Biregular Cremona transformations of the plane

Shamil Asgarli   Kuan-Wen Lai   Masahiro Nakahara   Susanna Zimmermann

Abstract

We study Cremona transformations that induce bijections on the k-rational points. These form a subgroup inside the Cremona group. When k is a finite field, we study the possible permutations induced on $\mathbb{P}^2(k)$, with special attention to the case of characteristic two.

Contents

1 Introduction

We call a birational self-map of a variety a *birational permutation* if both it and its inverse are defined on all rational points of the variety. In particular, such a map induces a bijection on the set of rational points. Over a finite field, the rational points form a finite set, so such biregular maps induce permutations in the usual sense. Fixing a variety and a finite ground field, one can ask what kind of permutations on the rational points can be realized this way.

In this paper, we focus on the birational self-maps of a projective space $\mathbb{P}^n$, i.e. the *Cremona transformations*. They form a group $\mathrm{Cr}_n(k)$ where k is the ground field. We say that a

2010 Mathematics Subject Classification 14E07, 14G15, 20B30.
Keywords: birational permutations, Cremona transformations, finite fields

Cremona transformation is *biregular* if it is a birational permutation. Clearly, biregular elements form a subgroup $\mathrm{BCr}_n(k) \subset \mathrm{Cr}_n(k)$. When $k = \mathbb{F}_q$, the finite field of q elements, there is a group homomorphism

$$\sigma_q \colon \mathrm{BCr}_n(\mathbb{F}_q) \longrightarrow \mathrm{Sym}(\mathbb{P}^n(\mathbb{F}_q))$$

which maps a biregular element to the induced permutation on the set of $\mathbb{F}_q$-points. When the dimension $n = 2$, the image of σ_q satisfies

- $\mathrm{Im}(\sigma_q) = \mathrm{Sym}(\mathbb{P}^2(\mathbb{F}_q))$ if q is odd or $q = 2$.
- $\mathrm{Im}(\sigma_q)$ contains the alternating subgroup $\mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$ if $q = 2^m \geq 4$.

This result was proved by Cantat [Can09] based on a geometric construction. In this paper, we follow the same general strategy, but provide an arithmetic approach to this result which leads to more explicit formulas in Section 2.

When $q = 2^m \geq 4$, we expect that the inclusion $\mathrm{Im}(\sigma_q) \supseteq \mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$ is in fact an equality; in other words, no odd permutation can be realized from a birational permutation. We take two approaches to examine this conjecture: (1) Study properties of the group $\mathrm{BCr}_2(k)$ for a general perfect field k, including a list of generators. (2) Focus on elements in $\mathrm{BCr}_2(\mathbb{F}_q)$ that are conjugate to an automorphism of a rational surface. Our first main result is:

Theorem 1.1. *Assume that k is perfect.*

1. *Let $\mathbf{T} \subset \mathrm{Cr}_2(k)$ be the set of generators for $\mathrm{Cr}_2(k)$ given in [Isk91]. Then $\mathbf{T} \cap \mathrm{BCr}_2(k)$ forms a set of generators for $\mathrm{BCr}_2(k)$.*
2. *$\mathrm{BCr}_2(k)$ is not a finitely generated group if k admits a quadratic extension.*
3. *$\mathrm{BCr}_2(k)$ is a non-normal subgroup in $\mathrm{Cr}_2(k)$.*
4. *$\mathrm{BCr}_2(k) \subset \mathrm{Cr}_2(k)$ is of infinte index.*

A precise list of generators of $\mathrm{BCr}_2(k)$ is given in Proposition 4.4. Over $\mathbb{F}_q$ where $q = 2^m \geq 4$, all but one family of generators from the list can be shown to induce even permutations. This is primarily due to our second main result:

Theorem 1.2. *Assume that $q = 2^m \geq 4$. Then the elements of $\mathrm{BCr}_2(\mathbb{F}_q)$ belonging to the following categories induce even permutations.*

1. *Elements conjugate to automorphisms of a del Pezzo surface.*
2. *Elements conjugate to a birational self-map of a conic bundle over $\mathbb{P}^1$ preserving the fiber class.*
3. *Elements of finite order.*

Using Theorems 1.1 and Theorem 1.2, we can reduce the parity problem to a single class of birational maps. In general, a *quintic transformation* means a plane Cremona transformation defined by the linear system of quintic curves passing through six geometric points with multiplicity two. The class of birational maps for which the parity problem is still open consists of the quintic transformations with a point of degree six as base locus. In the following, we denote such a quintic transformation by f_{66}.

Corollary 1.3. *If every quintic transformation f_{66} over $\mathbb{F}_q$, where $q = 2^m \geq 4$, induces an even permutation on $\mathbb{P}^2(\mathbb{F}_q)$, then $\mathrm{Im}(\sigma_q) = \mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$.*

During this project, Lian Duan was able to write a Magma code to enumerate all possible quintic transformations f_{66} over $\mathbb{F}_4$ and $\mathbb{F}_8$, and verified that all such transformations induce even permutations on $\mathbb{F}_q$-points for $q = 4$ and $q = 8$, respectively. Combining the results of his experiment with Corollary 1.3, we deduce the following theorem.

Theorem 1.4. $\mathrm{Im}(\sigma_q) = \mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$ *for* $q = 4$ *and* $q = 8$.

The proof of Theorem 1.2 relies heavily on being able to study the parity of a birational permutation under conjugation by a birational map. For the sake of consistency, we denote the group of birational self-maps of a surface X defined over a field k as $\mathrm{Cr}_X(k)$, and denote by $\mathrm{BCr}_X(k)$ the subgroup of biregular elements. In this notation, $\mathrm{BCr}_2(k)$ defined earlier is a shorthand for $\mathrm{BCr}_{\mathbb{P}^2}(k)$. In general, we expect that the parity of a birational permutation is governed by the birational geometry of the underlying variety over $\mathbb{F}_q$ where $q = 2^m \geq 4$. In the two-dimensional case, for example, the parity of a birational permutation is invariant under the conjugation of a birational map. More precisely:

Theorem 1.5. *Let $h\colon X \dashrightarrow Y$ be a birational map between smooth projective surfaces defined over $\mathbb{F}_q$ where $q = 2^m \geq 4$. Suppose that there are $\alpha_X \in \mathrm{BCr}_X(\mathbb{F}_q)$ and $\alpha_Y \in \mathrm{BCr}_Y(\mathbb{F}_q)$ fitting into the commutative diagram*

$$\begin{tikzcd}
X \arrow[r, dashed, "\alpha_X"] \arrow[d, dashed, "h"'] & X \arrow[d, dashed, "h"] \\
Y \arrow[r, dashed, "\alpha_Y"] & Y.
\end{tikzcd}$$

Then the actions of α_X and α_Y on $X(\mathbb{F}_q)$ and $Y(\mathbb{F}_q)$, respectively, have the same parity.

This paper is organized as follows: In Section 2, we discuss the realizability of all permutations on the rational points in the plane over finite fields of odd characteristics and $\mathbb{F}_2$. Section 3 concerns the parity problem over a non-prime field of characteristic two, starting with the analysis of the parities induced by linear transformations. Afterwards, we prove Theorem 1.5, and use it to reduce the proof of Theorem 1.2 to the case of automorphisms. In Section 4, we give a list of generators of $\mathrm{BCr}_2(k)$ when k is a perfect field and prove Theorem 1.1 (1). We then analyze whether each generator induces an even permutation, and deduce Corollary 1.3. Lastly, we develop some basic properties of $\mathrm{BCr}_2(k)$ as a subgroup of $\mathrm{Cr}_2(k)$ to finish the proof of Theorem 1.1.

Acknowledgements

We thank Brendan Hassett for suggesting us the problem in the present paper. We thank Lian Duan for the computational aid with Magma. During this project, the first author was partially supported by funds from NSF Grant DMS-1701659. The third author was supported by EPSRC grant EP/R021422/2. The last author was supported by ANR Project FIBALGA ANR-18-CE40-0003-01 and Project PEPS 2019 “JC/JC”.

2 Realizing arbitrary permutations

The purpose of this section is to provide an arithmetic approach to the theorem below. One advantage of this approach is that it allows one to easily construct explicit examples of birational permutations on $\mathbb{P}^2$ via a computer algebra system.

Theorem 2.1. *Consider the canonical homomorphism*

$$\sigma_q \colon \mathrm{BCr}_2(\mathbb{F}_q) \to \mathrm{Sym}(\mathbb{P}^2(\mathbb{F}_q)).$$

Then the image of σ_q satisfies

- $\mathrm{Im}(\sigma_q) = \mathrm{Sym}(\mathbb{P}^2(\mathbb{F}_q))$ *if q is odd or $q = 2$.*
- $\mathrm{Im}(\sigma_q) \supseteq \mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$ *if $q = 2^m \geq 4$.*

Cantat's proof of Theorem 2.1 in [Can09] is built upon a property about the subgroups of $\mathrm{Sym}(\mathbb{P}^n(\mathbb{F}_q))$ which contain $\mathrm{PSL}_{n+1}(\mathbb{F}_q)$: The elements in $\mathrm{Sym}(\mathbb{P}^n(\mathbb{F}_q))$ which preserve the collinearity, i.e., map collinear points to collinear points, are called *collineations*. They form a subgroup

$$\mathrm{P\Gamma L}_n(\mathbb{F}_q) \subseteq \mathrm{Sym}(\mathbb{P}^n(\mathbb{F}_q))$$

which clearly contains $\mathrm{PSL}_{n+1}(\mathbb{F}_q)$. Recall that the alternating group

$$\mathrm{Alt}(\mathbb{P}^n(\mathbb{F}_q)) \subseteq \mathrm{Sym}(\mathbb{P}^n(\mathbb{F}_q))$$

is the subgroup of index two consisting of even permutations.

Theorem 2.2 ([Bha81, KM74, Lis75, Pog74])**.** *Let $G \subseteq \mathrm{Sym}(\mathbb{P}^n(\mathbb{F}_q))$ be a subgroup. If G contains $\mathrm{PSL}_{n+1}(\mathbb{F}_q)$, then either $G \subseteq \mathrm{P\Gamma L}_n(\mathbb{F}_q)$ or $G \supseteq \mathrm{Alt}(\mathbb{P}^n(\mathbb{F}_q))$.*

Applying this result to the image subgroup $\sigma_q(\mathrm{BCr}_2(\mathbb{F}_q))$, Cantat concluded that σ_q is surjective by constructing an element $f \in \mathrm{BCr}_2(\mathbb{F}_q)$ such that

- f does not preserve the collinearity on $\mathbb{P}^2(\mathbb{F}_q)$,
- f induces an odd permutation on $\mathbb{P}^2(\mathbb{F}_q)$.

Our main goal in this section is to exhibit the construction of f explicitly using input from the theory of primitive roots.

This section is organized as follows. In §2.1 we consider a certain quadric surface $Q \subset \mathbb{P}^3$; we construct a birational map $g : Q \dashrightarrow Q$ that preserves a conic fibration $Q \to \mathbb{P}^1$, and satisfies certain properties. In particular, in §2.2 we explain how the map g should behave on the special fiber of the conic fibration. In §2.3 we construct f from g by projecting from a point on Q, and prove Theorem 2.1 for the case of odd q. The characteristic 2 case is treated in §2.4.

2.1 Birational maps preserving the conic fibrations

We first recall the examples constructed in [Can09, §3]. Consider a smooth quadric Q and a line L in $\mathbb{P}^3$, both defined over $\mathbb{F}_q$, such that L meets Q in a pair of conjugate points over the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. The projection from L then induces a rational map $\pi_L \colon Q \dashrightarrow \mathbb{P}^1$ fibered in the conics cut out by the planes containing L. Assume further that there exists $P_0 \in \mathbb{P}^1(\mathbb{F}_q)$ over which the fiber $C_0 := \pi_L^{-1}(P_0)$ is smooth.

The hypothesis implies that every degenerate fiber defined over $\mathbb{F}_q$ is a union of lines $L_1 \neq L_2$ conjugate to each other over $\mathbb{F}_{q^2}/\mathbb{F}_q$, where the node $P := L_1 \cap L_2$ appears as the only $\mathbb{F}_q$-point. The projection from such a node then defines a birational map $\pi_P \colon Q \dashrightarrow \mathbb{P}^2$. Together with the fiber structure, we obtain the following diagram defined over $\mathbb{F}_q$:

$$\begin{tikzcd} Q \arrow[r, dashed, "\pi_P", "\sim"'] \arrow[d, dashed, "\pi_L\text{: conic fibration}"'] & \mathbb{P}^2 \\ \mathbb{P}^1 & \end{tikzcd} \tag{2.1}$$

Below are explicit examples of this which we use later:

Example 2.3. Assume that q is odd. Let $[x : y : z : w]$ be a system of homogeneous coordinates on $\mathbb{P}^3$. Choose a non-square $t \in \mathbb{F}_q \setminus \mathbb{F}_q^2$. Then the data

$$Q := \left\{x^2 - ty^2 + z^2 = w^2\right\} \subset \mathbb{P}^3, \quad L := \{z = w = 0\} \subset \mathbb{P}^3,$$

and $P := [0 : 0 : 1 : 1] \in Q$ provide an example of (2.1). Here the projection map is explicitly given by $\pi_L([x : y : z : w]) = [z : w]$, and the degenerate fiber through P is defined as $x^2 - ty^2 = 0$ on the plane with parametric equations

$$\mathbb{P}^2 \hookrightarrow \mathbb{P}^3 : [x : y : u] \mapsto [x : y : u : u].$$

For a smooth fiber, one can choose

$$C_0 := \pi_L^{-1}([0 : 1]) = \left\{x^2 - ty^2 = w^2\right\} \subset Q. \tag{2.2}$$

Example 2.4. When $q = 2^m$ for $m \geq 1$, we need another set of data as the quadric in the previous example is not smooth in characteristic 2. Following Cantat, we use the following quadric:

$$Q := \{x^2 + rxy + sy^2 + z^2 + x(z + w) + y(z + w) + zw = 0,\}$$

where $r, s \in \mathbb{F}_q$ are chosen so that the polynomial $X^2 + rX + s = 0$ has no roots in $\mathbb{F}_q$.

Cantat's construction of a desired $f \in \mathrm{BCr}_2(\mathbb{F}_q)$ can be roughly divided into two parts:

(1) Constructing a birational self-map g on Q which preserves the fiber structure, acts as a prescribed odd permutation on $C_0(\mathbb{F}_q)$, and acts as the identity on the other $\mathbb{F}_q$-fibers.

(2) Descending g down to $\mathbb{P}^2$ as $f := \pi_P \circ g \circ \pi_P^{-1}$, and showing that f induces an odd permutation on the $\mathbb{F}_q$-points and does not preserve collinearity.

Let us now construct the function g in (1) above in the case of odd characteristic. We keep the notation of Example 2.3. The process starts with constructing a suitable automorphism on a single smooth fiber over $\mathbb{F}_q$. Here we choose $\pi_L^{-1}([0 : 1]) \subset Q$, or equivalently, the conic

$$C_0 := \left\{x^2 - ty^2 = w^2\right\} \cong \mathbb{P}^1 \tag{2.3}$$

lying on the plane $\{z=0\} \subset \mathbb{P}^3$. The automorphisms we are interested in have the form

$$\mathbb{P}^2 \to \mathbb{P}^2 : [x:y:w] \mapsto [\alpha x + t\beta y : \beta x + \alpha y : w],$$

where the parameters (α, β) are points on the affine conic

$$S^\circ := \left\{\alpha^2 - t\beta^2 = 1\right\} \subset \mathbb{A}^2.$$

Note that the formula gives the identity map when $(\alpha, \beta) = (1, 0)$. In general, this induces an automorphism $g_0 \colon C_0 \xrightarrow{\sim} C_0$ as one can verify that

$$(\alpha x + t\beta y)^2 - t(\beta x + \alpha y)^2 = x^2 - ty^2 = w^2. \tag{2.4}$$

In the following, we develop a method in extending such automorphisms to the whole quadric Q as a birational map. Moreover, the extensions would fix the $\mathbb{F}_q$-points not lying on C_0. In §2.2, we show the existence of automorphisms f_0 which induce odd permutations on $C_0(\mathbb{F}_q)$. Hence such extensions induce odd permutations on $Q(\mathbb{F}_q)$. The method is built upon the following lemma about interpolations. We only need the case $n = 1$ for our purposes; we present the proof of the general case as it is not any harder.

Lemma 2.5. *Let $\mathbb{F}_q$ be a finite field. Fix any $P_0 \in \mathbb{P}^n(\mathbb{F}_q)$ and $P_1, P_2 \in \mathbb{P}^1(\mathbb{F}_q)$ such that $P_1 \neq P_2$. There exists a rational map $h \colon \mathbb{P}^n \dashrightarrow \mathbb{P}^1$ defined over $\mathbb{F}_q$ such that*

- *$h(P_0) = P_1$,*
- *$h(P) = P_2$ for all $P \in \mathbb{P}^n(\mathbb{F}_q) \setminus \{P_0\}$.*

Proof. We use an argument inspired by partition of unity. We first show that given $P_0 \in \mathbb{F}_q^{n+1} \setminus \{0\}$, there exists a homogeneous polynomial $f_{P_0} \in \mathbb{F}_q[x_0, ..., x_n]$ such that for each $P \in \mathbb{F}_q^{n+1} \setminus \{0\}$,

$$f_{P_0}(P) = \begin{cases} 1 & \text{if } P = \lambda P_0 \text{ for } \lambda \in \mathbb{F}_q^* \\ 0 & \text{otherwise} \end{cases}$$

Indeed, after applying a $\mathrm{GL}_{n+1}(\mathbb{F}_q)$-action, we may assume that $P_0 = (1, 0, ..., 0)$, in which case the polynomial

$$f_{P_0} = x_0^{q-1} \prod_{i=1}^{n} (x_0^{q-1} - x_i^{q-1})$$

satisfies the desired property. Next, consider

$$f := \frac{1}{q-1} \sum_{P \in \mathbb{F}_q^{n+1}} f_P \in \mathbb{F}_q[x_0, ..., x_n].$$

By construction, $f(P) = 1$ for each $P \in \mathbb{F}_q^{n+1} \setminus \{0\}$. In order to prove the lemma, write $P_1 = [\alpha : \beta]$, $P_2 = [\gamma : \delta]$, and lift $P_0 \in \mathbb{P}^n(\mathbb{F}_q)$ to $\tilde{P}_0 \in \mathbb{F}_q^{n+1}$. Consider $h : \mathbb{P}^n \dashrightarrow \mathbb{P}^1$ defined by,

$$h(P) = [\gamma f(P) + (\alpha - \gamma) f_{\tilde{P}_0}(P) : \delta f(P) + (\beta - \delta) f_{\tilde{P}_0}(P)].$$

The map h is well-defined, and has the desired interpolation property. □

We continue working with the notation retained from Example 2.3. In particular, the quadric $Q \subset \mathbb{P}^3$ is defined by the $x^2 - ty^2 + z^2 = w^2$ where $t \in \mathbb{F}_q \setminus \mathbb{F}_q^2$ is a non-square element. Similarly, recall the definitions of the plane conic C_0 and the affine conic S° from the beginning of §2.1.

Proposition 2.6. *For every $(\alpha_0, \beta_0) \in S^\circ(\mathbb{F}_q)$, the automorphism*

$$g_0 \colon C_0 \xrightarrow{\sim} C_0 : [x : y : w] \mapsto [\alpha_0 x + t\beta_0 y : \beta_0 x + \alpha_0 y : w].$$

extends to a birational self-map $g \colon Q \dashrightarrow Q$ which preserves the fibration $\pi_L \colon Q \dashrightarrow \mathbb{P}^1$ and satisfies

- $g|_{C_0} = g_0$,
- $g|_C = \mathrm{id}$ *for all $\mathbb{F}_q$-fibers $C \neq C_0$ of π_L.*

Proof. Let ζ be an affine coordinate on $\mathbb{P}^1$. We identify S° as an open subset of $\mathbb{P}^1$ via the stereographic projection from $(-1, 0) \in S^\circ$:

$$S^\circ \hookrightarrow \mathbb{P}^1 : (\alpha, \beta) \mapsto \zeta = \frac{\beta}{1 + \alpha}.$$

Let $\zeta_0 \in \mathbb{P}^1$ denote the image of $(\alpha_0, \beta_0) \in S^\circ$ under the map. Note that $(1, 0) \in S^\circ$ is mapped to $0 \in \mathbb{P}^1$. Note also that we can recover α and β by

$$\alpha = \frac{1 + t\zeta^2}{1 - t\zeta^2}, \quad \beta = \frac{2\zeta}{1 - t\zeta^2}. \tag{2.5}$$

Consider the fibration $\pi_L \colon Q \dashrightarrow \mathbb{P}^1$, and let

$$P_0 := [0 : 1] = \pi_L(C_0) \in \mathbb{P}^1.$$

By Lemma 2.5, there exists a rational function

$$\zeta = h(z, w) \in \mathbb{F}_q(\mathbb{P}^1)$$

such that $h(P_0) = \zeta_0$ and $h(P) = 0$ for all $P \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{P_0\}$. Substituting it into (2.5), we obtain two rational functions

$$\alpha(z, w) = \frac{1 + th(z, w)^2}{1 - th(z, w)^2}, \quad \beta(z, w) = \frac{2h(z, w)}{1 - th(z, w)^2},$$

which determine a birational self-map on Q via the inhomogeneous formula:

$$g \colon Q \dashrightarrow Q : [x : y : z : w] \mapsto [\alpha x + t\beta y : \beta x + \alpha y : z : w].$$

Note that this is well-defined due to the same computation as (2.4). From the construction, we have

- $(\alpha(P_0), \beta(P_0)) = (\alpha_0, \beta_0)$,
- $(\alpha(P), \beta(P)) = (1, 0)$ for all $P \in \mathbb{P}^1 \setminus \{P_0\}$,

where the first one implies that $g|_{C_0} = g_0$, and the second one implies that $g|_C = \mathrm{id}$ for all $\mathbb{F}_q$-fibers $C \neq C_0$. □

2.2 Special actions on the smooth fiber

We continue to use the notation in Example 2.3. Note that, as $C_0 \cong \mathbb{P}^1$, it is straightforward to find an automorphism on C_0 which induces an odd permutation of the $\mathbb{F}_q$-points. However, it is not obvious that every such automorphism can be extended to Q in a way which allows one to control the induced permutation on the other $\mathbb{F}_q$-points. Here we consider automorphisms of the form

$$g_0 \colon C_0 \xrightarrow{\sim} C_0 : [x : y : w] \mapsto [\alpha x + t\beta y : \beta x + \alpha y : \gamma w] \tag{2.6}$$

where $[\alpha : \beta : \gamma] \in \mathbb{P}^2$ is any $\mathbb{F}_q$-point on the conic

$$S := \{\alpha^2 - t\beta^2 = \gamma^2\} \subset \mathbb{P}^2.$$

Note that every $\mathbb{F}_q$-point on S has $\gamma \neq 0$ since $t \in \mathbb{F}_q$ is a non-square. Due to this fact, we will assume that $\gamma = 1$ in the following for the convenience of computations.

