Albanian Journal of Mathematics

Për një Shqipëri të shkencës dhe kulturës.

Volume 8, 2014

www.albanian-j-math.com

ALBANIAN JOURNAL OF MATHEMATICS
Volume 8, Number 1, Pages 3–8
ISSN: 1930-1235; (**2014**)

EQUATIONS FOR SUPERELLIPTIC CURVES OVER THEIR MINIMAL FIELD OF DEFINITION

Lubjana Beshaj
Department of Mathematics and Statistics
Oakland University
Rochester, MI, 48386.
Email: beshaj@oakland.edu

Fred Thompson
Department of Mathematics and Statistics
Oakland University
Rochester, MI, 48386.
Email: fjthomps@oakland.edu

Abstract. Let $\mathcal{X}_g$ be a genus $g \geq 2$ superelliptic curve, F its field of moduli, and K the minimal field of definition. In this short note we construct an equation of the curve $\mathcal{X}_g$ over its minimal field of definition K when $\mathcal{X}_g$ has extra automorphisms. We make use of the dihedral invariants of superelliptic curves as defined by Shaska in [6] and results on the automorphism groups of superelliptic curves as in [10].

1. Introduction

Given an algebraic curve $\mathcal{X}$ of genus $g \geq 2$, it is an open problem to determine an equation for $\mathcal{X}$ over its minimal field of definition K. It is well known that the minimal field of definition is an algebraic extension of the field of moduli F. While for small genus it is known how to construct such equations, in general this is still an open problem. The overall strategy is to describe the point in the moduli space $\mathcal{M}_g$ corresponding to the given curve. This determines the field of moduli F and the minimal field of definition K is a finite extension of the field of moduli.

1991 *Mathematics Subject Classification.* 11G30 and 11G50 and 14G40.

Key words and phrases. genus 3 hyperelliptic curves and dihedral invariants and absolute invariants .

However, describing the moduli point explicitly can be done only for superelliptic curves of small genus; see [1–3].

Superelliptic curves are curves with affine equation $y^n = f(x)$. Such curves have at least an automorphism of order n. The quotient by the automorphism group of such curves is a genus 0 curve, hence a conic. This conic always has a rational point over a quadratic extension of the field of moduli. Hence, for superelliptic curves $[K : F] \leq 2$. If the automorphism group of $\mathcal{X}$ is isomorphic to the cyclic group of order n then an idea of Clebsch can be extended to determine if the field of moduli is a field of definition. Moreover an equation can be determined over the minimal field of definition. This is intended in [5].

When the superelliptic curves have extra automorphisms, i.e. the automorphism group has size $> n$ then the algorithm suggested above does not work. The isomorphism classes of such curves are determined by dihedral invariants (or Shaska invariants) as in [4, 8, 9].

In this short note we give an equation of superelliptic curves of genus $g \geq 2$ with extra automorphisms over the minimal field of definition K and determine the algebraic conditions in terms of such invariants of curves when the field of moduli is a field of definition.

Our main result is the following. Let $\mathcal{X}$ be a genus $g \geq 2$ superelliptic curve, defined over $\mathbb{C}$, with an extra automorphism, $\mathfrak{s}_1, \dots, \mathfrak{s}_g$ its dihedral invariants, F the field of moduli, and K its minimal field of definition. Then,

i) The minimal field of definition K is $K = F(\sqrt{\Delta_\mathfrak{s}})$
ii) The equation of $\mathcal{X}$ over K is

$$y^n = A\, x^{\delta(s+1)} + A\, x^{\delta s} + \sum_{i=1}^{s-1} 2^{s-i}\, \mathfrak{s}_1 \cdot \frac{\mathfrak{s}_s^i \mathfrak{s}_i - A\mathfrak{s}_{s+1-i}}{2^s \mathfrak{s}_1^2 - \mathfrak{s}_s^{s+1}} \cdot x^{\delta \cdot i} + 1$$

where

$$2^{s+1} A^2 - 2^{s+1} \mathfrak{s}_1 A + \mathfrak{s}_s^{s+1} = 0.$$

and $\Delta_\mathfrak{s}$ is the discriminant of the above quadratic,

$$\Delta_\mathfrak{s} = 2^{s+1} \left(2^{s+1} \mathfrak{s}_1^2 - 4 \mathfrak{s}_s^{s+1} \right).$$

Hence, this provides an Weierstrass equation of the curve over $k(\sqrt{\Delta_\mathfrak{s}})$.

An immediate consequence of the above result is that the field of moduli is a field of definition when the above quadratic has rational solutions. This happens if and only if Δ_s is a complete square.

It was noted in [9] that when Δ_s the automorphism group of the curve is larger and can be explicitly determined. The case when the genus g is odd differs from the case when it is even. As a corollary we get that if $\Delta_s = 0$ then the field of moduli is a field of definition as noted in [9] for hyperelliptic curves.

The results of this paper determine when the field of moduli is a field of definition and give an equation of the curve over the minimal field of definition for almost all superelliptic curves with extra automorphism. The next natural thing to study is the case of the generic superelliptic curve, that is the curves with equation $y^n = f(x)$ and automorphism group of order $n > 2$. Such algorithm is given in [7] for genus $g = 2$ and it is intended in [5] for all superelliptic curves.

2. Preliminaries

Let $\mathcal{X}_g$ be a genus $g \geq 2$ curve with full automorphism group $G = Aut(\mathcal{X}_g)$. The curve $\mathcal{X}_g$ is called a **superelliptic curve** if there exists an element $\tau \in G$ which is central in G and $g(\mathcal{X}_g/\langle\tau\rangle) = 0$. Denote by H the cyclic group generated by τ, $H = \langle\tau\rangle$. Thus, $\overline{G} = G/H$ is called the reduced automorphism group of $\mathcal{X}_g$ with respect to H.

Superelliptic curves are curves with affine equation $y^n = f(x)$. Denote with $K = k(x, y)$ the function field of $\mathcal{X}_g$ and by $k(x)$ the genus zero subfield of K fixed by H. Then, $[K : k(x)] = n$, where $n = |H|$. The group $\overline{G}$ is a subgroup of the group of automorphisms of a genus zero curve. Therefore, $\overline{G} < PGL_2(k)$ and $\overline{G}$ is finite. Then, $\overline{G}$ is isomorphic to one of the following groups C_m, D_m, A_4, S_4, A_5. Since G is a degree n extension of $\overline{G}$ and we know the possible groups that occur as $\overline{G}$, it is possible to determine G and the equation of K, see [10].

The group G acts on $k(x)$ via the natural way. The fixed field of this action is a genus 0 field, say $k(z)$. Thus, z is a degree $|G|$ rational function in x, say $z = \phi(x)$.

Given a superelliptic curve $\mathcal{X}_g$ with equation $y^n = f(x)$ such that $\Delta(f, x) \neq 0$, the genus of the curve can be calculated using the following formula

$$g = 1 + \frac{1}{2}\left(nd - n - d - \gcd(d, n)\right).$$

where $\deg f = d > n$. If d and n are relatively prime then $g = \frac{(n-1)(d-1)}{2}$, see [11] for proof.

Much interesting to us are superelliptic curves with extra automorphism. Let $\mathcal{X}_g$ be a superelliptic curve that has an extra automorphism $\sigma \in G$ such that its projection $\overline{\sigma} \in \overline{G}$ has order $\delta \geq 2$. Then the equation of the superelliptic curve is given as $y^n = g(x^\delta)$ or $y^n = xg(x^\delta)$, for some $g \in k[x]$, see [4] for proof. In other words $\mathcal{X}_g$ has equation

$$y^n = g(x^\delta) := x^{s\delta} + a_{s-1}x^{(s-1)\delta} + \cdots + a_1x^\delta + 1,$$

or

$$y^n = xg(x^\delta) := x^{(s+1)\delta} + a_sx^{s\delta} + \cdots + a_1x^\delta + x.$$

For both cases the dihedral invariants of such curves or *Shaska-invariants* denoted by $\mathfrak{s}$-invariants are defined in [6, 8, 9]. They were discovered by Shaska in his thesis for curves of genus 2 with extra automorphisms and later generalized to all hyperelliptic curves in [9] for all hyperelliptic curves with extra automorphisms. Such invariants are used by many authors in computational aspects of hyperelliptic and superelliptic curves such as Duursma, Ritzenthaler, Lauter, Lercier, et al. We define them for our purposes in the next section.

3. Equation of superelliptic curves and dihedral invariants

Let $\mathcal{X}_g$ be a superelliptic curve defined over a field k, char$k = 0$ such that $\mathcal{X}_g$ has an extra involution and its Weierstrass equation is given by

$$y^n = x^{\delta(s+1)} + a_sx^{\delta s} + a_{s-1}x^{\delta(s-1)} + \cdots + a_2x^{\delta\cdot 2} + a_1x^\delta + 1 \tag{1}$$

Our main goal is to find an equation of this curve defined over its minimal field of definition. The corresponding moduli point of such curves is determined by the dihedral invariants $\mathfrak{s}_1, \ldots, \mathfrak{s}_s$ and the field of moduli is $k(\mathfrak{s}_1, \ldots, \mathfrak{s}_s)$.

Recall that the dihedral invariants are defined as follows

$$\begin{aligned}
\mathfrak{s}_1 &= a_1^{s+1} + a_s^{s+1}\\
\mathfrak{s}_2 &= a_1^{s-1}a_2 + a_s^{s-1}a_{s-1}\\
&\dots\\
\mathfrak{s}_i &= a_1^{s+1-i}a_i + a_s^{s+1-i}a_{s+1-i}\\
&\dots\\
\mathfrak{s}_{s+1-i} &= a_1^{i}a_{s+1-i} + a_s^{i}a_i\\
&\dots\\
\mathfrak{s}_{s-1} &= a_1^{2}a_{s-1} + a_s^{2}a_2\\
\mathfrak{s}_s &= 2a_1a_s
\end{aligned}$$

Notice that these invariants are homogenous polynomials of degree $s+1$ to 2 respectively. The field of moduli of the corresponding curve is given by $k(\mathfrak{s}_1, \dots, \mathfrak{s}_s)$. Our goal is to find a Weierstrass equation over $k(\mathfrak{s}_1, \dots, \mathfrak{s}_s)$ of the curve in Eq. (1).

We perform a coordinate change

$$x \to \sqrt[\delta]{a_s}\, x$$

to get

$$y^n = a_s^{s+1}\, x^{\delta(s+1)} + a_s^{s+1}\, x^{\delta s} + a_{s-1}\cdot a_s^{s-1}\, x^{\delta(s-1)} + \dots + a_2 \cdot a_s^2\, x^{\delta\cdot 2} + a_1 a_s\, x^{\delta} + 1$$

Denote by $A := a_s^{s+1}$. Then we have

$$2^{s+1}A^2 - 2^{s+1}\mathfrak{s}_1 A + \mathfrak{s}_s^{s+1} = 0.$$

This quadratic has discriminant

$$\Delta_{\mathfrak{s}} = 2^{s+1}\left(2^{s+1}\mathfrak{s}_1^2 - 4\mathfrak{s}_s^{s+1}\right)$$

The equation of the curve becomes

$$y^n = A\, x^{\delta(s+1)} + A\, x^{\delta s} + \sum_{i=1}^{s-1} a_i a_s^i \cdot x^{\delta\cdot i} + 1$$

We will show that all coefficients $a_i a_s^i$, $i = 1, \dots, s-1$, can be expressed in terms of the dihedral invariants and A. Hence, we have an equation of the curve over the quadratic extension $k\sqrt{\Delta_{\mathfrak{s}}}$.

Theorem 1. *Let $\mathcal{X}$ be a genus $g \geq 2$ superelliptic curve, defined over $\mathbb{C}$, with an extra automorphism, $\mathfrak{s}_1, \dots, \mathfrak{s}_g$ its dihedral invariants, F the field of moduli, and K its minimal field of definition. Then, the following are true*

i) The minimal field of definition K is $K = F(\sqrt{\Delta_{\mathfrak{s}}})$
ii) The equation of $\mathcal{X}$ over K is

$$y^n = A\, x^{\delta(s+1)} + A\, x^{\delta s} + \sum_{i=1}^{s-1} 2^{s-i}\, \mathfrak{s}_1 \cdot \frac{\mathfrak{s}_s^i \mathfrak{s}_i - A\mathfrak{s}_{s+1-i}}{2^s\mathfrak{s}_1^2 - \mathfrak{s}_s^{s+1}} \cdot x^{\delta\cdot i} + 1 \tag{2}$$

where

$$2^{s+1}A^2 - 2^{s+1}\mathfrak{s}_1 A + \mathfrak{s}_s^{s+1} = 0.$$

Proof. Part i) is an immediate consequences of the above. To prove part ii) we have to express the coefficients $a_i a_s^i$ of $x^{\delta \cdot i}$, $i = 2, \dots, s-1$, in terms of $\mathfrak{s}_1, \dots, \mathfrak{s}_s$. From the definitions of $\mathfrak{s}_i$ we get the following equations:

$$\begin{cases} \mathfrak{s}_1 = a_1^{s+1} + a_s^{s+1} \\ \mathfrak{s}_s = 2 a_1 a_s \\ \mathfrak{s}_i = a_1^{s+1-i} a_i + a_s^{s+1-i} a_{s+1-i} \\ \mathfrak{s}_{s+1-i} = a_1^i a_{s+1-i} + a_s^i a_i \\ A = a_s^{s+1} \end{cases}$$

We multiply both sides in the definition of $\mathfrak{s}_i$ by $a_s^i a_1^i = \left(\frac{\mathfrak{s}_s}{2}\right)^i$ and have

$$\left(\frac{\mathfrak{s}_s}{2}\right)^i \mathfrak{s}_i = a_1^{s+1} \cdot a_i \cdot a_s^i + a_s^{s+1} \cdot a_1^i \cdot a_{s+1-i} \tag{3}$$

From the definition of $\mathfrak{s}_{s+1-i}$ we have

$$a_1^i a_{s+1-i} = \mathfrak{s}_{s+1-i} - a_i a_s^i,$$

which we substitute in the Eq. (3). Hence,

$$\boxed{a_i a_s^i = \frac{1}{a_1^{s+1} - a_s^{s+1}} \left(\frac{\mathfrak{s}_s^i}{2^i} \mathfrak{s}_i - A\, \mathfrak{s}_{s+1-i} \right)}$$

Denote by $B := a_1^{s+1} - a_s^{s+1}$. Notice that

$$\begin{aligned} \left(a_1^{s+1} - a_s^{s+1}\right)\left(a_1^{s+1} + a_s^{s+1}\right) &= a_1^{2(s+1)} - a_s^{2(s+1)} \\ &= a_1^{2(s+1)} + 2\left(a_1 a_s\right)^{s+1} + a_s^{2(s+1)} - 2\left(a_1 a_s\right)^{s+1} \\ &= \left(a_1^{s+1} + a_s^{s+1}\right)^2 - 2\left(\frac{\mathfrak{s}_s}{2}\right)^{s+1} \\ &= \mathfrak{s}_1^2 - \frac{1}{2^s}\, \mathfrak{s}_s^{s+1} \end{aligned}$$

Hence, $B\mathfrak{s}_1 = \mathfrak{s}_1^2 - \frac{1}{2^s}\, \mathfrak{s}_s^{s+1}$ and

$$B = \mathfrak{s}_1 - \frac{1}{2^s} \frac{\mathfrak{s}_s^{s+1}}{\mathfrak{s}_1},$$

provided that $\mathfrak{s}_1 \neq 0$.

Hence,

$$a_i a_s^i = 2^{s-i}\, \mathfrak{s}_1 \cdot \frac{\mathfrak{s}_s^i \mathfrak{s}_i - A \mathfrak{s}_{s+1-i}}{2^s \mathfrak{s}_1^2 - \mathfrak{s}_s^{s+1}}$$

as claimed. This completes the proof. □

The natural question is for what values of $\mathfrak{s}_1, \dots, \mathfrak{s}_s$ is

$$\Delta_{\mathfrak{s}} = 2^{s+1}\left(2^{s+1}\mathfrak{s}_1^2 - 4\mathfrak{s}_s^{s+1}\right)$$

a complete square in K. In this case the field of moduli would be equal to the field of definition.

Albanian J. Math. **8** (2014), no. 1, 3-8.

References

[1] T. Shaska, *Some Remarks on the Hyperelliptic Moduli of Genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130.

[2] T. Shaska and F. Thompson, *Bielliptic curves of genus 3 in the hyperelliptic moduli*, Appl. Algebra Engrg. Comm. Comput. **24** (2013), no. 5, 387–412.

[3] T. Shaska, L. Beshaj, and Shor. C., *On Jacobian of curves with superelliptic components*, Contemporary Math. (to appear).

[4] Lubjana Beshaj, Valmira Hoxha, and Tony Shaska, *On superelliptic curves of level n and their quotients, I*, Albanian J. Math. **5** (2011), no. 3, 115–137.

[5] Tony Shaska and Fred Thompson, *Equations over the minimal field of definition for superelliptic curves, II*, work in progress.

[6] Tanush Shaska, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2003, pp. 248–254 (electronic), DOI 10.1145/860854.860904. MR2035219 (2005c:14037)

[7] Jean-Fran**c**cois Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334 (French). MR1106431 (92g:14022)

[8] Jannis A. Antoniadis and Aristides Kontogeorgis, *On cyclic covers of the projective line*, Manuscripta Math. **121** (2006), no. 1, 105–130.

[9] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115.

[10] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213.

[11] Christopher Towse, *Weierstrass weights of fixed points of an involution*, Math. Proc. Cambridge Philos. Soc. **122** (1997), no. 3, 385–392, DOI 10.1017/S0305004197001837. MR1466643 (98i:14033)

ALBANIAN JOURNAL OF MATHEMATICS
Volume 8, Number 1, Pages 9–21
ISSN: 1930-1235; (**2014**)

SYMMETRIC TENSOR RANK AND THE IDENTIFICATION OF A POINT USING LINEAR SPANS OF AN EMBEDDED VARIETY

Edoardo Ballico
Department of Mathematics
University of Trento
38123 Povo (TN), Italy
Email: ballico@science.unitn.it

Abstract. Let $X \subset \mathbb{P}^n$ be an integral and non-degenerate variety. Fix $P \in \mathbb{P}^n$. In this paper we discuss the minimal integer $\sum_{i=1}^{k} \sharp(S_i)$ such that $S_i \subset X$ and $\{P\} = \cap_{i=1}^{k}\langle S_i\rangle$, where $\langle\ \rangle$ denote the linear span (in positive characteristic sometimes this integer is $+\infty$). We use tools introduced for the study of the X-rank of P. Our main results are when X is a Veronese embedding of $\mathbb{P}^m$ (it is related to the symmetric tensor rank of P) or when X is a curve.

1. Introduction

Let $X \subseteq \mathbb{P}^n$ be an integral and non-degenerate variety defined over an algebraically closed field $\mathbb{K}$. For any $P \in \mathbb{P}^n$ the X-rank $r_X(P)$ of P is the minimal cardinality of a finite set $S \subset X$ such that $P \in \langle S\rangle$, where $\langle\ \rangle$ denote the linear span. Let $ir_X(P)$ be the minimal integer s such that there are finite sets $S_i \subset X$, $i \geq 1$, such that $\sharp(S_i) \leq s$ for all i and $\{P\} = \cap_{i\geq 1}\langle S_i\rangle$. We prove that $ir_X(P) < +\infty$ if $\mathrm{char}(\mathbb{K}) = 0$ (Proposition 3), but we show that in positive characteristic this is not true in a few cases (Proposition 3). We call $ir_X(P)$ the *identification rank* of P with respect to X or the *X-identification rank* of P. Let $\alpha(X,P)$ be the minimal integer x such that there are finitely many finite sets $S_i \subset X$, say $S_1,\dots,S_k$, such that $\{P\} = \cap_{i=1}^{k}\langle S_i\rangle$ and $\sum_{i=1}^{k}\sharp(S_i) = x$ (we don't fix the integer k and we don't assume that the sets S_i are disjoint, although the last condition is always satisfied if $k = 2$). The integer $\alpha(X,P)$ is the minimal number of points of X needed to identify P among all the points of $\mathbb{P}^n$ using only the operations of linear algebra: first taking several linear spans of points of X and then taking the intersection of these linear subspaces. It is the analogous in projective geometry of the minimal number of photos needed to identify a point of $\mathbb{R}^3$. With a smaller number of points we may only identify a linear subspace, L, containing P, but we cannot distinguish P from the other points of $\mathbb{P}^n$. One could allow both intersections and unions of

2000 *Mathematics Subject Classification.* 14N05; 14H99; 15A69.
Key words and phrases. X-rank; symmetric tensor rank; strange curve; Veronese varieties.

linear spaces $\langle S_i\rangle$, $S_i \subset X$, but obviously in this way the minimal number $\sum_i \sharp(S_i)$ is at least the integer $\alpha(X,P)$ as we defined it. We say that $\alpha(X,P)$ is the *identification number* of P with respect to X. This concept has an obvious geometric meaning, but as in the case of the usual X-rank other related technical definitions may help to compute it. The integer $ir_X(P)$ is quite useful to get an upper bound for the integer $\alpha(X,P)$.

These two integers $ir_X(P)$ and $\alpha(X,P)$ are the key definitions introduced in this paper. We also add other related numerical invariants related to $ir_X(P)$ and $\alpha(X,P)$. We will see in the proofs that these invariants are quite useful to compute $ir_X(P)$ and $\alpha(X,P)$. First of all, several times it is important to look at zero-dimensional subschemes, not just finite sets, to take the linear span. This was a key ingredient for the study of binary forms ([14], [8], §3, [20], §4) and it is very useful also for multivariate polynomials ([8]). The *cactus rank* $z_X(P)$ of P with respect to X is the minimal degree of a zero-dimensional scheme $Z \subset X$ such that $P \in \langle Z\rangle$ ([10], [9]). Let $iz_X(P)$ be the minimal integer t such that there are zero-dimensional subschemes $Z_i \subset X$, $i \ge 1$, such that $\{P\} = \cap_i \langle Z_i\rangle$. Obviously $iz_X(P) \le ir_X(P)$ and $iz_X(P) = 1$ if and only if $P \in X$. Let $\gamma(X,P)$ be the minimal integer x such that there are finitely many zero-dimensional schemes $Z_i \subset X$, say $Z_1,\dots,Z_k$, such that $\{P\} = \cap_{i=1}^k \langle Z_i\rangle$ and $\sum_{i=1}^k \deg(Z_i) = x$. Obviously

$$P \in X, \Leftrightarrow \alpha(X,P) = \Leftrightarrow \gamma(X,P) = 1.$$

Most of our results are for curves and Veronese varieties (in the latter case the X-rank of P is called the symmetric tensor rank of X) (see [2],[8],[15],[19],[20]). In the case of Veronese varieties we give a complete classification of the possible integers $ir_X(P)$, $iz_X(P)$ and $\alpha(X,P)$ when either P has border rank 2 (Theorem 4) or $r_X(P) = 3$ (Theorem 5).

We prove the following results.

Proposition 1. *Let $X \subset \mathbb{P}^{2k}$, $k \ge 1$, be an integral and non-degenerate curve. For a general $P \in \mathbb{P}^{2k}$ we have $r_X(P) = ir_X(P) = k+1$ and $\alpha(X,P) = 2k+2$.*

Theorem 1. *Assume $char(\mathbb{K}) = 0$. Let $X \subset \mathbb{P}^{2k+1}$ be an integral and non-degenerate curve. Fix a general $P \in \mathbb{P}^{2k+1}$.*

(a) If X is not a rational normal curve, then $r_X(P) = ir_X(P) = k+1$ and $\alpha(X,P) = 2k+2$.

(b) If X is a rational normal curve, then $r_X(P) = z_X(P) = k+1$, $ir_X(P) = iz_X(P) = k+2$ and $\alpha(X,P) = \gamma(X,P) = 2k+3$.

We also have a result on strange curves (Proposition 3), results on space curves (Theorems 2 and 3) and on rational normal curves (Propositions 5 and 6).

2. Arbitrary characteristic

For any integral variety $X \subset \mathbb{P}^n$ let $\sigma_t(X)$ denote the closure in $\mathbb{P}^n$ of the union of all linear spaces $\langle S\rangle$ with $S \subset X$ and $\sharp(S) = t$. Each $\sigma_t(X)$ is an integral variety, $\sigma_1(X) = X$ and $\dim(\sigma_t(X)) \le \min\{n, t\cdot\dim(X) - 1\}$. For each $P \in \mathbb{P}^n$ the X-border rank $b_X(P)$ of X is the minimal integer t such that $P \in \sigma_t(X)$. Let $\tau(X) \subseteq \mathbb{P}^n$ denote the tangent developable of X, i.e. the closure in $\mathbb{P}^n$ of all tangent spaces $T_QX \subseteq \mathbb{P}^n$, $Q \in X_{\mathrm{reg}}$. The algebraic set $\tau(X)$ is an integral variety,

$$\dim(\tau(X)) \le \min\{n, 2\cdot\dim(X)\}$$

and $\tau(X) \subseteq \sigma_2(X)$ (it is called the tangent developable of X).

Notation 1. For any linear subspace $V \subseteq \mathbb{P}^n$ let $\ell_V : \mathbb{P}^n \setminus V \to \mathbb{P}^{n-k-1}$, $k := \dim(V)$, denote the linear projection from V. If V is a single point, O, we often write ℓ_O instead of $\ell_{\{O\}}$.

Notation 2. Let $\mathcal{Z}(X,P)$ (resp. $\mathcal{S}(X,P)$) denote the set of all zero-dimensional schemes $Z \subset X$ (resp. finite sets $S \subset X$) such that $\deg(Z) = z_X(P)$ (resp. $\sharp(S) = r_X(P)$) and $P \in \langle Z \rangle$ (resp. $P \in \langle S \rangle$).

As in [11], Lemma 2.1.5, and [8], Proposition 11, we use the following important invariant $\beta(X)$ of the embedded variety $X \subset \mathbb{P}^n$.

Notation 3. Let $X \subset \mathbb{P}^n$ be an integral and non-degenerate variety. Let $\beta(X)$ denote the maximal integer t such that any zero-dimensional scheme $Z \subset X$ with $\deg(Z) \le t$ is linearly independent, i.e. $\dim(\langle Z \rangle) = \deg(Z) - 1$.

Remark 1. Let $X \subset \mathbb{P}^n$ be an integral and non-degenerate subvariety. Fix $P \in \mathbb{P}^n$. If $b_X(P) \le \beta(X)$ and X is either a smooth curve or a smooth surface, then $z_X(P) = b_X(P)$ ([11], Lemma 2.1.5, or [8], Proposition 11).

Take any integral and non-degenerate variety $X \subset \mathbb{P}^n$ and any finite set $S \subset X$ such that $\sharp(S) \le \beta(X)$. By the definition of $\beta(X)$ the set S is linearly independent. It seems better in Notation 3 to prescribe the linearly independence of an arbitrary zero-dimensional scheme $Z \subset X$ with $\deg(Z) \le \beta(X)$. Anyway, in many important cases (e.g. the Veronese varieties) the set-theoretic definition and the scheme-theoretic one chosen in Notation 3 give the same integer.

Remark 2. Obviously $\beta(X) \le n+1$ and equality holds if X is a rational normal curve. We claim that equality holds if and only if X is a rational normal curve. Indeed, if X is a curve with degree $d \ge n+1$, then a general hyperplane section of X contains d points spanning only a hyperplane. Now assume $\dim(X) \ge 2$. Let $H \subset \mathbb{P}^n$ be a general hyperplane. Since $H \cap X$ is infinite, we may find $S \subset H \cap X$ with $\sharp(S) = n+1$. Since S is linearly dependent, $\beta(X) \le n$ even in this case.

Remark 3. Fix an integral and non-degenerate variety $X \subset \mathbb{P}^n$ and $P \in \mathbb{P}^n$. Obviously $ir_X(P) = +\infty$ if and only if $ir_X(P) > n$. Since the intersection of $n-1$ hyperplanes of $\mathbb{P}^n$ contains at least a line, if $r_X(P) = ir_X(P) = n$, then $\alpha(X,P) = n^2$. We have $r_X(P) = n+1$ if and only if $\dim(X) = 1$ and X is a flat curve in the sense of [4]. Obviously if $r_X(P) = n+1$, then $ir_X(P) = +\infty$. See [4], Proposition 1 and Example 1, for two classes of flat curves.

Let $X \subsetneq \mathbb{P}^n$ be an integral and non-degenerate variety and $P \in \mathbb{P}^n$. We say that P is a *strange point* of X if for a general $Q \in X_{\mathrm{reg}}$ the Zariski tangent space T_QX contains P (we allow the case in which X is a cone with vertex containing P). The *strange set* of X is the set of all strange points of X (this set is always a linear subspace, but usually it is empty). If this set is not empty, then either $\mathrm{char}(\mathbb{K}) > 0$ or X is a cone and the strange set of X is the vertex of X ([7],[22]). Lines and smooth conics in characteristic two are the only smooth strange curves ([17], Theorem IV.3.9). Now fix $P \in \mathbb{P}^n \setminus X$ and set $f_{P,X} := \ell_P|X$. Since $P \notin X$, $f_{P,X}$ is a finite morphism and we have $\deg(X) = \deg(f_{P,X}) \cdot \deg(f_{P,X}(X))$. The point P is a strange point of X if and only if $f_{P,X}$ is not separable. We recall that a non-degenerate curve $X \subset \mathbb{P}^n$, $n \ge 3$, is said to be *very strange* if a general hyperplane section of X is not in linearly general position ([22]). A very strange curve is strange ([22], Lemma 1.1).

