FIRST STEPS IN THE GEOMETRY OF CURVES

PETE L. CLARK

We would now like to begin studying algebraic curves. However, to do this from the desired modern perspective we still need some further tools. Perhaps though by trying to study curves anyway the need for these specific tools will become clear.

Let $C_{/k}$ be a geometrically integral curve. We have already seen that there exists a unique curve $\tilde{C}_{/k}$ which is birational to C and is projective and nonsingular (and that this cannot be improved to smooth if k is not perfect). Thus the birational geometry of curves works out in the nicest possible way. One often takes advantage of this by defining a curve using a model which is incomplete, singular or both (but always geometrically integral!), with the understanding that what we are really interested in is the unique projective nonsingular model.

Perhaps the first thing we wish to define on algebraic curve is its **genus**, $g \in \mathbb{N}$. Classically the genus was viewed as a topological invariant. Namely, if $C_{/\mathbb{C}}$ is a nice curve, then $C(\mathbb{C})$ in the analytic topology is a compact complex manifold of dimension 1, so in particular a compact orientable real surface, and thus diffeomorphic to a sphere with g handles for some unique non-negative integer g. (Alternately, $2g = \dim_{\mathbb{Q}} H^1(C(\mathbb{C}), \mathbb{Q})$.)

For a nice curve over an arbitrary field k we could, in fact, make this topological definition work, but only with more sophistication and work than would be necessary to give a purely algebraic definition.

Perhaps the cleanest algebraic definition of the genus is $\dim_k H^1(C, \mathcal{O}_C)$, i.e., the dimension of the first sheaf cohomology group of the structure sheaf. This points out the need for sheaf cohomology, which we have not yet discussed.

Another useful algebraic definition – dual to the first – is $\dim_k H^0(C, \Omega_C)$. This is easier than the previous definition in that we are not really using cohomology: it is just the dimension of the space of global sections of a certain sheaf Ω_C, the **canonical sheaf**. However, to define this sheaf requires the notion of differentials.

The next issue is how to embed a curve into projective space. For this we need the theory of divisors, line bundles and linear systems, and the Riemann-Roch theorem. Let us come at this from a very naive perspective.

Let X be a variety which is geometrically integral and nonsingular in codimension 1 (e.g., normal). For $0 \leq i \leq d = \dim(X)$, we will define an abelian group $Z_i(X)$. By a **prime cycle**, we mean a reduced irreducible closed subvariety of X. Like every irreducible variety, a prime cycle has a well-defined dimension, and we

put $Z_i(X)$ to be the free abelian group generated by the prime cycles of dimension i. An element of the group $Z_{d-1}(X)$, of cycles of codimension one, is called a **Weil divisor**.

Since X is integral, it has a function field $k(X)$. To every function $f \in k(X)$, we can associate a Weil divisor $\mathrm{div}(f)$, as follows. The assumption that X is nonsingular in codimension one ensures precisely that the local ring of X at any irreducible Weil divisor Z is Noetherian, local and nonsingular, thus a DVR. So there exists a well-defined positive integer $\mathrm{ord}_Z(f)$, the order of vanishing of f along Z. (So, for instance, the order of vanishing is non-negative iff f is regular at every point of Z and is 0 iff f is regular and invertible at every point of Z.) We then define

$$\mathrm{div}(f) = \sum_Z \mathrm{ord}_Z(f)[Z].$$

Here the sum extends over all prime divisors, and the finiteness of nonzero orders comes down to a basic finiteness result in commutative algebra that I don't wish to linger over here.

0.1. **Meromorphic differentials on curves.**

Assume now that X is a curve, and let ω be a meromorphic differential on X, that is, a section of Ω_X over the generic point of X. Locally near any point p of X it can be written as fdt, where t is a uniformizing parameter at p, and we define $K := \mathrm{div}(\omega) = \sum_p \mathrm{ord}_p(f)p$. One has to check that this makes sense independently of the local representation of ω (but it does). Then in fact the degree of $\mathrm{div}(\omega)$ is $2g-2$. Because the module of meromorphic differentials of X over k is one-dimensional over $k(X)$, if ω_1 and ω_2 are any two meromorphic differentials, there exists a meromorphic function $f \in k(X)$ such that $\omega_2 = f\omega_1$, and thus $\mathrm{div}(\omega_2) - \mathrm{div}(\omega_1) = \mathrm{div}(f)$. This shows in particular that the degree of a meromorphic differential is well-defined.

Moreover, in the general case (of a projective variety X which is nonsingular in codimension 1) we define an equivalence relation on Weil divisors: we say D_1 is **linearly equivalent** to D_2 if $D_1 - D_2 = \mathrm{div}(f)$ is the divisor of some function. The quotient of $Z^1(X) = Z_{d-1}(X)$ modulo linear equivalence is called the **divisor class group**, $Cl(X)$. (When X is nonsingular, this will turn out to be isomorphic to the Picard group $\mathrm{Pic}(X)$, which we have not yet defined but with which the reader may be more familiar.) This group is a very important invariant of X.

0.2. **The index of a nice variety.**

Let $X_{/k}$ be a (nonempty!) nice variety. There is a map from the group of zero-cycles $Z_0(X)$ to $\mathbb{Z}$, called the degree:

$$\deg(\sum_P n_P[P] = \sum_P [k(P) : k]n_P;$$

here $k(P)$, is, as usual, the residue field at the closed point P. We define the **index** of X to be the cardinality of the cokernel of the degree map; in other words, the index of V is the least positive degree of a divisor on X.

This is an example *par excellence* of an arithmetic-geometric invariant of varieties which is only interesting over a non-algebraically closed ground field. Indeed, since any k-variety has a $\overline{k}$-valued point, the index of a variety over an algebraically closed field is equal to 1. (In fact, since V is assumed to be geometrically integral, it is enough for k to be separably closed.)

Exercise: The index of a variety is equal to the gcd of all degrees of closed points on V.

Exercise: a) If k is not perfect, we can also define the **separable index** i_s to be the gcd of all degrees of closed points with separable residue field extensions. What is an equivalent definition in terms of divisors? (Hint: you want to define a subgroup of $Z_0(X)$ generated by "separable" divisors.)
b) Show that $i(V) \mid i_s(V)$ for all V.
c**) Find a nice variety V over some (imperfect) field k such that $i_S(V) > i(V)$.[1]

It is natural to ask what possible values the index can assume. In fact, it is more interesting to ask this question among varieties with other discrete invariants fixed. For example, let k be a field, and let $g \in \mathbb{N}$. For which values of i does there exist a nice curve $C_{/k}$ with genus g and index i?

The first observation is that there is really only one class of divisors which are given to us for free on any curve of genus g: namely, the canonical class. Since the degree of any canonical divisor is $2g-2$, we get that the index of a genus g curve (over any field k) must divide $2g-2$.

When $g = 0$, this says the index is 1 or 2. We will see that these two cases correspond, over any field, to the case of plane conics with and without rational points.

When $g = 2$, this again says the index is 1 or 2, although here it is possible for the index to equal 1 and there still not to be rational points, as can be done with curves over a finite field for instance. In general, for higher genus, this says that there are only finitely many possible values for the index.

