ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 55 **2019** **Вып. 3**

УДК 621.391.15

© 2019 г. **И. Ланджев, А. Русева**

ДЕЛИМЫЕ ДУГИ, ДЕЛИМЫЕ КОДЫ И ЗАДАЧА О РАСШИРЕНИИ ДЛЯ ДУГ И КОДОВ[1]

Ранее авторами был разработан единый поход к задаче о расширении для дуг в $\mathrm{PG}(k-1,q)$, или, эквивалентным образом, для линейных кодов над конечными полями. Был введен специальный класс дуг, называемых $(t \bmod q)$-дугами, и было доказано, что свойство расширимости заданной дуги зависит от структуры специальной двойственной дуги, которая оказывается $(t \bmod q)$-дугой. Здесь изучается общая структура $(t \bmod q)$-дуг. Доказывается, что всякая такая дуга является суммой дополнений к гиперплоскостям. Кроме того, описываются такие дуги для малых значений t, что в случае $t = 2$ дает альтернативное доказательство теоремы Маруты о кодах, допускающих расширение. Этот результат геометрически эквивалентен утверждению, что любая 2-квазиделимая дуга в $\mathrm{PG}(k-1,q)$, $q \geqslant 5$, q нечетно, допускает расширение. В заключение наш подход применяется к задаче о расширении для шапок в $\mathrm{PG}(3,q)$.

Ключевые слова: конечные проективные геометрии, дуги, блокирующие множества, делимые дуги, квазиделимые дуги, граница Грайсмера, $(t \bmod q)$-дуги, дуги, допускающие расширение, шапки.

DOI: 10.1134/S0555292319030033

§ 1. Введение

Мы исследуем связь между возможностью расширения для дуг в конечных проективных геометриях (соответственно, линейных кодов над конечными полями) и их свойствами делимости. Для краткости мы не приводим основные понятия, относящиеся к дугам и кодам, а отсылаем читателя к [1, 2] для введения в конечную геометрию и к [3–5] для введения в теорию кодирования.

Линейный $[n,k,d]_q$-код называется грайсмеровым кодом, если его длина лежит на границе Грайсмера [6]:

$$n \geqslant g_q(k,d) := \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil. \tag{1}$$

Линейный $[n,k,d]_q$-код C называется кодом, допускающим t-расширение ($t \geqslant 1$), если существует линейный $[n+t,k,d+t]_q$-код C', такой что C может быть получен из C' t-кратным выкалыванием (удалением t координатных позиций во всех кодовых словах). В случае $t = 1$ их называют просто кодами, допускающими расширение.

[1] Работа выполнена при частичной финансовой поддержке Фонда научных исследований Софийского университета (контракт № 80-10-81/15.04.2019).

Линейный код над $\mathbb{F}_q$ называется делимым с делителем $\Delta > 1$, если вес каждого кодового слова кратен числу Δ. Почти очевидно, что если $(\Delta, q) = 1$, то код полной длины (т.е. код, в котором ни одна координатная позиция не является тождественно нулевой) является Δ-кратным повторением одного кода, т.е. конкатенацией Δ одинаковых кодов [7]. Несколько семейств классических кодов обладают нетривиальной делимостью. Самым ярким примером является семейство обобщенных кодов Рида–Маллера. Грайсмеровы коды с минимальным весом, делящимся на характеристику основного поля, также обладают свойством делимости. Процитируем замечательный результат из [7].

Теорема 1. *Пусть C – грайсмеров код над $\mathbb{F}_p$, где p – простое. Если минимальный вес кода C делится на p^e, то p^e является делителем кода.*

Линейный $[n,k,d]_q$-код называется t-квазиделимым по модулю Δ, если $d \equiv \equiv -t \pmod{\Delta}$ и все веса в коде сравнимы с $-t, \ldots, -1, 0$ по модулю Δ. Коды, получаемые t-кратным выкалыванием делимого кода с делителем Δ, являются t-квазиделимыми по модулю Δ. Довольно часто оказывается, особенно при малых значениях t, что t-квазиделимые коды допускают t-расширение до делимого кода. Так, например, классическая теорема Хилла–Лизака [8, 9] утверждает, что каждый линейный $[n,k,d]$-код с весами 0 и d по модулю q, где $(d,q) = 1$, допускает расширение до $[n+1,k,d+1]_q$-кода. Простейшим случаем здесь является $d \equiv -1 \pmod{q}$. Используя понятие квазиделимого кода, это можно сформулировать как утверждение, что любой 1-квазиделимый код допускает расширение. Недавно Марута [10–14] получил целый ряд результатов такого типа о возможности расширения. Наиболее интересный из них утверждает, что если $[n,k,d]_q$-код с нечетным $q \geqslant 5$ и $d \equiv -2 \pmod{q}$ имеет только веса $-2, -1, 0 \pmod{q}$, то он допускает расширение [12]. Это равносильно утверждению, что любой 2-квазиделимый код над полем порядка $q \geqslant 5$, где q нечетно, допускает расширение.

Попытка найти единый подход к вопросу о возможности расширения для кодов была сделана в [15], где эта задача рассматривалась с ее геометрической стороны. Хорошо известно, что линейные коды над конечными полями и дуги в конечных геометриях $\mathrm{PG}(k-1,q)$ – эквивалентные объекты: каждому линейному $[n,k,d]_q$-коду C можно поставить в соответствие $(n, n-d)$-дугу $\mathcal{K}_C$ в $\mathrm{PG}(k-1,q)$ (разумеется, не единственным способом), так что два кода C_1 и C_2 изоморфны тогда и только тогда, когда соответствующие им дуги $\mathcal{K}_{C_1}$ и $\mathcal{K}_{C_2}$ проективно эквивалентны [5, 16, 17]. Дуги, соответствующие кодам, лежащим на границе Грайсмера, называются грайсмеровыми дугами.

В настоящей статье мы применяем геометрический подход к задаче о расширении. Наша цель – описать свойство расширимости в терминах структуры некоторых дуг, называемых $(t \bmod q)$-дугами. С этой целью мы приводим различные конструкции и доказываем структурные результаты для $(t \bmod q)$-дуг, которые сами по себе являются интересными геометрическими объектами.

Статья имеет следующую структуру. В § 2 определяются $(t \bmod q)$-дуги и устанавливается связь между свойством расширимости для квазиделимых дуг и некоторыми структурными свойствами соответствующих $(t \bmod q)$-дуг. В § 3 приводятся общие результаты о $(t \bmod q)$-дугах. Многие из них относятся к случаю геометрий над простым полем $\mathbb{F}_p$. Мы описываем так называемую конструкцию поднятия для $(t \bmod q)$-дуг и доказываем, что над простым полем $\mathbb{F}_p$ всякая $(t \bmod p)$-дуга является суммой аффинных пространств, и следовательно, суммой поднятий дуг. Далее, § 4 посвящен $(2 \bmod q)$-дугам. Доказывается, что всякая $(2 \bmod q)$-дуга в $\mathrm{PG}(r,q)$ для нечетного $q \geqslant 5$ и $r \geqslant 3$ с точками кратностей 0, 1 и 2 является поднятием некоторой дуги. Из этого вытекает результат Маруты о возможности расширения для линейных кодов с весами $-2, -1, 0 \bmod q$ для нечетных $q \geqslant 5$. В § 5 наш подход применяется к задаче о расширении для шапок в $\mathrm{PG}(3,q)$.

§ 2. Квазиделимые дуги и свойство расширимости

Чтобы зафиксировать обозначения, изложим некоторые основные определения и факты о мультимножествах. Рассмотрим проективную геометрию $\Sigma = \mathrm{PG}(r,q)$, $r \geqslant 2$, $q = p^h$. Обозначим через $\mathcal{P}$ множество точек, а через $\mathcal{H}$ – множество гиперплоскостей геометрии Σ. Любое отображение $\mathcal{K}\colon \mathcal{P} \to \mathbb{N}_0$ из множества точек геометрии в множество целых неотрицательных чисел называется мультимножеством в Σ. По аддитивности это отображение продолжается на любое подмножество $\mathcal{Q}$ множества $\mathcal{P}$, т.е. $\mathcal{K}(\mathcal{Q}) = \sum_{P\in\mathcal{Q}} \mathcal{K}(P)$. Целое число $n := \mathcal{K}(\mathcal{P})$ называется мощностью мультимножества $\mathcal{K}$. Носителем $\mathcal{K}$ является множество всех точек положительной кратности:

$$\operatorname{supp}\mathcal{K} = \{P \in \mathcal{P} \mid \mathcal{K}(P) > 0\}.$$

Мультимножества с $\mathcal{K}(P) \in \{0,1\}$ называются проективными. Такие мультимножества можно рассматривать как обычные множества, отождествляя их с их носителями. Для каждого множества точек $\mathcal{Q} \subset \mathcal{P}$ определим его характеристическое (мульти)множество $\chi_{\mathcal{Q}}$ как

$$\chi_{\mathcal{Q}}(P) = \begin{cases} 1, & \text{если } P \in \mathcal{Q}, \\ 0 & \text{в противном случае.} \end{cases}$$

Обозначим через a_i количество гиперплоскостей H в Σ, таких что $\mathcal{K}(H) = i$. Последовательность (a_i) называется спектром мультимножества $\mathcal{K}$.

