ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 55 **2019** **Вып. 2**

УДК 621.391.15

© 2019 г. **Д.И. Кошелев**

НЕРАСЩЕПИМЫЕ ТОРИЧЕСКИЕ КОДЫ[1]

Вводится новый широкий класс корректирующих кодов, называемых нерасщепимыми торическими кодами. Они являются естественным обобщением торических кодов, где вместо обычных (т.е. расщепимых) алгебраических торов берутся нерасщепимые. Основным преимуществом новых кодов является их цикличность, и следовательно, они потенциально могут быть декодированы довольно быстро. Многие классические коды, такие как (дважды расширенные) коды Рида – Соломона и (проективные) коды Рида – Маллера, содержатся (с точностью до эквивалентности) в новом классе. Наши коды явно описываются в терминах алгебраической и торической геометрии над конечными полями, поэтому их легко построить на практике. Наконец, мы получаем новые циклические реверсивные коды, являющиеся нерасщепимыми торическими на поверхности дель Пеццо степени 6 с числом Пикара 1. Мы также вычисляем их параметры, которые, как оказывается, достигают текущих нижних границ, по крайней мере для малых конечных полей.

Ключевые слова: конечные поля, торические и циклические коды, нерасщепимые алгебраические торы и торические многообразия, поверхности дель Пеццо, эллиптические кривые.

DOI: 10.1134/S0555292319020025

§ 1. Введение

Имеется хорошо развитая теория так называемых *торических кодов* [1, глава 8], т.е. алгеброгеометрических кодов (Гоппы) [1, глава 7] на *торических многообразиях* [2] (размерности d над конечным полем $\mathbb{F}_q$). Эти коды были обнаружены в [3, 4] как обобщение кодов Рида – Соломона (для $d = 1$). Торические коды являются d-мерными циклическими кодами (также известными как мультициклические или абелевы) [5, 6]. Несмотря на это, достаточно быстрые способы их декодирования не известны, а неэффективные представлены в [7, § 5].

Помимо обычных (т.е. расщепимых) *торов* и торических многообразий существуют также *нерасщепимые* (над $\mathbb{F}_q$) [8]. Поэтому естественно рассмотреть алгеброгеометрические коды на последних. Мы называем их *нерасщепимыми торическими кодами*. У них есть некоторые преимущества. Во-первых, группы $\mathbb{F}_q$-точек нерасщепимых торов часто являются циклическими, поэтому соответствующие коды оказываются циклическими (с простыми корнями) [9, п. 1.2.2]. Более того, некоторые торические циклические коды являются также *реверсивными* [10]. Во-вторых, нерасщепимые торы содержат больше $\mathbb{F}_q$-точек, чем расщепимый тор, т.е. больше чем $(q-1)^d$. Другими словами, нерасщепимые торические коды длиннее расщепимых, следовательно, они потенциально могут иметь лучшую корректирующую способность для исправления ошибок. Наконец, многие классические коды, такие как дважды расши-

[1] Работа выполнена при частичной финансовой поддержке фонда Саймонса.

ренные коды Рида – Соломона [9, п. 4.4.1], циклические коды Рида – Маллера (и их проективный аналог [11]), эквивалентны некоторым нерасщепимым торическим.

Статья организована следующим образом. В § 2 мы напоминаем некоторые результаты теории нерасщепимых алгебраических торов и торических многообразий над конечными полями. В частности, пп. 2.2, 2.4 ограничены размерностью $d \leqslant 2$. Наконец, в п. 2.5, где рассматриваются только *поверхности дель Пеццо* степени 6 [12, § 3], мы получаем много результатов для поверхности $\mathcal{D}_6$ с $\mathbb{F}_q$-числом Пикара 1 (торическая поверхность дель Пеццо с наибольшим полем расщепления) и ее антиканонической линейной системы. Затем в п. 3.1 мы определяем и изучаем нерасщепимые торические коды методами алгебраической, торической и комбинаторной геометрии. В частности, это позволяет явно выписать порождающие матрицы для всех торических кодов и даже порождающие многочлены, если эти коды циклические. В п. 3.2 представлена полная классификация торических кодов (с точностью до эквивалентности) на $\mathbb{P}^1$, $\mathbb{P}^2$ и квадратичных поверхностях. Наконец, в п. 3.3 мы получаем новые циклические реверсивные нерасщепимые торические коды на поверхности $\mathcal{D}_6$, вычисляя их параметры. Согласно кодовым таблицам [13] оказывается, что по крайней мере для небольших q эти коды в настоящее время являются наилучшими.

§ 2. Торическая геометрия над конечными полями

2.1. Алгебраические торы. Пусть $\mathbb{F}_q$ – конечное поле порядка q характеристики p, $\overline{\mathbb{F}}_q$ – его алгебраическое замыкание, а $\mathbb{G}_m = \overline{\mathbb{F}}_q \setminus \{0\}$. По определению алгебраическая группа T над $\mathbb{F}_q$ называется *алгебраическим тором* размерности d, если существует изоморфизм алгебраических многообразий $\varphi\colon \mathbb{G}_m^d \xrightarrow{\sim} T$, определенный над некоторым расширением $\mathbb{F}_{q^e}$. Можно предполагать, что φ является изоморфизмом в категории алгебраических групп [12, теорема 7]. Если такое e минимально, то $\mathbb{F}_{q^e}$ называется *полем расщепления* тора T. Мы называем T *расщепимым*, если $e = 1$. Заметим, что в случае циклической группы $T(\mathbb{F}_q)$ ее порядок делит $q^e - 1$.

Пусть $x \in \mathbb{G}_m^d$, $m \in \mathbb{Z}^d$, а $\Phi \in \mathrm{GL}(d, \mathbb{Z})$. Всюду далее мы придерживаемся обозначений

$$x^m = x_1^{m_1} \cdot \ldots \cdot x_d^{m_d} \quad \text{и} \quad \Phi(x) = \left(x^{\Phi_{\square,1}}, \ldots, x^{\Phi_{\square,d}}\right),$$

где $\Phi_{\square,j}$ – j-й столбец матрицы Φ. Кроме того, мы предполагаем, что Φ действует на m слева, т.е. $\Phi(m) = \Phi m$.

Для данного тора T рассмотрим его *решетки характеров* $M = \mathrm{Hom}_{\overline{\mathbb{F}}_q}(T, \mathbb{G}_m)$ и *кохарактеров* $N = M^*$ с действиями Фробениуса $\Phi, \Phi^t \in \mathrm{GL}(d, \mathbb{Z})$ соответственно. Напомним, что они сопряжены в $\mathrm{GL}(d, \mathbb{Z})$. Порядок матрицы Φ (т.е. Φ^t) равен e, поэтому все ее собственные значения содержатся в $\mu_e = \{\zeta \in \overline{\mathbb{F}}_q \mid \zeta^e = 1\}$. *Ранг* r тора T определяется как ранг подрешетки инвариантов M^Φ (т.е. N^{Φ^t}). Тор T называется *изотропным*, если $r > 0$, т.е. при наличии у него нетривиальных $\mathbb{F}_q$-(ко)характеров. В противном случае T называется *анизотропным*.

Теорема 1 [14, п. 2.1.7]. *Следующие свойства эквивалентны*:
1. *Тор T расщепим*;
2. $r = d$;
3. *Все (ко)характеры тора T определены над $\mathbb{F}_q$*;
4. *Все собственные значения матрицы Φ равны* 1.

Теорема 2 [12, § 1]. *Отображение $T \mapsto \Phi$ является биекцией между множеством d-мерных $\mathbb{F}_q$-торов, расщепимых над $\mathbb{F}_{q^e}$, и множеством матриц (с точностью до сопряжения) из $\mathrm{GL}(d, \mathbb{Z})$ порядка e. Точнее говоря, под действием обратного отображения матрица Φ соответствует геометрическому фактору $T_\Phi = \mathbb{G}_m^d/\Phi$.*

Теорема 3 [12, § 2]. *При фиксированном d существует лишь конечное (с точностью до сопряжения) число конечных подгрупп в $\mathrm{GL}(d,\mathbb{Z})$. В частности, существует лишь конечное число d-мерных $\mathbb{F}_q$-торов.*

Теорема 4 [14, п. 2.1.7; 8, п. 9.2]. *Справедливы следующие утверждения*:

1. *Тор T обладает единственным максимальным расщепимым (анизотропным) $\mathbb{F}_q$-подтором T_s (соответственно, T_a);*
2. *Более того, $T_sT_a = T$ и $|T_s \cap T_a| < \infty$. Другими словами, отображение*

$$T_s \times T_a \to T, \quad (P_s, P_a) \mapsto P_s \cdot P_a$$

является $\mathbb{F}_q$-изогенией. В частности,

$$|T(\mathbb{F}_q)| = (q-1)^r |T_a(\mathbb{F}_q)|;$$

3. *Торы T_s и T_a соответствуют решеткам M^Φ и M/M^Φ с естественно индуцированным действием Φ. В частности, $r = \dim(T_s)$ и поля расщепления торов T и T_a совпадают.*

Лемма 1 [8, теорема 9.1.1]. *Прообраз $\varphi^{-1}(T(\mathbb{F}_q))$ равен "собственному пространству"*

$$\mathrm{E}_q(\Phi) = \{x \in \mathbb{G}_m^d(\mathbb{F}_{q^e}) \mid \Phi(x) = x^q\},$$

ассоциированному с собственным значением q.

Иначе говоря, если α – некоторый примитивный элемент поля $\mathbb{F}_{q^e}$, то

$$\mathbb{G}_m^d(\mathbb{F}_{q^e}) = \{(\alpha^{v_1}, \ldots, \alpha^{v_d}) \mid v_i \in \mathbb{Z}/(q^e-1)\}$$

и

$$\mathrm{E}_q(\Phi) = \left\{(\alpha^{v_1}, \ldots, \alpha^{v_d}) \;\Big|\; \sum_{i=1}^{d} \Phi_{i,j} v_i \equiv q v_j \pmod{q^e-1}\right\}.$$

Лемма 2. *Пусть $x \in \mathrm{E}_q(\Phi)$, $m \in M$, и пусть k – мощность орбиты вектора m относительно Φ. Тогда $x^{\Phi^s(m)} = x^{q^s m}$ для $0 \leqslant s \leqslant k-1$ (в частности, $x^m \in \mathbb{F}_{q^k}$).*

Доказательство. Утверждение следует из цепочки равенств

$$x^{\Phi(m)} = \prod_{i=1}^{d} x_i^{\sum\limits_{j=1}^{d} \Phi_{i,j} m_j} = \prod_{j=1}^{d} \left(\prod_{i=1}^{d} x_i^{\Phi_{i,j}} \right)^{m_j} = \prod_{j=1}^{d} x_j^{q m_j} = x^{qm}. \quad \blacktriangle$$

Теорема 5. *Верно, что*

$$|T(\mathbb{F}_q)| = \chi(q) \equiv \pm 1 \pmod{q},$$

где $\chi(\lambda) = \det(\lambda I - \Phi)$ – характеристический многочлен матрицы Φ. Более того, если тор T нерасщепим, то он имеет строго больше $\mathbb{F}_q$-точек, чем расщепимый, т.е.

$$|T(\mathbb{F}_q)| > (q-1)^d.$$

Доказательство. Первая часть утверждения доказана в [8, теорема 9.1.2]. Для второй приведем доказательство, предложенное Б. Кунявским в частном письме. Пусть $\lambda_1, \ldots, \lambda_d$ – все собственные значения матрицы Φ. По теореме 1 хотя бы одно из них отлично от 1. Таким образом, получаем строгое неравенство

$$|T(\mathbb{F}_q)| = \chi(q) = \prod_{i=1}^{d} |q - \lambda_i| > \prod_{i=1}^{d} (q - |\lambda_i|) = (q-1)^d. \quad \blacktriangle$$

Пусть $n, m \in \mathbb{N}$, $m \mid n$, и пусть $\mathrm{R}_{n,q}$ – ограничение скаляров Вейля тора $\mathbb{G}_m$ относительно расширения $\mathbb{F}_{q^n}/\mathbb{F}_q$ (см., например, [8, п. 3.12]). Универсальное свойство ограничения Вейля дает *отображение нормы* $\mathrm{N}_{n,m,q}\colon \mathrm{R}_{n,q} \to \mathrm{R}_{m,q}$ [15, § 5], являющееся сюръективным $\mathbb{F}_q$-гомоморфизмом алгебраических торов. В частности,

$$\mathrm{N}_{n,q} := \mathrm{N}_{n,1,q}\colon \mathrm{R}_{n,q} \to \mathbb{G}_m, \quad \mathrm{N}_{n,q}(P) = P \cdot P^{(1)} \cdot \ldots \cdot P^{(n-1)},$$

является обычным отображением нормы, т.е. произведением n сопряженных (над $\mathbb{F}_q$) точек. Кроме того, согласно [15, лемма 5.1.ii] ограничение отображения $\mathrm{N}_{n,m,q}$ на подгруппу $\mathrm{R}_{n,q}(\mathbb{F}_q)$ – это норма расширения $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$. Наконец, рассмотрим $\mathbb{F}_q$-торы

$$\mathrm{R}_{n,q}^{(m)} = \ker(\mathrm{N}_{n,m,q}), \quad \mathrm{T}_{n,q} = \bigcap_{\substack{m \mid n \\ m \neq n}} \mathrm{R}_{n,q}^{(m)}.$$

При $m = 1$ первый из них называется *норменным тором*. Интересно, что для n, равных произведению различных простых чисел, группы $\mathrm{T}_{n,q}(\mathbb{F}_q)$ используются в криптографии [15, § 6].

