Elliptic and hyperelliptic curves over supersimple fields

Amador Martin-Pizarro
University of Illinois at Urbana-Champaign

Anand Pillay*
University of Illinois at Urbana-Champaign

January 8, 2014

Abstract

We prove that if F is an infinite field with characteristic different from 2, whose theory is supersimple, and C is an elliptic or hyperelliptic curve over F with generic "modulus" then C has a generic F-rational point. The notion of generity here is in the sense of the supersimple field F.

1 Introduction and preliminaries

The archetypal example of a structure whose theory is uncountably categorical is an algebraically closed field $(K, +, \cdot)$. Among the starting points of stability-theoretic algebra was a converse to this. Macintyre proved [8] that an infinite field whose theory is uncountably categorical must be algebraically closed. The proof applied to the more general class of fields whose theory is totally transcendental, and was further generalized to the superstable case by Cherlin and Shelah [3].

*Partially supported by an NSF grants DMS-0070179 and DMS-0100979, and a Humboldt Foundation Research Award

Hrushovski [6], using work in [2] noticed that pseudofinite fields, although not uncountably categorical and not even stable, nevertheless have "good" stability-like properties: they have S_1-rank 1. He observed that the same is true for the more general class of "perfect, bounded, PAC fields". Here F is said to be bounded, if F has only finitely many finite extensions of degree n for each n, or equivalently if the absolute Galois group of F has only finitely many open subgroups of index n for each n. F is said to be PAC (standing for pseudo-algebraically closed) if every absolutely irreducible variety defined over F has an F-rational point.

In the meantime, Shelah's generalization of stability theory to the broader class of "simple theories" was completed by Kim and others. So in this language, Hrushovski had shown that perfect bounded PAC fields are supersimple (of SU-rank 1). This raised the issue of finding some kind of converse, in analogy with Macintyre's theorem. In [12] it was shown that supersimple fields are indeed perfect and bounded. So the remaining issue, raised explicitly in [7], is to prove that they are PAC. The PAC property is equivalent to demanding that the set of F-rational points of an absolutely irreducible variety over F is Zariski-dense. By [4] it is enough to look at the case where X is a curve over F (that is, a one-dimensional absolutely irreducible variety defined over F). In fact it suffices to prove that for any *smooth projective* curve C over F, $C(F)$ is Zariski-dense (that is infinite) in $C(\bar{F})$.

At this point we should say that we are not really sure whether the general conjecture (a supersimple field is PAC) is true.

Nevertheless the first general attack on the problem was in [13] where, among other things, the case of genus 0 curves was dealt with. In fact it was proved there that if F is supersimple then the Brauer group of every finite extension of F is trivial (so F has "cohomological dimension ≤ 1"). This implies that for any *rational* variety X defined over F, $X(F)$ is Zariski-dense. (By a rational variety we mean one which is birationally isomorphic over $\bar{F}$ to some $\mathbf{P}^n$.)

In the present paper we consider curves of higher genus. In fact we restrict our attention to elliptic and hyperelliptic curves. Our results are formulated using a model-theoretic notion of generic point, which we explain now. Let $F = (F, +, \cdot, ..)$ be an infinite field with possibly additional structure, whose theory is assumed to be supersimple. We will assume F to be saturated. The SU-rank of F is of the form $\omega^\alpha.m$ for some ordinal $\alpha \geq 0$ and integer $m \geq 1$. Let X be a variety defined over F of dimension d (as an algebraic

variety). Let k be a small subfield of F over which X is defined. We will say that $a \in X(F)$ is an s-generic point of X over k if $SU(tp(a/k)) = \omega^\alpha.md.$

The definition of a hyperelliptic curve often assumes the genus to be at least 2. As there are some other delicate issues, we will separate the elliptic and hyperelliptic cases. We assume F to be a perfect field, and sometimes assume its characteristic to be different from 2. By an elliptic curve C over F we mean a smooth projective (irreducible) curve of genus 1 defined over F, equipped with an F-rational point. The class of elliptic curves over $\bar{F}$ has a (coarse) moduli space M_1 which coincides with the affine line $\mathbf{A}^1$. This is the same as the moduli space of all curves of genus 1 over $\bar{F}$. For any genus 1 curve C over $\bar{F}$, $j(C)$, the j-invariant of C is the point on $\mathbf{A}^1(\bar{F}) = \bar{F}$ corresponding to C. If C is defined over F, $j(C) \in F$. If characteristic $\neq 2$, an elliptic curve over F can be written (in affine coordinates) as $y^2 = f(x)$ where f is a cubic monic polynomial over F with distinct roots (in $\bar{F}$).

By a hyperelliptic curve over a perfect field F we mean a smooth projective curve C of genus ≥ 2 defined over F such that over $\bar{F}$ there is a degree 2 map from C to $\mathbf{P}^1$. The class of hyperelliptic curves of genus g over $\bar{F}$ has again a coarse moduli space H_g defined over the prime field. H_g is an irreducible variety of dimension $2g-1$ which is moreover (by [1]) a *rational* variety. H_g is a subvariety of the moduli space M_g of *all* curves of genus g. M_g has dimension $3g-3$. So note that all curves of genus 2 are hyperelliptic. If C is hyperelliptic, then $m(C) \in H_g$ denotes the moduli of C; so if C is defined over F so is $m(C)$.

