Bijective Cremona transformations of the plane

Shamil Asgarli Kuan-Wen Lai Masahiro Nakahara Susanna Zimmermann

Abstract

We study the birational self-maps of the projective plane over finite fields that induce permutations on the set of rational points. As a main result, we prove that no odd permutation arises over a non-prime finite field of characteristic two, which completes the investigation initiated by Cantat about which permutations can be realized this way. Main ingredients in our proof include the invariance of parity under groupoid conjugations by birational maps, and a list of generators for the group of such maps.

Contents

2020 Mathematics Subject Classification 14E07, 14G15, 20B30.
Keywords: bijective Cremona transformations, birational permutations

1 Introduction

We call a birational self-map of a variety a *birational permutation* if both the map and its inverse are defined at all rational points on 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 a bijection induces a permutation in the usual sense. Fixing a variety and a finite ground field, 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 $\mathbb{P}^n$, that is, the *Cremona transformations*. They form a group $\mathrm{Cr}_n(k)$ where k is the ground field. We say that a Cremona transformation is *bijective* if it is a birational permutation. Clearly, bijective elements form a subgroup $\mathrm{BCr}_n(k) \subset \mathrm{Cr}_n(k)$. When $k = \mathbb{F}_q$, the finite field of q elements, the actions of bijective elements on the set of $\mathbb{F}_q$-points determines a group homomorphism

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

where $\mathrm{Sym}(\mathbb{P}^n(\mathbb{F}_q))$ is the symmetric group of the set $\mathbb{P}^n(\mathbb{F}_q)$. Let $\mathrm{Alt}(\mathbb{P}^n(\mathbb{F}_q)) \subset \mathrm{Sym}(\mathbb{P}^n(\mathbb{F}_q))$ be the alternating subgroup, which consists of even permutations. In the case $n = 2$, it is known that the image of σ_q satisfies

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

This result was mainly proved by Cantat [Can09], but the original proof has a minor gap. In Section 2, we review Cantat's construction and fill in the gap with a theorem by Cohen (Theorem 2.8) about primitive roots of $\mathbb{F}_{q^2}$.

The main focus of this paper is the case $q = 2^m \geq 4$. We prove that:

Theorem 1.1. *For $q = 2^m \geq 4$, the group $\mathrm{BCr}_2(\mathbb{F}_q)$ produces only even permutations on $\mathbb{P}^2(\mathbb{F}_q)$. As a result, we have $\mathrm{Im}(\sigma_q) = \mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$.*

Our proof for Theorem 1.1 relies on being able to transfer the parity problem from one surface to another. Let $\mathrm{Bir}_k(X)$ denote the group of birational self-maps of a variety X over a field k. In the same spirit of the notation $\mathrm{BCr}_n(k)$, we denote by $\mathrm{BBir}_k(X) \subset \mathrm{Bir}_k(X)$ the subgroup of birational permutations. For surfaces over $\mathbb{F}_q$, where $q = 2^m \geq 4$, the parity of a birational permutation is invariant under groupoid conjugations by birational maps in the following sense:

Theorem 1.2. *Let X and Y be smooth surfaces over $\mathbb{F}_q$, where $q = 2^m \geq 4$, together with two birational permutations $\alpha \in \mathrm{BBir}_{\mathbb{F}_q}(X)$ and $\beta \in \mathrm{BBir}_{\mathbb{F}_q}(Y)$. Suppose that there exists a birational map $h \colon X \dashrightarrow Y$ such that $\alpha = h^{-1}\beta h$, i.e., the following diagram commutes:*

$$\begin{array}{ccc} X & \overset{\alpha}{\dashrightarrow} & X \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ Y & \overset{\beta}{\dashrightarrow} & Y. \end{array}$$

Then the permutations induced by α on $X(\mathbb{F}_q)$ and β on $Y(\mathbb{F}_q)$ have the same parity.

Throughout the paper, we will call the groupoid conjugation demonstrated in Theorem 1.2 simply as "conjugation". Our next result studies birational permutations on conic bundles over $\mathbb{P}^1$, del Pezzo surfaces, and bijective Cremona maps on $\mathbb{P}^2$ of finite order. As an application of Theorem 1.2, we obtain:

Theorem 1.3. *Over $\mathbb{F}_q$, $q = 2^m \geq 4$, a birational permutation on a smooth surface induces an even permutation on the set of $\mathbb{F}_q$-points if it is conjugate to*

- *a birational permutation on a conic bundle over $\mathbb{P}^1$ preserving the fiber class,*
- *an automorphism of a rational del Pezzo surface, or*
- *an element of $\mathrm{BCr}_2(\mathbb{F}_q)$ of finite order.*

To complete the proof of Theorem 1.1, we first produce a list of generators for the bijective Cremona group, and then show that every generator is a composition of maps described as in Theorem 1.3. We state the result on the generators below and refer the reader to Lemma 5.4 for the complete list.

Theorem 1.4. *Let k be a perfect field and $\mathbf{T} \subset \mathrm{Cr}_2(k)$ be the set of generators for $\mathrm{Cr}_2(k)$ given by Iskovskikh [Isk91]. Then $\mathbf{T} \cap \mathrm{BCr}_2(k)$ forms a set of generators for $\mathrm{BCr}_2(k)$.*

Remark 1.5. The first version of this paper was announced on the arXiv in 2019, where Theorem 1.1 remained as a conjecture. In that version, we proved that all but the *quintic transformations* among the generators in Theorem 1.4 induce only even permutations, and verified with Magma [BCP97] that the quintic transformations over $\mathbb{F}_q$ for $q = 4, 8, 16$ are all even. In June 2021, we communicated with Julia Schneider on the *central symmetry* of a relation diagram of Sarkisov links, which allowed us to attack the quintic transformations and prove our conjecture.

In parallel to our work on the quintic transformations, we learned that Genevois, Lonjou, and Urech [GLU21] also came up with a proof for Theorem 1.1 based on our Theorem 1.3 and the main theorem of [LS21] with a more combinatorial approach. In fact, they observed that parity can still be defined for a birational self-map on a smooth rational surface over $\mathbb{F}_q$, $q = 2^m \geq 4$, even if the map is not bijective, which allowed them to prove Theorem 1.1 not only for $\mathbb{P}^2$ but also for all smooth rational surfaces.

Organization of the paper In Section 2, we discuss the realizability of all permutations on the rational points in the plane over finite fields of odd characteristics and $\mathbb{F}_2$. We study the parity problem over a non-prime field of characteristic 2 throughout Sections 3–5, where we assume that $k = \mathbb{F}_q$ with $q = 2^m \geq 4$ unless otherwise specified. In Section 3, we begin with the analysis of the parities induced by linear transformations and then prove Theorem 1.2. In Section 4, we study the birational permutations on certain rational surfaces and prove Theorem 1.3. In Section 5, we exhibit a list of generators for $\mathrm{BCr}_2(k)$ when k is a perfect field and prove Theorem 1.4. Then we analyze whether each generator induces an even permutation and deduce Theorem 1.1. In Section 6, we answer a few questions about $\mathrm{BCr}_2(k)$ as a subgroup of $\mathrm{Cr}_2(k)$, which include whether it is finitely generated, what its index is, and whether it is a normal subgroup.

Acknowledgements We thank Brendan Hassett for suggesting us the problem in the present paper. We also thank Zinovy Reichstein for a quick proof that $\mathrm{BCr}_2(k)$ is not finitely generated

when k is uncountable. We thank Julia Schneider for discussing with us on the key ideas that allowed us to attack the quintic transformations. Before we are able to prove our conjecture, Lian Duan assisted us designing a Magma code that can compute efficiently the parities of all possible quintic transformations over $\mathbb{F}_q$ for $q = 4, 8, 16$. We are very grateful for his generous help. Finally, we thank the anonymous referee for their valuable suggestions. During this project, the first author was partially supported by funds from NSF Grant DMS-1701659. The second author is supported by the ERC Synergy Grant ERC-2020-SyG-854361-HyperK. The third author was supported by EPSRC grant EP/R021422/2. The last author was supported by FIBALGA ANR-18-CE40-0003-01, PEPS 2019 "JC/JC" and Étoiles Montantes de la Région Pays de la Loire.

2 Realizing arbitrary permutations

Theorem 2.1 ([Can09]). *The image of the homomorphism* $\sigma_q \colon \mathrm{BCr}_2(\mathbb{F}_q) \to \mathrm{Sym}(\mathbb{P}^2(\mathbb{F}_q))$ *satisfies*

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

Cantat's proof of Theorem 2.1 is built upon a property about the subgroups of $\mathrm{Sym}(\mathbb{P}^n(\mathbb{F}_q))$ that 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

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

which contains $\mathrm{PSL}_{n+1}(\mathbb{F}_q)$.

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

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

- does not preserve the collinearity on $\mathbb{P}^2(\mathbb{F}_q)$, and
- 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 by Cohen.

2.1 Special birational maps on a quadric surface

We first recall a key construction in [Can09, §3]. Fix 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 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 an $\mathbb{F}_q$-point P_0 in the base $\mathbb{P}^1$ over which the fiber $C_0 := \pi_L^{-1}(P_0)$ is smooth.

This setting implies that every degenerate fiber over $\mathbb{F}_q$ is a union of distinct lines $L_1 \cup L_2$ conjugate to each other over $\mathbb{F}_{q^2}/\mathbb{F}_q$, on which the node $P := L_1 \cap L_2$ appears as the only $\mathbb{F}_q$-point.

The projection from P defines a birational map $\pi_P\colon Q \dashrightarrow \mathbb{P}^2$. Let us organize these maps into a diagram:

$$\begin{array}{ccc} Q & \overset{\pi_P}{\underset{\sim}{-\!\!\to}} & \mathbb{P}^2 \\ {\scriptstyle \pi_L\colon \text{conic fibration}}\big\downarrow & & \\ \mathbb{P}^1. & & \end{array} \tag{2.1}$$

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

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

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

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 $t \in \mathbb{F}_q$, namely, $t \neq s^2$ for all $s \in \mathbb{F}_q$. 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 parametrized by the map,

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

For a smooth fiber over $\mathbb{F}_q$, one can choose

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

Note that C_0 lies on the plane $\{z = 0\}$.

Let us construct the map g as in (1) in the case of odd characteristics using Example 2.3. (The case of characteristic 2 will be discussed in §2.3.2.) The process starts by constructing a suitable automorphism on the smooth fiber C_0 in (2.2) and then extend it to Q. Consider the automorphism on the plain $\{z = 0\}$:

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

where the parameter (α, β) is a point on the affine conic

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

Note that this is the identity map when $(\alpha, \beta) = (1, 0)$. For each $(\alpha, \beta) \in S^\circ$, the formula induces an automorphism $g_0\colon C_0 \xrightarrow{\sim} C_0$ as one can verify that

$$(\alpha x + t\beta y)^2 - t(\beta x + \alpha y)^2 = x^2 - ty^2. \tag{2.3}$$

Remark 2.4. The map g_0 can be expressed as

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

where $[\alpha : \beta : \gamma] \in \mathbb{P}^2$ is any $\mathbb{F}_q$-point on the (projective) 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, we assume that $\gamma = 1$ for the convenience of computation.

In the following, we exhibit how to extend g_0 to the whole quadric Q as a birational permutation that fixes the $\mathbb{F}_q$-points not lying on C_0. The method is built upon the following lemma about interpolations. Although 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 $P_1 \neq P_2$. Then there exists a rational map $h \colon \mathbb{P}^n \dashrightarrow \mathbb{P}^1$ 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. For every $P \in \mathbb{F}_q^{n+1} \setminus \{0\}$, there exists a homogeneous polynomial $f_P \in \mathbb{F}_q[x_0, ..., x_n]$ such that for each $P' \in \mathbb{F}_q^{n+1} \setminus \{0\}$,

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

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

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

satisfies the desired property. (The function f_P serves the role of the Dirac delta function.) Next, consider the homogeneous polynomial

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

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

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

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

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 $g \colon Q \dashrightarrow Q$ that 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.

(This element g can be viewed as the group version of the Dirac delta function.)

Proof. Let ζ be an affine coordinate on the base $\mathbb{P}^1$ of the fibration π_L. 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 this 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

$$\alpha = \frac{1+t\zeta^2}{1-t\zeta^2}, \quad \beta = \frac{2\zeta}{1-t\zeta^2}. \tag{2.4}$$

Let $P_0 := [0:1] = \pi_L(C_0) \in \mathbb{P}^1$. By Lemma 2.5, there exists a rational function $\zeta = h(z,w)$ on the base $\mathbb{P}^1$ over $\mathbb{F}_q$ 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 (2.4), 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 (2.3). By construction, we have

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

which respectively implies that $g|_{C_0} = g_0$ and that $g|_C = \mathrm{id}$ for all $\mathbb{F}_q$-fibers $C \neq C_0$. □

2.2 Odd permutations on the smooth fiber

Let us retain the notation from the previous section. Our goal here is to find a g_0 which acts transitively on $C_0(\mathbb{F}_q)$ and thus induces an odd permutation. Note that, as $C_0 \cong \mathbb{P}^1$, it is not hard to find an automorphism on C_0 which induces an odd permutation on the $\mathbb{F}_q$-points. However, it is not obvious that every such automorphism can be extended to Q while keeping control on the induced permutation on the other $\mathbb{F}_q$-points. In the following, we identify $\mathbb{F}_{q^2} \cong \mathbb{F}_q \oplus \sqrt{t^{-1}}\mathbb{F}_q$ 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. *Assume that g_0 is not the identity map, that is, $\alpha \neq 1$. Then, under a suitable choice of 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*

$$\beta + (\alpha - 1)\sqrt{t^{-1}} \in \mathbb{F}_{q^2} \tag{2.5}$$

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

Proof. 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

$$g_\theta(\zeta) = \frac{\beta\zeta + t^{-1}(\alpha-1)}{(\alpha-1)\zeta + \beta}. \tag{2.6}$$

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 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. Under the identification $\mathbb{P}^1 \cong \mathbb{P}(\mathbb{F}_q \oplus \sqrt{t^{-1}}\mathbb{F}_q)$, formula (2.6) can be rewritten as

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

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. □

Due to this lemma, to find g_0 that acts on $C_0(\mathbb{F}_q)$ transitively, it is sufficient to find a primitive root of $\mathbb{F}_{q^2}$ of the form (2.5). To attain this, we use the following result by 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 non-zero 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. Let us 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 above two expressions for ξ, we obtain

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

which implies that $(\alpha-1)^2 - t\beta^2 = -2(\alpha-1)$, thus $\alpha^2 - t\beta^2 = 1$, as required. □

2.3 Induced actions on the projective plane

Here we completes the proof of Theorem 2.1. We will first treat the case when q is odd using what we have established in the previous sections. The case $q = 2$ will be treated separately with a similar strategy, where we will also prove that the image of σ_q contains $\mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$ for $q = 2^m \geq 4$.

2.3.1 Proof of Theorem 2.1 for odd q 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 leaving all the other $\mathbb{F}_q$-fibers fixed. Recall that $\pi_P\colon Q \dashrightarrow \mathbb{P}^2$ is the projection from the node P of a degenerate fiber of the fibration $\pi_L\colon Q \dashrightarrow \mathbb{P}^1$. In particular, it has P as the only indeterminacy point and contracts the two branches of the degenerate fiber. In particular, it maps the smooth fiber C_0 isomorphically onto a smooth conic $C := \pi_P(C_0) \subset \mathbb{P}^2$.

Proposition 2.10. *The composition $f := \pi_P \circ g \circ \pi_P^{-1}\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ satisfies the following properties:*

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

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

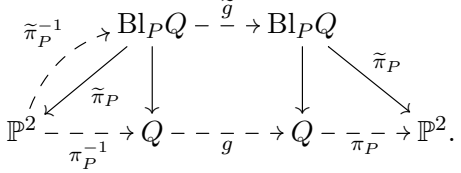
(3) *f acts transitively on $C(\mathbb{F}_q)$ and thus permutes as a $(q+1)$-cycle.*

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

Proof. Let us prove the statements one-by-one.

(1) We have the commutative diagram:



Note that this diagram factorizes $f = \pi_P \circ g \circ \pi_P^{-1}$ as $f = \widetilde{\pi}_P \circ \widetilde{g} \circ \widetilde{\pi}_P^{-1}$. The two lines passing through P in Q become disjoint (-1)-curves on $\mathrm{Bl}_P Q$ that are Galois conjugate to each other, and the morphism $\widetilde{\pi}_P$ is the blow-down of these two lines. Hence $\widetilde{\pi}_P$ and $\widetilde{\pi}_P^{-1}$ are both defined at all $\mathbb{F}_q$-points.

