A MAPLE PACKAGE FOR HYPERELLIPTIC CURVES

T. SHASKA AND S. ZHENG

Abstract. We implement a Maple package that addresses questions of the arithmetic of hyperelliptic curves. This implementation is based on [4], [9], [10], [12], [13], [15], [14], [11]. Our package has as main functions the following: determining the automorphism group of a genus g hyperelliptic curve $\mathcal{X}_g$ defined over $\mathbb{C}$, computing the isomorphism class $[\mathcal{X}_g]$ for $|\text{Aut }(\mathcal{X}_g)| > 2$, determining the field of moduli and the field of definition, and giving an explicit equation of the curve over $\mathbb{Q}$ when such equation exists. We can accomplish such tasks for many classes of hyperelliptic curves. For genus $g = 2$ we can answer these questions completely. Given a genus 2 curve C defined over $\mathbb{C}$, this package accomplishes the following: computes the moduli point $\mathfrak{p}(C) \in \mathcal{M}_2$, determines the automorphism group of C, determines if a rational model of C over the $\mathbb{Q}$ exists, computes such rational model when it exists, for $n = 2, 3, 5$, determines if the Jacobian of C is (n, n)-split, determines if C has small degree elliptic subcovers and computes such subcovers. To accomplish such tasks we have implemented many other functions such as Igusa invariants of binary sextics, absolute invariants, etc. We can do most of the above for genus 3 curves with automorphism group of order > 4. Conditions in terms of classical invariants of binary forms are implemented which check if a curve has reduced automorphism groups A_4, S_4, A_5.

1. Introduction

Hyperelliptic curves have seen a wide range of applications in the last few decades such as coding theory, cryptography, computer vision, etc. However, there are amazingly few packages in all of computer algebra systems that deal with the arithmetic of hyperelliptic curves. With this modest effort we are trying to fill this void and write a Maple package that will address some computational aspects of hyperelliptic curves. In this short note we give an overview of the functions defined in this package. The complete definitions and the mathematics behind the algorithms used in our package can mostly be found in [8], [9], [10], [12], [13], [3], [6].

In section 2, we give some basic definitions on hyperelliptic curves of any genus. In section 3, we briefly describe the genus 2 case. The classical invariants of binary sextics and a set of absolute invariants are defined. In terms of such invariants we can determine the automorphism group of genus 2 curves, if whether or not the curve has (n, n) split Jacobian for small n, the field of definition, and a rational model over the field of moduli. In section 4, we study the hyperelliptic curves of higher genus. In the first part we study the case when $g = 3$. We are able to determine the automorphism group of curves for $g = 3$ and provide a rational model over a field of moduli in all cases when the curve C has extra automorphisms

Key words and phrases. genus 2 curves, hyperelliptic curves, binary forms, automorphism groups.

and Aut (C) is not isomorphic to V_4. In the second part of section 4, we present some results which are valid for any genus.

Notation: Throughout this note all curves are defined over the field of complex numbers $\mathbb{C}$. A hyperelliptic curve C is given by the affine equation $y^2 = f(x)$.

2. Preliminaries

Let C denote a genus $g \geq 2$ hyperelliptic curve defined over $\mathbb{C}$. The automorphism group of C is denoted by Aut (C) and its reduced automorphism group by $\overline{Aut}\ (C)$. The $\overline{Aut}\ (C)$ is isomorphic to $\mathbb{Z}_n, D_n, A_4, S_4, A_5$. For the list of groups that occur as automorphism groups of hyperelliptic curves see [1], [2], [13].

A genus g hyperelliptic curve C which has a non-hyperelliptic involution in the automorphism group can be written as

$$y^2 = x^{2g+2} + a_g x^{2g} + \cdots + a_1 x^2 + 1 \tag{1}$$

and $\Delta(a_1, \ldots, a_g) \neq 0$ (i.e., Δ is the discriminant of the polynomial of the right hand side). We call the above equation the **normal form** of the curve C. The isomorphism classes of such curves are determined by dihedral invariants (cf. section 4).