To find such an automorphism which acts on $C_0(\mathbb{F}_q)$ transitively, we use the fact that $\mathbb{F}_{q^2} \cong \mathbb{F}_q \oplus \sqrt{t^{-1}}\mathbb{F}_q$ and view $C_0 \cong \mathbb{P}^1$ as the projectivization

$$C_0 \cong \mathbb{P}(\mathbb{F}_q \oplus \sqrt{t^{-1}}\mathbb{F}_q) \cong \mathbb{P}(\mathbb{F}_{q^2}).$$

Lemma 2.7. *Under a suitable choice of the isomorphism $C_0 \cong \mathbb{P}(\mathbb{F}_{q^2})$, the action of g_0 can be obtained as the multiplication on $\mathbb{F}_{q^2}$ by the element*

$$\beta + (\alpha - 1)\sqrt{t^{-1}} \in \mathbb{F}_{q^2} \tag{2.7}$$

where $\alpha, \beta \in \mathbb{F}_q$ satisfy $\alpha^2 - t\beta^2 = 1$.

Proof. It is easy to see that the statement holds when g_0 is the identity, i.e. $\alpha = 1$, so we assume that $\alpha \neq 1$ below.

First we identify C_0 with $\mathbb{P}^1$ using the stereographic projection from $[-1 : 0 : 1] \in C_0$. On the affine chart $w = 1$, this map can be defined as

$$\theta \colon C_0 \xrightarrow{\sim} \mathbb{P}^1 : (x, y) \mapsto \zeta = \frac{y}{1 + x}$$

where ζ is an affine coordinate on $\mathbb{P}^1$. Its inverse $\theta^{-1} \colon \mathbb{P}^1 \xrightarrow{\sim} C_0$ is

$$x = \frac{1 + t\zeta^2}{1 - t\zeta^2}, \quad y = \frac{2\zeta}{1 - t\zeta^2}.$$

We claim that $g_\theta := \theta \circ g_0 \circ \theta^{-1} \colon \mathbb{P}^1 \xrightarrow{\sim} \mathbb{P}^1$ is given by the formula

$$g_\theta(\zeta) = \frac{\beta\zeta + t^{-1}(\alpha - 1)}{(\alpha - 1)\zeta + \beta}. \tag{2.8}$$

Indeed, as $g_0(x, y) = (\alpha x + t\beta y, \beta x + \alpha y)$ in the affine coordinates, a straightforward computation shows that

$$g_\theta(\zeta) = \frac{\beta x(\zeta) + \alpha y(\zeta)}{1 + \alpha x(\zeta) + t\beta y(\zeta)} = \frac{\beta\left(\frac{1+t\zeta^2}{1-t\zeta^2}\right) + \alpha\left(\frac{2\zeta}{1-t\zeta^2}\right)}{1 + \alpha\left(\frac{1+t\zeta^2}{1-t\zeta^2}\right) + t\beta\left(\frac{2\zeta}{1-t\zeta^2}\right)}$$

$$= \frac{\beta(1 + t\zeta^2) + \alpha(2\zeta)}{(1 - t\zeta^2) + \alpha(1 + t\zeta^2) + t\beta(2\zeta)} = \frac{t\beta\zeta^2 + 2\alpha\zeta + \beta}{t(\alpha - 1)\zeta^2 + 2t\beta\zeta + (\alpha + 1)}.$$

Using the quadratic formula and the fact that $\alpha^2 - t\beta^2 = 1$, the numerator and the denominator can be decomposed into linear terms:

$$g_\theta(\zeta) = \frac{t\beta(\zeta + \frac{\alpha-1}{t\beta})(\zeta + \frac{\alpha+1}{t\beta})}{t(\alpha-1)(\zeta + \frac{\alpha+1}{t\beta})^2} = \frac{t\beta(\zeta + \frac{\alpha-1}{t\beta})}{t(\alpha-1)(\zeta + \frac{\alpha+1}{t\beta})}$$

which can be further simplified as

$$g_\theta(\zeta) = \frac{t\beta\zeta + (\alpha-1)}{t(\alpha-1)\zeta + \frac{(\alpha^2-1)}{\beta}} = \frac{t\beta\zeta + (\alpha-1)}{t(\alpha-1)\zeta + t\beta} = \frac{\beta\zeta + t^{-1}(\alpha-1)}{(\alpha-1)\zeta + \beta},$$

as claimed.

In view of (2.8) and the isomorphism $\mathbb{P}^1 \cong \mathbb{P}(\mathbb{F}_q \oplus \sqrt{t^{-1}}\mathbb{F}_q)$, we can conclude that

$$g_\theta = \begin{pmatrix} \beta & t^{-1}(\alpha-1) \\ \alpha-1 & \beta \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q).$$

It's easy to verify that this matrix acts on $\mathbb{F}_{q^2} \cong \mathbb{F}_q \oplus \sqrt{t^{-1}}\mathbb{F}_q$ as the multiplication by $\beta + (\alpha-1)\sqrt{t^{-1}}$, which completes the proof. □

As a consequence of the lemma, to find an automorphism as (2.6) which acts on $C_0(\mathbb{F}_q)$ transitively, it is sufficient to find a primitive root of $\mathbb{F}_{q^2}$ of the form (2.7). To attain this, we use the following result by S. D. Cohen:

Theorem 2.8 ([Coh83, Theorem 1.1])**.** *Let $\{\theta_1, \theta_2\}$ be a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and let a_1 be a nonzero member of $\mathbb{F}_q$. Then there exists a primitive root of $\mathbb{F}_{q^2}$ of the form $a_1\theta_1 + a_2\theta_2$ for some $a_2 \in \mathbb{F}_q$.*

Corollary 2.9. *There exists a primitive root of $\mathbb{F}_{q^2}$ of the form*

$$\beta + (\alpha-1)\sqrt{t^{-1}} \in \mathbb{F}_{q^2}^*$$

where $\alpha, \beta \in \mathbb{F}_q$ satisfy $\alpha^2 - t\beta^2 = 1$.

Proof. By applying Theorem 2.8 to the basis $\left\{1, \sqrt{t^{-1}}\right\}$, we find $c \in \mathbb{F}_q$ such that

$$\xi := c - \frac{t}{2}\sqrt{t^{-1}} \in \mathbb{F}_{q^2}$$

is a primitive root of $\mathbb{F}_{q^2}$. We claim that ξ^{-1} can be expressed as the required form. If we write $\xi^{-1} = \beta + (\alpha-1)\sqrt{t^{-1}}$, then

$$\xi = \frac{\beta}{\beta^2 - t^{-1}(\alpha-1)^2} - \frac{\alpha-1}{\beta^2 - t^{-1}(\alpha-1)^2}\sqrt{t^{-1}}.$$

Equating the coefficients of $\sqrt{t^{-1}}$ in the two expressions for ξ:

$$\frac{t}{2} = \frac{\alpha-1}{\beta^2 - t^{-1}(\alpha-1)^2}$$

which implies that

$$(\alpha-1)^2 - t\beta^2 = -2(\alpha-1) \Rightarrow \alpha^2 - t\beta^2 = 1,$$

as required. □

2.3 The induced actions on the projective plane

We are ready to establish Theorem 2.1 when q is odd. Note that Proposition 2.6 and Corollary 2.9 imply the existence of a birational self-map $g\colon Q \dashrightarrow Q$ acting transitively on the $\mathbb{F}_q$-points of a smooth fiber C_0, and leaves all the other $\mathbb{F}_q$-fibers fixed. The maps we constructed have the form:

$$g\colon Q \dashrightarrow Q : [x : y : z : w] \mapsto [\alpha x + t\beta y : \beta x + \alpha y : \gamma z : \gamma w]$$

where α, β, γ are homogeneous in z, w and satisfy $\alpha^2 - t\beta^2 = \gamma^2$.

Recall that Q and L are defined as

$$Q := \left\{x^2 - ty^2 + z^2 = w^2\right\} \subset \mathbb{P}^3, \quad L := \{z = w = 0\} \subset \mathbb{P}^3,$$

and we have picked $P = [0 : 0 : 1 : 1] \in Q$ as the node of one of the degenerate fibers in the fibration $\pi_L\colon Q \dashrightarrow \mathbb{P}^1$. Moreover, the conic $\pi_L^{-1}([0 : 1]) = \{z = 0\} \cap Q$ is smooth by hypothesis. We identify $H := \{z = 0\}$ with $\mathbb{P}^2$ via the identification $[x : y : u] \mapsto [x : y : 0 : u]$. Projection from P onto $H = \mathbb{P}^2$ defines a birational map

$$\pi_P\colon Q \dashrightarrow \mathbb{P}^2 : [x : y : z : w] \mapsto [x : y : w - z].$$

The inverse is given by:

$$\begin{aligned} &\pi_P^{-1}\colon \mathbb{P}^2 \dashrightarrow Q \\ &[x : y : u] \mapsto [2ux : 2uy : x^2 - ty^2 - u^2 : x^2 - ty^2 + u^2]. \end{aligned}$$

After composing the three maps, we get

$$f := \pi_P \circ g \circ \pi_P^{-1}\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$$

Proposition 2.10. *The induced map $f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ satisfies the following conditions:*

(1) $f \in \mathrm{BCr}_2(\mathbb{F}_q)$

(2) *f fixes all the $\mathbb{F}_q$-points away from the conic C_0.*

(3) *f transivitely permutes $C_0(\mathbb{F}_q)$ as a $(q + 1)$-cycle.*

(4) *There exists a triple of collinear points $P_1, P_2, P_3 \in \mathbb{P}^2(\mathbb{F}_q)$ such that $f(P_1), f(P_2), f(P_3)$ are not collinear.*

In particular, the induced permutation $\mathbb{P}^2(\mathbb{F}_q) \xrightarrow{f} \mathbb{P}^2(\mathbb{F}_q)$ does not preserve collineation, and moreover, induces a $(q + 1)$-cycle, and hence has odd sign as q is odd.

Proof. (1). We have the following commutative diagram:

$$\begin{tikzcd}
& \mathrm{Bl}_P Q \arrow[r, dashed, "\tilde{g}"] \arrow[dl, "\tilde{\pi}_P"'] \arrow[d] & \mathrm{Bl}_P Q \arrow[d] \arrow[dr, "\tilde{\pi}_P"] & \\
\mathbb{P}^2 \arrow[ur, dashed, bend left, "f_1"] \arrow[r, dashed, "\pi_P^{-1}"'] & Q \arrow[r, dashed, "g"'] & Q \arrow[r, dashed, "\pi_P"'] & \mathbb{P}^2
\end{tikzcd}$$

Note that the above diagram factorizes $f = \pi_P \circ g \circ \pi_P^{-1}$ as $f = \tilde{\pi}_P \circ \tilde{g} \circ f_1$. The two lines passing through P in Q become disjoint (-1)-curves on $\mathrm{Bl}_P Q$. The morphism $\tilde{\pi}_P$ is then the blow down of these two lines. Hence $\tilde{\pi}_P$ and f_1 are both defined at all the $\mathbb{F}_q$-points. It suffices to show that $\tilde{g}$ induces a bijection on the $\mathbb{F}_q$-points of $\mathrm{Bl}_P Q$. Indeed, this follows from the fact that g induces a bijection on $Q(\mathbb{F}_q)$ and fixes the blown up point P. It follows that f is defined on all $\mathbb{F}_q$-points of $\mathbb{P}^2$. By symmetry, the same argument applies to f^{-1}, and hence $f \in \mathrm{BCr}_2(\mathbb{F}_q)$.

(2). Let $A \in \mathbb{P}^2(\mathbb{F}_q) \setminus C_0(\mathbb{F}_q)$. In particular, $A \notin L$ as $L \cap C_0$ consists of two $\mathbb{F}_{q^2}$-points that are Galois conjugates. Then $\pi_P^{-1}(A) \in Q$ such that $A \notin \pi_L^{-1}([0:1]) = C_0$, and so $g(\pi_P^{-1}(A)) = \pi_P^{-1}(A)$. It follows that $f(A) = \pi_P \circ g \circ \pi_P^{-1}(A) = A$.

(3). Let $A \in C_0(\mathbb{F}_q)$. Then $\pi_P^{-1}(A) = A$ because the line joining A and P meets the quadric at $A \in Q$. Since g permutes the points of $C_0(\mathbb{F}_q)$ as a $(q+1)$-cycle, so does the map $f = \pi_P \circ g \circ \pi_P^{-1}$.

(4). Take an $\mathbb{F}_q$-point P which lies on C, and consider the tangent line $L = T_P C \subseteq \mathbb{P}^2$. Then $L \cap C = \{P\}$. The map acts as identity on all the $\mathbb{F}_q$-points of L except for P, and sends P to another point on C which does not lie on L. Consequently, the map does not preserve collinearity. □

By combining Theorem 2.2 and Proposition 2.10, we obtain Theorem 2.1 when q is odd.

2.4 The construction in characteristic two

The goal of this section is to prove Theorem 2.1 in the case $q = 2$, and show that the image of σ_q contains $\mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$ for $q = 2^m$ where $m \geq 2$. The strategy is the same as the case when q is odd.

We first explain the construction over $\mathbb{F}_2$. Consider the quadric surface given by

$$Q := \left\{x^2 + xy + y^2 + z^2 + x(z+w) + y(z+w) + zw = 0\right\} \subset \mathbb{P}^3,$$

As before, let $L := \{z = w = 0\} \subset \mathbb{P}^3$. We consider the projection $\mathbb{P}^3 \dashrightarrow \mathbb{P}^1$, given by $[x, y, z, w] \mapsto [z, w]$. Restricting the map to Q, we get a conic bundle $\pi_L : Q \to \mathbb{P}^1$. We analyze the conics on the three $\mathbb{F}_2$-fibers:

$$\begin{aligned}
C_0 &:= \pi_L^{-1}([0,1]) = \{[x,y,u] : x^2 + xy + y^2 + xu + yu = 0\} \\
C_1 &:= \pi_L^{-1}([1,0]) = \{[x,y,u] : x^2 + xy + y^2 + z^2 + xz + yz = 0\} \\
C_2 &:= \pi_L^{-1}([1,1]) = \{[x,y,u] : x^2 + xy + y^2 = 0]\}
\end{aligned}$$

One can check that C_0 is smooth, while C_1 and C_2 are both union of two $\mathbb{F}_4$-lines meeting at a single $\mathbb{F}_2$-point. In fact,

$$\begin{aligned}
C_0(\mathbb{F}_2) &= \{[0,0,1], [1,0,1], [0,1,1]\} \\
C_1(\mathbb{F}_2) &= \{[1,1,1]\} \\
C_2(\mathbb{F}_2) &= \{[0,0,1]\}
\end{aligned}$$

Consider the map $g : \mathbb{P}^3 \to \mathbb{P}^3$, given by $[x : y : z : w] \mapsto [y : x : z : w]$. By the symmetry of the defining equation, the quadric Q is preserved under g. It is also evident that g acts as a single transposition on $C_0(\mathbb{F}_2)$, and trivially on both $C_1(\mathbb{F}_2)$ and $C_2(\mathbb{F}_2)$. Using the same argument given in Proposition 2.10, we see that the induced map $f = \pi_P \circ g \circ \pi_P^{-1}$ is an element of $\mathrm{BCr}_2(\mathbb{F}_2)$. Furthermore, the induced permutation $f : \mathbb{P}^2(\mathbb{F}_2) \to \mathbb{P}^2(\mathbb{F}_2)$ is odd, as it transitively permutes the three points of $C_0(\mathbb{F}_q)$. It also does not preserve collineation for the same reason explained in Proposition 2.10 (4). By Theorem 2.2, $\sigma_2(\mathrm{BCr}_2(\mathbb{F}_2)) = \mathrm{Sym}(\mathbb{P}^2(\mathbb{F}_2))$.

For $q = 2^n$, we use the quadric Q given in Example 2.4:

$$Q := \{x^2 + rxy + sy^2 + z^2 + x(z + w) + y(z + w) + zw = 0\}$$

where $r, s \in \mathbb{F}_q$ are chosen so that the polynomial $X^2 + rX + s = 0$ has no roots in the field $\mathbb{F}_q$. The map $g : \mathbb{P}^3 \to \mathbb{P}^3$, given by $[x : y : z : w] \mapsto [y : x : z : w]$ preserves the quadric. It can be checked that the fiber $C_0 := \pi_L^{-1}([0 : 1])$ is a smooth conic. Using the same argument in Proposition 2.10, we see that the induced map $f = \pi_P \circ g \circ \pi_P^{-1}$ is an element of $\mathrm{BCr}_2(\mathbb{F}_q)$. Moreover, the induced permutation $f : \mathbb{P}^2(\mathbb{F}_q) \to \mathbb{P}^2(\mathbb{F}_q)$ does not preserve collineation by the same argument given in Proposition 2.10 (4) that involves looking at the tangent line: f fixes all the $\mathbb{F}_q$-points on the tangent line $T_P C$ except for P, while P is sent by f to another $\mathbb{F}_q$-point away from $T_P C$. By Theorem 2.2, we deduce that $\sigma_q(\mathrm{BCr}_2(\mathbb{F}_q)) \supseteq \mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$.

3 The parity problem in characteristic two

We assume that $k = \mathbb{F}_q$ where $q = 2^m \geq 4$ throughout this section. Our goal is to prove Theorem 1.2, which states that an element of $\mathrm{BCr}_2(\mathbb{F}_q)$ induces an even permutation if it belongs to one of the following categories.

(1) Elements conjugate to automorphisms of a del Pezzo surface.

(2) Elements conjugate to a birational self-map of a conic bundle over $\mathbb{P}^1$ preserving the fiber class.

(3) Elements of finite order.

In §3.1, we prove some preliminary results, including showing that any linear transformation on $\mathbb{P}^n$ induces an even permutation on the $\mathbb{F}_q$-points for any n. We also show that this is false for $\mathbb{F}_2$. We then prove Theorem 1.5 in §3.2 that implies the parity of a birational permutation is invariant under conjugation. This reduces the proof of first two items of Theorem 1.2 to just proving that any automorphism on either a conic bundle over $\mathbb{P}^1$ or a rational del Pezzo surface induces an even permutation on its k-points. We treat the case of conic bundles in §3.3 and of del Pezzo surfaces in §3.4. In §3.2.2, we show that the third item of Theorem 1.2 follows from the first two. We give the proof of Theorem 1.2 in §3.5.

3.1 Parities induced by linear transformations

In this section, we study the parities induced by linear automorphisms. Since the proof is easily adapted to $\mathbb{P}^n$ for any $n > 0$, including the plane, we work with projective spaces of arbitrary dimension. The results of this section also allows us to study the parity problem without choosing specific coordinates for $\mathbb{P}^n$.

3.1.1 Automorphisms of projective spaces

According to Waterhouse [Wat89], the group $\mathrm{GL}_{n+1}(\mathbb{F}_q)$ is generated by two elements A_n and B_n for all q and $n \geq 1$, which clearly descend to generators for $\mathrm{PGL}_{n+1}(\mathbb{F}_q)$. Therefore, to prove that $\mathrm{PGL}_{n+1}(\mathbb{F}_q) \subseteq \mathrm{Alt}(\mathbb{P}^n(\mathbb{F}_q))$, it is sufficient to verify that A_n and B_n induce even permutations.

The general formulas for A_n and B_n depend on whether $n = 1$ or $n \geq 2$. Let us denote by I_{n+1} the identity matrix of size $n+1$, and $E_{i,j}$ the square matrix of size $n+1$ with 1 at the (i,j)-th entry and zeros elsewhere. In the case $n \geq 2$, we can choose a generator α for the multiplicative group $\mathbb{F}_q^*$, and let

$$\begin{aligned} A_n &= I_{n+1} + (\alpha - 1)E_{2,2} + E_{n+1,1}, \\ B_n &= E_{1,2} + E_{2,3} + \cdots + E_{n+1,1}. \end{aligned}$$

For example, when $n = 2$ we get

$$A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

In the case $q > 2$ and $n = 1$, we choose a generator β for the multiplicative group $\mathbb{F}_{q^2}^*$, and define

$$\alpha := \beta^{q+1}, \quad s := \mathrm{Tr}(\beta) = \beta + \beta^q, \quad r := -\mathrm{Norm}(\beta) = -\beta^{q+1},$$

then we let

$$A_1 = \begin{pmatrix} 0 & r \\ 1 & s \end{pmatrix}, \quad B_1 = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}.$$

We emphasize that the case $q = 2$, $n = 1$ is not covered by the formulas above. In this last case, $\mathrm{GL}_2(\mathbb{F}_2)$ is generated by $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ which act respectively as a 3-cycle and a 2-cycle on $\mathbb{P}^1(\mathbb{F}_2)$.

Lemma 3.1. *Both A_1 and B_1 induce even permutations on $\mathbb{P}^1(\mathbb{F}_q)$ where $q = 2^m \geq 4$.*

Proof. The element α is a generator of $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$, so B_1 fixes $[1:0]$ and $[0:1]$ and acts as an $(q-1)$-cycle on

$$\mathbb{P}^1(\mathbb{F}_q) \setminus \{[1:0] \cup [0:1]\} \cong \mathbb{F}_q^*,$$

which is even for all $q = 2^m \geq 2$. On the other hand, A_1 can be decomposed into

$$\begin{pmatrix} 0 & r \\ 1 & s \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} =: A_{11}A_{12}A_{13}.$$

Among the factors:

- A_{11} has the same parity as B_1 since $r = -\alpha = \alpha$.
- A_{12} fixes $[0:1]$ and acts on $\mathbb{P}^1(\mathbb{F}_q) \setminus \{[0:1]\} \cong \mathbb{F}_q$ as a translation by s, which is a composition of $q/2$ transpositions (because $\mathrm{char}(k) = 2$) and thus even for $q = 2^m \geq 4$.
- A_{13} is an involution fixing $[1:1]$, so it is a composition of $q/2$ transpositions which is even for $q = 2^m \geq 4$.

As a result, A_1 acts as a compositions of three permutations which are all even, so A_1 is even. □

Lemma 3.2. *Assume that $n \geq 2$ and $q = 2^m \geq 2$. Then A_n induces an even permutation on $\mathbb{P}^n(\mathbb{F}_q)$.*

Proof. One can directly verify that $A_n = T_n M_n$ where

$$T_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 1 \end{pmatrix}, \quad M_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \alpha & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

It is sufficient to prove that both T_n and M_n induce even permutations. Note that M_n has order $q-1$ which is odd, so its action is even. Hence only T_n needs to be analyzed.

