Elliptic and Hyperelliptic Curves over Supersimple Fields in Characteristic 2

Amador Martin-Pizarro
Institut für Mathematik
Humboldt-Universität zu Berlin
Berlin, D-10099, Germany
pizarro@mathematik.hu-berlin.de
Ph:+-49-30-2093-5847
Fax:+-49-30-2093-5853

May 13, 2005

Abstract

In this paper, we extend a previous result of A. Pillay and the author regarding existence of rational points over elliptic and hyperelliptic curves with generic moduli defined over supersimple fields to the even characteristic case. We give a detailed exposition of the affine models of these families of curves in characteristic 2 and the transformations between members in the same rational isomorphism class.

Keywords: Model Theory Algebraic Geometry

1 Introduction and preliminaries

After the results of Kim and Pillay ([11]), simple unstable theories as introduced by Shelah ([22]) were recognized to be a good setting to carry over ideas from Geometric Model Theory. They lead to interesting consequences when considering additional algebraic structure, for example, fields. The first known example of a simple unstable field was given by [3]: pseudofinite fields (infinite models of the theory of finite fields). This was later generalized [10]

to the case of perfect pseudo-algebraically closed (in short, PAC) fields with small absolute Galois group (only finitely many field extensions of every finite degree). Recall that a perfect field is PAC if every absolutely irreducible variety defined over the field has a rational point. In fact, the above examples are supersimple fields of SU rank 1. It was shown in [20] that supersimple fields are perfect and have small absolute Galois group, but their definitive algebraic characterization (as in [14] for ω-stable fields) is still open. Motivated by [10], Pillay posed the question whether supersimple fields were PAC; as shown in [6], this reduces to the question of existence of rational points on absolutely irreducible plane curves. The first attempt was done in [21], where it was shown that supersimple fields have cohomological dimension at most one. It follows from this that rational curves become birationally isomorphic to the projective line over the supersimple field. So it became natural to ask what happens with curves of higher genus. In [17] some results were shown for certain families of elliptic and hyperelliptic curves. These results used s-genericity of the modulus of the curve in order to transform the equation describing the curve into one with generic independent coefficients, so that a generic solution can be found following the methods of [21], in particular a clever use of the Independence Theorem. However, the proofs exhibited did not work in characteristic 2. This article (which can be seen as a completion of [17]) deals exclusively with the remaining case. In this situation, not only the equations describing the curves are radically different (which involves a dual argument, switching the roles of addition and multiplication in the field), but no detailed description of the transformations between curves in the same family was available. Most of the material for this article has been extracted from the author's Ph.D. Thesis [16] under the supervision of A. Pillay.

We assume acquaintance with the ideas exhibited in [17], to which we will frequently refer for comparison with the methods used there.

We fix a supersimple theory T and a sufficiently saturated model $\mathcal{M}$. *Small* or *bounded* means of smaller cardinality than the saturation of $\mathcal{M}$, unless otherwise stated. A *supersimple field* K is a field definable in $\mathcal{M}$; it may be assumed to be definable over $\emptyset$. Moreover, we shall assume that K has characteristic 2. Let $\overline{K}$ be some fixed algebraic closure of K.

Recall the following definition from [17]:

Definition. Suppose $SU(K) = \omega^\alpha n$ (see [25]). Let V be a variety of dimen-

sion d defined over a small set $F \subset K$. A point P in $V(K)$ is *s-generic* over F if $SU(tp(P/F)) = \omega^\alpha nd$.

Note that s-genericity implies genericity in the sense of model theory if V is an algebraic group; hence in the sense of Algebraic Geometry. However, s-generic points need not exist (they do if V is K-rational).

We will show the following:

Theorem. *Let K be a supersimple field, K_0 a subfield of K whose cardinality is smaller than the cardinality of saturation and E an elliptic curve defined over K_0 with j-*invariant *s-generic over $\emptyset$, or $j = 0\,, 1728$. Then E has a K-rational point s-generic over K_0.*

Moreover, let C be a hyperelliptic curve defined over K_0 of genus g ($g \geq 2$) with s-generic modulus *over $\emptyset$ in the space of moduli of hyperelliptic curves of genus g. Then C has a K-rational point s-generic over K_0.*

Let us first make shed some remarks about moduli spaces: let $g \geq 2$ be a fixed integer. We are interested in the category $C(g)$ whose objects are smooth curves over $\overline{K}$ of genus g and whose arrows are morphisms between the curves defined over $\overline{K}$. When studying a given family of curves, we are concerned with the rational isomorphism types of the curves over $\overline{K}$ (with possible extra structure). The *space of moduli* is an abstract classification of these isomorphism types. We want to consider the equivalence relation on $C(g)$ given by rationally isomorphism (considering the additional structure) over $\overline{K}$. Such an equivalence relation is known as a *moduli problem*. The quotient set will be denoted by $\mathbb{M}_g$. We need to put some algebraic structure on $\mathbb{M}_g$ in order to call this set the moduli space for the moduli problem.

There is a purely algebraic construction of $\mathbb{M}_g$ in terms of *geometric invariant theory*. The idea can be summarized as follows: given $m \in \mathbb{N}$ with $m \geq 3$, any smooth curve C of genus g can be embedded over $\overline{K}$ as a smooth curve of degree $2(g-1)m$ in $\mathbb{P}^n$, where $n = (2m-1)(g-1) - 1$. Therefore, we attach to C such an embedding $\phi\colon C \to \mathbb{P}^n$. The family of pairs (C, ϕ) can be parametrized as a set $\mathcal{K}$. Moreover, $PGL(n+1, \overline{K})$ acts continuously on $\mathcal{K}$ and ϕ is determined uniquely modulo the action of $PGL(n+1, \overline{K})$ on $\mathcal{K}$. We are hence interested in the collections of orbits under the group G of rational isomorphisms over $\overline{K}$.