It suffices to show that $\widetilde{g}$ induces a bijection on the $\mathbb{F}_q$-points of $\mathrm{Bl}_P Q$. Indeed, g induces a bijection on $Q(\mathbb{F}_q)$ and fixes P. Hence $\widetilde{g}$ induces a birational self-map, and thus an automorphism, on the exceptional curve over P. As a result, f is defined at 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 $A \in \mathbb{P}^2(\mathbb{F}_q) \setminus C(\mathbb{F}_q)$. Then $\pi_P^{-1}(A) \in Q \setminus C_0$, which implies $g(\pi_P^{-1}(A)) = \pi_P^{-1}(A)$. Hence $f(A) = \pi_P \circ g \circ \pi_P^{-1}(A) = A$.

(3) This follows from the relation $f = \pi_P \circ g \circ \pi_P^{-1}$ and the fact that g permutes the points of $C_0(\mathbb{F}_q)$ as a $(q+1)$-cycle.

(4) Take an $\mathbb{F}_q$-point B on C and consider the tangent line $\ell := T_B C \subset \mathbb{P}^2$. Then $\ell \cap C = \{B\}$. The map f acts as the identity on all the $\mathbb{F}_q$-points of ℓ except for B, and sends B to another point on C not lying on ℓ. Consequently, the map does not preserve collinearity.

□

Theorem 2.1 in the case of odd q is then a consequence of Theorem 2.2 and Proposition 2.10.

Remark 2.11. Recall that Q and L are defined as

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

and $P = [0:0:1:1] \in Q$. Projection from P defines a birational map

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

whose inverse is given by

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

On the other hand, the map g has 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 $\alpha^2 - t\beta^2 = \gamma^2$. These expressions allow one to compute $f = \pi_P \circ g \circ \pi_P^{-1}$ explicitly. Also recall that the smooth fiber $C_0 = \pi_L^{-1}([0:1])$ lies on $H := \{z = 0\}$. To compute the action of f on $C = \pi_P(C_0)$, one may identify H with the codomain $\mathbb{P}^2$ of π_P via $[x:y:u] \mapsto [x:y:0:u]$.

2.3.2 The construction in characteristic 2 We first explain the construction over $\mathbb{F}_2$. Consider the quadric surface given by

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

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:

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

where we used the identification $H = \{z = 0\} \cong \mathbb{P}^2$ with homogeneous coordinates x, y and u mentioned in Remark 2.11.

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 $q = 2^m \geq 4$, following Cantat, we use the 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 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 $\sigma_q(\mathrm{BCr}_2(\mathbb{F}_q)) \supset \mathrm{Alt}(\mathbb{P}^2(\mathbb{F}_q))$.

3 Birational invariance of parity

In this section, we prove that automorphisms of $\mathbb{P}^n$ for $n \geq 1$ over $\mathbb{F}_q$, where $q = 2^m \geq 4$, induce only even permutations on the set of rational points. This result allows us to study the parity

problem without specifying a coordinate system on $\mathbb{P}^n$. Then we prove Theorem 1.2, namely, the invariance of parity under conjugations by birational maps. The proof of this theorem is built on the fact that one can resolve a birational map between surfaces over a perfect field via a sequence of blow-ups at closed points.

Example 3.1. It is easy to construct a counterexample to Theorem 1.2 for odd q 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 blow-up 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 choose $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ if $q = 2$.

3.1 Parities induced by linear transformations

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 $\mathrm{PGL}_{n+1}(\mathbb{F}_q) \subset \mathrm{Alt}(\mathbb{P}^n(\mathbb{F}_q))$, 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

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

For example, when $n = 2$ we get

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

In the case $n = 1$ and $q > 2$, 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 $A_1 = \begin{pmatrix} 0 & r \\ 1 & s \end{pmatrix}$ and $B_1 = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$. We emphasize that the case $n = 1$ and $q = 2$ is not covered by these formulas. 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 3.2. *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 for $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$, so B_1 fixes $[1:0]$ and $[0:1]$ and acts as a $(q-1)$-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 factorized as

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

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 even permutations, so A_1 is even. □

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

Proof. One can verify directly that $A_n = T_nM_n$, where

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

Note that M_n has an odd order $q-1$, so its action is even. Therefore, it is sufficient to prove that T_n induces an even permutation. First, by writing $T_n = I_{n+1} + E_{n+1,1}$, we obtain

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

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 its fixed locus is the hyperplane $\{x_0 = 0\}$. Hence the number of transpositions in T_n equals

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

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

Lemma 3.4. *Assume $n \geq 2$. If $q = 2^m \geq 4$, then the action of B_n on $\mathbb{P}^n(\mathbb{F}_q)$ is even. If $q = 2$, then the action is odd when $n = 2^\ell - 1$ for some ℓ and even otherwise.*

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 multiplication of B_n on $\mathbb{F}_q^{n+1}$ from the left as the action of b^{-1} on $\mathbb{F}_{q^{n+1}}$. Therefore, it is sufficient to compute the parity of the action of b on $\mathbb{F}_{q^{n+1}}$.

Let us write $n+1 = u2^\ell$ where u is odd. Then the parity of b^u is the same as the parity of b and the cycle decomposition of b^u contains only 2^r-cycles for $r \geq 0$. There is a filtration of $\mathbb{F}_{q^{n+1}}$ invariant under the action of b^u:

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

For each $1 \leq r \leq \ell$, there are $q^{u2^r} - q^{u2^{r-1}}$ many 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 b^u equals

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

On 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

$$\frac{1}{2^r}\left(\frac{q^{u2^r} - q^{u2^{r-1}}}{q-1}\right) = \frac{q^{u2^{r-1}}}{2^r}\left(\frac{q^{u2^{r-1}} - 1}{q-1}\right). \tag{3.1}$$

- Suppose $q = 2^m \geq 4$. Then $m \geq 2$, thus $mu2^{r-1} - r > 0$ for $u \geq 1$ and $1 \leq r \leq \ell$. Hence

$$\frac{q^{u2^{r-1}}}{2^r} = \frac{2^{mu2^{r-1}}}{2^r} = 2^{mu2^{r-1}-r} \tag{3.2}$$

  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 $1 \leq r \leq \ell$, thus the action is even itself.

- Suppose $q = 2$ and $n = 2^\ell - 1$ for some ℓ. Note that $\ell \geq 2$ as $n \geq 2$. Then $m = 1$ and $u = 1$. In this case, (3.2) equals 1 for $r = 1$ and is even for $2 \leq r \leq \ell$. This implies that (3.1) equals 1 for $r = 1$ and is even for $2 \leq r \leq \ell$. As a result, the action of b^u on $\mathbb{P}^n(\mathbb{F}_q)$ consists of one 2-cycle and an even number of 2^r-cycle for each $2 \leq r \leq \ell$, thus is an odd action.

- Suppose $q = 2$ and $n \neq 2^\ell - 1$ for all ℓ. Then $m = 1$ and $u > 1$. This implies that (3.2) is even for $1 \leq r \leq \ell$. We conclude that the action of b^u is even as in the first case.

These cover all the cases, so the proof is done. □

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

Proof. The case $n = 1$ (resp. $n \geq 2$) follows from Lemma 3.2 (resp. Lemmas 3.3 and 3.4). □

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 2 when studying the parity. For a permutation induced by a linear transformation, the following result shows that we can say more about the cycle type if its order is a power of 2.

Corollary 3.6. *Let $n \geq 1$ and $q = 2^m \geq 4$. Suppose that $\sigma \in \mathrm{PGL}_{n+1}(\mathbb{F}_q)$ induces a permutation of order 2^r on $\mathbb{P}^n(\mathbb{F}_q)$. Define c_i, where $0 \leq i \leq r$, to be the number of 2^i-cycles in the cycle decomposition. 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 all $i \geq 1$, the sum $c_1 + \cdots + c_r$ must be even due to Proposition 3.5. Then the relations

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

imply that c_0 is odd. Assume $n = 1$ and that σ is not the identity. Then σ fixes at most 2 points, which 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 as it fixes $1 + 2^j c_j \geq 3$ points. It follows that every nontrivial cycle in σ has the same size 2^j. If $2^j = q$, then σ is a q-cycle thus is odd, which is impossible by Proposition 3.5. Hence $2^j < q$, and the equalities $|\mathbb{P}^1(\mathbb{F}_q)| = q + 1 = 1 + 2^j c_j$ imply that $c_j = q/2^j > 1$. □

3.2 Projective bundles over finite sets

We define a *$\mathbb{P}^n$-bundle over a finite set B* to be the disjoint union of projective n-spaces:

$$\mathcal{P} = \coprod_{i \in B} P_i, \quad P_i \cong \mathbb{P}^n, \quad \text{equipped with the map} \quad h \colon \mathcal{P} \to B : P_i \mapsto i.$$

Consider the set $\mathcal{P}(k)$ of k-points on $\mathcal{P}$. We are interested in elements $\sigma \in \mathrm{Sym}(\mathcal{P}(k))$ of the form:

(1) For every $i \in B$, there exists $j \in B$ such that $\sigma(P_i(k)) = P_j(k)$. Then $h\sigma h^{-1}$ 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 linear isomorphism over k.

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

Lemma 3.7. *Let $k = \mathbb{F}_q$, $q = 2^m \geq 4$, and $\sigma \in \mathrm{Sym}(\mathcal{P}(k))$ 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. Therefore, it suffices to prove the statement under the hypothesis $O = B$. Note that the case $r = 1$ follows immediately from Proposition 3.5. Hence we 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, which are all odd since the assumption $r \geq 2$ implies $2^i r \geq 2$. 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. We conclude that σ is odd. □

3.3 Proof of the birational invariance of parity

Let X and Y be smooth surfaces over $k = \mathbb{F}_{2^m}$ where $m \geq 2$. Given $\alpha \in \mathrm{BBir}_k(X)$, $\beta \in \mathrm{BBir}_k(Y)$, and a birational map $h\colon X \to Y$ over k that satisfy $\alpha = h^{-1}\beta h$, we prove Theorem 1.2, namely, that the permutations induced by α and β on $X(k)$ and $Y(k)$, respectively, have the same parity. Note that, if h induces a bijection between $X(k)$ and $Y(k)$, then the relation $\alpha = h^{-1}\beta h$ implies immediately that the induced permutations have the same cycle type and thus the same parity. The main content of Theorem 1.2 consists in that the same conclusion holds even if h is not a bijection on the sets of rational points.

In the following, we establish Theorem 1.2 from scratch, starting from the case when the birational map $h\colon X \to Y$ is a blow-up at a set of closed points, then the case when h is a birational morphism, and finally the full generality.

Lemma 3.8. *Let Y be a smooth surface over $k = \mathbb{F}_{2^m}$, $m \geq 2$, and $h\colon X \to Y$ be a birational morphism over k that blows up a set $\overline{B} \subset Y(\overline{k})$ of closed points. Define $B := \overline{B} \cap Y(k)$ and $E := h^{-1}(B) \subset X$. Pick $\beta \in \mathrm{BBir}_k(Y)$ and assume that $\alpha := h^{-1}\beta h \in \mathrm{BBir}_k(X)$. Then we have $\alpha(E) = E$ and $\beta(B) = B$.*

Proof. The map α does not contract any curve in E. Indeed, every irreducible component of E is a rational curve over k, thus contains more than one k-points. If α contracts any of them, we would have $\alpha \notin \mathrm{BBir}_k(X)$, contradiction. It follows that $\alpha(E) = h^{-1}\beta h(E) = h^{-1}\beta(B)$ is a curve, so $\beta(B) \subset B$. Since β induces a bijection on $Y(k)$, we have $\beta(B) = B$, and hence $\alpha(E) = E$. □

Lemma 3.9. *Retain the setting from Lemma 3.8. Then the actions of α on $X(k)$ and β on $Y(k)$ have the same parity.*

Proof. Let $U := X \setminus E$ and $V := Y \setminus B$. Note that $h|_U\colon U \to V$, though may not be an isomorphism, induces a bijection on the sets of k-points. By Lemma 3.8, we have $\alpha(U) = U$ and $\beta(V) = V$, and the relation $\alpha = h^{-1}\beta h$ implies $\alpha|_U = (h|_U)^{-1}(\beta|_V)(h|_U)$. Hence the restrictions of α to U and β to V have the same parity when acting on the k-points.

Now consider the actions of α on E and β on B. Note that E is a $\mathbb{P}^1$-bundle over B. Restricting h to $E(k)$ induces the map among finite sets

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

as well as the relation $\beta|_{B(k)} = h|_{E(k)} \circ \alpha|_{E(k)} \circ (h|_{E(k)})^{-1}$. Then the permutations $\beta|_{B(k)}$ and $\alpha|_{E(k)}$ have the same parity by Lemma 3.7. This completes the proof. □

The following two lemmas will be needed in the proofs of the remaining cases.

Lemma 3.10. *Let X and Y be smooth surfaces over a perfect field k and $h\colon X \to Y$ a birational morphism over k. Then we can factorize h as a sequence of blow-ups at closed points*

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

Moreover, 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.

Proof. According to [Man86, Lemma 18.1.3], we can factorize h as a sequence of blow-ups at closed points. To prove the second statement, assume that there exists a point $x \in Y_i$ blown up by ϵ_{i+1} but not in the exceptional locus of ϵ_i. Consider the commutative diagram

$$\begin{array}{ccccc} Y'_{i+1} & \xrightarrow{\epsilon'_{i+1}} & Y'_i & \xrightarrow{\epsilon'_i} & Y_{i-1} \\ \downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle \mathrm{Bl}_x} & & \| \\ Y_{i+1} & \xrightarrow{\epsilon_{i+1}} & Y_i & \xrightarrow{\epsilon_i} & Y_{i-1} \end{array}$$

where ϵ'_i is ϵ_i followed by the blow-up 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. □

Lemma 3.11. *Let Y be a surface, β be a birational self-map on Y, and $q \in Y$ be a closed point at which β is well-defined. Let $\epsilon\colon Y' \to Y$ be the blow-up at the set $\{q, \beta(q)\}$, and E_q be the exceptional divisor over q. Then the composition $\epsilon^{-1}\beta\epsilon$, which is a birational self-map on Y', is well-defined everywhere on E_q.*

Proof. Let $q' := \beta(q)$ and $E_{q'} \subset Y'$ be the exceptional divisor over q'. Denote $\beta' := \epsilon^{-1}\beta\epsilon$. Then we have the commutative diagram

$$\begin{array}{ccccc} E_q & \hookrightarrow & Y' & \xrightarrow{\epsilon} & Y \\ & & \downarrow{\scriptstyle \beta'} & & \downarrow{\scriptstyle \beta} \\ E_{q'} & \hookrightarrow & Y' & \xrightarrow{\epsilon} & Y. \end{array}$$

The composition $\beta\epsilon\colon Y' \dashrightarrow Y$ pulls q' back as the divisor E_q while q' is blown up by ϵ as $E_{q'}$. By the universal property of blowing up, $\beta\epsilon$ factors through the bottom ϵ uniquely as

$$\begin{array}{ccccc} E_q & \hookrightarrow & Y' & \xrightarrow{\epsilon} & Y \\ {\scriptstyle \beta''_i|_{E_q}}\downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle \exists\, \beta''} & & \downarrow{\scriptstyle \beta} \\ E_{q'} & \hookrightarrow & Y' & \xrightarrow{\epsilon} & Y. \end{array}$$

Note that β'' is well-defined everywhere on E_q and $\beta'' = \epsilon^{-1}\beta\epsilon = \beta'$. Hence β' is well-defined everywhere on E_q. □

Now we prove the invariance of parity under conjugations by birational morphisms.

Lemma 3.12. *Let X and Y be smooth surfaces over $k = \mathbb{F}_{2^m}$, $m \geq 2$, and $h\colon X \to Y$ a birational morphism over k. Pick $\beta \in \mathrm{BBir}_k(Y)$ and assume that $\alpha := h^{-1}\beta h \in \mathrm{BBir}_k(X)$. Then the actions of α on $X(k)$ and β on $Y(k)$ have the same parity.*

Proof. By Lemma 3.10, we can factorize h as

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

such that the points in Y_i blown up by ϵ_{i+1} lie in the exceptional locus of ϵ_i. Denote $\beta_0 := \beta$ and define inductively that

$$\beta_i := \epsilon_i^{-1}\beta_{i-1}\epsilon_i \in \mathrm{Bir}_k(Y_i), \quad i = 1, \ldots, r. \tag{3.3}$$

Note that $\beta_r = \alpha$. Let us prove that every $\beta_i \in \mathrm{BBir}_k(Y_i)$ by induction. The case $i = 0$ follows by definition. Suppose that $\beta_{i-1} \in \mathrm{BBir}_k(Y_{i-1})$ and, to the contrary, that $\beta_i \notin \mathrm{BBir}_k(Y_i)$. Let $p \in Y_i(k)$ be a base-point of β_i. Consider the two points

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

There are three possible situations:

(1) q' is not blown up by ϵ_i. This implies that β_i is well-defined at p due to (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 $(\epsilon_{i+1} \cdots \epsilon_r)^{-1}$. Relations (3.3) imply that α^{-1} contracts the proper transform of $E_{q'}$ to $\widetilde{p}$, so $\widetilde{p}$ is a base-point of α, which contradicts the fact that $\alpha \in \mathrm{BBir}_k(X)$.