We will prove:

Theorem 1.1 *Let $F = (F, +, \cdot, ...)$ be a saturated supersimple field, with characteristic different from 2.*
(i) Let C be an elliptic curve over F. Let $k < F$ be a small field over which C is defined. Suppose that $j(C) \in F$ is either s-generic over k, or is equal to 0 or 128. Then C has an F-rational point which is s-generic over k.
(ii) Let C be a hyperelliptic curve of genus $g \geq 2$ over F, defined again over a small subfield $k < F$. Assume that $m(C) \in H_g(F)$ is s-generic over k. Then $C(F)$ has a point which is s-generic over k.

It follows from (ii) that if C is a curve of genus 2 defined over supersimple F with $m(C) \in M_2(F)$ an s-generic point of the moduli space of all curves of genus 2, then $C(F)$ has an s-generic point.

The proof of Theorem 1.1 is quite straightforward and consists of using an SU-rank computation to replace C by a curve C' isomorphic to C over F but now with *generic, independent* coefficients, and using [13]. In fact this general method is all we really have going for us (except possibly induction on Galois cohomology). One of the proofs that a superstable field is algebraically closed is of this form: given a polynomial equation $f(x) = 0$ over F, find a suitable transformation of it (over F) into a polynomial equation $g(x) = 0$ over F with generic, independent coefficients and use uniqueness of generic types to find an F-rational solution of the latter (see section 5 of [10]). Likewise, in [13] it was shown that in supersimple F, any curve of the form $y^n = ax^n + b$ ($b \neq 0$) over F has a generic solution, by transforming it into a curve $y^n = ax^n + b'$ over F, isomorphic over F to the original curve, and with b' generic, and then using the independence theorem. In the latter examples, the "moduli space" for such families of polynomials or curves (over $\bar{F}$) reduces to a single point. So it is not so surprising to see the restriction on the moduli in the hypotheses in Theorem 1.3.

We would like to thank Bjorn Poonen for his generous and detailed explanations to us of various definitions and facts regarding hyperelliptic curves. We would also like to thank Andreas Baudisch and the Humboldt University at Berlin for their hospitality in the autumn of 2001 when the work reported on here was begun.

2 Supersimple fields.

In this section we give some more details about s-genericity, as well as elaborating slightly on the results from [13] on generic types in groups and fields definable in simple theories. The reader is referred to [13] for the definition of generic types of groups definable in models of simple theories, as well as the properties of the SU-rank. More information is contained in [16] and [11].

Let us first try to distinguish the various notions of genericity we will be using. Typically the fields we work with will be perfect. Suppose F is a field, and X a variety defined over $F_0 < F$. Let $a \in X(F)$. We will say that a is an *a-generic*-point of X over F_0 if $tr.deg(F_0(a)/F_0) = dim(X)$ (algebraic-geometric dimension of X). a-generic refers to generic in the sense

of algebraic geometry. Let us note in passing that, assuming X to be absolutely irreducible, $X(F)$ is Zariski-dense in $X(\bar{F})$ if and only there is an elementary extension F' of F, such that $X(F')$ contains an a-generic point of X over F_0. So the supersimple implies PAC conjecture can be rephrased as: if $(F, +, \cdot, ...)$ is saturated field (possibly with additional structure) whose theory is supersimple, then for any absolutely irreducible variety X defined over a (small) subfield F_0 of F, $X(F)$ contains an a-generic point of X over F_0.

The next notion of generic is purely model-theoretic and makes sense in a (saturated) structure $(F, +, \cdot, ..)$ whose theory is supersimple. It is known that the SU-rank of F in this structure has the form $\omega^\alpha.m$ for some ordinal $\alpha \geq 0$ and integer $m \geq 1$. If X is a subset of the set F^n of n-tuples from F, which is definable over $F_0 < F$ say, then $a \in X$ is said to be generic in X over F if $SU(tp(a/F_0)) = max\{SU(tp(b/F_0)) : b \in X\}$. In general there may be no such generic points. But if X is F itself or some F^n, then they do exist. So $a \in F$ is generic over F_0 if $SU(tp(a/F_0)) = \omega^\alpha.m$, and if $a = (a_1, .., a_n) \in F^n$, a is generic in F^n over F_0 if $SU(tp(a/F_0)) = \omega^\alpha.m.n$. In the latter case, each a_i is generic in F over F_0 and moreover $\{a_1, .., a_n\}$ is F_0-independent in the sense of nonforking.

Finally we have *s-genericity* ("s" for supersimple). Let $(F, +, \cdot, ...)$ be a (saturated) supersimple expansion of a field F, with SU-rank $\omega^\alpha.m$. Let X be a variety of dimension d defined over (small) $F_0 < F$. $X(F)$ is a definable set in the structure $(F, +, \cdot, .)$ but of course may be empty. We will say that $a \in X(F)$ is an s-generic point of X over F_0 if $SU(tp(a/F_0) = \omega^\alpha.m.d$.

The following remark explains some rather obvious relations between these genericity notions.

Remark 2.1 *Suppose $(F, +, \cdot, ..)$ is a (saturated) supersimple expansion of a field F, with SU-rank $\omega^\alpha.m$.*
(i) Let a be a finite tuple from F with $trdeg(F_0(a)/F_0) = d$. Then $SU(tp(a/F_0)) \leq \omega^\alpha.md$.
(ii) Let X be a variety over F_0 of dimension d, and $a \in X(F)$. Then $SU(tp(a/F_0)) \leq \omega^\alpha.md$.
(iii) Let X be as in (ii). Suppose $a \in X(F)$ is an s-generic point of X over F_0. Then a is an a-generic point of X over F_0, and also a generic point of the definable set $X(F)$ over F_0.