First, by writing $T_n = I_{n+1} + E_{n+1,1}$, we have

$$T_n^2 = I_{n+1} + 2E_{n+1,1} + E_{n+1,1}^2 = I_{n+1},$$

so T_n is an involution. Thus its action on $\mathbb{P}^n(\mathbb{F}_q)$ is a product of disjoint transpositions. Second, T_n acts on the homogeneous coordinates as

$$[x_0 : x_1 : ... : x_n] \mapsto [x_0 : ... : x_{n-1} : x_0 + x_n],$$

so the fixed locus is exactly the hyperplane $\{x_0 = 0\}$. Therefore, the number of transpositions in T_n is

$$\frac{1}{2}\left(|\mathbb{P}^n(\mathbb{F}_q)| - |\mathbb{P}^{n-1}(\mathbb{F}_q)|\right) = \frac{1}{2}\left(\frac{q^{n+1}-1}{q-1} - \frac{q^n-1}{q-1}\right) = \frac{1}{2}\left(\frac{q^{n+1}-q^n}{q-1}\right) = \frac{q^n}{2},$$

which is even for $n \geq 2$ and $q = 2^m \geq 2$. □

Lemma 3.3. *Assume that $n \geq 2$ and $q = 2^m \geq 4$. Then B_n induces an even permutation on $\mathbb{P}^n(\mathbb{F}_q)$.*

Proof. We choose a generator $b \in \mathrm{Gal}(\mathbb{F}_{q^{n+1}}/\mathbb{F}_q) \cong \mathbb{Z}/(n+1)\mathbb{Z}$ and an element $\theta \in \mathbb{F}_{q^{n+1}}$ such that

$$\{\theta_i := b^i(\theta) : i = 0, \dots, n\} \subset \mathbb{F}_{q^{n+1}}$$

form a normal basis over $\mathbb{F}_q$. This identifies the underlying affine space $(\mathbb{F}_q)^{n+1}$ of $\mathbb{P}^n$ as

$$\mathbb{F}_q\theta_0 \oplus \mathbb{F}_q\theta_1 \oplus \cdots \oplus \mathbb{F}_q\theta_n \cong \mathbb{F}_{q^{n+1}}$$

where a point $(x_0, \dots, x_n) \in (\mathbb{F}_q)^{n+1}$ corresponds to $x_0\theta_0 + \cdots + x_n\theta_n \in \mathbb{F}_{q^{n+1}}$. Since $b(\theta_i) = \theta_{i+1}$ for $i = 0, \dots, n-1$ and $b(\theta_n) = \theta_0$, we have

$$b(x_0\theta_0 + x_1\theta_1 + \cdots + x_n\theta_n) = x_n\theta_0 + x_0\theta_1 + \cdots + x_{n-1}\theta_n,$$

which identifies the action of B_n on $(\mathbb{F}_q)^{n+1}$ from the left as the action of b^{-1} on $\mathbb{F}_{q^{n+1}}$.

Suppose that $n+1 = u2^\ell$ where u is odd. Then the parity of b^u is the same as the parity of b, and there is a filtration of $\mathbb{F}_{q^{n+1}}$ invariant under the action of b^u:

$$\mathbb{F}_{q^u} \subset \cdots \subset \mathbb{F}_{q^{u2^r}} \subset \cdots \subset \mathbb{F}_{q^{u2^\ell}} = \mathbb{F}_{q^{n+1}}.$$

For each $1 \leq r \leq \ell$, there are $q^{u2^r} - q^{u2^{r-1}}$ elements in $\mathbb{F}_{q^{u2^r}} \setminus \mathbb{F}_{q^{u2^{r-1}}}$, and the b^u-orbit of each element has size $[\mathbb{F}_{q^{u2^r}} : \mathbb{F}_{q^u}] = 2^r$. Therefore, the number of 2^r-cycles in the cycle decomposition of b^u equals

$$\frac{1}{2^r}|\mathbb{F}_{q^{u2^r}} \setminus \mathbb{F}_{q^{u2^{r-1}}}| = \frac{1}{2^r}(q^{u2^r} - q^{u2^{r-1}}).$$

Upon passing to the quotient space $\mathbb{P}^n(\mathbb{F}_q) = \mathbb{P}(\mathbb{F}_{q^{n+1}})$, which we consider as the set of $\mathbb{F}_q$-lines in $(\mathbb{F}_q)^{n+1}$ through the origin, the number of 2^r-cycles for the action of b^u becomes

$$\frac{1}{2^r}\left(\frac{q^{u2^r} - q^{u2^{r-1}}}{q-1}\right) = \frac{q^{u2^{r-1}}}{2^r}\left(\frac{q^{u2^{r-1}} - 1}{q-1}\right).$$

When $q = 2^m$, $m \geq 2$, we have $mu2^{r-1} - r > 0$ for $u \geq 1$ and $1 \leq r \leq \ell$, so the number

$$\frac{q^{u2^{r-1}}}{2^r} = \frac{2^{mu2^{r-1}}}{2^r} = 2^{mu2^{r-1}-r}$$

is even. As the fraction $\frac{q^{u2^{r-1}}-1}{q-1}$ is clearly an integer, we conclude that the number of 2^r-cycles in b^u when acting on $\mathbb{P}^n(\mathbb{F}_q)$ is even for all $r = 1, \ldots, \ell$, thus the action is even itself. □

Remark 3.4. Suppose the ground field is $\mathbb{F}_2$. Then the proof of Lemma 3.3 indicates that the action of B_n on $\mathbb{P}^n(\mathbb{F}_2)$ is even if $n = 2^\ell - 1$ for some $m \geq 1$ and odd otherwise. In the previous case, the action consists of exactly one 2-cycle and an even number of 2^r-cycles for every $2 \leq r \leq \ell$.

Proposition 3.5. *Over $k = \mathbb{F}_q$, $q = 2^m \geq 4$, and for any $n \geq 1$, the action of $\mathrm{PGL}_{n+1}(k)$ on $\mathbb{P}^n(k)$ induces even permutations.*

Proof. This follows from Lemma 3.1, 3.2, and 3.3. □

The parity of a permutation is invariant upon raising to an odd power, so we usually assume the order of a permutation to be a power of two when studying the parity. For a permutation induced by a linear transformation, the following lemma indicates that we can say more about the cycle type if its order is a power of two, which is a consequence of Proposition 3.5.

Corollary 3.6. *Assume that $k = \mathbb{F}_q$ where $q = 2^m \geq 4$ and $n \geq 1$. Suppose $\sigma \in \mathrm{PGL}_{n+1}(k)$ induces a permutation of order 2^r. Let c_i be the number of 2^i-cycles in its cycle decomposition, where $i = 0, \ldots, r$. Then c_0 is odd and the sum $c_1 + \cdots + c_r$ is even. In the case $n = 1$, there are only two possibilities:*

1. *$c_0 = q + 1$ and $c_i = 0$ for all $1 \leq i \leq r$, i.e. σ is the identity.*
2. *$c_0 = 1$ and $c_i = 0$ for all but one $1 \leq i \leq r$. The unique nonzero c_j where $1 \leq j \leq r$ equals $q/2^j > 1$.*

Proof. Because a 2^i-cycle is odd for $i \geq 1$, $c_1 + \cdots + c_r$ must be even due to the fact that σ is even by Proposition 3.5. Then the equations

$$|\mathbb{P}^n(k)| = q^n + \cdots + q + 1 = c_0 + 2c_1 + \cdots + 2^r c_r$$

imply that c_0 is odd.

Assume that $n = 1$ and that σ is not the identity. Then the fact that c_0 is odd implies that $c_0 = 1$. Let $1 \leq j \leq r$ be the smallest integer such that $c_j \neq 0$. Then σ^{2^j} becomes the identity since it fixes $1 + 2^j c_j \geq 3$ points. It follows that every nontrivial cycle in σ has the same size 2^j. Note that $2^j = q$ implies that σ is a q-cycle thus is odd, which is impossible by Proposition 3.5. Therefore, we have $2^j < q$ and the equality

$$|\mathbb{P}^1(k)| = q + 1 = 1 + 2^j c_j$$

implies that $c_j = q/2^j > 1$. □

3.1.2 Projective bundles over finite sets

Let B be a finite set. We define a $\mathbb{P}^n$*-bundle over* B to be a set of projective n-spaces indexed by B:

$$\mathcal{P} = \coprod_{i \in B} P_i, \quad P_i \cong \mathbb{P}^n$$

together with the natural map

$$h\colon \mathcal{P} \longrightarrow B : P_i \longmapsto i.$$

Since $\mathcal{P}$ is a disjoint union of projective spaces, we can consider the set $\mathcal{P}(k)$ of k-points in $\mathcal{P}$ in the usual way. We are interested in elements $\sigma \in \mathrm{Sym}(\mathcal{P}(k))$ of the form:

(1) For every $i \in B$, $\sigma(P_i(k)) = P_j(k)$ for some $j \in B$; in other words, the conjugation $\sigma_B := h\sigma h^{-1}$ is well-defined as an element of $\mathrm{Sym}(B)$.

(2) Each bijection $\sigma\colon P_i(k) \to P_j(k)$ is induced by a projective transformation over k.

Note that such elements form a subgroup of $\mathrm{Sym}(\mathcal{P}(k))$.

Lemma 3.7. *Assume that $k = \mathbb{F}_q$ where $q = 2^m \geq 4$. Let $\sigma \in \mathrm{Sym}(\mathcal{P}(k))$ be an element satisfying (1) and (2). Then σ and $\sigma_B := h\sigma h^{-1} \in \mathrm{Sym}(B)$ have the same parity.*

Proof. The parity of a permutation is invariant upon raising it to an odd power, so we can assume that both σ and σ_B consist of disjoint cycles of sizes powers of 2. Suppose that

$$O := \{p_1, ..., p_r\} \subset B, \quad r = 2^\ell \geq 1,$$

is one of the orbits of σ_B. Then the set of k-points in $h^{-1}(O) \subset \mathcal{P}$ is invariant under σ. This reduces the proof to the case $O = B$. Note that the case $r = 1$ follows immediately from Proposition 3.5. Hence we further assume that $r \geq 2$, in which case σ_B is odd, and so our goal is to prove that σ is also odd.

Fix an element $p \in O$. The assumption $O = B$ implies $\sigma_B^r = \mathrm{id}$, so σ^r acts on the k-points of $h^{-1}(p) \cong \mathbb{P}^n$. Denote this action as σ_p^r. Observe that, in the cycle decompositions, a u-cycle in σ_p^r contributes a (ur)-cycle in σ, and every cycle in σ is obtained this way. Assume that σ_p^r consists of c_i many 2^i-cycles where $i \geq 0$. Then σ consists of c_i many $(2^i r)$-cycles for $i \geq 0$, which are all odd since $2^i r \geq 2$ by the hypothesis that $r \geq 2$. By Corollary 3.6 applied to σ_p^r, the sum $\sum_{i \geq 0} c_i$, which also equals the number of cycles in σ, is an odd integer. Therefore, σ is odd. □

3.2 Birational invariance of the parity

In this section, we investigate how the conjugation via a birational map affects the parity of a birational permutation. The main result is Theorem 1.5 given in the introduction, whose proof will be given in §3.2.1. As an application, we illustrate in §3.2.2 how the theorem simplifies the parity problem for elements of finite order in $\mathrm{BCr}_2(k)$. Recall that for the sake of consistency, given a variety X defined over k, we denote its group of birational self-maps as $\mathrm{Cr}_X(k)$ and the subgroup of biregular elements as $\mathrm{BCr}_X(k)$.

Example 3.8. It is easy to construct a counterexample to Theorem 1.5 in the cases that q is odd and $q = 2$. Consider an element $g \in \mathrm{PGL}_3(\mathbb{F}_q)$ of the form

$$g = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that g fixes $p = [0 : 0 : 1]$. Let X be the blowup of $\mathbb{P}^2$ at p. Then g lifts to an automorphism on X which acts on the exceptional $\mathbb{P}^1$ as $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and the parity is altered via the lifting if this matrix acts as an odd permutation on $\mathbb{P}^1(\mathbb{F}_q)$. For example, one can choose $\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$ if q is odd, where α is a generator for the multiplicative group $\mathbb{F}_q^*$, and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ if $q = 2$.

In view of Theorem 1.5, one may wonder if there exists a birational odd permutation on a surface over $\mathbb{F}_q$ where $q = 2^m \geq 4$. Below we exhibit an example of an odd permutation over $\mathbb{F}_4$ induced from an automorphism.

Example 3.9. Write $\mathbb{F}_4 = \mathbb{F}_2(\xi)$, where $\xi^2 + \xi + 1 = 0$, and let $\bar{\xi}$ denote the Galois conjugate of ξ. Consider the elliptic curve in Weierstrass equation

$$E : y^2 + xy = x^3 + 1.$$

Then $j(E) = 1$ and $\mathrm{Aut}(E) \cong \mathbb{Z}/2\mathbb{Z}$ is generated by $\sigma_E \colon (x, y) \mapsto (x, y+x)$ [Sil09, Propositions A.1.1 & A.1.2]. A straightforward computation shows that $E(\mathbb{F}_2) = \{(1, 0), (0, 1), (1, 1), p_\infty\}$ where p_∞ is the point at infinity, and there are additional four points $(\xi, 0)$, $(\bar{\xi}, 0)$, (ξ, ξ), $(\bar{\xi}, \bar{\xi})$ over $\mathbb{F}_4$. The involution σ_E fixes $(0, 1)$, p_∞ and exchanges points in the pairs

$$\{(1, 0), (1, 1)\},\ \{(\xi, 0), (\xi, \xi)\},\ \{(\bar{\xi}, 0), (\bar{\xi}, \bar{\xi})\}.$$

In particular, σ_E acts as a product of three transpositions on $E(\mathbb{F}_4)$ hence is an odd permutation. Define $X := \mathbb{P}^1 \times E$ and consider it as a $\mathbb{P}^1$-bundle over E. Then σ_E can be extended as $\sigma_X \in \mathrm{Aut}(X)$ where

$$\sigma_X \colon X \to X : (p, q) \mapsto (p, \sigma_E(q))$$

whose action on $X(\mathbb{F}_4)$ is odd by Lemma 3.7. In fact, it is not hard to see that the permutation consists of 5 disjoint permutations of the same type as σ_E.

3.2.1 Proof of Theorem 1.5

Remark 3.10. Let Y be a smooth projective surfaces over a perfect field k, $\sigma_Y \in \mathrm{BCr}_Y(k)$ and $h\colon X \to Y$ the blow-up of a finite set of k-rational points B and $E = h^{-1}(B)$ the union of its exceptional divisors. Suppose that $\sigma_X := h^{-1}\sigma_Y h \in \mathrm{BCr}_X(k)$. Then σ_X does not contract any curve in E as they are all rational, and hence $\sigma_X(E) = h^{-1}\sigma_Y h(E) = h^{-1}(\sigma_Y(B))$ is a curve. It follows that $\sigma_Y(B) \subset B$. Since σ_Y induces a bijection on $Y(k)$, we have $\sigma_Y(B) = B$ and hence $\sigma_X(E) = E$.

Lemma 3.11. *Let Y be a smooth projective surface over $k = \mathbb{F}_{2^m}$, $m > 1$. Let $\sigma_Y \in \mathrm{BCr}_Y(k)$ and $h\colon X \to Y$ the blow-up of a set $B \subset Y$ of closed points. If $\sigma_X := h^{-1}\sigma_Y h \in \mathrm{BCr}_X(k)$, then σ_Y and σ_X have the same parity.*

Proof. First, if $B(k) = \emptyset$, then $h|_{X(k)}\colon X(k) \to Y(k)$ is a bijecton and σ_X and σ_Y have the same cycle type. Otherwise, define $U := X \setminus E$ and $V := Y \setminus B$ where E is the exceptional locus lying over B. Then h can be divided into two parts $h|_E\colon E \to B$ and $h|_U\colon U \to V$ such that for any $b \in B(k)$ and $v \in V(k)$,

$$\sigma_Y|_B(b) = h|_E \circ \sigma_X|_E \circ (h|_E)^{-1}(b) \quad \text{and} \quad \sigma_Y|_V(v) = h|_U \circ \sigma_X|_U \circ (h|_U)^{-1}(v),$$

by Remark 3.10. Because $h|_U$ is an isomorphism, the second relation implies that $\sigma_X|_U$ and $\sigma_Y|_V$ have the same cycle type on $U(k)$ and $V(k)$ respectively. Note that the exceptional divisor $E \subset X$ is a $\mathbb{P}^1$-bundle over B over the algebraic closure $\bar{k}$ of k. Restricting h to $E(k)$ induces the relations among finite sets

$$E(k) \cong \mathbb{P}^1(k) \times B(k) \xrightarrow{h|_{E(k)}} B(k),$$

as well as the relation between permutations

$$\sigma_Y|_{B(k)} = h|_{E(k)} \circ \sigma_X|_{E(k)} \circ (h|_{E(k)})^{-1}.$$

Then $\sigma_Y|_{B(k)}$ and $\sigma_X|_{E(k)}$ share the same parity by Lemma 3.7 (here we use $k = \mathbb{F}_q, q = 2^m \geq 4$), hence the conclusion follows. □

Lemma 3.12. *Let Y be a smooth projective surface over $k = \mathbb{F}_{2^m}$, $m > 1$ and $h\colon X \to Y$ a birational morphism. Let $\sigma_Y \in \mathrm{BCr}_Y(k)$. If $\sigma_X := h^{-1}\sigma_Y h \in \mathrm{BCr}_X(k)$, then σ_Y and σ_X have the same parity.*

Proof. If h is the blow-up of a set of closed points in Y, the claim is Lemma 3.11. In the general case, we can decompose h into a sequence of blowups at closed points [Man86, Lemma 18.1.3]

$$h\colon X = Y_r \xrightarrow{\epsilon_r} Y_{r-1} \xrightarrow{\epsilon_{r-1}} \cdots \xrightarrow{\epsilon_2} Y_1 \xrightarrow{\epsilon_1} Y. \tag{3.1}$$

This sequence can be arranged in the way that the points in Y_i blown up by ϵ_{i+1} lie in the exceptional locus of ϵ_i. Indeed, if there exists a point $x \in Y_i$ blown up by ϵ_{i+1} but not in the exceptional locus of ϵ_i, we can form new maps

$$\begin{tikzcd} Y'_{i+1} \arrow[r, "\epsilon'_{i+1}"] \arrow[d, "\sim"] & Y'_i \arrow[r, "\epsilon'_i"] \arrow[d, "\mathrm{Bl}_x"] & Y_{i-1} \arrow[d, equal] \\ Y_{i+1} \arrow[r, "\epsilon_{i+1}"] & Y_i \arrow[r, "\epsilon_i"] & Y_{i-1} \end{tikzcd} \tag{3.2}$$

where ϵ'_i is ϵ_i followed by the blowup at x, and ϵ'_{i+1} blows up the same points as ϵ_{i+1} except for x. Then Y'_{i+1} and Y_{i+1} are canonically isomorphic and we can replace $\epsilon_i\epsilon_{i+1}$ by $\epsilon'_i\epsilon'_{i+1}$. Repeating this process from $i = r - 1$ to $i = 1$ gives us the desired sequence.

Let $\sigma_0 := \sigma_Y$ and define inductively that

$$\sigma_i := \epsilon_i^{-1}\sigma_{i-1}\epsilon_i \in \mathrm{Cr}_{Y_i}(k), \quad i = 1, \ldots, r. \tag{3.3}$$

Note that $\sigma_r = \sigma_X$. Let us prove that every $\sigma_i \in \mathrm{BCr}_{Y_i}(k)$ by induction. The case $i = 0$ follows from the definition. Suppose that $\sigma_{i-1} \in \mathrm{BCr}_{Y_{i-1}}(k)$ and, to the contrary, that $\sigma_i \notin \mathrm{BCr}_{Y_i}(k)$. Let $p \in Y_i(k)$ be a base-point of σ_i. Consider the two points

$$q := \epsilon_i(p) \in Y_{i-1}(k), \quad q' := \sigma_{i-1}(q) \in Y_{i-1}(k).$$

There are three conditions to analyze:

(1) q' is not blown up by ϵ_i. This implies that σ_i is well-defined at p by (3.3), which contradicts our assumption.

(2) q' is blown up by ϵ_i while q is not. Let $E_{q'} \subset Y_i$ denote the exceptional divisor over q'. In this case, p does not lie in the exceptional locus of ϵ_i, so it is mapped bijectively to a point $\widetilde{p} \in X(k)$ via the inverses of the blowups in (3.1). The relation (3.3) implies that σ_X^{-1} contracts the proper transform of $E_{q'}$ to $\widetilde{p}$, so $\widetilde{p}$ is a base-point of σ_X, which contradicts the fact that σ_X is biregular.

(3) q' and q are both blown up by ϵ_i. Let $E_q \subset Y_i$ and $E_{q'} \subset Y_i$ denote the exceptional divisors over q and q', respectively. In this case, we have the commutative diagram

$$\begin{tikzcd}
E_q \arrow[r, hook] & Y_i \arrow[r, "\epsilon_i"] \arrow[d, dashed, "\sigma_i"] & Y_{i-1} \arrow[d, dashed, "\sigma_{i-1}"] \\
E_{q'} \arrow[r] & Y_i \arrow[r, "\epsilon_i"] & Y_{i-1}.
\end{tikzcd}$$

The composition $\sigma_{i-1}\epsilon_i \colon Y_i \dashrightarrow Y_{i-1}$ pulls q' back as the divisor E_q while q' is blown up by ϵ_i as $E_{q'}$. By the universal property of blowing up, $\sigma_{i-1}\epsilon_i$ factors through ϵ_i uniquely as

$$\begin{tikzcd}
E_q \arrow[r, hook] \arrow[d, "\sigma'_i|_{E_q}"', "\sim"] & Y_i \arrow[r, "\epsilon_i"] \arrow[d, dashed, "\exists\, \sigma'_i"] & Y_{i-1} \arrow[d, dashed, "\sigma_{i-1}"] \\
E_{q'} \arrow[r] & Y_i \arrow[r, "\epsilon_i"] & Y_{i-1}.
\end{tikzcd}$$

Note that σ'_i is well-defined on E_q and $\sigma'_i = \epsilon_i^{-1}\sigma_{i-1}\epsilon_i = \sigma_i$. Hence σ_i is well-defined on E_q and in particular at p, a contradiction.

