A GENERALIZATION OF BRING’S CURVE IN ANY CHARACTERISTIC

GÁBOR KORCHMÁROS, STEFANO LIA, AND MARCO TIMPANELLA

Abstract. A natural generalization of Bring’s curve valid over any field \( K \) of zero characteristic or positive characteristic \( p \geq 7 \), is the algebraic variety \( V \) of \( \text{PG}(m-1, K) \), \( m \geq 5 \), which is the complete intersection of the projective algebraic hypersurfaces of homogeneous equations \( x_k^1 + \cdots + x_k^m = 0 \) with \( 1 \leq k \leq m-2 \). In positive characteristic, we also assume \( m \leq p-1 \). Up to a change of coordinates in \( \text{PG}(m-1, K) \), we show that \( V \) is a projective, absolutely irreducible, non-singular curve of \( \text{PG}(m-2, K) \). We show that, if the automorphism group \( \text{Aut}(V) \) is tame (in particular in characteristic zero), then \( \text{Aut}(V) \) is linear and isomorphic to \( \text{Sym}_m \). Remarkably, in positive characteristic, \( \text{Aut}(V) \) may be larger; in particular \( \text{Aut}(V) \) happens to contain non-tame projectivities and this occurs precisely when \( m = p-1 \). In positive characteristic, we further investigate the two extremal cases, \( m = 5 \) and \( m = p-1 \), providing information on the number of rational points. In particular, for \( m = 5 \) we show that there exist infinitely many primes \( p \) such that \( V \) is an \( \mathbb{F}_p^2 \)-maximal curve of genus 4. We also highlight connections with previous work by Rédei on the famous Minkowski conjecture proven by Hajós (1941), as well as with more recent results by Rodríguez Villegas, Voloch, and Zagier (2001) on plane curves attaining the Stöhr-Voloch bound, and the regular sequence problem for systems of diagonal equations introduced by Conca, Krattenthaler, and Watanabe (2009).

Keywords: algebraic curves, function fields, positive characteristic, automorphism groups.

Subject classifications: 14H37, 14H05.

1. Introduction

Bring’s curve is well known from classical geometry as being the curve with the largest automorphism group among all genus 4 complex curves; see [4]. Its canonical representation in the complex 4-space is the complete intersection of three algebraic hypersurfaces of equation \( x_1^k + \cdots + x_5^k = 0 \) with \( 1 \leq k \leq 3 \). A natural generalization of Bring’s curve valid over any field \( K \) of zero characteristic, or positive characteristic \( p \geq 7 \), is the algebraic variety \( V \) of \( \text{PG}(m-1, K) \), \( m \geq 5 \), which is the complete intersection of the projective algebraic hypersurfaces of homogeneous equations

\[
\begin{align*}
X_1^1 + X_2^1 + \cdots + X_m^1 &= 0; \\
X_1^2 + X_2^2 + \cdots + X_m^2 &= 0; \\
& \quad \vdots \\
X_1^{m-2} + X_2^{m-2} + \cdots + X_m^{m-2} &= 0.
\end{align*}
\]

From now on we assume \( m \leq p-1 \) when \( K \) has characteristic \( p \). The first equation in (1) implies that \( V \) is contained in the hyperplane of homogeneous equation \( X_1 + X_2 + \cdots + X_m = 0 \). Up to a change of coordinates in \( \text{PG}(m-1, K) \), we show that \( V \) is a projective, absolutely irreducible, non-singular curve of degree \((m-2)!\) embedded in \( \text{PG}(m-2, K) \); see Theorem 1.10.

The symmetric group \( \text{Sym}_m \) has a natural action on the coordinates \((X_1 : \ldots : X_m)\) of \( \text{PG}(m-1, K) \). Therefore, the automorphism group \( \text{Aut}(V) \) of \( V \) has a subgroup \( G \) isomorphic to \( \text{Sym}_m \). We prove that \( G = \text{Aut}(V) \) whenever \( \text{Aut}(V) \) is tame, and in particular in zero characteristic; see Theorem 1.11. In Section
we show however that if \( p = m - 1 \) then \( \text{Aut}(V) \) is non-tame, i.e. \( V \) has an automorphism of order \( p \) fixing a point of \( V \). In particular, the linear subgroup \( L \text{Aut}(V) \) of \( \text{Aut}(V) \) is isomorphic to \( S_p \) and hence \( \text{Aut}(V) \) properly contains \( G \); see Theorem 7.2 whose proof uses the deep Zalesskiı˘-Sereˇkind classification theorem from Group theory. In Section 8 we investigate the quotient curves of \( V \) with respect to subgroups of \( G \).

The most interesting cases for the choice of a subgroup are the stabilizers of one or more coordinates. Since two such subgroups are conjugate in \( G \) if they fix the same number of coordinates, it is enough to consider the stabilizer \( G_{d+1,\ldots,m} \) of the coordinates \( X_{d+1}, \ldots, X_m \) in \( \text{Aut}(V) \) with \( 1 \leq d \leq m - 1 \). A careful analysis of the actions of these stabilizers on the points of \( V \), carried out in Section 6 together with the Hurwitz genus formula, allows to compute the genus of the quotient curve \( V_d = V/G_{d+1,\ldots,m} \); see Proposition 6.3. The quotient curve \( V_d \) turns out to be rational for \( d = m - 2 \), otherwise its genus \( g \) is quite large; see (18).

The projection of \( V \) from the \( m - d - 1 \) dimensional projective subspace \( \Sigma \) of equations \( X_1 = 0, \ldots, X_d = 0 \) is also a useful tool for the study of \( V \) by virtue of the fact that \( \Sigma \cap V = \emptyset \). Let \( V_d \) be the curve obtained by projecting \( V \) from the vertex \( \Sigma \) to a projective subspace \( \Sigma' \) of dimension \( d - 1 \) disjoint from \( \Sigma \). Comparison of \( V_d \) with the quotient curve \( V_d \) shows that they are actually isomorphic; see Proposition 6.1. Therefore, the function field extension \( \mathbb{K}(V) : \mathbb{K}(V_d) \) is Galois, that is, the vertex \( \Sigma \) can be viewed as a Galois subspace (also called higher dimensional Galois-point) for \( V \). This shows that there are many higher dimensional Galois-subspaces for \( V \), which is a somewhat rare phenomena. For results and open problems on Galois-points; see the recent papers [2, 12, 13, 15, 21]. In Section 6.1 the case \( d = m - 3 \) is investigated more closely. An explicit equation of \( V_{m-3} \) is given in Theorem 6.3 which shows that if \( \mathbb{K} \) is either an algebraic closure of the rational field \( \mathbb{Q} \), or of the prime field \( \mathbb{F}_p \), then \( V_{m-3} \) coincides with the plane curve of degree \( m - 2 \) investigated by Rodríguez Villegas, Voloch and Zagier [20], who pointed out that this curve has many points; in particular, for \( m = p - 1 \), it is a non-singular plane curve attaining the Stöhr-Voloch bound.

From an algebraic number theory point of view, (11) is a particular system of diagonal equations. Proposition 6.7 shows that every solution of (11) also satisfies further diagonal equations. On the other hand, Lemmas 5.2 and 5.3 imply that \( \{1, 2, \ldots, m\} \) provides a regular sequence of symmetric polynomials, i.e. the system of diagonal equations of \( x_1^k + \cdots + x_m^k = 0 \) with \( k \) ranging over \( \{1, 2, \ldots, m\} \) has only the trivial solution \( (0, 0, \ldots, 0) \). This gives a different proof for Proposition 2.9 of the paper of Conca, Krattenthaler and Watanabe [7] where the authors relied on the interpretation of the \( q \)-analogue of the binomial coefficient as a Hilbert function. In the same paper [7], the general notion of a regular sequence associated to \( \mathcal{A} \subset \mathbb{N}^* \) was introduced as any system of diagonal equations \( x_1^k + \cdots + x_m^k = 0 \) with \( k \in \mathcal{A} \) which has only the trivial solution \( (0, 0, \ldots, 0) \). [7] Lemma 2.8 shows (over the complex field) a simple necessary condition on \( \mathcal{A} \) to be a regular system, namely that \( m! \) divides the product of the integers in \( \mathcal{A} \). In this context, the major issue to find easily expressible sufficient conditions turned out to be surprisingly difficult. For the smallest case \( m = 3 \), the conjecture is that the above necessary condition is also sufficient, that is, \( \mathcal{A} = \{a, b, c\} \) is associated to a regular system whenever \( abc \equiv 0 \pmod{6} \). Evidences for this conjecture were given in [7] and later in [3]. For further developments related to regular sequences, see [10, 11, 14, 25, 26].

In positive characteristic, an algebraic closure of the prime field \( \mathbb{F}_p \) with \( p \geq 7 \) is chosen for \( \mathbb{K} \) and two extremal cases are investigated further, namely \( m = 5 \) and \( m = p - 1 \). In the former case, \( V \) can be viewed as the characteristic \( p \) version of the Bring curve, and for infinitely many primes \( p \) we prove that \( V \) is an \( \mathbb{F}_{p^2} \)-maximal, that is the number of points of \( V \) defined over \( \mathbb{F}_{p^2} \) attains the Hasse-Weil upper bound \( p^2 + 1 + 2gp = p^2 + 1 + 8p \). We also show that the smallest such primes are 29, 59, 149, 239, 839. Our result gives a new contribution to the study of \( \mathbb{F}_{p^2} \)-maximal curves of small genera, initiated by Serre in 1985 and continued until nowadays; see [3, 17, 18, 32]. For \( m = p - 1 \), \( V \) is never \( \mathbb{F}_{p^2} \)-maximal instead. In fact, the number of points of \( V \) does not increase passing from \( \mathbb{F}_p \) to \( \mathbb{F}_{p^2} \) so that \( V \) has as many as \( (p - 2)! \) points defined over \( \mathbb{F}_{p^2} \) whereas its genus is equal to \( \frac{1}{2}(((p - 3)(p - 4) - 4)(p - 3)) + 1 \); see Lemmas 4.2, 4.4 and Theorem 8.5. A more general question for \( m = p - 1 \) is to determine the length of the set \( V(\mathbb{F}_p) \) consisting of all points of \( V \) in \( \text{PG}(p - 2, \mathbb{F}_p) \). For \( i = 1 \), Lemma 5.2 shows \( V(\mathbb{F}_p) = (p - 2)! \). Unfortunately, the elementary argument used in the proof of Lemma 5.2 seems far away from being sufficient to tackle
the general case. Even in the second particular case \( i = 2 \), settled in Theorem 4.3, the proof relies on the Stöhr-Voloch bound and on the structure of the \( G \)-orbits on the points of \( V \) determined in Section 5. On the other hand, Theorem 5.5 yields \( |V(\mathbb{F}_{p^d})| > |V(\mathbb{F}_p)| \) where \( d \) stands for the smallest integer such that \((p - 2) | (p^d - 1)\). The proof uses methods from Galois theory. It remains unsolved the problem whether \( |V(\mathbb{F}_{p^d})| > |V(\mathbb{F}_p)| \) holds for some intermediate value \( i \).

An important question on the geometry of curves is to compute the possible intersection multiplicities \( I(P, V \cap \Pi) \) between \( V \) and hyperplanes \( \Pi \) through a point \( P \) generally chosen in \( V \), also called orders. In the classical case (zero characteristic), the orders are precisely the non negative integers smaller than the dimension of the space where the curve is embedded, but this may fail in positive characteristic. If this occurs, then the curve is called non-classical. For plane curves, non-classicality means that all non-singular points of the curve are flexes. In our case, Lemma 8.10 shows the existence of a hyperplane \( \pi \) such that \( I(P, V \cap \Pi) \) is at least \( p \). Since \( V \) is embedded in \( \text{PG}(p - 3, p) \), this implies that \( V \) is non-classical; see Theorem 8.11. In Section 8.3, the intersection multiplicities \( I(P, V \cap \Pi) \) for \( P \in V(\mathbb{F}_p) \) are investigated. By Proposition 8.14, such intersection multiplicities are \( 1, 2, 3 \). This, together with Lemma 8.10 yields that \( 1, 2, 3, p \) are orders of \( V \).

Another concept of non-classicality, due to Stöhr and Voloch [33], arose from their studies on the maximum number \( N_{p^d} = N_{p^d}(g, r, d) \) of points of an irreducible curve of a given genus \( g \), embedded in \( \text{PG}(r, \mathbb{F}_{p^d}) \) as a curve of degree \( d \) can have. The Stöhr-Voloch upper bound on \( N_{p^d} = N_{p^d}(g, r, d) \) is known to be a deep result; in particular it may be used to give a proof for the Hasse-Weil upper bound. Also, the Stöhr-Voloch bound shows that the curves with large \( N_{p^d} = N_{p^d}(g, r, d) \) have the property that the osculating hyperplane to the curve at a generically chosen point on it also passes through the Frobenius image of the point. A curve with this purely geometric property can only exist in positive characteristic, and if this occurs the curve is called Frobenius non-classical. Apart from the trivial case \( p^2 = 2 \), Frobenius non-classical curves are also non-classical. In Section 8.4, the intersection multiplicities \( I(P, V \cap \Pi) \) for \( P \in V(\mathbb{F}_p) \) are investigated. By Proposition 8.14, such intersection multiplicities are \( 1, 2, 3 \). This, together with Lemma 8.10 yields that \( 1, 2, 3, p \) are orders of \( V \).

Over a finite field, the number of solutions of a system of diagonal equations has been the subject of many papers where the authors mainly rely on character sums and the distributions of their values. In the present work related with the famous Minkowski conjecture, originally proven by Hajós in 1941. Rédei proved that Minkowski conjecture holds if the following claim is true: if an algebraic abelian group of order \( p^2 \) is factored as the product of two sets of length \( p \), both containing the identity element, then at least one of the factors is a subgroup; see [30]. Rédei and later on Wang, Panico and Szabolcs Szabó [38] showed this claim is true if each solution \( [\xi_1, \ldots, \xi_p] \) over \( \mathbb{F}_p \) of the system of diagonal equations

\[
\begin{align*}
X_1 + X_2 + \ldots + X_p &= 0; \\
X_1^2 + X_2^2 + \ldots + X_p^2 &= 0; \\
&\quad \mathrel{\ldots} \\
&\quad \mathrel{\ldots} \\
X_1^{(p-1)/2} + X_2^{(p-1)/2} + \ldots + X_p^{(p-1)/2} &= 0,
\end{align*}
\]

(2)

has either equal components or \( [\xi_1, \ldots, \xi_p] \) is a permutation of the elements of \( \mathbb{F}_p \). That such particular \( p \)-tuples are exactly the solutions over \( \mathbb{F}_p \) of system (2) was first shown by Rédei himself in [30]. The above quoted paper by Wang, Panico and Szabó also contains a proof. In Section 11.1 we give a geometric interpretation of their results in terms of the variety \( V \).

2. Basic definitions and notation

In this paper, \( p \geq 7 \) stands for a prime and \( K \) for an algebraically closed field of characteristic zero or \( p \). Also, we let \( m \geq 6 \), and assume \( m \leq p - 1 \) when \( K \) has characteristic \( p \). For a projective, geometrically
irreducible, non-singular curve $\mathcal{X}$, the automorphism group of $\mathcal{X}$ fixing $\mathbb{K}$ element-wise is denoted by $\text{Aut}(\mathcal{X})$. If $\mathcal{X}$ has genus $g \geq 2$ then $\text{Aut}(\mathcal{X})$ is finite and Henn’s classification theorem states that $|\text{Aut}(\mathcal{X})| < 8g^3$ with exactly two exceptions, namely the Hermitian curve and the Roquette curve. In the exceptional cases, no subgroup of $\text{Aut}(\mathcal{X})$ is isomorphic to $\text{Alt}_m$; see [16, Theorem 11.127].

2.1. Action of $\text{Sym}_m$ as a projectivity group of $\text{PG}(m-2, \mathbb{K})$. Henceforth, $\mathbf{V}_m$ denotes the $m$-dimensional $\mathbb{K}$-vector space with basis $\{X_1, X_2, \ldots, X_m\}$, and $\text{PG}(m-1, \mathbb{K})$ the $(m-1)$-dimensional projective space over $\mathbb{K}$ arising from $\mathbf{V}_m$.

The group $G = \text{Sym}_m$, viewed as the symmetric group on $\{X_1, \ldots, X_m\}$, has a natural faithful representation in $\mathbf{V}_m$, where $g \in G$ takes the vector $v = \sum_{i=1}^{m} \lambda_i X_i$ to the vector $v' = \sum_{i=1}^{m} \lambda_i g(X_i)$. With $v' = g(v)$, $g$ becomes a linear transformation of $\mathbf{V}_m$ and $G$ is viewed as a subgroup of $\text{GL}(m, \mathbb{K})$. Since no non-trivial element of $G$ preserves each 1-dimensional subspace of $\mathbf{V}_m$, $G$ acts faithfully on $\text{PG}(m-1, \mathbb{K})$ and $G$ can also be regarded as a subgroup of the projective linear group $\text{PGL}(m, \mathbb{K})$ of $\text{PG}(m-1, \mathbb{K})$. For $1 \leq i < j \leq m$, the transposition $\sigma = (X_i X_j)$, as a linear transformation of $\mathbf{V}_m$, is associated with the $(0,1)$-matrix $(g_{i,j})_{i,j}$ whose 1 entries are $g_{i,j}$, $l = n$ and $g_{i,j}, g_{j,i}$. As a projectivity of $\text{PG}(m-1, \mathbb{K})$, $\sigma$ is the involutory homology whose center is the point $C = (0 : \cdot \cdot \cdot : 1 : \cdot \cdot \cdot : -1 : \cdot \cdot \cdot : 0)$, where 1 and $-1$ are in $i$-th and $j$-th positions, respectively, and whose axis is the hyperplane $\Pi$ of equation $X_i = X_j$.

Therefore, the fixed points of $\sigma$ are those of $\Pi$ and $C$, whereas the fixed hyperplanes of $\sigma$ are those through $C$ and $\Pi$. Since any two transpositions with no common fixed point commute, the center of either lies on the axis of the other. The $m$-cycle $\sigma = (X_m X_{m-1} \ldots X_1)$, as a linear transformation of $\mathbf{V}_m$, is associated with the $(0,1)$-matrix $(g_{i,n})_{i,n}$ whose 1 entries are $g_{i,n}$ for $l = 1, \ldots, m-1$ and $g_{m,1}$. As a projectivity, $\sigma$ fixes the point $P_\omega = (\omega : \omega^2 : \cdot \cdot \cdot : \omega^m = 1)$, where $\omega$ is any element whose order divides $m$. Similarly, the $(m-1)$-cycle $\sigma = (X_{m-1} X_{m-2} \ldots X_1)$, as a linear transformation of $\mathbf{V}_m$, is associated with the $(0,1)$-matrix $(g_{l,n})_{l,n}$ whose 1 entries are $g_{l,n}$ for $l = 1, \ldots, m-2$ and $g_{m-1,1}, g_{m,m}$. As a projectivity, $\sigma$ fixes the point $P_\varepsilon = (\varepsilon : \varepsilon^2 : \cdot \cdot \cdot : \varepsilon^{m-1} = 1 : 0)$ for any element $\varepsilon$ of $\mathbb{K}$ whose order divides $m-1$.

2.2. Projections. We also recall how the projection from a linear subspace $\Sigma$ of dimension $d$ to a disjoint linear subspace $\Sigma'$ is performed.

If $\mathcal{C}$ is an irreducible, non-singular algebraic curve embedded in $\text{PG}(m-1, \mathbb{K})$, which is disjoint from $\Sigma$, then the projection determines a regular mapping $\pi : \mathcal{C} \to \text{PG}(m-2, \mathbb{K})$. The geometric interpretation of $\pi$ is straightforward. Take any $(m-2-d)$-dimensional subspace $\Sigma'$ of $\text{PG}(m-1, \mathbb{K})$ disjoint from $\Sigma$. Then through any point of $P \in \mathcal{C}$ there is a unique $(d+1)$-dimensional subspace $\Lambda_P$ containing $\Sigma$ and this subspace meets $\Sigma'$ in a unique point, the image $\pi(P)$ of $P$ projected from $\Sigma$. Moreover, $\mathcal{C}$ is projected into an irreducible, possibly singular, curve $\mathcal{F}$ embedded in $\Sigma' \cong \text{PG}(m-2, \mathbb{K})$.

