Non-Split Toric BCH Codes on Singular del Pezzo Surfaces

Dmitrii Koshelev

Abstract—In the article we construct low-rate non-split toric $q$-ary codes on some singular surfaces. More precisely, we consider non-split toric cubic and quartic del Pezzo surfaces, whose singular points are $F_q$-conjugate. Our codes turn out to be BCH ones with sufficiently large minimum distance $d$. Indeed, we prove that $d - d^* \geq q - [2\sqrt{q}] - 1$, where $d^*$ is the designed minimum distance. In other words, we significantly improve upon BCH bound. On the other hand, the defect of the Griesmer bound for distance. In other words, we significantly improve upon BCH bound. On the other hand, the defect of the Griesmer bound for the new codes is $\leq [2\sqrt{q}] - 1$, which also seems to be quite good. It is worth noting that to better estimate $d$ we actively use the theory of elliptic curves over finite fields.

I. INTRODUCTION

THIS article continues our first one [1] about non-split toric codes, i.e., algebraic geometry (AG) codes [2] on non-split toric varieties [3] over a finite field $F_q$. It is wonderful circumstance that most of these codes are (simple-root) cyclic [4, Chapter 7]. Therefore they have more chances to be used in practice than other algebraic geometry codes on high-dimensional varieties. In [1] we assume everywhere that toric varieties are smooth, however there are no any obstacles to consider non-split toric codes on singular ones.

There is the well known classification of toric (possibly singular) del Pezzo surfaces [5]. They bijectively correspond (up to an equivalence) to so-called reflexive polygons [3, §8.3]. There are exactly 16 such polygons [3, Theorem 8.3.7], but only 5 of them (see Figure 1 and Table I) are quite symmetric, i.e., have an integral action of order greater than 2. The last condition seems to be necessary for constructing good non-split toric codes.

Non-split toric codes $C_6, C_8, C_9$ (Tables III and IV) associated with such smooth polygons (i.e., $Pol_6, Pol_8, Pol_9$) have already been considered, for example, in [1, §2.3] (also see [6, §4.2]), [7, Proposition 4.7], and [8, §2] respectively. The other polygons $Pol_3, Pol_4$ correspond to some singular cubic (§ II-A) and quartic (§ II-B) del Pezzo surfaces respectively. As far as we know, algebraic geometry codes $C_3, C_4$ (Tables III and IV) on the given surfaces have not been studied yet. However, AG codes on some smooth cubic and quartic del Pezzo surfaces are described in [6, §6], [9, §4.1, §5.1], and [11].

II. TORIC DEL PEZZO SURFACES AND REFLEXIVE POLYGONS

Let $F_q$ be a finite field of characteristic $p$. Consider a toric (possibly singular) del Pezzo surface $S$ over $F_q$, i.e., a toric one, whose anticanonical divisor $-K_S$ is an ample Cartier divisor. Let $\varphi_{\min}: S' \to S$ be the minimal resolution of singularities. The surface $S'$ is a so-called weak (or generalized) del Pezzo surface. The self-intersection $K_S^2$ is said to be degree of $S$ (or $S'$). Besides, the Fano index of $S$ is the maximal number $i \in \mathbb{N}$ such that $K_S \sim iH$ for some Cartier divisor $H$ on $S$, which can be taken over $F_p$. The theory of (not necessarily toric) del Pezzo surfaces (with more focus on $K_S^2 = 3, 4$) can be found, for example, in [5].

Lemma 1 [3, Prop. 11.2.8], [5, Prop. 0.6], [12, Fig. 1]:
1) $-K_S$ is very ample, $\dim |-K_S| = K_S^2$, and also $3 \leq K_S^2 \leq 9$;
2) The surface $S$ may only have singularities of the types $A_1, A_2, A_3$ [3, Example 10.1.5];
3) $\varphi_{\min}$ is a crepant morphism, i.e., $K_{S'} := \varphi_{\min}^*(K_S)$ is a canonical divisor.

A lattice convex polygon $P \subset \mathbb{R}^2$ is said to be reflexive (or Gorenstein) if $O := (0, 0)$ is its internal point and the dual (convex) polygon $P^\circ$ is also lattice. In this case, $P^\circ$ is obviously reflexive.

Lemma 2 [3, Exer. 2.3.5.a, Def. 2.3.12, Thm 10.5.10]: If $P$ is reflexive, then
1) $O$ is the unique internal point of $P$;
2) All vertices of $P$ are ray generators of the normal fan of $P^\circ$;
3) $|P \cap \mathbb{Z}^2| + |P^\circ \cap \mathbb{Z}^2| = 14$.

Theorem 1 [3, Theorems 6.2.1, 8.3.4]: The maps
$$P \mapsto (S_P, D_P) \quad [3, \S2.3, \S4.2],$$
$$\langle S, -K_S \rangle \mapsto P_{-K_S} \quad [3, \S4.3]$$
are inverse to each other between reflexive polygons (up to an equivalence) and toric (possibly singular) del Pezzo surfaces provided with the anticanonical divisor that is the sum of all prime torus-invariant divisors.