Теорема 6 [14, п. 2.1.7; 15, § 5]. *Справедливы следующие утверждения*:

1. $(\mathrm{R}_{n,q})_a = \mathrm{R}_{n,q}^{(1)}$, *и поэтому* $\mathrm{T}_{n,q}$ *является анизотропным тором*;
2. *Поля расщепления торов* $\mathrm{R}_{n,q}$, $\mathrm{R}_{n,q}^{(1)}$ *и* $\mathrm{T}_{n,q}$ *равны* $\mathbb{F}_{q^n}$;
3. $\dim(\mathrm{T}_{n,q}) = \varphi(n)$ *и* $\mathrm{T}_{n,q}(\mathbb{F}_q) \simeq \mathbb{Z}/(\Phi_n(q))$, *где* φ – *функция Эйлера, а* Φ_n – n*-й круговой многочлен.*

2.2. Алгебраические торы размерности 1 и 2.

Теорема 7 [16]. *Существуют лишь следующие одномерные алгебраические* $\mathbb{F}_q$*-торы*:

T	e	r	Φ	$T(\mathbb{F}_q)$
$\mathbb{G}_m$	1	1	1	$\mathbb{Z}/(q-1)$
$T_2 = \mathrm{R}_{2,q}^{(1)}$	2	0	-1	$\mathbb{Z}/(q+1)$

.

Теорема 8 [16]. *Существуют лишь следующие двумерные алгебраические* $\mathbb{F}_q$*-торы*:

T	e	r	$\Phi \in \mathrm{GL}(M)$	$T(\mathbb{F}_q)$
$\mathbb{G}_m^2$	1	2	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$(\mathbb{Z}/(q-1))^2$
$T_{2.a} = T_2^2$	2	0	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$(\mathbb{Z}/(q+1))^2$
$T_{2.b} = \mathbb{G}_m \times T_2$	2	1	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\mathbb{Z}/(q-1) \times \mathbb{Z}/(q+1)$
$T_{2.c} = \mathrm{R}_{2,q}$	2	1	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\mathbb{Z}/(q^2-1)$
$T_3 = \mathrm{R}_{3,q}^{(1)}$	3	0	$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$	$\mathbb{Z}/(q^2+q+1)$
$T_4 = \mathrm{R}_{2,q}\big(\mathrm{R}_{2,q^2}^{(1)}\big)$	4	0	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\mathbb{Z}/(q^2+1)$
$T_6 = \mathrm{T}_{6,q}$	6	0	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	$\mathbb{Z}/(q^2-q+1)$

.

В работе [16] не приведены значения r и $T(\mathbb{F}_q)$, которые очевидны или следуют из теоремы 6. Кроме того, в [16] тор T_3 (соответственно, T_4) обозначается через T_4 (соответственно, T_5). Мы поменяли обозначение, потому что степень расширения тора T_3 (соответственно, T_4) равна 3 (соответственно, 4). Кроме того, мы будем обозначать матрицу Φ для T_i через Φ_i.

Помимо классификации нам будет полезна

Теорема 9 [17]. *Все $\mathbb{F}_q$-торы размерности 1 и 2 являются рациональными над $\mathbb{F}_q$.*

2.3. Торические многообразия. Мы сохраняем обозначения из п. 2.1. Пусть T – $\mathbb{F}_q$-тор, а V – проективное гладкое $\mathbb{F}_q$-многообразие (размерности d). Мы говорим, что V является *торическим многообразием* (относительно T), если оно содержит T в качестве открытого подмножества и групповая операция на T может быть продолжена до действия тора T на V. Оно называется *расщепимым*, если T расщепим. Кроме того, пусть V' – другое торическое многообразие относительно некоторого тора T'. Тогда морфизм $\varphi\colon V \to V'$ называется *морфизмом торических многообразий*, если его ограничение $\varphi\colon T \to T'$ является гомоморфизмом.

Теорема 10. *Пусть V – проективное гладкое $\mathbb{F}_q$-многообразие с точным действием $\mathbb{F}_q$-тора T и открытой орбитой U. Тогда T и U изоморфны над $\mathbb{F}_q$ (с учетом действия T), и поэтому V является торическим многообразием (относительно T).*

Доказательство. Орбита U является T-торсором, поэтому T и U изоморфны над $\overline{\mathbb{F}}_q$, а многообразие V геометрически рационально. По теореме из [18, § 2] оно имеет $\mathbb{F}_q$-точку. С другой стороны, [19, предложение 4] гарантирует существование $\mathbb{F}_q$-точки на U, и таким образом, T и U изоморфны над $\mathbb{F}_q$. ▲

В дальнейшем мы будем использовать следующие обозначения:

$$M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}, \quad N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R}, \quad \rho(V) = \operatorname{rank}(\operatorname{Pic}(V)),$$
$$\overline{V} = V \otimes_{\operatorname{Spec}(\mathbb{F}_q)} \operatorname{Spec}(\overline{\mathbb{F}}_q),$$

и пусть $\operatorname{TDiv}(V)$ – множество T-инвариантных $\mathbb{F}_q$-дивизоров на V. Используя стандартную терминологию торической геометрии (см., например, [2]), рассмотрим следующие множества:

Poly: Пары (P, Φ), где $P \subset M_{\mathbb{R}}$ – полномерный гладкий *выпуклый решетчатый многогранник*, а $\Phi \in \mathrm{GL}(M)$ – матрица конечного порядка, такая что $\Phi(P) = P$.

Fan: Тройки (Σ, Φ, D), где Σ – проективный гладкий *веер* в $N_{\mathbb{R}}$, инвариантный относительно матрицы $\Phi \in \mathrm{GL}(N)$ конечного порядка. Другими словами, для любого конуса $\sigma \in \Sigma$ мы имеем, что $\Phi(\sigma) \in \Sigma$. Наконец, D – (очень) обильная Φ-инвариантная целочисленная комбинация лучей из Σ.

Split: Тройки (V, Φ, D), где V – расщепимое торическое $\mathbb{F}_q$-многообразие, Φ – автоморфизм на V (как торического многообразия), а $D \in \operatorname{TDiv}(V)$ – (очень) обильный Φ-дивизор.

Tor: Тройки (V, T, D), где V – торическое $\mathbb{F}_q$-многообразие относительно $\mathbb{F}_q$-тора T, а $D \in \operatorname{TDiv}(V)$ – (очень) обильный дивизор.

Хорошо известно, что эти множества соответствуют друг другу с помощью следующих отображений (расщепимый случай обсуждается в [2]):

1. Отображение

$$\mathbf{Poly} \to \mathbf{Fan}, \quad (P, \Phi) \mapsto (\Sigma_P, \Phi^t, D_P),$$

где Σ_P и D_P – это соответствующие многограннику P нормальный веер [2, теорема 2.3.2] и целочисленная комбинация лучей [2, § 4.2];

2. Отображение

$$\mathbf{Fan} \to \mathbf{Split}, \quad (\Sigma, \Phi, D) \mapsto (V_\Sigma, \Phi, D),$$

где V_Σ – соответствующее вееру Σ расщепимое торическое многообразие [2, § 3.1], а Φ – автоморфизм на $\mathbb{G}_m^d$ из п. 2.1, продолженный на V_Σ;

3. Отображение

$$\mathbf{Split} \to \mathbf{Tor}, \quad (V_\Sigma, \Phi, D) \mapsto (V_{\Sigma,\Phi}, T_\Phi, D),$$

где

$$V_{\Sigma,\Phi} = V_\Sigma/\Phi, \quad T_\Phi = \mathbb{G}_m^d/\Phi$$

– геометрические факторы многообразий V_Σ и $\mathbb{G}_m^d$ по автоморфизму Φ. Торическое многообразие $V_{\Sigma,\Phi}$ называется *моделью Демазюра* тора T_Φ.

Теорема 11 [12, §§ 1, 2]. *Все $\mathbb{F}_q$-формы многообразия V_Σ (без торической структуры) являются торическими, т.е. имеют вид $V_{\Sigma,\Phi}$ для $\Phi \in \mathrm{Aut}(\Sigma)$. Кроме того, для $\Phi' \in \mathrm{Aut}(\Sigma)$ многообразия $V_{\Sigma,\Phi}, V_{\Sigma,\Phi'}$ изоморфны над $\mathbb{F}_q$ (как торические многообразия), если и только если матрицы Φ, Φ' сопряжены в $\mathrm{Aut}(\Sigma)$. Наконец, $V_\Sigma, V_{\Sigma,\Phi}$ изоморфны над $\mathbb{F}_{q^e}$.*

Наоборот, рассмотрим матрицу $\Phi \in \mathrm{GL}(N)$ и тор T_Φ. Имеется проективный гладкий веер в $N_\mathbb{R}$, инвариантный относительно Φ. Другими словами, существует торическое $\mathbb{F}_q$-многообразие относительно T_Φ.

Пусть Σ^{Φ^t} – множество инвариантных конусов веера Σ относительно матрицы $\Phi^t \in \mathrm{Aut}(\Sigma)$. Кроме того, для $\sigma \in \Sigma^{\Phi^t}$ обозначим через $\sigma^* \subset M_\mathbb{R}$ конус, двойственный к σ, а через $T_{\Phi,\sigma}$ – тор, соответствующий ограничению действия Φ на подрешетку $M_\sigma = -\sigma^* \cap \sigma^* \cap M$ (размерности $d - \dim(\sigma)$).

Теорема 12 [20, теорема 1.3.2, следствие 1.3.6]. *Имеется естественное биективное соответствие*

$$V_{\Sigma,\Phi}(\mathbb{F}_q) = \bigsqcup_{\sigma \in \Sigma^{\Phi^t}} T_{\Phi,\sigma}(\mathbb{F}_q).$$

В частности, для анизотропного тора T_Φ выполнено равенство $V_{\Sigma,\Phi}(\mathbb{F}_q) = T_\Phi(\mathbb{F}_q)$.