In the particular case where $\Sigma$ and $\Sigma'$ are the subspaces defined as the intersections of the hyperplanes of equations $X_{d+2}, \ldots, X_m = 0$ and $X_1, \ldots, X_{d+1} = 0$, respectively, then the projection from the vertex $\Sigma$ to $\Sigma'$ maps a point $P = (x_1 : \ldots : x_m) \in \text{PG}(m-1, \mathbb{K}) \setminus \Sigma$ to the point $P' = (0 : \ldots : 0 : x_{d+2} : \ldots : x_m)$. Let $H$ be the subgroup of $\text{PGL}(m-1, \mathbb{K})$ which preserves $\mathcal{C}$ and fixes each $d+1$-dimensional subspace through $\Sigma$. The points of the quotient curve $\tilde{\mathcal{C}} = \mathcal{C}/H$ can be viewed as $H$-orbits of the points of $\mathcal{C}$. Therefore every point $\tilde{P} \in \tilde{\mathcal{C}}$ is identified by a unique $H$-orbit, say $\overline{H_P}$. Moreover, such an $H$-orbit $\overline{H_P}$ is contained in a unique $(d+1)$-dimensional subspace through $\Sigma$, which also meets $\mathcal{C}$ in a unique point. Therefore, the notation $\Lambda_P$ for that subspace passing through the point $P \in \mathcal{C}$ is meaningful. Thus the sequence $\overline{P} = \overline{H_P} \rightarrow \Lambda_P \rightarrow \pi(P)$ is well defined. Actually it is a surjective homomorphism from $\tilde{\mathcal{C}}$ to $\mathcal{F}$. It is bijective if and only if $|H| = |\Lambda_P \cap \mathcal{C}|$ for all but finitely many points $P \in \mathcal{C}$. In this case $\Sigma$ is called a $d$-dimensional outer Galois subspace, and for $d = 0$ an outer Galois-point; see [21]. If $N$ is a subgroup of the normalizer of $H$ in the $\mathbb{K}$-automorphism group of $\mathcal{C}$ then the quotient group $N/H$ is a subgroup of the $\mathbb{K}$-automorphism group of $\tilde{\mathcal{C}}$. The genera $g(\mathcal{C})$ and $g(\tilde{\mathcal{C}})$ of the curves $\mathcal{C}$ and $\tilde{\mathcal{C}}$ are linked by the Hurwitz genus formula. In particular, if $H$ is tame, then $g(\mathcal{C}) = g(\tilde{\mathcal{C}})$.
prime to the order \( \ell = |H| \) of \( H \), then

\[
2g(\mathcal{C}) - 2 = |H|\left(2g(\mathcal{C}) - 2\right) + \sum_{i=1}^{m}(\ell - \ell_i),
\]

where \( \ell_1, \ldots, \ell_r \) denote the lengths of the short-orbits of \( H \) on \( \mathcal{C} \).

The equations in (1) define a (possibly reducible and singular) projective variety \( V \) of \( PG(m - 1, \mathbb{K}) \) so that the points of \( V \) are the nontrivial solutions of (1) up to a non-zero scalar. Actually, \( V \) is contained in the hyperplane of \( PG(m - 1, \mathbb{K}) \) of equation \( X_1 + X_2 + \ldots X_m = 0 \). Therefore, \( V \) is a projective variety embedded in \( PG(m - 2, \mathbb{K}) \). Moreover, \( G = Sym_m \) preserves \( V \) and no nontrivial element of \( G \) fixes \( V \) pointwise. Therefore, \( G \) is a subgroup of the \( \mathbb{K} \)-automorphism group of \( V \).

2.3. Bézout’s theorem. The higher dimensional generalization of Bézout’s theorem about the number of common points of \( m - 1 \) hypersurfaces \( \mathcal{H}_1, \ldots, \mathcal{H}_{m-1} \) of \( PG(m - 1, \mathbb{F}_q) \) states that either that number is infinite or does not exceed the product \( \deg(\mathcal{H}_1) \cdots \deg(\mathcal{H}_{m-1}) \). For a discussion on Bézout’s theorem and its generalization; see [35].

2.4. Background on algebraic curves. We report some background from [16 Chapter 7]; see also [33]. Let \( \Gamma \) be a projective, absolutely irreducible, not necessarily non-singular curve, embedded in a projective space \( PG(r, \mathbb{K}) \). For a non-singular model \( \mathcal{X} \) of \( \Gamma \), let \( \mathbb{K}(\mathcal{X}) = \mathbb{K}(\Gamma) \) denote the function field of \( \mathcal{X} \). There exists a bijection between the points of \( \mathcal{X} \), and the places of \( \mathbb{K}(\mathcal{X}) \) and the branches of \( \Gamma \). For any point \( P \in \mathcal{X} \) (more precisely, for any branch of \( \Gamma \) centered at \( P \)) the different intersection multiplicities of hyperplanes with the curve at \( P \) are considered. There is only a finite number of these intersection multiplicities, the number being equal to \( r + 1 \). There is a unique hyperplane, called osculating hyperplane, with the maximum intersection multiplicity. The hyperplanes cut out on \( \Gamma \) a simple, fixed point free, not-necessarily complete linear series \( \Sigma \) of dimension \( r \) and degree \( n \), where \( n \) is the degree of the curve \( \Gamma \). An integer \( j \) is a \((\Sigma, P)\)-order if there is a hyperplane \( H \) such that \( I(P, H \cap \Gamma) = j \). Notice that, if \( P \) is a singular point, then \( P \) is intended as a branch of \( \Gamma \) centered at \( P \). In the case that \( \Sigma \) is the canonical series, it follows from the Riemann–Roch theorem that \( j \) is a \((\Sigma, P)\)-order if and only if \( j + 1 \) is a Weierstrass gap. For any non-negative integer \( i \), consider the set of all hyperplanes \( H \) of \( PG(r, \mathbb{K}) \) for which the intersection number is at least \( i \). Such hyperplanes correspond to the points of a subspace \( \Pi_i \) in the dual space of \( PG(r, \mathbb{K}) \). Then we have the decreasing chain

\[
PG(r, \mathbb{K}) = \Pi_0 \supset \Pi_1 \supset \Pi_2 \supset \cdots
\]

An integer \( j \) is a \((\Sigma, P)\)-order if and only if \( \Pi_j \) is not equal to the subsequent space in the chain. In this case \( \Pi_{j+1} \) has codimension 1 in \( \Pi_j \). Since \( \deg(\Sigma) = n \), we have that \( \Pi_i \) is empty as soon as \( i > n \).

The number of \( (\Sigma, P) \)-orders is exactly \( r + 1 \); they are \( j_0(P), j_1(P), \ldots, j_r(P) \) in increasing order, and \( (j_0(P), j_1(P), \ldots, j_r(P)) \) is the order-sequence of \( \Gamma \) at \( P \).

Here \( j_0(P) = 0 \), and \( j_1(P) = 1 \) if and only if the branch \( P \) is linear (in particular when \( P \) is a non-singular point).

Consider the intersection \( \Pi_\ell \) of hyperplanes \( H \) of \( PG(r, \mathbb{K}) \), for which

\[
I(P, H \cap \gamma) \geq j_{\ell+1}.
\]

Then the flag \( \Pi_0 \subset \Pi_1 \subset \cdots \subset \Pi_{r-1} \subset PG(r, \mathbb{K}) \) can be viewed as the algebraic analogue of the Frenet frame in differential geometry. Notice that \( \Pi_0 \) is just \( P \), the centre of the branch \( \gamma \), and \( \Pi_1 \) is the tangent line to the branch \( \gamma \) at \( P \). Furthermore, \( \Pi_{r-1} \) is the osculating hyperplane at \( P \).

The order-sequence is the same for all but finitely many points of \( \Gamma \), each such exceptional point is called a \( \Sigma \)-Weierstrass point of \( \Gamma \). The order-sequence at a generally chosen point of \( \Gamma \) is the order sequence of \( \Gamma \) and denoted by \((\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r)\). Here \( j_i(P) \) is at least \( \varepsilon_i \) for \( 0 \leq i \leq r \) at any point of \( \Gamma \).

Now let \( \Gamma \) be defined over \( \mathbb{F}_q \) and viewed as a curve over the algebraic closure \( \mathbb{K} = \overline{\mathbb{F}}_q \). Stöhr and Voloch [33] (see also [16 Chapter 8]) introduced a divisor with support containing all points of \( P \in \Gamma \) for which...
the osculating hyperplane contains the Frobenius image \( \Phi(P) \) of \( P \). Since every \( \mathbb{F}_r \)-rational point has this property, an upper bound on the number of \( \mathbb{F}_r \)-rational points is obtained, unless all (but finitely many) osculating hyperplanes have that property. In such an exceptional case, the curve is called Frobenius non-classical. Curves with many rational points are often Frobenius non classical (and in particular, non-classical for \( q \neq 2 \)). Actually, Stöhr and Voloch were able to give a bound on the number of \( \mathbb{F}_r \)-rational points for any (Frobenius classical, or non-classical) curve \( \Gamma \). There exists a sequence of increasing non-negative integers \( \nu_0, \ldots, \nu_{r-1} \) with \( \nu_0 \geq 0 \) such that \( \det(W^{\nu_0, \ldots, \nu_{r-1}}(x_0, \ldots, x_r)) \neq 0 \). In fact, if the \( \nu_i \) are chosen minimally in lexicographical order, then there exists an integer \( I \) with \( 0 < I \leq r \) such that

\[
\nu_i = \begin{cases} 
\varepsilon_i & \text{for } i < I, \\
\varepsilon_{i+1} & \text{for } i \geq I. 
\end{cases}
\]

The Stöhr-Voloch divisor of \( \Gamma \) is

\[
S = \text{div}(W^{\nu_0, \ldots, \nu_{r-1}}(x_0, \ldots, x_r)) + (\nu_1 + \cdots + \nu_{r-1}) \text{div}(d\zeta) + (q + r)E,
\]

where \( E \) and \( e_P \) are defined as before for the ramification divisor. The sequence \( (\nu_0, \nu_1, \ldots, \nu_{r-1}) \) is the Frobenius order-sequence, and \( \Gamma \) is Frobenius-classical if \( \nu_i = i \) for \( 0 \leq i \leq r \). Also, \( \deg S = (\nu_1 + \cdots + \nu_{r-1})(2q - 2) + (q + r)n \), where \( n = \deg(\Gamma) \). From this the Stöhr-Voloch bound follows:

\[
|\Gamma(\mathbb{F}_r)| \leq \frac{1}{r}(\nu_1 + \cdots + \nu_{r-1})(2q - 2) + (\ell + r)n,
\]

which is a deep result on the number of \( \mathbb{F}_r \)-rational points of \( \mathbb{F}_r \)-rational curves. For instance, the Hasse-Weil upper bound was re-proven in \([33]\); see also \([16, \text{Chapter 9}]\).

2.5. Preliminary results from projective geometry and linear groups in positive characteristic.

In the \( r \)-dimensional projective space \( PG(r, \mathbb{K}) \) with \( r \geq 3 \) and defined over \( \mathbb{K} \), a (non-trivial) projectivity \( u \in PG(r, \mathbb{K}) \) is a perspectivity if \( u \) fixes all points of a hyperplane called the axis, and preserve all lines through a point, called the center. From now on in this subsection, we assume \( \mathbb{K} \) to be of positive characteristic \( p \geq 7 \). Then, \( u \) is either an elation or an homology according as the axis contains the center or does not. Since \( p \neq 2 \), no elation preserves a non-singular quadric of \( PG(r, \mathbb{K}) \).

Let \( \mathbb{F}_q \) be a finite subfield of \( \mathbb{K} \) of order \( q \). We recall some basic facts about projective orthogonal groups over \( \mathbb{F}_q \). If \( r \) is even then there is up to conjugacy in \( PGL(r, \mathbb{F}_q) \) just one projective orthogonal group \( P\Omega^+_1(q) \) whereas for \( r \) odd there are two, \( P\Omega^+(r, 1, q) \) and \( P\Omega^-(r, 1, q) \).

A projective orthogonal group has exactly two classes of conjugate involutory homologies, each of them generates an index 2 subgroup \( U \) containing no elations. Furthermore,

\[
|U| = \begin{cases} 
\frac{1}{2}q^{n^2}(q^2 - 1)(q^4 - 1) \cdots (q^{2n} - 1) & \text{for } r = 2n, \\
\frac{1}{2}q^{n(n-1)}(q^2 - 1)(q^4 - 1) \cdots (q^{2n} - 2)(q^n - 1) & \text{for } r = 2n - 1 \text{ and } U < P\Omega^+(r, 1, q), \\
\frac{1}{2}q^{n(n-1)}(q^2 - 1)(q^4 - 1) \cdots (q^{2n} - 2)(q^n + 1) & \text{for } r = 2n - 1 \text{ and } U < P\Omega^-(r, 1, q). 
\end{cases}
\]

The following result is a consequence of the classification theorem of Zalesskii and Serežkin \([41]\); see also \([39]\).

Result 2.1. Let \( N \leq PGL(r, 1, \mathbb{K}) \) be a finite irreducible subgroup of the projective orthogonal group \( P\Omega(r, 1, \mathbb{K}) \) for \( r \) even, and of \( P\Omega^+(r, 1, \mathbb{K}) \) or \( P\Omega^-(r, 1, \mathbb{K}) \) for \( r \) odd. Assume that \( N \) is generated by a conjugacy class of involutory homologies. If \( r \geq 8, p > r \) and \( p \) divides \( |N| \) then \( N \) is conjugate in \( PGL(r, 1, \mathbb{K}) \) either to a projective orthogonal group over a finite subfield of \( \mathbb{K} \), or to one of its two subgroups \( U \) generated by a class of conjugate involutory homologies, unless \( N \cong \text{Sym}_{r+1} \) or \( N \cong \text{Sym}_p \) with \( p = r + 3 \).

As a corollary, we have the following result.
Result 2.2. Let \( N \leq PGL(m - 1, \mathbb{K}) \) be a finite irreducible subgroup of the projective orthogonal group \( P\Omega(m - 1, \mathbb{K}) \) for \( m \) odd, and of \( P\Omega^+(m - 1, \mathbb{K}) \) or \( P\Omega^-(m - 1, \mathbb{K}) \) for \( m \) even. Assume that \( N \) is generated by involutory homologies. If \( m \geq 8, p \geq m + 1 \) and \( p \) divides \( |N| \) then either
\[
|N| > 8\left(\frac{1}{2}(m - 2)(m - 3) - 4(m - 2)! + 2\right)^3,
\]
or \( p = m + 1 \) and \( N \) is isomorphic to \( \text{Sym}_p \).

We also report the following classification theorem from Guralnick; see [19].

Result 2.3. Let \( \Gamma \) be an almost simple transitive permutation group of prime degree \( p \). Then, up to an isomorphism, \( T \leq \Gamma \leq \text{Aut}(T) \) for some non-abelian simple group \( T \) where \( T \) is isomorphic to one of the following groups:

(i) \( \text{Alt}_n \);
(ii) \( \text{PSL}(r, d^n) \) with \( p = (d^r - 1)/(d - 1) \), \( r \) prime, and \( \text{PSL}(r, d) \leq \Gamma \leq \text{PGL}(r, d) \);
(iii) \( \text{PSL}(2, 11) \) for \( p = 11 \);
(iv) \( M_{11} \) for \( p = 11 \), or \( M_{23} \) for \( p = 23 \).

Result 2.4. For an odd prime power \( d \), let \( H \) be a cyclic subgroup of \( \text{PGL}(r, d) \) fixing a point \( P \). Then \( H \) is not sharply transitive on the remaining \( d^{-1} + \ldots + d \) points of \( \text{PG}(r, d) \).

Proof. Look at the set \( \mathcal{L} \) consisting of all lines through \( P \). The subgroup \( H \) is a collineation group of \( \text{PG}(r, d^n) \) and induces on \( \mathcal{L} \) a transitive permutation group. The point \( P \) is the center of each non-trivial collineation in the kernel \( K \) of the permutation representation of \( H \) on \( \mathcal{L} \). Thus, \( \bar{H} = H/K \) is a collineation group of the quotient projective space \( \text{PG}(r - 1, d) \) of \( \text{PG}(r, d) \) with respect to \( \mathcal{L} \). Clearly, \( \bar{H} \) acts transitively on the set of all points of \( \text{PG}(r - 1, d) \). Since \( H \) is cyclic, this action is regular. Hence, \( |H| \) is equal to the number of points of \( \text{PG}(r - 1, d) \). From \( d^{r - 1} + \ldots + d = |H| = |ar{H}| = (d^{r - 2} + \ldots + d + 1)||K| \) whence \( |K| = d \). Since \( d \) is a power of the characteristic of the coordinatizing field of \( \text{PG}(r, d) \), and \( K \) has order \( d \), it turns out that \( K \) is an elation group. Let \( \pi \) be the axis of \( K \). Since \( K \) centralizes \( H \), it turns out that \( \pi \) is preserved \( H \). But then \( H \) is not transitive on the set of points of \( \text{PG}(r, d) \) different from \( P \). \( \square \)

2.6. Power sums and elementary symmetric polynomials. In \( \mathbb{K}[X_1, \ldots, X_m] \), let
\[
p_k(X_1, \ldots, X_m) = \sum_{i=1}^{m} X_i^k, \quad k \geq 1
\]
and let \( \sigma_k(X_1, \ldots, X_n) \) be the \( k \)-th elementary symmetric polynomial for \( k \geq 0 \). The Newton identities are
\[
k\sigma_k(X_1, \ldots, X_m) = \sum_{i=1}^{k} (-1)^{i-1}\sigma_{k-i}(X_1, \ldots, X_m)p_i(X_1, \ldots, X_m), \quad m \geq k \geq 1.
\]
whence
\[
p_k(X_1, \ldots, X_m) = (-1)^{k-1}k\sigma_k(X_1, \ldots, X_m) + \sum_{i=1}^{k-1}(-1)^{k-1+i}\sigma_{k-i}(X_1, \ldots, X_m)p_i(X_1, \ldots, X_n), \quad 1 \leq k \leq m.
\]

Therefore, (4) is equivalent to system
\[
\sigma_1(X_1, \ldots, X_m) = \sigma_2(X_1, \ldots, X_m) = \cdots = \sigma_{m-2}(X_1, \ldots, X_m) = 0.
\]

3. Some particular solutions of system (1) of diagonal equations

Lemma 3.1. Let \( \varepsilon \in \mathbb{K} \) be a \((m - 1)\)-th primitive root of unity. Then \( (\varepsilon, \varepsilon^2, \ldots, \varepsilon^{m-1} = 1, 0) \) is a solution of system (1).
Lemma 3.3. System (1) has no nontrivial solution $(x_1, x_2, \ldots, x_{m-1}, x_m)$ for $x_{m-1} = x_m = 0$.

Proof. For a solution $x = (x_1, x_2, \ldots, x_{m-1}, x_m)$ of system (1), let $y_j$ be the pairwise distinct non-zero coordinates of $x$. For $1 \leq j \leq k$, the multiplicity of $y_j$ is defined to be the number $n_j$ of the coordinates of $x$ which are equal to $y_j$. Since $x_{m-1} = x_m = 0$ we have $k \leq m - 2$. The first $k$ equations of (1) read

$$\begin{cases}
n_1 y_1 + n_2 y_2 + \ldots + n_k y_k = 0; \\
n_1 y_1^2 + n_2 y_2^2 + \ldots + n_k y_k^2 = 0; \\
\quad \vdots \\
n_1 y_1^k + n_2 y_2^k + \ldots + n_k y_k^k = 0.
\end{cases}$$

Then $(y_1, y_2, \ldots, y_k)$ is a nontrivial solution of the linear system

$$\begin{cases}
n_1 X_1 + n_2 X_2 + \ldots + n_k X_k = 0; \\
n_1 y_1 X_1 + n_2 y_2 X_2 + \ldots + n_k y_k X_k = 0; \\
\quad \vdots \\
n_1 y_1^{k-1} X_1 + n_2 y_2^{k-1} X_2 + \ldots + n_k y_k^{k-1} X_k = 0.
\end{cases}$$

whose determinant is equal to the product of $\prod_{i=1}^{k} n_i$ by the $k \times k$ Vandermonde determinant $\Delta = \prod_{1 \leq i < j \leq k} (y_i - y_j)$. Since either $p = 0$ or, if $p > 0$ then $n_i < p$ holds, it turns out that $\Delta = 0$ and hence $y_i = y_j$ for some $i \neq j$. But this contradicts the definition of $y_1, \ldots, y_k$. \hfill $\square$

Lemma 3.4. No nontrivial solution $(x_1, x_2, \ldots, x_{m-1}, x_m)$ of system (1) has either

(i) four coordinates $x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}$ such that $x_{i_1} = x_{i_2}$ and $x_{i_3} = x_{i_4}$ with pairwise distinct indices $i_1, i_2, i_3, i_4$, or

(ii) three coordinates $x_{i_1}, x_{i_2}, x_{i_3}$ such that $x_{i_1} = x_{i_2} = x_{i_3}$ with pairwise distinct indices $i_1, i_2, i_3$, or

(iii) three coordinates $x_{i_1}, x_{i_2}, x_{i_3}$ such that $x_{i_1} = x_{i_2}$ and $x_{i_3} = 0$ with two distinct indices $i_1, i_2$.