Proof. (i) We may suppose a is an n-tuple $(a_1, .., a_n)$, and $a_i \in F_0(a_1, .., a_d)^{alg}$

for all i. As $SU(tp(a_i/F_0)) \leq \omega^\alpha.m$ for each i, it follows that $SU(tp(a_1,..,a_d/F_0)) \leq \omega^\alpha.md$. As $a \in acl(F_0, a_1,..,a_d)$ in the structure F, it follows that $SU(tp(a/F_0)) \leq \omega^\alpha.md$.
(ii) and (iii) follows directly from (i).

The main results of this paper give the existence of s-generic points for suitable curves over supersimple fields. The next remark shows that the statement "any absolutely irreducible variety defined over the (saturated) supersimple field $(F, +, \cdot, ..)$ has an s-generic point", should not be too much to hope for, at least if we believe the conjecture "supersimple implies PAC".

Lemma 2.2 *Suppose that the the field F is perfect, bounded and PAC, and that $(F, +, \cdot, ...)$ is an expansion of $(F, +, \cdot)$ which is saturated and (whose theory is) supersimple. Let X be an absolutely irreducible variety defined over small $F_0 < F$. Then there is a point in $X(F)$ which is s-generic point over F_0.*

Proof. From our assumptions and [6], the "pure field" $(F, +, \cdot)$ is supersimple of SU-rank 1 and moreover model-theoretic algebraic closure in $(F, +, \cdot)$ is precisely (relative) field-theoretic algebraic closure. We may assume X to be a subvariety of affine n-space. Let $dim(X) = d$. Note that $(F, +, \cdot)$ is saturated. As F is PAC, $X(F)$ contains an a-generic point $a = (a_1, .., a_n)$ of X over k. We may assume that $a_1, .., a_d$ are (field-theoretically) algebraically independent over F_0. So $a_1, .., a_d$ are model-theoreticaly algebraically independent over F_0, whereby $(a_1, .., a_d)$ realises a generic type of the additive group F^d over F_0 in the sense of $Th(F, +, \cdot)$. Let $\phi(x_1, .., x_d)$ be the formula (over F_0) $\exists x_{d+1}..x_n((x_1, .., x_d, .., x_n) \in X)$. So $\phi(x_1, .., x_d)$ is generic for F^d (in $Th(F, +, \cdot)$). Write y for the tuple $(x_1, .., x_d)$. So whenever $(c_i : i < \omega)$ is an indiscernible (over F_0 in the sense of $(F, +, \cdot)$) sequence of elements of F^d, $\{\phi(y - c_i) : i < \omega\}$ is consistent. Now work in the expansion $(F, +, \cdot, ...)$. Let $(c_i : i < \omega)$ be indiscernible over F_0, where the $c_i \in F^d$. Then $(c_i : i < \omega)$ is also indiscernible over F_0 in $(F, +, \cdot)$ so $\{\phi(y - c_i) : i < \omega\}$ is consistent. It follows that the formula $\phi(y)$ is generic for F^d in $Th(F, +, \cdot, ..)$, so realized by some $(b_1, .., b_d)$ with $SU(tp(b_1, .., b_d/F_0) = \omega^\alpha.md$. So clearly $X(F)$ contains an s-generic point of X over F_0.

Let us now elaborate slightly on a result from [13] on generic types in groups definable in simple theories.

Let $\bar{M}$ be a saturated model of a simple theory, and G a group definable (without parameters) in $\bar{M}$. For any small set A of parameters from $\bar{M}$, by G^0_A, the connected component of G over A, we mean the smallest type-definable over A subgroup of G of bounded index (in fact of index at most $2^{|A|+|T|}$). G^0_A is normal in G. If $p(x)$ is a Lascar strong type over A of an element of G, then all realizations of p are in the same coset of G^0_A in G. We will call this coset $C_A(p)$. So $C_A(p)$ is an element of the group G/G^0_A.

Lemma 2.3 *(With above notation.) Let p, q, r be Lascar strong types over A of elements of G which are generic. Suppose $C_A(p) \cdot C_A(q) = C_A(r)$ in G/G^0_A. Then there are realizations a, b, c of p, q, r respectively, such that $a.b = c$ and $\{a, b, c\}$ is pairwise A-independent.*

Proof. The proof is essentially identical to that of Proposition 2.2 in [13] but we give it for completeness. Choose b, c independent realizations of q, r repectively, and let a' be such that $a'.b = c$. Then a' is generic over A and $\{a', b, c\}$ are pairwise A-independent. Moreover $a' \in C_A(p)$. Choose a realising p independent from a' over A. Then $(a')^{-1}.a = d$ is generic over A, in G^0_A and $\{a, a', d\}$ is pairwise A-independent. Then d^{-1} is generic in G^0_A. So $d^{-1} \in St(q) = \{x \in G$: for some b_1 realizing q independent from x over A, $x.b_1$ realizes $q\}$. By the independence theorem we may choose d' realizing $Lstp(d/A)$ and independent from b, a' over A such that $d'^{-1}.b$ realizes q and $a'.d'$ realizes p. Then $\{a'.d', d'^{-1}.b, c\}$ is pairwise A-independent and solves the problem.

We will be making heavy use of Remark 3.3 from [13]. This remark says roughly that (in a field whose theory is simple) any coset of a type-definable additive subgroup of bounded index meets any coset of a type-definable multiplicative subgroup of bounded index in a generic set. However the proof given in [13] is incorrect. (It is assumed there that the multiplicative identity of the field is contained in any additive connected component.) So we will take the opportunity here to give a correct proof.