Теорема 13 [12, § 1]. *Естественное вложение $\mathrm{Pic}(V_\Sigma) \hookrightarrow \mathrm{Pic}(\overline{V_\Sigma})$ является изоморфизмом. Другими словами, любой дивизор на $\overline{V_\Sigma}$ эквивалентен некоторому $\mathbb{F}_q$-дивизору. В то же время существует естественный изоморфизм между $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-модулем $\mathrm{Pic}(\overline{V_{\Sigma,\Phi}})$ и Φ-модулем $\mathrm{Pic}(V_\Sigma)$. В частности,*

$$\rho(V_{\Sigma,\Phi}) = \mathrm{rank}(\mathrm{Pic}(V_\Sigma)^\Phi).$$

Теорема 14 [8, теорема 4.3.1; 20, п. 1.3]. *Имеет место точная последовательность Φ-модулей*

$$0 \to M \to \mathrm{TDiv}(V_\Sigma) \to \mathrm{Pic}(V_\Sigma) \to 0,$$

а при переходе к инвариантам получаем точную последовательность групп

$$0 \to M^\Phi \to \mathrm{TDiv}(V_\Sigma)^\Phi \to \mathrm{Pic}(V_\Sigma)^\Phi \to \mathrm{Pic}(T_\Phi) \to 0.$$

Более того, группа

$$\mathrm{Pic}(T_\Phi) \simeq \mathrm{H}^1(\Phi, M)$$

конечна, и поэтому количество Φ^t-орбит на $\Sigma(1)$ равно $r(T_\Phi) + \rho(V_{\Sigma,\Phi})$.

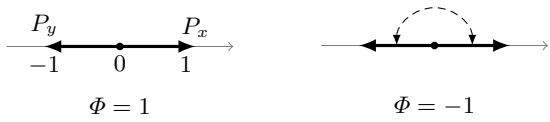

Рис. 1. Действия на примитивных векторах веера $\Sigma_{\mathbb{P}^1}$

При рассмотрении торических кодов нас будет интересовать образ $\mathrm{TDiv}(V_\Sigma)^\Phi$ в $\mathrm{Pic}(V_\Sigma)^\Phi$, который мы обозначаем через $\mathrm{TPic}(V_\Sigma, \Phi)$. В частности,

$$\mathrm{TPic}(V_\Sigma, I) = \mathrm{Pic}(V_\Sigma).$$

2.4. Проективная прямая $\mathbb{P}^1$ и торические поверхности. Хорошо известно, что $\mathbb{P}^1$ является единственным одномерным проективным гладким торическим многообразием. Пусть x, y – его однородные координаты. Простыми $\mathbb{G}_m$-инвариантными дивизорами на $\mathbb{P}^1$ являются лишь точки $P_x = (0:1)$, $P_y = (1:0)$.

Теорема 15 [2, пример 2.4.10]. *Веер прямой $\mathbb{P}^1$ и все возможные действия на нем представлены на рис.* 1. *Точнее говоря,*

$$\mathrm{Aut}(\Sigma_{\mathbb{P}^1}) = \langle -1 \rangle \simeq \mathbb{Z}/2.$$

Кроме того, ясно, что

$$\mathrm{Pic}(\mathbb{P}^1) = \mathbb{Z}[P_y], \quad \mathrm{TPic}(\mathbb{P}^1, -1) = \mathbb{Z}[D_{x,y}],$$

где $D_{x,y} = P_x + P_y$.

Далее мы будем говорить о торических поверхностях. Нам понадобится обозначение $\mathbb{V}(f_1, \ldots, f_n)$ для алгебраического многообразия, порожденного некоторым семейством $\mathbb{F}_q$-многочленов $f_1, \ldots, f_n$, $n \in \mathbb{N}$.

Теорема 16 [21, § 4.1]. *Любая торическая $\mathbb{F}_q$-поверхность может быть получена с помощью последовательности раздутий в $\mathbb{F}_q$-орбитах тор-инвариантных точек, начиная с $\mathbb{F}_q$-минимальных поверхностей, являющихся $\mathbb{F}_q$-формами для*
1. $\mathbb{P}^2$;
2. $\mathbb{P}^1 \times \mathbb{P}^1$;
3. *Поверхностей Хирцебруха $\mathbb{F}_m$ при $m > 1$;*
4. *Поверхности дель Пеццо степени* 6 *с $\mathbb{F}_q$-числом Пикара* 1.

Проективная плоскость $\mathbb{P}^2$. Напомним, что формы (над любым полем) плоскости $\mathbb{P}^2$ называются *поверхностями Севери – Брауэра.* Согласно [22, предложение 4.5.10; 18, § 2] имеет место

Лемма 3. *Не существует поверхностей Севери – Брауэра над $\mathbb{F}_q$, отличных от $\mathbb{P}^2$.*

Пусть x, y, z – однородные координаты на $\mathbb{P}^2$. Хорошо известно, что $\mathbb{P}^2$ является расщепимой торической поверхностью и все ее простые тор-инвариантные дивизоры – это прямые $L_x = \mathbb{V}(x)$, $L_y = \mathbb{V}(y)$, $L_z = \mathbb{V}(z)$.

Теорема 17 [2, пример 3.1.9]. *Веер плоскости $\mathbb{P}^2$ и все возможные действия на нем (с точностью до сопряжения) представлены на рис.* 2. *Точнее говоря,*

$$\mathrm{Aut}(\Sigma_{\mathbb{P}^2}) = \langle \Phi_3^t \rangle \rtimes \langle \Phi_{2.c} \rangle \simeq S_3.$$

Кроме того, ясно, что

$$\mathrm{Pic}(\mathbb{P}^2) = \mathrm{TPic}(\mathbb{P}^2, \Phi_{2.c}) = \mathbb{Z}[L_z], \quad \mathrm{TPic}(\mathbb{P}^2, \Phi_3) = \mathbb{Z}[D_{x,y,z}],$$

где $D_{x,y,z} = L_x + L_y + L_z$.

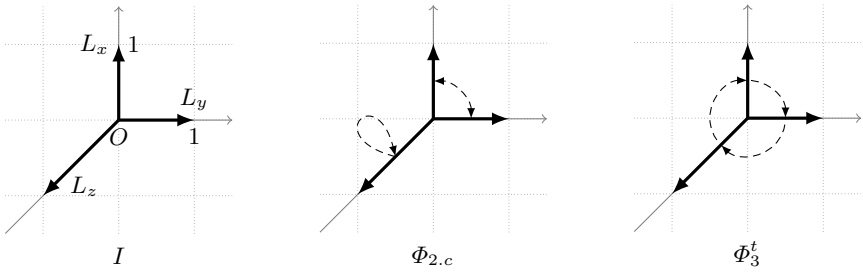

Рис. 2. Действия на примитивных векторах веера $\Sigma_{\mathbb{P}^2}$

Квадратичные поверхности. Рассмотрим две различные точки $P_1, P_2 \in \mathbb{P}^2$ и прямую L между ними. Последовательное раздутие в точках P_1, P_2 и стягивание собственного прообраза прямой L приводит к $\mathbb{F}_q$-поверхности Q. Если P_1, P_2 определены над $\mathbb{F}_q$, то Q называется *гиперболической квадратичной поверхностью* $\mathcal{H}$. В противном случае, т.е. если P_1, P_2 сопряжены над $\mathbb{F}_q$, поверхность Q называется *эллиптической квадратичной поверхностью* $\mathcal{E}$.

Теорема 18. *Во-первых,* $\mathcal{E}$ *является единственной нетривиальной* $\mathbb{F}_q$*-формой для* $\mathcal{H}$*. Кроме того, имеются следующие* $\mathbb{F}_q$*-изоморфизмы*:

$$\mathcal{H} \simeq \mathbb{P}^1 \times \mathbb{P}^1 \simeq \mathbb{V}(xy - zt), \quad \mathcal{E} \simeq \mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathbb{P}^1) \simeq \mathbb{V}(xy - Q(z,t)),$$

где x, y, z, t *– однородные координаты для* $\mathbb{P}^3$*, поверхность* $\mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathbb{P}^1)$ *– ограничение скаляров Вейля, а*

$$Q(z,t) = \begin{cases} z^2 - at^2 & (\text{где } a \in \mathbb{F}_q^*,\ \sqrt{a} \notin \mathbb{F}_q), \quad \text{если } p \neq 2, \\ z^2 + zt + at^2 & (\text{где } a \in \mathbb{F}_q^*,\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a) = 1), \quad \text{если } p = 2. \end{cases}$$

Доказательство. Классификация $\mathbb{F}_q$-форм следует из результатов [23, лемма 15.3.1; 12, § 3]. В свою очередь, наличие изоморфизмов обсуждается, например, в [24, п. 2.2.1; 25, пример 3.8]. ▲

Пусть x, y и u, v – две пары однородных координат на $\mathbb{P}^1 \times \mathbb{P}^1$. Действие тора $\mathbb{G}_m^2$ на $\mathcal{H}$ естественно наследуется от действия тора $\mathbb{G}_m$ на $\mathbb{P}^1$, а соответствующие простые $\mathbb{G}_m^2$-инвариантные дивизоры – это прямые

$$L_x = \{P_x\} \times \mathbb{P}^1, \quad L_y = \{P_y\} \times \mathbb{P}^1, \quad L_u = \mathbb{P}^1 \times \{P_u\}, \quad L_v = \mathbb{P}^1 \times \{P_v\}.$$

Теорема 19 [2, пример 3.1.12]. *Веер поверхности* $\mathcal{H}$ *и все возможные действия на нем (с точностью до сопряжения) представлены на рис.* 3*. Точнее говоря,*

$$\mathrm{Aut}(\Sigma_{\mathcal{H}}) = \langle \Phi_4^t \rangle \rtimes \langle \Phi_{2.c} \rangle \simeq D_4.$$

Заметим, что в геометрических терминах автоморфизм $\Phi_{2.c}$ является инволюцией $(P, Q) \mapsto (Q, P)$.

Лемма 4. *Имеются* $\mathbb{F}_q$*-изоморфизмы (без учета торической структуры)*

$$\mathcal{H} \simeq V_{\Sigma_{\mathcal{H}}, \Phi_{2.a}} \simeq V_{\Sigma_{\mathcal{H}}, \Phi_{2.b}}, \quad \mathcal{E} \simeq V_{\Sigma_{\mathcal{H}}, \Phi_{2.c}} \simeq V_{\Sigma_{\mathcal{H}}, \Phi_4}.$$

Доказательство. Достаточно явно реализовать все торические $\mathbb{F}_q$-формы поверхности $\mathcal{H}$. Первая часть леммы очевидна, потому что $\mathbb{P}^1 \times \mathbb{P}^1$ является торической поверхностью относительно торов $T_{2.a}$, $T_{2.b}$. С другой стороны, благодаря универсальному свойству ограничения Вейля действие тора $\mathbb{G}_m$ (соответственно, T_2) на $\mathbb{P}^1$

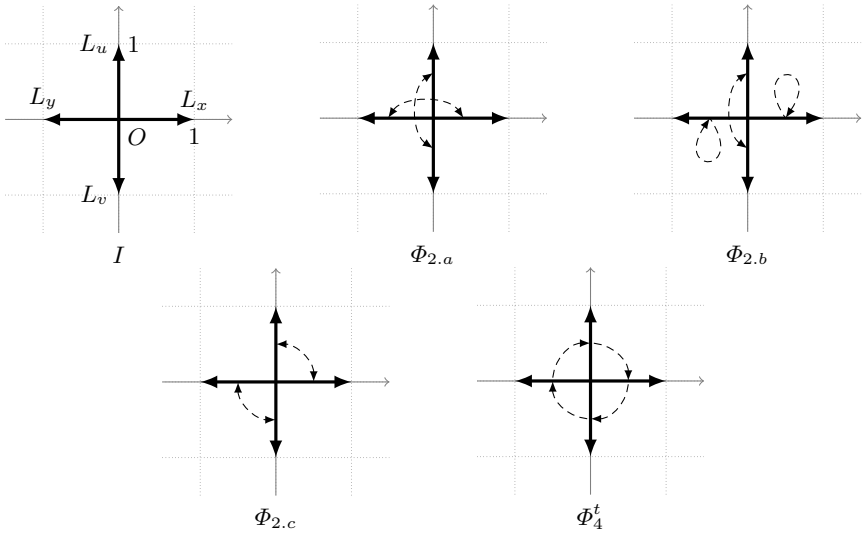

Рис. 3. Действия на примитивных векторах веера $\Sigma_{\mathcal{H}}$

преобразуется в действие тора $T_{2.c}$ (соответственно, T_4) на $\mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathbb{P}^1)$. Таким образом, вторая часть также верна. ▲