Since we get contradictions in all possible conditions, we conclude that $\sigma_i \in \mathrm{BCr}_{Y_i}(k)$, hence the claim is fulfilled by induction. As a result, the permutations induced by σ_i, $i = 0, \dots, r$, which include σ_X and σ_Y, have the same parity by Lemma 3.11. □

Proof of Theorem 1.5. We are now ready to prove Theorem 1.5 in the general case. We can eliminate the base locus of h by a sequence of blowups at closed points [Kol07, Corollary 1.76]

$$\begin{tikzcd}
X_r \arrow[r, "\epsilon_r"] \arrow[rrrrd, "\widetilde{h}"'] & X_{r-1} \arrow[r, "\epsilon_{r-1}"] & \cdots \arrow[r, "\epsilon_2"] & X_1 \arrow[r, "\epsilon_1"] & X_0 = X \arrow[d, dashed, "h"] \\
& & & & Y
\end{tikzcd}$$

Let $E_i \subset X_i$ denote the exceptional locus of ϵ_i, and let

$$C_{i-1} := \epsilon_i(E_i) \subset X_{i-1}, \quad i = 1, \dots, r$$

denote the center. Through the same process as (3.2), one can arrange the blowups above so that $C_i \subset E_i$ for $i = 1, \dots, r-1$. Let $\sigma_0 := \sigma_X$ and define inductively that

$$\sigma_i := \epsilon_i^{-1}\sigma_{i-1}\epsilon_i \in \mathrm{Cr}_{X_i}(k), \quad i = 1, \dots, r. \tag{3.4}$$

We claim that, for each i, there exists a birational morphism

$$\eta_i \colon Z_i \to X_i \ \text{ such that } \ \tau_i := \eta_i^{-1}\sigma_i\eta_i \in \mathrm{BCr}_{Z_i}(k). \tag{3.5}$$

We prove the claim by induction starting from $i = 1$. Consider the action of σ_X on $X(k)$ and let $O \subset X(k)$ be one of its orbits. Then there are two situations:

(a) If $O \cap C_0 = \emptyset$, then σ_1 is well-defined on $(\epsilon_1^{-1}(O))(k) \subset X_1(k)$.

(b) Assume that $O \cap C_0 \neq \emptyset$. Note that, if $O \subset C_0$, then one can argue that σ_1 is well-defined on $(\epsilon_1^{-1}(O))(k) \subset X_1(k)$ in a similar way as (3) in Lemma 3.12. In general, there exists $q \in O \setminus C_0$ such that $\sigma_0(q) \in C_0$, and

$$O \setminus C_0 = \{q, \sigma_0^{-1}(q), \dots, \sigma_0^{-\ell}(q)\},$$

for some $\ell \geq 0$. In this case, σ_1 is undefined at the $p := \epsilon_1^{-1}(q)$ due to (3.4). Blowing p up will resolve this indeterminacy for a similar reason as (3) in Lemma 3.12, but this will produce a new base-point for σ_1 at $p' := \epsilon_1^{-1}(\sigma_0^{-1}(q))$. By repeating the same process until all points in $\epsilon_1^{-1}(O \setminus C_0)$ are blown up, the base-points coming from O will be resolved.

Let $O_1, \dots, O_n \subseteq X(k)$ be the orbits of σ_1 which meet C_0 nontrivially. Define

$$B_1 := \bigcup_{j=1}^{n} \epsilon_1^{-1}(O_j \setminus C_0) \subseteq X_1(k) \setminus E_1,$$

and consider the blowup

$$\eta_1 \colon Z_1 := \mathrm{Bl}_{B_1} X_1 \longrightarrow X_1.$$

Then $\tau_1 := \eta_1^{-1}\sigma_1\eta_1 \in \mathrm{BCr}_{Z_1}(k)$ according to (b).

Assume that there is a desired blowup (3.5) for some $1 \leq i \leq r-1$. The fiber product $X'_{i+1} := X_{i+1} \times_{X_i} Z_i$ fits into the commutative diagram

$$\begin{tikzcd}
 & X'_{i+1} \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & Z_i \arrow[d, "\eta_i"] & \\
\cdots \arrow[r] & X_{i+1} \arrow[r, "\epsilon_{i+1}"] & X_i \arrow[r, "\epsilon_i"] & \cdots
\end{tikzcd}$$

where π_1 and π_2 are the projections to the first and the second components, respectively. Due to the fact that $B_i \subset X_i(k) \setminus E_i$ and $C_i \subset E_i$, we have $B_i \cap C_i = \emptyset$, so that X'_{i+1} is constructed by blowing up X_i at B_i and C_i where the order does not matter. In particular, π_2 is the blowup

$$\pi_2 \colon X'_{i+1} \cong \mathrm{Bl}_{\eta_i^{-1}(C_i)} Z_i \longrightarrow Z_i.$$

By hypothesis, we have $\tau_i := \eta_i^{-1}\sigma_i\eta_i \in \mathrm{BCr}_{Z_i}(k)$, and it can be lifted to X'_{i+1} as

$$\sigma'_{i+1} := \pi_2^{-1}\tau_i\pi_2 \in \mathrm{Cr}_{X'_{i+1}}(k).$$

Note that, by tracking the commutative diagram above, we have

$$\sigma'_{i+1} = \pi_2^{-1}\tau_i\pi_2 = \pi_2^{-1}\eta_i^{-1}\sigma_i\eta_i\pi_2 = \pi_1^{-1}\epsilon_{i+1}^{-1}\sigma_i\epsilon_{i+1}\pi_1 = \pi_1^{-1}\sigma_{i+1}\pi_1. \tag{3.6}$$

Let $O_1, \dots, O_n \subseteq Z_i(k)$ be the orbits of the action of τ_i on $Z_i(k)$ such that $O_j \cap \eta_i^{-1}(C_i) \neq \emptyset$ for all j. Define

$$B'_{i+1} := \bigcup_{j=1}^{n} \pi_2^{-1}(O_j \setminus \eta_i^{-1}(C_i)) \subseteq X'_{i+1}(k).$$

Consider the blowup

$$\eta'_{i+1} \colon Z_{i+1} := \mathrm{Bl}_{B'_{i+1}} X'_{i+1} \longrightarrow X'_{i+1}.$$

Then $\tau_{i+1} := \eta'^{-1}_{i+1}\sigma'_{i+1}\eta'_{i+1} \in \mathrm{BCr}_{Z_{i+1}}(k)$ by the same reasoning as the $i = 1$ case. Define

$$\eta_{i+1} := \pi_1\eta'_{i+1} \colon Z_{i+1} \longrightarrow X_{i+1}.$$

Using (3.6), we obtain

$$\tau_{i+1} = \eta'^{-1}_{i+1}\sigma'_{i+1}\eta'_{i+1} = \eta'^{-1}_{i+1}\pi_1^{-1}\sigma_{i+1}\pi_1\eta'_{i+1} = \eta_{i+1}^{-1}\sigma_{i+1}\eta_{i+1}.$$

Hence statement (3.5) is fulfilled for $i + 1$.

By induction, (3.5) holds for $i = 1, \dots, r$. In particular, there exists a birational morphism

$$\eta_r \colon Z_r \to X_r \ \text{ such that } \ \tau_r := \eta_r^{-1}\sigma_r\eta_r \in \mathrm{BCr}_{Z_r}(k).$$

As a result, we obtain the commutative diagram

$$\begin{tikzcd}
 & Z_r \arrow[dl, "f"'] \arrow[dr, "g"] & \\
X \arrow[rr, dashed, "h"] & & Y
\end{tikzcd}$$

where $f = \epsilon_1 \cdots \epsilon_r \eta_r$ and $g = \widetilde{h}\eta_r$ are birational morphisms. Moreover,

$$\begin{aligned}
\sigma_Z := f^{-1}\sigma_X f &= (\epsilon_1 \cdots \epsilon_r\eta_r)^{-1}\sigma_0(\epsilon_1 \cdots \epsilon_r\eta_r) \\
&= \eta_r^{-1}\epsilon_r^{-1} \cdots \epsilon_1^{-1}\sigma_0\epsilon_1 \cdots \epsilon_r\eta_r = \eta_r^{-1}\sigma_r\eta_r = \tau_r,
\end{aligned}$$

which belongs to $\mathrm{BCr}_{Z_r}(k)$. Using the relations $h = gf^{-1}$ and $\sigma_Y = h\sigma_X h^{-1}$, we derive that

$$\sigma_Z = f^{-1}\sigma_X f = g^{-1}h\sigma_X h^{-1}g = g^{-1}\sigma_Y g.$$

Therefore, the actions of σ_X, σ_Y, and σ_Z on the k-points have the same parity by Lemma 3.12, which completes the proof. □

3.2.2 Birational self-maps of finite order

Theorem 1.5 allows us to transfer the parity problem from one surface to another via conjugations. In the case that $f \in \mathrm{BCr}_2(k)$ has finite order, we have the following fact.

Lemma 3.13. *Let k be a perfect field. Suppose $G \subseteq \mathrm{Cr}_2(k)$ is a finite subgroup. Then there exists a surface X together with a birational map $\phi\colon X \dashrightarrow \mathbb{P}^2$ such that there is an injective homomorphism*

$$\phi^*\colon G \hookrightarrow \mathrm{Aut}(X) : g \to \phi^{-1}g\phi. \tag{3.7}$$

Moreover, X can be minimal with respect to G in the sense that

(1) *X admits a structure of a conic bundle with $\mathrm{Pic}(X)^G \cong \mathbb{Z}^2$, or*

(2) *X is isomorphic to a del Pezzo surface with $\mathrm{Pic}(X)^G \cong \mathbb{Z}$.*

Proof. The same argument in the proof of [DI09, Lemma 3.5] works in our situation. As a consequence, there exists a surface X and a birational map $\phi\colon X \dashrightarrow \mathbb{P}^2$ such that (3.7) holds.

Now consider G as a subgroup of $\mathrm{Aut}(X)$. Assume that X is not minimal with respect to G, i.e. there exists a surface Y and a birational morphism $h\colon X \to Y$ together with an inclusion

$$h^*\colon G \hookrightarrow \mathrm{Aut}(Y) : g \to h^{-1}gh$$

such that the rank of $\mathrm{Pic}(Y)^G$ is strictly less than the rank of $\mathrm{Pic}(X)^G$. This process terminates at either (1) or (2) by [Isk79, Theorem 1G]. □

As a corollary, given $f \in \mathrm{BCr}_2(k)$ of finite order, we can always conjugate it to an automorphism on a minimal surface. This reduces the parity problem for such elements to the problem on the parities induced by the automorphisms on a conic bundle or a del Pezzo surface. We start the investigation case-by-case starting from §3.3.

Since the parity of a permutation is invariant upon taking an odd power, we will usually assume the order of an induced permutation to be 2^r for some $r > 0$ when studying its parity. The following lemma will be useful in this situation.

Lemma 3.14. *Let X be a surface defined over $k = \mathbb{F}_q$, $q = 2^m \geq 4$, which is rational over the algebraic closure, and let $\sigma \in \mathrm{Sym}(X(k))$.*

(1) *If $\mathrm{ord}(\sigma) = 2^r$ for some $r \geq 0$, then σ has odd number of fixpoints.*

(2) *If $\mathrm{ord}(\sigma) = 2$ and the number of fixpoints equals 1 modulo 4, then σ is an even permutation.*

Proof. It is well-known that $|X(k)| = q^2 + aq + 1$ for some non-negative integer a [Wei56]; see also [Poo17, Proposition 9.3.24]. On the other hand, the cardinality of each orbit of σ divides $\mathrm{ord}(\sigma) = 2^r$, so

$$q^2 + aq + 1 = 2\ell + |\{\text{fixpoints of } \sigma\}|, \quad \text{for some } \ell \geq 0,$$

which implies (1) immediately.

Assume that $\mathrm{ord}(\sigma) = 2$ and that σ has $4b + 1$ fixpoints for some $b \geq 0$. In particular, σ can be decomposed into a product of disjoint 2-cycles. The amount of the 2-cycles equals

$$\frac{1}{2}(|X(k)| - (4b + 1)) = \frac{1}{2}(q^2 + aq - 4b) \equiv 0 \mod 2.$$

Hence the induced permutation is even. □

We use a simple observation to end this section.

Proposition 3.15. *Let X be a del Pezzo surface defined over a finite field $k = \mathbb{F}_q$. Then* $\mathrm{Aut}(X)$ *is a finite group.*

Proof. If X is a del Pezzo surface, then the anticanonical class $-K_X$ is ample and thus $-rK_X$ becomes very ample for some $r \geq 1$. The linear system $|-rK_X|$ defines an embedding $X \hookrightarrow \mathbb{P}^n$. Since every $f \in \mathrm{Aut}(X)$ preserves K_X, it extends to an automorphism on $\mathbb{P}^n$. Hence f is of finite order because $\mathrm{PGL}_{n+1}(\mathbb{F}_q)$ is a finite group. □

3.3 Birational self-maps on conic bundles

Fix the ground field as $k = \mathbb{F}_q$ where $q = 2^m \geq 4$. Here we show that the birational permutations on a conic bundle preserving the fibration induce even permutations.

Recall that, over a finite field k, a conic $C \subset \mathbb{P}^2_k$ is isomorphic to one of the following four configurations

(I) C is smooth, i.e. $C \cong \mathbb{P}^1_k$.

(II) C is double line.

(III) $C = \ell \cup \ell'$ where ℓ and ℓ' are distinct lines defined over k.

(IV) $C = \ell \cup \ell'$ where ℓ and ℓ' are conjugate over the quadratic extension.

Let B be a finite set. We define a *conic bundle over B* to simply be a set of conics indexed by B:

$$\mathcal{C} = \bigcup_{i \in B} C_i$$

together with the natural map

$$h\colon \mathcal{C} \longrightarrow B : C_i \longmapsto i.$$

As $\mathcal{C}$ is a union of conics, we can consider the set $\mathcal{C}(k)$ of k-points on $\mathcal{C}$ in the usual way. We are interested in elements $\sigma \in \mathrm{Sym}(\mathcal{C}(k))$ of the form:

(1) For every $i \in B$, $\sigma(C_i(k)) = C_j(k)$ for some $j \in B$; in other words, the conjugation $\sigma_B := h\sigma h^{-1}$ is well-defined as an element of $\mathrm{Sym}(B)$.

(2) Each bijection $\sigma\colon C_i(k) \to C_j(k)$ is induced by an isomorphism between conics over k.

Note that such elements form a subgroup of $\mathrm{Sym}(\mathcal{C}(k))$.

Lemma 3.16. *Let $k = \mathbb{F}_q$, $q = 2^m \geq 4$. Assume that $\sigma \in \mathrm{Sym}(\mathcal{C}(k))$ satisfies (1) and (2). Then σ and $\sigma_B := h\sigma h^{-1} \in \mathrm{Sym}(B)$ share the same parity.*

Proof. Since the parity of a permutation is invariant upon raising it to an odd power, we can assume that both σ and σ_B consist of disjoint cycles of sizes powers of 2. In particular, each nontrivial cycle is an odd permutation. Suppose that

$$O := \{p_1, ..., p_r\} \subset B, \quad r = 2^s \geq 1,$$

is one of the orbits of σ_B. Then the set of k-points in $h^{-1}(O) \subset \mathcal{C}$ is invariant under σ, and it's sufficient to show that this action is odd. This reduces the case to $O = B$.

By hypothesis, the fibers over O are mutually isomorphic and thus of the same type. If they are of type (IV), then the node in each fiber appears as the only one k-point in that fiber. It follows that σ has the same cycle type as σ_B, hence are both odd. Case (II) can be reduced to Case (I) by considering the reduced substructure. On the other hand, Case (I) follows from Lemma 3.7.

Assume that the fibers are of type (III). Then each $C_i := h^{-1}(p_i) = \ell_i \cup \ell'_i$ where ℓ_i and ℓ'_i are copies of $\mathbb{P}^1_k$. In this case, the nodes

$$\delta_i := \ell_i \cap \ell'_i, \quad i = 1, ..., r$$

form an orbit of size r. Let σ_L denote the action of σ on the set of lines

$$L := \{\ell_1, \ell'_1, \ell_2, \ell'_2, \dots, \ell_r, \ell'_r\}.$$

Then there are two possibilities:

(i) L has two orbits of size r. More precisely, we can relabel the components of C_i as ℓ_i^+ and ℓ_i^- such that
$$\sigma_L = (\ell_1^+, \dots, \ell_r^+)(\ell_1^-, \dots, \ell_r^-).$$

(ii) L forms a single orbit of size $2r$. In this case, using the notation from the previous case we can write
$$\sigma_L = (\ell_1^+, \dots, \ell_r^+, \ell_1^-, \dots, \ell_r^-).$$

In both cases, we use those lines to form a new conic bundle

$$\widetilde{\mathcal{C}} = \mathcal{C}^+ \amalg \mathcal{C}^- \xrightarrow{\widetilde{h} = h^+ \amalg h^-} O^+ \amalg O^-,$$

where $O^{\pm} = \{p_1^{\pm}, ..., p_r^{\pm}\}$ are two copies of O, and

$$\mathcal{C}^{\pm} = \{\ell_1^{\pm}, \dots, \ell_r^{\pm}\} \xrightarrow{h^{\pm}} O^{\pm} : \ell_i^{\pm} \longmapsto p_i^{\pm}.$$

For each $i = 1, ..., r$, the node δ_i splits as $\delta_i^+ \in \ell_i^+$ and $\delta_i^- \in \ell_i^-$.

Suppose that we are in case (i). Replacing the cycle $(\delta_1, \dots, \delta_r)$ in σ by the product

$$(\delta_1^+, \dots, \delta_r^+)(\delta_1^-, \dots, \delta_r^-)$$

produces $\widetilde{\sigma} \in \mathrm{Sym}(\widetilde{\mathcal{C}}(k))$ which satisfies (1), (2), and

$$\widetilde{h}\widetilde{\sigma}\widetilde{h}^{-1} = (p_1^+, ..., p_r^+)(p_1^-, ..., p_r^-),$$

which is even. Because the fibers of $\widetilde{h}$ are smooth, we conclude that $\widetilde{\sigma}$ is even by the result of the previous case. It follows that σ is odd since σ has one less odd cycle than $\widetilde{\sigma}$.

Suppose that we are in case (ii). Replacing the cycle $(\delta_1, \dots, \delta_r)$ in σ by the cycle

$$(\delta_1^+, \dots, \delta_r^+, \delta_1^-, \dots, \delta_r^-)$$

produces $\widetilde{\sigma} \in \mathrm{Sym}(\widetilde{\mathcal{C}}(k))$ which satisfies (1), (2), and

$$\widetilde{h}\widetilde{\sigma}\widetilde{h}^{-1} = (p_1^+, ..., p_r^+, p_1^-, ..., p_r^-),$$

which is odd. We conclude in a similar way that $\widetilde{\sigma}$ is odd. Therefore, σ is also odd in this case. □

For our applications of the above lemma, we are interested in the case where B is the set of k-points on a curve. The following corollary is then immediate.

Corollary 3.17. *Let $\mathcal{C} \to D$ be a conic bundle over a curve D defined over $k = \mathbb{F}_q$, where $q = 2^n \geq 4$. For $f \in \mathrm{BCr}_{\mathcal{C}}(k)$ preserving the conic bundle structure, let $\rho(f) \in \mathrm{Aut}(D)$ be the induced automorphism on D.*

(1) *The permutation of $\mathcal{C}(k)$ induced by f and the permutation of $D(k)$ induced by $\rho(f)$ have the same parity.*

(2) *If $D = \mathbb{P}^1$, the permutation of $\mathcal{C}(k)$ induced by f is even.*

Proof. The bundle morphism $\pi\colon \mathcal{C} \to D$ sends $\mathcal{C}(k)$ onto $B := D(k)$, so f induces a permutation σ_f on $\mathcal{C}(k)$ satisfying (1) and (2). Let σ_B be the permutation of B induced by $\rho(f)$. By Lemma 3.16, σ and σ_B have the same parity. If $D = \mathbb{P}^1$, it follows from Proposition 3.5 that σ_B and hence σ are even. □

3.4 Automorphisms of rational del Pezzo surfaces

Recall that, over an arbitrary field k, a *del Pezzo surface* X is a smooth projective surface such that the anticanonical divisor $-K_X$ is ample. The *degree* of X is defined as the integer $d = K_X^2$ which takes values from 1 to 9. For example, a del Pezzo surface X of degree 9 is a *Severi-Brauer surface*, i.e. $X_{\overline{k}} := X \otimes_k \overline{k} \cong \mathbb{P}^2_{\overline{k}}$.

In this section, we investigate the parities of the permutations on $X(k)$ induced by automorphisms on a rational del Pezzo surface X defined over $k = \mathbb{F}_q$, where $q = 2^m \geq 4$. Our goal is to prove the following theorem:

Theorem 3.18. *Every automorphism on a rational del Pezzo surface X defined over $k = \mathbb{F}_q$, $q = 2^m \geq 4$, induces an even permutation on $X(k)$.*

Remark 3.19. Over $\mathbb{F}_2$ there are rational del Pezzo surfaces X of degree 6 which have an automorphism inducing an odd permutation on $X(\mathbb{F}_2)$, as is shown in Proposition 4.7.

A rational del Pezzo surface of degree 9 over k is just $\mathbb{P}^2_k$, so this case is covered by Proposition 3.5. We proceed the proof case-by-case with the degree d going from high to low in a similar way as the proof of [Man86, Theorem 29.4].

Proposition 3.20. *The claim of Theorem 3.18 holds for rational del Pezzo surfaces X of degree $d = K_X^2$, $3 \leq d \leq 8$.*

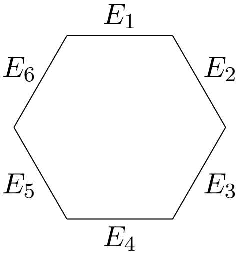
Proof. Let $g \in \mathrm{Aut}(X)$. Since raising g to an odd power does not change the parity of its permutations, we can assume g has order a power of 2. By Lemma 3.14(1), there exists $p \in X(k)$ that is fixed by g.

Case $(d = 8)$**:** If X is not minimal (over k), then there exists a (-1)-curve $E \subset X$ defined over k, and the contraction of E gives a morphism $h\colon X \to \mathbb{P}^2$. Every $g \in \mathrm{Aut}(X)$ leaves E invariant, hence is conjugate to an automorphism of $\mathbb{P}^2$ fixing $h(E) \in \mathbb{P}^2$. It follows that g induces an even permutation on $X(k)$ by Propositions 3.5 and Theorem 1.5.