Lemma 2.4 *Let F be a field definable in a saturated model $\bar{M}$ of a simple theory. Let A be a small set of parameters. Let T be a type-definable multiplicative subgroup of F of bounded index, and B a type-definable additive subgroup of F of bounded index. Then for any $e \neq 0$ and a in F, $e \cdot T \cap (a+B)$ is generic in F.*

Let us first note that the special case where $a = 0$ *is* correctly proved in Lemma 3.2 of [13].
Let M be a model over which T and B are defined and which moreover contains all representatives of cosets of T in F^*. We may assume that $B = (F^+)^0_M$, the smallest type-definable over M additive subgroup of F of bounded index. We will first show:
Claim. T meets every coset S of B in a generic set.
Proof of claim. Let $b \in S$ be generic over M. We can find $c \in F$, independent from b over M, such that $b + c \in T$. Let M' be a model containing c and independent from b over M, so $tp(b/M')$ is still generic. So the multiplicative stabilizer $Stab^*(tp(b/M'))$ of $tp(b/M')$ has bounded index in F^*, and so contains the multiplicative connected component $(F^*)^0_{M'}$ of F^* over M'. By 3.2 of [13], $(F^*)^0_{M'}$ meets $(F^+)^0_{M'}$ in a generic set. Thus there is d in this intersection which is generic over M', such that d is independent from b over M' and $d \cdot b$ realizes $tp(b/M')$. Note that $d \in T$. As multiplication by elements of M' fixes setwise $(F^+)^0_{M'}$, $d \cdot c \in (F^+)^0_{M'}$.
Note that b, c, d are M-generic and independent. So $a = d(c + b)$ is generic over M. As $d \in T$ and $c + b \in T$, $a \in T$. On the other hand, $a = dc + db$. Now dc is in $(F^+)^0_{M'}$ so in $(F^+)^0_M = B$. Also db, realizing the same type as b over M', is in S. So $a \in S$. The claim is proved.

Now we will complete the proof of the lemma. Any coset of T in F^* has the form $e \cdot T$ for some $e \in M$. Fix such a coset $e \cdot T$, as well as a coset S of $B = (F^+)^0_M$. As multiplication by elements of M fixes B, $e^{-1} \cdot S$ is also a coset of B. By the Claim, $T \cap e^{-1} \cdot S$ is generic. Now multiply by e to get $e \cdot T \cap S$ being generic.

Corollary 2.5 *Let F be a field definable in the (saturated) model $\bar{M}$ of the simple theory T. Let A be a small set of parameters. Let T be a multiplicative subgroup of F of bounded index, type-definable over A, and $e \in F^*$. Let p, q be generic Lascar strong types over A of F. Then there are a, b, c in F such that, a realizes p, b realizes q, $c \in eT$, $\{a, b, c\}$ is pairwise independent over A, and $a + b = c$.*

Proof. Let X be $e.T$. So X is type-definable over $bdd(A)$. Let $C_A(p)$ be the coset of $(F^+)^0_A$ in F^+ determined by p, and likewise for $C_A(q)$. Let $C = C_A(p) + C_A(q)$. By Lemma 2.4, the type-definable over $bdd(A)$ set $X \cap C$ is generic and thus extends to a Lascar strong type r over A. By construction

$C_A(r) = C$ and $r(x)$ implies $x \in X$. By 2.3, we can find a, b, c realizing p, q, r respectively, pairwise independent over A such that $a + b = c$. (Note we may choose (a, b, c) independent from e over A by taking a nonforking extension of $Lstp(a, b, c/A)$ over $A \cup \{e\}$.)

3 Algebraic curves

We give some more details about the algebraic-geometric objects which concern us. We are interested not only in algebraic curves but also, of course, in rationality issues. We will take [15] as our basic reference for elliptic curves. We found the literature on hyperelliptic curves less satisfactory, especially regarding the positive characteristic case and rationality issues. Nevertheless [9] gives a detailed treatment in the Riemann surface case and the general theory there extends to positive characteristic. We also use [9] as a basic reference for the theory of algebraic curves. Another reference is [14]. The notion we will use of "a hyperelliptic curve over a field F" is the weakest possible, and was suggested by Poonen.

Let us fix a perfect field F. Let k be an algebraically closed field containing F, which we will view as a universal domain for algebraic geometry. By a *curve* C we mean a smooth, projective, irreducible variety over k. So C is a closed subvariety of some $\mathbf{P}^n$ over k. We say that C is defined over F if it can be defined by equations with coefficients in F. So by a curve over F we mean a curve which is defined over F. The genus of a curve C is the dimension of the k-vector space $\Omega^1(C)$ of regular differential forms on C. We will make use of divisors on curves in our definition below of a hyperelliptic curve. Recall that a divisor on C is a finite set of points of C, each point being equipped with a multiplicity (a nonzero integer). The degree of a divisor is the sum of the multiplicities. Divisors can be added in the natural way. (In fact the set of divisors on C is the free abelian group with generators the points of C.) Any rational function F on C has an associated divisor $div(f)$, consisting of the poles and zeroes of f equipped with the obvious multiplicities. These are called principal divisors. Likewise a rational differential form ω on C determines a divisor $div(\omega)$, and such a thing is called a canonical divisor. The canonical divisors form a single coset (translate) of the set of principal divisors. A divisor D on C is said to be effective ($D \geq 0$) if it has nonnegative degree. Given a canonical divisor K, $L(K)$ is the set of

rational functions f on C such that $div(f)+K \geq 0$. $L(K)$ is a k-vector space (isomorphic to $\Omega^1(C)$) and for $g \geq 1$, one obtains from $L(K)$ a map ϕ_K from C to $\mathbf{P}^{g-1}$ called the canonical map. (If $f_1, .., f_g$ form a basis of $L(K)$, then $\phi_K(a) = [f_1(a) : ... : f_g(a)]$). It is important to know that if C happens to be defined over F, then we obtain a canonical map $\phi_K : C \to \mathbf{P}^{g-1}$ defined over F. Of course ϕ_K only has a chance of being meaningful if $g \geq 2$.

