На правах рукописи

Волков Владислав Владимирович

ИНТЕГРАЛЬНАЯ ТЕОРЕМА КОШИ В АРИФМЕТИКЕ И АДДИТИВНОЙ КОМБИНАТОРИКЕ

Специальность 01.01.06 —
«Математическая логика, алгебра и теория чисел»

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Санкт-Петербург — 2016

Работа выполнена в Санкт-Петербургском Государственном Университете

Научный руководитель: доктор физико-математических наук, профессор
Востоков Сергей Владимирович

Официальные оппоненты: **Кузьмин Леонид Викторович,**
доктор физико-математических наук,
Национальный исследовательский центр «Курчатовский институт»,
ведущий научный сотрудник

Горчинский Сергей Олегович,
кандидат физико-математических наук,
ФГБУН «Математический институт им. В. А. Стеклова Российской академии наук»,
старший научный сотрудник

Ведущая организация: Федеральное государственное бюджетное учреждение науки «Институт проблем передачи информации имени А. А. Харкевича Российской академии наук»

Защита состоится 15 марта 2017 г. в 16:00 на заседании диссертационного совета Д 002.202.02 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук по адресу: 191023, Санкт-Петербург, наб. р. Фонтанки, д. 27, ПОМИ РАН.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук, `http://www.pdmi.ras.ru/`.

Автореферат разослан «___» __________ 2017 года.

Ученый секретарь
диссертационного совета
доктор физ.-мат. наук Малютин Андрей Валерьевич

Общая характеристика работы

Актуальность темы.

Аналогия в математике играет двоякую роль: во-первых, способствует бурному развитию одних направлений за счёт методов и понятий уже активно разработанных в других направлениях, во-вторых, позволяет увидеть общую картину и объединить различные области в рамках некоторого более абстрактного подхода. Одним из классических примеров этого феномена является связь между теорией чисел и теорией функций, впервые отмеченная Леопольдом Кронекером: простые идеалы в кольцах алгебраических чисел играют роль аналогичную точкам римановой поверхности в теории алгебраических функций, дробные идеалы соответствуют дивизорам, сами числа соответствуют алгебраическим функциям и т. д.

Эта аналогия была также отмечена Давидом Гильбертом. Он замечал, что его закон взаминости произведения символов норменного вычета:

$$\prod_{\mathfrak{P}} (a, b)_{r,\mathfrak{P}} = 1\,,$$

напоминает интегральную теорему Коши об обнулении интеграла функции охватывающего все её особые точки. Напомним, что самим Гильбертом данный закон был исследован в квадратичном случае (в котором он равнозначен обычному квадратичному закону взаимности для символов Лежандра) и позже был обобщён в работах Н. Г. Чеботарёва, Э. Артина и Г. Хассе.

И. Р. Шафаревич в своей работе [6] даёт уточнение: закон взаимности Гильберта аналогичен следствию интегральной теоремы Коши, которое гласит, что сумма вычетов мероморфной 1-формы на компактной римановой поверхности равна нулю. Аналитически этот результат может быть описан следующим образом: пусть ω — мероморфная (т. е. голоморфная вне некоторого конечного множества своих полюсов S, где она имеет вычеты конечного порядка) 1-форма на римановой поверхности C, и $S = \{p_1, p_2 \ldots, p_n\}$ — её полюса. Тогда

$$\sum_{i=1}^{n} \operatorname{res}_{p_i} \omega = 0.$$

Этот результат легко выводится из теоремы Коши, гласящей, что

$$\operatorname{res}_p \omega = 2\pi i \oint_{\gamma_p} \omega,$$

где γ_p — контур вокруг точки p, не содержащий полюсов ω, кроме p. И. Р. Шафаревич также отмечает, что с этой точки зрения символ Гильберта $(a,b)_{r,\mathfrak{P}}$ играет роль вычета некоторого дифференциала в точке $\mathfrak{P}$. Как и в случае вычета дифференциала значение символа $(a,b)_{r,\mathfrak{P}}$ зависит лишь от поведения a и b в точке $\mathfrak{P}$, то есть от разложения a и b в $\mathfrak{P}$-адические ряды. Тем не менее его классические определения, включая приведённое выше, имеют мало общего с данной аналогией и зависят от свойств всего поля Γ (или его $\mathfrak{P}$-пополнения K). Отсюда возникает задача построения символа $(a,b)_{r,\mathfrak{P}}$, а впоследствии и всей локальной теории полей классов, более явным и естественным образом. Эта задача решается с помощью получения явных формул для символа $(a,b)_{r,\mathfrak{P}}$ и его переопределения через данные формулы в виде вычета некоторого ряда.

Данная аналогия была развита в работе С. В. Востокова и М. А. Иванова [7]. В ней явная формула символа была построена с помощью интеграла Шнирельмана, являющегося прямым аналогом контурного интеграла, и с её помощью прояснена вышеописанная аналогия для кругового поля. В данной работе для некоторых специальных функций $\Phi(\alpha,\beta)$ и s показано, что

$$\int_{0,p} \Phi(\alpha,\beta)/s = \operatorname{res}_X(\Phi(\alpha,\beta)/s),$$
$$(\alpha,\beta)_{n,K} = \zeta^{\int_{0,p}\Phi(\alpha,\beta)},$$

где $\int_{0,p}$ — интеграл Шнирельмана, $(\cdot,\cdot)_{n,K}$ — локальный символ Гильберта порядка n, ζ — первообразный корень степени p^n из единицы, содержащийся в поле K. Отсюда для кругового поля $\mathbb{Q}(\zeta)$ выводится следующий результат:

$$\begin{array}{ccc} \left(\dfrac{\alpha}{\beta}\right)_{p^n}\left(\dfrac{\beta}{\alpha}\right)_{p^n}^{-1} & = & \zeta^{\int\Phi(\alpha,\beta)/s} \\ \| & & \| \\ \left(\dfrac{\alpha,\,\beta}{\zeta-1}\right)_{p^n} & = & \zeta^{\operatorname{res}\Phi(\alpha,\beta)/s}, \end{array}$$

где в левом столбце оказывается закон взаимности, а в правом аналог теоремы Коши.

