{kt-1}}{\Gamma(kt)} \left(1 + \frac{(kt-1)kt}{2Q} + O(Q^{-2})\right).$$

Ввиду формулы

$$\sum_{m=0}^{M-k} \binom{k+m}{k} = \sum_{m=k}^{M} \binom{m}{k} = \binom{M+1}{k+1}$$

получаем, что

$$\sum_{m=0}^{Q-\nu_t} \binom{m+k(t-1)-1}{k(t-1)-1} = \binom{Q-\nu_t+k(t-1)}{k(t-1)}.$$

При заданном достаточно большом Q и условии $\sum_{j=1}^{t} \nu_j = Q$ минимальное, среднее и максимальное значение $\tau_k(\beta)$ соответственно равны

$$\tau_k\left(\omega^Q\right) = \binom{Q+k-1}{k-1} \le \frac{\binom{Q+kt-1}{kt-1}}{\binom{Q+t-1}{t-1}} \le$$
$$\le \tau_k\left(\omega_1^{Q/t} \cdot \ldots \cdot \omega_t^{Q/t}\right) = \binom{\frac{Q}{t}+k-1}{k-1}^t.$$

Мы полагаем, что Q значительно больше t, поэтому без ограничения общности можем считать $\frac{Q}{t}$ целым числом.

Предложение 5. *Пусть $Q, k, t > 0$, тогда*

$$\sum_{\beta:\Omega(\beta)\le Q} \frac{\Omega(\beta)\cdot\tau_k(\beta)}{e^{b\Omega(\beta)}-1} =$$
$$= \left(\frac{1}{1-e^{-b}}\right)^{kt} - \frac{1}{be^{bQ}} \sum_{m=0}^{kt-1} \frac{\left(Q+\frac{kt}{2}\right)^{kt-1-m}}{(kt-1-m)!} \times$$
$$\times \sum_{2q_2+\ldots+(kt-1)q_{kt-1}=m} \frac{b_2^{q_2}\ldots b_{kt-1}^{q_{kt-1}}}{q_2!\ldots q_{kt-1}!} (kt)^{q_2+\ldots+q_{kt-1}}.$$

Доказательство. По предложению 4 имеем

$$\sum_{\beta:\Omega(\beta)\le Q} \frac{\Omega(\beta)\cdot\tau_k(\beta)}{e^{b\Omega(\beta)}-1} =$$
$$= \sum_{m\le Q} \frac{m}{e^{bm}-1} \binom{m+kt-1}{kt-1} = \sum_{m\le Q} \frac{m\cdot\tau_{kt}(\omega^m)}{e^{bm}-1}$$

для произвольного $\omega \in P$. Справедливы разложения

$$\tfrac{1}{e^{bm}-1} = \sum_{j=1}^{\infty} \tfrac{1}{e^{bmj}},$$

$$\tfrac{\tau_{kt}(\omega^m)}{e^{bmj}} = \sum_{\nu_1+\ldots+\nu_{kt}=m} e^{-bj(\nu_1+\ldots+\nu_{kt})},$$

где $0 \le \nu_q \le m$, $q = 1, \ldots, kt$. Следовательно, мы можем записать

$$\sum_{m\le Q} \tfrac{m\cdot\tau_{kt}(\omega^m)}{e^{bm}-1} = \sum_{j=1}^{\infty} \sum_{\nu_1+\ldots+\nu_{kt}\le Q} \tfrac{\nu_1+\ldots+\nu_{kt}}{e^{bj(\nu_1+\ldots+\nu_{kt})}}.$$

Заметим, что

$$\sum_{\nu_1+\ldots+\nu_{kt}\le Q} \tfrac{\nu_1+\ldots+\nu_{kt}}{e^{bj(\nu_1+\ldots+\nu_{kt})}} = \\ = -\tfrac{\mathrm{d}}{\mathrm{d}a} \sum_{\nu_1+\ldots+\nu_{kt}\le Q} e^{-a(\nu_1+\ldots+\nu_{kt})}\Big|_{a=bj},$$

поэтому мы будем вычислять сумму

$$B(a) = \sum_{\nu_1+\ldots+\nu_{kt}=1}^{Q} e^{-a(\nu_1+\ldots+\nu_{kt})}.$$

Для $\sigma > 0$ и достаточно большого $T > 0$ справедлива формула

$$\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT} \frac{y^s}{s}\mathrm{d}s = \\ = \begin{cases} 1 + O\left(\frac{y^\sigma}{T|\log y|}\right), & \text{если} \quad y > 1, \\ O\left(\frac{y^\sigma}{T|\log y|}\right), & \text{если} \quad 0 < y < 1. \end{cases}$$

Значит, при $1 \le \nu_1 + \ldots + \nu_{kt} \le Q$ и $a > 0$ справедливо равенство

$$e^{-a(\nu_1+\ldots+\nu_{kt})} = \tfrac{e^{-a(\nu_1+\ldots+\nu_{kt})}}{2\pi i}\times \\ \times \int_{\sigma-iT}^{\sigma+iT} \tfrac{\exp\{a\left(Q-(\nu_1+\ldots+\nu_{kt})\right)s\}}{s}\mathrm{d}s + \\ + R\big(T, \sigma, Q-(\nu_1+\ldots+\nu_{kt})\big).$$

Функция

$$F(s) = \left(\frac{1}{1-e^{-as}}\right)^{kt}$$

имеет единственный полюс порядка kt в точке $s = 0$. Тогда функция

$$F(s+1) - 1 = \\ = -1 + \sum_{\nu_1=0}^{\infty} e^{-a\nu_1(s+1)} \ldots \sum_{\nu_{kt}=0}^{\infty} e^{-a\nu_{kt}(s+1)} = \\ = \sum_{n=1}^{\infty} \sum_{\nu_1+\ldots+\nu_{kt}=n} e^{-a(\nu_1+\ldots+\nu_{kt})(s+1)}$$

имеет также единственный полюс порядка kt в точке $s = -1$. Таким образом,

$$B(a) = \tfrac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT} \tfrac{e^{aQs}}{s}\big(F(s+1)-1\big)\mathrm{d}s + R(a),$$

где

$$R(a) \ll \tfrac{e^{aQ\sigma}}{aT} \sum_{\nu_1+\ldots+\nu_{kt}=1}^{\infty} \tfrac{e^{-a(\nu_1+\ldots+\nu_{kt})(\sigma+1)}}{\left|Q-(\nu_1+\ldots+\nu_{kt})\right|} = \\ = \tfrac{e^{aQ\sigma}}{aT} \sum_{m=1}^{\infty} \tfrac{\tau_{kt}(\omega^m)}{\left|Q-m\right| e^{am(\sigma+1)}},$$

причем здесь и далее мы считаем, что слагаемое с $m = Q$ пропущено.

Очевидно,

$$R(a) \ll \tfrac{e^{aQ\sigma}}{aT} \sum_{m=1}^{\infty} \tfrac{\tau_{kt}(\omega^m)}{e^{am(\sigma+1)}} = \\ = \tfrac{e^{aQ\sigma}}{aT}\big(F(\sigma+1)-1\big) = \\ = \tfrac{e^{aQ\sigma}}{aT(1-e^{-a(\sigma+1)})^{kt}} - \tfrac{e^{aQ\sigma}}{aT}.$$

Выберем произвольное большое число U и рассмотрим прямоугольный контур Γ с вершинами в точках $-U - iT$, $-U + iT$, $\sigma + iT$, $\sigma - iT$. Оценим интегралы

$$I_1 = \tfrac{1}{2\pi i}\int_{-U+iT}^{\sigma+iT} \tfrac{e^{aQs}}{s}\big(F(s+1)-1\big)\mathrm{d}s,$$

$$I_2 = \tfrac{1}{2\pi i}\int_{-U-iT}^{-U+iT} \tfrac{e^{aQs}}{s}\big(F(s+1)-1\big)\mathrm{d}s.$$

При $s = \rho + iT$, $-U \le \rho \le \sigma$ найдем минимум функции

$$|1 - e^{-a(\rho+1+iT)}|^2 = \\ = (1 - e^{-a(\rho+1)}\cos aT)^2 + e^{-2a(\rho+1)}(\sin aT)^2.$$

Производная по ρ равна нулю в точке ρ_0, если

$$e^{-a(\rho_0+1)} = \cos(aT) > 0, \\ \rho_0 = -1 - \tfrac{\ln\cos aT}{a}.$$

Если $\cos(aT) < 0$ или $\sigma < \rho_0$ то, все равно при $T \ne \frac{\pi n}{a}$, $n \in \mathbb{Z}$, получаем, что

$$|F(s+1)-1| \ll \left|\tfrac{1}{1-e^{-a(s+1)}}\right|^{kt} \ll |\sin aT|^{-kt}.$$

Значит,

$$|I_1| \ll \tfrac{1}{T(\sin aT)^{kt}} \int_{-U}^{\sigma} e^{aQ\rho}\mathrm{d}\rho \ll \tfrac{e^{aQ\sigma}}{aTQ|\sin aT|^{kt}}.$$

При $s = -U + i\kappa$ и достаточно большом $U > \frac{1}{a}$ имеем

$$|F(s+1) - 1| = \\ = \left|\left(\tfrac{1}{1-e^{a(U-1)}e^{-ai\kappa}}\right)^{kt} - 1\right| \ll 1.$$

Следовательно,

$$|I_2| \ll \tfrac{1}{e^{aUQ}} \int_{-T}^{T} \tfrac{\mathrm{d}\kappa}{\sqrt{U^2+t^2}} \ll \tfrac{\arctan\frac{T}{U}}{e^{aUQ}}.$$

По теореме Коши о вычетах имеем

$$\tfrac{1}{2\pi i}\int_\Gamma \tfrac{e^{aQs}}{s}\big(F(s+1)-1\big)\mathrm{d}s = \\ = (\operatorname*{res}_{s=0} + \operatorname*{res}_{s=-1})\tfrac{e^{aQs}}{s}\big(F(s+1)-1\big) = \\ = \left(\tfrac{1}{1-e^{-a}}\right)^{kt} - 1 + \operatorname*{res}_{s=-1}\left(\tfrac{e^{aQs}}{s}F(s+1)\right).$$

Производящая функция полиномов Бернулли имеет вид

$$\frac{te^{tx}}{e^t-1} = \sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!},$$

следовательно,

$$\frac{1}{1-e^{-a(s+1)}} = \sum_{n=-1}^{\infty} B_{n+1}(1)\frac{\big(a(s+1)\big)^n}{(n+1)!},$$

причем $B_n(1) = B_n$ при $n > 1$, $B_0(1) = 1$, $B_1(1) = \frac{1}{2}$, наконец $B_n = 0$ при нечетных $n > 1$. Используя это, находим

$$\tfrac{1}{1-e^{-a(s+1)}} = \tfrac{1}{a(s+1)}\exp\left\{\tfrac{a(s+1)}{2} - \tfrac{\big(a(s+1)\big)^2}{24} + \right. \\ \left. + \tfrac{\big(a(s+1)\big)^4}{2880} - \tfrac{\big(a(s+1)\big)^6}{181440} + O\Big(\big(a(s+1)\big)^8\Big)\right\}.$$

Кроме того, в окрестности точки $s = -1$ имеем

$$-\frac{1}{s} = \frac{1}{1-(s+1)} = \sum_{m=0}^{\infty}(s+1)^m.$$

Тогда вычет в точке $s = -1$ равен

$$\operatorname*{res}_{s=-1} = \operatorname*{res}_{s=-1}\tfrac{e^{aQs}}{s}\left(\tfrac{1}{1-e^{-a(s+1)}}\right)^{kt} = \\ = -\tfrac{1}{a^{kt}e^{aQ}}\operatorname*{res}_{s=-1}\sum_{m=-kt}^{\infty}(s+1)^m\exp\big\{a_1(s+1)a + \\ + a_2(s+1)^2a^2 + \ldots + a_{kt-1}(s+1)^{kt-1}a^{kt-1}\big\},$$

где

$$a_1 = Q + \tfrac{kt}{2}, \quad a_2 = -\tfrac{kt}{24}, \quad a_3 = 0, \\ a_4 = \tfrac{kt}{2880}, \quad a_5 = 0, \quad a_6 = -\tfrac{kt}{181440}, \quad \ldots$$

Достаточно рассмотреть в степени экспоненты только первые $kt-1$ слагаемых, так как при разложении в ряд Тейлора остальные слагаемые не повлияют на вычет. Выпишем коэффициент при $(s+1)^{-1}$ после разложения экспоненты в ряд Тейлора:

$$\operatorname*{res}_{s=-1} = -\tfrac{1}{e^{aQ}}\sum_{m=1}^{kt-1} a^{m-kt}\times \\ \times\sum_{q_1,\ldots,q_{kt-1}} \frac{a_1^{q_1}a_2^{q_2}\ldots a_{kt-1}^{q_{kt-1}}}{\big(q_1+q_2+\ldots+q_{kt-1}\big)!} \\ \times\frac{\big(q_1+q_2+\ldots+q_{kt-1}\big)!}{q_1!q_2!\ldots q_{kt-1}!}, \tag{5}$$

где при каждом m второе суммирование ведется по всем целым $q_i \geq 0$ таким, что $q_1 + 2q_2 + \ldots + (kt-1)q_{kt-1} = m$.

С другой стороны, ввиду разложения

$$\tfrac{1}{s} = -\tfrac{1}{1-(s+1)} = \\ = -\exp\left(-\ln(1-(s+1))\right) = \\ = -\exp\left(\sum_{l=1}^{\infty}\tfrac{(s+1)^l}{l}\right),$$

имеем

$$\operatorname*{res}_{s=-1} = -\tfrac{1}{e^{aQ}}\operatorname*{res}_{s=-1}\tfrac{1}{(a(s+1))^{kt}}\times \\ \times\exp\left(\sum_{l=1}^{kt-1}(s+1)^l\left(a^lb_lkt + \tfrac{1}{l}\right) + aQ(s+1)\right) = \\ = -\sum_{q_1+2q_2+\ldots+(kt-1)q_{kt-1}=kt-1}\tfrac{1}{a^{kt}e^{aQ}}\times \\ \times\frac{\big(a(b_1kt+Q)+1\big)^{q_1}\ldots\big(a^{kt-1}b_{kt-1}kt+\frac{1}{kt-1}\big)^{q_{kt-1}}}{q_1!q_2!\ldots q_{kt-1}!} = \\ = -\sum_{q_1+2q_2+\ldots+(kt-1)q_{kt-1}\leq kt-1}\tfrac{1}{e^{aQ}}\times \\ \times\frac{a_1^{q_1}a_2^{q_2}\ldots a_{kt-1}^{q_{kt-1}}}{q_1!q_2!\ldots q_{kt-1}!}a^{q_1+2q_2+\ldots+(kt-1)q_{kt-1}-kt},$$

где последнее равенство следует из формулы (5).

Рассмотрим в (5) слагаемые, для которых $q_1 + 2q_2 = kt-1$, $q_3 = \ldots = q_{kt-1} = 0$:

$$\tfrac{1}{ae^{aQ}}\sum_{q_1+2q_2=kt-1}\frac{a_1^{q_1}a_2^{q_2}}{q_1!q_2!} = \\ = \tfrac{1}{ae^{aQ}}\sum_{j=0}^{(kt-1)/2}\frac{\left(Q+\frac{kt}{2}\right)^{kt-1-2j}\left(-\frac{kt}{24}\right)^j}{j!(kt-1-2j)!}.$$

Эта часть суммы дает главную часть вычета, а все остальные слагаемые попадают в остаток вида

$$\begin{cases} O\left(\frac{\left(Q+\frac{kt}{2}\right)^{kt-5}}{ae^{aQ}(kt-3)!}\right), & \text{если} \quad Q \succ (kt)^{\frac{3}{2}}, \\ O\left(\frac{kt^{2kt}\exp\left\{\left(\frac{Q}{kt}+\frac{1}{2}\right)^2\right\}}{ae^{aQ}\left(Q+\frac{kt}{2}\right)^{kt+3}}\right), & \text{если } Q \prec (kt)^{\frac{3}{2}}. \end{cases}$$

Итак, при $Q \succ (kt)^{\frac{3}{2}}$

$$\frac{1}{2\pi i}\int\limits_{\Gamma}\frac{e^{aQs}}{s}\big(F(s+1)-1\big)\mathrm{d}s = \left(\frac{1}{1-e^{-a}}\right)^{kt} - 1 - \\ -\frac{1}{ae^{aQ}}\left(\sum\frac{a_1^{q_1}a_2^{q_2}\ldots a_{kt-1}^{q_{kt-1}}}{q_1!q_2!\ldots q_{kt-1}!} + O\left(\frac{\left(Q+\frac{kt}{2}\right)^{kt-4}}{(kt-5)!}\right)\right).$$

Далее, дифференцируя по a, находим

$$\sum_{j=1}^{\infty}\frac{\mathrm{d}}{\mathrm{d}a}\left(\frac{1}{1-e^{-a}}\right)^{kt}\Big|_{a=bj} = \\ = \int\limits_{b}^{\infty}\frac{\mathrm{d}}{\mathrm{d}u}\left(\frac{1}{1-e^{-u}}\right)^{kt} = \left(\frac{1}{1-e^{-b}}\right)^{kt},$$

$$\sum_{j=1}^{\infty}\frac{\mathrm{d}}{\mathrm{d}a}\,\frac{1}{ae^{aQ}}\Big|_{a=bj} = \int\limits_{b}^{\infty}\frac{\mathrm{d}}{\mathrm{d}u}\frac{1}{ue^{uQ}} = \frac{1}{be^{bQ}}.$$

Тогда

$$\sum_{m\le Q}\frac{m\cdot\tau_{kt}(\omega^m)}{e^{bm}-1} = \left(\frac{1}{1-e^{-b}}\right)^{kt} - \\ -\frac{1}{be^{bQ}}\sum_{m=0}^{kt-1/2}\frac{\left(Q+\frac{kt}{2}\right)^{kt-1-2m}\left(-\frac{kt}{24}\right)^m}{(kt-1-2m)!\cdot m!} + R,$$

где остаток

$$R \ll \sum_{j=1}^{\infty}\frac{\mathrm{d}}{\mathrm{d}a}\left(\frac{e^{aQ\sigma-a(\sigma+1)}}{aT(1-e^{-a(\sigma+1)})^{kt}} + \frac{e^{aQ\sigma}}{aTQ|\sin aT|^{kt}} + \right. \\ \left. + \frac{\arctan\frac{T}{U}}{e^{aUQ}} + \frac{1}{ae^{aQ}}\frac{\left(Q+\frac{kt}{2}\right)^{kt-4}}{(kt-5)!}\right)\Bigg|_{a=bj}.$$

Выберем

$$T = T(a) = \frac{2\pi r + \pi/2}{a},$$

где

$$r = \left[\frac{e^{aQ\sigma+aUQ}}{\left(1-e^{-a(\sigma+1)}\right)^{kt}}\right],$$

и достаточно большое U, тогда

$$R \ll \sum_{j=1}^{\infty}\frac{\mathrm{d}}{\mathrm{d}a}\,\frac{1}{ae^{aQ}}\frac{\left(Q+\frac{kt}{2}\right)^{kt-5}}{(kt-3)!}\Bigg|_{a=bj} \ll \\ \ll \frac{1}{be^{bQ}}\frac{\left(Q+\frac{kt}{2}\right)^{kt-4}}{(kt-5)!}.$$

Аналогичным образом в общем случае мы можем получить

$$\sum_{m\le Q}\frac{m\cdot\tau_{kt}(\omega^m)}{e^{bm}-1} = \\ = \left(\frac{1}{1-e^{-b}}\right)^{kt} - \frac{1}{be^{bQ}}\sum_{m=0}^{kt-1}\frac{\left(Q+\frac{kt}{2}\right)^{kt-1-m}}{(kt-1-m)!}\times \\ \times\sum_{2q_2+\ldots+(kt-1)q_{kt-1}=m}\frac{b_2^{q_2}\ldots b_{kt-1}^{q_{kt-1}}}{q_2!\ldots q_{kt-1}!}(kt)^{q_2+\ldots+q_{kt-1}},$$

причем остатка не будет, так как мы можем U устремить к бесконечности.