Let us now discuss moduli. The set of curves of genus g has a "coarse moduli space" M_g which parametrizes this set of curves up to isomorphism. One can consult [5] for an account of the theory of moduli of curves. For our purposes however it will be enough to know a few naive things:
(i) M_g is an irreducible variety defined over the prime field.
(ii) To each curve of genus g is associated its moduli $m(C) \in M_g$, and every point of M_g arises this way.
(iii) Two curves C and C' of genus g are isomorphic (*over* k) just if $m(C) = m(C')$.
(iv) $m(C)$ is rational in the coefficients defining C. In particular if C is defined over F, then $m(C) \in M_g(F)$.

Finally we bring in elliptic curves, hyperelliptic curves and their moduli spaces. By an elliptic curve we mean a curve C of genus 1 equipped with a distinguished point P. By an elliptic curve over F we mean an elliptic curve (C, P) such that C is defined over F and $P \in C(F)$. An elliptic curve (C, P) has a (unique) commutative algebraic group structure such that P is the identity element. If (C, P) is over F then the group structure is also defined over F. Note that by virtue of the group structure, the group of automorphisms (over k) of a curve of genus 1 acts transitively on C. Thus the "moduli space of elliptic curves" can be identified with the moduli space M_1 of curves of curves of genus 1. M_1 turns out to be just the affine line. The moduli of an elliptic curve C is usually called its j-invariant. If (C, P) is an elliptic curve over F and the characteristic of F is not 2, then (C, P) is isomorphic over F to a plane curve (subvariety of $\mathbf{P}^2$) with affine equation $y^2 = f(x)$ where f is a monic cubic polynomial over F without multiple roots (in k). In this representation the distinguished point is the point at infinity. Further changes of coordinates over F lead to simplifications. For example if the characteristic is neither 2 nor 3 then we can take f to be of the form $x^3 + ax + b$, and then the j-invariant of C is $1728(4a^3/(4a^3 + 27b^2))$. A detailed account is in [15] which we will refer to below.

Now suppose the genus of C is ≥ 2. We say that C is a *hyperelliptic*

curve, if the canonical map from C to $\mathbf{P}^{g-1}$ is *not* an embedding. By [9] (p.204), this is equivalent to each of the following conditions:
(i) the canonical map is a degree 2 map with image a rational curve in $\mathbf{P}^{g-1}$.
(ii) there is a degree 2 map from C onto $\mathbf{P}^1$.
We should say that we are working over the universal domain k here. (ii) is often the usual definition of a hyperelliptic curve (and makes sense and is true of curves of genus 1).

By a hyperelliptic curve *over* F, we will simply mean a hyperelliptic curve C which is defined over F. (So in contradistinction to the definition of elliptic curves, we do *not* require additional specification or even existence of any kind of F-rational point.)

Let C be a hyperelliptic curve over F. By property (i) and previous remarks there is a degree 2 map defined over F from C to a rational curve $X \subseteq \mathbf{P}^{g-1}$ (namely the canonical map). If X happens to have an F-rational point then it is isomorphic to $\mathbf{P}^1$ over F and so we have a degree 2 map from C to $\mathbf{P}^1$ defined over F. If the characteristic of F is not 2, and C has genus g, it follows that C is isomorphic over F to a curve with affine equation $y^2 = f(x)$ where f is a monic polynomial of degree $2g+1$ or $2g+2$ without multiple roots. (This is mentioned in Proposition 4.11 of [9] in the Riemann surface case. In general, a model over F of the form $y^2 = f(x)$ is obtained by Kummer theory applied to function fields. As the number of branch points of the map taking (x, y) to x is $2g+2$ by the Hurwitz formula, one obtains the constraints on the degree of f. In fact if there is an F-rational branch point, it can be moved to infinity and one obtains an equation with $f(x)$ of degree $2g+1$. Otherwise one gets degree of f to be $2g+2$.) Now if $Th(F, +, \cdot)$ (or an expansion) is supersimple then we know from [13] that any rational curve over F does have an F-rational point. So we conclude:

Fact 3.1 *Suppose that $Th(F, +, \cdot, ..)$ is supersimple with characteristic $\neq 2$. Let C be a hyperelliptic curve of genus $g \geq 2$ defined over F. Then C is isomorphic over F to a curve with (affine) equation $y^2 = f(x)$ where f is monic, of degree $2g+1$ or $2g+2$, and without multiple roots.*

The family of hyperelliptic curves of genus g over k admits a moduli space H_g which is a subvariety of M_g and is also defined over the prime field. Moreover $dim(H_g) = 2g-1$ and by [1] H_g is a rational variety.

It is worth saying a little about where the moduli space H_g comes from. Consider hyperelliptic curves C of genus g over k. Any such curve is a double

cover of $\mathbf{P}^1$ with $2g+2$ branch points in $\mathbf{P}^1$. Let S be the set of branch points. Then C and C' are isomorphic over k if there is an automorphism of $\mathbf{P}^1$ taking the set S to the set S'. Thus H_g is the set of subsets of $\mathbf{P}^1$ of size $2g+2$ quotiented by the action of PGL_2. The dimension of H_g is $2g-1$ (as PGL_2 acts strictly 3-transitively on $\mathbf{P}^1$).