It need not be the case that all orbits are closed. If this were the case, we would consider $\mathbb{M}_g$ to be the quotient space of $\mathcal{K}$ modulo the action of G and say that the moduli problem has a *fine moduli space*. This would mean

that every orbit of smooth curves of genus g could be mapped to one and only one point of $\mathbb{M}_g$, which would then happen to be an abstract variety of dimension $3g-3$ defined over the prime field of $\overline{K}$. Unfortunately, the moduli problem for all smooth curves of genus g (with no extra structure) has no fine moduli space.

Suppose therefore that an orbit X is not closed. Then, when considering the quotient space $\mathbb{M}_g$, the set X and its closure will be identified. The techniques of geometric invariant theory show that there is a natural way to *remove* non-closed orbits and obtain a quotient set $\mathbb{M}_g$, which is an open subset of a projective variety defined over the prime field of $\overline{K}$. There exists a natural compactification (which will also be denoted by $\mathbb{M}_g$) of this set. For the moduli problem for all smooth curves of genus g, this compactification is irreducible of dimension $3g-3$ as a variety. Moreover, if we accidentally removed a closed orbit at the beginning, and then considered the correspondent quotient set, there is a point in the compactification which corresponds to that orbit. The variety $\mathbb{M}_g$ is a *coarse moduli space* for the moduli problem. The family of smooth curves of genus g over K has a coarse moduli space.

Note. *If a coarse moduli space exists, then it is unique up to rational isomorphism. This discussion can be also applied to some specific collection of smooth curves of genus g and then we refer to the coarse (resp. fine) moduli space for this collection.*

Recall that if C is a curve of genus g defined over a small subfield F of $\overline{K}$, the modulus of C is rational over the algebraic closure of F in $\overline{K}$.

By an *elliptic curve* over K, we understand a pair (E,O) consisting of a projective nonsingular curve E of genus 1 defined over K and a distinguished K-rational point O. Such a curve E is rationally isomorphic over K to one given by a *Weierstrass equation* over K mapping O to $[0,0,1]$. Hence, we will drop the mention of O when referring to the elliptic curve E. According to the Weierstrass equation, there are two cases to consider (Appendix A in [24]):

- $y^2+xy=x^3+a_2x^2+a_6$. Let us call the quantity $j=a_6^{-1}\neq 0$ the *j-invariant* of the curve. Any other elliptic curve E' over $\overline{K}$ which is isomorphic to E over $\overline{K}$ is obtained after a change of variables of the form:
$$x=x'$$
$$y=y'+sx'$$

with s in $\overline{K}$ such that $s^2 + s + a_2 + a_2' = 0$. Note that $j = j'$.

- $y^2 + a_3 y = x^3 + a_4 x + a_6$ with $j = 0$. In this case, the changes of variables preserving the $\overline{K}$-isomorphism class of E are of the form:

$$\begin{aligned} x &= u^2 x' + s^2 \\ y &= u^3 y' + u^2 s x' + t \end{aligned}$$

with u, s and r in $\overline{K}$ such that:

$$\begin{aligned} u^3 &= a_3/a_3' \\ s^4 + a_3 s + a_4 - u^4 a_4' &= 0 \\ t^2 + a_3 t + s^6 + a_4 s^2 + a_6 - u^6 a_6' &= 0 \end{aligned}$$

It follows that two elliptic curves are rationally isomorphic over $\overline{K}$ if and only if they have the same j-invariant. Moreover, for any j in K, there is an elliptic curve defined over K whose j-invariant is K. That is, the space of moduli of elliptic curves over K is the affine line.

Let now g be an integer $g \geq 2$, and C a curve of genus g. Via the canonical linear system (*i.e* the effective divisor on the curve equivalent to the canonical divisor), we obtain the canonical map. We say that V is hyperelliptic if this map is not injective. Hence, it defines a non-constant morphism of degree 2 from C onto a smooth rational curve. Since K is perfect, we may assume that such a smooth rational curve is $\mathbb{P}^1$ (The 2-torsion part of $\mathrm{Br}(K)$ is trivial). Hence, we have a separable 2-cover $\phi\colon C \to \mathbb{P}^1$.

By *Artin-Schreier theory*, such a curve is a smooth model for an affine equation of the form $y^2 + y = w$ where w is a rational function over K. By [5] we may assume it is written in *Artin-Schreier special form*, that is, all irreducible factors of the denominator of w occur with odd multiplicity and $\deg(w)$ is either positive and odd or negative. Thus, the equation can be rewritten as $y^2 + y = \lambda \frac{r}{s^2 t}$, with λ in K, and r, s and t monic polynomials over K with t square-free. Such an equation is called a *normal model* for a hyperelliptic curve. We rewrite the above equation as $y^2 + vy = u$ where $u = tr$ is monic and $v = (\sqrt{\lambda})^{-1} st$ (note that by assumption any irreducible divisor of v is a simple divisor of u). According to the (*possible*) ramification of the cover over the point at infinity (by the Hurwitz' formula), we obtain the following classification ([5]):

If $\deg(w)$ is non-positive (the point at infinity is not ramified), then we

have that $\deg(v) = g+1$. Since $\deg(w) \leq 0$, we conclude that $\deg(u) \leq 2g+2$.