Мультимножества можно рассматривать как дуги или блокирующие множества. Мультимножество $\mathcal{K}$ в Σ называется (n,w)-мультидугой (или просто (n,w)-дугой), если

(1) $\mathcal{K}(\mathcal{P}) = n$;
(2) $\mathcal{K}(H) \leqslant w$ для любой гиперплоскости H;
(3) существует гиперплоскость H_0, для которой $\mathcal{K}(H_0) = w$.

Аналогично, мультимножество $\mathcal{K}$ в Σ называется (n,w)-блокирующим множеством относительно гиперплоскостей (в англоязычной литературе используется также термин (n,w)-minihyper), если

(1) $\mathcal{K}(\mathcal{P}) = n$;
(2) $\mathcal{K}(H) \geqslant w$ для любой гиперплоскости H;
(3) существует гиперплоскость H_0, для которой $\mathcal{K}(H_0) = w$.

Будем говорить, что (n,w)-дуга $\mathcal{K}$ в Σ допускает t-расширение, если существует $(n+t,w)$-дуга $\mathcal{K}'$ в той же геометрии, такая что $\mathcal{K}'(P) \geqslant \mathcal{K}(P)$ для любой точки $P \in \mathcal{P}$. Говорят, что дуга просто допускает расширение, если она допускает 1-расширение. Дуги, допускающие расширение, соответствуют кодам, допускающим расширение, и наоборот. Аналогично, (n,w)-блокирующее множество $\mathcal{K}$ в Σ назовем t-приводимым, если существует $(n-t,w)$-блокирующее множество $\mathcal{K}'$ в Σ, такое что $\mathcal{K}'(P) \leqslant \mathcal{K}(P)$ для любой точки $P \in \mathcal{P}$.

Скажем, что (n,w)-дуга $\mathcal{K}$ со спектром (a_i) делима с делителем $\Delta > 1$, если $a_i = 0$ для всех $i \not\equiv n \pmod{\Delta}$. Назовем (n,w)-дугу $\mathcal{K}$, такую что $w \equiv n+t \pmod{q}$, t-квазиделимой с делителем $\Delta > 1$ (или t-квазиделимой по модулю Δ), если $a_i = 0$ для всех $i \not\equiv n, n+1, \dots, n+t \pmod{\Delta}$, $1 \leqslant t \leqslant q-1$. Легко видеть, что линейные коды, соответствующие делимым (соответственно, t-квазиделимым) дугам, являются делимыми (соответственно, t-квазиделимыми) с тем же делителем. В настоящей статье делители Δ – всегда степени характеристики основного поля $\mathbb{F}_q$.

Для заданной проективной геометрии $\Sigma = \mathrm{PG}(r,q)$ определим ее двойственную геометрию $\widetilde{\Sigma}$ обычным способом: гиперплоскости в Σ будем рассматривать как точки, подпространства коразмерности два – как прямые, и будем сохранять инцидентность. Если S – подпространство в Σ (проективной) размерности s, то будем обозначать через $\widetilde{S}$ подпространство в $\widetilde{\Sigma}$, соответствующее подпространству S. Очевидно, размерность $\widetilde{S}$ в $\widetilde{\Sigma}$ равна $r-1-s$. Для любой t-квазиделимой (n,w)-дуги $\mathcal{K}$ с делителем q в Σ, $t<q$, можно определить двойственную дугу $\widetilde{\mathcal{K}}$ в геометрии $\widetilde{\Sigma}$ как

$$\widetilde{\mathcal{K}}\colon \begin{cases} \widetilde{\mathcal{P}} \to \{0,1,\ldots,t\}, \\ \widetilde{H} \to \widetilde{\mathcal{K}}(\widetilde{H}) = n+t-\mathcal{K}(H) \pmod q, \end{cases} \tag{2}$$

где $\widetilde{\mathcal{P}} = \mathcal{H}$ – множество всех точек в $\widetilde{\Sigma}$, т.е. множество всех гиперплоскостей в Σ. Это означает, что гиперплоскости кратностей, сравнимых с $n+a \pmod q$, становятся $(t-a)$-точками в двойственной геометрии. В частности, максимальные гиперплоскости являются 0-точками относительно $\widetilde{\mathcal{K}}$. Заметим, что размер $\widetilde{\mathcal{K}}$ зависит от спектра дуги $\mathcal{K}$, а не только от параметров дуги. Следующий простой результат устанавливает базовые свойства делимости двойственной дуги $\widetilde{\mathcal{K}}$.

Теорема 2. *Пусть $\mathcal{K}$ – (n,w)-дуга в $\Sigma = \mathrm{PG}(r,q)$, являющаяся t-квазиделимой по модулю q, где $t<q$. Для любого подпространства $\widetilde{S}$ в $\widetilde{\Sigma}$, такого что* $\dim \widetilde{S} \geqslant 1$,

$$\widetilde{\mathcal{K}}(\widetilde{S}) \equiv t \pmod q.$$

Доказательство. Пусть $\widetilde{S}$ – прямая в двойственной геометрии $\widetilde{\Sigma}$. Она соответствует подпространству S коразмерности 2 в Σ. Обозначим через H_i, $i=0,\ldots,q$, множество всех гиперплоскостей, проходящих через S. Тогда

$$n = \sum_{i=0}^{q} \mathcal{K}(H_i) - q\mathcal{K}(S).$$

Рассматривая обе части равенства по модулю q и используя тот факт, что $\mathcal{K}(H_i) + \widetilde{\mathcal{K}}(\widetilde{H_i}) \equiv n+t \pmod q$, получаем

$$(q+1)(n+t) - \sum_{i=0}^{q} \widetilde{\mathcal{K}}(\widetilde{H}_i) \equiv n \pmod q,$$

откуда

$$\widetilde{\mathcal{K}}(\widetilde{S}) = \sum_{i=0}^{q} \widetilde{\mathcal{K}}(H_i) \equiv t \pmod q.$$

Для подпространств S большей размерности можно использовать тот факт, что кратность любой прямой в $\widetilde{S}$ равна t по модулю q, и суммировать кратности всех прямых, проходящих через точку в $\widetilde{S}$. ▲

Это наблюдение приводит к следующему определению. Пусть t – фиксированное неотрицательное целое число. Дугу $\mathcal{F}$ в Σ будем называть $(t \bmod q)$-*дугой*, если $\mathcal{F}(S) \equiv t \pmod q$ для любого подпространства S размерности не менее 1. По теореме 2, если $\mathcal{K}$ – дуга, t-квазиделимая по модулю q, то ее двойственная дуга $\widetilde{\mathcal{K}}$, определенная в (2), является $(t \bmod q)$-дугой с точками кратностей не выше t.

Пусть $\mathcal{K}$ – (n,w)-дуга в Σ, являющаяся t-квазиделимой по модулю q. Следующая теорема устанавливает связь между свойством расширимости дуги $\mathcal{K}$ и структурой $(t \bmod q)$-дуги $\widetilde{\mathcal{K}}$.

Теорема 3. *Пусть $\mathcal{K}$ – (n,w)-дуга в $\Sigma = \mathrm{PG}(r,q)$, являющаяся t-квазиделимой по модулю q, где $t < q$, и пусть двойственная ей дуга $\widetilde{\mathcal{K}}$ определена в* (2). *Если*

$$\widetilde{\mathcal{K}} = \sum_{i=1}^{c} \chi_{\widetilde{P}_i} + \mathcal{K}'$$

для некоторого мультимножества $\mathcal{K}'$ в $\widetilde{\Sigma}$ и для c не обязательно различных гиперплоскостей $\widetilde{P}_1, \ldots, \widetilde{P}_c$ в $\widetilde{\Sigma}$, то $\mathcal{K}$ допускает c-расширение. В частности, если в носителе $\widetilde{\mathcal{K}}$ содержится гиперплоскость, то $\mathcal{K}$ допускает расширение. (*Здесь мы по определению полагем* $(\mathcal{K}_1 + \mathcal{K}_2)(P) := \mathcal{K}_1(P) + \mathcal{K}_2(P)$.)