In the next two sections we prove our results on the existence of "generic" F-rational points on "generic" elliptic and hyperelliptic curves over a supersimple field F. We separate into the elliptic and hyperelliptic cases (and there is further case division for hyperelliptic curves). The proof could be somewhat streamlined by deducing more or less everything from the proof of the even degree hyperelliptic case (by adding dummy terms) but for the sake of exposition and intelligibility we stick with the current presentation and apologize for any repetition and superfluity in the arguments.

4 The case of elliptic curves

We work with fields of characteristic different from 2. We prove:

Proposition 4.1 *Suppose $Th(F,+,\cdot,..)$ is supersimple, and C is an elliptic curve over F with j-invariant j.*
(i) if $j=0$ or 128 then $C(F)$ has an s-generic point.
(ii) If j is s-generic then $C(F)$ has an s-generic point.

Proof of (i). First suppose $char(F) \neq 3$. If $j=0$ then by Prop. 1.1 (a) of Appendix A in [15] C can be written in the form $y^2 = x^3 + c$ with $c \neq 0$. By Proposition 3.4 of [13], $y^6 = x^6 + c$ has an s-generic solution over c in F, say (a,b). But then (a^2, b^3) is a generic solution of the original curve. If $j = 128$ then C has the form $y^2 = x^3 + cx$ with $c \neq 0$. By [13] again, we can find an s-generic solution (a,b) in F of $y^2 = x^4 + c$. Then (a^2, ab) solves the original equation.
Now suppose $char(F) = 3$. So $1728 = 0 \bmod 3$. By Prop. 1.1 (b) of Appendix A of [15], C can be written, over F, in the form $y^2 = x^3 + ax + b$. Now $\{x^3 + ax : x \in F\}$ is an additive subgroup H say, of F, of finite index. By Lemma 2.4, every coset of H in F meets the squares in a generic set. So C has an s-generic (over $\{a,b\}$) point in F.

Proof of (ii). Suppose first the characteristic is different from 3. Then by Prop. 1.1 (a) in Appendix A of [15], we can write C in the form $y^2 =$

$x^3 + ax + b$, and j is
$1728(4a^3/4a^3 + 27b^2)$. (*)
Let u be generic in F over $\{a, b\}$. The map taking (x, y) to (u^2x, u^3y) yields an isomorphism (defined over F) between the elliptic curve C and the elliptic curve C' defined by $y^2 = x^3 + a'x + b'$ where $a' = u^4a$ and $b' = u^6b$. Note that C' is also defined over F and
(**) $j(C') = 1728(4a'^3/4a'^3 + 27b'^2) = j(C) = j$.
Claim 1. a' and b' are generic independent elements of F.
Proof. u is generic in F over $\{a, b, j\}$, so $a' = u^4a$ is generic in F over $\{a, b, j\}$. In particular (under our assumption that j is generic in F), a' and j are independent generics of F. By (**) $(b')^2 = 4a'^3(1728 - j)/27j$. Properties of generics imply that b' is generic, and independent of a'. The claim is proved.

Claim 2. The curve C' has an s-generic (over a', b') solution in F.
Proof. Let $d \in F$ be generic over a', and let $p(x) = Lstp(d^3 + a'd/a')$. Then $p(x)$ is a generic type over a'. ($d^3 + a'd$ is interalgebraic with d over a' so has the same SU-rank as d over a'.) Let $q = Lstp(b'/a')$, also a generic type. By Corollary 2.5, there are c, a'', b'' in F with c a square in F, a'' a realization of p and b'' a realization of q such that $\{c, a'', b''\}$ is pairwise a'-independent, and $c = a'' + b''$. By automorphism (over a') we may assume that $b'' = b'$. Note that a'' is generic over a', b'. By definition of $p(x)$ there is $d' \in F$ such that $d'^3 + d'a' = a''$. Note that d' is also generic in F over a', b'. Hence $(d', \sqrt{c})$ is an s-generic over a', b' point of $C'(F)$.

By Claim 2, we may find a point (x', y') of $C(F)$ which is s-generic over $\{a', b', a, b, u\}$. But then $(u^{-2}a', u^{-3}b')$ is clearly an s-generic point of $C(F)$ (over all parameters mentioned). This completes the proof when the characteristic is neither 2 nor 3.

When the characteristic is 3, by Prop.1.1 (b) in Appendix A of [15], C can be written over F in the form $y^2 = x^3 + ax^2 + b$ (with $b \neq 0$), and $j = -a^3/b$. Let $u \in F$ be generic over $\{a, b, j\}$. The map taking (x, y) to (u^2x, u^3y) is an isomorphism defined over F between C and the curve C' defined by $y^2 = x^3 + a'x^2 + b'$ where $a' = u^2a$ and $b' = u^6b$ (and where of course C' has j-invariant $-a'^3/b' = j$). As above we can show that a' and b' are generic independent in F, C' has an s-generic point in F, and so does C.

5 The case of hyperelliptic curves

Again we assume that $char(F) \neq 2$. We will prove:

Proposition 5.1 *Let $(F, +, \cdot, ..)$ be an infinite saturated field (with additional structure) whose theory is supersimple. Let C be a hyperelliptic curve of genus $g \geq 2$, defined over F. Suppose that $m(C) \in H_g(F)$ is an s-generic point of H_g. Then C has an s-generic F-rational point.*

Proof. Suppose that the $SU(F) = \omega^\alpha.m$. We will make use of an "ω^α-weight" of types, which we will just call $w(-)$. If $A \subset F$ and a is a finite tuple from F then $SU(tp(a/A)) = \omega^\alpha.r + \beta$ where $\beta < \omega^\alpha$. We define $w(tp(a/A)$ to be r. So if a is a single element, then $w(tp(a/A)) = m$ iff $tp(a/A)$ is generic. The SU-rank inequalities give us $w(tp((a,b)/A)) = w(tp(a/(A,b)) + w(tp(b/A))$. We also sometimes write $w(a/A)$ for $w(tp(a/A))$.