If $\deg(w)$ is odd positive, the point at infinity is ramified. Hence $\deg(u) = 2g+1$ and $\deg(v) \leq g$. The function field extension is *imaginary*.

Given a hyperelliptic curve C over K, a point P in $\mathbb{P}^1$ is a *branch point* if ϕ ramifies at the preimage of P in C. In the case of characteristic 2, the branch points are the poles of the rational form w (plus ∞ in the imaginary case). There are at most $g+1$ branch points.

As in the case of characteristic different from 2, the family of hyperelliptic curves of genus g over a field K admits a coarse moduli space $\mathbb{T}_g$, which is a rational variety over K of dimension $2g-1$ (see [1]). Note that in this case, the class of rational isomorphism in $\overline{K}$ of a hyperelliptic curve is not uniquely determined by the set of branch points modulo $PGL(2, \overline{K})$, since we have to consider also transformations of the form $x = x'$, $y = y + b(x')$ for b in $\overline{K}[x]$ (the cover has non-trivial involutions). From [1] we obtain a nice description of $\mathbb{T}_g$ as follows:

Let $H^0(\mathbb{P}^1, \mathcal{O}(m))$ denote the set of homogeneous forms over K of degree m in 2 variables. Then, $\mathbb{T}_g$ is isomorphic to:

$$H^0(\mathbb{P}^1, \mathcal{O}(g+1)) \times H^0(\mathbb{P}^1, \mathcal{O}(2g+2))$$

modulo the action of $(K^* \ltimes H^0(\mathbb{P}^1, \mathcal{O}(g+1))) \times PGL(2, \overline{K})$, where we define

$$(a, b) \otimes (v, u) = (bv, b^2u + bav + a^2)$$

for b in K^*, a in $H^0(\mathbb{P}^1, \mathcal{O}(g+1))$ and (v, u) in $H^0(\mathbb{P}^1, \mathcal{O}(g+1)) \times H^0(\mathbb{P}^1, \mathcal{O}(2g+2))$. The action of $PGL(2, \overline{K}) = \mathrm{Aut}(\mathbb{P}^1)$ on $H^0(\mathbb{P}^1, \mathcal{O}(g+1)) \times H^0(\mathbb{P}^1, \mathcal{O}(2g+2))$ is the natural one.

An equivalence class (v, u) in the above quotient set is identified with the pair of polynomials defining the curve dehomogenizing them with respect to the second variable. As shown above, the branch points determine the degree of v. Since $\dim_K H^0(\mathbb{P}^1, \mathcal{O}(m)) = m+1$, and denoting by $\mathbb{T}_g^{(r)}$ the set of modulus of hyperelliptic curves with at most r branch points, we deduce that, for $3 \leq r \leq g+1$, we have that $\dim_K \mathbb{T}_g^{(r)} = (2g+3) + (r+1) - (1+g+2) - 3 = g + r - 2$. Note that $\mathbb{T}_g^{(r)}$ is closed in $\mathbb{T}_g$.

2 Results

The same assumptions as in the previous sections hold here. In order to prove the theorem, we will divide it into two cases, depending whether the

curve is elliptic or hyperelliptic.

Theorem 2.1. *Let E an elliptic curve defined over K with j-invariant j s-generic over $\emptyset$, or $j = 0$. Then E has a K-rational point s-generic over the set of parameters defining E.*

Remark 2.2. Since the family of elliptic curves has a coarse moduli space isomorphic to $\mathbb{A}^1$, it makes sense to talk about s-generic points in the moduli space. In this case, s-generic and generic in the sense of Model Theory coincide.

Proof. We first consider the case of generic j-invariant. Take a *Weierstrass equation* for E of the form $E : y^2 + xy = x^3 + ax^2 + b$.

In this case $j = b^{-1}$, hence b is also generic over $\emptyset$. Consider the transformation $x = x'$, $y = x'y'$. It puts the equation in the form $y^2 + y + a = \frac{x^3+b}{x^2}$.

Take now λ in K generic over a independent from b and define $e = \frac{b}{\lambda^3}$. By properties of generics, e is also generic and independent from λ over $\{a\,,\,b\}$. Considering the transformation $x = \lambda x'$ and renaming, we obtain an equation of the form $y^2 + y + a = \lambda\frac{x^3+e}{x^2}$. Choose a small model N containing the parameters $\{e\,,a\,,b\}$ and some u generic over N. Define $p = \mathrm{Lstp}(\frac{u^3+e}{u^2}/N)$ and $q = \mathrm{Lstp}(\lambda/N)$.

The additive subgroup $H_1 = \langle w^2 + w \mid w \in K\rangle$ is definable over $\emptyset$ and of finite index in K^+ (since H_1 contains a generic element). By Lemma 2.4 in [17], there is a generic Lascar strong type r over N in $C_1 \cap (a + H_1)$, where $C_1 = C_N(p) \cdot C_N(q)$ in $K^*/(K^*)_N$ (recall notation from [17]). By Lemmas 2.3 in [17], there are x and y in K generic elements over $N \cup \{\lambda\}$ such that $\frac{x^3+e}{x^2}$ realizes p and $y^2+y+a = \lambda\frac{x^3+e}{x^2}$ holds (after applying automorphisms). We obtain hence a K-rational point in E s-generic over $\{a\,,\,b\}$.