Задача построения явных формул, описанных выше, для символа Гильберта имеет долгую историю. Её началом можно считать ещё работу Э. Куммера [8]. Другой тип явных формул имеет свои корни в работе Артина и Хассе 1928 года [9]. Дальнейшее развитие построения явных формул для символа Гильберта шло по двум направлениям — построение формул типа Артина-Хассе и типа Куммера. Формулы типа Куммера представляют символ Гильберта в виде вычета определённого ряда. В формулах типа Артина-Хассе символ Гильберта выражается через след некоторого элемента, при этом на нормирование второго аргумента накладывается некоторое ограничение, делающее формулы неполными.

Формулы Куммеровского типа получили своё продолжение в работе И. Р. Шафаревича [6]. Более элементарные формулы в общем случае были получены в конце семидесятых годов независимо С. В. Востоковым [10] и Г. Брюкнером [11]. В работе Востокова был преобразован и развит подход, использованный Шафаревичем. Метод, предложенный в этой работе, был впоследствии успешно применён в значительном количестве других важных случаев. Схема развитая С. В. Востоковым была многократно использована в целом ряде работ связанных с построением формул типа Куммера.

Теория полей классов для многомерного локального поля была построена в конце семидесятых годов независимо в случае нулевой характеристики К. Като в серии работ [12—15] и более явным образом, с учётом топологии в случае ненулевой характеристики А. Н. Паршиным [16—19]. В этих работах было построено отображение Паршина-Като, выполняющее роль отображения взаимности многомерной локальной теории полей классов.

Явные формулы для мультипликативного случая в многомерном разнохарактеристическом поле построил Востоков в работе [20]. Эти формулы, в частности, сыграли важную роль в явном построении локальной теории полей классов многомерного разнохарактеристического поля, проведённом И. Б. Фесенко [21]. В дальнейшем для многомерного поля явные формулы были также построены в работе [22] для поля смешанной характеристики, в работах [23; 24] для полей конечной характеристики с квазиконечным и совершенным полем вычетов, в работах [25; 26] для формальных групп Хонды, в работе [27] для формальных групп Любина-Тейта.

В первой главе данной работы метод С. В. Востокова применяется для получения явной формулы подобного рода для многочленной формальной группы.

Другой интересной специализацией теоремы Коши о вычетах является комбинаторная теорема о нулях (Combinatotial Nullstellensatz).

Теорема (Алон)**.** *Пусть* $\mathbb{F}$ *— произвольное поле и пусть* $F = F(x_1, \ldots, x_n)$ *многочлен из* $\mathbb{F}[x_1, x_2, \ldots, x_n]$*. Предположим также, что степень* $\deg(F)$ *многочлена* F *равна* $\sum_{i=1}^{n} d_i$*, где* d_i *— целые неотрицательные числа. Пусть кроме того, коэффициент при мономе* $\prod x_i^{d_i}$ *в* F *не равен нулю. Тогда если множества* $C_1, C_2, \ldots, C_n \subset \mathbb{F}$ *таковы, что* $|C_i| > d_i$*, то найдутся такие* $c_1 \in C_1$*, …,* $c_n \in C_n$*, что*

$$F(c_1, \ldots, c_n) \neq 0.$$

Несмотря на свою достаточно короткую историю, этот результат успел зарекомендовать себя в качестве мощного инструмента в комбинаторике. Впервые метод, использующие идеи, лежащие в основе комбинаторной теоремы о нулях, был представлен в работе [28] в 1996 году и использован для получения новых вариантов теоремы Коши-Девенпорта. В 1999 Н. Алон [29] сформулировал данные идеи в виде комбинаторной теоремы о нулях и продемонстрировал широкий спектр её возможностей в ряде областей комбинаторики. Усиленная версия комбинаторной теоремы о нулях была независимо получена М. Ласоном [30] и Р. Н. Карасёвым и Ф. В. Петровым [31].

Интересным вопросом является понимание алгебраической природы комбинаторной теоремы о нулях. В частности, удачное обобщение результата могло бы найти применение в получении нового подхода к таким результатам как соотношения Макдональда над системами корней. Н. Алон в своей работе [29] проводил аналогию между комбинаторной теоремой о нулях и теоремой Гильберта о нулях (отсюда и название). В работе [31] была предложена аналогия с интерполяционной формулой Лагранжа, которая и привела к формуле (**??**). Р. Н. Карасёвым [32] было отмечено, что по своей сути формула (**??**) есть вариант теоремы Коши о вычетах. Более того, в случае комплексного поля им был представлен прямой вывод комбинаторной теоремы о нулях (**??**), из следующей формы теоремы о вычетах.

Теорема. *Пусть $D_1, \ldots, D_n$ дивизоры на компактном аналитическом многообразии M размерности n, пересечение которых имеет нулевую размерность. Тогда для любой голоморфной формы $\omega \in \Omega^n(M \setminus \cup_{i=1}^n D_i)$ имеет место соотношение:*

$$\sum_{x \in D_1 \cap \ldots \cap D_n} \operatorname{res}_x \omega = 0.$$

Также можно отметить, что формула (**??**) следует из основного результата работы [33], который был получен в качестве обобщения формулы Эйлера-Якоби.

Во второй главе рассматриваются обобщения комбинаторной теоремы о нулях и их применение к комбинаторике.

Последняя глава работы посвящена применению новой версии комбинаторной теоремы о нулях, описанной во второй главе, к гипотезе Форрестера [34]. Даётся положительный ответ на эту гипотезу, и в едином стиле устанавливается подход ко многим аналогичным соотношениям. Ниже приведена краткая история вопроса.

Наиболее известным из соотношений, о которых идет речь, является соотношение Дайсона. В 1962 году Ф. Дайсон [35] предложил заменить классические модели случайных матриц Вигнера (основанные на распределении Гаусса) тем, что сейчас носит название круговых ансамблей. Изучение плотности совместного распределения их собственных чисел привело Дайсона к следующей гипотезе. Рассмотрим семейство многочленов Лорана:

$$\mathcal{D}(\boldsymbol{x}; \boldsymbol{a}) := \prod_{1 \le i \ne j \le n} \left(1 - \frac{x_i}{x_j}\right)^{a_i}$$

параметризованное набором неотрицательных целых чисел $\boldsymbol{a} = (a_1, \ldots, a_n)$, где $\boldsymbol{x} = (x_1, \ldots, x_n)$ — независимые переменные. Обозначая через $\mathrm{CT}[\mathcal{L}(\boldsymbol{x})]$ свободный член многочлена Лорана $\mathcal{L} = \mathcal{L}(\boldsymbol{x})$, гипотезу Дайсона можно переписать в виде соотношения:

$$\mathrm{CT}[\mathcal{D}(\boldsymbol{x}; \boldsymbol{a})] = \frac{(a_1 + a_2 + \cdots + a_n)!}{a_1! a_2! \ldots a_n!} =: \binom{|\boldsymbol{a}|}{\boldsymbol{a}},$$

где $|\boldsymbol{a}| = a_1 + a_2 + \cdots + a_n$.