If X is minimal, then it is a quadric surface obtained by blowing up $\mathbb{P}^2_k$ at a point of degree 2 (resp. two rational points), and then contracting the proper transform of the unique line through that point (resp. the two rational points). In particular, over the quadratic extension $L := \mathbb{F}_{q^2}$, we have $X_L \cong \mathbb{P}^1_L \times \mathbb{P}^1_L$. Let X_7 be the blow up of X at p and let E be the exceptional curve. Then the two rulings of $X \cong \mathbb{P}^1_L \times \mathbb{P}^1_L$ meeting at p lift to disjoint (-1)-curves $E_1, E_2 \subset X_7$ over L that are conjugate to each other (resp. rational), and g is conjugate to $g' \in \mathrm{Aut}(X_7)$ which leaves the set $\{E_1, E_2\}$ invariant. Let $h\colon X_7 \to \mathbb{P}^2_k$ be the contraction of E_1, E_2. Then $hg'h^{-1}$ is a $\mathrm{PGL}_3(k)$-action on $\mathbb{P}^2$ leaving the set $\{h(E_1), h(E_2)\}$ invariant. It then follows from Propositions 3.5 and Theorem 1.5 that g induces an even permutation.

Case $(d = 7)$**:** There is a unique (-1)-curve E on X that is invariant under both the Galois action and g. Hence, blowing down E, we get $X \to X_8$ where X_8 is a del Pezzo surface of degree 8, and g descends to an automorphism g_8 on X_8. The result then follows from Theorem 1.5 and Case $d = 8$.

Case $(d = 6)$**:** Over the algebraic closure, $X_{\overline{k}}$ contains six (-1)-curves E_1, ..., E_6 whose intersection relations can be depicted as a hexagon:



This configuration is invariant under $\mathrm{Gal}(\overline{k}/k)$,

If p does not lie on any of the lines on $X_{\overline{k}}$, then the blow up $X_5 = \mathrm{Bl}_p(X)$ is a del Pezzo surface of degree 5, and g lifts to an automorphism g_5 of X_5. Let E_p denote the exceptional curve over p. Over $\overline{k}$, there are exactly three disjoint (-1)-curves intersecting E_p. The set of these lines is invariant under both $\mathrm{Gal}(\overline{k}/k)$ and g_5, we contract them and get $X_5 \to X_8$, where X_8 is a del Pezzo surface of degree 8, and g_5 descends to an automorphism g_8 of X_8. By Case $d = 8$, g_8 induces an even permutation on $X_8(k)$, and we finish by applying Theorem 1.5.

Suppose p lies on some line, say E_1, on $X_{\overline{k}}$. If p does not lie on any other line, then E_1 must be invariant under both $\mathrm{Gal}(\overline{k}/k)$ and g. We can then blow down E_1 to get $X \to X_7$ where X_7 is a del Pezzo surface of degree 7, and g descends to an automorphism g_7 of X_7. By Case $d = 7$, g_7 induces an even permutation on $X_7(k)$, and we finish by applying Theorem 1.5. Otherwise, p lies on the intersection of two lines, say E_1, E_2. Then the orbit structure of $\{E_1, \ldots, E_6\}$ under $\mathrm{Gal}(\overline{k}/k)$ or g is either (1) $\{E_1\}, \ldots, \{E_6\}$ or (2) $\{E_1, E_2\}, \{E_3, E_6\}, \{E_4, E_5\}$. It follows then that $\{E_3, E_6\}$ must always be invariant under both $\mathrm{Gal}(\overline{k}/k)$ and g, so blowing down E_3, E_6 yields $X \to X_8$ and the automorphism descends to one on X_8. We finish by applying Case $d = 8$ and Theorem 1.5.

Case $(d = 5)$**:** If p does not lie on any exceptional curves, then the blow up $X_4 = \mathrm{Bl}_p(X)$ is a del Pezzo surface of degree 4. Moreover, g lifts to an automorphism g_4 on X_4. Let E_p denote the exceptional curve lying above p. There are 5 pairwise disjoint (-1) curves which intersect E_p, and they must be Galois invariant. Hence we can blow these down to get $X_4 \to \mathbb{P}^2$, and g_4 also descends to an automorphism on $\mathbb{P}^2$. An application of Propositions 3.5 and Theorem 1.5 does the job.

Suppose p lies on a (-1)-curve. We denote the set of (-1)-curves on $X_{\overline{k}}$ by $\{D_{ij}\}$, where $1 \le i < j \le 5$ and D_{ij} intersects D_{kl} if and only if i, j, k, l are all distinct. Suppose that p lies on D_{12}. If p does not lie on any other D_{ij}, then D_{12} is invariant under both $\mathrm{Gal}(\overline{k}/k)$ and g, so we can blow down $X \to X_6$ to a del Pezzo surface of degree 6, and g descends to an automorphism on X_6. We are then done by Case $d = 6$ and Theorem 1.5. If p lies on another line, we can assume this is D_{34}. By the intersection properties, these are the only two lines that p can lie on. It follows then that $D_{12} \cup D_{34}$ is defined over k and invariant under g. The other lines which intersect $D_{12} \cup D_{34}$ are D_{35}, D_{45}, D_{15}, and D_{25}. Hence $D_{35} \cup D_{45} \cup D_{15} \cup D_{25}$ is defined over k and invariant under g. They are pairwise disjoint, and blowing these down gives $X \to \mathbb{P}^2$ and g descends to an automorphism of $\mathbb{P}^2$. We are done after applying Propositions 3.5 and Theorem 1.5.

Case $(d = 4)$**:** First assume that p does not lie on a (-1)-curve. Then the blowup of X at p is a cubic surface $X_3 \subset \mathbb{P}^3$, and the exceptional curve $E \subset X$ is a line in $\mathbb{P}^3$ defined over k. Moreover, each plane $H \subset \mathbb{P}^3$ containing E intersects X_3 residually in a conic, so the pencil of such planes induces a conic bundle $X_3 \to \mathbb{P}^1_k$ defined over k. Corollary 3.17 yields the claim in this case.

Now suppose that p lies on a (-1)-curve. If it lies on only one such curve, then we can blow this curve down, and g will descend to an automorphism of a del Pezzo surface of degree 5. Then Case $d = 5$ and Theorem 1.5 gives the result. Otherwise, p lies on exactly two (-1)-curves. This defines a (singular) conic Q on X. We can then define a conic bundle structure as follows: The linear system $|-K_X|$ induces an embedding of X into $\mathbb{P}^4$ as an intersection of two quadrics. Consider the pencil of hyperplanes containing Q. Each hyperplane intersects X at a conic residual to Q. This defines a morphism $X \to \mathbb{P}^1$ where the fibers are conics. Since g preserves Q and extends to an automorphism of $\mathbb{P}^4$, it preserves the conic bundle structure. Hence, it follows from Corollary 3.17 that g induces an even permutation on $X(k)$.

Case $(d = 3)$**:** If p does not lie on any (-1)-curves, then the automorphism lifts onto the blow up $\mathrm{Bl}_p(X)$ which is a del Pezzo surface of degree 2. Then the result follows from Case $d = 2$ proved in Proposition 3.22 and Theorem 1.5.

Suppose p lies on exactly one (-1)-curve. Then this curve is defined over k and invariant under g. Hence blowing down, g descends to an automorphism g_4 of a del Pezzo surface of degree 4. Then the result follows from Case $d = 4$ and Theorem 1.5.

Suppose p lies on exactly two (-1)-curves L_1, L_2. The plane containing L_1, L_2 intersect X at a third (-1)-curve L_3. Since $L_1 \cup L_2$ is invariant under both Galois action and g, we have L_3 must be also be invariant under both Galois action and g. Hence we can blow down L_3 and conclude as in the previous case.

Suppose p lies on three (-1)-curves L_1, L_2, L_3. Then p is an Eckardt point, and g lifts to an automorphism g_2 on the blow up $\mathrm{Bl}_p(X)$ which is a weak del Pezzo surface of degree 2. The strict transforms of L_i give a Galois invariant set of 3 disjoint (-2) curves on $\mathrm{Bl}_p(X)$. We can blow these down to get $\mathrm{Bl}_p(X) \to Y$, and g_2 descends to an automorphism on Y. The morphism $\mathrm{Bl}_p(X) \to \mathbb{P}^2$ induced by the projection from p, factors through $Y \to \mathbb{P}^2$ which is a double cover ramified along a singular quartic curve. The same argument as in the Case $d = 2$ in Proposition 3.22 shows that every automorphism of Y induces an even permutation. We finish by applying Theorem 1.5. □

To prove Theorem 3.18 for degree $d = 1, 2$, we first begin with a proposition on permutations induced by double covers that will be used in both cases.

Proposition 3.21. *Let $\pi \colon X \to Y$ be a degree two Galois cover of a weighted projective space $Y = \mathbb{P}[a_0, \dots, a_n]$, where a_i are weights, over $k = \mathbb{F}_q$, where $q = 2^m \geq 2$. Suppose X is given by*

$$w^2 + fw + g = 0$$

where f, g are nonzero homogeneous polynomials in the weighted polynomial ring $k[x_0, \dots, x_n]$ of degrees $d, 2d$ respectively.

Let $\beta \in \operatorname{Aut}(X)$ be the deck transformation and $B \subset X$ be the branch locus defined by $f = 0$. Assume that there is an exact sequence of groups

$$1 \longrightarrow \langle \beta \rangle \longrightarrow \operatorname{Aut}(X) \xrightarrow{\pi_*} \operatorname{Aut}(Y)$$

where $\pi_* h = \pi h \pi^{-1}$ for $h \in \operatorname{Aut}(X)$, and that β acts as an even permutation on $X(k)$. Then every $h \in \operatorname{Aut}(X)$ induces an even permutation on $U(k) := X(k) \setminus B(k)$.

Proof. Let $h \in \operatorname{Aut}(X)$ and let $h_0 \in \operatorname{Aut}(Y)$ be the induced automorphism. Since h_0 must fix the ramification locus of π, it follows that $h_0^*(f) = cf$ for some constant $c \in k$. Let $k(X)$ be the function field of X, it is a quadratic extension of $k(Y)$, so by Artin-Shreier theory, it is given by

$$u^2 + u = z$$

for some $z \in k(Y)$. Set $w' = g/(fw)$. Then our original equation becomes

$$w'^2 + w' = g/f^2$$

This is our Artin-Shreier extension. Now consider the double cover coming from the composition $h_0 \circ \pi \colon X \to Y$. Under this viewpoint, we can repeat the same calculation to conclude that $k(X)$ is given by the extension

$$w''^2 + w'' = g'/c^2 f^2$$

where g' is $h_0^*(g)$ It is well-known that these two extensions are the same if and only if there exists some $a \in k(Y)$ such that

$$g'/c^2 f^2 = g/f^2 + a^2 + a$$

So

$$g' = c^2 g + c^2 f^2 (a^2 + a)$$

By degree considerations, we must have $a \in k$.

Define an automorphism $h' \in \operatorname{Aut}(X)$ by

$$x, y, z \mapsto h_0(x), h_0(y), h_0(z), \quad w \mapsto cw + caf.$$

Let us show that h' induces even permutation on $X(k) \setminus B(k)$.

If $a = 0$: Let $p \in \pi(X(k)) \subset Y(k)$ not lying on the branch locus, and O_p be the orbit of p under h_0. Let $i = |O_p|$ and note that $\pi^{-1}(O_p)$ consists of $2i$ many k-points. It follows from $a = 0$ that $\pi^{-1}(O_p)$ breaks into two orbits of size i under h'. Hence h induces an even permutation on $\pi^{-1}(O_p)$. It follows then that h' induces even permutation on $X(k)$.

If $a = 1$: After composing with the Geiser involution (which we know is an even permutation on $U(k)$), we are reduced to case $a = 0$.

If $a \neq 0, 1$: Keep the notation of p, O_p, i as before. Since $h_0^*(f) = cf$, plugging in p gives $f(h_0(p)) = cf(p)$. This implies h_0 rescales the coordinates of p by a constant e such that $e^d = c$. Now

$$h_0^{*i}(g) = c^{2i} g + i(a^2 + a) c^{2i} f^2.$$

Plugging in p, we get

$$c^{2i} g(p) = g(h_0(p)) = c^{2i} g(p) + i(a^2 + a) c^{2i} f(p)^2,$$

so that $i(a^2+a)=0$, which implies i is even. Hence $h'^{*i}(w)=c^i w$, so both points above p are fixed by h'^i. So then $\pi^{-1}(O_p)$ breaks into two orbits of size i under h', which shows h' induces even permutation on $U(k)$ as before.

Now we finish the proof by showing h has even permutation on $U(k)$. The composition hh'^{-1} acts as the identity on Y, so it is either the identity or β. But h' and $\beta h'$ both induce even permutation on $U(k)$, so we are done. □

Proposition 3.22. *The claim of Theorem 3.18 holds for del Pezzo surfaces X of degree $d=K_X^2$ for $d=1,2$.*

Proof. **Case** $(d=2)$**:** The anticanonical divisor embeds X as a hypersurface of degree 4 in the weighted projective space $\mathbb{P}[w:x:y:z]=\mathbb{P}[2:1:1:1]$,

$$w^2+fw=g \tag{3.8}$$

where $f,g\in k[x,y,z]$ have degrees 2, 4 respectively [Kol99, Theorem III.3.5]. The linear system $|-K_X|$ gives a double cover $\pi\colon X\to\mathbb{P}^2$ sending $[w:x:y:z]$ to $[x:y:z]$. The double cover involution on X is called the Geiser involution, which we denote by γ. Since K_X is preserved under any automorphism, we have an exact sequence

$$0\to\langle\gamma\rangle\to\mathrm{Aut}(X)\to\mathrm{Aut}(\mathbb{P}^2). \tag{3.9}$$

Let us first prove that γ induces an even permutation. By Lemma 3.14, it suffices to show that the fixed point set $\mathrm{Fix}(\gamma)(\mathbb{F}_q)$ of γ in $X(k)$ has cardinality $|\mathrm{Fix}(\gamma)(\mathbb{F}_q)|\equiv 1 \bmod 4$. We have

$$\gamma([w:x:y:z])=[-w-f:x:y:z]. \tag{3.10}$$

Over characteristic 2, the fixed locus is given by $f=0$, a conic in $\mathbb{P}^2$. This contains $q+1$ many $\mathbb{F}_q$-points if it is smooth. If singular it contains either 1, $2q+1$, or $q+1$ many $\mathbb{F}_q$-points if it is a union of two conjugate $\mathbb{F}_q$-lines, two $\mathbb{F}_q$-lines, or double line respectively. In particular, $|\mathrm{Fix}(\gamma)(\mathbb{F}_q)|\equiv 1 \bmod 4$, and so γ is even by Lemma 3.14.

Now applying Proposition 3.21, we get that for any $h\in\mathrm{Aut}(X)$ induces an even permutation on $X(k)\setminus B(k)$ where $B:=V(f)$. Hence, to finish the proof for $d=2$, it suffices to show h induces an even permutation on $B(k)$. Since f has degree 2, B is a conic in $\mathbb{P}^2$, so the result follows from Corollary 3.17.

Case $(d=1)$**:** The equation for X can be given as a hypersurface of degree 6 in the weighted projective space $\mathbb{P}[w:z:x:y]=\mathbb{P}[3:2:1:1]$,

$$w^2+a_1wz+a_3w=z^3+a_2z^2+a_4z+a_6 \tag{3.11}$$

where $a_i\in k[x,y]$ is homogeneous of degree i [Kol99, Theorem III.3.5]. The linear system $|-K_X|$ defines a rational map $\rho\colon X\dashrightarrow\mathbb{P}^1$ which sends $[w:z:x:y]$ to $[x:y]$. The fibers of ρ are affine elliptic curves. Since K_X is fixed under any automorphism of X, we have a homomorphism $\mathrm{Aut}(X)\to\mathrm{Aut}(\mathbb{P}^1)$, and set G to be the kernel. Hence, we have an exact sequence

$$1\to G\to\mathrm{Aut}(X)\to\mathrm{Aut}(\mathbb{P}^1).$$

Any $g\in G$ is of the form $g\colon[w:z:x:y]\to[W(w,z,x,y):Z(w,z,x,y):x:y]$, preserves the equation of S, so comparing the degrees in x,y yields that $W=w$ or $W=w-a_1wz-a_3$ and

$Z^3 = z^3$. Moreover, if $a_4 \neq 0$ we have $Z = z$. It follows that if $a_4 \neq 0$, then $G \simeq \mathbb{Z}/2\mathbb{Z}$ and is generated by the involution

$$\beta\colon [w : z : x : y] \mapsto [w - a_1wz - a_3 : z : x : y], \tag{3.12}$$

which is called the Bertini involution. Suppose that $a_4 = 0$. If $a_2 \neq 0$, then $Z^2 = z$ implies that $G = \langle \beta \rangle$. If $a_2 = 0$ and there exists a primitive 3rd root of unity δ, then G is generated by β and $[w : z : x : y] \mapsto [w : \delta z : x : y]$, and hence $G \simeq \mathbb{Z}/6\mathbb{Z}$. If there is no such δ, then $G = \langle \beta \rangle$.

We first show that the unique element β of order two in G induces an even permutation. By Lemma 3.14, it suffices to show that the fixed point set $\mathrm{Fix}(\beta)(\mathbb{F}_q)$ of β in $X(k)$ has cardinality $|\mathrm{Fix}(\beta)(\mathbb{F}_q)| \equiv 1 \bmod 4$. Note that for smooth fibers of the elliptic fibration $\rho\colon X \to \mathbb{P}^1$, β restricts to taking the inverse in the group law of the elliptic curve. Since char $k = 2$, the locus of fixed points is given by $a_1(x, y)z + a_3(x, y) = 0$. Note that $x = y = 0, z = w = 1$ is a fixed rational point, and the only such point when $x = y = 0$. We now proceed by two cases:

If $a_1 \neq 0$, then the fixed locus restricted to the open set $a_1(x, y) \neq 0$ is given by

$$z = a_3(x, y)/a_1(x, y),$$
$$w^2 = z^3 + a_2(x, y)z^2 + a_4(x, y)z + a_6(x, y),$$

which gives q more fixed $\mathbb{F}_q$-points. Now let $x_0, y_0 \in \mathbb{F}_q$, not both zero, be such that $a_1(x_0, y_0) = 0$. If $a_3(x_0, y_0) \neq 0$, then $\rho^{-1}([x_0 : y_0])$ has no fixed $\mathbb{F}_q$-points. If $a_3(x_0, y_0) = 0$, then $\rho^{-1}([x_0 : y_0])$ is a singular affine curve with q-many $\mathbb{F}_q$-points (unique solution in w for every choice of z) which are all fixed under β. Hence, if $a_1 \neq 0$ we have a total of either $q + 1$ or $2q + 1$ fixed $\mathbb{F}_q$-points on X. In particular, $|\mathrm{Fix}(\beta)(\mathbb{F}_q)| \equiv 1 \bmod 4$.

If $a_1 = 0$, then we must have $a_3 \neq 0$ since X is smooth. If $x_0, y_0 \in \mathbb{F}_q$, not both zero, such that $a_3(x_0, y_0) = 0$, then the same argument as above shows that $\rho^{-1}([x_0 : y_0])$ has q many fixed $\mathbb{F}_q$-points. Again, $|\mathrm{Fix}(\beta)(\mathbb{F}_q)| \equiv 1 \bmod 4$. It follows by Lemma 3.14 that β induces an even permutation.

The involution β is also the deck transformation of the double cover $X \to \mathbb{P}[2, 1, 1]$ defined by $[w : z : x : y] \mapsto [z : x : y]$, where $\mathbb{P}[2, 1, 1]$ is the weighted projective space with weights $2, 1, 1$. This double cover is given by $|-2K_X|$ which is preserved under any automorphism of X, so induces an exact sequence

$$1 \to \langle \beta \rangle \to \mathrm{Aut}(X) \to \mathrm{Aut}(\mathbb{P}[2, 1, 1]).$$

Now applying Proposition 3.21, we get that any $h \in \mathrm{Aut}(X)$ induces an even permutation on $X(k) \setminus B(k)$ where $B := V(a_1z + a_3)$. It suffices to show h induces an even permutation on $B(k)$. Since that $p = (x = y = 0, z = w = 1) \in B(k)$ is the unique base point of $|-K_X|$, it is fixed under h. Moreover, since we only care about the rational points, it suffices to consider the reduced subscheme $B_0 := B_{red} \setminus \{p\}$. We proceed by cases:

If $a_1 \neq 0$ and $a_1 \nmid a_3$: B_0 is isomorphic to $\mathbb{A}^1$. Hence $h|_{B_0}$ induces an even permutation by Proposition 3.5.

If $a_1 \neq 0$ and $a_1 \mid a_3$: B_0 is isomorphic to a union of $\mathbb{A}^1$ and $\mathbb{A}^1$ meeting at a point. The result again follows from Proposition 3.5.

If $a_1 = 0$: B_0 is isomorphic to a disjoint union of r copies of $\mathbb{A}^1$ where $0 \leq r \leq 3$. The result again follows from Proposition 3.5. □

Proof of Theorem 3.18. Let X be a rational del Pezzo surface and $d = K_x^2$. The claim follows from Proposition 3.5 for $d = 9$, Proposition 3.20 for $d = 3, \ldots, 8$ and Proposition 3.22 for $d = 1, 2$. □

3.5 Proof of Theorem 1.2

We can finally assemble the proof of Theorem 1.2.

Proof of Theorem 1.2. The statement for elements conjugate to a birational self-map of a conic bundle over $\mathbb{P}^1$ follows from Corollary 3.17 and Theorem 1.5. The statement for elements conjugate to an automorphism of a del Pezzo surface follows from Theorem 3.18 and Theorem 1.5. Finally, for elements of finte order, Lemma 3.13 implies such elements are of the two types above, so we are done. □

4 General studies over perfect fields

4.1 A list of generators

Throughout this section, let k be a perfect field. In this section, we provide a list of generators of $\mathrm{BCr}_2(k)$, for which we will compute the sign of the induce permutation if k is finite.

Lemma 4.1. *Let $k = \mathbb{F}_q$ for $q = p^m$, where $p \geq 2$ is a prime and $m \geq 1$.*

(1) Let p, p', q, q' be four points of degree 2 in $\mathbb{P}^2$ in general position. Then there exists $A \in \mathrm{Aut}(\mathbb{P}^2)$ that sends p, p' onto q, q'.

(2) Let p, q be two points of degree 4 in $\mathbb{P}^2$ in general position. Then there exists $A \in \mathrm{Aut}(\mathbb{P}^2)$ that sends p onto q.

Proof. (1) Let p_1, p_2 (resp. p_1', p_2', resp. q_1, q_2 resp. q_1', q_2') be the geometric components of p (resp. p' resp. q resp. q'). Then each p_i, p_i', q_i, q_i' is defined over $\mathbb{F}_{q^2}$, $i = 1, 2$, and there exists a unique $\mathbb{F}_{q^2}$-automorphism A of $\mathbb{P}^2$ that sends p_i onto q_i and p_i' onto q_i' for $i = 1, 2$. For any $g \in \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ we have

$$(A^g A^{-1})(q_i) = A^g((p_i^{g^{-1}})^g) = (Ap_i^{g^{-1}})^g = (q_i^{g^{-1}})^g = q_i.$$

In particular, $A^g A^{-1}$ is the identity map for all $g \in \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. It follows that A is defined over $\mathbb{F}_q$.

