

COMPUTATIONAL ALGEBRA AND ALGEBRAIC CURVES

TANUSH SHASKA

Department of Mathematics,
University of Idaho,
Moscow, ID, 83843

ABSTRACT. The development of computational techniques in the last decade has made possible to attack some classical problems of algebraic geometry. In this survey, we briefly describe some open problems related to algebraic curves which can be approached from a computational viewpoint.

1. INTRODUCTION

Computational algebra is a very active and rapidly growing field, with many applications to other areas of mathematics, as well as computer science and engineering. In this survey, however, we will focus on applications that computational algebra has on classical problems of mathematics and more explicitly on algebraic curves.

We survey topics related to automorphisms of algebraic curves, field of moduli versus field of definition, Hurwitz groups and Hurwitz curves, genus 2 curves with split Jacobians etc. The problems we suggest are a very narrow trend in algebraic geometry. However, they provide examples of how new computational techniques can be used to answer some old questions.

In the second section we describe genus 2 curves with split Jacobians. There are many papers written on these topic going back to Legendre and Jacobi in the context of elliptic integrals. The problem we suggest is to compute the moduli space of covers of degree 5, 7 from a genus 2 curve to an elliptic curve. This problem is completely computational and could lead to some better understanding of some conjectures on elliptic curves; see Frey [Fr].

In section three, we discuss the automorphism groups of algebraic curves. There has been some important progress on this topic lately, however much more can be done. Extending some of the results to positive characteristic would be important. Further we suggest computing the equations of Hurwitz curves of genus 14 and 17.

In section 4 we study hyperelliptic curves. Finding invariants which classify the isomorphism classes of hyperelliptic curves of genus $g \geq 3$ is still an open problem. However, it is an easier problem to deal with hyperelliptic curves with extra automorphisms. The main result here is from [GS] where dihedral invariants were introduced which identify the isomorphism classes of such curves. Using these dihedral invariants one can determine the automorphism group of hyperelliptic curves; see [Sh5]. However, implementing such algorithm is still a challenge since the loci of curves with prescribed automorphism group are still to be computed in terms of dihedral invariants. The second problem of section 4 is to find what solvable

groups can occur as monodromy groups of full moduli dimension for coverings of the Riemann sphere with a genus two curve; see section 4.1, for details.

In the last section we focus on the field of moduli of algebraic curves. This is a classical problem of algebraic geometry that goes back to Weil and Shimura among many others. An answer to the conjecture of section 5 would be important in algebraic geometry, but also from a computational viewpoint. Problems 7 - 10 suggest some variations of the field of moduli problem.

Acknowledgment: Most of the topics discussed in this paper are joint work with my collaborators. I would like to thank J. Gutierrez, B. Guralnick, K. Magaard, S. Shpectorov, H. Völklein, M. Fried, J. Schicho, I. Shparlinski among many others for many helpful discussions. This paper originated from my talk in ACA 03, held in Raleigh, North Carolina. I want to thank the organizing committee of ACA 03, especially M. Giesbrecht, H. Hong, E. Kaltofen, and A. Szanto. Finally, I would like to thank E. Volcheck for suggesting that I summarize my talk at ACA 03 in this article for the Communications of Computer Algebra.

2. GENUS 2 CURVES WITH SPLIT JACOBIAN

First, we focus on genus 2 curves whose Jacobians are isogenous to a product of elliptic curves. These curves have been studied extensively in the 19th century in the context of elliptic integrals. Legendre gave the first example of such a curve and then Jacobi, Clebsch, Hermite, Goursat, Brioschi, and Bolza explored them further. In the late 20th century Frey and Kani, Kuhn, Gaudry and Schost, Shaska and Voelklein, and many others have studied these curves further. They are of interest for the arithmetic of genus 2 curves as well as elliptic curves. See [FK] for some conjectures that relate this topic with the arithmetic of elliptic curves.