(3) q' and q are both blown up by ϵ_i. By Lemma 3.11, the map β_i is well-defined everywhere on the exceptional divisor $E_q \subset Y_i$ over q. Since $p \in \epsilon_i^{-1}(q) = E_q$, we conclude that β_i is well-defined at p, contradiction.

Since we get contradictions in all possible cases, we conclude that $\beta_i \in \mathrm{BBir}_k(Y_i)$, hence the claim is fulfilled by induction. By Lemma 3.9, the permutations induced by β_i for all i, including α and β, have the same parity. □

Before entering the proof of the general case, let us introduce a method about resolving a birational self-map as a birational permutation. Let X' be a smooth surface over a finite field k and $\epsilon\colon X \to X'$ be a birational morphism over k that blows up a set $C \subset X'$ of closed points with exceptional locus $E \subset X$. Pick $\alpha' \in \mathrm{BBir}_k(X')$ and define $\alpha := \epsilon^{-1}\alpha'\epsilon$. Note that α belongs to $\mathrm{Bir}_k(X)$ but may not belong to $\mathrm{BBir}_k(X)$ in general.

Lemma 3.13. *Retain the notation above. Let $O_1, \ldots, O_n \subset X'(k)$ be the orbits of α' that meet the center C nontrivially. Note that the preimages of $O_j \setminus C$ in X make up the subset*

$$B := \bigcup_{j=1}^{n} \epsilon^{-1}(O_j \setminus C) \;\subset\; X(k) \setminus E.$$

Consider the blow-up $\eta\colon Z := \mathrm{Bl}_B X \longrightarrow X$. Then the composition $\eta^{-1}\alpha\eta$ belongs to $\mathrm{BBir}_k(Z)$.

Proof. Let $O \subset X'(k)$ be any of the orbits of α'. Note that, if $O \cap C = \emptyset$, then α is well-defined on the subset $(\epsilon^{-1}(O))(k) \subset X(k)$. Assume $O \cap C \neq \emptyset$. Then there are two possibilities:

(a) If $O \subset C$, then one can show that α is well-defined on $(\epsilon^{-1}(O))(k) \subset X(k)$ by applying Lemma 3.11 possibly a multiple of times.

(b) If $O \not\subset C$, then there exists $q \in O \setminus C$ such that $\alpha'(q) \in C$ and

$$O \setminus C = \{q, \alpha'^{-1}(q), \dots, \alpha'^{-\ell}(q)\} \quad \text{for some} \quad \ell \geq 0.$$

Note that $O \setminus C$ is a finite set as we are working over a finite field. In this case, α is undefined at $\epsilon_1^{-1}(q)$. Blowing up $\epsilon_1^{-1}(q)$ will resolve this indeterminacy by Lemma 3.11, though this will create a new base-point at $\epsilon^{-1}(\alpha'^{-1}(q))$. By blowing up this point and then $\epsilon^{-1}(\alpha'^{-2}(q)), \dots, \epsilon^{-1}(\alpha'^{-\ell}(q))$ subsequently, the base-points in $\epsilon^{-1}O$ will all be resolved.

By applying the above to $O_1, \dots, O_n$, we conclude that $\eta^{-1}\alpha\eta \in \mathrm{BBir}_k(Z)$. □

Proof of Theorem 1.2. We can eliminate the indeterminacy locus of h by a sequence of blow-ups at closed points [Kol07, Corollary 1.76]

$$\begin{array}{ccccccccc} X_r & \xrightarrow{\epsilon_r} & X_{r-1} & \xrightarrow{\epsilon_{r-1}} & \cdots & \xrightarrow{\epsilon_2} & X_1 & \xrightarrow{\epsilon_1} & X_0 = X \\ & \searrow^{\widetilde{h}} & & & & & & & \downarrow h \\ & & & & & & & & Y \end{array}$$

For each ϵ_i where $1 \leq i \leq r$, let $E_i \subset X_i$ be its exceptional locus and $C_{i-1} := \epsilon_i(E_i) \subset X_{i-1}$ be its center. We also define $C_r := \emptyset$. By Lemma 3.10, we can assume $C_i \subset E_i$ for $i = 1, \dots, r-1$. Let $\alpha_0 := \alpha$ and define inductively that

$$\alpha_i := \epsilon_i^{-1}\alpha_{i-1}\epsilon_i \in \mathrm{Bir}_k(X_i), \quad i = 1, \dots, r. \tag{3.4}$$

Let us prove by induction on i that there exists a birational morphism

$$\eta_i \colon Z_i \longrightarrow X_i \quad \text{such that} \quad \begin{cases} \tau_i := \eta_i^{-1}\alpha_i\eta_i \in \mathrm{BBir}_k(Z_i) \\ \text{its center } B_i \subset X_i \text{ is disjoint from } C_i. \end{cases} \tag{3.5}$$

For the initial case $i = 1$, consider the action of α_0 on $X(k)$ and let $O_1, \dots, O_n \subset X(k)$ be the orbits that meet C_0 nontrivially. Define

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

and consider the blow-up

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

Then $\tau_1 := \eta_1^{-1}\alpha_1\eta_1 \in \mathrm{BBir}_k(Z_1)$ by Lemma 3.13. Moreover, B_1 is disjoint from E_1 by construction. As $C_1 \subset E_1$, we conclude that $B_1 \cap C_1 = \emptyset$. This completes the initial step.

Assume that there exists an η_i as in (3.5) for some $1 \leq i \leq r-1$. Consider the fiber diagram

$$\begin{array}{ccccccc} & & X'_{i+1} := X_{i+1} \times_{X_i} Z_i & \xrightarrow{\pi_2} & Z_i & & \\ & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \eta_i} & & \\ \cdots & \longrightarrow & X_{i+1} & \xrightarrow{\epsilon_{i+1}} & X_i & \xrightarrow{\epsilon_i} & \cdots \end{array}$$

where π_1 and π_2 are the projections to the components of X'_{i+1}. Note that X'_{i+1} is the blow-up of X_i at the disjoint union $B_i \cup C_i$, and we can identify π_2 as the blow-up

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

By hypothesis, we have $\tau_i = \eta_i^{-1}\alpha_i\eta_i \in \mathrm{BBir}_k(Z_i)$, which can be lifted to X'_{i+1} as

$$\alpha'_{i+1} := \pi_2^{-1}\tau_i\pi_2 \in \mathrm{Bir}_k(X'_{i+1}).$$

By tracking the fiber diagram above, we obtain

$$\alpha'_{i+1} = \pi_2^{-1}\tau_i\pi_2 = \pi_2^{-1}\eta_i^{-1}\alpha_i\eta_i\pi_2 = \pi_1^{-1}\epsilon_{i+1}^{-1}\alpha_i\epsilon_{i+1}\pi_1 = \pi_1^{-1}\alpha_{i+1}\pi_1. \tag{3.6}$$

Let $O_1, \ldots, O_n \subset Z_i(k)$ be the orbits of the action of τ_i that satisfy $O_j \cap \eta_i^{-1}C_i \neq \emptyset$. Define

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

and consider the blow-up

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

Then $\tau_{i+1} := \eta'^{-1}_{i+1}\alpha'_{i+1}\eta'_{i+1} \in \mathrm{BBir}_k(Z_{i+1})$ by Lemma 3.13. Define

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

Using (3.6), we obtain

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

Hence η_{i+1} satisfies the first requirement in (3.5). For the second requirement, recall that η_{i+1} is constructed by subsequently blowing up $\epsilon_{i+1}^{-1}B_i \subset X_{i+1}$ and $B'_{i+1} \subset X'_{i+1}$. The set $\epsilon_{i+1}^{-1}B_i$ is disjoint from C_{i+1} because $C_{i+1} \subset E_{i+1}$ and $B_i \cap C_i = \emptyset$. On the other hand, the image

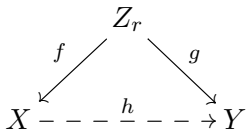
$$\eta_i\pi_2(B'_{i+1}) = \epsilon_{i+1}\pi_1(B'_{i+1}) \subset X_i$$

is disjoint from C_i, so $\pi_1(B'_{i+1})$ is disjoint from E_{i+1} and thus from C_{i+1}. We conclude that the center B_{i+1} of η_{i+1} is disjoint from C_{i+1}. This completes the inductive step.

Formula (3.5) with $i = r$ gives a birational morphism

$$\eta_r \colon Z_r \longrightarrow X_r \quad \text{ such that } \quad \tau_r := \eta_r^{-1}\alpha_r\eta_r \in \mathrm{BBir}_k(Z_r).$$

As a result, we obtain the commutative diagram



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

$$\gamma := f^{-1}\alpha f = (\epsilon_1 \cdots \epsilon_r \eta_r)^{-1}\alpha_0(\epsilon_1 \cdots \epsilon_r \eta_r) = \eta_r^{-1}\epsilon_r^{-1} \cdots \epsilon_1^{-1}\alpha_0\epsilon_1 \cdots \epsilon_r\eta_r = \eta_r^{-1}\alpha_r\eta_r = \tau_r,$$

which belongs to $\mathrm{BBir}_k(Z_r)$. Using the relations $h = gf^{-1}$ and $\beta = h\alpha h^{-1}$, we deduce that

$$\gamma = f^{-1}\alpha f = g^{-1}h\alpha h^{-1}g = g^{-1}\beta g.$$

By Lemma 3.12, the actions of α and β on the sets of k-points induce the same parity as the action of γ, which completes the proof. □

4 Birational permutations on rational surfaces

We prove Theorem 1.3 in this section. Using Theorem 1.2, this amounts to showing that over $\mathbb{F}_q$, $q = 2^m \geq 4$, permutations induced by the following maps are all even:

- Birational permutations on a conic bundle over $\mathbb{P}^1$ preserving the fiber class.
- Automorphisms of a rational del Pezzo surface.
- Elements of $\mathrm{BCr}_2(\mathbb{F}_q)$ of finite order.

One may wonder if there exists a surface over $\mathbb{F}_q$, $q = 2^m \geq 4$, that admits a birational odd permutation. Below we exhibit such an example over $\mathbb{F}_4$.

Example 4.1. Let us write $\mathbb{F}_4 = \mathbb{F}_2(\xi)$, where $\xi^2 + \xi + 1 = 0$, and let $\overline{\xi}$ denote the Galois conjugate of ξ. Consider the elliptic curve defined by the Weierstrass equation

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

Then $j(E) = 1$, and the group $\mathrm{Aut}(E) \cong \mathbb{Z}/2\mathbb{Z}$ is generated by $\sigma_E \colon (x, y) \mapsto (x, y + x)$ [Sil09, Propositions A.1.1 & A.1.2]. One can verify straightforwardly that

$$E(\mathbb{F}_2) = \{(1,0), (0,1), (1,1), p_\infty\}, \qquad E(\mathbb{F}_4) = E(\mathbb{F}_2) \cup \{(\xi,0), (\overline{\xi},0), (\xi,\xi), (\overline{\xi},\overline{\xi})\}$$

where p_∞ denotes the point at infinity. Moreover, the involution σ_E fixes $(0,1)$, p_∞, and exchanges points in each of the pairs $\{(1,0),(1,1)\}$, $\{(\xi,0),(\xi,\xi)\}$, $\{(\overline{\xi},0),(\overline{\xi},\overline{\xi})\}$. In particular, σ_E acts on $E(\mathbb{F}_4)$ as a product of three transpositions and thus is odd. Now consider the $\mathbb{P}^1$-bundle

$$X := \mathbb{P}^1 \times E \longrightarrow E$$

and define $\sigma_X \in \mathrm{Aut}(X)$ by $\sigma_X(p, q) = (p, \sigma_E(q))$. Then σ_X acts on $X(\mathbb{F}_4)$ as an odd permutation by Lemma 3.7. In fact, it is not hard to see that this permutation consists of 5 disjoint permutations of the same type as σ_E.

4.1 Birational permutations on conic bundles

Over a finite field k, a conic $C \subset \mathbb{P}^2_k$ can only be one of the followings:

(I) C is smooth, which implies that $C \cong \mathbb{P}^1_k$.

(II) C is a double line.

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

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

As an analogue of projective bundles over finite sets (see §3.2), given a finite set B, we define a *conic bundle over* B to be a union of conics indexed by B:

$$\mathcal{C} = \bigcup_{i \in B} C_i \quad \text{equipped with the map} \quad h \colon \mathcal{C} \to B : C_i \mapsto i.$$

Consider the set $\mathcal{C}(k)$ of k-points on $\mathcal{C}$. We are interested in elements $\sigma \in \mathrm{Sym}(\mathcal{C}(k))$ of the form:

(1) For every $i \in B$, there exists $j \in B$ such that $\sigma(C_i(k)) = C_j(k)$. Then $h\sigma h^{-1}$ 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 4.2. *Let $k = \mathbb{F}_q$, $q = 2^m \geq 4$, and $\sigma \in \mathrm{Sym}(\mathcal{C}(k))$ 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. 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 this setting, each nontrivial cycle is an odd permutation. Suppose that

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

is any orbit of σ_B. Then σ acts on the set of k-points on $h^{-1}(O) \subset \mathcal{C}$, and it suffices to show that this action is odd. This reduces the proof to the case $O = B$.

By property (2), the fibers over O are mutually isomorphic and thus of the same type. If they are of type (I), then the statement follows from Lemma 3.7. The case of type (II) is covered by the previous case by passing to the reduced substructure. If they are of type (III), then the node in each fiber appears as the only k-point in that fiber. This implies that σ and σ_B have the same cycle type, thus are both odd.

Assume that the fibers are of type (IV), that is, $C_i = h^{-1}(p_i) = \ell_i \cup \ell'_i$ where ℓ_i and ℓ'_i are copies of $\mathbb{P}^1_k$. Let σ_L denote the action of σ on the set of lines

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

In this case, the nodes $\delta_i := \ell_i \cap \ell'_i$ for $i = 1, \ldots, r$ form a single orbit under the action of σ. This forces σ_L to be one of the following forms:

(i) L has two orbits of size r. In this case, we can relabel the components of C_i as ℓ_i^+ and ℓ_i^- such that there is a cycle decomposition $\sigma_L = (\ell_1^+, \ldots, \ell_r^+)(\ell_1^-, \ldots, \ell_r^-)$.

(ii) L forms a single orbit of size $2r$. In this case, we can relabel the components of C_i as ℓ_i^+ and ℓ_i^- such that $\sigma_L = (\ell_1^+, \dots, \ell_r^+, \ell_1^-, \dots, \ell_r^-)$.

In both cases, we have the $\mathbb{P}^1_k$-bundles

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

where $O^\pm = \{p_1^\pm, ..., p_r^\pm\}$ are two copies of O. Taking their (disjoint) union gives a conic bundle

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

Note that the node δ_i splits as $\delta_i^+ \in \ell_i^+$ and $\delta_i^- \in \ell_i^-$ for each $1 \le i \le r$.

