ISSN 0032-9460, Problems of Information Transmission, 2019, Vol. 55, No. 2, pp. 124–144. © Pleiades Publishing, Inc., 2019.
Russian Text © The Author(s), 2019, published in Problemy Peredachi Informatsii, 2019, Vol. 55, No. 2, pp. 28–49.

CODING THEORY

Non-split Toric Codes

D. I. Koshelev[a,b,c]

[a] *Algebra and Number Theory Laboratory,*
Kharkevich Institute for Information Transmission Problems,
Russian Academy of Sciences, Moscow, Russia
[b] *Department of Discrete Mathematics,*
Moscow Institute of Physics and Technology (State University), Moscow, Russia
[c] *Versailles Laboratory of Mathematics,*
Versailles Saint-Quentin-en-Yvelines University, Versailles, France
e-mail: dishport@yandex.ru

Received November 22, 2018; revised January 9, 2019; accepted January 15, 2019

Abstract—We introduce a new wide class of error-correcting codes, called non-split toric codes. These codes are a natural generalization of toric codes where non-split algebraic tori are taken instead of usual (i.e., split) ones. The main advantage of the new codes is their cyclicity; hence, they can possibly be decoded quite fast. Many classical codes, such as (doubly-extended) Reed–Solomon and (projective) Reed–Muller codes, are contained (up to equivalence) in the new class. Our codes are explicitly described in terms of algebraic and toric geometries over finite fields; therefore, they can easily be constructed in practice. Finally, we obtain new cyclic reversible codes, namely non-split toric codes on the del Pezzo surface of degree 6 and Picard number 1. We also compute their parameters, which prove to attain current lower bounds at least for small finite fields.

Key words: finite fields, toric and cyclic codes, non-split algebraic tori, toric varieties, del Pezzo surfaces, elliptic curves.

DOI: 10.1134/S0032946019020029

1. INTRODUCTION

There is a well-developed theory of so-called *toric codes* [1, ch. 8], i.e., algebraic geometry (Goppa) codes [1, ch. 7] on *toric varieties* [2] (of dimension d over a finite field $\mathbb{F}_q$). These codes were discovered in [3,4] as a generalization of Reed–Solomon codes (for $d = 1$). Toric codes are d-dimensional cyclic (also known as multicyclic or abelian) codes [5,6]. In spite of this, sufficiently fast decoding methods for them are not known; inefficient decoding methods are presented in [7, Section 5].

Besides ordinary (i.e., split) *tori* and toric varieties, there are *non-split* (over $\mathbb{F}_q$) ones [8]. Therefore, it is natural to consider algebraic geometry codes on the latter. We call them *non-split toric codes*. They have some advantages. First, $\mathbb{F}_q$-point groups of non-split tori are often cyclic; hence, the corresponding codes prove to be (simple-root) cyclic [9, Section 1.2.2]. Moreover, some toric cyclic codes are also *reversible* [10]. Second, non-split tori contain more $\mathbb{F}_q$-points than the split torus, i.e., more than $(q-1)^d$. In other words, non-split toric codes are longer than split ones; hence, they may have better error-correction capabilities. Finally, many classical codes, such as doubly-extended Reed–Solomon codes [9, Section 4.4.1] and cyclic Reed–Muller codes (and their projective analogs [11]), are equivalent to some non-split toric codes.

The paper is organized as follows. In Section 2 we recall some results of the theory of non-split algebraic tori and toric varieties over finite fields. In particular, Sections 2.2 and 2.4 are restricted to dimension $d \leq 2$. Finally, Section 2.5 focuses only on *del Pezzo surfaces* of degree 6 [12, Section 3],

where we produce many results for the surface $\mathcal{D}_6$ of Picard $\mathbb{F}_q$-number 1 (the toric del Pezzo surface with the largest splitting field) and its anticanonical linear system. Next, in Section 3.1 we define and study non-split toric codes by methods of algebraic, toric, and combinatorial geometries. In particular, this allows to explicitly write out generator matrices for all toric codes and even generator polynomials for cyclic toric codes. In Section 3.2 full classification of toric codes is presented (up to equivalence) on $\mathbb{P}^1$, $\mathbb{P}^2$, and quadratic surfaces. Finally, in Section 3.3 we obtain new cyclic reversible non-split toric codes on $\mathcal{D}_6$ and compute their parameters. According to code tables [13] it turns out that at least for small q these codes are currently the best known.

2. TORIC GEOMETRY OVER FINITE FIELDS

2.1. Algebraic Tori

Let $\mathbb{F}_q$ be a finite field of order q and characteristic p, $\overline{\mathbb{F}}_q$ its algebraic closure, and $\mathbb{G}_m = \overline{\mathbb{F}}_q \setminus \{0\}$. By definition, an algebraic group T over $\mathbb{F}_q$ is said to be an *algebraic torus* of dimension d if there is an isomorphism of algebraic varieties $\varphi\colon \mathbb{G}_m^d \xrightarrow{\sim} T$ defined over some extension $\mathbb{F}_{q^e}$. We may assume φ to be an isomorphism in the category of algebraic groups [12, Theorem 7]. If such e is minimal, then $\mathbb{F}_{q^e}$ is called the *splitting field* of the torus T. We say that T is *split* if $e = 1$. Note that in the case of a cyclic group $T(\mathbb{F}_q)$ its order divides $q^e - 1$.

Let $x \in \mathbb{G}_m^d$, $m \in \mathbb{Z}^d$, and $\Phi \in \mathrm{GL}(d, \mathbb{Z})$. Throughout the paper we stick to the notation

$$x^m = x_1^{m_1} \cdot \ldots \cdot x_d^{m_d} \qquad \text{and} \qquad \Phi(x) = \big(x^{\Phi_{\square,1}}, \ldots, x^{\Phi_{\square,d}}\big),$$

where $\Phi_{\square,j}$ is the jth column of Φ. Besides, we assume that Φ acts on m from the left, i.e., $\Phi(m) = \Phi m$.

For a given T, consider its *lattices of characters* $M = \mathrm{Hom}_{\overline{\mathbb{F}}_q}(T, \mathbb{G}_m)$ and *cocharacters* $N = M^*$ with Frobenius actions $\Phi, \Phi^t \in \mathrm{GL}(d, \mathbb{Z})$ respectively. Recall that these matrices are conjugate in $\mathrm{GL}(d, \mathbb{Z})$. The order of Φ (i.e., Φ^t) is e; hence, all its eigenvalues are contained in $\mu_e = \{\zeta \in \overline{\mathbb{F}}_q \mid \zeta^e = 1\}$. The *rank*, r, of T is by definition the rank of the invariant sublattice M^Φ (i.e., N^{Φ^t}). A torus T is said to be *isotropic* if $r > 0$, i.e., if it has nontrivial $\mathbb{F}_q$-(co)characters. Otherwise, T is said to be *anisotropic*.

Theorem 1 [14, Section 2.1.7]. *The following properties are equivalent*:

1. *A torus T is split*;
2. $r = d$;
3. *All (co)characters of T are defined over $\mathbb{F}_q$*;
4. *All eigenvalues of Φ are equal to* 1.

Theorem 2 [12, Section 1]. *The map $T \mapsto \Phi$ is a bijection between the set of d-dimensional $\mathbb{F}_q$-tori split over $\mathbb{F}_{q^e}$ and the set of matrices (up to conjugation) from $\mathrm{GL}(d, \mathbb{Z})$ of order e. More precisely, under the inverse map, a matrix Φ corresponds to the geometric quotient $T_\Phi = \mathbb{G}_m^d/\Phi$.*

Theorem 3 [12, Section 2]. *For a fixed d there are only finitely many (up to conjugation) finite subgroups in $\mathrm{GL}(d, \mathbb{Z})$. In particular, there are only finitely many d-dimensional $\mathbb{F}_q$-tori.*

Theorem 4 [14, Section 2.1.7; 8, Section 9.2]. *We have the following*:

1. *A torus T has a unique maximal split (anisotropic) $\mathbb{F}_q$-subtorus T_s (respectively, T_a)*;
2. *Moreover, $T_sT_a = T$ and $|T_s \cap T_a| < \infty$. In other words, the map*

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

is an $\mathbb{F}_q$-isogeny. In particular,

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

3. *The tori T_s and T_a correspond to the lattices M^Φ and M/M^Φ with a naturally induced action of Φ. In particular, $r = \dim(T_s)$, and the splitting fields of T and T_a coincide.*

Lemma 1 [8, Theorem 9.1.1]. *The preimage $\varphi^{-1}(T(\mathbb{F}_q))$ is equal to the "eigenspace"*

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

associated with the eigenvalue q.