Proof. We use the argument in the proof of Lemma 3.3. For a non-trivial solution $x = (x_1, x_2, \ldots, x_{m-1}, x_m)$ of system (1), let $y_1, \ldots, y_k$ be the pairwise distinct non-zero coordinates of $x$ with multiplicities $n_j$ for $j = 1, \ldots, k$. If $x$ is a counterexample to Lemma 3.4 then $k \leq m - 2$. But the proof of Lemma 3.3 shows that this is actually impossible. \hfill $\square$

Lemma 3.5. Up to a non-zero scalar, system (1) has finitely many solutions $(x_1, x_2, \ldots, x_{m-1}, x_{m-1}, 0)$.

Proof. We again use the idea from the proof of Lemma 3.3. For a non-trivial solution $x = (x_1, x_2, \ldots, x_{m-1}, 0)$ of system (1), let $y_1, \ldots, y_k$ be the pairwise distinct non-zero coordinates of $x$ with multiplicities $n_j$ for $j = 1, \ldots, k$. Furthermore, one of them can be assumed to be equal to 1. Up to a relabelling of indices, $n_k$
Lemma 4.4.

\[
\begin{align*}
\xi_1 X_1 + \xi_2 X_2 + \cdots + \xi_{m-1} X_{m-1} &= -n;
\xi_1 y_1 + \xi_2 y_2 X_2 + \cdots + \xi_{m-1} y_{m-1} X_{m-1} &= -n;
\cdots \cdots \cdots \cdots \cdots
\xi_1 y_1^{k-2} X_1 + \xi_2 y_2^{k-2} X_2 + \cdots + \xi_{m-1} y_{m-1}^{k-2} X_{m-1} &= -n.
\end{align*}
\]

Assume on the contrary that system (8) has infinitely many solutions. Since \(n_k \neq 0\), the determinant of (8) vanishes. On the other hand, up to a non-zero constant, it is a Vandermonde determinant with parameters \((y_1, \ldots, y_{m-1})\). Therefore, \(y_i = y_j\) must occur for some \(i \neq j\) contradicting the definition of \(y_1, \ldots, y_k\). \(\square\)

4. The variety defined by system (11)

We keep upon with the notation introduced in Section 2. In particular, \(V\) stands for the projective algebraic variety of \(\text{PG}(m-1, \mathbb{K})\) defined by the equations of system (11).

Our goal is to prove that \(V\) is an irreducible non-singular curve. This requires some technical lemmas involving both the geometry of \(V\) and the transpositions of \(G\). We begin by stating and proving them.

Lemma 4.1. \(V\) has dimension 1.

Proof. From [28, Corollary 5] applied to \(r = m - 2\) and \(n = m - 1\), we have \(\dim(V) \geq 1\). On the other hand, we show that there exists a projective subspace of codimension 2 which is disjoint from \(V\). By [28, Corollary 4], this will yield \(\dim(V) \leq m - 1 - (m - 1 - 2) - 1 \leq 1\). Lemma 3.3 ensures that a good choice for such a subspace of codimension 2 is the intersection \(\Lambda\) of the hyperplanes of equation \(X_m = 0\) and \(X_{m-1} = 0\). \(\square\)

Lemma 4.2. \(V\) is non-singular.

Proof. The Jacobian matrix of \(V\) is

\[
\nabla(V) = \frac{\partial(f_1, \ldots, f_{m-2})}{\partial(X_1, \ldots, X_m)} = \begin{pmatrix}
\frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_m}
\frac{\partial f_2}{\partial X_1} & \cdots & \frac{\partial f_2}{\partial X_m}
\cdots & \cdots & \cdots
\frac{\partial f_{m-2}}{\partial X_1} & \cdots & \frac{\partial f_{m-2}}{\partial X_m}
\end{pmatrix}
\]

Up to the non-zero factor \((m-2)!\), the determinants of maximum order \(m-2\) are Vandermonde determinants. Therefore, for some point \(P = (x_1 : \ldots : x_m) \in V\), \(\nabla(V)\) evaluated at \(P\) has rank less than \(m-2\) if and only if \((x_1, \ldots, x_m)\) has one of the properties (i) and (ii). But Lemma 3.4 rules out these possibilities, and hence the point \(P\) is non-singular. \(\square\)

Lemma 4.3. \(\deg(V) = (m-2)!\).

Proof. Let \(\Pi\) be the hyperplane with equation \(X_{m-1} = X_m\). Since \(V\) has dimension 1, \(\Pi\) intersects \(V\) in at least one point \(P = (x_1 : x_2 : \cdots : x_{m-2} : x_{m-1} : x_m)\). By Lemma 3.3 \(x_{m-1} \neq 0\) and so \(P = (x_1/x_{m-1} : \cdots : x_{m-2}/x_{m-1} : 1 : 1)\). Also, from Lemma 3.4 \(x_1/x_{m-1}, \ldots, x_{m-2}/x_{m-1}\) are pairwise distinct. Since any permutation of \(x_1/x_{m-1}, \ldots, x_{m-2}/x_{m-1}\) gives rise to a new point of \(V\) on \(P\), we obtain \(|\Pi \cap V| = (m-2)!\) and hence \(\deg(V) \geq (m-2)!\). On other hand, the higher dimensional generalization of Bézout’s theorem yields \(\deg(V) \leq (m-2)!\) whence the claim follows. \(\square\)

Lemma 4.4. Let \(P = (\xi_1 : \xi_2 : \cdots : \xi_m)\) be a point of \(V\), and fix \(r \geq 2\) indices \(1 \leq j_1 < \cdots < j_r \leq m\). Let \(R = (x_1 : x_2 : \cdots : x_m)\) be a point of \(V\) such that \(x_{j_1} = \xi_{j_1}, \ldots, x_{j_r} = \xi_{j_r}\). Then there is a permutation \(\rho\) on \(\{1, \ldots, m\}\) with \(\rho(j_i) = j_i\) for \(i = 1, \ldots, r\) such that \(x_k = \xi_{\rho(k)}\) for \(k = 1, \ldots, m\).
Proof. If there is a pair \( \{i, \ell\} \) with \( i \neq \ell \) such that \( \xi_{\ell j} = \xi_{j \ell} \), let \( \Pi \) be the hyperplane of equation \( X_{\ell j} = X_{j \ell} \). Lemma 3.4 shows that the \( m - 2 \) coordinates of \( P \) other than \( \xi_{j \ell} \) and \( \xi_{\ell j} \) are pairwise distinct. Therefore the permutations on the coordinates other than \( X_{\ell j} \) and \( X_{j \ell} \) give rise as many as \( (m - 2)! \) pairwise distinct points of \( V \). By Lemma 4.3 these are all points in \( V \cap \Pi \). From this the claim follows. If no such pair \( \{i, \ell\} \) exists, take for \( \Pi \) the hyperplane of equation \( X_{j} = \xi_{j}X_{m} \). Then the above argument still works, and the claim holds true. \( \square \)

Lemma 4.5. For a \( m \)-th primitive root of unity \( \omega \), let \( P_{\omega} = (\omega : \omega^2 : \ldots : \omega^m = 1) \) be a point of \( V \). Then the stabilizer of \( P_{\omega} \) in \( G \) is a cyclic group of order \( m \), and it acts on \( \{X_1, \ldots, X_m\} \) as a \( m \)-cycle. Moreover if \( \mathcal{O}_{\omega} \) is the \( G \)-orbit of \( P_{\omega} \), then \( |\mathcal{O}_{\omega}| = (m - 1)! \), and if \( \Pi_{\omega} \) is the hyperplane \( X_{m-1} = \omega X_{m} \), then \( \Pi_{\omega} \cap \mathcal{O}_{\omega} = V \cap \Pi_{\omega} \).

Proof. Let \( u \in \text{PGL}(m - 1, \mathbb{K}) \) be given by the \((0,1)\)-matrix \( \{g_{i,j}\} \) whose 1 entries are \( g_{i,i+1} \) for \( i = 1, 2, \ldots, p - 2, \) and \( g_{m-1,1} \). Clearly, \( u \in G \) and \( P_{\omega} \) is fixed by \( u \). Also \( u \) has order \( m \) and acts on \( \{X_1, \ldots, X_m\} \) as a \( m \)-cycle. Therefore, \( |G_P| \geq m \). We show that equality holds. Let \( \sigma \) be permutation on \( \{1, 2, \ldots, m - 1\} \). If \( P_{\omega} = P_{\sigma} \), then \( \omega^i = \omega^{\sigma(i)} \) for any \( i \leq m - 1 \). Thus \( \sigma(i) - i \equiv 0 \pmod{m} \) whence \( \sigma(i) = i \) follows. Therefore \( |G_P| = m \). From this \( |\mathcal{O}_{\omega}| = |G|/|G_P| = (m - 1)! \) follows. Since \( \mathcal{O}_{\omega} \subseteq \Pi_{\omega} \) and \( |V \cap \Pi_{\omega}| \leq \deg(V) \) by Lemma 4.2, the last claim follows from Lemma 4.3. \( \square \)

Lemma 4.6. For a \((m - 1)\)-th primitive root of unity \( \varepsilon \), let \( P_\varepsilon = (\varepsilon : \varepsilon^2 : \ldots : \varepsilon^{m-1} = 1 : 0) \). Then the stabilizer of \( P_\varepsilon \) in \( G \) is a cyclic group of order \( m - 1 \) which acts on \( \{X_1, \ldots, X_{m-1}\} \) as a cycle.

Proof. Let \( h \in \text{PGL}(m - 1, \mathbb{K}) \) be given by the \((0,1)\)-matrix \( \{g_{i,j}\} \) whose 1 entries are \( g_{i,i+1} \) for \( i = 1, 2, \ldots, m - 2, \) and \( g_{m-1,1} \). Clearly \( h \) takes \( P_\varepsilon \) to the point \( Q = (\varepsilon^2 : \varepsilon^3 : \ldots : 1 : \varepsilon : 0) \). Actually, \( Q = P_\varepsilon \) as the coordinates of \( Q \) are proportional to those of \( P_\varepsilon \). It remains to show that any \( g \in G \) fixing \( P_\varepsilon \) is a power of \( h \). Let \( g : (X_1 : X_2 : \ldots : X_{m-1} : 0) \rightarrow (Y_1 : Y_2 : \ldots : Y_{m-1} : 0) \) where \( Y_1Y_2\cdots Y_{m-1} = 1 \). Since \( g \) fixes \( P_\varepsilon \), there exists \( (y_1 : y_2 : \ldots : y_{m-1}) \) with \( \pi(\varepsilon^i) = y_i \) for \( i = 1, \ldots, m - 1 \) such that \( (\varepsilon, \varepsilon^2, \ldots, \varepsilon^{m-1} = 1) \) and \( (y_1, y_2, \ldots, y_{m-1}) \) are proportional. Then \( y_{m-1} = \varepsilon^1 \) whence \( y_i = \varepsilon^i-j \). Thus \( \pi(\varepsilon^j) = \varepsilon^{i-j} \) whence \( Y_i = X_{i+(m-1-j)} \) where the indices are taken modulo \( m - 1 \). Hence \( g = h^{m-1-j} \) which proves the first claim. Since \( h \) fixes \( X_m \), \( G \) acts on \( \{X_1, \ldots, X_{m-1}\} \) as a cycle. \( \square \)

Lemma 4.7. Let \( \Pi_{\infty} \) be the hyperplane of equation \( X_m = 0 \). Then \( \Pi_{\infty} \) intersects \( V \) transversally at each of their \((m - 2)\) common points. Moreover, \( \mathcal{O}_\varepsilon = V \cap \Pi_{\infty} \) is the orbit of \( P_\varepsilon \) under the action of the stabilizer of \( \Pi_{\infty} \) in \( G \).

Proof. Since \( |G| = m! \), the subgroup of \( G \) preserving \( \Pi_{\infty} \) has order \( (m - 1)! \). Since \( P_\varepsilon \in \Pi_{\infty} \), Lemma 4.6 yields that \( \mathcal{O}_\varepsilon \) contains at least \((m - 1)!/(m - 1) = (m - 2)! \) pairwise distinct points of \( V \). On the other hand, \(|V \cap \Pi_{\infty}| \leq \deg(V) \) by Lemma 4.2. As \( \deg(V) = (m - 2)! \) by Lemma 4.3, the first claim follows. Since the stabilizer of \( \Pi_{\infty} \) in \( G \) has order \((m - 1)! \), the first claim together with Lemma 4.6 prove the second claim. \( \square \)

Lemma 4.8. Let \( g \in G \) be a nontrivial element fixing a point of \( V \). If \( g \) acts on \( V_m \) fixing \( X_1 \) and \( X_j \) then \( g \) is a transposition on \( \{X_1, X_2, \ldots, X_m\} \) and an involutory homology of \( \text{PG}(m - 2, \mathbb{K}) \). Furthermore, the fixed points of \( g \) in \( V \) are as many as \((m - 2)! \) and they are all the common points of \( V \) with the hyperplane of equation \( X_l = X_n \) where \( X_n = g(X_l) \), and \( l \neq n \).

Proof. Up to a change of the indices, \( g \) fixes \( X_m \) and \( X_{m-1} \). Let \( P = (x_1, \ldots, x_{m-1}, x_m) \in V \) be a fixed point of \( g \). From Lemma 5.3, \( x_m \) and \( x_m \) do not vanish simultaneously. Therefore, \( x_m = 1 \) may be assumed. Furthermore, if \( X_m(l) = g(X_l) \) then \( g(P) = P \) yields \( x_{g(l)} = cx_l \) for some \( c \in \mathbb{K} \) and \( l = 1, \ldots, m \). In particular, since \( g(X_m) = X_m \), we have \( x_m = cx_m \) whence \( c = 1 \). As \( g \) is nontrivial, the set \( M = \{l \mid l \neq g(l), 1 \leq l \leq m - 2\} \) is non empty. By \( c = 1, l \in M \) yields that \( x_{g(l)} = x_l \). By (i) and (ii) of Lemma
this implies \(|M| \leq 2\). Since also \(|M| \geq 2\) holds, the claim follows. To show the other claims, observe that the transposition \(g = (X_1 X_n)\) is the involutory homology of \(P\(m - 1, K\)\) associated with the \((0, 1)\) matrix \(\{g_{u,v}\}\) whose 1 entries are \(g_{u,v}\) for \(u \in \{1, 2, \ldots, m\}\backslash \{l, n\}\), \(g_{l,n}\) and \(g_{n,l}\). In particular, its axis is the hyperplane \(\Pi\) of equation \(X_l = X_n\), and its center is the point \(C = (0 : 0 : \cdots : -1 : \cdots : 0 : \cdots : 1 : \cdots : 0)\). Moreover, \(x_l = x_n\) as \(P\) is fixed by \(g\). From Lemma 3.3, \(x_l = x_n = 1\) may be assumed. This together with (i) of Lemma 3.4 yield that \(x_u \neq x_v\) for \(1 \leq u < v \leq m\) and \((u, v) \neq (i, j)\). Therefore, the images of \(P\) under the action of the stabilizer \(H\) of \(X_l\) and \(X_n\) in \(G\) are all pairwise distinct and their number is \(|H| = (m - 2)!\). Since \(H\) preserves both \(V\) and \(\Pi\), all the images of \(P\) are in \(V \cap \Pi\). Thus \(|V \cap \Pi| \geq (m - 2)!\). On the other hand, Lemma 4.3 shows \(|V \cap \Pi| \leq (m - 2)!\) whence the second part of the claim follows.

Lemma 4.9. \(V\) has a unique component of dimension 1.

Proof. From Lemma 4.1, the irreducible components of \(V\) have dimension at most 1, and at least one of them is an absolutely irreducible curve \(C\). Let \(P\) be a common point of \(C\) and \(\Pi\). By the second claim of Lemma 3.7, we can assume \(P = P_e\) for a \((m - 1)\)-th primitive root of unity \(\varepsilon\). Since \(P\) is a nonsingular point of \(V\), \(C\) is the unique irreducible component of \(V\) containing \(P\). The last claim in Lemma 3.7 ensures that this holds for each point in \(V \cap \Pi\). In particular, the 1-dimensional irreducible components of \(V\) are exactly the images of \(C\) under the action of \(G\). Clearly, these absolutely irreducible curves \(C = C_1, C_2, \ldots, C_l\) have the same degree \(k = \deg(C)\), and \(kl = \deg(V)\). The hyperplane \(\Pi\) of equation \(X_m = X_{m-1}\) meets \(C\) nontrivially, and let \(R \in C \cap \Pi\). Clearly the transposition \(g = (X_m X_{m-1})\) in \(G\) which fixes each \(X_i\) for \(1 \leq i \leq m - 2\) and interchanges \(X_m\) with \(X_{m-1}\) fixes \(R\). Furthermore, \(C\) contains a point \(S \in V\) lying on the hyperplane of equation \(\omega : X_{m-1} = \omega X_m\). By Lemma 1.3, \(S \in \mathcal{O}_m\) and some element \(u \in G_{S}\) acts on the basis \((X_1, X_2, \ldots, X_m)\) as a \(m\)-cycle. Since \(S\) is a nonsingular point, \(u\) preserves \(C\). Indeed, assume on the contrary that \(u\) takes \(C\) to \(C_i\), \(i \neq 1\). Then, since \(u\) fixes \(S\), \(S\) must be in the intersection \(C \cap C_i\), a contradiction with the non-singularity of \(S\). Therefore \(g\) and \(u\) are automorphisms of \(C\). By a well known result, the group generated by the transposition \(g\) and the \(m\)-cycle \(u\) is the whole symmetric group \(G = \text{Sym}_m\). This shows that \(G\) preserves \(C\) and hence \(l = 1\).

From now on, the irreducible non-singular curve \(C\) stands for the unique 1-dimensional component of \(V\). As \(G\) preserves \(C\) and \(G \leq \text{PGL}(m, K)\), \(G\) is a \(K\)-automorphism group of \(C\). Since every hyperplane meets \(C\), the final claim of Lemma 4.5 shows that some point of \(\mathcal{O}_m\) (and hence \(P_e\)) is in \(C\). Therefore, the \(G\)-orbit \(\mathcal{O}_m\) of \(P_e\) has length \(|G|/m = (m - 1)!\). Similarly, Lemmas 4.6 and 4.7 yield that \(P_e \in C\), and hence the \(G\)-orbit \(\mathcal{O}_m\) of \(P_e\) has length \(|G|/(m - 1) = m(m - 2)!\). A third short \(G\)-orbit \(\mathcal{O}_g\) arises from transpositions, as Lemma 4.8 shows that every transposition of \(G\) fixes a point of \(C\).

Lemma 4.10. The hyperplane of equation \(X_1 + X_2 + \cdots + X_m = 0\) is the unique hyperplane of \(\text{PG}(m - 1, K)\) which contains \(C\).