Theorem 2 [3, Theorem 8.3.7], [12, Figure 1]: Up to an equivalence (isomorphism) there are exactly 16 reflexive polygons (split toric del Pezzo surfaces).
It is immediately checked that all reflexive polygons having an action of order greater than 2 are represented in Figure 1. For a polygon \( \text{Pol}_i \) the subscript \( i \) is the amount of integral points on its boundary. In turn, the superscript \( t \) denotes the transposition operation of \( \Phi_t \) as a matrix (of order \( i \)) in \( \text{GL}(2, \mathbb{Z}) \). The corresponding non-split toric del Pezzo surfaces (with their Fano index) are contained in Table I. We recall that the action \( \Phi_t \) (or \( \Phi_f \)) complies with the Frobenius action on toric invariant curves and points of the surface. Finally, it is notable that all the five surfaces have Picard \( \mathbb{F}_2 \)-number 1.

**Lemma 3** [3, Proposition 4.2.5, Exer-s 4.3.2, 10.5.7,b]:

1. For \( K_S^3 \leq 7 \) the Fano index of \( S \) is equal to 1;
2. Any smooth irreducible curve from \( |-K_S| \) is elliptic;
3. \( \text{Pic}(S) \) is a free abelian group.

**A. Toric (Singular) Cubic Surface in \( \mathbb{P}^3 \)**

Choose an element \( \alpha \in \mathbb{F}_q^3 \setminus \mathbb{F}_q \) and consider the so-called norm cubic \( \mathbb{F}_q \)-surface [13, Example 1.3.10]

\[
S_3 : X_0 \cdot X_1 \cdot X_2 = x_3^3 \subset \mathbb{P}^3_{(x_0:x_1:x_2:x_3)},
\]

where

\[
X_0 := x_0 + \alpha x_1 + \alpha^2 x_2, \quad X_1 := x_0 + \alpha^3 x_1 + \alpha^2 x_2, \\
X_2 := x_0 + \alpha^3 x_1 + \alpha^2 x_2.
\]

For \( i \in \mathbb{Z}/3 \) let

\[
\tilde{L}_i : X_i = x_i = 0, \quad \tilde{P}_i := \tilde{L}_{i+1} \cap \tilde{L}_{i+2}, \\
L_i := \text{pr}(\tilde{L}_i), \quad P_i := \text{pr}(\tilde{P}_i) = L_{i+1} \cap L_{i+2},
\]

where \( \text{pr} : S_3 \rightarrow \mathbb{P}^2_{(x_0:x_1:x_2)} \) is the well-defined projection of degree 3. Finally, let

\[
\tilde{L}_3 := \sum_{i=0}^{2} \tilde{L}_i, \quad L_3 := \sum_{i=0}^{2} L_i, \quad \text{and} \quad P_3 := \{P_i\}_{i=0}^{2}.
\]

**Remark 1:** The surface \( S_3 \) is toric with respect to the torus \( T_3 \cong S_3 \setminus \{x_3 = 0\} \) (see [1, Theorem 8]) and the lines \( \tilde{L}_i \) (resp. \( \tilde{P}_i \)) are the unique \( T_3 \)-invariant curves (resp. points) on \( S_3 \). Moreover, they are \( \mathbb{F}_q \)-conjugate.

**Table I**

| No | (polygon, action) | toric surface | Fano index | (polygon^1, action^1' ) |
|----|-------------------|--------------|------------|------------------------|
| 1  | (Pol_3, \( \Phi_t^3 \)) | \( S_3 \) (III-A) | 5          |                        |
| 2  | (Pol_4, \( \Phi_t^4 \)) | \( S_4 \) (III-B) | 4          |                        |
| 3  | (Pol_6, \( \Phi_6 \)) | \( D_6 \) [1, §2.5] | 3 (up to an equivalence) |                |
| 4  | (Pol_9, \( \Phi_9 \)) | \( E \) [1, §2.4] | 2          | 2                      |
| 5  | (Pol_9, \( \Phi_9 \)) | \( \mathbb{P}^2 \) | 3          | 1                      |

**Lemma 4** [12, Table 7]: We have:

1. The points \( \tilde{P}_i \) are the unique singularities on \( S_3 \) (of type \( A_2 \));
2. \( \varphi_{\min} : S_3^2 \rightarrow S_3 \) is the simultaneous blowing up at them;
3. \( L_i \) are the unique lines on \( S_3 \).

**Theorem 3** [3, Exer. 8.3.8.c], [5, Exam. 8.7.b], [12, Table 7], [13, Exam. 1.3.10]:

1. \( S_3 \) is the unique (up to an \( \mathbb{F}_q \)-isomorphism) del Pezzo surface of degree 3 toric with respect to the torus \( T_3 \);
2. \( S_3 \) is the non-split toric surface associated with the pair \( (\text{Pol}_3, \Phi^3_t) \);
3. \( S_3 \) is the so-called fake projective plane [14, Example 1.2], i.e., the quotient \( \mathbb{P}^2/\sigma \) under a transformation \( \sigma \in \text{PGL}(3, \mathbb{F}_q) \), whose fixed point set is \( P_3 \);
4. \( S_3^3 \) is the blowing up of del Pezzo surface \( D_3 \) of degree 6 (see 1, §2.5) at one of the two triples

\[
Q_3 = \{Q_0, Q_1, Q_2\}, \quad Q_3^* = \{Q_0^*, Q_1^*, Q_2^*\}
\]

of \( \mathbb{F}_q \)-conjugate \( T_3 \)-invariant points.

**Proof:** All statements can be found in the references, except that the action \( \Phi^3_t \) on the polygon \( \text{Pol}_3 \) is the only one of order 3 (up to a conjugation in \( \text{Aut}(\text{Pol}_3) \)). This fact is necessary in order to correctly pass from the split torus case (in those references) to that of \( T_3 \).