More precisely, if α is a primitive element of $\mathbb{F}_{q^e}$, then

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

and

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

Lemma 2. *Let $x \in \mathrm{E}_q(\Phi)$, $m \in M$, and let k be the cardinality of the orbit of m under Φ. Then $x^{\Phi^s(m)} = x^{q^s m}$ for $0 \le s \le k-1$ (in particular, $x^m \in \mathbb{F}_{q^k}$).*

Proof. The proposition follows from the chain of equalities

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

Theorem 5. *We have*

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

where $\chi(\lambda) = \det(\lambda I - \Phi)$ is the characteristic polynomial of Φ. Moreover, if a torus T is non-split, then it has strictly more $\mathbb{F}_q$-points than a split one, i.e.,

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

Proof. The first part is proved in [8, Theorem 9.1.2]. For the second, we repeat a proof suggested by B. Kunyavskii in a private letter. Let $\lambda_1, \dots, \lambda_d$ be all eigenvalues of Φ. By Theorem 1, at least one of them is different from 1. Thus, we obtain a strict inequality

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

Let $n, m \in \mathbb{N}$, $m \mid n$, and let $\mathrm{R}_{n,q}$ be the Weil scalar restriction of $\mathbb{G}_m$ with respect to the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ (see, e.g., [8, Section 3.12]). The universal property of the Weil restriction gives the *norm map* $\mathrm{N}_{n,m,q} \colon \mathrm{R}_{n,q} \to \mathrm{R}_{m,q}$ [15, Section 5], which is a surjective $\mathbb{F}_q$-homomorphism of algebraic tori. In particular,

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

is the usual norm map, i.e., the product of n conjugate (over $\mathbb{F}_q$) points. Besides, according to [15, Lemma 5.1.ii], the restriction of $\mathrm{N}_{n,m,q}$ to the subgroup $\mathrm{R}_{n,q}(\mathbb{F}_q)$ is the norm map for the extension $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$. Finally, consider $\mathbb{F}_q$-tori

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

For $m = 1$ the former is called a *norm one torus*. It is interesting that for n equal to a product of different primes, the groups $\mathrm{T}_{n,q}(\mathbb{F}_q)$ are used in cryptography [15, Section 6].

Theorem 6 [14, Section 2.1.7; 15, Section 5]. *We have the following*:

1. $(\mathrm{R}_{n,q})_a = \mathrm{R}^{(1)}_{n,q}$, *and hence* $\mathrm{T}_{n,q}$ *is an anisotropic torus*;
2. *The splitting fields of* $\mathrm{R}_{n,q}$, $\mathrm{R}^{(1)}_{n,q}$, *and* $\mathrm{T}_{n,q}$ *are equal to* $\mathbb{F}_{q^n}$;
3. $\dim(\mathrm{T}_{n,q}) = \varphi(n)$ *and* $\mathrm{T}_{n,q}(\mathbb{F}_q) \simeq \mathbb{Z}/(\Phi_n(q))$, *where* φ *is the Euler function and* Φ_n *is the* n*-th cyclotomic polynomial.*

2.2. Algebraic Tori of Dimensions 1 *and* 2

Theorem 7 [16]. *There are only the following one-dimensional algebraic* $\mathbb{F}_q$*-tori*:

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

.

Theorem 8 [16]. *There are only the following two-dimensional algebraic* $\mathbb{F}_q$*-tori*:

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	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\mathbb{Z}/(q^2-1)$
$T_3 = \mathrm{R}^{(1)}_{3,q}$	3	0	$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$	$\mathbb{Z}/(q^2+q+1)$
$T_4 = \mathrm{R}_{2,q}(\mathrm{R}^{(1)}_{2,q^2})$	4	0	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\mathbb{Z}/(q^2+1)$
$T_6 = \mathrm{T}_{6,q}$	6	0	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	$\mathbb{Z}/(q^2-q+1)$

.

The paper [16] does not give values of r and $T(\mathbb{F}_q)$ that either are obvious or follow from Theorem 6. Besides, in [16] the torus T_3 (respectively, T_4) is denoted by T_4 (respectively, T_5). We have changed the notation, because the extension degree for T_3 (respectively, T_4) is 3 (respectively, 4). Also, we will denote the matrix Φ for a torus T_i by Φ_i.

Besides the classification, we need the following fact.

Theorem 9 [17]. *All* $\mathbb{F}_q$*-tori of dimensions* 1 *and* 2 *are rational over* $\mathbb{F}_q$.

2.3. Toric Varieties

We keep the notation of Section 2.1. Let T be an $\mathbb{F}_q$-torus and V a smooth projective $\mathbb{F}_q$-variety (of dimension d). We say that V is a *toric variety* (with respect to T) if it contains T as an open subset and the group operation on T can be extended to an action of T on V. It is called *split* if T is split. Besides, let V' be another toric variety with respect to some torus T'. Then a morphism $\varphi\colon V \to V'$ is called a *morphism of toric varieties* if its restriction $\varphi\colon T \to T'$ is a homomorphism.

Theorem 10. *Let V be a projective smooth $\mathbb{F}_q$-variety with a faithful action of an $\mathbb{F}_q$-torus T and an open orbit U. Then T and U are $\mathbb{F}_q$-isomorphic (under the action of T), and hence V is a toric variety (with respect to T).*

Proof. The orbit U is a T-torsor; hence, T and U are isomorphic over $\overline{\mathbb{F}}_q$, and the variety V is geometrically rational. By the theorem in [18, Section 2], it has an $\mathbb{F}_q$-point. On the other hand, [19, Proposition 4] guarantees the existence of an $\mathbb{F}_q$-point on U, and thus T and U are $\mathbb{F}_q$-isomorphic. $\triangle$

Throughout the paper we will use the following notation:

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

and $\operatorname{TDiv}(V)$ is the set of T-invariant $\mathbb{F}_q$-divisors on V. Turning to the standard terminology of the toric geometry (see, e.g., [2]), consider the following sets:

Poly: Pairs (P, Φ), where $P \subset M_{\mathbb{R}}$ is a full-dimensional smooth *convex lattice polytope* and $\Phi \in \operatorname{GL}(M)$ is a finite-order matrix such that $\Phi(P) = P$;

Fan: Triples (Σ, Φ, D), where Σ is a projective smooth *fan* in $N_{\mathbb{R}}$ invariant under a finite-order matrix $\Phi \in \operatorname{GL}(N)$. In other words, for any cone $\sigma \in \Sigma$, we have $\Phi(\sigma) \in \Sigma$. Finally, D is a (very) ample Φ-invariant integral combination of rays from Σ;

Split: Triples (V, Φ, D), where V is a split toric $\mathbb{F}_q$-variety, Φ is an automorphism of V (as a toric variety), and $D \in \operatorname{TDiv}(V)$ is a (very) ample Φ-divisor;

Tor: Triples (V, T, D), where V is a toric $\mathbb{F}_q$-variety with respect to an $\mathbb{F}_q$-torus T, and $D \in \operatorname{TDiv}(V)$ is a (very) ample divisor.

It is well known that these sets correspond to each other under the following maps (the split case is discussed in [2]):

1. The map
$$\textbf{Poly} \to \textbf{Fan}, \quad (P, \Phi) \mapsto (\Sigma_P, \Phi^t, D_P),$$
where Σ_P and D_P are, respectively, the normal fan [2, Theorem 2.3.2] and integral ray combination [2, Section 4.2] corresponding to P;
2. The map
$$\textbf{Fan} \to \textbf{Split}, \quad (\Sigma, \Phi, D) \mapsto (V_\Sigma, \Phi, D),$$
where V_Σ is the split toric variety [2, Section 3.1] corresponding to Σ and Φ is an automorphism of $\mathbb{G}_m^d$ from Section 2.1 extended to V_Σ;
3. The map
$$\textbf{Split} \to \textbf{Tor}, \quad (V_\Sigma, \Phi, D) \mapsto (V_{\Sigma,\Phi}, T_\Phi, D),$$
where
$$V_{\Sigma,\Phi} = V_\Sigma/\Phi, \qquad T_\Phi = \mathbb{G}_m^d/\Phi$$
are geometric quotients of V_Σ and $\mathbb{G}_m^d$ by the automorphism Φ. The toric variety $V_{\Sigma,\Phi}$ is called the *Demazure model* of the torus T_Φ.

Theorem 11 [12, Sections 1 and 2]. *All $\mathbb{F}_q$-forms of V_Σ (without a toric structure) are toric varieties, i.e., they look like $V_{\Sigma,\Phi}$ for $\Phi \in \operatorname{Aut}(\Sigma)$. Besides, for $\Phi' \in \operatorname{Aut}(\Sigma)$ the varieties $V_{\Sigma,\Phi}$ and $V_{\Sigma,\Phi'}$ are $\mathbb{F}_q$-isomorphic (as toric varieties) if and only if the matrices Φ and Φ' are conjugate in $\operatorname{Aut}(\Sigma)$. Finally, V_Σ and $V_{\Sigma,\Phi}$ are isomorphic over $\mathbb{F}_{q^e}$.*

Conversely, consider a matrix $\Phi \in \operatorname{GL}(N)$ and the torus T_Φ. There is a projective smooth fan in $N_{\mathbb{R}}$ invariant under Φ. In other words, there is a toric $\mathbb{F}_q$-variety with respect to T_Φ.

