

*Pacific
Journal of
Mathematics*

**ALGEBRAIC FAMILIES OF HYPERELLIPTIC CURVES
VIOLATING THE HASSE PRINCIPLE**

NGUYEN NGOC DONG QUAN

Volume 274 No. 1

March 2015

ALGEBRAIC FAMILIES OF HYPERELLIPTIC CURVES VIOLATING THE HASSE PRINCIPLE

NGUYEN NGOC DONG QUAN

In 2000, Colliot-Thélène and Poonen showed how to construct algebraic families of genus-one curves violating the Hasse principle. Poonen explicitly constructed such a family of cubic curves using the general method developed by Colliot-Thélène and himself. The main result in this paper generalizes the result of Colliot-Thélène and Poonen to arbitrarily high genus hyperelliptic curves. More precisely, for $n > 5$ and $n \not\equiv 0 \pmod{4}$, we show that there is an explicit algebraic family of hyperelliptic curves of genus n that are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction.

1. Introduction	141
2. The Hasse principle for certain threefolds in $\mathbb{P}_{\mathbb{Q}}^5$	144
3. Infinitude of triples (p, b, d) .	152
4. Hyperelliptic curves violating the Hasse principle	153
5. Infinitude of sextuples $(p, b, d, \alpha, \beta, \gamma)$	161
6. Algebraic families of hyperelliptic curves violating the Hasse principle	166
Acknowledgements	181
References	181

1. Introduction

The aim of this article is to prove the following result.

Theorem 1.1 (see Theorem 6.8). *Let $n > 5$ be an integer such that $n \not\equiv 0 \pmod{4}$. Then there is an algebraic family C_t of hyperelliptic curves of genus n such that C_t is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction for all $t \in \mathbb{Q}$. Furthermore, C_t contains no zero-cycles of odd degree over \mathbb{Q} for all $t \in \mathbb{Q}$.*

MSC2010: 14G05, 11G35, 11G30.

Keywords: Azumaya algebras, Brauer groups, Brauer–Manin obstruction, Hasse principle, hyperelliptic curves.

We will shortly relate this theorem to existing results in literature, and sketch the ideas of the proof of Theorem 1.1. Let us begin by briefly recalling some terminology which appears in many places in this paper. For a basic introduction to the Brauer–Manin obstruction, see [Skorobogatov 2001; Poonen 2008].

Recall from [Poonen 2001] that an *algebraic* family of curves is a family of curves depending on a parameter T such that substituting any rational number for T results in a smooth curve over \mathbb{Q} .

A smooth geometrically irreducible curve \mathcal{C} over \mathbb{Q} is said to *satisfy the Hasse principle* if the everywhere local solvability of \mathcal{C} is equivalent to the global solvability of \mathcal{C} . In more concrete terms, this means that

$$\mathcal{C}(\mathbb{Q}) \neq \emptyset \text{ if and only if } \mathcal{C}(\mathbb{Q}_p) \neq \emptyset \text{ for every prime } p \text{ including } p = \infty.$$

If \mathcal{C} has points locally everywhere but has no rational points, we say that \mathcal{C} is a *counterexample to the Hasse principle*. Furthermore, if we also have $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ (see [Poonen 2008], or [Skorobogatov 2001] for the definition of $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}}$), we say that \mathcal{C} is a *counterexample to the Hasse principle explained by the Brauer–Manin obstruction*. The Hasse principle fails in general. The first counterexamples of genus-one curves to the Hasse principle were discovered by Lind [1940] and independently shortly thereafter by Reichardt [1942].

Let us relate Theorem 1.1 to existing results in literature. For $n = 1$, Colliot-Thélène and Poonen [2000] showed how to produce one-parameter families of curves of genus one violating the Hasse principle. Poonen [2001] explicitly constructed an algebraic family of genus-one cubic curves violating the Hasse principle using the general method developed in [Colliot-Thélène and Poonen 2000]. It is not known whether there exists an algebraic family of curves of genus n violating the Hasse principle for all $n \geq 2$.

Here, as throughout the article, we say that a smooth geometrically irreducible variety \mathcal{V} over \mathbb{Q} *satisfies* CHP if it is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction. A smooth geometrically irreducible variety \mathcal{V} over \mathbb{Q} is said to *satisfy* NZC if it contains no zero-cycles of odd degree over \mathbb{Q} .

Coray and Manoil [1996] showed that for each positive integer $n \geq 2$, the smooth projective model of the affine curve defined by

$$(1) \quad z^2 = 605 \cdot 10^6 x^{2n+2} + (18x^2 - 4400)(45x^2 - 8800)$$

satisfies CHP and NZC. The Coray–Manoil family of curves is the first family of hyperelliptic curves of varying genus that satisfies CHP and NZC. Although the authors restricted themselves to constructing only one hyperelliptic curve of genus n satisfying CHP and NZC for each integer $n \geq 2$, it seems plausible that their approach can be modified to produce algebraic families of hyperelliptic curves

of arbitrary genus satisfying CHP and NZC. Since we will follow the approach of Coray and Manoil with some modifications to prove Theorem 1.1, we briefly recall their main ideas for constructing the family (1).

Colliot-Thélène, Coray and Sansuc [Colliot-Thélène et al. 1980] proved that the threefold $\mathcal{Y}_{(5,1,1)}$ in $\mathbb{P}_{\mathbb{Q}}^5$, defined by

$$\mathcal{Y}_{(5,1,1)} : \begin{cases} u_1^2 - 5v_1^2 = 2xy, \\ u_2^2 - 5v_2^2 = 2(x + 20y)(x + 25y), \end{cases}$$

satisfies CHP and NZC. Building on this result, Coray and Manoil [1996] introduced a geometric construction of hyperelliptic curves that allows to smoothly embed the family of curves defined by (1) into the threefold $\mathcal{Y}_{(5,1,1)}$. It follows immediately from functoriality that the Coray–Manoil family of curves satisfies CHP and NZC.

In order to generalize the result of Coray and Manoil, we first construct a family of threefolds in $\mathbb{P}_{\mathbb{Q}}^5$ that satisfies CHP and NZC and has the threefold $\mathcal{Y}_{(5,1,1)}$ as a member. The construction of such threefolds is achieved by building on that of the threefold $\mathcal{Y}_{(5,1,1)}$. In order to show that the Brauer–Manin obstruction for these threefolds is nonempty, we also need to show the existence of infinitely many primes p and q satisfying certain quadratic equations. We do this by calling on the result of [Iwaniec 1974] that a quadratic polynomial in two variables represents infinitely many primes. Since the existence of certain threefolds in $\mathbb{P}_{\mathbb{Q}}^5$ satisfying CHP and NZC is of interest in its own right, we state this result here.

Theorem 1.2. *Let p be a prime such that $p \equiv 5 \pmod{8}$ and 3 is quadratic non-residue in \mathbb{F}_p^\times . Then there exist infinitely many pairs $(b, d) \in \mathbb{Z}^2$ such that any smooth and proper \mathbb{Q} -model \mathcal{Z} of the smooth \mathbb{Q} -variety \mathcal{X} in $\mathbb{A}_{\mathbb{Q}}^5$, defined by*

$$\begin{cases} 0 \neq u_1^2 - pv_1^2 = 2x, \\ 0 \neq u_2^2 - pv_2^2 = 2(x + 4pb^2)(x + p^2d^2), \end{cases}$$

satisfies CHP and NZC.