We now consider the case $j = 0$. A *Weierstrass equation* for E is of the form $E : y^2+ay+b = x^3+cx$. We choose u , t and s in K generic independent over $\{a\,,\,b\,,\,c\}$ and define

$$a' = au^{-3} \qquad b' \;= u^{-6}(t^2 + at + s^6 + cs^2 + b) \qquad c' = u^{-4}(s^4 + as + c)$$

The transformation

$$x = u^2x' + s^2 \qquad y = u^3y' + u^2sx' + t$$

maps E to $E' : y^2 + a'y + b' = x^3 + c'x$. Since $(a'\,,\,b'\,,\,c')$ and $(s\,,\,u\,,\,t)$ are interalgebraic over $\{a\,,\,b\,,\,c\}$, the curve E' is defined over K with generic

independent coefficients over $\emptyset$. Hence, we may assume E already was.

The field K is perfect, so there is some λ in K with $c = \lambda^2$. The transformation $x = x'\lambda$ puts the equation in the form $y^2 + ay + b = \lambda^3(x^3 + x)$, where λ is generic independent from $\{a\,,\,b\}$ over $\emptyset$ (because c already was). Again, $H_1 = \langle w^2 + aw \mid w \in K\rangle$ is an additive subgroup definable over $\{a\}$ of finite index. Choose d in K generic over $\{a\,,\,b\}$, and define $p = \mathrm{Lstp}(\lambda^3/\{a\,,\,b\})$ and $q = \mathrm{Lstp}(d^3 + d/\{a\,,\,b\})$. As in the previous case, there are x and y in K generic over $\{a\,,\,b,\,\lambda\}$ such that $x^3 + x$ realizes q, $y^2 + ay + b$ lies in $H_1 + b$, and $y^2 + ay + b = \lambda^3(x^3 + x)$ holds (possibly after applying automorphisms of $\mathcal{M}$). We obtain in this fashion a K-rational point for E which is s-generic over the set of parameters defining E. □

We observe that properties of generics were strongly used in order to go from a given equation to one with generic independent coefficients. It makes one guess that the PAC-conjecture may not hold, since it is not clear to us how to apply the above arguments to the more general case, where the j-invariant (or the modulus, in the next proof) is non-generic. In the case of hyperelliptic curves, the role of the ordinal-valued SU-rank will become more evident. Throughout the proof, we use a weight on types already stated in [17]. We assume $SU(K) = \omega^\alpha\, n$ for some ordinal α and some n in $\mathbb{N}$. Let p be an m-type over A. We write $w(p) = r$ if $SU(p) = \omega^\alpha\, r + \beta$ with $\beta < \omega^\alpha$. We write $w(\vec{a}/A)$ for $w(tp(\vec{a}/A))$. If a is a single element, then $w(a/A) = n$ if and only if a is generic over A in K in the sense of Model Theory. By Lascar inequalities, we have $w(\vec{a}\vec{b}/A) = w(\vec{a}/A\vec{b}) + w(\vec{b}/A)$.

We have the following:

Theorem 2.3. *Let F be a small subfield of K and C a hyperelliptic curve defined over F with s-generic* modulus $m(C)$ *in $\mathbb{T}_g$ over $\emptyset$. Then C has a K-rational solution s-generic over F.*

Proof. The proof goes again by finding an appropriate transformation defined over K preserving the modulus of the curve and mapping C to another curve defined over K with generic independent coefficients over $\emptyset$. We then use the Lemmas of [17] in order to find an s-generic solution for C over F. We treat the transformations separately according to the degree of the form defining C.

Form of positive degree. The curve C has an equation of the form $y^2 + v(x)y = u(x)$, where u is a monic polynomial over F of degree $2g + 1$ and v is also a polynomial over F of degree at most g. Since $m(C)$ is s-generic, it is also

generic in the sense of Algebraic Geometry. Hence, it lies on $\mathbb{T}_g \setminus \mathbb{T}_g^{(g)}$, the non-empty open set of the moduli space of hyperelliptic curves corresponding to curves with exactly $g+1$ branch points. Hence $\deg(v) = g$ (since ∞ is ramified so we are fixing one of the branch points). We will consider transformations preserving the rational isomorphism class of C and fixing the point of infinity.

Let $\vec{u}$ and $\vec{v}$ denote the tuples of the coefficients of the polynomials defining C. Consider now $\lambda\,,\ \mu\,,\ r\,,\ a_0, \ldots, a_{\deg(v)}$ in K generic independent over F and define $A(x) = \sum_{i=0}^{\deg(v)} a_i x^i$. The transformation:

$$(x, y) \to \left(\lambda x + \mu, r^{-1}\lambda^{\deg(v)}(y + A(x))\right)$$

determines a rational isomorphism defined over K between C and the curve

$$C' : y^2 + yr\tilde{v}(x) = \lambda^{\deg(u)-2\deg(v)} r^2 \tilde{u}(x) + A^2(x) + A(x)r\tilde{v}(x) \qquad (2.1)$$

We have that C' is another hyperelliptic curve defined over K. Suppose that $\{\alpha_i\}_{1\leq i\leq \deg(v)}$ and $\{\beta_j\}_{1\leq j\leq \deg(u)}$ are the zeroes of u and v, and likewise $\{\tilde{\alpha}_i\}_{1\leq i\leq \deg(v)}$ and $\{\tilde{\beta}_j\}_{1\leq j\leq \deg(u)}$ the zeroes of $\tilde{u}$ and $\tilde{v}$ (all of them lying in some algebraic extension of K). Hence, we have that $\tilde{\alpha}_i = (\alpha_i - \mu)/\lambda$ and $\tilde{\beta}_j = (\beta_j - \mu)/\lambda$ for $1 \leq i \leq \deg(v)$ and $1 \leq j \leq \deg(u)$.