Гипотеза Дайсона была доказана Д. Гансоном и К. Вилсоном [36] в том же году.

В 1975 году Г. Эндрюс [37] выдвинул в качестве гипотезы q-аналог соотношения Дайсона. Эта версия соотношения оказалось куда сложнее и, несморя на ряд предпринятых попыток [38—40], задача была решена лишь в 1985 году в работе Д. Зейлбергера и Д. Брессоуда [41]. В 2012 году вариант комбинаторный теоремы о нулях предложенный Р. Н. Карасёвым и Ф. В. Петровым [31], привел к очень короткому доказательству q-версии соотношения Дайсона в работе Г. Каройи и З. Нади [42].

Соотношение Дайсона и подобные ему тесно связаны с так называемой интегральной формулой Селберга [43], интерес к которой вызван её связью с теорией случайных матриц, статистической механикой, специальной теорией функции и другими областями. Исчерпывающий обзор можно найти в работе [44]. Для нас же интересна равносильная переформулировка интегральной формулы Селберга в виде соотношения Морриса:

$$\mathrm{CT}\left[\prod_{j=1}^{n}(1-x_j)^a(1-1/x_j)^b\mathcal{D}(\boldsymbol{x};k)\right] = \prod_{j=0}^{n-1}\frac{(a+b+kj)!(kj+k)!}{(a+kj)!(b+kj)!k!},$$

где параметры a, b, k являются целыми неотрицательными числами (подробности приведены в работе [45]).

В 1987 году Аомото [46] доказал расширенную версию интегральной формулы Селберга.

В своей работе 1995 года [34] Форрестер начал изучение аналога интегральной формулы Селберга для некоторой волновой функции основного состояния. Представленный в виде свободного члена полинома Лорана

$$\mathcal{F}(\boldsymbol{x};n_0;a,b,k) = \mathcal{M}(\boldsymbol{x};a,b,k)\prod_{n_0<i\neq j\leq n}\left(1-\frac{x_i}{x_j}\right),$$

где $\mathcal{M}(\boldsymbol{x};a,b,k)$ — полином из соотношения Морриса, нормирующий множитель для наиболее интересного случая может быть переписан в виде следующего гипотетического тождества:

$$\mathrm{CT}\left[\mathcal{F}(\boldsymbol{x};n_0;a,b,k)\right] =$$
$$= M(n_0;a,b,k)\times\prod_{j=0}^{n-n_0-1}\frac{(j+1)(a+b+kn_0+(k+1)j)!(kn_0+(k+1)j+k)!}{(a+kn_0+(k+1)j)!(b+kn_0+(k+1)j)!k!}.$$

В работе [47] был сформулирован и изучался q-аналог описанной выше гипотезы Форрестера. Несмотря на ряд предпринятых попыток [48—54], эти гипотезы были доказаны лишь в некоторых конкретных случаях. В третьей главе данной работы получено полное доказательство гипотезы Форрестера и её q-версии, основанное на комбинаторной теореме о нулях.

Целью работы является: построение явной формулы символа Гильберта $(\cdot,\cdot)_c$ относительно многочленной формальной группы $F_c(X,Y) = X+Y+cXY$, где c — единица в поле K, для одномерного локального поля и многомерного разнохарактеристического локального поля, которая известным образом приводит к явному закону взаимности относительно данной формальной группы; изучение приложений комбинаторной теоремы о нулях в алгебраической комбинаторике; изучение обобщений комбинаторной теоремы о нулях и её применение к вопросам соотношений на свободные члены полиномов Лорана.

Актуальность темы. вопросов, рассмотренных в первой главе, подтверждается большим количеством работ многих известных математиков, посвященных явным формулам символа Гильберта, конструктивным подходам к локальной теории полей классов, и связанными с этими вопросами приложениями в криптографии. Актуальность второй и третьей главы подтверждается текущим бурным развитием рассматриваемой области, множеством работ, посвященных различным приложениям комбинаторной теоремы о нулях в алгебраической комбинаторике, а также связью полученных результатов с теоретической квантовой физикой, в которой и была поставлена гипотеза Форрестера.

Научная новизна: впервые явные формулы символа Гильберта получены для формальной группы, коэффициенты которой не обязаны лежать в подполе инерции поля K. Получены новые обобщения комбинаторной теоремы о нулях. Дан положительный ответ на гипотезу Форрестера, являвшуюся до этого момента открытой. Все основные результаты, представленные в работе, являются оригинальными.

Теоретическая и практическая значимость. Работа носит теоретический характер. Результаты первой главы работы могут быть использованы в дальнейших исследованиях явных форм символа Гильберта в более общих случаях и для построения конструктивного подхода к локальным теориям полей классов по аналогии с мультипликативным случаем. Результаты второй и третьей главы могут быть использованы для приложений в комбинаторике и соотношениях по типу Дайсона, играющих важную роль в моделях случайных матриц, подтверждение гипотезы Форрестера важно также для теоретической квантовой физики.

Методология и методы исследования. В работе используются методы общей теории локальных полей, локальной теории полей классов и теории формальных групп, а также полиномиальный метод в комбинаторике. Работа применяет подход к явным формулам Гильберта Куммеровского типа, представленный С. В. Востоковым, а также комбинаторную теорему о нулях в форме, представленной Р. Н. Карасёвым и Ф. В. Петровым.

Основные положения, выносимые на защиту:

1. Явная формула символа Гильберта $(\cdot,\cdot)_c$ многочленной формальной группы F_c в разнохарактеристическом многомерном локальном поле.
2. Обобщение комбинаторной теоремы о нулях для аффиных гиперповерхностей.
3. Обобщение комбинаторной теоремы о нулях на Эрмитову интерполяцию.
4. Неравенство Коши-Дэвенпорта для алгебраической сложности.
5. Положительный ответ на гипотезу Форрестера.