Let C be a curve of genus 2 and $\psi_1 : C \rightarrow E_1$ a map of degree n , from C to an elliptic curve E_1 , both curves defined over \mathbb{C} . In [Sh1], we show that this map induces a degree n map $\phi_1 : \mathbb{P}^1 \rightarrow \mathbb{P}^1$. We determine all possible ramifications for ϕ_1 . If $\psi_1 : C \rightarrow E_1$ is maximal (i.e., does not factor non-trivially) then there exists a maximal map $\psi_2 : C \rightarrow E_2$, of degree n , to some elliptic curve E_2 such that there is an isogeny of degree n^2 from the Jacobian J_C to $E_1 \times E_2$. We say that J_C is (n, n) -decomposable. If the degree n is odd the pair (ψ_2, E_2) is canonically determined; see [Sh1] for details.

We denote the moduli space of such degree n coverings $\phi : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ by \mathcal{L}_n . This space is studied by Kani and it is called “modular diagonal space”. It can be viewed also as the Hurwitz space of covers $\phi : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ with ramification determined above. For our purposes, \mathcal{L}_n will simply be the locus of genus 2 curves whose Jacobian is (n, n) -isogenous to a product of two elliptic curves.

The locus \mathcal{L}_2 of these genus 2 curves is a 2-dimensional subvariety of the moduli space \mathcal{M}_2 and is studied in detail in [SV1]. An equation for \mathcal{L}_2 is already in the work of Clebsch and Bolza. We use a birational parametrization of \mathcal{L}_2 by affine 2-space to study the relation between the j -invariants of the degree 2 elliptic subfields. This extends work of Geyer, Gaudry, Stichtenoth and others. We find a 1-dimensional family of genus 2 curves having exactly two isomorphic elliptic subfields of degree 2; this family is parameterized by the j -invariant of these subfields. This was a joint project with H. Völklein, published in the proceedings of professor Abhyankar’s 70th birthday conference.

If $n > 2$, the surface \mathcal{L}_n is less understood. The case $n = 3$ was initially studied by Kuhn [Ku] where some computations for $n = 3$ were performed. The computation of the equation of \mathcal{L}_3 was a major computational effort. A detailed description of this computation is given in [Sh2]. Computational algebra techniques (i.e., Groebner basis, Buchberger algorithm) and computational algebra packages (i.e., Magma, Maple, GAP) were used. In [Sh2], we study genus 2 function fields K with degree 3 elliptic subfields. We show that the number of $\text{Aut}(K)$ -classes of such subfields of fixed K is 0, 1, 2 or 4. Also we compute an equation for the locus of such K in the moduli space of genus 2 curves. Equations of \mathcal{L}_n for $n > 5$ are still unknown.

Let \mathcal{C} be a genus 2 curve defined over k , $\text{char}(k) = 0$. If $\bar{k}(\mathcal{C})$ has a degree 3 elliptic subfield then the automorphism group $\text{Aut}(\mathcal{C})$ is isomorphic to one of the following: \mathbb{Z}_2 , V_4 , D_8 , or D_{12} , where D_n is the dihedral group of order n . There are exactly six genus two curves \mathcal{C} defined over \mathbb{C} with $\text{Aut}(\mathcal{C})$ isomorphic to D_8 (resp., D_{12}). We further show that only four (resp., three) of the curves with group D_8 (resp., D_{12}) are defined over \mathbb{Q} . This is summarized in [Sh3].

Continuing on the work of the above papers, we suggest the following problem:

Problem 1. *Determine the locus \mathcal{L}_n in \mathcal{M}_2 for $n = 5, 7$. Further, determine the relation between the elliptic curves E_1 and E_2 in each case.*

Using techniques from [SV1, Sh2] this becomes simple a computational problem. However, determining such loci requires the use of a Groebner basis algorithm. Computationally this seems to be difficult for $n = 5, 7$.

3. THE AUTOMORPHISM GROUP OF A COMPACT RIEMANN SURFACE

Computation of automorphism groups of compact Riemann surfaces is a classical problem that goes back to Schwartz, Hurwitz, Klein, Wiman and many others. Hurwitz showed that the order of the automorphism group of a compact Riemann surface of genus g is at most $84(g-1)$, which is known as the Hurwitz bound. Klein was mostly interested with the real counterpart of the problem, hence the term “compact Klein surfaces”. Wiman studied automorphism groups of hyperelliptic curves and orders of single automorphisms.