The next step is to choose a family of hyperelliptic curves of arbitrary genus that can be smoothly embedded into the family of threefolds in Theorem 1.2 using the geometric construction of Coray and Manoil. For each $n \geq 2$, we define a family of hyperelliptic curves of genus n of the shape

$$(2) \quad z^2 = p\alpha^2 Q^2 x^{2n+2} + (2b^2 Px^2 + \beta Q)(d^2 pPx^2 + 2\beta Q),$$

where α, β, γ are certain rational numbers, and P, Q depend on $\alpha, \beta, \gamma, p, b, d$. In order to apply the geometric construction of hyperelliptic curves of Coray and Manoil, the polynomials on the right-hand side of (2) are required to be separable.

In order to smoothly embed these hyperelliptic curves into the threefolds in Theorem 1.2, we impose certain conditions on α, β, γ such that these rational numbers satisfy certain local congruences and certain conics in $\mathbb{P}_{\mathbb{Q}}^2$ constructed

from sextuples $(p, b, d, \alpha, \beta, \gamma)$ possess at least one nontrivial rational point. Lemmas 5.1 and 5.4 show that there are infinitely many sextuples $(p, b, d, \alpha, \beta, \gamma)$ satisfying these conditions. For any such sextuple, it follows from functoriality and Theorem 1.2 that the family of hyperelliptic curves of genus n defined by (2) satisfies CHP and NZC for each $n \geq 2$.

In the last step, the main difficulty is to show the existence of rational functions in $\mathbb{Q}(T)$ that parametrize rational numbers α, β, γ such that for each integer $n \geq 2$, substituting any rational number for T in the polynomials on the right-hand side of (2) results in a separable polynomial of degree $2n+2$ over \mathbb{Q} . We do this by calling on a *separability criterion* from [Dong Quan 2014], which will be reviewed in Section 6.

After this article was finished, the author learned that Bhargava, Gross, and Wang [Bhargava et al. 2013] showed that for any integer $n \geq 1$, there is a positive proportion of everywhere locally solvable hyperelliptic curves over \mathbb{Q} of genus n that have no points over any number field of odd degree over \mathbb{Q} . Despite this remarkable result, it cannot determine whether an explicit hyperelliptic curve over \mathbb{Q} satisfies CHP and NZC. The main theorem of this article describes an explicit algebraic family of such curves of genus n with $\gcd(n, 4) = 1$ and $n > 5$.

2. The Hasse principle for certain threefolds in $\mathbb{P}_{\mathbb{Q}}^5$

In this section, we will construct families of threefolds satisfying CHP and NZC. We begin by stating some lemmas that we will need in the proof of the main results throughout the paper.

Lemma 2.1 (see [Coray and Manoil 1996, Lemma 4.8]). *Let k be a number field, and let \mathcal{V}_1 and \mathcal{V}_2 be (proper) k -varieties. Assume that there is a k -morphism $\alpha : \mathcal{V}_1 \rightarrow \mathcal{V}_2$ and $\mathcal{V}_2(\mathbb{A}_k)^{\text{Br}} = \emptyset$. Then $\mathcal{V}_1(\mathbb{A}_k)^{\text{Br}} = \emptyset$.*

Lemma 2.2 (see, for example, [Corn 2007, Proposition 6.4]). *Let \mathcal{X} be a smooth F -variety. Let L/F be a cyclic extension, and let $F(\mathcal{X})$ be the function field of \mathcal{X} . Let f be an element of $F(\mathcal{X})$, and let $\mathcal{X}_L = \mathcal{X} \times_F L$. Then the class of the cyclic algebra $(L/F, f) \in \text{Br}(F(\mathcal{X}))$ lies in the image of the inclusion $\text{Br}(\mathcal{X}) \hookrightarrow \text{Br}(F(\mathcal{X}))$ if and only if $\text{div}(f) = \text{Norm}_{L/F}(D)$ for some $D \in \text{Div}(\mathcal{X}_L)$.*

Lemma 2.3 (Lang–Nishimura, [Colliot-Thélène et al. 1980, p. 164, Lemme 3.1.1]). *Let F be a field, and let \mathcal{X} be an integral F -variety. Let \mathcal{Y} be a proper F -variety, and let $f : \mathcal{X} \rightarrow \mathcal{Y}$ be an F -rational map. If $\mathcal{X}(F)$ contains a regular F -point, then $\mathcal{Y}(F)$ is nonempty. In particular, the condition $\mathcal{X}(F) \neq \emptyset$ is an F -birational invariant in the category of smooth, proper and integral F -varieties \mathcal{X} .*

We now describe a construction of certain Azumaya algebras on certain threefolds.

Lemma 2.4. *Let p be a prime such that $p \equiv 5 \pmod{8}$. Assume that:*

(A1) *3 is a quadratic nonresidue in \mathbb{F}_p^\times .*

(B) *There exists a pair $(b, c) \in \mathbb{Z}^2$ such that $\gcd(b, c) = 1$, $b \not\equiv 0 \pmod{p}$, and $q := |pc - 4b^2|$ is either 1 or an odd power of an odd prime. Here $|\cdot|$ denotes the absolute value in \mathbb{Q} . Furthermore, if $b \equiv 0 \pmod{3}$, then $c \equiv 2 \pmod{3}$.*

Let \mathcal{V} be a smooth, proper \mathbb{Q} -model of the smooth \mathbb{Q} -variety \mathcal{U} in $\mathbb{A}_{\mathbb{Q}}^5$ defined by

$$(3) \quad \mathcal{U}: \begin{cases} 0 \neq u_1^2 - pv_1^2 = 2x, \\ 0 \neq u_2^2 - pv_2^2 = 2(x + 4pb^2)(x + p^2c). \end{cases}$$

Let $\mathbb{Q}(\mathcal{V})$ be the function field of \mathcal{V} , and let \mathcal{A} be the class of the quaternion algebra $(p, x + 4pb^2)$. Then \mathcal{A} is an Azumaya algebra of \mathcal{V} , that is, \mathcal{A} belongs to the subgroup $\text{Br}(\mathcal{V})$ of $\text{Br}(\mathbb{Q}(\mathcal{V}))$.

Proof. Let $K = \mathbb{Q}(\sqrt{p})$. Let Γ be the divisor defined over $\mathbb{Q}(\sqrt{p})$ and lying on \mathcal{V} defined by

$$\Gamma: \quad f := x + 4pb^2 = 0, \quad u_2 - \sqrt{p}v_2 = 0, \quad u_1^2 - pv_1^2 = -8pb^2.$$

Let σ be a generator of $\text{Gal}(K/\mathbb{Q})$. We see that $\text{div}(f) = \Gamma + \sigma\Gamma$, and it thus follows from Lemma 2.2 that \mathcal{A} is in the image of $\text{Br}(\mathcal{V}) \hookrightarrow \text{Br}(\mathbb{Q}(\mathcal{V}))$. \square

Lemma 2.5. *Let p be a prime such that $p \equiv 5 \pmod{8}$. Assume that conditions (A1) and (B) in Lemma 2.4 are true. Then there exists a nonzero integer a such that*

$$(4) \quad \gcd((a^2 + 2pb^2)(2a^2 + p^2c), 3(2b^2 + pc)) = 1.$$

Proof. Assume that $H_1 := 2b^2 + pc = \pm \prod_{i=1}^m l_i^{\alpha_i}$, where l_i are distinct primes and $\alpha_i \in \mathbb{Z}_{>0}$. Note that since $q = |pc - 4b^2|$ is either 1 or an odd power of an odd prime, c is odd. Thus H_1 is odd, and therefore $l_i \neq 2$ for each $1 \leq i \leq m$. We also have that $l_i \neq p$ for each $1 \leq i \leq m$; otherwise, $l_i = p$ for some integer $1 \leq i \leq m$. Since $2b^2 + pc \equiv 0 \pmod{l_i}$ and $l_i = p$, it follows that $b \equiv 0 \pmod{p}$, which is a contradiction. We consider the following cases:

Case 1. $b \equiv 0 \pmod{3}$.