Предложение доказано. □

Следствие 1. *Пусть $k, t > 0$, $Q \succ kt$, тогда*

$$\sum_{\beta:\Omega(\beta)\le Q}\frac{\Omega(\beta)\cdot\tau_k(\beta)}{e^{b\Omega(\beta)}-1} = \left(\frac{1}{1-e^{-b}}\right)^{kt} - \\ -\frac{1}{be^{bQ}}\left(\sum_{m=0}^{kt-1/2}\frac{\left(Q+\frac{kt}{2}\right)^{kt-1-2m}\left(-\frac{kt}{24}\right)^m}{(kt-1-2m)!\cdot m!} + \right. \\ \left. + O\left(\frac{\left(Q+\frac{kt}{2}\right)^{kt-4}}{(kt-5)!}\right)\right).$$

Предложение 6. *Справедливо тождество*

$$\frac{1}{2\pi i}\int\limits_{C}\frac{1}{(1-z)^{kt}}\sum_{m\le Q}\frac{m\cdot z^{-m-1}}{e^{bm}-1}dz = \\ = \sum_{\beta:\Omega(\beta)\le Q}\frac{\Omega(\beta)\cdot\tau_k(\beta)}{e^{b\Omega(\beta)}-1}.$$

Доказательство. Если m — целое число, то

$$\int_0^1 e^{2\pi i\alpha m}\mathrm{d}\alpha = \begin{cases} 1, & \text{если} \quad m = 0, \\ 0, & \text{иначе.} \end{cases}$$

Имеем

$$\sum_{\nu_1+\ldots+\nu_{kt}\le Q}\frac{1}{e^{bj(\nu_1+\ldots+\nu_{kt})}} = \\ = \sum_{m\le Q}\sum_{\nu_1=0}^{\infty}\frac{1}{e^{bj\nu_1}}\cdots\sum_{\nu_{kt}=0}^{\infty}\frac{1}{e^{bj\nu_{kt}}}\times \\ \times\int\limits_0^1 e^{2\pi i\alpha(\nu_1+\ldots+\nu_{kt}-m)}\mathrm{d}\alpha = \\ = \sum_{m\le Q}\int\limits_0^1\left(\frac{1}{1-e^{2\pi i\alpha-bj}}\right)^{kt}e^{-2\pi i\alpha m}\mathrm{d}\alpha = \\ = \int\limits_0^1\left(\frac{1}{1-e^{2\pi i\alpha-bj}}\right)^{kt}\frac{1-e^{-2\pi i\alpha(Q+1)}}{1-e^{-2\pi i\alpha}}\mathrm{d}\alpha.$$

Сделаем замену $z = e^{2\pi i\alpha - bj}$, тогда

$$\int\limits_0^1 \left(\frac{1}{1-e^{2\pi i\alpha - bj}}\right)^{kt} e^{-2\pi i\alpha m}\mathrm{d}\alpha = \frac{e^{-bjm}}{2\pi i}\int\limits_C \frac{z^{-m-1}}{(1-z)^{kt}}\mathrm{d}z,$$

где $C = C(bj)$ — контур в форме окружности с центром в 0 и радиусом $e^{-bj} < 1$.

Тогда получаем

$$\sum_{m\le Q}\frac{m\cdot\tau_{kt}(\omega^m)}{e^{bm}-1} = \sum_{j=1}^{\infty}\sum_{\nu_1+\ldots+\nu_{kt}\le Q}\frac{\nu_1+\ldots+\nu_{kt}}{e^{bj(\nu_1+\ldots+\nu_{kt})}} =$$
$$= \frac{1}{2\pi i}\int\limits_C \frac{1}{(1-z)^{kt}}\sum_{m\le Q}\frac{m\cdot z^{-m-1}}{e^{bm}-1}\mathrm{d}z.$$

Предложение доказано. □

Direct additive problem on the distribution of integer-valued random variables

G.V. Fedorov

Abstract

The subject of our attention in this paper are direct additive problems with a growing number of terms. Such problems are usually formulated in the language of probability theory, while we speak about increasing sums of random variables. We continue the research of V.P. Maslov and V.E. Nazaikinsky and consider a more general formulation of the problem than [5], namely, we admit a growing number of degrees of freedom in each dimension of the system. For this system with one linear inequality we find the asymptotic distribution of the random variable and the asymptotic behavior for the entropy. The physical interpretation of the problems under consideration is discussed in [4] - [3].

Keywords: Direct additive problems, distribution of random variables, entropy, multidimensional divisor function

Литература

1. *Hardy G. H.* Ramanujan. — Cambridge, 1940.
2. *Maslov V. P.*, *Nazaikinskii V. E.* On the Bose–Einstein distribution and Bose condensation // arXiv:0812.4885v1 [math.PR]. — 29 Dec 2008. — с. 1—25.
3. *Маслов В. П.* Бозе-конденсат в d-мерном случае, в частности при $d = 2$ и $d = 1$ // Доклады РАН. — 2012. — т. 446, № 2. — с. 145—148.
4. *Маслов В. П.* Математическое разрешение парадокса Гиббса // Матем. заметки. — 2011. — т. 89, № 2. — с. 272—284.
5. *Маслов В. П.*, *Назайкинский В. Е.* О распределении целочисленных случайных величин, связанных одним линейным неравенством. I // Матем. заметки. — 2008. — т. 83, № 2. — с. 232—263.
6. *Маслов В. П.*, *Назайкинский В. Е.* О распределении целочисленных случайных величин, связанных одним линейным неравенством. II // Матем. заметки. — 2008. — т. 83, № 3. — с. 381—401.

7. *Маслов В. П.*, *Назайкинский В. Е.* О распределении целочисленных случайных величин, связанных одним линейным неравенством. III // Матем. заметки. — 2008. — т. 83, № 6. — с. 880—898.

8. *Постников А. Г.* Введение в аналитическую теорию чисел. — Гл. ред. физ.-мат. лит. изд. “Наука”, 1971.

9. *Успенский Я. В.* Асимптотическое выражение числовых функций, встречающихся в задаче о разбиении чисел на слагаемые // Изв. Российск. АН. — 1920. — т. 14. — с. 199—218.

Свойства фактор-отображения моментов для симплектических многообразий с инвариантными лагранжевыми подмногообразиями

В.С.Жгун[1]

[1] *ФГУ ФНЦ НИИСИ РАН, Москва, Россия, E-mail: zhgoon@mail.ru*

Аннотация

В работе мы исследуем геометрию фактор отображения момента для гамильтоновых многообразий содержащих инвариантное лагранжево подмногообразие. В частности при некоторых дополнительных предположениях на особенности слоев отображения моментов показана равноразмерность фактор отображения моментов вне множества коразмерности 2. Также нами получено новое доказательство того, что малая группа Вейля G-многообразия порождена отражениями. Подчеркнем, что новое доказательство не использует теоремы о гладкой эквивариантной компактификации, а также теоремы об односвязности проективных гладких унирациональных многообразий.

Ключевые слова: гамильтоновы многообразия, лагранжевы подмногообразия, отображение моментов, малая группа Вейля.

В настоящей статье мы продолжим исследование гамильтоновых многообразий (а именно, симплектических многообразий, снабжённых действием редуктивной группы и отображением моментов), содержащих инвариантные лагранжевы подмногообразия, начатое авторами в [6]. Основным результатом работы является обобщение теоремы Ф.Кнопа [4] о равноразмерности фактор-отображения моментов для кокасательных расслоений к многообразиям с действием редуктивной группы. В этом направлении стоит упомянуть результаты, полученные Лосевым [5], о равноразмерности фактор-отображения моментов для так называемых конических гамильтоновых многообразий. Мы не будем приводить определение последнего класса многообразий, поскольку условия, накладываемые нами, имеют несколько иную природу.

Также мы дадим новое доказательство теоремы Кнопа о том, что малая группа Вейля порождается отражениями. Преимущество этого доказательство перед оригинальным в том, что оно не использует редукцию к случаю гладкой компактификации однородного пространства и теорему об односвязности проективного унирационального многообразия. Мы надеемся, что в дальнейшем наши результаты могут быть использованы при исследовании малой группы Вейля симплектических многообразий.

1. Пусть G — связная редуктивная алгебраическая группа над алгебраически замкнутым полем $\Bbbk$ нулевой характеристики. Обозначим через B борелевскую подгруппу в G, через U — унипотентный радикал B, через T — максимальный тор в B. Алгебры Ли этих и других групп мы будем обозначать соответствующими строчными готическими буквами. Отождествим пространства $\mathfrak{g}$ и $\mathfrak{g}^*$ с помощью G-инвариантной симметрической билинейной формы на $\mathfrak{g}$. Также нам понадобится группа Вейля $W = N_G(T)/T$. Напомним, что для G-многообразия X *решёткой весов* называется решетка $\Lambda(X)$, состоящая из весов всех B-полуинвариантных рациональных функций на X (ее ранг обозначим $\mathrm{rk}(X)$). Для линейных алгебраических групп $G \supset H$ и квазипроективного H-многообразия Z через $G *_H Z$ обозначим квазипроективное G-многообразие, полученное как фактор $G \times Z$ по следующему действию H: $(g, z) \mapsto (gh^{-1}, hz)$.

Пусть M — гладкое алгебраическое G-многообразие с симплектической формой ω. Многообразие M называется *гамильтоновым*, если существует такое G-эквивариантное отображение $\Phi : M \to \mathfrak{g}^*$, называемое *отображением моментов*, что для $\xi \in \mathfrak{g}$, рассматриваемого как линейная функция на $\mathfrak{g}^*$, косой градиент его обратного образа $\Phi^*\xi \in \Bbbk[M]$ является полем скоростей ξ_*. Это эквивалентно условию: $\langle d_p\Phi(\nu), \xi\rangle = \omega(\xi p, \nu)$, $\forall p \in M$, $\nu \in T_pM$, $\xi \in \mathfrak{g}$, где ξp — вектор скорости ξ в точке p. Для подгруппы $H \subset G$ обозначим через Φ_H композицию $M \to \mathfrak{g}^* \to \mathfrak{h}^*$ (ограничение отображения моментов на $\mathfrak{h}$). Также нас будет интересовать факторизованное отображение моментов $\Phi : M \to \mathfrak{g}^*/\!\!/G \cong \mathfrak{t}^*/W$, полученное как композиция отображения моментов и последующего категорного фактора π_G по действию группы G.

Нам необходимо напомнить следующие результаты, доказанные в работе [6] (см. также [8]), являющиеся краеугольным камнем исследовании геометрии симплектических многообразий с инвариантными лагранжевыми многообразиями. Эти результаты для удобства читателя мы сформулируем в виде одной теоремы.

Теорема 1. *Пусть M — гамильтоново G-многообразие, $S \subset M$ — G-инвариантное лагранжево подмногообразие. Пусть $P \supset B$ — нормализатор типичной B-орбиты в S, а P_0 — нормализатор типичной U-орбиты в S. Тогда $\overline{\Phi(M)} = G\mathfrak{p}_0^\perp$, причем существует такая компонента $\mathcal{W}$ многообразия $\Phi^{-1}(\mathfrak{p}_0^\perp)$, что $G\mathcal{W} = M$, а морфизм действия $G *_P \mathcal{W} \to M$ конечен в общей точке.*

Сформулируем один из основных результатов работы.

Теорема 2. *Пусть M — гамильтоново G-многообразие, обладающее G-инвариантным лагранжевым квазиаффинным подмногообразием $S \subset M$. Предположим, что множество особенностей многообразия $\mathcal{W}$ имеет коразмерность по крайней мере 2. Тогда вне G-инвариантного подмногообразия в M коразмерности $\geqslant 2$ отображение $\Phi_{/\!\!/G}$ равноразмерно.*

Воспользовавшись этим результатом, мы получим доказательство следующей теоремы Ф.Кнопа [4].

Теорема 3. *Малая группа Вейля W_X для квазиаффинного G-многообразия X порождена отражениями.*

Отметим, что наше доказательство не требует теоремы о гладкой эквивариантной компактификации, а также теоремы об односвязности проективных гладких унирациональных многообразий.

Замечание 1. *Пусть $P = P_{\mathrm{u}} \leftthreetimes L$ — разложение Леви, где $L \supset T$. Тогда из теоремы о локальной структуре (см. например [3]) следует, что $L_0 = L \cap P_0$ содержит $[L, L]$, а также, что $P_{\mathrm{u}} \leftthreetimes L_0$ — разложение Леви для P_0. Заметим также, что $\Lambda(S)$ отождествляется с решеткой характеров тора $A = P/P_0 = T/T_0$, где $T_0 = T \cap P_0$. Отождествляя $\mathfrak{g}$ и $\mathfrak{g}^*$ с помощью инвариантной билинейной формы, мы можем также отождествить $\mathfrak{a}$ и $\mathfrak{a}^*$. Также заметим, что $\mathcal{W}$ является неприводимой компонентой многообразия $\Phi^{-1}(\mathfrak{u}^\perp)$.*

Лемма 1. *Пусть* $\pi_G : \mathfrak{g}^* \to \mathfrak{g}^*/\!\!/G \cong \mathfrak{t}^*/W$ *— морфизм факторизации. Ограничение* π_G *на* $\mathfrak{u}^\perp \cong \mathfrak{b}$ *может быть представлено как композиция проекции на* $\mathfrak{t}^*$ *с последующей факторизацией по действию* W.

Доказательство. Действительно, в замыкании G-орбиты элемента $\xi \in \mathfrak{u}^\perp$ содержится элемент $\lim_{t\to 0} \lambda(t)\xi\lambda(t)^{-1} \in \mathfrak{t}^*$, где $\lambda(t)$ — однопараметрическая подгруппа, соответствующая элементу из внутренности положительной камеры Вейля, отвечающей выбору борелевской подалгебры $\mathfrak{b} \supset \mathfrak{t}$. □

Замечание 2. *Из вышесказанного несложно получить, что образ* $\Phi_{/\!\!/G}(M)$ *после нормализации отождествляется с* $\mathfrak{a}^*/W(\mathfrak{a}^*)$, *где* $W(\mathfrak{a}^*) = N_G(\mathfrak{a}^*)/Z_G(\mathfrak{a}^*)$. *Таким образом,* $\dim \Phi_{/\!\!/G}(M) = \mathrm{rk}(S)$.

2. Перейдем к доказательству теоремы 2. Для этого выберем набор B-полуинвариантных рациональных функций $f_i \in \Bbbk(S)^{(B)}_{\chi_i}$, веса χ_i которых линейно независимы и порождают решетку весов $\Lambda(S)$. Воспользовавшись теоремой о локальной структуре, как и в [8, §5], получаем набор P-полуинвариантных рациональных функций $F_i \in \Bbbk(M)^{(P)}_{\chi_i}$ с теми же весами. Заметим, что ограничения функций F_i на $\mathcal{W}$ корректно определены и не обращаются тождественно в нуль, поскольку $S \subset \mathcal{W}$. Легко показать (см. [8, §5]), что векторные поля косых градиентов ∇F_i касаются многообразия $\mathcal{W}$ в схемном смысле, то есть задают дифференцирования пучка регулярных функций, сохраняющие пучок идеалов многообразия $\mathcal{W}$.

Заметим, что в силу G-инвариантности морфизма и Теоремы 2, для доказательства равноразмерности $\Phi_{/\!\!/G}$ достаточно ограничиться слоями $\Phi^{-1}_{/\!\!/G}(\Phi_{/\!\!/G}(x))$ для точек $x \in \mathcal{W}$. Обозначим $\Phi_{\mathcal{W}} := \Phi_{/\!\!/G}|_{\mathcal{W}}$.

Более того, поскольку $P_u^- P$ плотно в G и P нормализует $\mathcal{W}$, имеем

$$\Phi^{-1}_{/\!\!/G}(\Phi_{/\!\!/G}(x)) = G\Phi^{-1}_{\mathcal{W}}(\Phi_{\mathcal{W}}(x)) =$$

$$= \overline{P_u^-(\Phi^{-1}_{\mathcal{W}}(\Phi_{\mathcal{W}}(x)))}.$$

Тем самым

$$\dim \Phi^{-1}_{/\!\!/G}(\Phi_{/\!\!/G}(x)) \leqslant \dim(\Phi^{-1}_{\mathcal{W}}(\Phi_{\mathcal{W}}(x))) + \dim P_u^-. \tag{1}$$

Следующая лемма утверждает, что множество особых точек многообразия $\mathcal{W}$ ведет себя специальным образом при отображении моментов (напомним, что компонента $\mathcal{W}$ приведена).

Лемма 2. *Пусть* $\mathcal{W}^{sing}$ *— множество особых точек* $\mathcal{W}$. *Тогда* $\Phi(\mathcal{W}^{sing})$ *не содержит целиком ни один слой морфизма факторизации* $\mathfrak{g}^* \to \mathfrak{g}^*/\!\!/G$.