Наконец, легко доказывается, что

$$\mathrm{Pic}(\mathcal{H}) = \mathbb{Z}[L_y] \oplus \mathbb{Z}[L_v], \quad \mathrm{TPic}(\mathcal{H}, \Phi_{2.a}) = \mathbb{Z}[D_{x,y}] \oplus \mathbb{Z}[D_{u,v}],$$
$$\mathrm{TPic}(\mathcal{H}, \Phi_{2.b}) = \mathbb{Z}[L_y] \oplus \mathbb{Z}[D_{u,v}], \quad \mathrm{Pic}(\mathcal{E}) = \mathrm{TPic}(\mathcal{H}, \Phi_{2.c}) = \mathbb{Z}[D_{y,v}],$$
$$\mathrm{TPic}(\mathcal{H}, \Phi_4) = \mathbb{Z}[D_{x,y,u,v}],$$

где

$$D_{x,y} = L_x + L_y, \quad D_{u,v} = L_u + L_v, \quad D_{y,v} = L_y + L_v, \quad D_{x,y,u,v} = D_{x,y} + D_{u,v}.$$

Поверхности Хирцебруха $\mathbb{F}_m$ при $m > 0$. Эти поверхности задаются уравнением

$$\mathbb{F}_m = \mathbb{V}(u^m y - v^m x) \subset \mathbb{P}^2_{(x:y:z)} \times \mathbb{P}^1_{(u:v)}.$$

Проекция $f\colon \mathbb{F}_m \to \mathbb{P}^1_{(u:v)}$ является единственным $\mathbb{P}^1$-расслоением на $\mathbb{F}_m$. Легко доказать, что не существует нетривиальных $\mathbb{F}_q$-форм для $\mathbb{F}_m$, и эта поверхность является расщепимой торической. Ее тор-инвариантные простые дивизоры имеют вид

$$F_u = \mathbb{V}(u, x), \quad F_v = \mathbb{V}(v, y), \quad \Sigma = \mathbb{V}(x, y), \quad S = \mathbb{V}(\mathbb{F}_m, z).$$

Кривые F_u, F_v являются слоями расслоения f над точками $P_u, P_v \in \mathbb{P}^1$ соответственно. В свою очередь, кривые Σ и S являются образами сечений для f, чьи кратности самопересечения равны $-m$ и m соответственно.

Рассмотрим матрицу

$$\Phi_{\mathbb{F}_m} = \begin{pmatrix} 1 & 0 \\ m & -1 \end{pmatrix} \in \mathrm{GL}(M)$$

и заметим, что она сопряжена к $\Phi_{2.b}$, если $2 \mid m$, и к $\Phi_{2.c}$, если $2 \nmid m$.

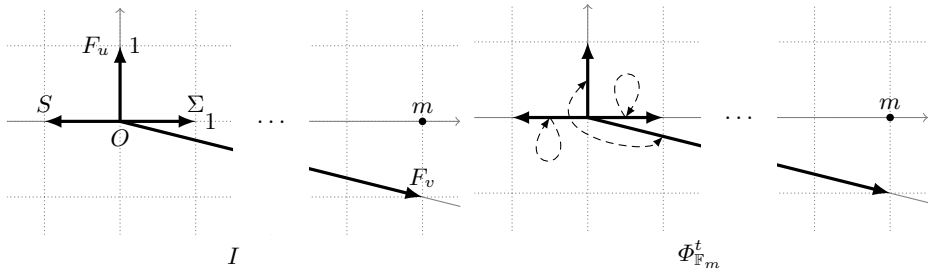

Рис. 4. Действия на примитивных векторах веера $\Sigma_{\mathbb{F}_m}$ при $m > 0$

Теорема 20 [2, пример 3.1.16]. *Веер поверхности $\mathbb{F}_m$ и все возможные действия на нем представлены на рис.* 4. *Точнее говоря,*

$$\mathrm{Aut}(\Sigma_{\mathbb{F}_m}) = \langle \Phi^t_{\mathbb{F}_m} \rangle \simeq \mathbb{Z}/2.$$

Наконец, легко проверяется, что

$$\mathrm{Pic}(\mathbb{F}_m) = \mathbb{Z}[S] \oplus \mathbb{Z}[F_v], \quad \mathrm{TPic}(\mathbb{F}_m, \Phi_{\mathbb{F}_m}) = \mathbb{Z}[S] \oplus \mathbb{Z}[D_m],$$

где

$$D_m = \begin{cases} F_u + F_v, & \text{если } 2 \mid m, \\ \Sigma + \dfrac{m-1}{2}(F_u + F_v), & \text{если } 2 \nmid m, \end{cases} \qquad D_m \sim \begin{cases} 2F_v, & \text{если } 2 \mid m, \\ S - F_v, & \text{если } 2 \nmid m. \end{cases}$$

Стоит также отметить, что дивизор $r_1 S + r_2 F_v$ (очень) обилен тогда и только тогда, когда $r_1, r_2 > 0$.

2.5. Поверхности дель Пеццо степени 6. В этом пункте мы будем использовать обозначения для $\mathbb{P}^2$ и базовые факты из [12, § 3]. Рассмотрим точки

$$P_x = (1:0:0), \quad P_y = (0:1:0), \quad P_z = (0:0:1).$$

Хорошо известно, что совокупное раздутие $\mathbb{P}^2$ в этих точках дает $\mathbb{F}_q$-*поверхность дель Пеццо* $\mathcal{D}_1$ степени 6, и она единственна над $\overline{\mathbb{F}}_q$. Кроме того, $\mathcal{D}_1$ является торической поверхностью, потому что точки P_x, P_y, P_z тор-инвариантны.

Пусть E_x, E_y, E_z – исключительные кривые, ассоциированные с точками P_x, P_y, P_z соответственно, а $\widetilde{L}_x, \widetilde{L}_y, \widetilde{L}_z$ – собственные прообразы прямых L_x, L_y, L_z соответственно. Эти шесть кривых являются единственными тор-инвариантными простыми дивизорами на $\mathcal{D}_1$. Кроме того, дивизор

$$H_0 = E_x + E_y + E_z + \widetilde{L}_x + \widetilde{L}_y + \widetilde{L}_z$$

антиканоничен и дает $\mathbb{F}_q$-вложение $\mathcal{D}_1 \hookrightarrow \mathbb{P}^6$.

Теорема 21. *Веер поверхности $\mathcal{D}_1$ и все возможные действия на нем представлены на рис.* 5, *где*

$$\Phi'_{2.c} = (-1)\Phi_{2.c} = \Phi_4 \Phi_{2.c} \Phi_4^{-1}.$$

Точнее говоря,

$$\mathrm{Aut}(\Sigma_{\mathcal{D}_1}) = \mathrm{Aut}(\Sigma_{\mathbb{P}^2}) \times \langle \Phi_{2.a} \rangle = \langle \Phi_6^t \rangle \rtimes \langle \Phi_{2.c} \rangle \cong D_6.$$

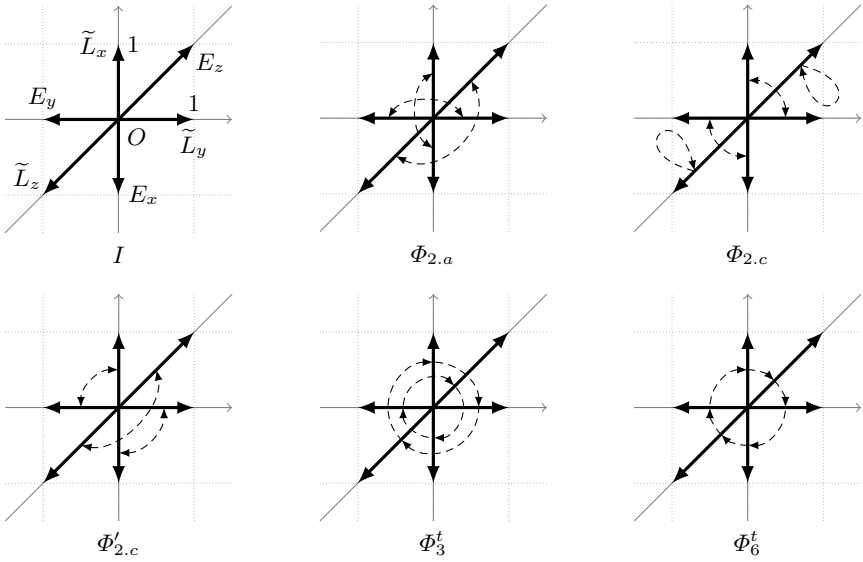

Рис. 5. Действия на примитивных векторах веера $\Sigma_{\mathcal{D}_1}$

Таблица 1

$\mathbb{F}_q$-поверхности дель Пеццо степени 6

$\mathcal{D}$	$\lvert\mathcal{D}(\mathbb{F}_q)\rvert$	$\rho(\mathcal{D})$
$\mathcal{D}_1 = \mathrm{Bl}_{1,1,1}(\mathbb{P}^2) = \mathrm{Bl}_{1,1}(\mathcal{H})$	q^2+4q+1	4
$\mathcal{D}_{2.a} = \mathrm{Bl}_2(\mathcal{H})$	q^2+2q+1	3
$\mathcal{D}_{2.c} = \mathrm{Bl}_{1,2}(\mathbb{P}^2) = \mathrm{Bl}_{1,1}(\mathcal{E})$	q^2+2q+1	3
$\mathcal{D}'_{2.c} = \mathrm{Bl}_2(\mathcal{E})$	q^2+1	2
$\mathcal{D}_3 = \mathrm{Bl}_3(\mathbb{P}^2)$	q^2+q+1	2
$\mathcal{D}_6$	q^2-q+1	1

Заметим, что в геометрических терминах $\Phi_{2.a}$ является стандартным квадратичным преобразованием

$$\mathbb{P}^2 \dashrightarrow \mathbb{P}^2, \quad (x:y:z) \mapsto (yz:xz:xy) = (x^{-1}:y^{-1}:z^{-1}),$$

поднятым на $\mathcal{D}_1$.

Будем обозначать через $\mathcal{D}_i$ (соответственно, $\mathcal{D}'_{2.c}$) торическую поверхность $V_{\Sigma_{\mathcal{D}_1},\Phi_i}$ (соответственно, $V_{\Sigma_{\mathcal{D}_1},\Phi'_{2.c}}$). Подчеркнем, что поверхности $\mathcal{D}_{2.c}$ и $\mathcal{D}'_{2.c}$ не изоморфны над $\mathbb{F}_q$, хотя обе содержат тор $T_{2.c}$. Кроме того, для произвольной торической поверхности S обозначим через $\mathrm{Bl}_{a_1,\dots,a_n}(S)$ ее раздутие в некоторых $\mathbb{F}_q$-орбитах (мощностей $a_1,\dots,a_n$, $n \in \mathbb{N}$) тор-инвариантных точек. Вообще говоря, такое раздутие, разумеется, зависит от выбора $\mathbb{F}_q$-орбит с данными мощностями. Согласно теоремам 12, 14 и рис. 5 справедлива

Теорема 22. *Все $\mathbb{F}_q$-поверхности дель Пеццо степени 6 приведены в табл. 1. В частности, $\mathcal{D}_6$ является единственной среди них $\mathbb{F}_q$-минимальной поверхностью.*

В дальнейшем мы сосредоточим свое внимание на поверхности $\mathcal{D}_6$, потому что торические коды на ней, кажется, имеют наилучшие параметры по сравнению с осталь-

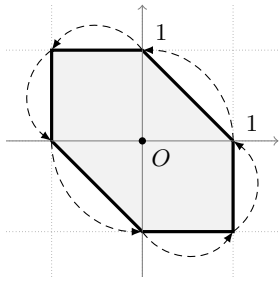

Рис. 6. Многоугольник P_{H_0} с действием Φ_6

ными поверхностями дель Пеццо степени 6. Прежде всего,

$$\mathrm{Pic}(\mathcal{D}_6) = \mathrm{TPic}(\mathcal{D}_1, \Phi_6) = \mathbb{Z}[H_0],$$

а многоугольник P_{H_0} с действием Φ_6 изображен на рис. 6. Следующая лемма представляет собой элементарное упражнение.