By assumption (B), one knows that $c \equiv 2 \pmod{3}$. Define $a := \prod_{i=1}^m l_i$. We contend that a satisfies (4). Indeed, we have that $l_i \neq 3$ for each $1 \leq i \leq m$; otherwise, $l_i = 3$ for some integer $1 \leq i \leq m$. Since $b \equiv 0 \pmod{3}$ and $p \neq 3$, it follows that $c \equiv 0 \pmod{3}$, which is a contradiction.

Let $H_2 := a^2 + 2pb^2$ and $H_3 := 2a^2 + p^2c$. We see that $a^2 = \prod_{i=1}^m l_i^2 \equiv 1 \pmod{3}$. Since $p \neq 3$, we deduce that $H_2 \equiv 1 \pmod{3}$ and $H_3 \equiv 2 + c \equiv 1 \pmod{3}$, and thus $H_2H_3 \equiv 1 \pmod{3}$.

Suppose that l_j divides H_2 for some integer $1 \leq j \leq m$. Since $a = \prod_{i=1}^m l_i \equiv 0 \pmod{l_j}$, it follows that $b \equiv 0 \pmod{l_j}$. Thus $c \equiv 0 \pmod{l_j}$, which is a contradiction to (B).

Suppose that l_j divides H_3 for some integer $1 \leq j \leq m$. Since $a = \prod_{i=1}^m l_i \equiv 0 \pmod{l_j}$ and $l_j \neq p$, it follows that $c \equiv 0 \pmod{l_j}$. Hence $b \equiv 0 \pmod{l_j}$, which is a contradiction to (B). Therefore, in any event, (4) holds.

Case 2. $b \not\equiv 0 \pmod{3}$ and $c \equiv 0 \pmod{3}$.

Let $a := \prod_{i=1}^m l_i$. By (A1), we know that $p \equiv 2 \pmod{3}$. Hence repeating in the same manner as in Case 1, we deduce that (4) holds.

Case 3. $b \not\equiv 0 \pmod{3}$ and $c \not\equiv 0 \pmod{3}$.

Let $a := 3 \prod_{i=1}^m l_i$. The same arguments as in Case 1 show that (4) holds. \square

Following the techniques in the proof of [Colliot-Thélène et al. 1980, Proposition 7.1], we now prove the main theorem in this section.

Theorem 2.6. *We maintain the same notation as in Lemma 2.4. Let p be a prime such that $p \equiv 5 \pmod{8}$. Assume further that (A1) and (B) are true. Let \mathcal{U} and \mathcal{V} be the \mathbb{Q} -varieties defined in Lemma 2.4. Let \mathcal{T} be the singular \mathbb{Q} -variety in $\mathbb{P}_{\mathbb{Q}}^5$ defined by*

$$(5) \quad \mathcal{T} : \begin{cases} u_1^2 - pv_1^2 = 2xy, \\ u_2^2 - pv_2^2 = 2(x + 4pb^2y)(x + p^2cy). \end{cases}$$

Then \mathcal{U}, \mathcal{V} and \mathcal{T} satisfy CHP and NZC.

Proof. The proof of Theorem 2.6 is divided into several steps.

Step 1. $\mathcal{U}(\mathbb{Q}) = \mathcal{T}(\mathbb{Q})$.

It is clear that $\mathcal{U}(\mathbb{Q}) \subseteq \mathcal{T}(\mathbb{Q})$. Assume that there is a point

$$P := (x : y : u_1 : v_1 : u_2 : v_2) \in \mathcal{T}(\mathbb{Q}).$$

Suppose first that $y = 0$. Then $u_1 = v_1 = 0$. If furthermore $x = 0$, then $u_2 = v_2 = 0$, which is a contradiction. Hence $x \neq 0$, and thus $2 = (u_2/x)^2 - p(v_2/x)^2$. Hence 2 is the norm of an element in $\mathbb{Q}(\sqrt{p})^\times$, and therefore 2 is the norm of an element in $\mathbb{Q}_p(\sqrt{p})^\times$. Thus the local Hilbert symbol $(2, p)_p$ is 1. On the other hand, using [Cohen 2007, p. 296, Theorem 5.2.7] and $p \equiv 5 \pmod{8}$, we deduce that

$$(2, p)_p = \left(\frac{2}{p}\right) = -1,$$

which is a contradiction.

Now we assume that $y \neq 0$, and with no loss of generality, assume further that $y = 1$. We consider the following cases:

Case 1. $x = 0$.

The second equation of (5) implies that $u_2^2 - pv_2^2 = 8p^3b^2c$. Thus $8p^3b^2c$ is the norm of an element in $\mathbb{Q}_2(\sqrt{p})^\times$, and hence the local Hilbert symbol $(8p^3b^2c, p)_2$ is 1. Since $q = |pc - 4b^2|$ is either 1 or an odd power of an odd prime, c is odd.

Hence $v_2(8p^3b^2c) = 3 + 2v_2(b)$, which is an odd integer. Using [Cohen 2007, loc. cit.], we deduce that

$$(8p^3b^2c, p)_2 = \left(\frac{p}{2}\right) = -1,$$

which is a contradiction.

Case 2. $x = -4pb^2$.

It follows from (5) that $u_1^2 - pv_1^2 = -8pb^2$. Using the same arguments as in Case 1, we deduce that $-8pb^2$ is not the norm of any element in $\mathbb{Q}_2(\sqrt{p})^\times$, which is a contradiction to the last identity.

Case 3. $x = -p^2c$.

We see from (5) that $u_1^2 - pv_1^2 = -2p^2c$. Using the same arguments as in Case 1, we deduce that $-2p^2c$ is not the norm of any element in $\mathbb{Q}_2(\sqrt{p})^\times$, which is a contradiction to the last identity.

Therefore, in any event, we have shown that if the point $P := (x : y : u_1 : v_1 : u_2 : v_2)$ belongs to $\mathcal{T}(\mathbb{Q})$, then $y = 1$, $x \neq 0$, $x + 4pb^2 \neq 0$ and $x + p^2c \neq 0$. In other words, the point P satisfies

$$\begin{cases} 0 \neq u_1^2 - pv_1^2 = 2x, \\ 0 \neq u_2^2 - pv_2^2 = 2(x + 4pb^2)(x + p^2c), \end{cases}$$

and thus $P \in \mathcal{U}(\mathbb{Q})$. Therefore $\mathcal{U}(\mathbb{Q}) = \mathcal{T}(\mathbb{Q})$.

Step 2. \mathcal{U} , \mathcal{V} , and \mathcal{T} are everywhere locally solvable.

We now prove that \mathcal{U} , \mathcal{V} and \mathcal{T} are everywhere locally solvable. By Lemma 2.3, it suffices to prove that \mathcal{U} is everywhere locally solvable. Recall that by Lemma 2.5, there is a nonzero integer a such that

$$\gcd((a^2 + 2pb^2)(2a^2 + p^2c), 3(2b^2 + pc)) = 1.$$

Hence it suffices to consider the following cases:

Case I. l is a prime such that $l \neq p$ and $\gcd(l, (a^2 + 2pb^2)(2a^2 + p^2c)) = 1$.

