# HOW MANY RATIONAL POINTS CAN A CURVE HAVE?

LUCIA CAPORASO, JOE HARRIS, AND BARRY MAZUR

## CONTENTS

## 1. INTRODUCTION

This paper is concerned with two conjectures in number theory describing the behavior of the number of rational points on an algebraic curve defined over a number field, as that curve varies.

**Uniformity Conjecture.** *Let $K$ be a number field and $g \geq 2$ an integer. There exists a number $\mathrm{B}(K, g)$ such that no smooth curve $X$ of genus $g$ defined over $K$ has more than $\mathrm{B}(K, g)$ $K$-rational points.*

**Universal Bound Conjecture.** *Let $g \geq 2$ be an integer. There exists a number $\mathrm{N}(g)$ such that for any number field $K$ there are only finitely many smooth curves of genus $g$ defined over $K$ with more than $\mathrm{N}(g)$ $K$-rational points.*

It is worth pointing out here that, in the statement of the Universal Bound Conjecture, by "finitely many curves" we really mean "finitely many $K$-isomorphism classes of curves".

The first Conjecture comes naturally from a well known theorem of Faltings, to the effect that any smooth curve of genus $g \geq 2$ defined over a number field $K$ has only finitely many $K$-rational points. The second may at first seem less likely. In both cases, our motivation for considering these questions is the recent theorem [CHM] that they are consequences of the

*Lang Conjectures*. For a discussion of this theorem, see the companion paper [C] in this volume; for a broader discussion of the Lang Conjectures, see [L].

The purpose of this note is not to offer any arguments for the truth or falsity of these conjectures, but rather to record what can be said at present about the numbers $\mathrm{B}(\mathbb{Q}, g)$ and $\mathrm{N}(g)$ assuming they exist (when we speak of $\mathrm{B}(K, g)$ and $\mathrm{N}(g)$ we mean the minimal number for which the conclusion of the corresponding conjecture holds). We do this in hopes of stimulating further discussion concerning these questions.

To begin with, the current records for $\mathrm{B}(\mathbb{Q}, g)$ for low values of $g$ are

$\mathrm{B}(\mathbb{Q}, 2) \geq 144$ (A. Brumer)
$\mathrm{B}(\mathbb{Q}, 3) \geq 72$ (A. Brumer)
$\mathrm{B}(\mathbb{Q}, 4) \geq 126$ (N. Elkies)
$\mathrm{B}(\mathbb{Q}, 5) \geq 132$ (N. Elkies)

One can also ask for lower bounds for $\mathrm{B}(K, g)$ for fixed number fields $K$ and varying $g$; and for $\mathrm{N}(g)$ for varying $g$. We will sketch below some methods for producing such lower bounds. In response to the circulation of a draft of this note, A. Brumer and J.-F. Mestre have independently produced methods yielding better bounds than ours (the more elementary of Mestre's methods is described in section 5 below). One common feature of all the presently known methods is that they produce bounds of the form $c \cdot g + O(1)$. It is thus natural to speculate about the possible constants $c$, by defining

$$\overline{\mathrm{B}}(K) = \limsup_{g \to \infty} \frac{\mathrm{B}(K, g)}{g}.$$

and

$$\overline{\mathrm{N}} = \limsup_{g \to \infty} \frac{\mathrm{N}(g)}{g}.$$

and asking whether $\overline{\mathrm{B}}(K)$ and $\overline{\mathrm{N}}$ are finite.

The methods we outline in this paper currently give $\overline{\mathrm{B}}(\mathbb{Q}) \geq 6$ and $\overline{\mathrm{N}} \geq 8$. We are happy to list the following improvement on these bounds:

Mestre: For all $g$, $\mathrm{B}(\mathbb{Q}, g) \geq 8g + 12$, and $\mathrm{N}(g) \geq 16(g + 1)$.

Brumer: For all $g$ and for $K$ any field containing a primitive $(g + 1)^{st}$ root of unity, $\mathrm{B}(K, g) \geq 16(g + 1)$; and for all $g$, $\mathrm{N}(g) \geq 16(g + 1)$.

We should also mention a very recent note of Abramovich in which he proves that, assuming the Weak Lang Conjecture, the number $\mathrm{B}(K, g)$ is bounded as $K$ varies over all quadratic extensions of a given number field.

The results of sections 3 and 4 of this paper are based largely on conversations with David Eisenbud, Noam Elkies and Nick Shepherd-Barron, to whom we are very grateful. The results of section 5.3 are, as the title suggests, entirely the work of J.-F. Mestre. We thank the referee of this paper for his/her detailed report, and for noticing and correcting a mistake in Corollary 5.1.

## 2. Lower bounds on $\mathrm{B}(\mathbb{Q}, g)$

Here is a simple method of obtaining smooth curves of a given genus with a fair number of $\mathbb{Q}$-rational points. As we indicated in the introduction, the results obtained in this section are weaker, for all but finitely many values of $g$, than the results obtained by Mestre in section 5.3; we include this discussion in the hopes that an improvement of the method (or a combination of the two) may yield stronger results still.

Suppose we have an $m$-dimensional linear system of curves on a surface $S$ defined over $\mathbb{Q}$, whose general member is a smooth curve of genus $g$. For any $m$ rational points $p_1, \ldots, p_m$ of $S$ there will exist at least one member $C$ of the linear series passing through them; if the linear system is base point free and the points are suitably general on $S$, $C$ will be a general member of our linear series and so will be a smooth curve of genus $g$ possessing at least $m$ rational points. The only further wrinkle we will introduce is this: if in addition we can ensure that $C$ has nontrivial automorphisms defined over $\mathbb{Q}$, we may hope that applying these automorphisms to the points $p_i$ will produce more rational points.

Given that our goal is to locate linear series whose dimension is large relative to the genus of their members, where do we look? Compare the adjunction formula

$$g = \frac{C \cdot C + K_S \cdot C}{2} + 1$$

for the genus of a curve $C$ on a surface $S$, and the Riemann-Roch formula, which in case $\mathcal{O}(C)$ has no higher cohomology says that

$$\dim(|C|) = h^0(\mathcal{O}_S(C)) - 1 = \frac{C \cdot C - K_S \cdot C}{2} + \chi(\mathcal{O}_S) - 1$$

where $|C|$ is the complete linear series associated to $C$. Together, these suggest the answer: on a surface whose canonical bundle is as negative as possible. The first places to look, accordingly, are rational surfaces. (This has the further virtue of making it easy to locate as many rational points on $S$ as we want, in as general position as we want.) Now, any rational surface is a blow-up of either $\mathbb{P}^2$ or a rational ruled surface; and if we compare the self-intersection $C \cdot C$ and intersection number $K_S \cdot C$ with the canonical class of a curve $C$ on such a blow-up to its image in the plane or ruled surface, we see we might as well restrict our attention to the latter: the self-intersection of the image will be greater, and the intersection number with the canonical bundle less, for the image curve than for the original.

Moreover, as between the plane and ruled surfaces, the latter have an advantage: since all line bundles on the plane are rational multiples of each other, as the degree of a curve in the plane grows its self-intersection must increase quadratically, while its intersection number with the anticanonical increase linearly. Thus asymptotically the dimension of a linear class can only increase linearly. Thus asymptotically the dimension of a linear series in the plane can only grow as fast as the genus, giving us curves with $g + o(g)$ rational points. Inasmuch as the Picard number of a rational ruled surface is 2, however, we have the option of taking curves whose class is not simply a multiple of the canonical class; and this, as we will see, will allow us to choose curves of increasing genus whose intersection numbers with the anticanonical class grow at the same rate as their self-intersections.