Достоверность результатов и апробация работы. Достоверность полученных результатов обеспечивается их строгим математическим доказательством. Основные результаты работы докладывались на Санкт-Петербургском алгебраическом семинаре имени Д. К. Фаддеева, на Санкт-Петербургском семинаре по формальным группам и теории ветвления (рук. проф. С. В. Востоков) и в виде выносного доклада на международной конференции

«Arithmetic Days» (2013). Результаты находятся в соответствии с результатами, полученными другими авторами.

Публикации. Основные результаты по теме диссертации изложены в рецензируемых научных изданиях [1—5], рекомендованных ВАК. Работы [1—5] написаны в соавторстве. В работе [1] диссертанту принадлежат построение формального спаривания, док-во основной леммы и проекция формального спаривания на числа (разделы 3, 5, 7, 8), остальные результаты получены совместно. В работах [2; 3] диссертантом получены независимость спаривания от разложения в аргументы, лемма о замене переменной и основная теорема (разделы 4, 5, 6 работы [3]), остальные результаты получены совместно. В работе [4] диссертанту принадлежат результаты изложенные в §1, результаты §2 получены Ф. В. Петровым. В работе [5] общий план и основной результат в виде доказательства гипотезы Форрестера были получены независимо диссертантом совместно с Ф. В. Петровым, и Г. Каройи совместно с З. Нади. В частности диссертантом получена версия комбинаторной теоремы о нулях с Эрмитовой интерполяцией (теорема 2.4), Ф. В. Петрову принадлежит идея тензорного подхода к подобным теоремам (лемма 2.1), остальные части доказательства получены ими совместно. Г. Каройи и З. Надю принадлежит альтернативный подход к последнему шагу доказательства основного тождества, изложенный в пункте 7.4. Совместно всеми авторами получены остальные части работы, в частности обобщение гипотезы Форрестера в виде тождества Аомото-Форрестера (теорема 6.2). С. В. Востокову принадлежит общее руководство диссертационной работой.

Объем и структура работы. Диссертация состоит из введения и трёх глав. Полный объём диссертации составляет 86 страниц. Список литературы содержит 111 наименований.

Содержание работы

Во введении обсуждаются рассматриваемые в диссертации задачи, излагается история вопроса и даётся обзор состояния исследований в области, формулируются основные результаты диссертации, описывается структура диссертации.

Первая глава посвящена основным определениям, вспомогательным сведениям и ранее известным результатам, которые используются в последующих главах. Основные результаты работы изложены во второй, третьей и четвертой главе.

Во второй главе диссертации использованы стандартные для локальной теории полей классов обозначение. Через K обозначается основное рассматриваемое (многомерное) локальное поле характеристики ноль, содержащее корень p^m-ой степени из единицы ζ. Максимальный идеал кольца целых $\mathcal{O}_K$ поля K обозначается $\mathfrak{M}$. Действие формальной группы $F_c = X+Y+cXY$ задаёт на идеале $\mathfrak{M}$ структуру формально $\mathbb{Z}_p$-модуля $F_c(\mathfrak{M})$. Через $[a]_c$ обозначается a-изогения формальной группы F_c. Подполе инерции поля K обозначено через T. Стандартным образом автоморфизм Фробениуса в $T/\mathbb{Q}_p$ продолжается на кольцо рядов над $\mathcal{O}_T$ — кольцом целых поля T. Группа представителей Тейхмюллера в поле K обозначается $\mathfrak{R}$. Напоминаются классические определения и основные свойства мультипликативных функций Артина-Хассе E и ℓ.

Классический символ Гильберта относительно формальной группы F_c, в случае одномерного локального поля K несложно задать с помощью стандартной локальной теории полей классов. Отображение Артина устанавливает изоморфизм между мультипликативной группой локального поля и группой Галуа максимального абелевого расширения

$$\Xi\colon K^* \to \mathrm{Gal}(K^{ab}/K)\,.$$

Для элемента $\beta \in K$ вводится обозначение $[p^m]_c^{-1}(\beta)$, символизирующее любое из решений уравнения $[p^m]_c(t) = \beta$. Тогда символ Гильберта $(\cdot,\cdot)_c$ относительно формальной группы F_c задаётся следующим образом:

$$(\alpha,\beta)_c = [p^m]_c^{-1}(\beta)^{\Xi(\alpha)} -_{F_c} [p^m]_c^{-1}(\beta)\,,$$

где $\alpha \in K^*$, $\beta \in F_c(\mathfrak{M})$. Легко видеть, что правая часть не зависит от конкретного выбора $[p^m]_c^{-1}(\beta)$ и лежит в $\langle\xi\rangle_c$, где ξ — корень изогении $[p^m]_c$. Из основных свойств отображения взаимности Артина немедленно следуют ключевые свойства символа $(\cdot,\cdot)_c$: билинейность, символьное свойство и норменное свойство.

В многомерном случае аналогичное построение можно осуществить с помощью отображения Паршина-Като:

$$\Xi\colon K_n(K^*) \to \mathrm{Gal}(K^{ab}/K)\,,$$

где K_n — K-группа Милнора. Построение и свойства данного отображения описаны, например, в [12—14].

Далее в первой главе описываются примарные элементы, построенные в работах [10], [20] и некоторые технические вспомогательные утверждения.

Вторая часть первой главы посвящена некоторым предварительным сведениям из соответствующих областей алгебраической комбинаторики, необходимым в главах 3 и 4. В частности дан формульный вариант комбинаторной теоремы о нулях, изученный Р. Н. Карасёвым и Ф. В. Петровым в работе [31]:

Теорема 1. *Пусть $\mathbb{F}$ произвольное поле и $F \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ многочлен степени не выше $\deg(F) \leq d_1 + d_2 + \cdots + d_n$. Тогда для любых множеств $C_1, C_2, \ldots, C_n$ в $\mathbb{F}$ таких, что $|C_i| = d_i + 1$, коэффициент при мономе $\prod x_i^{d_i}$ в F равен*

$$\sum_{c_1 \in C_1} \sum_{c_2 \in C_2} \cdots \sum_{c_n \in C_n} \frac{F(c_1, c_2, \ldots, c_n)}{\phi_1'(c_1)\phi_2'(c_2)\ldots\phi_n'(c_n)},$$

где $\phi_i(z) = \prod_{c \in C_i}(z - c)$.