A field $F \subset \mathbb{C}$ is called a **field of definition** of C if there exists C' defined over F such that C' is isomorphic to C over $\mathbb{C}$. The field of definition is the extension field $\mathbb{Q}(\mathfrak{p})$ of $\mathbb{Q}$.

The **field of moduli** of C is a subfield $F \subset \mathbb{C}$ such that for every automorphism $\sigma \in$ Aut $(\mathbb{C})$ the following holds: C is isomorphic to C^σ if and only if $\sigma_F = id$.

We will use $\mathfrak{p} = [C] \in \mathcal{M}_2$ to denote the corresponding **moduli point** and $\mathcal{M}_2(\mathfrak{p})$ the residue field of $\mathfrak{p}$ in $\mathcal{M}_2$. The field of moduli of C coincides with the residue field $\mathcal{M}_2(\mathfrak{p})$ of the point $\mathfrak{p}$ in $\mathcal{M}_2$.

If there is a curve C' isomorphic to C and defined over $M(\mathfrak{p})$, we say that C has a **rational model over its field of moduli**. The field of moduli of curves is not necessarily a field of definition. For details see [4], [12].

3. Curves of genus 2

Genus 2 curves are the most used of all hyperelliptic curves due to their application in cryptography and also best understood. The moduli space $\mathcal{M}_2$ of genus 2 curves is a 3-dimensional variety. To understand how to describe the moduli points of this space we need to define the invariants of binary sextics. For details on such invariants and on the genus 2 curves in general the reader can check [5], [10], [7].

3.1. Invariants of curves and moduli points.

Let C be a genus 2 curve with equation

$$y^2 = a_6 x^6 + a_5 x^5 \ldots a_1 x + a_0$$

The **classical invariants** (sometimes called **Igusa invariants**) are defined as follows

$$
\begin{aligned}
J_2 :=& -240a_0a_6 + 40a_1a_5 - 16a_2a_4 + 6a_3^2\\
J_4 :=& 48a_0a_4^3 + 48a_2^3a_6 + 4a_2^2a_4^2 + 1620a_0^2a_6^2 + 36a_1a_3^2a_5 - 12a_1a_3a_4^2 - 12a_2^2a_3a_5 + 300a_1^2a_4a_6\\
&+ 300a_0a_5^2a_2 + 324a_0a_6a_3^2 - 504a_0a_4a_2a_6 - 180a_0a_4a_3a_5 - 180a_1a_3a_2a_6 + 4a_1a_4a_2a_5\\
&- 540a_0a_5a_1a_6 - 80a_1^2a_5^2\\
J_6 :=& 176a_1^2a_5^2a_3^2 + 64a_1^2a_5^2a_4a_2 + 1600a_1^3a_5a_4a_6 + 1600a_1a_5^3a_0a_2\\
&- 160a_0a_4^4a_2 - 96a_0^2a_4^3a_6 + 60a_0a_4^3a_3^2 + 72a_1a_3^4a_5 - 24a_1a_3^3a_4^2\\
&- 160a_2^4a_4a_6 - 96a_2^3a_0a_6^2 + 60a_2^3a_3^2a_6 - 24a_2^2a_3^3a_5 + 8a_2^2a_3^2a_4^2\\
&- 900a_2^2a_1^2a_6^2 - 24a_2^3a_4^3 - 36a_2^4a_5^2 - 36a_1^2a_4^4 + 424a_0a_4^2a_2^2a_6\\
&+ 492a_0a_4^2a_2a_3a_5 + 20664a_0^2a_4a_6^2a_2 + 3060a_0^2a_4a_6a_3a_5 - 468a_0a_4a_3^2a_2a_6\\
&- 198a_0a_4a_3^3a_5 - 640a_0a_4a_2^2a_5^2 + 3472a_0a_4a_2a_5a_1a_6 - 18600a_0a_4a_1^2a_6^2\\
&- 876a_0a_4^2a_1a_6a_3 + 492a_1a_3a_2^2a_4a_6 - 238a_1a_3^2a_2a_4a_5 + 76a_1a_3a_2a_4^3\\
&+ 3060a_1a_3a_0a_6^2a_2 + 1818a_1a_3^2a_0a_6a_5 - 198a_1a_3^3a_2a_6 + 26a_1a_3a_2^2a_5^2\\
&- 1860a_1^2a_3a_2a_5a_6 + 330a_1^2a_3^2a_6a_4 + 76a_2^3a_4a_3a_5 - 876a_2^2a_0a_6a_3a_5\\
&+ 616a_2^3a_5a_1a_6 + 2250a_0^2a_5^3a_3 - 900a_0^2a_5^2a_4^2 - 10044a_0^2a_6^2a_3^2\\
&+ 28a_1a_4^2a_2^2a_5 - 640a_1^2a_4^2a_2a_6 + 26a_1^2a_4^2a_3a_5 - 1860a_1a_4a_0a_5^2a_3\\
&+ 616a_1a_4^3a_0a_5 - 18600a_0^2a_5^2a_6a_2 + 59940a_0^2a_5a_6^2a_1 + 330a_0a_5^2a_3^2a_2\\
&- 119880a_0^3a_6^3 - 320a_1^3a_5^3 - 2240a_1^2a_5^2a_0a_6 + 2250a_1^3a_3a_6^2 + 162a_0a_6a_3^4\\
J_{10} :=& a_6^{-1}Res_X(f, \frac{\partial f}{\partial X})
\end{aligned}
\tag{2}
$$