Доказательство. Поскольку $\mathcal{W}$ — компонента $\Phi^{-1}_{P_0}(0)$ прообраза нуля для ограничения отображения моментов на $\mathfrak{p}_0$, касательное пространство в точке $m \in \mathcal{W}$ описывается как косоортогональное дополнение к орбите $(\mathfrak{p}_0 m)^\angle$. Множество точек, где морфизм Φ не является гладким является множеством точек m, для которых $\dim(\mathfrak{p}_0 m)^\angle > \dim \mathcal{W}$. Таким образом, $\mathcal{W}^{sing}$ содержится в множестве точек, где размерность P_0–орбит общего положения строго меньше $\dim P_u$.

Пусть $m \in \mathcal{W}^{sing}$ — точка общего положения, а $\xi = \Phi(m) \in \mathfrak{p}_0^\perp$. Рассмотрим разложение Жордана $\xi = \xi_s + \xi_n$, где $\xi_n \in \mathfrak{z}_{\mathfrak{p}_u}(\xi_s)$. Действуя группой $Ad(P_u)$ на ξ, можно считать, что также выполнено включение $\xi_s \in \mathfrak{a}$ (что следует из сопряженности максимальных торов). Тогда $P_0\xi \subset \xi_s + \mathfrak{p}_u$.

Нам понадобится предложение о присоединенных орбитах, в формулировке которого участвуют обозначения, не связанные с остальным текстом статьи.

Предложение 1. *[1, Sec. 5.1, 5.5] Рассмотрим произвольную параболическую подгруппу* P *в* G, *с подгруппой Леви* L *и унипотентном радикалом* P_u. *Пусть* $O_{\mathfrak{l}}$ *— нильпотентная присоединенная орбита* L *в* $\mathfrak{l}$. *Пусть* $x \in \mathfrak{z}(\mathfrak{l})$ *— произвольный элемент центра* $\mathfrak{l}$. *Тогда существует единственная* G*-орбита* $O_{\mathfrak{g}}$ *пересекающая* $x + O_{\mathfrak{l}} + \mathfrak{p}_u$ *по открытому плотному подмножеству. Пересечение* $O_{\mathfrak{g}} \cap (x + O_{\mathfrak{l}} + \mathfrak{p}_u)$ *составляет одну* P*-орбиту. Выполнено следующее равенство* $\mathrm{codim}_{\mathfrak{g}} O_{\mathfrak{g}} = \mathrm{codim}_{\mathfrak{l}} O_{\mathfrak{l}}$.

Также для точки общего положения $z \in x + O_{\mathfrak{l}} + \mathfrak{p}_u$ стабилизатор z в $\mathfrak{p}_u^-$ тривиален, а подпространство $[\mathfrak{p}_u^-, z]$ трансверсально к $[\mathfrak{l}, z] + \mathfrak{p}_u$. Для неприводимых компонент стабилизаторов выполнено равенство $(P_z)^0 = (G_z)^0$.

Таким образом, в аффинном подпространстве $\xi_s + \mathfrak{p}_u$ содержится единственная плотная P-орбита. Поскольку $\dim P_0 m < \dim P_u$, замыкание множества $\Phi(\mathcal{W}^{sing}) \cap (\xi_s + \mathfrak{p}_u)$ строго содержится в $\xi_s + \mathfrak{p}_u$. Что и требовалось.

□

Лемма 3. *В множестве гладких точек $\mathcal{W}$ найдется подмножества коразмерности $\geqslant 2$, такое что для всех гладких точек x, лежащих вне этого подмножества имеем $\operatorname{codim}_{\mathcal{W}}(\Phi_{\mathcal{W}}^{-1}(\Phi_{\mathcal{W}}(x))) \geqslant \operatorname{rk}(S)$.*

Из леммы 3 непосредственно следует доказательство теоремы 2. Для этого заметим, что G-разнесение множества не уменьшает его коразмерность, поэтому выкидывая G-инвариантное подмножество коразмерности $\geqslant 2$ из M, можно считать, что морфизм $\Phi_{\mathcal{W}}$ равноразмерен. Из неравенства (1) и леммы 3 следует, что

$$\dim \Phi_{/\!/G}^{-1}(\Phi_{/\!/G}(x)) \leqslant \dim \mathcal{W} - \operatorname{rk}(S) + \dim P_u =$$

$$= \dim M - \operatorname{rk}(S).$$

Теорема о полунепрерывности размерности слоев морфизма дает обратную оценку. Это завершает доказательство теоремы 2 .

Для доказательства леммы 3 нам понадобятся некоторые факты про скобку Пуассона. Отметим, что эти утверждения являются алгебраической интерпретацией стандартной конструкции гамильтоновой редукции.

Лемма 4. *Пусть $F \in \mathcal{O}_{\mathcal{W}}$ росток функций на $\mathcal{W}$. И пусть $\widetilde{F}$ некоторое его поднятие до ростка пучка $\mathcal{O}_M$. Тогда образ поля $(\nabla \widetilde{F})_x$ для $x \in \mathcal{W}$ при композиции отображений $d\Phi_T$ не зависит от выбора поднятия.*

Доказательство. Действительно, два поднятия различаются на росток $F_{\mathcal{J}} \in \mathcal{J}(U)$. Пусть $\xi \in \mathfrak{t}$, тогда $\langle d\Phi((\nabla F_{\mathcal{J}})_x), \xi \rangle = \{\xi, F_{\mathcal{J}}\} \in \mathcal{J}(U)$, где последнее включение следует из того, что $\mathcal{J}(U)$ порожден обратными образами фунций на $\mathfrak{p}_0$, тождества Лейбница и $[\mathfrak{t}, \mathfrak{p}_0] \subset \mathfrak{p}_0$. □

Лемма 5. *На подпучке $\mathfrak{p}_0$-инвариантных функций пучка $\mathcal{O}_{\Phi_{P_0}^{-1}(0)}$ существует скобка Пуассона, полученная ограничением на $\Phi_{P_0}^{-1}(0)$ скобки Пуассона на M.*

Доказательство. Пучок идеалов $\mathcal{J}$ этого многообразия порожден образом $\mathfrak{p}_0$ при отображении Φ^*. заметим, что из тождества Лейбница и из того, что $\mathfrak{p}_0$ является подалгеброй Ли следует, что $\{\mathcal{J}, \mathcal{J}\} \subset \mathcal{J}$. Более того для ростка $f \in \mathcal{O}_M$ $\mathfrak{p}_0$-инвариантной функции на $\Phi^{-1}(\mathfrak{p}_0^{\perp})$ и $\xi \in \mathfrak{p}_0$ выполнено $\{\xi, f\} = \xi f \in \mathcal{J}$. Из вышесказанного получаем, что на кольце $\mathcal{O}^{\mathfrak{p}_0}_{\Phi_{P_0}^{-1}(0)}$ корректно определена скобка Пуассона, полученная ограничением скобки Пуассона на M. □

В следующей лемме из коммутативной алгебры мы воспользуемся стандартными обозначениями, не связанными с остальным текстом. Несмотря на то, что эта лемма содержится в работе Д.Б.Каледина, мы приведем ее доказательство несколько отличное по форме от [2].

Лемма 6. *Пусть $\mathfrak{q}$ — ассоциированный изолированный примарный идеал в разложении идеала I кольца A. И пусть ∂ — дифференцирование кольца A в себя, такое что $\partial(I) \subset \mathfrak{q}$, тогда $\partial(\mathfrak{q}) \subset \mathfrak{q}$.*

Доказательство. Пусть $\mathfrak{p}$ — простой идеал ассоциированный с $\mathfrak{q}$. Согласно [9, теор. 8, §5] мы имеем следующую характеризацию изолированного ассоциированного примарного идеала:

$$\mathfrak{q} = \{x \in A | \ \exists y \notin \mathfrak{p}, xy \in I\}$$

Дифференцируя включение $xy \in I$ и умножая равенство на y получаем:

$$xy\partial y + y^2 \partial x \in \mathfrak{q}.$$

Откуда $y^2 \partial x \in \mathfrak{q}$. Учитывая, что $y^2 \notin \mathfrak{p}$ получаем $\partial x \in \mathfrak{q}$. □

Следствие 1. *Пусть* $\{\cdot,\cdot\}$ *— скобка Пуассона кольца* A*, а* I *— идеал, для которого* $\{I,I\}\subset\mathfrak{q}$ *для некоторого ассоциированного изолированного примарного идеала* $\mathfrak{q}$*, тогда* $\{\mathfrak{q},\mathfrak{q}\}\subset\mathfrak{q}$.

Следствие 2. *Скобку Пуассона на* $\mathcal{O}_M$ *можно ограничить на* $\mathcal{O}_{\mathcal{W}}^{\mathfrak{p}_0}$.

Лемма 7. *Пусть дифференцирование* ∂ *алгебры* A *сохраняет идеал* $I\subset A$*, тогда оно сохраняет и его радикал* $\mathrm{rad}(I)$.

Доказательство. Пусть $f\in\mathrm{rad}(I)$, т.е. $f^n\in I$, для некоторого n. Рассмотрим

$$\partial^n(f^n)=(\partial f)^n+$$

$$+\sum_{i_0+i_1+\ldots+i_k=n}a_{i_0i_1\ldots i_k}f^{i_0}(\partial^{i_1}f)\ldots(\partial^{i_k}f).$$

Поскольку $\partial^n(f^n)\in I$ и все слагаемые последней суммы принадлежат $\mathrm{rad}(I)$ получаем $(\partial f)^n\in I$, откуда $\partial f\in\mathrm{rad}(I)$. □

3. Приведем доказательство леммы 3 в несколько шагов. Из леммы 1 следует, что ограничение $\Phi_{/\!/G}$ на $\mathcal{W}$ может быть представлено как композиция отображения моментов Φ, проекции на $\mathfrak{t}^*$ и факторизации по действию группы W. Тем самым, размерность слоев $\Phi_{\mathcal{W}}$ такая же, как у отображения Φ_T.

Без ограничения общности можно считать, что многообразие $\mathcal{W}$ гладко и, в частности, нормально. Если множество неопределенности функции $F_i|_{\mathcal{W}}$ является дивизором в $\mathcal{W}$, то в силу нормальности $\mathcal{W}$ можно доопределить функцию $F_i|_{\mathcal{W}}$, так что множество неопределенности будет имеет коразмерность $\geqslant 2$. Поскольку нас интересует равноразмерность морфизма $\Phi_{\mathcal{W}}$ для точек $x\in\mathcal{W}$ вне множества коразмерности $\geqslant 2$, мы можем считать, что точка x принадлежит не более чем одному простому дивизору $D\subset\mathcal{W}$ из множества дивизоров нулей-полюсов функций $F_i|_{\mathcal{W}}$. В случае, когда $x\in D$ мы полагаем, что x гладкая точка D. Также корректно определена кратность функции $F_i|_{\mathcal{W}}$ в дивизоре D. Деля или перемножая функции F_i (и тем самым, не изменяя линейное пространство, порожденное их характерами χ_i), без ограничения общности можно считать, что $x\in\mathcal{W}$ принадлежит дивизору нулей функции F_1, который мы обозначим через D, а остальные F_i не имеют нулей и полюсов в D. Росток функции $F_i|_{\mathcal{W}}$ в окрестности точки, где ее значение конечно можно поднять до ростка регулярной функции $\widetilde{F}_i\in\mathcal{O}_M$. По лемме 4 образ $\Phi_T(\nabla\widetilde{F}_i)$ не будет зависеть от поднятия, поэтому для краткости мы положим $\nabla F_i:=\nabla\widetilde{F}_i$.

Шаг 1. Равноразмерность слоев морфизма $\Phi_{\mathcal{W}}$ *вне дивизоров нулей-полюсов функций* $F_i|_{\mathcal{W}}$. Для необходимой оценки на размерность слоя отображения Φ_T в гладкой точке $x\in\mathcal{W}$, мы покажем, что существует набор векторных полей порождающих в T_xM подпространство размерности $\mathrm{rk}(X)$, трансверсальное к касательному пространству в x к слою отображения Φ_T. Непосредственно из определений имеем $d_x\Phi_T(\nabla F_i)=F_i(x)\chi_i$, где, допуская вольность речи, мы обозначаем через $\chi_i\in\mathfrak{t}^*$ дифференциал соответствующего характера тора T. Отсюда мы получаем, что в случае, когда все F_i не имеют ни нулей ни полюсов в точке x, образы $F_i(x)\chi_i$ векторов $(\nabla F_i)_x$ под действием дифференциала $d\Phi_T$ порождают все пространство $\mathfrak{a}^*$, что дает искомую трансверсальность.

Далее, можно считать, что вся неприводимая компонента слоя $\Phi_{\mathcal{W}}^{-1}(\Phi_{\mathcal{W}}(x))$, размерность которой нас интересует, целиком лежит в D, поскольку иначе все сводится к шагу 1.

Шаг 2. Случай касания векторными полями дивизора $D\cap\mathcal{W}$. Предположим, что все ∇F_i (для $i>2$) касаются дивизора $D\cap\mathcal{W}$ в его гладких точках. Тогда для точки x, лежащей в $D\cap\mathcal{W}$, существует подпространство размерности $\dim\mathfrak{a}^*-1$ в $T_x(D\cap\mathcal{W})$, порожденное векторами $(\nabla F_i)_x$ (для $i=2,\ldots,\dim\mathfrak{a}^*$), на котором дифференциал $d_x\Phi_T$ имеет нулевое ядро. Тогда из точной последовательности для касательных пространств имеем:

$$0\to T_x\Phi_{\mathcal{W}}^{-1}(\Phi_{\mathcal{W}}(x))\to T_x(D\cap\mathcal{W})\to T_x\Phi_{\mathcal{W}}(D\cap\mathcal{W}),$$

откуда

$$\dim\Phi_{\mathcal{W}}^{-1}(\Phi_{\mathcal{W}}(x))\leqslant\dim T_x\Phi_{\mathcal{W}}^{-1}(\Phi_{\mathcal{W}}(x))\leqslant$$

$$\leqslant \dim T_x(D \cap \mathcal{W}) - (\dim \mathfrak{a}^* - 1) = \dim \mathcal{W} - \dim \mathfrak{a}^*,$$

что дает искомую оценку сверху на размерность слоя.

Шаг 3. Равноразмерность слоев морфизма $\Phi_{\mathcal{W}}$, в случае, когда не все поля ∇F_i касаются неприводимой компоненты $D_{\mathcal{W}}$ дивизора $D \cap \mathcal{W}$. Можно считать, что D локально задается уравнением $F_D = 0$ (для некоторой рациональной функции). Положим $F_1 = F_D^k \widetilde{F}_1$, где $\widetilde{F}_1$ не обращается тождественно в нуль на D. Предположим, что одно из векторных полей ∇F_j, например ∇F_2, не касается дивизора D. Тогда функция $\{F_D, F_2\} = \langle dF_D, \nabla F_2 \rangle$ не равна нулю тождественно на D. Рассмотрим

$$\widetilde{F}_2 := \{\ldots\{\{F_1, \underbrace{F_2\}F_2\}\ldots F_2\}}_{k} =$$

$$= k!\widetilde{F}_1\{F_D, F_2\}^k + F_D F',$$

где функция F' не имеет полюсов в дивизоре D. Ясно, что $\widetilde{F}_2$ не обращается тождественно в нуль на дивизоре D и является P-полуинвариантной с весом $\chi_1 + k\chi_2$. Веса функций F_i для всех $i > 1$ вместе с весом функции $\widetilde{F}_2$ линейно независимы и порождают все $\mathfrak{a}^*$. К тому же эти функции не обращаются в нуль на D, что дает искомый набор векторных полей как в шаге 1. Это доказывает лемму 3, а также завершает доказательство теоремы 2.

Замечание 3. *Теорему 2 можно усилить в случае, если $\operatorname{codim}_{\mathcal{W}} \mathcal{W}^{sing} = 1$. Однако, нужно потребовать, чтобы выполнялось следующее условие. Для любой компоненты D многообразия $\mathcal{W}^{sing}$ найдется множество B-полуинвариантных функций определенных в общей точке дивизора D (возможно имеющих там полюс) веса которых составляют базис $\Lambda_{\mathbb{Q}}(X)$ и такое, что для любых двух функций f_1, f_2 из этого набора с дивизорами нулей-полюсов содержащими D в носителе, найдутся $n_1, n_2 \in \mathbb{Z}$, такие что $f_1^{n_1}/f_2^{n_2}$ не обращается в нуль в общей точке D.*

Для завершения доказательства равноразмерности слоев морфизма $\Phi_{\mathcal{W}}$ в точках $\mathcal{W}$ вне множества коразмерности 2 достаточно доказать ее в общей точке множества $\mathcal{W}^{sing}$. Тем самым, достаточно доказать утверждение о равноразмерности лишь для гладких точек многообразия $\mathcal{W}^{sing}$. Для этого нам понадобится следующая лемма.

Лемма 8. *Пусть $\partial \in Der(\mathcal{O}_Y, \mathcal{O}_Y)$ дифференцирование пучка $\mathcal{O}_Y$ многообразия Y. Тогда ∂ сохраняет пучок идеалов $\mathcal{I}_{Y^{sing}}$ множества особых точек многообразия Y.*

Доказательство. Согласно лемме 7, достаточно доказать утверждение для любого идеала определяющего множество Y^{sing}.

Вопрос является локальным, поэтому будем считать, что n-мерное многообразие Y задано в аффинном пространстве $\mathbb{A}^N$ (с координатами x_i) как множество нулей идеала $I_Y = (f_1, \ldots, f_m)$. Заметим, что тогда дифференцирование $\partial : \Bbbk[Y] \to \Bbbk[Y]$ продолжается до дифференцирования $\partial : \Bbbk[x_1, \ldots, x_N] \to \Bbbk[x_1, \ldots, x_N]$ (для этого в качестве значений ∂ на x_i возьмем произвольные прообразы $\partial(x_i) \in \Bbbk[Y]$ в $\Bbbk[x_1, \ldots, x_N]$).

Мы покажем, что ∂ сохраняет идеал многообразия нулей дифференциальных n-форм, который определяет подсхему особых точек, а затем воспользуемся леммой 7.

Идеал, задающий множество особенностей Y, — это идеал J_Y, порожденный $n \times n$ минорами якобиевой матрицы $J = \left(\frac{\partial f_i}{\partial x_j}\right)_{i,j}$. Иными словами, J_Y порожден коэффициентами при базисных мономах $dx_{j_1} \wedge \ldots \wedge dx_{j_n}$ форм вида $df_{i_1} \wedge \ldots \wedge df_{i_n}$, для всех наборов $j_1, \ldots, j_n$. Покажем, что если дифференцирование ∂ сохраняет I_Y, то оно сохраняет идеал $I_Y + J_Y$.