Proof. We have \(P_{e} \in C\). Since \(G\) preserves \(C\), this yields that \(Q = (\omega : 1 : \omega^2 : \cdots : \omega^{m-1})\) is in \(C\), as well. Assume that \(C\) is contained in a hyperplane \(\Pi\) of equation \(\alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_m X_m = 0\) with \(\alpha_i \in K\). Then \(\alpha_1 + \omega \alpha_2 + \omega^2 \alpha_3 + \cdots + \omega^{m-1} \alpha_m = 0\) and \(\omega \alpha_1 + \alpha_2 + \omega^2 \alpha_3 + \cdots + \omega^{m-1} \alpha_m = 0\) whence \(\alpha_1 = \alpha_2\) by subtraction. Similar argument shows that any two consecutive coefficient in the equation of \(\Pi\) are equal. This yields \(\alpha_1 = \alpha_2 = \cdots = \alpha_m\), that is \(\Pi\) has equation \(X_1 + X_2 + \cdots + X_m = 0\). On the other hand, as we have already pointed out in Section 2 the first equation in System (11) shows that hyperplane of equation \(X_1 + X_2 + \cdots + X_m = 0\) contains \(C\).

Lemma 4.11. Every transposition of \(G\) fixes exactly \((m - 2)!\) points of \(C\).

Proof. We have already pointed out in the proof of Lemma 4.3 that the transposition \(g = (X_{m-1} X_m)\) fixes a point \(R \in C \cap \Pi\) where \(\Pi\) is the hyperplane of equation \(X_m = X_{m-1}\). By Lemma 3.3 and 3.4, we can assume \(R = (x_1 : \cdots : x_{m-2} : 1 : 1)\) and that \(x_1, \ldots, x_{m-2}\) are pairwise distinct and non zero. Therefore any point whose first \(m - 2\) coordinates are a permutation on \(\{x_1, \ldots, x_{m-2}\}\) is also fixed by \(g\). Thus \(g\) has
at least \((m - 2)!\) fixed points. On the other hand, if \(P \in C\) is not on \(\Pi\) then the last two coordinates of \(P\) are different and hence \(P\) is not fixed by \(g\). Therefore, the claim holds for \(g\). Since the transpositions are pair-wise conjugate in \(G\), the claim holds true for every transposition in \(G\).

\[\square\]

**Lemma 4.12.** Let \(P\) be a point of \(C\) which is fixed by a transposition \(g \in G\). Then the tangent \(\ell\) to \(C\) at \(P\) is the line joining \(P\) with the center of \(g\).

**Proof.** W.l.o.g. we can assume \(g = (X_m - X_m)\). Then \(g\) is an homology with center \(C = (0 : 0 : \cdots : 0 : -1 : 1)\) and axis the (pointwise fixed) hyperplane \(\Pi\) of equation \(X_m = X_{m-1}\). Also, \(P = (x_1 : \cdots : x_{m-2} : 1 : 1)\). The tangent line \(\ell\) is the intersection of the tangent hyperplanes in \(P\) of the hypersurfaces of equation \(f_i = 0\) of system \((\Pi)\), \(i = 1, \ldots, m - 2\), and hence its equation is given by

\[
\begin{align*}
X_1 + X_2 + \ldots + X_{m-2} + X_{m-1} + X_m &= 0; \\
x_1X_1 + x_2X_2 + \ldots + x_{m-2}X_{m-2} + X_{m-1} + X_m &= 0; \\
\ldots \ldots \\
\ldots \ldots \\
x_1^{m-2}X_1 + x_2^{m-2}X_2 + \ldots + x_{m-2}^{m-2}X_{m-2} + X_{m-1} + X_m &= 0.
\end{align*}
\]

(9)

Since the coordinates of \(C\) satisfy system \((\Pi)\), the claim follows.

\[\square\]

**Lemma 4.13.** Let \(H\) be the stabilizer of \(X_i\) and \(X_j\) in \(G\). Then the quotient curve \(\tilde{C}\) of \(C\) with respect to \(H\) is rational.

**Proof.** Up to a reordering of the coordinates, we can assume \((i, j) = (m - 1, m)\). The hyperplanes \(\Pi_{\lambda, \mu}\) of equations \(\lambda X_{m-1} + \mu X_m = 0\) form the pencil through the intersection \(\Sigma\) of the hyperplanes \(X_{m-1} = 0\) and \(X_m = 0\). \(\Sigma\) is a subspace of \(\text{PG}(m, F)\) of codimension 2, and it is disjoint from \(C\) by Lemma 4.8. Furthermore, \(H\) preserves each \(\Pi_{\lambda, \mu}\). Take any point of \(P \in C\) whose stabilizer \(H_P\) in \(H\) is trivial. Then the \(H\)-orbit \(\Delta\) of \(P\) has length \((m - 2)!\) and \(\Delta\) is contained in the unique hyperplane \(\Pi_{\lambda, \mu}\) of the pencil which contains \(P\). Since \(\deg(C) = (m - 2)!\), \(\Delta\) coincides with the intersection of \(C\) with \(\Pi_{\lambda, \mu}\). If the stabilizer \(H_P\) of \(P \in C\) in \(H\) is nontrivial, from Lemma 4.8 and the proof of Lemma 4.11 then \(|H_P| = 2\) and the only nontrivial element in \(H_P\) is a transposition \(h\). Indeed if \(h'\) is a non-trivial element of \(H_P\), from Lemma 4.8 it is a transposition \((X_i X_j)\), and from the proof of Lemma 4.11 \(x_i = x_j\) and \(x_{m-1} = x_m\), which is a contradiction with Lemma 4.4. From Lemma 4.12 the tangent line \(\ell\) to \(C\) at \(P\) contains the center \(C\) of \(h\). The hyperplane \(\Pi\) of equation \(X_{m-1} - X_m = 0\) is the axis of the transposition \(g\) which interchanges \(X_m\) and \(X_{m-1}\). Since \(g\) and \(h\) commute, it follows that \(C \in \Pi\). Therefore, \(\ell\) is contained in \(\Pi\), and hence \(I(P, C \cap \Pi) \geq 2\), where \(I(P, C \cap \Pi)\) is the intersection multiplicity of \(C\) and \(\Pi\) at \(P\). From the higher dimensional generalization of Bézout’s theorem, \(|C \cap \Pi| \leq \frac{1}{2}(m - 2)!\). Thus, \(|C \cap \Pi| = \frac{1}{2}(m - 2)!\), and, again, \(\Delta\) coincides with \(C \cap \Pi\). This shows that \(\tilde{C}\) is isomorphic to the rational curve which is the projection of \(C\) from the vertex \(\Sigma\).

\[\square\]

**Lemma 4.14.** Let \(g\) be the genus of \(C\). Then

\[
2g - 2 = \frac{1}{2}((m - 2)(m - 3) - 4)(m - 2)!.
\]

**Proof.** Let \(H \cong \text{Sym}_{m-2}\) be the subgroup of \(G\) which fixes both \(X_m\) and \(X_{m-1}\). From Lemma 4.8 if \(h \in H\) has a fixed point in \(C\) then \(h\) is a transposition. If \(P\) is a fixed point of a transposition then, up to a reordering of the coordinates, \(P = (1, 1, x_3, \ldots, x_{m-1}, x_m)\). A point whose coordinates are a permutation of those of \(P\) is another fixed point of the transposition. Among these points, those which are contained in the hyperplane \(X_{m-1} = X_m\), fixed by \(H\), are as many as \((m - 2)!\), and no more, since \(\deg(C) = (m - 2)!\). Therefore, the number of short orbits of \(H\) is equal to the number of choices of two values among \(x_3, \ldots, x_m\). As these are \(m - 2\) such distinct values, the short orbits are as many as \((m - 2)(m - 3)\). The claim follows from the Riemann-Hurwitz formula.

\[\square\]

**Lemma 4.15.** \(V\) is irreducible, that is, \(V = C\).
Proof. Suppose on the contrary the existence of a point \( Q = (q_1 : \cdots : q_{m-1} : q_m) \) of \( V \) which is not in \( C \). Since \( (1 : 0 : 0 : \cdots : 0) \) is not a point of \( V \), both \( q_m = 1 \) and \( q_{m-1} = \lambda \neq 0 \) may be assumed. Then \( Q \) is contained in the hyperplane \( \Pi \) of equation \( X_{m-1} = \lambda X_m \). Choose a point \( P \in C \) lying on \( \Pi \). The stabilizer \( H \) of \( X_{m-1} \) and \( X_m \) in \( G \) preserves \( \Pi \). Since \( H \) also preserves \( C \), the \( H \)-orbit of \( P \) is contained in \( \Pi \). As \( P \in \Pi \), this together with Lemma 4.10 yield \( |\Delta| < |H| \), that is, \( H_P \) is nontrivial. As in the proof of Lemma 4.13, from Lemma 4.8 and Lemma 4.11 we obtain \( |H_P| = 2 \). Therefore, \( |\Delta| = \frac{1}{2}(m - 2)! \). Thus, the higher dimensional generalization of Bézout’s theorem yields that the length of the \( H \)-orbit of \( Q \) is also less than \( (m - 2)! \), that is, \( H_Q \) is non-trivial. This is a contradiction, since Lemma 4.8 together with Lemma 4.11 yields that all the fixed points of any transposition of \( G \) are on \( C \). \( \square \)

Lemmas 4.2 and 4.16 have the following corollary.

Theorem 4.16. \( V \) is an irreducible non-singular curve of \( \text{PG}(m-2, K) \).

5. The Action of \( G \) on \( V \)

As we have already pointed out, \( G \) has at least three short orbits on \( V \), named \( \Omega_\omega \), \( \Omega_\varepsilon \) and \( \Omega_\theta \). We prove that they are the only short \( G \)-orbits.

Lemma 5.1. The short \( G \)-orbits on \( V \) are exactly \( \Omega_\omega \), \( \Omega_\varepsilon \) and \( \Omega_\theta \), and they have lengths \((m-1)!, m(m-2)! \) and \( m!/2 \).

Proof. Since \( |\Omega_\omega| = (m-1)! \), \( |\Omega_\varepsilon| = m(m-2)! \) and \( \Omega_\theta \) are short \( G \)-orbits, and \( |\Omega_\theta| \leq \frac{1}{2} m! \), the Hurwitz genus formula \( (1) \) applied to the \( G \) yields

\[
2g - 2 \geq -2m! + (m! - (m-1)!) + (m! - m(m-2)!)) + (m! - \frac{1}{2} m!).
\]

Comparison with \( (10) \) shows that equality holds. Therefore, no further short \( G \)-orbits on \( V \) exist, and \( |\Omega_\theta| = \frac{1}{2} m! \), that is, the stabilizer of a point on \( V \) which is fixed by a transposition contains no more nontrivial element of \( G \). \( \square \)

Lemma 5.2. The short \( G \)-orbit \( \Omega_\omega \) consists of the common points of \( V \) and the hypersurface \( \Sigma_{m-1} \) of equation

\[
X_1^{m-1} + X_2^{m-1} + \ldots + X_m^{m-1} = 0.
\]

Proof. We observe first that no point of the \( G \)-orbit \( \Omega_\varepsilon \) is in \( \Sigma_{m-1} \). In fact, if \( P = (\xi_1 : \cdots : \xi_{m-1} : 0) \in \Omega_\varepsilon \) then \( \xi_j^{m-1} = 1 \) and hence \( \sum_{j=1}^{m-1} \xi_j^{m-1} = m - 1 \neq 0 \), thus \( P \notin \Sigma_{m-1} \). On the other hand, it is readily seen that \( P \in \Sigma_{m-1} \) for any \( P \in \Omega_\omega \). From the higher dimensional generalization of Bézout’s theorem, \(|V \cap \Sigma_{m-1}| \leq (m-1)! \). Furthermore, since \( G \) also preserves \( \Sigma_{m-1} \), the intersection \( V \cap \Sigma_{m-1} \) is \( G \)-invariant, as well. Therefore, Lemma 5.1 yields \( V \cap \Sigma_{m-1} = \Omega_\omega \). \( \square \)

A similar argument can be used to prove the following lemmas.

Lemma 5.3. The short \( G \)-orbit \( \Omega_\varepsilon \) consists of the common points of \( V \) and the hypersurface \( \Sigma_m \) of equation

\[
X_1^m + X_2^m + \ldots + X_m^m = 0.
\]

Lemma 5.4. The short \( G \)-orbit \( \Omega_\theta \) consists of the common points of \( V \) and the hypersurface \( \Sigma_{m(m-1)/2} \) of equation

\[
X_1^{m(m-1)/2} + X_2^{m(m-1)/2} + \ldots + X_m^{m(m-1)/2} = 0.
\]

Lemma 5.5. Let \( P_\omega \) be the point of \( V \) given in Lemma 4.5. Then the number of fixed points on \( V \) of the involution in the stabilizer of \( P_\omega \) in \( G \) is

\[
\frac{2^{m/2} (m/2)!}{m}.
\]
if \( m \) is even, and
\[
2^{(m-1)/2} \left( \frac{(m-1)/2)!}{m} \right),
\]
if \( m \) is odd.

Proof. We will perform the proof for \( m \) even. The same approach can be applied for \( m \) being odd. Let \( u \) be the (unique) involution in \( G \) which fixes \( P_\omega \). Then \( u \) acts on \((X_1, \ldots, X_m)\) as the involutory permutation \((X_1X_{(m+2)/2})(X_2X_{(m+4)/2}) \cdots (X_{m/2}X_m)\). Therefore, the centralizer \( C_G(u) \) of \( u \) in \( G \) has order \( 2^{m/2}(m/2)! \), and hence \( u \) has as many as
\[
k = \frac{m!}{2^{m/2}(m/2)!}
\]
conjugate in \( G \). We show that if \( v \) is conjugate of \( u \) in \( G \) and \( u \neq v \) then \( u \) and \( v \) has no common fixed point. Assume on the contrary the existence of a point \( Q \in V \) such that \( u(Q) = v(Q) \). Then \( u \) and \( v \) are two distinct involutions in the stabilizer \( G_\Omega \) of \( Q \) in \( G \). On the other hand, since either \( p = 0 \) or \( p > 0 \) and \( p \nmid |G| \), \( G_\Omega \) is cyclic, and hence it contains at most one involution; a contradiction. Therefore, each point in the \( G \)-orbit \( \Omega_\omega \) is the fixed point of exactly one involution which is conjugate to \( u \) in \( G \). If \( N_u \) counts the fixed points of \( u \) in \( \Omega_\omega \), this yields that \( |\Omega_\omega| = kN_u \). Therefore, the number of fixed points \( v \) in \( \Omega_\omega \) equals \( m! \). It remains to show that \( u \) has no further fixed points on \( V \). By Lemma 5.1, the stabilizer of any point \( Q \in \Omega_\omega \) in \( G \) has odd order and hence contains no involution. By Lemma 5.1, the 1-point stabilizer of the remaining short orbit has order 2 and its non-trivial element is a transposition. Since \( u \) is not a transposition, the claim follows.

Theorem 5.6. \( G \) is an irreducible group in \( PG(m-2, K) \).

Proof. Assume on the contrary that \( G \) preserves a projective subspace \( \Pi \) of \( PG(m-2, K) \). Any homology \( g \in G \) induces a projectivity \( \bar{g} \) of \( \Pi \) where \( \bar{g} \) is either the identity or a homology of \( \Pi \) and in the latter case \( g \) and \( \bar{g} \) have the same center. From Lemma 4.3, the transpositions in \( G \) are involutory homologies in \( G \), and hence such involutory homologies form a conjugacy class \( D \) in \( G \). Therefore, two cases occur, namely either each involutory homology in \( D \) fixes \( \Pi \) pointwise, or the center of each involutory homology lies in \( \Pi \). From the proof of Lemma 4.3, in the former case \( \Pi \) is contained in any hyperplane \( \Pi_{ij} \) of equation \( X_i = X_j \) with \( 1 \leq i < j \leq m \); but these hyperplanes have no common point, a contradiction; in the latter case, \( \Pi \) contains all points \( C_{ij} = (0 : 0 : \cdots : -1 : \cdots : 0 : \cdots : 1 : \cdots : 0) \) with \( 1 \leq i < j \leq m \), but these points generate \( PG(m-2, K) \), a contradiction.

These results on the action of \( G \) also allow to show that every solution of \( \{1\} \) satisfies further diagonal equations.

Proposition 5.7. Every solution of \( \{1\} \) also satisfies the following equations.
\[
\begin{align*}
X_1^{m+2} + X_2^{m+2} + \cdots + X_m^{m+2} &= 0, \\
X_1^{m+3} + X_2^{m+3} + \cdots + X_m^{m+3} &= 0, \\
& \quad \vdots \\
X_1^{2m-3} + X_2^{2m-3} + \cdots + X_m^{2m-3} &= 0.
\end{align*}
\]

Proof. Let \( P = (a_1, \ldots, a_m) \) be any point of \( V \). If \( P \in \Omega_\omega \) then \( a_i = a_i^{m+1} \) and hence \( a_i^{m+1+l} = a_i^{1+l} \) for any positive integer \( l \). Therefore, the claim holds for every \( P \in \Omega_\omega \).

Let \( \mathcal{H}_j \) be the (irreducible) hypersurface of equation \( X_1^{m+1+j} + X_2^{m+1+j} + \cdots + X_m^{m+1+j} = 0 \). Then \( \Omega_\omega \) is contained in \( \mathcal{H}_j \). We prove that \( \mathcal{H}_j \) contains \( V \) as far as \( j \leq m-4 \). Assume on the contrary that this
does not occur for some $j$. Then Lemma 4.3 together with Bézout’s theorem applied to the intersection of $\mathcal{H}_j$ with $V$ yield

$$\sum_{Q \in \mathcal{H} \cap V} I(Q, \mathcal{H} \cap V) = (m + 1 + j)(m - 2)!.$$  

(17)

We show that $\mathcal{H}_j$ contains some points of $V$ other than those in $\Omega_w$. As $G$ also preserves $\mathcal{H}_j$, the intersection number $I(Q, \mathcal{H}_j \cap V)$ is invariant when $Q$ ranges over an $G$-orbit. For a point $Q \in \Omega_w$, let $\lambda = I(P, \mathcal{H}_j \cap V)$. Then $\sum_{Q \in \Omega_w} I(Q, \mathcal{H}_j \cap V) = \lambda(m - 1)!$ whence $\lambda(m - 1) \leq m + 1 + j$. For $\lambda \geq 2$, this would yield $2(m - 1) \leq m + 1 + j$, that is, $j > m - 4$, a contradiction. Therefore $\lambda = 1$. Since $(m + 1 + j)(m - 2)! > (m - 1)!$, the claim follows.

Let $R$ be a point $R \in \mathcal{H} \cap V$ not in $\Omega_w$. From Lemma 5.1 the $G$-orbit of $R$ has length at least $m(m - 2)!$. Then $\mathcal{H}_j$ and $V$ have at least $((m - 1) + m)(m - 2)! = (2m - 1)(m - 2)!$ common points. Since $j \leq m - 3$ implies $2m - 1 > m + 1 + j$, this contradicts (17).

Lemma 5.8. The group $G_{m,m-1,m-2}$ acts on $\Omega_\theta$ with $\lambda_1$ short orbits and $\lambda_2$ long orbits where

$$\lambda_1 = (m - 2)(m - 3)(m - 4), \quad \lambda_2 = 3(m - 2)^2.$$  

Proof. Fix a point $P \in \Omega_\theta$. As in the proof of Lemma 4.11 assume that $P = (x_1, \ldots, x_m)$ where $x_i = x_j = t$ for some $1 \leq i < j \leq m$, $t \in \mathbb{K}$ and $x_k \neq x_l$ whenever $(k, l) \neq (i, j)$. So, the coordinates $(x_1, \ldots, x_m)$ of $P$ are $m - 1$ different values from $\mathbb{K}$. The points of $\Omega_\theta$ are those whose coordinates are a permutation of $x_1, \ldots, x_m$, that is $Q \in \Omega_\theta$ if and only if $Q = (x_{\sigma(1)}, \ldots, x_{\sigma(m)})$ for a permutation $\sigma \in G$. Two points are in the same short $G_{m,m-1,m-2}$-orbit if and only if they share the last three coordinates, hence a short $G_{m,m-1,m-2}$-orbit arises every time we fix an ordered triple $(a, b, c)$, with $a, b, c \neq t$. This can be done in $(m - 2)(m - 3)(m - 4)$ different ways. A long $G_{m,m-1,m-2}$-orbit arises every time we fix an ordered triple $(x_a, x_b, x_c)$, with either one or two of the values $x_a, x_b, x_c$ being equal to $t$. This can be done in $3(m - 2)(m - 3)$ and $3(m - 2)$ different ways respectively. Therefore $\lambda_1 = (m - 2)(m - 3)(m - 4)$ and $\lambda_2 = 3(m - 2)^2$. 