Write the above equation for C' as $y^2 + yv'(x) = u'(x)$. Let now $\vec{u}'$ and $\vec{v}'$ denote the tuples of coefficients of the polynomials $u'\,,\ v'$.

By construction, $m(C) = m(C')$ is rational over $\vec{v}', \vec{u}'$.

Claim The tuple $(\vec{v}'\vec{u}')$ is s-generic over $\emptyset$.

Proof of the claim. This is a weight argument as in [17]. Since $m(C)$ is s-generic over $\emptyset$ in the moduli space, which has dimension $2g-1$, we have that $w(m(C)) = n(2g-1)$.

Subclaim The tuple $(\mu, \lambda, r, a_0, ..., a_{\deg(v)})$ is interalgebraic with $(\vec{v}', \vec{u}')$ over $\vec{u}, \vec{v}$.

Proof of the subclaim. We need only check that $\lambda, \mu, r, a_0, ..., a_{\deg(v)}$ lie in $\mathrm{acl}(\vec{u}'\vec{v}'/\vec{u}, \vec{v})$. The zeroes of v' are $\tilde{\alpha_1}, \ldots, \tilde{\alpha}_{\deg(v)}$ (which are interalgebraic, as a tuple, with the tuple of its coefficients, being the latter the symmetric functions on the former set). Since $\deg(v) \geq 2$, this tuple is interalgebraic with the pair (λ, μ) over the coefficients of v. Now, it follows that r is in $\mathrm{acl}(\vec{u}', \vec{v}', \lambda, \mu/\vec{u}, \vec{v})$. Comparing the right hand side of (2.1), we conclude that $\vec{a}$ is in $\mathrm{acl}(\vec{u}', \vec{v}', \lambda, \mu, r/\vec{u}, \vec{v})$.

End of the proof of the subclaim.

By Lascar inequalities, we have:

1. $w(\vec{u}\vec{v}\,\vec{u}'\vec{v}') = w(\vec{u}'\vec{v}'/\vec{u}\vec{v}) + w(\vec{u}\vec{v}) \overset{\text{subclaim}}{=} w(\lambda, \mu, r, a_0, ..., a_{\deg(v)}/\vec{u}\vec{v}) + w(\vec{u}\vec{v}) = (2 + 1 + \deg(v) + 1)n + w(\vec{u}\vec{v}) = (4 + \deg(v))n + w(\vec{u}\vec{v}) = (4+\deg(v))n+w(\vec{u}\vec{v}/m(C))+w(m(C)) = (4+\deg(v))n+w(\vec{u}\vec{v}/m(C))+(2g-1)n = (2g+3+\deg(v))n + w(\vec{u}\vec{v}/m(C))$.

2. $w(\vec{u}\vec{v}\,\vec{u}'\vec{v}') = w(\vec{u}\vec{v}/\vec{u}'\vec{v}') + w(\vec{u}'\vec{v}') \underset{m(C)\in\text{acl}(\vec{u}'\vec{v}')}{\leq} w(\vec{u}\vec{v}/m(C)) + w(\vec{u}'\vec{v}')$.

Thus, $w(\vec{u}'\vec{v}') \geq (2g + 3 + \deg(v))n$. Since $(\vec{u}'\vec{v}')$ is a $(2g + 3 + \deg(v))$-tuple, we have that it is an s-generic tuple over $\emptyset$ (note that after applying the transformation u' need no longer be monic).
End of the proof of the claim.
Form of degree 0. Let C come in a normal form as $y^2 + v(x)y = u(x)$ with u and v polynomials with coefficients in F such that $\deg(u) = 2g + 2$ and $\deg(v) = g + 1$. We take a , b , c and d in K defining an s-generic element in $SL(2, K)$ over F (that is, $ad-bc = 1$, and a , b and c are generic independent over F). We choose also λ , $a_0, \ldots, a_{\deg(v)}$ in K generic independent from $\{a\,,\, b\,,\, c\}$ over F and define $A(x) = \sum_{i=0}^{\deg(v)} a_i x^i$.

Consider the following transformation:

$$(x, y) \to \left(\frac{ax + b}{cx + d}, \lambda^{-1}(y + A(x))(\frac{c}{cx + d})^{\deg(v)}\right)$$

This transformation is defined over K and it maps C to the curve:

$$C' : y^2 + y\lambda v(\frac{a}{c})\tilde{v}(x) = \lambda^2 u(\frac{a}{c})\tilde{u}(x) + A(x)^2 + A(x)\lambda v(\frac{a}{c})\tilde{v}(x) \qquad (2.2)$$

Suppose that $\{\alpha_i\}_{1\leq i\leq \deg(v)}$ and $\{\beta_j\}_{1\leq j\leq \deg(u)}$ are the zeroes of u and v and likewise, $\{\tilde{\alpha_i}\}_{1\leq i\leq \deg(v)}$ and $\{\tilde{\beta}_j\}_{1\leq j\leq \deg(u)}$ the zeroes of $\tilde{u}$ and $\tilde{v}$ (in some algebraic extension of K). Then, we have that $\tilde{\alpha_i} = \frac{d\alpha_i - d}{a - c\alpha_i}$ and $\tilde{\beta}_j = \frac{d\beta_j - b}{a - c\beta_j}$, for $1 \leq i \leq \deg(v)$ and $1 \leq j \leq \deg(u)$. The curve C' is also hyperelliptic and defined over K.