Here J_{10} is the discriminant of $f(x)$. The **absolute invariants** are defined as follows

$$
i_1 := 144\frac{J_4}{J_2^2}, \quad i_2 := -1728\frac{J_2J_4 - 3J_6}{J_2^3}, \quad i_3 := 486\frac{J_{10}}{J_2^5}, \tag{3}
$$

for $J_2 \neq 0$. In the case $J_2 = 0$ we define

$$
\mathfrak{a}_1 := \frac{J_4 \cdot J_6}{J_{10}}, \quad \mathfrak{a}_2 := \frac{J_6 \cdot J_{10}}{J_4^4} \tag{4}
$$

to determine genus two fields with $J_2 = 0$, $J_4 \neq 0$, and $J_6 \neq 0$ up to isomorphism.

For a given genus 2 curve C the corresponding **moduli point** $\mathfrak{p} = [C]$ is defined as

$$
\mathfrak{p} = \begin{cases}
(i_1, i_2, i_3) \;\; if \; J_2 \neq 0\\
(\mathfrak{a}_1, \mathfrak{a}_2) \;\; if \; J_2 = 0, J_4 \neq 0, J_6 \neq 0\\
\dfrac{J_6^5}{J_{10}^3} \;\; if \; J_2 = 0, J_4 = 0, J_6 \neq 0\\
\dfrac{J_4^5}{J_{10}^2} \;\; if \; J_2 = 0, J_6 = 0, J_4 \neq 0
\end{cases}
$$

Notice that the definition of $\mathfrak{a}_1, \mathfrak{a}_2$ can be totally avoided if one uses absolute invariants with J_{10} in the denominator. However, the degree of such invariants is higher and therefore they are not effective computationally.

3.2. **Automorphism groups.** A list of groups that can occur as automorphism groups of hyperelliptic curves is given in [13] among many other references. The function in the package that computes the automorphism group is given by *AutGroup*().

The output is the automorphism group. Since there is always confusion on the terminology when describing certain groups we also display the GAP identity of the group from the `SmallGroupLibrary`.

For a fixed group G one can compute the locus of genus g hyperelliptic curves with automorphism group G. For genus 2 this loci is well described as subvarieties of $\mathcal{M}_2$.