The 20th century produced a huge amount of literature on the subject. Baily [Ba] gave an analytical proof of a theorem of Hurwitz: if $g \geq 2$, there exists a curve of genus g with non-trivial automorphisms. In other papers was treated the number of automorphisms of a Riemann surface; see Accola [Ac1], Maclachlan [Mc1], [Mc2] among others. Accola [Ac2] gives a formula relating the genus of a Riemann surface with the subgroups of the automorphism group; known as Accola’s theorem. Harvey studied cyclic groups and Lehner and Newman maximal groups that occur as automorphism groups of Riemann surfaces.

A group of automorphisms of a compact Riemann surface X of genus g can be faithfully represented via its action on the abelian differentials on X as a subgroup of $GL(g, \mathbb{C})$. There were many efforts to classify the subgroups G of $GL(g, \mathbb{C})$ that so arise, via the cyclic subgroups of G and conditions on the matrix elements of G . In a series of papers, I. Kuribayashi, A. Kuribayashi, and Kimura compute the lists of subgroups which arise this way for $g = 3, 4$, and 5 .

By covering space theory, a finite group G acts (faithfully) on a genus g curve if and only if it has a genus g generating system; see [MS]. Using this purely group-theoretic condition, Breuer [Br] classified all groups that act on a curve of genus

≤ 48 . This was a major computational effort using the computer algebra system GAP. It greatly improved on several papers dealing with small genus, by various authors.

Of course, for each group in Breuer’s list, all subgroups are also in the list. This raises the question how to pick out those groups that occur as the **full automorphism group** of a genus g curve. This question is answered in the following paper.

Let G be a finite group, and $g \geq 2$. In a joint project with Magaard, Shpectorov, and Völklein we study the locus of genus g curves that admit a G -action of given type, and inclusions between such loci; see [MS]. We use this to study the locus of genus g curves with prescribed automorphism group G . We completely classify these loci for $g = 3$ (including equations for the corresponding curves), and for $g \leq 10$ we classify those loci corresponding to “large” G .

We suggest the following:

Problem 2. *Determine the list of possible automorphism groups of algebraic curves of small genus (i.e., $g \leq 10$) in every characteristic.*

For $g = 2$ this list is well known (it appears also in [SV1]). For $g = 3$ it can probably be completed from work of Brock, Wolper and others. However, for $g > 3$ such list of groups is unknown. It would be nice to have a complete list for “small genus”, say $g \leq 10$. Since, such lists tend to grow as genus grows, such information could be organized in a database and be very helpful to the mathematics community. It is important to mention that such lists are not known even in characteristic zero.

In [Sh5] (ISSAC 03) a new algorithm was introduced to compute the automorphism group of a given hyperelliptic curve. However, this will be discussed in more detail in the next section.

3.1. Hurwitz curves. A Hurwitz curve is a genus g curve, defined over an algebraically closed field of characteristic zero, which has $84(g - 1)$ automorphisms. A group G that can be realized as an automorphism group of a Hurwitz curve is called a Hurwitz group. There are a lot of papers by group-theoretists on Hurwitz groups, surveyed by Conder. It follows from Hurwitz’s presentation that a Hurwitz group is perfect. Thus every quotient is again a Hurwitz group, and if such a quotient is minimal then it is a non-abelian simple group. Several infinite series of simple Hurwitz groups have been found by Conder, Malle, Kuribayashi, Zalessky, Zimmermann and others. In 2001, Wilson showed the monster is a Hurwitz group; see [MS] for a complete list of references.

Klein’s quartic is the only Hurwitz curve of genus $g \leq 3$. Fricke showed that the next Hurwitz group occurs for $g = 7$ and has order 504. Its group is $SL(2, 8)$, and an equation for it was computed by Macbeath in 1965. Klein’s quartic and Macbeath’s curve are the only Hurwitz curves whose equations are known. Further Hurwitz curves occur for $g = 14$ and $g = 17$ (and for no other values of $g \leq 19$). It is natural, to try to write equations for these Hurwitz curves of genus 14, 17.

Problem 3. *Compute equations for the Hurwitz curves of genus 14, and possibly 17.*

4. COMPUTATIONAL ASPECTS OF HYPERELLIPTIC CURVES

It is an interesting and difficult problem in algebraic geometry is to obtain a generalization of the theory of elliptic modular functions to the case of higher genus.