Rewrite the above equation for C' as $y^2 + yv'(x) = u'(x)$. Let $\vec{u}$ and $\vec{v}$ (resp. $\vec{u}'$ and $\vec{v}'$) denote the tuples of coefficients of the polynomials u and v (resp. u' and v'). Again, the modulus of the curve $m(C) = m(C')$ is rational

over $\vec{v}'\vec{u}'$.

Claim The tuple $(a\,,\,b\,,\,c\,,\,\lambda\,,\,a_0,\ldots,a_{\deg(v)})$ is interalgebraic with $(\vec{v}'\vec{u}')$ over $\vec{u}\vec{v}$.

Proof of the claim. We need only prove that $a\,,\,b\,,\,c\,,\,\lambda\,,\,a_0,\ldots,a_{\deg(v)}$ lie in $\mathrm{acl}(\vec{u}'\vec{v}'/\vec{u}\vec{v})$. The tuple of zeroes of v' (which is interdefinable with the tuple of its coefficients) coincides with the tuple of zeroes of $\tilde{v}$. Since $\deg(v)\geq 3$, this tuple is interalgebraic with the tuple $(a\,,\,b\,,\,c)$ over $\vec{v}$, because any element of $SL(2,K)$ is determined by the image of three points in the projective space. Now, $\lambda\,,\,a_0,\ldots,a_{\deg(v)}$ lie in $\mathrm{acl}(\vec{u}',\vec{v}',a,b,c/\vec{u},\vec{v})$ by a similar argument as in the imaginary case.

End of the proof of the claim.

Claim The tuple $(\vec{v}'\vec{u}')$ is s-generic over $\emptyset$.

Proof of the claim. By Lascar inequalities, we have

1. $w(\vec{u}\vec{v}\,\vec{u}'\vec{v}') = w(\vec{u}'\vec{v}'/\vec{u}\vec{v}) + w(\vec{u}\vec{v}) \overset{\text{claim}}{=} w(a,b,c,\lambda,a_0,...,a_{\deg(v)}/\vec{u}\vec{v}) + w(\vec{u}\vec{v}) = (3+1+\deg(v)+1)n + w(\vec{u}\vec{v}) = (5+\deg(\vec{v}))n + w(\vec{u}\vec{v}) = (5+\deg(v))n+w(\vec{u}\vec{v}/m(C))+w(m(C)) = (5+\deg(v))n+w(\vec{u}\vec{v}/m(C))+(2g-1)n = (2g+4+\deg(v))n + w(\vec{u}\vec{v}/m(C))$.

2. $w(\vec{u}\vec{v}\,\vec{u}'\vec{v}') = w(\vec{u}\vec{v}/\vec{u}'\vec{v}') + w(\vec{u}'\vec{v}') \underset{m(C)\in acl(\vec{u}'\vec{v}')}{\leq} w(\vec{u}\vec{v}/m(C)) + w(\vec{u}'\vec{v}')$.

Thus, $w(\vec{v}'\vec{u}')\geq(2g+4+\deg(v))n$. Being the length of $(\vec{v}'\vec{u}')$ exactly $2g+4+\deg(v)$, we conclude that $(\vec{v}'\vec{u}')$ is an s-generic tuple.

End of the proof of the claim.

Form of negative degree. In this case, C has a normal equation of the form $y^2+v(x)y=u(x)$, where u is a monic polynomial of degree at most $2g+1$ and v is a polynomial of degree $g+1$ both with coefficients in F.

Since $m(C)$ is generic in the sense of Algebraic Geometry, it lies on the open set $\mathbb{T}_g\setminus\mathbb{T}_g^{(g)}$ of moduli of hyperelliptic curves with exactly $g+1$ *distinct* branch points. The zero set of v is contained in the zero set of u (*without counting multiplicities*), therefore we have that $deg(u)\geq g+1$.

We take $a\,,\,b\,,\,c$ and d in K defining an s-generic element in $SL(2,K)$ over F (that is, $ad-bc=1$ and $a\,,\,b$ and c are generic independent over F). We choose also $\lambda\,,\,a_0,\ldots,a_{\deg(u)-g-1}$ in K generic independent from $\{a\,,\,b\,,\,c\}$ over F and define $A(x)=\sum_{i=0}^{\deg(u)-g-1}a_ix^i$.

Consider the following transformation:

$$(x,y) \to \left(\frac{ax+b}{cx+d}, \lambda^{-1}(y+A(x))(\frac{c}{cx+d})^{g+1} \right)$$

This transformation is defined over K and it maps C to the curve:

$$C' : y^2 + y\lambda v(\frac{a}{c})\tilde{v}(x) = \lambda^2 u(\frac{a}{c})\tilde{u}(x)(\frac{cx+d}{c})^{2g+2-\deg(u)} + A(x)^2 + A(x)\lambda v(\frac{a}{c})\tilde{v}(x) \quad (2.3)$$

Suppose that $\{\alpha_i\}_{1\leq i\leq \deg(v)}$ and $\{\beta_j\}_{1\leq j\leq \deg(u)}$ are the zeroes of u and v, and likewise $\{\tilde{\alpha_i}\}_{1\leq i\leq \deg(v)}$ and $\{\tilde{\beta_j}\}_{1\leq j\leq \deg(u)}$ the zeroes of $\tilde{u}$ and $\tilde{v}$) (in some algebraic extension of K). We have that $\tilde{\alpha_i} = \frac{d\alpha_i - b}{a - c\alpha_i}$ and $\tilde{\beta_j} = \frac{d\beta_j - b}{a - c\beta_j}$, for $1 \leq i \leq \deg(v)$ and $1 \leq j \leq \deg(u)$. The curve C' is also hyperelliptic and defined over K.