From [1, Theorem 14] or one of Statements 3, 4 of Theorem 3 it follows that the Picard \( \mathbb{F}_q \)-number of \( S_3 \) is equal to 1. Since the Fano index of \( S_3 \) is also 1, we obtain

**Lemma 5:** The Picard \( \mathbb{F}_q \)-group of the surface \( S_3 \) equals

\[
\text{Pic}(S_3) = (-K_{S_3}) \cong \mathbb{Z}.
\]

For the sake of definiteness, we choose the triple \( Q_3 \) and thus we deal with the diagram

\[
\varphi_{\min} : S_3 \leftarrow S_3^3 \rightarrow D_3 \rightarrow \mathbb{P}^2,
\]

where \( bl_{Q_3}, bl_{P_3} \) are the blowing up maps at \( Q_3, P_3 \) respectively. Besides, let

\[
\varphi := bl_{P_3} \circ bl_{Q_3} \circ \varphi_{\min}^{-1} : S_3 \rightarrow \mathbb{P}^2.
\]

**Corollary 1:** The anticanonical linear system of \( S_3 \) equals

\[
\{-K_S\} = \varphi^*(\mathcal{L}) - 2\tilde{L}_3,
\]

where \( \mathcal{L} := |L_3 - P_3 - Q_3| \) is the (incomplete) linear system of all (possibly reducible or singular) \( \mathbb{F}_q \)-cubics \( C \subset \mathbb{P}^2 \) passing through \( P_3 \) such that \( L_i \) is a tangent of \( C \) at \( P_{i+1} \) (resp. \( P_{i+2} \) for the triple \( Q_3^* \)).
For more clarity on what is going on, see Figures 2, 3, where arrows denote the Frobenius action. In the second figure $E_{P_i}$ are the exceptional curves associated with the points $P_i$ and $L_i$ (resp. $C$) are the proper preimages of $L_i$ (resp. $C \neq L_i$) with respect to $b|_{P_i}$. As usual, we also use the notations $E_{P_i} := \sum_{i=0}^{2} E_{P_i}$ and $L_3 := \sum_{i=0}^{2} L_i$.

Proof: Let us freely use known identities for direct and inverse images of (possibly incomplete) linear systems on algebraic surfaces (see, e.g., [15, §II.5-6, §IV.2]). First, $b|_{P_i} [L_3 - P_3] = [b|_{P_i} L_3 - E_{P_i}] + E_{P_3} = [L_3 + E_{P_3}] + E_{P_3}$.

Therefore

$L^* := b|_{P_3} (L) = \tilde{L} + E_{P_3}$, where $\tilde{L} := [L_3 + E_{P_3} - Q_3]$.

Next, let $E_{Q_3}$ be the exceptional divisor associated with the point set $Q_3$ and $\tilde{L}_3$ (resp. $\tilde{E}_{P_3}$) be the proper preimage of $L_3$ (resp. $E_{P_3}$) with respect to $b|_{Q_3}$. We have:

$b|_{Q_3}^* (L) = [b|_{Q_3}^* (L_3 + E_{P_3}) - E_{Q_3}] = \tilde{L} + E_{Q_3}$,

$L^{**} := b|_{Q_3}^* (L^*) = [b|_{Q_3}^* (\tilde{L} + E_{P_3})] = \tilde{L} + \tilde{E}_{P_3} + 2E_{Q_3}$,

where $\tilde{L} = [L_3 + \tilde{E}_{P_3} + E_{Q_3}]$.

From the identities

$(\varphi_{min})_* (\tilde{L}_3) = (\varphi_{min})_* (\tilde{E}_{P_3}) = 0$,

$(\varphi_{min})_* (E_{Q_3}) = \hat{L}_3 \sim -K_{S_3}$

it follows that

$\varphi^* (L) = (\varphi_{min})_* (L^{**})$ =

$(\varphi_{min})_* (\tilde{L}) + (\varphi_{min})_* (\tilde{E}_{P_3} + 2E_{Q_3}) = [-K_{S_3}] + 2\hat{L}_3$.

Finally, $L$ has the geometric description declared in the corollary by virtue of [15, Exercise V.3.2].

One can easily check that

Remark 2: Any $C \in L$ different from $L_3$ is an absolutely irreducible (possibly singular) $\mathbb{F}_q$-cubic.

Remark 3: Given $C \in L$, the divisor $D := \varphi^* (C) - 2\hat{L}_3$ is an elliptic curve if and only if $C$ is one too. Moreover, in this case $\varphi: D \to C$ is an isomorphism.

**Lemma 6:** Let $E \in L$ be an elliptic $\mathbb{F}_q$-curve and $O \in E(\mathbb{F}_p)$ be one of its flexes, which, as is known, always exists over $\mathbb{F}_p$ (for details see [16, Chapter 11]). Then the $P_i$ are points of order 9 (with respect to $O$ as the neutral element of the chord-tangent group law on $E$) such that $\langle P_0 \rangle = \langle P_1 \rangle = \langle P_2 \rangle$.

Proof: By definition of $L$ in Corollary 1,

$2P_0 + P_1 = 2P_1 + P_2 = 2P_2 + P_0 = O$,

hence we see that

$9P_0 = O, \quad 7P_0 = P_1, \quad 4P_0 = P_2$.

Similarly, $P_0, P_2$ (resp. $P_0, P_1$) are expressed through $P_1$ (resp. $P_2$).

Finally, the points $P_i$ of order 9, otherwise they would be equal.

**Theorem 4:** For any elliptic $\mathbb{F}_q$-curve $E \in [-K_{S_3}]$ the order $|E(\mathbb{F}_p)|$ is divisible by 3.

Proof: The result is proved by exhibiting an $\mathbb{F}_q$-point of order 3 on $E$.