Proposition 2. *Fix an integral and non-degenerate variety $X \subsetneq \mathbb{P}^n$. Set $m := \dim(X)$ and fix $P \in \mathbb{P}^n$. If P is not a strange point of X, then $ir_X(P) \le n-m+1$.*

Proof. We will follow the proof of part (a) of [4], Theorem 1. If $P \in X$, then $ir_X(P) = 1$. Hence we may assume $P \notin X$. First assume $m = 1$. Let $H \subset \mathbb{P}^n$ be a general hyperplane containing P. Since P is not a strange point of X, H is transversal to X, i.e. $H \cap \mathrm{Sing}(X) = \emptyset$ and $\sharp(X \cap H) = \deg(X)$. Since X is reduced and irreducible, we have $h^1(\mathcal{I}_X) = 0$. From the exact sequence

$$(1) \qquad 0 \to \mathcal{I}_X \to \mathcal{I}_X(1) \to \mathcal{I}_{X\cap H,H}(1) \to 0$$

we get that the set $H \cap X$ spans H. Since $P \in H$, we get the existence of $S_H \subset X \cap H$ such that $\sharp(S_H) \le n$ and $P \in \langle S_H\rangle$. Fix general hyperplanes H_i, $i \le i \le n$, containing P and such that $\{P\} = H_1 \cap \cdots \cap H_n$. Take $S_{H_i} \subset X \cap H_i$ as above. Since $\{P\} = \cap_{i=1}^n \langle S_{H_i}\rangle$, we get $ir_X(P) \le n$. Now assume $m \ge 2$. We use induction on m. Take a general hyperplane $H \subset \mathbb{P}^n$ containing P. Bertini's theorem gives that $X \cap H$ is geometrically integral ([18], part 4) of Th. I.6.3). Fix a general $Q \in (X \cap H)_{\mathrm{reg}}$. For general H we may take as Q a general point of X. Hence $P \notin T_QX$. Hence $P \notin (T_QX) \cap H = T_Q(X \cap H)$. Thus P is not a strange point of $X \cap H$. By the inductive assumption in $H \cong \mathbb{P}^{n-1}$ we get $ir_{X\cap H}(P) \le n-m+1$. Since $ir_X(P) \le ir_{X\cap H}(P)$, we are done. □

Proposition 3. *Fix an integral and non-degenerate strange curve $X \subset \mathbb{P}^n$. Fix $P \in \mathbb{P}^n \setminus X$ and assume that P is the strange point of X. Let s (resp. p^e) denote the separable (resp. inseparable) degree of $f_{P,X}$. Set $d := \deg(X)$ and $c := \deg(f_{P,X}(X))$. We have $d = sp^ec$.*

(a) If $s \ge 2$, then $ir_X(P) = 2$.

(b) If $s = 1$, $c \ne n-1$ and X is not very strange, then $ir_X(P) \le n$.

(c) If $s = 1$ and $c = n-1$, then $r_X(P) = n+1$ and $ir_X(P) = +\infty$.

Proof. Since $P \notin X$, $f_{P,X}$ is a finite morphism. Hence $\deg(X) = \deg(f_{P,X}) \cdot \deg(f_{P,X}(X))$, i.e. $d = sp^ec$.

First assume $s \ge 2$. Fix general $P_1, P_2 \in f_{P,X}(X)$. By assumptions there are $O_{ij} \in f_{P,X}^{-1}(P_i)$, $i = 1, 2$, $j = 1, 2$, such that $O_{i1} \ne O_{i2}$. Set $S_i := \{O_{i1}, O_{i2}\}$. Since $P \in \langle S_i\rangle$, $i = 1, 2$, and the two lines $\langle S_i\rangle$ are different, we get $ir_X(P) = 2$.

From now on we assume $s = 1$ and that X is not very strange. Let $u : Y \to X$ denote the normalization map. Let $\mathcal{H}$ be the set of all hyperplanes of $\mathbb{P}^{n-1}$ transversal to $f_{P,X}(X)$. We have $\dim(\mathcal{H}) = n-1$. Since $f_{P,X}(X)$ is non-degenerate, we have $\deg(f_{P,X}(X)) \ge n-1$.

First assume $c \ne n-1$. Hence for every $H \in \mathcal{H}$ we may find a set $A_H \subset H \cap f_{P,X}(X)$ such that $\sharp(A_H) = n$ and $\langle A_H\rangle = H$. Notice that A_H is linearly dependent. Fix $S_H \subset X$ such that $\sharp(S_H) = n$ and $f_{P,X}(S_H) = A_H$. If $P \notin \langle S_H\rangle$, then S_H is linearly dependent. Since X is not very strange, we have $X \cap \langle S\rangle = S$ (as sets) for a general set $S \subset X$ such that $\sharp(S) = n-1$. Hence there is at most an $(n-2)$-dimensional family of linearly dependent subsets of X with cardinality n. Hence there is a non-empty open subset $\mathcal{H}'$ of $\mathcal{H}$ such that $P \in \langle S_H\rangle$ for every $H \in \mathcal{H}'$. Since $\cap_{H\in\mathcal{H}'} H = \emptyset$, we get $\{P\} = \cap_{H\in\mathcal{H}'}\langle S_H\rangle$. Hence $ir_X(P) \le n$.

Now assume $c = n-1$. Hence $f_{P,X}(X)$ is a rational normal curve. In particular $f_{P,X}(X)$ is smooth. Since $f_{P,X} \circ u : Y \to f_{P,X}(X)$ is a purely inseparable morphism between smooth curves, it is injective. Hence $f_{P,X}$ is injective. Since $f_{P,X}(X)$ is a rational normal curve, for every $S \subset X$ with $\sharp(S) \le n$, the set $f_{P,X}(S)$ is a linearly independent set with $\sharp(S)$ elements. Hence $P \notin \langle S\rangle$. Hence $r_X(P) = n+1$. Hence $ir_X(P) > n$, i.e. $ir_X(P) = +\infty$. □

All strange curves may be explicitly constructed (see [7] for the case $n = 2$ and [3] for the case $n > 2$).

3. Curves

We use the following obvious observations (true in arbitrary characteristic) and whose linear algebra proof is left to the reader (parts (a) and (b) of Lemma 1 just say that two distinct lines have at most one common point and that if $P \in \langle\{P_1, P_2\}\rangle$ and $ir_X(P) < 4$, then there is $S \subset X$ with $\sharp(S) \le 3$, $P \in \langle S\rangle$ and $\langle\{P_1, P_2\}\rangle \nsubseteq \langle S\rangle$).

Lemma 1. *Let $X \subset \mathbb{P}^3$ be an integral and non-degenerate curve. Fix $P \in \mathbb{P}^3 \setminus X$.*

(a) If $r_X(P) = ir_X(P) = 2$, then $\alpha(X, P) = 4$.

(b) If $r_X(P) = 2$ and $ir_X(P) = 3$, then $\alpha(X, P) = 5$.

(c) If $r_X(P) = ir_X(P) = 3$, then $\alpha(X, P) = 9$.

Remark 4. Now assume that X is a singular curve, but take a zero-dimensional scheme $Z \subset X_{\text{reg}}$ such that $k := \deg(Z) \le \beta(X)/2$. Since Z is curvilinear, it has finitely many linear subschemes. Since Z is linearly independent, the set $\Psi := \langle Z\rangle \setminus_{Z' \subsetneq Z} \langle Z'\rangle)$ is a non-empty open subset of the $(k-1)$-dimensional linear space $\langle Z\rangle$. Fix any $P \in \Psi$. Lemma 3 gives $z_X(P) = k$ and that Z is the only degree k subscheme of X whose linear span contains P. Since $Z \subset X_{\text{reg}}$, Z is smoothable. Hence [8], Proposition 11, give $b_X(P) = k$.

Lemma 2. *Let $X \subset \mathbb{P}^n$ be an integral and non-degenerate curve. Fix $P \in \mathbb{P}^n$ such that $z_X(P) \le \beta(X)/2$. Then:*

(i) *There is a unique zero-dimensional scheme $A \subset X$ such that $P \in \langle A\rangle$ and $\deg(A) \le z_X(P)$. We have $\deg(A) = z_X(P)$.*

(ii) *Fix any zero-dimensional scheme $W \subset X$ such that $\deg(W) \le \beta(X) - z_X(P)$ and $P \in \langle W\rangle$. Then $W \supseteq A$. We have $ir_X(P) \ge iz_X(P) \ge \beta(X) - z_X(P) + 1$.*

(iii) *Assume that A is not reduced. Then $r_X(P) \ge \beta(X) - z_X(P) + 1$. If $r_X(P) = \beta(X) - z_X(P) + 1$, then $S \cap A = \emptyset$ for all sets $S \subset X$ such that $\sharp(S) = r_X(P)$ and $P \in \langle S\rangle$.*

Proof. Assume the existence of zero-dimensional schemes A, W such that $A \neq W$, $P \in \langle A\rangle \cap \langle W\rangle$, $P \notin \langle A'\rangle$ for all $A' \subsetneq A$ and $\deg(A) + \deg(W) \le \beta(X)$. Lemma 3 gives the existence of $W' \subsetneq W$ such that $P \in \langle W'\rangle$. If $W' \neq W$, then we continue taking W' instead of W. We get parts (a) and (b).

The first assertion of part (iii) follows from part (ii), while the second one follows from Lemma 3. □

Proposition 4. *Let $X \subset \mathbb{P}^3$ be a rational normal curve. Then $ir_X(P) = 3$ for all $P \in \mathbb{P}^3 \setminus X$.*

Proof. Lines and smooth conics in characteristic two are the only smooth strange curves ([17], Theorem IV.3.9). Fix $P \in \mathbb{P}^3 \setminus X$. Since X is not strange, we have $ir_X(P) \le 3$ (Proposition 3) (even in positive characteristic). Since $\sigma_2(X) = \mathbb{P}^3$ ([1], Remark 1.6), Remark 3 gives $z_X(P) = 2$. Since $\beta(X) = 4$, Lemma 3 gives $ir_X(P) \ge 3$. □

Let X be a smooth elliptic curve defined over $\mathbb{K}$. We recall that the 2-rank of X is the number, ϵ, of pairwise non-isomorphic line bundles L on X such that $L^{\otimes 2} \cong \mathcal{O}_X$ ([23], Chapter III). If $\mathrm{char}(\mathbb{K}) \neq 2$, then $\epsilon = 4$, while $\epsilon \in \{1, 2\}$ if $\mathrm{char}(\mathbb{K}) = 2$ ([23], Corollary III.6.4).

Theorem 2. *Let $X \subset \mathbb{P}^3$ be a smooth elliptic curve. Fix $P \in \mathbb{P}^3 \setminus X$. Let ϵ be the 2-rank of the elliptic curve X. There are exactly ϵ quadric cones W_i, $1 \le i \le \epsilon$ containing X. Call O_i, $1 \le i \le \epsilon$, the vertex of W_i.*

(a) The points O_i, $1 \le i \le \epsilon$, are the only points $Q \in \mathbb{P}^3$ such that $\mathcal{Z}(X, P)$ and $\mathcal{S}(X, Q)$ are infinite; we have $ir_X(O_i) = 2$ for all i; each point O_i is contained in TX.

(b) If $P \in (TX \cup \bigcup_{i=1}^{\epsilon} W_i)$, but $P \neq O_i$ for any i, then $ir_X(P) = 3$.

(c) If $P \notin (TX \cup \bigcup_{i=1}^{\epsilon} W_i)$, then $ir_X(P) = 2$.

Proof. Call R_i, $1 \le i \le \epsilon$, the pairwise non-isomorphic line bundles on X such that $R_i^{\otimes 2} \cong \mathcal{O}_X$. Since $\deg(X)$ is even and $\mathbb{K}$ is algebraically closed, there is a line bundle $\mathcal{L}$ on X such that $\mathcal{L}^{\otimes 2} \cong \mathcal{O}_X(1)$. Set $L_i := R_i \otimes \mathcal{L}$. It is easy to check that the line bundles L_i, $1 \le i \le \epsilon$, are pairwise non-isomorphic and that, up to isomorphisms, they are the only line bundles A on X such that $A^{\otimes 2} \cong \mathcal{O}_X(1)$.

Since X is not strange, Proposition 3 gives $ir_X(P) \le 3$. Since $P \notin X$, Remark 3 and [1], Remark 1.6, give $z_X(P) = 2$. Obviously, if $\sharp(\mathcal{Z}(X, P)) = 1$, then $ir_X(P) > 2$. Since $\ell_P(X)$ spans $\mathbb{P}^2$, we have $\deg(\ell_P(X)) \ge 2$. Hence either $\deg(\ell_P(X)) = 4$ and $\ell_P|X$ is birational onto its image or $\deg(\ell_P|X) = 2$.

First assume $\deg(\ell_P|X) = 2$. In this case we get that $\mathcal{Z}(X, P)$ is infinite. Since $\ell_P(X) \cong \mathbb{P}^1$, the morphism $\ell_P|X$ is not purely inseparable. Hence a general fiber of it is formed by two distinct points of X spanning a line through P. Hence $ir_X(P) = 3$. We get $\mathcal{O}_X(1) \cong \ell_P(\mathcal{O}_{\ell_P(X)}(1))$. Since $\mathcal{O}_{\ell_P(X)}(1) \cong R^{\otimes 2}$ with R a degree 1 line bundle on $\ell_P(X)$, $\ell_P^*(R)$ is one of the line bundles L_i, $1 \le i \le \epsilon$. Since $X \neq \mathbb{P}^1$, $\ell_P|X$ has at least one ramification point. Hence $O_i \in TX$ for all i. The construction may be inverted in the following sense. Fix one of the line bundles L_i, $1 \le i \le \epsilon$. Since X is an elliptic curve, we have $h^0(X, L_i) = 2$ and the linear map $j : S^2(H^0(X, L_i)) \to H^0(X, \mathcal{O}_X(1))$ is injective with as image a hyperplane of the 4-dimensional linear space $H^0(X, \mathcal{O}_X(1))$, i.e. (by the linear normality of X) a point, $\widetilde{O}_i$ of $\mathbb{P}^3 = \mathbb{P}(H^0(X, \mathcal{O}_X(1))^\vee)$. The definition of j gives that $\ell_{\widetilde{O}_i}|X$ has degree 2.

Now assume $\deg(\ell_P(X)) = 4$. The genus formula for plane curves gives that $\ell_P(X)$ has 1 or 2 singular points and that if it has two singular points, then they are either ordinary nodes or ordinary cusps. If $\ell_P(X)$ has either a unique singular point or at least one cusp, then $ir_X(P) > 2$ and hence $ir_X(P) = 3$. In particular this is the case if $P \in TX$. Hence if $P \in TX$ and $P \neq O_i$, then $ir_X(P) = 3$. Now assume $P \notin TX$. In this case $ir_X(P) = 2$ if and only if $\ell_P(X)$ has two singular points. If the plane curve $\ell_P(X)$ has a unique singular point, then it is an ordinary tacnode. Let $T \subset \mathbb{P}^3$ be a line secant to X, but not tangent to X. Since X is the complete intersection of two quadric surfaces, there is a unique quadric surface, W, containing $X \cup \{P\}$. Call T a line in W containing P. $X \cup T$ is contained in a unique quadric surface, W. If W is singular, i.e. if $W = W_i$ for some i, then there is a unique line through P and secant to X. If W is smooth, i.e. if $P \notin W_i$ for any i, then there are two such lines, both of them containing two distinct points of X, because we assumed $P \notin TX$. Hence $ir_X(P) = 2$ in this case. □

Theorem 3. *Let $X \subset \mathbb{P}^3$ be an integral and non-degenerate curve. Assume that X is not strange and that X has only planar singularities. There is a non-empty open subset Ω of $\mathbb{P}^3 \setminus X$ such that $ir_X(P) = 2$ for all $P \in \Omega$ if and only if X is not a rational normal curve..*

Proof. Set $d := \deg(X)$ and $q := p_a(X)$. Since Proposition 4 gives that " only if " part, it is sufficient to prove the " if " part. Assume $d \geq 4$. It is easy to check the existence of a non-empty open subset W of $\mathbb{P}^3 \setminus X$ such that $\ell_P|X$ is birational onto its image for all $P \in W$. By assumption for each $O \in \mathrm{Sing}(X)$ the Zariski tangent plane $T_O X$ of X at O is a plane. Since $\mathrm{Sing}(X)$ is finite, we get finitely many planes $T_O X$, $O \in \mathrm{Sing}(X)$, and we call W' the intersection of W with the complement of the union of these planes. Let G be the intersection of W' with the complement of the tangent developable $\tau(X)$ of X. For each $P \in G$ the morphism $\ell_P|X$ is unramified and birational onto its image. Hence the singularities of the degree d plane curve $\ell_P(X)$ comes only from the non-injectivity of $\ell_P|X$ and the singularities of X. To prove Theorem 3 it is sufficient to prove that the set of all $P \in G$ such that $\ell_P|X$ has at least two fibers with cardinality ≥ 2 contains a non-empty open subset. For any $O \in \mathrm{Sing}(X)$ let $C_O(X)$ the cone with vertex O and the plane curve $\overline{\ell_O(X \setminus \{O\})}$ as its base. Set $G' := G \setminus G \cap (\cup_{O \in \mathrm{Sing}(X)} C_O(X))$. The set G' is a non-empty open subset of G and for every $P \in G'$ no point of $X \setminus \mathrm{Sing}(X)$ is mapped onto a point of $\ell_P(\mathrm{Sing}(X))$. Hence for each $P \in G'$ the plane curve $\ell_P(X)$ has $\sharp(\mathrm{Sing}(X))$ singular points isomorphic to the corresponding singular points of X, plus some other singular points and the integer $p_a(\ell_P(X)) - q = (d-1)(d-2)/2 - q$ is the sum of the contributions of the other singular points. Since X is not strange, it is not very strange, i.e. a general secant line of X contains only two points of X ([22], Lemma 1.1). This is equivalent to the existence of a non-empty open subset G'' of G' such that for all $P \in G''$ each singular point of $\ell_P(X) \setminus \ell_P(\mathrm{Sing}(X))$ has only two branches.

Claim: There is a non-empty open subset G_1 of G'' such that for every $P \in G_1$, $\ell_P(X) \setminus \ell_P(\mathrm{Sing}(X))$ has only ordinary double points as singularities.

Proof of the Claim: Fix $P \in G''$. Fix $O \in \ell_P(X) \setminus \ell_P(\mathrm{Sing}(X))$. By the definition of G'' there are exactly two points $Q_1, Q_2 \in X$ such that $\ell_P(Q_1) = \ell_P(Q_2) = O$, X is smooth at Q_1 and Q_2, and $\ell_P|X$ is unramified at each Q_i. Hence $\ell_P(X) \setminus \ell_P(\mathrm{Sing}(X))$ has only ordinary double points as singularities if and only if $\ell_P(T_{Q_1}X) \neq \ell_P(T_{Q_2}X)$, i.e. if and only if the planes $\langle \{P\} \cup T_{Q_i}X \rangle$, $i = 1, 2$, are distinct. This is certainly true if $T_{Q_1}X \cap T_{Q_2}X = \emptyset$. Let $\mathcal{V}$ denote the set of all $(Q_1, Q_2) \in (X \setminus \mathrm{Sing}(X)) \times (X \setminus \mathrm{Sing}(X))$ such that $Q_1 \neq Q_2$. Let $\mathcal{U}$ be the set of all $(Q_1, Q_2) \in \mathcal{V}$ such that $T_{Q_1}X \cap T_{Q_2}X \neq \emptyset$. Since X is not strange, $\mathcal{U}$ is a union of finitely many subvarieties of dimension ≤ 1; it is here that we use the full force of our assumption " X not strange ", not only the far weaker condition " X not very strange ". Let Δ be the closure in $\mathbb{P}^3$ of the union of the lines $\langle \{Q_1, Q_2\} \rangle$ with $(Q_1, Q_2) \in \mathcal{U}$. We have $\dim(\Delta) \leq 2$. Set $G_1 := G'' \cap (\mathbb{P}^3 \setminus \Delta)$. By construction this set G_1 satisfies the Claim.

Now we prove that we may take $\Omega := G_1$. Fix $P \in G_1$ and call x the number of the singular points of $\ell_P(X) \setminus \ell_P(\mathrm{Sing}(X))$. By the claim it is sufficient to prove the inequality $x \geq 2$. Since $\ell_P(X)$ is a plane curve of degree d, it has arithmetic genus $(d-1)(d-2)/2$. Since each point of $\ell_P(X) \setminus \ell_P(\mathrm{Sing}(X))$ is an ordinary node, $\ell_P|X$ is unramified at each point of $\mathrm{Sing}(X)$ and $\ell_P^{-1}(\ell_P(X)\setminus\ell_P(\mathrm{Sing}(X)))$, we have $x = p_a(\ell_P(X)) - p_a(X) = (d-1)(d-2)/2 - q$. Hence it is sufficient to prove that $q \le (d-1)(d-2)/2 - 2$. This is true by the assumption $d \ge 4$ and Castelnuovo's inequality for the arithmetic genus of space curves (use [22], Lemma 1.1, that X is not strange and that the upper bound needs only that a general plane section of X is in linearly general position). □

Proof of Proposition 1: Let Δ denote the set of all linearly independent subsets of X with cardinality $k+1$. Since $\sigma_{k+1}(X) = \mathbb{P}^{2k}$ and $\dim(\sigma_k(X)) = 2k-1$ ([1], Remark 1.6), we have $r_X(P) = k+1$. A dimensional count gives that $\mathcal{S}(X,P)$ has a one-dimensional irreducible component, Γ. Fix $A, B \in \Gamma$. It is sufficient to prove that $\{P\} = \langle A\rangle \cap \langle B\rangle$. Since any two k-dimensional linear subspaces meet, the set A may be seen as a general element of Δ and, after fixing A, P may be seen as a general element of $\langle A\rangle$. Hence it is sufficient to prove that $\langle A\rangle \cap \langle B\rangle$ is a single point for a general $(A,B) \in \Delta\times\Delta$, i.e. to check that $A\cup B$ spans $\mathbb{P}^{2k}$. For fixed A, we have $\langle A\cup B\rangle = \mathbb{P}^{2k}$ for a general $B \subset X$, because X spans $\mathbb{P}^{2k}$. □

Proof of Theorem 1: Since $\sigma_{k+1}(X) = \mathbb{P}^{2k+1}$ and P is general, we have $r_X(P) \le k+1$ ([1], Remark 1.6). Since $\dim(\sigma_k(X)) = 2k-1$ ([1], Remark 1.6) and P is general, we have $r_X(P) \ge k+1$. Hence $r_X(P) = k+1$. X is not a rational normal curve if and only if there are $S_1, S_2 \subset X$ such that $S_1 \ne S_2$, $\sharp(S_1) = \sharp(S_2) = k+1$ and $P \in \langle S_1\rangle \cap \langle S_2\rangle$ ([13], Theorem 3.1). Let Ω be the set of all $Q \in \mathbb{P}^{2k+1}\setminus\sigma_k(X)$ such that there are only finitely many sets $S \subset X$ with $\sharp(S) = k+1$ and $Q \in \langle S\rangle$. Ω is a non-empty open subset of $\mathbb{P}^{2k+1}$. Since P is general, we may assume $P \in \Omega$.

(i) In this step we assume that X is not a rational normal curve. Let Γ denote the set of all finite sets $S \subset X$ such that $\sharp(S) = k+1$ and $\dim(\langle S\rangle) = k$. We proved the existence of $S_i \in \Gamma$, $i = 1,2$, such that $P \in \langle S_1\rangle \cap \langle S_2\rangle$. To prove part (a) it is sufficient to prove that $\{P\} = \langle S_1\rangle \cap \langle S_2\rangle$ for a general P. Assume that this is not true, i.e. assume that $\langle S_1\rangle \cap \langle S_2\rangle$ is a linear space of dimension $\rho > 0$. Notice that $\mathcal{S}(X,P) = \{S \in \Gamma : P \in \langle S\rangle\}$. Set $\Gamma(S_1) := \{S \in \Gamma : S\cap S_1 = \emptyset, \langle S\rangle\cap\langle S_1\rangle\cap\Omega \ne \emptyset\}$. Since $\dim\langle S_1\rangle = k$ and $P \in \Omega\cap\langle S_1\rangle$, then $\Gamma(S_1) \ne \emptyset$ and $\Gamma(S_1)$ has pure dimension k. Since P is general in $\mathbb{P}^{2k+1}$, we may assume that S_1 is general in Γ and that S_2 is general in one of the irreducible components of $\Gamma(S_1)$. We get that for a general $P' \in \Omega\cap\langle S_1\rangle$ there is a ρ-dimensional family of sets S with $P' \in \langle S\rangle$, absurd.

(ii) In this step we assume that X is a rational normal curve. We know that $r_X(P) = k+1$. We proved that $ir_X(P) \ge k+2$ and hence that $\alpha(X,P) \ge 2k+3$. For a sufficiently general $P \in \mathbb{P}^{2k+1}$ we call S_P the only subset of X with cardinality $k+1$ and whose linear span contains P. Since $\beta(X) = 2k+2$ and $P \notin \sigma_k(X)$, Remark 3 gives $z_X(P) = k+1$ and that S_P is the only degree $k+1$ zero-dimensional subscheme of X whose linear span contains P. Hence $iz_X(P) \ge k+2$ and $\gamma(X,P) \ge 2k+3$.

Fix a general $Q \in X$ and let $\phi : X \to \mathbb{P}^{2k}$ denote the morphism induced from $\ell_Q|(X\setminus\{Q\})$. The morphism ϕ is an embedding of $X \cong \mathbb{P}^1$ as a rational normal curve of $\mathbb{P}^{2k}$. Fix a general $P' \in \mathbb{P}^{2k}$. Proposition 1 gives the existence of $A_1, A_2 \subset \phi(X)$ such that $\sharp(A_1) = \sharp(A_2) = k+1$ and $\langle A_1\rangle \cap \langle A_2\rangle = \{P'\}$. For a fixed point $\phi(Q)$, but for general P' we may also assume $\phi(Q) \notin (A_1\cup A_2)$. Hence there is a unique set $B_i \subset X\setminus\{Q\}$ such that $\phi(B_i) = A_i$. Set $E_i := \{Q\}\cup B_i$. Fix $P'' \in \mathbb{P}^{2k+1}$ such that $\ell_Q(P'') = P'$. For fixed Q, but general P' we may consider

P'' as a general point of $\mathbb{P}^{2k+1}$. We have $\langle\{Q, P''\}\rangle = \langle E_1\rangle \cap \langle E_2\rangle$. Varying Q in X we get $ir_X(P) \le k+2$ and hence $ir_X(P) = k+2$. Let Θ be the set of all finite subsets $A \subset X$ such that $\sharp(A) = k+2$ and $P \in \langle A\rangle$. Assume for the moment the existence of $A \in \Theta$ such that $A \cap S_P = \emptyset$, i.e. such that $\sharp(A \cup S_P) = 2k+3$. Since $\beta(X) = 2k+2$ and $\sharp(A \cup S_P) = 2k+3$, we get $\langle S_P \cup A\rangle = \mathbb{P}^{2k+1}$, i.e. $\dim(\langle A\rangle \cap \langle S_P\rangle) = 0$ (Grassmann's formula). Since $P \in \langle A\rangle \cap \langle S_P\rangle$, we get $\{P\} = \langle A\rangle \cap \langle S_P\rangle$, i.e. $\alpha(X, P) \le 2k+3$. Hence $\alpha(X, P) = \gamma(X, P) = 2k+3$. Now assume $A \cap S_P \ne \emptyset$ for all $A \in \Theta$. Since P is general and $\sigma_{k+2}(X) = \mathbb{P}^{2k+1}$, Terracini's lemma (or a dimensional count) gives $\dim(\Theta) = 2$. For any $Q \in S_P$ set $\Theta_Q := \{A \in \Theta : Q \in A\}$. The proof of the inequality $ir_X(P) \le 2k+3$ also shows $\dim(\Theta_Q) = 1$. Since S_P is finite, we get $\dim(\Theta) = 1$, a contradiction. □

4. Veronese varieties

For all integers $m \ge 1$ and $d \ge 1$ let $\nu_d : \mathbb{P}^m \to \mathbb{P}^n$, $n := \binom{m+d}{m} - 1$ denote the order d embedding of $\mathbb{P}^m$ induced by the vector space of all degree d homogeneous polynomials in $d+1$ variables. Set $X_{m,d} := \nu_d(\mathbb{P}^m)$.

We often use the following elementary lemma ([5], Lemma 1).

Lemma 3. *Fix any $P \in \mathbb{P}^n$ and two zero-dimensional subschemes A, B of $\mathbb{P}^n$ such that $A \ne B$, $P \in \langle A\rangle$, $P \in \langle B\rangle$, $P \notin \langle A'\rangle$ for any $A' \subsetneq A$ and $P \notin \langle B'\rangle$ for any $B' \subsetneq B$. Then $h^1(\mathbb{P}^n, \mathcal{I}_{A\cup B}(1)) > 0$.*

We first need the case $m = 1$ of Theorem 4, i.e. we need to study the case in which X is a rational normal curve (Propositions 5,6 and 7).