Fig. 1. Actions on primitive vectors of the fan $\Sigma_{\mathbb{P}^1}$.

Let Σ^{Φ^t} be the set of invariant cones of Σ with respect to a matrix $\Phi^t \in \mathrm{Aut}(\Sigma)$. Also, for $\sigma \in \Sigma^{\Phi^t}$ we denote by $\sigma^* \subset M_{\mathbb{R}}$ the cone dual to σ, and by $T_{\Phi,\sigma}$ the torus corresponding to the restriction of Φ to the sublattice $M_\sigma = -\sigma^* \cap \sigma^* \cap M$ (of dimension $d - \dim(\sigma)$).

Theorem 12 [20, Theorem 1.3.2, Corollary 1.3.6]. *There is a natural bijective correspondence*

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

In particular, for an anisotropic torus T_Φ we have the equality $V_{\Sigma,\Phi}(\mathbb{F}_q) = T_\Phi(\mathbb{F}_q)$.

Theorem 13 [12, Section 1]. *The natural embedding* $\mathrm{Pic}(V_\Sigma) \hookrightarrow \mathrm{Pic}(\overline{V_\Sigma})$ *is an isomorphism. In other words, any divisor on* $\overline{V_\Sigma}$ *is equivalent to some* $\mathbb{F}_q$*-divisor. At the same time, there is a natural isomorphism between the* $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$*-module* $\mathrm{Pic}(\overline{V_{\Sigma,\Phi}})$ *and* Φ*-module* $\mathrm{Pic}(V_\Sigma)$*. In particular,*

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

Theorem 14 [8, Theorem 4.3.1; 20, Section 1.3]. *There is an exact sequence of Φ-modules*

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

passing to invariants, we obtain an induced sequence of groups

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

Moreover, the group

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

is finite, and hence the number of Φ^t-orbits on $\Sigma(1)$ is $r(T_\Phi) + \rho(V_{\Sigma,\Phi})$.

When considering toric codes, we will be interested in the image of $\mathrm{TDiv}(V_\Sigma)^\Phi$ in $\mathrm{Pic}(V_\Sigma)^\Phi$, which we denote by $\mathrm{TPic}(V_\Sigma, \Phi)$. In particular,

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

2.4. Projective Line $\mathbb{P}^1$ and Toric Surfaces

It is well known that $\mathbb{P}^1$ is a unique one-dimensional projective smooth toric variety. Let x, y be its homogeneous coordinates. Prime $\mathbb{G}_m$-invariant divisors on $\mathbb{P}^1$ are only the points $P_x = (0:1)$ and $P_y = (1:0)$.

Theorem 15 [2, Example 2.4.10]. *The fan of $\mathbb{P}^1$ and all possible actions on it are represented in Fig.* 1*. More precisely,*

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

Besides, it is clear that

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

where $D_{x,y} = P_x + P_y$.

From now on we will discuss toric surfaces. We will need the notation $\mathbb{V}(f_1, \ldots, f_n)$ for the algebraic variety generated by some family of $\mathbb{F}_q$-polynomials $f_1, \ldots, f_n$, $n \in \mathbb{N}$.

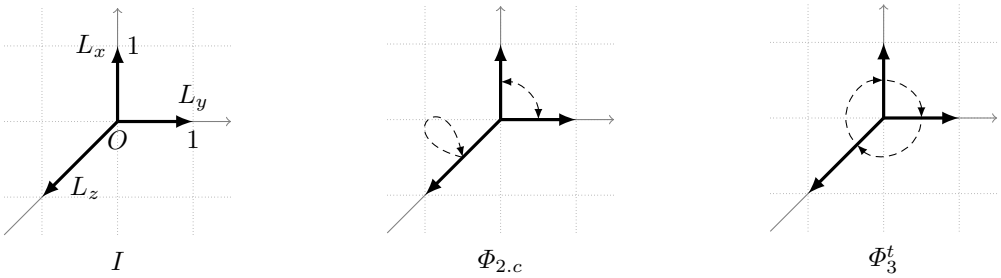

Fig. 2. Actions on primitive vectors of the fan $\Sigma_{\mathbb{P}^2}$.

Theorem 16 [21, Section 4.1]. *A toric $\mathbb{F}_q$-surface can be obtained by a sequence of blowings up at $\mathbb{F}_q$-orbits of torus-invariant points starting from $\mathbb{F}_q$-minimal surfaces that are $\mathbb{F}_q$-forms of*

1. $\mathbb{P}^2$;
2. $\mathbb{P}^1 \times \mathbb{P}^1$;
3. *Hirzebruch surfaces $\mathbb{F}_m$ for $m > 1$;*
4. *The del Pezzo surface of degree 6 and Picard $\mathbb{F}_q$-number 1.*

Projective plane $\mathbb{P}^2$. Recall that forms of $\mathbb{P}^2$ (over any field) are called *Severi–Brauer surfaces*. According to Châtelet [22, Proposition 4.5.10] and Katz [18, Section 2], we have the following.

Lemma 3. *There are no Severi–Brauer surfaces over $\mathbb{F}_q$ different from $\mathbb{P}^2$.*

Let x, y, z be homogeneous coordinates of $\mathbb{P}^2$. It is well known that $\mathbb{P}^2$ is a split toric surface and all its prime torus-invariant divisors are the lines $L_x = \mathbb{V}(x)$, $L_y = \mathbb{V}(y)$, and $L_z = \mathbb{V}(z)$.

Theorem 17 [2, Example 3.1.9]. *The fan of $\mathbb{P}^2$ and all possible actions on it (up to conjugation) are presented in Fig. 2. More precisely,*

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

Finally, it is clear that

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

where $D_{x,y,z} = L_x + L_y + L_z$.

Quadratic surfaces. Consider two different points $P_1, P_2 \in \mathbb{P}^2$ and the line L between them. Successive blowings up at the points P_1 and P_2 and blowing down the proper preimage of L result in an $\mathbb{F}_q$-surface Q. If P_1 and P_2 are $\mathbb{F}_q$-points, then Q is called a *hyperbolic quadratic surface* $\mathcal{H}$. Otherwise, i.e., if P_1 and P_2 are $\mathbb{F}_q$-conjugate, then Q is called an *elliptic quadratic surface* $\mathcal{E}$.

Theorem 18. *First, $\mathcal{E}$ is a unique nontrivial $\mathbb{F}_q$-form of $\mathcal{H}$. Furthermore, there are the following $\mathbb{F}_q$-isomorphisms*:

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

where x, y, z, t are homogeneous coordinates of $\mathbb{P}^3$, the surface $\mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathbb{P}^1)$ is the Weil scalar restriction, and

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

Proof. The classification of $\mathbb{F}_q$-forms follows from [23, Lemma 15.3.1; 12, Section 3]. On the other hand, the existence of isomorphisms is discussed, for example, in [24, Section 2.2.1; 25, Example 3.8]. $\triangle$

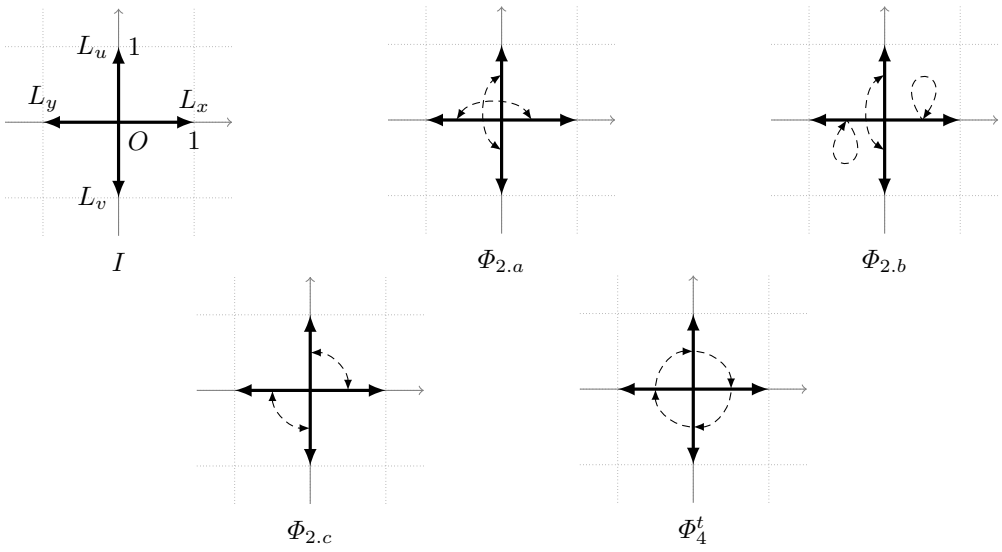

Fig. 3. Actions on primitive vectors of the fan $\Sigma_{\mathcal{H}}$.