We are thus led to examine curves on a rational ruled surface. For simplicity, we will restrict our attention further to the surface $S = \mathbb{P}^1 \times \mathbb{P}^1$ (as the reader can readily verify, the calculations analogous to the following may be carried out as well on any rational ruled surface, and will yield exactly the same results). By way of terminology, if a curve $C$ on $S$ is linearly equivalent to $d$ lines of the first ruling plus $e$ lines of the second (that is,

$$\mathcal{O}_S(C) \cong \pi_1^*\mathcal{O}_{\mathbb{P}^1}(d) \otimes \pi_2^*\mathcal{O}_{\mathbb{P}^1}(e))$$

we will say that $C$ has *class* $(d, e)$. For example, since the canonical bundle of $S$ has class $(-2, -2)$, applying the adjunction formula we see that the (arithmetic) genus of a curve of class $(d, e)$ on $S$ is $(d-1)(e-1)$. The preceding discussion also suggests that we look for our curve $C$ among curves whose classes are as far removed as possible from multiples of the canonical class of $S$; and since any non-rational curve on $S$ has class $(d, e)$ with $d, e \geq 2$, we will look first at the linear series $\mathcal{D}$ of curves of class $(2, g+1)$ on $S$. The dimension of the linear series $\mathcal{D}$ is $3(g+2) - 1 = 3g + 5$, as may be seen either from the Riemann-Roch formula or, more directly, from the fact that the vector space of bihomogeneous polynomials $F(X_0, X_1; Y_0, Y_1)$ of bidegree $(d, e)$ in two sets of two variables has dimension $(d+1)(e+1)$. It follows that, for any positive $g$, and any $3g+5$ rational points $p_1, \ldots, p_{3g+5} \in S(\mathbb{Q})$ we can find a curve in this linear system passing through $p_1, \ldots, p_{3g+5}$; and if the points $p_1, \ldots, p_{3g+5}$ are general on $S$ then $C$ will be a smooth curve of genus $g$ defined over $\mathbb{Q}$.

Now, a bonus: as long as the points $p_i$ are chosen generically, for each $i = 1, \ldots, 3g+5$ the curve $C$ will intersect the line of the second ruling through $p_i$ – that is, the line $\pi_2^{-1}(\pi_2(p_i))$ – in two distinct points, $p_i$ and a second point $q_i$ also defined over $\mathbb{Q}$ (alternatively, we may observe that $C$ is a hyperelliptic curve, $q_i$ is simply the image of $p_i$ under the hyperelliptic involution on $C$). Finally, as long as no two of the points $p_i$ have the same image in the second factor, none of the points $q_i$ will coincide with a point $p_j$. We see that the curve $C$ will thus have at least $2(3g+5) = 6g+10$ rational points; that is, we have established the

**Theorem 2.1.** $\mathrm{B}(\mathbb{Q}, g) \geq 6g + 10$.

We can also improve the constant term "10" in this statement. The idea is simple: if the presence of the hyperelliptic involution on the curve $C$ doubled the number of rational points we were able to make $C$ contain, why not look for curves in this linear series that have other automorphisms as well? The immediate answer is that, while every curve with class $(2, n)$ on $S$ is necessarily hyperelliptic, the locus of those with strictly larger automorphism groups is a proper subvariety $\Psi$ of the space $\mathbb{P}^{3g+5}$ parametrizing $\mathcal{D}$. This has two negative effects: first, it reduces our degree of freedom in choosing a curve $C$, that is, the number of points of $S$ we can make $C$ pass through. Secondly, we know nothing about the geometry of the components of $\Psi$. In particular, irreducible components $\Psi_0$ of $\Psi$ may have no rational points on them, meaning there are no curves $C \subset S$ defined over $\mathbb{Q}$ with $[C] \in \Psi_0$.

We may deal with the second objection by focussing our attention on components of $\Psi$ that are linear spaces of $\mathbb{P}^{3g+5}$ (though, since these components tend to be small, the first objection will remain a problem). Specifically, suppose that $G$ is any finite group of automorphisms of $\mathbb{P}^1$, all of which are defined over $\mathbb{Q}$, let

$$V_G \subset H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(g+1))$$

be the space of polynomials of degree $g+1$ invariant under $G$, and assume that the polynomials in $V_G$ have no common zeroes. Let

$$W_G = \pi_1^* H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(2)) \otimes \pi_2^* V_G$$

be the space of bihomogeneous polynomials of bidegree $(2, g+1)$ on $\mathbb{P}^1 \times \mathbb{P}^1$ invariant under the action of $G$ on the second factor. If we denote by $\rho_G(g)$ the dimension of the vector space $V_G$, then the dimension of the linear series of curves associated to $W_G$ will be simply $m = 3\rho_G(g) - 1$, and we can find a curve $C$ in this linear series containing a given collection $p_1, \ldots, p_m$ of that many points. Moreover, if $p_1, \ldots, p_m$ are rational, and general on $S$ (so that in particular their orbits are of maximal size and have disjoint images in the second factor), the curve $C$ will be smooth of genus $g$ and defined over $\mathbb{Q}$, and will contain the orbits under $G$ of the points $p_i$; thus we may conclude that $C$ has at least

$$|C(\mathbb{Q})| \geq 2 \cdot |G| \cdot (3\rho_G(g) - 1)$$

rational points. The question then becomes, which is greater: the loss of degrees of freedom, as measured (roughly) by the ratio of $\rho_G(g)$ to the dimension $g+2$ of the space of all polynomials of degree $g+1$ on $\mathbb{P}^1$, or the gain in automorphism group, as measured simply by the order $|G|$ of $G$? The answer is, they are very nearly equal; and the occasional net profit will produce only a bounded number of additional rational points.

For example, consider the simplest case, $G = \mathbb{Z}/2\mathbb{Z}$ (there is only one possible action up to conjugation). In this case we have

$$\rho_{\mathbb{Z}/2\mathbb{Z}}(g) = \begin{cases} \frac{g+2}{2} & \text{if } g \text{ is even; and} \\ \frac{g+3}{2} & \text{if } g \text{ is odd} \end{cases}$$

so that we have a slight gain in case $g$ is odd: specifically, the curve $C$ through $n = 3(g+3)/2 - 1$ general rational points of $S$ will have at least

$$4n = 6(g+3) - 4 = 6g + 14$$

rational points. Note that we do slightly worse than before if $g$ is even; as we will see, this is typical. Note also that, instead of looking at the space $V_G$ of polynomials invariant under $G$, we could have looked at the complementary space of anti-invariant polynomials and again found curves $C$ with automorphism group containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, but the dimension of this linear series would have been no greater for $g$ even and strictly less for $g$ odd; again, this is typical.

Consider now other possible groups $G$. In fact, there are up to conjugation only five other finite groups of automorphisms of $\mathbb{P}^1$ all of whose elements are defined over $\mathbb{Q}$: the symmetric group $S_3$, acting as the group of automorphisms fixing the subset $\{0, 1, \infty\} \subset \mathbb{P}^1$; the dihedral group $D_4$ of order 8, acting as the group of automorphisms fixing the subset $\{0, 1, -1, \infty\} \subset \mathbb{P}^1$, and the subgroups $\mathbb{Z}/3\mathbb{Z}$ of $S_3$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ of $D_4$. Moreover, these proper subgroups of $S_3$ and $D_4$ do not yield better results than $S_3$ and $D_4$, so we will only consider the two larger groups.