(2) Let p_1, p_2, p_3, p_4 (resp. q_1, q_2, q_3, q_4) its geometric components of p (resp. q). Then each p_i and q_i is defined over $\mathbb{F}_{q^4}$, $i = 1, 2$, and over $\mathbb{F}_{q^2}$, p (resp. q) splits into two orbits, say $\{p_1, p_2\}$ and $\{p_3, p_4\}$ (resp. $\{q_1, q_2\}$ and $\{q_3, q_4\}$). By (1), there exists a $\mathbb{F}_{q^2}$-automorphism A of $\mathbb{P}^2$ that sends p_i onto q_i, $i = 1, \ldots, 4$. As analogously to above, we obtain that $A^g A^{-1} q_i = (Ap_i^{g^{-1}})^g = q_i$ for any $g \in \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ and for $i = 1, \ldots, 4$; hence A is defined over $\mathbb{F}_q$. □

Let S be a smooth projective surface over a perfect field k, B a point or a curve defined over k, and $\pi\colon S \to B$ a surjective morphism over k. We say that S/B is a Mori fibre surface if π has connected fibres, the relative Picard rank $\rho(S/B)$ of S over B is $\rho(S/B) = 1$ and $-K_S$ is π-ample, that is $-K_S \cdot C > 0$ for all curves C contracted by π.

A Sarkisov link is a birational map $\phi\colon S \dashrightarrow S'$ between two Mori fibre spaces $\pi\colon S \to B$ and $\pi'\colon S' \to B'$ that is one of the following four types:

type I: B is a point, B' is a curve and φ is the blow-up of a point.

type II: $B \simeq B'$, and $\phi = \eta_2\eta_1$, where η_1 is the blow-up of a point $p = \{p_1, \ldots, p_d\}$ of degree d with the p_i in general position, and η_2 is the contraction of an orbit of (-1)-curves of cardinality e. We write $\phi = f_{de}$ if we want to emphasize the degree of the base-point of ϕ.

type III: the inverse of a link of type I, i.e. B is a curve, B' is a point and ϕ is the contraction of a Galois-orbit of disjoint (-1)-curves defined over the algberaic closure of k.

type IV: $S = S'$ and B, B' are both curves. If S is rational, then $B = B' \simeq \mathbb{P}^1$ and the ϕ is the exchange of the two fibrations.

Proposition 4.2. *Let $X \to B$ and $X' \to B'$ be Mori fibre surfaces and $\psi\colon X \dashrightarrow X'$ a birational map. Then there is a decomposition $\psi = \phi_r \cdots \phi_1$ into Sarkisov links and isomorphism of Mori fibre surfaces such that*

(1) *for $i = 1, \dots, r-1$, $\phi_{i+1}\phi_i$ is not an automorphism,*

(2) *for $i = 1, \dots, r$, every base-point of ϕ_i is a base-point of $\phi_r \cdots \phi_i$.*

Proof. The claim follows from the proof of [Isk96, Theorem 2.5], see also [BM14, Proposition 2.7]. □

Remark 4.3. In particular, if ψ induces a map $X(k) \to X'(k)$, then the link ϕ_1 does not have any rational base-points. Moreover, the rational base-points of

$$\psi(\phi_1)^{-1} = \phi_r \cdots \phi_2$$

are exactly the base-points of $(\phi_1)^{-1}$. Since $\phi_2\phi_1$ is not an automorphism, ϕ_2 does not have a rational base-point.

The proof of the following proposition is similar to the proof of [BM14, Theorem 1.2], which shows that $\mathrm{BCr}_2(\mathbb{R})$ is generated by $\mathrm{Aut}(\mathbb{P}^2)$ and elements of $\mathrm{BCr}_2(\mathbb{R})$ of degree 5; the latter are in family (1) and they are the only non-linear maps in the generating set from Proposition 4.4 that exist over $k = \mathbb{R}$.

A surface X_d, X'_d denote del Pezzo surfaces of degree d and Q, Q' del Pezzo surfaces of degree 8 with $\rho(Q) = \rho(Q') = 1$.

Proposition 4.4. *Let k be a perfect field. Then $\mathrm{BCr}_2(k)$ is generated by $\mathrm{Aut}(\mathbb{P}^2)$ and the set of elements f in the list below that exist over k.*

(1) *f sends the pencil of conics passing through two points of degree 2 in general position onto a pencil of conics passing through two points of degree 2 in general position.*
If k is finite, we can choose the two pencils to pass through the same points.

(2) *f sends the pencil of conics passing through one point of degree 4 in general position onto a pencil of conics passing through a point of degree 4 in general position.*
If k is finite, we can choose the two pencils to pass through the same points.

(3) *f is one of the following compositions, where X_d is a del Pezzo surface of degree $d = (K_{X_d})^2$ and f_{ab} is a Sarkisov link of type II blowing up a point of degree a and its inverse blowing up a point of degree b:*

$$\begin{tikzcd}
& X_6 \arrow[dl] \arrow[dr] & & & X_2 \arrow[dl] \arrow[dr] & & & X_1 \arrow[dl] \arrow[dr] & & & X_3 \arrow[dl] \arrow[dr] & \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{33}"] & & \mathbb{P}^2 & \mathbb{P}^2 \arrow[rr, dashed, "f_{77}"] & & \mathbb{P}^2 & \mathbb{P}^2 \arrow[rr, dashed, "f_{88}"] & & \mathbb{P}^2 & \mathbb{P}^2 \arrow[rr, dashed, "f_{66}"] & & \mathbb{P}^2
\end{tikzcd} \tag{4.1}$$

or

$$\begin{tikzcd}
 & X_7 \arrow[dl] \arrow[dr, "p"] & & X_{8-d} \arrow[dl] \arrow[dr] & & X_7 \arrow[dl, "p'"'] \arrow[dr] & & d \in \{7,6\} \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"] & & Q \arrow[rr, dashed, "f_{dd}"] & & Q \arrow[rr, dashed, "f_{12}"] & & \mathbb{P}^2 & p' = f_{dd}(p)
\end{tikzcd} \tag{4.2}$$

or

$$\begin{tikzcd}
 & X_7 \arrow[dl] \arrow[dr, "p"] & & X_3 \arrow[dl] \arrow[dr] & & X_{5-d} \arrow[dl] \arrow[dr] & & X_3 \arrow[dl] \arrow[dr] & & X_7 \arrow[dl, "p'"'] \arrow[dr] & & d \in \{3,4\} \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"] & & Q \arrow[rr, dashed, "f_{52}"] & & X_5 \arrow[rr, dashed, "f_{dd}"] & & X_5 \arrow[rr, dashed, "f_{52}^{-1}"] & & Q \arrow[rr, dashed, "f_{12}"] & & \mathbb{P}^2 & p' = f_{52}^{-1} f_{dd} f_{52}(p)
\end{tikzcd} \tag{4.3}$$

or

$$\begin{tikzcd}
 & X_7 \arrow[dl] \arrow[dr, "p"] & & X_3 \arrow[dl] \arrow[dr] & & X_4 \arrow[dl, "p'"'] \arrow[dr] & & p' = f_{52}(p) \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"] & & Q \arrow[rr, dashed, "f_{52}"] & & X_5 \arrow[rr, dashed, "f_{15}"] & & \mathbb{P}^2 &
\end{tikzcd} \tag{4.4}$$

or

$$\begin{tikzcd}
 & X_7 \arrow[dl] \arrow[dr, "p"] & & X_3 \arrow[dl] \arrow[dr] & & X_3' \arrow[dl] \arrow[dr] & & X_7' \arrow[dl, "p'"'] \arrow[dr] & & p' = f_{25} f_{52}(p) \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"] & & Q \arrow[rr, dashed, "f_{52}"] & & X_5 \arrow[rr, dashed, "f_{25}"] & & Q' \arrow[rr, dashed, "f_{12}"] & & \mathbb{P}^2 &
\end{tikzcd} \tag{4.5}$$

or

$$\begin{tikzcd}
 & X_7 \arrow[dl] \arrow[dr, "p"] & & X_5 \arrow[dl] \arrow[dr, "t"] & & X_5' \arrow[dl, "p'"'] \arrow[dr] & & X_7' \arrow[dl, "t'"'] \arrow[dr] & & p' = f_{31}(p) \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"] & & Q \arrow[rr, dashed, "f_{31}"] & & X_6 \arrow[rr, dashed, "f_{13}"] & & Q' \arrow[rr, dashed, "f_{12}"] & & \mathbb{P}^2 & t' = f_{13}(t)
\end{tikzcd} \tag{4.6}$$

or

$$\begin{tikzcd}
 & X_7 \arrow[dl] \arrow[dr, "p"] & & X_5 \arrow[dl] \arrow[dr, "r"] & & X_{6-d} \arrow[dl] \arrow[dr] & & X_5' \arrow[dl, "f_{dd}(r)"'] \arrow[dr] & & X_7' \arrow[dl, "p'"'] \arrow[dr] & & d \in \{2,3,4,5\} \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"] & & Q \arrow[rr, dashed, "f_{31}"] & & X_6 \arrow[rr, dashed, "f_{dd}"] & & X_6' \arrow[rr, dashed, "f_{13}"] & & Q' \arrow[rr, dashed, "f_{12}"] & & \mathbb{P}^2 & p' = f_{13} f_{dd} f_{31}(p)
\end{tikzcd} \tag{4.7}$$

or

$$\begin{tikzcd}
 & X_4' \arrow[dl] \arrow[dr, "p"] & & X_{5-d} \arrow[dl] \arrow[dr] & & X_4' \arrow[dl, "p'"'] \arrow[dr] & & d \in \{4,3\} \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{51}"] & & X_5 \arrow[rr, dashed, "f_{dd}"] & & X_5 \arrow[rr, dashed, "f_{15}"] & & \mathbb{P}^2 & p' = f_{dd}(p)
\end{tikzcd} \tag{4.8}$$

Moreover, all links of the form f_{dd} can be chosen to be involutions, except possibly f_{66} in (4.1), f_{33} and f_{22} in (4.7).

Since the proof of Proposition 4.4 is quite long, we will check afterwards in Lemma 4.5 that the generators (4.5) and (4.6), (4.7, $d = 2$) and (4.8, $d = 4$) are redundant.

Proof. First note that any element in (3) is contained in $\mathrm{BCr}_2(k)$ as they only contract non-rational curves. The list of involutions is from [Isk96, Theorem 2.6]. For (1) and (2), the claim over a finite field k follows from Lemma 4.1.

Let $\psi \in \mathrm{BCr}_2(k)$. There is a decomposition into Sarkisov links $\psi = \phi_r \cdots \phi_1$ as in Proposition 4.2. We do induction on r, the case $r = 0$ corresponding to $\psi \in \mathrm{Aut}(\mathbb{P}^2)$. Let $r \geq 1$. Then ϕ_1 is a link of type I or II, and its base-point is a base-point of ψ, so is of degree ≥ 2. By [Isk96, Theorem 2.6(i,ii)], ϕ_1 a link of type I with a base-point of degree 4 or a link of type II of the form $f_{88}, f_{77}, f_{66}, f_{33}, f_{21}$ or f_{51}. We are going to look at these cases separately.

(a) If $\phi_1 : \mathbb{P}^2 \dashrightarrow X$ is a link of type I, then it is the the blow-up of a point of degree $d_1 = 4$; $X/\mathbb{P}^1$ is a conic bundle whose fibres are the strict transforms of conics through the four points, and $K_X^2 = 5$. Now ϕ_2 is either a link of type II of conic bundles, a link of type III [Isk96, Theorem 2.6(i-iv)], or an isomorphism. As $\phi_2\phi_1 \notin \mathrm{Aut}(\mathbb{P}^2)$ by hypothesis (see Proposition 4.2(1)), ϕ_2 is a link of type II of conic bundles or an isomorphism. Moreover, $\psi\phi_1^{-1} = \phi_r \cdots \phi_2$ is well defined on $X(k)$, so ϕ_2 is well defined on $X(k)$ as well by Remark 4.3. Let $r - 1 \geq s \geq 2$ be the maximal index such that ϕ_i is an isomorphism over $\mathbb{P}^1$ or a link of type II over $\mathbb{P}^1$ without a rational base-point for any $2 \leq i \leq s$. The map $\phi_s \cdots \phi_1$ is a birational map over $\mathbb{P}^1$ from X to a Mori fibre surface $X'/\mathbb{P}^1$. We now look at two cases

If ϕ_{s+1} is a link of type III, then $\nu' := \phi_{s+1}\phi_s \cdots \phi_2\phi_1$ is as in (2). Note that $\psi\nu^{-1} = \phi_r \cdots \phi_{s+2}$ is as in Proposition 4.2.

If ϕ_{s+1} is not a link of type III, then the map $\nu := \phi_1^{-1}\phi_s \cdots \phi_2\phi_1 \in \mathrm{BCr}_2(k)$ is as in (2) and the map $\psi\nu^{-1} = \phi_r \cdots \phi_{s+1}\phi_1$ is as in Proposition 4.2 since the base-point of ϕ_1 is a base-point of $\phi_r \cdots \phi_{s+1}$ by construction.

(b) Suppose that ϕ_1 is a link of type II, i.e. one of the forms f_{33}, f_{66}, f_{77}, f_{88}, f_{21}, or f_{51}. In the first four cases it is of the form (4.1) and we proceed by induction with $\psi\phi_1^{-1} = \phi_r \cdots \phi_2$. If ϕ_1 is of the form f_{21} (case **(b1)**) or f_{51} (case **(b2)**), then ϕ_1^{-1} has a rational base-point p, which is the unique base-point of $\psi\phi_1^{-1} = \phi_r \cdots \phi_2$. Since $\phi_2\phi_1$ is not an automorphism by hypothesis, p is not a base-point of ϕ_2. Then $\phi_2(p)$ is the unique rational base-point of $\psi\phi_1^{-1}\phi_2^{-1} = \phi_r \cdots \phi_3$. It may or may not be a base-point of ϕ_3.

(b1) Suppose that $\phi_1 = f_{21} \colon \mathbb{P}^2 \dashrightarrow Q$. Then ϕ_2 is a link of type I (case **(b1.1)**) or II [Isk96, Theorem 2.6]. If ϕ_2 is a link of II, then it is of the form f_{77}, f_{66}, f_{44} (case **(b1.2)**) or f_{52} (case **(b1.3)**) or f_{31} (case **(b1.4)**) by [Isk96, Theorem 2.6(ii)]. The option $\phi_2 = f_{12}$ does not occur since it forces $\phi_2\phi_1 \in \mathrm{Aut}_k(\mathbb{P}^2)$, which is not allowed by hypothesis.

(b1.1) Suppose that $\phi_2 \colon Q \dashrightarrow X$ is a link of type I. Then it is the inverse of blowing-up a point t of degree 2 [Isk96, Theorem 2.6(i)]. Then $K_X^2 = 6$ and $X \to \mathbb{P}^1$ is a Mori fibre space whose fibres are the images by $\phi_2\phi_1$ of conics in $\mathbb{P}^2$ passing through p and $\phi_1^{-1}(t)$. Now, ϕ_3 is an isomorphism or a link ϕ_3 of type II or III. We will assume that ϕ_3 is not an isomorphism, as otherwise we can assume that ϕ_4 is not an isomorphism and continue the argument below with ϕ_4 instead of ϕ_3. Since $\phi_3\phi_2$ is not an automorphism by hypothesis, $\phi_3 \colon X \dashrightarrow X'$ is a link of type II over $\mathbb{P}^1$.

(b1.1.i) If ϕ_3 has a rational base-point q, then $q = \phi_2(p)$, where p is the base-point of ϕ_1^{-1}, as it is the unique rational base-point of $\phi_r \cdots \phi_3$ by hypothesis, see (b). There exists a link $\phi_2' \colon X' \to Q'$ of type III to a quadric surface Q'. Let $q' \in X'$ be the base-point of ϕ_3^{-1}. It is a rational point, so there exists a link $f_{12} \colon Q' \dashrightarrow \mathbb{P}^2$ of type II with base-point $\phi_2'(q')$. The map $\nu := f_{12}\phi_2'\phi_3\phi_2\phi_1 \in \mathrm{BCr}_2(k)$ sends the pencil of conics through $p, \phi_1^{-1}(t)$ onto the pencil of conics through the base-point of f_{12}^{-1} and the image by f_{12} of the base-point of ϕ_2^{-1}, hence belongs to the family (1). The map $\psi\nu^{-1} = \phi_r \cdots \phi_4\phi_2' f_{12}^{-1}$ is a decomposition as in Proposition 4.2 and we can proceed by induction.

(b1.1.ii) Suppose that ϕ_3 has no rational base-point. Let $3 \leq s \leq r - 1$ be the maximal index such that ϕ_i is an isomorphism over $\mathbb{P}^1$ or a link of type II with no rational base-points for all $3 \leq i \leq s$ and consider the map $\phi_s \cdots \phi_3 \colon X \dashrightarrow X'$. The map ϕ_{s+1} is a link of type III or a link of type II with a rational base-point. If ϕ_{s+1} is a link of type II, we proceed as in (b1.1.i) with $\phi_{s+1}\phi_s \cdots \phi_3$ instead of ϕ_3. If ϕ_{s+1} is a link of type III, then ϕ_{s+1} is a contraction $X' \to Q'$

to a quadric surface Q'. Recall from (b) that $\phi_2(p)$ is the unique rational base-point of $\phi_r \cdots \phi_3$, where p is the base-point of ϕ_1^{-1}. There exists a link $f_{12}\colon Q' \dashrightarrow \mathbb{P}^2$ of type II with base-point $(\phi_{s+1}\phi_s \cdots \phi_3\phi_2)(p)$. The map $\nu := f_{12}\phi_{s+1} \cdots \phi_1$ sends the pencil of conics through $p, \phi_1^{-1}(t)$ onto the pencil of conics through the base-point of f_{12}^{-1} and the image by f_{12} of the base-point of ϕ_{s+1}^{-1}. We proceed as in (b1.1.i).

(b1.2) If $\phi_2 \in \{f_{77}, f_{66}\}$, then ϕ_2 is, up to an automorphism of Q, a birational involution of Q [Isk96, Theorem 2.6(ii)]. Recall from (b) that ϕ_1^{-1} has a rational base-point $p \in Q$, which is the unique rational base-point of $\phi_r \cdots \phi_2$. There exists a link $f_{12}\colon Q \dashrightarrow \mathbb{P}^2$ of type II with base-point $\phi_2(p)$. Then $f_{12}\phi_2\phi_1 \in \mathrm{BCr}_2(k)$ and is as in (4.2). Furthermore, $\psi(f_{12}\phi_2\phi_1)^{-1} = \phi_r \cdots \phi_3 f_{12}^{-1}$ is a decomposition as in Proposition 4.2 as the base-point of f_{12}^{-1} is a base-point of $\phi_r \cdots \phi_3 f_{12}^{-1}$ by construction.

If $\phi_2 = f_{44}\colon Q \dashrightarrow Q'$, let $f_{12}\colon Q' \dashrightarrow \mathbb{P}^2$ be the link of type II with $\phi_2(p)$ as base-point and q, q' the base-point of ϕ_2, ϕ_2^{-1}, respectively. Then $f_{12}\phi_2\phi_1$ sends the pencil of conics through $\phi_1^{-1}(q)$ onto the pencil of conics through $f_{12}(q')$, so it is a member of (2).

(b1.3) Suppose that $\phi_2 = f_{52}\colon Q \dashrightarrow X_5$, where X_5 is a del Pezzo surface of degree 5. Then ϕ_3 is one of $f_{33}, f_{44}, f_{15}, f_{25}$ [Isk96, Theorem 2.6].

If $\phi_3 \in \{f_{33}, f_{44}\}$, then it is a birational self-map of X_5 [Isk96, Theorem 2.6(ii)]. Let $f_{12}\colon Q \dashrightarrow \mathbb{P}^2$ be a link of type II with base-point $(\phi_2^{-1}\phi_3\phi_2)(p)$, where p is the (rational) base-point of ϕ_1^{-1} according to (b). Then $\nu := f_{12}\phi_2^{-1}\phi_3\phi_2\phi_1$ is in the family (4.3) and $\psi\nu^{-1} = \phi_r \cdots \phi_4\phi_2 f_{12}^{-1}$ is a decomposition as in Propostion 4.2.

If $\phi_3 = f_{15}$, then its base-point is $q = \phi_2(p)$ by (b) and so $\phi_3\phi_2\phi_1$ is as in (4.4).

If $\phi_3 = f_{25}$, then it is a map to a quadric surface Q'. Let $f_{12}\colon Q' \dashrightarrow \mathbb{P}^2$ be a link of type II whose base-point is $\phi_3\phi_2(p)$, where p is the (rational) base-point of ϕ_1^{-1} according to (b). Then $f_{12}\phi_3\phi_2\phi_1 \in \mathrm{BCr}_2(k)$ is as in (4.5), and $\psi(f_{12}\phi_3\phi_2\phi_1)^{-1} = \phi_r \cdots \phi_4 f_{12}^{-1}$ is a decomposition as in Proposition 4.2.

(b1.4) If $\phi_2 = f_{31}\colon Q \dashrightarrow X_6$, then $\psi\phi_1^{-1}\phi_2^{-1} = \phi_r \cdots \phi_3$ has two rational base-points, namely $\phi_2(p)$ and the base-point t of ϕ_2^{-1}. Furthermore, ϕ_3 is a link of type II of the form $f_{55}, f_{44}, f_{33}, f_{22}$ or f_{13} or a link of type III to a quadric surface [Isk96, Theorem 2.6]. The latter forces $\phi_3\phi_2$ to be an automorphism, which contradicts our hypothesis, see Proposition 4.2(1).

Suppose that $\phi_3 = f_{13}\colon X_6 \dashrightarrow Q'$ is a link to a quadric surface Q'. As $\psi\phi_1^{-1}\phi_2^{-1} = \phi_r \cdots \phi_3$ has exactly two rational base-points, namely $\phi_2(p)$ and t, and the base-point of q of ϕ_3 is a base-point of $\phi_r \cdots \phi_3$ by hypothesis (see Proposition 4.2(2)), it follows that $q = \phi_2(p)$ or $q = t$. The latter forces $\phi_3\phi_2$ to be an automorphism, which contradicts our hypothesis (see Proposition 4.2(1)), so $q = \phi_2(p)$. Let $f_{12}\colon Q' \dashrightarrow \mathbb{P}^2$ be a link of type II with base-point $\phi_3\phi_2(t)$. Then $\nu := f_{12}\phi_3\phi_2\phi_1$ is of the form (4.6) and $\psi\nu^{-1} = \phi_r \cdots \phi_4 f_{12}^{-1}$ is as in Proposition 4.2.