Proposition 5. *Let $X \subset \mathbb{P}^d$, $d \ge 3$, be a rational normal curve. Fix a set $A \subset X$ with $\sharp(A) = 2$ and any $P \in \langle A\rangle \setminus A$. Then $r_X(P) = z_X(P) = 2$, $ir_X(P) = iz_X(P) = d$ and $\alpha(X, P) = \gamma(X, P) = d+2$. Moreover, there is a set $B \subset X$ such that $\sharp(B) = d$ and $\{P\} = \langle A\rangle \cap \langle B\rangle$.*

Proof. Since $\beta(X) = d+1 \ge 3$, we have $A = \langle A\rangle \cap X$. Hence $P \notin X$. Hence $ir_X(P) = 2 = iz_X(P)$. Fix a zero-dimensional scheme $W \subset X$ such that $P \in \langle W\rangle$, $P \notin \langle W'\rangle$ for any $W' \subsetneq W$ and $W \ne A$. Since $\beta(X) = d+1$, Lemma 3 gives $\deg(W) \ge d$. Hence $ir_X(P) \ge iz_X(P) \ge d$ and $\alpha(X, P) \ge \gamma(X, P) \ge d+2$. Hence to conclude the proof it is sufficient to find a set $B \subset X$ such that $\sharp(B) = d$ and $\{P\} = \langle A\rangle \cap \langle B\rangle$. Set $Y := \ell_P(X)$. Since $P \in \langle A\rangle$ and $P \notin X$, the curve Y is a linearly normal curve with degree d, arithmetic genus 1 and a unique singular point, which is an ordinary node. Fix a general hyperplane $H \subset \mathbb{P}^{d-1}$ and set $E := Y \cap X$. Since H is general, it does not contain the singular point of Y and it is transversal to Y. Hence E is a set of d points and there is $B \subset X$ such that $\sharp(B) = d$ and $\ell_P(B) = E$. Since $\sharp(B) \le \beta(X)$, B is linearly independent. Since E is linearly dependent, we have $P \in \langle B\rangle$. Since $\sharp(A \cup B) = d+2 = \beta(X)+1$, we have $\langle A \cup B\rangle = \mathbb{P}^d$. Hence Grassmann's formula gives $\{P\} = \langle A\rangle \cap \langle B\rangle$. □

Proposition 6. *Let $X \subset \mathbb{P}^d$, $d \ge 3$, be a rational normal curve. Fix $P \in \tau(X) \setminus X$, i.e. fix $P \in \sigma_2(X)$ such that $r_X(P) > 2$. Then $z_X(P) = 2$, $iz_X(P) = d$, $\gamma(X, P) = d+2$, $r_X(P) = d$, $ir_X(P) = d$ and $\alpha(X, P) = d^2$. Moreover, there are a zero-dimensional $A \subset X$ and a finite set $B \subset X$ such that $\deg(A) = 2$, $\sharp(B) = d$ and $\{P\} = \langle A\rangle \cap \langle B\rangle$.*

Proof. First of all we explain the " i.e. " part. Since $\beta(X) \ge 2$, Remark 3 gives that for each $Q \in \sigma_2(X) \setminus X$ there is a degree 2 zero-dimensional scheme $A_Q \subset X$

such that $Q \in \langle A_Q \rangle$. Since $\beta(X) \geq 4$, we also get the uniqueness of A_Q. Hence $P \in \tau(X) \Leftrightarrow A_P$ is not reduced $\Leftrightarrow r_X(P) > 2$. Set $A := A_P$. Lemma 3 gives $r_X(P) \geq d$ and $iz_X(P) \geq d$. We repeat the proof of Proposition 5 (now Y is a degree d linearly normal curve with a cusp). We get the existence of a set $B \subset X$ such that $\sharp(B) = d$ and $\{P\} = \langle A \rangle \cap \langle B \rangle$. Hence $iz_X(P) = d$, $\gamma(X,P) = d$. Since $d \geq 3$, X is not strange. Hence $ir_X(P) \leq d$ (Proposition 3). Since $r_X(P) \geq d$, we get $r_X(P) = ir_X(P) = d$. Since $r_X(P) = d$, P is contained in no linear space of dimension $\leq d-2$ spanned by a finite subset of X. Hence $\alpha(X,P) = d^2$ (Remark 3). □

Proposition 7. *Let $X \subset \mathbb{P}^d$, $d \geq 5$, be a rational normal curve. Fix a set $A \subset X$ such that $\sharp(A) = 3$ and any $P \in \langle A \rangle$ such that $P \notin \langle A' \rangle$ for any $A' \subsetneq A$. Then $r_X(P) = z_X(P) = 3$, $ir_X(P) = iz_X(P) = d-1$ and $\alpha(X,P) = \gamma(X,P) = d+2$.*

Proof. Since $\beta(X) \geq 5$, Lemma 3 gives $z_X(P) = 3$, $iz_X(P) \geq \beta(X)+1-\sharp(A) = d-1$ and hence $r_X(P) = 3$, $ir_X(P) \geq d-1$, $\alpha(X,P) \geq \gamma(X,P) \geq d+2$.

Set $Y := \ell_P(X)$. Since $\beta(X) = d+1 \geq 5$ and $P \notin \langle A' \rangle$ for any $A' \subsetneq A$, $\ell_P|X$ is an embedding. Hence Y is a smooth rational curve of degree d spanning $\mathbb{P}^{d-1}$. Fix any $E \subset X \setminus A$ with $\sharp(E) = d-4$ and set $F := \ell_P(E)$. Since $\sharp(A \cup E) \leq \beta(X)$, F is a set of $d-4$ points of Y spanning a $(d-5)$-dimensional linear subspace disjoint from the line $\langle \ell_P(A) \rangle$.

Claim: For general E we have $\langle F \rangle \cap Y = F$ (as schemes) and $\ell_{\langle F \rangle}|(Y \setminus F)$ extends to an embedding $\phi : Y \to \mathbb{P}^3$ with $\phi(Y) \subset \mathbb{P}^3$ a smooth and rational curve of degree 4 with $\phi(\ell_P(A))$ the union of 3 distinct and collinear points.

Proof of the Claim: The map ϕ is induced by the linear projection of X from the linear subspace $\langle \{P\} \cup E \rangle$. Since $E \cap A = \emptyset$ and $\sharp(E \cup A) \leq \beta(X)$, we have $\langle E \rangle \cap \langle A \rangle = \emptyset$. Hence $\phi(A)$ is the union of 3 distinct collinear points. For degree reasons we get $\langle F \rangle \cap Y = F$ (as schemes), i.e. $\deg(\phi)\cdot\deg(\phi(Y)) = \deg(Y) - d + 4 = 4$. Since $\phi(Y)$ spans $\mathbb{P}^3$, we get $\deg(\phi) = 1$. Since $\phi(Y)$ has a 3-secant line, the curve Y is not the complete intersection of two quadric surfaces. Hence $\phi(Y)$ is smooth and rational.

Since $h^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(2)) = 10 = h^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(8)) + 1$, the Claim implies the existence of a quadric surface T containing $\phi(Y)$. Since $\phi(Y)$ has genus $\neq 1$, T is not a cone ([17], V.Ex.2.9). Hence $\phi(Y)$ is a curve of type $(1,3)$ on the smooth quadric surface T. The set $\phi(\ell_P(A))$ is contained in a line of type $(1,0)$. Let G be the intersection of $\phi(Y)$ with a general line of type $(1,0)$ of T. Since any two different lines of T are disjoint, we have $\phi(A) \cap G = \emptyset$. Since $\phi(\ell_P(A))$ is reduced, in arbitrary characteristic we get that G is reduced. Since the set $\phi(F)$ is finite, for a general line of type $(1,0)$ on T we have $G \cap \phi(F) = \emptyset$. Hence there is $G' \subset Y \setminus F$ such that $\phi(G') = G$. Let $B \subset X$ be the only set such that $\ell_P(B) = F \cup G'$. Since $\sharp(B) \leq \beta(X)$, we have $\dim(\langle B \rangle) = d-2$. Since G is linearly dependent, $F \cup G'$ is linearly dependent. Hence $P \in \langle B \rangle$. Since $A \cap B = \emptyset$ and $\beta(X) = d+1 \leq \sharp(A \cup B)$, we have $\langle A \cup B \rangle = \mathbb{P}^d$. Hence Grassmann's formula gives that $\langle A \rangle \cap \langle B \rangle$ is a single point. Hence $\{P\} = \langle A \rangle \cap \langle B \rangle$. Hence $ir_X(P) \leq d-1$ and $\alpha(X,P) \leq d+2$. Since we proved the opposite inequalities, we are done. □

Theorem 4. *Fix integers $m \geq 1$ and $d \geq 3$. Set $n := n_{m,d} := \binom{m+d}{m} - 1$ and $X := X_{m,d}$. Fix $P \in \sigma_2(X_{m,d}) \setminus X$.*

(a) Assume $P \notin \tau(X)$, i.e. assume $r_X(P) = 2$. Then $ir_X(P) = d$, $z_X(P) = 2$, $iz_X(P) = d$ and $\alpha(X,P) = \gamma(X,P) = d+2$

(b) Assume $P \in \tau(X)\backslash X$. Then $z_X(P) = 2$, $iz_X(P) = ir_X(P) = d$, $\gamma(X,P) = d+2$. If $m = 1$, then $\alpha(X,P) = d^2$. If $m \geq 2$, then $\alpha(X,P) = 3d$.

Proof. Since $d \geq 3$, we have $\sigma_2(X) \neq \tau(X)$, $\sigma_2(X) \setminus \tau(X) = \{P \in \sigma_2(X) : r_X(P) = 2\}$ and $r_X(P) = d$ for each $P \in \tau(X) \setminus X$ ([8], Theorem 32). Since the case $m = 1$ is true (Propositions 5 and 6), we assume $m \geq 2$. Since $\beta(X) = d+1$ (e.g. by [8], Lemma 34), Remark 3 and Lemma 3 imply the existence of a unique zero-dimensional scheme $Z \subset X$ such that $\deg(Z) = 2$ and $P \in \langle Z \rangle$. We have $r_X(P) = 2$ if and only if Z is reduced. Let $A \subset \mathbb{P}^m$ be the degree 2 zero-dimensional scheme such that $\nu_d(A) = Z$. Let $L \subset \mathbb{P}^m$ be the line spanned by A. Set $R := \nu_d(L)$. Since $Z \subset R$, we have $r_X(P) \leq r_R(P)$, $z_X(P) \leq z_R(P)$, $ir_X(P) \leq ir_R(P)$, $iz_X(P) \leq iz_R(P)$, $\alpha(X,P) \leq \alpha(R,P) = d$ and $\gamma(X,P) \leq \gamma(R,P)$. Propositions 5 and 6 give $ir_R(P) = iz_R(P) = d$ and $\gamma(R,P) = d+2$. Let $W \subset \mathbb{P}^m$ be a zero-dimensional scheme such that $P \in \langle \nu_d(W) \rangle$, $P \notin \langle \nu_d(W') \rangle$ for any $W' \subsetneq W$ and $W \neq A$. Since $\beta(X) \geq d+1$, Lemma 3 gives $\deg(W) \geq d$. Hence $iz_X(P) \geq d$ and $\gamma(X,P) \geq d+2$. Hence $ir_X(P) = iz_X(P) = d+2$ and $\gamma(X,P) = d+2$. In case (a) we have $\alpha(X,P) = d+2$, because $\alpha(R,P) = d+2$ (Proposition 5). Now assume that Z is not reduced, i.e. assume $P \in \tau(X)$. Let $C \subset \mathbb{P}^m$ be a smooth conic containing A. The curve $\nu_d(C)$ is a degree $2d$ rational normal curve in its linear span. Since $P \in \langle Z \rangle \subset \langle \nu_d(C) \rangle$, the " Moreover " part of Proposition 6 applied to $\nu_d(C)$ gives the existence of a set $B \subset C$ such that $\sharp(B) = 2d$ and $\langle Z \rangle \cap \langle \nu_d(B) \rangle = \{P\}$. Let $M \subseteq \mathbb{P}^m$ be the plane containing $C \cup L$. Since the restriction maps $H^0(\mathbb{P}^m, \mathcal{O}_{\mathbb{P}^m}(d)) \to H^0(M, \mathcal{O}_M(d))$ and $H^0(M, \mathcal{O}_M(d)) \to H^0(T, \mathcal{O}_T(d))$ are surjective for $T = L$, $T = C$, and $T = C \cup L$, we get $\dim(\langle \nu_d(C \cup L) \rangle) = 3d-1$, $\dim(\langle \nu_d(C) \rangle) = 2d$ and $\dim(\langle R \rangle) = d$. Hence Grassmann's formula gives $\langle \nu_d(C) \rangle \cap \langle R \rangle = \langle Z \rangle$. Fix $E \subset L$ such that $\{P\} = \langle Z \rangle \cap \langle \nu_d(E) \rangle$ (the " Moreover " part of Proposition 6). Since $\nu_d(E) \subset R$, P is the only point in the intersection of $\langle \nu_d(B) \rangle \subset \langle \nu_d(C) \rangle$ and $\langle \nu_d(E)$. Hence $\alpha(X,P) \leq 3d$. Now assume $a := \alpha(X,P) < 3d$ and take $S = S_1 \cup \cdots \cup S_k \subset \mathbb{P}^m$ such that $\sharp(S) = a$ and $\{P\} = \cap_{i=1}^k \langle \nu_d(S_i) \rangle$. We proved that $\sharp(S_i) \geq d$ for all i. Hence $k = 2$, $2d \leq a \leq 3d-1$ and $d \leq \sharp(S_i) \leq 2d-1$ for all i.

Claim: Take a finite set $E \subset \mathbb{P}^m$ such that $P \in \langle \nu_d(E) \rangle$, $P \notin \langle E' \rangle$ for any $E' \subsetneq E$, $E \neq A$, and $\deg(E) \leq 2d-1$. Then $E \subset L$.

Proof of the Claim: Since $P \in \langle Z \rangle$, Lemma 3 and [8], Lemma 34, give the existence of a line $D \subset \mathbb{P}^m$ such that $\deg(D \cap (E \cup A)) \geq d+2$. First we will check that $E \subset D$ and then we will see that $D = L$. Let $H \subset \mathbb{P}^m$ be a general hyperplane containing D. Since E is reduced, A is curvilinear and H is general, we have $H \cap (A \cup E) = D \cap (A \cup E)$. Let $\mathrm{Res}_H(A \cup E)$ denote the residual scheme of $A \cup E$ with respect to H, i.e. the closed subscheme of $\mathbb{P}^m$ with $\mathcal{I}_{A\cup E} : \mathcal{I}_H$ as its ideal sheaf. Since $\deg(\mathrm{Res}_H(A \cup E)) = \deg(A \cup E) - \deg((A \cup E) \cap H)) \leq d$, we have $h^1(\mathbb{P}^m, \mathcal{I}_{\mathrm{Res}_H(A\cup E)}(d-1)) = 0$. Since A is connected and not reduced, [6], Lemma 4, gives $A \cup E \subset H$. Since this is true for a general H containing D, we get $E \subset D$. We also get $A \subset D$ and hence $D = L$.

Apply the Claim first to S_1 and then to S_2. We get $S \subset L$. Hence $\alpha(X,P) = \alpha(R,P) = d^2$, a contradiction. □

Remark 5. Fix a linear subspace $U \subsetneq \mathbb{P}^m$ and take $P \in \langle \nu_d(U)\rangle$. We have $r_{X_{m,d}}(P) = r_{\nu_d(U)}(P)$ ([21], Proposition 3.1) and every $S \subset X$ evincing $r_X(P)$ is contained in $\nu_d(U)$ ([19], Exercise 3.2.2.2). Part (b) of Theorem 4 shows that sometimes $ir_X(P) < ir_{\nu_d(U)}(P)$.

Theorem 5. *Assume $m \ge 2$ and $d \ge 5$. Fix a finite set $A \subset \mathbb{P}^m$ such that $\sharp(A) = 3$. Set $X := X_{m,d}$ and $n := \binom{m+d}{m} - 1$. Fix $P \in \langle \nu_d(A)\rangle$ such that $P \notin \langle \nu_d(A')\rangle$ for any $A' \subsetneq A$.*

(a) Assume that A is contained in a line. Then $r_X(P) = z_X(P) = 3$, $ir_X(P) = iz_X(P) = d-1$ and $\alpha(X,P) = \gamma(X,P) = d+2$.

(b) Assume that A is not contained in a line. Then $r_X(P) = z_X(P) = 3$ and $\alpha(X,P) = 2d+2$.

Proof. Since $\beta(X) \ge 5$, $\nu_d(A)$ is the only subscheme of X with degree ≤ 3 whose linear span contains P. Hence $r_X(P) = z_X(P) = 3$. Since $\beta(X) = d+2$, Lemma 3 also gives $ir_X(P) \ge iz_X(P) \ge d-1$ and $\alpha(X,P) \ge \gamma(X,P) \ge d+2$.

First assume the existence of a line $L \subset \mathbb{P}^m$ such that $A \subset L$. Set $R := \nu_d(L)$. Since $P \in \langle R\rangle$, Proposition 7 gives $ir_X(P) \le ir_R(P) = d-1$, $iz_X(P) \le iz_R(P) = d-1$, $\alpha(X,P) \le \alpha(R,P) = d+2$ and $\gamma(X,P) \le \gamma(R,P) = d+2$, concluding the proof of part (a).

Now assume that A is not contained in a line. Write $A = \{O_1,O_2,O_3\}$. Fix $i \in \{1,2,3\}$ and set $\{j,h\} := \{1,2,3\}\setminus\{i\}$. Set $L_i := \langle\{O_j,O_h\}\rangle \subset \mathbb{P}^m$. Since $P \in \langle \nu_d(A)\rangle$ and $P \notin \langle \nu_d(A')\rangle$ for any $A' \subsetneq A$, the set $\langle\{P,\nu_d(O_i)\}\rangle \cap \langle\{\nu_d(O_h),\nu_d(O_j)\}\rangle$ is a single point, P_i. Notice that $P_i \in \langle \nu_d(L_i)\rangle$ and that $r_{\nu_d(L_i)}(P_i) = 2$. The " Moreover " part of Proposition 5 gives the existence of a set $E_i \subset L_i$ such that $\sharp(S_i) = d$ and $\{P_i\} = \langle\{\nu_d(O_h),\nu_d(O_j)\}\rangle \cap \langle \nu_d(E_i)\rangle$. Hence $\langle \nu_d(A)\rangle \cap \langle \nu_d(\{O_i\}\cup E_i)\rangle$ is the line $\langle\{\nu_d(O_i),P_i\}\rangle$. Taking the intersection of two of these lines we get $ir_X(P) \le d+1$ and $\alpha(X,P) \le 2d+2$. Since $r_X(P) = d+1$ (proof of this case in [8], Theorem 37), we get $ir_X(P) = d+1$. Lemma 3 also gives $iz_X(P) \ge d+1$ and that for each subscheme $W \subset \mathbb{P}^m$ with $\deg(W) \le d+1$ and $P \in \langle W\rangle$ we have $W \supseteq A$. Hence $iz_X(P) = d+1$. Assume $a := \alpha(X,P) \le 2d+1$ and take $S = S_1 \cup \cdots \cup S_k$ with $\{P\} = \cap_{i=1}^k \langle \nu_d(S_i)\rangle$ and $\sharp(S_1) + \cdots + \sharp(S_k) = a$. Since $a \le 2d+1$ and each subscheme $W \subset \mathbb{P}^m$ with $\deg(W) \le d+1$ and $P \in \langle W\rangle$ contains A, we get $k=2$ and that one of the sets S_i is just A. Since $P \in \langle S_1\rangle \cap \langle S_2\rangle$, $P \notin \langle U\rangle$ for any $U \subsetneq S_i$, $i = 1,2$, and $\sharp(S_1 \cup S_2) \le 2d+1$, there is a line $D \subset \mathbb{P}^m$ such that $\sharp(D \cap (S_1 \cup S_2)) \ge d+2$ and $S_1 \setminus S_1 \cap D = S_2 \setminus S_2 \cap D$ ([6], Lemma 4). Since $S_1 \cap S_2 = \emptyset$, we get $S_1 \cup S_2 \subset D$. Since A is not contained in a line and $A = S_i$ for some i, we get a contradiction. □

References

[1] B. Ådlandsvik, Joins and higher secant varieties. Math. Scand. **62** (1987), 213–222.

[2] L. Albera, P. Chevalier, P. Comon and A. Ferreol, On the virtual array concept for higher order array processing. IEEE Trans. Sig. Proc., **53** (2005), no. 4, 1254–1271.

[3] E. Ballico, On strange projective curves. Rev. Roum. Math. Pures Appl. **37** (1992), 741–745.

[4] E. Ballico, An upper bound for the X-ranks of points of $\mathbb{P}^n$ in positive characteristic. Albanian J. Math. **5** (2011), no. 1, 3–10.

[5] E. Ballico and A. Bernardi, Decomposition of homogeneous polynomials with low rank. Math. Z. **271** (2012) 1141–1149.

[6] E. Ballico and A. Bernardi, Stratification of the fourth secant variety of Veronese variety via the symmetric rank. Adv. Pure Appl. Math. **4** (2013), no. 2, 215–250; DOI: 10.1515/apam-2013-0015

[7] V. Bayer and A. Hefez, Strange plane curves. Comm. Algebra **19** (1991), no. 11, 3041–3059.

[8] A. Bernardi, A. Gimigliano and M. Idà, On the stratification of secant varieties of Veronese varieties via symmetric rank. J. Symbolic. Comput. **46** (2011), no. 1, 34–53.

[9] A. Bernardi and K. Ranestad, The cactus rank of cubic forms. J. Symbolic. Comput. 50 (2013) 291–297. DOI: 10.1016/j.jsc.2012.08.001

[10] W. Buczyńska and J. Buczyński, Secant varieties to high degree Veronese reembeddings, catalecticant matrices and smoothable Gorenstein schemes. J. Algebraic Geometry 23 (2014) 63–90 S 1056-3911(2013)00595-0

[11] J. Buczyński, A. Ginensky and J. M. Landsberg, Determinantal equations for secant varieties and the Eisenbud-Koh-Stillman conjecture. J. London Math. Soc. (2) **88** (2013), 1–24; doi:10.1112/jlms/jds073

[12] J. Buczyński and J. M. Landsberg, Ranks of tensors and a generalization of secant varieties. Linear Algebra Appl. **438** (2013), no. 2, 668–689.

[13] L. Chiantini and C. Ciliberto, On the concept of k-secant order of a variety. J. London Math. Soc. (2) **73** (2006), no. 2, 436–454.

[14] G. Comas and M. Seiguer, On the rank of a binary form. Found. Comp. Math. **11** (2011), no. 1, 65–78.

[15] P. Comon, G. Golub, L.-H. Lim and B. Mourrain, Symmetric tensors and symmetric tensor rank. SIAM Journal on Matrix Analysis Appl. **30** (2008), no. 3, 1254–1279.

[16] A. Couvreur, The dual minimum distance of arbitrary dimensional algebraic-geometric codes. J. Algebra **350** (2012), no. 1, 84–107.

[17] R. Hartshorne, Algebraic Geometry. Springer, Berlin, 1977.

[18] J.-P. Jouanolou, Théorèmes de Bertini et applications. Progress in Mathematics, 42. Birkhäuser Boston, Inc., Boston, MA, 1983.

[19] J. M. Landsberg, Tensors: Geometry and Applications. Graduate Studies in Mathematics, Vol. 128, Amer. Math. Soc. Providence, 2012.

[20] J. M. Landsberg and Z. Teitler, On the ranks and border ranks of symmetric tensors. Found. Comput. Math. **10** (2010), no. 3, 339–366.

[21] L. H. Lim, V. de Silva, Tensor rank and the ill-posedness of the best low-rank approximation problem. SIAM J. Matrix Anal. Appl. **30** (2008), no. 3, 1084–1127.

[22] J. Rathmann, The uniform position principle for curves in characteristic p. Math. Ann. **276** (1987), no. 4, 565–579.

[23] J. Silverman, The arithmetic of elliptic curves, Springer, Berlin, 1986.

ALBANIAN JOURNAL OF MATHEMATICS
Volume 8, Number 1, Pages 23–35
ISSN: 1930-1235; (**2014**)

CLASSIFYING FAMILIES OF SUPERELLIPTIC CURVES

Rezart Muço
Research Institute of Science and Technology
Vlora, Albania
Email: rmuco@risat.org

Nejme Pjero
Research Institute of Science and Technology
Vlora, Albania
Email: npjero@risat.org

Ervin Ruci
Geolitica Inc.
Ottawa, Canada
Email: eruci@risat.org

Eustrat Zhupa
UIST "St. Paul the Apostle"
Ohrid, Macedonia
Email: eustrat.zhupa@uist.edu.mk

Abstract. This paper is the first version of a project of classifying all superelliptic curves of genus $g \leq 48$ according to their automorphism group. We determine the parametric equations in each family, the corresponding signature of the group, the dimension of the family, and the inclussion among such families. At a later stage it will be determined the decomposition of the Jacobians and each locus in the moduli spaces of curves.

1. Introduction

In this paper we study some very classical problems related to algebraic curves and the possibility of organizing such results in a database of curves. Such information would be quite useful to researchers working on coding theory, cryptography, mathematical physics, quantum computing, etc.

In section 2 we give a brief review of the background on algebraic curves. Throughout this paper, by "curve" we mean a smooth, irreducible algebraic curve, defined over an algebraically closed field k of characteristic zero. For the reader

2000 *Mathematics Subject Classification.* 11G30 and 11G50 and 14G40.
Key words and phrases. superelliptic curves and field of moduli and minimal field of definition.

who is interested in details and full treatment of the subject we suggest the classical books [1,2,7,8].

Identifying isomorphic classes of algebraic curves is a fundamental problem of algebraic geometry which goes bach to the XIX century mathematics as a branch of invariant theory. Especially of interest are invariants of binary forms as they determine the isomorphic classes of hyperelliptic curves and superelliptic curves (cf. Section 5).

In section 3 we give the basic background of the binary forms and their invariants. In section 5 we discuss in more detail superelliptic curves. We define such curves and describe their automorphism groups and the signature σ of the covering $\mathcal{X}_g \to \mathcal{X}_g/G$. The Hurwitz space $\mathcal{H}(g, G, \sigma)$ is a quasi-projective variety and the dimension and irreducibility can be determined as explained in section 5. Such information enables us to fully understand such families of superelliptic curves. Identifying the isomorphism classes of such curves can be done via the invariants of binary forms (see Section 3) or the dihedral invariants as defined in [4].

In section 5 we propose the idea of creating a database for all the algebraic curves. The superelliptic curves consist of the bulk of the cases. We propose what invariants need to be included in this database based on the fact that how easy it is to compute such invariants. The main criteria of this proposed database is the automorphism group. Each family of curves with fixed genus $g \geq 2$, group G, and signature σ defines a locus in $\mathcal{M}_g$. We compute the dimension and the irreducibility of such loci and an equation of such loci whenever possible. For each family we discuss the decomposition of the corresponding Jacobians. Some computational packages are given as examples for curves of small genus. We don't describe in details the mathematics behind such computer packages but for the interested reader they can be found in [13,14] and others.

2. Preliminaries on curves

By a *curve* we mean a complete reduced algebraic curve over $\mathbb{C}$ which might be singular or reducible. A *smooth curve* is implicitly assumed to be irreducible. The basic invariant of a smooth curve C is its genus which is half of the first Betti number of the underlying topological space. We will denote the genus of C by $g(C) = \frac{1}{2} \operatorname{rank} \left(H^1(C, \mathbb{Z})\right)$.

Let $f : \mathcal{X} \to \mathcal{Y}$ be a non-contant holomorphic map between smooth curves $\mathcal{X}$ and $\mathcal{Y}$ of genera g and g'. For any $q \in \mathcal{X}$ and $p = f(q)$ in $\mathcal{Y}$ chose local coordinates z and w centered at q and p such that f has the standart form $w = z^{\nu(q)}$. Then, for any p on C' define

$$f^\star(p) = \sum_{q \in f^{-1}(p)} \nu(q) q.$$

If D is any divisor on $\mathcal{X}$ then define $f^\star(D)$ to be the divisor on $\mathcal{X}$ by extending the above $f^\star(p)$. The degree of n the divisor $f^\star(p)$ is independent of p and is called the *degree* of the map f. The *ramification divisor* R on C of the map f is defined by

$$R = \sum_{q \in C} \left(\nu(p) - 1\right) q$$

The integer $\nu(q) - 1$ is called the *ramification index* of f at q. For any meromorphic differential ϕ on C' we have

$$(f^\star(\phi)) = f^\star\left((\phi)\right) + R$$

Counting degrees we get the Riemann-Hurwitz formula

$$2g - 2 = n(2g' - 2) + \deg R$$

Let $\mathcal{X}_g$ be a genus $g \geq 2$ curve and G its automorphism group (i.e, the group of automorphisms of the function field $\mathbb{C}(\mathcal{X}_g)$). That G is finite will be shown in section **??** using Weierstrass points.

Assume $|G| = n$. Let L be the fixed subfield of $\mathbb{C}(\mathcal{X}_g)$. The field extension $\mathbb{C}(\mathcal{X}_g)/L$ correspond to a finite morphism of curves $f : \mathcal{X}_g \to \mathcal{X}_g/G$ of degree n. Denote the genus of the quotient curve $\mathcal{X}_g/G$ by g' and R the ramification divisor. Assume that the covering has s branch points. Each branch point q has n/e_P points in its fiber $f^{-1}(q)$, where e_P is the ramification index of such points $P \in f^{-1}(q)$.

Then, $R = \sum_{i=1}^{s} \frac{n}{e_P}(e_P - 1)$. By the Riemann-Hurwitz formula we have

$$\frac{2}{n}(g-1) = 2g' - 2 + \frac{1}{n}\deg R = 2g' - 2 + \sum_{i=1}^{s}\left(1 - \frac{1}{e_P}\right)$$

Since $g \geq 2$ then the left hand side is > 0. Then

$$2g' - 2 + \sum_{i=1}^{s}\left(1 - \frac{1}{e_P}\right) \geq 0.$$

The fact that g', s, and e_P are non-negative integers implies that the minimum value of this expression is $1/42$. This implies that $n \leq 84(g-1)$.