To start with $S_3$, observe that its action on $\mathbb{P}^1$ is simply the action associated to the standard two-dimensional representation of $S_3$; we have to ask simply what are the dimensions of the subspaces of invariant vectors in the symmetric powers of this representation. The calculation is a standard one, and we simply list the result here: the dimensions are

$$\rho_{S_3}(g) = \begin{cases} g/6 & \text{if } g \equiv 0 \bmod 6; \\ (g+5)/6 & \text{if } g \equiv 1 \bmod 6; \\ (g+4)/6 & \text{if } g \equiv 2 \bmod 6; \\ (g+3)/6 & \text{if } g \equiv 3 \bmod 6; \\ (g+2)/6 & \text{if } g \equiv 4 \bmod 6; \text{ and} \\ (g+7)/6 & \text{if } g \equiv 5 \bmod 6. \end{cases}$$

In case $g$ is congruent to 1, 2 or 5 mod 6, this yields an improvement: we can find curves in this linear series with at least $6g+18, 6g+12$ and $6g+30$ rational points, respectively.

The case of the action of the dihedral group $D_4$ is slightly complicated by the fact that the action is not linear, that is, the action of $D_4$ on $\mathbb{P}^1$ cannot be lifted to an action on a two-dimensional vector space. Instead, the inverse image in $SL_2$ of the group $D_4 \subset PGL_2$ described above is a group $H$ of order 16 that does not split. It may seem at first that we are getting a bad deal here: we have to look for invariants under the action of a group of order 16, but the resulting curves only have 8 extra automorphisms. In fact, however, the action of $D_4$ on the even Veronese images of $\mathbb{P}^1$ is linear; that is, the action of $H$ on the even symmetric powers of its two-dimensional representation factors through the surjection $H \to D_4$; and for some of these powers we do realize some advantage. It is straightforward to write out the character table for the group $H$ and calculate the dimensions of the subspaces of invariant vectors; again, we will spare the reader the details and simply write out the results, which are (for $g$ odd)

$$\rho_{D_4}(g) = \begin{cases} (2g+14)/16 & \text{if } g \equiv 1 \bmod 8; \\ (2g+10)/16 & \text{if } g \equiv 3 \bmod 8; \\ (2g+6)/16 & \text{if } g \equiv 5 \bmod 8; \\ (2g+18)/16 & \text{if } g \equiv 7 \bmod 8. \end{cases}$$

This yields, in case $g$ is congruent to 1 or 7 mod 8, curves with $6g+26$ and $6g+38$ rational points, respectively; in the remaining cases we do not do as well as previously. Again, in the case of either $S_3$ or $D_4$ we could also look at the subspaces of polynomials of degree $g+1$ corresponding to other one-dimensional representations than the trivial; but in each case these do not give any further results. Summarizing what we have found, we have:

**Proposition 2.1.**

$$\mathrm{B}(\mathbb{Q}, g) \geq \begin{cases} 6g+38 & \textit{if } g \equiv 7 \textit{ mod } 8; \\ 6g+26 & \textit{if } g \equiv 1 \textit{ mod } 8; \\ 6g+30 & \textit{if } g \equiv 5 \textit{ mod } 6; \\ 6g+18 & \textit{if } g \equiv 1 \textit{ mod } 6; \\ 6g+12 & \textit{if } g \equiv 2 \textit{ mod } 6; \\ 6g+14 & \textit{if } g \textit{ is odd; and} \\ 6g+10 & \textit{in general.} \end{cases}$$

## 3. Lower bounds on N(3)

By our definition of $\mathrm{N}(g)$, in order to establish a lower bound $\mathrm{N}(g) \geq \mathrm{N}_0$ it suffices to exhibit a number field $K$ and an infinite collection of non-isomorphic curves $C_\lambda$ of genus $g$ defined over $K$ such that

$$|C_\lambda(K)| \geq \mathrm{N}_0$$

for all $\lambda$. In this section, we will do so by exhibiting one-parameter families $\{C_\lambda\}$ of curves of genus 3 on a fixed surface $S$, such that various curves on $S$ cut the curves $C_\lambda$ in rational points. We will start with the

**Proposition 3.1.** $\mathrm{N}(3) \geq 72$.

*Proof.* The surface we will use for this case (and the next one as well) is the quartic surface $S \subset \mathbb{P}^3$ defined, in terms of homogeneous coordinates $[X, Y, Z, W]$ on $\mathbb{P}^3$, by the equation

$$X(X^3 - Y^3) = Z(Z^3 - W^3).$$

The key feature of this surface is that it contains a total of 64 lines. To see this, first introduce the two lines $L$ and $M \subset \mathbb{P}^3$ given by

$$Z = W = 0$$

and

$$X = Y = 0$$

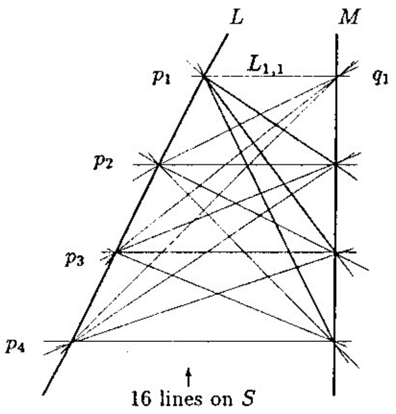
respectively. $L$ meets $S$ in the four points

$$\begin{aligned} p_1 &= [0,1,0,0], \quad p_2 = [1,1,0,0], \\ p_3 &= [1,\omega,0,0] \quad \text{and} \quad p_4 = [1,\omega^2,0,0] \end{aligned}$$

where $\omega$ is a cube root of unity; and similarly $M$ meets $S$ in the four points

$$\begin{aligned} q_1 &= [0,0,0,1], \quad q_2 = [0,0,1,1], \\ q_3 &= [0,0,1,\omega] \quad \text{and} \quad q_4 = [0,0,1,\omega^2]. \end{aligned}$$

The first thing to observe is that $S$ contains the 16 lines $L_{i,j} = \overline{p_i q_j}$ for $1 \leq i,\ j \leq 4$. Here is a picture representing them; for future reference, we will call these the *lines of type A*.



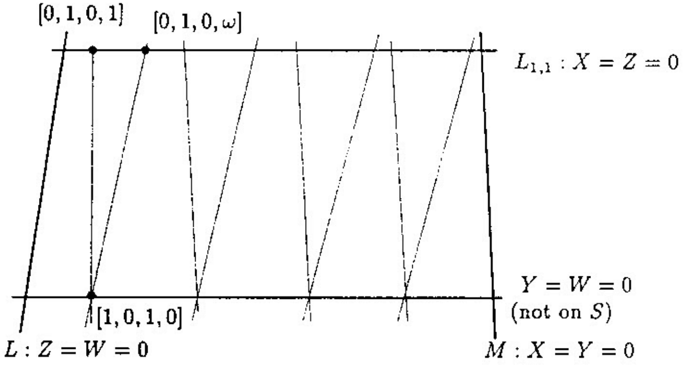
Next, observe that the points $p_i \in L$ form the configuration of 4 points on $\mathbb{P}^1$ with the greatest number of symmetries, and likewise for the points $q_i \in M$; in fact, for any even permutation $\sigma \in A_4$ of the set $\{1,\ldots,4\}$, there is a (unique) isomorphism $\varphi_\sigma : L \to M$ between the two lines carrying the point $p_i$ to the point $q_{\sigma(i)}$ for $i = 1,\ldots,4$. The surface

$$Q_\sigma = \bigcup_{p \in L} \overline{p, \varphi_\sigma(p)}$$

given as the union of the lines in $\mathbb{P}^3$ joining points of $L$ to their images in $M$ under $\varphi_\sigma$ is a smooth quadric surface. Its intersection with $S$ contains the four lines $L_{i,\sigma(i)}$, $i = 1,\ldots,4$, all of which belong to one ruling of $Q_\sigma$; its intersection with $S$ must therefore consist of these four lines and four additional lines of the second ruling of $Q_\sigma$ (that is, the ruling including the lines $L$ and $M$).