Заметим, что дифференцирование ∂ продолжается до дифференцирования алгебры дифференциальных форм (которое называется производной Ли). Пусть ξ — векторное поле на $\mathbb{A}^n$, соответствующее дифференцированию $\tilde{\partial}$. Считая без ограничения общности, что $\{i_1, \ldots, i_n\} =$

$\{1,\dots,n\}$, применим ∂ к форме $\omega = df_1 \wedge \dots \wedge df_n$ двумя способами. Обозначая через $J_{j_1,\dots,j_n}$ минор матрицы J, составленный из первых n строк и столбцов $j_1,\dots,j_n$, получаем

$$\partial\omega = \sum_{j_1,\dots,j_n} (\partial J_{j_1,\dots,j_n}) dx_{j_1} \wedge \dots \wedge dx_{j_n} +$$

$$+ \sum_{i,j_1,\dots,j_n} J_{j_1,\dots,j_n} dx_{j_1} \wedge \dots \wedge d(\partial x_{j_i}) \wedge \dots \wedge dx_{i_n}$$

Заметим, что коэффициенты при $dx_{i_1} \wedge \dots \wedge dx_{i_n}$ (базисных формах) в разложении форм из второй суммы принадлежат идеалу J_Y.

С другой стороны, по формуле Картана имеем $\partial\omega = d\imath_\xi\omega + \imath_\xi d\omega$, где $\imath_\xi$ — оператор подстановки векторного поля ξ в дифференциальную форму. Учитывая, что ω замкнута и $\imath_\xi df_i = \partial f_i = \sum_{k=1}^m h_{ik} f_k$, получаем, что производная Ли равна:

$$\partial\omega = d\imath_\xi\omega = d(\textstyle\sum_{i=1}^n (-1)^{i-1} (\imath_\xi df_i) df_1 \wedge \dots \wedge df_n) =$$

$$= \textstyle\sum_{i=1}^n (-1)^{i-1} \sum_{j=1}^m (h_{ij} df_j \wedge df_1 \wedge \dots \widehat{df_i} \dots \wedge df_n +$$

$$+ f_j dh_{ij} \wedge df_2 \dots \widehat{df_i} \dots \wedge df_n).$$

Заметим, что коэффициенты при базисных формах в разложении форм из первого слагаемого принадлежат J_Y, а коэффициенты в разложении форм из второго слагаемого принадлежат I_Y. Приравнивая в двух выражениях для $\partial\omega$ коэффициенты при базисных формах, получаем, что $\partial J_{i_1,\dots,i_n}$ принадлежат идеалу $I_Y + J_Y$,что и требовалось. □

Из леммы 8 следует, что векторные поля ∇F_i касаются множества $\mathcal{W}^{sing}$ в подмножестве его гладких точек. Применяя рассуждения из шага 2 к множеству $\mathcal{W}^{sing}$, получаем требуемое.

3 Теорема 1 позволяет ввести группу Вейля гамильтонова многообразия с инвариантными лагранжевыми подмногообразиями следующим стандартным образом (ср. [3],[7]). Предположим, что мы находимся в симплектически стабильном случае, то есть общий элемент $\Phi(M)$ — полупрост, или что эквивалентно $Z_G(\mathfrak{a}) = L$. В этом случае P_u действует свободно на общей точке из $\mathfrak{a}^*$ и многообразие $G *_P \mathcal{W}$ бирационально изоморфно $G/L \times \Sigma$, где Σ — специальным образом выбранная компонента связности $\Phi^{-1}(\mathfrak{a}^*)$. Из того, что существует морфизм $G *_P \mathcal{W} \to M$, являющийся рациональным накрытием, как и в работе [7, Sec.5] получаем, что M бирационально изоморфно $G *_{N_M} \Sigma$, для некоторой подгруппы N_M, такой что $L \subset N_M \subset N_G(\mathfrak{a}^*)$. Группу $W_M = N_M/L \subset W(\mathfrak{a}^*)$ назовем малой группой Вейля гамильтонова многообразия M. Указанный выше бирациональный изоморфизм дает отображение $\Psi : M \to \mathfrak{a}^*/W(\mathfrak{a}^*)$, являющееся разложением Штейна отображения моментов. Для квазиаффинного G-многообразия X под малой группой Вейля W_X понимается малая группа Вейля кокасательного расслоения T^*X. В [3] показано, что для общий слой отображения Ψ связен. Там же показано как свести случай произвольного X к квазиаффинному.

Из теоремы 2 следует следующая теорема Ф.Кнопа [4].

Теорема 4. *Малая группа Вейля W_X для квазиаффинного G-многообразия X порождена отражениями.*

Лемма 9. *Рассмотрим квазиаффинные G-многообразия X и Y, а также G-эквивариантный, доминантный, конечный в общей точке морфизм $f : X \to Y$. Тогда $W_X = W_Y$.*

Доказательство. Переходя к открытым G-инвариантным подмножествам мы можем считать, что $f : X \to Y$ сюрьективен и этален. Легко видеть из конечости отображения на общих U-орбитах, а также B-орбитах, что нормализаторы общих B-орбит на X и на Y совпадают $P_X = P_Y$. Более того, индуцированное отображение $T^*X \to T^*Y$ и индуцированное отображение $\mathcal{N}(X) \to \mathcal{N}(Y)$ конормальных расслоений к типичным U-орбитам также имеет степень $\deg f$. Рассмотрим следующую

коммутативную диаграмму конечных в общей точке морфизмов:

$$\begin{tikzcd} G *_P \mathcal{N}(X) \arrow[r] \arrow[d] \arrow[dr] & T^*X \arrow[d] \\ G *_P \mathcal{N}(Y) \arrow[r] & T^*Y \end{tikzcd}$$

где вертикальные отображения имеют степень $\deg f$, а степени горизонтальных отображений равны $|W_X|$ и $|W_Y|$ соответственно. Вычисляя степень отображения отвечающего диагональной стрелке двумя способами получаем, что $|W_X| = |W_Y|$. Поскольку W_X является подфактором в W_Y (см. [4]), получаем, что W_X совпадает с W_Y.

□

Доказательство теоремы 4. Предположим противное. Пусть W_X^r — нормальная подгруппа, порожденная отражениями из W_X. Группа $\overline{W} = W_X/W_X^r$ действует без отражений на факторе $\mathfrak{a}^*/W_X^r$, который является линейным пространством по теореме Шевалле-Шепарда-Тодда. Следовательно множество точек $\mathfrak{a}^*/W_X^r$ неподвижных относительно какого-либо элемента из $W_X \setminus W_X^r$ имеет коразмерность $\geqslant 2$. Прообраз в $\mathfrak{a}^*$ дополнения к этому множеству обозначим через $\mathfrak{a}^r$ (которое W_X-инвариантно). Рассмотрим следующую коммутативную диаграмму:

$$\begin{tikzcd} p_1^{-1}(T_x^*X) \arrow[r] \arrow[d] & T^*X \times_{\mathfrak{a}^*/W_X} \mathfrak{a}^*/W_X^r \arrow[r, "p_2"] \arrow[d, "p_1"] & \mathfrak{a}^*/W_X^r \arrow[d] \\ T_x^*X \arrow[r] & T^*X \arrow[r, "\Psi"] & \mathfrak{a}^*/W_X \end{tikzcd}$$

Положим $\widehat{T}_X = T^*X \times_{\mathfrak{a}^*/W_X} \mathfrak{a}^*/W_X^r$. Морфизм $p_1 : \widehat{T}_X \to T^*X$ является конечным, он также неразветвлен над подмножеством $R := \Psi^{-1}(\mathfrak{a}^r/W_X)$. Дополнение к этому множеству в T^*X имеет коразмерность $\geqslant 2$ поскольку по теореме 2 морфизм Ψ равноразмерен вне множества коразмерности 2. Для точки общего положения $x \in X$, пересечение T_x^*X и R также имеет коразмерность $\geqslant 2$ в T_x^*X (что следует из вычисления размерности общего слоя ограничения на R проекции на X). Это показывает, что алгебраическая фундаментальная группа $T_x^*X \setminus R$ тривиальна и прообраз $p_1^{-1}(T_x^*X \setminus R)$ является объединением компонент, изоморфных $T_x^*X \setminus R$. Поскольку p_1 конечно, замыкание любой такой компоненты изоморфно отображается на T_x^*X (поскольку последнее многообразие нормально). Более того, число этих компонент равно $|\overline{W}|$.

Рассмотрим композицию $\widehat{T}_X \to T^*X \to X$. Пусть $\widetilde{X}$ — спектр нормализации $\mathbb{K}[X]$ в $\mathbb{K}(\widehat{T}_X)$. Тогда общие слои отображения $q : \widehat{T}_X \to \widetilde{X}$ — неприводимы, а морфизм $\widetilde{p} : \widetilde{X} \to X$ конечен и G-эквивариантен. Легко видеть, что для точки общего положения $x \in X$ объединение неприводимых компонент многообразия $p_1^{-1}(T_x^*X)$ дизъюнктно и отождествляется с $\sqcup_{\widetilde{p}(\widetilde{x})=x} q^{-1}(\widetilde{x})$. Отсюда также следует, что конечный морфизм $\widetilde{p} : \widetilde{X} \to X$ имеет степень $|\overline{W}|$. Переходя к G-инвариантному открытому подмножеству в X, можно считать, что $\widetilde{p}$ этально, и в частности $T^*\widetilde{X} \cong \widetilde{p}^*T^*X$. Последнее влечет наличие G-эквивариантного морфизма $\widehat{T}_X \to T^*\widetilde{X}$. Степень отображения композиции $\widehat{T}_X \to T^*\widetilde{X} \to T^*X$ равна $|\overline{W}|$. Покольку это степень отображения $T^*\widetilde{X} \to T^*X$, то мы получаем, что отображение $\widehat{T}_X \to T^*\widetilde{X}$ имеет степень 1 и, в силу нормальности $T^*\widetilde{X}$, является изоморфизмом. Поскольку общие слои отображения $T^*\widetilde{X} \to \mathfrak{a}^*/W_X^r$ неприводимы, имеем $W_{\widetilde{X}} = W_X^r$. По лемме 9 получаем $W_{\widetilde{X}} = W_X$. □

On geometry of quotient moment map for special hamiltonian varieties

V.S.Zhgoon

Abstract

We study geometry of quotient moment map for Hamiltonian varieties containing invariant lagrangian subvariety. In particular under additional assumptions on the singularities of fibers of the moment map we show that the fibers of the quotient moment map are equidimensional in the complement of the subset of codimension 2. Also we get a new proof of the fact that little Weyl group of G-variety is generated by reflections. We emphasize that a new proof does not use the theorem on smooth equivariant compactification and the theorem on simplly-connectedness of smooth unirational varieties.

Keywords: hamiltonian varieties, lagrangian subvarieties, moment map, little Weyl group.

Литература

1. *Collingwood D. H.*, *McGovern W. M.* Nilpotent orbits in semisimple Lie algebra: an introduction. — CRC Press, 1993.
2. *Kaledin D. B.* Normalization of a Poisson algebra is Poisson // Proceedings of the Steklov Institute of Mathematics. — 2009. — т. 264, № 1. — с. 70—73.
3. *Knop F.* The asymptotic behavior of invariant collective motion // Inventiones mathematicae. — 1994. — т. 116, № 1. — с. 309—328.
4. *Knop F.* Weylgruppe und Momentabbildung // Inventiones mathematicae. — 1990. — т. 99, № 1. — с. 1—23.
5. *Losev I.* On fibers of algebraic invariant moment maps // Transformation Groups. — 2009. — т. 14, № 4. — с. 887.
6. *Timashev D. A.*, *Zhgoon V. S.* Hamiltonian actions on symplectic varieties with invariant Lagrangian subvarieties // arXiv preprint arXiv:1109.5239. — 2011.
7. *Vinberg È. B.* Equivariant symplectic geometry of cotangent bundles // Moscow Mathematical Journal. — 2001. — т. 1, № 2. — с. 287—299.
8. *Жгун В. С.*, *Тимашёв Д. А.* Симплектические многообразия с инвариантными лагранжевыми подмногообразиями // Доклады Академии наук. т. 443. — Наука. 2012. — с. 418—418.
9. *Зарисский О.*, *Самюэль П.* Коммутативная алгебра, т. 1, ИЛ // Москва. — 1963.

Об одном неравенстве для положительно определенных функций и множество представителей вычетов по двум модулям

Ю. Н. Штейников[1]

[1] *ФГУ ФНЦ НИИСИ РАН, Москва, Россия, E-mail: yuriisht@gmail.com*

Аннотация

В данной статье исследуются числа в заданном интервале, которые представляют два множества вычетов по двум различным модулям. Выводятся некоторые явные верхние оценки на множество этих совместных вычетов на заданном интервале. Эти оценки являются правильными по порядку. В доказательстве используется одно неравенство для положительно определенных сеточных функций [1]. Данная работа представляет собой несколько расширенный вариант статьи [3]. В отличие от работы [3] основной результат доказывается несколько другим способом.

Ключевые слова: вычеты, сравнение, решето

1. Введение

Для натурального q через $\mathbb{Z}_q$ мы будем обозначать кольцо вычетов по модулю q. Рассмотрим такую задачу. Пусть p_1, p_2 - достаточно большие натуральные числа, $p_1 < p_2, A := p_2/p_1$. Пусть также имеются множества

$$G_1 \subseteq \mathbb{Z}_{p_1}, G_2 \subseteq \mathbb{Z}_{p_2}.$$

По определению положим

$$\overline{G_1} := \{n \in \mathbb{N} : n \in G_1 \pmod{p_1}\};$$

$$\overline{G_2} := \{n \in \mathbb{N} : n \in G_2 \pmod{p_2}\}.$$

Пусть также дано натуральное z, и мы хотим нетривиально оценить сверху

$$|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|.$$

Оценка этой величины, когда $p_1 = q_1^2, p_2 = q_2^2$ и q_1, q_2 являются простыми числами, а G_1, G_2 являются мультипликативными подгруппами групп $\mathbb{Z}_{p_1}^*$ и $\mathbb{Z}_{p_2}^*$ размеров $q_1 - 1$ и $q_2 - 1$ соответственно, рассматривался в работе [1]. Оценка размера $[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}$ была нужна для задачи об оценке первого натурального a, не обладающего свойством делимости частного Ферма на простое число. Отметим, если p_1 и p_2 являются взаимно простыми, то с помощью китайской теоремы об остатках получаем:

$$|[1, p_1 p_2] \bigcap \overline{G_1} \bigcap \overline{G_2}| = |G_1||G_2|.$$

Нам понадобятся такие величины. Для целого k обозначим через $f_1(k)$ - число решений сравнения относительно $x_1, x_2 \in G_1$

$$x_1 - x_2 \equiv kp_2 \pmod{p_1}.$$

Введем по определению

$$N_1 := \sum_{0 \le k \le \frac{z}{A}} f_1(k).$$

Аналогично, через $f_2(k)$ обозначим число решений сравнения относительно $x_1, x_2 \in G_2$

$$x_1 - x_2 \equiv kp_1 \pmod{p_2}. \tag{1}$$

И

$$N_2 := \sum_{0 \le k \le z} f_2(k). \tag{2}$$

Наша цель - оценить размер $|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|$ через N_1 и N_2. В работе [1] , когда множества G_1, G_2 являлись подгруппами, величины N_1, N_2 были явно оценены. В работе понадобится также одно неравенство для положительно-определенных сеточных функций. Этому неравенству мы отводим следующий раздел статьи.

2. Об одном специальном неравенстве для положительно-определенных функций.

$f \in C(\mathbb{R})$ называют положительно-определенной если для любого конечного вектора коэффициентов $c_a \in \mathbb{C}, a \in X$ выполнено неравенство

$$\sum_{a,b \in X} c_a \overline{c_b} f(a-b) \ge 0. \tag{3}$$

Для периодичных, симметричных, сеточных функций $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{R}$ положительно-определенными функциями называются неотрицательные функции, у которых коэффициенты Фурье неотрицательные. Иными словами, для всякого $a \in \mathbb{Z}/n\mathbb{Z}$ должно выполняться неравенство:

$$\sum_{0 \le x \le n-1} f(x) e_n(-ax) \ge 0. \tag{4}$$

Следующее неравенство было доказано Д.В. Горбачевым [2]. Мы его формулируем в несколько ослабленной форме.

Теорема 1. *Пусть f - положительно определенная сеточная функция. Тогда справедливо неравенство*

$$\sum_{|k| \le 2m} f(k) \le C \sum_{|k| \le m} f(k) \tag{5}$$

где C - некоторая абсолютная постоянная и может быть взята равной π^2.

На основе этого утверждения мы выведем такое утверждение.

Предложение 1. *Существует такая абсолютная константа $C > 0$, что для любого n имеет место неравенство:*

$$\sum_{0 \le k \le 2n} f_1(k) \le C \sum_{0 \le k \le n} f_1(k) \tag{6}$$

Доказательство. Для удобства обозначим

$$q_1 := \frac{p_1}{\gcd(p_1, p_2)}, q_2 := \frac{p_2}{\gcd(p_1, p_2)}.$$

Функция f_1 является четной и неотрицательной. Легко видеть, что для любого k верно $f_1(k + q_1) = f_1(k)$. Поэтому можно считать, что она задана на кольце вычетов по модулю q_1. Покажем теперь, что f_1 является положительно определенной функцией. Иными словами убедимся, что ее дискретное преобразование Фурье неотрицательно. Отметим сразу, что для неотрицательных, положительно определенных функций справедливость неравенства (6) следует из работы [2].