Во **второй главе** явная формула символа Гильберта для многочленной формальной группы F_c строится для многомерного разнохаратеристического локального поля K.

Общий план построения состоит в следующем: сначала производится формальная замена простого элемента верхнего поля π на независимую переменную t_n, затем все необходимые построения производятся над кольцом рядов $\mathcal{O}_T\{\{t_1\}\}\ldots\{\{t_{n-1}\}\}((t))$ — формальным аналогом поля K, полученное спаривание с помощью разложения элементов K в ряды по системе униформизующих $t_1, \ldots, t_{n-1}, \pi$ с коэффициентами из $\mathcal{O}_T = W(K^{(0)})$ — кольца векторов Витта над последним полем вычетов K (и проекции $t_n \mapsto \pi$) переносится на числа, наконец с помощью вычислений на базисе Гензеля проверяется идентичность построенного спаривания и символа Гильберта $(\cdot,\cdot)_c$. Тем самым для символа Гильберта даётся явная формула, описанная в построении формального спаривания над рядами.

В начале главы определяются аналоги функций Артина-Хассе относительной формальной группы F_c, проверяются их основные свойства.

Затем явной формулой задаётся спаривание $[\cdot,\cdot]_c\colon \mathcal{H}_{\mathfrak{m}}{}^n \times \mathcal{H}_{\mathfrak{c}} \to \mathcal{O}_T/p^m$, где $\mathcal{H}_{\mathfrak{m}}$, $\mathcal{H}_{\mathfrak{c}}$ — группа и кольцо рядов от n переменных с коэффициентами в поле T (поле частных OO_T) соответствующие группе K^* и максимальному идеалу $\mathfrak{M}$ кольца целых (относительно n-мерного нормирования) $\mathcal{O}_K$ поля K.

Далее проверяется свойство билинейности спаривания $[\cdot,\cdot]_c$. В едином ключе с помощью индукции по размерности n доказывается символьное свойство и ряд других ключевых для многомерного случая свойств: кососимметричность, гиперболичность и соотношение Стейнберга.

С помощью этих утверждений спаривание $[\cdot,\cdot]_c$ преобразуется в спаривание $\langle\cdot,\cdot\rangle_c : K_n(\mathcal{H}_{\mathfrak{m}}) \times \mathcal{H}_{\mathfrak{c}} \to \mathcal{O}_T/p^m$. Далее проверяются свойства независимости спаривания от разложения аргументов в ряд и замены переменной. С их помощью формальное спаривание $\langle\cdot,\cdot\rangle_c$ проецируется на числа в виде спаривания $\{\cdot,\cdot\}_c\colon K^* \times F_c(\mathfrak{M}) \to \langle\xi\rangle$. Классический символ Гильберта $(\cdot,\cdot)_c$ в этом случае задаётся с помощью отображения Паршина-Като $\Xi\colon K_n(K^*) \to \mathrm{Gal}(K^{ab}/K)$. Наконец доказывается теорема, являющаяся основным результатом второй главы:

Теорема. *Для любых элементов $\alpha \in K_n(K)$ и $\beta \in F_c(\mathfrak{M})$ значения спариваний $\{\cdot,\cdot\}_c$ и $(\cdot,\cdot)_c$ совпадают:*

$$\{\alpha,\beta\}_c = (\alpha,\beta)_c\,.$$

Третья глава работы посвящена обобщениям комбинаторной теоремы о нулях и их приложениям к комбинаторике.

В начале главы описывается абстрактный подход к комбинаторной теореме о нулях, как к некоторому утверждению о координатах тензоров. В этом стиле даётся новое доказательство теоремы 1 (сформулированной в несколько более сильной форме). Затем формулируется доказывается обобщение данной теоремы на случай мультимножеств.

Теорема. *Пусть* $F \in \mathbb{F}[x_1, \ldots, x_n]$ *многочлен, причем ни один его моном не мажорирует моном* $M = \prod x_i^{d_i}$. *Пусть также* $C_1, \ldots, C_n$ *произвольные мультимножества в* $\mathbb{F}$ *с соответствующими функциями кратности* $\omega_1, \ldots, \omega_n$, *такие что* $|C_i| = d_i + 1$ *для каждого* i. *Потребуем также, чтобы либо* $\mathrm{char}(\mathbb{F}) = 0$ *либо* $\mathrm{char}(\mathbb{F}) \geq \omega_i(c)$ *при всех* i *и* $c \in \mathbb{F}$. *Тогда коэффициент при мономе* M *у многочлена* F *может быть вычислен следующим образом*

$$[M]F = \sum_{c_1 \in C_1} \sum_{m_1 < \omega_1(c_1)} \cdots \sum_{c_n \in C_n} \sum_{m_n < \omega_n(c_n)} \prod_{i=1}^{n} \kappa(C_i, c_i, m_i) \frac{\partial^{m_1 + \cdots + m_n} F}{\partial x_1^{m_1} \ldots \partial x_n^{m_n}}(c_1, \ldots, c_n),$$

где

$$\kappa(C_i, c_i, m_i) = \frac{1}{m_i! \cdot (\omega_i(c_i) - 1 - m_i)!} \cdot \left(\frac{1}{\prod_{c \in C_i \setminus \{c_i\}} (x - c)^{\omega_i(c)}} \right)^{(\omega_i(c_i) - 1 - m_i)} \Bigg|_{x = c_i}.$$

В частности, если $[M]F \neq 0$, *то существует система представителей* $c_i \in C_i$ *с кратностями* $m_i < \omega_i(c_i)$, *такая что*

$$\frac{\partial^{m_1 + \cdots + m_n} F}{\partial x_1^{m_1} \ldots \partial x_n^{m_n}}(c_1, \ldots, c_n) \neq 0.$$

Рассматривается также ещё одно обобщение комбинаторной теоремы о нулях, связанное с переходом от поля к аффинным пространствам над ним.