Доказательство. Проведем индукцию по c. Так как максимальные гиперплоскости соответствуют 0-точкам в двойственной геометрии, то условие теоремы состоит в существовании точки $P \in \Sigma$, не инцидентной максимальным гиперплоскостям. При увеличении кратности точки P на 1 мы также увеличим кратность всех гиперплоскостей, проходящих через P. Следовательно, кратность всех точек гиперплоскости $\widetilde{P}_1 := \widetilde{P}$ в двойственной геометрии увеличится на 1. Это означает, что дуга

$$\mathcal{L}(Q) = \begin{cases} \mathcal{K}(Q), & \text{если } Q \neq P_1, \\ \mathcal{K}(Q) + 1, & \text{если } Q = P_1, \end{cases}$$

является $(n+1,w)$-дугой в Σ и что

$$\widetilde{\mathcal{L}} = \widetilde{\mathcal{K}} - \chi_{\widetilde{P}_1} = \sum_{i=2}^{c} \chi_{\widetilde{P}_i} + \mathcal{K}'$$

для некоторой дуги $\mathcal{K}'$. Поскольку $\widetilde{\mathcal{L}}$ допускает $(c-1)$-расширение по предположению индукции, отсюда следует утверждение теоремы. ▲

§ 3. Структурные результаты для $(t \bmod q)$-дуг

В этом параграфе будем изучать $(t \bmod q)$-дуги как чисто геометрические объекты безотносительно задачи о расширении. Начнем с простой конструкции.

Теорема 4. *Пусть $\mathcal{F}_1$ и $\mathcal{F}_2$ – $(t_1 \bmod q)$- и $(t_2 \bmod q)$-дуги, соответственно, в $\mathrm{PG}(r,q)$. Тогда $\mathcal{F}_1 + \mathcal{F}_2$ является $(t \bmod q)$-дугой, где $t = t_1 + t_2 \pmod q$. Аналогично $\alpha\mathcal{F}_1$, $\alpha \in \{0, \ldots, p-1\}$, является $(t \bmod q)$-дугой с $t \equiv \alpha t_1 \pmod q$.*

Эта теорема имеет полезное следствие в случае $t = 0$, когда $q = p$ – простое число.

Следствие 1. *Пусть $\mathcal{F}$ и $\mathcal{G}$ – $(0 \bmod p)$-дуги в $\mathrm{PG}(r,p)$, где p – простое. Тогда $\mathcal{F} + \mathcal{G}$ и $\alpha\mathcal{F}$, $\alpha \in \{0, \ldots, p-1\}$, также являются $(0 \bmod p)$-дугами. В частности, множество всех $(0 \bmod p)$-дуг в $\mathrm{PG}(r,p)$ является векторным пространством над $\mathbb{F}_p$.*

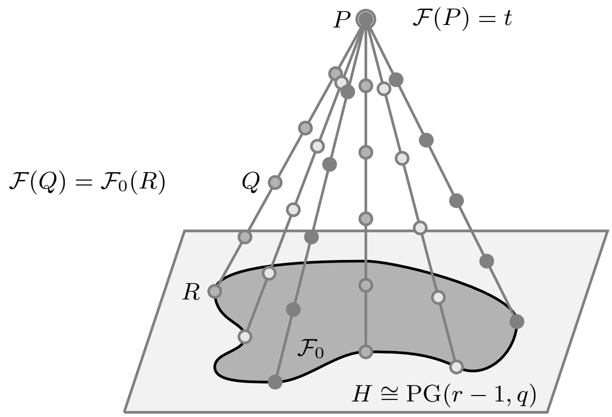
Следующая конструкция менее очевидна.

Теорема 5. *Пусть $\mathcal{F}_0$ – $(t \bmod q)$-дуга в гиперплоскости $H \cong \mathrm{PG}(r-1,q)$ в геометрии $\Sigma = PG(r,q)$, $q = p^h$. Для фиксированной точки $P \in \Sigma \setminus H$ определим дугу $\mathcal{F}$ в Σ следующим образом:*

– $\mathcal{F}(P) = t$;

– *Для каждой точки $Q \neq P$ положим $\mathcal{F}(Q) = \mathcal{F}_0(R)$, где $R = \langle P, Q \rangle \cap H$.*

Тогда $\mathcal{F}$ является $(t \bmod q)$-дугой размера $q|\mathcal{F}_0| + t$.



К доказательству теоремы 5

Доказательство. Как уже было отмечено, достаточно доказать, что кратность любой прямой равна t по модулю q. Для прямых, проходящих через точку P, это очевидно. Теперь рассмотрим прямую L в Σ, не инцидентную точке P. Пусть π – плоскость, проходящая через P и L: $\pi = \langle L, P\rangle$. Положим $L' = \pi \cap H$. Очевидно, L содержит точки тех же кратностей, что и L'. Прямая L' имеет кратность $\mathcal{F}(L') = \mathcal{F}_0(L) \equiv t \pmod q$, откуда следует результат. Эта конструкция изображена на рисунке. ▲

Назовем $(t \bmod q)$-дугу, полученную в теореме 5, *поднятием дуги* $\mathcal{F}_0$, а точку P – *точкой поднятия*. Можно слегка обобщить понятие поднятия дуги, заменяя точку P на подпространство U. Пусть $\mathcal{F}_0$ – $(t \bmod q)$-дуга в подпространстве V в геометрии $\Sigma = \mathrm{PG}(r,q)$, и пусть U – дополнительное подпространство в Σ, т.е. $\dim U + \dim V = r - 1$, $U \cap V = \varnothing$. Дуга $\mathcal{F}$ в Σ, определяемая условиями

– $\mathcal{F}(P) = t$ для любой точки $P \in U$;
– Для каждой точки $Q \neq P$ полагаем $\mathcal{F}(Q) = \mathcal{F}_0(R)$, где $R = \langle U, Q\rangle \cap H$

называется *поднятием дуги из подпространства* U. Очевидно, что $\mathcal{F}$ также является $(t \bmod q)$-дугой. Заметим, что если дуга поднята из подпространства, то ее можно рассматривать как поднятие из любой точки этого подпространства. Имеет место также частичное обращение этого наблюдения.

Лемма 1. *Пусть $\mathcal{F}$ – $(t \bmod q)$-дуга в $\mathrm{PG}(r,q)$, являющаяся поднятием из точек P и Q, $P \neq Q$. Тогда $\mathcal{F}$ является также поднятием из прямой PQ. В частности, все точки поднятия $(t \bmod q)$-дуги образуют подпространство S в геометрии $\mathrm{PG}(r,q)$.*

Доказательство. Все точки прямой PQ являются t-точками. Пусть R – произвольная точка в Σ. Тогда все точки прямой PR (соответственно, QR), отличные от P (соответственно, Q), имеют одинаковую кратность, скажем, a. Тогда все точки плоскости $\langle P, Q, R\rangle$ вне прямой PQ также имеют одинаковую кратность a, что и доказывает лемму. ▲

Всюду далее мы будем рассматривать только геометрии $\Sigma = \mathrm{PG}(r,p)$ над простыми полями $\mathbb{F}_p$. Обозначим через V множество всех $(0 \bmod p)$-дуг в $\mathrm{PG}(r,p)$. Следующий результат является аналогом наблюдения, сделанного в теореме 4 и следствии 1.

Лемма 2. *Пусть $\mathcal{F}$ и $\mathcal{G}$ – $(0 \bmod p)$-дуги в $\mathrm{PG}(r,p)$, являющиеся поднятиями из одного и того же подпространства U, $\dim U \geqslant 0$. Тогда $\mathcal{F} + \mathcal{G}$ и $\alpha\mathcal{F}$, $\alpha \in \{0, 1, \ldots, p-1\}$, также являются $(0 \bmod p)$-дугами, поднятыми из U. В частности, $(0 \bmod p)$-дуги, поднятые из U, образуют подпространство в V.*

Теперь обозначим через A матрицу инцидентности точек и прямых в геометрии $\mathrm{PG}(r,p)$, где p – простое, относительно некоторого фиксированного упорядочивания точек. Пусть $\mathcal{F}$ – дуга в $\mathrm{PG}(r,p)$ с точками кратностей не выше $p-1$. Тогда дугу $\mathcal{F}$ можно задать вектором $\boldsymbol{x}$ над $\mathbb{F}_p$:

$$\boldsymbol{x} = \Big(\mathcal{F}(P_1), \dots, \mathcal{F}(P_{\frac{p^{r+1}-1}{p-1}})\Big),$$

где кратности точек рассматриваются как элементы поля $\mathbb{F}_p$. Очевидно, что $\mathcal{F}$ является $(0 \bmod p)$-дугой тогда и только тогда, когда

$$\boldsymbol{x}A = \mathbf{0}, \tag{3}$$

где через $\mathbf{0}$ обозначен нулевой вектор. Отсюда

$$\dim V = \frac{q^{r+1}-1}{q-1} - \mathrm{rk}_p\, A.$$

Ранг матрицы A известен из знаменитой теоремы Хамады [18], которую мы приведем в ее общем виде.