These four lines will indeed be distinct, as the two surfaces $Q_\sigma$ and $S$ have different degrees. We will denote them $M_{\sigma,i}$, $i = 1,\ldots,4$ (the order is not significant), and call them *lines of type B*. Note that these four lines are distinct from the 16 lines $L_{i,j}$ (they are skew to $L$ and $M$, which the $L_{i,j}$ are not), and that none of the four can lie on a second quadric $Q_{\sigma'}$ (the intersection of any two quadrics $Q_\sigma$ and $Q_{\sigma'}$ will consist of the two lines $L$ and $M$ and two lines of the first ruling). Since there are 12 permutations $\varphi$, we arrive in this way at 48 lines $\{M_{\sigma,i}\}$ distinct from each other and from the lines $L_{i,j}$; thus $S$ contains a total of 64 lines. (In fact, these are all the lines on $S$; for a proof of this fact, and the fact that no smooth quartic surface in $\mathbb{P}^3$ contains more than 64 lines, see [S].)

Here, for example, is a picture showing the four lines of intersection of the quadrics $Q_{Id}$ and $Q_\sigma$, where $Id$ is the identity and $\sigma = (2,3,4)$, and the eight lines $\{M_{Id,i}, M_{\sigma,i}\}$.



Note that of the four lines $L_{i,i}$ contained in $Q_{Id}$ the only one contained in $Q_\sigma$ is $L_{1,1}$, corresponding to the fixed point 1 of the permutation $\sigma$; the intersection $Q_{Id} \cap Q_\sigma$ consists thus of $L, M, L_{1,1}$ and a fourth line not contained in $S$. We see moreover that the lines of type B contained in both $Q_{Id}$ and $Q_\sigma$ must meet this fourth line in its four points of intersection with $S$, and so meet each other there; but they meet $L_{1,1}$ at different points.

Now let $\{H_\lambda\}_{\lambda \in \mathbb{P}^1}$ be a general pencil of hyperplanes in $\mathbb{P}^3$ defined over $\mathbb{Q}$, and let $C_\lambda = H_\lambda \cap S$ be the corresponding hyperplane sections. Note that, since the pencil $\{C_\lambda\}$ consists of stable curves (every $C_\lambda$ is either a smooth curve or an irreducible curve with a single node), we get a map $\mathbb{P}^1 \to \overline{M}_3$ sending $\lambda$ to the isomorphism class of $C_\lambda$; since both smooth and irreducible nodal curves appear in the pencil, the map will be nonconstant, hence finite.

The base locus $N = \cap H_\lambda$ of the pencil is a line meeting $S$ in four points $r_1,\ldots,r_4$, none of which will lie on a line of $S$. Let $K$ be any number field such that the 64 lines of $S$ and the four points $r_i$ are defined over $K$. For finitely many values of $\lambda \in K$, $C_\lambda$ will either be singular or will contain one of the points of pairwise intersection of the lines of $S$. For the remaining (infinitely many) values of $\lambda$, the curve $C_\lambda$ will be smooth, and the points of intersection of $C_\lambda$ with the lines of $S$, together with the four points $r_i \in C_\lambda$, will all be distinct. We thus have

$$|C_\lambda(K)| \geq 68$$

and since only finitely many curves $C_{\lambda'}$ can be isomorphic over $K$ to a given $C_\lambda$, we conclude that $\mathrm{N}(3) \geq 68$.

We can do slightly better by using the fact that, in addition to its lines, the surface $S$ also contains lots of plane conic curves. To exhibit such conics, take a pair of incident lines of the form $M_{Id,i}$ and $M_{\tau,j}$, where $\tau = (12)(34)$. Recall that the intersection $Q_{Id}$ and $Q_\tau$ will consist of $L, M$ and two further lines not contained in $S$. These lines will each meet $S$ in four points, through which the lines $M_{Id,i}$ and $M_{\tau,j}$ must pass; so we can certainly choose $i$ and $j$ so that $M_{Id,i}$ and $M_{\tau,j}$ meet. For example, we could take $M_{Id,i}$ and $M_{\tau,j}$ the lines passing through the point $[1, \alpha, 1, \alpha]$, where $\alpha = 1 + \sqrt{3}$, that is,

$$M_{Id,i} = \mathrm{V}(X - Z, W - Y)$$

and

$$M_{\tau,j} = \mathrm{V}(Y + 2X - \sqrt{3}W, Y - X - \sqrt{3}Z).$$

The plane they span has equation

$$\Gamma = (W - Y - (\sqrt{3} - 1)(X - Z))$$

and intersects $S$ in the union of these two lines and the irreducible conic given in $\Gamma$ by the equation

$$X^2 + XY + Y^2 + (5\sqrt{3} - 9)XZ + (3 - 2\sqrt{3})YZ + (6 - 3\sqrt{3})Z^2 = 0.$$

Other conics can be found by applying automorphisms of $S$ to this one.

Now, if $C \subset S$ is a conic, then over some number field $L$ it will have infinitely many rational points $s_\alpha$. Moreover, each such point will lie on a (unique) hyperplane $H_\lambda$ of the pencil discussed above; and that hyperplane will intersect $C$ in $s_\alpha$ and one other point $t_\alpha$, also defined over $L$ and distinct from $s_\alpha$ except for the (at most) two values of $\lambda$ for which $H_\lambda$ is tangent to $C$. Since only finitely many planes $H_\lambda$ of our pencil contain points of intersection of $C$ with lines of $S$, we thus have infinitely many values of $\lambda$ for which $C_\lambda$ contains two additional points rational over $L$, and we conclude that $\mathrm{N}(3) \geq 70$.