In the elliptic case this is done by the so-called *j-invariant* of elliptic curves. In the case of genus $g = 2$, Igusa (1960) gives a complete solution via *absolute invariants* i_1, i_2, i_3 of genus 2 curves. Generalizing such results to higher genus is much more difficult due to the existence of non-hyperelliptic curves. However, even restricted to the hyperelliptic moduli \mathcal{H}_g the problem is still unsolved for $g \geq 3$. In other words, there is no known way of identifying isomorphism classes of hyperelliptic curves of genus $g \geq 3$. In terms of classical invariant theory this means that the field of invariants of binary forms of degree $2g + 2$ is not known for $g \geq 3$.

The following is a special case of $g = 3$.

Problem 4. *Find invariants which classify the isomorphism classes of genus 3 hyperelliptic curves.*

This is equivalent with determining the field of invariants of binary octavics. The covariants of binary octavics were determined in 1880 by von Gall. The generators of the ring of invariants were determined by Shioda in 1965. However, the field of invariants is unknown. This is a computational problem and should be possible to solve with now-day techniques. Extending this to positive characteristic would be quite interesting.

In a joint paper with J. Gutierrez, we find invariants that identify isomorphism classes of genus g hyperelliptic curves with extra (non-hyperelliptic) involutions; see [GS]. This result gives a nice way of doing computations with these curves. We call such invariants *dihedral invariants* of hyperelliptic curves. Let \mathcal{L}_g be the locus in \mathcal{H}_g of hyperelliptic curves with extra involutions. \mathcal{L}_g is a g -dimensional subvariety of \mathcal{H}_g . The dihedral invariants yield a birational parametrization of \mathcal{L}_g . Computationally these invariants give an efficient way of determining a point of the moduli space \mathcal{L}_g . Moreover, we show that the field of moduli is a field of definition (see below) for all $\mathbf{p} \in \mathcal{L}_3$ such that $|\text{Aut}(\mathbf{p})| > 4$.

Dihedral invariants can be used to study the field of moduli of hyperelliptic curves in \mathcal{L}_g (cf. section 5). Whether or not the field of moduli is a field of definition is in general a difficult problem that goes back to Weil, Shimura et al. In ASCM 2003, we conjecture that for each $\mathbf{p} \in \mathcal{H}_g$ such that $|\text{Aut}(\mathbf{p})| > 2$ the field of moduli is a field of definition. Making use of dihedral invariants we show that if the Klein 4-group can be embedded in the reduced automorphism group of $\mathbf{p} \in \mathcal{L}_g$ the our conjecture holds; see [Sh4] for details.

The families of hyperelliptic curves with reduced automorphism group (i.e., the automorphism group modulo the hyperelliptic involution) isomorphic to A_4 or a cyclic group, are studied in [Sh6]. We characterize such curves in terms of classical invariants of binary forms and in terms of dihedral invariants. Further, we describe algebraically the loci of such curves for $g \leq 12$ and show that for all curves in these loci the field of moduli is a field of definition.

New techniques for computing the automorphism group of a genus g hyperelliptic curve \mathcal{X}_g are discussed in [Sh5]. The first technique uses the classical $GL_2(k)$ -invariants of binary forms. This is a practical method for curves of small genus, but has limitations as the genus increases, due to the fact that such invariants are not known for large genus. The second approach, which uses dihedral invariants of hyperelliptic curves, is a very convenient method and works well in all genera. We define the normal decomposition of a hyperelliptic curve with extra automorphisms. Then, dihedral invariants are defined in terms of the coefficients of this normal decomposition. We define such invariants independently of the automorphism group

$\text{Aut}(\mathcal{X}_g)$. However, to compute such invariants the curve is required to be in its normal form. This requires solving a nonlinear system of equations. We discover conditions in terms of classical invariants of binary forms for a curve to have reduced automorphism group A_4 , S_4 , A_5 .

In the case of hyperelliptic curves the list of groups are completely determined in characteristic zero by work of Bujalance, Gromadzky, and Gamboa. We suggest the following:

Problem 5. *Implement a fast algorithm that does the following: Given a genus g hyperelliptic curve \mathcal{X}_g , determine the automorphism group of \mathcal{X}_g .*

The known algorithms (even the recent ones) approach the problem by solving a system of equations via Groebner basis. This is normally inefficient and expensive. We have implemented such programs for small g and these results can be extended even further. It will be valuable to organize such results in a computer algebra package and extend to $g \leq 10$.