Т е о р е м а 6. *Ранг над полем $\mathbb{F}_{p^h}$ матрицы инцидентности точек и d-подпространств в $\mathrm{PG}(r,p^h)$ равен*

$$R_d(r,p^h) = \sum_{s_0} \dots \sum_{s_{h-1}} \prod_{j=0}^{h-1} \sum_{i=0}^{L(s_{j+1},s_j)} (-1)^i \binom{r+1}{i} \binom{r + s_{j+1}p - s_j - ip}{i},$$

где $s_h = s_0$, суммы берутся по всем целым s_j, $j = 0, \dots, h-1$, таким что $d+1 \leqslant \leqslant s_j \leqslant r+1$, $0 \leqslant s_{j+1}p - s_j \leqslant (r+1)(p+1)$, а $L(s_{j+1}, s_j)$ – наибольшее целое число, не превосходящее $(s_{j+1}p - s_j)/p$, т.е.

$$L(s_{j+1}, s_j) = \left\lfloor \frac{s_{j+1}p - s_j}{r} \right\rfloor.$$

Отметим, что в обозначениях Хамады $A = R_1(r,p)$. Приведенная выше формула не слишком удобна. Для специального случая $d = 1$, т.е. для матрицы инцидентности точек и прямых, и при $h = 1$, т.е. для простого поля, имеется формула замкнутого вида для ранга, найденная ван Линтом. Мы приводим ее в качестве следствия (подробнее см. в [19]).

С л е д с т в и е 2. *Для матрицы инцидентности точек и прямых в геометрии $\mathrm{PG}(r,p)$ справедлива формула*

$$\mathrm{rk}_p\, R_1(r,p) = \frac{p^{r+1}-1}{p-1} - \binom{p+r-1}{r}.$$

С л е д с т в и е 3. *Размерность векторного пространства всех $(0 \bmod p)$-дуг равна* $\dim V = \binom{p+r-1}{r}$.

Теперь мы можем охарактеризовать векторное пространство V всех $(0 \bmod p)$-дуг.

Т е о р е м а 7. *Векторное пространство всех $(0 \bmod p)$-дуг в $\mathrm{PG}(r,p)$ порождается дополнениями к гиперплоскостям.*

Д о к а з а т е л ь с т в о. Пусть B – матрица инцидентности точек и гиперплоскостей в $\mathrm{PG}(r,p)$. Из теоремы 6, как и из множества других источников (см. [20–22]), известно, что

$$\mathrm{rk}_p\, B = \binom{p+r-1}{r} + 1.$$

Пусть $T_1, \ldots, T_{s+1}$, $s = \binom{p+r-1}{r}$, – такие гиперплоскости, что их характеристические векторы χ_{T_i}, $i = 1, \ldots, s+1$, образуют базис в пространстве столбцов матрицы B. Ясно, что вектор из всех единиц $\boldsymbol{j}$ лежит в этом пространстве столбцов, поскольку сумма всех столбцов матрицы B над полем $\mathbb{F}_p$ равна $\boldsymbol{j}$. Значит, существуют $\lambda_i \in \mathbb{F}_p$, такие что

$$\lambda_1\chi_{T_1} + \ldots + \lambda_s\chi_{T_s} + \lambda_{s+1}\chi_{T_{s+1}} = \boldsymbol{j}. \tag{4}$$

Без ограничения общности можно считать, что $\lambda_{s+1} \neq 0$. Предположим, что векторы $\boldsymbol{j} - \chi_{T_1}, \ldots, \boldsymbol{j} - \chi_{T_s}$ линейно зависимы над $\mathbb{F}_p$. Тогда существуют элементы $\mu_i \in \mathbb{F}_p$, не все равные нулю, такие что

$$\mu_1(\boldsymbol{j} - \chi_{T_1}) + \ldots + \mu_s(\boldsymbol{j} - \chi_{T_s}) = \mathbf{0}. \tag{5}$$

Ясно, что $\mu_1 + \ldots + \mu_s \neq 0$, поскольку в противном случае $\chi_{T_1}, \ldots, \chi_{T_s}$ были бы линейно зависимыми. Тогда из (4), (5) получаем

$$\Big(\mu_1 - \lambda_1 \sum_i \mu_i\Big)\chi_{T_1} + \ldots + \Big(\mu_s - \lambda_s \sum_i \mu_i\Big)\chi_{T_s} - \lambda_{s+1}\sum_i \mu_i\chi_{T_i} = \mathbf{0}.$$

Так как $\lambda_{s+1} \sum\limits_i \mu_i \neq 0$, мы пришли к противоречию с линейной независимостью векторов $\chi_{T_1}, \ldots, \chi_{T_s}$. Следовательно, векторы $\boldsymbol{j} - \chi_{T_1}, \ldots, \boldsymbol{j} - \chi_{T_s}$ линейно независимы, и

$$s \leqslant \mathrm{rk}_p\langle \boldsymbol{j} - \chi_T \mid T \text{ – гиперплоскость}\rangle \leqslant s+1.$$

С другой стороны, вектор $\boldsymbol{j} - \chi_T$ является решением уравнения (3) для любой гиперплоскости T. Поэтому по следствию 3 получаем

$$\mathrm{rk}_p\langle \boldsymbol{j} - \chi_T \mid T \text{ – гиперплоскость}\rangle = \binom{p+r-1}{r}. \quad \blacktriangle$$

Далее, поскольку дуга, соответствующая $\boldsymbol{j} - \chi_T$, является поднятием из любой точки гиперплоскости T, отсюда вытекают следующие утверждения.

Следствие 4. *Всякая* $(0 \bmod p)$*-дуга в* $\mathrm{PG}(r,p)$ *является суммой поднятий дуг.*

Следствие 5. *Всякая* $(t \bmod p)$*-дуга в* $\mathrm{PG}(r,p)$ *является суммой поднятий дуг.*

Доказательство. Любую $(t \bmod p)$-дугу $\mathcal{F}$ можно представить в виде $\mathcal{F} = t\chi_H + \mathcal{F}_0$, где H – фиксированная гиперплоскость, а $\mathcal{F}_0$ – $(0 \bmod p)$-дуга. Теперь результат вытекает из следствия 3 и того факта, что $t\chi_T$ очевидным образом является поднятием. $\blacktriangle$

В случае плоскости можно доказать еще больше. Любую $(t \bmod p)$-дугу можно представить в виде суммы не более чем p поднятий дуг.

Теорема 8. *Пусть* $P_1, \ldots, P_p$ *–* p *точек коники в* $\mathrm{PG}(2,p)$*. Обозначим через* V_i *векторное пространство всех* $(0 \bmod p)$*-дуг, поднятых из* P_i, $i = 1, \ldots, p$*, а через* V *– векторное пространство всех* $(0 \bmod p)$*-дуг. Тогда*

$$V = V_1 + V_2 + \ldots + V_p.$$

Д о к а з а т е л ь с т в о. Через P_{p+1} обозначим $(p+1)$-ю точку коники, а через V_{p+1} – подпространство всех $(t \bmod p)$-дуг, поднятых из P_{p+1}. Вначале докажем, что

$$(V_{i_1} + \ldots + V_{i_k}) \cap V_{i_{k+1}} = V_{i_1} \cap V_{i_{k+1}} + \ldots + V_{i_k} \cap V_{i_{k+1}} \tag{6}$$