Rewrite the above equation for C' as $y^2 + yv'(x) = u'(x)$. Let $\vec{u}$ and $\vec{v}$ (resp. $\vec{u'}$ and $\vec{v'}$) denote the tuples of coefficients of the polynomials u and v (resp. u' and v'), respectively. As in the previous cases, the modulus of the curve $m(C) = m(C')$ is rational over $\vec{v'}\vec{u'}$.

Claim The tuple $(a\,,\,b\,,\,c\,,\,\lambda\,,\,a_0,\ldots,a_{\deg(u)-g-1})$ is interalgebraic with $(\vec{v'}\vec{u'})$ over $\vec{u}\vec{v}$.

Proof of the claim. The tuple of zeroes of v' (which is interdefinable with $\vec{v'}$) coincides with the tuple of zeroes of $\tilde{v}$, and this one is interalgebraic with the tuple (a,b,c,d) over $\vec{v}$ (tracing back the transformation), since $\deg(v) \geq 3$ (any element of $\mathrm{SL}(2,\mathrm{K})$ is determined by its action on three different points in $\mathbb{P}^1$). Now, it is clear that λ is in $\mathrm{acl}(\vec{u'},\vec{v'},a,b,c,d/\vec{u},\vec{v})$. Comparing the right hand of the equation (2.3), we also conclude that $a_0,\ldots,a_{\deg(u)-g-1}$ lie in $\mathrm{acl}(\vec{u'},\vec{v'},a,b,c,d,\lambda/\vec{u},\vec{v})$.

End of the proof of the claim.

By Lascar inequalities, we have:

1. $w(\vec{u}\vec{v}\,\vec{u'}\vec{v'}) = w(\vec{u'}\vec{v'}/\vec{u}\vec{v}) + w(\vec{u}\vec{v}) = w(a,b,c,d,\lambda,a_0,\ldots,a_{\deg(u)-g-1}/\vec{u}\vec{v}) + w(\vec{u}\vec{v}) = (3+1+\deg(u)-g-1+1)n + w(\vec{u}\vec{v}) = (4+\deg(u)-g)n + w(\vec{u}\vec{v}) = (4+\deg(u)-g)n + w(\vec{u}\vec{v}/m(C)) + w(m(C)) = (4+\deg(u)-g)n + w(\vec{u}\vec{v}/m(C)) + (2g-1)n = (3+\deg(u)+g)n + w(\vec{u}\vec{v}/m(C)$.

2. $w(\vec{u}\vec{v}\,\vec{u'}\vec{v'}) = w(\vec{u}\vec{v}/\vec{u'}\vec{v'}) + w(\vec{u'}\vec{v'}) \leq w(\vec{u}\vec{v}/m(C)) + w(\vec{u'}\vec{v'})$.

Thus, $w(\vec{v}'\vec{u}') \geq (g+3+\deg(u))n$. Since $(\vec{v}'\vec{u}')$ is a $(g+2+\deg(u)+1)$-tuple, we have that it is an s-generic tuple over $\emptyset$ (again by Lascar inequalities).

Therefore, we are reduced to proving the statement of the theorem for a hyperelliptic curve C defined over K with generic independent coefficients over $\emptyset$ (note that, after the transformations, we do not assume that u or v are monic). Consider the equation $y^2 + y = u(x)/v(x)^2$ and, after dividing (*if necessary*), we may assume it is of the form $y^2 + y + a = u(x)/v(x)^2$ for some a in K, with $\deg(u) \neq 2\deg(v)$.

Take λ in K generic over $F \cup \{\vec{u}\,,\, \vec{v}\}$ (recall previous notation). After the transformation $(x, y) \to (\lambda x, y)$, we obtain an equation of the form:

$$y^2 + y + a = \lambda^{\deg(u)-2\deg(v)} \frac{u'(x)}{v'(x)^2}$$

where

$$u'_i = u_i \lambda^{i-\deg(u)} \qquad v'_j \;\; = v_j \lambda^{j-\deg(v)}$$

Again, λ is generic over $F \cup \{\vec{u}'\,,\, \vec{v}'\}$ by properties of generics. Consider now a small model N containing $F \cup \{\vec{u}'\,,\, \vec{v}'\}$ independent from λ. We define $p(x) = \mathrm{Lstp}(\lambda^{\deg(u)-2\deg(v)}/N)$ and $q(x) = \mathrm{Lstp}(\frac{u'(s)}{v'(s)^2}/N)$, with s in K generic over N.

The additive subgroup $H_1 = \langle w^2 + w \mid w \in K \rangle$ is definable over $\emptyset$ and has finite index (because it contains a generic element). By Lemma 2.4 in [17], there is a generic Lascar strong type r over N in $C_1 \cap (a + H_1)$, where $C_1 = C_N(p) \cdot C_N(q)$ in $K^*/(K^*)_N$. Apply Lemma 2.3 in [17] to p, q and r to find x and y in K generic over $N \cup \lambda$ (possibly after N-automorphisms) such that $y^2 + y + a$ realizes r, the element $u'(x)/v'(x)^2$ is a realization of q and $y^2 + y + a = \lambda^{\deg(u)-2\deg(v)} \frac{u'(x)}{v'(x)^2}$ holds. We therefore obtain a K-rational point in C which is s-generic over F. □

Remark 2.4. Let $r \geq 3$. For imaginary hyperelliptic curves defined over K, an s-generic point over $\emptyset$ in $\mathbb{T}_g^{(r)}$=$\{$ moduli of hyperelliptic curves of genus g with at most r branch points$\}$ (as a closed subvariety of the moduli space of hyperelliptic curves of genus g) determines an equation for C where $\deg(u) = 2g+1$ and $\deg(v) = r-1$ (since ∞ is ramified, we fix it). We may proceed as in the above proof in the imaginary case, and apply a generic transformation using now $(2 + (g-2))$ generic independent parameters. Since $\deg(v) =$

$r-1 \geq 2$, we conclude that the new tuple of coefficients is interalgebraic with these parameters over the previous tuple of coefficients. Via the same weight argument as in the previous case (recall that $\dim(\mathbb{T}_g^{(r)}) = g+r-2$), we conclude that the new $(2g+r+2)$-tuple of coefficients is s-generic over $\emptyset$ and the above proof follows.