4.1. The monodromy group of a genus 2 curve covering \mathbb{P}^1 . Determining the monodromy group of a generic genus g curve covering \mathbb{P}^1 is a problem with a long history which goes back to Zariski and relates to Brill-Noether theory. Let \mathcal{X}_g be generic curve of genus g and $f : X_g \rightarrow \mathbb{P}^1$ a degree n cover. Denote by $G := \text{Mon}(f)$, the monodromy group of $f : X_g \rightarrow \mathbb{P}^1$. Zariski showed that for $g > 6$, G is not solvable. For $g \leq 6$ the situation is more technical. This has been studied by many authors e.g., Fried, Guralnick, Neubauer, Magaard, Völklein et al. However, the problem is open for $g = 2$. Guralnick and Fried, in a preprint dated at 1986, have shown that for G primitive in S_n and solvable there are six possibilities for G . Two of those are obvious cases S_3, S_4 . The other four groups are D_{10} , $\mathbb{Z}_3^2 \rtimes D_8$, $\text{AGL}_2(3)$, $S_4 \wr \mathbb{Z}_2$; see [FG]. The corresponding signatures are:

$$(2^2, 2^2, 2^2, 2^2, 2^2, 2^2), (2^3, 2^3, 2^3, 2^3, 2^4, 2^4), \\ (2^3, 2^3, 2^3, 2^3, 3^2, 3^2), (2^6, 2^6, 2^6, 2^4, 2^4, 2^4).$$

Problem 6. *For each case above, determine the locus of such genus 2 curves in \mathcal{M}_2 (e.g., the equation of such locus in terms of invariants i_1, i_2, i_3) and its dimension.*

Notice that via the braid group action (using GAP), we can show that the corresponding Hurwitz spaces are irreducible. We expect in all cases that the dimension of the locus in \mathcal{M}_2 is ≤ 2 .

5. FIELD OF MODULI VERSUS THE FIELD OF DEFINITION

Let \mathcal{X} be a curve defined over k . A field $F \subset k$ is called a *field of definition* of \mathcal{X} if there exists \mathcal{X}' defined over F such that $\mathcal{X} \cong \mathcal{X}'$. The **field of moduli** of \mathcal{X} is a subfield $F \subset k$ such that for every automorphism σ of k \mathcal{X} is isomorphic to \mathcal{X}^σ if and only if $\sigma_F = \text{id}$.

The field of moduli is not necessary a field of definition. To determine the points $\mathfrak{p} \in \mathcal{M}_g$ where the field of moduli is not a field of definition is a classical problem in algebraic geometry and has been the focus of many authors, Weil, Shimura, Belyi, Coombes-Harbater, Fried, Débes, Wolfart among others.

Weil (1954) showed that for every algebraic curve with trivial automorphism group, the field of moduli is a field of definition. Shimura (1972) gave the first example of a family of curves such that the field of moduli is not a field of definition.

Shimura's family were a family of hyperelliptic curves. Further he adds: “... the above results combined together seem to indicate a rather complicated nature of the problem, which almost defies conjecture. A new viewpoint is certainly necessary to understand the whole situation”

It seems as hyperelliptic curves provide the most interesting examples. For example, we are not aware of any explicit examples of non-hyperelliptic curves such that the field of moduli is not a field of definition. Moreover, with the help of dihedral invariants we have a way of describing the points of moduli in the locus \mathcal{L}_g . Hence, we focus on hyperelliptic curves.

We call a point $\mathbf{p} \in \mathcal{H}_g$ a *moduli point*. The field of moduli of \mathbf{p} is denoted by $F_{\mathbf{p}}$. If there is a curve \mathcal{X}_g defined over $F_{\mathbf{p}}$ such that $\mathbf{p} = [\mathcal{X}_g]$, then we call such a curve a *rational model over the field of moduli*. Consider the following problem:

Let the moduli point $\mathbf{p} \in \mathcal{H}_g$ be given. Find necessary and sufficient conditions that the field of moduli $F_{\mathbf{p}}$ is a field of definition. If \mathbf{p} has a rational model \mathcal{X}_g over its field of moduli, then determine explicitly the equation of \mathcal{X}_g .