By Remark 3 we are in the conditions of the previous lemma, i.e., up to an $\mathbb{F}_q$-isomorphism $E \in L$. This curve has the group structure with respect to any point $O' \in E(\mathbb{F}_p) \neq \emptyset$ (instead of a flex $O \in E(\mathbb{F}_p)$) as the neutral element. It is well known that there is the group $\mathbb{F}_q$-isomorphism $\tau(P) := P + O'$, $\tau: E \approx E$. At the same time, $E$ has a Weierstrass form $W: y^2 + h(x)y = f(x)$ defined over $\mathbb{F}_p$, where $\deg(h) \leq 1$, $\deg(f) = 3$. Let $\sigma: E \approx W$ be the corresponding $\mathbb{F}_q$-isomorphism such that $\sigma(O')$ is the point at infinity.

Consider the $\mathbb{F}_q$-point $(x_0, y_0) := (\sigma \circ \tau)(3P_0)$ of order 3 on $W$. If $x_0 \in \mathbb{F}_p$ (e.g., this is true for $p = 3$), then $y_0 \in \mathbb{F}_q$ and all is proved. Otherwise the 3-division polynomial $\psi_3$ (see, e.g., [17, Exercise 3.7]) has exactly two $\mathbb{F}_q$-irreducible factors, namely the $\mathbb{F}_q$-minimal (cubic) polynomial of $x_0$ and $x - x_1$ for some $x_1 \in \mathbb{F}_q$. Note that the 3-torsion subgroup $W[3]$ is generated, for example, by the points $(x_0, y_0), (x_0^2, y_0^2)$. Therefore $W[3] \subset W(\mathbb{F}_q)[3]$ and thus $(x_1, y_1) \in W(\mathbb{F}_q)[3]$ for an appropriate $y_1$.

**Corollary 2:** For $p = 3$ supersingular elliptic curves (i.e., of $j$-invariant 0) [2, §2.4.3] do not belong to $[-K_{S_3}]$.

Finally, carefully analyzing small values $q$, we get the following result.
Corollary 3: For $q \geq 3$ and any $\mathbb{F}_q$-divisor $D \in | - K_{S_q} |$ we have
\[ | \text{Supp}(D)(\mathbb{F}_q) | \leq 3 | N_q(1) / 3 \],
where the number $N_q(1)$ is given in Theorem 10.

B. Toric (Singual) Intersection of Two Quadrics in $\mathbb{P}^4$

Let us fist suppose that $p > 2$. Choose quadratic non-residues $b \in \mathbb{F}_q$, and $a := a_0 + a_1 \sqrt{b} \in \mathbb{F}_q$ (for some $a_0, a_1 \in \mathbb{F}_q$) and consider the following intersection of two $\mathbb{F}_q$-quadratics:
\[ S_4^2 : \{ x_0^2 + bx_1^2 - a_0(y_0^2 + by_1^2) - 2a_1b[y_0y_1] = z^2, \quad \mathbb{P}_4 \}
\]
where $(x_0 : x_1 : y_0 : y_1 : z)$ are the corresponding homogeneous coordinates. Note that the affine open subset $U := S_4^2 \setminus \{ z = 0 \}$ is the Weil restriction (with respect to the extension $\mathbb{F}_q / \mathbb{F}_p$) of the $\mathbb{F}_p$-conic
\[ C_2 : x^2 - ay^2 = 1 \subset \mathbb{A}_x(y)
\]
if $x = x_0 + x_1 \sqrt{b}$, $y = y_0 + y_1 \sqrt{b}$. At the same time, $C_2$ is isomorphic to the torus $T_2$ from [1, Theorem 7].

For $p = 2$ we can take elements $b \in \mathbb{F}_q$, $a \in \mathbb{F}_q^2$ such that $T_{\mathbb{F}_q / \mathbb{F}_p}(b) = T_{\mathbb{F}_q / \mathbb{F}_p}(a) = 1$. As is well known, the equation $x^2 + bx + (a \text{ resp. } x^2 + x + a)$ has no roots over $\mathbb{F}_p$ (resp. $\mathbb{F}_q$).

Thus no problems to write out the equations of $C_2$ and $S_3$ in even characteristic.

For $i \in \mathbb{Z} / 4$ we enumerate the lines $\widehat{L}_i$ of $S_4 \setminus \{ z = 0 \}$ such that $\widehat{P}_i = \widehat{L}_{i+1} \cap \widehat{L}_{i+2}$ is a point. Also, let
\[ L_i := \text{pr}(\widehat{L}_i), \quad P_i := \text{pr}(\widehat{P}_i) = L_{i+1} \cap L_{i+3}, \]
where
\[ \text{pr} : S_4 \rightarrow \mathcal{E} \subset \mathbb{P}_3(x_0 : x_1 : y_0 : y_1) \]
is the well-defined projection of degree 2 onto the elliptic quadratic surface $\mathcal{E}$ (from Table 1). Finally, let
\[ \mathcal{L}_4 := \{ \widehat{L}_i \}_{i=0}^3 \quad \text{and} \quad \mathcal{P}_4 := \{ P_i \}_{i=0}^3 \]

Remark 4: The surface $S_4$ is toric with respect to the torus $T_2 \simeq U$ (see [1, Theorem 8]) and the lines $\widehat{L}_i$ (resp. $\widehat{P}_i$) are the unique $T_2$-invariant curves (resp. points) on $S_4$. Moreover, they are $\mathbb{F}_p$-conjugate.