However, when $g = 1$, this says that the index divides 0: this is no restriction at all! It has been known for a long time that there exist fields k such that for every positive integer i there is a genus one curve of index i. An especially simple case is $k = \mathbb{C}((t))$, in which the result is due, independently, to Ogg and Shafarevich (as a corollary of more general results). The case of $\mathbb{Q}_p$ is due to Lang and Tate. On November 2, 2004, I was able to show that for any number field K and any $i \in \mathbb{Z}^+$, there exists a genus one curve $C_{/K}$ of index i.

For higher genus, over a locally compact non-Archimedean field the fact that for any $g \in \mathbb{N}$ and $i \mid 2g-2$ there exists a curve C with genus g and index i is due to Shahed Sharif (in his PhD thesis, when the characteristic is not 2) and myself (a couple of weeks later, but before I saw his thesis). These methods show that for any g, there exists a number field K (depending upon g) and a curve $C_{/K}$ of genus

[1]So far as I know this is an open question.

g with index $2g-2$. There are still some open cases.

Exercise **: Suppose that instead of a number field, K is a global function field, i.e., the function field of a nice curve over a finite field. Can one show that there exist genus one curves C of every index over K?[2]

0.3. **Linear systems.**

Linear system: Let D_0 be a Weil divisor on X. We define the **complete linear system** $L(D)$ of D, as follows: it is the set of effective divisors D which are linearly equivalent to D_0. Note that $L(D)$ is empty if $\deg(D_0) < 0$, and also if $\deg(D_0) = 0$ unless D_0 is linearly equivalent to the zero divisor.

There are many useful equivalent ways of viewing this linear system. One way is as follows: every $D \in L(D_0)$ is of the form $D_0 + \operatorname{div}(f)$, so we may identify D with the function f, in which case the effectivitiy of D becomes the condition $\operatorname{div}(f) \geq -D_0$. Thus $L(D_0)$ can be viewed as the set of all functions $\{f \mid \operatorname{div}(f) \geq -D_0\}$. This is nice, because if we adjoin the 0 function to $L(D_0)$, then it is easily seen to be a k-vector space, under the operations of multiplication of functions and multiplication of a function by a scalar. For reasons that we will explain later, it turns out that this vector space is finite-dimensional; we denote its dimension by $l(D)$. Once we notice that $\operatorname{div}(f) = \operatorname{div}(\alpha \cdot f)$ for any $\alpha \in k^\times$, it becomes more natural yet to consider the corresponding projective space $\mathbb{P}(D) \cong \mathbb{P}^{l(D)-1}$.

And now a miracle occurs: we define the **base locus** of D to be the set of all closed points $x \in X$ such that $f(x) = 0$ for all $f \in \mathbb{P}(D)$. The base locus is a proper closed subset of X and may well be empty. On the complement of the base locus, we can define a morphism from X to $\mathbb{P}(D)$ given by $x \mapsto (f(x))$. To be more precise about this, if we choose a basis $f_0, \ldots, f_{l(D)-1}$ for $L(D)$, then the corresponding map gets coordinatized as

$$x \mapsto [f_0(x) : \ldots : f_{l(D)-1}(x)].$$

To interpret this property in projective space, at any given point x we are free to rescale the functions by any common value: our goal is to make all of the coordinates finite and not all of the coordinates equal to 0. But in fact if all of the coordinates are 0 there is nothing we can do: that means that x is an element of the base locus, and the map cannot be defined at x. But otherwise, it is easy to see that by dividing all the elements by the function $f_i(x)$, where i is chosen such that the valuation of f_i at x is minimal, we will get an expression in which all coordinates are finite and not all are zero.[3]

Moreover, different choices of basis correspond to linear automorphisms of $L(D)$ modulo scalars, i.e., $PGL(L(D))$, and this is precisely the automorphism group of

[2]I was so excited about the result that I got on election day that it never occurred to me to look at the function field analogue.

[3]Note that this is more correct than what I said the first time I tried to define linear systems and simpler than the correction that I made a few lectures later. In my defense, this simple explanation is hard to find in the literature!

the projective space. Also the degree of the map is equal to the degree of D.

Thus an effective Weil divisor on X gives a rational map into a projective space.

Example: $\mathbb{P}^1$.

Example: An elliptic curve.

Theorem 1. *(Riemann-Roch for nice curves) Let X be a nice curve over a field k, and let D be a Weil divisor on X. Let K be the divisor of a meromorphic differential on X. Then*

$$l(D) - l(K - D) = \deg(D) - g(X) + 1.$$

0.4. **Ample and very ample divisors.**

Let D be a divisor on a nice variety V. We say that D is **very ample** if the induced rational map $\varphi_D : V \to \mathbb{P}^N$ is a morphism which is a closed immersion (i.e., an embedding!). We say that a divisor D is **ample** if some positive integer multiple is very ample.

Remark: This is of course a slightly weird definition: among other things, one would expect very ample to be defined in terms of ample rather than the other way around. There are also other equivalent formulations. But this simple one is useful (and, one gets used to it).

We quote without proof some simple and useful criteria for divisors on curves to be ample or very ample.

Proposition 2. *Let D be a divisor on a nice curve $C_{/k}$.*
a) A divisor is ample iff it has positive degree. a) The complete linear system $|D|$ has no base points iff: for all closed points P of C, $\dim |D - P| = \dim |D| - 1$.
b) D is very ample iff for any two closed points (P, Q) of C (the case $P = Q$ is not excluded), then $\dim |D - P - Q| = \dim |D| - 2$.
c) So if $\deg D \geq 2g$, $|D|$ has no base points.
d) If $\deg D \geq 2g + 1$, then D is very ample. e) D is ample iff $\deg D > 0$.

Some general terminology: a variety is said to be **Fano** if its anticanonical bundle – i.e., $-K$, where K is the canonical bundle – is very ample. A variety is said to be **of general type** if some positive multiple of the canonical bundle induces an embedding on a dense open subset. Roughly speaking, a variety is **Calabi-Yau** if its canonical class is linearly equivalent to 0.

Then:

(i) A nice curve is Fano iff it has genus 0.
(ii) A nice curve is Calabi-Yau iff it has genus 1.
(iii) A nice curve is of general type iff it has genus at least 2.

Let us now return to the case of genus 0 curves. The anticanonical class is represented by any divisor of degree 2; according to Proposition X.Xd) this makes it

very ample. By Riemann-Roch, $\dim |-K| = 3$, so

$$\varphi_{-D} : C \to \mathbb{P}^2$$

is a degree 2 embedding. Thus its image must be a conic curve in $\mathbb{P}^2$, which is uniquely determined up to projective automorphisms (and of course, rescaling). We have proven:

Theorem 3. *A nice genus 0 curve over an arbitrary field k is "anticanonically isomorphic" to a plane conic, i.e., a curve of the form*

$$a_1X^2 + a_2Y^2 + a_3Z^2 + a_4XY + a_5XZ + a_6YZ = 0.$$

If the characteristic of k is different from 2, then any quadratic form can be diagonalized, and thus we can get an equation of the form

$$aX^2 + bY^2 = Z$$

for $a, b \in k^\times$.