Example 1. *Let $y^2 = f(x)$ be a genus 2 curve where $f := x^5 + 2x^3 - x$. Then the function* `AutGroup`*(f,x) displays:*

> `AutGroup`*(f,x);*

$$[D_4, (8, 3)]$$

Example 2. *Let $y^2 = f(x)$ be a genus 2 curve where $f := x^6 + 2x^3 - x$. Then the function* `AutGroup`*(f,x) displays:*

> `AutGroup`*(f,x);*

$$[V_4, (4, 2)]$$

We also have implemented the functions: `LocusCurvesAut_V_4()`,
`LocusCurvesAut_D_4()`, `LocusCurvesAut_D4_J2()`, `LocusCurvesAut_D_6()`,
which gives equations for the locus of curves with automorphism group D_4 or D_6.

3.3. **Genus 2 curves with split Jacobians.** A genus 2 curve which has a degree n maximal map to an elliptic curve is said to have (n, n)-*split Jacobian*; see [15] for details. Genus 2 curves with split Jacobian are interesting in number theory, cryptography, and coding theory. We implement an algorithm which checks if a curve has $(3, 3)$, and $(5, 5)$-split Jacobian. The case of $(2, 2)$-split Jacobian corresponds to genus 2 curves with extra involutions and therefore can be determined by the function `LocusCurvesAut_V_4()`.

The function which determines if a genus 2 curve has $(3, 3)$-split Jacobian is `CurvDeg3EllSub()` if the curve has $J_2 \neq 0$ and `CurvDeg3EllSub_J_2()` otherwise; see [11]. The input of `CurvDeg3EllSub()` is the triple (i_1, i_2, i_3) or the pair $(\mathfrak{a}_1, \mathfrak{a}_2)$ for `CurvDeg3EllSub_J_2 ()`. If the output is 0, in both cases, this means that the corresponding curve to this moduli point has $(3, 3)$-split Jacobian. Below we illustrate with examples in each case.

Example 3. *Let $y^2 = f(x)$ be a genus 2 curve where $f := 4x^6 + 9x^5 + 8x^4 + 10x^3 + 5x^2 + 3x + 1$. Then,*

> $i_1 := i\_1(f, x); i_2 := i\_2(f, x); i_3 := i\_3(f, x);$

$$i_1 := \frac{78741}{100}, \quad i_2 := \frac{53510733}{2000}, \quad i_3 := \frac{38435553}{51200000}$$

> `CurvDeg3EllSub`(i_1, i_2, i_3)*;*

$$0$$

This means that the above curve has a $(3, 3)$-split Jacobian.

Example 4. *Let $y^2 = f(x)$ be a genus 2 curve where $f := 4x^6 + (52\sqrt{6} - 119)x^5 + (39\sqrt{6} - 24)x^4 + (26\sqrt{6} - 54)x^3 + (13\sqrt{6} - 27)x^2 + 3x + 1$. Then,*

> $a_1 := a\_1(f,x); a_2 := a\_2(f,x);$

$$a_1 := \frac{1316599234443}{270840023}\sqrt{6} + \frac{6310855638567}{541680046},$$
$$a_2 := \frac{-96672521239976}{11832080720323281 21}\sqrt{6} + \frac{1467373119039023}{7099248432193968726}$$

> `CurvDeg3EllSub_J_2`(a_1, a_2)

$$0$$

This means that the curve has $J_2 = 0$ and $(3,3)$-split Jacobian.

3.4. **Rational model of genus 2 curve.** For details on the rational model over its field of moduli see [3], [6], [14]. The rational model of C (if such model exists) is determined by the function `Rational_Model()`.

Example 5. *Let $y^2 = f(x)$ be a genus 2 curve where $f := x^5 + \sqrt{2}x^3 + x$. Then,*

> `Rational_Model(f,x);`

$$x^5 + x^3 + \frac{1}{2}x$$

Example 6. *Let $y^2 = f(x)$ be a genus 2 curve where $f := 5x^6 + x^4 + \sqrt{2}x + 1$. Then,*

> `Rational_Model(f,x);`

$$\begin{aligned}
&- 365544026018739971082698131028050365165449396926201478x^6 \\
&- 606501618836700589954579317910699990585971018672445125x^5 \\
&- 369842283192872727990502041940062429271727924754392250x^4 \\
&- 323876769753148934149200031494342152476630742883562 50x^3 \\
&+ 741684900791983289870476522884202717842981712209375 00x^2 \\
&+ 382746484937726017233573508295419718289657325511718 75x \\
&+ 650173246311921392746085957103494954308712336718750 0
\end{aligned}$$

Notice that our algorithm doesn't always find the minimal rational model of the curve. An efficient way to do this has yet to be determined.