Лемма 5. *Для $r \in \mathbb{N}$ множество*

$$\{(0,0)\} \cup \{1 \leqslant i,\ 0 \leqslant j,\ i+j \leqslant r\} \subset M$$

состоит из представителей всех орбит относительно действия Φ_6 на $P_{rH_0} \cap M$. Кроме того, ненулевые точки этого множества представляют орбиты мощности 6. В частности,

$$|P_{rH_0} \cap M| = 3r(r+1) + 1.$$

Пусть $\boldsymbol{P} = \{P_1, P_2, P_3\}$ – тройка неколлинеарных $\mathbb{F}_q$-сопряженных точек на $\mathbb{P}^2$, а $\boldsymbol{Q} = \{Q_1, Q_2\}$ – пара различных $\mathbb{F}_q$-сопряженных точек на $\mathbb{P}^2$. В частности, эти пять точек находятся в общем положении, поэтому можно рассмотреть однозначно определенную невырожденную конику $\mathcal{C}$, проходящую через них. Для $i, j \in \{1,2,3\}$ $(i \neq j)$, $k \in \{1,2\}$ обозначим через $\mathcal{L}_{i,j}$, $\mathcal{M}$ и $\mathcal{N}_{j,k}$ прямые, проходящие, соответственно, через P_i и P_j, Q_1 и Q_2, P_j и Q_k. Кроме того, пусть

$$\mathcal{L} = \mathcal{L}_{1,2} + \mathcal{L}_{1,3} + \mathcal{L}_{2,3}, \quad \mathcal{N} = \sum_{j,k=1}^{3,2} \mathcal{N}_{j,k}.$$

Все упомянутые геометрические объекты представлены на рис. 7.

Поскольку прямые $\mathcal{N}_{j,k}$ сопряжены друг другу и любая торическая $\mathbb{F}_q$-поверхность однозначно определена действием Фробениуса на ее простых тор-инвариантных дивизорах, справедлива

Лемма 6. *Поверхность $\mathcal{D}_6$ получается раздутием $\mathbb{P}^2$ в орбитах $\boldsymbol{P}, \boldsymbol{Q}$ с последующим стягиванием собственных прообразов $\widetilde{\mathcal{M}}, \widetilde{\mathcal{C}}$ кривых $\mathcal{M}, \mathcal{C}$ соответственно.*

Будем обозначать через $\mathcal{B}$ соответствующую поверхность раздутия (являющуюся поверхностью дель Пеццо степени 4), а через φ_u (соответственно, φ_d) – отображение раздутия (стягивания). Другими словами, имеем диаграмму

$$\mathbb{P}^2 \xleftarrow{\varphi_u} \mathcal{B} \xrightarrow{\varphi_d} \mathcal{D}_6.$$

Кроме того, пусть

$$P_{\mathcal{M}} = \varphi_d(\widetilde{M}), \quad P_{\mathcal{C}} = \varphi_d(\widetilde{C}), \quad \varphi_{ud} = \varphi_u \circ \varphi_d^{-1},$$

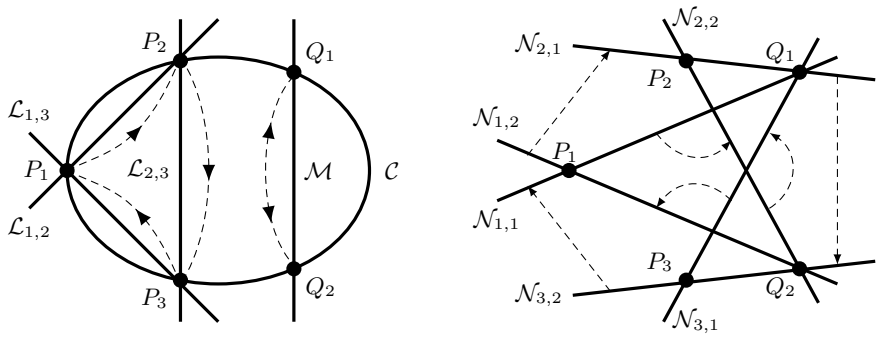

Рис. 7. Точки P_j, Q_k, прямые $\mathcal{L}_{i,j}, \mathcal{M}, \mathcal{N}_{j,k}$ и коника $\mathcal{C}$

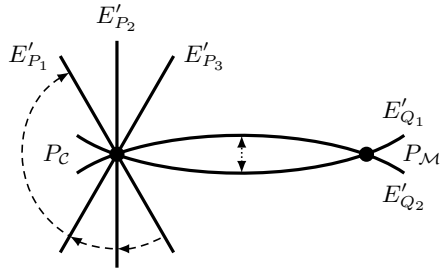

Рис. 8. Точки $P_{\mathcal{M}}, P_{\mathcal{C}}$ и кривые $E'_{\boldsymbol{P}}, E'_{\boldsymbol{Q}}$

и пусть

$$\mathcal{L}' = \mathcal{L}'_{1,2} + \mathcal{L}'_{1,3} + \mathcal{L}'_{2,3}$$

– собственный прообраз дивизора $\mathcal{L}$ относительно φ_{ud}. Наконец, пусть

$$E_{\boldsymbol{P}} = E_{P_1} + E_{P_2} + E_{P_3}, \quad E_{\boldsymbol{Q}} = E_{Q_1} + E_{Q_2}$$

– исключительные дивизоры, ассоциированные с $\boldsymbol{P}, \boldsymbol{Q}$ соответственно, и

$$E'_{\boldsymbol{P}} = (\varphi_d)_*(E_{\boldsymbol{P}}) = E'_{P_1} + E'_{P_2} + E'_{P_3}, \quad E'_{\boldsymbol{Q}} = (\varphi_d)_*(E_{\boldsymbol{Q}}) = E'_{Q_1} + E'_{Q_2}$$

(см. рис. 8). Заметим, что имеются биективные соответствия

$$\mathcal{D}_6 \setminus (E'_{\boldsymbol{P}} \cup E'_{\boldsymbol{Q}}) \xrightarrow{\varphi_{ud}}{\sim} \mathbb{P}^2 \setminus (\mathcal{M} \cup \mathcal{C}),$$
$$T_6(\mathbb{F}_q) \setminus \{P_{\mathcal{M}}, P_{\mathcal{C}}\} = \mathcal{D}_6(\mathbb{F}_q) \setminus \{P_{\mathcal{M}}, P_{\mathcal{C}}\} \xrightarrow{\varphi_{ud}}{\sim} \mathbb{P}^2(\mathbb{F}_q) \setminus (\mathcal{M} \cup \mathcal{C}).$$

Прямые $\mathcal{N}_{j,k}$ не являются касательными к $\mathcal{C}$, поэтому их собственные прообразы $\widetilde{\mathcal{N}}_{j,k} \subset \mathcal{B}$ не пересекают $\widetilde{\mathcal{C}}$ (и, разумеется, $\widetilde{\mathcal{M}}$). Следовательно, $\widetilde{\mathcal{N}}_{j,k} \xrightarrow{\varphi_d}{\sim} \varphi_d(\widetilde{\mathcal{N}}_{j,k})$, и мы будем использовать для них одно и то же обозначение. Легко видеть, что $\widetilde{\mathcal{N}}_{j,k}$ – исключительные кривые на $\mathcal{D}_6$, и таким образом,

$$H_0 = \sum_{j,k=1}^{3,2} \widetilde{\mathcal{N}}_{j,k} \in \mathrm{Div}(\mathcal{D}_6) \quad (\text{или } \mathrm{Div}(\mathcal{B})).$$

Лемма 7. *Множество гиперплоских $\mathbb{F}_q$-сечений на $\mathcal{D}_6 \subset \mathbb{P}^6$ представляется в виде*

$$|H_0| = \varphi_{ud}^*(\mathbb{L}) - 2E'_{\boldsymbol{P}} - 3E'_{\boldsymbol{Q}},$$

где неполная линейная система

$$\mathbb{L} = |\mathcal{N} - 2\boldsymbol{P} - 3\boldsymbol{Q}|$$

по определению состоит из плоских (возможно, приводимых) $\mathbb{F}_q$-секстик, проходящих через $\boldsymbol{P}$ с кратностью 2 и через $\boldsymbol{Q}$ с кратностью 3.

Доказательство. Действительно, нетрудно доказать, что

$$\varphi_u^*(\mathbb{L}) - 2E_{\boldsymbol{P}} - 3E_{\boldsymbol{Q}} = |\varphi_u^*(\mathcal{N}) - 2E_{\boldsymbol{P}} - 3E_{\boldsymbol{Q}}| = |H_0| \subset \mathrm{Div}(\mathcal{B}),$$

поэтому

$$\varphi_{ud}^*(\mathbb{L}) - 2E'_{\boldsymbol{P}} - 3E'_{\boldsymbol{Q}} = (\varphi_d)_*\big(\varphi_u^*(\mathbb{L}) - 2E_{\boldsymbol{P}} - 3E_{\boldsymbol{Q}}\big) = (\varphi_d)_*\big(|H_0|\big) =$$
$$= |H_0| \subset \mathrm{Div}(\mathcal{D}_6).$$

Для лучшего понимания прямого и обратного образов дивизоров на алгебраических многообразиях см., например, [26, §§ II.5, II.6, IV.2]. ▲

Согласно формуле из [26, пример V.3.9.2] для рода абсолютно неприводимой кривой (разновидность формулы Плюккера) легко убедиться, что справедлива

Лемма 8. *Существуют лишь следующие разложения на неприводимые компоненты для $\mathbb{F}_q$-кривых из $\mathbb{L}$:*

6: *Секстика с $\mu_{\boldsymbol{P}} = 2$, $\mu_{\boldsymbol{Q}} = 3$;*

$5 + \mathcal{M}$: *Квинтика с $\mu_{\boldsymbol{P}} = \mu_{\boldsymbol{Q}} = 2$ и $\mathcal{M}$;*

$4 + \mathcal{C}$: *Квартика с $\mu_{\boldsymbol{P}} = 1$, $\mu_{\boldsymbol{Q}} = 2$ и $\mathcal{C}$;*

$3 + \mathcal{C} + \mathcal{M}$: *Кубика с $\mu_{\boldsymbol{P}} = \mu_{\boldsymbol{Q}} = 1$, $\mathcal{C}$ и $\mathcal{M}$;*

$2 + 2 \cdot \mathcal{C}$: *Коника с $\mu_{\boldsymbol{P}} = 0$, $\mu_{\boldsymbol{Q}} = 1$ и две копии коники $\mathcal{C}$;*

$2 + 2 \cdot \mathcal{M} + \mathcal{C}$: *Коника с $\mu_{\boldsymbol{P}} = 1$, $\mu_{\boldsymbol{Q}} = 0$, две копии прямой $\mathcal{M}$ и коника $\mathcal{C}$;*

$2 \cdot \mathcal{C} + \mathcal{M} + 1$: *Две копии коники $\mathcal{C}$, $\mathcal{M}$ и прямая;*

$\mathcal{M} + 1 + 2 + 2^{(1)}$: *Прямая $\mathcal{M}$, еще одна прямая и две $\mathbb{F}_q$-сопряженные коники с $\mu_{\boldsymbol{P}} = 1$, такие что $\mathcal{M}$ является касательной к каждой из них в единственной точке из $\boldsymbol{Q}$;*

$2' + 2 + 2^{(1)}$: *Коника и две $\mathbb{F}_q$-сопряженные коники, как в предыдущем случае;*

$3 \cdot \mathcal{C}$: *Три копии коники $\mathcal{C}$;*

$2 \cdot \mathcal{C} + 2 \cdot \mathcal{M}$: *Две копии коники $\mathcal{C}$ и прямой $\mathcal{M}$;*

$\mathcal{L} + 3 \cdot \mathcal{M}$: *Прямые $\mathcal{L}_{i,j}$ и три копии прямой $\mathcal{M}$;*

$\mathcal{N}$: *Прямые $\mathcal{N}_{j,k}$;*

Вырожденные случаи: *Остальные разложения, не содержащие $\mathbb{F}_q$-кривых, отличных от $\mathcal{M}$ и $\mathcal{C}$.*

В частности, во всех случаях имеется не более чем одна абсолютно неприводимая $\mathbb{F}_q$-кривая (геометрического рода $g \leqslant 1$), отличная от $\mathcal{M}$ и $\mathcal{C}$. Более того, для этой кривой $g = 1$ лишь в случаях 6, $5+\mathcal{M}$, $4+\mathcal{C}$ и $3+\mathcal{C}+\mathcal{M}$, в которых отсутствуют особые точки вне $\boldsymbol{P}$ и $\boldsymbol{Q}$.