The next thing to observe is that if our genus zero curve has a k-rational point, it is isomorphic to the projective line. Indeed, choose one such point O, and consider the set of all lines in $\mathbb{P}^2$ passing through O. Every line except for the tangent line intersects the conic in a unique point $P \neq O$; whereas the tangent line intersects O with multiplicity 2. From this one gets a geometrically defined explicit isomorphism $\mathbb{P}^1 \to C$ (this is one of the oldest arguments in algebraic geometry).

Obviously the converse is also true: $\mathbb{P}^1_{/k}$ has k-rational points. (It even has "many" k-rational points in that $\mathbb{P}^1(k)$ is Zariski-dense in $\mathbb{P}^1(\overline{k})$.)

Correspondence between genus 0 curves and quaternion algebras...

We also want to show that a conic without rational points has index 2, i.e., has no rational points over any odd extension. There are many ways of doing this: for instance, one can prove it using quaternion algebras, or using the algebraic theory of quadratic forms (Springer's Theorem). Or one can use Riemann-Roch: indeed, Riemann-Roch implies that any divisor on a genus 0 curve of positive degree is linearly equivalent to an effective divisor. So if C had a divisor of degree 1 it would have a k-point! Note that this argument also works verbatim for elliptic curves, but not for curves of any higher genus (and indeed the result is not true in any higher genus!).

0.5. **Curves of genus one.**

Exercise: Let p be a prime number. Consider the plane curve $C_p/\mathbb{Q}$ given by the equation

$$C_p : X^3 + pY^3 + p^2Z^3 = 0.$$

a) Show that C_p is a smooth curve of genus one.
b) Show that the index of C_p is 3. In particular, C_p is not hyperelliptic.
c)* Suppose that $p \equiv 1 \pmod 3$. Show that C_p has no rational points over any abelian number field.

0.6. **Curves of genus two.**

Genus 2: the canonical divisor has degree $2g-2=2$. By Riemann-Roch it gives a degree 2 map

$$C \to \mathbb{P}^1.$$

Note that, ignoring the theory of base points of linear systems, we know we can extend this rational map to a morphism because C is a smooth curve! In other words C is **canonically** a double cover of $\mathbb{P}^1$.

Definition: A curve C of any genus which admits a separable degree 2 morphism to $\mathbb{P}^1$ is **hyperelliptic**.

We remark that this definition is nonstandard. For instance:

Exercise X.X: Show that any nice curve of genus 0 is hyperelliptic.

By the Riemann-Hurwitz theorem, a hyperelliptic curve has $2g+2$ branch points, so we get a a model of the form

$$y^2 = P_{2g+2}(x).$$

Exercise: Show that if $k = \overline{k}$ we can find also give a defining equation of the form $y^2 = P_{2g+1}$. (Hint: use an automorphism of $\mathbb{P}^1$ to map one of the branch points to infinity.)

The preimage of infinity consists of two k-rational points if the leading coefficent a of P is a square in k, and otherwise consists of a single closed point whose reisdue field is $k(\sqrt{a})$. If $g > 0$, then both of the closed points are singular, and increasingly so as the genus increases. Therefore this is not the smooth projective model of C. However, in practice this is no problem: it is easier to work with a hyperelliptic model than almost any other smooth projective model.

Applications:

1) Let us plug in $D = K$. By the above remarks, $l(K-K) = l(0) = 1$, so we get

$$l(K) = \deg(K) - g + 2 = g.$$

When $g = 0$, the canonical divisor has degree -2 so is not effective. But we can take the anticanonical divisor $-K$, which has degree 2. According to Riemann Roch then we get

$$l(-K) = l(2k) + \deg(-K) + 1 = 3,$$

so the corresponding rational map is from X to $\mathbb{P}^2$. It is easy to check that there are no base points and in fact that this map is an embedding. Since $deg(-K) = 2$, the image of X in $\mathbb{P}^2$ is a quadric hypersurface, that is, a **conic curve**. Thus any nice curve of genus 0 has an (anti!)canonical representation as a plane conic.

1. Hyperelliptic curves

Definition: A nice curve $C_{/k}$ is **hyperelliptic** if it admits a finite separable morphism $C \to \mathbb{P}^1$ of degree 2.

Remark: This definition coincides with Liu's definition, except in the (completely innocuous) point that we place no genus restrictions on curves whatsoever, whereas Liu requires $g(X) \geq 1$. Indeed:

Exercise X.X: Show that every curve of genus 0 is hyperelliptic.

Exercise: a) Let $\varphi : X \to Y$ be a finite morphism of nice curves over k, of degree d. Letting, as before, $i(C)$ denote the index of a curve, show

$$i(Y) \leq i(X) \leq di(Y).$$

b) Deduce that the index of a hyperelliptic curve is 1 or 2. (In fact, show that the least degree of a rational point on a hyperelliptic curve is at most 2. Why is this a stronger statement?)

Exercise X.X: a) Show that any elliptic curve is hyperelliptic.
b) Exhibit a genus one curve without rational points which is hyperelliptic.
c) Show that there is a genus one curve (over some field) which is not hyperelliptic.

This definition of hyperelliptic curves differs from the one which is standard in algebraic geometry in two ways: first it allows some curves of genus one (and also all curves of genus zero, but that's of no consequence) to be hyperelliptic. As you can see from the above exercise, any genus 1 curve with a rational point is hyperelliptic, so when $k = \overline{k}$ we would simply be calling all elliptic curves hyperelliptic, and there is nothing gained by doing this. However, in the arithmetic case the term "hyperelliptic curve of genus one" is by no means redundant.

Another definition is that we require the morphism $C \to \mathbb{P}^1$ to be rational over the ground field and that the target curve be k-isomorphic to $\mathbb{P}^1$ (equivalently, to have k-rational points). Let us call a curve **biconic** if there exists a degree 2 separable morphism $f : C \to V$, where V is a smooth genus zero curve (i.e., a plane conic). Note that any biconic curve is geometrically hyperelliptic, and indeed becomes hyperelliptic over some quadratic extension field.

Construction of hyperelliptic curves: for simplicity, we assume now that the characteristic of k is different from 2. Let $C \to \mathbb{P}^1$ be a hyperelliptic curve. Then the function field $k(C)$ of C is a quadratic extension of $k(\mathbb{P}^1) = k(x)$, and therefore is given by taking the square root of a rational function $f = \frac{P}{Q}$. Since $k(x)(\sqrt{\frac{P}{Q}}) = k(x)(\sqrt{PQ})$, we may assume without loss of generality that $f = P(x)$ is a polynomial of degree $d > 0$ and that P has no repeated roots over f. Therefore $k(C)$ is the fraction field of $k[x, y]/(y^2 - P(x))$.

Apply Riemann-Hurwitz: get C has degree g if $d = 2g + 1$ or $d = 2g + 2$. Explain that the point at infinity is singular in the projective model, and that there exist two points at infinity iff the leading coefficient of P is a square in k. C can

be defined by a polynomial of degree $2g+1$ iff it admits a k-rational **Weierstrass point**.

Proposition 4. *A nice curve C of genus $g \geq 1$ is hyperelliptic iff it admits a divisor D with* $\deg(D) = l(D) = 2$.

Proof: Liu Lemma 7.4.8, p. 287.

Corollary 5. *Every curve of genus* 2 *is hyperelliptic.*

Proof: By Riemann-Roch, a canonical divisor K on a genus two curve has $\deg(K) = l(K) = 2$.