Recall that the surface $\mathcal{E}$ is also toric for $T_4$.

Lemma 7 [12, Table 6]: We have:
1) The points $\widehat{P}_i$ are the unique singularities on $S_4$ (of type $A_1$);
2) $\varphi_{\text{min}} : S_4 \rightarrow S_4$ is the simultaneous blowing up at them;
3) $\widehat{L}_i$ are the unique lines on $S_4$.

The following theorem is an analogue of Theorem 3, hence its statements are proved in a similar way. Unfortunately, we did not find quite exact references.

Theorem 5: We have:
1) $S_4$ is the unique (up to an $\mathbb{F}_q$-isomorphism) del Pezzo surface of degree 4 toric with respect to the torus $T_4$;
2) $S_4$ is the non-split toric surface associated with the pair $(\text{Pol}_4, \Phi_4^2)$;
3) $S_4$ is the quotient $\mathcal{E} / \sigma$ under an automorphism $\sigma$ of $\mathcal{E}$ (in particular, $\sigma \in \text{PGL}(4, \mathbb{F}_q))$, whose fixed point set is $\mathcal{P}_4$;
4) $S_4'$ is the blowing up of $\mathcal{E}$ at the set $\mathcal{P}_4$ of all (i.e., four $\mathbb{F}_q$-conjugate) $T_4$-invariant points.

From [1, Theorem 14] or one of Statements 3, 4 of Theorem 5 it follows that the Picard $\mathbb{F}_q$-number of $S_4$ is equal to 1. Since the Fano index of $S_4$ is also 1, we obtain

Lemma 8: The Picard $\mathbb{F}_q$-group of the surface $S_4$ equals
\[ \text{Pic}(S_4) = (-K_{S_4}) \simeq \mathbb{Z} \]

It is well known that besides $T_4$ the surface $\mathcal{E}$ is toric for the torus $T_{2, \sigma}$ (from [1, Theorem 8]). Let $M_i$ be the lines outside $T_{2, \sigma}$ and $R_i$ be their intersection points. The blowing up of $\mathcal{E}$ at the $\mathbb{F}_q$-point $R_0$ (or $R_2$) gives the nonsingular del Pezzo surface $D_7$ of degree 7, which is also the blowing up of $\mathbb{P}_2^2$ at a pair $Q_2 = \{ Q_1, Q_2 \}$ of $\mathbb{F}_q$-conjugate points. Thus we have the diagram
\[ S_4 \xleftarrow{\varphi_{\text{min}}^b} L_4 \xrightarrow{\text{bl}(P_4)} \mathcal{E} \xleftarrow{D_7} \mathbb{P}_2^2, \]
where $\text{bl}(P_4)$, $\text{bl}(R_0)$, $\text{bl}(Q_2)$ are the corresponding blowing up maps. Besides, let
\[ \chi := \text{bl}(P_4) \circ \varphi_{\text{min}}^{-1}, \quad \psi := \text{bl}(Q_2) \circ \varphi_{\text{min}}^{-1}, \quad \varphi := \psi \circ \chi \]
Further,
\[ \bar{M}_i := \chi^*(M_i), \quad \bar{M}_2 := \bar{M}_1 + \bar{M}_2, \quad L_i := \psi_s(L_i), \quad L_4 := \sum_{i=0}^3 L_i, \]
Finally, $L$ is the line through the points $Q_j \psi(M_j)$ and also we identify $P_i$ with $\psi(P_i)$. For more clarity on what is going on, see Figures 4, 5, where arrows denote the Frobenius action.

Repeating the arguments used for the proof of Corollary 1, we obtain the following result. Let us not write out its proof, because it is also very technical and does not contain new ideas.

Corollary 4: The anticanonical linear system of $S_4$ equals
\[ | - K_{S_4} | = \varphi^*(L) - \bar{L}_4 - 2\bar{M}_2, \]
where
\[ L := | \bar{L}_4 - P_4 - 2Q_2 | \]
is the (incomplete) linear system of all (possibly reducible or singular) quartics $C \subset \mathbb{P}_2^2$ passing through $P_4$ and through $Q_2$ with multiplicity at least 2.

One can easily check that

Remark 5: Any $C \in L$ contains at most one absolutely irreducible $\mathbb{F}_q$-curve (of geometric genus $g \leq 1$) different from $L$.

Remark 6: Given $C \in L$, the divisor $D := \varphi^*(C) - \bar{L}_4 - 2\bar{M}_2$ is an elliptic curve if and only if $C$ is one of the following quartics:
and hence $F$

Moreover, in the first case $|\sigma^{-1}(Q)| = 2$.

**Lemma 9:** Let $E \subset \mathbb{P}^2$ be an elliptic $\mathbb{F}_q$-curve passing through $P_1, Q_2$ and $O \in E(\mathbb{F}_q)$. Then

$$P_0 - P_2 = P_1 - P_3 = Q_1 - Q_2$$

is an $\mathbb{F}_q$-point of order 2 (with respect to $O$ as the neutral element of the chord-tangent group law on $E$).

**Proof:** By definition,

$$P_0 + P_1 + Q_1 = P_1 + P_2 + Q_2 = P_2 + P_3 + Q_1 = P_3 + P_0 + Q_2.$$

Therefore

$$P_0 + P_1 = P_2 + P_3, \quad P_1 + P_2 = P_3 + P_0, \quad P_0 + Q_2 = P_2 + Q_1$$

and hence

$$P_0 - P_2 = P_3 - P_1 = P_2 - P_0 = Q_2 - Q_1.$$

This is an $\mathbb{F}_q$-point, because $Q_1, Q_2$ are $\mathbb{F}_q$-conjugate.