Next we define another important invariant of the algebraic curves. Let $w_1, \dots, w_g$ be a basis of $H^0(C, K)$ and $\gamma_1, \dots, \gamma_{2g}$ a basis for $H_1(C, \omega)$. The *period matrix* Ω is the $g \times 2g$ matrix $\Omega = \left[\int_{\gamma_i} w_j\right]$. The collumn vectors of the period matrix generate a lattice Λ in $\mathbb{C}^g$, so that the quotient $\mathbb{C}^g/\Lambda$ is a complex torus. This complex torus is called the *Jacobian variety* of C and denoted by the symbol $J(C)$. For more details see [1] or [8].

If $\Lambda \subset \Lambda'$ are lattices of rank $2n$ in $\mathbb{C}^n$ and $A = \mathbb{C}^n/\Lambda$, $B = \mathbb{C}^n/\Lambda'$, then the induced map $A \to B$ is an *isogeny* and A and B are said to be *isogenous.*

The *moduli space* $\mathcal{M}_g$ of curves of genus g is the set of isomorphism classes of smooth, genus g curves. $\mathcal{M}_g$ has a natural structure of a quasi-projective normal variety of dimension $3g-3$. The compactification $\bar{\mathcal{M}}_g$ of $\mathcal{M}_g$ consists of isomorphism classes of stable curves. A *stable curve* is a curve whose only singularities are nodes and whose smooth rational components contain at least three singular points of the curve; see [1, pg. 29] and [2, Chapter XII]. $\bar{\mathcal{M}}_g$ is a projective variety

Both $\mathcal{M}_g$ and $\bar{\mathcal{M}}_g$ are singular. All the singularities arise from curves with nontrivial automorphism group. It is precisely such curves that we intend to classify in this paper.

2.1. Automorphism groups.

2.2. Superelliptic curves. A curve $\mathcal{X}$ is called superelliptic if there exist an element $\tau \in \text{Aut}(\mathcal{X})$ such that τ is central and $g(\mathcal{X}/\langle\tau\rangle) = 0$. Denote by K the function field of $\mathcal{X}_g$ and assume that the affine equation of $\mathcal{X}_g$ is given some polynomial in terms of x and y.

Let $H = \langle\tau\rangle$ be a cyclic subgroup of G such that $|H| = n$ and $H \triangleleft G$, where $n \geq 2$. Moreover, we assume that the quotient curve $\mathcal{X}_g/H$ has genus zero. The **reduced automorphism group of $\mathcal{X}_g$ with respect to H** is called the group $\Gamma := G/H$, see [4], [11].

Assume $k(x)$ is the genus zero subfield of K fixed by H. Hence, $[K : k(x)] = n$. Then, the group Γ is a subgroup of the group of automorphisms of a genus zero field. Hence, $\Gamma < PGL_2(k)$ and Γ is finite. It is a classical result that every finite subgroup of $PGL_2(k)$ is isomorphic to one of the following: C_m, D_m, A_4, S_4, A_5.

The group Γ acts on $k(x)$ via the natural way. The fixed field of this action is a genus 0 field, say $k(z)$. Thus, z is a degree $|\Gamma| := m$ rational function in x, say $z = \phi(x)$. G is a degree n extension of Γ and Γ is a finite subgroup of $PGL_2(k)$. Hence, if we know all the possible groups that occur as Γ then we can determine G and the equation for K. The list of all groups of superelliptic curves and their equations are determined in [11] and [12].

Let C be a superelliptic curve given by the equation

$$y^n = f(x),$$

where $\deg f = d$ and $\Delta(f, x) \neq 0$. Assume that $d > n$. Then C has genus

$$g = \frac{1}{2}\Big(n(d-1) - d - \gcd(n, d)\Big) + 1$$

Moreover, if n and d are relatively prime then $g = \frac{(n-1)(d-1)}{2}$, see [4] for details.

3. Invariants of binary forms

In this section we define the action of $GL_2(k)$ on binary forms and discuss the basic notions of their invariants. Let $k[X, Z]$ be the polynomial ring in two variables and let V_d denote the $(d + 1)$-dimensional subspace of $k[X, Z]$ consisting of homogeneous polynomials.

$$f(X, Z) = a_0X^d + a_1X^{d-1}Z + \cdots + a_dZ^d \tag{3.1}$$

of degree d. Elements in V_d are called *binary forms* of degree d. We let $GL_2(k)$ act as a group of automorphisms on $k[X, Z]$ as follows:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k), \ \textit{then} \quad M\begin{pmatrix} X \\ Z \end{pmatrix} = \begin{pmatrix} aX + bZ \\ cX + dZ \end{pmatrix} \tag{3.2}$$

This action of $GL_2(k)$ leaves V_d invariant and acts irreducibly on V_d.

Remark 3.1. It is well known that $SL_2(k)$ leaves a bilinear form (unique up to scalar multiples) on V_d invariant. This form is symmetric if d is even and skew symmetric if d is odd.

Let A_0, A_1, ..., A_d be coordinate functions on V_d. Then the coordinate ring of V_d can be identified with $k[A_0, \dots, A_d]$. For $I \in k[A_0, \dots, A_d]$ and $M \in GL_2(k)$, define $I^M \in k[A_0, \dots, A_d]$ as follows

$$I^M(f) := I(M(f)) \tag{3.3}$$

for all $f \in V_d$. Then $I^{MN} = (I^M)^N$ and Eq. (3.3) defines an action of $GL_2(k)$ on $k[A_0, \dots, A_d]$. A homogeneous polynomial $I \in k[A_0, \dots, A_d, X, Z]$ is called a *covariant* of index s if $I^M(f) = \delta^s I(f)$, where $\delta = \det(M)$. The homogeneous degree in $a_1, \dots, a_n$ is called the *degree* of I, and the homogeneous degree in X, Z is called the *order* of I. A covariant of order zero is called *invariant*. An invariant is a $SL_2(k)$-invariant on V_d.

We will use the symbolic method of classical theory to construct covariants of binary forms. Let

$$f(X,Z) := \sum_{i=0}^{n} \binom{n}{i} a_i X^{n-i} Z^i, \quad \textit{and} \quad g(X,Z) := \sum_{i=0}^{m} \binom{m}{i} b_i X^{n-i} Z^i$$

be binary forms of degree n and m respectively with coefficients in k. We define the **r-transvection** as in [10]. It is a homogeneous polynomial in $k[X,Z]$ and therefore a covariant of order $m+n-2r$ and degree 2. In general, the r-transvection of two covariants of order m,n (resp., degree p,q) is a covariant of order $m+n-2r$ (resp., degree $p+q$).

For the rest of this paper $F(X,Z)$ denotes a binary form of order $d := 2g+2$ as below

$$F(X,Z) = \sum_{i=0}^{d} a_i X^i Z^{d-i} = \sum_{i=0}^{d} \binom{n}{i} b_i X^i Z^{n-i} \tag{3.4}$$

where $b_i = \frac{(n-i)!\ i!}{n!} \cdot a_i$, for $i = 0, \dots, d$. We denote invariants (resp., covariants) of binary forms by I_s (resp., J_s) where the subscript s denotes the degree (resp., the order). We define the following covariants and invariants:

$$\begin{aligned}
I_2 &:= (F,F)^d, & J_{4j} &:= (F,F)^{d-2j}, \ j = 1, \dots, g, \\
I_4 &:= (J_4,J_4)^4, & I_4' &:= (J_8,J_8)^8, \\
I_6 &:= ((F,J_4)^4, (F,J_4)^4)^{d-4}, & I_6' &:= ((F,J_8)^8, (F,J_8)^8)^{d-8}, \\
I_6^* &:= ((F,J_{12})^{12}, (F,J_{12})^{12})^{d-12}, & I_3 &:= (F,J_d)^d, \\
M &:= ((F,J_4)^4, (F,J_8)^8)^{d-10}, & I_{12} &:= (M,M)^8
\end{aligned} \tag{3.5}$$

Absolute invariants are called $GL_2(k)$-invariants. We define the following absolute invariants:

$$i_1 := \frac{I_4'}{I_2^2},\ i_2 := \frac{I_3^2}{I_2^3},\ i_3 := \frac{I_6^*}{I_2^3},\ j_1 := \frac{I_6^{'}}{I_3^2},\ j_2 := \frac{I_6}{I_3^2},\ s_1 := \frac{I_6^2}{I_{12}},\ s_2 := \frac{(I_6^{'})^2}{I_{12}}$$

$$\mathfrak{v}_1 := \frac{I_6}{I_6^*},\ \mathfrak{v}_2 := \frac{(I_4^{'})^3}{I_3^4},\ \mathfrak{v}_3 := \frac{I_6}{I_6^{'}},\ \mathfrak{v}_4 := \frac{(I_6^*)^2}{I_4^3}.$$

In the case $g = 10$ and $I_{12} = 0$ we define

$$\begin{aligned}
I_6^\star &:= ((F,J_{16})^{16}, (F,J_{16})^{16})^{d-16}), \\
S &:= (J_{12},J_{16})^{12}, \\
I_{12}^* &:= (\,(J_{16},S)^4,\ (J_{16},S)^4\,)^{12}
\end{aligned} \tag{3.6}$$

and

$$\mathfrak{v}_5 := \frac{I_6^\star}{I_{12}^*}.$$

For a given curve $\mathcal{X}_g$ we denote by $I(\mathcal{X}_g)$ or $i(\mathcal{X}_g)$ the corresponding invariants.

3.1. **Invariants of binary Sextics.** Let $f(X,Y)$ be the binary sextic $f(X,Y) = \sum_{i=0}^{6} a_i X^i Y^{6-i}$, defined over an algebraically closed field k. We define the following covariants:

$$H = (f,f)^2, \quad i = (f,f)^4, \quad l = (i,f)^3, \tag{3.7}$$

Then, the following

$$\begin{aligned} J_2 &= (f,f)^6, & J_4 &= (i,i)^4, \\ J_6 &= (l,l)^2, & J_{10} &= (f,l^3)^6, \end{aligned} \tag{3.8}$$

are $SL_2(k)$- invariants; see [13] for details.

The absolute invariants t_1, t_2 and t_3 called absolute invariants are:

$$t_1 = \frac{J_2^5}{J_{10}}, \qquad t_2 = \frac{J_2^3 \cdot J_4}{J_{10}}, \qquad t_3 = \frac{J_2^2 \cdot J_6}{J_{10}}, \tag{3.9}$$

Lemma 3.2. *Two genus two curves C and C' are isomorphicm if and only if they have the same absolute invariants.*

3.2. **Invariants of binary octavics.** Let $f(X,Y)$ be the binary octavic $f(X,Y) = \sum_{i=0}^{8} a_i X^i Y^{8-i}$. defined over an algebraically closed field k. We define the following covariants:

$$\begin{aligned} &g = (f,f)^4, \quad k = (f,f)^6, \quad h = (k,k)^2, \\ &m = (f,k)^4, \quad n = (f,h)^4, \quad p = (g,k)^4, \quad q = (g,h)^4, \end{aligned} \tag{3.10}$$

where the operator $(\cdot,\cdot)^n$ denotes the n-th transvection of two binary forms; see [13] among many other references. Then, the following

$$\begin{aligned} J_2 &= 2^2 \cdot 5 \cdot 7 \cdot (f,f)^8, & J_3 &= \frac{1}{3} \cdot 2^4 \cdot 5^2 \cdot 7^3 \cdot (f,g)^8, \\ J_4 &= 2^9 \cdot 3 \cdot 7^4 \cdot (k,k)^4, & J_5 &= 2^9 \cdot 5 \cdot 7^5 \cdot (m,k)^4, \\ J_6 &= 2^{14} \cdot 3^2 \cdot 7^6 \cdot (k,h)^4, & J_7 &= 2^{14} \cdot 3 \cdot 5 \cdot 7^7 \cdot (m,h)^4, \\ J_8 &= 2^{17} \cdot 3 \cdot 5^2 \cdot 7^9 \cdot (p,h)^4, & J_9 &= 2^{19} \cdot 3^2 \cdot 5 \cdot 7^9 \cdot (n,h)^4, \\ J_{10} &= 2^{22} \cdot 3^2 \cdot 5^2 \cdot 7^{11} (q,h)^4 \end{aligned} \tag{3.11}$$

are $SL_2(k)$- invariants; see [13] for details.

Next, we define $GL(2,k)$-invariants as follows

$$t_1 := \frac{J_3^2}{J_2^3}, \quad t_2 := \frac{J_4}{J_2^2}, \quad t_3 := \frac{J_5}{J_2 \cdot J_3}, \quad t_4 := \frac{J_6}{J_2 \cdot J_4}, \quad t_5 := \frac{J_7}{J_2 \cdot J_5}, \quad t_6 := \frac{J_8}{J_2^4},$$

There is an algebraic relation

$$T(t_1, \dots, t_6) = 0 \tag{3.12}$$

that such invariants satisfy, computed in [13]. The field of invariants $\mathcal{S}_8$ of binary octavics is $\mathcal{S}_8 = k(t_1, \dots, t_6)$, where $t_1, \dots, t_6$ satisfies the equation $T(t_1, \dots, t_6) = 0$. Hence, we have an explicit description of the hyperelliptic moduli $\mathcal{H}_3$; see [13] for details.

Throughout this paper we will use the following important result

Lemma 3.3 (Shaska [13]). *Two genus 3 hyperelliptic curves C and C', defined over an algebraically closed field k of characteristic zero, with J_2, J_3, J_4, J_5 nonzero are isomorphic over k if and only if $t_i(C) = t_i(C')$, for $i = 1, \dots 6$.*

In the cases of curves when $t_1, \dots, t_6$ are not defined we will define new invariants as suggested in [13]. From [13, Lemma 4] we know that $J_2, \dots, J_7$ can't all be 0, otherwise the binary form would have a multiple root.

3.3. **Invariants of binary decimics.** Let $f(X,Y)$ be the binary decimic defined over an algebraically closed field k. We define the following covariants:

$$\begin{aligned} &k = (f,f)^8, \quad q = (f,f)^6, \quad m = (m,k)^4, \\ &r = (f,q)^8, \quad k_q = (q,q)^6, \quad k_m = (m,m)^4, \quad m_q = (q,k_q)^4 \end{aligned} \tag{3.13}$$

and the following invariants:

$$\begin{aligned} J_2 &= (f,f)^{10}, & A_6 &= (m,m)^6, \\ J_4 &= (k,k)^4, & C_6 &= (r,r)^2, \\ J_8 &= (k,k_m)^4, & J_{14} &= ((k_q,k_q)^2, m_q)^4, \\ J_9 &= ((k,m)^1, k\cdot k)^8, & A_{14} &= ((k,k)^2 \cdot (k,k)^2, (m,m)^2)^8, \\ J_{10} &= ((m,m)^2, k\cdot k)^8 \end{aligned} \tag{3.14}$$

Theorem 3.4. *The eight invariants J_2, J_4, A_6, C_6, J_8, J_9, J_{10}, $J_{14} + A_{14}$ form a homogeneous system of parameters for the ring $\mathcal{O}(V_n)^{SL_2}$ of invariants of the binary decimics.*

For the proof the reader can check [6]. We still do not know a set of $GL_2(k)$-invariants for the binary decimics.

4. A list of all superelliptic curves with extra automorphisms

To create a database of algebraic curves which contains enough information we have to start with superelliptic curves as the simplest cases of all the families. It turns out that the superelliptic curves are the overwhelming majority of automorphism groups of curves for any fixed genus.

In the tables below are displayed all superelliptic curves for genus $5 \leq g \leq 10$. The cases for $g < 5$ have appeared before in the literature. The first column of the table represents the case from Table 1 of [11], the second column is the reduced automorphism group. In the third column we put information about the full automorphism group. Such groups are well known and we only display the 'obvious' cases, for full details one can check [11] and [12].

In the fourth column is the level n of the superelliptic curve; see [4]. Hence, the equation of the curve is given by $y^n = f(x)$, where $f(x)$ is the polynomial displayed in the last column. Columns 5 and 6 respectively represent the order of an automorphism in the reduced automorphism group and the signature of the covering $\mathcal{X} \to \mathcal{X}/G$. The sixth column represents the dimension of the corresponding locus in the moduli space $\mathcal{M}_g$. Throughout these tables $f_1(x)$ is as follows

$$f_1(x) = x^{12} - a_1 x^{10} - 33x^8 + 2a_1 - 33x^4 - a_1 x^2 + 1$$

The signatures of the coverings are not fully given. Indeed, for a full signature $(\sigma_1, \dots, \sigma_r)$ we know that $\sigma_1 \cdots \sigma_r = 1$. Hence, $\sigma_r = \sigma_{r-1}^{-1} \cdots \sigma_1^{-1}$. We do not present σ_r.

Table 1. Superelliptic curves for genus $5 \leq g \leq 10$

Nr.	$\bar{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
				Genus 5			
1	C_m	C_2^2	2	2	2^7	5	$x^{12} + \sum_{i=1}^{5} a_i x^{2i} + 1$
1		$C_3 \times C_2$	2	3	$2^3, 3^2$	3	$x^{12} + \sum_{i=1}^{3} a_i x^{3i} + 1$
1		$C_2 \times C_4$	2	4	$2^2, 4^2$	2	$x^{12} + a_2 x^8 + a_1 x^4 + 1$
2		C_{22}	2	11	11, 22	0	$x^{11} + 1$
2		C_{22}	11	2	2, 22	0	$x^2 + 1$
3		C_2	2	1	2^{11}	9	$x^{10} + \sum_{i=1}^{9} a_i x^i + 1$
3		C_4	2	2	2	4	$x^{10} + \sum_{i=1}^{4} a_i x^{2i} + 1$
4	D_{2m}		2	2	2^6	3	$\prod_{i=1}^{3} (x^4 + a_i x^2 + 1)$
4			2	3	2^4, 3	2	$(x^6 + a_1 x^3 + 1)(x^6 + a_2 x^3 + 1)$
4			2	6	2^3, 6	1	$x^{12} + a_1 x^6 + 1$
5			2	4	2^2, 4^2	1	$(x^4 - 1)(x^8 + a_1 x^4 + 1)$
5			2	12	2, 4, 12	0	$x^{12} - 1$
6			2	5	2^3, 10	1	$x(x^{10} + a_1 x^5 + 1)$
7			2	2	2^3, 4^2	2	$(x^4 - 1)(x^4 + a_1 x^2 + 1)(x^4 + a_2 x^2 + 1)$
7			2	3	2, 3, 4^2	1	$(x^6 - 1)(x^6 + a_1 x^3 + 1)$
8			2	2	2^3, 4^2	2	$x(x^2 - 1)(x^4 + a_1 x^2 + 1)(x^4 + a_2 x^2 + 1)$
8			2	10	2, 4, 20	0	$x(x^{10} - 1)$
10	A_4		2		2^2, 3^2	1	$f_1(x)$
20	S_4		2	0	3, 4^2	0	$x^{12} - 33x^8 - 33x^4 + 1$
25	A_5		2		2,3,10	0	$x(x^{10} + 11x^5 - 1)$
				Genus 6			
1	C_m	C_2^2	2	2	2^8	6	$x^{14} + \sum_{i=1}^{6} a_i x^{2i} + 1$
2		C_{26}	2	13	$13, 26$	0	$x^{13} + 1$
2		C_{21}	3	7	$7, 21$	0	$x^7 + 1$
2		C_{20}	4	5	$5, 20$	0	$x^5 + 1$
2		C_{10}	5	2	$2, 5, 10$	1	$x^4 + a_1 x^2 + 1$
2		C_{20}	5	4	$4, 20$	0	$x^4 + 1$
2		C_{21}	7	3	$3, 21$	0	$x^3 + 1$
2		C_{26}	13	2	$2, 26$	0	$x^2 + 1$
3		C_2	2	1	2^{13}	11	$x^{12} + \sum_{i=1}^{11} a_i x^i + 1$
3		C_4	2	2	$2^5, 4^2$	5	$x^{12} + \sum_{i=1}^{5} a_i x^{2i} + 1$
3		C_6	2	3	$2^3, 6^2$	3	$x^{12} + \sum_{i=1}^{3} a_i x^{3i} + 1$
3		C_8	2	4	$2^2, 8^2$	2	$x^{12} + \sum_{i=1}^{2} a_i x^{4i} + 1$
3		C_3	3	1	3^7	5	$x^6 + \sum_{i=1}^{5} a_i x^i + 1$
3		C_6	3	2	$3^2, 6^2$	2	$x^6 + a_2 x^4 + a_1 x^2 + 1$
3		C_4	4	1	4^5	3	$x^4 + \sum_{i=1}^{3} a_i x^i + 1$
3		C_5	5	1	5^4	2	$x^3 + a_1 x + a_2 x^2 + 1$
4	D_{2m}	$D_{14} \times C_2$	2	7	$2^3, 7$	1	$x^{14} + a_1 x^7 + 1)$
5		G_5	2	2	2^5, 4	3	$(x^2 - 1) \prod_{i=1}^{3} (x^4 + a_i x^2 + 1)$
5		G_5	2	14	$2, 4, 14$	0	$x^{14} - 1$
5		$D_{10} \times C_2$	5	5	$2, 5, 10$	0	$x^5 - 1$
6		D_8	2	2	$2^5, 4$	3	$x \cdot \prod_{i=1}^{3} (x^4 + a_i x^2 + 1)$
6		$D_6 \times C_2$	2	3	2^4, 6	2	$x \cdot \prod_{i=1}^{2} (x^4 + a_i x^2 + 1)$

Table 1. (Cont.)

Nr.	$\bar{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
6		D_{24}	2	6	2^3, 12	1	$x(x^{12} + a_1 x^6 + 1)$
6		$D_6 \times C_3$	3	3	$2^2, 3, 9$	1	$x(x^6 + a_1 x^3 + 1)$
6		D_{16}	4	2	2^2, 4, 8	1	$x(x^4 + a_1 x^2 + 1)$
8		G_8	2	4	2^2, 4, 8	1	$x(x^4 - 1)(x^8 + a_1 x^4 + 1)$
8		G_8	2	12	2, 4, 24	0	$x(x^{12} - 1)$
8		$D_4 \times C_3$	3	2	2, 3, 6^2	1	$x(x^2 - 1)(x^4 + a_1 x^2 + 1)$
8		$D_{12} \times C_3$	3	6	2, 6, 18	0	$x(x^6 - 1)$
8		G_8	4	4	2, 8, 16	0	$x(x^4 - 1)$
8		$D_6 \times C_5$	5	3	2, 10, 15	0	$x(x^3 - 1)$
8		$D_4 \times C_7$	7	2	2, 14^2	0	$x(x^2 - 1)$
9		G_9	2	2	2^2, 4^3	2	$x(x^4 - 1) \cdot \prod_{i=1}^{2} (x^4 + a_i x^2 + 1)$
9		G_9	2	3	$2, 4^2, 6$	1	$x(x^6 - 1)(x^6 + a_1 x^3 + 1)$
18	S_4	G_{18}	4	0	2, 3, 16	0	$x(x^4 - 1)$
19		G_{19}	2	0	2, 6, 8	0	$x(x^4 - 1)(x^8 + 14 x^4 + 1)$

Genus 7

1	C_m	C_2^2	2	2	2^9	7	$x^{16} + \sum_{i=1}^{7} a_i x^{2i} + 1$
1		$C_2 \times C_4$	2	4	$2^3, 4^2$	3	$x^{16} + \sum_{i=1}^{3} a_i x^{4i} + 1$
1		${C_3}^2$	3	3	3^4	2	$x^9 + a_2 x^6 + a_1 x^3 + 1$
2		C_6	2	3	$2^4, 3, 6$	4	$x^{15} + \sum_{i=1}^{4} a_1 x^{3i} + 1$
2		C_{10}	2	5	$2^2, 5, 10$	2	$x^{15} + a_1 x^5 + a_2 x^{10} + 1$
2		C_{30}	2	15	15, 30	0	$x^{15} + 1$
2		C_6	3	2	2, 3^3, 6	3	$x^8 + a_3 x^6 + a_2 x^4 + a_1 x^2 + 1$
2		C_{12}	3	4	3, 4, 12	1	$x^8 + a_1 x^4 + 1$
2		C_{24}	3	8	8, 24	0	$x^8 + 1$
2		C_{30}	15	2	2, 30	0	$x^2 + 1$
3		C_2	2	1	2^{15}	13	$x^{14} + \sum_{i=1}^{13} a_i x^i + 1$
3		C_4	2	2	$2^6, 4^2$	6	$x^{14} + \sum_{i=1}^{6} a_i x^{2i} + 1$
3		C_3	3	1	3^8	6	$x^7 + \sum_{i=1}^{6} a_i x^i + 1$
4	D_{2m}	$D_4 \times C_2$	2	2	2^7	4	$\prod_{i=1}^{4} (x^4 + a_i x^2 + 1)$
4		$D_8 \times C_2$	2	4	2^4, 4	2	$(x^8 + a_1 x^4 + 1)(x^8 + a_2 x^4 + 1)$
4		$D_{16} \times C_2$	2	8	2^3, 8	1	$x^{16} + a_1 x^8 + 1$
5		G_5	2	16	2, 4, 16	0	$x^{16} - 1$
5		$D_6 \times C_3$	3	3	2, 3^2, 6	1	$(x^3 - 1)(x^6 + a_1 x^3 + 1)$
5		$D_{18} \times C_3$	3	9	2, 6, 9	0	$x^9 - 1$
6		$D_{14} \times C_2$	2	7	2^3, 14	1	$x(x^{14} + a_1 x^7 + 1)$
7		G_7	2	2	2^4, 4^2	3	$(x^4 - 1) \prod_{i=1}^{3} (x^4 + a_i x^2 + 1)$
7		G_7	2	4	2, 4^3	1	$(x^8 - 1)(x^8 + a_1 x^4 + 1)$
8		G_8	2	2	2^4, 4^2	3	$x(x^2 - 1) \prod_{i=1}^{3} (x^4 + a_i x^2 + 1)$
8		G_8	2	14	2, 4, 28	0	$x(x^{14} - 1)$
8		$D_{14} \times C_3$	3	7	2, 6, 21	0	$x(x^7 - 1)$
8		G_8	8	2	2,16^2	0	$x(x^2 - 1)$
11	A_4	K	2	0	2^2, 3, 6	1	$(x^4 + 2\sqrt{-3} x^2 + 1)\, f_1(x)$

Table 1. (Cont.)

Nr.	$\bar{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
Genus 8							
1	C_m	C_2^2	2	2	2^{10}	8	$x^{18} + \sum_{i=1}^{8} a_i x^{2i} + 1$
1		$C_2 \times C_3$	2	3	$2^5, 3^2$	5	$x^{18} + \sum_{i=1}^{5} a_i x^{3i} + 1$
1		$C_2 \times C_6$	2	6	$2^2, 6^2$	2	$x^{18} + a_1 x^6 + a_2 x^{12} + 1$
2		C_{34}	2	17	17, 34	0	$x^{17} + 1$
2		C_{34}	17	2	2, 34	0	$x^2 + 1$
3		C_2	2	1	2^{17}	15	$x^{16} + \sum_{i=1}^{1} 5 a_i x^i + 1$
3		C_4	2	2	$2^7, 4^2$	7	$x^{16} + \sum_{i=1}^{7} a_i x^{2i} + 1$
3		C_8	2	4	$2^3, 8^2$	3	$x^{16} + a_1 x^4 + a_2 x^8 + a_3 x^{12} + 1$
4	D_{2m}	$D_6 \times C_2$	2	3	2^5, 3	3	$\prod_{i+1}^{3} (x^6 + a_i x^3 + 1)$
4		$D_{18} \times C_2$	2	9	2^3, 9	1	$x^{18} + a_1 x^9 + 1$
5		G_5	2	2	2^6, 4	4	$(x^2 - 1) \prod_{i=1}^{4} (x^4 + a_i x^2 + 1)$
5		G_5	2	6	2^2, 4, 6	1	$(x^6 - 1)(x^{12} + a_1 x^6 + 1)$
5		G_5	2	18	2, 4, 18	0	$x^{18} - 1$
6		D_8	2	2	2^6, 4	4	$x \prod_{i=1}^{4} (x^4 + a_i x^2 + 1)$
6		D_{16}	2	4	2^4, 8	2	$x(x^8 + a_1 x^4 + 1)(x^8 + a_2 x^4 + 1)$
6		D_{32}	2	8	2^3, 16	1	$x(x^{16} + a_1 x^8 + 1)$
7		G_9	2	3	2^2, 3, 4^2	2	$(x^6 - 1)(x^6 + a_1 x^3 + 1)(x^6 + a_2 x^3 + 1)$
8		G_8	2	16	2, 4, 32	0	$x(x^{16} - 1)$
9		G_9	2	2	$2^3, 4^3$	3	$x(x^4 - 1) \prod_{i+1}^{3} (x^6 + a_i x^3 + 1)$
9		G_9	2	4	2, 4^2, 8	1	$x(x^8 - 1)(x^8 + a_1 x^4 + 1)$
13	A_4	K	2	0	2, 3^2, 4	1	$x(x^4 - 1) f_1(x)$
22	S_4	G_{22}	2	0	3, 4, 8	0	$x(x^4 - 1)(x^{12} - 33x^8 - 33x^4 + 1)$
Genus 9							
1	C_m	C_2^2	2	2	2^{11}	9	$x^{20} + \sum_{i=1}^{9} a_i x^{2i} + 1$
1		$C_2 \times C_4$	2	4	$2^4, 4^2$	4	$x^{20} + \sum_{i=1}^{4} a_i x^{4i} + 1$
1		$C_2 \times C_5$	2	5	$2^3, 5^2$	3	$x^{20} + a_1 x^5 + a_2 x^{10} + a_3 x^{15} + 1$
1		$C_2 \times C_4$	4	2	$2^2, 4^3$	3	$x^8 + a_1 x^2 + a_2 x^4 + a_3 x^6 + 1$
2		C_{38}	2	19	19, 38	0	$x^{19} + 1$
2		C_6	3	2	2, 3^4, 6	4	$x^{10} + a_1 x^2 + a_2 x^4 + a_3 x^6 + a_4 x^8 + 1$
2		C_{15}	3	5	3, 5, 15	1	$x^{10} + a_1 x^5 + 1$
2		C_{30}	3	10	10, 30	0	$x^{10} + 1$
2		C_{28}	4	7	7, 28	0	$x^7 + 1$
2		C_{14}	7	2	2,7, 14	1	$x^4 + a_1 x^2 + 1$
2		C_{28}	7	4	4, 28	0	$x^4 + 1$
2		C_{30}	10	3	3, 30	0	$x^3 + 1$
2		C_{38}	19	2	2, 38	0	$x^2 + 1$
3		C_2	2	1	2^{19}	17	$x^{18} + \sum_{i=1}^{17} a_i x^i + 1$
3		C_4	2	2	$2^8, 4^2$	8	$x^{18} + \sum_{i=1}^{8} a_i x^{2i} + 1$
3		C_6	2	3	$2^5, 6^2$	5	$x^{18} + \sum_{i=1}^{5} a_i x^{3i} + 1$
3		C_{12}	2	6	$2^2, 12^2$	2	$x^{18} + a_1 x^6 + a_2 x^{12} + 1$
3		C_3	3	1	3^{10}	8	$x^9 + \sum_{i=1}^{8} a_i x^i + 1$
3		C_9	3	3	$3^2, 9^2$	2	$x^9 + a_2 x^6 + a_1 x^3 + 1$

Table 1. (Cont.)