Therefore, we conclude the following:

Corollary 2.5. *Suppose K has characteristic 2. Let F be a small subfield of K and C an imaginary hyperelliptic curve of genus g defined over F whose modulus is s-generic over $\emptyset$ in $\mathbb{T}_g^{(r)}$ for some $r \geq 3$. Then, C has a K-rational point s-generic over F.*

Remark 2.6. The same arguments exhibited here can be in principle applied to cyclic covers of the projective line of degree p (a prime different from 2). Unfortunately, in order to apply *Kummer* theory, we need p-roots of unity in K (which need not be the case). We could assume K has a primitive p-root of unity, by going to a finite algebraic extension L of K (which is interpretable in K via a basis, and hence, *supersimple*). Two questions come up naturally:

- If we find L-rational s-generic points in the cover, can we conclude that there are K-rational s-generic points?
- There is a coarse moduli space of such covers (the moduli space is called *space of Hurwitz*, see [4]). What is its dimension? Moreover, what are the invariants of the cover (for example: the set of branch points modulo $PGL(2, \overline{K})$, etc...)? (This is needed to study the transformations).

Acknowledgements. The author wants to thank the referee for useful remarks in editing this article.
Many thanks are also due to the University of Illinois at Urbana-Champaign, especially the Logic group for its support and guidance.

References

[1] U. Boshle. Pencils of quadrics and hyperelliptic curves in characteristic 2. *Journal für die reine und angewandte Mathematik*, 407:75–98, 1990.

[2] E. Bouscaren, editor. *Model Theory and Algebraic Geometry: an introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture*, volume 1696 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Germany, 1998.

[3] Z. Chatzidakis, L. van den Dries, and A. Macintyre. Definable sets over finite fields. *Journal für die reine und angewandte Mathematik*, 427:107–135, 1992.

[4] M. Emsalem. Spaces of hurwitz. *Séminaires & Congrès*, 5:63–99, 2001.

[5] A. Enge. How to distinguish hyperelliptic curves in even characteristic. In *Public Key Cryptography and Computational Number Theory*, pages 49–58. de Gruyter, Berlin, Germany, 2001.

[6] M. Fried and M. Jarden. *Field Arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete, 3te Folge*. Springer-Verlag, Berlin, Germany, 1986.

[7] L. Gatto. *Intersection Theory on Moduli Spaces of Curves*, volume 61 of *Monografías de matemática*. Instituto de matemática Pura e Aplicada, Rio de Janeiro, Brasil, 2000.

[8] J. Harris and I. Morrison. *Moduli of Curves*, volume 187 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Germany, 1998.

[9] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Germany, 1977.

[10] E. Hrushovski. Pseudofinite fields and related structures. preprint, 1992.

[11] B. Kim and A. Pillay. Simple theories. *Annals of Pure and Applied Logic*, 88:149–164, 1997.

[12] B. Kim and A. Pillay. From stability to simplicity. *Bulletin of Symbolic Logic*, 4:17–36, 1998.

[13] D. Lorenzini. *An Invitation to Algebraic Geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Rhode Island, USA, 1996.

[14] A. Macintyre. On ω_1-categorical theories of fields. *Fundamenta Mathematicae*, 71:1–25, 1971.

[15] D. Marker. *Model Theory: an introduction*, volume 217 of *Graduate Texts Mathematics*. Springer, Berlin, Germany, 2000.

[16] A. Martin-Pizarro. *Algebraic Curves over Supersimple Fields*. PhD thesis, University of Illinois at Urbana-Champaign, Urbana-Champaign, IL, USA, dec 2003.

[17] A. Martin-Pizarro and A. Pillay. Elliptic and hyperelliptic curves over supersimple fields, 2003. To appear.

[18] R. Miranda. *Algebraic Curves and Riemann Surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Rhode Island, USA, 1995.

[19] A. Pillay. Definability and definable groups in simple theories. *Journal of Symbolic Logic*, 63:788–796, 1998.

[20] A. Pillay and B. Poizat. Corps et chirurgie. *Journal of Symbolic Logic*, 60:528–533, 1995.

[21] A. Pillay, T. Scanlon, and F. Wagner. Supersimple fields and division rings. *Mathematics Research Letters*, 5:473–483, 1998.

[22] S. Shelah. Stability, the f.c.p. and superstability; model theoretic properties of formulas in first-order theories. *Annals of Mathematical Logic*, 3:271–362, 1971.

[23] S. Shelah. Simple unstable theories. *Annals of Mathematical Logic*, 19:177–203, 1980.

[24] J.H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Germany, 1986.

[25] F.O. Wagner. Groups in simple theories. preprint, 1997.

[26] F.O. Wagner. *Simple Theories*. Kluwer Academic Publishers, Dordrecht, The Nederlands, 2000.