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

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

defines an element $\widetilde{\sigma} \in \mathrm{Sym}(\widetilde{\mathcal{C}}(k))$ that satisfies (1) and (2). Now we have

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

which is even. Because the fibers of $\widetilde{h}$ are smooth, we conclude that $\widetilde{\sigma}$ is even by the result for type (I). Since σ has one less odd cycle than $\widetilde{\sigma}$, the parity of σ is odd. If case (ii) holds, we can define $\widetilde{\sigma} \in \mathrm{Sym}(\widetilde{\mathcal{C}}(k))$ by replacing $(\delta_1, \dots, \delta_r)$ in σ with the cycle

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

Then $\widetilde{\sigma}$ satisfies (1) and (2), and we have

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

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

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

Corollary 4.3. *Let $\mathcal{C} \to D$ be a conic bundle over a curve D over $k = \mathbb{F}_q$, $q = 2^m \ge 4$. Suppose that $f \in \mathrm{BBir}_k(\mathcal{C})$ preserves the conic bundle structure, and let $\rho(f) \in \mathrm{Aut}(D)$ be the induced automorphism on D. Then*

- *the actions of f on $\mathcal{C}(k)$ and $\rho(f)$ on $D(k)$ have the same parity, and*
- *f induced an even permutation on $\mathcal{C}(k)$ if $D = \mathbb{P}^1$.*

Proof. The fibers of $\mathcal{C}$ over $D(k)$ form an example of a conic bundle over a finite set. The action of f on $\mathcal{C}(k)$ satisfies properties (1) and (2). Then the first conclusion follows Lemma 4.2, and the second statement follows from Proposition 3.5. □

4.2 Automorphisms of rational del Pezzo surfaces

Over an arbitrary field k, a *del Pezzo surface* X is defined to be 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*, namely, a surface that satisfies $X_{\overline{k}} := X \otimes_k \overline{k} \cong \mathbb{P}^2_{\overline{k}}$. Below is a simple observation about automorphisms of del Pezzo surfaces over finite fields:

Proposition 4.4. *Let X be a del Pezzo surface over a finite field k. Then $\mathrm{Aut}(X)$ is a finite group.*

Proof. 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 $\mathbb{P}^n$. This defines an embedding $\mathrm{Aut}(X) \hookrightarrow \mathrm{PGL}_{n+1}(k)$. Then the statement follows as $\mathrm{PGL}_{n+1}(k)$ is a finite group when k is finite. □

A surface X over a field k is called *rational* if there exists a birational map $X \dashrightarrow \mathbb{P}^2$ defined over k. In this section, we investigate the parities of the permutations on $X(\mathbb{F}_q)$ induced by automorphisms of a rational del Pezzo surface X over $\mathbb{F}_q$ for $q = 2^m \geq 4$. Our goal is to prove the following theorem:

Theorem 4.5. *Automorphisms of a rational del Pezzo surface X over $\mathbb{F}_q$ for $q = 2^m \geq 4$ induce only even permutations on $X(\mathbb{F}_q)$.*

We will proceed the proof case-by-case with the degree d going from high to low. As the parity of a permutation is invariant upon taking an odd power, we will assume the order of a permutation to be a power of 2 when studying its parity. The following lemma will be useful under this assumption:

Lemma 4.6. *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 fixed points.*

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

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]). Since the size of each orbit of σ divides $\mathrm{ord}(\sigma) = 2^r$, we have

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

which implies (1). Assume $\mathrm{ord}(\sigma) = 2$, that is, σ is an involution. In particular, σ is a product of disjoint 2-cycles. If σ has $4b + 1$ fixed points, then the amount of 2-cycles equals

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

which is an even number for $q = 2^m \geq 4$. This proves (2). □

Remark 4.7. Over $\mathbb{F}_2$, there exists an automorphism of a rational del Pezzo surfaces X which induces an odd permutation on $X(\mathbb{F}_2)$. To construct an example, one can start with a quadratic transformation $f \in \mathrm{BCr}_2(\mathbb{F}_2)$, that is, f is defined by the linear system of conics passing through three non-collinear points in $\mathbb{P}^2$ that form a $\mathrm{Gal}(\mathbb{F}_8/\mathbb{F}_2)$-orbit. By Lemma 5.6, upon composing f with a linear transformation, we can assume that f is involutive, so that $\mathrm{Bs}(f) = \mathrm{Bs}(f^{-1})$. Blowing up $\mathbb{P}^2$ at $\mathrm{Bs}(f)$ produces a del Pezzo surface X of degree 6 and resolves f as an automorphism f' on X. The action of f on $\mathbb{P}^2(\mathbb{F}_2)$ is odd by Lemma 5.7, so the action of f' on $X(\mathbb{F}_2)$ is odd as well by Theorem 1.2.

4.2.1 Rational del Pezzo surfaces of degree at least 4 Here we prove that the claim of Theorem 4.5 holds for rational del Pezzo surfaces of degree $d \geq 4$. The case $d = 9$ is covered by Proposition 3.5 since a rational Severi–Brauer surface is isomorphic to $\mathbb{P}^2$ by Châtelet. (See, for example, [GS17, Theorem 5.1.3].) We prove the remaining cases below:

Proposition 4.8. *Automorphisms of a rational del Pezzo surface X over $k = \mathbb{F}_q$, $q = 2^m \geq 4$, of degree $4 \leq d \leq 8$ induce only even permutations on $X(\mathbb{F}_q)$.*

Proof. Let $g \in \mathrm{Aut}(X)$. Because raising to an odd power does not change the parity of a permutation, we can assume the action on $X(k)$ induced by g has order a power of 2. This allows us to choose a point $p \in X(k)$ fixed by g as guaranteed by Lemma 4.6 (1).

Case $d = 8$. If X is not minimal (over k), then there exists a (-1)-curve $E \subset X$ over k, and contracting E gives a morphism $h\colon X \to \mathbb{P}^2$. Every $g \in \mathrm{Aut}(X)$ leaves E invariant, thus is conjugate to an automorphism of $\mathbb{P}^2$ fixing $h(E) \in \mathbb{P}^2$. Therefore, g induces an even permutation on $X(k)$ by Proposition 3.5 and Theorem 1.2.

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 the fixed point 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. both rational) over k, 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 and 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 Proposition 3.5 and Theorem 1.2 that g induces an even permutation.

Case $d = 7$. There is a unique (-1)-curve E on X that is invariant under both $\mathrm{Gal}(\overline{k}/k)$ and g. Hence contracting E gives $X \to X_8$ 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 1.2 and Case $d = 8$.

Case $d = 6$. Over the algebraic closure, $X_{\overline{k}}$ is obtained by blowing up three points a_1, a_2, a_3 in $\mathbb{P}^2_{\overline{k}}$, and it contains six (-1)-curves E_1, ..., E_6 such that, for $i \neq j$, we have $E_i \cdot E_j = 1$ if $j \equiv i + 1 \pmod 6$ and $E_i \cdot E_j = 0$ otherwise. Note that both $\mathrm{Gal}(\overline{k}/k)$ and g act on this set of (-1)-curves and preserve the intersection relations.

If p does not lie on any of these (-1)-curves, 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. Over $\overline{k}$, the three lines in $\mathbb{P}^2_{\overline{k}}$ that pass through p and one of a_1, a_2, a_3 lift to pairwise disjoint (-1)-curves on X_5 that meet three disjoint members of $\{E_1, \ldots, E_6\}$. Since this configuration is invariant under the action of both $\mathrm{Gal}(\overline{k}/k)$ and g_5, we can contract the three new (-1)-curves to get $X_5 \to X_8$, where X_8 is a del Pezzo surface of degree 8, such that 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 1.2.

Suppose p lies on one of the (-1)-curves, say, E_1. If p does not lie on any other (-1)-curve, then E_1 is 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 1.2. Otherwise, p lies on the intersection of two lines, say, E_1 and E_2. Then the orbit structure of $\{E_1, \ldots, E_6\}$ under both $\mathrm{Gal}(\overline{k}/k)$ and g is either $\{E_1\} \cup \cdots \cup \{E_6\}$ or $\{E_1, E_2\} \cup \{E_3, E_6\} \cup \{E_4, E_5\}$. In either case,

$\{E_3, E_6\}$ is invariant under both $\mathrm{Gal}(\overline{k}/k)$ and g, so blowing down E_3, E_6 yields $X \to X_8$, and g descends to an automorphism on X_8. We finish by applying Case $d = 8$ and Theorem 1.2.

Case $d = 5$. Over the algebraic closure, $X_{\overline{k}}$ is obtained by blowing up four points b_1, b_2, b_3, b_3 in $\mathbb{P}^2_{\overline{k}}$, and it contains ten (-1)-curves, where six of them come from the lines passing through two of b_1, b_2, b_3, b_3, and the remaining four are the exceptional curves. Let us denote the (-1)-curve passing through b_i and b_j as D_{kl}, where $k < l$ and $\{k, l\} = \{1, 2, 3, 4\} \setminus \{i, j\}$, and denote the exceptional curve over b_i as D_{i5}. In this setting, we have $D_{ij} \cdot D_{kl} = 1$ if i, j, k, l are pairwise distinct and $D_{ij} \cdot D_{kl} = 0$ otherwise.

If p does not lie on any of the (-1)-curves, then the blow-up $X_4 = \mathrm{Bl}_p(X)$ is a del Pezzo surface of degree 4, and g lifts to an automorphism g_4 on X_4. Let $E_p \subset X_4$ denote the exceptional curve lying above p. Over $\overline{k}$, the lines (resp. the conic) passing through p and one of (resp. all of) b_1, b_2, b_3, b_4 lift to five pairwise disjoint (-1)-curves that intersect E_p. These (-1)-curves form a set invariant under $\mathrm{Gal}(\overline{k}/k)$, so we can blow them down to get $X_4 \to \mathbb{P}^2$, and g_4 also descends to an automorphism on $\mathbb{P}^2$. An application of Proposition 3.5 and Theorem 1.2 does the job.

Suppose p lies on a (-1)-curve, say, 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 contract it to get $X \to X_6$, where X_6 is a del Pezzo surface of degree 6, and g descends to an automorphism of X_6. We are then done by Case $d = 6$ and Theorem 1.2. If p lies on another (-1)-curve, we can assume this is D_{34}. One can verify that these are the only two (-1)-curves that contain p. It follows that $D_{12} \cup D_{34}$ is defined over k and invariant under g. The other (-1)-curves that intersect $D_{12} \cup D_{34}$ are $D_{35}, D_{45}, D_{15}, D_{25}$. Hence the union $D_{35} \cup D_{45} \cup D_{15} \cup D_{25}$ is defined over k and invariant under g. These four curves are pairwise disjoint. Contracting them gives $X \to \mathbb{P}^2$, and g descends to an automorphism of $\mathbb{P}^2$. We are done after applying Proposition 3.5 and Theorem 1.2.

Case $d = 4$. First assume that p does not lie on a (-1)-curve. Then the blow-up 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 $\mathbb{P}^3$ over k. Each plane $H \subset \mathbb{P}^3$ containing E intersects X_3 in a residual conic, so the pencil of such planes determines a conic bundle $X_3 \to \mathbb{P}^1$ over k. Corollary 4.3 yields the claim in this case.

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 the claim follows from Case $d = 5$ and Theorem 1.2. Otherwise, p lies on exactly two (-1)-curves. This defines a (singular) conic Q on X. We can then define a conic bundle as follows: The linear system $|-K_X|$ embeds 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 4.3 that g induces an even permutation on $X(k)$. □

4.2.2 Rational del Pezzo surfaces of low degrees To prove Theorem 4.5 for rational del Pezzo surfaces of degree $d = 1, 2, 3$, we first prove a fact about permutations induced by a double cover structure that appear in these cases.

Lemma 4.9. *Let $Y = \mathbb{P}(a_0, \ldots, a_n)$ be a weighted projective space, with a_i the weights, over $k = \mathbb{F}_q$, where $q = 2^m \geq 2$. Let $\pi \colon X \to Y$ be a degree two Galois cover where X is given by*

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

for some nonzero homogeneous polynomials f and g in the weighted polynomial ring $k[x_0, \dots, x_n]$ of degrees d and $2d$, respectively. Let $\beta \in \mathrm{Aut}(X)$ be the deck transformation and $B \subset X$ be the ramification locus defined by $f = 0$. Assume that there is an exact sequence of groups

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

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

Proof. Let $h \in \mathrm{Aut}(X)$ and denote $h_0 := \pi_* h \in \mathrm{Aut}(Y)$. Since h_0 fixes the branch locus, $h_0^*(f) = cf$ for some nonzero constant $c \in k$. Let $k(X)$ be the function field of X, which is a quadratic extension over $k(Y)$, so by the Artin–Shreier theory, it is given by

$$u^2 + u = z \quad \text{for some} \quad z \in k(Y).$$

In our setting, the equation $w^2 + fw + g = 0$ can be turned into

$$w'^2 + w' = \frac{g}{f^2} \quad \text{where} \quad w' = \frac{g}{fw}. \tag{4.1}$$

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

$$w''^2 + w'' = \frac{g'}{c^2 f^2} \quad \text{where} \quad g' = h_0^*(g). \tag{4.2}$$

It is well-known that (4.1) and (4.2) define the same extension if and only if there exists $a \in k(Y)$ such that

$$\frac{g'}{c^2 f^2} = \frac{g}{f^2} + a^2 + a, \qquad \text{or equivalently,} \qquad g' = c^2 g + c^2 f^2 (a^2 + a). \tag{4.3}$$

By comparing the degrees among the terms, we conclude that $a \in k$.

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

$$x_i \mapsto h_0^*(x_i), \quad w \mapsto cw + caf.$$

Then $h'^*(f) = cf$ and $h'^*(g) = g'$, and one can use (4.3) to verify that this is well-defined. Let us show that h' induces an even permutation on $X(k) \setminus B(k)$ case-by-case:

- ($a = 0$) Let $p \in \pi(X(k)) \subset Y(k)$, singular or non-singular, and not lying on the branch locus, and O_p be the orbit of p under h_0. Let $r = |O_p|$ and note that $\pi^{-1}(O_p)$ consists of $2r$ many k-points. The assumption $a = 0$ implies that $\pi^{-1}(O_p)$ breaks into two orbits of the same size under h'. Hence h' induces an even permutation on $\pi^{-1}(O_p)$. As a consequence, h' induces an even permutation on $X(k) \setminus B(k)$.
- ($a = 1$) The transformation β is defined by $\beta^*(x_i) = x_i$ and $\beta^*(w) = w + f$, so $h'\beta$ has the same formula as h' but with $a = 0$, thus induces an even permutation on $X(k) \setminus B(k)$ by the previous case. The fact that β fixes every point on B implies that it is an even permutation on $X(k) \setminus B(k)$. Therefore, h' is an even permutation on $X(k) \setminus B(k)$.

- ($a \neq 0, 1$) Keep the notation of p, O_p, r as in the case $a = 0$. Because h_0^r fixes p as a point in $Y = \mathbb{P}(a_1, \ldots, a_n)$, it rescales the coordinates of p by a constant e respecting the weights. Since $h_0^*(f) = cf$, plugging in p gives $f(h_0(p)) = cf(p)$. This implies $e^d = c^r$. As a result, we get $g(h_0^r(p)) = c^{2r} g(p)$. On the other hand, applying h_0^* inductively on (4.3) gives

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

  Plugging in p, we get

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

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

Now we finish the proof by showing h is an even permutation on $X(k) \setminus B(k)$. The composition hh'^{-1} acts as the identity on Y, so it is either the identity or β. Because h' and $\beta h'$ both induce even permutations on $X(k) \setminus B(k)$, the result follows. □

Proposition 4.10. *Automorphisms of a rational del Pezzo surface X over $\mathbb{F}_q$, where $q = 2^m \geq 4$, of degree $d = 2, 3$ induce only even permutations on $X(\mathbb{F}_q)$.*

Proof. **Case $d = 2$.** The anticanonical model of X is a hypersurface of degree 4 in the weighted projective space $\mathbb{P}(w, x, y, z) = \mathbb{P}(2, 1, 1, 1)$, defined by

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

where $f, g \in k[x, y, z]$ have degrees 2, 4 respectively [Kol99, Theorem III.3.5]. The linear system $|-K_X|$ defines 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

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

Let us first prove that γ induces an even permutation. By Lemma 4.6 (2), 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

$$\gamma([w : x : y : z]) = [-w - f : x : y : z]. \tag{4.4}$$

In 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 consists respectively of two conjugate $\mathbb{F}_{q^2}$-lines, two $\mathbb{F}_q$-lines, or a double line. Because $q = 2^m \geq 4$, we have $|\mathrm{Fix}(\gamma)(\mathbb{F}_q)| \equiv 1 \bmod 4$, as desired.

Now applying Lemma 4.9, we conclude that every $h \in \mathrm{Aut}(X)$ induces an even permutation on $X(k) \setminus B(k)$ where $B = \{f = 0\}$. Hence, to finish the proof for $d = 2$, it suffices to show h induces an even permutation on $B(k)$. Since B is a conic in $\mathbb{P}^2$, this follows from Lemma 4.2.

Case $d = 3$**.** Let $g \in \mathrm{Aut}(X)$ and assume that its action on $X(k)$ has order a power of 2. Then Lemma 4.6 (1) implies that g has a fixed point $p \in X(k)$. If p does not lie on any (-1)-curve of $X_{\overline{k}}$, then g lifts to 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 above and Theorem 1.2.