Согласно леммам 7, 8 и свойствам раздутий [26, § V.3] получаем

Следствие 1. *Полная классификация гиперплоских $\mathbb{F}_q$-сечений на $\mathcal{D}_6 \subset \mathbb{P}^6$ представлена в табл. 2.*

Таблица 2

Классификация гиперплоских $\mathbb{F}_q$-сечений на $\mathcal{D}_6 \subset \mathbb{P}^6$

$S \in \mathbb{L}$	$H = \varphi_{ud}^*(S) - 2E'_{\boldsymbol{P}} - 3E'_{\boldsymbol{Q}}$	$\lvert H(\mathbb{F}_q)\rvert$	$\mu_{P_{\mathcal{M}}}(H)$	$\mu_{P_{\mathcal{C}}}(H)$
6	Эллиптическая или рациональная кривая с одной особой точкой (кратности 2)	[9, теорема 3.3.12] или $\leqslant q+2$ соответственно	0	0
$5+\mathcal{M}$			1	0
$4+\mathcal{C}$			0	1
$3+\mathcal{C}+\mathcal{M}$			1	1
$2+2\cdot\mathcal{C}$	Рациональная кривая, гладкая вне $P_{\mathcal{M}}, P_{\mathcal{C}}$	$\leqslant q+2$	0	2
$2+2\cdot\mathcal{M}+\mathcal{C}$			2	1
$2\cdot\mathcal{C}+\mathcal{M}+1$			1	2
$\mathcal{M}+1+2+2^{(1)}$	Три рациональные кривые, гладкие вне $P_{\mathcal{M}}, P_{\mathcal{C}}$; две из них $\mathbb{F}_q$-сопряжены		3	2
$2'+2+2^{(1)}$		$\leqslant q+4$	2	2
$3\cdot\mathcal{C}$	$E'_{\boldsymbol{P}}$	1	0	3
$2\cdot\mathcal{C}+2\cdot\mathcal{M}$	$E'_{\boldsymbol{Q}}$	2	2	2
$\mathcal{L}+3\cdot\mathcal{M}$	$\mathcal{L}'$	1	3	0
$\mathcal{N}$	H_0	0	0	0
Вырожденные случаи	Одна или две $\mathbb{F}_q$-орбиты сопряженных гладких рациональных кривых	$\leqslant 4$		

Следствие 2. *При $q \geqslant 5$ каждая эллиптическая $\mathbb{F}_q$-кривая изоморфна над $\mathbb{F}_q$ некоторому гиперплоскому сечению на $\mathcal{D}_6 \subset \mathbb{P}^6$.*

Доказательство. С одной стороны, классификация элементов из $|H_0|$ (следствие 1) не зависит от выбора множеств $\boldsymbol{P}, \boldsymbol{Q}$. С другой стороны, при $q \geqslant 5$ любая эллиптическая $\mathbb{F}_q$-кривая E содержит такие множества. Действительно, пусть S – множество точек из $E(\mathbb{F}_{q^3})$, коллинеарных с их $\mathbb{F}_q$-сопряженными. По теореме Безу мощность данного множества ограничена числом $3(q^2+q)$, потому что уравнение коллинеарности для трех сопряженных точек, очевидно, имеет степень q^2+q. Применяя границу Хассе [9, п. 3.3.3], мы видим, что

$$|E(\mathbb{F}_{q^3}) \setminus S| \geqslant q^3 - 3q^2 - \lfloor 2q\sqrt{q}\rfloor - 3q + 1 > 0,$$
$$|E(\mathbb{F}_{q^2}) \setminus E(\mathbb{F}_q)| \geqslant q^2 - 3q - \lfloor 2\sqrt{q}\rfloor > 0$$

для $q \geqslant 5$. ▲

§ 3. Торические коды

3.1. Определение и основные свойства. Данный пункт основывается на результатах пп. 2.1, 2.3. Рассмотрим тройку $(V, T, D) \in \mathbf{Tor}$ и соответствующие ей объекты $(V_\Sigma, \Phi, D) \in \mathbf{Split}$, $(P_D, \tilde{\Phi}) \in \mathbf{Poly}$. Пусть $\varphi\colon V_\Sigma \xrightarrow{\sim} V$ – $\mathbb{F}_{q^e}$-изоморфизм (торических многообразий) и $T(\mathbb{F}_q) = \{P_0, \dots, P_{n-1}\}$.

Отображение вычисления

$$\mathrm{Ev}\colon \mathrm{H}^0(V, D) \to \mathbb{F}_q^n, \quad \mathrm{Ev}(f) = (f(P_0), \dots, f(P_{n-1})),$$

корректно определено, потому что $T \cap \mathrm{Supp}(D) = \varnothing$. Мы будем предполагать, что оно инъективно, т.е. не существует $\mathbb{F}_q$-кривой из линейной системы $|D|$, полностью содержащей $T(\mathbb{F}_q)$. По определению *торический код* – это образ

$$\mathcal{C}_q(V, T, D) = \mathrm{Im}(\mathrm{Ev}).$$

Он называется *расщепимым*, если тор T расщепим.

Мы хотели бы переписать данное определение более конструктивно. Напомним, что обычное отображение Фробениуса V соответствует (посредством φ) действию Φ на V_Σ. В то же время [2, предложение 4.3.3]

$$\mathrm{H}^0(\overline{V}, D) \xrightarrow{\varphi^*}{\sim} \mathrm{H}^0(\overline{V_\Sigma}, D), \quad \mathrm{H}^0(V_\Sigma, D) = \mathbb{F}_q[\{x^m \mid m \in P_D \cap M\}].$$

Следовательно, φ^* является изоморфизмом $\mathbb{F}_q$-пространств $\mathrm{H}^0(V, D)$ и

$$\mathcal{L}(P_D, \Phi) := \mathrm{H}^0(\overline{V_\Sigma}, D)^{\Phi^*} = \left\{ \sum c_m x^m \;\middle|\; c_m \in \mathbb{F}_{q^e},\ c_m^q = c_{\Phi(m)} \right\}.$$

Таким образом, по лемме 1 код $\mathcal{C}_q(V, T, D)$ также равен образу отображения вычисления $\mathcal{L}(P_D, \Phi) \to \mathbb{F}_q^n$ в точках из $\mathrm{E}_q(\Phi)$, которые мы продолжаем обозначать через $P_0, \ldots, P_{n-1}$.

Код $\mathcal{C}_q(V, T, D)$ невырожден и не имеет повторений. Действительно, D является очень обильным дивизором, поэтому для произвольного базиса $f_1, \ldots, f_k$ пространства $\mathrm{H}^0(V, D)$ отображение

$$\varphi_D \colon V \hookrightarrow \mathbb{P}^{k-1}, \quad \varphi_D(P) = (f_1(P) : \ldots : f_k(P)),$$

является вложением. Следовательно, $\mathcal{C}_q(V, T, D)$ может быть определен как алгеброгеометрический код (Гоппы), соответствующий (в смысле [9, теорема 1.1.6]) проективной системе $\varphi_D(T(\mathbb{F}_q))$ без кратных точек. Линейно эквивалентные дивизоры определяют эквивалентные коды Гоппы, поэтому можно предполагать, что D является эффективным дивизором из $\mathrm{TPic}(V, \Phi)$.

Замечание 1. По определению длина n и размерность k кода $\mathcal{C}_q(V, T, D)$ равны $|T(\mathbb{F}_q)|$ и $|P_D \cap M|$ соответственно.

Теорема 23. *Пусть* $C = \mathcal{C}_q(V, T, D)$ *и* $C' = \mathcal{C}_{q^e}(V, \mathbb{G}_m^d, D)$. *Тогда*

$$C = \left(C'_{\mathrm{E}_q(\Phi)}\right)\big|_{\mathbb{F}_q} = \left(C'|_{\mathbb{F}_q}\right)_{\mathrm{E}_q(\Phi)}.$$

Другими словами, любой торический код C *является последовательным выкалыванием* [9, п. 1.1.6] *расщепимого торического кода* C' *в множестве координат* $\mathrm{E}_q(\Phi)$ *и ограничением* [9, п. 1.2.3] *на* $\mathbb{F}_q$ (*или в другом порядке*).

Доказательство. Второе равенство выполнено, потому что кодовые операции выкалывания и ограничения на подполе всегда коммутируют. Первое следует из легко проверяемых тождеств

$$C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^e} = C'_{\mathrm{E}_q(\Phi)}, \quad \left(C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^e}\right)\big|_{\mathbb{F}_q} = C. \quad \blacktriangle$$

Замечание 2. Теорема 23 позволяет нам думать о нерасщепимых торических кодах как о многомерном аналоге кодов БЧХ [9, п. 1.2.2]. Однако идея рассматривать подкоды торических кодов над подполем уже возникала в [27].

Пусть $O(m_0), \ldots, O(m_{l-1})$ – все орбиты действия Φ на $P_D \cap M$, $k_i = |O(m_i)|$, а $\{b_{i,j}\}_{j=0}^{k_i-1}$ – базис $\mathbb{F}_q$-пространства $\mathbb{F}_{q^{k_i}}$. Кроме того, через $\mathrm{Tr}_{k_i,q}$ обозначим отображение следа относительно расширения $\mathbb{F}_{q^{k_i}}/\mathbb{F}_q$.

Легко видеть, что имеет место

Лемма 9. *Множество*

$$\left\{ \sum_{s=0}^{k_i-1} b_{i,j}^{q^s} x^{\Phi^s(m_i)} \right\}_{i=0,\, j=0}^{l-1,\, k_i-1}$$

является базисом $\mathbb{F}_q$*-пространства* $\mathcal{L}(P_D, \Phi)$.

Из лемм 2 и 9 немедленно вытекает

Теорема 24. *Порождающая матрица кода $\mathcal{C}_q(V,T,D)$ имеет вид*

$$\begin{pmatrix} \operatorname{Tr}_{k_0,q}(b_{0,0}P_0^{m_0}) & \operatorname{Tr}_{k_0,q}(b_{0,0}P_1^{m_0}) & \dots & \operatorname{Tr}_{k_0,q}(b_{0,0}P_{n-1}^{m_0}) \\ \operatorname{Tr}_{k_0,q}(b_{0,1}P_0^{m_0}) & \operatorname{Tr}_{k_0,q}(b_{0,1}P_1^{m_0}) & \dots & \operatorname{Tr}_{k_0,q}(b_{0,1}P_{n-1}^{m_0}) \\ \dots & \dots & \dots & \dots \\ \operatorname{Tr}_{k_{l-1},q}(b_{l-1,k_{l-1}}P_0^{m_{l-1}}) & \operatorname{Tr}_{k_{l-1},q}(b_{l-1,k_{l-1}}P_1^{m_{l-1}}) & \dots & \operatorname{Tr}_{k_{l-1},q}(b_{l-1,k_{l-1}}P_{n-1}^{m_{l-1}}) \end{pmatrix}.$$

До конца п. 3.1 будем предполагать, что $T(\mathbb{F}_q) = \langle P\rangle \hookrightarrow \mathbb{F}_{q^e}^*$ является циклической группой, $P_s = P^s$ для $0 \leqslant s \leqslant n-1$, а $b_{i,j} = b_i^{q^j}$ – нормальные базисы расширений $\mathbb{F}_{q^{k_i}}/\mathbb{F}_q$ для $0 \leqslant i \leqslant l-1$. Доказательство следующей леммы легко может быть получено из доказательства предложения 4.1.22 в [9].