Nr.	$\bar{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
3		C_4	4	1	4^7	5	$x^6 + \sum_{i=1}^5 a_i x^i + 1$
3		C_8	4	2	$4^2, 8^2$	2	$x^6 + a_2x^4 + a_1x^2 + 1$
3		C_7	7	1	7^4	2	$x^3 + a_1x + a_2x^2 + 1$
4	D_{2m}	$D_4 \times C_2$	2	2	2^8	5	$\prod_{i=1}^5 (x^4 + a_ix^2 + 1))$
4		$D_{10} \times C_2$	2	5	2^4, 5	2	$(x^{10} + a_1x^5 + 1)(x^{10} + a_2x^5 + 1)$
4		$D_{20} \times C_2$	2	10	2^3, 10	1	$x^{20} + a_1x^{10} + 1$
4		$D_4 \times C_4$	4	2	$2^3, 4^2$	2	$(x^4 + a_1x^2 + 1)(x^4 + a_2x^2 + 1)$
4		$D_8 \times C_4$	4	4	$2^2, 4^2$	1	$x^8 + a_1x^4 + 1$
5		G_5	2	4	2^3, 4^2	2	$(x^4 - 1)(x^8 + a_1x^4 + 1)(x^8 + a_2x^4 + 1)$
5		G_5	2	20	2, 4, 20	0	$x^{20} - 1$
5		G_5	4	8	$2,8^2$	0	$x^8 - 1$
6		$D_6 \times C_2$	2	3	2^5, 6	3	$x \prod_{i=1}^3 (x^6 + a_ix^3 + 1)$
6		$D_{18} \times C_2$	2	9	2^3, 18	1	$x(x^{18} + a_1x^9 + 1)$
6		$D_6 \times C_4$	4	3	2^2, 4, 12	1	$x(x^6 + a_1x^3 + 1)$
7		G_7	2	2	2^5, 4^2	4	$(x^4 - 1) \prod_{i=1}^4 (x^4 + a_ix^2 + 1)$
7		G_9	2	5	2, 4^2, 5	1	$(x^{10} - 1)(x^{10} + a_1x^5 + 1)$
7		G_7	4	2	2, 4, 8^2	1	$(x^4 - 1)(x^4 + a_1x^2 + 1)$
8		G_8	2	2	2^5, 4^2	4	$x(x^2 - 1) \prod_{i=1}^4 (x^4 + a_ix^2 + 1)$
8		G_8	2	6	2^2, 4, 12	1	$x(x^6 - 1)(x^{12} + a_1x^6 + 1)$
8		G_8	2	18	2, 4, 36	0	$x(x^{18} - 1)$
8		$D_6 \times C_3$	3	3	2, 3, 6, 9	1	$x(x^3 - 1)(x^6 + a_1x^3 + 1)$
8		$D_{18} \times C_3$	3	9	2, 6, 27	0	$x(x^9 - 1)$
8		G_8	4	2	2, 4, 8^2	1	$x(x^2 - 1)(x^4 + a_1x^2 + 1)$
8		G_8	4	6	2, 8, 24	0	$x(x^6 - 1)$
8		$D_6 \times C_7$	7	3	2, 14, 21	0	$x(x^3 - 1)$
8		G_8	10	2	2, 20^2	0	$x(x^2 - 1)$
9		G_9	2	3	$2^2, 4^2, 6$	2	$x(x^6 - 1)(x^6 + a_1x^3 + 1)(x^6 + a_2x^3 + 1)$
12	A_4	K	2	0	2^2, 6^2	1	$(x^8 + 14x^4 + 1) f_1(x)$
17	S_4	G_{17}	4	0	2, 4, 12	0	$x^8 + 14x^4 + 1$
21		G_{21}	2	0	4^2 6	0	$(x^8 + 14x^4 + 1)(x^{12} - 33x^8 - 33x^4 + 1)$
27	A_5		2		2, 5, 6	0	$x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1$

Genus 10

1	C_m	C_2^2	2	2	2^{12}	10	$x^{22} + \sum_{i=1}^{10} a_i x^{2i} + 1$
1		$C_2 \times C_3$	3	2	$2^2, 3^5$	5	$x^{12} + \sum_{i=1}^5 a_i x^{2i} + 1$
1		C_3^2	3	3	3^5	3	$x^{12} + a_1x^3 + a_2x^6 + a_3x^9 + 1$
1		$C_3 \times C_4$	3	4	$3^2, 4^2$	2	$x^{12} + a_1x^4 + a_2x^8 + 1$
1		$C_2 \times C_6$	6	2	$2^2, 6^2$	2	$x^6 + a_1x^2 + a_2x^4 + 1$
2		C_6	2	3	2^6, 3, 6	6	$x^{21} + \sum_{i=1}^6 a_i x^{3i} + 1$
2		C_{14}	2	7	2^2, 7, 14	2	$x^{21} + a_1x^7 + a_2x^{14} + 1$
2		C_{42}	2	21	21, 42	0	$x^{21} + 1$
2		C_{33}	3	11	11, 33	0	$x^{11} + 1$
2		C_{10}	5	2	2, 5^2, 10	2	$x^6 + a_2x^4 + a_1x^2 + 1$
2		C_{15}	5	3	3, 5, 15	1	$x^6 + a_1x^3 + 1$
2		C_{30}	5	6	6, 30	0	$x^6 + 1$

TABLE 1. (Cont.)

Nr.	$\bar{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
2		C_{30}	6	5	5, 30	0	$x^5 + 1$
2		C_{33}	11	3	3, 33	0	$x^3 + 1$
2		C_{42}	21	2	2, 42	0	$x^2 + 1$
3		C_2	2	1	2^{21}	19	$x^{20} + \sum_{i=1}^{19} a_i x^i + 1$
3		C_4	2	2	$2^9, 4^2$	9	$x^{20} + \sum_{i=1}^{9} a_i x^{2i} + 1$
3		C_8	2	4	$2^4, 8^2$	4	$x^{20} + a_1x^4 + a_2x^8 + a_3x^{12} + a_4x^{16} + 1$
3		C_{10}	2	5	$2^3, 10^2$	3	$x^{20} + a_1x^5 + a_2x^{10} + a_3x^{15} + 1$
3		C_3	3	1	3^{11}	9	$x^{10} + \sum_{i=1}^{9} a_i x^i + 1$
3		C_6	3	2	$3^4, 6^2$	4	$x^{10} + a_1x^2 + a_2x^4 + a_3x^6 + a_4x^8 + 1$
3		C_5	5	1	5^6	4	$x^5 + \sum_{i=1}^{4} a_i x^i + 1$
3		C_6	6	1	6^5	3	$x^4 + a_1x + a_2x^2a_3x^3 + 1$
4	D_{2m}	$D_{22} \times C_2$	2	11	2^3, 11	1	$x^{22} + a_1x^{11} + 1$
4		$D_4 \times C_3$	3	2	$2^3, 3^3$	3	$\prod_{i=1}^{3}(x^4 + a_ix^2 + 1)$
4		$D_6 \times C_3$	3	3	$2^2, 3^3,$	2	$(x^6 + a_1x^3 + 1)(x^6 + a_2x^3 + 1)$
4		$D_{12} \times C_3$	3	6	$2^2, 3, 6$	1	$(x^{12} + a_1x^6 + 1$
4		$D_6 \times C_6$	6	3	$2^2, 3, 6$	1	$x^6 + a_1x^3 + 1$
5		G_5	2	2	2^7, 4	5	$(x^2 - 1)\prod_{i=1}^{5}(x^4 + a_ix^2 + 1)$
5		G_5	2	22	2, 4, 22	0	$x^{22} - 1$
5		$D_8 \times C_3$	3	4	2, 3, 4, 6	1	$(x^4 - 1)(x^8 + a_1x^4 + 1)$
5		$D_{24} \times C_3$	3	12	2, 6, 12	0	$x^{12} - 1$
5		G_5	6	2	2^2, 6, 12	1	$(x^2 - 1)(x^4 + a_1x^2 + 1)$
5		G_5	6	6	2, 6, 12	0	$x^6 - 1$
6		D_8	2	2	2^7, 4	5	$x\prod_{i=1}^{5}(x^4 + a_ix^2 + 1)$
6		$D_{10} \times C_2$	2	5	2^4, 10	2	$x(x^{10} + a_1x^5 + 1)(x^{10} + a_2x^5 + 1)$
6		D_{40}	2	10	2^3, 20	1	$x(x^{20} + a_1x^{10} + 1)$
6		$D_{10} \times C_3$	3	5	2^2, 3, 15	1	$x(x^{10} + a_1x^5 + 1)$
6		D_{24}	6	2	2^2, 6, 12	1	$x(x^4 + a_1x^2 + 1)$
7		$D_4 \times C_3$	3	2	2, 3^2, 6^2	2	$(x^2 - 1)(x^4 + a_1x^2 + 1)(x^4 + a_2x^2 + 1)$
7		$D_6 \times C_3$	3	3	$3^2, 6^2$	1	$(x^6 - 1)(x^6 + a_1x^3 + 1)$
8		G_8	2	4	2^3, 4, 8	2	$x(x^4 - 1)(x^8 + a_1x^4 + 1)(x^8 + a_2x^4 + 1)$
8		G_8	2	20	2, 4, 40	0	$x(x^{20} - 1)$
8		$D_4 \times C_3$	3	2	2,$3^2, 6^2$	2	$x(x^2 - 1)(x^4 + a_1x^2 + 1)(x^4 + a_2x^2 + 1)$
8		$D_{20} \times C_3$	3	10	2, 6, 30	0	$x(x^{10} - 1)$
8		$D_{10} \times C_5$	5	5	2, 10, 25	0	$x(x^5 - 1)$
8		G_8	6	4	2, 12, 24	0	$x(x^4 - 1)$
8		$D_4 \times C_{11}$	11	2	2, 22^2	0	$x(x^2 - 1)$
9		G_9	2	2	$2^4, 4^3$	4	$x(x^4 - 1)\prod_{i=1}^{4}(x^4 + a_ix^2 + 1)$
9		G_9	2	5	$2, 4^2, 10$	1	$x(x^{10} - 1)(x^{10} + a_1x^5 + 1)$
10	A_4		3	0	2, 3^3	1	$f_1(x)$
14			2	0	2, 3, 4, 6	1	$x(x^4 - 1)(x^4 + 2\sqrt{-3}\,x^2 + 1)\,f_1(x)$
18	S_4	G_{18}	6	0	2, 3, 24	0	$x(x^4 - 1)$
20		$S_4 \times C_3$	3	0	3, 4, 6	0	$x^{12} - 33x^8 - 33x^4 + 1$
25	A_5	$A_5 \times C_3$	3	0	2, 3, 15	0	$x(x^{10} + 11x^5 - 1)$

5. Final remarks

Following the methods described above we intend to create a database of all superelliptic curves of genus $g \leq 48$, inclusions among the loci, and the corresponding parametric equations for each family. Each locus can be determined in terms of the invariants of binary forms, but this is a difficult task computationally since such forms are not known for high degree binary forms. However, such loci can also be described in terms of the dihedral invariants of superelliptic curves.

In a further stage we intend to add to such database the minimal equation of such curves, the corresponding minimal height, and the moduli height for genus $g = 2, 3$ as defined in [3] and even the decompositions of their Jacobians in terms of their dihedral invariants; see [9] and [5] for details.

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 267, Springer-Verlag, New York, 1985. MR770932 (86h:14019)

[2] Enrico Arbarello, Maurizio Cornalba, and Pillip A. Griffiths, *Geometry of algebraic curves. Volume II*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 268, Springer, Heidelberg, 2011. With a contribution by Joseph Daniel Harris. MR2807457 (2012e:14059)

[3] L Beshaj and T Shaska, *Heights on algebraic curves*, On the arithmetic of superelliptic curves, 2015.

[4] Lubjana Beshaj, Valmira Hoxha, and Tony Shaska, *On superelliptic curves of level n and their quotients, I*, Albanian J. Math. **5** (2011), no. 3, 115–137. MR2846162 (2012i:14036)

[5] Lubjana Beshaj, Tony Shaska, and Caleb Shor, *On jacobians of curves with superelliptic components*, Contemporary Mathematics **619** (2014).

[6] Andries E. Brouwer and Mihaela Popoviciu, *The invariants of the binary decimic*, J. Symbolic Comput. **45** (2010), no. 8, 837–843. MR2657667 (2011f:13007)

[7] Igor V. Dolgachev, *Classical algebraic geometry*, Cambridge University Press, Cambridge, 2012. A modern view.

[8] William Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. MR1042981 (90k:14023)

[9] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115. MR2135032 (2006b:14049)

[10] Vishwanath Krishnamoorthy, Tanush Shaska, and Helmut Völklein, *Invariants of binary forms*, Progress in Galois theory, 2005, pp. 101–122. MR2148462 (2006b:13015)

[11] R. Sanjeewa, *Automorphism groups of cyclic curves defined over finite fields of any characteristics*, Albanian J. Math. **3** (2009), no. 4, 131–160. MR2578064 (2011a:14045)

[12] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)

[13] T. Shaska, *Some remarks on the hyperelliptic moduli of genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130. MR3200084

[14] T. Shaska and F. Thompson, *Bielliptic curves of genus 3 in the hyperelliptic moduli*, Appl. Algebra Engrg. Comm. Comput. **24** (2013), no. 5, 387–412. MR3118614

ALBANIAN JOURNAL OF MATHEMATICS
Volume 8, Number 1, Pages 37–45
ISSN: 1930-1235; (**2014**)

ON STREAM CIPHER BASED ON FAMILY OF GRAPHS $\widetilde{D(n,q)}$ OF INCREASING GIRTH

Monika Polak
University of Maria Curie Sklodowska
Lublin, Poland
Email: monika.katarzyna.polak@gmail.com

Vasyl Ustimenko
University of Maria Curie Sklodowska
Lublin, Poland
Email: vasyl@hektor.umcs.lublin.pl

Abstract. In this short paper we present symmetric encryption algorithm based on family of bipartite graphs $\widetilde{D(n,q)}$. It is a fast stream cipher with computation speed $O(n)$ for the key of fixed length. If the key is linear function from n the efficiency is $O(n^2)$. Encryption map has a multivariate nature, so the security level can be evaluated via degrees and other parameters of corresponding multivariate polynomials. We show that the degree of graph based encryption maps are growing with the growth of the dimension of the plain space. Therefore this algorithm is resistant to linearization attacks.

1. Introduction

Multivariate polynomials are just polynomials in several variables. In this article we are interested in polynomials over finite fields. Though multivariate polynomial cryptography is a potential candidate for post quantum cryptography, schemes based on it are mostly used for digital signature purpose only; see [1] for further details. Multivariate cryptography is proposed as a tool for public key cryptography, but only few encryption schemes were developed untill now, see for example [2].

In this paper we explore the possibility of using multivariate polynomial systems for symmetric encryption. Main security assumption of presented symmetric scheme is backed by the NP-hardness of the problem to solve nonlinear system of equations over a finite field. There are many different algorithms where graphs are used. Graph based algorithms are used, in particular, in cryptography, coding theory, car navigation systems, sociology, mobile robotics and even in computer games. Families of graphs can be used to create multivariate polynomials for cryptographic schemes. Graphs were first used in cryptography by Ustimenko in [3,4]. There are other examples of crypto-systems based on graphs $D(n,q)$, which were introduced

2000 *Mathematics Subject Classification.* 05C90 and 94C15 and 94A60 .
Key words and phrases. data security and stream cipher and graph based algorithm and multivariate transformations.

in [5]. Multivariate maps used in this algorithms were investigated in [6–8]. A. Wróblewska proved that maps related to $D(n,q)$ are cubical; see [7]. Computer simulations of multivariate maps based on graph $D(n,K)$ are designed in [9, 10].

2. Families of graphs

For our purposes we are interested only in simple graphs. *Simple graph* is a undirected graph containing no graph loops or multiple edges. By $\Gamma(V,E)$ we denote graph where V is a set of vertices and E is a set of edges. We say that graph is *connected* if for arbitrary pair of vertices $v_1, v_2 \in V$ there is a path from v_1 to v_2. The *girth* of a connected, simple graph is a length of the shortest cycle in a graph. Graph $\Gamma(V = V_1 \cup V_2, E)$ is *bipartite* if set of vertices can be divided into two sets V_1 and V_2 ($V_1 \cap V_2 = \emptyset$) such that every edge connects a vertex in V_1 to one in V_2.

We refer to bipartite graph $\Gamma(V_1 \cup V_2, E)$ as *regular* one if every vertex from V_1 and V_2 has the same constant degree. Mentioned definitions and more facts from Simple Graphs Theory can be find in [11].

The following interpretation of family of graphs $D(n,q)$ can be find in [5]. Let $\mathbb{F}_q$ be a finite field. Firstly, let us recall the definition of graph $D(q)$ corresponding to infinite incidence structure (P,L,I), where P is collection of points and L is collection of lines. By I we denote the incidence relation for this graph. Let us to use the notions for points and lines introduced in [5]:

$$\begin{aligned}(p) &= (p_{1,0}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, ..., p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,1}...),\\ [l] &= [l_{0,1}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, ..., l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,1}...].\end{aligned}$$

Two types of brackets allow us to distinguish points and lines. Points and lines are elements of two copies of the vector space over $\mathbb{F}_q$. In an infinite incidence structure (P,L,I) the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$(1) \qquad \begin{cases} l_{1,1} - p_{1,1} = l_{0,1}p_{1,0} \\ l_{1,2} - p_{1,2} = l_{1,1}p_{1,0} \\ l_{2,1} - p_{2,1} = l_{0,1}p_{1,1} \\ l_{i,i} - p_{i,i} = l_{0,1}p_{i-1,i}, \\ l'_{i,i} - p'_{i,i} = l_{i,i-1}p_{1,0} \\ l_{i,i+1} - p_{i,i+1} = l_{i,i-1}p_{1,0} \\ l_{i+1,i} - p_{i+1,i} = l_{0,1}p'_{i,i} \end{cases}$$

where $i \geq 2$.

The set of vertices of infinite incidence structure (P,L,I) is $V = P \cup L$ and the set of edges E consisting of all pairs $\{(p),[l]\}$ for which $(p)I[l]$. Bipartite graphs $D(n,q)$ have partition sets P_n (collection of points) and L_n (collection of lines) isomorphic to vector space $\mathbb{F}_q^n$, where $n \in \mathbb{N}_+$. For each positive integer $n > 2$ the finite incidence structures (P_n, L_n, I_n) can be obtained in a following way. P_n and L_n are obtained from P and L, respectively, by projecting each vector onto its n initial coordinates with respect to the natural order. The incidence relations I_n are then defined by imposing the first $n-1$ incidence equations and ignoring all others. The graphs corresponding to the finite incidence structures (P_n, L_n, I_n) are denoted by $D(n,q)$.

The family of graphs $\widetilde{D(n,q)}$ was firstly introduced in [5] as a tool in construction of family of graphs $D(n,q)$. The applications of this family of graphs weren't contemplated before. In the construction of the family of graphs graphs $\widetilde{D(q)}$ Cartan matrix

$$\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$$

and Lie algebra are used. Lie algebra is a vector space over finite field with the bilinear product satisfying certain properties (see [12]). Let us to use the analogical notions for points and lines in graph $\widetilde{D(q)}$:

$$(p) = (p_{1,0}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p_{2,3}, ..., p_{i,i}, p_{i,i+1}, p_{i+1,1} ...),$$
$$[l] = [l_{0,1}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l_{2,3}, ..., l_{i,i}, l_{i,i+1}, l_{i+1,1} ...].$$

In infinite incidence structure $(\widetilde{P, L, I})$ the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$(2) \qquad \begin{cases} l_{1,1} - p_{1,1} = l_{0,1}p_{1,0} \\ l_{1,2} - p_{1,2} = l_{0,1}p_{1,1} \\ l_{2,1} - p_{2,1} = l_{1,1}p_{1,0} \\ l_{i,i} - p_{i,i} = l_{0,1}p_{i,i-1} + l_{i-1,i}p_{1,0} \\ l_{i,i+1} - p_{i,i+1} = l_{0,1}p_{i,i} \\ l_{i+1,i} - p_{i+1,i} = l_{i,i}p_{1,0} \end{cases}$$

where $i \geq 2$.

The graphs $\widetilde{D(n,q)}$ corresponding to the finite incidence structures $(\widetilde{P_n, L_n, I_n})$ can be obtained by the same way as for graphs $D(n,q)$.

Graphs from families $D(n,q)$ and $\widetilde{D(n,q)}$ are bipartite, q-regular, sparse and without short cycles. The girth in graphs from described families increasing with growing n. In fact $D(n,q)$ is a family of graphs of large girth and there is a conjecture that $\widetilde{D(n,q)}$ is another family of graphs of large girth.

3. Algorithm

The family of graphs $\widetilde{D(n,q)}$ can be use as a tool for symmetric encryption. Firstly let $v = (v_1, v_2, v_3, v_4, \ldots, v_n) \in \widetilde{D(n,q)}$ (or $v = [v_1, v_2, v_3, v_4, \ldots, v_n] \in \widetilde{D(n,q)}$) and $N_t(v)$ be the operator of taking neighbor of vertex v where first coordinate is $v_1 + t$:

$$N_t(v_1, v_2, v_3, v_4, v_5) \to [v_1 + t, *, *, *, *],$$
$$N_t[v_1, v_2, v_3, v_4, v_5] \to (v_1 + t, *, *, *, *).$$

The remaining coordinates can be determined uniquely using relations in Eq. (2). We can construct multivariate map F in a following way:

$N_{t_1}\left(\overline{x}\right)$ is given by:

$$\begin{bmatrix} x_1+t_1 \\ x_2+x_1(x_1+t_1) \\ x_3+x_2(x_1+t_1) \\ x_4+x_1x_2+x_1^2(x_1+t_1) \\ x_5+x_1x_3+(x_1x_2+x_4)(x_1+t_1) \\ x_6+x_5(x_1+t_1) \\ x_7+x_1x_5+x_1^2x_3+(x_1^2x_2+x_1x_4)(x_1+t_1) \\ \vdots \\ x_{3i+5}+x_1x_{3i+3}+(x_1x_{3i+2}+x_{3i+4})(x_1+t_1) \\ x_{3i+6}+x_{3i+5}(x_1+t_1) \\ x_{3i+7}+x_1x_{3i+5}+x_1^2x_{3i+3}+(x_1^2x_{3i+2}+x_1x_{3i+4})(x_1+t_1) \\ \vdots \\ {}_1f_n(x_1,x_2,\ldots,x_n) \end{bmatrix} = \begin{bmatrix} {}_{t_1}x_1 \\ {}_{t_1}x_2 \\ {}_{t_1}x_3 \\ {}_{t_1}x_4 \\ {}_{t_1}x_5 \\ {}_{t_1}x_6 \\ {}_{t_1}x_7 \\ \vdots \\ {}_{t_1}x_{3i+5} \\ {}_{t_1}x_{3i+6} \\ {}_{t_1}x_{3i+7} \\ \vdots \\ {}_{t_1}x_n \end{bmatrix}$$

We have $N_{t_2}\left[\overline{{}_{t_1}x}\right]$ given by:

$$\begin{pmatrix} {}_{t_1}x_1+t_2 \\ x_2-(t_1+t_2){}_{t_1}x_1 \\ x_3+(t_1+t_2){}_{t_1}x_1^2 \\ x_4-(t_1+t_2){}_{t_1}x_2 \\ x_5+({}_{t_1}x_1^2x_1-x_3)(t_1+t_2) \\ x_6-({}_{t_1}x_1^2x_1-x_3){}_{t_1}x_1(t_1+t_2) \\ x_7-(t_1+t_2){}_{t_1}x_5 \\ \vdots \\ x_{3i+5}+({}_{t_1}x_1{}^2x_{3i+1}+x_{1}{}_{t_1}x_{1}{}_{t_1}x_{3i}-x_{3i+3})(t_1+t_2) \\ x_{3i+6}-({}_{t_1}x_1{}^2x_{3i+1}+x_{1}{}_{t_1}x_{1}{}_{t_1}x_{3i}-x_{3i+3}){}_{t_1}x_1(t_1+t_2) \\ x_{3i+7}-(t_1+t_2){}_{t_1}x_{3i+5} \\ \vdots \\ {}_2f_n(x_1,x_2,\ldots,x_n) \end{pmatrix} = \begin{pmatrix} {}_{t_2}x_1 \\ {}_{t_2}x_2 \\ {}_{t_2}x_3 \\ {}_{t_2}x_4 \\ {}_{t_2}x_5 \\ {}_{t_2}x_6 \\ {}_{t_2}x_7 \\ \vdots \\ {}_{t_2}x_{3i+5} \\ {}_{t_2}x_{3i+6} \\ {}_{t_2}x_{3i+7} \\ \vdots \\ {}_{t_2}x_n \end{pmatrix}$$

$N_{t_3}\left(\overline{{}_{t_2}x}\right)$ is given by:

$$\begin{bmatrix} {}_{t_2}x_1+t_3 \\ {}_{t_1}x_2+(t_2+t_3){}_{t_2}x_1 \\ {}_{t_1}x_3+(t_2+t_3){}_{t_2}x_2 \\ {}_{t_1}x_4+(t_2+t_3){}_{t_2}x_1^2 \\ {}_{t_1}x_5+(t_2+t_3)({}_{t_1}x_4-{}_{t_1}x_{1}{}_{t_2}x_1^2) \\ {}_{t_1}x_6+(t_2+t_3){}_{t_2}x_5 \\ {}_{t_1}x_7+({}_{t_1}x_4-{}_{t_1}x_{1}{}_{t_2}x_1^2)(t_2+t_3){}_{t_2}x_1 \\ \vdots \\ {}_{t_1}x_{3i+5}+(t_2+t_3)({}_{t_1}x_{3i+4}-{}_{t_2}x_{1}{}_{t_2}x_{3i+1}{}_{t_1}x_1-{}_{t_1}x_{3i}{}_{t_2}x_2^2) \\ {}_{t_1}x_{3i+6}+(t_2+t_3){}_{t_2}x_{3i+5} \\ {}_{t_1}x_{3i+7}+(t_2+t_3)({}_{t_1}x_{3i+4}-{}_{t_2}x_{1}{}_{t_2}x_{3i+1}{}_{t_1}x_1-{}_{t_1}x_{3i}{}_{t_2}x_1{}^2){}_{t_2}x_1 \\ \vdots \\ {}_3f_n(x_1,x_2,\ldots,x_n) \end{bmatrix} = \begin{bmatrix} {}_{t_3}x_1 \\ {}_{t_3}x_2 \\ {}_{t_3}x_3 \\ {}_{t_3}x_4 \\ {}_{t_3}x_5 \\ {}_{t_3}x_6 \\ {}_{t_3}x_7 \\ \vdots \\ {}_{t_3}x_{3i+5} \\ {}_{t_3}x_{3i+6} \\ {}_{t_3}x_{3i+7} \\ \vdots \\ {}_{t_3}x_n \end{bmatrix}$$