Let x, y and u, v be two pairs of homogeneous coordinates on $\mathbb{P}^1 \times \mathbb{P}^1$. The action of $\mathbb{G}_m^2$ on $\mathcal{H}$ is naturally induced from the action of $\mathbb{G}_m$ on $\mathbb{P}^1$, and the corresponding prime $\mathbb{G}_m^2$-invariant divisors are the lines

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

Theorem 19 [2, Example 3.1.12]. *The fan of $\mathcal{H}$ and all possible actions on it (up to conjugation) are presented in Fig.* 3. *More precisely,*

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

Note that in geometric terms $\Phi_{2.c}$ is the involution $(P, Q) \mapsto (Q, P)$.

Lemma 4. *We have $\mathbb{F}_q$-isomorphisms (without a toric structure)*

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

Proof. It suffices to explicitly realize all toric $\mathbb{F}_q$-forms of $\mathcal{H}$. The first part of the lemma is obvious, because $\mathbb{P}^1 \times \mathbb{P}^1$ is a toric surface with respect to the tori $T_{2.a}$ and $T_{2.b}$. On the other hand, by the universal property of the Weil restriction, the action of $\mathbb{G}_m$ (respectively, T_2) on $\mathbb{P}^1$ is transferred to the action of $T_{2.c}$ (respectively, T_4) on $\mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathbb{P}^1)$. Thus, the second part is also true. $\triangle$

Finally, it is easily proved that

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

where

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

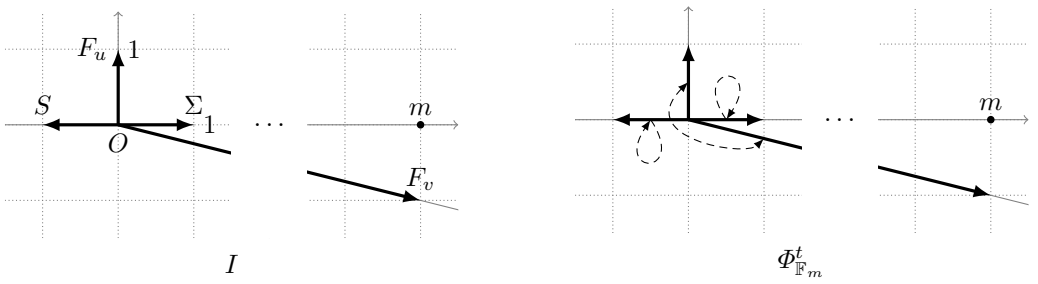

Fig. 4. Actions on primitive vectors of the fan $\Sigma_{\mathbb{F}_m}$ $m > 0$.

Hirzebruch surfaces $\mathbb{F}_m$ for $m > 0$. These surfaces are defined by the equation

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

The projection $f\colon \mathbb{F}_m \to \mathbb{P}^1_{(u:v)}$ is a unique $\mathbb{P}^1$-fibration on $\mathbb{F}_m$. It is easily proved that there are no nontrivial $\mathbb{F}_q$-forms for $\mathbb{F}_m$ and that $\mathbb{F}_m$ is a split toric surface. Its torus-invariant prime divisors have the form

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

The curves F_u and F_v are fibers of f over the points $P_u, P_v \in \mathbb{P}^1$, respectively. On the other hand, the curves Σ and S are images of the sections for f with self-intersections $-m$ and m, respectively.

Consider the matrix

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

and note that it is conjugate to $\Phi_{2.b}$ if $2 \mid m$ and to $\Phi_{2.c}$ if $2 \nmid m$.

Theorem 20 [2, Example 3.1.16]. *The fan of $\mathbb{F}_m$ and all possible actions on it are presented in Fig.* 4. *More precisely,*

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

Finally, it is easy to check that

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

where

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

It is also worth noting that a divisor $r_1 S + r_2 F_v$ is (very) ample if and only if $r_1, r_2 > 0$.

2.5. Del Pezzo Surfaces of Degree 6

In this subsection we will use the above notation for $\mathbb{P}^2$ and basic facts from [12, Section 3]. Consider the points

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

It is well known that simultaneous blowing up $\mathbb{P}^2$ at these points results in an $\mathbb{F}_q$*-surface* $\mathcal{D}_1$ of degree 6 and that such a surface is unique over $\overline{\mathbb{F}}_q$. Furthermore, $\mathcal{D}_1$ is a toric surface, because the points P_x, P_y, and P_z are torus-invariant.

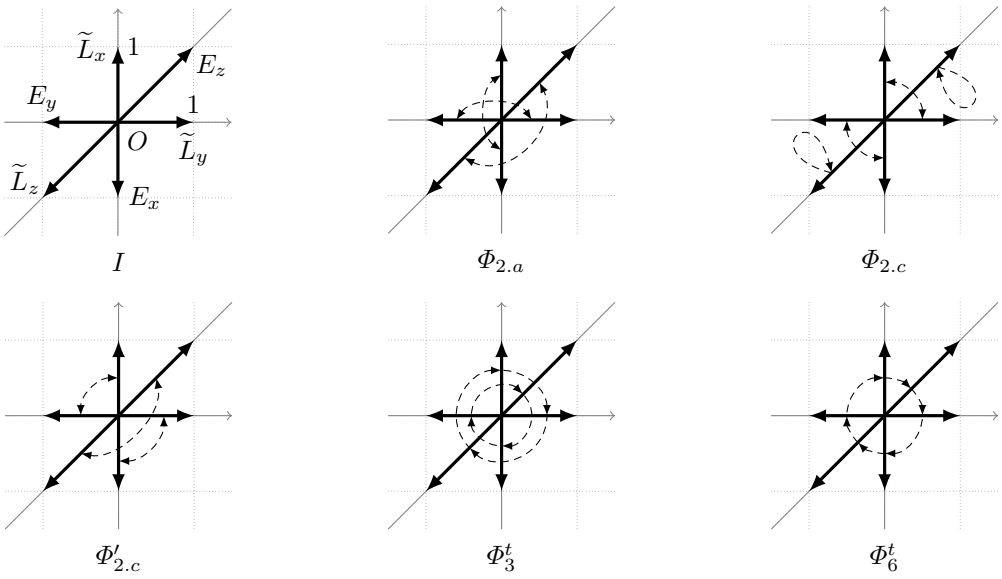

Fig. 5. Actions on primitive vectors of the fan $\Sigma_{\mathcal{D}_1}$.

Let E_x, E_y, and E_z be exceptional curves associated with the points P_x, P_y, and P_z, respectively, and let $\widetilde{L}_x$, $\widetilde{L}_y$, and $\widetilde{L}_z$ be proper preimages of the lines L_x, L_y, and L_z, respectively. These six curves are unique torus-invariant prime divisors on $\mathcal{D}_1$. Furthermore, the divisor

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

is anticanonical and gives an $\mathbb{F}_q$-embedding $\mathcal{D}_1 \hookrightarrow \mathbb{P}^6$.

Theorem 21. *The fan of $\mathcal{D}_1$ and all possible actions on it are presented in Fig.* 5, *where*

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

More precisely,

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

Note that in geometric terms $\Phi_{2.a}$ is the standard quadratic transform

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

lifted to $\mathcal{D}_1$.

We will denote by $\mathcal{D}_i$ (respectively, $\mathcal{D}'_{2.c}$) the toric surface $V_{\Sigma_{\mathcal{D}_1},\Phi_i}$ (respectively, $V_{\Sigma_{\mathcal{D}_1},\Phi'_{2.c}}$). We stress that the surfaces $\mathcal{D}_{2.c}$ and $\mathcal{D}'_{2.c}$ are not isomorphic over $\mathbb{F}_q$, but they both contain the torus $T_{2.c}$. Furthermore, for a toric surface S, let us denote by $\mathrm{Bl}_{a_1,\dots,a_n}(S)$ blowing up S at some $\mathbb{F}_q$-orbits (of cardinalities $a_1, \dots, a_n$, $n \in \mathbb{N}$) of torus-invariant points. In general, this blowing up, of course, depends on a choice of $\mathbb{F}_q$-orbits with given cardinalities. According to Theorems 12 and 14 and Fig. 5, we have the following.

Theorem 22. *All del Pezzo $\mathbb{F}_q$-surfaces of degree* 6 *are presented in Table* 1. *In particular, $\mathcal{D}_6$ is a unique $\mathbb{F}_q$-minimal surface among them.*

From now on we focus on the surface $\mathcal{D}_6$, because toric codes on it seem to have the best parameters compared to those on other del Pezzo surfaces of degree 6. First of all,

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

and the polygon P_{H_0} with the action of Φ_6 is presented in Fig. 6. The following lemma is an elementary exercise.