Лемма 10. *Код $\mathcal{C}_q(V,T,D)$ является циклическим кодом без кратных корней (т.е. $p \nmid n$).*

Теорема 25. *Проверочный многочлен циклического кода $\mathcal{C}_q(V,T,D)$ равен*

$$h(x) = \prod_{i=0}^{l-1} h_{P^{-m_i}}(x), \quad \text{где} \quad h_{P^{-m_i}}(x) = \prod_{j=0}^{k_i-1} \left(x - P^{-\Phi^j(m_i)}\right)$$

– минимальный (над $\mathbb{F}_q$) многочлен элемента P^{-m_i}.

Доказательство. По определению проверочный многочлен равен фактору x^n-1 по порождающему многочлену g. В то же время g равен наибольшему общему делителю базисных многочленов

$$B_{i,j}(x) = \sum_{s=0}^{n-1} \operatorname{Tr}_{k_i,q}(b_i^{q^j} P^{sm_i}) x^s.$$

Пусть $n_{i,t} = \operatorname{ord}\left(P^{m_i(q^t-1)}\right)$ и

$$S_t = \sum_{s=0}^{n-1} \left(P^{m_i(q^t-1)}\right)^s = \frac{n}{n_{i,t}} \sum_{s=0}^{n_{i,t}-1} \left(P^{m_i(q^t-1)}\right)^s = \begin{cases} n = \pm 1, & \text{если } n_{i,t} = 1, \\ 0 & \text{в противном случае.} \end{cases}$$

В частности, $S_0 = n = \pm 1$. Таким образом,

$$B_{i,j}(P^{-m_i}) = \sum_{t=0}^{k_i-1} b_i^{q^{j+t}} S_t \neq 0$$

и $h(P^{-m_i}) = 0$. Наконец, $\deg(h_{P^{-m_i}}) = k_i$, поэтому $\deg(h) = k$, т.е. мы нашли все корни многочлена h. ▲

Напомним, что циклический код называется *реверсивным*, если его порождающий (или, эквивалентно, проверочный) многочлен самодвойственен.

Следствие 3. *Если многогранник P_D центрально-симметричен (т.е. $-P_D = P_D$), то код $\mathcal{C}_q(V,T,D)$ реверсивен.*

Среди центрально-симметричных многогранников выделим так называемые *многогранники дель Пеццо*, которые обсуждаются в [19]. В то же время теорию циклических реверсивных кодов (или, эквивалентно, LCD-кодов) можно найти в [10, 28, 29].

3.2. Торические коды на $\mathbb{P}^1$ и торических поверхностях. Мы сохраняем обозначения из п. 2.4.

Таблица 3

Торические коды на $\mathbb{P}^1$

	n	k	d	ограничения	ссылка
$\mathrm{RS}_q(r)$	$q-1$	$r+1$	$n-r$	$0<r<q-1$	[9, п. 1.2.1]
$\mathrm{PRS}_q(r)$	$q+1$			$0<r<q+1,\ 2 \mid r$	[9, п. 4.4.1]

Таблица 4

Торические коды на $\mathbb{P}^2$

	n	k	d	ограничения	ссылка
$\mathcal{C}_q(\mathbb{P}^2, \mathbb{G}_m^2, rL_z)$	$(q-1)^2$	$\dfrac{(r+1)(r+2)}{2}$	$n-r(q-1)$	$0<r<q-1$	[4, теорема 1.3]
$\mathcal{C}_q(\mathbb{P}^2, T_{2.c}, rL_z)$	q^2-1		$n-rq$	$0<r<q$	[30, §§ 2, 3]
$\mathcal{C}_q(\mathbb{P}^2, T_3, \frac{r}{3}D_{x,y,z})$	q^2+q+1		$n-(rq+1)$	$0<r<q+1,$ $3 \mid r$	[11, § 2]

Теорема 26. *Коды*

$$\mathrm{RS}_q(r) = \mathcal{C}_q(\mathbb{P}^1, \mathbb{G}_m, rP_y), \quad \mathrm{PRS}_q(r) = \mathcal{C}_q(\mathbb{P}^1, T_2, \frac{r}{2}D_{x,y})$$

являются единственными возможными (с точностью до эквивалентности) среди торических кодов на $\mathbb{P}^1$, *и их параметры представлены в табл.* 3.

Код $\mathrm{RS}_q(r)$ известен как (*выколотый*) *код Рида – Соломона*, а $\mathrm{PRS}_q(r)$ эквивалентен так называемому *проективному* (*дважды расширенному*) *коду Рида – Соломона*, потому что для четного r дивизоры rP_y и $\frac{r}{2}D_{x,y}$ эквивалентны. Более того, согласно теореме 23 это код БЧХ (не примитивный и не в узком смысле). Наконец, легко видеть, что многогранник дивизора $\frac{r}{2}D_{x,y}$ является отрезком $\left[-\frac{r}{2}, \frac{r}{2}\right]$, поэтому по следствию 3 код $\mathrm{PRS}_q(r)$ реверсивен.

Теорема 27. *Все возможные (с точностью до эквивалентности) торические коды на* $\mathbb{P}^2$ *представлены в табл.* 4.

Второй код табл. 4 известен как (*выколотый*) *код Рида – Маллера*, а третий эквивалентен так называемому *проективному коду Рида – Маллера*, потому что для $3 \mid r$ дивизоры rL_z и $\frac{r}{3}D_{x,y,z}$ эквивалентны.

Теорема 28. *Коды*

$$C_1 = \mathcal{C}_q(\mathcal{H}, \mathbb{G}_m^2, r_1L_y + r_2L_v), \quad C_{2.a} = \mathcal{C}_q(\mathcal{H}, T_{2.a}, \frac{r_1}{2}D_{x,y} + \frac{r_2}{2}D_{u,v}),$$
$$C_{2.b} = \mathcal{C}_q(\mathcal{H}, T_{2.b}, r_1L_y + \frac{r_2}{2}D_{u,v}), \quad C_{2.c} = \mathcal{C}_q(\mathcal{E}, T_{2.c}, rD_{y,v}),$$
$$C_4 = \mathcal{C}_q(\mathcal{E}, T_4, \frac{r}{2}D_{x,y,u,v})$$

являются единственными возможными (с точностью до эквивалентности) среди торических кодов на квадратичных поверхностях, и их параметры представлены в табл. 5.

Легко доказывается, что

$$C_1 = \mathrm{RS}_q(r_1) \otimes \mathrm{RS}_q(r_2), \quad C_{2.a} = \mathrm{PRS}_q(r_1) \otimes \mathrm{PRS}_q(r_2),$$
$$C_{2.b} = \mathrm{RS}_q(r_1) \otimes \mathrm{PRS}_q(r_2),$$

Таблица 5

Торические коды на квадратичных поверхностях

	n	k	d	ограничения		ссылка
C_1	$(q-1)^2$	$(r_1+1)(r_2+1)$	$(q-1-r_1)\times$ $\times(q-1-r_2)$	$0<r_1,r_2<q-1$		[4, теорема 1.4]
$C_{2.a}$	$(q+1)^2$		$(q+1-r_1)\times$ $\times(q+1-r_2)$	$0<r_1,r_2<q+1$, $2\mid r_1$	$2\mid r_2$	[31, замечание 3.2]
$C_{2.b}$	q^2-1		$(q-1-r_1)\times$ $\times(q+1-r_2)$	$0<r_1<q-1$, $0<r_2<q+1$		
$C_{2.c}$		$(r+1)^2$	$n-r(q+1)$	$0<r<q-1$		[31, предложение 4.2]
C_4	q^2+1			$0<r<q$, $2\mid r$		[31, предложение 4.7]

где символ $\otimes$ обозначает тензорное (кронекерово) произведение кодов. В то же время $C_{2.c}$ является примитивным кодом БЧХ в узком смысле согласно [31, предложение 4.2]. Наконец, код C_4 реверсивен по следствию 3, поскольку многоугольник дивизора $\frac{r}{2}D_{x,y,u,v}$ является, как легко видеть, замкнутым квадратом $\left[-\frac{r}{2},\frac{r}{2}\right]\times\left[-\frac{r}{2},\frac{r}{2}\right]$.

Лемма 11 [4, теорема 1.5]. *Все возможные (с точностью до эквивалентности) расщепимые торические коды на поверхностях Хирцебруха $\mathbb{F}_m$ при $m>0$ имеют вид*

$$\mathcal{C}_q(\mathbb{F}_m,\mathbb{G}_m^2,r_1S+r_2F_v),\quad \text{где}\quad 0<r_1,r_2,mr_1+r_2<q-1,$$

и их параметры равны

$$n=(q-1)^2,\quad k=\frac{(r_1+1)(mr_1+2r_2+2)}{2},\quad d=n-(q-1)(mr_1+r_2).$$

Замечание 3. Автор изучил нерасщепимые торические коды на поверхностях Хирцебруха и пришел к выводу, что они не представляют большого интереса.

3.3. Торические коды на поверхностях дель Пеццо степени 6. Мы сохраняем обозначения из пп. 2.5, 3.1. Среди всех поверхностей дель Пеццо степени 6 поверхность $\mathcal{D}_6$ кажется наиболее подходящей для рассмотрения на ней торических кодов, потому что ее поле расщепления является наибольшим. Другими словами, данная поверхность "самая нерасщепимая". Для сравнения см. неторические и расщепимые торические коды на поверхности $\mathcal{D}_1$ в [32; 33, пример 5.2] соответственно.

Пусть $\beta\in\mathbb{F}_{q^6}^*$ – элемент порядка $n=q^2-q+1$, и пусть $P_\beta=(\beta,\beta^q)$. Ясно, что

$$\mathrm{E}_q(\Phi_6)=\langle P_\beta\rangle\simeq\langle\beta\rangle$$

и $P_\beta^{(i,j)}=\beta^{i+jq}$ для $(i,j)\in M$. Напомним также, что через h_{β^i} обозначается минимальный (над $\mathbb{F}_q$) многочлен элемента β^i, где $0\leqslant i\leqslant n-1$.

В следующей теореме используется величина $N_q(1)$, т.е. максимально возможное число $\mathbb{F}_q$-точек на эллиптической кривой. Известно [9, теорема 3.4.49], что

$$N_q(1)=\begin{cases}q+\lfloor 2\sqrt{q}\rfloor, & \text{если } \sqrt{q}\notin\mathbb{N},\ p<q \text{ и } p\mid\lfloor 2\sqrt{q}\rfloor,\\ q+\lfloor 2\sqrt{q}\rfloor+1 & \text{в противном случае.}\end{cases}$$

Эллиптические кривые, для которых число $\mathbb{F}_q$-точек достигает $N_q(1)$, называются $\mathbb{F}_q$-*оптимальными* ($\mathbb{F}_q$-*максимальными*, если $\sqrt{q}\in\mathbb{N}$). Такие кривые интересны

сами по себе, потому что алгеброгеометрические коды на них являются так называемыми *почти МДР-кодами* с достаточно большой длиной [9, п. 4.4.2].