Definition: We say that a curve C is **canonical** if the canonical divisor is very ample.

Clearly a canonical curve must have genus at least 2, and by the previous corollay, at least 3. (One might say that a curve of genus 0 is **anti-canonical**.)

Proposition 6. *Let C be a nice curve of genus at least* 2*. Then exactly one of the following holds:*
(i) C is rationally hyperelliptic.
(ii) C is not rationally hyperelliptic but is biconic.
(iii) C is a canonical curve.

Proof: ...

Corollary 7. *Let $g \geq 2$ be an **even** integer, and let $C_{/k}$ be a non-canonical curve, i.e., the canonical map is* $2:1$ *onto a conic curve V. Then (since g is even) this conic has a rational point, and thus C is hyperelliptic.*

Proof: The conic V is a degree $g-1$ curve in $\mathbb{P}^{g-1}$. Since g is even, $g-1$ is odd, therefore the intersection with any hyperplane gives a divisor of odd degree $g-1$ on V. This implies that its index is odd, and therefore its index is one, and therefore (by a previous application of R-R) it has a k-rational point.

Exercise $*.*$: Prove or disprove: let k be a field for which there exists a conic curve $V_{/k}$ without a rational point. (N.B.: equivalently, $\mathrm{Br}(k)[2] \neq 0$. This holds e.g. for all locally compact fields except $\mathbb{C}$, and also for all global fields and all infinite, finitely generated fields.) Show that for any odd g there exists a genus g curve $C_{/k}$ with a $2:1$ map $C \to V$ such that C is **not** hyperelliptic.

2. Canonical curves

I hope you have noticed that we have not, as yet, seen a single canonical curve of genus $g > 1$. As we saw, in genus $g = 0$ or $g = 2$, all curves are hyperelliptic. However, we showed that the isomorphism classes of hyperelliptic curves of genus g form a variety of dimension $2g-1$, whereas we have earlier stated (to be sure, without any kind of justification!) that there is a moduli space of all curves of genus g of dimension $3g-3$. If so, this indicates that for all $g \geq 3$, a general curve of genus g is not hyperelliptic.

So, let's try to see that this is the case, starting with $g = 3$. A canonical curve of genus 3 is embedded in $\mathbb{P}^{3-1} = \mathbb{P}^2$ as a degree 4 hypersurface: i.e., it is a smooth

plane quartic.

We know that any nonbiconic curve of genus 3 is a smooth plane quartic. The smooth plane quartics form an open subset of the complete linear system of all degree 4 divisors on $\mathbb{P}^2$. More concretely, the space of all plane quartics (including the singular, reduced, and/or reducible ones) is naturally isomorphic to $\mathbb{P}(\mathrm{Sym}^4(V))$, where V is a three dimensional k-vector space. Since $\dim \mathrm{Sym}^r(V) = \binom{\dim(V)+r-1}{r}$, this space of all quartics is $\mathbb{P}^{14}$. Of course many of these quartics will be isomorphic to each other. We have at least the group $PGL_3 = \mathrm{Aut}(\mathbb{P}^2)$ acting as linear changes of variables. Thus a sampling space for all canonical curves of genus 3 is birational to $\mathbb{P}^{14}/PGL_3$, so has dimension $14 - (9-1) = 6 = 3 \cdot 3 - 3$.

The upshot of this "back of the envelope" style computation is that if we believe that there really is a 6-dimensional family of moduli of curves of genus 3, then it must be that a general plane quartic is a a canonical curve of genus 3. In fact it is the case that any smooth plane quartic curve is a curve of genus 3 such that the given planar embedding $C \hookrightarrow \mathbb{P}^2$ *is* the canonical embedding: equivalently, intersecting C with a hyperplane gives a canonical divisor. Indeed there is a much more general result about the canonical class on a complete intersection in projective space. These matters are treated well in Hartshorne: we just summarize the results:

Let $Y = F_1 \cap \ldots F_r$ a complete intersection of r hypersurfaces in $\mathbb{P}^N$. Say that F_i has degree d_i.[4] We have

$$\omega_Y \cong \mathcal{O}_Y(\Sigma d_i - N - 1).$$

In plainer langugage: the complete linear system of divisors on Y that we get by intersecting various hyperplanes H with Y is in fact the complete linear system $|nK|$ for some integer multiple n of the canonical divisor K: precisely, $n = \sum_{i=1}^r d_i - (N+1)$.

This is an exceedingly useful result. For instance, the case at hand is $r = 1$, $d = 4$, $N = 2$. It tells us that the divisor $H \cap C$ on a plane quartic curve is $4 - (2+1)$ times the canonical divisor: in other words, it *is* the canonical divisor, so this is the canonical embedding, as we wanted.

More generally, let $C_d \subset \mathbb{P}^2$ be a smooth plane curve of degree d. We get $K \sim (d-3)(H \cap C)$. But we know that the degree of $H \cap C$ is the degree of C: d, so this tells us that

$$2g(C_d) - 2 = \deg(K) = d(d-3),$$

and thus

$$g(C_d) = \frac{(d-1)(d-2)}{2}.$$

In other words, the genus of any smooth plane curve of degree d is $\frac{(d-1)(d-2)}{2}$.

[4]It follows from the Bertini theorem, valid over any infinite field k, that for any set of positive integersd_i there exist hypersurfaces of those degrees such that their intersection is smooth of codimension r.

Remark: This is also a special case of the important **adjunction formula** for a curve on an algebraic surface. (More on this later...)

In particular, curves of degree 1 and 2 have genus zero, curves of degree 3 have genus one, and curves of degree at least 4 have higher genus. We also get that for $d > 3$, the canonical divisor is a positive multiple of a very ample divisor, so is itself very ample: thus such curves are not biconic.

This gives us many examples of canonical curves, since it is no trouble to write down a smooth plane curve of any given degree. For instance, over $k = \mathbb{Q}$ (or any field whose characteristic does not divide d), the curve

$$F_d : X^d + Y^d + Z^d = 0$$

is a smooth plane curve of degree d, hence a nonhyperelliptic curve of genus $\frac{(d-1)(d-2)}{2}$.

Example (two ways to view a genus one curve as a complete intersection): In the more general case of r hypersurfaces of degrees $d_1, \ldots, d_r$ intersecting in $\mathbb{P}^{r+1}$ we will get a genus one curve precisely when $d_1 + \ldots + d_r = r + 2$. Notice that it adds nothing new to consider any $d_i = 1$ – it simply means that the complete intersection can be viewed as taking place in a smaller projective space. There are not very many ways to add up r integers each greater than 1 and attain $r + 2$; indeed we have only $3 = 1 + 2$ and $2 + 2 = 2 + 2$, corresponding to a plane cubic and to the intersection of two quadric surfaces in $\mathbb{P}^3$.

Unfortunately this also shows that the curves which can be embedded in $\mathbb{P}^2$ are extremely limited. On the one hand, there are no such hyperelliptic curves (quite generally, the above formula shows that the canonical class of a complete intersection is ample iff it is very ample). On the other hand, even on the level of genera we are getting only a very sparse set: e.g. there are no plane curves of genus 2, 4 or 5.