Suppose that $\phi_3\colon X_6 \dashrightarrow X_6'$ is one of $f_{55}, f_{44}, f_{33}, f_{22}$. There is a link $f_{13}\colon X_6' \dashrightarrow Q'$ of type II with base-point $\phi_3(t)$, and $f_{12}\colon Q' \dashrightarrow \mathbb{P}^2$ a link of type II with base-point $f_{13}\phi_3\phi_2(p)$. Then $\nu := f_{12}f_{13}\phi_3 \cdots \phi_1$ is of the form (4.7) and $\psi\nu^{-1} = \phi_r \cdots \phi_4 f_{13}^{-1} f_{12}^{-1}$ is a decomposition as in Proposition 4.2. By [Isk96, Theorem 2.6], f_{55} and f_{44} can be taken to be birational involutions.

(b2) Finally, suppose that $\phi_1 = f_{51}\colon Q \dashrightarrow X_5$. Then, as ϕ_2 has no rational base-point by (b), it is a link of type II and hence of the form f_{44}, f_{33}, f_{25} [Isk96, Theorem 2.6]. We proceed as in case (b1.3) with ϕ_2 instead of ϕ_3 and construct a map as in (4.8) if $\phi_2 = f_{dd}$, $d = 3, 4$, or the inverse of a map of type (4.4) if $\phi_2 = f_{25}$.

□

Lemma 4.5. *In the list in Proposition 4.4, the generators (4.5) and (4.6), (4.7, $d=2$) and (4.8, $d=4$) are redundant.*

Proof. **(4.5):** Consider a map $\psi := f_{12}f_{25}f_{52}f_{21}$ as in (4.5) and denote by q_5 (resp. q_2) the base-point of f_{52} (resp. f_{25}) and q_2' (resp. q_5') the base-point of f_{52}^{-1} (resp. f_{25}^{-1}). We complete the blow-up diagram of ψ given in Proposition 4.4(4.5) as follows:

$$\begin{tikzcd}
 & & & X_1 \arrow[llld, "q_5"'] \arrow[ld, "q_2'"'] \arrow[rd, "q_2"] \arrow[rrrd, "q_5'"] & & & \\
X_6 \arrow[rd, "q_2'"'] & & X_3 \arrow[ld, "q_5"'] \arrow[rd, "q_2"'] & & X_3' \arrow[ld, "q_2'"] \arrow[rd, "q_5'"] & & X_6' \arrow[ld, "q_2"] \\
 & Q \arrow[rr, dashed, "f_{52}"] & & X_5 \arrow[rr, dashed, "f_{25}"] & & Q' &
\end{tikzcd}$$

Thus ψ sends the pencil of conics through the base-point of f_{21} and $f_{21}^{-1}(q_2')$ onto the pencil of conics through the base-point of f_{12}^{-1} and $f_{12}(q_2)$, and is hence in the family (1).

(4.6): Consider a map $\psi := f_{12}f_{13}f_{31}f_{21}$ as in (4.6) and denote by q_2, q_3, q_3', q_2' the base-point of $f_{21}, f_{31}, f_{13}^{-1}, f_{12}^{-1}$ respectively. We complete the blow-up diagram of ψ given in Proposition 4.4(4.6) as follows:

$$\begin{tikzcd}
 & & & & X_4 \arrow[llld, "q_3"'] \arrow[ld, "p'"'] \arrow[rd, "t"] \arrow[rrrd, "q_3'"] & & & & \\
 & X_7 \arrow[ld, "q_2"'] \arrow[rd, "p"] & & X_5 \arrow[ld, "q_3"'] \arrow[rd, "t"] & & X_5' \arrow[ld, "p'"'] \arrow[rd, "q_3'"] & & X_7' \arrow[ld, "t'"'] \arrow[rd, "q_2'"] & \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"] & & Q \arrow[rr, dashed, "f_{31}"] & & X_6 \arrow[rr, dashed, "f_{13}"] & & Q' \arrow[rr, dashed, "f_{12}"] & & \mathbb{P}^2
\end{tikzcd}$$

where $p' = f_{31}(p)$ and $t' = f_{13}(t)$. Let r_1, r_2 (resp. s_1, s_2, s_3) be the geometric components of q_2 (resp. $f_{21}^{-1}(q_3)$). On X_4, there are exactly sixteen (-1)-curves over the algebraic closure $\bar{k}$ of k:

- The exceptional divisor of r_1, r_2; they make up an orbit of length 2.
- The exceptional divisor of s_1, s_2, s_3; they make up an orbit of length 3.
- The strict transform of the conic through r_1, r_2, s_1, s_2, s_3, which is rational.
- The strict transform of the line through r_1, r_2, which is rational.
- The strict transform of the line through s_i, s_j, $i \neq j$; they make up an orbit of length 3.
- The strict transform of the line through r_i, s_j; they make up an orbit of length 6 whose members are not disjoint.

It follows that the blow-up of q_2, q_2' is redundant and $\psi = f_{33}$.

(4.7, $d=2$): Consider a map $\psi := f_{12}f_{13}f_{22}f_{31}f_{21}$ as in (4.7) and denote by q_3, q_2, q_2', q_3' the base-points of $f_{31}, f_{22}, f_{22}^{-1}, f_{13}^{-1}$ respectively. We complete the blow-up of ψ given in Proposition 4.4(4.7) as follows:

$$\begin{tikzcd}
 & & X_6 \arrow[dd, "q_2"'] & & & X_3 \arrow[lll, "q_3"'] \arrow[rrr, "q_3'"] \arrow[lld, "q_2"] \arrow[d, "t"] \arrow[rrd, "q_2'"] & & & X_6' \arrow[dd, "q_2'"] & & \\
 & X_7 \arrow[ld] \arrow[rd, "p"] & & X_5 \arrow[ld, "q_3"] \arrow[rd, "t"] & & X_4 \arrow[ld, "q_2"'] \arrow[rd, "q_2'"] & & X_5' \arrow[ld, "t'"'] \arrow[rd, "q_3'"'] & & X_7' \arrow[ld, "p'"] \arrow[rd] & \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"'] & & Q \arrow[rr, dashed, "f_{31}"'] & & X_6 \arrow[rr, dashed, "f_{22}"'] & & X_6' \arrow[rr, dashed, "f_{13}"'] & & Q' \arrow[rr, dashed, "f_{12}"'] & & \mathbb{P}^2
\end{tikzcd}$$

where $p' = (f_{13}f_{22}f_{31})(p)$ and $t' = f_{22}(t)$. Thus ψ belongs to the family (1).

(4.8, $d = 4$): Consider a map $\psi := f_{15}f_{44}f_{51}$ as in (4.8). Let q_4, q_4', q_5, q_5' be the base-point of $f_{44}, f_{44}^{-1}, f_{51}, f_{15}$, respectively. We complete the blow-up of ψ given in Proposition 4.4(4.8) as follows, where Y is the blow-up of X_1 at the point p, and is not a del Pezzo surface:

$$\begin{tikzcd}
 & & & & Y \arrow[dllll, "q_5"'] \arrow[dll, "q_4"] \arrow[d, "p"] \arrow[drr, "q_4'"'] \arrow[drrrr, "q_5'"] & & & & \\
X_5' \arrow[dr, "q_4"'] & & X_4 \arrow[dl, "q_5"'] \arrow[dr, "p"] & & X_1 \arrow[dl, "q_4"'] \arrow[dr, "q_4'"] & & X_4' \arrow[dl, "p'"'] \arrow[dr, "q_5'"] & & X_5'' \arrow[dl, "q_4'"] \\
 & \mathbb{P}^2 \arrow[rr, dashed, "f_{51}"] & & X_5 \arrow[rr, dashed, "f_{44}"] & & X_5 \arrow[rr, dashed, "f_{15}"] & & \mathbb{P}^2 &
\end{tikzcd}$$

where $p' = f_{dd}(p)$. With Lemma 4.1, we obtain that ψ is in the family (2). □

Lemma 4.6. *Let $\mathbf{T} \subset \mathrm{Cr}_2(k)$ be the set of generators for $\mathrm{Cr}_2(k)$ given in* [Isk91]*. Then $\mathbf{T} \cap \mathrm{BCr}_2(k)$ forms a set of generators for $\mathrm{BCr}_2(k)$.*

Proof. We compare the list of generators in [Isk91] contained in $\mathrm{BCr}_2(k)$ with the list of generators in Proposition 4.4, and see that the two lists coincide, if we replace "preserving the pencil of conics through a point of degree 4 (resp. two points of degree 2)" by "sending the pencil of conics trough a point of degree 4 (resp. two points of degree 2) onto a pencil of conics of the same kind" in [Isk91]:

Prop. 4.4	(1)	(2)	(4.1)	(4.2)	(4.3)
[Isk91]	A11	(15),(20)	(7),(8),(19'),(15"')	(10),(11)	(12),(13)

Prop. 4.4	(4.4)	(4.5)	(4.6)	(4.7)	(4.8)
[Isk91]	A17	(14)	(19')	(16),(17),(11"),(18)	(21),(22)

while type (9), (9'), (11'), (15'), (15"), (19) from [Isk91] are not contained in $\mathrm{BCr}_2(k)$. Note that (4.6) is covered by (19') by Lemma 4.5. □

4.2 Revisiting the parity problem

In this section we prove that almost all of the generators given in Proposition 4.4 can only induce an even permutation when the ground field is $k = \mathbb{F}_{2^m}$ for $m > 1$. We will rely heavily on the results proven in Section 3.

4.2.1 Parities of the generators (4.1)

Here we prove that f_{33}, f_{77}, and f_{88} always induce even permutation.

Up to an automorphism of $\mathbb{P}^2$, the maps f_{77} and f_{88} are Geiser and Bertini involutions respectively. They are given by equations (3.10) and (3.12) respectively. By Theorem 3.18, these and hence f_{77} and f_{88} induce even permutation on $\mathbb{P}^2(\mathbb{F}_{2^m})$, $m > 1$.

The birational map f_{33} is the usual quadratic transformation which is defined as follows. Fix three non-colinear points in $\mathbb{P}^2$. The linear system of conics passing through these points defines a birational map $f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$, called a *quadratic transformation.* Choose a coordinate system $[x : y : z]$ for $\mathbb{P}^2$. Then, up to a projective transformation (over $\bar{k}$), the map is given by the equation $f([x : y : z]) = [yz : xz : xy]$.

Proposition 4.7. *Let $f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ be a quadratic transformation over a finite field $\mathbb{F}_{2^m}$. Suppose f is regular. Then the permutation induced on the points $\mathbb{P}^2(k)$ under σ is odd when $m = 1$ and even when $m > 1$.*

Proof. The base points of f form a Galois orbit under some Galois action σ of order three:

$$p = [a : b : c], \quad p^\sigma = [a^\sigma : b^\sigma : c^\sigma], \quad p^{\sigma^2} = [a^{\sigma^2} : b^{\sigma^2} : c^{\sigma^2}].$$

Let $s : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ be the standard quadratic transformation defined by the three base points $[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1]$. Consider the action of $\mathrm{PGL}(3)$ on $\mathbb{P}^2$ as the multiplication from the left on column vectors. Under the linear transformation

$$g := \begin{pmatrix} a & a^\sigma & a^{\sigma^2} \\ b & b^\sigma & b^{\sigma^2} \\ c & c^\sigma & c^{\sigma^2} \end{pmatrix},$$

we have $f = gsg^{-1}$. The fix points under the standard transformation s are

$$[1 : 1 : 1], \quad [-1 : 1 : 1], \quad [1 : -1 : 1], \quad [1 : 1 : -1]$$

which are all the same over characteristic two, so f has exactly one fix point

$$g([1 : 1 : 1]) = [a + a^\sigma + a^{\sigma^2} : b + b^\sigma + b^{\sigma^2} : c + c^\sigma + c^{\sigma^2}]$$

which is clearly defined over k. Note that f is an involution:

$$f \circ f = (gsg^{-1}) \circ (gsg^{-1}) = s \circ s = \mathrm{id}.$$

Hence f acts on $\mathbb{P}^2(k)$ as a product of $\frac{1}{2}(2^{2m} + 2^m)$ transpositions. Thus the permutation is odd when $m = 1$ and even when $m > 1$. □

4.2.2 Parities of the generators (4.2) to (4.8)

Any birational map $f \in \mathrm{BCr}_2(k)$ which over $\bar{k}$ is a Geiser involution (resp. Bertini involution) up to an element of $\mathrm{PGL}_3(k)$ lifts to an automorphism of a del Pezzo surface of degree 2 (resp. degree 1). In fact, the geometric description of f is analogous to the one of the Geiser involution (resp. Bertini involution) over $\bar{k}$ and to the Geiser involution (resp. Bertini involution) over k with only one base-point. It yields directly that f lifts to an automorphism of a del Pezzo surface of degree 2 (resp. degree 1). Hence, f induces an even permutation by Theorem 3.18.

Generator (4.2), (4.3), or (4.7, $d = 4, 5$): Let f be the corresponding birational map. Note that we can take f_{dd} in the respective generator to be an involution, so that geometrically f_{dd} is either a Geiser or Bertini involution, which induces an even permutation. Upon applying an automorphism of $\mathbb{P}^2$ or Q, we can assume that f is conjugate to f_{dd}. Hence, f also induces an even permutation by Theorem 1.5.

Generator (4.4): Let q_2 be a point of degree 2 and q_5 a point of degree 5, both in general position. Over $\bar{k}$ there are exactly two cubic curves passing through q_5, q_2 with a double point at one of the points of q_2, and we call C_2 its orbit over k. Similarly, there are exactly five cubic curves with a double point at one of the points of q_5, and we call C_5 its orbit over k. We complete the blow-up diagram of $f = f_{15}f_{52}f_{21}$. By abuse of notation we write p for $f_{21}(L)$, $f_{52}(p)$ and their image in X_3. In X_3 there are exactly two curves which over $\bar{k}$ are orbits of disjoint (-1)-curves of length 2 and 5, namely the strict transforms of C_2 and C_5, denoted by $\tilde{C}_2$ and $\tilde{C}_5$.

$$\begin{tikzcd}
& & & X_2 \arrow[lld, "q_5"'] \arrow[d, "p"] \arrow[rrd, "\tilde{C}_2"] & & & \\
& X_7 \arrow[ld, "q_2"'] \arrow[rd, "p"] & & X_3 \arrow[ld, "q_5"'] \arrow[rd, "\tilde{C}_2"] & & X_4 \arrow[ld, "p"'] \arrow[rd, "\tilde{C}_5"] & \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"] & & Q \arrow[rr, dashed, "f_{52}"] & & X_5 \arrow[rr, dashed, "f_{15}"] & & \mathbb{P}^2
\end{tikzcd}$$

The blow-up diagram of f shows that f has the same geometric description as a Geiser involution over k with base-points q_2 and q_5. Thus, up to composition by an element of $\mathrm{PGL}_3(k)$, f lifts to an automorphism of the del Pezzo surface X_2. Now Theorem 3.18 and Proposition 3.5 imply that f induces en even permutation over $k = \mathbb{F}_q, q = 2^m \geq 4$.

Generator (4.5) By Lemma 4.5, this map is, up to an automorphism of $\mathbb{P}^2$, a member of the family (1) and hence induces an even permutation for $k = \mathbb{F}_{2^m}$, $m \geq 2$ by Corollary 3.17.

Generator (4.6) By Lemma 4.5, this generator is equal to f_{33}, so is treated in Proposition 4.7.

Generator (4.7, $d = 3$) We can complete the blow up diagram as in Lemma 4.5 to get

$$\begin{tikzcd}
& & X_5'' \arrow[dd, "p_3"'] & & & X_2 \arrow[lll, "q_3"'] \arrow[rrr, "q_3'"] \arrow[lld, "p_3"] \arrow[d, "t"] \arrow[rrd, "p_3'"] & & & X_5''' \arrow[dd, "p_3'"] & & \\
& X_7 \arrow[ld] \arrow[rd, "p"] & & X_5 \arrow[ld, "q_3"] \arrow[rd, "t"] & & X_3 \arrow[ld, "p_3"'] \arrow[rd, "p_3'"] & & X_5' \arrow[ld, "t'"'] \arrow[rd, "q_3'"'] & & X_7' \arrow[ld, "p'"] \arrow[rd] & \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{21}"'] & & Q \arrow[rr, dashed, "f_{31}"'] & & X_6 \arrow[rr, dashed, "f_{33}"'] & & X_6' \arrow[rr, dashed, "f_{13}"'] & & Q' \arrow[rr, dashed, "f_{12}"'] & & \mathbb{P}^2
\end{tikzcd}$$

where q_3, p_3, q_3', p_3' are the base points of $f_{31}, f_{33}, f_{13}, f_{33}^{-1}$ respectively. Hence, the composition $f_{13}f_{33}f_{31}$ is geometrically a Geiser involution. Hence the permutation induced on $Q \dashrightarrow Q$ is even. Since $f = f_{12}f_{13}f_{33}f_{31}f_{21}$ is conjugate to $f_{13}f_{33}f_{31}$ (upon applying automorphism of $\mathbb{P}^2$), f also induces an even permutation by Theorem 1.5.

Generator (4.8) The case $d = 4$ follows from Lemma 4.5. If $d = 3$, we have the blow up diagram,

$$\begin{tikzcd}
& & & X_1 \arrow[lld, "q_3"] \arrow[d, "p"] \arrow[rrd, "q_3'"] & & & \\
& X_4 \arrow[ld, "q_5"'] \arrow[rd, "p"] & & X_2 \arrow[ld, "q_3"'] \arrow[rd, "q_3'"] & & X_4' \arrow[ld, "p'"'] \arrow[rd, "q_5'"] & \\
\mathbb{P}^2 \arrow[rr, dashed, "f_{51}"] & & X_5 \arrow[rr, dashed, "f_{33}"] & & X_5 \arrow[rr, dashed, "f_{15}"] & & \mathbb{P}^2
\end{tikzcd}$$

where q_3, q_3', q_5, q_5' are the base points of $f_{33}, f_{33}^{-1}, f_{51}, f_{15}$ respectively. Hence, $f = f_{15}f_{33}f_{51}$ is a Bertini involution, so f induces an even permutation.

Proof of Corollary 1.3. By Corollary 3.17 and results proven in §4.2.1 and §4.2.2, it follows that the only generator listed in Proposition 4.4 for which we do not know to induce even permutations is f_{66} in (4.1). □

The difficulty in proving that f_{66} induces an even permutation is that the points of degree 6 being blown up by f_{66} and its inverse cannot be identified with one another via an automorphism on the respective surface. This is in contrast with f_{33}, f_{77}, f_{88} in which we were able to do this. In particular, we cannot apply Theorem 1.2.

4.3 Some basic properties

In this section we prove the remaining parts of Therorem 1.1:

Theorem 4.8. *Let k be a perfect field. Then $\mathrm{BCr}_2(k)$ satisfies the following properties:*

(1) *$\mathrm{BCr}_2(k)$ is not finitely generated if k admits a quadratic extension.*

(2) *$\mathrm{BCr}_2(k) \subset \mathrm{Cr}_2(k)$ is not a normal subgroup.*

(3) *$\mathrm{BCr}_2(k) \subset \mathrm{Cr}_2(k)$ is of infinite index.*

The Cremona group $\mathrm{Cr}_2(k)$ itself is not finitely-generated over any field k [Can12, Proposition 3.3], [Can18, Proposition 3.6]. Our proof for (1) borrows ideas from Cantat's proof.

This proof is organized as follows. We first prove (1) for fields k such that $\overline{k}/k$ is a finite extension. For (1) in all other cases, our strategy is to construct elements of $\mathrm{BCr}_2(k)$ whose indeterminacy locus consists of a point of arbitrarily large degree. The construction is a Sarkisov link of type II for conic bundles. We prove (2) in §4.3.2 and (3) in §4.3.2. The proof of Theorem 4.8 is given at the end of this section.

4.3.1 Non-finite generation of $\mathrm{BCr}_2(k)$

Let k_0 be the prime field of k, which is either $\mathbb{Q}$ or $\mathbb{F}_q$ depending on the characteristic. For each $f \in \mathrm{BCr}_2(k)$, let $\mathrm{Bs}(f) \subset \mathbb{P}^2(\overline{k})$ denote the indeterminacy locus of f. For any extension K/k_0, we say $\mathrm{Bs}(f)$ is defined over K if every point in $\mathrm{Bs}(f)$ is defined over K. Let k_f be the minimal field extension of k_0 satisfying:

(1) f and f^{-1} are both defined over k_f,

(2) $\mathrm{Bs}(f)$ and $\mathrm{Bs}(f^{-1})$ are both defined over k_f.

Lemma 4.9. *If $[\bar{k} : k] < \infty$, then $\mathrm{BCr}_2(k)$ is not finitely-generated.*

Proof. Assume that $\mathrm{BCr}_2(k)$ is generated by a finite subset S. Let k_S be the compositum of $\{k_f\}_{f \in S}$. Since every $g \in \mathrm{BCr}_2(k)$ is a composition of elements of S, it follows that $k_g \subseteq k_S$. Choosing $g \in \mathrm{PGL}_3(k)$ to be the map $g\colon [x : y : z] \mapsto [x + ay : y : z]$ for some $a \in k$, we obtain that $k_g = k_0(a) \subseteq k_S$. As $a \in k$ is arbitrary, we have $k \subseteq k_S$. Now, $k_0 \subseteq k \subseteq k_S$ is a tower of field extensions where $[k_S : k]$ is finite and k_S is finitely-generated over k_0. By the Artin-Tate lemma, k is a finitely-generated extension of k_0, which is impossible for fields with $[\bar{k} : k] < \infty$ (see for instance [Jac89, Theorem 8.37] for this basic fact from field theory). □

Proposition 4.10. *Suppose that $[\overline{k} : k] = \infty$, and let T be a quadratic extension of k and K/T be a non-trivial extension. Then there exists $f \in \mathrm{BCr}_2(k)$ whose base locus contains a point of degree $[K : k]$ over k.*

The construction of the Cremona maps in Proposition 4.10 requires careful selections of the candidates for the indeterminacy points in $\mathbb{P}^2$. Before we prove Proposition 4.10, we first prove two statements which help us accomplish the positioning problem.

Remark 4.11. Suppose that $[\overline{k}:k]=\infty$ and that k has a quadratic extension T/k. There exists four points $\{a_1,a_2,b_1,b_2\}$ in $\mathbb{P}^2(T)$ such that $\{a_1,a_2\}$ and $\{b_1,b_2\}$ form $\mathrm{Gal}(T/k)$-orbits, and no three of these four points are collinear. Indeed, pick any $a_1\in\mathbb{P}^2(T)\setminus\mathbb{P}^2(k)$. Let a_2 be its Galois conjugate. Consider the k-line α spanned by a_1 and a_2. Take β to be any other k-line. Since $\beta\cong\mathbb{P}^1$ over k, we can find a pair of Galois-conjugate points $\{b_1,b_2\}$ on β.