Suppose p lies on exactly one (-1)-curve L. Then L is defined over k and invariant under g. Contracting L gives a del Pezzo surface X_4 of degree 4, and g descends to an automorphism of X_4. Then the result follows from Proposition 4.8 and Theorem 1.2.

Suppose p lies on exactly two (-1)-curves L_1, L_2. The linear system $|-K_X|$ embeds X as a cubic surface in $\mathbb{P}^3$. The plane containing L_1, L_2 intersects X at a third (-1)-curve L_3. Since the union $L_1 \cup L_2$ is invariant under both $\mathrm{Gal}(\overline{k}/k)$ and g, the curve L_3 is also invariant under $\mathrm{Gal}(\overline{k}/k)$ and g. Hence we can contract 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 $X_2 := \mathrm{Bl}_p(X)$, which is a weak del Pezzo surface of degree 2. The strict transforms of L_1, L_2, L_3 give a $\mathrm{Gal}(\overline{k}/k)$-invariant set of three disjoint (-2)-curves on X_2. We can contract them to get $X_2 \to Y$, and g_2 descends to an automorphism on Y. The morphism $X_2 \to \mathbb{P}^2$ 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 singular points of Y are above the singular points of the quartic.) The same argument as in Case $d = 2$ above shows that every automorphism of Y induces an even permutation. We finish by applying Theorem 1.2. □

Proposition 4.11. *Automorphisms of a rational del Pezzo surface X over $\mathbb{F}_q$, where $q = 2^m \geq 4$, of degree $d = 1$ induce only even permutations on $X(\mathbb{F}_q)$.*

Proof. The anticanonical model of X is a hypersurface of degree 6 in the weighted projective space $\mathbb{P}(w, z, x, y) = \mathbb{P}(3, 2, 1, 1)$, defined by

$$w^2 + a_1 wz + a_3 w = z^3 + a_2 z^2 + a_4 z + a_6$$

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

$$\rho \colon X \dashrightarrow \mathbb{P}^1 : [w : z : x : y] \mapsto [x : y]$$

whose indeterminacy locus consists of the single point $O := [1 : 1 : 0 : 0] \in X(\mathbb{F}_q)$, and its general fibers are elliptic curves possessing O as the identity elements. Since K_X is fixed under any automorphism of X, we get an exact sequence

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

Every element in G has the form $[w : z : x : y] \mapsto [W(w, z, x, y) : Z(w, z, x, y) : x : y]$ which preserves the equation of X. Comparing the degrees in x, y yields that $W = w$ or $W = w - a_1 z - a_3$, and $Z^3 = z^3$. Furthermore, if $a_4 \neq 0$, then $Z = z$, which implies that $G \simeq \mathbb{Z}/2\mathbb{Z}$ and is generated by the *Bertini involution*

$$\beta \colon [w : z : x : y] \mapsto [w - a_1 z - a_3 : z : x : y]. \tag{4.5}$$

(This involution induces the inverse map under the group law when restricting to a smooth fiber of the elliptic fibration $\rho \colon X \dashrightarrow \mathbb{P}^1$.) Suppose that $a_4 = 0$. If $a_2 \neq 0$, then $Z^2 = z^2$, thus $Z = z$, which implies again that $G = \langle \beta \rangle$. If $a_2 = 0$ and there exists a primitive third root of unity δ, then

G is generated by β and the element $[w : z : x : y] \mapsto [w : \delta z : x : y]$, hence $G \simeq \mathbb{Z}/6\mathbb{Z}$. If there is no such δ, then $G = \langle\beta\rangle$.

We first show that the involution β induces an even permutation on $X(\mathbb{F}_q)$. By Lemma 4.6 (2), it suffices to show that the fixed point set $\mathrm{Fix}(\beta)(\mathbb{F}_q)$ of β in $X(\mathbb{F}_q)$ has cardinality 1 mod 4. In characteristic 2, the fixed locus is given by $a_1(x,y)z + a_3(x,y) = 0$. Note that $O = [1 : 1 : 0 : 0]$ is a fixed rational point, and is the only such point when $x = y = 0$. We now proceed by two cases depending on whether $a_1 = a_1(x,y)$ is the zero polynomial or not:

- If $a_1 \neq 0$, each $[x : y] \in \mathbb{P}^1(\mathbb{F}_q)$ with $a_1(x,y) \neq 0$ contributes a fixed $\mathbb{F}_q$-points by setting
$$z = a_3(x,y)/a_1(x,y),$$
$$w^2 = z^3 + a_2(x,y)z^2 + a_4(x,y)z + a_6(x,y),$$
which gives q more points. Now let $[x_0 : y_0] \in \mathbb{P}^1(\mathbb{F}_q)$ 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 $\mathbb{F}_q$-point. 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, together with O, 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 $a_3 \neq 0$ since X is smooth. Let $[x_0 : y_0] \in \mathbb{P}^1(\mathbb{F}_q)$ be 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. Hence, $|\mathrm{Fix}(\beta)(\mathbb{F}_q)| = q + 1 \equiv 1 \bmod 4$.

The involution β is also the deck transformation of the double cover $X \to \mathbb{P}(2,1,1)$ which maps $[w : z : x : y]$ to $[z : x : y]$. This double cover is defined by $|-2K_X|$, which is preserved under any automorphism of X, so there is an exact sequence
$$1 \longrightarrow \langle\beta\rangle \longrightarrow \mathrm{Aut}(X) \longrightarrow \mathrm{Aut}(\mathbb{P}(2,1,1)).$$
By Lemma 4.9, we get that any $h \in \mathrm{Aut}(X)$ induces an even permutation on $X(\mathbb{F}_q) \setminus B(\mathbb{F}_q)$ where $B := \{a_1 z + a_3 = 0\}$. It remains to show that h induces an even permutation on $B(\mathbb{F}_q)$. Note that $O \in B(\mathbb{F}_q)$ is the unique base-point of $|-K_X|$, so it is fixed under h. Moreover, since we only care about the rational points, it suffices to consider the reduced subscheme $B_0 := B_{red} \setminus \{O\}$. We proceed by cases:

- If $a_1 \neq 0$ and a_1 does not divide a_3, then B_0 is isomorphic to $\mathbb{A}^1$. Hence $h|_{B_0}$ induces an even permutation as a consequence of Proposition 3.5.
- If $a_1 \neq 0$ and a_1 divides a_3, then B_0 is isomorphic to a union of two copies of $\mathbb{A}^1$ meeting at a point, where one copy is a section of the elliptic fibration while the other is a fiber. The result again follows from Proposition 3.5.
- If $a_1 = 0$, then B_0 is isomorphic to a disjoint union of r copies of $\mathbb{A}^1$ where $0 \leq r \leq 3$. The case $r = 0$ is trivial, and the case $r = 1$ follows from Proposition 3.5. If $r = 2$, we can identify the disjoint union $\mathbb{A}^1 \cup \mathbb{A}^1$ as the smooth part of a degenerate conic, so this case is covered by Lemma 4.2. Suppose that $r = 3$. If h leaves one $\mathbb{A}^1$ invariant while switches the other two, then the claim follows from Proposition 3.5 and Lemma 4.2. If h acts on the three copies of $\mathbb{A}^1$ as a 3-cycle, we can first compactify each $\mathbb{A}^1$ as a $\mathbb{P}^1$, which gives us a $\mathbb{P}^1$-bundle over a finite set of 3 elements, and then extend the action of h to this bundle by multiplying it with a disjoint 3-cycle. This new permutation is even by Lemma 3.7, which implies that the original permutation is even.

As a result, the actions of h are even on $X(\mathbb{F}_q) \setminus B(\mathbb{F}_q)$ and $B(\mathbb{F}_q)$, thus is even on $X(\mathbb{F}_q)$. □

Proof of Theorem 4.5. Let $d = K_X^2$ be the degree of X. The claim follows from Proposition 3.5 for $d = 9$, from Proposition 4.8 for $4 \leq d \leq 8$, from Proposition 4.10 for $d = 2, 3$, and from Proposition 4.11 for $d = 1$. □

4.3 Birational self-maps of finite order

Lemma 4.12. *Let k be a perfect field. Suppose $G \subset \mathrm{Cr}_2(k)$ 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*

$$\phi^*\colon G \hookrightarrow \mathrm{Aut}(X) : g \to \phi^{-1} g \phi. \tag{4.6}$$

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 first statement can be proved by the same argument as in [DI09, Lemma 3.5]. 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

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

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.

Proof of Theorem 1.3. The statement for birational permutations on a conic bundle over $\mathbb{P}^1$ follows from Corollary 4.3. The statement for automorphisms of del Pezzo surfaces follows from Theorem 4.5. For birational permutations conjugate to maps of the previous two types, we apply Theorem 1.2. Note that this covers the elements in $\mathrm{BCr}_2(\mathbb{F}_q)$ of finite order due to Lemma 4.12. □

5 Non-existence of odd permutations

In this section, we produce a list of generators for $\mathrm{BCr}_2(k)$ where k is a perfect field. Then we conclude the proof of Theorem 1.1 by showing that the generators in this list induce only even permutations over $k = \mathbb{F}_{2^m}$ for $m \geq 2$. Throughout this section, we say a smooth zero-dimensional subscheme of a del Pezzo surface X (resp. a conic bundle X) is *in general position* if the blow-up of X at the subscheme is still a del Pezzo surface (resp. a conic bundle over the same base).

5.1 A list of generators over perfect fields

Lemma 5.1. *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. To prove (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 $g \in \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. Hence A is defined over $\mathbb{F}_q$.

To prove (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 those p_i in general position, and η_2 is the contraction of an orbit of (-1)-curves of size 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 5.2. *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 $i = 1, \ldots, r-1$, $\phi_{i+1}\phi_i$ is not an automorphism,*

(2) *for $i = 1, \ldots, r$, 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 5.3. 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 Lemma 5.4 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 $\rho(Q) = \rho(Q') = 1$.

Lemma 5.4. *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:*

$$\begin{array}{cccc} & X_6 & & \\ \swarrow & & \searrow & \\ \mathbb{P}^2 & \overset{f_{33}}{\dashrightarrow} & \mathbb{P}^2 & \end{array} \qquad \begin{array}{cccc} & X_2 & & \\ \swarrow & & \searrow & \\ \mathbb{P}^2 & \overset{f_{77}}{\dashrightarrow} & \mathbb{P}^2 & \end{array} \qquad \begin{array}{cccc} & X_1 & & \\ \swarrow & & \searrow & \\ \mathbb{P}^2 & \overset{f_{88}}{\dashrightarrow} & \mathbb{P}^2 & \end{array} \qquad \begin{array}{cccc} & X_3 & & \\ \swarrow & & \searrow & \\ \mathbb{P}^2 & \overset{f_{66}}{\dashrightarrow} & \mathbb{P}^2 & \end{array} \tag{5.1}$$

or

$$\begin{array}{ccccccc} & X_7 & & X_{8-d} & & X_7 & \\ \swarrow^{p} & & \swarrow & & \swarrow^{p'} & & \searrow \\ \mathbb{P}^2 & \overset{f_{21}}{\dashrightarrow} & Q & \overset{f_{dd}}{\dashrightarrow} & Q & \overset{f_{12}}{\dashrightarrow} & \mathbb{P}^2 \end{array} \qquad \begin{array}{l} d \in \{7, 6\} \\ p' = f_{dd}(p) \end{array} \tag{5.2}$$

or

$$\begin{array}{ccccccccccc} & X_7 & & X_3 & & X_{5-d} & & X_3 & & X_7 & \\ \swarrow^{p} & & \swarrow & & \swarrow & & \swarrow & & \swarrow^{p'} & & \searrow \\ \mathbb{P}^2 & \overset{f_{21}}{\dashrightarrow} & Q & \overset{f_{52}}{\dashrightarrow} & X_5 & \overset{f_{dd}}{\dashrightarrow} & X_5 & \overset{f_{52}^{-1}}{\dashrightarrow} & Q & \overset{f_{12}}{\dashrightarrow} & \mathbb{P}^2 \end{array} \qquad \begin{array}{l} d \in \{3, 4\} \\ p' = f_{52}^{-1} f_{dd} f_{52}(p) \end{array} \tag{5.3}$$

or

$$\begin{array}{ccccccccc} & X_7 & & X_3 & & X_4 & \\ \swarrow^{p} & & \swarrow & & \swarrow^{p'} & & \searrow \\ \mathbb{P}^2 & \overset{f_{21}}{\dashrightarrow} & Q & \overset{f_{52}}{\dashrightarrow} & X_5 & \overset{f_{15}}{\dashrightarrow} & \mathbb{P}^2 \end{array} \qquad p' = f_{52}(p) \tag{5.4}$$

or

$$\begin{array}{ccccccccccc} & X_7 & & X_3 & & X'_3 & & X'_7 & \\ \swarrow^{p} & & \swarrow & & \swarrow & & \swarrow^{p'} & & \searrow \\ \mathbb{P}^2 & \overset{f_{21}}{\dashrightarrow} & Q & \overset{f_{52}}{\dashrightarrow} & X_5 & \overset{f_{25}}{\dashrightarrow} & Q' & \overset{f_{12}}{\dashrightarrow} & \mathbb{P}^2 \end{array} \qquad p' = f_{25} f_{52}(p) \tag{5.5}$$

or

$$\begin{array}{ccccccccccc} & & X_7 & & & & X_5 & & X_5' & & X_7' & & \\ & \swarrow & & \searrow^{p} & & \swarrow & & \searrow^{t} & \swarrow^{p'} & & \searrow^{t'} \swarrow & & \searrow \\ \mathbb{P}^2 & & \xrightarrow{f_{21}} & & Q & & \xrightarrow{f_{31}} & & X_6 & \xrightarrow{f_{13}} & & Q' & \xrightarrow{f_{12}} & \mathbb{P}^2 \end{array} \quad \begin{array}{l} p' = f_{31}(p) \\ t' = f_{13}(t) \end{array} \tag{5.6}$$

or

$$\begin{array}{ccccccccccc} & & X_7 & & & & X_5 & & X_{6-d} & & X_5' & & X_7' & & \\ & \swarrow & & \searrow^{p} & & \swarrow & & \searrow^{r} & & \swarrow^{f_{dd}(r)} & & \swarrow^{p'} \searrow & & \searrow \\ \mathbb{P}^2 & & \xrightarrow{f_{21}} & & Q & & \xrightarrow{f_{31}} & & X_6 & \xrightarrow{f_{dd}} & X_6' & \xrightarrow{f_{13}} & Q' & \xrightarrow{f_{12}} & \mathbb{P}^2 \end{array} \quad \begin{array}{l} d \in \{2,3,4,5\} \\ p' = f_{13} f_{dd} f_{31}(p) \end{array} \tag{5.7}$$

or

$$\begin{array}{ccccccccc} & & X_4' & & & & X_{5-d} & & X_4' & & \\ & \swarrow & & \searrow^{p} & & \swarrow & & \searrow & \swarrow^{p'} & \searrow & \\ \mathbb{P}^2 & & \xrightarrow{f_{51}} & & X_5 & & \xrightarrow{f_{dd}} & & X_5 & \xrightarrow{f_{15}} & \mathbb{P}^2 \end{array} \quad \begin{array}{l} d \in \{4,3\} \\ p' = f_{dd}(p) \end{array} \tag{5.8}$$

Moreover, all links of the form f_{dd} can be chosen to be involutions, except possibly f_{66} in (5.1), f_{33} and f_{22} in (5.7).

Since the proof of Lemma 5.4 is quite long, we will check afterwards in Lemma 5.5 that the generators (5.5) and (5.6), (5.7, $d = 2$) and (5.8, $d = 4$) are redundant.

Proof. First note that any element in (3) is contained in $\mathrm{BCr}_2(k)$ as they only contract curves not defined over the ground field k. The list of involutions is from [Isk96, Theorem 2.6]. For (1) and (2), the claim over a finite field k follows from Lemma 5.1.

Let $\psi \in \mathrm{BCr}_2(k)$. There is a decomposition into Sarkisov links $\psi = \phi_r \cdots \phi_1$ as in Proposition 5.2. 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 5.2 (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 5.3. 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 5.2.

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 5.2 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 (5.1) 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 5.2 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 (5.2). Furthermore, $\psi(f_{12}\phi_2\phi_1)^{-1} = \phi_r \cdots \phi_3 f_{12}^{-1}$ is a decomposition as in Proposition 5.2 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 (5.3) and $\psi\nu^{-1} = \phi_r \cdots \phi_4\phi_2 f_{12}^{-1}$ is a decomposition as in Propostion 5.2.

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 (5.4).

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 (5.5), 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 5.2.

(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 5.2(1).