One way to generalize the above is to consider complete intersections of $N - 1$ hypersurfaces in $\mathbb{P}^N$ rather than just one hypersurface in $\mathbb{P}^2$. This indeed helps a bit. For instance:

Proposition 8. *Let $C_{/k}$ be a nonhyperelliptic curve of genus 4. Then its canonical embedding is the complete intersection of an irreducible quadric and an irreducible cubic. Conversely, any such nonsingular curve in $\mathbb{P}^3$ is a canonical curve of genus 4.*

We omit the proof: see e.g. Hartshorne.

However, even complete intersections are a very limited class of curves:

Exercise: Find the smallest integer g such that no smooth curve of genus g can be a complete intersection in projective space.

So we need to do something else to construct even a single canonical curve of each given genus $g \geq 3$ (let alone to find a $3g-3$-dimensional family of such curves).

From the perspective of the function field, there is little difficulty in constructing curves of higher genus which are not evidently hyperelliptic. By separable Noether normalization, any nice curve $C_{/k}$ admits a finite separable map to the projective line. Turning this around, this means that any function field is a finite separable map of the rational function field $k(t)$. If we choose a finite separable extension $L/k(t)$ then, with suitable technique, we can use the Riemann-Hurwitz formula to compute the genus of the corresponding curve C (i.e., with $k(C) \cong L$). By definition, hyperelliptic curves arise this way from quadratic field extensions $L/k(t)$; by taking any higher degree d for $[L : k(t)]$, we get a curve which is not necessarily hyperelliptic.

To take a simple example, let p be a prime number – which we shall assume is not the characteristic of k – and let us consider field extensions L which are obtained by simply adjoining a pth root of a nonconstant function $f \in k(t)$. Note that $L/k(t)$ is Galois iff k contains the pth roots of unity, in which case the Galois group is cyclic. In any case, the geometric extension $\overline{L} = \overline{k}L$ of $\overline{k}(t)$ is cyclic, so the curve that we get has the cyclic group $C_p = \langle \varphi \rangle$ as a group of automorphisms, with $C/\varphi \cong \mathbb{P}^1$. Such curves are called **superelliptic**.

Any superelliptic curve has the plane equation

$$y^p = P_1(x)^{a_1} \cdots P_r(x)^{a_r},$$

where each $P_i(x)$ is a separable irreducible polynomial over k, and $0 < a_i < p$ for all i. To fix ideas, suppose we take

$$y^p = \prod_{i=1}^{2n} (x - a_i),$$

where $a_1, \ldots, a_{2n}$ are distinct elements of k. As in the hyperelliptic case, taking the number of branch points to be even means that the point at infinity on $\mathbb{P}^1$ is not a branch point. So we have $2n$ different fixed points. Moreover, since the extension $\overline{L}/\overline{k}(t)$ is Galois, the ramification indices over the preimages must all be equal. This means that they must all be equal to p, i.e., we have full ramification at each point. The Riemann-Hurwitz formula then gives

$$2g(C) - 2 = p(2g(\mathbb{P}^1) - 2) + \sum_{i=1}^{n} (p-1) = 2n(p-1) - 2p,$$

so

$$g(C) = 1 + n(p-1) - p = n(p-1) - (p-1) = (n-1)(p-1).$$

Note that if $p > 2$ the genus is always even, and conversely every curve of even genus can be obtained for $p = 3$.

We now wish to show that most of these curves are canonical, i.e., not geometrically hyperelliptic. This is a special case of a very interesting problem: given a curve $C_{/k}$, find all degrees of maps $C \to \mathbb{P}^1$. Let us call this the **degree sequence** $D(C)$. As we have seen, it makes a difference here whether the ground field is algebraically closed: e.g. there exist curves which are geometrically hyperelliptic but not hyperelliptic. So let us also define $\overline{D}(C) := D(C_{\overline{k}})$, the **geometric degree sequence**.

Remark on terminology: if $d \in D(C)$, then C is said to be d-gonal. When $d = 3$, one says "trigonal". We warn that in practice it is often the case that the terminology "d-gonal" is used when "geometrically d-gonal" is meant.

The least element of $D(C)$ (resp. $\overline{D}(C)$) is called the **gonality** (resp. the **geometric gonality**) of C. This is an important numerical invariant of a curve both geometrically and arithmetically. As for the latter:

Exercise: Suppose $C_{/k}$ is a nice curve.
a) Show that the index of C divides the gonality of C.
b) Show that the gonality of C divides $2g(C) - 2$.

Coming back to our goal of constructing many canonical curves, here now is the intuition: a curve of large genus will not admit two "independent" maps $x, y : C \to \mathbb{P}^1$ of small degrees d_1 and d_2. Here independent can be made precise as follows: $k(x, y) = k(C)$. Thus $k(C)$ is the fraction field of a ring $k[x, y]/P(x, y)$, where $P(x, y)$ is a polynomial relation between x and y. Here the degree of $P(x, y)$ in x (resp. in y) is d_1 (resp. d_2), so the total degree of P is at most $d = d_1 + d_2$. But the genus of the normal model of a plane curve of degree d is at most $\frac{(d-1)(d-2)}{2}$.

One easy way to ensure that the maps x, y are "independent" is to require that their degrees d_1 and d_2 be coprime: then $[k(C) : k(x, y)]$ divides $[k(C) : k(x)] = d_1$ and $[k(C) : k(y)] = d_2$, so $[k(C) : k(x, y)] = 1$. In particular, for any odd prime p, if C is a curve of genus

$$g > \frac{(p+1)p}{2}$$

with a morphism $x : C \to \mathbb{P}^1$ of degree p, then C cannot also have a degree 2 morphism to $\mathbb{P}^1$: that is, C is not hyperelliptic. Taking $p = 3$, we have proved:

Theorem 9. *Let k be a field of characteristic different from 3. Then for any integer $n > 3$, there exists a nice curve $C_{/k}$ of genus $2n$ which is trigonal but not geometrically hyperelliptic.*

This was just a first effort: the argument can be refined and extended in many ways. For instance:

Theorem 10. *(Accola, Namba) Let $C_{/k}$ be a nice curve admitting finite morphisms $x, y : C \to \mathbb{P}^1$ of degrees d_1 and d_2 respectively. Assume the morphisms are independent in the sense that $k(C) = k(x, y)$. Then*

$$g(C) \leq (d_1 - 1)(d_2 - 1).$$

This shows that the superelliptic trigonal curves constructed above of genus 4 and 6 are also canonical.

Exercise: Prove Theorem of Accola and Namba, according to the following outline:
(a) Note that it suffices to assume $k = \overline{k}$.
(b) Adjust g by a linear automorphism so that the branch loci of x and y are distinct. Consider the map $\phi : C \to \mathbb{P}^2$ by $p \mapsto [x(p) : y(p) : 1]$. Show that the

independence of x and y implies that the map $\phi : C \to \phi(C)$ is birational. Equivalently, the image $C' = \phi(C)$ is a plane curve and $\phi : C \to C'$ is its normalization. (c) Show that C has a singularity at $[1 : 0 : 0]$ (resp. $[0 : 1 : 0]$) of multiplicity d_1 (resp. d_2). Using the formula for the genus of a singular plane curve, show that – with $d = d_1 + d_2$ –

$$g(C) \leq \frac{(d-1)(d-2)}{2} - \frac{(d_1-1)(d_1-2)}{2} - \frac{(d_2-1)(d_2-1)}{2}.$$

Exercise: For which genera can you construct a superelliptic, nonhyperelliptic curve of genus g?