Table 1. Del Pezzo $\mathbb{F}_q$-surfaces of degree 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

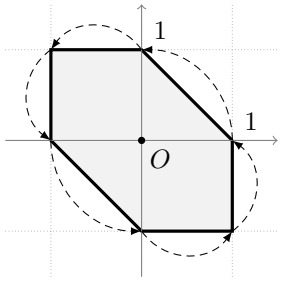

Fig. 6. The polygon P_{H_0} with the action of Φ_6.

Lemma 5. *For $r \in \mathbb{N}$, the set*

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

consists of representatives of all orbits under the action of Φ_6 on $P_{rH_0} \cap M$. Furthermore, nonzero points in this set represent orbits of cardinality 6. In particular,

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

Let $\boldsymbol{P} = \{P_1, P_2, P_3\}$ be a set of noncollinear $\mathbb{F}_q$-conjugate points on $\mathbb{P}^2$ and $\boldsymbol{Q} = \{Q_1, Q_2\}$ a set of different $\mathbb{F}_q$-conjugate points on $\mathbb{P}^2$. In particular, these five points are in general position; hence, we can consider a uniquely defined nondegenerate conic $\mathcal{C}$ passing through them. For $i, j \in \{1,2,3\}$ $(i \ne j)$, $k \in \{1,2\}$, we denote by $\mathcal{L}_{i,j}$, $\mathcal{M}$, and $\mathcal{N}_{j,k}$ the lines passing through P_i and P_j, Q_1 and Q_2, and P_j and Q_k, respectively. Furthermore, let

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

All these geometric objects are presented in Fig. 7.

Since the lines $\mathcal{N}_{j,k}$ are conjugate to each other and any toric $\mathbb{F}_q$-surface is uniquely defined by the Frobenius action on its prime torus-invariant divisors, we have the following.

Lemma 6. *The surface $\mathcal{D}_6$ is obtained by blowing up $\mathbb{P}^2$ at the orbits $\boldsymbol{P}$ and $\boldsymbol{Q}$ followed by blowing down the proper preimages $\widetilde{\mathcal{M}}$ and $\widetilde{\mathcal{C}}$ of the curves $\mathcal{M}$ and $\mathcal{C}$, respectively.*

We will denote by $\mathcal{B}$ the corresponding blowing-up surface (which is a del Pezzo surface of degree 4), and by φ_u (respectively, φ_d), the blowing up (down) map. In other words, we have the diagram

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

Next, let

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

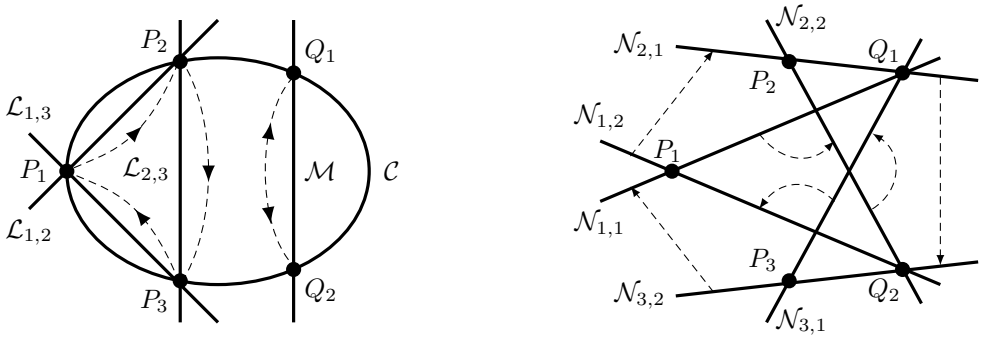

Fig. 7. Points P_j and Q_k, lines $\mathcal{L}_{i,j}$ and $\mathcal{M}, \mathcal{N}_{j,k}$, and the conic $\mathcal{C}$.

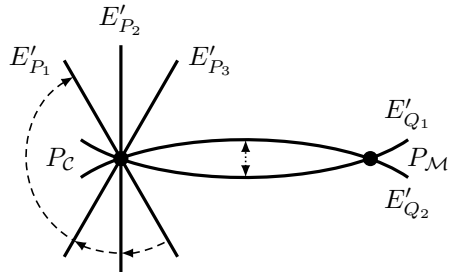

Fig. 8. Points $P_{\mathcal{M}}$ and $P_{\mathcal{C}}$ and curves $E'_{\boldsymbol{P}}$ and $E'_{\boldsymbol{Q}}$.

and let

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

be the proper preimage of $\mathcal{L}$ under φ_{ud}. Finally, let

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

be the exceptional divisors associated with $\boldsymbol{P}$ and $\boldsymbol{Q}$, respectively, and

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

(see Fig. 8 for clarity). Note that there are bijective correspondences

$$\mathcal{D}_6 \setminus (E'_{\boldsymbol{P}} \cup E'_{\boldsymbol{Q}}) \overset{\varphi_{ud}}{\xrightarrow{\sim}} \mathbb{P}^2 \setminus (\mathcal{M} \cup \mathcal{C}),$$

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

The lines $\mathcal{N}_{j,k}$ are not tangents to $\mathcal{C}$; hence, their proper preimages $\widetilde{\mathcal{N}}_{j,k} \subset \mathcal{B}$ do not intersect $\widetilde{\mathcal{C}}$ (or $\widetilde{\mathcal{M}}$, of course). Therefore, $\widetilde{\mathcal{N}}_{j,k} \overset{\varphi_d}{\xrightarrow{\sim}} \varphi_d(\widetilde{\mathcal{N}}_{j,k})$, and we will not make any difference in the notation. It is easily seen that $\widetilde{\mathcal{N}}_{j,k}$ are exceptional curves on $\mathcal{D}_6$, and thus

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

Lemma 7. *The set of hyperplane $\mathbb{F}_q$-sections on $\mathcal{D}_6 \subset \mathbb{P}^6$ has the form*

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

where the incomplete linear system

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

by definition consists of plane (possibly reducible) $\mathbb{F}_q$-sextics passing through $\boldsymbol{P}$ with multiplicity 2 and through $\boldsymbol{Q}$ with multiplicity 3.

Proof. Indeed, it is easily proved that

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

and hence

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

For better understanding of direct and inverse images of divisors on algebraic varieties, see, e.g., [26, Sections II.5, II.6, IV.2]. $\triangle$

According to the formula in [26, Example V.3.9.2] (a version of the Plücker formula) for the genus of an absolutely irreducible curve, one can easily check the following fact.

Lemma 8. *The only decompositions into irreducible components for $\mathbb{F}_q$-curves from $\mathbb{L}$ are the following*:

6: *A sextic with $\mu_{\boldsymbol{P}} = 2$, $\mu_{\boldsymbol{Q}} = 3$;*
$5 + \mathcal{M}$: *A quintic with $\mu_{\boldsymbol{P}} = \mu_{\boldsymbol{Q}} = 2$ and $\mathcal{M}$;*
$4 + \mathcal{C}$: *A quartic with $\mu_{\boldsymbol{P}} = 1$, $\mu_{\boldsymbol{Q}} = 2$, and $\mathcal{C}$;*
$3 + \mathcal{C} + \mathcal{M}$: *A cubic with $\mu_{\boldsymbol{P}} = \mu_{\boldsymbol{Q}} = 1$, $\mathcal{C}$, and $\mathcal{M}$;*
$2 + 2 \cdot \mathcal{C}$: *A conic with $\mu_{\boldsymbol{P}} = 0$, $\mu_{\boldsymbol{Q}} = 1$, and two copies of $\mathcal{C}$;*
$2 + 2 \cdot \mathcal{M} + \mathcal{C}$: *A conic with $\mu_{\boldsymbol{P}} = 1$, $\mu_{\boldsymbol{Q}} = 0$, two copies of $\mathcal{M}$, and $\mathcal{C}$;*
$2 \cdot \mathcal{C} + \mathcal{M} + 1$: *Two copies of $\mathcal{C}$, $\mathcal{M}$, and a line;*
$\mathcal{M} + 1 + 2 + 2^{(1)}$: *The line $\mathcal{M}$, another line, and two $\mathbb{F}_q$-conjugate conics with $\mu_{\boldsymbol{P}} = 1$ such that $\mathcal{M}$ is tangent to each of them at exactly one point from $\boldsymbol{Q}$;*
$2' + 2 + 2^{(1)}$: *A conic and two $\mathbb{F}_q$-conjugate conics as in the previous case;*
$3 \cdot \mathcal{C}$: *Three copies of $\mathcal{C}$;*
$2 \cdot \mathcal{C} + 2 \cdot \mathcal{M}$: *Two copies of $\mathcal{C}$ and two copies of $\mathcal{M}$;*
$\mathcal{L} + 3 \cdot \mathcal{M}$: *The lines $\mathcal{L}_{i,j}$ and three copies of $\mathcal{M}$;*
$\mathcal{N}$: *The lines $\mathcal{N}_{j,k}$;*
Degenerate cases: *Other decompositions not containing $\mathbb{F}_q$-curves different from $\mathcal{M}$ and $\mathcal{C}$.*

In particular, in all cases there is no more than one absolutely irreducible $\mathbb{F}_q$-curve (of geometric genus $g \le 1$) different from $\mathcal{M}$ and $\mathcal{C}$. Moreover, for this curve we have $g = 1$ only in cases 6, $5 + \mathcal{M}$, $4 + \mathcal{C}$, and $3 + \mathcal{C} + \mathcal{M}$ with no singular points outside $\boldsymbol{P}$ and $\boldsymbol{Q}$.