Let $x = 2a^2$. Since $2x = 4a^2$ is a square in \mathbb{Z} , we see that the local Hilbert symbol $(2x, p)_l$ satisfies

$$(2x, p)_l = (4a^2, p)_l = 1.$$

Thus $2x$ is the norm of an element in $\mathbb{Q}_l(\sqrt{p})^\times$.

We see that

$$\begin{aligned} v_l(2(x + 4pb^2)(x + p^2c)) &= v_l(4(a^2 + 2pb^2)(2a^2 + p^2c)) \\ &= 2v_l(2) + v_l((a^2 + 2pb^2)(2a^2 + p^2c)) = 2v_l(2). \end{aligned}$$

Hence, using [Cohen 2007, loc. cit.], we deduce that the local Hilbert symbol $(2(x + 4pb^2)(x + p^2c), p)_l$ equals 1. Thus $2(x + 4pb^2)(x + p^2c)$ is the norm of an element in $\mathbb{Q}_l(\sqrt{p})^\times$. Therefore \mathcal{U} is locally solvable at l .

Case II. l is a prime such that $\gcd(l, 3(2b^2 + pc)) = 1$. Note that p is among these primes.

Assume first that $l = p$, and set $x = 2pb^2$. We see that $2x = p(2b)^2$, and $2(x + 4pb^2)(x + p^2c) = p^2(12b^2)(2b^2 + pc)$. Note that $(2b)^2 \not\equiv 0 \pmod{p}$ and $(12b^2)(2b^2 + pc) \equiv 6(2b^2)^2 \not\equiv 0 \pmod{p}$. Hence, using [Cohen 2007, loc. cit.], we deduce that the local Hilbert symbol $(2x, p)_p$ satisfies

$$(2x, p)_p = (-1)^{(p-1)/2} \left(\frac{(2b)^2}{p} \right) = 1.$$

Hence $2x$ is the norm of an element in $\mathbb{Q}_p(\sqrt{p})$.

By (A1), we know that 6 is quadratic residue in \mathbb{F}_p^\times . Since $(12b^2)(2b^2 + pc) \equiv 6(2b^2)^2 \pmod{p}$, we see that $(12b^2)(2b^2 + pc)$ is a quadratic residue in \mathbb{F}_p^\times . Thus using the same arguments as above, we deduce that

$$(2(x + 4pb^2)(x + p^2c), p)_p = (p^2(12b^2)(2b^2 + pc), p)_p = 1.$$

Therefore $2(x + 4pb^2)(x + p^2c)$ is the norm of an element in $\mathbb{Q}_p(\sqrt{p})$. Hence \mathcal{U} is locally solvable at p .

Suppose that $l \neq p$, and set $x = 2pb^2$. We see that

$$\begin{aligned} v_l(2x) &= v_l(4pb^2) = v_l(p) + 2v_l(2b) = 2v_l(2b), \\ v_l(2(x + 4pb^2)(x + p^2c)) &= v_l(p^2(12b^2)(2b^2 + pc)) \\ &= 2v_l(2b) + v_l(3(2b^2 + pc)) = 2v_l(2b). \end{aligned}$$

Using the same arguments as in Case I, we deduce that \mathcal{U} is locally solvable at l .

It is not difficult to see that $\mathcal{U}(\mathbb{R}) \neq \emptyset$. It follows from Cases I and II that \mathcal{U} is everywhere locally solvable, and thus \mathcal{U}, \mathcal{V} and \mathcal{T} are everywhere locally solvable.

Step 3. \mathcal{V} satisfies CHP.

We will prove that $\mathcal{V}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$. Let $\mathbb{Q}(\mathcal{V})$ be the function field of \mathcal{V} , and let \mathcal{A} be the class of quaternion algebra $(p, x + 4pb^2)$ in $\text{Br}(\mathbb{Q}(\mathcal{V}))$. It follows from Lemma 2.4 that \mathcal{A} is an Azumaya algebra of \mathcal{V} . We will prove that for any $P_l \in \mathcal{V}(\mathbb{Q}_l)$,

$$(6) \quad \text{inv}_l(\mathcal{A}(P_l)) = \begin{cases} 0 & \text{if } l \neq 2, \\ \frac{1}{2} & \text{if } l = 2. \end{cases}$$

Since \mathcal{V} is smooth, we know that $\mathcal{U}(\mathbb{Q}_l)$ is l -adically dense in $\mathcal{V}(\mathbb{Q}_l)$. It is well-known (see, for example, [Viray 2012, Lemma 3.2]) that $\text{inv}_l(\mathcal{A}(P_l))$ is a continuous

function on $\mathcal{V}(\mathbb{Q}_l)$ with the l -adic topology. Hence it suffices to prove (6) for $P_l \in \mathcal{U}(\mathbb{Q}_l)$.

Suppose that $l = \infty$, or l is an odd prime such that $l \neq p$ and p is a square in \mathbb{Q}_l^\times . We see that $p \in \mathbb{Q}_l^{2,\times}$, and hence the local Hilbert symbol $(p, t)_l$ is 1 for any $t \in \mathbb{Q}_l^\times$. Thus $\text{inv}_l(\mathcal{A}(P_l))$ is 0.

Suppose that l is an odd prime such that $l \neq p$ and p is not a square in \mathbb{Q}_l^\times . Let $P_l \in \mathcal{U}(\mathbb{Q}_l)$, and let $x = x(P_l)$. It follows from (3) and [Cohen 2007, loc. cit.] that $v_l(x)$ and $v_l((x+4pb^2)(x+p^2c))$ are even, and hence the sum $v_l(x+4pb^2) + v_l(x+p^2c)$ is even. Assume first that $v_l(x) < 0$. We deduce that $v_l(x+4pb^2) = v_l(x)$, and hence it is even. Suppose now that $v_l(x) \geq 0$. We then see that $v_l(x+4pb^2) \geq 0$ and $v_l(x+p^2c) \geq 0$. We contend that at least one of the last two numbers is zero. Otherwise, since $x \in \mathbb{Z}_l$, one sees that $x+4pb^2 \equiv 0 \pmod{l}$ and $x+p^2c \equiv 0 \pmod{l}$. Hence l divides $p(pc-4b^2)$, and thus by condition (B), we deduce that l divides pq .

If q is 1, then $l = p$, which is a contradiction. If q is an odd power of an odd prime, say q_1^{2m+1} for some odd prime q_1 and $m \in \mathbb{Z}_{\geq 0}$, then $l = q_1$. By condition (B), we know that $q = q_1^{2m+1} \equiv \pm 4b^2 \not\equiv 0 \pmod{p}$. Hence

$$l = q_1 \equiv \pm \left(\frac{2b}{q_1^m}\right)^2 \pmod{p}.$$

Since -1 is a square in \mathbb{F}_p^\times , it follows from the congruence above that l is a square in \mathbb{F}_p^\times . By the quadratic reciprocity law, p is a square in \mathbb{Q}_l^\times , which is a contradiction. Since the sum $v_l(x+4pb^2) + v_l(x+p^2c)$ is even and at least one of the two summands is even, we deduce that each of them is even. Hence, using [Cohen 2007, loc. cit.], we deduce that the local Hilbert symbol $(p, x+4pb^2)_l$ is 1. Therefore $\text{inv}_l(\mathcal{A}(P_l))$ is 0.