A quartic $C \in \mathcal{L}$ from Remark 6.2 gives a geometric interpretation of the group law on the elliptic curve $D$. Note that $C$ is similar to a (twisted) Edwards quartic [18], because both curves have two nodes. The group law on the latter is represented in [19, §4]. An analog for $C$ is defined in the following way.

For points $R_1, R_2 \in C \setminus Q_2$ let $R_1 \cdot R_2$ be the eighth intersection point of $C$ with the unique conic passing through $R_1, R_2, P_1, Q_1, Q_2$. If $R_1 = R_2$ (resp. $R_1 = P_1$ or $R_2 = P_1$), then this conic intersects $C$ at $R_1$ (resp. $P_1$) with the intersection number at least 2 (3 if $R_1 = R_2 = P_1$). Besides, let $R_1$ be the third intersection point of $C$ with the unique line passing through $R_1, Q_2$. The points $R_1, R_2$ and $R_3$ are correctly defined by [20, §3.3, §5.3]. Then the addition and subtraction (with $P_0$ as the neutral point) have the form

$$R_1 + R_2 := R_1 \cdot R_2, \quad -R_1 := R_1 \cdot P_3$$

respectively. This can be proved in the same way as [19, Theorem 2]. Note that sometimes $R_1 + R_2$ or $-R_1$ falls into $Q_2$. Finally, $P_2$ is obviously a point of order 2.

**Theorem 6:** For any elliptic $\mathbb{F}_q$-curve $E \in [-K_{S_1}]$ the order $|E(\mathbb{F}_q)|$ is even.

**Proof:** The result is proved by exhibiting an $\mathbb{F}_q$-point of order 2 on $E$.

By Lemma 9 it remains to only consider the case with a quartic $C \in \mathcal{L}$ from Remark 6.2. The corresponding elliptic curve $D$ has the group structure with respect to any point $O \in D(\mathbb{F}_q) \neq \emptyset$ (instead of $\varphi^{-1}(P_0)$) as the neutral element. It is well known that there is the group $\mathbb{F}_q$-isomorphism $\tau(\mathcal{P}) := P + O, \tau : D \rightarrow D$. At the same time, $D$ has a Weierstrass form $W : y^2 + h(x)y = f(x)$ defined over $\mathbb{F}_q$, where $\deg(h) \leq 1$, $\deg(f) = 3$. Let $\sigma : D \sim W$ be the corresponding $\mathbb{F}_q$-isomorphism such that $\sigma(O)$ is the point at infinity.

Consider the $\mathbb{F}_q$-point $(x_0, y_0) := (\sigma \circ \tau \circ \varphi^{-1})(P_2)$ of order 2 on $W$. For $p = 2$ it is the only such point, hence it is defined over $\mathbb{F}_q$. For $p > 3$, as is known, $y_0 = f(x_0) = 0$. If $x_0 \in \mathbb{F}_q$, then all is proved. Otherwise $f(x)$ has exactly two $\mathbb{F}_q$-irreducible factors, namely the $\mathbb{F}_q$-minimal (quadratic) polynomial of $x_0$ and $x - x_1$ for some $x_1 \in \mathbb{F}_q$. Thus $(x_1, 0) \in W(\mathbb{F}_q)[2]$.

**Corollary 5:** For $p = 2$ supersingular elliptic curves (i.e., of $j$-invariant 0) [2, §2.4.3] do not belong to $[-K_{S_1}]$.

Finally, carefully analyzing small values $q$, we get the following result.

**Corollary 6:** For any $\mathbb{F}_q$-divisor $D \in [-K_{S_1}]$ we have

$$|\text{Supp}(D)(\mathbb{F}_q)| \leq 2|N_q(1)/2|,$$

where the number $N_q(1)$ is given in Theorem 10.

**TABLE II**

| $q$ | $N_q(1)$ | elliptic $\mathbb{F}_q$-curve | $j$-invariant | is supersing. |
|-----|----------|-------------------------------|---------------|--------------|
| 2   | 5        | $y^2 + y = x^3 + x$           | 0             | yes          |
| 3   | 7        | $y^2 = x^3 + 2x + 1$          | 0             | yes          |
| 4   | 9        | $y^2 + y = x^3$               | 0             | yes          |
| 5   | 10       | $y^2 = x^3 + 3x$              | 1728          | no           |
| 7   | 13       | $y^2 = x^3 + 3$               | 0             | no           |
| 8   | 14       | $y^2 + xy + y = x^3 + 1$      | 1             | no           |
| 9   | 16       | $y^2 = x^3 + x$               | 0             | yes          |

Fig. 4. The lines $\tilde{L}_i, L \subset \mathbb{P}^2$. 

Fig. 5. The lines $L_i, M_i \subset E$. 

1) $E \cup L$, where $E \subset \mathbb{P}^2$ is an elliptic curve passing through $P_1, Q_2$.