для любого множества индексов $\{i_1, \ldots, i_{k+1}\} \subseteq \{1, \ldots, p+1\}$. Рассмотрим следующие цепочки вложений:

$$\begin{array}{ccccc}
(V_1+V_2)\cap V_{p+1} & \subseteq & (V_1+V_2+V_3)\cap V_{p+1} & \subseteq \ldots \subseteq & (V_1+\ldots+V_p)\cap V_{p+1} \\
\cup & & \cup & & \cup \\
V_1\cap V_{p+1}+V_2\cap V_{p+1} & \subseteq & V_1\cap V_{p+1}+V_2\cap V_{p+1}+V_3\cap V_{p+1} & \subseteq \ldots \subseteq & V_1\cap V_{p+1}+\ldots+V_p\cap V_{p+1}.
\end{array}$$

Очевидно, $\dim(V_1 + V_2) \cap V_{p+1} = \dim(V_1 \cap V_{p+1} + V_2 \cap V_{p+1}) = 2$. Более того,

$$\dim(V_1 + \ldots + V_p) \cap V_{p+1} \leqslant \dim V_{p+1} = p.$$

Предположим, что для некоторого k выполнено равенство

$$V_1 \cap V_{p+1} + \ldots + V_k \cap V_{p+1} = V_1 \cap V_{p+1} + \ldots + V_k \cap V_{p+1} + V_{k+1} \cap V_{p+1}. \tag{7}$$

Очевидно, $\dim V_i \cap V_j = 1$, $i \neq j$, и дуги в $V_i \cap V_j$ являются кратными вектора $\boldsymbol{j} - \chi_{P_i P_j}$. Теперь из (7) имеем

$$\boldsymbol{j} - \chi_{P_{k+1} P_{p+1}} \in \langle \boldsymbol{j} - \chi_{P_1 P_{p+1}}, \ldots, \boldsymbol{j} - \chi_{P_k P_{p+1}} \rangle.$$

Это противоречит теореме 1.10 из [23], которая утверждает, что векторы $\boldsymbol{j} - \chi_{P_i P_j}$, $1 \leqslant i < j \leqslant p+1$, линейно независимы. Поэтому

$$\dim(V_1 \cap V_{p+1} + \ldots + V_k \cap V_{p+1}) = k$$

для всех $k \in \{2, \ldots, p\}$. Тогда, поскольку $\dim(V_1 + \ldots + V_p) \cap V_{p+1} \leqslant p$, то

$$(V_1 + \ldots + V_p) \cap V_{p+1} = V_1 \cap V_{p+1} + \ldots + V_p \cap V_{p+1},$$

откуда, в свою очередь, следует, что $\dim(V_1 + \ldots + V_k) \cap V_{p+1} = k$ для всех k. Тогда получаем

$$(V_1 + \ldots + V_k) \cap V_{p+1} = V_1 \cap V_{p+1} + \ldots + V_k \cap V_{p+1}$$

для всех $k \leqslant p$, поэтому, очевидно, равенство (6) выполнено и для любого подмножества индексов $\{i_1, \ldots, i_{k+1}\}$.

Далее, в силу (6) можно применить формулу для размерности

$$\dim(V_1 + \ldots + V_p) = \sum_i \dim V_i - \sum_{i,j} (\dim V_i \cap V_j) + \sum_{i,j,k} \dim(V_i \cap V_j \cap V_k) - \ldots,$$

которая в общем случае не верна. Поскольку $V_i \cap V_j \cap V_k = (0)$, получаем

$$\dim(V_1 + V_2 + \ldots + V_p) = \sum_i \dim V_i - \sum_{i,j} \dim(V_i \cap V_j) =$$

$$= p \cdot p - \binom{p}{2} \cdot 1 = \binom{p+1}{2},$$

что совпадает с размерностью пространства всех плоских $(0 \bmod p)$-дуг. Отсюда следует, что всякая $(0 \bmod p)$-дуга в $\mathrm{PG}(2, p)$ является суммой не более чем p поднятий дуг. ▲

С л е д с т в и е 6. *Любую* $(t \bmod p)$*-дугу в* $\mathrm{PG}(2, p)$ *можно представить в виде суммы не более чем* p *поднятий дуг.*

Замечание 1. Весьма вероятно, что теорема 8 и следствие 5 верны не только для случая плоскости, но и в геометриях произвольной размерности. Если удастся доказать (6), то останется проверить простое биномиальное тождество. Но проблема в том, что в размерностях $r \geqslant 3$ нет аналога теоремы 1.10 из [23].

§ 4. (t mod q)-дуги с ограниченными кратностями точек

Напомним, что (t mod q)-дуги, получаемые из t-квазиделимых дуг, имеют дополнительное свойство, что кратности точек в них ограничены сверху величиной t.

Оказывается, что если (t mod q)-дуга в $\mathrm{PG}(r,q)$ имеет свойство, что ее ограничение на любую гиперплоскость является поднятием из точки, то и сама дуга является поднятием.

Теорема 9. *Пусть* $\mathcal{K}$ – (t mod q)*-дуга в* $\mathrm{PG}(r,q)$*, такая что ограничение* $\mathcal{K}|_H$ *на любую гиперплоскость* H *в* $\mathrm{PG}(r,q)$ *является поднятием. Тогда и сама* $\mathcal{K}$ *является поднятием дуги.*

Доказательство. Рассмотрим (t mod q)-дугу $\mathcal{K}$ в $\mathrm{PG}(r,q)$. Пусть S – произвольное подпространство $\mathrm{PG}(r,q)$ коразмерности 2. Обозначим через H_i, $i=0,\ldots,q$, гиперплоскости, проходящие через S. Дуги $\mathcal{K}|_{H_i}$ являются поднятыми (t mod q)-дугами. Обозначим через P_i, $i=0,\ldots,q$, соответствующие точки поднятия.

Предположим, что для некоторых индексов, скажем, i и j, выполнено $P_i \in S$ и $P_j \in H_j \setminus S$. Очевидно, прямая P_iP_j полностью состоит из t-точек. Пусть L – произвольная прямая в H_j, инцидентная точке P_j, и положим $L \cap S = Q_j$. Все точки на прямой P_jQ_j, отличные от P_j, имеют одинаковую кратность a, где $0 \leqslant a \leqslant t$. Таким образом, все точки плоскости $\langle P_i, P_j, Q_j\rangle$ вне прямой P_iP_j являются a-точками. Теперь ясно, что $\mathcal{K}|_{H_j}$ можно рассматривать как поднятие из прямой P_iP_j, и следовательно, из любой точки прямой P_iP_j.

Предположим, что $P_i \in H_i \setminus S$ для всех $i=0,\ldots,q$. Если точки $P_0,\ldots,P_q$ коллинеарны, то $\mathcal{K}$ является поднятием из прямой $\langle P_i \mid i=0,\ldots,q\rangle$.

Теперь предположим, что точки P_i не коллинеарны. Тогда существует гиперплоскость H в $\mathrm{PG}(r,q)$, не содержащая ни одной точки P_i. Положим $T = H \cap S$. Если обозначить $G_i = H \cap H_i$, то все дуги $\mathcal{K}|_{G_i}$ проективно эквивалентны дуге $\mathcal{K}|_S$.

Предположим сперва, что точка поднятия Q дуги $\mathcal{K}|_H$ содержится в $G_i \setminus T$. Положим $Q_i = S \cap QP_i$. Очевидно, P_iQ_i – прямая из t-точек. Рассмотрим произвольную прямую L в H_i, проходящую через P_i. Если точки на L, отличные от P_i, являются a-точками, то все точки на прямой, проходящей через Q и $L \cap G_i$, отличные от Q, также являются a-точками. Следовательно, все точки плоскости $\langle L, Q_i\rangle$ вне прямой P_iQ_i являются a-точками, и дуга $\mathcal{K}|_{H_i}$ поднята из P_iQ_i. Таким образом, ее можно рассматривать как поднятие из любой точки прямой P_iQ_i, в частности, из Q_i.

Пока что мы доказали, что без ограничения общности можно считать, что все точки P_i содержатся в S. Рассмотрим подпространство T в S, натянутое на точки P_i: $T = \langle P_i \mid i=0,\ldots,q\rangle$. Все точки подпространства T имеют максимальную кратность. Пусть $Q \in S \setminus T$ – точка кратности a. Все точки в $\langle T, Q\rangle \setminus T$ также имеют кратность a. Следовательно, ограничение $\mathcal{K}|_S$ является поднятием из подпространства T. Поскольку мы выбирали произвольное S, ограничение дуги $\mathcal{K}$ на любое подпространство коразмерности 2 является поднятием дуги.