Далее в третьей главе рассматриваются различные приложения вышеописанных теорем к задачам комбинаторики. Эти приложения в основном посвящены задачам о размерах множеств сумм с ограничениями. А именно рассмотрим семейство подмножеств циклической группы $\mathbb{Z}_{(p)} := \mathbb{Z}/p\mathbb{Z}$ порядка p и обозначим его $\mathcal{S} = \{S_{ij} \mid 1 \leq i < j \leq n\}$. Для произвольного набора подмножеств $A_1, \ldots, A_n \subseteq \mathbb{Z}_{(p)}$ рассмотрим следующее множество сумм с ограничениями:

$$\bigwedge\nolimits_{\mathcal{S}} A_i = \{a_1 + \cdots + a_n \mid a_i \in A_i,\, a_j - a_i \notin S_{ij} \text{ for } i < j\}.$$

В случае $S_{ij} = \varnothing$ оценка $|\bigwedge_{\mathcal{S}} A_i| \geqslant \min\{p, \sum |A_i| - n + 1\}$ представляет собой классическую теорему Коши-Дэвенпорта. В случае $S_{ij} = 0$ оценка $|\bigwedge_{\mathcal{S}} A_i| \geq$

$\min\{p, n|A| - n^2 + 1\}$ является гипотезой Эрдёша-Гейлброна [55], впервые доказанной Дж. Диас да Сильвой и Я. Хэмидоном [56]. Элементарный подход к этим утверждениям с помощью полиномиального метода был получен в работе [28].

Этот подход теперь развивается и применяется для доказательства ряда утверждений о размерах множеств сумм с ограничениями $\bigwedge_{\mathcal{S}} A_i$.

В заключении третьей главы комбинаторная теорема о нулях для аффинных пространств используется для получения неравенства Коши-Дэвенпорта для алгебраической сложности.

Определение 1. Пусть $\mathbb{F}$ — поле, A — непустое подмножество аффинного пространства $\mathbb{F}^n$. Назовем *алгебраической сложностью* множества A минимальную степень гиперповерхности H, содержащей A:

$$w(A) := \inf\{\deg H \mid H \supset A, H \text{ — аффинная гиперповерхность в } \mathbb{F}^n\}.$$

Понятие *алгебраической сложности* тесно связано с понятием алгебраической иммунности булевых функций в случае поля характеристики 2, которое изучается, например, в работах [57—60].

Предложение 1 (Неравенство Коши – Дэвенпорта для алгебраической сложности)**.** *Пусть $p(\mathbb{F})$ — аддитивный порядок единицы в поле $\mathbb{F}$. Пусть A, $B \subset \mathbb{F}^n$ — конечные непустые подмножества. Тогда*

$$w(A + B) \geqslant \min\{p(\mathbb{F}), w(A) + w(B) - 1\}.$$

В **четвертой главе** работы изучаются соотношения на свободный член полиномов Лорана и подход к ним с помощью комбинаторной теоремы о нулях. Основным результатом главы является получение положительного ответа на гипотезу Форрестера (включая её q-версию).

Исторически первым соотношением рассматриваемого в данной главе типа является, описанное в введении, соотношение Дайсона. В первой части четвертой главы доказано следующее обобщение соотношения Дайсона (частный случай гипотезы Каделла [61]):

Теорема. *Пусть $m < n$. Тогда*

$$\mathrm{CT}\left[\prod_{1\le i<j\le n}\left(\frac{x_i}{x_j}\right)_{a_i}\left(\frac{qx_j}{x_i}\right)_{a_j^*}\right] = \frac{1-q^{1+|\boldsymbol{a}|}}{1-q^{1+\sum_{v=m+1}^{n} a_v}}\begin{bmatrix}|\boldsymbol{a}|\\ \boldsymbol{a}\end{bmatrix},$$

где $a_n^* = a_n + \chi(i \le m)$ и $a_j^* = a_j$ в противном случае.

Далее приводится новое, основанное на комбинаторной теореме о нулях, доказательство соотношения Морриса [45] и его q-версии:

$$\mathrm{CT}\left[\prod_{j=1}^{n}(1-x_j)^a(1-1/x_j)^b\mathcal{D}(\boldsymbol{x};k)\right] = \prod_{j=0}^{n-1}\frac{(a+b+kj)!(kj+k)!}{(a+kj)!(b+kj)!k!};$$

$$\mathrm{CT}\left[\prod_{j=1}^{n}(qx_j)_a(1/x_j)_b\mathcal{D}_q(\boldsymbol{x};k)\right] = \prod_{j=0}^{n-1}\frac{(q)_{a+b+kj}(q)_{kj+k}}{(q)_{a+kj}(q)_{b+kj}(q)_k}.$$

В данном доказательстве (как и в последующих в этой главе) ключевую роль играет общность полученной ранее комбинаторной теоремы о нулях с кратностями. Лишь часть случаев может быть доказана с помощью стандартной формулы теоремы 1.

Далее вводится матричная запись рассматриваемых соотношений. А именно через $\boldsymbol{B} = (\beta_{ij})$ обозначим $(n+1)\times(n+1)$ матрицу со строками и столбцами, пронумерованными от 0 до n. При некоторых условиях корректности, такой матрице можно сопоставить многочлен Лорана

$$\mathcal{L}(x_0,\boldsymbol{x};\boldsymbol{B}) = \prod_{0\le i\ne j\le n}\left(1-\frac{x_i}{x_j}\right)^{\beta_{ij}}$$

и его q-аналог

$$\mathcal{L}_q(x_0,\boldsymbol{x};\boldsymbol{B}) = \prod_{0\le i<j\le n}\left(\frac{x_i}{x_j}\right)_{\beta_{ij}}\left(\frac{qx_j}{x_i}\right)_{\beta_{ji}}.$$

В этих обозначениях соотношение Аомото и гипотеза Форрестера объединяются в одно, более общее утверждение. А именно, при $m \ge n - n_0$

рассматривается следующая матрица:

$$\boldsymbol{B}_{\mathcal{AF}} = \left(\begin{array}{c|ccc|ccc|ccc} 0 & b & \dots & b & b & \dots & b & b & \dots & b \\ \hline a & 0 & \dots & k & k & \dots & k & k & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a & k & \dots & 0 & k & \dots & k & k & \dots & k \\ \hline a+1 & k & \dots & k & 0 & \dots & k & k & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a+1 & k & \dots & k & k & \dots & 0 & k & \dots & k \\ \hline a+1 & k & \dots & k & k & \dots & k & 0 & \dots & k+1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a+1 & k & \dots & k & k & \dots & k & k+1 & \dots & 0 \end{array}\right) \quad \begin{array}{c} 0 \\ \hline 1 \\ \vdots \\ n-m \\ \hline n-m+1 \\ \vdots \\ n_0 \\ \hline n_0+1 \\ \vdots \\ n \end{array}.$$

Для такой матрицы демонстрируется справедливость следующего соотношения Аомото-Форрестера.