4. Hyperelliptic curves of higher genus

A genus g hyperelliptic curve C which has a non-hyperelliptic involution in the automorphism group can be written as

$$y^2 = x^{2g+2} + a_g x^{2g} + \cdots + a_1 x^2 + 1 \tag{5}$$

and $\Delta(a_1, \ldots, a_g) \neq 0$ (i.e., Δ is the discriminant of the right hand side). We call the above equation the **normal form** of the curve C.

The following

$$u_i := a_1^{g-i+1}\, a_i \;+\; a_g^{g-i+1}\, a_{g-i+1}, \quad for \quad 1 \leq i \leq g \tag{6}$$

are invariants under the D_{g+1}-action and are called **dihedral invariants** of the genus g. For a detailed treatment of such invariants see [4].

The functions `Normalpol()` and `Dih_Inv()` compute the normal form and the dihedral invariants of a curve $y^2 = f(x)$, provided that $f(x)$ is a decomposable polynomial in x^2.

Example 7. *Let $y^2 := f(x)$ be a genus 5 curve where $f := 6x^{12} + 4x^8 + 3x^4 + 2x^2 + 12$. Then,*

>`Normalpol(f,x);`

$$x^{12} + \frac{1}{3}\cdot 2^{\frac{3}{2}} x^8 + \frac{1}{4}\cdot 2^{\frac{1}{3}} x^4 + \frac{1}{6}\cdot 2^{\frac{1}{6}} x^2 + 1$$

> `Dih_Inv(f,x);`

$$[\frac{1}{23328}, \frac{1}{2592}, 0, \frac{1}{54}, 0]$$

4.1. **Genus 3 hyperelliptic curves.** Every genus $g = 3$ hyperelliptic curve is given by a homogenous equation $y^2 z^6 = f(x, z)$ where $f(x, z)$ is a binary octavic (i.e., a degree 8 homogenous polynomial)

$$f(x, z) = \sum_{i=0}^{8} a_i x^i z^{8-i}.$$

We define the following covariants:

$$g = (f, f)^4, \quad k = (f, f)^6, \quad h = (k, k)^2, \quad m = (f, k)^4,$$
$$n = (f, h)^4, \quad p = (g, k)^4, \quad q = (g, h)^4,$$

where the symbol $(f, g)^k$ denotes the k-th transvection of binary forms (cf. section 4.2).

Then the following

$$J_2 = (f, f)^8, \quad J_3 = (f, g)^8, \quad J_4 = (k, k)^4, \tag{7}$$
$$J_5 = (m, k)^4, \quad J_6 = (k, h)^4, \quad J_7 = (m, h)^4$$

are invariants of binary octavics.

4.1.1. *Automorphism groups of Genus 3 hyperelliptic curves.* A list of groups that can occur as automorphism groups of hyperelliptic curves is given in [13] among many other references. The function in the package that computes the automorphism group is given by `AutGroup()`. The output a the GAP identity of the group.

For a fixed group G one can compute the locus of genus g hyperelliptic curves with automorphism group G. For genus 3 this loci is well described as subvarieties of $\mathcal{M}_3$. The list of groups for $g = 3$ is: ${\mathbb{Z}_2}^3, \mathbb{Z}_2\times\mathbb{D}_8, \mathbb{Z}_2\times\mathbb{Z}_2, \mathbb{Z}_2\times\mathbb{Z}_4, \mathbb{U}_6, \mathbb{V}_8, \mathbb{Z}_2\times\mathbb{S}_4, \mathbb{Z}_6$.