6. Quotient curves of $V$

We have already determined the quotient curve of $V$ with respect to the subgroup of $G$ which fixes two given coordinates $X_i$ and $X_j$; see Lemma 4.3. In this section, we consider the more general case where the subgroup $H_l$ of $G$ fixes $l \geq 3$ coordinates. Let $d = m - 1 - l$. W.l.o.g. these coordinates are assumed to be $X_{d+2}, \ldots, X_m$. The hyperplanes $\Pi_i : X_i = 0$ with $i = d + 2, \ldots, m$ meet in a $d$-dimensional subspace $\Sigma$ which is disjoint from $V$ by Proposition 3.3. Clearly, $H_l$ preserves $\Sigma$. Furthermore, the hyperplanes $\Pi_i : X_i = 0$ with $i = 1, \ldots, d + 1$ meet in a $(m - d - 1)$-dimensional subspace $\Sigma'$ disjoint from $\Sigma$. Clearly, $H_l$ fixes $\Sigma'$ pointwise. Projecting $V$ from $\Sigma$ on $\Sigma'$ produces a curve $\tilde{V}$ of $\Sigma'$ whose degree is equal to $(m - 2)!/(m - l)!$.

Proposition 6.1. Let $H_l$ be the stabilizer of $(X_{j_1}, \ldots, X_{j_l})$ in $G$. If $l \geq 2$ then the quotient curve $V/H_l$ is isomorphic to $\tilde{V}$.

Proof. Take a point $P \in V$ such that no nontrivial element of $H_l$ fixes $P$. Then the $H_l$-orbit $\Omega$ of $P$ has length $(m - l)! = (d + 1)!$. On the other hand, Lemma 4.4 shows that $\Sigma$ and $P$ generate a $(d + 1)$-dimensional subspace $\Sigma$ that cuts out on $V$ a set of $(d + 1)!$ points. Since $\Omega$ is contained in $\Sigma$, it turns out that $\Omega = V \cap \Sigma'$ whence the claim follows.

Remark 6.2. Proposition 6.1 shows that $\Sigma$ is an outer Galois subspace of $V$.

Proposition 6.3. Let $g$ be the genus of the quotient curve $V/H_l$ where $H_l$ is the stabilizer of $(X_{j_1}, \ldots, X_{j_l})$. If $l \geq 2$ then

$$2g - 2 = \frac{(m - 2)(m - 3) - 4 - (m - l)(m - 1 - l)}{2(m - l)!}(m - 2)!$$

(18)
Proof. The number of transpositions in $H_t$ is equal to $\frac{1}{2}(m-l)(m-1-l)$. By Lemma 4.11, each such transposition has as many as $(m-2)!$ fixed points. From Lemmas 4.5, 4.6, and 5.1, no nontrivial element of $H_t$ other than its transpositions fixes a point of $V$. Therefore, the claim follows from the Hurwitz genus formula 3.

6.1. Quotient curve of $V$ by the 3-coordinate stabilizer of $G$. In this section $H = G_{m,m-1,m-2}$ is the stabilizer of $X_m, X_{m-1}, X_{m-2}$ in $G$, and $\tilde{X}$ is the quotient curve of $V$ with respect to $H$. Then $\tilde{X}$ is an irreducible plane curve of degree $m-2$ whose genus equals $\frac{1}{2}(m^2 - 7m + 12)$ by 18. Hence $\tilde{X}$ is non-singular. The following proposition shows that $\tilde{X}$ coincides with the curve introduced and investigated in 39.

Theorem 6.4. $\tilde{X}$ has homogeneous equation $G_{m-2}(x, y, z) = 0$ where

$$G_{m-2}(x, y, z) = \sum_{i,j,k \geq 0, i+j+k=m-2} x^i y^j z^k.$$  

Proof. Since $|H| = (m-3)!$, Lemma 4.13 yields that $\tilde{X}$ contains as many as $(m-1)(m-2)$ points $(\alpha : \beta : 1)$ with $\alpha^m = \beta^m = 1$ but $\alpha, \beta \neq 1$. Let $\tilde{X}$ be the plane curve with homogeneous equation $G_{m-2}(x, y, z) = 0$. By 39 Equation (2)

$$G_{m-2}(x, y, z) = \frac{1}{x-y}\left(\frac{x^m - z^m}{x-z} - \frac{y^m - z^m}{y-z}\right).$$

This shows that $\tilde{X}$ also contains each point $(\alpha : \beta : 1)$ with $\alpha^m = \beta^m = 1$ but $\alpha, \beta \neq 1$. Therefore, $\tilde{X}$ and $\tilde{X}$ have at least $(m-1)(m-2)$ pairwise distinct points. On the other hand, since $\tilde{X}$ and $\tilde{X}$ both have degree $m-2$, Bézout’s theorem applied to $\tilde{X}$ and $\tilde{X}$ yields that if $\tilde{X}$ and $\tilde{X}$ were distinct then they could share at most $(m-2)^2$ points. Therefore, $\tilde{X} = \tilde{X}$. □

Theorem 6.4 shows that $\mathbb{K}(\tilde{X}) = \mathbb{K}(x, y)$ with $G_{m-2}(x, y, 1) = 0$. From Lemma 4.13 the quotient curve of $V$ with respect to the stabilizer of $X_m, X_{m-1}$ is rational. Therefore its function field is $\mathbb{K}(x)$.

Theorem 6.5. The Galois closure $M$ of $\mathbb{K}(\tilde{X})|\mathbb{K}(x)$ is $\mathbb{K}(V)$, with Galois group isomorphic to $\text{Sym}_{m-2}$.

Proof. Since $\mathbb{K}(V)|\mathbb{K}(x)$ is a Galois extension, $M$ may be assumed to be a subfield of $\mathbb{K}(V)$. Thus $\mathbb{K}(V)|M$ is a Galois extension, as well. Galois theory yields that $\text{Gal}(\mathbb{K}(V)|M)$ is a normal subgroup of $\text{Gal}(\mathbb{K}(V)|\mathbb{K}(x))$. Since $\text{Gal}(\mathbb{K}(V)|\mathbb{K}(x)) \cong \text{Sym}_{m-2}$, for $m \geq 7$ and $m = 5$, the unique non-trivial normal subgroup of $\text{Gal}(\mathbb{K}(V)|\mathbb{K}(x))$ is $\text{Alt}_{m-2}$. On the other hand, as $\text{Gal}(\mathbb{K}(\tilde{X}))$ is the fixed field of $G_{m,m-1,m-2}$, $\text{Gal}(\mathbb{K}(\tilde{X})) \subseteq M \neq \mathbb{K}(V)$ would imply that $\text{Alt}_{m-2}$ is isomorphic to a subgroup of $\text{Sym}_{m-3}$ which is impossible by $|\text{Sym}_{m-3}| < |\text{Alt}_{m-2}|$. If $m = 6$, a further case arises, namely $\text{Gal}(\mathbb{K}(V)|M)$ is normal in $\text{Alt}_4$ and of order 4. However, this is again impossible since $4 \nmid |\text{Sym}_3| = 6$. Thus $M = \mathbb{K}(V)$ and $\text{Gal}(\mathbb{K}(\tilde{X})|\mathbb{K}(x))$ is isomorphic to the subgroup of $G$ fixing $x$. Since this subgroup is isomorphic to the stabilizer of $X_m, X_{m-1}$ in $G$, we have $\text{Gal}(\mathbb{K}(\tilde{X})|\mathbb{K}(x)) \cong \text{Sym}_{m-2}$. □

7. The automorphism group of $V$

We are now in position to prove that $G$ is the whole automorphism group of $V$ whenever $\text{Aut}(V)$ is tame, and in particular in zero characteristic. However, as Theorem 4.2 shows, this is not true in positive characteristic, in which case $\text{Aut}(V)$ may contain additional elements of order $p$.

Theorem 7.1. If $\mathbb{K}$ has zero characteristic, or it has positive characteristic and the $\mathbb{K}$-automorphism group of $V$ is tame, then $G$ is the $\mathbb{K}$-automorphism group of $V$.

Proof. For $m = 5$, $V$ is the characteristic $p$ version of the Bring curve of genus 4 whose automorphism group is isomorphic to $\text{Sym}_5$. Therefore, we may limit ourselves to the cases where $m \geq 6$.

By way of a contradiction assume that $G = \text{Sym}_m$ is a proper subgroup of the $\mathbb{K}$-automorphism group $\Gamma$ of $V$. Then two cases arise, according as $G$ is a normal subgroup of $\Gamma$ or is not.
In the former case, assume that the centralizer $\mathcal{C}_\Gamma(G)$ of $G$ in $\Gamma$ is trivial. Then for any $\gamma \in \Gamma$ the map $g \mapsto \gamma^{-1}g\gamma$ is a non trivial automorphism of $G$. Hence $\Gamma$ is isomorphic to a subgroup of $\text{Aut}(G)$. However, if $m \neq 6$, then $\text{Aut}(G) \cong G$, see for instance [40] Section 2.4. Hence $G = \Gamma$, a contradiction. In the remaining case, $m = 6$, then $G \cong P\gamma L(2, 9)$ and $\text{Aut}(G) \cong P\gamma L(2, 9)$; see [40] Section 2.4.2. Therefore, $[\Gamma : G] = 2$. Lemma 5.1 shows that $G$ has a unique orbit of length $(m - 1)! = 120$, namely $\Omega_m$. Since $G$ is a normal subgroup of $\Gamma$, this yields that $\Gamma$ also preserves $\Omega_m$. Hence, the stabilizer of $P_\omega \in \Omega_m$ of $\Gamma$ has order 12. This yields that $\Gamma$ has a cyclic subgroup of order 12, but this is impossible since $P\gamma L(2, 9)$ has two subgroups of order 12, up to conjugation, but neither is cyclic.

Otherwise, $\mathcal{C}_\Gamma(G)$ is a nontrivial subgroup of $\Gamma$ which is disjoint from $G$ as $G$ has trivial center. Furthermore, since $\mathcal{C}_\Gamma(G)$ is contained in the normalizer of $G$ in $\Gamma$, $\mathcal{C}_\Gamma(G)$ induces a permutation group on the set of the short orbits of $G$. By Lemma 5.1 there are three such orbits and they have pairwise different lengths. Therefore, this permutation group is trivial, that is, $\mathcal{C}_\Gamma(G)$ preserves each of the three short orbits of $G$.

Also, $\mathcal{C}_\Gamma(G) \cong \mathcal{C}_\Gamma(G)G/G$ is an isomorphic to a nontrivial $\mathcal{K}$-automorphism group $\bar{G}$ of the quotient curve $\bar{V} = V/G$ which fixes three points of $\bar{V}$. However, this is impossible as $\bar{V}$ is rational by Lemma 5.1.

In the case where $G$ is not normal in $\Gamma$, take any conjugate $\bar{G} = g^{-1}G\gamma$ of $G$ with $\gamma \in \Gamma$, and consider their intersection $N = G \cap \bar{G}$. Assume first $N = \text{Alt}_m$. If this occurs for every $\gamma \in \Gamma$, then $N$ is a normal subgroup of $\Gamma$. As shown before, this is impossible. Now take $\bar{G}$ such that $N \neq \text{Alt}_m$. Then $[N] \leq (m - 1)!$; see [3] Theorem 5.2B]. Therefore, $|G, \bar{G}| \geq |G|^2/(m - 1)! = m \cdot m!$, whence $|\Gamma| \geq m \cdot m!$. A comparison with [10] gives

$$\frac{|\Gamma|}{g - 1} = \frac{4m^2(m - 1)}{(m - 2)(m - 3) - 4}$$

whence $|\Gamma| > 84(g - 1)$ for $m = 5, 6$ and $m > 15$ whereas $40(g - 1) < |\Gamma| \leq 84(g - 1)$ for the remaining cases of $m$.

Since $\Gamma$ is assumed to be tame, $\Gamma$ has exactly three short orbits, and the classical Hurwitz bound yields $|\Gamma| \leq 84(g - 1)$. So we are left with $7 \leq m \leq 15$. From Hurwitz’s proof given in [29] or [13] Theorem 11.56, it follows that $|\Gamma| > 40(g - 1)$ is only possible when $V$ has two points with stabilizers of $\Gamma$ of order 2 and 3, respectively. But Lemma 5.1 shows that the three nontrivial point stabilizers of $\Gamma$ have order $m, m - 1$ and 2. This completes the proof.

\begin{theorem}
If $\text{Aut}(V)$ contains some non-tame projectivities then $m = p - 1$ and the linear subgroup $L\text{Aut}(V)$ of $\text{Aut}(V)$ is isomorphic to $\text{Sym}_p$.
\end{theorem}

\begin{proof}
Let $g \in \text{Aut}(V)$ be a projectivity preserving $V$. We show that $g$ preserves the non-degenerate quadric $Q$ of $PG(m - 2, \mathcal{K})$ of equations

$$\begin{align*}
X_1 + X_2 + \ldots + X_m &= 0, \\
X_1^2 + X_2^2 + \ldots + X_m^2 &= 0.
\end{align*}$$

Since $g$ is a projectivity, Lemma 5.1 yields that $g$ preserves the hyperplane of equation $X_1 + X_2 + \ldots + X_m = 0$. Furthermore, $g(Q)$ is a quadric of equation $F = F(X_1, X_2, \ldots, X_m) = 0$ where $\deg(F) = 2$. Since $g \in \text{Aut}(V)$,

$$F = u_1(X_1 + X_2 + \ldots + X_m) + u_1(X_1^2 + X_2^2 + \ldots + X_m^2) + \ldots + u_{m-2}(X_1^{m-2} + X_2^{m-2} + \ldots + X_m^{m-2})$$

where $u_1, u_2, \ldots, u_{m-2} \in \mathcal{K}[X_1, X_2, \ldots, X_m]$. Therefore, $u_i = 0$ for $2 < i \leq m - 2$. Now, take any point $P = P(\xi_1, \ldots, \xi_m) \in Q$. Then $F(\xi_1, \xi_2, \ldots, \xi_m) = u_1(\xi_1 + \xi_2 + \ldots + \xi_m) + u_2(\xi_1^2 + \xi_2^2 + \ldots + \xi_m^2) = 0 + 0 = 0$. Therefore, $g(P) \in Q$. In particular, $L\text{Aut}(V)$ contains no elation.

Let $N$ be the subgroup generated by all involutory homologies of $L\text{Aut}(V)$. From Lemma 5.1, $G = \text{Sym}_m$ is generated by involutory homologies and hence $L\text{Aut}(V)$ contains $G$. Also, $N$ is a normal subgroup of $L\text{Aut}(V)$. The centralizer of $\text{Sym}_m$ in $L\text{Aut}(V)$ is trivial, since the centers of the involutory homologies in $G$ span $PG(m - 2, \mathcal{K})$ as we have pointed out in the proof of Theorem 5.6. Therefore, if $N = G$ is
supposed, then $\text{LAut}(V)$ is isomorphic to a subgroup of the automorphism group $\text{Aut}(\text{Sym}_m)$ of $\text{Sym}_m$. For $m \neq 6$, $\text{Aut}(\text{Sym}_m) \cong \text{Sym}_m$, see for instance [10] Section 2.4. From this, $\text{LAut}(V) \cong \text{Sym}_m$ whence $\text{LAut}(V) = G$ for $m \neq 6$ but this contradicts the hypothesis that $\text{Aut}(V)$ contains non-tame projectivities. In the exceptional case, $|\text{Aut}(\text{Sym}_6)| = 2|\text{Sym}_6| = 1440 = 2^5 \cdot 3^2 \cdot 5$; in particular $p$ does not divide $|\text{LAut}(V)|$, and hence $\text{LAut}(V) = G$ by Theorem 7.1. Therefore, $G$ is a proper subgroup of $N$. Now, we apply Result 2.2 to $N$. By Lemma 1.14 and Henn’s classification theorem [16] Theorem 11.127, inequality 41 does not hold in our case. Therefore, $m = p - 1$ and $N \cong \text{Sym}_m$.

We have to show that if $m = p - 1$ then $\text{LAut}(V)$ is indeed larger than $\text{Sym}_m$. Let $m = p - 1$. We show that the linear map

$$
\lambda : (X_1, \ldots, X_j, \ldots, X_{p-1}) \mapsto (X_1 - X_{p-1}, \ldots, X_j - X_{p-1}, \ldots, X_{p-2} - X_{p-1}, -X_{p-1})
$$

preserves $V$. By Section 2.4, in the function field $\mathbb{K}(V)$, $\sigma_k(X_1, X_2, \ldots, X_p) = 0$ for $k = 1, \ldots, p - 3$. We will use the following equations

$$
\sigma_k(X_1, \ldots, X_{p-2}) = \sigma_k(X_1, \ldots, X_{p-1}) - X_{p-1} \sigma_{k-1}(X_1, \ldots, X_{p-2}).
$$

Since $\sigma_1(X_1, \ldots, X_{p-2}) = -X_{p-1}$, induction on $k$ gives

(21)  
$$
\sigma_k(X_1, \ldots, X_{p-2}) = (-1)^k X_{p-1}^k,
$$

Write $\sigma_k(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1}, -X_{p-1})$ as a sum of two terms:

$$
\sigma_k(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1}, -X_{p-1}) = \left( \sum_{1 \leq i_1 < \cdots < i_k \leq p-2} (X_{i_1} - X_{p-1}) \cdots (X_{i_k} - X_{p-1}) \right) - X_{p-1} \left( \sum_{1 \leq i_1 < \cdots < i_k \leq p-2} (X_{i_1} - X_{p-1}) \cdots (X_{i_k} - X_{p-1}) \right)
$$

which is equal to

$$
\sigma_k(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1}) - X_{p-1} \sigma_{k-1}(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1}).
$$

Next, write $\sigma_k(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1})$ as a polynomial in $X_{p-1}$. Expanding $\sigma_k$ shows that each product $X_{i_1} \cdots X_{i_j}$, with $X_{i_1} \in \{X_1, \ldots, X_{p-2}\}$, appears every time when the remaining $k - j$ factors in the product are equal to $X_{p-1}$. This occurs every time when the remaining $k - j$ indeterminates $X_{i_1}$ are chosen among $\{X_1, \ldots, X_{p-2}\} \setminus \{X_{i_1}, \ldots, X_{i_j}\}$, that is, it appears $(\binom{p-2-j}{k-j})$ times. Summing up,

$$
\sigma_k(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1}) = \sum_{j=0}^{k} (-1)^{k-j} \binom{p-2-j}{k-j} X_{p-1}^k \sigma_j(X_1, \ldots, X_{p-2}).
$$

This together with (21) yield

$$
\sigma_k(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1}) = (-1)^k X_{p-1}^k \sum_{j=0}^{k} \binom{p-2-j}{k-j}.
$$

To compute the sum on the right hand side, the following identities will be useful

$$
\binom{n}{k} = \binom{n+1}{k} - \binom{n}{k-1}, \quad \binom{p-1}{k} \equiv (-1)^k \pmod{p}.
$$

Now,

$$
\sum_{j=0}^{k} \binom{p-2-j}{k-j} = \sum_{j=0}^{k-1} \left( \binom{p-2-j+1}{k-j} - \binom{p-2-j}{k-j-1} \right) + \binom{p-2-k}{0} = \binom{p-1}{k} - \binom{p-2-k+1}{0} + \binom{p-2-k}{0} = \binom{p-1}{k} \equiv (-1)^k \pmod{p};
$$

$$
\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}, \quad \binom{p-1}{k} \equiv (-1)^k \pmod{p}.
$$
Summing up,
\[\sigma_k(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1}, -X_{p-1}) = \]
\[\sigma_k(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1}) - X_{p-1}\sigma_k(X_1 - X_{p-1}, X_2 - X_{p-1}, \ldots, X_{p-2} - X_{p-1}) = \]
\[(-1)^{2k} X_{p-1}^k + (-1)^{2k-2+1} X_{p-1}^k = 0.\]

By Section 2.8 this completes the proof. It also shows for \( m = p - 1 \) that the projectivity \( \Lambda \) of \( PG(m - 2, K) \) defined by \( \lambda \) preserves \( V \). We point out that \( \Lambda \) is an involutory homology. From the definition of \( \lambda \), every point on the hyperplane \( H_{p-1} \) of equation \( X_{p-1} = 0 \), as well as, the point \( C = (1 : 1 : \cdots : 2) \) are fixed by \( \Lambda \). Therefore, \( \Lambda \) is a homology with center \( C \) and axis \( H_{p-1} \). Furthermore, \( \Lambda^2 \) the identity and hence \( \Lambda \) is an involution. \( \square \)

In the subsequent sections we further investigate the two extremal cases in positive characteristic, namely \( m = 5 \) and \( m = p - 1 \). Accordingly, from now on, \( K \) stands for the algebraic closure of the field \( \mathbb{F}_p \) where \( p \geq 7 \) is a prime. Then, \( V \) is defined over \( \mathbb{F}_p \) and viewed as a curve defined over \( K \). The group \( G \) is also defined over \( \mathbb{F}_p \), and it preserves the set \( \mathcal{X}(\mathbb{F}_p) \) of points of \( V \) defined over \( \mathbb{F}_p \) for every \( i \geq 1 \).