Finally, we can play the same game with two conics simultaneously: we have the

**Lemma 3.1.** *Let $C$ and $D \subset \mathbb{P}^3$ be two plane conics, $\{H_\lambda\}$ a pencil of planes in $\mathbb{P}^3$, none of which contains $C$ or $D$. Suppose that $\{H_\lambda\}$ is defined over a number field $K$. There exists an extension $L$ of $K$ and infinitely many values $\lambda \in L$ for which the four points of intersection of $H_\lambda$ with $C \cup D$ are defined over $L$.*

*Proof.* We simply observe here that the pencil $\{H_\lambda\}$ defines a correspondence of bidegree (2,2) on the product $C \times D$: that is, the incidence correspondence

$$E = \{(p, q) : p, q \in H_\lambda \quad \text{for some } \lambda\} \subset C \times D$$

is a curve of bidegree (2,2) in $C \times D \cong \mathbb{P}^1 \times \mathbb{P}^1$. If $E$ is smooth and irreducible, it is a curve of genus 1; otherwise all components of $E$ are rational curves. Either way, for some extension $L$ of $K$, $E$ has infinitely many $L$-rational points $\{(p_\alpha, q_\alpha)\}$ with distinct images in $C$ and $D$. Throwing away those pairs $(p_\alpha, q_\alpha)$ with either $p_\alpha$ or $q_\alpha$ contained in the base locus of the pencil, each pair $p_\alpha$ and $q_\alpha$ lies on a unique hyperplane $H_{\lambda(\alpha)}$ of the pencil; and since by hypothesis each plane $H_\lambda$ contains at most finitely many pairs $p_\alpha$ and $q_\alpha$ we arrive at infinitely many $\lambda \in L$ satisfying the statement of the Lemma. □

Inasmuch as $S$ does contain more than one conic, we have completed the proof of Proposition 3.1. □

## 4. A LOWER BOUND ON N(2)

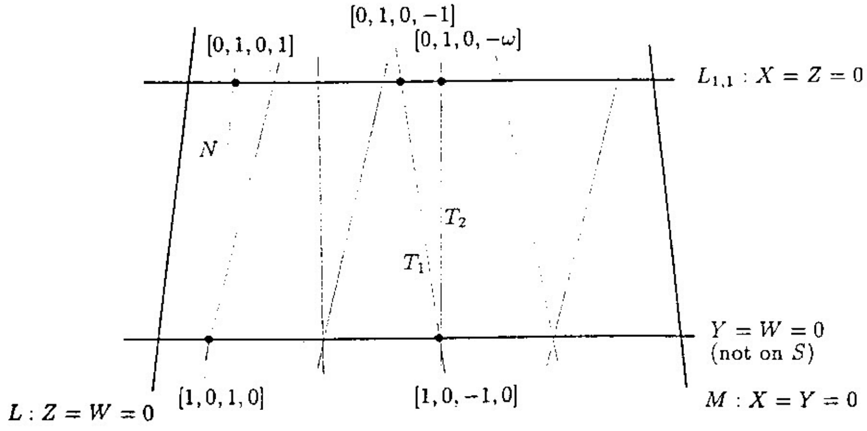
We can play a similar game for curves of genus two, again using the quartic surface $S$ above but now looking at the normalizations $C$ of the intersections $C_0$ of $S$ with tangent planes $H$. We will get in this way curves of genus 2, with 64 rational points coming from the lines of $S$; in addition, we will have the points conjugate to these 64 points under the hyperelliptic involution on the curves $C$. We will thus prove the

**Proposition 4.1.** $\mathrm{N}(2) \geq 128$.

*Proof.* To carry out the program outlined above, we have three things to check: that there are enough tangent planes to $S$ defined over a fixed number field $K$, that the 128 points described above are indeed all distinct on a general curve $C$ constructed in this way, and that the curves $C$ obtained do indeed vary in moduli. We will give a lemma for each of these points, starting with the straightforward

**Lemma 4.1.** *The surface $S$ contains an infinite (and hence Zariski dense) collection of rational curves defined over $\overline{\mathbb{Q}}$.*

*Proof.* Start with three lines $N, T_1, T_2$ on $S$, with $T_1$ and $T_2$ meeting at a point $p$ and $N$ disjoint from both.



For example, we could take

$$\begin{aligned} N &= M_{Id,1} = \mathrm{V}(X - Z, Y - W) \\ T_1 &= \mathrm{V}(X + Z, Y + W) \\ T_2 &= \mathrm{V}(X + Z, \omega Y + W) \end{aligned}$$

with $p = [1, 0, -1, 0]$.

Now consider the pencil $\{H_\lambda\}$ of planes containing $N$. The general plane $H_\lambda$ meets $S$ in the union of $N$ and a smooth plane cubic $C_\lambda$, so that projection from $N$ expresses $S$ as an elliptic surface over $\mathbb{P}^1$, with two sections

$$\begin{aligned} p(\lambda) &= T_1 \cap C_\lambda \\ q(\lambda) &= T_2 \cap C_\lambda \end{aligned}$$

given by $T_1$ and $T_2$. We can thus form a sequence of sections $p_n(\lambda)$ by adding multiples of $(p(\lambda) - q(\lambda))$ to $q(\lambda)$, that is, we can specify, for general $\lambda$,

$$p_n(\lambda) \sim n \cdot p(\lambda) - (n-1) \cdot q(\lambda)$$

on $C_\lambda$.

We claim next that the difference $p(\lambda) - q(\lambda)$ is not torsion in the Picard group of $C_\lambda$ for general $\lambda$. To see this, observe that the plane $H_{\lambda_0} = \mathrm{V}(Y - W)$ spanned by $N$ and $p$ intersects $S$ in the union of the line $N$ and the smooth cubic

$$C_{\lambda_0} = \mathrm{V}(X^3 + X^2Z + XZ^2 + Z^3 + W^3).$$

The two sections $p(\lambda)$ and $q(\lambda)$ thus agree in the smooth fiber $C_{\lambda_0}$ and not in general; we conclude that the difference cannot be torsion for all $\lambda$.

The sections $p_n$ thus give an infinite sequence of distinct rational curves $\Sigma_n$ on $S$, all defined over $K$; this completes the proof of Lemma 4.1.

Remark. In fact, the argument above allows us to identify number fields $K$ (for example, $K = \mathbb{Q}(\omega)$, where $\omega^3 = 1$) such that the surface $S$ contains infinitely many rational curves defined over $K$; but we don't need this for what follows. The point is that we do not need the fact that there exists a number field $K$ such that $S(K)$ is Zariski dense, but only the weaker statement that for any proper closed subvariety $T \subset S$ there is a number field $K$ such that $S(K)$ contains infinitely many points not in $T$. Thus the fact that all the $\Sigma_n$ may be defined over the same field $K$ is not logically relevant.

As we suggested above, our infinite family of curves of genus 2 with 128 rational points will consist of the normalizations $C$ of the intersections $C_0$ of $S$ with tangent planes $H = \mathbb{T}_pS$ to $S$ at the points $p \in \Sigma_n$ for $n$ sufficiently large, which are in effect general points. The 128 points will be the points $r_i$ of intersection of the curves $C_0$ with the 64 lines of $S$, together with their conjugates under the hyperelliptic involution, which are simply the remaining points $s_i$ of intersection of $C_0$ with the lines spanned by the points $r_i$ and the point $p$ of tangency. The next part of the argument, then, is to see that these points are indeed distinct. This is the content of the following Lemma.

**Lemma 4.2.** *Let $p \in S$ be a general point, and let $H = \mathbb{T}_pS \subset \mathbb{P}^3$ be the projective tangent plane to $S$ at $p$. The following are true:*

*a). $H$ intersects the 64 lines of $S$ at distinct points $r_1, \dots, r_{64}$.*

*b). No two of the points $r_i$ are collinear with $p$.*

*c). The line joining $p$ to $r_i$ is not tangent to $S$ at $r_i$.*

*d). The tangent lines to the branches of $H \cap S$ at $p$ do not meet any line of $S$ (i.e., the line joining $p$ to $r_i$ is not tangent to either of the branches of $H \cap S$ at $p$).*

*In sum: by c), the line $\overline{pr}_i$ meets $S$ with multiplicity one at $r_i$; by d) it meets $S$ with multiplicity 2 at $p$, and hence it meets $S$ exactly once more at a point $s_i \neq p, r_i$; and by b) the points $s_i$ are all distinct from each other and from the $r_i$.*

*Proof.* Part a) simply says that for general $p \in S$, the tangent plane $\mathbb{T}_pS$ does not contain any of the points of pairwise intersection of the 64 lines of $S$, which follows from the fact that the dual surface is nondegenerate.