Повторим эти рассуждения для подпространств меньших размерностей. Для подпространств размерности 2 это означает, что любая плоскость содержит прямую, состоящую из t-точек, а остальные ее точки имеют кратность a. Легко проверить, что в таком случае имеется гиперплоскость, состоящая из t-точек, а все остальные точки вне этой гиперплоскости являются a-точками. Но такая дуга, очевидно, является поднятием. ▲

В случае плоскости нетривиальные $(t \bmod q)$-дуги можно строить как σ-двойственные к определенным блокирующим множествам. Пусть $\mathcal{K}$ – мультимножество в Σ. Рассмотрим функцию σ, такую что $\sigma(\mathcal{K}(H))$ – неотрицательное целое число для всех гиперплоскостей H. Мультимножество

$$\widetilde{\mathcal{K}}^{\sigma}: \begin{cases} \mathcal{H} \to \mathbb{N}_0, \\ H \mapsto \sigma(\mathcal{K}(H)), \end{cases} \tag{8}$$

в двойственном пространстве $\widetilde{\Sigma}$ называется *σ-двойственным* к $\mathcal{K}$. Если σ – линейная функция, то параметры мультимножества $\widetilde{\mathcal{K}}^{\sigma}$, а также его спектр, легко вычисляются по параметрам и спектру $\mathcal{K}$ [2].

Теорема 10. *$(t \bmod q)$-дуга в $\mathrm{PG}(2,q)$ размера $mq+t$ с точками максимальной кратности t существует тогда и только тогда, когда существует блокирующее множество в $\mathrm{PG}(2,q)$ с параметрами $((m-t)q+m, m-t)$ и прямыми с кратностями из множества $\{m-t, m-t+1, \ldots, m\}$.*

Доказательство. Пусть $\mathcal{F}$ – $(t \bmod q)$-дуга в $\mathrm{PG}(2,q)$ размера $mq+t$. Тогда дуга $\mathcal{F}^{\sigma}$, где $\sigma(x) = (x-t)/q$, является $((m-t)q+m, m-t)$-блокирующим множеством в двойственной плоскости. Более того, кратности прямых относительно этого блокирующего множества принадлежат множеству $\{m-t, m-t+1, \ldots, m\}$. Чтобы убедиться в этом, обозначим спектр дуги $\mathcal{F}$ через (a_i). Несложные вычисления дают

$$\sum_i a_{t+iq} = q^2+q+1, \qquad \sum_i (t+iq)a_{t+iq} = (mq+t)(q+1).$$

Отсюда

$$|\mathcal{F}^{\sigma}| = \sum_i i a_{t+iq} = (m-t)q+m.$$

Далее, обозначим через b_i число i-прямых, проходящих через фиксированную c-точку P (относительно $\mathcal{F}$), $0 \leqslant c \leqslant t$. Снова подсчитаем

$$\sum_i b_{t+iq} = q+1, \qquad \sum_i (t+iq)b_{t+iq} = mq+t+cq,$$

откуда $\sum\limits_i i b_{t+iq} = m-t+c$. Значит, $\mathcal{F}^{\sigma}$ – блокирующее множество с параметрами $((m-t)q+m, m-t)$, а кратности прямых лежат в интервале от $m-t$ (при $c=0$) до m (при $c=t$).

В другую сторону утверждение доказывается аналогично. Если начать с блокирующего множества с данными параметрами и кратностями прямых из множества $\{m-t, \ldots, m\}$, то можно рассмотреть $(m-t+j)$-прямые как j-точки двойственной геометрии, $j = 0, \ldots, t$. Теперь параметры двойственной дуги легко проверяются. ▲

§ 5. (2 mod q)-дуги с ограниченными кратностями точек

Для начала заметим, что $(1 \bmod q)$-дуга, возникающая из 1-квазиделимой дуги, проективна, и поэтому является либо гиперплоскостью, либо всем пространством. В обоих случаях она содержит полную гиперплоскость, откуда следует, что любая 1-квазиделимая дуга допускает расширение. Теорема Хилла – Лизака о расширении [8] на первый взгляд имеет несколько более общий характер, но ее можно получить из нашего подхода, слегка изменив определение $\widetilde{\mathcal{K}}$.

Рассмотрим случай $(2 \bmod q)$-дуг для геометрий $\mathrm{PG}(r,q)$ с нечетным $q \geqslant 5$. В частности, $(2 \bmod q)$-дуги в плоскости $\mathrm{PG}(2,q)$ с максимальной кратностью точек 2 были описаны в [12]. Они имеют следующий вид:

(I) Дуга, поднятая из 2-прямой; такая дуга имеет $2q+2$ точек, и имеются две возможности:

  (I-1) двойная прямая, или

  (I-2) сумма двух различных прямых;

(II) Дуга, поднятая из $(q+2)$-прямой; такая прямая содержит i двойных точек, $q-2i+2$ простых точек, а также 0-точки в количестве $i-1$, где $i=1,\ldots,\dfrac{q+1}{2}$; будем говорить, что такая дуга имеет тип (II-i), если она поднята из прямой с i двойными точками;

(III) Дуга, поднятая из $(2q+2)$-прямой, или, что то же самое, сумма двух копий плоскости;

(IV) Исключительная $(2 \bmod q)$-дуга при нечетном q; она состоит из точек овала, фиксированной касательной к этому овалу и двух копий каждой внутренней точки овала (см. также [24]).

Теперь докажем, что в размерностях выше 2 каждая $(2 \bmod q)$-дуга является поднятием дуги. Рассмотрим проекцию φ из 2-точки P на некоторую плоскость, не инцидентную этой точке. Пусть L – прямая, инцидентная точке P. Для образа прямой L имеются следующие возможности:

Тип прямой L	Кратность L	Тип точки $\varphi(L)$
$(2,0,\ldots,0)$	2	ω
$(2,1,\ldots,1)$	$q+2$	α
$(2,2,\ldots,2)$	$2q+2$	β
$(2,\underbrace{2,\ldots,2}_{i},\underbrace{1,\ldots,1}_{q-2i},\underbrace{0,\ldots,0}_{i})$	$q+2$	γ_i

.

Отметим, что $i=1,\ldots,\dfrac{q-1}{2}$ для типа γ_i. Тогда образы плоских $(2 \bmod q)$-дуг при проекции φ имеют следующий вид:

Тип	Образ плоской дуги	Примечание
(I-1)	$(\beta,\omega,\ldots,\omega)$	
(I-2)	$(\alpha,\alpha,\omega,\ldots,\omega)$	
(II-i)	$(\underbrace{\beta,\ldots,\beta}_{i},\underbrace{\alpha,\ldots,\alpha}_{q-2i+1},\underbrace{\omega,\ldots,\omega}_{i-1})$	Проекция из исключительной 2-точки
	$(\beta,\gamma_i,\gamma_i,\ldots,\gamma_i)$	Проекция из любой другой 2-точки
(III)	$(\beta,\beta,\ldots,\beta)$	
(IV)	$(\alpha,\gamma_{\frac{q-1}{2}},\ldots,\gamma_{\frac{q-1}{2}})$	Проекция из 2-точки на овале
	$(\underbrace{\gamma_{\frac{q-1}{2}},\ldots,\gamma_{\frac{q-1}{2}}}_{\frac{q+3}{2}},\underbrace{\gamma_{\frac{q-3}{2}},\ldots,\gamma_{\frac{q-3}{2}}}_{\frac{q-1}{2}})$	Проекция из внутренней точки овала

.

Пусть задана $(2 \bmod q)$-дуга $\mathcal{K}$ в $\mathrm{PG}(3,q)$, где q нечетно; рассмотрим проекцию из 2-точки P. Из последней таблицы следует, что

(i) Никакая прямая в плоскости проекции не инцидентна точкам типа ω и точкам типа γ_i;

(ii) Если на прямой в плоскости проекции существуют точки типа γ_i и точки типа γ_j, где $i \neq j$, то $i=\dfrac{q-3}{2}$, $j=\dfrac{q-1}{2}$.

Предположим вначале, что существует плоскость π_0, такая что $\mathcal{K}|_\pi$ является исключительной дугой (IV). Пусть φ – проекция из 2-точки, лежащей на овале. Тогда образ плоскости π_0 имеет тип $(\alpha,\gamma_{\frac{q-1}{2}},\ldots,\gamma_{\frac{q-1}{2}})$. Обозначим через L прямую типа α и зафиксируем 1-точку Q на этой прямой. Предположим, что в плоскости проекции есть точка типа β. Тогда плоскость проекции содержит прямую типа $(\beta, \alpha, \ldots, \alpha)$, а все остальные прямые, проходящие через эту точку типа β, имеют тип $(\beta, \gamma_{\frac{q-1}{2}}, \ldots, \gamma_{\frac{q-1}{2}})$, поскольку ω и $\gamma_{\frac{q-1}{2}}$ несовместны. Следовательно, прямые в плоскости проекции, проходящие через точку типа α, имеют следующие типы:

- $(\alpha, \alpha, \ldots, \alpha, \beta)$, такая прямая ровно одна;
- $(\alpha, \gamma_{\frac{q-2}{2}}, \ldots, \gamma_{\frac{q-2}{2}}, \gamma_{\frac{q-2}{2}})$, имеется q таких прямых.