$N_{t_4}\,[\overline{{}_{t_3}x}]$ is

$$\begin{pmatrix} {}_{t_3}x_1+t_4 \\ {}_{t_2}x_2-(t_3+t_4){}_{t_3}x_1 \\ {}_{t_2}x_3+(t_3+t_4){}_{t_3}x_1^2 \\ {}_{t_2}x_4-(t_3+t_4){}_{t_3}x_2 \\ {}_{t_2}x_5+({}_{t_3}x_1^2{}_{t_2}x_1-{}_{t_2}x_3)(t_3+t_4) \\ {}_{t_2}x_6-({}_{t_3}x_1^2{}_{t_2}x_1-{}_{t_2}x_3){}_{t_3}x_1(t_3+t_4) \\ {}_{t_2}x_7-(t_3+t_4){}_{t_3}x_5 \\ \vdots \\ {}_{t_2}x_{3i+5}+({}_{t_3}x_1^2{}_{t_2}x_{3i+1}+{}_{t_3}x_1{}_{t_2}x_1{}_{t_3}x_{3i}-{}_{t_2}x_{3i+3})(t_3+t_4) \\ {}_{t_2}x_{3i+6}-({}_{t_3}x_1^2{}_{t_2}x_{3i+1}+{}_{t_3}x_1{}_{t_2}x_1{}_{t_3}x_{3i}-{}_{t_2}x_{3i+3}){}_{t_3}x_1(t_3+t_4) \\ {}_{t_2}x_{3i+7}-(t_3+t_4){}_{t_3}x_{3i+5} \\ \vdots \\ {}_4f_n(x_1,x_2,\dots,x_n) \end{pmatrix} = \begin{pmatrix} {}_{t_4}x_1 \\ {}_{t_4}x_2 \\ {}_{t_4}x_3 \\ {}_{t_4}x_4 \\ {}_{t_4}x_5 \\ {}_{t_4}x_6 \\ {}_{t_4}x_7 \\ \vdots \\ {}_{t_4}x_{3i+5} \\ {}_{t_4}x_{3i+6} \\ {}_{t_4}x_{3i+7} \\ \vdots \\ {}_{t_4}x_n \end{pmatrix}$$

and $N_{t_5}\,(\overline{{}_{t_4}x})$

$$\begin{bmatrix} {}_{t_4}x_1+t_5 \\ {}_{t_3}x_2+(t_4+t_5){}_{t_4}x_1 \\ {}_{t_3}x_3+(t_4+t_5){}_{t_4}x_2 \\ {}_{t_3}x_4+(t_4+t_5){}_{t_4}x_1^2 \\ {}_{t_3}x_5+(t_4+t_5)({}_{t_3}x_4-{}_{t_3}x_{1_{t_4}}x_1^2) \\ {}_{t_3}x_6+(t_4+t_5){}_{t_4}x_5 \\ {}_{t_3}x_7+({}_{t_3}x_4-{}_{t_3}x_{1_{t_4}}x_1^2)(t_4+t_5){}_{t_4}x_1 \\ \vdots \\ {}_{t_3}x_{3i+5}+(t_4+t_5)({}_{t_3}x_{3i+4}-{}_{t_4}x_{1_{t_4}}x_{3i+1}{}_{t_3}x_1-{}_{t_3}x_{3i_{t_4}}x_1^2) \\ {}_{t_3}x_{3i+6}+(t_4+t_5){}_{t_4}x_{3i+5} \\ {}_{t_3}x_{3i+7}+(t_4+t_5)({}_{t_3}x_{3i+4}-{}_{t_4}x_{1_{t_4}}x_{3i+1}{}_{t_3}x_1-{}_{t_3}x_{3i_{t_4}}x_1^2){}_{t_4}x_1 \\ \vdots \\ {}_5f_n(x_1,x_2,\dots,x_n) \end{bmatrix} = \begin{bmatrix} {}_{t_5}x_1 \\ {}_{t_5}x_2 \\ {}_{t_5}x_3 \\ {}_{t_5}x_4 \\ {}_{t_5}x_5 \\ {}_{t_5}x_6 \\ {}_{t_5}x_7 \\ \vdots \\ {}_{t_5}x_{3i+5} \\ {}_{t_5}x_{3i+6} \\ {}_{t_5}x_{3i+7} \\ \vdots \\ {}_{t_5}x_n \end{bmatrix}$$

and so on. Operator N_{t_k} works as follows:

$$\begin{gathered} {}_{t_{k-1}}x_1 \longrightarrow {}_kf_1(x_1,x_2,\dots,x_n), \\ {}_{t_{k-1}}x_2 \longrightarrow {}_kf_2(x_1,x_2,\dots,x_n), \\ {}_{t_{k-1}}x_3 \longrightarrow {}_kf_3(x_1,x_2,\dots,x_n), \\ {}_{t_{k-1}}x_4 \longrightarrow {}_kf_4(x_1,x_2,\dots,x_n), \\ {}_{t_{k-1}}x_5 \longrightarrow {}_kf_5(x_1,x_2,\dots,x_n), \\ {}_{t_{k-1}}x_6 \longrightarrow {}_kf_6(x_1,x_2,\dots,x_n), \\ {}_{t_{k-1}}x_7 \longrightarrow {}_kf_7(x_1,x_2,\dots,x_n), \\ \vdots \\ {}_{t_{k-1}}x_n \longrightarrow {}_kf_n(x_1,x_2,\dots,x_n). \end{gathered}$$

If we calculate the next few vectors we see a regularity and so we can formulate general formulas for functions f_i which are depend from k. Let $l=2,3,4,\dots$ then:

$$N_{t_{2l+1}}({}_{2l}x_1,{}_{2l}x_2,{}_{2l}x_3,\dots,{}_{2l}\,x_n) \longrightarrow$$

$$\begin{bmatrix} {}_{t_{2l}}x_1 + t_{2l+1} \\ {}_{t_{2l-1}}x_2 + (t_{2l} + t_{2l+1})\,{}_{t_{2l}}x_1 \\ {}_{t_{2l-1}}x_3 + (t_{2l} + t_{2l+1})\,{}_{t_{2l}}x_2 \\ {}_{t_{2l-1}}x_4 + (t_{2l} + t_{2l+1})\,{}_{t_{2l}}x_1^2 \\ {}_{t_{2l-1}}x_5 + (t_{2l} + t_{2l+1})({}_{t_{2l-1}}x_4 - {}_{t_{2l-1}}x_1\,{}_{t_{2l}}{x_1}^2) \\ {}_{t_{2l-1}}x_6 + (t_{2l} + t_{2l+1})\,{}_{t_{2l}}x_5 \\ {}_{t_{2l-1}}x_7 + ({}_{t_{2l-1}}x_4 - {}_{t_{2l-1}}x_1\,{}_{t_{2l}}x_1^2)(t_{2l} + t_{2l+1})\,{}_{t_{2l}}x_1 \\ \vdots \\ {}_{t_{2l-1}}x_{3i+5} + (t_{2l} + t_{2l+1})({}_{t_{2l-1}}x_{3i+4} - {}_{t_{2l}}x_1\,{}_{t_{2l}}x_{3i+1}\,{}_{t_{2l-1}}x_1 - {}_{t_{2l-1}}x_{3i}\,{}_{t_{2l}}x_1^2) \\ {}_{t_{2l-1}}x_{3i+6} + (t_{2l} + t_{2l+1})\,{}_{t_{2l}}x_{3i+5} \\ {}_{t_{2l-1}}x_{3i+7} + (t_{2l} + t_{2l+1})({}_{t_{2l-1}}x_{3i+4} - {}_{t_{2l}}x_1\,{}_{t_{2l}}x_{3i+1}\,{}_{t_{2l-1}}x_1 - {}_{t_{2l-1}}x_{3i}\,{}_{t_{2l}}x_1^2)\,{}_{t_{2l}}x_1 \\ \vdots \\ {}_{2l+1}f_n(x_1, x_2, \dots, x_n) \end{bmatrix} = [\overline{{}_{t_{2l+1}}x}],$$

$$N_{t_{2l}}[{}_{2l-1}x_1, {}_{2l-1}x_2, {}_{2l-1}x_3, \dots, {}_{2l-1}x_n] \longrightarrow$$

$$\begin{pmatrix} {}_{t_{2l-1}}x_1 + t_{2l} \\ {}_{t_{2l-2}}x_2 - (t_{2l-1} + t_{2l})\,{}_{t_{2l-1}}x_1 \\ {}_{t_{2l-2}}x_3 + (t_{2l-1} + t_{2l})\,{}_{t_{2l-1}}x_1^2 \\ {}_{t_{2l-2}}x_4 - (t_{2l-1} + t_{2l})\,{}_{t_{2l-1}}x_2 \\ {}_{t_{2l-2}}x_5 + ({}_{t_{2l-1}}x_1^2\,{}_{t_{2l-2}}x_1 - {}_{t_{2l-2}}x_3)(t_{2l-1} + t_{2l}) \\ {}_{t_{2l-2}}x_6 - ({}_{t_{2l-1}}x_1^2\,{}_{t_{2l-2}}x_1 - {}_{t_{2l-2}}x_3)\,{}_{t_{2l-1}}x_1(t_{2l-1} + t_{2l}) \\ {}_{t_{2l-2}}x_7 - (t_{2l-1} + t_{2l})\,{}_{t_{2l-1}}x_5 \\ \vdots \\ {}_{t_{2l-2}}x_{3i+5} + ({}_{t_{2l-1}}x_1^2x_{3i+1} + {}_{t_{2l-1}}x_1\,{}_{t_{2l-2}}x_1\,{}_{t_{2l-1}}x_{3i} - {}_{t_{2l-2}}x_{3i+3})(t_{2l-1} + t_{2l}) \\ {}_{t_{2l-2}}x_{3i+6} - ({}_{t_{2l-1}}x_1^2x_{3i+1} + {}_{t_{2l-1}}x_1\,{}_{t_{2l-2}}x_1\,{}_{t_{2l-1}}x_{3i} - {}_{t_{2l-2}}x_{3i+3})\,{}_{t_{2l-1}}x_1(t_{2l-1} + t_{2l}) \\ {}_{t_{2l-2}}x_{3i+7} - (t_{2l-1} + t_{2l})\,{}_{t_{2l-1}}x_{3i+5} \\ \vdots \\ {}_{2l}f_n(x_1, x_2, \dots, x_n) \end{pmatrix} = (\overline{{}_{t_{2l}}x}).$$

Denote the composition of $N_{t_1} \circ N_{t_2} \circ N_{t_3} \ldots \circ N_{t_k}$ as $N_{t_1,t_2,\dots,t_k}$. It is easy to check that if $N_{t_1,t_2,\dots,t_k}(\bar{x}) = \bar{y}$ then $N_{-t_k,-t_{k-1},\dots,-t_1}(\bar{y}) = \bar{x}$.

The following

$$N_{t_1,t_2,\dots,t_k}(x_1, x_2, \dots x_n) \to ({}_kf_1, {}_kf_2, \dots, {}_kf_n),$$

is a polynomial transformation of $\mathbb{F}_q^n$ into itself such that

$$\begin{aligned} x_1 &\longrightarrow {}_kf_1(x_1, x_2, \dots, x_n), \\ x_2 &\longrightarrow {}_kf_2(x_1, x_2, \dots, x_n), \\ &\vdots \\ x_n &\longrightarrow {}_kf_n(x_1, x_2, \dots, x_n). \end{aligned}$$

Computations show that $\deg_k f_i$ is growing independent from the choice of string $t_1, t_2, \dots, t_k$.

If char$\mathbb{F}_q \neq 2$ then graph $\widetilde{D(n,q)}$ is connected and there exist a path dependent of the choice of $t_1, t_2, \dots, t_k$ conducting one vertex (x) to another one (y).

Let S be a matrix containing degrees of polynomials ${}_kf_{i+1}$, for $i = 1, 2, \dots, n-1$, depending on the length of the password k. Position $s_{i,j}$ shows the degree of polynomial ${}_kf_{i+1}$ if the used password is of length j. The first 5 rows (for $n = 2, 3, 4, 5, 6$) for matrix S are completed as follows: $s_{1,l} = s_{2,l} = 2$, $s_{3,2l-1} = 3$, $s_{3,2l} = 2$, $s_{4,l} = 3$, $s_{5,2l} = 4$, $s_{5,2l+1} = 3$ and the first column corresponding to

TABLE 1. Table contains degree of polynomials ${}_kf_n$ for different length k of key parameter t

		k																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	...
	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	...
	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	...
	4	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	...
	5	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	...
	6	2	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	...
	7	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	...
	8	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	...
	9	2	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	...
	10	4	3	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	...
n	11	3	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	...
	12	2	5	4	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6	...
	13	4	3	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6	5	...
	14	3	4	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	...
	15	2	5	4	7	6	7	6	7	6	7	6	7	6	7	6	7	6	7	6	7	...
	16	4	3	6	5	7	6	7	6	7	6	7	6	7	6	7	6	7	6	7	6	...
	17	3	4	5	6	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

$k = 1$ is completed according to the scheme: $s_{3l+1,1} = 3$, $s_{3l+2,2} = 2$, $s_{3l+3,3} = 4$, $l = 1, 2, 3 \ldots$. The the remaining positions in the matrix S can be completed recursively:

$$\begin{aligned}
s_{3l+3,2l} &= s_{3l+3-2,2l-1} = s_{3l+1,2l-1},\\
s_{3l+3,2l+1} &= s_{3l+3-2,2l+1} + 1 = s_{3l+1,2l+1} + 1,\\
s_{3l+4,2l} &= s_{3l+4-5,2l-1} + 2 = s_{3l-1,2l-1} + 2,\\
s_{3l+4,2l+1} &= s_{3l+4-4,2l+1-1} + 2 = s_{3l,2l} + 2,\\
s_{3l+5,2l} &= s_{3l+5-1,2l} + 1 = s_{3l+1,2l} + 1,\\
s_{3l+5,2l+1} &= s_{3l+5-1,2l+1-1} = s_{3l+4,2l},
\end{aligned}$$

where $l = 1, 2, 3, \ldots$.

Let L_1 and L_2 be sparse affine transformation of the vector space $\mathbb{F}_q^n$

$$\begin{aligned}
L_1 = T_{A,b} &: \bar{x} \longrightarrow \bar{x}A + b,\\
L_2 = T_{C,d} &: \bar{x} \longrightarrow \bar{x}C + d,
\end{aligned}$$

where $A = \left[a_{i,j}\right]$ and $C = \left[c_{i,j}\right]$ are $n \times n$ matrices with $a_{i,j}, c_{i,j} \in \mathbb{F}_q$, $|A| \neq 0$ and $|C| \neq 0$. It is clear that

$$\begin{aligned}
L_1^{-1} &= T_{A,b}^{-1} = T_{A^{-1},-bA^{-1}},\\
L_2^{-1} &= T_{C,d}^{-1} = T_{C^{-1},-dC^{-1}}.
\end{aligned}$$

Alice and Bob agree private encryption key $K_e = (L_1, L_2, \mathrm{t} = (t_1, t_2, \ldots, t_k), n)$, where $t_{i+1} \neq -t_i$ for $i = 1, \ldots, k-1$ and they must keep the key in secret. Messages are written using characters belonging to the alphabet $\mathbb{F}_q$. To encode they use the composition:

$$F = L_1 \circ N_{t_1,t_2,\ldots,t_{2s}} \circ L_2 = L_1 \circ N_{t_1} \circ N_{t_2} \circ N_{t_3} \ldots \circ N_{t_k} \circ L_2.$$

Alice and Bob can use their knowledge about quadruple (L_1, L_2, t,n) for the decryption. The decryption map is of the form:

$$L_2^{-1} \circ N_{-t_k,-t_{k-1},\ldots,-t_1} \circ L_1^{-1}.$$

Let $q = p^m$, where p is prime number. Cipher-text before transmitting should be rewritten in alphabet $\mathbb{F}_p$ to hide key parameter n.

Let $g(n, k)$ denote the degree of polynomial ${}_kf_n$. If k is fixed $\lim\limits_{n\to\infty} g(n, k) = k+3$ and if n is fixed then $\lim\limits_{k\to\infty} g(n, k) = \left\lfloor \frac{n}{3} \right\rfloor + 2$. We propose to use key parameter $t = (t_1, t_2, \ldots, t_k)$ of length $k = \alpha n + \beta$, $\alpha \in (0, 1)$. This choice of k allows us to create multivariate map F of unbounded degree.

Theorem 3.1. *In password is of length $k = \alpha n + \beta \in \mathbb{N}$ then degree (maximal degree of monomial) of multivariate map F:*

$$\begin{aligned} x_1 &\longrightarrow {}_kf_1(x_1, x_2, \ldots, x_n),\\ x_2 &\longrightarrow {}_kf_2(x_1, x_2, \ldots, x_n),\\ &\vdots\\ x_n &\longrightarrow {}_kf_n(x_1, x_2, \ldots, x_n) \end{aligned}$$

and is unbounded:

$$\deg F_{\mathrm{t},n} = \deg F(L_1, L_2, \mathrm{t}, n, \mathbb{F}_q) = g(n, k)$$

and

$$\lim_{k\to\infty, n\to\infty} g(n, k) = \infty$$

Proof. The proof in a natural way follows from recursive equations (3) and mathematical induction. □

For fixed L_1, L_2 and $2k \leq g(\widetilde{D(n, q)})$ different keys produce distinct cipher-text ($g(\widetilde{D(n, q)})$ is the girth of graph). The encoding complexity is $O(n^2)$. It is impractical to decrypt a message on the basis of the cipher-text and knowledge of the encryption/decryption algorithm. We do not need to keep the algorithm secret. To decrypt a message without knowledge of secret key we need to solve nonlinear system of equations over finite field (the maximum degree of this polynomials is keep in secret). According to Theorem 1 the degree of map F is unbounded if key parameter t is of length $k = \alpha n + \beta$. The $\deg F^{-1} = \deg F$ so Linearization Attacks on this symmetric-key algorithm are impossible. Solving such system of equation is a NP-hard problem in general.

Remark 3.2. *One can try Dijkstra's algorithm of finding the shortest pass between plaintext and cipher-text. Notice that its complexity is $O(v \log v)$, but here v is exponential q^n. Therefore we get worse complexity then even brute force search via the key space.*

References

[1] Ding J., Gower J. E., Schmidt D. S., *Multivariate Public Key Cryptosystems*, 260. Springer, Advances in Information Security, Vol. 25, (2006)

[2] Koichi Sakumoto, *Public-Key Identification Schemes Based on Multivariate Cubic Polynomials*, in Lecture Notes in Computer Science, Vol. 7293, pp 172–189 (2012)

[3] Ustimenko V., *Coordinatisation of Trees and their Quotients*, in the "Voronoj's Impact on Modern Science", Kiev, Institute of Mathematics, Vol. 2, pp 125–152 (1998)

[4] Ustimenko V., *CRYPTIM: Graphs as Tools for Symmetric Encryption*, Lecture Notes in Computer Science, Springer, Vol. 2227, pp 278–287 (2001)

[5] Lazebnik F., Ustimenko V. A. and Woldar A. J., *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, Vol.32, N1, pp 73–79 (1995)

[6] Ustimenko V. *Maximality of affine group and hidden graph cryptosystems*, J. Algebra Discrete Math., No. 1, pp 133–150 (2005)

[7] Wróblewska A., *On some properties of graph based public keys*, Albanian Journal of Mathematics, Vol. 2, No. 3, pp 229–234, NATO Advanced Studies Institute: "New challenges in digital communications" (2008)

[8] Ustimenko V., Wrb́lewska A., *On some algebraic aspects of data security in cloud computing*, Proceedings of International conference "Applications of Computer Algebra", Malaga, pp 144–147 (2013)

[9] Kotorowicz J., Ustimenko V., *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condensed Matters Physics, Special Issue: Proceedings of the international conferences "Infinite particle systems, Complex systems theory and its application", Kazimerz Dolny, Poland, 2006, 11 (No. 2(54)), pp 347–360 (2008)

[10] Klisowski M., Ustimenko V., *On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator*, Mathematics in Computer Science, , Vol. 6, No. 2, pp 181–198 (2012)

[11] Biggs N. L., *Algebraic Graph Theory*, (2nd ed), Cambridge, University Press (1993)

[12] Bourbaki N., *Lie Groups and Lie Algebras*, Springer (1989)

[13] Shaska T., Ustimenko V., *On some applications of graph theory to cryptography and turbocoding.* Albanian J. Math., vol. 2, no. 3, pp. 249âĂŞ255. In: Proceedings of the NATO Advanced Studies Institute: New challenges in digital communications (2008)

[14] Koblitz N., *Algebraic Aspects of Cryptograph*, Springer (1998)

[15] Simonovitz M., *Extermal Graph Theory* , In "Selected Topics in Graph Theory", 2, edited by L. W. Beineke and R. J. Wilson, Academic Press, London, pp 161–200 (1983)

[16] Ustimenko V., *Some optimisation problems for graphs and multivariate cryptography* (in Russian), In Topics in Graph Theory: A tribute to A.A. and T. E. Zykova on the ocassion of A. A. Zykov birthday, pp 15–25, (2013), www.math.uiuc.edu/kostochka.

[17] Ustimenko V., *On the extremal graph theory for directed graphs and its cryptographical applications* In: Shaska T., Huffman W.C., Joener D. and Ustimenko V., Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, Vol. 3, pp 181–200 (2007).

[18] Ustimenko V., *On the cryptographical properties of extreme algebraic graphs*, in Algebraic Aspects of Digital Communications, IOS Press (Lectures of Advanced NATO Institute, NATO Science for Peace and Security Series - D: Information and Communication Security, Vol. 24, p 296 (2009)

ALBANIAN JOURNAL OF MATHEMATICS
Volume 8, Number 1, Pages 49–53
ISSN: 1930-1235; (**2014**)

ON THE CONGRUENT NUMBER PROBLEM OVER INTEGERS OF REAL NUMBER FIELDS

Albertas Zinevičius

Department of Mathematics and Informatics,
Vilnius University,
Naugarduko 24, Vilnius, LT-03225,
Lithuania
and
Institute of Mathematics and Informatics,
Akademijos 4, Vilnius, LT-08663,
Lithuania
Email: albertas.zinevicius@mif.vu.lt

Abstract. Given a real finite field extension $K/\mathbb{Q}$ of degree d and class number h_K and a positive integer a, we show that there is a set of rational prime numbers of relative density at least $1/(2dh_K)$ that have a principal prime factor $\pi\mathcal{O}_K \subset \mathcal{O}_K$ of degree one such that the equation $a\pi^2 = x^4 - y^2$ has no nontrivial solutions in $\mathcal{O}_K$.

1. Introduction

The classical congruent number problem asks for an algorithm that would decide if a given positive integer n is the area of a right triangle with rational side lengths. The existence of such a triangle is equivalent to the solvability of the equation

$$y^2 = x^4 - 16n^2 \tag{1}$$

in rational numbers (x, y) with x nonzero. It is known that the existence of such a (surprisingly simple) algorithm would follow from the conjecture of Birch and Swinnerton-Dyer, as was shown in the work of Tunnell [12]. It was noted by Jedrzejak [6] that, under assumption of the same conjecture, Tunnell's theorem together with the work of Tada [10] imply that every positive integer is the area of some right triangle with side lengths in the quartic extension $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

It is difficult to expect, on the other hand, that the equation (1) could have solutions among the integers $\mathcal{O}_K$ of a fixed number field K for all n. Indeed, as it was remarked by Stoll [9], the conjecture of Bombieri-Lang suggests the opposite.

2010 *Mathematics Subject Classification.* 11D45, 11H06.
Key words and phrases. Congruent numbers, real number fields, rings of integers, prime ideals.

That this can never happen when K is a cyclic extension, can be concluded from the following statement that we showed in [13]:

Theorem A. *Let K be a finite Galois extension of the field of rational numbers with cyclic Galois group* $\mathrm{Gal}(K/\mathbb{Q})$ *and let a be a nonzero (rational) integer. Then the set of rational prime numbers p for which the equation*

$$ap^2 = x^4 - y^2 \tag{2}$$

in unknowns x, y does not have a solution $(x, y) \in \mathcal{O}_K \times \mathcal{O}_K$ with $x \neq 0$, has lower relative density at least $1/2$ in the set of (rational) prime numbers that remain inert in K.

The conjectural solvability of (1) in some number fields for all positive integers n raises the question of whether one could expect to find a number field K in which all the equations (1) were solvable when the parameter n also varies over K (rather than $\mathbb{Q}$). This still has the same geometric interpretation when the extension K is real. The analogous question for integers of number fields becomes easier and can be settled:

Theorem 1. *Let K be a finite real extension of the field of rational numbers, of degree d and class number h_K, and let a be a positive integer. Then there is a set of rational prime numbers p of relative density at least $1/(2dh_K)$, such that the principal ideal $p\mathcal{O}_K$ has a principal prime factor $\pi\mathcal{O}_K$ of degree one for which the equation*

$$a\pi^2 = x^4 - y^2 \tag{3}$$

in unknowns x, y does not have a solution $(x, y) \in \mathcal{O}_K \times \mathcal{O}_K$ with $x \neq 0$.

Most of the proof of this observation translates *mutatis mutandis* from the proof of Theorem A, which is indebted to the results of Jarden-Narkiewicz and Green-Tao. Additionally, a fundamental result of class field theory is employed in Lemma 3. The proof does not suggest that the density $1/(2dh_K)$ could be precise for some number fields K. The author of this note would find it interesting to see a demonstration that (1) does not have solutions over $\mathcal{O}_K$ for many rational integer values of the parameter n.

2. Proof of Theorem 1

For the proof of the theorem we borrow two statements from [4] and [5], respectively, that we state here as lemmas:

Lemma 1. *Let A be any subset of the prime numbers of positive relative upper density. Then A contains infinitely many arithmetic progressions of length l for all l.*

Lemma 2. *If R is a finitely generated integral domain of zero characteristic and l is an integer, then there exists a constant $A_l(R)$ such that every arithmetic progression in R having more than $A_l(R)$ elements contains an element which is not a sum of l units.*

In addition, we will use the following lemma:

Lemma 3. *The relative density of prime numbers $p \subset \mathbb{Z}$ such that the principal ideal $p\mathcal{O}_K \subset \mathcal{O}_K$ has a principal prime factor $\mathfrak{p} = \pi\mathcal{O}_K$ of degree one that remains inert in the quadratic extension $K(\sqrt{-a})/K$, is at least $1/(2dh_K)$.*

Proof of Lemma 3. Notice first that, since K is a subfield of the real numbers, its Hilbert class field $\operatorname{Cl}(K)$ is also a subfield of the real numbers (as $\operatorname{Cl}(K)/K$ must be unramified at the infinite prime). Therefore there is an element $\sigma \in \operatorname{Gal}(\operatorname{Cl}(K)(\sqrt{-a})/K)$ that fixes $\operatorname{Cl}(K)$ but is not the identity automorphism.

Let L be the Galois closure of the extension $\operatorname{Cl}(K)(\sqrt{-a})/\mathbb{Q}$. Since the extension $L/\operatorname{Cl}(K)(\sqrt{-a})$ is Galois and $\sigma \in \operatorname{Aut}(\operatorname{Cl}(K)(\sqrt{-a}))$, one can extend σ to an element of $\operatorname{Gal}(L/\operatorname{Cl}(K))$. More precisely, there are $[L : \operatorname{Cl}(K)(\sqrt{-a})]$ distinct elements $\sigma_j \in \operatorname{Gal}(L/\operatorname{Cl}(K)), j = 1, \ldots, [L : \operatorname{Cl}(K)(\sqrt{-a})]$, that coincide with σ on the subfield $\operatorname{Cl}(K)(\sqrt{-a})$.

Recall that for any tower of number fields $E \subset E' \subset E''$, where E''/E is Galois, the decomposition type of a prime ideal $\mathfrak{q} \subset \mathcal{O}_E$, that does not divide $\Delta_{E''/E}$, in the extension E'/E coincides with the cycle structure of the permutation of $\operatorname{Gal}(E''/E)/\operatorname{Gal}(E''/E')$ that is induced by the action of (any) Frobenius element $\operatorname{Frob}_{\mathfrak{q}}$ of the prime ideal $\mathfrak{q}$.

When $E = \mathbb{Q}, E' = K, E'' = L$ and p is a rational prime that does not divide the discriminant $\Delta_{L/\mathbb{Q}}$, it follows that the ideal $p\mathcal{O}_K \subset \mathcal{O}_K$ has a prime factor $\mathfrak{p} \subset \mathcal{O}_K$ of degree one if and only if the conjugacy class of the Frobenius element $\operatorname{Frob}_p \in \operatorname{Gal}(L/\mathbb{Q})$ intersects the subgroup $\operatorname{Gal}(L/K)$ (see, e.g., [7]). In particular, when the conjugacy class of Frob_p contains one of σ_j as above, $p\mathcal{O}_K$ has a prime factor $\mathfrak{p}$ of degree one.

Likewise, when $E = K, E' = \operatorname{Cl}(K), E'' = L$, it follows that a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ as above splits completely in the extension $\operatorname{Cl}(K)/K$. Indeed, we may assume, without a loss of generality, that

$$\operatorname{Frob}_p(x) \equiv x^{\#\mathbb{Z}/p\mathbb{Z}} \mod \mathfrak{q}$$

for all $x \in \mathcal{O}_L$ and a prime ideal $\mathfrak{q} \subset \mathcal{O}_L$ that lies over $\mathfrak{p}$ (by replacing Frob_p, if necessary, with another element from the conjugacy class of Frob_p). Since $\mathfrak{p}$ is of degree 1, we have $\#\mathbb{Z}/p\mathbb{Z} = \#\mathcal{O}_K/\mathfrak{p}$. Hence holds

$$\operatorname{Frob}_p(x) \equiv x^{\#\mathcal{O}_K/\mathfrak{p}} \mod \mathfrak{q},$$

for all $x \in \mathcal{O}_L$. Thus Frob_p is also a Frobenius element $\operatorname{Frob}_{\mathfrak{p}}$ of $\mathfrak{p}$ (with respect to the extension L/K). The cycle structure of the permutation of the group $\operatorname{Gal}(L/K)/\operatorname{Gal}(L/\operatorname{Cl}(K))$ induced by $\operatorname{Frob}_{\mathfrak{p}}$ is then the same as that induced by any σ_j that is in the same conjugacy class as Frob_p. Consequently, it is the product of 1-cycles (since $\sigma_j \in \operatorname{Gal}(L/\operatorname{Cl}(K))$ acts on $\operatorname{Gal}(L/K)/\operatorname{Gal}(L/\operatorname{Cl}(K))$ trivially).

On the other hand, the permutation of $\operatorname{Gal}(L/K)/\operatorname{Gal}(L/K(\sqrt{-a}))$ induced by the σ_j is not the trivial one since $\sigma_j \notin \operatorname{Gal}(L/K(\sqrt{-a}))$. Consequently, the prime ideal $\mathfrak{p}$ remains inert in the extension $K(\sqrt{-a})/K$.