Suppose that $l = p$. Let $P_p \in \mathcal{U}(\mathbb{Q}_p)$ and $x = x(P_p)$. Since the local Hilbert symbol $(p, 2)_p$ is -1 , we deduce from (3) and [Cohen 2007, loc. cit.] that

$$(7) \quad \begin{cases} x = p^n \alpha & \text{with } n \in \mathbb{Z}, \alpha \in \mathbb{Z}_p^\times \text{ and } \left(\frac{\alpha}{p}\right) = -1, \\ (x+4pb^2)(x+p^2c) = p^m \beta & \text{with } m \in \mathbb{Z}, \beta \in \mathbb{Z}_p^\times \text{ and } \left(\frac{\beta}{p}\right) = -1. \end{cases}$$

Assume that $n \leq 0$. We see that $p^{-n}x \equiv \alpha \pmod{p}$. Hence $p^{-n}(x+4pb^2) \equiv \alpha \pmod{p}$ and $p^{-n}(x+p^2c) \equiv \alpha \pmod{p}$. Thus the product of the two last congruences contradicts the second equation of (7). Hence, with no loss of generality, we may assume that $n \geq 1$. Assume first that $n = 1$. We deduce that $p^{-1}x \equiv \alpha \pmod{p}$, and hence $p^{-1}(x+p^2c) = p^{-1}x + pc \equiv \alpha \pmod{p}$. Thus, by (7), there exists an integer $k \in \mathbb{Z}$ such that $p^k(x+4pb^2) \equiv \beta\alpha^{-1} \pmod{p}$. We see that $\left(\frac{\beta\alpha^{-1}}{p}\right) = 1$. Hence, using [Cohen 2007, loc. cit.], we deduce that the local Hilbert symbol $(p, x+4pb^2)_p$ satisfies

$$(p, x+4pb^2)_p = \left(\frac{\beta\alpha^{-1}}{p}\right) = 1.$$

Therefore $\text{inv}_p(\mathcal{A}(P_p))$ is 0.

Suppose now that $n \geq 2$. We see that

$$p^{-1}(x + 4pb^2) = p^{n-1}\alpha + 4b^2 \equiv 4b^2 \pmod{p}.$$

Hence, using the same arguments as above, we deduce that the local Hilbert symbol $(p, x + 4pb^2)_p$ is 1, and thus $\text{inv}_p(\mathcal{A}(P_p))$ equals 0.

Therefore, in any event, we see that $\text{inv}_p(\mathcal{A}(P_p)) = 0$.

Suppose that $l = 2$. Let $P_2 \in \mathcal{U}(\mathbb{Q}_2)$, and let $x = x(P_2)$. Since the local Hilbert symbol $(p, 2)_2$ satisfies

$$(p, 2)_2 = \left(\frac{p}{2}\right) = -1,$$

we deduce from (3) and [Cohen 2007, loc. cit.] that

$$(p, x)_2 = (p, (x + 4pb^2)(x + p^2c))_2 = -1.$$

Hence $v_2(x)$ and $v_2((x + 4pb^2)(x + p^2c))$ are odd. Thus $v_2(x + 4pb^2) + v_2(x + p^2c)$ is odd. We contend that $v_2(x) \geq 0$. Otherwise, we deduce that

$$v_2(x + 4pb^2) + v_2(x + p^2c) = 2v_2(x),$$

which is a contradiction since the left-hand side is odd whereas the right-hand side is even. Since $v_2(x)$ is odd and $v_2(x) \geq 0$, we see that $v_2(x) \geq 1$. Since c is odd, it follows that $v_2(p^2c) = 0$. Hence $v_2(x + p^2c) = v_2(p^2c) = 0$, and thus $v_2(x + 4pb^2)$ is odd. Since $p \equiv 5 \pmod{8}$, the local Hilbert symbol $(p, x + 4pb^2)_2$ satisfies

$$(p, x + 4pb^2)_2 = \left(\frac{p}{2}\right) = -1.$$

Therefore $\text{inv}_2(\mathcal{A}(P_2))$ equals $\frac{1}{2}$.

Thus, in any event, $\sum_l \text{inv}_l \mathcal{A}(P_l) = \frac{1}{2}$ for any $(P_l)_l \in \mathcal{V}(\mathbb{A}_{\mathbb{Q}})$. Thus $\mathcal{V}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$.

Step 4. \mathcal{U} and \mathcal{T} satisfy CHP.

For any point $P_l \in \mathcal{U}(\mathbb{Q}_l)$, let $x = x(P_l)$. By the definition of \mathcal{U} , we see that $x + 4pb^2$ is nonzero. By what we have proved in Step 3, we know that the local Hilbert symbol $(p, x + 4pb^2)_l$ satisfies

$$(p, x + 4pb^2)_l = \begin{cases} 1 & \text{if } l \neq 2, \\ -1 & \text{if } l = 2. \end{cases}$$

Hence it follows that $x + 4pb^2$ is the norm of an element of $\mathbb{Q}_l(\sqrt{p})$ for every $l \neq 2$ including $l = \infty$, and that $x + 4pb^2$ is not a local norm of any element of $\mathbb{Q}_2(\sqrt{p})$. Thus we deduce that

$$(8) \quad \prod_l (p, x + 4pb^2)_l = -1,$$

where the product is taken over every prime l , including $l = \infty$. Therefore it follows from the product formula [Cohen 2007, Theorem 5.3.1] that $\mathcal{U}(\mathbb{Q})$ is empty; otherwise there exists a rational point $P \in \mathcal{U}(\mathbb{Q})$. Thus the element $x + 4pb^2$ is in \mathbb{Q}^\times , where $x = x(P)$. Hence, by the product formula, we see that

$$\prod_l (p, x + 4pb^2)_l = 1,$$

which is a contradiction to (8). Hence \mathcal{U} satisfies CHP, and it thus follows from Step 1 that \mathcal{T} satisfies CHP.

Step 5. \mathcal{U}, \mathcal{V} and \mathcal{T} satisfy NZC.

Note that since $\mathcal{T}(\mathbb{Q}) = \emptyset$, it follows from the Amer–Brumer theorem [Amer 1976; Brumer 1978] that \mathcal{T} does not contain any zero-cycle of odd degree over \mathbb{Q} . Thus \mathcal{U}, \mathcal{V} and \mathcal{T} satisfy NZC, and hence our contention follows. \square

The following result plays a key role in constructing algebraic families of curves satisfying CHP and NZC.

Theorem 2.7. *Let p be a prime such that $p \equiv 5 \pmod{8}$. Assume (A1), and assume further that the following is true:*

(A2) *There exists a pair (b, d) of integers such that b, d are odd, $b \not\equiv 0 \pmod{3}$, $b \not\equiv 0 \pmod{p}$ and $q := |pd^2 - 4b^2|$ is either 1 or an odd prime.*

Let \mathcal{Z} be a smooth and proper \mathbb{Q} -model of the smooth \mathbb{Q} -variety \mathcal{X} in $\mathbb{A}_{\mathbb{Q}}^5$ defined by

$$(9) \quad \mathcal{X} : \begin{cases} 0 \neq u_1^2 - pv_1^2 = 2x, \\ 0 \neq u_2^2 - pv_2^2 = 2(x + 4pb^2)(x + p^2d^2). \end{cases}$$

Let $\mathcal{Y} \subset \mathbb{P}_{\mathbb{Q}}^5$ be the singular \mathbb{Q} -variety defined by

$$(10) \quad \mathcal{Y} : \begin{cases} u_1^2 - pv_1^2 = 2xy, \\ u_2^2 - pv_2^2 = 2(x + 4pb^2y)(x + p^2d^2y). \end{cases}$$

Then \mathcal{X}, \mathcal{Y} and \mathcal{Z} satisfy CHP and NZC.