According to Lemmas 7 and 8 and properties of blowing up [26, Section V.3], we obtain the following.

Corollary 1. *A complete classification of hyperplane $\mathbb{F}_q$-sections on $\mathcal{D}_6 \subset \mathbb{P}^6$ is presented in Table 2.*

Corollary 2. *For $q \ge 5$, every elliptic $\mathbb{F}_q$-curve is isomorphic over $\mathbb{F}_q$ to some hyperplane section on $\mathcal{D}_6 \subset \mathbb{P}^6$.*

Proof. On the one hand, the classification of elements from $|H_0|$ (Corollary 1) does not depend on the choice of point sets $\boldsymbol{P}$ and $\boldsymbol{Q}$. On the other hand, for $q \ge 5$ any elliptic $\mathbb{F}_q$-curve E contains such sets. Indeed, let S be the set of points from $E(\mathbb{F}_{q^3})$ that are collinear with their $\mathbb{F}_q$-conjugates. By the Bézout theorem, the cardinality of this set is bounded by $3(q^2 + q)$, because

Table 2. Classification of hyperplane $\mathbb{F}_q$-sections on $\mathcal{D}_6 \subset \mathbb{P}^6$.

$S \in \mathbb{L}$	$H = \varphi_{ud}^*(S) - 2E'_{\boldsymbol{P}} - 3E'_{\boldsymbol{Q}}$	$\lvert H(\mathbb{F}_q)\rvert$	$\mu_{P_{\mathcal{M}}}(H)$	$\mu_{P_{\mathcal{C}}}(H)$
6	An elliptic curve or a rational curve with a unique singular point (of multiplicity 2)	[9, Theorem 3.3.12] or $\le q+2$, respectively	0	0
$5+\mathcal{M}$			1	0
$4+\mathcal{C}$			0	1
$3+\mathcal{C}+\mathcal{M}$			1	1
$2+2\cdot\mathcal{C}$	A rational curve smooth outside $P_{\mathcal{M}}$ and $P_{\mathcal{C}}$	$\le q+2$	0	2
$2+2\cdot\mathcal{M}+\mathcal{C}$			2	1
$2\cdot\mathcal{C}+\mathcal{M}+1$			1	2
$\mathcal{M}+1+2+2^{(1)}$	Three rational curves smooth outside $P_{\mathcal{M}}$ and $P_{\mathcal{C}}$, two of them being $\mathbb{F}_q$-conjugate		3	2
$2'+2+2^{(1)}$		$\le q+4$	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
Degenerate cases	One or two $\mathbb{F}_q$-orbits of conjugate smooth rational curves	≤ 4		

the collinearity equation for three conjugate points is obviously of degree q^2+q. Applying the Hasse bound [9, Section 3.3.3], we see that

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

for $q \ge 5$. $\triangle$

3. TORIC CODES

3.1. Definition and Main Properties

This subsection is based on the result of Sections 2.1 and 2.3. Consider a triple $(V,T,D) \in \mathbf{Tor}$ and the corresponding triples $(V_\Sigma, \Phi, D) \in \mathbf{Split}$, $(P_D, \Phi) \in \mathbf{Poly}$. Let $\varphi\colon V_\Sigma \xrightarrow{\sim} V$ be an $\mathbb{F}_{q^e}$-isomorphism (of toric varieties) and $T(\mathbb{F}_q) = \{P_0, \dots, P_{n-1}\}$.

The evaluation map

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

is well defined, because $T \cap \mathrm{Supp}(D) = \varnothing$. We will assume that the map is injective, i.e., in the linear system $|D|$ there is no $\mathbb{F}_q$-curve that completely contains $T(\mathbb{F}_q)$. By definition, a *toric code* is the image

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

It is said to be *split* if the torus T is split.

We would like to rewrite this definition more constructively. Recall that the usual Frobenius map on V corresponds (by means of φ) to the action of Φ on V_Σ. At the same time [2, Proposition 4.3.3], we have

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

Hence, φ^* is an isomorphism of $\mathbb{F}_q$-spaces $\mathrm{H}^0(V,D)$, and

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

Therefore, by Lemma 1, the code $\mathcal{C}_q(V,T,D)$ is also equal to the image of the evaluation map $\mathcal{L}(P_D,\Phi) \to \mathbb{F}_q^n$ at the points of $\mathrm{E}_q(\Phi)$, which we continue to denote by $P_0,\dots,P_{n-1}$.

The code $\mathcal{C}_q(V,T,D)$ is nondegenerate and has no repetitions. Indeed, D is a very ample divisor; hence, for a basis $f_1,\dots,f_k$ of $\mathrm{H}^0(V,D)$, the map

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

is an embedding. Therefore, $\mathcal{C}_q(V,T,D)$ can be defined as an algebraic geometry (Goppa) code corresponding (in the sense of [9, Theorem 1.1.6]) to the projective system $\varphi_D(T(\mathbb{F}_q))$ without multiple points. Linearly equivalent divisors define equivalent Goppa codes, and hence we may assume D to be an effective divisor from $\mathrm{TPic}(V,\Phi)$.

Remark 1. By the definition, the length n and dimension k of a code $\mathcal{C}_q(V,T,D)$ are equal to $|T(\mathbb{F}_q)|$ and $|P_D \cap M|$, respectively.

Theorem 23. *Let $C = \mathcal{C}_q(V,T,D)$ and $C' = \mathcal{C}_{q^e}(V,\mathbb{G}_m^d,D)$. Then*

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

In other words, any toric code C is a result of successive puncturing [9, Section 1.1.6] *of the split toric code C' at the coordinate set $\mathrm{E}_q(\Phi)$ and the restriction* [9, Section 1.2.3] *to $\mathbb{F}_q$ (or in the reverse order).*

Proof. The right-hand equality is true, because the code operations of puncturing and subfield restriction are always commutative. The left-hand equality follows from the easily proved relations

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

Remark 2. Theorem 23 allows us to think about non-split toric codes as high-dimensional analogs of BCH codes [9, Section 1.2.2]. However, the idea of considering subfield-subcodes of toric codes has already arisen in [27].

Let $O(m_0),\dots,O(m_{l-1})$ be all orbits under the action of Φ on $P_D \cap M$, $k_i = |O(m_i)|$, and let $\{b_{i,j}\}_{j=0}^{k_i-1}$ be a basis of the $\mathbb{F}_q$-space $\mathbb{F}_{q^{k_i}}$. Furthermore, by $\mathrm{Tr}_{k_i,q}$ we denote the trace map with respect to the extension $\mathbb{F}_{q^{k_i}}/\mathbb{F}_q$.

One can easily prove the following result.

Lemma 9. *The set*

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

is a basis of the $\mathbb{F}_q$-space $\mathcal{L}(P_D,\Phi)$.

From Lemmas 2 and 9 we immediately obtain the following.

Theorem 24. *A generator matrix of a code $\mathcal{C}_q(V,T,D)$ has the form*

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

In the rest of Section 3.1 we will assume that $T(\mathbb{F}_q) = \langle P \rangle \hookrightarrow \mathbb{F}_{q^e}^*$ is a cyclic group, $P_s = P^s$ for $0 \le s \le n-1$, and $b_{i,j} = b_i^{q^j}$ is a normal basis of $\mathbb{F}_{q^{k_i}}/\mathbb{F}_q$ for $0 \le i \le l-1$. A proof of the following lemma can easily be obtained from that of Proposition 4.1.22 in [9].

Lemma 10. *$\mathcal{C}_q(V,T,D)$ is a simple-root (i.e., $p \nmid n$) cyclic code.*

Theorem 25. *The parity-check polynomial of the cyclic code $\mathcal{C}_q(V,T,D)$ is*

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

is the minimal (over $\mathbb{F}_q$) polynomial of P^{-m_i}.

Proof. By definition, the parity-check polynomial is equal to the quotient of $x^n - 1$ by the generator polynomial g. At the same time, g is equal to the greatest common divisor of the basis polynomials

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

Let $n_{i,t} = \mathrm{ord}\left(P^{m_i(q^t-1)}\right)$ and

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

In particular, $S_0 = n = \pm 1$. Thus,

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

and $h(P^{-m_i}) = 0$. Finally, $\deg(h_{P^{-m_i}}) = k_i$, and hence $\deg(h) = k$; i.e., we have found all roots of the polynomial h. $\triangle$

Recall that a cyclic code is said to be *reversible* if its generator (or, equivalently, parity-check) polynomial is self-reciprocal.