Остается убедиться в неотрицательности преобразования Фурье. Пусть

$$e_q(k) := exp(2\pi i k/q). \tag{7}$$

Известно, что для любого целого x:

$$\sum_{0 \le a \le q-1} e_q(ax) = q, \tag{8}$$

только если

$$x \equiv 0 \pmod{p}, \tag{9}$$

а в остальных случаях

$$\sum_{0\le x\le q-1} e_q(ax) = 0. \qquad (10)$$

Поэтому мы можем написать,

$$f_1(k) =$$
$$= \frac{1}{p_1}\sum_{x_1,x_2\in G_1}\sum_{0\le a\le p_1-1} e_{p_1}(a(x_1-x_2-kp_2)) =$$
$$= \frac{1}{p_1}\sum_{0\le a\le p_1-1} e_{p_1}(-akp_2)\times$$
$$\times \sum_{x_1\in G_1} e_{p_1}(ax_1)\sum_{x_2\in G_1} e_{p_1}(-ax_2).$$

Обозначим $S(a,G_1)=\sum_{x\in G_1} e_{p_1}(ax)$. Тогда

$$f_1(k) = \frac{1}{p_1}\sum_{0\le a\le p_1-1} |S(a,G_1)|^2 e_{p_1}(-akp_2) =$$
$$= \frac{1}{p_1}\sum_{0\le a\le p_1-1} |S(a,G_1)|^2 e_{q_1}(-akq_2) =$$
$$= \frac{1}{p_1}\sum_{0\le a\le q_1-1} L(a) e_{q_1}(-akq_2),$$

где

$$L(a) := \sum_{0\le t\le p_1-1, t\equiv a \pmod{q_1}} |S(t,G_1)|^2 \ge 0.$$

Через q_2^* обозначим обратный элемент к элементу $q_2 \pmod{q_1}$ в кольце вычетов по модулю q_1. Таким образом, мы получили

$$f_1(k) = \frac{1}{p_1}\sum_{0\le a\le q_1-1} L(-aq_2^*) e_{q_1}(ak).$$

Отсюда следует, что преобразование Фурье для f_1 неотрицательно. Тем самым мы показали справедливость неравенства (6). Тем самым мы показали справедливость предложения 1.

□

В следующей главе мы выведем некоторые известные оценки на искомое множество совместных вычетов с использованием одного результата из [1].

3. Предварительные оценки на множество совместных вычетов

Теперь приведем утверждение из работы [1] и далее покажем, какие оценки на величину $|[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}|$ можно получить с помощью оценок на N_1 и N_2. Введем для начала некоторые определения.

Пусть Λ_1 и Λ_2 есть непустые конечные множества. Для множества $L\subseteq\Lambda_1\times\Lambda_2$ пусть

$$L(x,.) := \{y\in\Lambda_2 : (x,y)\in L\};$$

$$L(.,y) := \{x\in\Lambda_1 : (x,y)\in L\}.$$

Всюду в работе выражение $a(n)\ll b(n)$ (обозначение И.М. Виноградова) будет означать, что для всех n выполнено неравенство $|a(n)|\le cb(n)$ для некоторой абсолютной константы $c>0$.

Лемма 1. *Для любого множества $L\subseteq\Lambda_1\times\Lambda_2$ существуют подмножество $B\subseteq L$ и натуральные k_1 и k_2, что справедливы неравенства:*

1) $|B|\ge|L|/2$;
2) $|B(x,.)|\le k_1$ для любого $x\in\Lambda_1$;
3) $|B(.,y)|\le k_2$ для любого $y\in\Lambda_2$;
4)$\sum_{x\in\Lambda_1:|B(x,.)|>\frac{k_1}{2}}|B(x,.)|\gg\frac{L}{\log(|\Lambda_1|+|\Lambda_2|)}$;
5)$\sum_{y\in\Lambda_2:|B(.,y)|>\frac{k_2}{2}}|B(.,y)|\gg\frac{L}{\log(|\Lambda_1|+|\Lambda_2|)}$.

Из этой леммы следует такое утверждение.

Предложение 2. *Предположим даны достаточно большие p_1,p_2,z причем $\gcd(p_1,p_2)=1$, $A:=\frac{p_2}{p_1}>1$,$z<p_2$. Пусть имеются множества $G_1\subseteq\mathbb{Z}_{p_1}, G_2\subseteq\mathbb{Z}_{p_2}$ и соответственно заданы величины N_1,N_2. Тогда справедлива оценка:*

$$|[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}|\ll\max\{N_1,N_2\}\log p_1.$$

Доказательство. Пусть $\Lambda_1:=\mathbb{Z}_{p_1},\Lambda_2:=\mathbb{Z}_{p_2}$. Каждому элементу

$$m\in[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}$$

биективно сопоставим пару в $\mathbb{Z}_{p_1}\times\mathbb{Z}_{p_2}$ по правилу $(m \pmod{p_1}, m \pmod{p_2})$ Обозначим множество таких пар через L.

Используя Лемму 1 для множества L, мы получаем существование такого множества

$$B \subseteq [1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2},$$

натуральных k_1, k_2 и абсолютной константы $c > 0$, что справедливы следующие утверждения:

1) для каждого вычета по модулю p_1 имеется не более k_1 чисел из B, представляющих этот вычет.

2) для каждого вычета по модулю p_2 имеется не более k_2 чисел из B, представляющих этот вычет.

3) имеется не менее $\frac{c|[1,p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|}{k_1 \log p_1}$ вычетов по модулю p_1, каждый из которых содержит не менее $k_1/2$ чисел из B, представляющих этот вычет.

4) имеется не менее $\frac{c|[1,p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|}{k_2 \log p_1}$ вычетов по модулю p_2, каждый из которых содержит не менее $k_2/2$ чисел из B, представляющих этот вычет.

Будем считать, что k_2 не меньше k_1. Если какой-то класс вычетов по модулю p_2 содержит не менее $k_2/2$ чисел из B, то у нас имеется не менее $k_2^2/8$ пар $(a, b) \in B \times B$ таких, что

$$a \geq b; a \equiv b \pmod{p_2}$$

Теперь суммируя по всем таким вычетам по модулю p_2, можно получить не менее $\frac{c|[1,p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|k_2}{8 \log p_1}$ пар $(a, b) \in B \times B$, что

$$a - b = lp_2, 0 \leq l \leq \frac{z}{A}$$

Так как среди элементов B имеется не более k_1 чисел, представляющих любой фиксированный вычет по модулю p_1, то мы заключаем, что имеется не менее $\frac{c|[1,p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|k_2}{8k_1 \log p_1}$ решений сравнения

$$x_1 - x_2 \equiv lp_2 \pmod{p_1}, 0 \leq l \leq \frac{z}{A}.$$

Но число решений последнего сравнения есть величина N_1. Получаем,

$$\frac{|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|k_2}{k_1 \log p_1} \ll N_1.$$

Значит, в случае $k_2 \geq k_1$ следует неравенство

$$|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}| \ll N_1 \log p_1.$$

Так как мы не знаем, какое из чисел k_1, k_2 является наибольшим, то получаем заявленную оценку

$$|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}| \ll \max\{N_1, N_2\} \log p_1.$$

Тем самым предложение 2 доказано. □

4. Основное утверждение

Теперь мы готовы сформулировать и доказать первую теорему в этой работе.

Теорема 2. *Предположим даны числа p_1, p_2, A, z, $p_1 < p_2$, множества G_1, G_2 и соответственно заданы величины N_1, N_2. Тогда справедлива оценка:*

$$|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}| \ll (N_1 N_2)^{1/2}.$$

Доказательство. Так как числа $1, \ldots, p_1$ пробегают полную систему вычетов по модулю p_1, то множеству G_1 можно естественным образом взаимно однозначно сопоставить множество чисел $\overline{G_1} \bigcap [1, p_1]$. Теперь каждый элемент $g \in \overline{G_1} \bigcap [1, p_1]$ отобразим в $\mathbb{Z}_{p_2}$ по правилу

$$g \to g \pmod{p_2}.$$

Обозначим образ этого отображения через $G_1', G_1' \subseteq \mathbb{Z}_{p_2}$. Тем самым у нас имеется взаимно-однозначное соответствие между тремя множествами

$$G_1 \to \overline{G_1} \bigcap [1, p_1] \to G_1' \qquad (11)$$

Таким образом нам необходимо оценить сверху

$$\sum_{0 \leq k \leq z-1} |G_2 \bigcap (G_1' + kp_1)|.$$

Прежде всего заметим, что достаточно доказать теорему для $z \leq q_2$. Действительно, пусть $z > q_2$.

Обозначим $K := z/q_2 > 1$. Пользуясь тем, что

$$G_1' + q_2 p_1 = G_1'$$

получаем

$$\sum_{0\le k\le z-1}|G_2\bigcap G_1'+kp_1|\ll$$

$$K\sum_{0\le k\le q_2-1}|G_2\bigcap G_1'+kp_1|.$$

Заметим, что для любого l

$$f_1(l+q_1)=f_1(l), f_2(l+q_2)=f_2(l).$$

Поэтому,

$$\sum_{0\le k\le \frac{z}{A}} f_1(k)=$$

$$=\sum_{0\le k\le Kq_1} f_1(k)\gg K\sum_{0\le k\le q_1-1} f_1(k).$$

Аналогично,

$$\sum_{0\le k\le z} f_2(k)\gg K\sum_{0\le k\le q_2-1} f_2(k).$$

Поэтому, из этих неравенств убеждаемся, что теорему достаточно доказать для

$$z\le q_2.$$

Пусть $z\le q_2$.

Разобьем множество $\mathbb{Z}_{p_2}$ на множества $\{\Delta_i\}, 1\le i\le \gcd(p_1,p_2)$ следующим образом.

Определим для $1\le i\le \gcd(p_1,p_2)$ наборы

$$\Delta_i:=\{i+lp_1\}_{0\le l\le q_2-1}.$$

Они не пересекаются и покрывают все $\mathbb{Z}_{p_2}$.

Теперь каждый Δ_i еще разобьем на непересекающиеся множества $\Delta_{i,j}$. Для $1\le j\le J:=[\frac{q_2}{z}]$ по определению полагаем

$$\Delta_{i,j}:=\{i+lp_1\}_{(j-1)z\le l\le jz-1}.$$

Если $\bigcup_{1\le j\le J}\Delta_{i,j}$ не покрывает весь Δ_i, то положим

$$\Delta_{i,J+1}:=\Delta_i\setminus\bigcup_{1\le j\le J}\Delta_{i,j}.$$

Определим множество

$$S_{i,j}:=\Delta_{i,j}\bigcap G_2.$$

Далее введем множество

$$s_{i,j}:=\bigcup_{0\le l\le z-1}\{g\in G_1':g+lp_1\in\Delta_{i,j}\}.$$

Тогда

$$|[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}|\le\sum_{i,j}|S_{i,j}||s_{i,j}|.$$

Отметим, что $g+kp_1, 0\le k\le z-1$ пробегает прогрессию длины z с шагом p_1 и поэтому каждый $g\in G_1'$ может принадлежать не более трем множествам $s_{i,j}$. Отсюда следует, что

$$\sum_{i,j}s_{i,j}\ll|G_1|;\sum_{i,j}S_{i,j}=|G_2|.$$

Далее

$$\sum_{i,j}|S_{i,j}||s_{i,j}|\le(\sum_{i,j}|S_{i,j}|^2)^{1/2}(\sum_{i,j}|s_{i,j}|^2)^{1/2}.$$

Сперва оценим первую сумму :

$$\sum_{i,j}|S_{i,j}|^2=$$

$$=\sum_{i,j}|\{(a,b)\in G_2\times G_2:a,b\in\Delta_{i,j}\}|\le$$

$$\le|\{(a,b)\in G_2\times G_2:a-b\equiv kp_1\pmod{p_2},$$

$$-z+1\le k\le z-1\}|\ll N_2.$$

Теперь оценим вторую сумму:

$$\sum_{i,j}|s_{i,j}|^2=\sum_{i,j}|\{(a,b)\in G_1'\times G_1':a,b\in s_{i,j}\}|.$$

Так как каждый элемент $g\in G_1'$ может принадлежать не более чем трем множествам $s_{i,j}$, то каждая пара $(a,b)\in G_1'\times G_1'$ которая подсчитывается в последней сумме может быть подсчитана не более трех раз для разных $s_{i,j}$. Значит,

$$\sum_{i,j}|s_{i,j}|^2\ll$$

$$\ll|\{(a,b)\in G_1'\times G_1':\exists(i,j):a,b\in s_{i,j}\}|.$$

Поймем, что значит условие $a,b\in s_{i,j}$ для некоторых i,j. Это означает, что для некоторых $0\le k,k'\le z-1$ выполнено

$$a+kp_1, b+k'p_1\in s_{i,j}.$$

Из этого условия следует, что

$$a, b \in G_1' \times G_1' :$$

$$a - b \equiv kp_1 \pmod{p_2}, -2z+2 \le k \le 2z-2.$$

В самом начале мы строили взаимно-однозначное соответствие (2) между G_1 и G_1'. Для каждого $a \in G_1'$ обозначим через $f(a)$ его прообраз в G_1. Можно увидеть, что если

$$a, b \in G_1' \times G_1' :$$

$$a - b \equiv kp_1 \pmod{p_2}, -2z+2 \le k \le 2z-2$$

то

$$f(a), f(b) \in G_1 \times G_1 :$$

$$: f(a) - f(b) \equiv kp_2 \pmod{p_1},$$

$$-2z/A \le k \le 2z/A.$$

Поэтому мы заключаем, что

$$\sum_{i,j} |s_{i,j}|^2 \ll \sum_{0 \le k \le \frac{2z}{A}} f_1(k).$$

Пользуясь неравенством (6), мы получаем

$$\sum_{0 \le k \le \frac{2z}{A}} f_1(k) \ll \sum_{0 \le k \le \frac{z}{A}} f_1(k),$$

то есть $\sum_{0 \le k \le \frac{2z}{A}} f_1(k) \ll N_1$. Таким образом:

$$|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}| \le \sum_{i,j} |S_{i,j}||s_{i,j}| \ll$$

$$\ll (\sum_{i,j} |S_{i,j}|^2)^{1/2} (\sum_{i,j} |s_{i,j}|^2)^{1/2} \ll (N_1 N_2)^{1/2}.$$

Этим мы завершаем доказательство Теоремы 2. □

5. Оптимальность найденных оценок

Докажем еще одно утверждение, которое показывает некоторую точность оценки в Теореме 2.

Теорема 3. *Пусть целые параметры* $p, m_1, m_2, z, l \to \infty$, *причем*

$$zm_1 < p/10, zm_2 < pl/10,$$

$$\sqrt{\frac{\max\{m_1, m_2\}}{\min\{m_1, m_2\}}} = o(z) \qquad (12)$$

Тогда существуют подмножества

$$G_1 \subseteq \mathbb{Z}_p, G_2 \subseteq \mathbb{Z}_{p+1}$$

такие, что выполнены следующие условия:

1) $|G_1| \asymp m_1, |G_2| \asymp m_2$,

2) число решений сравнения относительно x_1, x_2, n

$$x_1 - x_2 \equiv n \pmod{p}, 0 \le n \le z; x_1, x_2 \in G_1$$

есть $O(m_1)$.

3) число решений сравнения относительно x_1, x_2, n

$$x_1 - x_2 \equiv n \pmod{p+1}, 0 \le n \le z; x_1, x_2 \in G_2$$

есть $O(lm_2)$.

4) величина

$$|[1, pz] \bigcap \overline{G_1} \bigcap \overline{G_2}|$$

по порядку больше чем $(m_1 m_2)^{1/2}$.

Замечания

1)Пусть для примера p_1 и p_2 взаимно просты и $p_1 \asymp p_2$ и пусть $zm > p_1 l'$, где l' какая-то растущая величина при $p_1 \to \infty$. Тогда можно показать, что для любого подмножества $G_1 \subseteq \mathbb{Z}_{p_1}, |G_1| = m$ число решений сравнения относительно x_1, x_2, n

$$x_1 - x_2 \equiv np_2 \pmod{p_1}, 0 \le n \le z; x_1, x_2 \in G_1$$

будет иметь по порядку не меньше $l'm$ решений. Поэтому в условии Теоремы 3 мы требуем условия $zm_1 < p/10, zm_2 < pl/10$.

2)Пусть $p_1 \asymp p_2$ и

$$z \ll \sqrt{\frac{\max\{m_1, m_2\}}{\min\{m_1, m_2\}}}.$$

Так как для любого целого k справедлива оценка

$$|[kp_1+1,(k+1)p_1]\bigcap\overline{G_1}\bigcap\overline{G_2}|\ll$$

$$\ll\min\{m_1,m_2\},$$

то

$$|[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}|\ll$$

$$\ll z\min\{m_1,m_2\}\ll(m_1m_2)^{1/2}.$$

Поэтому условие

$$\sqrt{\frac{\max\{m_1,m_2\}}{\min\{m_1,m_2\}}}=o(z)$$

также является необходимым.

Доказательство. Мы можем считать, что l по порядку меньше чем m_1,m_2 а также считать справедливость соотношения

$$l\sqrt{\frac{\max\{m_1,m_2\}}{\min\{m_1,m_2\}}}=o(z).$$

Для удобства обозначим

$$m:=\min\{m_1,m_2\}.$$

Каждое из $\mathbb{Z}_p$ и $\mathbb{Z}_{p+1}$ разобьем на подмножества и на них определим G_1 и G_2.

Пусть для $1\le i\le[p/z]$

$$\delta_i:=\{(i-1)z+1\pmod p,\dots$$

$$\dots,iz\pmod p\}\bigcap\mathbb{Z}_p$$

и быть может

$$\delta_{[p/z]+1}:=\mathbb{Z}_p\setminus\bigcup_{1\le i\le[p/z]}\delta_i.$$

Тем самым, $\mathbb{Z}_p=\bigcup_i\delta_i$. Из условия (3) следует, что всего множеств $\{\delta_i\}$ не меньше $10m_1$

Так же разобьем $\mathbb{Z}_{p+1}$ на множества γ_i. Пусть для $1\le i\le[\frac{p+1}{z}]$

$$\gamma_i:=\{(i-1)z+1\pmod{p+1},\dots$$

$$\dots,iz\pmod{p+1}\}\bigcap\mathbb{Z}_{p+1}$$

и быть может

$$\gamma_{[\frac{p+1}{z}]+1}:=\mathbb{Z}_{p+1}\setminus\bigcup_{1\le i\le[\frac{p+1}{z}]}\gamma_i.$$

Мы получили $\mathbb{Z}_{p+1}=\bigcup_i\gamma_i$. Из условия (3) следует, что всего множеств $\{\gamma_i\}$ не меньше $\frac{10m_2}{l}$.

Определим теперь G_1,G_2. Пусть для $1\le i\le[\frac{m}{l}]$

$$G_1\bigcap\delta_i:=\{(i-1)z+1\pmod p,\dots$$

$$\dots,(i-1)z+\left[\sqrt{\frac{m_1l}{m}}\right]\pmod p\},$$

$$G_2\bigcap\gamma_i:=\{iz-\left[l\sqrt{\frac{m_2}{m}}\right]+1\pmod{p+1},\dots$$

$$\dots,iz\pmod{p+1}\}.$$

Для $[\frac{m}{l}]+1\le i\le[\frac{m}{l}]+m_1$

$$G_1\bigcap\delta_i:=\{(i-1)z+1\pmod p\}.$$

Для $[\frac{m}{l}]+1\le i\le[\frac{m}{l}]+[\frac{m_2}{l}]$

$$G_2\bigcap\gamma_i:=\{iz-l+1\pmod{p+1},\dots$$

$$\dots,iz\pmod{p+1}\}.$$

Так как $[\frac{m}{l}]+m_1<2m_1$, а всего множеств $\{\delta_i\}$ не меньше $10m_1$, поэтому мы можем так определить G_1. Аналогично $[\frac{m}{l}]+[\frac{m_2}{l}]\le\frac{2m_2}{l}$ то мы можем так определить и G_2.