Remark 2.8. In Section 3, we will prove that there are infinitely many triples (p, b, d) satisfying (A1) and (A2).

Proof. Let $c = d^2$. We contend that the pair (b, c) satisfies (B) in Lemma 2.4. Indeed, we note that $\gcd(b, d) = 1$; otherwise, there exists an odd prime l such that $b = lb_1$ and $d = ld_1$ for some integers $b_1, d_1 \in \mathbb{Z}$. Hence $q = l_1^2 |pd_1^2 - 4b_1^2|$, which is a contradiction to (A2). Thus $\gcd(b, d) = 1$, and it follows that $\gcd(b, c) = 1$.

We know that $q = |pc - 4b^2|$ is either 1 or an odd prime, and that $b \not\equiv 0 \pmod{3}$ and $b \not\equiv 0 \pmod{p}$. Hence the pair (b, c) satisfies (B). Thus by Theorem 2.6, we deduce that \mathcal{X}, \mathcal{Y} and \mathcal{Z} satisfy CHP and NZC. \square

3. Infinitude of triples (p, b, d) .

In this section, we will prove that there are infinitely many triples (p, b, d) satisfying (A1) and (A2). We begin by recalling a theorem of Iwaniec's.

Let $P(x, y)$ be a quadratic polynomial in two variables x and y . We say that P depends essentially on two variables if $\partial P/\partial x$ and $\partial P/\partial y$ are linearly independent as elements of the \mathbb{Q} -vector space $\mathbb{Q}[x, y]$.

Theorem 3.1 [Iwaniec 1974, p. 443]. *Let $P(x, y) = ax^2 + bxy + cy^2 + ex + fy + g$ be a quadratic polynomial defined over \mathbb{Q} , and assume that the following are true:*

- (i) a, b, c, e, f, g are in \mathbb{Z} and $\gcd(a, b, c, e, f, g) = 1$.
- (ii) $P(x, y)$ is irreducible in $\mathbb{Q}[x, y]$, represents arbitrarily large odd numbers and depends essentially on two variables.
- (iii) $D = af^2 - bef + ce^2 + (b^2 - 4ac)g = 0$ or $\Delta = b^2 - 4ac$ is a perfect square.

Then

$$\frac{N}{\log N} \ll \sum_{\substack{p \leq N, p=P(x,y) \\ p \text{ prime}}} 1.$$

We now prove the main lemma in this section.

Lemma 3.2. *Let p be a prime such that $p \equiv 5 \pmod{8}$, and assume that 3 is a quadratic nonresidue in \mathbb{F}_p^\times . Then there are infinitely many triples (p, b, d) satisfying (A1) and (A2).*

Proof. The result follows immediately by applying Theorem 3.1 to

$$P(x, y) := p(2x + 1)^2 - 4(6py + b_0)^2 \in \mathbb{Q}[x, y],$$

where b_0 is an odd integer such that $\gcd(b_0, 3p) = 1$. □

Example 3.3. Let $(p, b, d) = (5, 1, 1)$. We see that the triple (p, b, d) satisfies (A1) and (A2). Let $\mathcal{Y}_{(5,1,1)}$ be the singular \mathbb{Q} -threefold in $\mathbb{P}_{\mathbb{Q}}^5$ defined by

$$\mathcal{Y}_{(5,1,1)} : \begin{cases} u_1^2 - 5v_1^2 = 2xy, \\ u_2^2 - 5v_2^2 = 2(x + 20y)(x + 25y). \end{cases}$$

By Theorem 2.7, $\mathcal{Y}_{(5,1,1)}$ satisfies CHP and NZC. The threefold $\mathcal{Y}_{(5,1,1)}$ is the well-known Colliot-Thélène–Coray–Sansuc threefold [Colliot-Thélène et al. 1980, p. 186, Proposition 7.1].

Example 3.4. Let $(p, b, d) = (29, 1, 3)$. We see that

$$q = |pd^2 - 4b^2| = |29 \cdot 3^2 - 4 \cdot 1^2| = 257,$$

which is an odd prime. Hence $(29, 1, 3)$ satisfies (A1) and (A2). Let $\mathcal{Y}_{(29,1,3)}$ be the singular \mathbb{Q} -threefold in $\mathbb{P}_{\mathbb{Q}}^5$ defined by

$$\mathcal{Y}_{(29,1,3)} : \begin{cases} u_1^2 - 29v_1^2 = 2xy, \\ u_2^2 - 29v_2^2 = 2(x + 116y)(x + 7569y). \end{cases}$$

By Theorem 2.7, $\mathcal{Y}_{(29,1,3)}$ satisfies CHP and NZC.

4. Hyperelliptic curves violating the Hasse principle

In this section, we give a sufficient condition under which, for each integer $n \geq 2$ and $n \not\equiv 0 \pmod{4}$, there exist hyperelliptic curves of genus n that lie on the threefolds \mathcal{Y} in Theorem 2.7, and satisfy CHP and NZC. The sufficient condition is in terms of the existence of certain sextuples $(p, b, d, \alpha, \beta, \gamma)$, and obtained using the geometric construction of hyperelliptic curves due to [Coray and Manoil 1996, Proposition 4.2].

Theorem 4.1. *Let p be a prime such that $p \equiv 5 \pmod{8}$, and let $(p, b, d) \in \mathbb{Z}^3$ be a triple of integers satisfying (A1) and (A2). Let n be an integer such that $n \geq 2$, and let $(\alpha, \beta, \gamma) \in \mathbb{Q}^3$ be a triple of rational numbers such that $\alpha\beta\gamma \neq 0$. Assume further that the following are true:*

(A3) *We have*

$$(11) \quad P := p\alpha^2 + 2\beta^2 - 2p\gamma^2 \neq 0,$$

$$(12) \quad Q := 4bdp\gamma - 4b^2\beta - d^2p\beta \neq 0,$$

and the conic $\mathcal{Q}_1 \subset \mathbb{P}_{\mathbb{Q}}^2$, defined by

$$\mathcal{Q}_1 : pU^2 - V^2 - (\beta PQ)T^2 = 0,$$

has a point $(u, v, t) \in \mathbb{Z}^3$ with $uvt \neq 0$ and $\gcd(u, v, t) = 1$.

(S) *The polynomial $P_{p,b,d,\alpha,\beta,\gamma}(x) \in \mathbb{Q}[x]$, defined by*

$$P_{p,b,d,\alpha,\beta,\gamma}(x) := p\alpha^2 Q^2 x^{2n+2} + (2b^2 Px^2 + \beta Q)(d^2 p Px^2 + 2\beta Q),$$

is separable; that is, $P_{p,b,d,\alpha,\beta,\gamma}(x)$ has exactly $2n + 2$ distinct roots in \mathbb{C} .

Let \mathcal{C} be the smooth projective model of the affine curve defined by

$$(13) \quad \mathcal{C} : z^2 = p\alpha^2 Q^2 x^{2n+2} + (2b^2 Px^2 + \beta Q)(d^2 p Px^2 + 2\beta Q).$$

Then $\mathcal{C}(\mathbb{Q}_l) \neq \emptyset$ for every prime $l \neq 2, p$, and $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$. Furthermore, \mathcal{C} satisfies NZC.