8. The case of positive characteristic: \( m = p - 1 \)

Throughout this section we always assume \( m = p - 1 \).

8.1. The action of \( \text{LAut}(V) \) on \( V \). First, we point out a result on the number of solutions of System \( \mathbb{F}_p \).

**Theorem 8.1.** System \( \mathbb{F}_p \) modulo \( p \) has as many as \((p - 1)! \) solutions.

**Proof.** One can count the solutions of \( \mathbb{F}_p \) modulo \( p \) up to a non-zero constant factor by computing the number of points of \( V \) over \( \mathbb{F}_p \). Since any primitive \((p - 1)\)-th roots of unity in \( K \) is in \( \mathbb{F}_p \), Lemma 1.5 yields \(|V(\mathbb{F}_p)| = (p - 2)! \), and the claim follows. \( \square \)

**Proposition 8.2.** The short orbits of \( \text{LAut}(V) \) on \( V \) are exactly \( \Omega_{\omega} \) and \( \Omega_{\varepsilon} \cup \Omega_{\theta} \), and they have lengths \((m - 1)! \) and \( m(m - 2)! + m! \), respectively.

**Proof.** Theorem 7.1 shows that \( \Omega_{\omega} \) consists of all \( \mathbb{F}_p \)-rational points of \( V \). From the proof of Theorem 7.2 \( \text{LAut}(V) \) is defined over \( \mathbb{F}_p \). Therefore a short orbit of \( \text{LAut}(V) \) is \( \Omega_{\omega} \). Since \( p \) is prime to \( |\Omega_{\omega}| \), this yields that the order of the stabilizer of a point in \( \Omega_{\omega} \) is divisible by \( p \), i.e. \( \Omega_{\omega} \) is a non-tame orbit. Actually, \( \Omega_{\omega} \) is the unique non-tame orbit of \( \text{LAut}(V) \) on \( V \). In fact, since \( p^2 \) does not divide \( \text{LAut}(V) \), any two \( p \)-subgroup of \( \text{LAut}(V) \) are conjugate in \( \text{LAut}(V) \), and hence the fixed points of the \( p \)-subgroups of \( \text{LAut}(V) \) belong to the same orbit of \( \text{LAut}(V) \). From [15] Theorem 11.56, \( \text{LAut}(V) \) has either one or two tame short orbits on \( V \).

The former case is investigated first. Let \( \Omega \) be the unique tame-orbit of \( \text{LAut}(V) \) on \( V \). Choose a point \( Q \) from \( \Omega \). Then \( Q \) is fixed by a cyclic group of odd order \( p - 2 \). From the proof of Theorem 7.2 \( Q \) is also fixed by the involutory homology \( \Lambda \). Therefore, the stabilizer of \( Q \) in \( \text{LAut}(V) \) is a cyclic group of order \( 2(p - 2)\mu \). Since the quotient curve \( V/\text{LAut}(V) \) is rational by Lemma 4.13, the Hurwitz genus formula applied to \( \text{LAut}(V) \) gives
\[2g(V) - 2 = (p - 2)!\kappa(p - 1) - \frac{p^i}{2(p - 2)\mu}\]
where \( \kappa \) counts the ramification groups of \( \text{LAut}(V) \) at \( P \). This together with Lemma 4.14 yield
\[p^2 - 5p + 4 + \frac{p(p - 1)}{\mu} = 2\kappa(p - 2)(p - 1).\]
In particular, Equation 22 yields \( \mu |(p - 1) \) by \( p \) \( \nmid \kappa \). Taking 22 \( \mod p \), \( 4\kappa \equiv 4 \pmod p \) is obtained whence \( \kappa \equiv 1 \pmod p \) follows. For \( \kappa \geq p + 1 \), 22 is impossible. Thus \( \kappa = 1 \), and hence \( \mu = 1 \), that is,
This time the Stöhr-Voloch bound gives

$$|\text{LAut}(V)| = 2(p-2)$$. Therefore, the unique short tame-orbit $\Omega$ of $\text{LAut}(V)$ has size $(p-1)(p-3)!+(p-1)/2$.

Since $\Omega$ contains both $\Omega_x$ and $\Omega_\theta$, this yields $\Omega = \Omega_x \cup \Omega_\theta$.

It remains to rule out the possibility of two short tame-orbits. Assume on the contrary that $\Omega_x$ and $\Omega_\theta$ are two distinct short non-tame orbits of $\text{LAut}(V)$. We may suppose $\Omega_x \subseteq \Omega_1$. From the Hurwitz genus formula applied to $\text{LAut}(V)$,

$$2g(V) - 2 = (p-2)!((\kappa(p-1)) - 1) - \frac{p!}{2(p-2)\mu} + |\Omega_2|(|\text{LAut}(V)| - 1).$$

Since $|\text{LAut}(V)| - 1 \geq \frac{7}{2}|\text{LAut}(V)|$, and $(p-2)!((p-1)-1) > \frac{7}{2}p!/(p-2)$, this yields $4g(V) - 4 > |\text{LAut}(V)|$. But this is impossible, as $4g(V) - 4 = 2((p-2)(p-3) - 4)(p-3)! < p! = |\text{LAut}(V)|$. □

**Proposition 8.3.** $\text{LAut}(V)$ acts on $\Omega_\omega$ as a primitive permutation group.

**Proof.** Let $P$ be a point in $\Omega_x$. Then the stabilizer $U$ of $P$ in $\text{LAut}(V)$ contains a cyclic group $H$ of order $p - 1$. From the proof of Proposition 5.2, $U$ also contains a Sylow $p$-subgroup $S_p$ of order $p$. Since $|\Omega_x| = (p-3)!$ and $|\text{LAut}(V)| = p!$, it follows that $|U| = p(p-1)$. Therefore $U = S_p \rtimes H$. Now, look at the natural action of $\text{Sym}_p$ on a set $\Theta$ of size $p$. Since $|U| = p(p-1)$, $U$ acts as a $2$-transitive permutation group.

Take a subgroup $W$ of $S_p$ that contains $U$ properly. From the classical Burnside theorem [6], Chapter X, Section 151-154, $W$ is an almost simple group, i.e. there exists a simple group $T$ such that $T \leq W \leq \text{Aut}(T)$ up to an isomorphism. Thus Guralnick’s classification, see Result 2.3, applies to $T$. Case (ii) is ruled out by Result 2.4. Cases (iii) are also impossible as neither $PGL(2,11)$ nor $\text{Aut}(M_{11}) = M_{11}$ have a subgroup of order $11 \cdot 10 = 110$ whereas $\text{Aut}(M_{23}) = M_{23}$ has no subgroup of order $23 \cdot 22 = 506$. Therefore, Case (i) occurs and hence $W = \text{Alt}_p$, or $W = \text{Sym}_p$. But $\text{Alt}_p$ contains no cyclic group of order $p - 1$ whence $W = \text{Sym}_p$ follows. □

**8.2. Further results on $V(\mathbb{F}_{p^n})$**. From the proof of Theorem 8.1, $V(\mathbb{F}_p)$ is the $G$-orbit $O_\omega$ defined in Lemma 4.5. Furthermore, Lemmas 4.6 and 4.7 have the following corollary.

**Lemma 8.4.** The $G$-orbit $O_\omega$ is contained in $V(\mathbb{F}_p)$ but not in $V(\mathbb{F}_{p^n})$ for $j < i$, where $\mathbb{F}_{p^n}$ is the smallest subfield of $\mathbb{K}$ containing a $(p-2)$-th primitive root $\epsilon$ of unity.

We are in a position to prove the following theorem.

**Theorem 8.5.** The curve $V$ has no proper $\mathbb{F}_{p^n}$-rational point, that is $V(\mathbb{F}_p) = V(\mathbb{F}_p)$.

**Proof.** By way of a contradiction, $|V(\mathbb{F}_{p^n})| > |V(\mathbb{F}_p)|$ is assumed. Then, since $G$ takes $\mathbb{F}_{p^n}$-rational points to $\mathbb{F}_{p^n}$-rational points, there exists a $G$-orbit $\Omega$ entirely contained in $V(\mathbb{F}_{p^n}) \setminus V(\mathbb{F}_p)$. $\Omega$ is a long orbit, that is $|\Omega| = (p-1)!$, and let $H$ be the stabilizer of $X_{p-1}, X_{p-2}, X_{p-3}$ in $G$. Then $H$ partitions $\Omega$ into $(p-1)(p-2)(p-3)$ long $H$-orbits. Since each $H$-orbit corresponds to a point of $\mathcal{X} = V/H$, it follows that

$$|\mathcal{X}(\mathbb{F}_{p^n}) \setminus \mathcal{X}(\mathbb{F}_p)| \geq (p-1)(p-2)(p-3).$$

On the other hand, the Stöhr-Voloch bound [3.3] (see also [10] Theorem 8.41) applied to $\mathcal{X}$ gives

$$2|\mathcal{X}(\mathbb{F}_{p^n})| \leq (2g(\mathcal{X}) - 2) + (p^2 + 2)(p-3) = (p-6)(p-3) + (p^2 + 2)(p-3) = (p-3)(p^2 + p - 4).$$

Therefore, $(p-1)(p-2)(p-3) \leq (p-3)(p^2 + p - 4)$. But then $p < 7$, a contradiction.

Assume now that $\Omega$ is a short orbit. From Lemma 5.1 the only possibility is that $\Omega = \Omega_\theta$ for some transposition $\theta \in G$. Since each $H$-orbit corresponds to a point of $\mathcal{X}$, Lemma 5.8 implies

$$|\mathcal{X}(\mathbb{F}_{p^n}) \setminus \mathcal{X}(\mathbb{F}_p)| \geq \lambda_1 + \lambda_2 = (p-3)(p^2 - 6p + 11).$$

This time the Stöhr-Voloch bound gives

$$2 \cdot (p-3)(p^2 - 6p + 11) \leq (p-3)(p^2 + p - 4),$$

which is only possible for $p = 7$. However, a Magma aided computation rules out this possibility. □
From Lemmas 4.3 and 1.4, \( \Omega_0 = V(\mathbb{F}_p) \) and \( \Omega_0 \subset V(\mathbb{F}_p) \) respectively, where \( \mathbb{F}_p \) is the smallest subfield of \( \mathbb{K} \) containing a primitive \((p - 2)\)-th root of unity. We prove an analog claim for \( \Omega_\theta \). As pointed out in the proof of Lemma 4.11, \( \Omega_\theta \) has a point \( P \) whose last two coordinates are equal 1.

**Lemma 8.6.** Let \( P = (\xi_1, \xi_2, \ldots, \xi_{p-3}, 1, 1) \) be a point of \( \Omega_\theta \). Then \( \xi_{p-3} \in \mathbb{F}_p \) for some \( 1 < j \leq p - 3 \). Furthermore, if \( \xi_{p-3} \notin \mathbb{F}_p \) with \( j < p - 3 \) then, up to a permutation of the indices \( \{1, 2, \ldots, p - 4\} \),

\[
x_j = x_{p-3}^{p^j} \quad j = 1, 2, \ldots, p - 4.
\]

**Proof.** Since both \( V \) and \( \Omega_\theta \) are defined over \( \mathbb{F}_p \), Lemma 5.1 shows that the Frobenius map \( \Phi \) takes \( P \) to the point \( P^{(p)} \in \Omega_\theta \) where \( P^{(p)} = (\xi_1^p, \xi_2^p, \ldots, \xi_{p-3}^p, 1, 1) \). Also, \( \Phi^i \) takes \( P \) to the point

\[
P^{(p^i)} = (\xi_1^{p^i}, \xi_2^{p^i}, \ldots, \xi_{p-3}^{p^i}, 1, 1)
\]

of \( \Omega_\theta \). To prove the first claim, assume on the contrary \( \xi_{p-3} \notin \mathbb{F}_p \) for \( j \leq p - 3 \). Then \( \xi_{p-3}, \xi_{p-3}^p, \ldots, \xi_{p-3}^{p^{p-3}} \) are pairwise distinct. On the other hand, from Lemma 4.5, \( \xi_{p-3} \notin \mathbb{F}_p \), which is a contradiction. To prove the second claim, we may assume that \( \xi_{p-3} \notin \mathbb{F}_p \). Then the previous argument shows that \( \{\xi_{p-3}, \xi_{p-3}^p, \ldots, \xi_{p-3}^{p^{p-3}}\} = \{\xi_1, \xi_2, \ldots, \xi_{p-3}\} \) whence the claim follows. \( \square \)

Theorem 6.4 together with Lemma 8.6 have the following corollary.

**Proposition 8.7.** Let \( \mathbb{F}_{p^d} \) be the subfield of \( \mathbb{K} \) which is the splitting field of the polynomial \( f(X) = X^{p-3} + 2X^{p-4} + 3X^{p-5} + \ldots + (p - 3)X + p - 2 \). Then \( \Omega_\theta \subset V(\mathbb{F}_{p^d}) \) but \( \Omega_\theta \not\subset V(\mathbb{F}_{p^i}) \) for \( i < j \).

The proof of the following theorem relies on Proposition 8.7.

**Theorem 8.8.** Let \( d \) be the smallest positive integer such that \( (p - 2) \mid (pd - 1) \). Then \( \Omega_\theta, \Omega_\epsilon \subset V(\mathbb{F}_{p^d}) \) but \( \Omega_\theta, \Omega_\epsilon \not\subset V(\mathbb{F}_{p^i}) \) for \( i < d \).

**Proof.** By definition, \( \mathbb{F}_{p^d} \) is the smallest extension of \( \mathbb{F}_p \) containing a primitive \((p - 2)\)-th root of unity. So, the claim holds for \( \Omega_\epsilon \). To complete the proof, consider the polynomial

\[
g(X) = \frac{X^{p-2} - 1}{X - 1} = X^{p-3} + X^{p-4} + \ldots + X + 1,
\]

whose splitting field is \( \mathbb{F}_{p^d} \). We prove that \( g(1 - X) = f(X) \). Indeed

\[
g(1 - X) = \sum_{i=0}^{p-3} \sum_{j=0}^{i} \binom{i}{j}(-X)^j,
\]

and for \( i \in \{0, \ldots, p - 3\} \) the coefficient of \( X^i \) in \( g(1 - X) \) is

\[
(-1)^i \sum_{k=i}^{p-3} \binom{k}{i} = (-1)^i \sum_{k=0}^{p-3-i} \binom{i + k}{i} = (-1)^i \binom{p - 2}{p - 3 - i} = (-1)^i \binom{p - 2}{i + 1}.
\]

Thus,

\[
g(1 - X) = \sum_{i=0}^{p-3} \binom{p - 2}{i + 1}(-X)^i = \sum_{i=0}^{p-3} (p - 2 - i)X^i = f(X).
\]

Therefore the splitting field of \( f(X) \) coincides with the splitting field of \( g(X) \) and Proposition 8.7 yields the claim. \( \square \)
8.3. Non-classicality and Frobenius non-classicality of \( V \). For \( m = p - 1 \), Proposition 8.10 has the following corollary.

**Proposition 8.9.** If \( K \) has characteristic \( p \) then \( V \) is contained in the Hermitian variety \( H_{p-3} \) which is the intersection of the hyperplane \( \Pi \) of equation \( X_1 + X_2 + \ldots + X_{p-1} = 0 \) with the Hermitian variety \( H_{p-2} \) of equation \( X_1^{p+1} + \ldots + X_{p-1}^{p+1} = 0 \).

**Lemma 8.10.** For a point \( P \in V \), let \( \Pi_P \) be the tangent hyperplane to \( H_{p-3} \) at \( P \). Then \( I(P, V \cap \Pi_P) \geq p \).

**Proof.** Clearly, \( \Pi_P \) is the intersection of the tangent hyperplane of \( \Pi \) with the Hermitian variety \( H_{p-2} \) at \( P \). Since \( V \) is contained in \( \Pi \), \( I(P, V \cap \Pi_P) = I(P, V \cap \alpha_P) \) holds. Hence, it is enough to show that \( I(P, V \cap \alpha_P) \) is at least \( p \).

Let \( P = (\xi_1 : \ldots : \xi_{p-2} : \xi_{p-1}) \). Up to a change of coordinates, \( \xi_{p-1} = 1 \) may be assumed. In the affine space \( AG(p-2, K) \) with infinite hyperplane \( X_{p-1} = 0 \), \( H_{p-2} \) has equation \( X_1^{p+1} + X_2^{p+1} + \ldots + X_{p-2}^{p+1} + 1 = 0 \). For every \( i = 1, \ldots, p-2 \), let \( x_i(t) = \xi_i + \rho_i(t) \) with \( x_i(t), \rho_i(t) \in K[[t]] \) and \( \text{ord}(\rho_i(t)) \geq 1 \) be a primitive representation of the unique branch of \( V \) centered at \( P \). By Proposition 8.9 \( V \) is contained in \( H \). Therefore, \( x_1(t)^{p+1} + x_2(t)^{p+1} + \ldots + x_{p-2}(t)^{p+1} + 1 \) vanishes in \( K[[t]] \).

Since \( \Pi_P \) has equation \( \xi_1^p x_1 + \xi_2^p x_2 + \ldots + \xi_{p-2}^p x_{p-2} + 1 = 0 \) in \( AG(p-2, K) \), the claim follows. \( \square \)

Since the dimension of \( PG(p-2, K) \) is smaller than \( p \), Lemma 8.10 has the following corollary.