Using Fact 3.1, we separate into two cases, according to whether f has odd or even degree.
Case 1. C can be written over F in the form $y^2 = f(x)$ where $f(x)$ is a monic polynomial over F of degree $2g+1$ without multiple roots (in $\bar{F}$).
Let $f(x) = x^n + a_{n-1}x^{n-1} + ...a_1x + a_0$. So $n = 2g+1$, and so $dim(H_g) = 2g-1 = n-2$. Let $m(C) \in H_g(F)$ be the modulus of C; our assumption on the s-genericity of $m(C)$, means that $SU(tp(m(C)) = \omega^\alpha.m.(n-2)$ whereby $w(tp(m(C))) = m.(n-2)$.
Note that $m(C)$ is rational over $\{a_0, .., a_{n-1}\}$.
Choose $u, r \in F$ generic independent over $\{a_0, .., a_{n-1}, m(C)\}$. The map taking (x, y) to $(u^2x + r, u^n y)$ yields an isomorphism, defined over F between the hyperelliptic curve C and a hyperelliptic curve C' defined by $y^2 = g(x) = x^n + a'_{n-1}x^{n-1} + .. + a'_1x + a'_0$ over F. If $\alpha_1, .., \alpha_n$ are the zeroes of $f(x)$ in $\bar{F}$ then $u^2\alpha_1 + r, .., u^2\alpha_n + r$ are the zeroes of $g(x)$ in $\bar{F}$, and the a'_i are the symmetric functions in these zeroes. In any case $m(C) = m(C')$ is rational over the a'_i's.
Claim. $a'_0, .., a'_{n-1}$ are generic independent in F.
Proof. This is an easy weight argument. Let a denote the tuple $(a_0, .., a_{n-1})$, and a' the tuple $(a'_0, .., a'_{n-1})$. We have to prove that $w(a') = mn$.
Let us make some observations.
(i) $\{u, r\}$ is interalgebraic with a' over a (in the sense of fields, so also in the supersimple structure $(F, +, \cdot, ..)$), whereby $w(u, r/a) = w(a'/a)$.

Justification. $\{u, r\}$ is interalgebraic with $\{\alpha'_i : i = 1, , .n\}$ over $\{\alpha_i : i = 1, .., n\}$, a' is interalgebraic with $\{\alpha'_i : i = 1, .., n\}$, and a is interalgebraic with $\{\alpha_i : i = 1, .., n\}$.
(ii) $w(m(C)) = m(n-2)$.
Now (iii) $w(a, a') = w(a'/a) + w(a) = w(u, r/a) + w(a) = 2m + w(a)$.
Also
(iv) $w(a, a') = w(a/a') + w(a') \leq w(a/m(C)) + w(a') = w(a) - w(m(C)) + w(a')$.
By (ii), (iii) and (iv), $w(a') = 2m + m(n-2) = mn$. As a' is an n-tuple it follows that $SU(a') = \omega^{\alpha}.mn$ and $a'_0, .., a'_{n-1}$ are independent generic in F, proving the claim.

The rest of the proof in this case is as in that of Claim 2 of the previous section : Let $A' = \{a'_1, .., a'_{n-1}\}$. Let $p(z)$ be a Lascar strong type over A' which is generic and implies "$\exists x(z = x^n + a'_{n-1}x^{n-1} + .. + a'_1 x)$". Let $q(w) = Lstp(a'_0/A')$. Then by Corollary 2.5 there are $c, z', w' \in F$ generic and pairwise independent over A' such that c is a square in F, z' realizes p and w' realizes q. We may assume that $w' = a'_0$. This yields an s-generic point (x, y) say over $\{a'_0, .., a'_{n-1}\}$ of $C'(F)$. We may assume (x, y) is also s-generic on $C(F)$ over $\{a'_0, .., a'_{n-1}, a_0, .., a_{n-1}, u, r\}$. Then $((x - r)u^{-2}, u^{-n}y)$ is an s-generic point on $C(F)$ over all parameters.

Case 2. C is of the form $y^2 = f(x)$, where f is a monic polynomial over F of degree $2g + 2$ without multiple roots.

This case is a little more subtle and will use the full strength of Corollary 2.5. Let $n = 2g+2$. So the SU-rank of the type of $m(C)$ is $\omega^{\alpha}.m(n-3)$, and $w(m(C)) = m(n-3)$. We will use a "generic" fractional linear transformation to transform C into a curve C' over F defined by $ey^2 = g(x)$, where g has degree n with generic independent coefficents, and $e \in F$ is nonzero. We cannot in general arrange to get e to be 1 (or even a square).