Proof. The proof follows closely that of [Coray and Manoil 1996, Proposition 4.2]. We begin by recalling the geometric construction of hyperelliptic curves due to Coray and Manoil.

Let $\mathcal{C}_a \subset \mathbb{A}_K^2$ be the affine curve defined by $z^2 = P(x)$, where $P(x)$ is a separable polynomial of degree $2n+2$ and K is a number field. Recall from [Silverman 1986, Chapter II, Exercise 2.14] that the smooth projective model of \mathcal{C}_a can be described as the closure of the image of \mathcal{C}_a under the mapping

$$\begin{aligned} \mathcal{C}_a &\rightarrow \mathbb{P}_K^{n+2}, \\ (x, z) &\mapsto (1, x, \dots, x^{n+1}, z). \end{aligned}$$

Following [Coray and Manoil 1996, Proposition 4.2], we will index the coordinates of \mathbb{P}_K^{n+2} in such a way that z_i corresponds to x^i for $0 \leq i \leq n+1$ and z_{n+2} corresponds to z .

Using the above arguments, we deduce from (13) that \mathcal{C} can be smoothly embedded into the intersection of quadrics defined by

$$(14) \quad \begin{cases} z_{n+2}^2 = p\alpha^2 Q^2 z_{n+1}^2 + (2b^2 P z_2 + \beta Q z_0)(d^2 p P z_2 + 2\beta Q z_0), \\ z_1^2 = z_2 z_0. \end{cases}$$

Recall that $(u, v, t) \in \mathbb{Z}^3$ is the point on the conic \mathcal{Q}_1 defined in (A3) that is assumed to exist. Upon letting

$$z_0 = \frac{1}{\beta Q} x, \quad z_1 = \frac{t}{u} u_1, \quad z_2 = \frac{2p}{P} y, \quad z_{n+1} = \frac{1}{\alpha Q} v_2, \quad z_{n+2} = u_2,$$

we deduce from (14) that

$$(15) \quad \begin{cases} \frac{\beta P Q t^2}{p u^2} u_1^2 = 2xy, \\ u_2^2 - p v_2^2 = 2(x + 4pb^2 y)(x + p^2 d^2 y). \end{cases}$$

We see that (15) defines a singular del Pezzo surface $\mathcal{D} \subseteq \mathbb{P}_{\mathbb{Q}}^4$. We contend that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ and \mathcal{D} does not contain any zero-cycle of odd degree over \mathbb{Q} . Indeed, upon letting

$$v_1 = \frac{v}{pu} u_1,$$

we deduce from the first equation of (15) and (A3) that

$$u_1^2 - p v_1^2 = u_1^2 - p \frac{v^2}{p^2 u^2} u_1^2 = \frac{\beta P Q t^2}{p u^2} u_1^2 = 2xy.$$

Therefore \mathcal{D} is a hyperplane section of the threefold \mathcal{Y} in Theorem 2.7. Hence there exists a sequence of \mathbb{Q} -morphisms

$$\mathcal{C} \rightarrow \mathcal{D} \rightarrow \mathcal{Y}.$$

Hence it follows from Lemma 2.1 and Theorem 2.7 that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$. Thus $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$. Furthermore, since \mathcal{Y} does not contain any zero-cycle of odd degree over \mathbb{Q} , neither do \mathcal{C} and \mathcal{D} .

We now prove that \mathcal{C} is locally solvable at primes l with $l \neq 2, p$. We consider the following cases:

Case I. $l = \infty$ or l is an odd prime such that $l \neq p$ and $(\frac{p}{l}) = 1$.

We know that the curve \mathcal{C}^* , defined by

$$\mathcal{C}^* : z^2 = p\alpha^2 Q^2 x^{2n+2} + y^{2n-2} (2b^2 P x^2 + \beta Q y^2) (d^2 p P x^2 + 2\beta Q y^2),$$

is an open subscheme of \mathcal{C} . We see that $P_{\infty} = (x : y : z) = (1 : 0 : \sqrt{p}\alpha Q)$ belongs to $\mathcal{C}^*(\mathbb{Q}_l) \subset \mathcal{C}(\mathbb{Q}_l)$, and hence \mathcal{C} is locally solvable at l .

Case II. l is an odd prime such that $(\frac{2}{l}) = 1$.

It follows from (13) that the point $P_1 = (x, z) = (0, \sqrt{2}\beta Q)$ belongs to $\mathcal{C}(\mathbb{Q}_l)$.

Case III. l is an odd prime such that $l \neq p$ and $(\frac{2p}{l}) = 1$.

Let $F(x, z)$ be the defining polynomial of \mathcal{C} , defined by

$$F(x, z) = p\alpha^2 Q^2 x^{2n+2} + (2b^2 P x^2 + \beta Q) (d^2 p P x^2 + 2\beta Q) - z^2.$$

We see that

$$\begin{aligned} & F(1, \sqrt{2p}(\gamma Q + bdP)) \\ &= (p\alpha^2 Q^2 + 2p(bdP)^2 + 4b^2\beta PQ + \beta p PQ d^2 + 2\beta^2 Q^2) - 2p(\gamma Q + bdP)^2. \end{aligned}$$

Hence, it follows from (11) and (12) that

$$p\alpha^2 Q^2 + 4b^2\beta PQ + \beta p PQ d^2 + 2\beta^2 Q^2 = 2p\gamma^2 Q^2 + 4p(\gamma Q)(bdP).$$

Thus

$$p\alpha^2 Q^2 + 2p(bdP)^2 + 4b^2\beta PQ + \beta p PQ d^2 + 2\beta^2 Q^2 = 2p(\gamma Q + bdP)^2.$$

Hence, we deduce that $F(1, \sqrt{2p}(\gamma Q + bdP)) = 0$, and therefore the point $P_2 = (1, \sqrt{2p}(\gamma Q + bdP))$ belongs to $\mathcal{C}(\mathbb{Q}_l)$.

Thus, in any event, \mathcal{C} is locally solvable at primes l with $l \neq 2, p$, which proves our contention. \square

Remark 4.2. Theorem 4.1 constructs hyperelliptic curves of genus at least two such that they satisfy NZC and all conditions in CHP except the local solvability at 2 and p . The rest of this section presents certain sufficient conditions for which

those hyperelliptic curves arising from Theorem 4.1 are locally solvable at 2 and p , and hence satisfy CHP and NZC.