Теорема 29. *Рассмотрим* $r \in \mathbb{N}$, *такое что* $rN_q(1) < n$ *и для любого разбиения* $r = \sum_{i=1}^{m} r_i > m$ (*где* $r_i \in \mathbb{N}$) *выполнено неравенство*

$$m(q+1) + \lfloor 2\sqrt{q} \rfloor \sum_{i=1}^{m} g_i \leqslant rN_q(1), \quad \text{где} \quad g_i = 3r_i(r_i-1)+1.$$

Тогда торический код $\mathcal{C}_{q,r} = \mathcal{C}_q(\mathcal{D}_6, T_6, rH_0)$ *имеет параметры*

$$n = q^2 - q + 1, \quad k = 3r(r+1)+1, \quad d \geqslant n - rN_q(1).$$

Более того, если в определении кода $C_{q,r}$ *точка* P_β *взята в качестве образующей группы* $\mathrm{E}_q(\Phi_6)$, *то* $C_{q,r}$ *является циклическим реверсивным кодом с проверочным многочленом*

$$h(x) = (x-1) \prod_{\substack{1 \leqslant i;\ 0 \leqslant j \\ i+j \leqslant r}} h_{\beta^{i+jq}}(x).$$

Доказательство. Длина n очевидна. Вначале оценим минимальное расстояние d. Пусть $D = \sum_{i=1}^{m} C_i$ – разложение на неприводимые (над $\mathbb{F}_q$) компоненты для произвольного элемента линейной системы $|rH_0|$. Группа Пикара поверхности $\mathcal{D}_6$ порождается дивизором H_0, поэтому $C_i \sim r_i H_0$, $r_i \in \mathbb{N}$ и $\sum_{i=1}^{m} r_i = r$. В частности, арифметический род g_i кривой C_i равен $3r_i(r_i-1)+1$ (см., например, [26, пример V.1.3]). Поэтому согласно [34, предложение 2.3] получаем

$$|C_i(\mathbb{F}_q)| \leqslant q + g(C_i)\lfloor 2\sqrt{q} \rfloor + 1 + g_i - g(C_i) \leqslant q + g_i \lfloor 2\sqrt{q} \rfloor + 1.$$

Более того, если $r = m$ (т.е. $r_i = g_i = 1$ для $1 \leqslant i \leqslant m$), то $|C_i(\mathbb{F}_q)| \leqslant N_q(1)$ по следствию 1. Таким образом,

$$|D(\mathbb{F}_q)| \leqslant \sum_{i=1}^{m} |C_i(\mathbb{F}_q)| \leqslant rN_q(1),$$

и мы получаем желаемую границу на d, поскольку $T(\mathbb{F}_q) = \mathcal{D}_6(\mathbb{F}_q)$. В свою очередь, размерность k следует из леммы 5 и неравенства $rN_q(1) < n$.

Цикличность кода $\mathcal{C}_{q,r}$ имеет место в соответствии с леммой 10. Многогранник $P_{rH_0} = rP_{H_0}$ (см. рис. 6 при $r = 1$) центрально-симметричен, следовательно, реверсивность кода $\mathcal{C}_{q,r}$ вытекает из следствия 3. Наконец, требуемый проверочный многочлен получается с помощью леммы 5 и теоремы 25. ▲

Из теоремы 29 и следствия 2 немедленно получаем

Следствие 4. *При* $q \geqslant 5$ *код* $\mathcal{C}_{q,1}$ *является* $[n, 7, n - N_q(1)]_q$*-кодом.*

Замечание 4. При малых q коды $\mathcal{C}_{q,1}$ имеют параметры

$$[21, 7, 11]_5, \quad [43, 7, 30]_7, \quad [57, 7, 43]_8, \quad [73, 7, 57]_9.$$

Коды $\mathcal{C}_{7,1}$, $\mathcal{C}_{8,1}$, $\mathcal{C}_{9,1}$ уже были найдены (с помощью не исчерпывающего компьютерного поиска) в [35–37] соответственно. Согласно таблицам Брауэра – Грассла [13] на данный момент они известны как наилучшие для заданных q, n и k. Таким образом, можно предположить, что коды $\mathcal{C}_{q,r}$ (по крайней мере, при $r = 1$) также достаточно хороши и для больших q.

Замечание 5. В соответствии со следствиями 1, 2 и теоремой Дойринга – Ватерхауза [9, теорема 3.3.12] мы знаем все веса кода $\mathcal{C}_{q,1}$ при $q \geqslant 5$. В частности, его кодовые слова минимального веса (с точностью до умножения на элемент из $\mathbb{F}_q^*$) биективно соответствуют $\mathbb{F}_q$-оптимальным эллиптическим кривым из $|H_0|$. Однако в этой линейной системе имеется много различных (как множества) эллиптических кривых, которые $\mathbb{F}_q$-изогенны, т.е. имеют равное количество $\mathbb{F}_q$-точек. Тем не менее, благодаря реверсивности любого кода $\mathcal{C}_{q,r}$ для полного вычисления его спектра достаточно решить систему линейных уравнений, полученную из тождества Мак-Вильямс [9, теорема 1.1.17].

Автор выражает глубокую благодарность своему научному руководителю М.А. Цфасману, а также В. Батыреву, С. Горчинскому, Г. Кабатянскому, Б. Кунявскому, К. Логинову, А. Перепечко, С. Рыбакову, К. Шрамову, В. Стукопину, Д. Тимашеву, А. Трепалину, С. Влэдуцу, И. Воробьеву и участникам семинара по теории кодирования в ИППИ РАН под руководством Л.А. Бассалыго за помощь и ценные замечания.

СПИСОК ЛИТЕРАТУРЫ

1. *Martínez-Moro E., Munuera C., Ruano D.* Advances in Algebraic Geometry Codes. Singapore: World Sci., 2008.
2. *Cox D.A., Little J.B., Schenck H.K.* Toric Varieties. Providence, R.A.: Amer. Math. Soc., 2011.
3. *Hansen J.P.* Toric Surfaces and Error-Correcting Codes // Coding Theory, Cryptography and Related Areas (Proc. Int. Conf. on Coding Theory, Cryptography and Related Areas, held in Guanajuato, Mexico, in April 1998). Berlin: Springer, 2000. P. 132–142.
4. *Hansen J.P.* Toric Varieties Hirzebruch Surfaces and Error-Correcting Codes // Appl. Algebra Engrg. Comm. Comput. 2002. V. 13. № 4. P. 289–300.
5. *Берман С.Д.* К теории групповых кодов // Кибернетика. 1967. Т. 3. № 1. С. 31–39.
6. *Берман С.Д.* Полупростые циклические и абелевы коды. II // Кибернетика. 1967. Т. 3. № 3. С. 21–30.
7. *Joyner D.* Toric Codes over Finite Fields // Appl. Algebra Engrg. Comm. Comput. 2004. V. 15. № 1. P. 63–79.
8. *Voskresenskii V.E.* Algebraic Groups and Their Birational Invariants. Providence, R.A.: Amer. Math. Soc., 1998.
9. *Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А.* Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2003.
10. *Massey J.L.* Reversible Codes // Inform. and Control. 1964. V. 7. № 3. P. 369–380.
11. *Lachaud G.* The Parameters of Projective Reed–Müller Codes // Discrete Math. 1990. V. 81. № 2. P. 217–221.
12. *Воскресенский В.Е.* Проективные инвариантные модели Демазюра // Изв. АН СССР. Сер. матем. 1982. Т. 46. № 2. С. 195–210.
13. *Grassl M.* Bounds on the Minimum Distance of Linear Codes and Quantum Codes (electronic tables). Available at `http://www.codetables.de` (accessed on October 12, 2018).
14. *Платонов В.П., Рапинчук А.С.* Алгебраические группы и теория чисел. М.: Наука, 1991.
15. *Rubin K., Silverberg A.* Compression in Finite Fields and Torus-Based Cryptography // SIAM J. Comput. 2008. V. 37. № 5. P. 1401–1428.
16. *Воскресенский В.Е.* О двумерных алгебраических торах // Изв. АН СССР. Сер. матем. 1965. Т. 29. № 1. С. 239–244.
17. *Воскресенский В.Е.* О двумерных алгебраических торах. II // Изв. АН СССР. Сер. матем. 1967. Т. 31. № 3. С. 711–716.
18. *Graber T., Harris J., Mazur B., Starr J.* Arithmetic Questions Related to Rationally Connected Varieties // The Legacy of Niels Henrik Abel (The Abel Bicentennial Conf. Oslo, Norway. June 3–8, 2002). Berlin: Springer, 2004. P. 531–542.

19. *Воскресенский В.Е., Клячко А.А.* Торические многообразия Фано и системы корней // Изв. АН СССР. Сер. матем. 1984. Т. 48. № 2. С. 237–263.
20. *Batyrev V.V., Tschinkel Y.* Rational Points of Bounded Height on Compactifications of Anisotropic Tori // Int. Math. Res. Notices. 1995. V. 1995. № 2. P. 591–635.
21. *Ballard M.R., Duncan A., McFaddin P.K.* On Derived Categories of Arithmetic Toric Varieties // `arXiv:1709.03574v3 [math.AG]`, 2018.
22. *Poonen B.* Rational Points on Varieties. Providence, R.A.: Amer. Math. Soc., 2017.
23. *Hirschfeld J.W.P.* Finite Projective Spaces of Three Dimensions. Oxford: Oxford Univ. Press, 1986.
24. *Couvreur A.* Construction of Rational Surfaces Yielding Good Codes // Finite Fields Appl. 2011. V. 17. № 5. P. 424–441.
25. *Kollár J.* Looking for Rational Curves on Cubic Hypersurfaces // Higher-Dimensional Geometry over Finite Fields (Proc. of the NATO Advanced Study Institute. Göttingen, Germany. June 25 – July 6, 2007). Amsterdam: IOS Press, 2008. P. 92–122.
26. *Хартсхорн Р.* Алгебраическая геометрия. М.: Мир, 1981.
27. *Hernando F., O'Sullivan M.E., Popovici E., Srivastava S.* Subfield-Subcodes of Generalized Toric Codes // Proc. 2010 IEEE Int. Sympos. on Information Theory (ISIT'2010). Austin, TX, USA. June 13–18, 2010. P. 1125–1129.
28. *Massey J.L.* Linear Codes with Complementary Duals // Discrete Math. 1992. V. 106–107. P. 337–342.
29. *Yang X., Massey J.L.* The Condition for a Cyclic Code to Have a Complementary Dual // Discrete Math. 1994. V. 126. № 1–3. P. 391–393.
30. *Kasami T., Lin S., Peterson W.* New Generalizations of the Reed–Muller Codes. I: Primitive Codes // IEEE Trans. Inform. Theory. 1968. V. 14. № 2. P. 189–199.
31. *Couvreur A., Duursma I.* Evaluation Codes from Smooth Quadric Surfaces and Twisted Segre Varieties // Des. Codes Cryptogr. 2013. V. 66. № 1–3. P. 291–303.
32. *Богуславский М.И.* Сечения поверхностей Дель Пеццо и обобщенные веса // Пробл. передачи информ. 1998. Т. 34. № 1. С. 18–29.
33. *Ruano D.* On the Parameters of r-Dimensional Toric Codes // Finite Fields Appl. 2007. V. 13. № 4. P. 962–976.
34. *Aubry Y., Perret M.* A Weil Theorem for Singular Curves // Arithmetic, Geometry and Coding Theory (Proc. Int. Conf. held at Luminy, France, June 28 – July 2, 1993). Berlin: de Gruyter, 1996. P. 1–7.
35. *Даскалов Р., Христов П.* Новые квазициклические коды над $GF(7)$ с одним порождающим многочленом // Пробл. передачи информ. 2002. Т. 38. № 1. С. 59–63.
36. *Даскалов Р.Н., Христов П.В.* Новые квазициклические вырожденные линейные коды над $GF(8)$ // Пробл. передачи информ. 2003. Т. 39. № 2. С. 29–35.
37. *Даскалов Р.Н., Методиева Е., Христов П.В.* Новые границы для минимального расстояния линейных кодов над $GF(9)$ // Пробл. передачи информ. 2004. Т. 40. № 1. С. 15–26.

Кошелев Дмитрий Игоревич
Институт проблем передачи информации
им. А.А. Харкевича РАН, лаборатория
алгебры и теории чисел
Московский физико-технический институт
(государственный университет), кафедра
дискретной математики
Университет Версаль-Сен-Кантен-ан-Ивелин,
лаборатория математики Версаля
`dishport@yandex.ru`

Поступила в редакцию
22.11.2018
После доработки
09.01.2019
Принята к публикации
15.01.2019