Убедимся, что G_1,G_2 имеют размеры порядка m_1 и m_2 соответственно. Действительно

$$|G_1|=\sum_{1\le i\le[\frac{m}{l}]+m_1}|\delta_i\bigcap G_1|=$$

$$=\left[\frac{m}{l}\right]\left[\sqrt{\frac{m_1l}{m}}\right]+m_1\asymp m_1.$$

Аналогично проверяется что и $|G_2|$ имеет порядок m_2.

Теперь убедимся, что число решений сравнения относительно x_1,x_2,n

$$x_1-x_2\equiv n\pmod{p+1},0\le n\le z;x_1,x_2\in G_2$$

есть величина $O(lm_2)$.

Действительно, пусть сравнение выполнено для некоторого $0 \le n \le z$ и элемент $x_2 \in \gamma_i$ для некоторого i. Получаем,

$$x_1 \equiv x_2 + n \pmod{p+1}, 0 \le n \le z.$$

Тогда элемент x_1 обязан принадлежать либо γ_i, либо γ_{i+1}. Если обозначить

$$v_i := |G_2 \bigcap \gamma_i|,$$

то число рассматриваемых сравнений оценивается величиной

$$\sum_{1 \le i \le [\frac{m}{l}]+[\frac{m_2}{l}]} v_i(v_i + v_{i+1}) \le$$

$$\le 2l^2 \frac{m_2}{m}\frac{m}{l} + 2l^2 \frac{m_2}{l} = O(lm_2).$$

Аналогично можно показать, что число решений сравнения относительно x_1, x_2, n

$$x_1 - x_2 \equiv n \pmod{p}, 0 \le n \le z; x_1, x_2 \in G_1$$

есть величина $O(m_1)$.

Наконец осталось оценить снизу размер $[1, pz] \bigcap \overline{G_1} \bigcap \overline{G_2}$. Обозначим также $u_i := |G_1 \bigcap \delta_i|$ По условию (3) следует, что $u_i, v_i = o(z)$. Поэтому

$$|[1, pz] \bigcap \overline{G_1} \bigcap \overline{G_2}| \ge$$

$$\ge \sum_{1 \le i \le [\frac{m}{l}]-1} v_i u_{i+1} \gg l\sqrt{\frac{m_2}{m}}\sqrt{\frac{m_1 l}{m}}\frac{m}{l}.$$

Последняя величина по порядку больше, чем $(m_1 m_2)^{1/2}$. Этим мы завершаем доказательтсво Теоремы 3. $\square$

On one inequality for double positive definite functions and joint representatives of residues by two different modulos.

Yu. N. Shteinikov

Abstract

In this paper, we study numbers in a given interval that represent two sets of residues with respect to two different modules. Some explicit upper estimates for the size of the set of joint representatives that are correct in order are derived. In the proof, one inequality for positive-definite functions [2] is used. This paper is a somewhat extended version of the article [3]. Unlike the work [3] the main result is proved in a somewhat different way.

Keywords: residues, congruence, sieve

Литература

1. On the divisibility of Fermat quotients / J. Bourgain [и др.] // The Michigan Mathematical Journal. — 2010. — т. 59, № 2. — с. 313—328.
2. *Горбачев Д. В.* Некоторые неравенства для дискретных положительно определенных функций // Известия ТулГУ. Естественные науки. — 2015. — т. 83, № 2. — с. 5—12.
3. *Штейников Ю. Н.* О множестве совместных представителей вычетов по двум модулям. // Тр. МИАН. — 2015. — т. 290. — с. 202—210.

О цепочках вложенных подпространств и многообразиях полных флагов

В.С. Жгун[1]

[1] *ФГУ ФНЦ НИИСИ РАН, Москва, Россия, E-mail: zhgoon@mail.ru*

Аннотация

В работе описана новая конструкция, дающая вложение специального вида многообразия полных флагов произвольной редуктивной группы. А именно, для произвольной редуктивной группы строятся вложения реализующие многообразие обобщенных полных флагов в качестве орбиты цепочки попарно вложенных подпространств специального вида, граф вложения которых является диаграммой Дынкина, снабженной дополнительными данными. Эта конструкция дает новые реализации вложений даже для классических групп. В частности, для SL_n показано, что цепочка вложенных подпростанств фиксированной размерности и графом вложений полностью определяет классический флаг.

Ключевые слова: редуктивная алгебраическая группа, обобщенное многообразие полных флагов, система корней, неприводимое представление

Пусть G — редуктивная алгебраическая группа над алгебраически замкнутым полем $\Bbbk$ нулевой характеристики, а B — борелевская подгруппа в G (максимальная связная разрешимая подгруппа). В случае группы GL_n подгруппа B является группой треугольных матриц UT_n и является стабилизатором полного флага в $\Bbbk^n$, то есть цепочки подпространств $0 \subset \langle e_1 \rangle \subset \langle e_1, e_2 \rangle \ldots \subset \langle e_1, \ldots, e_n \rangle$, где вектора $e_1, \ldots, e_n \in \Bbbk^n$ образуют базис. Как хорошо известно, для группы G и ее борелевской подгруппы B существует вложение $G \subset GL_n$ для некоторого n, такое что $B = UT_n \cap G$. Таких вложений может быть много, однако для классических групп SO_n и SP_n можно реализовать борелевскую подгруппу как стабилизатор флага изотропных подпространств (то есть тех, на которых билинейная форма тождественно обращается в нуль). Цель настоящей заметки дать аналогичную конструкцию для произвольной группы G в терминах диаграмм Дынкина. Однако в конструкции будут рассмотрены не только флаги подпространств, а цепочки вложенных подпространств, графы вложений которых отвечают диаграммам Дынкина. Все основные определения и понятия, связанные с редуктивными алгебраическими группами, борелевскими и параболическими подгруппами и системами корней, содержатся в следующих источниках [3],[2],[1].

Далее будем считать, что G — проста. Зафиксируем максимальный тор T в B, группа Вейля которого обозначается через $W := N_G(T)/T$. Пусть Δ, Δ^+, Π — система корней, система положительных корней и система простых корней, соответствующие этому выбору. Для простого корня $\alpha \in \Pi$

обозначим через π_α соответствующий фундаментальный вес, а через s_α соответствующее отражение. Для доминантного веса ω через $V(\omega)$ обозначим неприводимое представление группы G с соответствующим старшим весом. Обозначим через P_α параболическую подгруппу, стабилизирующую точку $\langle v_{\pi_\alpha}\rangle \in \mathbb{P}(V(\pi_\alpha))$, где v_{π_α} — вектор старшего веса π_α. (Для подмножества в векторном пространстве с помощью $\langle . \rangle$ мы обозначаем его линейную оболочку. Для линейного пространства V' через $[V']$ обозначим соответствующую точку в грассманиане.) Пусть L_α — подгруппа Леви группы P_α, содержащая T. Системой простых корней для группы L_α является $\Pi \setminus \alpha$.

Наша цель построить цепочку вложенных подпространств стабилизатором которой будет группа B. Зафиксируем простой корень β. Для всех $\alpha \in \Pi$ рассмотрим набор подпространств $\langle P_\alpha v_{\pi_\beta}\rangle$ пространства $V(\pi_\beta)$. Заметим, что система корней $\Pi \setminus \alpha$ может быть разложимой. Рассмотрим неприводимую подсистему $\Pi_{\widehat{\alpha},\beta}$ в системе простых корней $\Pi \setminus \alpha$ содержащую корень β (то есть подсистему простых корней, соответствующую компоненте связности диаграммы Дынкина с выкинутой вершиной α, содержащей β). Обозначим также через $L_{\widehat{\alpha},\beta}$ соответствующую подгруппу Леви (положим, что $L_{\widehat{\beta},\beta} := T$). Ориентируем диаграмму Дынкина так, чтобы все пути шли к концевым вершинам от вершины β. Это ориентированный граф является графом вложений для подгрупп $L_{\widehat{\alpha},\beta}$ и тем самым он является графом вложений для подпространств

$$\langle P_\alpha v_{\pi_\beta}\rangle = \langle L_{\widehat{\alpha},\beta} v_{\pi_\beta}\rangle.$$

Чтобы показать последнее равенство, рассмотрим разложение $P_\alpha = L_{\widehat{\alpha},\beta} L_{\widehat{\alpha},\widehat{\beta}} (P_\alpha)_u$, где $L_{\widehat{\alpha},\widehat{\beta}}$ подгруппа Леви соотвествующая компонентам диаграммы Дынкина системы $\Pi \setminus \alpha$ не содержащим β, а $(P_\alpha)_u$ — унипотентный радикал P_α. Далее заметим, что $L_{\widehat{\alpha},\widehat{\beta}}$ и $(P_\alpha)_u$ действуют тривиально на $\langle v_{\pi_\beta}\rangle$.

Теорема 1. *Группа B является стабилизатором системы подпространств $\langle P_\alpha v_{\pi_\beta}\rangle$ для $\alpha \in \Pi$ в пространстве $V(\pi_\alpha)$.*

Доказательство. Поскольку $B = \cap_{\alpha\in\Pi} P_\alpha$ достаточно показать, что P_α является стабилизатором подпространства $\langle P_\alpha v_{\pi_\beta}\rangle$. Очевидно, что P_α стабилизирует это подпространство, к тому же, подгруппа P_α не содержится ни в какой собственной подгруппе в G. Поэтому необходимо показать только то, что подпространство $\langle P_\alpha v_{\pi_\beta}\rangle$ не совпадает с пространством $V(\pi_\beta)$.

Лемма 1. *Пусть $\Delta \subset V$ — неразложимая система корней, и $v \in V$ — произвольный вектор. Тогда в Δ найдется базис пространства V, состоящий из корней не ортогональных v.*

Доказательство. Предположим, что корни из Δ не ортогональные v порождают собственное подпространство V'. Возьмем вектор из $\alpha \in \Delta$ ортогональный v, такой что $\alpha \notin V'$. Если существует корень β не ортогональный v и α, то, как следует из классификации двумерных систем корней, линейная комбинация β и α является корнем не пропорциональным ни α ни β. Этот корень не ортогонален v и не принадлежит V', что противоречит выбору V'. Таким образом, все корни $\alpha \notin V'$ ортогональны к V', что противоречит неразложимости системы корней Δ. □

Из леммы следует, что найдутся вектора $\gamma \in \Delta$ не ортогональные π_β, порождающие векторное пространство весов тора T. Пространство $V(\pi_\beta)$ будет содержать вектора $s_\gamma v_{\pi_\beta}$ с весами $s_\gamma \pi_\beta = \pi_\beta - c_\gamma \gamma$ и весом π_β, линейная оболочка которых совпадает со всем пространством весов. Поскольку веса подпространства $\langle P_\alpha v_{\pi_\beta}\rangle$ лежат в $\pi_\beta + \sum_{\gamma\in\Pi_{\widehat{\alpha},\beta}} c_\gamma \gamma$, оно не совпадает с $V(\pi_\beta)$. □

Пример $G = GL(V)$, где $V = \Bbbk^{n+1}$. В этом случае $\Lambda^i V$ $(1 \leqslant i \leqslant n)$ является фундаментальным представлением со старшим вектором $e_1 \wedge \ldots \wedge e_i$. Параболическая группа P_i — группа блочно-треугольных матриц с центральными блоками $i \times i$ и $(n+1-i) \times (n+1-i)$, образующими подгруппу Леви $GL_i \times GL_{n-i+1}$.

В случае представления $\Bbbk^{n+1}$ применение параболических подгрупп P_i к вектору e_1 дает стандартный флаг. В случае представления $\Lambda^m \Bbbk^{n+1}$ мы имеем набор подпространств $\langle P_i e_1 \wedge \ldots \wedge e_m \rangle$ (размерность которого равна n_i), образующих следующую цепочку вложенных подпространств:
$e_1 \wedge \Lambda^{m-1} V \supset \ldots \supset e_1 \wedge \ldots \wedge e_i \wedge \Lambda^{m-i} V \supset \ldots \supset e_1 \wedge \ldots \wedge e_m \subset \ldots \subset \Lambda^m \langle e_1, \ldots, e_j \rangle \subset \ldots \subset \Lambda^m \langle e_1, \ldots, e_n \rangle$.

Заметим, что если у нас дано условие $[x] \in G[\langle P_i e_1 \wedge \ldots \wedge e_m \rangle] \subset Gr(n_i, \Lambda^m)$, то есть мы знаем, что $[x]$ имеет вид либо $e_1 \wedge \ldots \wedge e_i \wedge \Lambda^{m-i} V$ либо $\Lambda^m \langle e_1, \ldots, e_i \rangle$, то по нему восстанавливается подпространство $\langle e_1, \ldots, e_i \rangle$.

Предложение 1. *Подпространство $\langle e_1, \ldots, e_i \rangle$ является аннулятором пространства $e_1 \wedge \ldots \wedge e_i \wedge \Lambda^{m-i} V$ при отображении $V \otimes \Lambda^m V \to \Lambda^{m+1} V$.*

Предложение 2. *Подпространство $\langle e_1, \ldots, e_i \rangle$ является образом пространства $\Lambda^m \langle e_1, \ldots, e_i \rangle$ при отображении $\Lambda^m V \otimes \Lambda^{m-1} V^* \to V$.*

Учитывая, что вложение подпространств дает вложение образов и обратное включение для их аннуляторов получаем следующее:

Предложение 3. *Рассмотрим набор элементов $[V_i'] \in G[\langle P_i e_1 \wedge \ldots \wedge e_m \rangle] \subset Gr(n_i, \Lambda^m V)$, для того, чтобы этот набор стабилизировался некоторой борелевской подгруппой необходимо и достаточно, чтобы выполнялась следующая цепочка включений:*

$$V_1' \supset V_2' \supset \ldots \supset V_m' \subset V_{m+1}' \subset \ldots \subset V_m'.$$

Иными словами, для набора элементов из произведения $G/P_1 \times \ldots \times G/P_n$ и диагонального действия группы G, условие того, что стабилизатор является борелевской подгруппой, записывается как условие включения для n-подпространств. Автору кажется интересной задача насколько этот результат обобщается на другие простые группы.

On the sequences of embedded spaces and generalized flag manifolds.

V.S.Zhgoon

Abstract

We describe a new construction that provide an equivariant embedding of the special type for generalized flag manifolds. For an arbitrary reductive group we give the embeddings that realize generalized flag manifold as an orbit of chain of embedded linear spaces, those graph of embedding is the corresponding Dynkin diagram with additional data. This construction give new embeddings even for classical groups. In particular fo SL_n we show that a chain of linear spaces of fixed dimension and the graph defines completely the corresponding classical flag.

Keywords: reductive algebraic group, generalized flag variety, root system, Dynkin diagram, irreducible representation.

Литература

1. *Humphreys J. E.* Linear algebraic groups. т. 21. — Springer Science & Business Media, 2012.
2. *Бурбаки Н.* Группы и алгебры Ли. — Рипол Классик, 1972.
3. *Винберг Э.*, *Онищик А.* Семинар по группам Ли и алгебраическим группам, УРСС // Москва. — 1995.

Неполные суммы характеров на сдвинутой геометрической прогрессии.

Ю. Н. Штейников[1]

[1] *ФГУ ФНЦ НИИСИ РАН, Москва, Россия, E-mail: yuriisht@gmail.com*

Аннотация

Изучаются верхние оценки на суммы характеров от сдвинутой геометрической прогрессии по простому модулю. Излагаются два подхода к оценке таких сумм.

Ключевые слова: характер, поле, группа

1. Введение

Всюду в этой работе p это большое простое число, и χ нетривиальный характер Дирихле по модулю p, $\gcd(a,p)=1$, $\mathbb{Z}_p$ это поле вычетов по модулю p и $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$. Пусть $l \in \mathbb{Z}_p^*$, где $ord(l) = L$, что означает, что L это наименьшее положительное число n что $l^n \equiv 1 \pmod p$. Для $1 \le K \le L$ обозначим

$$S(\chi, a, l, K) := \sum_{1 \le k \le K} \chi(a + l^k),$$

где $a \in \mathbb{Z}, \gcd(a,p) = 1$.

Пусть $G \subset \mathbb{Z}_p^*$– мультипликативная подгруппа

$$S(\chi, a, G) := \sum_{x \in G} \chi(a + x).$$

Открытым вопросом является оценка $|S(\chi, a, G)|$ когда $|G| \sim p^{\frac{1}{2}}$. Жан Бургейн поставил этот вопрос (смотри обзор М-Ч. Чанг).Точная формулировка этого вопроса такова.

Вопрос (Ж. Бургейн) Пусть G - подгруппа, $G \subset \mathbb{Z}_p^*$, $|G| \sim p^{\frac{1}{2}}$, χ – нетривиальный характер по модулю p, $\gcd(a,p) = 1$. Получить нетривиальные по порядку оценки для

$$|S(\chi, a, G)|.$$

В этой работе мы устанавливаем оценки для модуля $S(\chi, a, l, K)$, которые являются неполными аналогами величин $S(\chi, a, G)$.

Главной целью этой статьи представляется вывести оценки для модуля величины $S(\chi, a, l, K)$ когда K существенно больше $p^{\frac{1}{2}}$. Главный результат представлен в следующих теоремах. Некоторые результаты по оценкам сумм характеров изложены в работах[3], [2], [1].

Теорема 1. *Справедлива следующая оценка*

$$|S(\chi, a, l, K)| \ll \sqrt{p} \log p.$$

Мы можем слегка улучшить предыдущую оценку для $|S(\chi, a, l, K)|$. Справедлива и такая

Теорема 2. *Пусть $K \ge p^{\frac{1}{2}}$, тогда следующая оценка имеет место*

$$|S(\chi, a, l, K)| \ll \sqrt{p}(\log \frac{K}{\sqrt{p}} + 1).$$

Теорема 2 несколько сильнее Теоремы 1, но тем не менее мы выведем их двумя разными способами.