Теорема. *Пусть n натуральное число. Для произвольных целых неотрицательных чисел a,b,k и m,$n_0 \leq n \leq m+n_0$ имеет место*

$$\mathrm{CT}[\mathcal{L}_q(x_0,\boldsymbol{x};\boldsymbol{B}_{\mathcal{AF}})] = \prod_{j=0}^{n-1} \frac{(q)_{a+b+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}(q)_{kj+\chi(j>n_0)(j-n_0)+k}}{(q)_{a+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}(q)_{b+kj+\chi(j>n_0)(j-n_0)}(q)_k} \times$$
$$\times \prod_{j=1}^{n-n_0} \frac{1-q^{(k+1)j}}{1-q^{k+1}}.$$

В случае $m = 0$, из этой теоремы следует гипотеза Бейкера и Форрестера (гипотеза 2.1 [47]), а при специализации в $q = 1$ получается соответственно оригинальная гипотеза Форрестера. Случай же $n_0 = n$ дает q-аналог соотношения Аомото.

Этот результат является основным результатом четвертой главы и завершает работу.

Публикации автора по теме диссертации

1. *Востоков С. В.*, *Волков В. В.* Явная форма символа Гильберта для многочленных формальных модулей // Алгебра и анализ. — 2014. — Т. 26, № 5. — С. 125—141.
2. *Востоков С. В.*, *Волков В. В.*, *Бондарко М. В.* Явная форма символа Гильберта для многочленных формальных модулей в многомерном локальном поле I // Зап. научн. сем. ПОМИ. — 2014. — Т. 430. — С. 53—60.
3. *Востоков С. В.*, *Волков В. В.* Явная форма символа Гильберта для многочленных формальных модулей в многомерном локальном поле II // Зап. научн. сем. ПОМИ. — 2016. — Т. 443. — С. 46—60.
4. *Волков В. В.*, *Петров Ф. В.* Некоторые обобщения теоремы Коши-Дэвенпорта // Зап. научн. сем. ПОМИ. — 2015. — Т. 432. — С. 105—110.
5. A new approach to constant term identities and Selberg-type integrals / G. Károlyi [и др.] // Advances in Mathematics. — 2015. — Т. 277. — С. 252—282.

Список литературы

6. *Шафаревич И. Р.* Общий закон взаимности // Матем. сб. — 1950. — Т. 26(68), № 1. — С. 113—146.
7. *Востоков С. В.*, *Иванов М. А.* Интегральная теорема Коши и классический закон взаимности // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. — 2012. — Т. 154. — С. 73—82.
8. *Kummer E.* Uber die allgemeinen Reziprozitatsgesetze der Potenzreste // J. reine und angew. Math. — 1858. — Jg. 56. — S. 270–279.
9. *Artin E.*, *Hasse H.* Die beiden Erganzungssatze zum Reziprozitatsgesetz der l^n-ten Potenzreste im Korper der l^n-ten Einheitswurzeln // Abh. Mathem. Seminar, Hamburg. — 1928. — Jg. 6. — S. 146–162.

10. *Востоков С. В.* Явная форма закона взаимности // Изв. АН СССР, Сер. матем. — 1978. — Т. 42, № 6. — С. 1288—1321.

11. *Bruckner H.* Explizites Reziprozitatsgesetz und Anwendungen // Vorlesungen aus dem Fachbereich Mathematik der Universitat Essen. — 1979.

12. *Kato K.* A generalization of local class field theory by using K-groups. I. // Proc. Jap. Acad. — 1977. — Vol. 53. — Pp. 140–143.

13. *Kato K.* A generalization of local class field theory by using K-groups. II. // Proc. Jap. Acad. — 1978. — Vol. 54. — Pp. 250–255.

14. *Kato K.* A generalization of local class field theory by using K-groups. II. // J . Fac. Sci. Univ, Tokyo. — 1979. — Vol. 26. — Pp. 303–376.

15. *Kato K.* The Existence theorem for higher local class field theory. — Inst. Hautes Etudes Sci. Publ. Math., preprint, 1980.

16. *Паршин А. Н.* Поля классов и алгебраическая K-теория // Успехи мат. наук. — 1975. — Т. 30, № 1. — С. 253—254.

17. *Паршин А. Н.* К арифметике двумерных схем. I. Распределения и вычеты. // Изв. АН СССР. Сер мат. — 1976. — Т. 40. — С. 736—773.

18. *Паршин А. Н.* Абелевы накрытия арифметических схем. // Докл. АН СССР. — 1978. — Т. 243, № 4. — С. 855—858.

19. *Паршин А. Н.* Локальная теория полей классов // Тр. Матем. ин-та им. В. А. Стеклова АН СССР. — 1984. — Т. 165. — С. 143—170.

20. *Востоков С. В.* Явная конструкция теории полей классов многомерного локального поля // Изв. АН СССР. Сер. матем. — 1985. — Т. 49, № 2. — С. 283—308.

21. *Фесенко И. Б.* Теория полей классов многомерных локальных полей нулевой характеристики с полем вычетов положительной характеристики // Алгебра и анализ. — 1991. — Т. 3, № 3. — С. 649—678.

22. *Востоков С. В.* Спаривание Гильберта в полном многомерном поле // Тр. МИАН, Наука, Физматлит, М. — 1995. — Т. 208. — С. 80—92.

23. *Беккер Б. М.* Абелевы расширения полного дискретно нормированного поля конечной высоты // Алгебра и анализ. — 1991. — Т. 3, № 6. — С. 76—84.

24. *Fesenko I. B.* Abelian extensions of complete discrete valuation fields and their norm groups // Adv. Sov. Math. — 1994.

25. *Vostokov S. V.*, *Lorenz F.* Honda Groups and Explicit Pairings on the Modules of Cartier Curves // Contemp. Math. — 2002. — Vol. 300. — Pp. 143–170.

26. *Востоков С. В.*, *Лоренц Ф.* Явная формула символа Гильберта для групп Хонды в многомерном локальном поле // Матем. сб. — 2003. — Т. 194:2. — С. 3—36.