Corollary 3. *If P_D is a centrally symmetric polytope (i.e., $-P_D = P_D$), then $\mathcal{C}_q(V,T,D)$ is a reversible code.*

Among centrally symmetric polytopes, we highlight so-called *del Pezzo polytopes*, which are discussed in [19]. At the same time, the theory of cyclic reversible (or, equivalently, LCD) codes can be found in [10, 28, 29].

3.2. Toric Codes on $\mathbb{P}^1$ and Some Toric Surfaces

We keep the notation of Section 2.4.

Theorem 26. *The codes*

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

are all possible (up to equivalence) toric codes on $\mathbb{P}^1$, and their parameters are presented in Table 3.

The code $\mathrm{RS}_q(r)$ is known as a (*punctured*) *Reed–Solomon code*; $\mathrm{PRS}_q(r)$ is equivalent to the so-called *projective* (*doubly extended*) *Reed–Solomon code*, because for even r the divisors rP_y and $\frac{r}{2}D_{x,y}$ are equivalent. Moreover, according to Theorem 23, it is a (nonprimitive, non-narrow sense) BCH code. Finally, the polytope of $\frac{r}{2}D_{x,y}$ is clearly the closed line segment $\left[-\frac{r}{2}, \frac{r}{2}\right]$; hence, by Corollary 3, the code $\mathrm{PRS}_q(r)$ is reversible.

Table 3. Toric codes on $\mathbb{P}^1$.

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

Table 4. Toric codes on $\mathbb{P}^2$.

	n	k	d	Restrictions	Reference
$\mathcal{C}_q(\mathbb{P}^2, \mathbb{G}_m^2, rL_z)$	$(q-1)^2$	$\frac{(r+1)(r+2)}{2}$	$n-r(q-1)$	$0<r<q-1$	[4, Theorem 1.3]
$\mathcal{C}_q(\mathbb{P}^2, T_{2.c}, rL_z)$	q^2-1		$n-rq$	$0<r<q$	[30, Sections 2 and 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, Section 2]

Theorem 27. *All possible (up to equivalence) toric codes on $\mathbb{P}^2$ are presented in Table 4.*

The second code of Table 4 is known as a (*punctured*) *Reed–Muller code*; the third is equivalent to the so-called *projective Reed–Muller code*, because for $3 \mid r$ the divisors rL_z and $\frac{r}{3}D_{x,y,z}$ are equivalent.

Theorem 28. *The codes*

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

are all possible (up to equivalence) toric codes on quadratic surfaces, and their parameters are presented in Table 5.

It is easily proved that

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

where $\otimes$ denotes the tensor (Kronecker) product of codes. At the same time, $C_{2.c}$ is a primitive narrow-sense BCH code by [31, Proposition 4.2]. Finally, C_4 is a reversible code by Corollary 3, because the polygon of $\frac{r}{2}D_{x,y,u,v}$ is clearly the closed square $\left[-\frac{r}{2}, \frac{r}{2}\right] \times \left[-\frac{r}{2}, \frac{r}{2}\right]$.

Lemma 11 [4, Theorem 1.5]. *All possible (up to equivalence) split toric codes on Hirzebruch surfaces $\mathbb{F}_m$ for $m > 0$ are of the form*

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

and their parameters are

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

Remark 3. The author examined non-split toric codes on Hirzebruch surfaces and came to a conclusion that they are of little interest.

3.3. Toric Codes on del Pezzo Surfaces of Degree 6

We keep the notation of Sections 2.5 and 3.1. Among all del Pezzo surfaces of degree 6, the surface $\mathcal{D}_6$ seems to be the most appropriate for considering toric codes on it, because its splitting

Table 5. Toric codes on quadratic surfaces.

	n	k	d	Restrictions		Reference
C_1	$(q-1)^2$	$(r_1+1)(r_2+1)$	$(q-1-r_1)$ $\times(q-1-r_2)$	$0<r_1,r_2<q-1$		[4, Theorem 1.4]
$C_{2.a}$	$(q+1)^2$		$(q+1-r_1)$ $\times(q+1-r_2)$	$0<r_1,r_2<q+1$, $2\mid r_1$	$2\mid r_2$	[31, Remark 3.2]
$C_{2.b}$	q^2-1		$(q-1-r_1)$ $\times(q+1-r_2)$	$0<r_1<q-1$, $0<r_2<q+1$		
$C_{2.c}$		$(r+1)^2$	$n-r(q+1)$	$0<r<q-1$		[31, Proposition 4.2]
C_4	q^2+1			$0<r<q$, $2\mid r$		[31, Proposition 4.7]

field is the largest. In other words, this surface is "the most non-split." For comparison, see non-toric and split toric codes on the surface $\mathcal{D}_1$ in [32] and [33, Example 5.2], respectively.

Let $\beta\in\mathbb{F}_{q^6}^*$ be an element of order $n=q^2-q+1$, and let $P_\beta=(\beta,\beta^q)$. It is clear that

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

and $P_\beta^{(i,j)}=\beta^{i+jq}$ for $(i,j)\in M$. We also recall that h_{β^i} denotes the minimal (over $\mathbb{F}_q$) polynomial of β^i, where $0\le i\le n-1$.

In the next theorem we use the quantity $N_q(1)$, i.e., the maximum possible number of $\mathbb{F}_q$-points on an elliptic curve. It is known [9, Theorem 3.4.49] that

$$N_q(1)=\begin{cases}q+\lfloor 2\sqrt{q}\rfloor & \text{if } \sqrt{q}\notin\mathbb{N},\ p<q, \text{ and } p\mid\lfloor 2\sqrt{q}\rfloor,\\ q+\lfloor 2\sqrt{q}\rfloor+1 & \text{otherwise.}\end{cases}$$

Elliptic curves for which the number of $\mathbb{F}_q$-points attains $N_q(1)$ are called $\mathbb{F}_q$-*optimal* ($\mathbb{F}_q$-*maximal* if $\sqrt{q}\in\mathbb{N}$). Such curves are interesting in themselves, because algebraic geometry codes on them are so-called *almost MDS codes* with rather large lengths [9, Section 4.4.2].

Theorem 29. *Consider $r\in\mathbb{N}$ such that $rN_q(1)<n$ and for any partition $r=\sum\limits_{i=1}^{m}r_i>m$ (with $r_i\in\mathbb{N}$) we have the inequality*

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

Then the toric code $\mathcal{C}_{q,r}=\mathcal{C}_q(\mathcal{D}_6,T_6,rH_0)$ has parameters

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

Moreover, if the point P_β in the definition of $C_{q,r}$ is taken as a generator of $\mathrm{E}_q(\Phi_6)$, then $C_{q,r}$ is a cyclic reversible code with the parity-check polynomial

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

Proof. The length n is obvious. First, we will estimate the minimum distance d. Let $D=\sum\limits_{i=1}^{m}C_i$ be the decomposition into irreducible (over $\mathbb{F}_q$) components for an arbitrary element of the linear system $|rH_0|$. The Picard group of the surface $\mathcal{D}_6$ is generated by H_0; hence, $C_i\sim r_iH_0$, $r_i\in\mathbb{N}$

and $\sum_{i=1}^{m} r_i = r$. In particular, the arithmetic genus g_i of a curve C_i is $3r_i(r_i-1)+1$ (see, e.g., [26, Exercise V.1.3]). Therefore, by [34, Proposition 2.3] we obtain

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

Moreover, if $r = m$ (i.e., $r_i = g_i = 1$ for $1 \le i \le m$), then $|C_i(\mathbb{F}_q)| \le N_q(1)$ by Corollary 1. Thus,

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

and we get the desired bound on d, since $T(\mathbb{F}_q) = \mathcal{D}_6(\mathbb{F}_q)$. At the same time, the dimension k follows from Lemma 5 and the inequality $rN_q(1) < n$.

The cyclicity of $\mathcal{C}_{q,r}$ is implied by Lemma 10. The polygon $P_{rH_0} = rP_{H_0}$ (see Fig. 6 for $r = 1$) is centrally symmetric; therefore, the reversibility of $\mathcal{C}_{q,r}$ follows from Corollary 3. Finally, we obtain the desired parity-check polynomial by Lemma 5 and Theorem 25. $\triangle$

Theorem 29 and Corollary 2 immediately imply the following.

Corollary 4. *For $q \ge 5$, the code $\mathcal{C}_{q,1}$ is an $[n, 7, n - N_q(1)]_q$ code.*

Remark 4. For small q the codes $\mathcal{C}_{q,1}$ have parameters

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

The codes $\mathcal{C}_{7,1}$, $\mathcal{C}_{8,1}$, and $\mathcal{C}_{9,1}$ have already been found (by a non-exhaustive computer search) in [35–37], respectively. According to the Brouwer–Grassl tables [13], they are the best currently known for given q, n, and k. Thus, it seems that codes $\mathcal{C}_{q,r}$ (at least for $r = 1$) are also good enough for larger values of q.