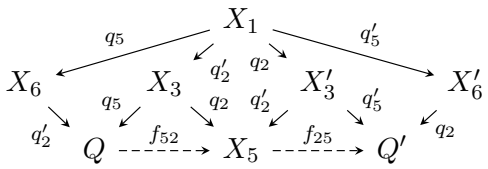
Suppose that $\phi_3 = f_{13}\colon X_6 \dashrightarrow Q'$ is a link to a quadric surface Q'. As $\psi\phi_1^{-1}\phi_2^{-1} = \phi_r \cdots \phi_3$ has exactly two rational base-points, namely $\phi_2(p)$ and t, and the base-point of q of ϕ_3 is a base-point of $\phi_r \cdots \phi_3$ by hypothesis (see Proposition 5.2(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 5.2(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 (5.6) and $\psi\nu^{-1} = \phi_r \cdots \phi_4 f_{12}^{-1}$ is as in Proposition 5.2.

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 (5.7) and $\psi\nu^{-1} = \phi_r \cdots \phi_4 f_{13}^{-1} f_{12}^{-1}$ is a decomposition as in Proposition 5.2. 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 (5.8) if $\phi_2 = f_{dd}$, $d = 3, 4$, or the inverse of a map of type (5.4) if $\phi_2 = f_{25}$. □

Lemma 5.5. *In the list in Lemma 5.4, the generators (5.5) and (5.6), (5.7, $d = 2$) and (5.8, $d = 4$) are redundant.*

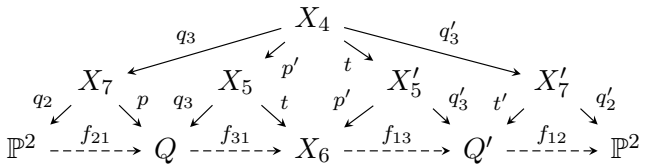
Proof. **(5.5):** Consider a map $\psi := f_{12}f_{25}f_{52}f_{21}$ as in (5.5) and denote by q_5 (resp. q_2) the base-point of f_{52} (resp. f_{25}) and q_2' (resp. q_5') the base-point of f_{52}^{-1} (resp. f_{25}^{-1}). We complete the blow-up diagram of ψ given in Lemma 5.4 (5.5) as follows:



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).

(5.6): Consider a map $\psi := f_{12}f_{13}f_{31}f_{21}$ as in (5.6) 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 Lemma 5.4 (5.6)

as follows:

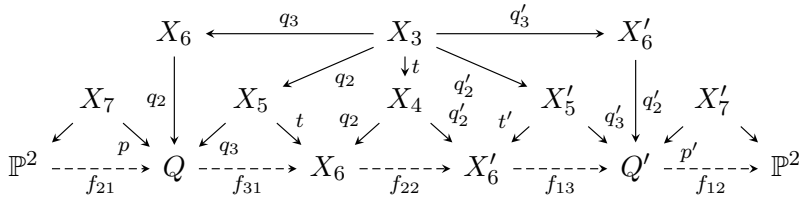


where $p' = f_{31}(p)$ and $t' = f_{13}(t)$. Let r_1, r_2 (resp. s_1, s_2, s_3) be the geometric components of q_2 (resp. $f_{21}^{-1}(q_3)$). On X_4, there are exactly sixteen (-1)-curves over the algebraic closure $\overline{k}$ of k:

- 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.

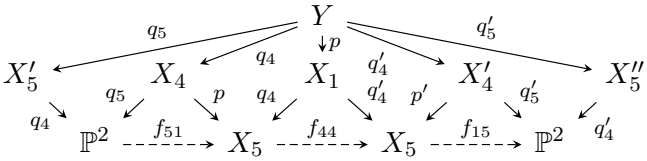
It follows that the blow-up of q_2, q_2' is redundant and $\psi = f_{33}$.

(5.7, $d = 2$): Consider a map $\psi := f_{12}f_{13}f_{22}f_{31}f_{21}$ as in (5.7) 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 Lemma 5.4 (5.7) as follows:



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

(5.8, $d = 4$): Consider a map $\psi := f_{15}f_{44}f_{51}$ as in (5.8). 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 Lemma 5.4 (5.8) as follows, where Y is the blow-up of X_1 at the point p, and is not a del Pezzo surface:



where $p' = f_{dd}(p)$. With Lemma 5.1, we obtain that ψ is in the family (2). □

Proof of Theorem 1.4. We compare the list of generators in [Isk91] contained in $\mathrm{BCr}_2(k)$ with the list of generators in Lemma 5.4, 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]:

Lemma 5.4	(1)	(2)	(5.1)	(5.2)	(5.3)
[Isk91]	A11	(15),(20)	(7),(8),(19'),(15"')	(10),(11)	(12),(13)

Lemma 5.4	(5.4)	(5.5)	(5.6)	(5.7)	(5.8)
[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 (5.6) is covered by (19') by Lemma 5.5. □

5.2 Revisiting the parity problem

Now let us prove that all generators given in Lemma 5.4 induce even permutations when the ground field is $k = \mathbb{F}_{2^m}$ for $m \geq 2$.

5.2.1 Parities of f_{33}, f_{77}, and f_{88} in (5.1) Up to automorphisms of $\mathbb{P}^2$, the maps f_{77} and f_{88} are Geiser and Bertini involutions respectively given by equations (4.4) and (4.5). By Theorem 4.5, they induce even permutations on $\mathbb{P}^2(\mathbb{F}_q)$ for $q = 2^m \geq 4$. On the other hand, the map f_{33} is a quadratic transformation, that is, a Cremona map defined by the linear system of conics passing through three non-collinear points in $\mathbb{P}^2$.

Lemma 5.6. *Let k be any field, $f \in \mathrm{BCr}_2(k)$ be a quadratic transformation and $\tau \in \mathrm{Cr}_2(k)$ be the standard quadratic involution $[x : y : z] \mapsto [yz : xz : xy]$.*

(1) *There exists $g \in \mathrm{PGL}_3(k)$ such that the composition gf is involutive.*

(2) *If f is involutive, then there exists $h \in \mathrm{PGL}_3(\overline{k})$ such that $\tau = h^{-1}fh$.*

Proof. There exists an extension k'/k of degree 3 and a generator $\sigma \in \mathrm{Gal}(k'/k) \cong \mathbb{Z}/3\mathbb{Z}$ such that

$$\mathrm{Bs}(f) = \{a, a^\sigma, a^{\sigma^2}\} \quad \text{for some} \quad a \in \mathbb{P}^2(k').$$

Since f is given by blowing up $\{a, a^\sigma, a^{\sigma^2}\}$ and then contracting the three lines passing through these points, the indeterminacy locus of f^{-1} is a Galois orbit for the same extension k'/k, namely,

$$\mathrm{Bs}(f^{-1}) = \{b, b^\sigma, b^{\sigma^2}\} \quad \text{for some} \quad b \in \mathbb{P}^2(k').$$

For every point $x = [x_0, x_1, x_2] \in \mathbb{P}^2$, we define

$$g_x := \begin{pmatrix} x_0 & x_0^\sigma & x_0^{\sigma^2} \\ x_1 & x_1^\sigma & x_1^{\sigma^2} \\ x_2 & x_2^\sigma & x_2^{\sigma^2} \end{pmatrix}$$

to be a linear map that sends the coordinate points $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0 : 1]$ to the Galois orbit points x, x^σ, x^{σ^2}, respectively. Note that g_x is invertible when x, x^σ, x^{σ^2} are not collinear. Let $g := g_a g_b^{-1}$, which can be easily verified to be defined over k. Then gf is involutive as the indeterminacy loci of this map and its inverse both coincide with $\{a, a^\sigma, a^{\sigma^2}\}$. This proves (1).

Assume that f is involutive, or equivalently, that $\mathrm{Bs}(f) = \{a, a^\sigma, a^{\sigma^2}\} = \mathrm{Bs}(f^{-1})$. Let $h = g_a$. Then the indeterminacy loci of $h^{-1}fh$ and its inverse both consist of the three coordinate points. This implies that $\tau = h^{-1}fh$ and thus proves (2). □

Recall that, for every $n \geq 1$, the *standard involution* $\tau\colon \mathbb{P}^n \dashrightarrow \mathbb{P}^n$ is defined by

$$\tau([x_0 : \cdots : x_n]) = [\tau_0 : \cdots : \tau_n] \quad \text{where} \quad \tau_i = \prod_{j \neq i} x_j.$$

In terms of the affine coordinates $(\xi_1, \ldots, \xi_n)$ where $\xi_i = x_i/x_0$, this map is written as

$$\tau(\xi_1, \ldots, \xi_n) = (\xi_1^{-1}, \ldots, \xi_n^{-1}).$$

From this expression, one can deduce that the fixed locus of τ consists of points of the form $[\pm 1 : \cdots : \pm 1]$. Note that these are the same point in characteristic 2. In the following, we prove a general fact about bijective Cremona transformations of $\mathbb{P}^n$ that are conjugate to τ by automorphisms, then use it to compute the parity induced by f_{33}.

Lemma 5.7. *Let $n \geq 1$, $k = \mathbb{F}_{2^m}$, and $f \in \mathrm{BCr}_n(k)$ be an involutive quadratic transformation. If there exists $h \in \mathrm{PGL}_{n+1}(\overline{k})$ such that $h^{-1}fh$ equals the standard involution τ, then the permutation induced by f on $\mathbb{P}^n(k)$ is odd when $m = 1$ and even when $m \geq 2$.*

Proof. The relation $\tau = h^{-1}fh$ implies that a point $x \in \mathbb{P}^n(\overline{k})$ is fixed by τ if and only if $h(x)$ is fixed by f. Because the fixed locus of τ consists of a single point $[1 : \cdots : 1]$, the fixed locus of f consists of a single point $y \in \mathbb{P}^n(\overline{k})$ as well. If $y \notin \mathbb{P}^n(k)$, then f acts on $\mathbb{P}^n(k)$ as an involution without a fixed point. This implies that the number of rational points

$$|\mathbb{P}^n(k)| = |\mathbb{P}^n(\mathbb{F}_{2^m})| = (2^m)^n + \cdots + 2^m + 1$$

is even, contradiction. Hence $y \in \mathbb{P}^n(k)$, and the action of f on $\mathbb{P}^n(k)$ is a composition of

$$\frac{1}{2}(|\mathbb{P}^n(k)| - 1) = \frac{1}{2}((2^m)^n + \cdots + 2^m)$$

many transpositions. The last integer is odd if $m = 1$ and even if $m \geq 2$, so the result follows. □

Proposition 5.8. *Let $k = \mathbb{F}_{2^m}$ with $m \geq 2$. Assume that $f \in \mathrm{BCr}_2(k)$ is of type f_{33}. Then f acts on $\mathbb{P}^2(k)$ as an even permutation.*

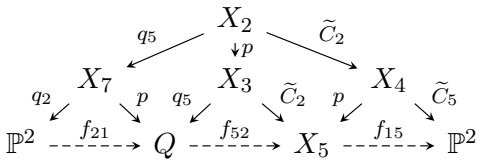
Proof. By Lemma 5.6, there exists $g \in \mathrm{PGL}_3(k)$ and $h \in \mathrm{PGL}_3(\overline{k})$ such that $h^{-1}gfh$ is the standard quadratic involution. It follows from Lemma 5.7 that gf acts on $\mathbb{P}^2(k)$ as an even permutation. Since g acts on $\mathbb{P}^2(k)$ evenly by Proposition 3.5, the result follows. □

5.2.2 Parities of the generators (5.2) to (5.8) Any birational map $f \in \mathrm{BCr}_2(k)$ which over $\overline{k}$ 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 $\overline{k}$ 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 4.5.

Generator (5.2), (5.3), or (5.7, $d = 4, 5$): 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 1.2.

Generator (5.4): Let q_2 be a point of degree 2 and q_5 a point of degree 5, both in general positions. Over $\overline{k}$ 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 $\overline{k}$ are orbits of disjoint (-1)-curves of length 2 and 5, namely the strict transforms of C_2 and C_5, denoted by $\widetilde{C}_2$ and $\widetilde{C}_5$.

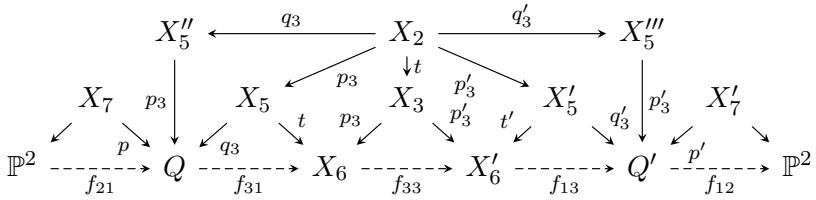


The blow-up diagram of f shows that f has the same geometric description as a Geiser involution over k with base-points q_2 and q_5. Thus, up to composition by an element of $\mathrm{PGL}_3(k)$, f lifts to an automorphism of the del Pezzo surface X_2. Now Theorem 4.5 and Proposition 3.5 imply that f induces en even permutation over $k = \mathbb{F}_q, q = 2^m \geq 4$.

Generator (5.5) By Lemma 5.5, 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 4.3.

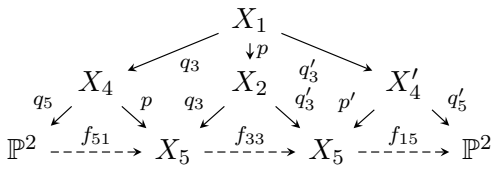
Generator (5.6) By Lemma 5.5, this generator is equal to f_{33}, so is treated in Proposition 5.8.

Generator (5.7, $d = 3$) We can complete the blow-up diagram as in Lemma 5.5 to get



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 1.2.

Generator (5.8) The case $d = 4$ follows from Lemma 5.5. If $d = 3$, we have the blow-up diagram,



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.

5.2.3 Parity of the generator f_{66} in (5.1) We finally prove that the remaining generator, namely $f_{66}\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$, induces a permutation of even parity on $\mathbb{P}^2(\mathbb{F}_{2^m})$ for $m \geq 2$.

Lemma 5.9 ([LS21, Lemma 4.20])**.** *Let $p_1, \ldots, p_6$ be a point of degree 6 in $\mathbb{P}^2$ over $\mathbb{F}_q$ such that $p_1, \ldots, p_6$ are in general position. Then at least $q^2 + q$ rational points of $\mathbb{P}^2$ are in general position with $p_1, \ldots, p_6$.*

Proof. Let σ be the generator of $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_q)$ and suppose that $\sigma^i(p_1) = p_i$ for $i = 1, \ldots, 6$. Let L_{ij} be the line through p_i, p_j, and let r be a rational point of $\mathbb{P}^2$ that is not on the intersection of L_{14}, L_{25}, L_{36}. The lines through the $p_1, ..., p_6$ make up three orbits, namely the orbit of L_{12}, L_{13} and L_{14}. We check that r is not contained in one of these three lines, from which it follows that r is not on any of the L_{ij}. If $r \in L_{12}$, then $L_{23} = \sigma(L_{12})$ contains r, p_2, so $L_{23} = L_{12}$, which is impossible. If $r \in L_{13}$, then r, p_3 are both contained in $\sigma^2(L_{13}) = L_{35}$, which is again impossible. If $r \in L_{14}$, then r is also contained in $\sigma(L_{14}) = L_{25}$ and $\sigma^2(L_{14}) = L_{36}$, which contradicts our choice of r. Finally, if $p_1, .., p_5, r$ lie on a conic C, then $\sigma(C)$ and C contain 5 common points and hence are equal, which is impossible. □

Lemma 5.10. *Suppose $p_1, \ldots, p_6$ make up a point of degree 6 in $\mathbb{P}^2$ over $\mathbb{F}_q$ such that no three are collinear and let L be the line through p_1 and p_2. Under the action of $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_q)$, there is at most one point $r \in L$ whose orbit in $\mathbb{P}^2$ is of length 2. In this case, r and its Galois conjugate form the only point of degree 2 contained in the orbit of L.*

Proof. Consider i as an integer modulo 6 and let

- σ to be the generator of $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_q)$ such that $\sigma^i(p_1) = p_{i+1}$, and
- $L_{p_ip_{i+1}}$ to be the line through p_i and p_{i+1} so that $L = L_{p_1p_2}$.