Let $f(x) = x^n + a_{n-1}x^{n-1} + .. + a_1 x + a_0$ and let again $a = (a_0, .., a_n)$. Let (u, r, s, t) be a generic point of $SL_2(F)$ over a. That is, the corresponding matrix has determinant 1, and u, r, s are generic independent elements of F over a. We will be considering the transformation h which takes a pair (x, y) to $(ux + r/sx + t), y/(sx + t)^{n/2})$. Let $\alpha_1, .., \alpha_n$ be the zeroes of $f(x) = 0$ in $\bar{F}$. Let $\beta_i = (t\alpha_i - r)/(u - s\alpha_i)$ for $i = 1, .., n$. It can then be checked that h induces an isomorphism between the $\bar{F}$-points of C and the $\bar{F}$ points of the

curve C' defined by $y^2 = f(u/s)(x-\beta_1)..(x-\beta_n)$. Noting that the symmetric functions in the β_i are F-rational, we see that $g(x) = (x-\beta_1)..(x-\beta_n) = x^n + a'_{n-1}x^{n-1} + .. + a'_1x + a'_0$ for some $a'_i \in F$. Let $a' = (a'_0, .., a'_{n-1})$. The curve $y^2 = f(u/s)g(x)$ is isomorphic over $\bar{F}$ to C'' defined by $y^2 = g(x)$, so C, C' and C'' have the same moduli, $m(C)$. In particular $m(C)$ is rational over a'.

Claim. $w(a') = mn$.
Proof. This is just like the proof of the claim in Case 1 above. First we have (i) (u, r, s, t) and a' are interalgebraic over a (in the supersimple field F).
Then (ii) $w(m(C)) = m(n-3)$.
(iii) $w(a, a') = w(a'/a) + w(a) = w(u, r, s, t/a) + w(a) = 3m + w(a)$.
(iv) $w(a, a') = w(a/a') + w(a') \leq w(a/m(C)) + w(a') = w(a) - w(m(C)) + w(a')$.
By (ii), (iii) and (iv), $3m + m(n-3) \leq w(a')$. As a' is an n-tuple, this forces $w(a') = nm$, proving the claim.

By the claim $a'_0, .., a'_{n-1}$ are generic independent in F. Let $e^{-1} = f(u/s)$. Let $A' = \{a'_1, .., a'_{n-1}\}$. Let T the group of squares in F^*. Putting $q(w) = Lstp(a'_0/A')$ and $p(z)$ some generic Lascar strong type over A' implying "$\exists x(z = x^n + a'_{n-1}x^{n-1} + .. + a'_1x)$", we obtain from Corollary 2.5, $e', z', w' \in F$ pairwise independent over A' with $e' \in e.T$. There is an automorphism fixing $acl^{eq}(A')$ and taking w' to a'_0. As $e.T$ is defined over $acl^{eq}(A')$ such an automorphism takes e' to some $e'' \in eT$. This shows that we may assume $w' = a'_0$. In any case, we obtain a point $(x, y) \in C'(F)$ such that x is generic over A'. If (x', y') realizes a nonforking extension of $Lstp(x, y/A')$ over $\{a', e\}$ we see as before that (x', y') is an s-generic point of $C'(F)$ over $\{a', e\}$. We may in addition assume that (x', y') is s-generic over $\{a, a', u, r, s, t\}$. The image of (x', y') under the inverse of h is then an s-generic point of the original curve C over all the parameters. This completes the proof.

We conclude the paper with some additional remarks regarding the methods. The general method (in both the elliptic and hyperelliptic cases) was to transform a curve defined by $y^2 = f(x)$ (f monic and of of degree n say over F) into one of the form $ey^2 = g(x)$ by an isomorphism defined over F and where g has generic independent coefficients. All that is needed is the weaker requirement that the constant coefficient a'_0 say of g is generic in F over the

other coefficients. So in the hyperelliptic case, one might expect to be able to do this under weaker assumptions on the SU-rank of the moduli of the original curve. However in the elliptic case, if $y^2 = x^3 + ax + b$ is over F and b *is* generic in F over a then the j-invariant of the elliptic curve *will be* generic in F, so we cannot really hope to weaken the genericity assumption on the moduli, while using the same methods.

References

[1] F.A. Bogomolov, Rationality of the moduli of hyperelliptic curves of arbitrary genus, Canadian Math. Soc, Conference Proceedings, vol 6, AMS, 1986.

[2] Z. Chatzidakis, A. Macintyre and L. Van den Dries, Definable sets over finite fields, J. Reine und Angew. Math., 427 (1992), 107-135.

[3] G. Cherlin and S. Shelah, Superstable fields and groups, Annals of Math. Logic 18 (1980), 227-270.

[4] M. Fried and M. Jarden, *Field Arithmetic*, Springer, 1986.

[5] J. Harris and I. Morrison, *Moduli of curves*, Graduate Texts in Mathematics 187, Springer, 1998.

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

[7] B. Kim and A. Pillay, From stability to simplicity, Bulletin of Symbolic Logic 4 (1998), 17-36.

[8] A. Macintyre, On ω_1-categorical fields, Fund. Math. (1971), 1-25.

[9] R. Miranda, *Algebraic curves and Riemann surfaces*, Graduate Studies in Mathematics, vol. 5, AMS, 1995.

[10] A. Pillay, Model theory of algebraically closed fields, in *Model Theory and Algebraic Geometry*, ed. E. Bouscaren, Lecture Notes in Math., 1696, Springer, 1998.

[11] A. Pillay, Definability and definable groups in simple theories, Journal of Symbolic Logic, 63 (1998), 788-796.

[12] A. Pillay and B. Poizat, Corps et Chirurgie, Journal of Symbolic Logic 60 (1995), 528-533.

[13] A. Pillay, T. Scanlon and Frank Wagner, Supersimple fields and division rings, Math. Research Letters 5 (1998), 473-483.

[14] I. R. Shafarevich, *Basic Algebraic Geometry I*, Springer, 1994.

[15] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer, 1986.

[16] F. Wagner, *Simple theories*, Kluwer, 2000.