Remark 5. By Corollaries 1 and 2 and the Deuring–Waterhouse theorem [9, Theorem 3.3.12], we know all weights of a code $\mathcal{C}_{q,1}$ for $q \ge 5$. In particular, its minimum-weight codewords (up to multiplication by an element of $\mathbb{F}_q^*$) bijectively correspond to $\mathbb{F}_q$-optimal elliptic curves from $|H_0|$. However, in this linear system there are many different (as sets) elliptic curves that are $\mathbb{F}_q$-isogenous, i.e., have the same number of $\mathbb{F}_q$-points. Nevertheless, by the reversibility of any code $\mathcal{C}_{q,r}$, for full computation of its spectrum it suffices to solve a system of linear equations derived from the MacWilliams identity [9, Theorem 1.1.17].

ACKNOWLEDGEMENT

The author is deeply grateful to his scientific advisor M.A. Tsfasman and also to V. Batyrev, S. Gorchinskiy, G. Kabatiansky, B. Kunyavskii, K. Loginov, A. Perepechko, S. Rybakov, K. Shramov, V. Stukopin, D. Timashev, A. Trepalin, S. Vlăduţ, I. Vorobyev, and participants of the Coding Theory seminar run by L.A. Bassalygo at the Institute for Information Transmission Problems of the Russian Academy of Sciences for their help and useful comments.

FUNDING

The research was supported in part by the Simons Foundation.

REFERENCES

1. *Advances in Algebraic Geometry Codes*, Martínez-Moro, E., Munuera, C., and Ruano, D., Eds., Singapore: World Sci., 2008.
2. Cox, D.A., Little, J.B., and 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)*, Buchmann, J., Høholdt, T., Stichtenoth, H., and Tapia-Recillas, H., Eds., Berlin: Springer, 2000, pp. 132–142.

4. Hansen, J.P., Toric Varieties Hirzebruch Surfaces and Error-Correcting Codes, *Appl. Algebra Engrg. Comm. Comput.*, 2002, vol. 13, no. 4, pp. 289–300.

5. Berman, S.D., On the Theory of Group Codes, *Kibernetika (Kiev)*, 1967, vol. 3, no. 1, pp. 31–39 [*Cybernetics* (Engl. Transl.), 1967, vol. 3, no. 1, pp. 25–31].

6. Berman, S.D., Semisimple Cyclic and Abelian Codes. II, *Kibernetika (Kiev)*, 1967, vol. 3, no. 3, pp. 21–30 [*Cybernetics* (Engl. Transl.), 1967, vol. 3, no. 3, pp. 17–23].

7. Joyner, D., Toric Codes over Finite Fields, *Appl. Algebra Engrg. Comm. Comput.*, 2004, vol. 15, no. 1, pp. 63–79.

8. Voskresenskii, V.E., *Algebraic Groups and Their Birational Invariants*, Providence, R.A.: Amer. Math. Soc., 1998.

9. Tsfasman, M.A.,Vlăduţ, S.G., and Nogin, D.Yu., *Algebrogeometricheskie kody. Osnovnye ponyatiya*, Moscow: MCCME, 2003. Translated under the title *Algebraic Geometric Codes: Basic Notions*, Providence, R.I.: Amer. Math. Soc., 2007.

10. Massey, J.L., Reversible Codes, *Inform. Control*, 1964, vol. 7, no. 3, pp. 369–380.

11. Lachaud, G., The Parameters of Projective Reed–Müller Codes, *Discrete Math.*, 1990, vol. 81, no. 2, pp. 217–221.

12. Voskresenskii, V.E., Projective Invariant Demazure Models, *Izv. Akad. Nauk SSSR Ser. Mat.*, 1982, vol. 46, no. 2, pp. 195–210 [*Math. USSR Izv.* (Engl. Transl.), 1983, vol. 20, no. 2, pp. 189–202].

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. Platonov, V.P. and Rapinchuk, A.S., *Algebraicheskie gruppy i teoriya chisel*, Moscow: Nauka, 1991. Translated under the title *Algebraic Groups and Number Theory*, Boston: Academic, 1994.

15. Rubin, K. and Silverberg, A., Compression in Finite Fields and Torus-Based Cryptography, *SIAM J. Comput.*, 2008, vol. 37, no. 5, pp. 1401–1428.

16. Voskresenskii, V.E., On Two-Dimensional Algebraic Tori, *Izv. Akad. Nauk SSSR Ser. Mat.*, 1965, vol. 29, no. 1, pp. 239–244.

17. Voskresenskii, V.E., On Two-Dimensional Algebraic Tori. II, *Izv. Akad. Nauk SSSR Ser. Mat.*, 1967, vol. 31, no. 3, pp. 711–716 [*Math. USSR Izv.* (Engl. Transl.), 1967, vol. 1, no. 3, pp. 691–696].

18. Graber, T., Harris, J., Mazur, B., and 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)*, Laudal, O.A., Ed., Berlin: Springer, 2004, pp. 531–542.

19. Voskresenskii, V.E. and Klyachko, A.A., Toroidal Fano Varieties and Root Systems, *Izv. Akad. Nauk SSSR Ser. Mat.*, 1984, vol. 48, no. 2, pp. 237–263 [*Math. USSR Izv.* (Engl. Transl.), 1985, vol. 24, no. 2, pp. 221–244].

20. Batyrev, V.V. and Tschinkel, Y., Rational Points of Bounded Height on Compactifications of Anisotropic Tori, *Int. Math. Res. Notices*, 1995, vol. 1995, no. 2, pp. 591–635.

21. Ballard, M.R., Duncan, A., and 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, vol. 17, no. 5, pp. 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)*, Kaledin, D. and Tschinkel Y., Eds., Amsterdam: IOS Press, 2008, pp. 92–122.

26. Hartshorne, R., *Algebraic Geometry*, Berlin: Springer, 1977. Translated under the title *Algebraicheskaya geometriya*, Moscow: Mir, 1981.

27. Hernando, F., O'Sullivan, M.E., Popovici, E., and Srivastava, S., Subfield-Subcodes of Generalized Toric Codes, in *Proc. 2010 IEEE Int. Sympos. on Information Theory (ISIT'2010), Austin, TX, USA, June 13–18, 2010*, pp. 1125–1129.

28. Massey, J.L., Linear Codes with Complementary Duals, *Discrete Math.*, 1992, vol. 106–107, pp. 337–342.

29. Yang, X. and Massey, J.L., The Condition for a Cyclic Code to Have a Complementary Dual, *Discrete Math.*, 1994, vol. 126, no. 1–3, pp. 391–393.

30. Kasami, T., Lin, S., and Peterson, W., New Generalizations of the Reed–Muller Codes. I: Primitive Codes, *IEEE Trans. Inform. Theory*, 1968, vol. 14, no. 2, pp. 189–199.

31. Couvreur, A. and Duursma, I., Evaluation Codes from Smooth Quadric Surfaces and Twisted Segre Varieties, *Des. Codes Cryptogr.*, 2013, vol. 66, no. 1–3, pp. 291–303.

32. Boguslavsky, M.I., Sections of the Del Pezzo Surfaces and Generalized Weights, *Probl. Peredachi Inf.*, 1998, vol. 34, no. 1, pp. 18–29 [*Probl. Inf. Transm.* (Engl. Transl.), 1998, vol. 34, no. 1, pp. 14–24].

33. Ruano, D., On the Parameters of r-Dimensional Toric Codes, *Finite Fields Appl.*, 2007, vol. 13, no. 4, pp. 962–976.

34. Aubry, Y. and 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)*, Pellikaan, R., Perret, M., and Vlăduţ, S., Eds., Berlin: de Gruyter, 1996, pp. 1–7.

35. Daskalov, R. and Hristov, P., New One-Generator Quasi-cyclic Codes over $GF(7)$, *Probl. Peredachi Inf.*, 2002, vol. 38, no. 1, pp. 59–63 [*Probl. Inf. Transm.* (Engl. Transl.), 2002, vol. 38, no. 1, pp. 50–54].

36. Daskalov, R. and Hristov, P., New Quasi-cyclic Degenerate Linear Codes over $GF(8)$, *Probl. Peredachi Inf.*, 2003, vol. 39, no. 2, pp. 29–35 [*Probl. Inf. Transm.* (Engl. Transl.), 2003, vol. 39, no. 2, pp. 184–190].

37. Daskalov, R., Metodieva, E., and Hristov, P., New Minimum Distance Bounds for Linear Codes over $GF(9)$, *Probl. Peredachi Inf.*, 2004, vol. 40, no. 1, pp. 15–26 [*Probl. Inf. Transm.* (Engl. Transl.), 2004, vol. 40, no. 1, pp. 13–24].