Suppose that there exists $r \in L_{p_1p_2}$ such that $\{r, \sigma(r)\}$ form a point of degree 2 in $\mathbb{P}^2$. Then

$$r \in L_{p_1p_2} \cap L_{p_3p_4} \cap L_{p_5p_6} \quad \text{and} \quad \sigma(r) \in L_{p_2p_3} \cap L_{p_4p_5} \cap L_{p_6,p_1}.$$

In particular, $\{r, \sigma(r)\}$ is contained in the orbit of $L_{p_1p_2}$. If $L_{p_1p_2}$ contains another point s whose orbit is of length 2. Then $L_{p_1p_2} \cap L_{p_3p_4}$ contains both r and s, thus $L_{p_1p_2} = L_{p_3p_4}$, which contradicts the hypothesis that no three of the p_i's are collinear. □

Lemma 5.11. *Let $C \subset \mathbb{P}^2$ be a singular cubic over an arbitrary field k. Then C is rational, that is, its normalization $\widetilde{C}$ is isomorphic to $\mathbb{P}^1$ over k.*

Proof. By Châtelet's theorem, $\widetilde{C} \cong \mathbb{P}^1$ over k if and only if $\widetilde{C}$ contains a k-point. This is always the case when C is a cuspidal cubic. Suppose that C is a nodal cubic and let $p \in C$ be the node. The linear system of lines passing through p is isomorphic to $\mathbb{P}^1$ over k. Note that $|\mathbb{P}^1(k)| \geq 3$ for any field k. Since the tangent cone at p contributes at most two elements to $\mathbb{P}^1(k)$, there exists a line $\ell \in \mathbb{P}^1(k)$ such that $\ell \cap C = \{p, p'\}$ for some k-point $p' \neq p$. The point p' induces a k-point on the normalization $\widetilde{C}$, so the proof is done. □

Lemma 5.12. *Let $q = 2^m \geq 2$ and suppose $p_1, \ldots, p_6$ make up a point of degree 6 in $\mathbb{P}^2$ over $\mathbb{F}_q$ contained in a singular cubic C. Then there are at least $\frac{1}{2}(q^2 - 2q - 2)$ points of degree 2 on C that are not on a conic with p_1, p_2, p_4, p_5.*

Proof. There is an involution σ on C which maps a general $x \in C(\overline{\mathbb{F}_q})$ to the residual intersection of the conic passing through p_1, p_2, p_4, p_5, x with C. Let $z \in C$ be the singular point and $\tau\colon \widetilde{C} \to C$ be the normalization. Then σ lifts to an involution $\widetilde{\sigma}$ on $\widetilde{C}$ which preserves the set $\tau^{-1}(z) \subset \widetilde{C}$. Notice that $\widetilde{C} \cong \mathbb{P}^1$ by Lemma 5.11. Then an elementary computation shows that $\widetilde{\sigma}$, up to conjugation over $\mathbb{F}_{q^6}$, acts on $\widetilde{C}$ as $x \mapsto x + a$ for some $a \in \mathbb{F}_{q^6}$.

If C is a nodal cubic, the total number of points of degree 2 on C is given by

$$\frac{1}{2}|C(\mathbb{F}_{q^2}) \setminus C(\mathbb{F}_q)| = \begin{cases} \frac{1}{2}(q^2 - q) & \text{if } \tau^{-1}(z) \text{ consists of two } \mathbb{F}_q\text{-points,} \\ \frac{1}{2}(q^2 - q - 2) & \text{if } \tau^{-1}(z) \text{ is a point of degree 2 over } \mathbb{F}_q. \end{cases}$$

If C is a cuspidal cubic, the total number of points of degree 2 on C is given by

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

Pick any $x \in C(\mathbb{F}_{q^2}) \setminus C(\mathbb{F}_q)$. Then x and its conjugate x^q lie on a conic with p_1, p_2, p_4, p_5 if and only if $x^q = x + a$. The last equation has at most q distinct solutions in x, so the number of degree-2 points on C lying on a conic with p_1, p_2, p_4, p_5 is at most $\frac{1}{2}q$. As a consequence, at least

$$\frac{1}{2}(q^2 - q - 2) - \frac{1}{2}q = \frac{1}{2}(q^2 - 2q - 2)$$

many points of degree 2 on C do not lie on a conic with p_1, p_2, p_4, p_5. □

Lemma 5.13. *Let $q = 2^m \geq 4$. Let p be a point of degree 6 in $\mathbb{P}^2$ over $\mathbb{F}_q$ such that its blow-up is a del Pezzo surface. Then there exists at least one point r of degree 2 in $\mathbb{P}^2$ such that the blow-up at p, r is still a del Pezzo surface (i.e. p, r are in general position).*

Proof. Choose a generator σ for $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_q)$ and let $p_1, \ldots, p_6$ be the orbit making up p such that $\sigma(p_i) = p_{i+1}$ for each i modulo 6. In the following, we prove that there exists a point $r = \{r_1, r_2\}$ of degree 2 in $\mathbb{P}^2$ such that

- no three of the eight points $p_1, \ldots, p_6, r_1, r_2$ are on a line,
- no six of them are on a conic, and
- no eight of them are on a nodal cubic with one being the double point.

Let $r = \{r_1, r_2\}$ be a point of degree 2 in $\mathbb{P}^2$ such that r_1 (resp. r_2) is not collinear with any two consecutive p_i's. Let L_{ij} be the line through p_i, p_j. The lines through the $p_1, ..., p_6$ make up three orbits, namely the orbit of L_{12}, L_{13} and L_{14}. By Lemma 5.10 there is at most one point of degree 2 in the orbit of L_{12}, and we choose r to be outside of the orbit of L_{12}. Note that the line through r is rational, so it cannot contain any p_i. Suppose that $r_1 \in L_{13}$. Then $r_1 \in \sigma^2(L_{13}) = L_{35}$ and thus $\sigma^2(L_{13}) \cap L_{13}$ contains p_3, r_1. This implies $\sigma(L_{13}) = L_{13}$, which is against our hypothesis. Suppose that $r_1 \in L_{14}$. Then $r_2 \in \sigma^3(L_{14}) = L_{14}$ and hence $L_{14} = \sigma^3(L_{14})$ is the line through r, which is impossible as we have already explained.

Suppose that $p_1, \ldots, p_4, r_1, r_2$ are on a conic C. Then $\sigma(C) \cap C$ contains p_2, p_3, p_4, r_1, r_2, hence $C = \sigma(C)$, that is, C is invariant under $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_q)$. This implies that C contains p, which is against our hypothesis. Suppose that $p_1, \ldots, p_5, r_1$ are on a conic C. Then $\sigma^2(C)$ passes through $p_3, p_4, p_5, p_6, p_1, r_1$. We have $C \cap \sigma^2(C)$ contains p_1, p_3, p_4, p_5, r_1 and hence $\sigma^2(C) = C$, which is

impossible as C does not contain p_6. To finish the conic case, recall from Lemma 5.9 that there is a rational point s in $\mathbb{P}^2$ such that $s, p_1, \dots, p_6$ are in general position. There exists a singular cubic containing $p_1, \dots, p_6$ with s its singular point. By Lemma 5.12, there are at least $\frac{1}{2}(q^2-2q-2) \geq 3$ points of degree 2 not on a conic with p_1, p_2, p_4, p_5. We can choose r_1, r_2 to be one of them.

Finally, if there is a nodal cubic C through the eight points $p_1, \dots, p_6, r_1, r_2$ with one of them its double point, then $\sigma(C) \neq C$ and $C \cdot \sigma(C) \geq 10$, which is impossible. □

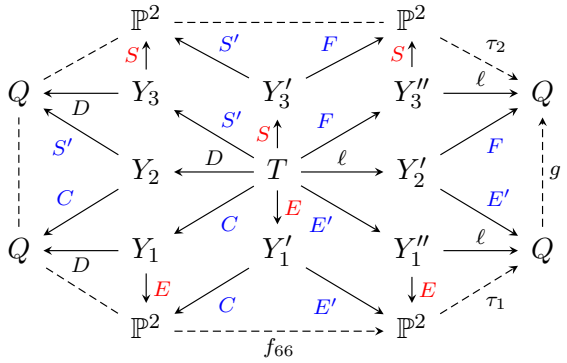
Remark 5.14. Let p, r be points in $\mathbb{P}^2$ of degree 6 and 2 such that their blow-up is a del Pezzo surface. On can describe the Bertini involution on this surface in a very nice way: Let S be the blow-up of p and view it as cubic surface in $\mathbb{P}^3$. We now can view r as a point of $\mathbb{P}^3$, and denote by $L \subset \mathbb{P}^3$ the line passing through r. We claim that L is not a (-1)-curve on S. Indeed, the 27 lines on S are the six exceptional divisors of the components $p_1, \dots, p_6$ of p, the 15 strict transforms of the lines through two of the p_i, and the 6 strict transforms of the conics passing through five of the p_i. None of these curves is defined over $\mathbb{F}_q$, while L is defined over $\mathbb{F}_q$. So, the line L intersects S transversely in r and a rational point s. The planes in $\mathbb{P}^3$ containing L induces an elliptic fibration on S, or more precisely, on the blow-up of S at r, s, where the exceptional curve of r defines a zero section. In particular, the Bertini involution can be defined as it is the multiplication by -1 using the group law on the generic fiber.

Proposition 5.15 ([LS21, Lemma 4.12 (2)])**.** *Assume that $m \geq 2$ and $q = 2^m \geq 4$. Then any link $f_{66} \colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ induces an even permutation on $\mathbb{P}^2(\mathbb{F}_q)$.*

Proof. Let p be the base-point of degree 6 of f_{66}. By Lemma 5.13, there exists a point r of degree 2 such that the blow-up at r, p is a del Pezzo surface T. Denote respectively by E_1, E_2 and $E'_1, \dots, E'_6$ the geometric components of their exceptional divisors. Let L be the pullback of the class of a line in $\mathbb{P}^2$. Then the only orbits of (-1)-curves in T of length at most 8 with pairwise disjoint members are as follows:

$$
\begin{aligned}
E &:= \{E_1, E_2\}, \\
E' &:= \{E'_1, \dots, E'_6\}, \\
\ell &:= \{L - E_1 - E_2\}, \\
C &:= \left\{ 2L - \sum\nolimits_{j \in \{1,\dots,6\}\setminus\{i\}} E'_j \;\middle|\; i = 1, \dots, 6 \right\}, \\
F &:= \left\{ 4L - 2E_1 - 2E_2 - 2E'_i - \sum\nolimits_{j \in \{1,\dots,6\}\setminus\{i\}} E'_j \;\middle|\; i = 1, \dots, 6 \right\}, \\
D &:= \left\{ 5L - E_1 - E_2 - 2\left(\sum\nolimits_{j=1}^{6} E'_j\right) \right\}, \\
S &:= \left\{ 6L - 3E_i - 2E_{3-i} - 2\left(\sum\nolimits_{j=1}^{6} E'_j\right) \;\middle|\; i = 1, 2 \right\}, \\
S' &:= \left\{ 6L - 2E_1 - 2E_2 - 3E'_i - 2\left(\sum\nolimits_{j \in \{1,\dots,6\}\setminus\{i\}} E'_j\right) \;\middle|\; i = 1, \dots, 6 \right\}.
\end{aligned}
$$

Drawing all possible blow-downs from T over $\mathbb{F}_q$, we obtain the following commutative diagram, where the arrows are denoted by the set of (-1)-curves they contract.



The Bertini involution $\beta \in \mathrm{Aut}(T)$ acts on the set $\{E, E', \ell, C, F, D, S, S'\}$, and it does not preserve any of them. It is thus a rotation of order 2, and it exchanges the rational curves ℓ, D. So, β is the birational map corresponding to the path of arrows from the lower left $\mathbb{P}^2$ to the upper right $\mathbb{P}^2$, that is,

$$\beta = \varepsilon \circ \tau_2^{-1} \circ g \circ \tau_1 \circ f_{66} \quad \text{for some} \quad \varepsilon \in \mathrm{PGL}_3(\mathbb{F}_q).$$

By Proposition 3.5, ε induces even parity on $\mathbb{P}^2(\mathbb{F}_q)$. By Theorem 4.5, the automorphism β induces an even permutation on $T(\mathbb{F}_q)$, and by Theorem 1.2, it induces an even permutation on $\mathbb{P}^2(\mathbb{F}_q)$. The map $\tau_2^{-1} \circ g \circ \tau_1$ is a generator of $\mathrm{BCr}_2(\mathbb{F}_q)$ of the form (5.2), and we showed in Section 5.2.2 that it induces an even permutation on $\mathbb{P}^2(\mathbb{F}_q)$. As a consequence, f_{66} induces an even permutation on $\mathbb{P}^2(\mathbb{F}_q)$. □

The Bertini involution acting on the commutative diagram in the above proof is a tool used in [LS21] to show that the Cremona group of rank 2 over an arbitrary perfect field is generated by involutions, where it is called *central symmetry* [LS21, Corollary 4.4].

Proof of Theorem 1.1. By Corollary 4.3, the results proved in §5.2.1 and §5.2.2, and Proposition 5.15, it follows that all generators of $\mathrm{BCr}(\mathbb{F}_q)$ induce even permutations on $\mathbb{P}^2(\mathbb{F}_q)$. □

6 Basic properties on the bijective Cremona group

In this section, we prove that the group $\mathrm{BCr}_2(k)$ is not finitely generated in most situations and is of infinite index as a subgroup of $\mathrm{Cr}_2(k)$. We also show that $\mathrm{BCr}_2(k)$ is not a normal subgroup of $\mathrm{Cr}_2(k)$, and discuss whether the kernel of the homomorphism $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^n(k))$ is a normal subgroup of $\mathrm{Cr}_n(k)$ or not.

6.1 Non-finite generation

The Cremona group $\mathrm{Cr}_2(k)$ itself is not finitely-generated over any field k. (See [Can12, Proposition 3.3] and [Can18, Proposition 3.6].) Here we prove that the same property holds for $\mathrm{BCr}_2(k)$ under the situations described below.

Proposition 6.1. *Let k be a field and let k^s be a separable closure. The group $\mathrm{BCr}_2(k)$ is not finitely generated provided that*

(1) *the field k is uncountable,*

(2) *the degree* $[k^s : k]$ *is finite, or*

(3) *the degree* $[k^s : k]$ *is infinite and* k *admits a separable quadratic extension* T/k.

We will prove the three statements in Proposition 6.1 separately. The proofs for (1) and (2) will come first as they are relatively shorter comparing to (3).

Proof of Proposition 6.1 (1). If k is uncountable, then $\mathrm{PGL}_3(k) \subset \mathrm{BCr}_2(k)$ is uncountable, thus $\mathrm{BCr}_2(k)$ cannot be a finitely generated group. (This proof was pointed out to us by Zinovy Reichstein.) □

Proof of Proposition 6.1 (2). Let k_0 be the prime field of k, which is either $\mathbb{Q}$ or $\mathbb{F}_p$ depending on the characteristic. For each $f \in \mathrm{BCr}_2(k)$, let $\mathrm{Bs}(f) \subset \mathbb{P}^2$ denote the base scheme of f, and let k_f/k_0 be the minimal field extension over which every geometric point of $\mathrm{Bs}(f)$ and $\mathrm{Bs}(f^{-1})$ (including the infinitely near ones) is defined. Note that f is defined over k_f by definition, and k_f may not contain k in general.

Assume that $\mathrm{BCr}_2(k)$ is generated by a finite subset Γ and let k_Γ be the composite of k_f for all $f \in \Gamma$. Since every $g \in \mathrm{BCr}_2(k)$ is a composition of elements of Γ, we have $k_g \subset k_\Gamma$. For every $a \in k$, the map $g\colon [x : y : z] \mapsto [x + ay : y : z]$ belongs to $\mathrm{PGL}_3(k)$, and thus $\mathrm{BCr}_2(k)$. Hence $k_g = k_0(a) \subset k_\Gamma$. This implies $k \subset k_\Gamma$ as $a \in k$ is arbitrary. Now we obtain a tower of field extensions

$$k_0 \subset k \subset k_\Gamma$$

where k_Γ is finitely-generated over k_0 and $[k_\Gamma : k]$ is finite. By the Artin–Tate lemma [AT51, Theorem 1], k is finitely-generated over k_0. Hence $[k : k_0]$ is finite. (See, e.g., [AM69, Proposition 7.9].) As $[k^s : k]$ is finite by hypothesis, we conclude that $[k^s : k_0]$ is finite, contradiction. □

When k^s/k is an infinite extension, our strategy is to construct a sequence of elements in $\mathrm{BCr}_2(k)$ whose indeterminacy loci contain points of arbitrarily large degrees. The construction requires careful selections of the candidates for the indeterminacy points in $\mathbb{P}^2$. Let us start with a few lemmas that help us deal with the positioning problem.