2) An irreducible quartic for which $Q_1, Q_2$ are the unique singularities (namely nodes).
III. BCH Codes

Let us recall some notions of BCH codes over an arbitrary finite field $\mathbb{F}_q$. Let $n, d^*, b \in \mathbb{N}$, where $d^*$ is so-called designed distance. Also, let $\alpha$ be a primitive $n$-th root of unity and $\epsilon := [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$. BCH$_q(n, d^*, b)$ is a cyclic code given by the generator polynomial

$$g(x) = \text{LCM}(m_{\alpha^b}, m_{\alpha^{b+1}}, \ldots, m_{\alpha^{b+d^*-2}}),$$

where $m_{\alpha^i}$ is the $\mathbb{F}_q$-minimal polynomial of $\alpha^i$. A BCH code is said to be primitive (resp. narrow-sense) if $n = q^e - 1$ (resp. $b = 1$). The theory of BCH codes is well represented, for example, in [4, §9].

**Theorem 7** [21, Theorem 9.1.a]: For a BCH$_q(n, d^*, b)$ code we have

$$k \geq n - \epsilon(d^* - 1), \quad d \geq d^*.$$

The second inequality is called the BCH bound.

**Theorem 8** [21, Proposition 2.3.9]: Let

$$r := b - 1, \quad s := n + 1 - d^* - b,$$

$$P_0 := (0 : 1), \quad P_\infty := (1 : 0).$$

A BCH$_q(n, d^*, b)$ code is obtained by the successive puncturing of the split toric code $\mathcal{C}_q^r(\mathbb{P}^1, \mathbb{G}_m, rP_0 + sP_\infty)$ (see the notation in [1, §3.1]) at the coordinate set $\sqrt{\mathbb{F}}_q$ and the restriction to $\mathbb{F}_q$ (or in another order).

**Corollary 7**: A primitive narrow-sense code BCH$_q(q^e - 1, d^*, 1)$ is the restriction to $\mathbb{F}_q$ of the Reed–Solomon $\mathbb{F}_q$-code of length $q^e - 1$ and dimension $q^e - d^*$.

IV. Codes Associated With the “Symmetric” Polygons

Next we will need the following facts.

**Theorem 9** (Griesmer Bound [2, Theorem 1.143]): For any linear $[n, k, d]_q$ code we have

$$\delta := n - \sum_{i=0}^{k-1} \left\lfloor \frac{d}{q^i} \right\rfloor \geq 0.$$

**Theorem 10** [2, Theorem 3.4.49]: The maximal possible number of $\mathbb{F}_q$-points on an elliptic $\mathbb{F}_q$-curve equals

$$N_q(1) = \begin{cases} q + [2\sqrt{q}] & \text{if } \sqrt{q} \not\in \mathbb{N}, \ p < q, \ & p \mid [2\sqrt{q}], \\ q + [2\sqrt{q}] + 1 & \text{otherwise} \end{cases}.$$

For small $q$ Table II (the original source is [22]) contains Weierstrass forms of $\mathbb{F}_q$-optimal elliptic curves, i.e., having $N_q(1)$ points over $\mathbb{F}_q$. According to [23, Theorem 4.6], Table I these curves are unique (up to $\mathbb{F}_q$-isomorphism) among $\mathbb{F}_q$-optimal. The last column of the table is filled by [23, Proposition 3.6.iv].

For $i \in \{3, 4, 6, 8, 9\}$ by $C_i$ we will denote the non-split toric $\mathbb{F}_q$-code associated with the polygon $Pol_i$ from Figure 1. In other words, $C_i$ are anticanonical codes on the non-split toric del Pezzo $\mathbb{F}_q$-surfaces from Table I. In particular, $C_9$ is equivalent to the so-called projective Reed–Muller code. The code parameters are represented in Table III (for a value $q$ satisfying the restriction). The bound on $d$ for the new codes $C_3, C_4$ follows from Corollaries 3, 6. Be careful that for very small $q$ (even if the restriction is satisfied) values of the column $\delta$ may be incorrect.

For $n, i \in \mathbb{N}$ let $\alpha \in \mathbb{F}_q$ be an element of order $n$ and $m_{\alpha^i}$ be the $\mathbb{F}_q$-minimal polynomial of $\alpha^i$. In Table IV by means of [1, Theorem 25] it is written the parity-check polynomials $h(x)$ of the codes from Table III. It is immediately checked that these codes are BCH$_q(n, d^*, b)$ ones. Finally, the column LCD answers whether a cyclic code is a linear code with complementary dual (or, equivalently, reversible) or not (details see in [24]). It is filled, looking at $h(x)$, but “yes” also follows from [1, Corollary 3] or [4, Problem 7.27]. As a result, the dual codes to $C_3, C_4$ are BCH$_q(n, n - 1)$ codes.

The output of the code [25] written in the language of the computer algebra system Magma motivates us to formulate

**Conjecture 1**: The lower bounds from Table III for the minimum distance $d$ of the codes $C_3, C_4$ are exact.

The codes $C_3, C_4$ for small $q$ are represented in Tables V, VI. The column LB$(d)$ (lower bound on $d$ for fixed $q$, $n$, $k$) is
rewritten from the Brouwer–Grassl tables [26]. Note that $C_3$ for $q = 3$ and $C_4$ for $q = 7$ (cf. [27]) have parameters that are the best known at the moment.

Remark 7: The codes $C_3$, $C_4$ can be naturally generalized, using for any $r \in \mathbb{N}$ the multiple polygons $rPol_3$, $rPol_4$ as well as it is done for $C_6$ in [1, Theorem 29]. However, in this case it seems that there are no elegant ways to quite exactly estimate the minimum distance $d$.

ACKNOWLEDGMENT

The author expresses his deep gratitude to his scientific advisor M. Tsfasman and thanks A. Perepechko, A. Trepalin, and K. Shramov for their help and useful comments.