As for part b), we need only check two of these lines $L, M \subset S$ at a time. If $L$ and $M$ meet, it is immediate, since $p$ will not lie in the plane they span. If they are skew, we have to check that the locus of triples

$$\{(p,q,r) : q \in L; r \in M;\ r, q \in \mathbb{T}_pS \quad \text{and} \quad p, q, r \text{ are collinear}\}$$

has dimension strictly less than 2, which amounts to saying that not every line joining $L$ and $M$ is tangent to $S$. But this is an immediate consequence of Bertini's theorem, which says that only finitely many planes containing $L$ are tangent to $S$ at a point outside $L$. Similarly, for part c) we have to check that not every line tangent to $S$ at a point of $L$ is tangent somewhere else, which also follows from Bertini's theorem.

Lastly, for part d) we note that by the irreducibility of $S$ there can be at most four lines on $S$ with the property that the tangent lines to the branches of $H \cap S$ at a general point $p$ meet $L$; but since the automorphism group of $S$ acts transitively on lines of type A and lines of type B, if there were any there would have to be at least 16. □

Finally, to complete our argument we have to check that, for $n \gg 0$, the family of curves obtained as normalizations of intersections of $S$ with planes tangent at points of the curve $\Sigma_n \subset S$ do in fact vary in moduli. We do this by a variant of the argument used before. We consider the map

$$\phi : S \dashrightarrow \overline{M}_2$$

sending a general point $p \in S$ to the normalization $C$ of the intersection $C_0$ of the tangent plane $\mathbb{T}_pS$ with $S$.

For general $p \in S$, $C$ is a smooth curve of genus 2, so the image of $\phi$ is not contained in the boundary of $\overline{M}_2$. On the other hand, it does hit the boundary: for example, if $p$ is a general point on a line $M_{\sigma,i} \subset S$, $C_0$ will consist of the union of $M_{\sigma,i}$ and a smooth cubic curve $E$ meeting it transversely, so that $C$ is the union of $E$ with a rational curve meeting it at two points, $q, r \in E$. Since $C$ is nodal, the map $\phi$ is regular, in a neighborhood of $p$, and sends $p$ to the point $[\overline{C}] \in \overline{M}_2$, where $\overline{C}$ is the curve obtained by identifying the points $q$ and $r$ on $E$. Finally, we note that as $p$ varies on $M_{\sigma,i}$ the $j$-invariant of $E$ varies (for special values of $p$, $E$ degenerates to a triangle, which corresponds to a pole of $j$). The image of $\phi$ thus meets the boundary of $\overline{M}_2$ in a curve, and we conclude that the image of $\phi$ must be two-dimensional; in particular, the positive-dimensional fibers of $\phi$ cannot be Zariski dense in $S$.

(Recalling the remark following the proof of Lemma (4.1), we should note that we don't really need to work quite this hard: if we use the fact that $S$ does indeed contain a Zariski dense collection of $K$-rational points for some number field $K$, we need only show that the image of $\phi$ is at least one-dimensional.)

In sum, then: for sufficiently large $n$, the curves of genus 2 obtained as the normalizations of the intersections of $S$ with tangent planes $\mathbb{T}_pS$ as $p$ varies along the curve $\Sigma_n \subset S$ do vary in moduli, and an infinite number have 128 or more $K$-rational points. Thus we have completed the proof of Proposition 4.1. □

## 5. Estimates on N($g$) for large $g$

In this section, we will derive lower bounds on N($g$) for general $g$, with a view toward estimating the limit

$$\overline{\mathrm{N}} = \limsup_{g\to\infty} \frac{\mathrm{N}(g)}{g}$$

discussed in the introduction.

We describe three approaches to this. The latter two yield in general a stronger result, but we mention all three methods in the hope that the reader may see a way of improving one.

**5.1. Plane sections of surfaces with lines.** Our first approach is a natural generalization of the way we derived a lower bound for N(3) in section 3 above. Specifically, if we have a surface $S \subset \mathbb{P}^3$ defined over $\overline{\mathbb{Q}}$ and containing a finite number $\ell$ of lines, then we can, by taking plane sections of $S$, find an infinite collection of curves defined over some number field $K$ (the common field of definition of $S$ and the lines on $S$) with $\ell$ or more $K$-rational points. This raises the question: what is the greatest number of lines a (non-ruled) surface of degree $d$ in $\mathbb{P}^3$ can have? Denoting this number by $\ell(d)$, we have the

**Lemma 5.1.** *$\ell(d) \geq 3d^2$ for all $d \geq 3$; and beyond that,*

$$\begin{aligned} \ell(4) &\geq 64 \\ \ell(6) &\geq 180 \\ \ell(8) &\geq 256 \\ \ell(12) &\geq 864 \\ \ell(20) &\geq 1600 \end{aligned}$$

*Proof.* All these assertions can be verified by exhibiting surfaces of the appropriate degree possessing the indicated number of lines; and all of these surfaces can be described in the same way. (This is in fact how the quartic surface of Sections 3 and 4 was obtained.) Specifically, let $F(X,Y)$ be any homogeneous polynomial of degree $d$, and denote its zero locus in $\mathbb{P}^1$ by $\Gamma$; let $\alpha$ be the order of the group $G$ of automorphisms of $\mathbb{P}^1$ carrying $\Gamma$ into itself. Consider the surface $S \subset \mathbb{P}^3$ defined by the equation

$$F(X,Y) - F(Z,W) = 0.$$

Let $\Gamma_1$ be the set of points $F(X,Y) = Z = W = 0$ on the line $L_1$ given by $Z = W = 0$, and similarly let $\Gamma_2$ be the locus $F(Z,W) = X = Y = 0$ on the line $L_2$ given by $X = Y = 0$. To begin with, we see that $S$ contains the $d^2$ lines joining $\Gamma_1$ to $\Gamma_2$. Moreover, if $\varphi : L_1 \to L_2$ is any isomorphism carrying $\Gamma_1$ to $\Gamma_2$, we consider the quadric

$$Q_\varphi = \bigcup_{p \in L_1} \overline{p, \varphi(p)}$$

given as the union of the lines in $\mathbb{P}^3$ joining points of $L_1$ to their images in $L_2$ under $\varphi$. Its intersection with $S$ contains the $d$ lines $\{\overline{p, \varphi(p)} : p \in \Gamma_1\}$, all of which belong to one ruling of $Q_\varphi$; its intersection with $S$ must therefore consist of these $d$ lines and $d$ additional lines of the second ruling of $Q_\varphi$ (that is, the ruling including the lines $L_1$ and $L_2$). Note that these $d$ lines, being skew to $L$ and $M$, are distinct from the $d^2$ lines joining $\Gamma_1$ to $\Gamma_2$, and that none of them can lie on a second quadric of the form $Q_{\varphi'}$ (the intersection of any two quadrics $Q_\varphi$ and $Q_{\varphi'}$ will consist of the two lines $L_1$ and $L_2$ and two lines of the first ruling). We thus have $d$ additional lines for every isomorphism $\varphi$, for a total of (at least) $d^2 + \alpha d$ lines.