**Theorem 8.11.** \( V \) is a Frobenius non-classical curve.

**Theorem 8.12.** \( V \) is a Frobenius non-classical curve.

**Proof.** Assume on the contrary that \( V \) is Frobenius classical. Then \( 0, 1, \ldots, p-4 \) are orders at a generically chosen point of \( V \). Lemma 8.10 yields that the last order, \( \varepsilon_{p-3} \), is equal to \( p \). Therefore, Lemma 8.10 also yields that the osculating tangent hyperplane to \( V \) at \( P \) coincides with the tangent hyperplane \( \Pi \) to Hermitian variety \( H_p \). Since \( \Pi \) passes through the Frobenius image of \( P \), it follows that \( V \) is Frobenius non-classical, a contradiction. \( \square \)

8.4. Some results on the orders of \( V \) at \( \mathbb{F}_p \)-rational points. Since \( G \) is transitive on \( V(\mathbb{F}_p) \), the orders of \( V \) are the same at every point \( P \in V(\mathbb{F}_p) \). From Lemma 3.2 such a point is \( P = (1 : \eta^{p-2} : \eta^{p-3} : \ldots : \eta) \) for a primitive element \( \eta \) of \( \mathbb{F}_p \). From Lemma 15 the stabilizer of \( P \) in \( G \) is a cyclic group of order \( p - 1 \) generated by the projectivity \( \sigma \) associated with the matrix

\[
M_\sigma = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
& & \ddots & & \\
0 & 0 & 0 & \cdots & 0 \\
1 & 0 & 0 & \cdots & 0
\end{pmatrix}.
\]

(23)

The eigenvalues of \( M_\sigma \) are \( \lambda_i = \eta^i \) for \( i = 0, \ldots, p-2 \). Moreover, then eigenvectors of \( M_\sigma \) are \( w_i = (1, \eta^i, \eta^{2i}, \ldots, \eta^{(p-2)i}) \). Thus the point of \( PG(p-2, \mathbb{F}_p) \) represented by \( w_i \) is in \( V \) if and only if \( \gcd(i, p-1) = 1 \). Therefore, \( \sigma \) has as many as \( \varphi(p-1) \) fixed points on \( V \).
Let \( \eta_i = \eta^i \) for \( i = 0, \ldots, p-2 \), and consider the change of the projective frame from \((X_1 : X_2 : \cdots : X_{p-1})\) to \((Y_1 : Y_2 : \cdots : Y_{p-1})\) defined by

\[
\begin{align*}
X_1 &= Y_1 + Y_2 + \cdots + Y_{p-1}; \\
X_2 &= Y_1 + \eta_1 Y_2 + \eta_1^2 Y_3 + \cdots + \eta_1^{p-2} Y_{p-1}; \\
X_3 &= Y_1 + \eta_2 Y_2 + \cdots + \eta_2^{p-2} Y_{p-1}; \\
&\vdots \\
X_{p-1} &= Y_1 + \eta_{p-2} Y_2 + \cdots + \eta_{p-2}^{p-2} Y_{p-1}.
\end{align*}
\]

(24)

With this transformation, \( P \) is taken to the fundamental point \( O = (0 : 0 : \cdots : 0 : 1) \). Let \( R \) be the matrix whose rows are the vectors \( w_i, i = 1, \ldots, p-1 \). Then \( R^{-1} M_\sigma R \) is the diagonal matrix

\[
D = \begin{pmatrix}
\eta & 0 & \cdots & 0 \\
0 & \eta^2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & 0 & \eta^{2u}
\end{pmatrix},
\]

where \( 2u = p-1 \), and hence it is the matrix associated to \( \sigma \) in the projective frame \((Y_1 : Y_2 : \cdots : Y_{p-1})\). Replacing \( X_i \) by \( X_i^{(24)} \) in \( (11) \), we obtain the equations of \( V \) in the projective frame \((Y_1 : Y_2 : \cdots : Y_{p-1})\). Now, we explicitly write down the equations defining \( V \) in the projective frame \((Y_1 : Y_2 : \cdots : Y_{p-1})\). From the first equation in \( (11) \), we obtain \( Y_1 = 0 \). In fact, \( \sum_{i=1}^{p-1} X_i = (p-1)Y_1 + Y_2 \sum_{j=0}^{p-2} \eta_1^j + \cdots + Y_{p-1} \sum_{j=0}^{p-2} \eta_{p-2}^j \), and for \( i = 1, \ldots, p-2 \) we have \( \sum_{j=0}^{p-2} \eta_i^j = (\eta_i^{p-1} - 1)/(\eta_i - 1) = 0 \). Therefore, \( V \) is a projective variety of \( \text{PG}(p-3, \mathbb{F}_p) \) with projective frame \((Y_2 : Y_3 : \cdots : Y_{p-1})\).

Since \( O \) is off the hyperplane of homogenous equation \( Y_{p-1} = 0 \), a branch representation of the unique branch \( \gamma \) of \( V \) centered at \( O \) has as components \( y_2 = y_2(t), \ldots, y_{p-2} = y_{p-2}(t), y_{p-1} = 1 \). Here \( y_i(t) \in \mathbb{F}_p[[t]] \). Furthermore, we can assume \( \text{ord}(y_{p-2}(t)) = 1 \), since \( O \) is a simple point of \( V \) and the tangent hyperplane to \( V \) at \( O \) does not contain the line of homogeneous equation \( Y_2 = 0, \ldots, Y_{p-3} = 0 \). Therefore,

\[
\begin{align*}
y_2(t) &= \alpha_{2,1} t + \alpha_{2,2} t^2 + \cdots \\
y_3(t) &= \alpha_{3,1} t + \alpha_{3,2} t^2 + \cdots \\
&\vdots \\
y_{p-2}(t) &= \alpha_{p-3,1} t + \alpha_{p-3,2} t^2 + \cdots \\
y_{p-1}(t) &= 1.
\end{align*}
\]

(25)

Since the projectivity \( \sigma \) preserves \( V \) and fixes \( O \), it also preserves \( \gamma \). Moreover, \( \sigma \) is associated to the above diagonal matrix \( D \). This yields that an equivalent branch representation is given by

\[
\begin{align*}
\tilde{y}_1(t) &= 0 \\
\tilde{y}_2(t) &= \eta^2(\alpha_{2,1} t + \alpha_{2,2} t^2 + \cdots) \\
\tilde{y}_3(t) &= \eta^3(\alpha_{3,1} t + \alpha_{3,2} t^2 + \cdots) \\
&\vdots \\
\tilde{y}_{p-2}(t) &= \eta^{p-3}(\alpha_{p-3,1} t + \alpha_{p-3,2} t^2 + \cdots) \\
\tilde{y}_{p-1}(t) &= \eta^{-1} t
\end{align*}
\]

(26)
From this $\alpha_{2,i} = 0$ for $i < 2u - 2$. More generally, $\alpha_{k,i} = 0$ for $2 \leq k \leq p - 3$ and $i < p - 1 - k$. Therefore, $\text{ord}(y_k(t)) \geq p - 1 - k$ for $2 \leq k \leq p - 3$. Moreover, the only coefficients $\alpha_{k,i} \neq 0$ are among those verifying $i + k \equiv 0 \pmod{p - 1}$, where $2 \leq k \leq p - 3$ and $i \geq 1$. Thus, the branch representation is

$$
\begin{cases}
  y_2(t) = \alpha_{2,p-3}t^{p-3} + \alpha_{2,2p-4}t^{2p-4} + \cdots + \alpha_{2,w(p-1)-2}t^{w(p-1)-2} + \cdots \\
  y_3(t) = \alpha_{3,p-4}t^{p-4} + \alpha_{3,4p-3}t^{4p-3} + \cdots + \alpha_{3,w(p-1)-3}t^{w(p-1)-3} + \cdots \\
  \vdots \\
  y_{p-4}(t) = \alpha_{p-4,3}t^3 + \alpha_{p-4,2p-5}t^{2p-5} + \cdots + \alpha_{p-4,w(p-1)+3}t^{w(p-1)+3} + \cdots \\
  y_{p-3}(t) = \alpha_{p-3,2}t^2 + \alpha_{p-3,p+1}t^{p+1} + \cdots + \alpha_{p-3,w(p-1)+2}t^{w(p-1)+2} + \cdots \\
  y_{p-2}(t) = t \\
  y_{p-1}(t) = 1.
\end{cases}
$$

We now show how to compute the remaining orders.

Recall that, in the new coordinates, the $k$-th equation in \(\mathbf{P}\) reads

$$
\sum_{j=1}^{p-1} \left( \sum_{i=2}^{p-2} \eta_{j-1}^{i-1}Y_i + \eta_j^{p-2}Y_{p-1} \right)^k,
$$

and that by the multinomial theorem

$$
\left( \sum_{i=2}^{p-2} s_i + v \right)^k = \sum_{k_2 + \cdots + k_{p-2} + l = k} \binom{k}{k_2, \ldots, k_{p-2}, l} \prod_{u=2}^{p-2} s_u^{k_u} \cdot v^l.
$$

Replacing $Y_i$ by $y_i(t) = \sum_{s=1}^{\infty} \alpha_{i,(p-1)s-i}t^{(p-1)s-i}$ in the $k$-th equation, it is obtained

$$
\sum_{j=1}^{p-2} \left( \sum_{i=2}^{p-2} \eta_{j-1}^{i-1} \left( \sum_{s=1}^{\infty} \alpha_{(p-1)s-i}t^{(p-1)s-i} \right) + \eta_j^{p-2} \right)^k = 0.
$$
For any fixed $k = 2$ we see that the quadratic term in $t$ in the $(p - 3)$-th equation, after the substitution $Y_i = y_i(t)$.

By Proposition 5.4, $k \in \{1, 2, \ldots, p - 3\} \cup \{p + 1, p + 2, \ldots, 2p - 5\}$. In order to compute the orders of $y_i(t)$, with $i < p - 1 - 2$, let $k \in \{p + 1, p + 2, \ldots, 2p - 5\}$, and write $k = 2p - 2 - \hat{k}$, $\hat{k} \in \{3, \ldots, p - 3\}$.

**Remark 8.13.** For any fixed $p$, the coefficients $\alpha_{p-1-\hat{k}, \hat{k}}$, for $\hat{k} \in \{3, \ldots, p - 3\}$, can be computed by taking into account the following constraints.

The expansion of (38) is of the form

$$
\sum_{j=1}^{p-1} \sum_{k_2+\cdots+k_{p-2}+1}^{k} \binom{k}{k_1, k_2, \ldots, k_{p-1-1}, l} \eta_{j-i}^{(2p-2)l} \prod_{i=2}^{p-2} \eta_{j-i}^{(i-1)k_i} t^{(p-1-i)k_i}.
$$

Here, $k_i \leq \hat{k}$ for terms of degree $\hat{k}$ in $t$. Moreover, since $k > p$ and

$$
\binom{k}{k_1, k_2, \ldots, k_{p-1-1}, l} = \frac{(k)!}{k_1!k_2!\cdots k_{2u-1}!!},
$$

we see that $l \geq p$ is a necessary condition in order to have a non-zero multinomial coefficient. Further, $l + \sum_{i=1}^{p-2} k_i = \hat{k}$, and each term of degree $\hat{k}$ corresponds to a choice of the indices such that $\sum (p-1-i)k_i = \hat{k}$.

Moreover, since for $u \neq 0$ (mod $p - 1$),

$$
\sum_{j=1}^{2u} \left( \eta_u^{j-1} \right) = \sum_{j=0}^{2u-1} \eta_u^j = \frac{\eta_u^{2u} - 1}{\eta_u - 1} = 0,
$$

every non-zero term must satisfy $\sum (i-1)k_i \equiv l$ (mod $p - 1$).

To illustrate Remark 8.13 we show that $\alpha_{p-1-3,3}$ is non-zero, whereas $\alpha_{2,p-1-2} = 0$.

- Let $\hat{k} = 3$, $k = 2p - 5$. In the $k$-th equation, the terms of degree $\hat{k}$ in $t$ are precisely the three terms corresponding to the choices $s = 1$, $i = p - 1 - 1$, $k_1 = 3$ and $l = 2p - 5 - 3$ (for $j \neq i$ it will be $k_j = 0$), or $s = 1$, $i = p - 1 - 1$, $k_1 = 1$ and $l = 2p - 5 - 1$ (for $j \neq i$, $k_j = 0$), and $s = 1$, $i = p - 1 - 1$, $k_1 = 1$, $i_2 = p - 1 - 2$, $k_{i_2} = 1$, $i_2 = 1$ and $l = 2p - 5 - 2$ (for $j \neq i$, $k_j = 0$).

$$
\binom{2p-5}{k_2, \ldots, k_{2u-1}, l} = \frac{(2p-5)!}{k_2!\cdots k_{2u-1}!!}
$$

Therefore, the term of degree 3 in the $(2p-5)$-th equation is

$$
2p-5 \left[ \binom{2p-5}{1, 1, 0, \ldots, 0, 2p-5-2} \alpha_{p-1-2,2} + \binom{2p-5}{3, 0, 0 \ldots, 0, 2p-5-3} + \binom{2p-5}{0, 0, 1, 0 \ldots, 0, 2p-5-1} \alpha_{p-1-3,3} \right] t^3 = \alpha_{p-1-2,2} \cdot (-5) \cdot (-6) + (-1)(-5)(-7) - 5\alpha_{p-1-3,3} t^3
$$

Since $\alpha_{p-3,3} = 2$, it follows $\alpha_{p-1-3,3} = 5 \neq 0$.

- Let $\hat{k} = p - 3$, $k = (p + 1)$. Observe that, in this case, the factors in the multinomial theorem are of the form $(k_1, k_2, \ldots, k_{2u-1})$ with $k_1 + k_2 + \cdots + k_{2u-1} + l = p + 1$. Also, the only non-zero coefficients are those with $k_i = p$ or $k_i = p + 1$ for some $i$. Moreover, for $u \neq 0$ (mod $p - 1$),

$$
\sum_{j=1}^{2u} \left( \eta_u^{j-1} \right) = \sum_{j=0}^{2u-1} \eta_u^j = \frac{\eta_u^{2u} - 1}{\eta_u - 1} = 0.
$$
Therefore, for \( k = p + 1 \), the possibly non-vanishing terms in equation (30), are those obtained for \( i + i = 2 \ (\mod \ 2u) \), taking \( \eta_{j-1}^{-1} y_i(t) \) with multiplicity \( p \) and \( \eta_{j-1}^{-1} y_i(t) \) with multiplicity 1 or taking \( \eta_{j-1}^{-1} y_i(t) \) with multiplicity 1 and \( \eta_{j-1}^{-1} y_i(t) \) with multiplicity \( p \), and those obtained for \( i = m + 1 \) and \( \eta_{j-1}^{-1} y_i(t) \) with multiplicity \( p + 1 \).

Therefore, the term of degree \( 2u - 2 \) in \( t \), can only be obtained by taking \( \eta_{j-1}^{-1} y_2(t) \) with multiplicity 1 and \( \eta_{j-1}^{-1} y_i(t) \) with multiplicity \( p \), namely it is \(-\alpha_{2,2u-2} t^{2u-2}\), and therefore \( \alpha_{2,2u-2} = 0 \). As a consequence, \( \text{ord}(y_2(t)) \geq 2p - 4 \).

**Proposition 8.14.** Each of the integers 1, 2, 3 are intersection multiplicities \( I(P, V \cap \pi) \) at any \( \mathbb{F}_p \)-rational point. Furthermore, the last order is at least \( 2p - 4 \).

8.5. **Case \( p = 7 \).** From Section 8.1, \( y_1(t) = 0 \), \( y_5(t) = t \), and \( \text{ord}(y_4(t)) = 2 \), with \( \alpha_{4,2} = 2 \), that is \( y_4(t) = 2 t^2 + \alpha_{4,4} t^4 + \cdots \). The second equation reads

\[-y_3^2 + 2 y_2 y_3 y_4 + 4 y_2^2 y_5 - y_5^2 + y_4 y_5 + 4 y_3 = 0;\]

whence \( \alpha_{3,3} = 5 \), that is \( y_3(t) = 5 t^3 + \alpha_{3,6} t^6 + \cdots \). The eighth equation reads

\[y_7^2 + y_2 + y_3 y_5 + y_3 y_7 + y_4^2 = 0.\]

Therefore it must be \( \text{ord}(y_2(t)) = 10 \).

Thus, the order sequence of the curve \( V \) at the origin is \((0, 1, 2, 3, 10)\).

8.6. **Case \( p = 11 \).** With the support of MAGMA the first terms of the branch expansions of the \( y_i \) can be computed.

\[
y_1(t) = 0; \quad y_2(t) = 7 t^{18} + \cdots; \\
y_3(t) = 5 t^7 + 6 t^{17} + \cdots; \\
y_4(t) = 3 t^6 + 2 t^{16} + \cdots; \\
y_5(t) = 9 t^5 + 4 t^{15} + \cdots; \\
y_6(t) = 3 t^4 + 0 t^{14} + \cdots; \\
y_7(t) = 5 t^3 + 6 t^{13} + \cdots; \\
y_8(t) = 2 t^2 + 4 t^{12} + \cdots; \\
y_9(t) = t.
\]

This shows that the order sequence of \( V \) at the origin is \((0, 1, 2, 3, 4, 5, 6, 7, 18)\).

9. **Maximality of the \( p \)-characteristic analog of the Bring curve for \( m = 5 \)**

10. **The case of positive characteristic; \( m = 5 \)**

In this section \( m = 5 \), that is, \( V \) is the \( p \)-characteristic analog of the Bring curve. Therefore, \( V \) has genus 4 and is embedded in \( \text{PG}(4, K) \) as the complete intersection of an hyperplane, a quadratic and a cubic surface, both non-singular. The (homogeneous) function field \( K(V) \) is \( F = K(x_1, x_2, x_3, x_4, x_5) \) with

\[
\begin{cases}
x_1 + x_2 + x_3 + x_4 + x_5 = 0; \\
x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = 0; \\
x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 = 0.
\end{cases}
\]

Our goal is to show that \( V \) is an \( \mathbb{F}_{p^2} \)-maximal curve, that is the number of points of \( V \) defined over \( \mathbb{F}_{p^2} \) attains the Hasse-Weil upper bond \( p^2 + 1 + 2 q p = p^2 + 1 + 8 p \) for infinitely many values of \( p \). The essential tool for the
proof is the Jacobian variety \( J_V \) associated with \( V \), with the following characterization of maximal curves due to Tate [34 Theorem 2(d)] and explicitly pointed out by Lachaud [23 Proposition 5]: a curve defined over \( \mathbb{F}_p \) of genus \( g \) is an \( \mathbb{F}_{p^2} \)-maximal curve if and only if its Jacobian is \( \mathbb{F}_{p^2} \)-isogenous to the \( g \)-th power of an \( \mathbb{F}_{p^2} \)-maximal elliptic curve. To determine \( J_V \) we use the following Kani-Rosen theorem [20 Theorem B] about the decomposition of the Jacobian variety of an algebraic curve with respect to an automorphism group \( G \) equipped by a partition, that is, the group \( G \) has a family of subgroups \( \{ H_1, \ldots, H_t \} \) such that \( G = H_1 \cup \cdots \cup H_t \) and \( H_i \cap H_j = \{ 1 \} \) for \( 1 \leq i < j \leq t \).

**Theorem 10.1** (Kani-Rosen). Let \( G \) be a finite automorphism group of an algebraic curve \( X \). If \( G \) is equipped by a partition, then the following isogeny relation holds:

\[
J_X^{1-1} \times J_{[G]} \sim J_{X/H_1}^{h_1} \times \cdots \times J_{X/H_t}^{h_t},
\]

where \( H_1, \ldots, H_t \) are the components of the partition and \( h_i = |H_i| \) for \( i = 1, \ldots, t \).

In fact, the Kani-Rosen theorem applies to \( G \) as \( G \cong \text{Sym}_5 \) and \( \text{Sym}_5 \cong \text{PGL}(2, 5) \) is equipped with a partition whose components form three conjugacy classes of lengths 15, 6, 10, namely those consisting of all cyclic subgroups of order 4, 5, and 6, respectively. Since Aut(\( V \)) acts on the set of five coordinates \( \{ X_1, \ldots, X_5 \} \), representatives of the conjugacy classes are: \( C_4 = \langle (X_1, X_2, X_3, X_4) \rangle \), \( C_6 = \langle (X_1, X_2, X_3, X_4, X_5) \rangle \), and \( C_8 = \langle (X_1, X_2, X_3)(X_4, X_5) \rangle \), respectively. In our case, since \( V/G \) is rational, Theorem 10.1 reads

\[
J_V^{30} \sim J_{V/C_4}^{30} \times J_{V/C_5}^{30} \times J_{V/C_6}^{30}
\]

Therefore, \( V \) is an \( \mathbb{F}_{p^2} \)-maximal curves if each \( J_{V/C_i} \), with \( i = 4, 5, 6 \) is either rational, or a \( \mathbb{F}_{p^2} \)-maximal elliptic curve. We show first that several quotient curves of \( V \) are rational.

**Proposition 10.2.** Each of the following quotient curves is a rational curve:

- \( V/C_5 \)
- \( V/G_8 \), where \( G_8 \) is a (dihedral) subgroup of \( G \) of order 8;
- \( V/G_{24} \), where \( G_{24} \) is a subgroup (isomorphic to \( \text{Sym}_4 \)) of \( G \) of order 24;
- \( V/G_{12} \), where \( G_{12} \) is a subgroup of \( G \) of order 12;
- \( V/G_{20} \), where \( G_{20} \) is a subgroup of \( G \) of order 20.