A fundamental result of class field theory asserts that prime ideals of K that split completely in the extension $\operatorname{Cl}(K)/K$ are principal [8]. Thus $\mathfrak{p} = \pi\mathcal{O}_K$ for some prime element $\pi \in \mathcal{O}_K$ that remains prime in $\mathcal{O}_{K(\sqrt{-a})}$.

By the Chebotarev density theorem [11], the density of rational prime numbers p with Frobenius symbol Frob_p (with respect to the extension $L/\mathbb{Q}$) in the same conjugacy class as some σ_j is equal to the number of elements in those conjugacy classes of $\mathrm{Gal}(L/\mathbb{Q})$ that contain some σ_j, divided by the size of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$. It is therefore, at least

$$\#\{\sigma_j\}/\#\,\mathrm{Gal}(L/\mathbb{Q}) = ([L:\mathrm{Cl}(K)]/2)/([\mathrm{Cl}(K):\mathbb{Q}][L:\mathrm{Cl}(K)]) = 1/(2dh_K).$$

□

Proof of Theorem 1. Let $\mathfrak{p} = \pi\mathcal{O}_K$ be a prime ideal as in Lemma 3. If the equation

$$a\pi^2 = x^4 - y^2 = (x^2+y)(x^2-y)$$

has a solution in $\mathcal{O}_K$ with $x \neq 0$ then either both x^2-y, x^2+y are divisible by π or not. In the first case,

$$\begin{cases} x^2 - y = \pi r \\ x^2 + y = \pi a r^{-1} \end{cases}$$

for some $r \in \mathcal{O}_K$ that divides a. Denote by σ the generator of $\mathrm{Gal}(K(\sqrt{-a})/K)$. By adding the equations one obtains

$$2x^2r = \pi(r^2+a) = \pi(r+\sqrt{-1})(r-\sqrt{-a}) = \pi(r+\sqrt{-1})\sigma(r+\sqrt{-a}).$$

We thus can see that, since π is a prime element of the ring of integers of $K(\sqrt{-a})$ that is mapped to an associate of itself by σ , the highest power of π that divides the right-hand side must be odd. On the other hand, the highest power of any prime element that divides the left-hand side and does not divide $2a$ is even. Therefore, the first case may hold for at most finitely many prime ideals $\pi\mathcal{O}_K$. We thus may restrict ourselves to the second case, i.e., assume that

$$\begin{cases} x^2 - y = \pi^2 a r^{-1} \\ x^2 + y = r \end{cases}$$

holds for some $r \in \mathcal{O}_K$ that divides a. By adding the equations again, one obtains

$$2x^2r = r^2 + \pi^2 a.$$

Let K' be a field extension of K that is generated by elements of the form $\sqrt{r}$, where $r \in \mathcal{O}_K$ divide a. Up to multiplication by units, there are only finitely many such r. Let $r_1, ..., r_v$ be their representatives. The Dirichlet unit theorem [2] tells also that the multiplicative group of units of $\mathcal{O}_K$ is finitely generated. Let $e_1, ..., e_s$ be its generators. Then $K' = K(\sqrt{2}, \sqrt{e_1}, ..., \sqrt{e_s}, \sqrt{r_1}, ..., \sqrt{r_v})$ is a finite extension of K. Over $\mathcal{O}_{K'}$ one can write

$$(x\sqrt{2r} - \pi\sqrt{a})(x\sqrt{2r} + \pi\sqrt{a}) = r^2.$$

Hence both $x\sqrt{2r} - \pi\sqrt{a}, x\sqrt{2r} + \pi\sqrt{a}$ are divisors of a^2 in $\mathcal{O}_{K'}$. Consequently, $2\pi\sqrt{a}$ is a sum of two divisors of a^2.

We claim that such ideals $\mathfrak{p} = \pi\mathcal{O}_K$ have density zero among the prime ideals of the ring $\mathcal{O}_K$. Let M denote the Galois closure of the field extension $K'/\mathbb{Q}$. Note that there is a subset $G_\pi \subset \mathrm{Gal}(M/\mathbb{Q})$ of cardinality d such that $Nm_{K/\mathbb{Q}}(\pi) =$

$\prod_{\sigma\in G_\pi}\sigma(\pi)$. Thus,

$$\prod_{\sigma\in G_\pi}\sigma(2\pi\sqrt{a}) = Nm_{K/\mathbb{Q}}(\pi)\prod_{\sigma\in G_\pi}\sigma(2\sqrt{a}).$$

On the other hand, $\sigma(2\pi\sqrt{a})$ is a sum of two divisors of a^2 in $\mathcal{O}_M$, and hence $\prod_{\sigma\in G_\pi}\sigma(2\pi\sqrt{a})$ is a sum of 2^d divisors of a^{2d} in $\mathcal{O}_M$. Furthermore, since $\mathfrak{p}$ is of degree one,

$$|Nm_{K/\mathbb{Q}}(\pi)| = \#\mathcal{O}_K/\mathfrak{p} = p.$$

Had prime ideals of the form $\mathfrak{p} = \pi\mathcal{O}_K$ positive upper density among the prime ideals of $\mathcal{O}_K$, then the upper density of rational prime numbers of the form $|Nm_{K/\mathbb{Q}}(\pi)|$ would also be positive in the set of rational prime numbers. Moreover, there would exist a fixed $G \subset \mathrm{Gal}(M/\mathbb{Q})$ such that $G_\pi = G$ for a positive fraction of the prime numbers $|Nm_{K/\mathbb{Q}}(\pi)|$. It would follow from the Lemma 1 that there must exist arbitrarily long arithmetic progressions with elements of the form $Nm_{K/\mathbb{Q}}(\pi)\prod_{\sigma\in G}\sigma(2\sqrt{a})$.

Let $r'_1, \dots, r'_l \in \mathcal{O}_M$ be the representatives of the divisors of a^{2d} modulo the multiplicative group of units of $\mathcal{O}_M$. Notice that the ring $\mathcal{O}_M[1/r'_1, \dots, 1/r'_l]$ is finitely generated. Furthermore, any term of an arithmetic progression as above is a sum of 2^d units in this ring. However, by Lemma 2, the length of such arithmetic progressions cannot be arbitrarily large, a contradiction. Thus, prime ideals $\pi\mathcal{O}_K$ as in Lemma 3 for which (3) holds have density zero.

□

References

[1] Chandrasekar V., *The congruent number problem*, Resonance **3**(8), 33-45 (1998).

[2] Narkiewicz W., *Elementary and analytic theory of algebraic numbers*, 3rd ed., p. 98, Springer-Verlag, Berlin-Heidelberg (2004).

[3] Girondo E., Gonzalez-Diez G., Gonzalez-Jimenez E., Steuding R., Steuding J., *Right triangles with algebraic sides and elliptic curves over number fields*, Math. Slovaca **59**(3), 299-306 (2009).

[4] Green B., Tao T., *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167**(2), 481-547 (2008).

[5] Jarden M., Narkiewicz W., *On sums of units*, Monatsh. Math. **150**(4), 327-332 (2006).

[6] Jedrzejak T., *Congruent numbers over real number fields*, Colloquium Mathematicum **128**(2), 179-186 (2012).

[7] Neukirch J., *Algebraische Zahlentheorie*, p. 570, Springer-Verlag, Berlin-Heidelberg (2007).

[8] Neukirch J., *Algebraische Zahlentheorie*, p. 429, Springer-Verlag, Berlin-Heidelberg (2007).

[9] Stoll M., personal communication (2014).

[10] Tada M., *Congruent numbers over real quadratic fields*, Hiroshima Math. J. **31**(2), 331-343 (2001).

[11] Tschebotareff N., *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. **95**, 191-228 (1925).

[12] Tunnell J.B., *A Classical Diophantine problem and modular forms of Weight 3/2*, Inventiones Mathematicae **72**, 323-334 (1983).

[13] Zinevičius A., *On the congruent number problem over integers of cyclic extensions* (to appear in Mathematica Slovaca).

ALBANIAN JOURNAL OF MATHEMATICS
Volume 8, Number 1, Pages 55–70
ISSN: 1930-1235; (**2014**)

GRÖBNER TECHNIQUES AND RIBBONS

Anand Deopurkar
Department of Mathematics
Columbia University
2990 Broadway, New York, NY 10027
Email: anandrd@math.columbia.edu

Maksym Fedorchuk
Department of Mathematics
Boston College
140 Commonwealth Avenue, Chestnut Hill, MA 02467
Email: maksym.fedorchuk@bc.edu

David Swinarski
Department of Mathematics
Fordham University
113 W 60th Street, New York, NY 10023
Email: dswinarski@fordham.edu

Abstract. We use Gröbner basis techniques to study the balanced canonical ribbon in each odd genus $g \geq 5$. We obtain equations and syzygies of the ribbon, give a Gröbner interpretation of part of Alper, Fedorchuk, and Smyth's proof of finite Hilbert stability for canonical curves, and discuss the obstacles in using ribbons to give a new proof of Generic Green's Conjecture (Voisin's Theorem).

1. Introduction

A canonical rational ribbon is a double structure on $\mathbb{P}^1$ with a very ample dualizing line bundle. As Bayer and Eisenbud show in their seminal paper [2], canonical rational ribbons arise as flat limits in families of canonically embedded curves specializing to a hyperelliptic curve in moduli. In [7], Fong proved that every canonically embedded rational ribbon can be smoothed to a canonical curve with the same Clifford index as the ribbon. Conversely, if one performs stable reduction on a family of smooth curves specializing to a ribbon, one will obtain as the stable limit a Deligne-Mumford stable curve in the closure of the hyperelliptic locus. Hence, it

2000 *Mathematics Subject Classification.* 13D02; 14Q05.
Key words and phrases. Ribbons, Gröbner basis, geometric invariant theory.

is useful to think of ribbons as possible replacements of hyperelliptic curves in the Hilbert scheme of canonical curves.

In [2], Bayer and Eisenbud studied ribbons with a view toward Generic Green's Conjecture (now Voisin's Theorem) on the graded Betti numbers of canonically embedded curves. By Fong's Theorem and the upper semicontinuity of Betti numbers, proving Green's Conjecture for ribbons would establish the result for a general canonical curve as well. However, it seems that the approach suggested in [2] has never been completed.

More recently, ribbons have appeared in the log minimal model program (LMMP) for the pair $(\overline{\mathcal{M}}_g, \delta)$, where $\overline{\mathcal{M}}_g$ is the moduli space of Deligne-Mumford stable curves, and δ is the divisor of nodal curves. Geometric invariant theory (GIT) calculations suggest that at a certain stage of the LMMP, the locus of hyperelliptic curves in $\overline{\mathcal{M}}_g$ will be flipped to a locus of canonically embedded A_{2g}-curves (see [6, Section 4]). While ribbons lie in codimension 2 inside the locus of A_{2g}-curves, their GIT stability analysis is simplified by the fact that some canonically embedded ribbons admit a $\mathbb{G}_m$-action.

It is conjectured that GIT quotients of the Hilbert scheme of canonical curves are log canonical models of $\overline{\mathcal{M}}_g$ that appear at later stages of the LMMP (see [16]). In [1], Alper, Fedorchuk, and Smyth prove that a general odd genus canonical ribbon is indeed GIT semistable in this setup by proving semistability of a special canonical ribbon with $\mathbb{G}_m$-action, called *the balanced ribbon*. We recall the definition of the balanced ribbon in Section 4. In Section 5.2, we reinterpret certain results of [1] in terms of Gröbner bases to gain further understanding of the combinatorics involved.

The outline of this paper is as follows. In Section 2, we describe the two problems we study using ribbons: Generic Green's Conjecture (Voisin's Theorem) and finite Hilbert stability of canonical curves. Section 3 is devoted to a detailed example of using Gröbner techniques to analyze rational normal curves. We included this as a model of how one can use Gröbner basis techniques to analyze ribbons. In Section 4, we describe balanced ribbons in detail and obtain their equations and first syzygies. The main result of the paper is Theorem 4.4. In Section 5, we discuss applications of Gröbner basis techniques for ribbons.

1.1. **Acknowledgements.** We would like to thank the American Institute of Mathematics for hosting the workshop "Log minimal model program for moduli spaces" organized by Jarod Alper, Brendan Hassett, David Smyth, and the second author, where we began work on this project. The second author is partially supported by NSF grant DMS-1259226.

2. Two problems involving ribbons

2.1. Ribbons.

We begin with the most general definition of ribbons:

Definition 2.1 ([2, §1]). *A* ribbon *on D is a scheme C equipped with an isomorphism $D \simeq C_{\text{red}}$ such that the ideal sheaf $\mathcal{I}$ of D in C satisfies $\mathcal{I}^2 = 0$, and $\mathcal{I}$ is a line bundle on D.*

In the sequel, we will only consider the case $D = \mathbb{P}^1$. In fact, we shall only consider a very special family of ribbons on $\mathbb{P}^1$, one in each odd genus, called balanced ribbons; see Definition 4.1.

Our motivation for studying ribbons is to gain insight into two problems in algebraic geometry: Generic Green's Conjecture (Voisin's Theorem) and finite Hilbert stability. In this section, we state these two problems.

2.2. **Generic Green's Conjecture.** Let $S = \mathbb{K}[x_0, \ldots, x_k]$, and let M be a finitely generated graded S-module. Let

$$\cdots \to \mathbf{F}_2 \to \mathbf{F}_1 \to \mathbf{F}_0 \to M \to 0$$

be the minimal graded free resolution of M. Since it is a graded free resolution, we have for each i that

$$\mathbf{F}_i = \bigoplus S(-j)^{\oplus \beta_{i,j}}.$$

The numbers $\beta_{i,j}$ are called the *graded Betti numbers* of M. By the definition of Tor, we also have $\beta_{i,j} = \dim_{\mathbb{K}} \operatorname{Tor}_i^S(M, \mathbb{K})_j$. (This observation will be important in the sequel; since the numbers $\beta_{i,j}$ are dimensions of cohomology groups, they are upper semicontinuous in flat families.)

The Betti table of M is the collection of Betti numbers. By convention, the entry in row j column i is $\beta_{i,i+j}$ so that the table looks as follows:

$$\begin{array}{cccccc}
\beta_{0,0} & \beta_{1,1} & \beta_{2,2} & \beta_{3,3} & \beta_{4,4} & \cdots \\
\beta_{0,1} & \beta_{1,2} & \beta_{2,3} & \beta_{3,4} & \beta_{4,5} & \cdots \\
\beta_{0,2} & \beta_{1,3} & \beta_{2,4} & \beta_{3,5} & \beta_{4,6} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

Definition 2.2. *A free resolution is* pure *if there is at most one nonzero $\beta_{i,j}$ for each $\mathbf{F}_i$. We will say that a homogeneous ideal in S has* pure Betti table *if its minimal graded free resolution is pure.*

Under the conventions for displaying Betti tables, purity corresponds to the property that there is at most one nonzero entry in each column.

We may now state the generic version of the famous Green's Conjecture [11], which was proven by Voisin in [21] for even genus and in [22] for odd genus.

Theorem 2.3 (Generic Green's Conjecture)**.** *The homogeneous coordinate ring of a general canonical curve of odd genus has a pure Betti table.*

2.3. **Finite Hilbert stability.** In the 1960's, Mumford developed geometric invariant theory (GIT) to construct the moduli space of smooth curves $\mathcal{M}_g$ as a quasi-projective variety. GIT has been an important (but difficult to wield) tool in algebraic geometry ever since.

One of Mumford's foundational insights was that GIT quotients should depend on two ingredients:

(1) a scheme X with an action of a reductive algebraic group G;
(2) a linearization of the group action, that is, a lifting of the group action to the action on sections of an ample line bundle L.

Given these two ingredients, the GIT quotient $X/\!\!/_L G$ is defined as $\operatorname{Proj}(R)$, where R is the ring of invariants of the section ring of L. There is a rational map from X to $X/\!\!/_L G$ which is defined at a point $x \in X$ if there exists an invariant section of a power of L that does not vanish at x. Such points are said to be *semistable.*

In the early 1980's, Gieseker built on Mumford's work and gave a GIT construction of the moduli space of stable curves $\overline{\mathcal{M}}_g$ [8, 9]. We describe his setup in more detail now:

Consider $X \subset \mathbb{P}^k$. Let $S = \mathbb{K}[x_0, \dots, x_k]$ and let I be the ideal of X. We call the point in the appropriate Grassmannian parameterizing the subspace $I_m \subseteq S_m$ the m^{th} *inner Hilbert point of* I, and if $S_m \to \mathrm{H}^0(X, \mathcal{O}_X(m))$ is surjective, we call the point in the appropriate Grassmannian parameterizing this quotient the m^{th} *outer Hilbert point of* X. (The adjectives "inner" and "outer" will be explained below in Section 3.4.) In each case, the Plücker line bundle on the relevant Grassmannian yields a GIT linearization of the natural $\mathrm{SL}(k+1)$-action.

The terminology *Hilbert points* comes from the fact that for sufficiently large m the sequence

$$0 \to I_m \to S_m \to \mathrm{H}^0(X, \mathcal{O}_X(m)) \to 0$$

is exact for all subschemes X with a fixed Hilbert polynomial $P(t)$. Therefore, the assignment

$$X \subset \mathbb{P}^k \mapsto [S_m \to \mathrm{H}^0(X, \mathcal{O}_X(m))] \in \mathbf{Gr}(P(m), S_m)$$

embeds the Hilbert scheme in the Grassmannian of $P(m)$-dimensional quotients of S_m.

Recently, Hassett, Hyeon, and many others have extended Gieseker's work with the aim of carrying out the log minimal model program for $\overline{\mathcal{M}}_g$. Specifically, Gieseker proved GIT stability of smooth curves of sufficiently high degree when $m \gg 0$, while the more recent work has focused on quotients when the curves are canonically or bicanonically embedded, and when the linearization parameter m is small. For example, the interesting values of m in the bicanonical case are $2 \leq m \leq 6$ [16]. We will refer to the GIT stability problem for small fixed m as *finite Hilbert stability* (in contrast with Gieseker's *asymptotic Hilbert stability*).

Ribbons play an important role in the proof of finite Hilbert stability. In [1], Alper, Fedorchuk, and Smyth show that in each odd genus, there is a ribbon called the balanced ribbon whose m^{th} Hilbert point is semistable for any $m \geq 2$. This implies that m^{th} Hilbert point of a general odd genus canonical curve is also Hilbert semistable. See Sections 4 and 5 for more details.

3. Motivating example: rational normal curves

In this section, we use Gröbner techniques to analyze the Betti tables and finite Hilbert stability of rational normal curves. The calculations below are presented as a model of what could be done for balanced ribbons. Some parts of the calculations below are standard exercises in commutative algebra. Also, one can give much more conceptual proofs of the two main results below using some of the additional good properties of rational normal curves. However, in this section, we use Gröbner basis calculations because these tools are available for ribbons, too.

3.1. **Parametrization.** Recall that the rational normal curve of degree k is the closure of the morphism $\operatorname{Spec} \mathbb{K}[t] \to \mathbb{P}^k$ given by

$$t \mapsto [1 : t : t^2 : \cdots : t^k].$$

3.2. **Elimination.** To obtain equations for the rational normal curve of degree k, we eliminate t from the parameterization above. Let $x_0, \dots, x_k$ be coordinates on $\mathbb{P}^k$. The parameterization above yields the equations $tx_i - x_{i+1}$ for $i = 0, \dots, k-1$. Hence, the elimination ideal is

$$I_E = \langle tx_i - x_{i+1} \mid i = 0, \dots, k-1 \rangle.$$

For the elimination order, we use the Bayer-Stillman 1-elimination order with t first, followed by grevlex on the variables $x_0, \dots, x_k$.

Theorem 3.1. *The following quadrics form a Gröbner basis with respect to the Bayer-Stillman elimination term order for the elimination ideal I_E of the rational normal curve of degree k:*

(1) $\{tx_i - x_{i+1} \mid i = 0, \dots, k-1\}$
(2) $\{x_{i+1}x_j - x_ix_{j+1} \mid 0 \leq i < j \leq k-1\}$

Proof. We use Buchberger's algorithm to show that Type (1) and Type (2) quadrics indeed form a Gröbner basis with respect to the specified term order. First, we compute the S-pairs for a pair of Type (1) generators listed above. Without loss of generality, suppose that $i < j$. We have

$$\begin{aligned} S(\underline{tx_i} - x_{i+1}, \underline{tx_j} - x_{j+1}) &= x_j(\underline{tx_i} - x_{i+1}) - x_i(\underline{tx_j} - x_{j+1}) \\ &= -\underline{x_jx_{i+1}} + x_ix_{j+1}. \end{aligned}$$

This cannot be further reduced using the Gröbner basis elements of the form $tx_\ell - x_{\ell+1}$, so we add $\underline{x_{i+1}x_j} - x_ix_{j+1}$ to the Gröbner basis.

Next, we consider the S-pairs between a generator of the form $\underline{tx_i} - x_{i+1}$ and a generator of the form $\underline{x_{a+1}x_b} - x_ax_{b+1}$. The leading terms are coprime unless $i = a+1$ or $i = b$. Suppose first that $i = a+1$. Then

$$\begin{aligned} S(\underline{tx_i} - x_{i+1}, \underline{x_ix_b} - x_{i-1}x_{b+1}) &= x_b(\underline{tx_i} - x_{i+1}) - t(\underline{x_ix_b} - x_{i-1}x_{b+1}) \\ &= -x_{i+1}x_b + tx_{i-1}x_{b+1}. \end{aligned}$$

Subtracting $x_{b+1}(tx_{i-1} - x_i)$ yields

$$-x_{i+1}x_b + x_ix_{b+1},$$

which is already in the Gröbner basis.

Similarly, we can argue that if $i = b$, the S-pair reduces to 0 under the Gröbner basis.

Finally, we consider the S-pairs between two generators of the form $\underline{x_{i+1}x_j} - x_ix_{j+1}$ and $\underline{x_{a+1}x_b} - x_ax_{b+1}$. The leading terms are coprime unless $i = a$, $j = a+1$, $i+1 = b$, or $j = b$. Suppose first that $i = a$. Then

$$\begin{aligned} S(\underline{x_{i+1}x_j} - x_ix_{j+1}, \underline{x_{i+1}x_b} - x_ix_{b+1}) &= x_b(\underline{x_{i+1}x_j} - x_ix_{j+1}) - x_j(\underline{x_{i+1}x_b} - x_ix_{b+1}) \\ &= -x_ix_{j+1}x_b + x_ix_jx_{k+1}. \end{aligned}$$

This reduces to 0 if we add $x_i(x_{j+1}x_b - x_jx_{b+1})$. The other cases ($j = a+1$, $i+1 = b$, $j = b$) are similar. □

Corollary 3.2. *The generators $\{x_{i+1}x_j - x_ix_{j+1} \mid 0 \leq i < j \leq k-1\}$ form a Gröbner basis with respect to the grevlex term order for the ideal of the rational normal curve of degree k.*

Definition 3.3. *For each subset $\{p, q, r\} \subset \{0, \dots, k-1\}$, we define*

$$\begin{aligned} S'_{p,q,r} := {} & x_r(x_p x_{q+1} - x_{p+1} x_q) \\ & - x_q(x_p x_{r+1} - x_{p+1} x_r) \\ & + x_p(x_q x_{r+1} - x_{q+1} x_r). \end{aligned} \tag{3.4}$$

$$\begin{aligned} S''_{p,q,r} := {} & x_{r+1}(x_p x_{q+1} - x_{p+1} x_q) \\ & - x_{q+1}(x_p x_{r+1} - x_{p+1} x_r) \\ & + x_{p+1}(x_q x_{r+1} - x_{q+1} x_r). \end{aligned} \tag{3.5}$$

Corollary 3.6. *A Gröbner basis for the module of linear syzygies between the quadrics of the rational normal curve of degree k is given by $S'_{p,q,r}$ and $S''_{p,q,r}$ for each subset $\{p, q, r\} \subset \{0, \dots, k-1\}$.*

Proof. This follows from the calculations in the proof of Theorem 3.1 and Schreyer's Theorem [4, Theorem 15.10]. □

3.3. **Purity of the Betti table.** In the proposition below, we outline one approach to computing the Betti numbers of the rational normal curve. It is based on a theorem of Hochster for computing the graded Betti numbers of squarefree monomial ideals.

Proposition 3.7.

(1) *The generators $\{x_i x_{j+1} - x_{i+1} x_j \mid 0 \leq i < j \leq k-1\}$ form a Gröbner basis with respect to the lex term order for the ideal of the rational normal curve of degree k.*

(2) *The lex initial ideal of the rational normal curve of degree k is $\{x_i x_{j+1} \mid 0 \leq i < j \leq k-1\}$. In particular, it is squarefree.*

(3) *The Stanley-Reisner complex Δ of $\mathrm{in}_{\mathrm{lex}} I$ can be identified with the interval $[0, k]$.*

(4) *The nonzero Betti numbers of $\mathrm{in}_{\mathrm{lex}} I$ are $\beta_{0,0} = 1$ and $\beta_{i,i+1} = i\binom{k}{i}$.*

(5) *The nonzero Betti numbers of I are $\beta_{0,0} = 1$ and $\beta_{i,i+1} = i\binom{k}{i}$.*

Proof. All five statements above are exercises using standard results in combinatorial commutative algebra. We give some hints. For Part (1), run Buchberger's algorithm with the lex term order. Part (2) follows immediately from Part (1).

For part (3), see [15, Ch. 1] for the relevant definitions. For part (4), we use Hochster's Theorem. A reference for Hochster's Theorem is [15, Corollary 5.12], where the notation is also explained. Hochster's Theorem states that the nonzero Betti numbers of S/I_Δ lie only in squarefree multidegrees σ, and

$$\beta_{i,\sigma}(S/I_\Delta) = \dim_{\mathbb{K}} \widetilde{H}^{|\sigma|-i-1}(\Delta|_\sigma; \mathbb{K}).$$

Since Δ is one-dimensional and contractible, the only nonzero cohomology of any $\Delta|_\sigma$ is in degrees -1 or 0. The cohomology in degree -1 gives the first row of the Betti table, and we can easily show that β_{ii} is 1 if $i = 0$ and is 0 if $i \neq 0$. The cohomology in degree 0 gives the second row of the Betti table. Here, $\dim_{\mathbb{K}} \widetilde{H}^{|\sigma|-i-1}(\Delta|_\sigma; \mathbb{K})$ is the number of connected components of $\Delta|_\sigma$ minus 1. We use a formula adapted from [10, p. 55]: Let $\Delta = [0, k]$. The number of subsets $\sigma \subset \{0, \dots, k\}$ such that $|\sigma| = i+1$ and $\Delta|_\sigma$ has $i - m + 1$ connected components is

$$c(m, k+1, i+1) = \binom{i}{m}\binom{k-i+1}{i-m+1}.$$

Thus

$$\begin{aligned}\beta_{i,i+1} &= \sum_{|\sigma|=i+1} \beta_{i,\sigma}(S/I_\Delta)\\ &= \sum_{m=0}^{i} (i-m)\binom{i}{m}\binom{k-i+1}{i-m+1}.\end{aligned}$$

We then use the following combinatorial identity: let k be an arbitrary positive integer, and let i be an integer such that $1 \leq i \leq k$. Then

$$\sum_{m=0}^{i} (i-m)\binom{i}{m}\binom{k-i+1}{i-m+1} = i\binom{k}{i+1}.$$

Finally, for the last part, since the Betti table of the lex initial ideal is pure, the Betti table of the rational normal curve is pure, also. Furthermore, these two ideals have the same Hilbert function. But the Hilbert function of an ideal with a pure Betti table determines the graded Betti numbers, and so the graded Betti numbers of the rational normal curve are equal to the graded Betti numbers of the lex initial ideal. □

Remark 3.8. *A more standard way to compute the Betti numbers of a rational normal curve is to use the fact that it is a determinantal variety and to use the Eagon-Northcott complex.*

3.4. **Finite Hilbert semistability.** Next, we seek to prove finite Hilbert semistability of a rational normal curve. We follow an approach first proposed by Bayer and Morrison that uses the *state polytope* of an ideal.

We first discuss state polytopes of points in a Grassmannian. Let $T \simeq \mathbb{G}_m^r$ be a torus. We identify the characters of T with $\mathbb{Z}^r$. Suppose V is a T-representation with a basis $\{v_1, \dots, v_n\}$ diagonalizing the T-action. Let $\{\chi_i\}_{i=1}^n$ be the characters of T corresponding to $\{v_i\}_{i=1}^n$. For any $0 \leq p \leq \dim(V)$, the Grassmannian (of p-dimensional quotients) $\mathbf{Gr}(p, V)$ admits a T-action, which is linearized by the Plücker coordinates

$$\{v_{i_1} \wedge \cdots \wedge v_{i_p} \mid i_1 < \cdots < i_p\}.$$

The T-state of a Plücker coordinate $v_{i_1} \wedge \cdots \wedge v_{i_p}$ is the associated character $\sum_{j=1}^p \chi_{i_j} \in \mathbb{Z}^r$ of T.

Definition 3.9 (State Polytopes for Grassmannian)**.** *Consider $Q \in \mathbf{Gr}(p, V)$. The T-state associated to a nonzero Plücker coordinate of Q is called a T-state of Q. The state polytope* State(Q) *of Q is defined to be the convex hull in $\mathbb{Z}^r$ of all T-states of Q.*

Remark 3.10. *T-states of $Q = [V \to W \to 0]$ come from nonzero Plücker coordinates of Q diagonalizing the T-action. These in turn correspond to subsets $\{v_{i_1}, \dots, v_{i_p} \mid i_1 < \cdots < i_p\} \subset V$ such that the images of $\{v_{i_1}, \dots, v_{i_p}\}$ span W. By a slight abuse of language, we will call such a subset a T-basis of W.*

We proceed to give a description of the state polytope of an ideal, since this is what we shall actually use. We refer to [3] and [17] for more details on state polytopes of ideals, and the original motivation for its definition.