Now, for any $d$ we can take $\Gamma$ the $d$-th roots of unity. In this case the dihedral group of order $\alpha = 2d$ acts and we get a total of $3d^2$ lines; in fact, this is just the Fermat surface. For general $d$, this is the best we can do by this method, but there are exceptions. For $d = 4$, we can take $\Gamma$ the vertices of a tetrahedron, on which the group $A_4$ acts, giving us $d^2 + 12d = 64$ lines; this is the quartic surface described in §3. For $d = 6$ and 8 we can take the faces and the vertices of a cube, respectively; the symmetric group $S_4$ then acts, giving us $d^2 + 24d = 180$ and 256 lines respectively. Finally, for $d = 12$ and 20 we can take the faces and vertices of a dodecahedron, on which $A_5$ acts; we obtain surfaces with $d^2 + 60d = 864$ and 1600 lines respectively. □

As we pointed out, whenever $g = (d-1)(d-2)/2$ we have $\mathrm{N}(g) \geq \ell(d)$, and we can therefore deduce from Lemma 5.1 that for such values of $g$ we have $\mathrm{N}(g) \geq 3d^2 = 6g + o(g)$. In other words, we may conclude that

$$\overline{\mathrm{N}} \geq 6.$$

This is not particularly striking; with only minimal efforts, for example, the method of Section 2 would yield this result; and indeed this method will give a stronger result below. Again, we mention this in the hope that the reader may see a way to improve the result. We should remark in particular that the only degrees for which the bound of Lemma 5.1 is known to be sharp are $d = 3$ and 4 (for a proof in case $d = 4$ see [S]).

The best upper bound on $\ell(d)$ in general known to us is

$$\ell(d) \leq 11d^2 - 24d,$$

(cf. [S]) which is sharp for $d = 3$ but not in general. In particular, this says that the limit

$$\bar{\ell} = \limsup_{d\to\infty} \frac{\ell(d)}{d^2} \leq 11$$

so the state of our knowledge is that $3 \leq \bar{\ell} \leq 11$. What we can say, of course, is that $\overline{\mathrm{N}} \geq 2\bar{\ell}$, so this approach has the potential to prove that $\overline{\mathrm{N}} \geq 22$, but not more (and even this seems unlikely).

A further remark is that, while this method does not yield the best asymptotic results, for some specific $g$ it does give lower bounds for $\mathrm{N}(g)$ that do exceed what we can show by other means. Specifically, for $d = 6, 8, 10, 12$ and 20 we can take general hyperplane sections of the surfaces $S$ of degree $d$ described in Lemma 5.1 to exhibit families of curves of genus $g = (d-1)(d-2)/2$. We can also, in each of these cases, take the pencil of plane curves of degree $d - 1$ and genus $g = (d-2)(d-3)/2$ cut out on $S$ by the planes containing a line $L \subset S$; each line on $S$ not meeting $L$ then provides a rational point on a general member of this pencil. (As the reader may verify, exactly $2d - 2 + \alpha$ lines of $S$ other than $L$ meet $L$.) Omitting the verification that the moduli of the curves in such a pencil do in fact vary, we tabulate the results in the

**Corollary 5.1.** *We have the following lower bounds on* $\mathrm{N}(g)$*:*

| $g$ | 6 | 10 | 15 | 21 | 28 | 36 | 45 | 55 | 153 | 171 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{N}(g) \geq$ | 145 | 180 | 217 | 256 | 261 | 320 | 781 | 864 | 1501 | 1600 |

Of course, there is no reason to restrict our attention to $\mathbb{P}^3$, except for sheer ignorance: we could ask in general for the maximal number of lines on nondegenerate surfaces in $\mathbb{P}^n$ with given degree and/or genus of hyperplane section. The problem is simply that we have no knowledge of the situation in general. For example, we could ask what is the maximum number of lines a smooth $K3$ surface of degree $2n + 2$ in $\mathbb{P}^n$ can have; but the answer to this – or even to the qualitative question of whether this number grows linearly with $n$ – is unclear.

**5.2. Base loci of pencils.** As we indicated, our second approach yields a stronger result in general; in particular, it improves our existing lower bound on $\overline{\mathrm{N}}$ to $\overline{\mathrm{N}} \geq 8$.

**Proposition 5.1.** *For all* $g$, $\mathrm{N}(g) \geq 8g + 14$. *In particular,* $\overline{\mathrm{N}} \geq 8$.

*Proof.* We will give first a simpler proof of the weaker statement that $\mathrm{N}(g) \geq 8g + 8$, and then indicate how this construction may be modified to yield the extra 6 points.

As in Section 2, we will work with the linear system $\mathcal{D}$ of curves of bidegree $(2, g+1)$ on $\mathbb{P}^1 \times \mathbb{P}^1$ – that is, zero loci of bihomogeneous polynomials of bidegree $(2, g + 1)$. Let $\mathcal{L} = \{C_\lambda\}_{\lambda\in\mathbb{P}^1}$ be a general pencil of curves in this linear series. Note that since $\mathcal{D}$ is a linear series of self-intersection $4g + 4$ without base points, $\mathcal{L}$ will have $4g + 4$ distinct base points $p_1, \ldots, p_{4g+4}$.

It is not hard to see by a dimension count that no member of the pencil will contain a fiber of $\mathbb{P}^1 \times \mathbb{P}^1$ over the second factor: inside the $(3g + 5)$-dimensional linear series $\mathcal{D}$ the locus of products of polynomials of bidegree $(2, g)$ with those of bidegree (0,1) is $(3g + 2) + 1 = 3g + 3$, so that a general line $\mathcal{L}$ in $\mathcal{D} \cong \mathbb{P}^{3g+5}$ will miss it. It follows in turn that no two base points of the pencil will lie in the same fiber of $\mathbb{P}^1 \times \mathbb{P}^1$ over the second factor. (We could also embed $\mathbb{P}^1 \times \mathbb{P}^1$ in $\mathbb{P}^{3g+5}$ by the linear series $\mathcal{D}$, realize the base points as the points of intersection of the image with a general codimension 2 subspace $\mathbb{P}^{3g+3} \subset \mathcal{D}$, and deduce this from the observation that the points are therefore in uniform position, that is, as $\mathcal{L} \subset \mathcal{D}$ varies, the monodromy action on the points $p_1, \ldots, p_{4g+4}$ is the full symmetric group.)

Now let $K$ be the number field generated over $\mathbb{Q}$ by the coordinates of the points $p_1, \ldots, p_{4g+4}$. We have immediately that $C_\lambda(K) \supset \{p_1, \ldots, p_{4g+4}\}$. Moreover, all the curves are hyperelliptic, and the images $q_i$ of the points $p_i$ under the hyperelliptic involution (that is, the points of $C_\lambda$ lying in the same fiber of $\mathbb{P}^1 \times \mathbb{P}^1$ over the second factor as the points $p_i$) are also defined over $K$. By what we said above, each $q_i$ is distinct from all the points $p_j$ for $j \neq i$. Hence except for the finitely many values of $\lambda$ for which $C_\lambda$ is tangent to the fiber of $\mathbb{P}^1 \times \mathbb{P}^1$ over the second factor at one of the points $p_i$, the set $\{q_i\}$ is disjoint from $\{p_i\}$. All but finitely many of the curves $C_\lambda$ thus contain at least $8g + 8$ $K$-rational points. Finally, as in Section 3, the curves $C_\lambda$ are all stable, with some singular, and so they do vary in moduli; we conclude that $\mathrm{N}(g) \geq 8g + 8$.