Example 8. *Let $y^2 := f(x)$ be a genus 3 curve where $f := 3x^8 + x^6 + x^4 + 2x^2 + 1$. Then,*

> `AutGroup(f,x);`

$$[\mathbb{Z}_2 \times \mathbb{Z}_2, (4, 2)]$$

4.1.2. *Rational model of genus 3 hyperelliptic curves.* We can determine the rational model of all hyperelliptic curves with extra automorphisms other than the case when the automorphism group is V_4.

Example 9. *Let $y^2 := f(x)$ be a genus 3 curve where $f := x^8 + \sqrt{2}$. Then,*

```
> Rational_Model(f,x);
```

$$x^8 - 1$$

Example 10. *Let $y^2 := f(x)$ be a genus 3 curve where $f := x^8 + 14x^4 + \sqrt{6}$. Then,*

```
> Rational_Model(f,x);
```

$$\frac{98}{3}\sqrt{6}x^8 + \frac{98}{3}\sqrt{6}x^4 + 1$$

This is correct since the field of moduli in this case is $\mathbb{Q}(\sqrt{6})$.

4.2. **Higher genus hyperelliptic curves.** We use the symbolic method of classical invariant theory to construct invariants of binary forms. Let $f(X,Y)$ and $g(X,Y)$ be binary forms of degree n and m respectively. We define the *r-transvection*

$$(f,g)^r := \frac{(m-r)!\,(n-r)!}{n!\,m!} \sum_{k=0}^{r} (-1)^k \binom{r}{k} \cdot \frac{\partial^r f}{\partial X^{r-k}\,\partial Y^k} \cdot \frac{\partial^r g}{\partial X^k\,\partial Y^{r-k}}$$

see [7] or [8] for details.

For the rest of this paper $F(X,Y)$ denotes a binary form of degree $d := 2g+2$. 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:

$$J_{4j} := (F,F)^{d-2j},\ j = 1,\dots,g, \qquad I_2 := (F,F)^d,$$
$$I_4 := (J_{12},J_{12})^{12}, \qquad I_6 := ((F,J_{12})^{12},(F,J_{12})^{12})^{d-12},$$
$$I_6^* := ((F,J_{20})^{20},(F,J_{20})^{20})^{d-20}.$$

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

$$i_1 := \frac{I_4}{I_2^2}, \quad i_2 := \frac{I_6}{I_2^3}, \quad i_3 = \frac{I_6^*}{I_2^3}, \quad i_4 = \frac{I_6^2}{I_4^3}$$

In [9], [8] we study the 1-dimensional loci of genus g hyperelliptic curves with reduced automorphism group A_4, A_5, S_5. The above invariants give some nice conditions to determine if the curves have such reduced automorphisms groups.

Lemma 1. *Let $\mathcal{X}_g$ be a hyperelliptic curve with genus g defined over $\mathbb{C}$.*
a) If $\overline{Aut}\ (\mathcal{X}_g) \cong A_5$ then
i) the invariants $(J_i,J_i)^i$ are zero for $i = 4, 8, 16, 28$;
ii) if $g \le 120$ then the invariant $(J_8,J_8)^8$ is zero;
iii) if $g \le 60$ then the invariants $(J_{16},J_{16})^{16}$ and $(J_{28},J_{28})^{28}$ are zero.
b) If $\overline{Aut}\ (\mathcal{X}_g) \cong A_4$ then $J_4(\mathcal{X}_g) = 0$.

Proof. See [9], [8]. □

For all curves C with $V_4 \hookrightarrow \overline{Aut}\ (C)$ we provide a rational model over the field of moduli as in [4]. Such models are also provided when $\overline{Aut}\ (C) \cong A_4, A_5$; see [8], [9].