In 1993, Mestre solved the above problem for genus two curves with automorphism group \mathbb{Z}_2 . Mestre's approach is followed by Cardona and Quer (2002) to prove that for points $\mathbf{p} \in \mathcal{M}_2$ such that $|\text{Aut}(\mathbf{p})| > 2$ the field of moduli is a field of definition; see also [Sh3] for a different approach. In his talk at ANTS V (see [Sh3]), the author conjectured the following:

Conjecture 1. *Let $\mathbf{p} \in \mathcal{H}_g$ be a moduli point such that $|\text{Aut}(\mathbf{p})| > 2$. Then, its field of moduli is a field of definition.*

The author has proved this conjecture for curves with reduced automorphism group isomorphic to A_4 and genus $g \leq 12$; see [Sh6]. Also the conjecture is true for $g = 3$ and $|\text{Aut}(\mathbf{p})| > 4$; see [GS]. Furthermore, we intend to investigate the conjecture in all cases:

Problem 7. *Investigate Conjecture 1 in all cases.*

In studying the above conjecture, we are looking for more than just a true or false answer. We would like a way to determine the field of moduli of any hyperelliptic curves with extra automorphisms. Generically, dihedral invariants accomplish this for curves with extra involutions (i.e., locus \mathcal{L}_g). However, there is also the singular locus in \mathcal{L}_g which needs to be considered. And then, there are also hyperelliptic curves with extra automorphisms which are not in \mathcal{L}_g . The upshot would be to solve the following:

Problem 8. *Let $\mathbf{p} \in \mathcal{H}_g$. Determine if the field of moduli is a field of definition. In that case, explicitly find a rational model of the curve over its field of moduli.*

The above problems lead to the following:

Problem 9. *Find necessary and sufficient conditions in terms of invariants of binary forms such that a hyperelliptic curve has no extra automorphisms.*

Such conditions were known to Clebsch and Bolza for $g = 2$. These conditions were used by Mestre in [Me]. Finding similar conditions for $g \geq 3$ would help extend Mestre's algorithm to $g \geq 3$. Solving the above problem would give a way of investigating Conjecture 1 without the hypothesis $|\text{Aut}(\mathbf{p})| > 2$.

Problem 10. *Find an algorithm which does the following: Let $\mathbf{p} \in \mathcal{H}_g$ such that $|\text{Aut}(\mathbf{p})| = 2$. Determine if the field of moduli is a field of definition.*