REFERENCES

[1] D. I. Koshelev, “Non-split toric codes,” Problems Inf. Transmiss., vol. 55, no. 2, pp. 124–144, Apr. 2019.
[2] M. Tsfasman, S. Vladut, and D. Nogin, Algebraic Geometric Codes: Basic Notions (Mathematical Surveys and Monographs). Providence, RI, USA: American Mathematical Society, 2007, vol. 139.
[3] D. Cox, J. Little, and H. Schenck, Toric Varieties (Graduate Studies in Mathematics), vol. 124. Providence, RI, USA: American Mathematical Society, 2011.
[4] F. MacWilliams and N. Sloane, The Theory of Error-Correction Codes (North-Holland Mathematical Library), vol. 16. Amsterdam, The Netherlands: North Holland, 1977.
[5] D. F. Coray and M. A. Tsfasman, “Arithmetic on singular del Pezzo surfaces,” Proc. London Math. Soc., vol. 3, no. 1, pp. 25–87, Jul. 1988.
[6] R. Blache et al., “Anticanonical codes from del Pezzo surfaces with Picard rank one,” Trans. Amer. Math. Soc., vol. 373, no. 8, pp. 5371–5393, May 2020.
[7] A. Couvreur and I. Duursma, “Evaluation codes from smooth quadric surfaces and twisted Segre varieties,” Des., Codes Cryptogr., vol. 66, nos. 1–3, pp. 291–303, Jan. 2013.
[8] G. Lachaud, “The parameters of projective Reed–Muller codes,” Discrete Math., vol. 81, no. 2, pp. 217–221, Apr. 1990.
[9] M. Boguslavsky, “Sections of the del Pezzo surfaces and generalized weights,” Problems Inf. Transmiss., vol. 34, no. 1, pp. 14–24, 1998.
[10] J. Little and H. Schenck, “Codes from surfaces with small Picard number,” SIAM J. Appl. Algebra Geometry, vol. 2, no. 2, pp. 242–258, Jan. 2018.
[11] M. Zarrar, “Error-correcting codes on low rank surfaces,” Finite Fields Appl., vol. 13, no. 4, pp. 727–737, Nov. 2007.
[12] U. Derenthal, “Singular del Pezzo surfaces whose universal torsors are hypersurfaces,” Proc. London Math. Soc., vol. 108, no. 3, pp. 638–681, Mar. 2014.
[13] V. Batyrev and Y. Tschinkel, “Rational points of bounded height on compactifications of anisotropic tori,” Int. Math. Res. Notices, vol. 1995, no. 12, pp. 591–635, 1995.
[14] A. M. Kasprzyk, “Bounds on fake weighted projective space,” Kodai Math. J., vol. 32, no. 2, pp. 197–208, Jun. 2009.
[15] R. Hartshorne, Algebraic Geometry (Graduate Texts in Mathematics), vol. 52. Berlin, Germany: Springer, 1977.
[16] J. Hirschfeld, Projective Geometries Over Finite Fields (Oxford Mathematical Monographs). Oxford, U.K.: Clarendon Press, 1998.
[17] J. Silverman, The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics), vol. 106. New York, NY, USA: Springer, 2009.
[18] D. Bernstein et al., “Twisted Edwards curves,” in Proc. Africacrypt, Casablanca, Morocco, 2008, pp. 389–405.
[19] C. Arène, T. Lange, M. Naehrig, and C. Ritzenthaler, “Faster computation of the Tate pairing,” J. Number Theory, vol. 131, no. 5, pp. 842–857, May 2011.
[20] W. Fulton, Algebraic Curves: An Introduction to Algebraic Geometry (Mathematics Lecture Note), vol. 30. Boston, MA, USA: Addison-Wesley, 1969.
[21] H. Stichtenoth, Algebraic Function Fields and Codes (Graduate Texts in Mathematics), vol. 254. Berlin, Germany: Springer, 2009.
[22] G. van der Geer, E. Howe, K. Lauter, and C. Ritzenthaler. Tables of Curves With Many Points. Accessed: Aug. 14, 2020. [Online]. Available: http://www.maths.org
[23] R. Schoof, “Nonsingular plane cubic curves over finite fields,” J. Comb. Theory A, vol. 46, no. 2, pp. 183–211, 1987.
[24] X. Yang and J. L. Massey, “The condition for a cyclic code to have a complementary dual,” Discrete Math., vol. 126, nos. 1–3, pp. 391–393, Mar. 1994.
[25] D. Koshelev. (2020). Magma Code. [Online]. Available: https://github.com/dishport/Non-split-toric-BCH-codes-on-singular-del-Pezzo-surfaces
[26] M. Grassl. Bounds on the Minimum Distance of Linear Codes and Quantum Codes. Accessed: Aug. 14, 2020. [Online]. Available: http://www.codetables.de
[27] R. Daskalov and T. Gulliver, “Bounds in minimum distance for linear codes over $GF(7)$,” J. Combinat. Math. Combinat. Comput., vol. 36, pp. 175–191, 2001.

Dmitrii Koshelev received the B.Sc. degree in information technology from Southern Federal University, Rostov-on-Don, Russia, in 2014, and the M.Sc. degree in mathematics from the Higher School of Economics, Moscow, Russia, in 2017. At the moment, he completes the Ph.D. studies in applied mathematics at the Université de Versailles Saint-Quentin-en-Yvelines (a member of Université Paris-Saclay). His research interests are various applications of algebraic geometry over finite fields to error-correcting coding theory and elliptic cryptography, including pairing-based and isogeny-based cryptography.