Обозначим точки, лежащие на $2(q+1)$-прямой (прообразе точки типа β), через $P_0, P_1, \ldots, P_q$. Предположим, что найдется точка P_i, такая что все плоскости, проходящие через QP_i (отличные от π_0), не имеют тип (IV). Тогда $\mathcal{K}$, очевидно, является поднятием. Если же для любой P_i имеется плоскость, проходящая через QP_i и такая, что ограничение дуги $\mathcal{K}$ на эту плоскость имеет тип (IV), то при проектировании из каждой P_i будут получаться одни и те же типы прямых в плоскости проекции (см. описание выше). Поэтому никакие три из q^2 1-точек в овале не коллинеарны. Следовательно, выбирая эти q^2 1-точек, а также, скажем, P_0 и P_1, мы построим (q^2+2)-шапку. Это приводит к противоречию, поскольку максимальный размер шапки в $\mathrm{PG}(3,q)$ равен q^2+1.

Мы доказали, что если в плоскости проекции имеется точка типа β, то дуга $\mathcal{K}$ является поднятием. Но точка типа β всегда обязана иметься, поскольку типы $\gamma_{\frac{q-1}{2}}$ и ω несовместны. Таким образом, мы доказали, что если существует плоскость π, такая что дуга $\mathcal{K}|_\pi$ имеет тип (IV), то $\mathcal{K}$ – поднятие дуги.

Теперь предположим, что такой плоскости, что $\mathcal{K}|_\pi$ имеет тип (IV), не существует. Тогда ограничение $\mathcal{K}$ на любую плоскость является поднятием, и по теореме 9 дуга $\mathcal{K}$ снова является поднятием. Итак, доказана следующая

Лемма 3. *Пусть $\mathcal{K}$ – $(2 \bmod q)$-дуга в $\mathrm{PG}(3,q)$, где q нечетно. Тогда $\mathcal{K}$ является поднятием дуги.*

Теперь применим индукцию по размерности. Тогда, снова используя теорему 9, получаем, что каждая $(2 \bmod q)$-дуга в геометрии размерности не менее 3 является поднятием.

Теорема 11. *Пусть $\mathcal{K}$ – $(2 \bmod q)$-дуга в $\mathrm{PG}(r,q)$, q нечетно, $r \geqslant 3$. Тогда $\mathcal{K}$ является поднятием дуги. В частности, носитель любой $(2 \bmod q)$-дуги в $\mathrm{PG}(r,q)$, $r \geqslant 2$, содержит гиперплоскость.*

Замечание 2. Теорема 11 дает альтернативное доказательство теоремы Маруты о расширимости кодов с весами $-2, -1, 0 \pmod q$ [12]. Существование такого кода равносильно существованию дуги $\mathcal{K}$, 2-квазиделимой по модулю q. В § 2 (формула (2)) мы определили $(t \bmod q)$-дугу $\widetilde{\mathcal{K}}$ в геометрии $\widetilde{\Sigma}$ для любой t-квазиделимой дуги $\mathcal{K}$ в геометрии Σ. По теореме 3, если носитель дуги $\widetilde{\mathcal{K}}$ содержит гиперплоскость, то $\mathcal{K}$ допускает расширение. Именно этот факт установлен в теореме 11.

§ 6. Пример

Технику, развитую в предыдущих параграфах, можно проиллюстрировать на примере задачи о расширимости шапок в $\mathrm{PG}(3,q)$. Напомним, что шапкой в $\mathrm{PG}(3,q)$ называется множество точек этой геометрии, никакие три из которых не коллинеарны. Хорошо известно, что максимальный размер шапки в $\mathrm{PG}(3,q)$ при $q>2$ равен q^2+1. Оказывается, что если шапка имеет размер q^2+1-t, где t не очень большое, то она допускает расширение. Другими словами, все полные шапки размера менее q^2+1 имеют менее q^2+1-t точек. Задача о нахождении значения t имеет важное значение в конечной геометрии.

Результат такого типа для четных q следующий [25].

Теорема 12. *В геометрии* $\mathrm{PG}(3,q)$ *при четном* q *для полной* k*-шапки, где* $k < q^2+1$, *справедливо неравенство*

$$k \leqslant q^2 - \frac{\sqrt{q}}{2} + 1. \tag{9}$$

Для нечетных q имеется более сильный результат. Известно, что в этом случае любая (q^2+1)-шапка является эллиптической квадрикой, и поэтому при больших значениях q справедлив следующий результат [25].

Теорема 13. *Пусть* $\mathcal{K}$ *–* k*-шапка в* $\mathrm{PG}(3,q)$, *где* $q \geqslant 67$ *нечетно, и пусть*

$$k > q^2 - \frac{q\sqrt{q}}{4} + 2q. \tag{10}$$

Тогда полная шапка, содержащая $\mathcal{K}$, *является эллиптической квадрикой.*

В этом параграфе мы покажем, как с помощью $(t \bmod q)$-дуг можно улучшить эти результаты при некотором дополнительном условии. Предположим, что $\mathcal{K}$ – (q^2+1-t)-шапка с $t < t_0$, где t_0 – наименьшее целое число, такое что существует блокирующее множество размера $q+1+t_0$ в $\mathrm{PG}(2,q)$, не содержащее полной прямой. Приведем некоторые оценки на t_0:

- $t_0 \geqslant \sqrt{q}$ для всех q, с равенством, когда q – квадрат [26];
- $\dfrac{q+1}{2}$, если $q = p$ – простое;
- $t_0 = q^{2/3} = p^2$, если $q = p^3$ [27, 28];
- $t_0 = p^e \left\lceil \dfrac{q/p^e + 1}{p^e + 1} \right\rceil$, если $q = p^h$ и $e \leqslant h/2$ [27, 28].

Теперь предположим, что $\mathcal{K}$ не содержит никакой $(q+2)$-плоскости. Разумеется, это условие всегда выполнено при нечетном q. Код, соответствующий такой шапке, имеет параметры $[q^2+1-t, 4, q^2-q-t]_q$. Минимальное расстояние выражается как

$$d = q^2 - q - t = q^3 - (q-1)q^2 - q - t,$$

т.е. в обозначениях из [15] имеем $s = 1$, $\varepsilon_2 = q-1$, $\varepsilon_1 = 1$, $\varepsilon_0 = t$. Поэтому теорему 6 из [15] непосредственно применить нельзя.

Заметим, что возможные кратности плоскости в $\mathrm{PG}(3,q)$ – это $0, 1, q+1-t, \ldots, q+1$. Следовательно, $\mathcal{K}$ является t-квазиделимой. Кроме того, если L – прямая, такая что $\mathcal{K}(L) = 2$, то $\widetilde{\mathcal{K}}(\widetilde{L}) = t$.

Заметим, что любая точка P из $\mathcal{K}$ содержится в 1-плоскости. Чтобы доказать это, рассмотрим проекцию φ из P на некоторую плоскость π, не проходящую через P. Тогда индуцированная плоская дуга $\mathcal{K}^{\varphi}$ проективна, поскольку $\mathcal{K}$ – шапка, и имеет параметры (q^2-t, q). Такая дуга является дополнением к $(q+1+t, 1)$-блокирующему множеству, которое с необходимостью содержит некоторую прямую L (так как $t < t_0$). Тогда плоскость $\langle P, L\rangle$ является 1-плоскостью (относительно $\mathcal{K}$). Заметим, что для 1-плоскости π имеем $\widetilde{\mathcal{K}}(\widetilde{\pi}) = 0$, а для 1-прямой L в π имеем $\widetilde{\mathcal{K}}(\widetilde{L}) = 1$.

Две 1-плоскости не могут пересекаться по 1-прямой (прямой подсчет). Рассмотрим две 1-плоскости π_0 и π_1, пересекающиеся по 0-прямой L. Пусть $\pi_2, \ldots, \pi_q$ – остальные $q-1$ плоскостей, проходящих через L, и пусть их кратности равны, соответственно, $q+1-b_i$, $i = 2, \ldots, q$. Снова простой подсчет показывает, что среди $\pi_2, \ldots, \pi_q$ нет ни одной 0- или 1-плоскости. Тогда

$$2 + \sum_{i=2}^{q} (q+1-b_i) = q^2 + 1 - t,$$

т.е. $\sum_{i=2}^{q} b_i = t$, откуда следует, что для 0-прямой L, лежащей в двух 1-плоскостях, выполнено $\widetilde{\mathcal{K}}(\widetilde{L}) = t$.