**Proof.** We apply the Riemann-Hurwitz formula to each of the groups \( C_5, G_8, G_{24}, \) and \( G_{12} \). For \( i \in \{5, 8, 12, 24\} \), let \( g_i \) denote the genus of the corresponding quotient curve. From Theorem 5.1 \( G \) acts on \( V \) with exactly 3 short orbits, namely \( \Omega_{\omega}, \Omega_{\epsilon}, \) and \( \Omega_{\theta} \), of length 24, 30 and 60 respectively. For \( C_5 \) the Riemann-Hurwitz formula reads

\[
6 = 10(\bar{g}_5 - 1) + \sum (5 - |\alpha_i|);
\]

with \( \alpha_i \) running over the set of short orbits of \( C_5 \). Since \( C_5 \) has at least four fixed points on \( \Omega_{\omega} \), it follows \( \bar{g}_5 = 0 \). Also, since a group of order 20 contains a subgroup of order 5, this implies \( g_{20} = 0 \). For \( G_8 \) the Riemann-Hurwitz formula reads

\[
6 = 16(\bar{g}_8 - 1) + \sum (8 - |\alpha_i|);
\]

with \( \alpha_i \) running over the set of short orbits of \( G_8 \). This implies \( \bar{g}_8 \leq 1 \). If equality holds then \( G_8 \) has a unique short orbit of length 2. On the other hand, since neither 30 nor 60 is divisible by 8, \( G_8 \) has a short orbit in both \( \Omega_{\epsilon} \) and \( \Omega_{\theta} \), a contradiction which implies \( \bar{g}_8 = 0 \). Finally, since \( \text{Sym}_4 \) contains a subgroup of order 8, \( g_{24} = 0 \) also holds. For \( G_{12} \), the Riemann-Hurwitz formula reads

\[
6 = 24(\bar{g}_{12} - 1) + \sum (12 - |\alpha_i|);
\]

with \( \alpha_i \) running over the set of short orbits of \( G_{12} \). This implies \( \bar{g}_{12} \leq 1 \). If equality holds then \( G_{12} \) has a unique short orbit of length 12, contained in \( \Omega_{\epsilon} \). From the orbit-stabilizer theorem follows that \( G_{12} \) contains an involution fixing a point in \( \Omega_{\epsilon} \). This implies that the involution must be the product of two transpositions, but it can be checked that the group \( G_{12} \) does not contains any such element. It follows \( g_{12} = 0 \). \( \square \)
Next we show for every \( p \geq 7 \) that \( J_V/C \), with \( i = 4, 6 \) is an elliptic curve, and that these two elliptic curves are pairwise isogenous over \( \mathbb{F}_p^2 \).

The above defined \( C_4 \) can be viewed as an automorphism group of \( F \) generated by the automorphism \((x_1, x_2, x_3, x_4, x_5) \mapsto (x_2, x_3, x_4, x_1, x_5)\). A Magma aided computation shows that each of following elements \( b, c, d, e \in L \) is left invariant by \( C_4 \):

\[
\begin{align*}
\text{b} &= \frac{-48x_2x_1^3x_3^3}{\text{Sym}^2 x_3^2} - \frac{48x_2x_1^3x_3^3}{\text{Sym}^2 x_3^2} - \frac{48x_2x_1^3x_3^3}{\text{Sym}^2 x_3^2} - \frac{48x_2x_1^3x_3^3}{\text{Sym}^2 x_3^2} - 24x_2x_1^3x_3^3 - 24x_2x_1^3x_3^3 - 24x_2x_1^3x_3^3 - 24x_2x_1^3x_3^3 - 108x_2x_1^3x_3^3 - 208/9x_2x_1^3x_3^3 - 28/9x_2x_1^3x_3^3 - 370/9x_2x_1^3x_3^3 - 668/9x_2x_1^3x_3^3 - 82/9x_2x_1^3x_3^3 - 1046/9x_1^3x_3^3 - 16/3x_2x_1^3x_3^3 - 104/9x_2x_1^3x_3^3 - 152/9x_2x_1^3x_3^3 - 44x_2x_1^3x_3^3 - 118/9x_2x_1^3x_3^3 - 730/9x_2x_1^3x_3^3 - 64/27x_2x_1^3x_3^3 - 8/3x_2x_1^3x_3^3 - 712/27x_2x_1^3x_3^3 - 92/27x_2x_1^3x_3^3 - 1306/27x_2x_1^3x_3^3 - 2128/243x_2x_1^3x_3^3 - 32/27x_2x_1^3x_3^3 - 5332/243x_2x_1^3x_3^3 - 1064/243x_2x_1^3x_3^3, \\
\text{c} &= -67/3x_2x_1^3x_3^3 + 54x_2x_1^3x_3^3 + 36x_2x_1^3x_3^3 + 18x_2x_1^3x_3^3 + 90x_2x_1^3x_3^3 / 27x_2x_1^3x_3^3 + 36x_2x_1^3x_3^3 + 144x_2x_1^3x_3^3 + 90x_2x_1^3x_3^3 + 45x_2x_1^3x_3^3 + 257/3x_2x_1^3x_3^3 + 90x_2x_1^3x_3^3 + 16x_2x_1^3x_3^3 + 154x_2x_1^3x_3^3 + 142/3x_2x_1^3x_3^3 + 50/3x_2x_1^3x_3^3 + 242x_2x_1^3x_3^3 + 299/3x_2x_1^3x_3^3 + 8/3x_2x_1^3x_3^3 + 209/3x_2x_1^3x_3^3 + 52/9x_2x_1^3x_3^3 - 110/9x_2x_1^3x_3^3 + 378/9x_2x_1^3x_3^3 + 139/3x_2x_1^3x_3^3 - 208/81x_2x_1^3x_3^3 + 532/81x_2x_1^3x_3^3 + 2260/81x_2x_1^3x_3^3 + 226/27x_2x_1^3x_3^3 + 2738/81x_2x_1^3x_3^3 + 4x_2x_1^3 + 208/81x_2x_1^3x_3^3 + 1460/81x_2x_1^3x_3^3 + 671/81x_2x_1^3x_3^3.
\end{align*}
\]

Moreover, let \( b = b/c, d = d/c \). From the above computation,

\[
135b_1^3 - 360b_1^2 + 240b_1 + 256 + 256d_1^2 = 0.
\]

Let \( F_1 \) be the subfield of \( F \) generated by \( b_1, d_1 \). Then \( F_1 \) is elliptic and the linear map \((b_1, d_1) \mapsto (x, y)\) with \( x = -256/135b_1, y = -65536/18225d_1 \), gives an equation

\[
y^2 = x^3 + 3^{11}3^{-4}5^{-1}2^2 + 2^{20}3^{-8}5^{-2}2 - 3^{32}3^{-12}5^{-4}
\]

for \( F_1 \). Furthermore, \( F_1 \) is the fixed field \( F^{C_4} \) of \( C_4 \). Indeed, since both \( b_1 \) and \( d_1 \) are fixed by \( C_4 \), \( F_1 \subseteq F^{C_4} \) holds. On the other hand, if equality does not hold then Galois theory yields that \( F_1 \) is the fixed field of a subgroup \( N \) of \( G \) strictly containing \( C_4 \). Since \( C_4 \) is cyclic and \( G \cong \text{Sym}_5 \), this yields that the order of \( N \) is either 8, 12, 20 or 24. But then \( V/N \) is rational by Proposition 11.2. Therefore, \( F_1 \) is \( F^{C_4} \).

The quotient curve \( V/C_6 \) can be investigated in a similar way. The subfield \( F^{C_6} \) of \( F \) is generated by \( A, B \) with

\[
5585034240000A^4 + 2322572688000AB + 2789729451000B^2 + 795273845000A^3B + 105608214000B^3 + 136633856000A^2B^2 + 287556736000A^3B + 684913664000B^3 + 1176764416000B^2 = 0.
\]

The birational map

\[
(A, B) \mapsto (2193^{-6}5^{-2}AB + 2^{20}3^{-6}5^{-2}B^2, 2^{23}3^{-7}2 \cdot 3^{-12}5^{-4}A^2 + 2^{30}3^{-3}2 \cdot 3^{-12}5^{-4}AB + 2^{29}149 \cdot 3^{-12}5^{-4}B^2 + 2^{38}3^{-12}5^{-4}B, -A^2 - 4AB - 4B^2),
\]

is a birational isomorphism over \( \mathbb{F}_p \) to the elliptic curve \( E_2 \) with equation

\[
y^2 = x^3 - 2^{20}3^{-8}5^{-2}71x^2 + 2^{-43}3^{-16}5^{-4}11x^2 - 2^{64}23 \cdot 3^{-24}5^{-6}.
\]

Since, by Proposition 11.2, the function field of the quotient curve of any subgroup of \( G \) properly containing \( C_6 \) is rational, it follows that \( K(A, B) = K(x_2, y_2) \) is the function field of \( V/C_6 \).
Furthermore, the elliptic curves $E_1$ and $E_2$ are isogenous over $\mathbb{F}_p$ via the isogeny
\[(x, y) \mapsto ((210^3-4^3 \cdot x^3 + 220 \cdot 17 \cdot 3^3-8^3 \cdot x^2 + 230 \cdot 11 \cdot 5^3 \cdot x + 94011 \cdot 3^3-16^5-4^4) \\
/(x^4 - 21 \cdot 3^3-8^3 \cdot x^2 + 220 \cdot 3^3-8^3-2^2 \cdot x^2 - 230 \cdot 3^3-16^5-2^2 \cdot y - \\
230 \cdot 3^3 \cdot 3^3 \cdot 18^5 \cdot y)/(x^3 - 210^3-3^3 \cdot 5^4 \cdot x^2 + 220 \cdot 3 \cdot 8^3 \cdot 2^2 \cdot x - 230 \cdot 3^3 \cdot 12^5-3^3)).\]

Observe that, since $p \geq 7$ the denominators do not vanish.

Summing up, the following theorem holds.

**Theorem 10.3.** For $p \geq 7$, the Jacobian variety $J_V$ of $V$ has a decomposition over $\mathbb{F}_p$ of the form $J_V \sim E^4$ where $E = E_1$ is the elliptic curve of Weierstrass equation
\[y^2 = x^3 + 2^1 \cdot 3 \cdot 45 \cdot 2 \cdot 5 - x^2 + 2^3 \cdot 20 \cdot 3 \cdot 8 \cdot 5 \cdot 2^2 - 2^2 \cdot 3 \cdot 3 \cdot 5 \cdot 2 \cdot y - \\
2 \cdot 3 \cdot 5 \cdot 3 \cdot 3 \cdot 18 \cdot 5 \cdot y)/(x^3 - 2 \cdot 10 \cdot 3 \cdot 3 \cdot 5 \cdot 4 \cdot 1 \cdot 2 \cdot 5 \cdot x^2 + 2 \cdot 3 \cdot 3 \cdot 5 \cdot 2 \cdot 2^2 \cdot x - 2^2 \cdot 3 \cdot 12 \cdot 2^5 - 3^3)).\]

Since $E$ is maximal over $\mathbb{F}_p$, for infinitely many primes $p$, Theorem 10.3 has the following corollary.

**Corollary 10.4.** $V$ is a $\mathbb{F}_p^\times$-maximal curve for infinitely many primes $p$.

**Remark 10.5.** The primes $p \leq 10000$ such that $V$ is $\mathbb{F}_p$-maximal are
\[p = 29, 59, 149, 239, 269, 839, 1439, 1559, 2789, 2909, 4079, 4799, 5519, 6959, 8069, 8819, 9479, 9749.\]

11. **Connections with classical results**

11.1. **Connection with Rédei’s work on the Minkowski conjecture.** From [33, Theorem 2.1] and [24, Lemma 6.1], every solution $(\xi_1, \ldots, \xi_p)$ with $\xi_i \in \mathbb{F}_p$ also satisfies the diagonal equations $X_1^k + X_2^k + \ldots + X_p^k = 0$ for $k = \frac{1}{2}(p + 1), \ldots, p - 3$.

Now, let $W$ be the algebraic variety of PG($p - 1, \mathbb{K}$) associated with the system
\[
\begin{align*}
X_1 + X_2 + \ldots + X_p &= 0; \\
X_2^2 + X_3^2 + \ldots + X_p^2 &= 0; \\
& \quad \vdots \\
X_p^{p-3} + X_p^{p-3} + \ldots + X_p^{p-3} &= 0.
\end{align*}
\]

of diagonal equations. Clearly $E = (1 : 1 : \cdots : 1)$ is a point of $W$. Furthermore, any $\ell$ line through $E$ and another point $P \in W$ is entirely contained in $W$. In fact, if $P = (a_1 : \cdots : a_p)$ then the points on $\ell$ distinct from $E$ are $Q = (\lambda + a_1 : \cdots : \lambda + a_p)$ with $\lambda \in \mathbb{K}$, and a straightforward computation, $(\lambda + a_1, \ldots, \lambda + a_p)$ is also a solution of (37). Since the hyperplane II of equation $X_p = 0$ does not contain $E$, the algebraic variety cut out on $W$ by II is associated with (1) for $m = p - 1$. Since this variety is $V$, Theorem 8.1 and Lemma 3.2 show that the points of $W$ over $\mathbb{F}_p$ are $E$ together with the points $(\xi_1 : \cdots : \xi_p)$ such that $[\xi_1, \ldots, \xi_p]$ is a permutation of the elements of $\mathbb{F}_p$. This gives a geometric interpretation for the result of Rédei [30] and of Wang, Panico and Szabó [30] reported in the Introduction.

11.2. **Connection with classical geometry via Serre’s work.** Let $\mathbb{K}(V)$ be the function field of $V$. Then $\mathbb{K}(V) = \mathbb{K}(x_1, \ldots, x_m)$ where $(x_1, \ldots, x_m)$ is a solution of (11), or equivalently of (13). Let $s := \sigma_{m-1}(x_1, \ldots, x_m)$ and $u := \sigma_m(x_1, \ldots, x_m)$. Then $x_1, \ldots, x_m$ are the roots of the polynomial $F(Y) = Y^m + (-1)^{m-1} s Y + (-1)^m u$. Replacing $Y$ in $F$ by $u/s Z$ gives $G(Z) = Z^m - Z^{m-1} - v$ with $v = u^{m-1}/s^m$. Therefore, $\mathbb{K}(V)$ is the Galois closure of the polynomial $Z^m - Z^{m-1} - v$. As Serre [31] Chapter 4 pointed out in zero characteristic, $G(Z)$ has a cycle of order $m$ at $\infty$, another of order $m - 1$ at 0, and a transposition at 1–1/m, and hence it has ramification type $(m, m - 1, 2)$. This holds true in our case, as $p > m$. Furthermore, using Serre’s observation together with some classical results on Galois extensions one can show that $V$ has the properties shown in Theorem 4.10 and in Lemmas 4.14 see [31, Section 4.4]. Concerning the action of $\text{Sym}_m$ on $V$, Lemma 4.14 can also be proven by using Serre’s observation together with (37). However, the study of $\text{Aut}(V)$ appears to require much more knowledge about the geometry of $V$ and from group theory; see the proofs of Theorems 7.1 and 7.2.
Acknowledgements

This research was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The research of M. Timpanella was funded by the Irish Research Council, grant n. GOIPD/2021/93.

References

[1] S.H. Alavi, T.C. Burness, Large subgroups of simple groups J. Algebra 421 (2015), 187-233.
[2] R. Auffarth, S. Rahausen, Galois subspaces for the rational normal curve, Comm. Algebra 49 (2021), 3635-3644.
[3] D. Bartoli, M. Giulietti, M.Q. Kawakita, M. Montanucci, New examples of maximal curves with low genus, Finite Fields Appl. 68 (2020), article 101744.
[4] H.W. Braden, T.P. Northover, Timothy P. Bring’s curve: its period matrix and the vector of Riemann constants, SIGMA Symmetry Integrability Geom. Methods Appl. 8 (2012), Paper 065, 20 pp.
[5] Ri-Xiang Chen, On two classes of regular sequences, J. Commut. Algebra 8 (2016), 29-42.
[6] W. Burnside, Theory of groups of finite order, second edition, Cambridge University Press, 2013.
[7] A. Conca, C. Krattenthaler, J. Watanabe, Regular sequences of symmetric polynomials, Rend. Semin. Mat. Univ. Padova 121 (2009), 179-199.
[8] J.D. Dixon, B. Mortimer, Permutation Groups, Springer, 1996.
[9] N.D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over \( \mathbb{Q} \), Invent. Math. 89, 561–567 (1987).
[10] R. Dvornicich, U. Zannier, Newton functions generating symmetric fields and irreducibility of Schur polynomials, Adv. Math. 222 (2009), 1982-2003.
[11] R. Fröberg, B. Shapiro, On Vandermonde varieties, Math. Scand. 119 (2016), 73-91.
[12] S. Fukasawa, Galois lines for the Artin-Schreier-Mumford curve, Comm. Algebra 49 (2021), 3635-3644.
[13] K. Higashine, A criterion for the existence of a plane model with two inner Galois points for algebraic curves, Hiroshima Math. J. 51 (2021), 163-176.
[14] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, Algebraic Curves Over a Finite Field, Princeton Univ. Press, Princeton and Oxford, 2008.
[15] M. Giulietti, M.Q. Kawakita, S. Lia, M. Montanucci, An \( \mathbb{F}_p^2 \)-maximal Wiman’s sextic and its automorphisms, Adv. Geom. arXiv:1805.06317
[16] M. Giulietti, G. Korchmáros, M. Montanucci, Maximal Curves over Finite Fields, Past, Present and Future, in Proc. of the international conference Curves over finite fields, Past, Present and Future dedicated to J.P. Serre, pg.30, 2021.
[17] R. M. Guralnick, Subgroups of prime power index in a simple group, J. Algebra 81 (1983), 304-311.
[18] E. Kani, M. Rosen, Idempotent relations and factors of Jacobians, Math. Ann. 284 (1989) 307–327.
[19] G. Korchmáros, S. Lia, M. Timpanella, Curves with more than one inner Galois point, J. Algebra, 566 (2021), 374-404.
[20] G. Korchmáros, S. Lia, M. Timpanella, A generalization of Bring’s curve in any characteristic, preliminary version.
[21] G. Lachaud, Sommes d’ Eisenstein et nombre de points de certaines courbes algébriques sur les corps fins, C.R. Acad. Sci. Paris, Sér. I 305 (1987) 729-732.
[22] R. Lidl -H. Niederreiter, Basic Algebraic Geometry 1: Varieties in Projective Space, Springer, Heidelberg, third edition, 2013.
[23] H. Melanová, B. Sturmfels, R. Winter, Recovery from Power Sums, arXiv:2106.13981v1 [math.AG] 26 Jun 2021.
[24] A. Seidenberg, Elements of the theory of algebraic curves, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1968
[25] I. R. Shafarevich, Basic Algebraic Geometry 1: Varieties in Projective Space, Springer, Heidelberg, third edition, 2013.
[26] E. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funkti onenkörper von Primzahl- charakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe, Arch. Math. 24 (1973), 527–544.
[27] L. Rédei, Lacunary Polynomials over Finite Fields, North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., Inc., New York, 1973.
[28] J.P. Serre, Topics in Galois Theory (Research Notes in Mathematics) 2nd Edition. Taylor and Francis, 2008.
[29] J.P. Serre, Rational points on curves over finite fields, handwritten notes of Serre’s Harward course 1985 by F. Gouvea, published in Documents Mathématiques (Paris) 18, Société Mathématique de France, Paris, 2020 with contributions of E. Howe, J. Oesterlé and C. Ritzenthaler.
[30] K.O. Stöhr, J.F. Voloch, Weierstrass points and curves over finite fields, Proc. Lond. Math. Soc. 52 (1986), 1-19.
[34] J. Tate, Endomorphisms of Abelian varieties over finite fields, Invent. Math. 2 (1966), 134–144.

[35] W. Vogel, Lectures on results on Bézout’s Theorem. Lecture Notes, Tata Institute of Fundamental Research of Bombay. (Notes by D. P. Patil). Berlin-Heidelberg-New York, Springer. 1984 I, No. 74.

[36] F. Rodriguez Villegas, F. Voloch, D. Zagier, Constructions of plane curves with many points, Acta Arith. 99, 85–96 (2001).

[37] B.L. van der Waerden, Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen, Math. Zeitschrift 111, 731-733.

[38] C. Ward, V.D. Panico, S. Szabó, Elementary proofs of two results of Rédei, J. Algebra Comput. Appl. 2 (2012), 1-6.

[39] A. Wagner, Groups generated by elations, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 41, 1974, 190-205.

[40] R.A. Wilson, The Finite Simple Groups, Springer Verlag 2009.

[41] A.E. Zalesskii, V.N. Serežkin, Finite linear groups generated by reflections, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 44 (1980), 1279-1307, translated in Math. USSR. Izvestijia 17 (1981), 477-503.

Gábor Korchmáros, Dipartimento di Matematica, Informatica ed Economia Università degli Studi della Basilicata. Email address: gabor.korchmaros@unibas.it

Stefano Lia, School of Mathematics and Statistics, University College Dublin, Belfield, Ireland. Email address: stefano.lia@ucd.ie

Marco Timpanella, Dipartimento di Matematica e Informatica, Università di Perugia. Email address: marco.timpanella@unipg.it