Theorem 11. *For any algebraically closed field k and any any prime number p, there exists a curve $C_{/k}$ whose gonality is exactly p.*

Exercise: Prove it.

3. Weierstrass points

Let $C_{/k}$ be a nice curve of genus g. A **Weierstrass point** on C is a geometric point P such that $l(|gP|) > 1$. To understand this definition, note that Riemann-Roch guarantees that $l(n|P|) > 1$ as long as $n > g$.

Exercise: Show that curves of genus 0 or 1 have no Weierstrass points.

Exercise: Show that the Weierstrass points on a hyperelliptic curve of genus $g \geq 2$ are precisely the preimages of the hyperelliptic branch points. In particular there are $2g + 2$ Weierstrass points.

Weierstrass gap sequence:

Theorem 12. *(Hurwitz) Let C be a nice curve of genus g over a field k of characteristic 0. Then the degree of the Weierstrass divisor is*

$$\deg(\mathbb{W}) = g^3 - g.$$

Let N be a positive integer. There is an algebraic curve $X_0(N)_{/\mathbb{Q}}$, which is the coarse moduli space for the moduli problem of pairs (E, C) where E is an elliptic curve and $C \subset E$ is a cyclic order n subgroup scheme. Well, almost. The moduli space of elliptic curves is the affine line $\mathbb{A}^1$ (via the j-invariant), and there are no elliptic curves with $j = \infty$. Thus $\mathbb{P}^1$ is the natural compactification of the smooth affine curve which is the coarse moduli space of elliptic curves. Similarly, the true coarse moduli space of the above moduli problem is denoted $Y_0(N)$, and its compactification is denoted $X_0(N)$. The compactification is obtained by adding the preimages of the point ∞ on the projective line; this is a finite set of points called **cusps**.

Since the Weierstrass points and the cusps are both "special points" on $X_0(N)$, it is reasonable to ask whether any of the cusps are Weierstrass points. This was first investigated by Atkin and Lehner in the 1960's; they found that if N is divisible by a sufficiently large power of a prime then indeed at least one of the cusps is

a Weierstrass point. However, the case of squarefree N is different. For instance, William Stein has computed that for all squarefree $N < 3000$, none of the cusps are Weiertrass points. There is also a beautiful theoretical result due to Ogg:

Theorem 13. *(Ogg) Let N be a positive integer such that $X_0(N)$ has genus 0 (a finite list of N), and let p be a prime which is prime to N. Then none of the Weierstrass points on $X_0(pN)$ are cusps.*

The proof uses exactly the sort of methods we wish to discuss towards the end of the course: the theory of models of curves.

4. The automorphism group

Let C be a nice curve over a field k. By the **automorphism group** $\mathrm{Aut}(C)$ we mean the group of self-isomorphisms of the geometric curve $C_{/\overline{k}}$. When k is perfect, there is a natural action of the Galois group $\mathrm{Gal}(\overline{k}/k)$ on $\mathrm{Aut}(C)$ such that for any algebraic extension l, the $\mathrm{Gal}(\overline{k}/l)$-fixed points are precisely the automorphisms which are defined over l. One might then write $\mathrm{Aut}(C)(l)$ for the set of l-rational automorphisms.

Exercise X.X: If k is not perfect, is every automorphism of C defined over a separable extension of k?

The following is a simple but extremely useful observation about automorphisms and linear systems.

Proposition 14. *Let $C_{/k}$ be a curve and $\varphi \in \mathrm{Aut}(C)(k)$ be a k-rational automorphism. Let $D \in Div(C)$ be an effective divisor such that $\varphi^*(D) \sim D$ (linearly equivalent). Then φ extends to a linear automorphism of $\mathbb{P}^(\ell(D) - 1)$ making the following diagram commute:*

$$C \to \mathbb{P}^{\ell(D)-1}$$
$$C \to \mathbb{P}^{\ell(D)-1}.$$

Proposition 15. *Let C be a curve of genus g and $\{P_1, \ldots, P_{2g+3}\}$ be a set of distinct geometric points. Suppose that $\varphi(P_i) = P_i$ for all i. Then φ is the identity.*

Proof: Suppose by way of contradiction that φ is not the identity. Then there exists a geometric point P which is not fixed by φ (recall that any variety of positive dimension over an algebraically closed field has infinitely many closed points); say $Q = \varphi^*(P)$. By Riemann-Roch, for some d with $1 \leq d \leq g+1$ there exists a rational function f on C whose polar divisor is $(f)_\infty = d[P]$. Then the polar divisor of $g := f - \varphi^*(f)$ is $d[P] + d[P']$, hence of degree $2d \leq 2g+2$. Therefore the divisor of zeros of g also has degree $2d \leq 2g+2$, but on the other hand every fixed point of f is also a zero of g, and we assumed that f has at least $2g+3$ fixed points: contradiction!

Remark: Of course the bound is sharp, since the hyperelliptic involution on a hyperelliptic curve of genus g has precisely $2g+2$ distinct geometric fixed points.

If $g = 0$, then $\mathrm{Aut}(C) \cong PGL_2(\overline{k})$. Moreover, when $C \cong \mathbb{P}^1$, then $\mathrm{Aut}(C)(k) \cong PGL_2(k)$. To see this, we reduce to the case in which $C \cong_k \mathbb{P}^1$. There exists a unique class D of divisors of degree 1, so if $\varphi : C \to C$ is any automorphism we

certainly must have $\varphi^*(D) \sim D$. Thus the automorphism extends to the ambient projective space $\mathbb{P}^1$, which is just $\varphi_D(C)$. This shows that every abstract automorphism of $\mathbb{P}^1$ is a linear automorphism, so $\mathrm{Aut}(\mathbb{P}^1) = PGL_2$.[5]

Remark: Suppose C has genus zero but $C(k) = \emptyset$. We mentioned briefly that C corresponds to a division quaternion algebra $B_{/k}$. This quaternion algebra has inside it a copy of k, so its unit group $B^\times$ has in it a copy of $k^\times$. By definition put $PGL(B) := B^\times/k^\times$. One can show that $\mathrm{Aut}(C)(k) = PGL(B)$. Note that if l/k is a field extension such that $C(l) \neq \emptyset$, then $B \otimes_k l \cong M_2(l)$, and indeed $PGL(B_{/l}) = PGL(M_2(l)) = PGL_2(l)$.

In summary, the automorphism group of a genus zero curve is infinite, and moreover has the natural structure of a connected linear algebraic group over k, of dimension 3.