Величины $S(\chi, a, l, K)$ могут считаться обобщениями величин $S(\chi, a, G)$. Действительно $G \subset \mathbb{Z}_p^*$ является циклической, что означает, что $G = \{l^k\}_{1 \le k \le |G|}$ для некоторого $l \in \mathbb{Z}_p^*$. Оценки сумм характеров изучались во множестве работ, среди которых упомянем статьи [1]-[8].

Мы используем обозначения $A(n) = O(B(n)), A(n) \ll B(n)$ которые эквивалентны утверждению о том, что существует константа c что неравенство

$$|A(n)| \le cB(n)$$

выполняется для всех n.

2. Предварительные результаты

В этом разделе мы выводим некоторые утверждения, которые используем для доказательства основных результатов. Но начнем с оценок для величин $|S(\chi, a, G)|$.

Лемма 1. *Пусть $G \subset \mathbb{Z}_p^*$ – любая мультипликативная подгруппа, тогда*

$$|S(\chi, a, G)| \le p^{1/2}.$$

В доказательстве мы используем идею И.М. Виноградова, (см. [9]) которая представлена в следующей лемме.

Лемма 2. *Пусть*

$$S := \sum_{0 \le x \le p-1} \sum_{0 \le y \le p-1} \alpha(x)\beta(y)\chi(xy + a),$$

и

$$\sum_{0 \le x \le p-1} |\alpha(x)|^2 \le X, \sum_{0 \le y \le p-1} |\alpha(y)|^2 \le Y$$

Тогда справедлива оценка

$$|S| \le (pXY)^{\frac{1}{2}}.$$

Теперь мы готовы доказать Лемму 1.

Доказательство. Пусть $G(x)$ – индикатор множества G. Мы имеем

$$\sum_{x \in G} \chi(x + a) = \frac{1}{|G|} \sum_{x, y \in G} \chi(xy + a) =$$

$$= \frac{1}{|G|} \sum_{0 \le x \le p-1} \sum_{0 \le y \le p-1} G(x)G(y)\chi(xy + a).$$

Применяя предыдущую лемму к последней сумме мы получаем требуемый результат. □

Теперь напомним некоторые результаты общего плана.

Хорошо известно, что $\chi \ne id$ то справедливо

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{p} \overline{\chi}(a) e^{2\pi i \frac{an}{p}},$$

где

$$\tau(\chi) = \sum_{a=1}^{p} \chi(a) e^{2\pi i \frac{a}{p}} \quad \text{и} \quad |\tau(\chi)| = \sqrt{p}.$$

Для $u \in \mathbb{R}$ пусть

$$\rho(u) := \min(\{u\}, 1 - \{u\}).$$

Следующий результат может быть найден в книге А.А. Карацубы [4].

Лемма 3. *Пусть $\alpha = \frac{b}{q}, \gcd(b, q) = 1$, $q \ge 1; U > 0, Q \ge 1$. справедливо*

$$\sum_{1 \le x \le Q} \min(U, \frac{1}{\rho(\alpha x)}) \ll (\frac{Q}{q} + 1)(U + q \log q)$$

Теперь мы готовы сформулировать и доказать вспомогательное утверждение.

Лемма 4. *Для любого нетривиального характера χ и ψ,*

$$\left| \sum_{1 \le k \le p-1} \chi(a + g^k)\psi(g^k) \right| \le \sqrt{p}.$$

Неравенство достигается, если $\chi\psi$ не тождественный характер.

Доказательство. Мы имеем

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{p} \overline{\chi}(a) e^{2\pi i \frac{an}{p}},$$

где

$$\tau(\chi) = \sum_{a=1}^{p} \chi(a) e^{2\pi i \frac{a}{p}} \quad \text{и} \quad |\tau(\chi)| = \sqrt{p}.$$

Тогда

$$\sum_{1\le k\le p-1} \chi(a+g^k)\psi(g^k) = \sum_{x=1}^{p} \chi(a+x)\psi(x) =$$

$$= \frac{1}{\tau(\overline{\chi})} \frac{1}{\tau(\overline{\psi})} \sum_{x=1}^{p} \left(\sum_{m_1=1}^{p} \overline{\chi}(m_1) e^{2\pi i \frac{(a+x)m_1}{p}} \right) \times$$

$$\times \left(\sum_{m_2=1}^{p} \overline{\psi}(m_2) e^{2\pi i \frac{xm_2}{p}} \right) =$$

$$= \frac{1}{\tau(\overline{\chi})\tau(\overline{\psi})} \sum_{m_1,m_2=1}^{p} \overline{\chi}(m_1)\overline{\psi}(m_2) e^{2\pi i \frac{am_1}{p}} \times$$

$$\times \sum_{x=1}^{p} e^{2\pi i \frac{(m_1+m_2)x}{p}} =$$

$$= \frac{\overline{\psi}(-1)}{\tau(\overline{\chi})\tau(\overline{\psi})} p \sum_{m=1}^{p} \overline{\chi}(m)\overline{\psi}(m) e^{2\pi i \frac{am}{p}},$$

абсолютная величина последнего выражения есть

$$\frac{p}{\sqrt{p}\cdot\sqrt{p}} \left| \sum_{m=1}^{p} \overline{\chi}(m)\overline{\psi}(m) e^{2\pi i \frac{am}{p}} \right|.$$

Если $\chi\psi$ тождественный характер, то

$$\left| \sum_{m=1}^{p-1} e^{2\pi i \frac{am}{p}} \right| = 1.$$

Если $\chi\psi$ не тождественный характер, тогда эта сумма является Гауссовой суммой и

$$\left| \sum_{m=1}^{p} \overline{\chi}(m)\overline{\psi}(m) e^{2\pi i \frac{am}{p}} \right| = \sqrt{p}.$$

Доказательство тем самым закончено. □

3. Доказательство основных результатов.

Сначала выведем Теорему 1.

Доказательство. Пусть g – первообразный корень по модулю p. Тогда $l = g^s$ для некоторого s и $L = \frac{p-1}{\gcd(s,p-1)}$. Мы определяем множество

$$V := \{1 \le n \le p-1 :$$

$$\exists k, 1 \le k \le K, n \equiv ks \pmod{p-1}\}.$$

Пишем далее

$$S(\chi, a, l, K) =$$

$$= \sum_{1\le k\le K} \chi(a+l^k) = \sum_{1\le k\le K} \chi(a+g^{ks}) =$$

$$= \sum_{1\le k\le p-1} \chi(a+g^k) \sum_{v\in V} \frac{1}{p-1} \sum_{\psi \pmod p} \psi(g^{k-v}) =$$

$$= \frac{1}{p-1} \sum_{\psi \pmod p} \sum_{1\le k\le p-1} \chi(a+g^k)\psi(g^k) \sum_{v\in V} \overline{\psi}(g^v).$$

мы отделяем слагаемое с $\psi = \psi_0$. Оно равно

$$\frac{K}{p-1} \sum_{1\le k\le p-1} \chi(a+g^k),$$

абсолютная величина которого есть $\frac{K}{p-1}$, которая достаточно мало.

Теперь разберемся со случаем $\psi \ne \psi_0$. Используя Лемму 4 мы получаем оценки для

$$\left| \sum_{1\le k\le p-1} \chi(a+g^k)\psi(g^k) \right| \ll \sqrt{p}. \qquad (1)$$

Мы имеем (1), далее покажем

$$\sum_{\substack{\psi \pmod p \\ \psi\ne\psi_0}} \left| \sum_{v\in V} \overline{\psi}(g^v) \right| \ll p \log L. \qquad (2)$$

Действительно,

$$\sum_{\substack{\psi \pmod p \\ \psi\ne\psi_0}} \left| \sum_{v\in V} \overline{\psi}(g^v) \right| =$$

$$= \sum_{1\le b\le p-2} \left| \sum_{1\le k\le K} e^{2\pi i \frac{bsk}{p-1}} \right| \le$$

$$\le \sum_{1\le b\le p-2} \min(K, \frac{1}{2\rho(\frac{bs}{p-1})}).$$

Вспоминая, что $\gcd(s, p-1) = \frac{p-1}{L}$ и используя Лемму 3, мы имеем

$$\sum_{1\le b\le p-2} \min(K, \frac{1}{2\rho(\frac{bs}{p-1})}) \ll$$

$$\ll (\frac{p}{L}+1)(L\log L) \ll p\log L.$$

Итак, мы показали (2).

Объединяя все вместе, мы получаем

$$\frac{1}{p-1} \sum_{\psi \pmod p \psi\ne\psi_0} \sum_{1\le k\le p-1} \chi(a+g^k)\psi(g^k)\times$$

$$\sum_{v\in V} \overline{\psi}(g^v) \ll$$

$$\ll \frac{\sqrt{p}}{p-1} \sum_{\substack{\psi \pmod p \\ \psi\ne\psi_0}} \left| \sum_{v\in V} \overline{\psi}(g^v) \right| \ll$$

$$\ll \frac{\sqrt{p}}{p-1} p\log p \ll \sqrt{p}\log p,$$

которое завершает доказательство Теоремы 1. □

Теперь дадим доказательство Теоремы 2. Мы используем подход И.М. Виноградова [9], где он рассматривает оценки сумм характеров. Обозначим

$$f(k) := \chi(a+l^k),$$

и тем самым необходимо установить оценки на

$$|\sum_{1\le k\le K} f(k)|.$$

Мы можем считать, что $K < \frac{L}{2}$.

Лемма 5. *Пусть* $P, M_1, \dots, M_m \in \mathbb{N}, P < \frac{L}{2}$ *и*

$$M_1+P \le M_2, \dots, M_{m-1}+P \le M_m \le M_1+L$$

мы имеем

$$\sum_{1\le i\le m} \left| \sum_{M_i+1\le x\le M_i+P} \sum_{0\le z\le P-1} f(x+z) \right| \ll$$

$$\ll (mp)^{\frac{1}{2}} P.$$

Доказательство. Пусть W это следующее множество

$$W := \{x \in \mathbb{Z}_p :$$

$$\exists i \in [1,m], \exists k \in [M_i+1, M_i+P],$$

$$x \equiv l^k \pmod p\}$$

и $W(x)$ это индикатор множества W. Мы имеем

$$\sum_{1\le i\le m} \left| \sum_{M_i+1\le x\le M_i+P} \sum_{0\le z\le P-1} f(x+z) \right| \ll$$

$$\ll \sum_{0\le x\le p-1} W(x) \left| \sum_{0\le z\le P-1} \chi(a+xl^z) \right|.$$

Используя неравенство Коши-Буняковского, последнее выражение

$$\left(\sum_{0\le x\le p-1} W(x) \right)^{\frac{1}{2}} \times$$

$$\times \left(\sum_{0\le x\le p-1} \left| \sum_{0\le z\le P-1} \chi(a+xl^z) \right|^2 \right)^{\frac{1}{2}} =$$

$$= (mP)^{\frac{1}{2}} \sigma^{\frac{1}{2}},$$

где

$$\sigma := \sum_{0\le x\le p-1} \left| \sum_{0\le z\le P-1} \chi(a+xl^z) \right|^2 =$$

$$= \sum_{0\le z,z'\le P-1} \sum_{0\le x\le p-1} \chi(a+xl^z)\overline{\chi}(a+xl^{z'}).$$

Мы отдельно рассматриваем случай $z = z'$, слагаемое соответствующее равно $P(p-1)$.

Теперь рассмотрим второй случай $z \ne z'$, фиксируем такие z, z'. Мы видим, что

$$\sum_{0\le x\le p-1} \chi(a+xl^z)\overline{\chi}(a+xl^{z'}) =$$

$$= \sum_{x=0, xl^{z'}\ne -a}^{p-1} \chi(\frac{a+xl^z}{a+xl^{z'}}).$$

Легко видеть, что выражение

$$\frac{a+xl^z}{a+xl^{z'}}$$

пробегает все множество $\mathbb{Z}_p$ за исключением одного, когда x пробегает интервал

$$x \in [0, p-1], xl^{z'} \neq -a \pmod p.$$

Так как $\chi \neq id$, для $z \neq z'$ мы имеем

$$\Big| \sum_{0 \le x \le p-1} \chi(a+xl^z)\overline{\chi}(a+xl^{z'}) \Big| \le 1.$$

Количество пар (z, z') с $z \neq z'$ есть $O(P^2)$.

Объединяя вышесказанное мы завершаем доказательство. □

Теперь выведем Теорему 2.

Доказательство. Мы следуем схеме, предложенной в работе [9]. Мы получим нужные оценки для

$$|\sum_{N+1 \le x \le N+K} f(x)|.$$

Мы можем предположить, что

$$K > 20p^{\frac{1}{2}}.$$

Обозначим h, τ, K_0, S_0 из равенств:

$$h = \frac{K}{p^{\frac{1}{2}}}; \tau = [\frac{\log h}{\log 3}];$$

$$K_0 = 2 * 3^\tau [\frac{K}{2 * 3^\tau}]; S_0 = \sum_{N+1 \le x \le N+K_0} f(x).$$

Достаточно получить верхнюю оценку для $|S_0 K_0|$. Для целых x, y мы определяем функцию

$$f_1(x, y) := f(x).$$

Тогда $S_0 K_0$ может быть рассмотрена как сумма $f_1(x, y)$ по тем целым точкам (x, y), принадлежащим квадрату $ABCD$ на решетке за исключением целых точек на сторонах AB и AD $ABCD$.

Точки квадрата на плоскости имеют следующие координаты

$$A = (N, 0); B = (N, K_0);$$

$$C = (N + K_0, K_0); D = (N + K_0, 0).$$

Множество целых точек квадрата $ABCD$ мы обозначим как H. Далее будем покрывать точки H параллелограммами.

Рассмотрим первый параллелограмм $A_1B_1C_1D_1$, где B_1 и D_1 есть середины BC и AD и $A_1D_1 = AD$. Пусть J - множество целых точек принадлежащих параллелограмму $A_1B_1C_1D_1$ за исключением точек на A_1D_1 и A_1B_1 фигуры $A_1B_1C_1D_1$. Легко видеть, что

$$\sum_{(x,y) \in J} f_1(x, y) = \sum_{x=M+1}^{M+K_0} \sum_{z=0}^{K_0-1} f(x+z),$$

где $M = N - \frac{K_0}{2} + 1$. Используя Лемму 5, мы имеем

$$|\sum_{(x,y) \in J} f_1(x, y)| \ll p^{\frac{1}{2}} K_0.$$

Нам необходимо разобраться с точками $(x, y) \in (H \bigcup J) \setminus (H \bigcap J)$.

Далее используем схему предложенную И.М. Виноградовым и будем покрывать параллелограммами которые меньше $A_1B_1C_1D_1$ в 3^r раз. Для одних знак величины в сумме для $f_1(x, y)$ для одних берется со знаком плюс, для других со знаком минус. Дальнейшие рассуждения абсолютно аналогичны работе [6]. Вспоминая определение τ мы получаем необходимую оценку для S_0 и для начальной суммы. С этим завершаем доказательство Теоремы 2. □

Incomplete character sums over shifted powers.

Yu. N. Shteinikov

Abstract

The upper bounds on the sums of characters from the shifted geometric progression over the prime modulus are studied. Two approaches to the estimation of such sums are outlined.

Keywords: character, field, group

Литература

1. *Bachman G.*, *Rachakonda L.* On a problem of Dobrowolski and Williams and the Pólya-Vinogradov inequality // The Ramanujan Journal. — 2001. — т. 5, № 1. — с. 65—71.
2. *Granville A.*, *Soundararajan K.* Large character sums: pretentious characters and the Pólya-Vinogradov theorem // Journal of the American Mathematical Society. — 2007. — т. 20, № 2. — с. 357—384.
3. *Vinogradov I. M.* A new improvement of the method of estimation of double sums // Doklady Akad. Nauk SSSR (NS). т. 73. — 1950. — с. 635—638.
4. *Карацуба А.* Основы аналитической теории чисел. — Рипол Классик, 1975.

Об одном быстром алгоритме проверки вырожденности теплицевых матриц

Ю.В. Кузнецов[1] и **М.М. Петрунин**[2]

[1] *ФГУ ФНЦ НИИСИ РАН, Москва, Россия, E-mail: ykuz@niisi.ras.ru*
[2] *ФГУ ФНЦ НИИСИ РАН, Москва, Россия, E-mail: petrunin@niisi.ras.ru*

Аннотация

В работе приводится описание переноса программной реализации ранее предложенного в [7] асимптотически наилучшего алгоритма проверки вырожденности теплицевых (ганкелевых) матриц над полем рациональных чисел $\mathbb{Q}$ на гетерогенный программно-аппаратный комплекс НИИСИ РАН. Для этой цели был использован подход, связанный с редукцией к конечному полю и опирающийся на платформу OpenCL. Многочисленные вычислительные эксперименты показали, что скорость работы указанного алгоритма на гетерогенном комплексе выросла более чем на 2 порядка по сравнению с эталонной реализацией на CPU.