27. *Востоков С. В.*, *Афанасьева С. С.*, *Беккер Б. М.* Символ Гильберта в многомерных локальных полях для формальной группы Любина–Тейта // Зап. научн. сем. ПОМИ. — 2012. — Т. 400. — С. 20—49.

28. *Alon N.*, *Nathanson M. B.*, *Ruzsa I. Z.* The polynomial method and restricted sums of congruence classes // J. Number Theory. — 1996. — Т. 56. — С. 404—417.

29. *Alon N.* Combinatorial Nullstellensatz // Combin. Probab. Comput. — 1999. — Т. 8. — С. 7—29.

30. *Lasoń M.* A generalization of Combinatorial Nullstellensatz // Electron. J. Combin. — 2010. — Т. 17.

31. *Karasev R. N.*, *Petrov F. V.* Partitions of nonzero elements of a finite field into pairs // Israel J. Math. — 2012. — Т. 192. — С. 143—156.

32. *Karasev R. N.* Residues and the Combinatorial Nullstellensatz. — 2015. — URL: `arXiv:1503.08004`.

33. Traces in strict Frobenius algebras and strict complete intersections / Kunz [u. a.] // Journal fur die reine und angewandte Mathematik. — 1987. — Jg. 381. — S. 181–204.

34. *Forrester P. J.* Normalization of the wavefunction for the Calogero–Sutherland model // Int. J. Mod. Phys. B. — 1995. — Т. 9. — С. 1243—1261.

35. *Dyson F. J.* Statistical theory of energy levels of complex systems. I // J. Math. Phys. — 1962. — Т. 3. — С. 140—156.

36. *Wilson K. G.* Proof of a conjecture by Dyson // J. Math. Phys. — 1962. — T. 3. — C. 1040—1043.

37. *Andrews G. E.* Problems and prospects for basic hypergeometric functions // Theory and Application of Special Functions. — New York : Academic Press, 1975. — C. 191—224.

38. *Kadell K. W. J.* A proof of Andrews's q-Dyson conjecture for $n = 4$ // Trans Amer. Math. Soc. — 1985. — T. 290. — C. 127—144.

39. *Stanley R. P.* The q-Dyson conjecture, generalized exponents, and the internal product of Schur functions // Combinatorics and Algebra. — Providence : Amer. Math. Soc., 1984. — C. 81—94.

40. *Stanley R. P.* The stable behavior of some characters of $\mathrm{SL}(n,\mathbb{C})$ // Lin. Multilin. Alg. — 1984. — T. 16. — C. 3—27.

41. *Zeilberger D.*, *Bressoud D. M.* A proof of Andrews' q-Dyson conjecture // Discrete Math. — 1985. — T. 54. — C. 201—224.

42. *Károlyi G.*, *Nagy Z. L.* A simple proof of the Zeilberger–Bressoud q-Dyson theorem // Trans Amer. Math. Soc. — 2014. — T. 142, № 9. — C. 3007—3011.

43. *Selberg A.* Bemerkninger om et multipelt integral // Norsk Mat. Tidsskr. — 1944. — T. 26. — C. 71—78.

44. *Forrester P. J.*, *O. W. S.* The importance of the Selberg integral // Bull. Amer. Math. Soc. (N. S.) — 2008. — T. 45. — C. 489—534.

45. *Morris W. G.* Constant Term Identities for Finite and Affine Root Systems: Conjectures and Theorems // Ph.D. Thesis, Univ. Wisconsin–Madison. — 1982.

46. *Aomoto K.* Jacobi polynomials associated with Selberg integrals // SIAM J. Math. Anal. — 1987. — T. 18. — C. 545—549.

47. *Baker T. H.*, *Forrester P. J.* Generalizations of the q-Morris constant term identity // J. Combin. Theory Ser. A. — 1998. — T. 81. — C. 69—87.

48. *Baratta W.* Some properties of Macdonald polynomials with prescribed symmetry // Kyushu J. Math. — 2010. — T. 64. — C. 323—343.

49. A unified elementary approach to the Dyson, Morris, Aomoto and Forrester constant term identities / I. M. Gessel [и др.] // J. Combin. Theory Ser. A. — 2008. — Т. 115. — С. 1417—1435.

50. *Hamada S.* Proof of Baker–Forrester's constant term conjecture for the cases $N_1 = 2{,}3$ // Kyushu J. Math. — 2002. — Т. 56. — С. 243—266.

51. *Kaneko J.* On Forrester's generalization of Morris constant term identity // q-series From a Contemporary Perspective. — Providence : Amer. Math. Soc., 2000. — С. 271—282.

52. *Kaneko J.* Forrester's constant term conjecture and its q-analogue // Physics and Combinatorics. — River Edge, NJ : World Sci. Publ., 2001. — С. 49—62.

53. *Kaneko J.* Forrester's conjectured constant term identity. II // Ann. Combin. — 2002. — Т. 6. — С. 383—397.

54. *Kaneko J.* On Baker–Forrester's constant term conjecture // J. Ramanujan Math. Soc. — 2003. — Т. 18. — С. 349—367.

55. *Erd P.*, *Graham R. L.* Old and New Problems and Results in Combinatorial Number Theory // L'Enseignement Mathématique. — 1980. — С. 203—228.

56. *Dias da Silva J. A.*, *Hamidoune Y. O.* Cyclic spaces for Grassmann derivatives and additive theory // Bull. London Math. Soc. — 1994. — Т. 26. — С. 140—146.

57. *Didier F.*, *Tillich J.-P.* Computing the Algebraic Immunity Efficiently // Fast Software Encryption: 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2006. — С. 359—374.

58. *Liu M.*, *Zhang Y.*, *Lin D.* Perfect Algebraic Immune Functions // Advances in Cryptology – ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. — С. 172—189.

59. Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks / F. Armknecht [и др.] // Advances in Cryptology - EUROCRYPT 2006: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006. Proceedings. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2006. — С. 147—164.

60. *Carlet C.* Algebraic Immunity of Boolean Functions // Encyclopedia of Cryptography and Security. — Boston, MA : Springer US, 2011. — С. 31—32.

61. *Kadell K. W. J.* Aomoto's machine and the Dyson constant term identity // Methods Appl. Anal. — 1998. — Т. 5. — С. 335—350.