Now let $C_{/k}$ be a curve of genus 1. Choosing a point $O \in C(\overline{k})$, we get a group law on $C_{/\overline{k}}$, so that a subgroup of $\mathrm{Aut}(C)$ is given by the translations by geometric points: namely $C(\overline{k})$. Another subgroup $\mathrm{Aut}(C,O)$ of $\mathrm{Aut}(C)$ is given by the automorphisms which fix the point O. This subgroup is nothing else than the unit group of the endomorphism ring $\mathrm{End}(E)$. In (relatively) elementary elliptic curve theory all possibilities for $\mathrm{End}(E)$ are computed: when $\mathrm{char}(k) = 0$, $\mathrm{End}(E)$ is either $\mathbb{Z}$, or is an order in an imaginary quadratic field. In any case $\mathrm{Aut}(C,O)$ is cyclic of order 2, 4 or 6. Indeed, up to isomorphism over $\overline{k}$ there is exactly one elliptic curve whose automorphism group has order 4 (resp. order 6): namely the one with $j = 1728$ (resp. $j = 0$). In positive characteristic all of the above endomorphism rings are possible (for a suitable choice of k) and also the endomorphism ring could be a rational quaternion algebra B which is ramified at ∞ and p. The ramification at ∞ means that $B \otimes_{\mathbb{Q}} \mathbb{R}$ is still a division algebra over $\mathbb{R}$. This implies that the unit group is both discrete and compact and therefore finite. In fact it is isomorphic to one of the following groups: ....

The two subgroups $C(\overline{k})$ and $\mathrm{Aut}(C,O)$ clearly intersect in identity. A bit of thought shows that

$$\mathrm{Aut}(C) \cong C(\overline{k}) \rtimes \mathrm{Aut}(C,O).$$

Thus the geometric automorphism group of a genus one curve is an extension of a connected projective algebraic group by a nontrivial finite group.

Remark: It can be shown that, in general, if $V_{/k}$ is a projective variety, then $\mathrm{Aut}(V_{/}\overline{k})$ has the structure of a **locally finite algebraic group scheme**, namely the extension of a connected group variety by a component group which is at most countable. Note that if the component group is inifnite, then the automorphism group is not an algebraic variety.

Now we assume that $g \geq 2$. Our goal is to show that $\mathrm{Aut}(C)$ is finite.

Assume first that k has characteristic 0, so that the set S of distinct Weierstrass

[5]The same argument in fact works for $\mathbb{P}^N$ for any N.

points is nonempty and finite. Because of the intrinsic nature of Weiertrass points we have a natural action of $\mathrm{Aut}(C)$ on S. Note that by the above, if the set of distinct Weierstrass points has cardinality at least $2g+3$, then this action is necessarily effective: i.e., any automorphism that fixes all the Weierstrass points is the identity, i.e.,

$$\mathrm{Aut}(C) \hookrightarrow \mathrm{Sym}(S),$$

which shows that $\mathrm{Aut}(C)$ is finite. Notice however, that if C is hyperelliptic there are precisely $2g+2$ Weierstrass points, and as above there *is* a nontrivial automorphism which fixes all the Weierstrass points, namely the hyperelliptic involution.

In fact this proof can be made to go through: first assume that C is not hyperelliptic. Then an analysis of the weights on the Weierstrass divisor shows that the set of distinct Weierstrass points has cardinality at least $2g+3$.

Consider now the hyperelliptic case.

Proposition 16. *Let C be a hyperelliptic curve of genus $g \geq 2$. Then the hyperelliptic involution ι lies in the center of* $\mathrm{Aut}(C)$.

Proof: Let $\sigma \in \mathrm{Aut}(C)$. Put $\iota' := \sigma\iota\sigma^{-1}$. Then ι' is also an involution; on the quotient C/ι' we identify Q with $\sigma\iota\sigma^{-1}Q$ for all Q. But this is the same equivalence relation as identifying P with ιP, so the quotient is again isomorphic to $\mathbb{P}^1$. Hence ι' is again a hyperelliptic involution. But the hyperelliptic involution is unique, so $\iota' = \iota$.

So let σ be an automorphism of C which fixes all $2g+2$ hyperelliptic fixed points. Then σ commutes with ι so σ induces an automorphism on the quotient $C/\iota \cong \mathbb{P}^1$. On the quotient, σ fixes all of the hyperelliptic fixed points, of which there are $2g+2 \geq 6 > 3$, so σ is the identity automorphism on $\mathbb{P}^1$. This means that for all points P, we have either $\sigma(P) = P$ or $\sigma(P) = \iota(P)$. Taking P to be any single non-hyperelliptic point, if $\sigma(P) = P$ then σ fixes $2g+3$ points so is the identity; if $\sigma(P) = \iota(P)$ then $\iota \circ \sigma$ fixes $2g+3$ fixed points, so is the identity, i.e., $\sigma = \iota$.

In fact this case of the argument works in arbitrary characteristic, since instead of saying "Weierstrass point" we can say "hyperelliptic branch point" which is again a canonical set of points.

4.1. **Curves without automorphisms: a theorem of Poonen.**

It has long been a sort of "folklore" that for any $g \geq 3$, a "sufficiently general" complex algebraic curve of genus g has trivial automorphism group. The modern interpretation of this is that there is a nonempty Zariski open subset of $(\mathcal{M}_g)_{/C}$ consisting of curves with this property. In fact, with some goodwill about the existence of $\mathcal{M}_g$, it is relatively easy to see that this locus of curves is Zariski-open: indeed, for any fixed finite group G, the locus of curves having a subgroup of automorphisms isomorphic to G is Zariski-closed (a nice way to see this is to consider the tricanonical representation of $\mathrm{Aut}(C)$; we do not enter into the details here!). Since we have now proven that there are only finitely many possibilities for the automorphism group in any fixed genus, the complement of these sets is open. In other words, the only thing to worry about is that there is a fixed nontrivial group G such that *every* curve of genus g has automorphisms by this group. (Since this

is exactly what happens in genus 2 with $G = C_2$, obviously this worry needs to be taken seriously!) Thus to believe that the generic curve is automorphismless it suffices to exhibit a single one.

Already in the work of Hurwitz one finds the claim that the general complex curve of genus $g \geq 3$ has no automorphisms, but the first person to rigorously prove this was W. Baily in 1961. A proof valid for any algebraically closed field k was given in the 1962 PhD thesis of Paul Monsky (at U. of Chicago, under W. Baily). This leaves open two points: first, what about curves over an arbitrary field k? Second, can the curves be written down explicitly?

Through a relatively explicit procedure, Accola in 1970 constructs autless trigonal complex curves of every genus $g \geq 5$. Note that none of the trigonal curves we constructed were autless: the reason is that we chose our cubic extensions to be (geometrically) Galois: a more general cubic extension of the form $k(C) = k(t)(f)$, where f is a root of

$$y^3 + a_2(t)y^2 + a_1(t)y + a_0(t) = 0$$

will indeed give more leeway.

Only about ten years ago did Bjorn Poonen solve the general problem, constructing for any field k – of characteristic $p \geq 0$ – and any $g \geq 3$ an autless curve $C_{/k}$ of genus g. Indeed his curves are all trigonal. The equations are as follows: Case 1: $p = 3$, $g \equiv 0$ or $1 \pmod 3$:

$$y^3 + y^2 = x^{g+1} - x^3 + 1.$$

Case 2: $p = 3$, $g \equiv 2 \pmod 3$:

$$y^3 + y^2 = x^2(x-1)^2(x^{g-1} - x^3 + 1).$$

Case 3: $p \neq 3$, $g \not\equiv 2 \pmod 3$, $g \not\equiv 0, -1 \pmod p$:

$$y^3 - 3y = gx^{g+1} - (g+1)x^g + 1.$$

...