Ключевые слова: ганкелевы, теплицевы матрицы, полуНОД-алгоритмы, аппроксимации Паде

1. Введение

Настоящая работа посвящена построению и исследованию быстрых алгоритмов для проверки вырожденности множества ганкелевых (или теплицевых) матриц над полем рациональных чисел $\mathbb{Q}$. Как известно, ганкелевы (теплицевы) матрицы играют важную роль в алгебре, теории функций, гармоническом анализе, проблеме моментов, функциональном анализе, теории вероятностей и многих прикладных вопросах. Особый интерес к построению и изучению быстрых алгоритмов проверки вырожденности ганкелевых или теплицевых матриц объясняется следующими обстоятельствами. В серии работ [5; 6; 8] 2009-2010 годов Платоновым В.П. (совместно с Беняш-Кривецом В.В.) была обнаружена глубокая связь между проблемой существования нетривиальных единиц в гиперэллиптических полях с произвольным полем констант, формальными рядами Лорана и ганкелевыми матрицами. При этом выяснилось, что в случае эллиптических полей существенную роль играет эффективность алгоритмов для проверки вырожденности ганкелевых (или тёплицевых) матриц. Однако ранее вышеуказанная проблема в такой постановке не исследовалась. Как правило, требовалось эффективно найти решение системы с теплицевой матрицей над комплексным или действительным полем при условии, что такое решение существует (т.е. при условии невырожденности самой матрицы). Первоначально на матрицы накладывались также дополнительные условия: требовалась невырожденность всех ее ведущих подматриц. Именно для этого случая ранее бы-

ли построены наиболее эффективные алгоритмы решения соответствующих систем [4] сложности $O(n \log^2 n)$. Существует тесная связь между теплицевыми матрицами, степенными рядами и аппроксимациями Паде, а именно, если записать условия на коэффициенты многочленов, образующих аппроксимант Паде степенного ряда, то возникает система линейных уравнений с теплицевой матрицей, на диагоналях которой находятся соответствующие члены этого ряда. Опираясь на хорошо разработанную и глубокую теорию аппрокимаций Паде, американским математикам Бренту, Густавсону и Юну в 1980 году [2] удалось построить первый асимптотически наилучший алгоритм решения систем с теплицевыми матрицами, который не накладывал ограничений на невырожденность ведущих подматриц. Однако строго доказать корректность своего алгоритма Бренту, Густавсону и Юну не удалось. Известная и широко цитируемая монография Ахо, Хопрокфта и Ульмана «Построение и анализ вычислительных алгоритмов»[1], на которую при доказательстве корректности ссылались упомянутые авторы содержала принципиальную ошибку. Эту ошибку удалось ликвидировать только спустя 10 лет американскому математику Ч.К. Япу[3]. Ранее с использованием подхода Брента, Густавсона и Юна нам удалось разработать асимптотически наилучший алгоритм проверки вырожденности теплицевых матриц, причем наш алгоритм также не накладывает ограничений на невырожденность ведущих подматриц. Важно отметить, что с точки зрения практической применимости любого алгоритма ключевым является вопрос о мультипликативной константе в оценке сложности этого алгоритма. Для вышеуказанного алгоритма в работе [7] удалось подсчитать значение мультипликативной константы, которое оказалось равно 468 и является в настоящее время наилучшим. При вычислении этой константы были использованы идеи из вышеупомянутой работы К.Ч. Япа, а также последние результаты, связанные с оценками мультипликативных констант для элементарных операций над степенными рядами. Отметим, что значение мультипликативной константы для алгоритма Брента, Густавсона и Юна решения систем с теплицевыми матрицами не известно.

В настоящей работе описывается перенос программной реализации вышеуказанного асимптотически наилучшего алгоритма проверки вырожденности теплицевых матриц над полем рациональных чисел $\mathbb{Q}$ на гетерогенный программно-аппаратный комплекс НИИСИ РАН. Для этого был использован подход, связанный с редукцией к конечному полю и опирающийся на платформу OpenCL. Многочисленные вычислительные эксперименты показали, что скорость работы указанного алгоритма выросла более чем на 2 порядка по сравнению с гомогенным комплексом.

2. Описание алгоритма

Напомним, что тёплицевой матрицей, называется матрица вида

$$\begin{pmatrix} a_n & a_{n-1} & \dots & a_0 \\ a_{n+1} & a_n & \dots & a_1 \\ \vdots & \vdots & \ddots & \vdots \\ a_{2n} & a_{2n-1} & \dots & a_n \end{pmatrix},$$

где $a_i \in \mathbb{Q}$.

Напомним также понятие аппроксимации Паде.

Пусть $a(x) = a_0 + a_1 x + a_2 x^2 + \dots$ – степенной ряд с $a_0 \neq 0$. Рациональная функция вида $u(x)/v(x)$, где $u,\ v$ — многочлены, называется (m, n) аппроксимантом Паде для ряда $a(x)$, если

$$\deg(u) \leq m, \quad \deg(v) \leq n,$$

$$a(x)v(x) - u(x) = O(x^{m+n+1}).$$

Элементарное изложение основных результатов теории Паде доступно в [9].

Известно, что существует связь между тёплицевой матрицей и аппроксимацией Паде, т.е. любую тёплицеву матрицу можно свести к соответствующей аппроксимации Паде и наоборот.

Рассмотрим многочлен $b = \sum_{i=0}^{2n} a_i x^i$, где a_i коэффициенты нашей тёплицевой матрицы, и многочлен $a = x^{2n+1}$. В работе [2] показано, что каждый шаг расширенного алгоритма Евклида, применённого к многочленам a и b, даёт определённую запись в таблицу Паде. Можно показать, что вырожденность тёплицевой матрицы эквивалентна нахождению соответствующей записи в таблице Паде на определённых позициях в соответствующем Паде блоке (окне). В работе [2] показано, что тёплицева матрица T невырождена тогда и только тогда, когда равен нулю коэффициент при n-ой степени полинома u_j в последовательности остатков расширенного алгоритма Евклида $u_0 = a, u_1 = b, u_2 \ldots$, где $\deg(u_{j-1}) \geq \frac{\deg(a)}{2} > \deg(u_j)$.

Напомним понятие ПолуНОД-алгоритмов для многочленов [1]. Эти алгоритмы по паре многочленов a и b, $\deg(a) > \deg(b)$, строят матрицу перехода Q такую, что $\begin{pmatrix} a \\ b \end{pmatrix} = Q \begin{pmatrix} u_i \\ u_{i+1} \end{pmatrix}$, где $\deg(u_{i+1}) < \lceil \frac{\deg(a)}{2} \rceil \leq \deg(u_i)$.

ПолуНОД-алгоритмы в первую очередь служат для построения соответствующих рекурсивных алгоритмов поиска НОД, но помимо этого часто используются как независимые процедуры в других алгоритмах.

Исходя из вышесказанного, проверка вырожденности тёплицевой матрицы сводится к построению многочленов a и b, применению к ним процедуры полуНОД и сравнение n-го члена результирующего u_j с нулём. Сложность алгоритма, таким образом, совпадает со сложностью алгоритма полуНОД применённого к многочленам степени не более $2n + 1$.

3. Описание алгоритма ПолуНОД

Для описания алгоритма нам понадобятся следующие известные факты.

Напомним понятие расширенного алгоритма Евклида для многочленов. Пусть даны многочлены a и b, $\deg a > \deg b$. Положим

$$u_0 = a, u_1 = b,$$
$$v_0 = 0, v_1 = 1,$$
$$w_0 = 1, w_1 = 0,$$

и определим

$$u_{i+1} = u_{i-1} - q_i u_i,$$
$$v_{i+1} = v_{i-1} - q_i v_i,$$
$$w_{i+1} = w_{i-1} - q_i w_i,$$

где q_i – частное, полученное от деления u_{i-1} на u_i, а u_{i+1} – соответствующий остаток.

Как известно, для всех $i \geq 0$ выполняется

$$w_i u_0 + v_i u_1 = u_i,$$
$$\text{НОД}(v_i, w_i) = 1,$$

при этом алгоритм остановится на шаге $i = k$, при котором $u_{k+1} = 0$, т.е. u_k делит u_{k-1}. В этом случае u_k – это НОД(a, b), а w_k и v_k – это такая пара многочленов, что $w_k u_0 + v_k u_1 = \text{НОД}(a, b)$.

Если у нас имеются 2 соседних члена u_i и u_{i+1} последовательности остатков $\{u_j\}$, то переход к следующей паре u_{i+1}, u_{i+2} можно представить в виде

$$\begin{pmatrix} u_{i+1} \\ u_{i+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \begin{pmatrix} u_i \\ u_{i+1} \end{pmatrix}$$

или

$$\begin{pmatrix} u_i \\ u_{i+1} \end{pmatrix} = \begin{pmatrix} q_{i+1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_{i+1} \\ u_{i+2} \end{pmatrix}$$

Матрицу вида $\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}$, где $\deg q > 0$ будем называть элементарной, а произведение конечного числа произвольных элементарных матриц – регулярной матрицей. Ясно, что если $\begin{pmatrix} a \\ b \end{pmatrix} = Q \begin{pmatrix} u_i \\ u_{i+1} \end{pmatrix}$, для некоторого i, то Q – регулярная матрица и $Q^{-1} = \begin{pmatrix} w_i & v_i \\ w_{i+1} & v_{i+1} \end{pmatrix}$, где w_i, v_i определены выше.

Примечательно, что верно и обратное утверждение, а именно, если $\begin{pmatrix} a \\ b \end{pmatrix} = Q \begin{pmatrix} a' \\ b' \end{pmatrix}$, Q – регулярная матрица и

$\deg(a') > \deg(b')$, то a' и b' – соседние члены последовательности остатков, т.е. для некоторого i $a' = u_i$ и $b' = u_{i+1}$ [3].

Приведём описание ПолуНОД-алгоритма из работы Тула и Япа [3], который авторы в этой работе называют HGCD. Отметим, что EMGCD из работы [2] Брента и др. фактически совпадает с HGCD, но дополнительно на каждом шаге вычисляет пару многочленов u_i, u_{i+1}, что для наших целей является лишней операцией.

Алгоритм HGCD

Вход: многочлены a, b, для которых $\deg b < \deg a = n$.

Выход: регулярная матрица Q такая, что $\deg(c') \geq n/2 > \deg(d')$, где $\begin{pmatrix} c' \\ d' \end{pmatrix} = Q^{-1} \cdot \begin{pmatrix} a \\ b \end{pmatrix}$.

Описание алгоритма $HGCD(a, b)$:

1. $m := \lceil \frac{\deg a}{2} \rceil$;
   если $\deg(b) < m$, алгоритм заканчивает работу и возвращает единичную матрицу E;
2. $a_0 := a \ div \ x^m; b_0 := b \ div \ x^m$;
   $R := HGCD(a_0, b_0)$;
   $\begin{pmatrix} a' \\ b' \end{pmatrix} := R^{-1} \begin{pmatrix} a \\ b \end{pmatrix}$;
3. если $\deg(b') < m$, алгоритм заканчивает работу и возвращает матрицу R;
4. $q := a' \ div \ b'$; $\begin{pmatrix} c \\ d \end{pmatrix} := \begin{pmatrix} b' \\ a' \mod b' \end{pmatrix}$;
5. $l := \deg(c); k := 2m - l$;
6. $c_0 := c \ div \ x^k; d_0 := d \ div \ x^k$;
   $S := HGCD(c_0, d_0)$;
7. $Q := R \cdot \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \cdot S$; Алгоритм заканчивает работу и возвращает матрицу Q.

Известно, что асимптотическая сложность вышеуказанного алгоритма HGCD составляет $O(n \log^2 n)$ [1]. В работе [7] было показано, что сложность полуНОД-алгоритма HGCD для двух многочленов степени не более n не превосходит $117n \log_2^2(n) + O(n \log(n))$ в случае $n = 2^k$ и $234n \log_2^2(n) + O(n \log(n))$ для всех n.

4. Перенос программной реализации алгоритма на гетерогенный программно-аппаратный комплекс НИИСИ РАН

Опишем построение вычислительной реализации алгоритма проверки вырожденности массива тёплицевым матриц.

Наши первые эталонные реализации алгоритма были построены с использованием системы компьютерной алгебры Sage, которая является надстройкой над высокоуровневым языком Python (популярный язык для научных расчётов) и обладает возможностью использования символьных вычислений, а также подключения других математических пакетов. Следует отметить, что Sage обладает очень мощным математическим аппаратом.

Далее первоначальный код на Sage был протестирован с использованием методологии модульного (unit) тестирования. Прогон тестов был автоматизирован с использованием языка Ruby и библиотеки watchr.

Вычисления над $\mathbb{Q}$ в силу особенностей хранения рациональных чисел в памяти компьютера (в общем случае, требуется более одной ячейки памяти) являются достаточно громоздкими. Помимо этого, сложность выполнения арифметических операций над полем рациональных чисел больше сложности выполнения целочисленных арифметических операций.

В рамках поэтапного ускорения программной реализации был произведён пе-

ренос кода на язык C. Для обеспечения поддержки вычислений над полем $\mathbb{Q}$ использовалась библиотека GMP. Для обеспечения тестирования был выбран Google Testing Framework, для автоматизации прогона тестов была также использована библиотека watchr.

Нам удалось в значительной степени уменьшить влияние вышеописанной проблемы, связанной с полем рациональных чисел, путём применения редукции в конечное поле $\mathbb{F}_p$ для подходящих простых p. В этом случае происходит естественное сведение задачи проверки вырожденности матрицы над $\mathbb{Q}$ к задаче проверки вырожденности соответствующей редуцированной матрицы над $\mathbb{F}_p$, для некоторого простого p. Редуцированная матрица может быть получена путём поэлементной редукции элементов матрицы в поле $\mathbb{F}_p$. Для достаточно малых p при использовании $\mathbb{F}_p$ в качестве базового поля все участвующие в вычислении коэффициенты остаются в пределах одной ячейки памяти и в пределах базовых типов используемых языков, что позволяет получить существенный прирост в скорости исполнения по сравнению с вычислениями над полем рациональных чисел.

Вышесказанное можно проиллюстрировать на следующем примере. Рассмотрим элемент одной из рассматриваемых нами матриц.

$$d = \frac{51212764270766313506230756524181}{607060240091291776605985812823401}$$

В то же время, при редукции в $\mathbb{F}_{31991}$ его значение становится следующим

$$d \mod 31991 = 26839.$$

В некотором роде редукция в конечное поле позволяет осуществить фильтрацию массива матриц, поступающих на вход алгоритма над полем рациональных чисел. На вход алгоритма, работающего над полем $\mathbb{Q}$ будут поступать только матрицы, соответствующие редукции которых в поле $\mathbb{F}_p$ являются вырожденными.

Применение вышеописанных идей даёт возможность создать программную реализацию на языке программирования C, и избавиться от недостатков, присущих системам компьютерной алгебры и языкам высокого уровня. Совокупный эффект от перехода к операциям в конечном поле и смены языка программирования позволил достичь прироста скорости более чем на порядок, по сравнению с реализацией на Sage для вычислений над $\mathbb{Q}$. Для достаточно большого случайного набора матриц время проверки над $\mathbb{Q}$ отфильтрованного над конечным полем массива оказывается мало по сравнению с временем работы алгоритма фильтрации над $\mathbb{F}_p$.

В целях ускорения программной реализации алгоритма над конечным полем в качестве поля констант использовался ряд методов оптимизации. В частности, существенный вклад внесло кеширование арифметических операций над конечным полем (сложение, умножение, взятие обратного). На первом этапе работы программы вычислялись таблицы значений для каждой арифметической операции, а на последующих этапах использовалось не прямое вычисление, а обращение к соответствующей таблице, что дало около 45% прироста скорости.

На следующем этапе основные усилия были сосредоточены на переносе реализации алгоритма проверки вырожденности тёплицевой матрицы над $\mathbb{F}_p$ на гетерогенный программно-аппаратный комплекс НИИСИ РАН, в состав которого входят графические ускорители.

Графические ускорители, ввиду особенностей аппаратной архитектуры, обладают рядом ограничений, что существенно усложняет процесс разработки и отладки, а также значительно повышает требования к алгоритму. Применение редукции в поле $\mathbb{F}_p$ позволило создать массивно-параллельную программную реализацию алгоритма, оптимизированную для исполнения в гетерогенных вычислительных системах. Вышеупомянутая реализация основана на открытом стандарте OpenCL, и способна исполняться как на центральном

процессоре, задействуя все его ядра, так и на графических ускорителях.

Вычислительное ядро OpenCL-программы было написано на OpenCL-диалекте языка C. Основная вычислительная нагрузка ложится на код ядра, и требования к эффективности управляющего кода, как правило, значительно ниже. В то же время объём кода, необходимого для подготовки устройства, данных и запуска ядра может очень сильно отличаться в зависимости от выбранной библиотеки или языка программирования. Нами было решено задействовать библиотеку PyOpenCL. Она позволила использовать высокоуровневый и компактный управляющий код на языке Python, что значительно ускорило написание, модульное тестирование и дальнейшее сопровождение OpenCL-программ.

Многочисленные эксперименты показали, что перенос CPU-кода на платформу OpenCL с последующим запуском в гетерогенной среде оказался оправданным. Фактически, эта процедура позволила увеличивать производительность программно-аппаратного комплекса за счёт компонентов с высоким отношением производительности к цене. Кроме того, использование OpenCL в качестве дополнительного преимущества в автоматическом режиме обеспечила максимальное задействование всех аппаратных компонентов комплекса.

Таким образом, в конечном итоге переход к алгоритму, использующему фильтрацию путём редукции в соответствующие $\mathbb{F}_p$, и применения многочисленных математических и вычислительных оптимизаций алгоритма удалось достичь скорости более чем на 2 порядка выше, чем при использовании реализации над $\mathbb{Q}$ в системе компьютерной алгебры Sage.

On some fast algorithm for checking nondegeneracy of Toeplitz matrices

Y.V. Kuznetsov, M.M. Petrunin

Abstract

The paper describes the conversion of software implementation previously proposed in [7] the asymptotically best algorithm for checking the degeneracy of the Toeplitz (Hankel) matrices over the field of rational numbers $\mathbb{Q}$ to heterogeneous software-hardware system of SRISA RAS. We used approach based on reduction to the finite field and based on the OpenCL platform. Numerous computational experiments have shown that the speed of this algorithm on the heterogeneous complex increased by more than 2 orders of magnitude comparison with the reference implementation on the CPU.

Keywords: Hankel matrices, Toeplitz matrices, HGCD-algorithms, Pade approximations

Литература

1. *Aho A. V.*, *Hopcroft J. E.*, *Ullman J. D.* The design and analysis of computer algorithms. — 1976.
2. *Brent R. P.*, *Gustavson F. G.*, *Yun D. Y.* Fast solution of Toeplitz systems of equations and computation of Padé approximants // Journal of Algorithms. — 1980. — т. 1, № 3. — с. 259—295.
3. *Thull K.*, *Yap C. K.* A unified approach to HGCD algorithms for polynomials and integers (manuscript). — 1990.
4. *Tyrtyshnikov E. E.* Fast algorithms for toeplitz and quasi-toeplitz systems // Russian Journal of Numerical Analysis and Mathematical Modelling. — 1989. — т. 4, № 5. — с. 419—430.
5. *Беняш-Кривец В. В.*, *Платонов В. П.* Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Математический сборник. — 2009. — т. 200, № 11. — с. 15—44.
6. *Беняш-Кривец В.*, *Платонов В.* О новом локально-глобальном принципе для квадратичных функциональных полей // Доклады Академии наук. — 2010. — т. 433, № 2. — с. 154—157.
7. *Кузнецов Ю. В.*, *Петрунин М. М.* Быстрый алгоритм проверки вырожденности ганкелевых матриц // Чебышевский сборник. — 2011. — т. 12, 2 (38).

8. *Платонов В. П.* Арифметика квадратичных полей и кручение в якобианах // Доклады РАН. — 2010. — т. 430, № 3. — с. 318—320.

9. *Тыртышников Е. Е.* Метод скачков и аппроксимации Паде // Численные методы, параллельные вычисления и информационные технологии.-М.: Изд-во МГУ им. МВ Ломоносова. — 2008. — с. 277—290.