REFERENCES

- [Ac1] R. ACCOLA, On the number of automorphisms of a closed Riemann surface, *Trans. Amer. Math. Soc.* **131** (1968), 398–408.
- [Ac2] R. ACCOLA, Two theorems on Riemann surfaces with noncyclic automorphism groups, *Proc. Amer. math. Soc.* **25** (1970), 598–602.
- [Ba] W. BAILY, On the automorphism group of a generic curve of genus > 2 , *J. Math. Kyoto Univ.* **1** (1961/1962), 101–108; correction, 325.
- [Br] TH. BREUER, Characters and automorphism groups of compact Riemann surfaces, *London Math. Soc. Lect. Notes* **280**, Cambridge Univ. Press 2000.
- [Bo] O. BOLZA, On binary sextics with linear transformations into themselves, *Amer. J. Math.* **10** (1888), 47–70.
- [BS] R. BRANDT AND H. STICHTENOGH, Die Automorphismengruppen hyperelliptischer Kurven. *Manuscripta Math* **55** (1986), no. 1, 83–92.
- [Bu] E. BUJALANCE E, J. M. GAMBOA, G. GROMADZKI, The full automorphism groups of hyperelliptic Riemann surfaces, *Manuscripta Math.* **79** (1993), no. 3–4, 267–282.
- [CF] J. W. S. CASSELS AND E. V. FLYNN; Prolegomena to a Middlebrow Arithmetic of Curves of Genus Two, *LMS*, 230, 1996.
- [Cl] A. CLEBSCH, Theorie der Binären Algebraischen Formen, Verlag von B.G. Teubner, Leipzig (1872).
- [DM] P. DELIGNE P, D. MUMFORD D, The irreducibility of the space of curves of given genus, *Publ. Math. Hautes Études Sci.* **36**, 75–109, 1969.
- [ES] T. EKEDAH T, J. P. SERRE, Exemples de courbes algébriques à jacobienne complètement décomposable. *C. R. Acad. Sci. Paris Sr. I Math.*, 317 (1993), no. 5, 509–513.
- [Fr] G. FREY, On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2. *Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993)*, 79–98, Ser. Number Theory, I, *Internat. Press, Cambridge, MA*, (1995).
- [FK] G. FREY AND E. KANI, Curves of genus 2 covering elliptic curves and an arithmetic application. *Arithmetic algebraic geometry (Texel, 1989)*, 153–176, *Progr. Math.*, 89, *Birkhäuser Boston, Boston, MA*, (1991).
- [FG] M. FRIED AND R. GURALNICK, Radicals don't uniformize the generic curve of genus $g > 6$. (preprint).
- [FMV] G. FREY, K. MAGAARD, AND H. VÖLKLEIN The general curve covers \mathbb{P} with monodromy group A_n , preprint.
- [Gu] J. GUTIERREZ, A polynomial decomposition algorithm over factorial domains, *Comptes Rendues Mathématiques, de Ac. de Sciences*, 13 (1991), 81–86.
- [Gu] J. GUTIERREZ, H. NIEDERREITER, I. SHPARLINSKI, On the multidimensional distribution of inverse congruential pseudorandom numbers in parts of the period. *Monatsh. Math.* **129** (2000), no. 1, 31–36.
- [GS] J. GUTIERREZ AND T. SHASKA, Hyperelliptic curves with extra involutions, (submitted), 2002.
- [Ku] M. R. KUHN, Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc* **307**, 41–49, 1988.
- [Ig] J. IGUSA, Arithmetic Variety Moduli for genus 2. *Ann. of Math.* (2), **72**, 612–649, 1960.
- [Mc1] C. MACLACHLAN, Abelian groups of automorphisms of compact Riemann surfaces, *Proc. London Math. Soc.* (3) **15** (1965), 699–712.
- [Mc2] C. MACLACHLAN, A bound for the number of automorphisms of a compact Riemann surface, *J. London Math. Soc.* (2) **44** (1969), 265–272.
- [MS] K. MAGAARD, T. SHASKA, S. SHPECTOROV, AND H. VÖLKLEIN, The locus of curves with prescribed automorphism group. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). *Sūrikaiseikikenkyūsho Kōkyūroku No.* 1267 (2002), 112–141.
- [Me] J. P. MESTRE, Construction de courbes de genre 2 à 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)*.
- [Sh] T. SHASKA, Curves of Genus Two Covering Elliptic Curves, *PhD thesis*, University of Florida, 2001.
- [Sh1] T. SHASKA, Curves of genus 2 with (n, n) -decomposable Jacobians, *J. Symbolic Comput.* **31** (2001), no. 5, 603–617.

- [Sh2] T. SHASKA, Genus 2 curves with degree 3 elliptic subcovers, *Forum. Math.*, 2002, (accepted May 2002).
- [Sh3] 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.
- [Sh4] T. SHASKA, Computational aspects of hyperelliptic curves, *Computer Mathematics* (Beijing, 2003), *Lect. Not. Ser. Comput.*, **10**, World Sci. Publishing, River Edge, NJ, 2003.
- [Sh5] T. SHASKA, Determining the automorphism group of hyperelliptic curves, *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, 2003.
- [Sh6] T. SHASKA, Some special families of hyperelliptic curves, *J. Algebra Appl.*, 2003.
- [SV1] T. SHASKA AND H. VÖLKLEIN, Elliptic subfields and automorphisms of genus two fields, *Algebra, Arithmetic and Geometry with Applications. Papers from Shreeeram S. Abhyankar's 70th Birthday Conference*, Springer (2003).
- [SV2] T. SHASKA AND H. VÖLKLEIN, Genus two curves with degree 5 elliptic subcovers (preprint).
- [Shi] T. SHIODA, Constructing curves with high rank via symmetry. *Amer. J. Math.* 120 (1998), no. 3, 551–566.
- [Wi] A. WIMAN, Über die hyperelliptischen Curven vom den Geschlechte $p = 4, 5$, und 6, welche eindeutige Transformationen in sich besitzen, *Bihang Kongl. Svenska Vetenskaps-Akademiens Handlingar* (1895), no. 21 (3), 1–41.