We can do slightly better by a variant of this technique: we can, by choosing the pencil well, ensure that $g$ of the base points lie on a fiber of $\mathbb{P}^1 \times \mathbb{P}^1$ over the first factor. Each $C_\lambda$ will then meet this fiber in those $g$ points, plus one more point that must likewise be defined over $K$; with this extra point and its hyperelliptic conjugate we get up to 8g+10. In fact, we can do this three times: choose $\{p_1, \ldots, p_g\}$, $\{p_{g+1}, \ldots, p_{2g}\}$ and $\{p_{2g+1}, \ldots, p_{3g}\}$ to be general $g$-tuples of points defined over $K$, each lying on a fiber of $\mathbb{P}^1 \times \mathbb{P}^1$ over the first factor. Let $\mathcal{D}_0$ be the linear series of curves of bidegree $(2, g+1)$ on $\mathbb{P}^1 \times \mathbb{P}^1$ passing through the points $\{p_1, \ldots, p_{3g}\}$, and let $\mathcal{L}$ be a general pencil in $\mathcal{D}_0$. It is not hard to see that $\mathcal{D}_0$ embeds the blow-up of $\mathbb{P}^1 \times \mathbb{P}^1$ at these points in $\mathbb{P}^5$, from which all the statements above about the base points of $\mathcal{L}$ follow.

Now let $K$ be the number field generated over $\mathbb{Q}$ by the coordinates of the base points of the pencil $\mathcal{L}$. As before, each member $C_\lambda$ of the pencil contains these points, plus their hyperelliptic conjugates. In addition, for $\alpha = 1, 2, 3$ the intersection of $C_\lambda$ with the fiber of $\mathbb{P}^1 \times \mathbb{P}^1$ over the first factor containing $\{p_{(\alpha-1)g+1}, \ldots, p_{\alpha g}\}$ will consist of $\{p_{(\alpha-1)g+1}, \ldots, p_{\alpha g}\}$ plus a $(g + 1)^{st}$ point $q_\alpha$, also defined over $K$. Moreover, by the same monodromy arguments on a general $C_\lambda$ the points $q_\alpha$, together with their hyperelliptic conjugates, will be distinct from each other and from the $8g+8$ points already found, bringing the total up to $8g+14$. □

A final remark: it seems a shame that we can't use the degree of freedom we have in choosing the pencil to improve the result of Proposition 5.1. After all, the Grassmannian of pencils in the linear series $\mathcal{D}$ has dimension $6g+8$, which should give us a fair amount of play. In the above construction, these degrees of freedom yield only 6 additional points, and in particular we get no better estimate on $\overline{\mathrm{N}}$.

**5.3. Mestre's method.** We will describe here the work of Jean-François Mestre. This technique gives us a way of writing down, for any number field $K$, a set of curves defined over $K$, dense in the hyperelliptic locus in moduli, that possess at least $8g+12$ $K$-rational points. This will of course give us a second demonstration of the fact that $\overline{\mathrm{N}} \geq 8$; and – inasmuch as the method works as well with $K = \mathbb{Q}$ – it will improve our estimate on $\mathrm{B}(\mathbb{Q}, g)$ for all but finitely many values of $g$.

The method is completely elementary. We start by fixing the number field $K$, and choosing $a_1, ...., a_{4g+6}$ any $4g+6$ distinct elements of $K$. Let $P = P_a$ then denote the polynomial

$$P(x) = \prod_{i=1}^{4g+6} (x - a_i) = x^{4g+6} + c_{4g+5}x^{4g+5} + .... + c_1x + c_0$$

Suppose we start naively trying to take a square root of $P$, that is, to find a polynomial

$$Q(x) = x^{2g+3} + b_{2g+2}x^{2g+2} + .... + b_1x + b_0$$

of degree $2g+3$ over the field $K$ whose square is $P$. We have no trouble starting out: we take $b_{2g+2} = c_{4g+5}/2$, so that the coefficients of $x^{4g+5}$ in $Q^2$ and $P$ will agree; and similarly we choose

$$b_{2g+1} = \frac{c_{4g+4} - b_{2g+2}^2}{2}$$

and so on. Problems arise only when we run out of coefficients of $Q$: we can continue in this way until we have chosen $b_0$ so as to make the coefficients of $x^{2g+3}$ in $Q^2$ and $P$ agree, but after that we have no further degrees of freedom.

What we have succeeded in doing in this way is writing our polynomial $P$ as the difference of a square and a polynomial of lower degree: we have

$$P = Q^2 - R$$

where $R = R_a$ is a polynomial of degree $2g+2$ or less over $K$. Now, let $X = X_a$ be the hyperelliptic curve defined by the equation

$$y^2 = R(x)$$

As will follow from the argument below, for a general choice of $a_1, \ldots, a_{4g+6} \in K$, the polynomial $R$ will be of degree exactly $2g+2$, and will have distinct roots, so that $X$ will be a smooth curve of genus $g$. What is more, we can exhibit explicitly $8g+12$ $K$-rational points on $X$: these are simply the points $\{(a_i, \pm Q(a_i)) : i = 1, \ldots, 4g+6\}$.

It remains to be seen that we do indeed get infinitely many isomorphism classes of curves $X_a$ in this way. In fact, we can see more than that: we claim that as $a_1, \ldots, a_{4g+6}$ vary in $K$, the polynomials $R_a$ sweep out a Zariski-dense subset of polynomials of degree $2g+2$. This will also establish the statement made above that for general choice of $a_i$ the polynomial $R$ is of degree $2g+2$ and has nonzero discriminant.

But this is clear: certainly as $a_1, \ldots, a_{4g+6}$ vary the polynomials $P_a$ sweep out a dense subset of the $4g+6$-dimensional space $U$ of monic polynomials of degree $4g+6$. On the other hand, if either $Q_a$ or $R_a$ were constrained to a proper subvariety of the spaces $V$ of monic polynomials of degree $2g+3$ and $W$ of polynomials of degree $2g+2$ respectively, the image of the map $V \times W \to U$ given by sending $(Q, R)$ to $Q^2 - R$ would have dimension strictly less than $\dim(V) + \dim(W) = 4g+6$.

We have thus established the

**Theorem 5.1.** *For any genus $g$ and number field $K$, $\mathrm{B}(K, g) \geq 8g+12$; and for any genus $g$, $\mathrm{N}(g) \geq 8g+12$. In particular, $\overline{\mathrm{N}} \geq 8$.*

## References

[ACGH] E.Arbarello, M.Cornalba, P.Griffiths, J.Harris. *Geometry of Algebraic Curves, Volume I.* Springer-Verlag, NY.

[C] L.Caporaso. *Distribution of rational points and Kodaira dimension of fiber products.* This volume, 1–12.

[CHM] L.Caporaso, J.Harris, B.Mazur. *Uniformity of rational points.* To appear in JAMS.

[L] S.Lang. *Hyperbolic and diophantine analysis.* Bull. Amer. Math. Soc. 14 , No. 2 (1986), 159–205.

[S] B.Segre. *The maximum number of lines lying on a quartic surface.* Quart. J. Math. (1943), 86–96.

Mathematics department, Harvard University, 1 Oxford st., Cambridge MA 02138, USA
*E-mail address:* caporaso@zariski.harvard.edu

Mathematics department, Harvard University, 1 Oxford st., Cambridge MA 02138, USA
*E-mail address:* harris@zariski.harvard.edu

Mathematics department, Harvard University, 1 Oxford st., Cambridge MA 02138, USA
*E-mail address:* mazur@zariski.harvard.edu