Definition 3.11. *The m^{th}* inner state *of a monomial ideal J is the sum of the exponent vectors of the degree m monomials in J:*

$$\sum_{\mathbf{x^a}\in J:\ \deg(\mathbf{x^a})=m} \mathbf{a},$$

The m^{th} inner state polytope *of an ideal $I \subset \mathbb{K}[x_0,\ldots,x_k]$ is the convex hull of the m^{th} inner states of the initial ideals of I.*

Similarly, we define the m^{th} outer state *of a monomial ideal J as the sum of the exponent vectors of the degree m monomials outside J, and the m^{th}* outer state polytope *of an ideal as the convex hull of the m^{th} outer states of the initial ideals of I.*

We now explain the relation between Definitions 3.9 and 3.11. To begin, let $S = \mathbb{K}[x_0,\ldots,x_k]$. Consider a subscheme $X \subset \mathbb{P}^k$ defined by homogeneous ideal I and with Hilbert polynomial $P(t)$. For an integer m such that $\mathrm{H}^1(\mathbb{P}^k, I(m)) = 0$, the m^{th} (inner or outer) Hilbert point of X is specified by the short exact sequence

$$0 \to I(m) \to S_m \to \mathrm{H}^0(X, \mathcal{O}_X(m)) \to 0.$$

Then for m large enough, the state polytope of the outer m^{th} Hilbert point of X considered as a point in the Grassmannian $\mathbf{Gr}(P(m), S_m)$ is the m^{th} outer state polytope of I; see [3] and [17].

Since for a fixed m, the union of the monomials inside and outside a monomial ideal must be all the degree m monomials, it follows that the inner and outer states of a monomial ideal are related by an affine linear transformation. Precisely, the sum of the m^{th} inner and outer states is

$$\left(\frac{m\binom{k+m}{k}}{k+1},\ldots,\frac{m\binom{k+m}{k}}{k+1}\right).$$

This allows us to phrase most of the results below in terms of either the inner or the outer state polytope, whichever is more convenient.

Let $P(t)$ denote the Hilbert polynomial of S/I as before. That is, $P(m) = \dim_{\mathbb{K}}((S/I)_m)$. Then the m^{th} outer state polytope as we defined it above lies in an affine hyperplane in $\mathbb{R}^{k+1}$ with equation $z_0 + \cdots + z_k = mP(m)$. In particular, the trivial character, which we denote $\mathbf{0}_m$, is represented by the point on this hyperplane with all coordinates equal. That is,

$$\mathbf{0}_m = \left(\frac{mP(m)}{k+1},\ldots,\frac{mP(m)}{k+1}\right)$$

for outer states. Similarly, when we are working with inner states, a formula for the trivial character is

$$\mathbf{0}_m = \left(\frac{m\binom{k+m}{k} - mP(m)}{k+1},\ldots,\frac{m\binom{k+m}{k} - mP(m)}{k+1}\right).$$

The connection between Hilbert semistability and state polytopes is given by the Hilbert-Mumford Numerical Criterion applied to Hilbert points and can be phrased as follows:

Proposition 3.12 ([3, Theorem 4.1], [17, Criterion 3.4])**.** *Let $X \subset \mathbb{P}^k$ have ideal $I \subset \mathbb{K}[x_0,\ldots,x_k]$, and let T be the maximal torus scaling these variables. The m^{th} inner (respectively, outer) Hilbert point of X is T-semistable if and only if the trivial character lies in the m^{th} inner (respectively, outer) state polytope of I.*

Observe that the proposition only gives Hilbert semistability with respect to T. However, under certain additional hypotheses, T semistability establishes $\mathrm{SL}(k+1)$ semistability.

Proposition 3.13. *Consider $X \subset \mathbb{P}^k$. Let $G \subseteq \mathrm{Stab}_{\mathrm{SL}(k+1)}(X)$ be a linearly reductive group. We say that $X \subset \mathbb{P}^k$ is* multiplicity free *with respect to G if no irreducible G-submodule has multiplicity greater than 1 in the representation of $G \to \mathrm{SL}(k+1)$.*

Suppose that X is multiplicity free. Choose coordinates $x_0, \dots, x_k$ on $\mathbb{P}^k$ that are adapted to the decomposition of $\mathbb{K}^{k+1}$ into irreducible G-submodules. Let T be the maximal torus scaling these variables.

Let $[X]_m$ be the m^{th} Hilbert point of $X \subset \mathbb{P}^k$. Then $[X]_m$ is T-semistable if and only if $[X]_m$ is $\mathrm{SL}(k+1)$-semistable.

Proof. This is proved in [17, Proposition 4.7] using Kempf's instability results [13]. (Morrison and Swinarski state the result for finite groups G, but their proof applies verbatim in the case of an arbitrary linearly reductive G.) When $G = \mathbb{G}_m$, as often is the case, the claim also follows directly from Luna's criteria for orbit closedness [Cor. 2 and Rem. 1][14]. □

Our strategy is now clear. To prove Hilbert stability of the rational normal curve for some finite degree m, we want to show that the trivial character is in the m^{th} state polytope of the rational normal curve. For this, it is enough to exhibit two initial ideals (vertices of the inner state polytope) such that the trivial character lies between them. Not surprisingly, our two choices are the lex and grevlex initial ideals. We leave the calculations to the reader.

Proposition 3.14.

(1) *The m^{th} outer state of the lex initial ideal is*

$$\left(\frac{1}{2}m^2 + \frac{1}{2}m,\ m^2,\ \dots,\ m^2,\ \frac{1}{2}m^2 + \frac{1}{2}m\right).$$

(2) *The m^{th} outer state of the grevlex initial ideal is*

$$\left(\frac{k}{2}m^2 - \frac{k-2}{2}m,\ m,\ \dots,\ m,\ \frac{k}{2}m^2 - \frac{k-2}{2}m\right).$$

(3) *For any $m \geq 2$, the m^{th} Hilbert point of the rational normal curve of degree k is $\mathrm{SL}(k+1)$-semistable.*

Remark 3.15. *A more conceptual proof of Proposition 3.14 part (3) follows from the fact that a rational normal curve is a homogeneous variety embedded by a complete linear system* [13, Corollary 5.1].

4. Equations and syzygies of balanced ribbons

We now apply to ribbons the techniques illustrated in the previous section for rational normal curves. In this section, we describe equations and syzygies of canonically embedded balanced ribbons, which we now define.

Definition 4.1. *Let $g = 2k+1$ be an odd integer with $k \geq 1$. The* balanced ribbon *of genus g is the nonreduced curve C obtained as follows: Let $U := \operatorname{Spec} \mathbb{K}[u,e]/(e^2)$,*

$V := \operatorname{Spec} \mathbb{K}[v,f]/(f^2)$, *and glue* $U \smallsetminus \{0\}$ *and* $V \smallsetminus \{0\}$ *via the isomorphism*

$$\begin{aligned} u &\mapsto v^{-1} - v^{-k-2} f, \\ e &\mapsto v^{-g-1} f. \end{aligned}$$

In [1, Lemma 3.1], Alper, Fedorchuk, and Smyth describe a basis of differentials on the balanced ribbon. Their result in our notation is as follows:

Proposition 4.2. *A basis of* $\mathrm{H}^0(C, \omega_C)$ *is given by differentials of the form* $f(t,e)\frac{dt \wedge de}{e^2}$, *where* $f(t,e)$ *ranges over the following functions:*

$$\begin{array}{rl} t^i & i = 0, 1, \ldots, k, \\ t^{2k-j} + (k-j)t^{k-j-1}e, & j = k-1, k-2, \ldots, 0. \end{array}$$

This leads to a parametrization of the canonically embedded balanced ribbon of genus g. Namely, the ribbon C is the closure of the map $\operatorname{Spec} \mathbb{K}[t,e]/(e^2) \to \mathbb{P}^{g-1}$ given by

$$t \mapsto [1 : t : t^2 : \cdots : t^k : t^{k+1} + e : t^{k+2} + 2te : \cdots : t^{2k} + kt^{k-1}e].$$

Definition 4.3. *Let* $S = \mathbb{K}[t, e, x_0, \ldots, x_{2k}]$. *The* elimination ideal I_E *of the canonically embedded balanced ribbon is the ideal generated by the following equations:*

$$\begin{array}{rl} t^i x_0 - x_i & i = 0, 1, \ldots, k, \\ (t^{2k-j} + (k-j)t^{k-j-1}e)x_0 - x_{2k-j}, & j = k-1, k-2, \ldots, 0, \\ e^2. & \end{array}$$

Equations for the canonically embedded balanced ribbon can be obtained from the parametric description above by eliminating the variables t and e from I_E.

Theorem 4.4. *The following* $\binom{g-2}{2} + g$ *quadrics and* g *cubics form a Gröbner basis with respect to the Bayer-Stillman elimination term order for the elimination ideal* I_E *of the balanced ribbon of genus* g*:*

(1) *The* 2×2 *minors of the catalecticant matrix*

$$\begin{bmatrix} x_0 & x_1 & x_2 & \cdots & x_{k-1} \\ x_1 & x_2 & x_3 & \cdots & x_k \end{bmatrix}$$

(2) *The* 2×2 *minors of the catalecticant matrix*

$$\begin{bmatrix} x_{2k} & x_{2k-1} & x_{2k-2} & \cdots & x_{k+1} \\ x_{2k-1} & x_{2k-2} & x_{2k-3} & \cdots & x_k \end{bmatrix}$$

(3) *For each pair* i, j *with* $0 \le i \le k-2$ *and* $0 \le j \le k-2$ *the following trinomial quadric:*

$$x_{i+2}x_{2k-j-2} - 2x_{i+1}x_{2k-j-1} + x_i x_{2k-j}.$$

(4) $\{tx_i - x_{i+1} \mid i = 0, \ldots, k-1\}$

(5) $\{ex_i + tx_{k+i} - x_{k+i+1} \mid i = 0, \ldots, k-1\}$

(6) $\{e(tx_{k+i} - x_{k+i+1}) \mid i = 0, \ldots, k-1\}$

(7) $\{t^2 x_{k+i} - 2tx_{k+i+1} + x_{k+i+2} \mid i = 0, \ldots, k-2\}$

(8) *One additional quadric:* e^2

(9) *The cubic* $ex_k x_{2k-1} + tx_{2k-1}x_{2k} - x_{2k}^2$

(10) *The cubic* $t^2 x_{2k-1} + ex_k - tx_{2k}$

Proof of Theorem 4.4. First, we show that polynomials listed in the statement of Theorem 4.4 are in the ideal I_E. This is straightforward, so we give just one example. We verify that a quadric from the third group is in I_E:

$$\begin{aligned}
&(t^{i+2}x_0 - x_{i+2})((t^{2k-j-2} + (k-j-2)t^{k-j-3}e)x_0 - x_{2k-j-2}) \\
&-2(t^{i+1}x_0 - x_{i+1})((t^{2k-j-1} + (k-j-1)t^{k-j-2}e)x_0 - x_{2k-j-1}) \\
&+(t^i x_0 - x_i)((t^{2k-j} + (k-j)t^{k-j-1}e)x_0 - x_{2k-j}) \\
&= x_{i+2}x_{2k-j-2} - 2x_{i+1}x_{2k-j-1} + x_i x_{2k-j}.
\end{aligned} \tag{4.5}$$

Next, we show that the polynomials listed generate I_E. For this, observe that

$$t^i x_0 - x_i = \sum_{j=0}^{i-1} t^{i-j-1}(tx_j - x_{j+1}) \tag{4.6}$$

and

$$\begin{aligned}
&t^{2k-j}x_0 + (k-j)t^{k-j-1}ex_0 - x_{2k-j} = \\
&\qquad (k-j)t^{k-j-1}(ex_0 + tx_k - x_{k+1}) + \sum_{p=0}^{k-1} t^{2k-j-p-1}(tx_p - x_{p+1}) \\
&\qquad - \sum_{p=0}^{k-j-2} (k-j-1-p)t^{k-j-p-2}(t^2 x_{k+p} - 2tx_{k+p+1} + x_{k+p+2}).
\end{aligned} \tag{4.7}$$

It remains to show that the polynomials listed in the statement of Theorem 4.4 form a Gröbner basis of I_E. For this, we use Buchberger's Algorithm.

There are 10 different types of generators, and hence 55 types of S-pairs. However, the generator types 8, 9, and 10 contain only one polynomial each, so we do not need to consider S-pairs of types $(8,8)$, $(9,9)$, or $(10,10)$. This leaves 52 types of S-pairs that we must reduce to zero. Of these pairs, 18 are coprime. We outline the calculations needed for the first three of the remaining 34 cases below.

Type (1,1). Consider two polynomials from the first group. Let $f = \underline{x_{a+1}x_b} - x_a x_{b+1}$, $g = \underline{x_{c+1}x_d} - x_c x_{d+1}$ with $a < b$ and $c < d$. We have done this calculation before in the context of the rational normal curve.

Type (1,2). Consider a polynomial from the first group and a quadric from the second group. The leading terms will be coprime. The only variable that can occur in both quadrics is x_k, and it never occurs in the leading term of the quadric from the first group.

Type (1,3). Consider a polynomial from the first group and a quadric from the third group. Let $f = \underline{x_{a+1}x_b} - x_a x_{b+1}$, $g = \underline{x_{i+2}x_{2k-j-2}} - 2x_{i+1}x_{2k-j-1} + x_i x_{2k-j}$. The leading terms of f and g are coprime unless $i+2 = a+1$ or $i+2 = b$.

Suppose $i+2=a+1$. The S-pair reduction is

$$\begin{aligned}
&x_{2k-j-2}(\underline{x_{i+2}x_b}-x_{i+1}x_{b+1})-x_b(\underline{x_{i+2}x_{2k-j-2}}-2x_{i+1}x_{2k-j-1}+x_ix_{2k-j})\\
&=-\underline{x_{b+1}x_{i+1}x_{2k-j-2}}+2x_bx_{i+1}x_{2k-j-1}-x_bx_ix_{2k-j}\\
&\quad+x_{b+1}(\underline{x_{i+1}x_{2k-j-2}}-2x_ix_{2k-j-1}+x_{i-1}x_{2k-j})\\
&=2\underline{x_bx_{i+1}x_{2k-j-1}}-x_bx_ix_{2k-j}-2x_{b+1}x_ix_{2k-j-1}+x_{b+1}x_{i-1}x_{2k-j}\\
&\quad-2x_{2k-j-1}(\underline{x_bx_{i+1}}-x_{b+1}x_i)\\
&=-\underline{x_bx_ix_{2k-j}}+x_{b+1}x_{i-1}x_{2k-j}\\
&\quad+x_{2k-j}(\underline{x_bx_i}-x_{i-1}x_{b+1})\\
&=0.
\end{aligned}$$

The proof when $i+2=b$ is similar.

All 52 cases are typed up in an appendix to this paper available at the third author's website. □

Corollary 4.8. *The quadrics of the first three types shown above form a Gröbner basis with respect to the grevlex term order for the ideal of the balanced ribbon.*

Definition 4.9. *For each triple (i,j,ℓ) with $0\le i\le k-3$, $0\le j\le k-2$, and $0\le \ell\le k-1$, we define*

$$\begin{aligned}
S_{i,j,l} := {}&x_{\ell+1}(x_{i+2}x_{2k-j-2}-2x_{i+1}x_{2k-j-1}+x_ix_{2k-j})\\
&-x_\ell(x_{i+3}x_{2k-j-2}-2x_{i+2}x_{2k-j-1}+x_{i+1}x_{2k-j})\\
&+x_{2k-j-2}(x_{i+3}x_\ell-x_{i+2}x_{\ell+1})\\
&-2x_{2k-j-1}(x_{i+2}x_\ell-x_{i+1}x_{\ell+1})\\
&+x_{2k-j}(x_{i+1}x_\ell-x_ix_{\ell+1}).
\end{aligned}\tag{4.10}$$

Corollary 4.11. *A basis for the module of linear syzygies between quadrics of the canonically embedded balanced ribbon of genus g is given by the syzygies $S'_{p,q,r}$, $S''_{p,q,r}$, and $S_{i,j,l}$ defined above and their images under the involution $x_i\leftrightarrow x_{2k-i}$.*

Proof. This follows from the calculations in the proof of Theorem 4.4. (Not all of the calculations are shown here, but they are all shown in the appendix.) □

5. Applications

5.1. **Betti numbers of ribbons.** We may combine the Gröbner basis calculation of the previous section with Fong's theorem to obtain amusing new proofs of weak versions of two classical theorems on canonical curves. The history of algebraic geometry in the twentieth century most certainly did not proceed via calculations on a single nonreduced curve in each odd genus!

Proposition 5.1 (Weak version of Petri's Theorem)**.** *The ideal of a general smooth canonical curve of odd genus is generated by quadrics.*

Proof. Since the ideal of the balanced ribbon is generated by quadrics, it has $\beta_{1,1+j}=0$ for all $j\ge 2$. Since graded Betti numbers are upper semicontinuous in flat families, and ribbons smooth to canonical curves by Fong's theorem, this implies the desired result. □

We reprove a weak version of a theorem due to Vishik and Finkelberg [20]; Polishchuk [19]; and Pareschi and Purnaprajna [18].

Proposition 5.2. *The ideal of a very general smooth canonical curve of odd genus is Koszul.*

Proof. Let $S = \mathbb{K}[x_0, \dots, x_k]$. If I has a quadratic Gröbner basis for some term order, then S/I is Koszul (see for instance [5, Theorem 6.7]). Since the balanced ribbon has a quadratic Gröbner basis, it is Koszul. Koszulity is not an open condition, but it is defined by the vanishing of *countably* many Ext groups. Since ribbons smooth to canonical curves by Fong's theorem, this implies the desired result. □

To execute Bayer and Eisenbud's original plan of using ribbons to give a new proof of Generic Green's Conjecture (Voisin's Theorem), one would need to show that the Betti table of the balanced ribbon is pure. Unfortunately, the next proposition shows that the analogue for ribbons of the proof of Proposition 3.7 fails.

Proposition 5.3. *The genus* 7 *balanced ribbon has* $50,913$ *monomial initial ideals with* $31,881$ *unique saturations. None of these monomial initial ideals has a pure Betti table; in particular, each of these monomial initial ideals has* $\beta_{3,4} > 0$.

In summary, to get a new proof of Generic Green's Conjecture (Voisin's Theorem) via ribbons, the Betti numbers of the balanced ribbon would need to be computed some other way.

5.2. **Finite Hilbert stability of ribbons.** In [1], Alper, Fedorchuk, and Smyth show that the m^{th} Hilbert point of a general bicanonical or canonical curve is semistable for any $m \geq 2$. They split the proof into four separate cases, treating odd genus and even genus separately, and canonical and bicanonical curves separately. We give a Gröbner interpretation of their proof for one of these cases: the case of odd genus canonical curves.

Balanced ribbons are used to establish semistability of odd genus canonical curves in [1, Section 4.1]. There the cases $m = 2$ and $m \geq 3$ are analyzed separately; for convenience, we will focus on the case $m = 2$ below. Alper, Fedorchuk, and Smyth's approach is to produce two points in the state polytope such that the trivial character lies between them. Specifically, in [1, (4.1) and (4.2)], they construct two monomial bases $\mathcal{B}^+$ and $\mathcal{B}^-$ of $\mathrm{H}^0(C, \omega_C^2)$ such that the outer state of $\mathcal{B}^+$ overrepresents the coordinates x_0, x_k, x_{2k} relative to the other coordinates, and the outer state of $\mathcal{B}^-$ underrepresents the coordinates x_0, x_k, x_{2k} relative to the other coordinates. Namely, these monomial bases are

$$\mathcal{B}^+ = \left\{ \{x_0 x_i\}_{i=0}^{2k},\ \{x_k x_i\}_{i=1}^{2k},\ \{x_{2k} x_i\}_{i=1}^{k-1},\ \{x_{2k} x_i\}_{i=k+1}^{2k} \right\} \tag{5.4}$$

and

$$\mathcal{B}^- = \left\{ \begin{array}{ll} \{x_i^2\}_{i=0}^{2k}, & \{x_i x_{i+1}\}_{i=0}^{2k-1}, \\ \\ \{x_i x_{k+i}\}_{i=1}^{k-1}, & \{x_i x_{k+i+1}\}_{i=0}^{k-1} \end{array} \right\}. \tag{5.5}$$

In [1, Lemma 3.6], Alper, Fedorchuk, and Smyth describe arbitrary monomial bases of $\mathrm{H}^0(C, \omega_C^m)$, thus obtaining a complete description of the m^{th} outer state polytope of I_C.

It is natural to wonder if the outer states of $\mathcal{B}^+$ and $\mathcal{B}^-$ are the outer states of initial ideals of I_C. To this end, we have the following result for $\mathcal{B}^+$:

Proposition 5.6. *For* $m = 2$, $\mathcal{B}^+$ *is the complement of the set of degree two generators in the initial ideal of* I_C *arising from the term order given by grevlex with the variables ordered* $x_0, x_k, x_{2k}, x_1, \dots, \widehat{x_k}, \dots, x_{2k-1}$.

Proof. Follows immediately from definitions and (5.4). □

The set $\mathcal{B}^-$ also has a Gröbner interpretation, but it is more subtle. First, we give the following easy lemma:

Lemma 5.7. *Let T be a torus and V be a T-representation. Suppose*

$$Q = [V \to W \to 0] \in \mathrm{Grass}(p, V)$$

is a point which is invariant under a linear subgroup $G \subset T$. Let

$$W = \bigoplus_{\chi \in S} W_\chi$$

be the weight space decomposition, where S is a finite set of distinct characters of G. Set

$$Q_\chi := [V \to W_\chi \to 0] \in \mathrm{Grass}(\dim(W_\chi), V).$$

Then

$$\mathrm{State}(W) = \sum_{\chi \in S} \mathrm{State}(W_\chi), \tag{5.8}$$

where the operation on the right is Minkowski sum of polytopes.

Proof. Let $v_1, \ldots, v_n$ be a basis of V diagonalizing the T-action. A state of Q corresponds to a T-basis $\{v_{i_1}, \ldots, v_{i_p}\}$ of W; see Remark 3.10. Evidently, every T-basis of W is obtained as the concatenation of T-bases of the summands W_χ. Hence a T-state of W is a sum of T-states of W_χ, and, conversely, a sum of T-states of W_χ is a state of W. It follows that State(W) is the Minkowski sum of State(W_χ), as desired. □

Proposition 5.9.

(1) *For genus 7, there exists no term order for which $\mathcal{B}^-$ is the complement of the set of degree two generators of the initial ideal of I_C.*[1]

(2) *The ideal I_C is bigraded, where the first grading is by degree and the second grading is by the weights of the $\mathbb{G}_m$-action. Let $I_C = \bigoplus I_p$ be its decomposition into $\mathbb{G}_m$-weight spaces. There exists a term order $\leq_p$ on each I_p such that $\mathcal{B}^-$ is the complement of the union of the degree two generators of the initial ideals $\mathrm{in}_{\leq_p} I_p$. Specifically:*

   (a) *If $p \leq k+2$ or $p \geq 3k-2$, let $\leq_p$ be the lexicographic term order with the variables $x_0, \ldots, x_{2k}$ in the usual order.*

   (b) *If $k+3 \leq p \leq 3k-3$, set $q = \lfloor \frac{p-k}{2} \rfloor$ and let $\leq_p$ be the lexicographic term order with the variables ordered $x_0, \ldots, \widehat{x_q}, \ldots, x_k, x_q, x_{k+1}, \ldots, x_{2k}$.*

Proof. For the first part, we can use `gfan` [12] to compute all 50,913 initial ideals for this example, and none of them gives $\mathcal{B}^-$.

For the second part, we can compute the initial ideals for each I_p with the given term orders. Observe that for $p \leq k+1$, $I_p(2)$ only contains binomials, and for $p = k+2$, $I_p(2)$ contains exactly one trinomial, and the initial ideals with respect to the lex term order are easily computed in these cases. For $k+3 \leq p \leq 2k$, the variable x_q cannot appear in any binomial in $I_p(2)$, so these leading monomials are also easily computed. The trinomials in $I_p(2)$ are indexed by $i = 0, \ldots, p-k-2$ and it is easy to compute the leading monomials under the term orders described. □

[1] Presumably the same result is true for all $g \geq 7$.

References

[1] Jarod Alper, Maksym Fedorchuk, and David Ishii Smyth, *Finite Hilbert stability of (bi)canonical curves*, Invent. Math. **191** (2013), no. 3, 671–718, DOI 10.1007/s00222-012-0403-6. MR3020172 ↑56, 58, 64, 67

[2] Dave Bayer and David Eisenbud, *Ribbons and their canonical embeddings*, Trans. Amer. Math. Soc. **347** (1995), no. 3, 719–756, DOI 10.2307/2154871. MR1273472 (95g:14032) ↑55, 56

[3] David Bayer and Ian Morrison, *Standard bases and geometric invariant theory. I. Initial ideals and state polytopes*, J. Symbolic Comput. **6** (1988), no. 2-3, 209–217, DOI 10.1016/S0747-7171(88)80043-9. Computational aspects of commutative algebra. MR988413 (90e:13001) ↑61, 62

[4] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. MR1322960 (97a:13001) ↑60

[5] Viviana Ene and Jürgen Herzog, *Gröbner bases in commutative algebra*, Graduate Studies in Mathematics, vol. 130, American Mathematical Society, Providence, RI, 2012. MR2850142 ↑67

[6] Maksym Fedorchuk and David Jensen, *Stability of 2nd Hilbert points of canonical curves*, Int. Math. Res. Not. IMRN **2013** (2013), no. 22, 5270–5287. MR3129099 ↑56

[7] Lung-Ying Fong, *Rational ribbons and deformation of hyperelliptic curves*, J. Algebraic Geom. **2** (1993), no. 2, 295–307. MR1203687 (94c:14020) ↑55

[8] David Gieseker, *Geometric invariant theory and applications to moduli problems*, Invariant theory. Proceedings of the 1st 1982 Session of the Centro Internazionale Matematico Estivo (CIME), Montecatini, June 10–18, 1982, 1983, pp. v+159. ↑57

[9] ______, *Lectures on moduli of curves*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics, vol. 69, Published for the Tata Institute of Fundamental Research, Bombay, 1982. ↑57

[10] Ian P. Goulden and David M. Jackson, *Combinatorial enumeration*, Dover Publications, Inc., Mineola, NY, 2004. With a foreword by Gian-Carlo Rota; Reprint of the 1983 original. MR2079788 (2005b:05001) ↑60

[11] Mark L. Green, *Koszul cohomology and the geometry of projective varieties*, J. Differential Geom. **19** (1984), no. 1, 125–171. ↑57

[12] Anders Jensen, `gfan`*: a software package for computing Gröbner fans and tropical varieties* (2011). Version 0.5. ↑68

[13] George R. Kempf, *Instability in invariant theory*, Ann. of Math. (2) **108** (1978), no. 2, 299–316. ↑63

[14] Domingo Luna, *Adhérences d'orbite et invariants*, Invent. Math. **29** (1975), no. 3, 231–238. ↑63

[15] Ezra Miller and Bernd Sturmfels, *Combinatorial commutative algebra*, Graduate Texts in Mathematics, vol. 227, Springer-Verlag, New York, 2005. MR2110098 (2006d:13001) ↑60

[16] Ian Morrison, *GIT constructions of moduli spaces of stable curves and maps*, Surveys in differential geometry. Vol. XIV. Geometry of Riemann surfaces and their moduli spaces, 2009, pp. 315–369. ↑56, 58

[17] Ian Morrison and David Swinarski, *Gröbner techniques for low-degree Hilbert stability*, Exp. Math. **20** (2011), no. 1, 34–56, DOI 10.1080/10586458.2011.544577. MR2802723 (2012g:14083) ↑61, 62, 63

[18] Giuseppe Pareschi and B. P. Purnaprajna, *Canonical ring of a curve is Koszul: a simple proof*, Illinois J. Math. **41** (1997), no. 2, 266–271. MR1441677 (98c:14027) ↑66

[19] Alexander Polishchuk, *On the Koszul property of the homogeneous coordinate ring of a curve*, J. Algebra **178** (1995), no. 1, 122–135, DOI 10.1006/jabr.1995.1342. MR1358259 (96j:14019) ↑66

[20] Alexander Vishik and Michael Finkelberg, *The coordinate ring of general curve of genus $g \geq 5$ is Koszul*, J. Algebra **162** (1993), no. 2, 535–539, DOI 10.1006/jabr.1993.1269. MR1254790 (94m:14036) ↑66

[21] Claire Voisin, *Green's generic syzygy conjecture for curves of even genus lying on a $K3$ surface*, J. Eur. Math. Soc. (JEMS) **4** (2002), no. 4, 363–404, DOI 10.1007/s100970200042. ↑57

[22] ______, *Green's canonical syzygy conjecture for generic curves of odd genus*, Compos. Math. **141** (2005), no. 5, 1163–1190, DOI 10.1112/S0010437X05001387. MR2157134 (2006c:14053) ↑57

Albanian Journal of Mathematics (ISSN: 1930-1235) was founded by T. Shaska in 2007 with the idea to support Albanian mathematicians in Albania and abroad.

The journal is not associated with any government institutions in Albania or any public or private universities in Albania or abroad. The journal does not charge any fees to the authors and has always been an open access journal. The journal supports itself with private donations and voluntary work from its staff. Its main office is in Vlora, Albania.

www.albanian-j-math.com