4.3. **List of functions:** In the genus 2 package there are the following functions:

a_1(C,x)	a_2(C,x)
i_1(C,x)	i_2(C,x)
i_3(C,x)	J_2(C,x)
J_4(C,x)	J_6(C,x)
J_10(C,x)	BranchLoc_Deg3EllSub(i_1, i_2)
CurvDeg3EllSub(i_1, i_2, i_3)	CurvDeg3EllSub_$J_2(s_1, s_2)$
LocusCurvesAut_$V_4(i_1, i_2, i_3)$	LocusCurvesAut_$D_4(i_1, i_2, i_3)$
LocusCurvesAut_$D_6(i_1, i_2, i_3)$	CurvDeg3EllSub_Degen(i_1, i_2, i_3)
AutGroup(C,x)	Rational_Model(C,x)

In the genus 3 package there are the following functions:

i_1(C,x)	i_2(C,x)
i_3(C,x)	J_2(C,x)
J_3(C,x)	J_4(C,x)
J_5(C,x)	J_6(C,x)
J_7(C,x)	J_8(C,x)
u_1(C,x)	u_2(C,x)
u_3(C,x)	J_14(C,x)
IsRational(C,x)	Normalpol(C,x)
Dih_Inv(C,x)	AutGroup(C,x)
Rational_Model(C,x)	

References

[1] R. Brandt and H. Stichtenoch, Die Automorphismengrupenn hyperelliptischer Kurven. *Manuscripta Math* **55** (1986), no. 1, 83–92.

[2] E. Bujalance, J.M. Gamboa, G. Gromadzki, The full automorphism groups of hyperelliptic Riemann surfaces, *Manuscripta Math.* **79** (1993), no. 3-4, 267–282.

[3] G. Cardona and J. Quer, Field of moduli and field of definition for curves of genus 2, (Ed. T. Shaska), *Lect. Notes in Computing*, vol 13. (2005). (to appear)

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

[5] J. Igusa, Arithmetic variety of moduli for genus 2. *Ann. of Math.* (2), 72, 612-649, (1960).

[6] P. Mestre, Construction de courbes de genre 2 á partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, volume 94. *Prog. Math.* , 313-334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17-21, (1990).

[7] V. Krishnamorthy, T. Shaska, and H. Völklein, Invariants of binary forms, *Developments in Mathematics*, Vol. 12, Springer 2004, pg. 101-122.

[8] D. Sevilla, T. Shaska, Hyperelliptic curves with reduced automorphism group A_5 (submitted).

[9] T. Shaska, Some special families of hyperelliptic curves, *J. Algebra Appl.*, vol **3**, No. 1 (2004), 75-89.

[10] T. Shaska, H. Völklein, Elliptic subfields and automorphisms of genus two fields, *Algebra, Arithmetic and Geometry with Applications. Papers from Shreeram S. Abhyankar's 70th Birthday Conference*, pg. 687 - 707, Springer (2004).

[11] T. Shaska, Genus 2 curves with degree 3 elliptic subcovers, *Forum. Math.*, vol. **16**, 2, pg. 263-280, 2004.

[12] T. Shaska, Computational aspects of hyperelliptic curves, Computer mathematics. Proceedings of the sixth Asian symposium (ASCM 2003), Beijing, China, April 17-19, 2003. River Edge, NJ: World Scientific. *Lect. Notes Ser. Comput.* 10, 248-257 (2003).

[13] T. Shaska, Detremining the automorphism group of hyperelliptic curves, *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pg. 248-254, 2003.

[14] T. Shaska, Genus 2 curves with (3,3)-split Jacobian and large automorphism group, Algorithmic Number Theory (Sydney, 2002), **6**, 205-218, *Lect. Not. in Comp. Sci.*, 2369, Springer, Berlin, 2002.

[15] T. Shaska, Curves of genus 2 with (n, n)-decomposable Jacobians, *J. Symbolic Comput.* 31 (2001), no. 5, 603–617.

E-mail address: shaska@oakland.edu

Department of Mathematics and Statistics,, Oakland University,, Rochester, MI, 48309

E-mail address: zhen8299@uidaho.edu

Department of Computer Science,, University of Idaho,, Moscow, ID, 83843