5. An embedding theorem and an immersion theorem

We wish here to present two theorems on curves, each of which tells us that all nice curves can be represented in a certain relatively concrete way. Of course, we wish to pursue these theorems over an arbitrary ground field k, which turns out not quite to be possible.

Theorem 17. *Let k be an infinite field. Then any nice curve $C_{/k}$ can be embedded in $\mathbb{P}^3_{/k}$.*

This result is not true for all curves over a finite field. Indeed, one has the following:

Proposition 18. *Let q be any prime power and N a positive integer. Then there exists a nice curve $C_{/\mathbb{F}_q}$ such that $\#C(\mathbb{F}_q) > N$.*

Exercise X.X: Prove it! (Suggestion: take C to be a hyperelliptic curve defined by a monic polynomial of large degree with many rational roots.)

This has the following consequence:

Corollary 19. *For any finite field $\mathbb{F}_q$ and any positive integer N, there exists a nice curve $C_{/\mathbb{F}_q}$ which cannot be embedded into $\mathbb{P}^N$.*

Proof: Indeed, if $C \hookrightarrow \mathbb{P}^N$ is an embedding over $\mathbb{F}_q$, then $\#C(\mathbb{F}_q) \leq \#\mathbb{P}^N(\mathbb{F}_q) = \frac{q^{N+1}-1}{q-1}$. But according to the proposition, we can find curves with arbitrarily many $\mathbb{F}_q$-rational points.

Theorem 20. *Let k be any infinite field and $C_{/k}$ a nice curve. Then there exists a plane curve $Y_{/k}$ whose only singularities (if any) are ordinary double points, such that $k(Y) \cong k(C)$ – i.e., Y is birational to C.*

Exercise: Show that this theorem also cannot hold for a curve C over a finite field k with sufficiently many k-rational points. Hint: C is isomorphic to the normalization $\tilde{Y}$ of Y. Consider the composition with the normalization map:

$$C \cong \tilde{Y} \to Y \hookrightarrow \mathbb{P}^2.$$

By using a bound on the cardinality of the fibers of $\tilde{Y} \to Y$, get a contradiction.

Proof of Theorem 1: Let C be a nice curve which is already embedded in projective space $\mathbb{P}^N$ for some $N \geq 4$. We want to show that C can also be embedded in $\mathbb{P}^3$. The idea is quite geometric: if H is a hyperplane in $\mathbb{P}^N$ and x is any k-valued point of $\mathbb{P}^N$ not contained in $H \cup C$, then there is a natural projection map from $\mathbb{P}^n \setminus x \to H$. Namely, for any point $x' \neq x$, we consider the unique line ℓ through x and x'. Since x is not in H, certainly ℓ does not lie in H and therefore $\ell \cap H$ consists of a single point $\pi(x')$. (If x' is l-rational for some extension field l/k, then so is $\pi(x')$.

The idea here is that if $N \geq 4$ and we choose a **sufficiently general** point x of $\mathbb{P}^N$, then the induced map $\pi : C \to \pi(C)$ will be an isomorphism, hence embedding C in a hyperplane of one smaller dimension. To be clear, this doesn't make complete sense yet – two obvious questions are (i) what does "sufficiently general" mean, and (ii) why does this construction work when $N \geq 4$ and not otherwise?

Let us examine what would cause the projection map not to be an embedding. If y and z are in $C(\overline{k})$, then $\pi(y) = \pi(z)$ iff the lines ℓ_{xy} and ℓx_z coincide, i.e., iff x, y and z are collinear. Another way of stating this is to consider the **secant variety** to C, which is the union of all secant lines ℓ_{yz} between distinct points on C. However, reecall that being an embedding in the geometric sense means being a "closed immersion", which means that we want the induced map on Zariski tangent spaces to be injective. This means that we also don't x to line on any of the tangent lines to any of the points y on C. Since a tangent line is just a limit of secant lines, this second condition just lies in the closure of the first, so is very natural.

To be precise, let us define the closed secant variety of C in $\mathbb{P}^N$ to be the closure of the subvariety of all secant lines to C. The secant variety itself is easily seen to be a locally closed subset of $\mathbb{P}^N$, hence itself a quasi-projective variety with a well-defined dimension d, which must also be the dimension of the closed secant variety.

Clearly the secant variety is determined by giving a line in $\mathbb{P}^N$ for each pair of

points on C, so it is three-dimensional. Therefore, if $N \geq 4$, the closed secant variety is a proper Zariski-closed subset of $\mathbb{P}^N$, and we need only apply the following easy result:

Proposition 21. *Let k be any infinite field, and let $V \subset \mathbb{P}^N$ be a Zariski-closed subset, with $\dim(V) < N$. Then $\mathbb{P}^N(k) \setminus V(k)$ is Zariski-dense in $\mathbb{P}^N$: in particular the set is infinite.*

Exercise: Prove it!

Exercise: To what extent does the projection map $\mathbb{P}^N \setminus x \to H$ depend on the choice of the hyerplane H?

Exercise: Show that if $\mathbb{F}_q$ is a finite field, then for any curve $C_{/\mathbb{F}_q}$ there exists a finite extension field $\mathbb{F}_{q^a}$ such that $C_{/\mathbb{F}_{q^a}}$ embeds in $\mathbb{P}^3$. Can a be chosen to be independent of C?

Exercise: Rephrase the above argument employing the language of incomplete linear systems. (Hint: For instance, Hartshorne uses this language.)

The proof of Theorem X.X is in fact a continuation of the proof of Theorem X.X. Namely, we have our nice curve C over an infinite field k embedded in $\mathbb{P}^3$, and once again we want to drop the dimension by 1 by projecting from a suitable point onto a fixed hyperplane. Since in this case the closed secant variety will be all of $\mathbb{P}^3$, we cannot expect the map to be an injection on points. However, since the dimension of the closed tangent variety is only 2, we still have a chance of finding an "immersion" of C in $\mathbb{P}^3$ in the more usual geometric sense: i.e., a map which is only an embedding locally. Let us consider the situation more carefully:

A **multisecant** of $C \subset \mathbb{P}^3$ is a line in $\mathbb{P}^3$ which meets X in at least three different (geometric) points. A **secant with coplanar tangent lines** is just what it sounds like: a secant joining distinct points y and z on C such that the tangent lines ℓ_y and ℓ_z lie in the same plane: equivalently, ℓ_y and ℓ_z intersect. (Recall that linear geometry in $\mathbb{P}^N$ is best understood by considering linear subspaces of one dimension higher in the associated affine space k^{N+1}.)

Proposition 22. *Let $C \subset \mathbb{P}^3$ be a curve, x a point not on C, and $\varphi : C \to \mathbb{P}^2$ the associated projection map. Then φ is birational onto its image with at most ordinary double point singularities if:*
(i) x lies on only finitely many secants of X.
(ii) x does not lie on any tangent line of X.
(iii) x does not lie on any multisecant of X.
(iv) x does not lie on any secant with coplanar tangent line.

This is a good exercise in honest geometric thinking and is left to the reader.

It remains to check that a sufficiently general point x satisfies all these conditions; it is enough to check that each of the conditions holds on the complement of a proper, Zariski-closed subset. This takes some honest work, and we refer the reader to Hartshorne, pp. 311-314.

Exercise: Read through Hartshorne's proof, and convince yourself that it remains valid verbatim for any infinite field k.