С учетом этих наблюдений оценим мощность дуги $\widetilde{\mathcal{K}}$. Рассмотрим 1-плоскость π (относительно шапки $\mathcal{K}$). Она содержит $q+1$ 1-прямых, $q^2 - t$ 0-прямых, лежащих в двух 1-плоскостях (поскольку каждая точка из $\mathcal{K}$ лежит на 1-плоскости), а также t 0-прямых, не содержащихся в какой-либо другой 1-плоскости. Для прямых L в плоскости π, являющихся 1- или 0-прямыми первого типа, имеем $\widetilde{\mathcal{K}}(\widetilde{L}) = t$; для 0-прямых L второго типа $\widetilde{\mathcal{K}}(\widetilde{L}) = t$ или $t + q$. Так как $\widetilde{\mathcal{K}}(\widetilde{\pi}) = 0$, то

$$|\widetilde{\mathcal{K}}| \leqslant t(q^2 + q + 1) + tq.$$

Предположим, что $|\widetilde{\mathcal{K}}| > t(q^2 + q + 1)$. Тогда легко проверить, что в $\widetilde{\mathrm{PG}}(3, q)$ существует плоскость кратности $t(q + 1) + q$ (относительно $\widetilde{\mathcal{K}}$). Тогда по теореме 10 существует блокирующее множество с параметрами $(q + 1 + t, 1)$ с прямыми кратностей $1, \ldots, t + 1$. Поскольку такое блокирующее множество обязательно содержит прямую, должно выполняться $t \geqslant q$, противоречие. Отсюда $|\widetilde{\mathcal{K}}| = t(q^2 + q + 1)$, и по следствию 3.5 из [29] дуга $\widetilde{\mathcal{K}}$ является суммой t плоскостей, а $\mathcal{K}$ допускает t-расширение. Итак, доказана следующая

Теорема 14. *Пусть $\mathcal{K}$ – $(q^2 + 1 - t)$-шапка в* $\mathrm{PG}(3, q)$ *с $t < t_0$, где t_0 – наименьшее целое число, такое что существует блокирующее множество размера $q + 1 + t_0$, не содержащее полной прямой. Кроме того, пусть $\mathcal{K}$ не содержит никакую $(q + 2)$-плоскость. Тогда $\mathcal{K}$ допускает расширение.*

Эта теорема охватывает случаи малых нечетных q и случаи четных q в предположении, что не существует плоскости, пересекающей эту шапку по гиперовалу.

СПИСОК ЛИТЕРАТУРЫ

1. *Hirschfeld J.W.P.* Projective Geometries over Finite Fields. Oxford: Clarendon, 1998.
2. *Landjev I., Storme L.* Linear Codes and Galois Geometries // Current Research Topics in Galois Geometries. New York: Nova Sci. Publ., 2012. P. 187–214.
3. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
4. *Heise W., Quatrocchi P.* Informations- und Codierungstheorie: mathematische Grundlagen der Daten-Kompression und -Sicherung in diskreten Kommunikationssystemen. Berlin: Springer, 1995.
5. *Tsfasman M.A., Vlăduţ S.G., Nogin, D.Yu.* Algebraic Geometric Codes: Basic Notions. Providence, R.I.: Amer. Math. Soc., 2007.
6. *Griesmer J.H.* A Bound for Error-Correcting Codes // IBM J. Res. Develop. 1960. V. 4. № 5. P. 532–542.
7. *Ward H.N.* Divisible Codes—A Survey // Serdica Math. J. 2001. V. 27. № 4. P. 263–278.
8. *Hill R., Lizak P.* Extensions of Linear Codes // Proc. 1995 IEEE Int. Sympos. on Information Theory (ISIT'1995). Whistler, BC, Canada. September 17–22, 1995. P. 345.
9. *Hill R.* An Extension Theorem for Linear Codes // Des. Codes Cryptogr. 1999. V. 17. № 1–3. P. 151–157.
10. *Maruta T.* On the Extendability of Linear Codes // Finite Fields Appl. 2001. V. 7. № 2. P. 350–354.
11. *Maruta T.* Extendability of Linear Codes over GF(q) with Minimum Distance d, $\gcd(d, q) = 1$ // Discrete Math. 2003. V. 266. № 1–3. P. 377–385.
12. *Maruta T.* A New Extension Theorem for Linear Codes // Finite Fields Appl. 2004. V. 10. № 4. P. 674–685.
13. *Maruta T.* Extension Theorems for Linear Codes over Finite Fields // J. Geom. 2011. V. 101. № 1–2. P. 173–183.

14. *Yoshida Y., Maruta T.* An Extension Theorem for $[n,k,d]_q$ Codes with $\gcd(d,q)=2$ // Australas. J. Combin. 2010. V. 48. P. 117–131.
15. *Landjev I., Rousseva A., Storme L.* On the Extendability of Quasidivisible Griesmer Arcs // Des. Codes Cryptogr. 2016. V. 79. № 3. P. 535–547.
16. *Dodunekov S., Simonis J.* Codes and Projective Multisets // Electron. J. Combin. 1998. V. 5. № 1. Research Paper R37.
17. *Landjev I.* The Geometric Approach to Linear Codes // Finite Geometries (Proc. 4th Isle of Thorns Conf. Chelwood Gate, UK. July 16–21, 2000). Dordrecht: Kluwer, 2001. P. 247–257.
18. *Hamada N.* The Rank of the Incidence Matrix of Points and d-Flats in Finite Geometries // J. Sci. Hiroshima Univ. Ser. A-I Math. 1968. V. 32. № 2. P. 381–396.
19. *Ceccherini P.V., Hirschfeld J.W.P.* The Dimension of Projective Geometry Codes // Discrete Math. 1992. V. 106/107. P. 117–126.
20. *Goethals J.-M., Delsarte P.* On a Class of Majority-Logic Decodable Cyclic Codes // IEEE Trans. Inform. Theory. 1968. V. 14. № 2. P. 182–188.
21. *MacWilliams F.J., Mann H.B.* On the p-Rank of the Design Matrix of a Difference Set // Inform. Control. 1968. V. 12. № 5. P. 474–489.
22. *Smith K.J.C.* On the p-Rank of the Incidence Matrix of Points and Hyperplanes in a Finfite Projective Geometry // J. Combin. Theory. 1969. V. 7. № 2. P. 122–129.
23. *Blokhuis A., Moorhouse G.E.* Some p-Ranks Related to Orthogonal Spaces // J. Algebraic Combin. 1995. V. 4. № 4. P. 295–316.
24. *Ball S., Hill R., Landjev I., Ward H.* On $(q^2+q+2,q+2)$-Arcs in the Projective Plane $\mathrm{PG}(2,q)$ // Des. Codes Cryptogr. 2001. V. 24. № 2. P. 205–224.
25. *Hirschfeld J.W.P.* Finite Projective Spaces in Three Dimensions. Oxford: Oxford Univ. Press, 1985.
26. *Bruen A.* Baer Subplanes and Blocking Sets // Bull. Amer. Math. Soc. 1970. V. 76. № 2. P. 342–344.
27. *Polverino O.* Small Blocking Sets in $\mathrm{PG}(2,p^3)$ // Des. Codes Cryptogr. 2000. V. 20. № 3. P. 319–324.
28. *Sziklai P., Szőnyi T.* Blocking Sets and Algebraic Curves // Rend. Circ. Mat. Palermo (2) Suppl. 1998. № 51. P. 71–86.
29. *Landjev I., Vandendriessche P.* A Study of (xv_t, xv_{t-1})-Minihypers in $\mathrm{PG}(t,q)$ // J. Combin. Theory Ser. A. 2012. P. 119. № 6. P. 1123–1131.

Ланджев Иван Николов
Новый болгарский университет, София, Болгария
Институт математики и информатики АН Болгарии,
София, Болгария
i.landjev@nbu.bg
Русева Ася Петрова
Факультет математики и информатики
Софийского университета им. св. Климента Охридского,
София, Болгария
assia@fmi.uni-sofia.bg

Поступила в редакцию
15.11.2018
После доработки
25.06.2019
Принята к публикации
27.06.2019