As a consequence of Remark 4.11, there exists a unique conic C_x through $\{a_1,a_2,b_1,b_2,x\}$ for every $x\in\mathbb{P}^2\setminus\{a_1,a_2,b_1,b_2\}$, which degenerates if and only if x lies on the line spanned by any two of the four points [BKT08, Theorem 1]. In particular, all but three of these conics are smooth, and the three degenerate ones consists of

$$\begin{aligned}C_0&=\mathrm{span}(a_1,a_2)\cup\mathrm{span}(b_1,b_2),\\ C_1&=\mathrm{span}(a_1,b_1)\cup\mathrm{span}(a_2,b_2),\\ C_2&=\mathrm{span}(a_1,b_2)\cup\mathrm{span}(a_2,b_1).\end{aligned}$$

Note that C_0, C_1, and C_2 are all defined over k.

Lemma 4.12. *Let k,T and a_1,a_2,b_1,b_2 as in Remark 4.11. Let $\ell_1\subset\mathbb{P}^2$ be a line over T passing through a_1, but not a_2,b_1,b_2, and let ℓ_2 be its $\mathrm{Gal}(T/k)$-conjugate. Let K/T be a Galois extension. There exists a closed point $x\in\ell_1$ defined over K/k but not over any proper subfield, such that*

(1) *r of the $\mathrm{Gal}(K/k)$-conjugates of x lie on ℓ_1 (resp. ℓ_2), where $r=\frac{1}{2}[K:k]$.*

(2) *Let $x_1=x,...,x_{2r}$ be the Galois conjugates of x. For each $1\le i\le 2r$, the unique conic passing through $\{a_1,a_2,b_1,b_2,x_i\}$ is non-singular.*

(3) *If x_i,x_j are any two distinct conjugates of x, the six points a_1, a_2, b_1, b_2, x_i, x_j do not lie on any conic.*

Proof. By the primitive element theorem, $K=k(z)$ for some $z\in K$, which can be seen as a K-point $z\in\mathbb{P}^1(K)=K\cup\{\mathrm{pt}\}$. Let $\{z=z_1,...,z_{2r}\}$ be the Galois orbit of z in the base $\mathbb{P}^1$. The space of conics in $\mathbb{P}^2$ passing through a_1,a_2,b_1,b_2 is parameterized by $\mathbb{P}^1$. Let $F_1,...,F_{2r}$ be the conics in $\mathbb{P}^2$ corresponding to the points $z_1,...,z_{2r}$, respectively. The conic F_1 intersects ℓ_1 at the point a_1, which is defined over K. Moreover, F_1 cannot be tangent to ℓ_1 at a_1 since otherwise F_1 is defined over T. Hence the residual intersection with ℓ_1 will be a point $x\neq a_1$ defined over K. Its Galois orbit $\{x_1=x,...,x_{2r}\}$ can be labeled in such a way so that x_i is on the conic F_i. In particular, they are all distinct. They equally distribute on l_1 and l_2 since $\mathrm{Gal}(T/k)\cong\mathbb{Z}/2\mathbb{Z}$ induces an involution on $\{x_1,...,x_{2r}\}$ compatible with the transposition on l_1 and l_2, which proves (1). The remaining properties follows easily from the construction: Property (2) holds since each F_i is defined over K but not over any proper subfield, while the three singular conics C_0, C_1, and C_2 are all defined over k. Finally, as F_i is the only conic passing through $\{a_1,a_2,b_1,b_2,x_i\}$ for every $1\le i\le 2r$, if $x_j\in F_i$, then $F_i=F_j$, which is a contradiction. This proves (3). □

Proof of Proposition 4.10. The construction is accomplished via several steps:

(1) Pick four points $a_1,a_2,b_1,b_2\in\mathbb{P}^2$ as in Remark 4.11. Blowup $\mathbb{P}^2$ along $\{a_1,a_2,b_1,b_2\}$ to obtain a conic bundle $\mathcal{C}\to\mathbb{P}^1$, which is fibered in the conics passing through $\{a_1,a_2,b_1,b_2\}$. Recall that only three of the fibers are degenerate, namely, C_0, C_1, and C_2. The exceptional divisors A_1,A_2,B_1,B_2 over a_1,a_2,b_1,b_2, respectively, form four sections of the bundle.

(2) Let x be the point obtained in Lemma 4.12 and consider it as a point on $\mathcal{C}$. Blow-up $\mathcal{C}$ along the $\mathrm{Gal}(K/k)$-orbit of x to obtain a map $X \to \mathcal{C}$. Let $E_1, \dots, E_{2r}$ be the exceptional divisors. Then $\mathrm{Pic}(X_K)$ is generated by $\{L, A_1, A_2, B_1, B_2, E_1, \dots E_{2r}\}$ where L is the pullback of a general hyperplane from $\mathbb{P}^2$. Let $F_1, \dots, F_{2r}$ denote the fibers of $\mathcal{C} \to \mathbb{P}^1$ that contain a Galois conjugate of the point x. By abuse of notation, we denote their strict transform in X by F_i as well. Let F denote a general fiber on X. Then $F^2 = 0$ and $F = F_i + E_i$ in $\mathrm{Pic}(X_K)$ for each i, from which we calculate that $F_i^2 = -1$.

(3) Using Castelnuovo's contractibility criterion (see [Băd01, Theorem 3.30] for the case of positive characteristics), blow-down $F_1, ..., F_{2r}$ to get $X \to \mathcal{C}'$. Let us denote again by A_i, B_i, F, E_i their images in $\mathcal{C}'$. Define the following divisor classes on $\mathcal{C}'$,

$$\begin{aligned} A_1' &= A_1 + rF - E_1 - \cdots - E_{2r} \\ A_2' &= A_2 + rF - E_1 - \cdots - E_{2r} \\ B_1' &= B_1 + rF - E_1 - \cdots - E_{2r} \\ B_2' &= B_2 + rF - E_1 - \cdots - E_{2r}. \end{aligned}$$

An easy intersection calculation shows that ${A_1'}^2 = -1,\ A_1' \cdot F = 1,\ A_1' \cdot E_i = 1$ for each i, and likewise for A_2', B_1', B_2'. We calculate that A_1', A_2', B_1', B_2' are classes of (-1)-curves.

(4) Since $X \to \mathcal{C}'$ only blows down components of fibers, we still have an induced morphism $\mathcal{C}' \to \mathbb{P}^1$ which is itself a conic fibration since the generic fiber is still the same. The blow-down of $\mathcal{C}'$ along A_1', A_2', B_1', B_2' is a smooth rational surface of Picard rank 1 containing a k-point from the initial $\mathbb{P}^2$, so it is isomorphic to $\mathbb{P}^2$ over k. Let $a_1', a_2', b_1', b_2' \in \mathbb{P}^2$ be the images of the (-1)-curves. Then the conic fibration $\mathcal{C}' \to \mathbb{P}^1$ corresponds to the family of conics passing through the points a_1', a_2', b_1', b_2'.

(5) The desired Cremona map f is then obtained from the composition

$$\begin{tikzcd} & & X \arrow[dl] \arrow[dr] & & \\ & \mathcal{C} \arrow[dl] & & \mathcal{C}' \arrow[dr] & \\ \mathbb{P}^2 \arrow[rrrr, dashed, "f"] & & & & \mathbb{P}^2. \end{tikzcd} \tag{4.9}$$

The map f belongs to $\mathrm{Cr}_2(k)$ since it is composed from maps defined over k. It has indeterminacy

$$\mathrm{Bs}(f) = \{a_1, a_2, b_1, b_2, x_1, ..., x_{2r}\}.$$

In particular, $f \in \mathrm{BCr}_2(k)$, and $\mathrm{Bs}(f)$ contains the $\mathrm{Gal}(K/k)$-orbit $\{x_1, ..., x_{2r}\}$ of size $2r = [K : k]$.

This process produces the desired Cremona maps whenever the point $x \in \mathcal{C}$, defined over K but not any proper subfield, has its $\mathrm{Gal}(K/k)$-conjugates lying on distinct fibers and disjoint from the sections A_1, A_2, B_1, B_2. □

It is worth mentioning that the transformation $\mathcal{C} \dashrightarrow \mathcal{C}'$ constructed in the proof of Proposition 4.10 is a Sarkisov link of type II for conic bundles.

Lemma 4.13. *If $[\bar{k} : k] = \infty$, then $\mathrm{BCr}_2(k)$ is not finitely generated.*

Proof. Recall the definition of k_f from the beginning of this section and define $k'_f = kk_f$ to be the composite field. Then k'_f is a finite extension of k. If $\mathrm{BCr}_2(k)$ is finitely-generated by $f_1, f_2, ..., f_r$, then for each $f \in \mathrm{BCr}_2(k)$, k'_f would is contained in the compositum of $k'_{f_1}, ..., k'_{f_r}$, and so

$$[k'_f : k] \leq \prod_{i=1}^{r} [k'_{f_i} : k],$$

implying that the set $\{[k'_f : k] : f \in \mathrm{BCr}_2(k)\}$ is bounded. The assumption $[\bar{k} : k] = \infty$ guarantees that k admits a field extension of arbitrarily large degree d. By Proposition 4.10 there exists $h \in \mathrm{BCr}_2(k)$ whose base-locus contains a point of degree d over k and hence $d \leq [k'_h : k]$, a contradiction. □

We end this section with the following proposition which gives another viewpoint for the Cremona map constructed in Proposition 4.10.

Proposition 4.14. *The Cremona map (4.9) is of the homaloidal type due to Ruffini. More explicitly, let $M \in \mathrm{Pic}(X)$ be the pullback of a hyperplane class from the right $\mathbb{P}^2$. Then we have*

$$M = (2n+1)L - 2\sum_{i=1}^{n} E_i - n(A_1 + A_2 + B_1 + B_2)$$

in $\mathrm{Pic}(X)$, where $n = 2r$ is the cardinality of the large Galois orbit.

Proof. The fiber class F corresponds to a conic in the right $\mathbb{P}^2$ passing through a'_1, a'_2, b'_1, b'_2, so the class in $\mathrm{Pic}(X)$ corresponding to a conic from the right $\mathbb{P}^2$ equals

$$\begin{aligned}
2M &= F + A'_1 + A'_2 + B'_1 + B'_2 \\
&= F + A_1 + A_2 + B_1 + B_2 + 2nF - 4\textstyle\sum_{i=1}^{n} E_i \\
&= (2n+1)(2L - A_1 - A_2 - B_1 - B_2) - 4\textstyle\sum_{i=1}^{n} E_i \\
&= (4n+2)L - 2n(A_1 + A_2 + B_1 + B_2) - 4\textstyle\sum_{i=1}^{n} E_i.
\end{aligned}$$

Divide both sides by 2 to get the result. □

4.3.2 Infinite index and non-normality

Lemma 4.15. *Let k be any field. Then $\mathrm{BCr}_2(k) \subset \mathrm{Cr}_2(k)$ is a subgroup of infinite index.*

Proof. First, assume that k is infinite. We inductively construct an infinite sequence of maps $f_1, f_2, f_3, ...$ in $\mathrm{Cr}_2(k)$ as follows. Let $f_1 \in \mathrm{Cr}_2(k)$ be the standard quadratic transformation $[x : y : z] \mapsto [yz : zx : xy]$. Assuming that f_i has been found, take three non-collinear points

$$\{a, b, c\} \in \mathbb{P}^2(k) \setminus \bigcup_{1 \leq j \leq i} \mathrm{Bs}(f_j)(k),$$

which is possible because k is infinite, and define $f_{i+1} := \tau \circ f_i$ where τ is a quadratic Cremona map with indeterminacy exactly at $\{a, b, c\}$. It is clear that

$$|\mathrm{Bs}(f_{i+1})(k)| \geq |\mathrm{Bs}(f_i)| + 3.$$

Note that the left-cosets $f_1\mathrm{BCr}_2(k)$, $f_2\mathrm{BCr}_2(k)$, ... are all pairwise disjoint because, by definition, the elements in $\mathrm{BCr}_2(k)$ cannot increase the indeterminacy points of f_i in $\mathbb{P}^2(k)$.

Next, assume that $k = \mathbb{F}_q$ is a finite field. Start with four points $a_1, a_2, b_1, b_2 \in \mathbb{P}^2(\mathbb{F}_q)$ such that no three are on a line. The main construction of the Cremona map carried out in proof of Propositon 4.10 still works, and for each even integer $n = 2r$, we get a map $f_r \in \mathrm{Cr}_2(\mathbb{F}_q)$ with $\mathrm{Bs}(f_r)$ containing a_1, a_2, b_1, b_2 with multiplicity $2r$ (Prop. 4.14). In particular, $f_r \notin \mathrm{BCr}_2(\mathbb{F}_q)$. We obtain an infinite sequence $\{f_1, f_2, f_3, \dots\}$ of elements in $\mathrm{Cr}_2(\mathbb{F}_q)$ such that the left cosets $f_1\mathrm{BCr}_2(\mathbb{F}_q)$, $f_2\mathrm{BCr}_2(\mathbb{F}_q)$, $f_3\mathrm{BCr}_2(\mathbb{F}_q)\dots$ are all pairwise disjoint. Indeed, for any $g \in \mathrm{BCr}_2(k)$ the multiplicity of $f_r g$ at a_1, a_2, b_1, b_2 is equal to $2r$. □

When k is algebraically-closed, Blanc [Bla10, Theorem 4.2] has shown that $\mathrm{Cr}_2(k)$ has no non-trivial closed normal subgroup with respect to its natural topology. Cantat and Lamy [CL13] prove that $\mathrm{Cr}_2(k)$ is not simple as an abstract group, and Lonjou generalises it for $\mathrm{Cr}_2(k)$ for any field k [Lon16].

Lemma 4.16. *For any field k, the group $\mathrm{BCr}_2(k)$ is not a normal subgroup of $\mathrm{Cr}_2(k)$.*

Proof. Let $f \in \mathrm{Cr}_2(k)$ be the standard quadratic involution $f : [x : y : z] \mapsto [yz : zx : xy]$. Let $g \in \mathrm{PGL}_3(k) \subset \mathrm{BCr}_2(k)$ be any map sending $[1 : 0 : 0]$ to $[1 : 1 : 1]$. Then $f^{-1}gf$ contracts the line $\{x = 0\}$ to the point

$$f^{-1}gf([0 : y : z]) = f^{-1}g([1 : 0 : 0]) = f^{-1}([1 : 1 : 1]) = [1 : 1 : 1].$$

In particular, $(f^{-1}gf)^{-1} = f^{-1}g^{-1}f$ possesses a k-rational point in its indeterminacy locus, and thus cannot be an element of $\mathrm{BCr}_2(k)$. □

We end with two propositions concerning the normality of the kernel of the natural homomorphism $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^n(k))$.

Lemma 4.17. *Let k be a finite field and $n \geq 2$. Then the kernel of the natural homomorphism $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^n(k))$ is not a normal subgroup of $\mathrm{Cr}_n(k)$.*

Proof. Let N be the kernel of $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^2(k))$ and suppose it is a normal subgroup of $\mathrm{Cr}_n(k)$. Let $l \in k[x_2, \dots, x_n]$ be linear and homogeneous, and consider the birational map

$$f\colon [x_0 : \cdots : x_n] \mapsto [x_0^2 : x_1 l : x_0x_2 : \cdots : x_0x_n]$$

with inverse

$$f^{-1}\colon [x_0 : \cdots : x_n] \mapsto [lx_0 : x_1x_0 : x_2l : \cdots : x_nl].$$

Both f and f^{-1} contract only two hypersurfaces, namely $H_l = \{l = 0\}$ and $x_0 = 0$. By assumption, N is normal, so fgf^{-1} is biregular, and hence g preserves $H_l \cup \{x_0 = 0\}$. We can do the same argument with $\alpha f \alpha^{-1}$ instead of f for any $\alpha \in \mathrm{Aut}(\mathbb{P}^n)$ and obtain that g preserves any rational hyperplane of $\mathbb{P}^n$. We write $g\colon [x_0 : \cdots : x_n] \mapsto [g_0 : \cdots : g_n]$ for some homogeneous $g_i \in$

$k[x_0,\dots,x_n]$ without a common non-constant factor. As g^{-1} preserves each rational hyperplane, we have $g_i = x_i g_i'$ for some $g_i' \in k[x_0,\dots,x_n]$, and for any $a_0,\dots,a_n \in k$ not all zero, we have $\sum_i a_i(x_i g_i') = \sum_i a_i g_i = p_{a_0,\dots,a_n}(\sum a_i x_i)$ for some $p_{a_0,\dots,a_n} \in k[x_0,\dots,x_n]$. It follows that $g_i = p_{a_0,\dots,a_n} \in k^*$ for $i = 0,\dots,n$, and so g is linear. Since $g \in N$, it fixes $|\mathbb{P}^n(k)| = q^n + q^{n-1} + \cdots + q + 1 \geq n+2$ points in $\mathbb{P}^2$, and so is equal to the identity map. We have reached a contradiction because $\mathrm{BCr}_n(k)$ is infinite by Proposition 4.10 and N is never trivial as it is of finite index in $\mathrm{BCr}_n(k)$. □

Proposition 4.18. *Let k be an infinite field and $n \geq 1$. Then the canonical homomorphism $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^n(k))$ is injective.*

Proof. Any element in the kernel of $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^n(k))$ coincides with the identity map on $\mathbb{P}^n(k)$, which is a dense subset of $\mathbb{P}^n(\bar{k})$, where $\bar{k}$ is the algebraic closure of k. It follows that f coincides with the identity everywhere. □

4.4 Proof of Theorem 1.1

Proof of Theorem 4.8. (1) is Lemma 4.9 and Lemma 4.13. (2) is Lemma 4.3.2, and finally (3) is Lemma 4.15. □

Proof of Theorem 1.1. (1) is Lemma 4.6 and the remaining points make up Theorem 4.8. □

References

[Băd01] Lucian Bădescu, *Algebraic surfaces*, Universitext, Springer-Verlag, New York, 2001. Translated from the 1981 Romanian original by Vladimir Maşek and revised by the author.

[Bha81] Prabir Bhattacharya, *On groups containing the projective special linear group*, Arch. Math. (Basel) **37** (1981), no. 4, 295–299.

[BKT08] Andrew Bashelor, Amy Ksir, and Will Traves, *Enumerative algebraic geometry of conics*, Amer. Math. Monthly **115** (2008), no. 8, 701–728.

[Bla10] Jérémy Blanc, *Groupes de Cremona, connexité et simplicité*, Ann. Sci. Éc. Norm. Supér. (4) **43** (2010), no. 2, 357–364.

[BM14] Jérémy Blanc and Frédéric Mangolte, *Cremona groups of real surfaces*, Automorphisms in birational and affine geometry, Springer Proc. Math. Stat **79** (2014), 3558.

[Can09] Serge Cantat, *Birational permutations*, C. R. Math. Acad. Sci. Paris **347** (2009), no. 21-22, 1289–1294.

[Can12] Segre Cantat, *Generators for the cremona group*, 2012. online access:
https://perso.univ-rennes1.fr/serge.cantat/Articles/hudson-pan-derksen.pdf.

[Can18] ———, *The Cremona group*, Algebraic geometry—Salt Lake City 2015. Part 1, 2018, pp. 101–142.

[CL13] Serge Cantat and Stéphane Lamy, *Normal subgroups in the Cremona group*, Acta Math. **210** (2013), no. 1, 31–94. With an appendix by Yves de Cornulier.

[Coh83] Stephen D. Cohen, *Primitive roots in the quadratic extension of a finite field*, J. London Math. Soc. (2) **27** (1983), no. 2, 221–228.

[DI09] Igor V. Dolgachev and Vasily A. Iskovskikh, *Finite subgroups of the plane Cremona group*, Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. I, 2009, pp. 443–548.

[Isk79] V. A. Iskovskih, *Minimal models of rational surfaces over arbitrary fields*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 1, 19–43, 237.

[Isk91] V. A. Iskovskikh, *Generators of the two-dimensional Cremona group over a nonclosed field*, Trudy Mat. Inst. Steklov. **200** (1991), 157–170.

[Isk96] ______, *Factorization of birational mappings of rational surfaces from the point of view of Mori theory*, Uspekhi Mat. Nauk **51** (1996), no. 4(310), 3–72.

[Jac89] Nathan Jacobson, *Basic algebra. II*, Second, W. H. Freeman and Company, New York, 1989.

[KM74] W. M. Kantor and T. P. McDonough, *On the maximality of* $\mathrm{PSL}(d+1, q)$, $d \geq 2$, J. London Math. Soc. (2) **8** (1974), 426.

[Kol07] János Kollár, *Lectures on resolution of singularities*, Annals of Mathematics Studies, vol. 166, Princeton University Press, Princeton, NJ, 2007.

[Kol99] J. Kollar, *Rational curves on algebraic varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, Springer Berlin Heidelberg, 1999.

[Lis75] R. List, *On permutation groups containing* $\mathrm{PSL}_n(q)$ *as a subgroup*, Geometriae Dedicata **4** (1975), no. 2/3/4, 373–375.

[Lon16] Anne Lonjou, *Non simplicit du groupe de cremona sur tout corps*, Ann. Inst. Fourier (Grenoble) **66** (2016), 20212046.

[Man86] Yu. I. Manin, *Cubic forms*, Second, North-Holland Mathematical Library, vol. 4, North-Holland Publishing Co., Amsterdam, 1986. Algebra, geometry, arithmetic, Translated from the Russian by M. Hazewinkel.

[Pog74] B. A. Pogorelov, *Maximal subgroups of symmetric groups that are defined on projective spaces over finite fields*, Mat. Zametki **16** (1974), 91–100.

[Poo17] Bjorn Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Wat89] William C. Waterhouse, *Two generators for the general linear groups over finite fields*, Linear and Multilinear Algebra **24** (1989), no. 4, 227–230.

[Wei56] André Weil, *Abstract versus classical algebraic geometry*, Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, vol. III, 1956, pp. 550–558.

S. Asgarli, Department of Mathematics
University of British Columbia
Vancouver, BC V6T1Z2, Canada
sasgarli@math.ubc.ca

K.-W. Lai, Department of Mathematics & Statistics
University of Massachusetts
Amherst, MA 01003, USA
lai@math.umass.edu

M. Nakahara, Department of Mathematics
University of Bath
Bath, BA2 7AY, UK
mn634@bath.ac.uk

S. Zimmermann, Laboratoire angevin de recherche en mathematiques (LAREMA), CNRS
Université d'Angers
2 Bd Lavoisier, 49045 Angers Cedex 01, France
susanna.zimmermann@univ-angers.fr