Lemma 6.2. *Suppose that* k *is a field with* $[k^s : k] = \infty$ *and let* T/k *be a separable quadratic extension. Then 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 them are collinear.*

Proof. Since T/k is separable, there exists a point in $\mathbb{P}^2$ of degree 2 that is reduced: we may take $a_1 = [a : 1 : 0]$ and $a_2 = [a' : 1 : 0]$, where $a, a' \in T \setminus k$ are the distinct roots of an irreducible quadratic polynomial over k. Take $\beta \subset \mathbb{P}^2$ to be any k-line not spanned by a_1 and a_2. Since $\beta \cong \mathbb{P}^1$ over k, we can find a pair of Galois-conjugate points $\{b_1, b_2\}$ on β in a similar way as before. Then $\{a_1, a_2\}$ and $\{b_1, b_2\}$ satisfy the requirements. □

As a consequence of Lemma 6.2, 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]. All but three of these conics are smooth, and the three degenerate ones are

$$\begin{aligned} C_0 &= \mathrm{span}(a_1, a_2) \cup \mathrm{span}(b_1, b_2), \\ C_1 &= \mathrm{span}(a_1, b_1) \cup \mathrm{span}(a_2, b_2), \\ C_2 &= \mathrm{span}(a_1, b_2) \cup \mathrm{span}(a_2, b_1). \end{aligned} \tag{6.1}$$

Note that these curves are defined over k.

Lemma 6.3. *Retain the notation from Lemma 6.2. 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_0/k be a non-trivial Galois extension different from T and let $K = K_0T$ be the composite field. Then there exists a closed point $x \in \ell_1$ defined over K/k but not over any proper subfield, such that*

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

(2) *Let $x = x_1, ..., x_{2r}$ be the $\mathrm{Gal}(K/k)$-conjugates of x. For each $1 \leq i \leq 2r$, the unique conic passing through $\{a_1, a_2, b_1, b_2, x_i\}$ is smooth.*

(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 a conic.*

Proof. Consider the $\mathbb{P}^1$ that parametrizes the conics passing through a_1, a_2, b_1, b_2. 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 $\mathbb{P}^1$, and let $F_1, ..., F_{2r}$ be the conics in $\mathbb{P}^2$ corresponding to these orbit points. Here we index the points in a way that the action of $\mathrm{Gal}(K/T)$ preserves the parities of the indices. In particular, the conic F_i with odd i (resp. even i) intersects ℓ_1 (resp. ℓ_2) at a_1 (resp. at a_2), and it cannot be tangent to ℓ_1 (resp. to ℓ_2) since otherwise it would be defined over T.

Let x_i be the residual intersection of F_i with ℓ_1 (resp. with ℓ_2) for odd i (resp. for even i) and let $x = x_1$. By construction, these points are all distinct, form an orbit under the action of $\mathrm{Gal}(K/k)$, and equally distribute on l_1 and l_2, which proves (1). Property (2) holds since each F_i is defined over K but not over any proper subfield, while the three degenerate conics C_0, C_1, C_2 are defined over k. Finally, if the set $\{a_1, a_2, b_1, b_2, x_i, x_j\}$ where $i \neq j$ lies on a conic C, then $C = F_i = F_j$, which contradicts the construction. This proves (3). □

Lemma 6.4. *Retain the notation from Lemma 6.3. Then there exists $f \in \mathrm{BCr}_2(k)$ whose indeterminacy locus contains a point of degree $[K : k]$ over k.*

Proof. The construction is accomplished via the following steps:

(1) Pick four points $a_1, a_2, b_1, b_2 \in \mathbb{P}^2$ as in Lemma 6.2. blow-up $\mathbb{P}^2$ along $\{a_1, a_2, b_1, b_2\}$ to obtain a conic bundle $\mathcal{C} \to \mathbb{P}^1$ 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, C_2 defined in (6.1). 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. Moreover, the $\mathrm{Gal}(K/k)$-action exchanges the irreducible components of the two singular fibres C_1 and C_2.

(2) Let x be the point obtained in Lemma 6.3 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 $X \to \mathcal{C}$. The strict transform of the fibers of $\mathcal{C} \to \mathbb{P}^1$ containing x is a $\mathrm{Gal}(K/k)$-orbit of (-1)-curves $F_1, \ldots, F_{2r}$ by Lemma 6.3(2). Using Castelnuovo's contractibility criterion in positive characteristics [Bǎd01, Theorem 3.30], blow down $F_1, ..., F_{2r}$ to get $X \to \mathcal{C}'$, and $\mathcal{C}'$ is a conic fibration over $\mathbb{P}^1$. The induced birational map $\phi \colon \mathcal{C} \dashrightarrow \mathcal{C}'$ preserves the conic fibrations.

(3) The birational map ϕ is regular around the singular fibers of $\mathcal{C} \to \mathbb{P}^1$, so $\phi(C_0), \phi(C_1), \phi(C_2)$ are the singular fibres of $\mathcal{C}'$ and the $\mathrm{Gal}(K/k)$-action exchanges the irreducible components of $\phi(C_1)$ and $\phi(C_2)$. Hence $K^2_{\mathcal{C}'} = 5$. Sine $\mathcal{C}'$ has a k-point, it follows from [Sch20, Lemma 6.5]

that there is a birational morphism $\mathcal{C}' \to \mathbb{P}^2$ contracting a $\mathrm{Gal}(K/k)$-orbit O of four points. Since $\mathcal{C}' \to \mathbb{P}^1$ has three singular fibres, one of which has $\mathrm{Gal}(K/k)$-invariant components, it follows that O is the union of two $\mathrm{Gal}(K/k)$-orbits $\{a_1', a_2'\}$ and $\{b_1', b_2'\}$.

The desired Cremona map f is then obtained from the composition

$$\begin{array}{ccccc} & & X & & \\ & \swarrow^{\text{contracting } E_i\text{'s}} & & \searrow^{\text{contracting } F_i\text{'s}} & \\ & \mathcal{C} & \xrightarrow{\phi} & \mathcal{C}' & \\ \swarrow & & & & \searrow \\ \mathbb{P}^2 & & \xrightarrow{f} & & \mathbb{P}^2. \end{array} \tag{6.2}$$

The map f belongs to $\mathrm{Cr}_2(k)$ since it is composed from maps defined over k. As for the indeterminacy loci, we have

$$\mathrm{Bs}(f) = \{a_1, a_2, b_1, b_2, x_1, \dots, x_{2r}\}, \qquad \mathrm{Bs}(f^{-1}) = \{a_1', a_2', b_1', b_2', y_1, \dots, y_{2r}\}$$

where $y_1, \dots, y_{2r}$ are the images of $F_1, ..., F_{2r}$ in the final $\mathbb{P}^2$. This shows that $f \in \mathrm{BCr}_2(k)$, and $\mathrm{Bs}(f)$ contains the $\mathrm{Gal}(K/k)$-orbit $\{x_1, ..., x_{2r}\}$ of size $2r = [K : k]$. □

Proof of Proposition 6.1 (3). Let k_f'/k be the be the minimal field extension over which every geometric point of $\mathrm{Bs}(f)$ and $\mathrm{Bs}(f^{-1})$ (including the infinitely near ones) is defined. 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 be contained in the composite of $k_{f_1}', ..., k_{f_r}'$, and so

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

which implies that the set of integers $\{[k_f' : k] : f \in \mathrm{BCr}_2(k)\}$ is bounded. The assumption $[k^s : k] = \infty$ guarantees that k admits a Galois extension K_0/k such that $K = K_0 T$ has arbitrarily large degree d over k. By Lemma 6.4, there exists $h \in \mathrm{BCr}_2(k)$ whose indeterminacy locus contains a point of degree d over k and hence $d \leq [k_h' : k]$, contradiction. □

6.2 The infinite index

The construction of the Cremona maps in Lemma 6.4 can be used to show that $\mathrm{BCr}_2(k)$ is of infinite index as a subgroup of $\mathrm{Cr}_2(k)$. Before proving this statement, let us remark that the transformation between conic bundles $\mathcal{C} \dashrightarrow \mathcal{C}'$ in the proof of Lemma 6.4 is a Sarkisov link of type II. The discovery of the induced Cremona maps can date back to 1877 by Ruffini, whose homaloidal type, as computed in the following lemma, is documented in [Hud24, page 234].

Lemma 6.5. *Consider the Cremona map (6.2). Let $M \in \mathrm{Pic}(X)$ be the pullback of a line class from the right $\mathbb{P}^2$. Then*

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

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

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

Divide both sides by 2 to get the result. □

Proposition 6.6. *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. Let us construct inductively an infinite sequence of maps $f_1, f_2, f_3, \ldots$ in $\mathrm{Cr}_2(k)$ as follows: Let f_1 be the identity map. Suppose that f_i is constructed and let $U \subset \mathbb{P}^2$ be the open subset such that $f_i|_U$ is an isomorphism. As k is infinite, we can take three non-collinear points $\{a, b, c\} \subset U(k)$. Define $f_{i+1} := \tau \circ f_i$ where τ is the quadratic transformation with $\mathrm{Bs}(\tau) = \{f_i(a), f_i(b), f_i(c)\}$. Then we have

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

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

Now assume that $k = \mathbb{F}_q$ is a finite field. The same idea as in the proof of Lemma 6.2 produces four points $a_1, a_2, b_1, b_2 \in \mathbb{P}^2(\mathbb{F}_q)$ such that no three are collinear. The main construction of the Cremona map carried out in Lemma 6.4 still works, and for each even integer $n = 2r$, we get a map $f_r \in \mathrm{Cr}_2(\mathbb{F}_q)$ such that $\mathrm{Bs}(f_r)$ supports at a_1, a_2, b_1, b_2 with multiplicity $2r$ (Lemma 6.5). We obtain an infinite sequence $\{f_1, f_2, f_3, \ldots\}$ of elements in $\mathrm{Cr}_2(\mathbb{F}_q)$ such that the left cosets $f_1\mathrm{BCr}_2(\mathbb{F}_q)$, $f_2\mathrm{BCr}_2(\mathbb{F}_q), \ldots$ 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 $2r$. □

6.3 On the non-normality

Over an algebraically closed field k, Blanc [Bla10, Theorem 4.2] proved that $\mathrm{Cr}_2(k)$ has no non-trivial closed normal subgroup with respect to its natural topology. On the other hand, Cantat and Lamy [CL13] proved that $\mathrm{Cr}_2(k)$ is not simple as an abstract group, and Lonjou generalized this result to any field k [Lon16]. Here we prove that $\mathrm{BCr}_2(k)$ is not a normal subgroup of $\mathrm{Cr}_2(k)$. For the kernel of the homomorphism $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^n(k))$, we prove that it is not a normal subgroup of $\mathrm{Cr}_n(k)$ when k is finite and that it is trivial when k is infinite.

Proposition 6.7. *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 $f : [x : y : z] \mapsto [yz : zx : xy]$ and $g \in \mathrm{PGL}_3(k) \subset \mathrm{BCr}_2(k)$ be any map sending $[1 : 0 : 0]$ to $[1 : 1 : 1]$. Then $f^{-1}gf$ contracts the line $\{x = 0\}$ to the point

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

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

Proposition 6.8. *Let k be a finite field. Then the kernel of $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^n(k))$, where $n \geq 2$, is not a normal subgroup of $\mathrm{Cr}_n(k)$.*

Proof. Let N denote the kernel of $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^2(k))$. Suppose, to the contrary, that N is a normal subgroup of $\mathrm{Cr}_n(k)$. Let $\ell \in k[x_2, \dots, x_n]$ be a linear homogeneous polynomial. Consider the birational map

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

and its inverse

$$f^{-1}\colon [x_0 : \cdots : x_n] \mapsto [\ell x_0 : x_1x_0 : x_2\ell : \cdots : x_n\ell].$$

A straightforward computation shows that both f and f^{-1} contract two and only two hypersurfaces, namely, the hyperplanes $\{x_0 = 0\}$ and $\{\ell = 0\}$. Moreover, f and f^{-1}, respectively, contracts the union $\{x_0 = 0\} \cup \{\ell = 0\}$ onto

$$\mathrm{Bs}(f^{-1}) = \{\ell = x_0 = 0\} \cup \{\ell = x_1 = 0\}, \quad \mathrm{Bs}(f) = \{x_0 = x_1 = 0\} \cup \{x_0 = \ell = 0\}.$$

For every $g \in N$, we claim that

$$g(\{x_0 = 0\} \cup \{\ell = 0\}) = \{x_0 = 0\} \cup \{\ell = 0\}. \tag{6.3}$$

First note that $g(\{x_0 = 0\} \cup \{\ell = 0\})$ is a hypersurface due to the facts that g is bijective and that $\{x_0 = 0\} \cup \{\ell = 0\}$ contains k-points. Since N is normal, we have $fg = hf$ for some $h \in N$. Suppose that $g(\{x_0 = 0\} \cup \{\ell = 0\})$ is not contained in $\{x_0 = 0\} \cup \{\ell = 0\}$. Then $fg(\{x_0 = 0\} \cup \{\ell = 0\})$ is a hypersurface while $hf(\{x_0 = 0\} \cup \{\ell = 0\})$ is not, contradiction. Therefore, we have

$$g(\{x_0 = 0\} \cup \{\ell = 0\}) \subset \{x_0 = 0\} \cup \{\ell = 0\}.$$

The same argument with g replaced by g^{-1} implies that

$$\{x_0 = 0\} \cup \{\ell = 0\} \subset g(\{x_0 = 0\} \cup \{\ell = 0\}).$$

Hence (6.3) follows. By applying the same argument with f replaced by $\alpha f \alpha^{-1}$ for any $\alpha \in \mathrm{Aut}(\mathbb{P}^n)$, we conclude that (6.3) holds for any union of two distinct rational hyperplanes. This implies that g preserves any rational hyperplane of $\mathbb{P}^n$.

Write $g \in N$ as $g([x_0 : \cdots : x_n]) = [g_0 : \cdots : g_n]$ where $g_i \in k[x_0, \dots, x_n]$ are homogeneous polynomials without a common factor. As g preserves each coordinate hyperplane $\{x_i = 0\}$, we have $g_i = x_i g_i'$ for some $g_i' \in k[x_0, \dots, x_n]$. The fact that g^{-1} also preserves each $\{x_i = 0\}$ then implies that

$$g^{-1}(\{x_i = 0\}) = \{g_i = 0\} = \{x_i g_i' = 0\} = \{x_i = 0\}$$

hence $x_i g_i' = a_i x_i$ for some $a_i \in k^*$. Therefore $g_i' = a_i \in k^*$ for all i 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 $\mathbb{P}^n$, and thus equal to the identity map. We conclude that $N = \{\mathrm{Id}\}$, which is a contradiction because $\mathrm{BCr}_n(k)$ is infinite by Lemma 6.4 and N is never trivial as it is of finite index in $\mathrm{BCr}_n(k)$. □

Proposition 6.9. *If k is an infinite field, then $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^n(k))$, where $n \geq 1$, is injective.*

Proof. Every element in the kernel of $\mathrm{BCr}_n(k) \to \mathrm{Sym}(\mathbb{P}^n(k))$ fixes $\mathbb{P}^n(k)$, which is a Zariski dense subset of $\mathbb{P}^n$. This forces such an element to be the identity map. □

References

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[AT51] Emil Artin and John T. Tate, *A note on finite ring extensions*, J. Math. Soc. Japan **3** (1951), 74–77.

[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.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).

[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.

[GLU21] Anthony Genevois, Anne Lonjou, and Christian Urech, *Cremona groups over finite fields, Neretin groups, and non-positively curved cube complexes* (2021). Preprint, arXiv:2110.14605v1.

[GS17] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 165, Cambridge University Press, Cambridge, 2017.

[Hud24] Hilda P. Hudson, *Plane Homaloidal Families of General Degree*, Proc. London Math. Soc. (2) **22** (1924), 223–247.

[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.

[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.

[LS21] Stéphane Lamy and Julia Schneider, *Generating the Cremona groups by involutions* (2021). Preprint, arXiv:2110.02851v1.

[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.

[Sch20] Julia Schneider, *Relations in the cremona group over perfect fields*, Annales de l'Institut Fourier (to appear), 2020.

[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
Email: sasgarli@math.ubc.ca

K.-W. Lai, Mathematisches Institut der Universität Bonn
Endenicher Allee 60, 53121 Bonn, Deutschland
Email: kwlai@math.uni-bonn.de

M. Nakahara, Department of Mathematics
University of Washington
Seattle, WA 98195, USA
Email: mn75@uw.edu

S. Zimmermann, Univ Angers, CNRS, LAREMA, SFR MATHSTIC, F-49000 Angers, France
Email: susanna.zimmermann@univ-angers.fr