Lemma 4.3. *Let p be a prime such that $p \equiv 5 \pmod{8}$, and let $(b, d) \in \mathbb{Z}^3$ be a pair of integers satisfying (A1) and (A2). Assume that there is a triple $(\alpha, \beta, \gamma) \in \mathbb{Q}^3$ satisfying (A3) in Theorem 4.1, and assume further that $\alpha, \beta, \gamma \in \mathbb{Z}_p$. Then there is a rational number $\bar{\beta} \in \mathbb{Q}$ such that $\beta = p\bar{\beta}$ and $\bar{\beta} \in \mathbb{Z}_p$.*

Proof. Let \mathcal{Q}_1 be the conic defined in (A3). Assume that $(u, v, t) \in \mathbb{Z}^3$ belongs to $\mathcal{Q}_1(\mathbb{Q})$ such that $uvt \neq 0$ and $\gcd(u, v, t) = 1$. We see that

$$pu^2 - v^2 - \beta PQt^2 = 0,$$

where P and Q are defined by (11) and (12), respectively. Taking the identity above modulo p , it follows that

$$v^2 \equiv 8b^2\beta^4t^2 \pmod{p}.$$

Since 2 is a quadratic nonresidue in \mathbb{F}_p^\times and $b \not\equiv 0 \pmod{p}$, we deduce from the congruence above that

$$v \equiv \beta t \equiv 0 \pmod{p}.$$

Assume that $\beta \not\equiv 0 \pmod{p}$. Then $v \equiv t \equiv 0 \pmod{p}$, and hence $v = pv_1$ and $t = pt_1$ for some integers v_1, t_1 . Substituting v and t into the defining equation of the conic \mathcal{Q}_1 , we get

$$u^2 - pv_1^2 - p\beta PQt_1^2 = 0,$$

and hence it follows that p divides u . Thus p divides $\gcd(u, v, t)$, which is a contradiction. Therefore there is a rational number $\bar{\beta} \in \mathbb{Q}$ such that $\beta = p\bar{\beta}$ and $\bar{\beta} \in \mathbb{Z}_p$. \square

Remark 4.4. By Lemma 4.3, one knows that if $(\alpha, \beta, \gamma) \in \mathbb{Q}^3$ satisfies (A3) and $\alpha, \beta, \gamma \in \mathbb{Z}_p$, then there is a rational number $\bar{\beta}$ such that $\beta = p\bar{\beta}$ and $\bar{\beta} \in \mathbb{Z}_p$. Hence one sees that $P = pP_1$ and $Q = pQ_1$, where

$$\begin{aligned} P_1 &:= \alpha^2 + 2p\bar{\beta}^2 - 2\gamma^2, \\ Q_1 &:= 4bd\gamma - 4b^2\bar{\beta} - d^2p\bar{\beta}. \end{aligned}$$

We also see that P_1 and Q_1 belong to \mathbb{Z}_p .

In the proofs of Corollaries 4.6 and 4.8 below, we will use Hensel's lemma to deduce the local solvability at primes 2 and p . For the sake of self-containedness, we recall the statement of Hensel's lemma.

Theorem 4.5 [Borevich and Shafarevich 1966, Section 5.2, Theorem 3]. *Let p be a prime. Let $F(x_1, x_2, \dots, x_n) \in \mathbb{Z}_p[x_1, x_2, \dots, x_n]$ be a polynomial whose*

coefficients are p -adic integers. Let δ be a nonnegative integer. Assume that there are p -adic integers a_1, a_2, \dots, a_n such that for some integer $1 \leq k \leq n$, we have

$$\begin{aligned} F(a_1, a_2, \dots, a_n) &\equiv 0 \pmod{p^{2\delta+1}}, \\ \frac{\partial F}{\partial x_k}(a_1, a_2, \dots, a_n) &\equiv 0 \pmod{p^\delta}, \\ \frac{\partial F}{\partial x_k}(a_1, a_2, \dots, a_n) &\not\equiv 0 \pmod{p^{\delta+1}}. \end{aligned}$$

Then there exist p -adic integers $\theta_1, \theta_2, \dots, \theta_n$ such that $F(\theta_1, \theta_2, \dots, \theta_n) = 0$.

The following result provides a sufficient condition under which certain hyperelliptic curves of odd genus satisfy CHP and NZC.

Corollary 4.6. *We maintain the same notation and assumptions as in Theorem 4.1. Assume (A1)–(A3) and (S). Assume further that the following are true:*

- (A4) $\alpha, \beta, \gamma \in \mathbb{Z}_2^\times, \alpha, \gamma, d \in \mathbb{Z}_p^\times$ and $\beta \in \mathbb{Z}_p$.
- (A5) $\gamma Q_1 + bdP_1 \equiv 0 \pmod{p^2}$, where $\bar{\beta}, P_1$ and Q_1 are defined as in Remark 4.4.
- (A6) $n \not\equiv -2(\gamma/\alpha)^2 \pmod{p}, n \geq 3$ and n is odd.

Let \mathcal{C} be the smooth projective model of the affine curve defined by (13). Then \mathcal{C} satisfies CHP and NZC.

Proof. By Theorem 4.1, it suffices to prove that \mathcal{C} is locally solvable at 2 and p .

Step 1. \mathcal{C} is locally solvable at p .

We will use Theorem 4.5 with the exponent $\delta = 3$ to prove the local solvability of \mathcal{C} at p . We consider the system of equations

$$(16) \quad \left\{ \begin{aligned} F(x, z) &= p\alpha^2 Q^2 x^{2n+2} + (2b^2 P x^2 + \beta Q)(d^2 p P x^2 + 2\beta Q) - z^2 \\ &\equiv 0 \pmod{p^7}, \\ \frac{\partial F}{\partial x}(x, z) &= (2n+2)p\alpha^2 Q^2 x^{2n+1} + 4b^2 P x(d^2 p P x^2 + 2\beta Q) \\ &\quad + 2d^2 p P x(2b^2 P x^2 + \beta Q) \\ &\equiv 0 \pmod{p^3}, \\ \frac{\partial F}{\partial x}(x, z) &\not\equiv 0 \pmod{p^4}. \end{aligned} \right.$$

Repeating the same arguments as in Case III of the proof of Theorem 4.1, we deduce that

$$F(1, 0) = 2p(\gamma Q + bdP)^2.$$

By Remark 4.4, one knows that $P = pP_1$ and $Q = pQ_1$. Hence

$$(17) \quad F(1, 0) = 2p^3(\gamma Q_1 + bdP_1)^2.$$

Thus it follows from (A5) and (17) that $F(1, 0) \equiv 0 \pmod{p^7}$. On the other hand, we see that

$$(18) \quad \frac{\partial F}{\partial x}(1, 0) = p^3((2n+2)\alpha^2 Q_1^2 + 4b^2 P_1(d^2 P_1 + 2\bar{\beta} Q_1) + 2d^2 P_1(2b^2 P_1 + p\bar{\beta} Q_1)).$$

Since $\alpha, \bar{\beta}, \gamma$ and P_1, Q_1 are in \mathbb{Z}_p , one obtains that

$$\frac{\partial F}{\partial x}(1, 0) \equiv 0 \pmod{p^3}.$$

Assume that

$$(19) \quad \frac{1}{p^3} \left(\frac{\partial F}{\partial x}(1, 0) \right) \equiv 0 \pmod{p}.$$

Since $\gamma \in \mathbb{Z}_p^\times$, it follows from (A5) that

$$(20) \quad Q_1 \equiv -\frac{bd}{\gamma} P_1 \pmod{p}.$$

Upon replacing Q_1 by $-(bd/\gamma)P_1$ in (19), we deduce that

$$\frac{2P_1^2 bd}{\gamma^2} ((n+1)\alpha^2 bd + \gamma(4bd\gamma - 4b^2\bar{\beta} - d^2 p\bar{\beta})) \equiv 0 \pmod{p}.$$

Thus it follows from the definition of Q_1 in Remark 4.4 that

$$\frac{2P_1^2 bd}{\gamma^2} ((n+1)\alpha^2 bd + \gamma Q_1) \equiv 0 \pmod{p}.$$

Note that $P_1 \in \mathbb{Z}_p^\times$; otherwise, we deduce from the definition of P_1 in Remark 4.4 that

$$\alpha^2 - 2\gamma^2 \equiv P_1 \equiv 0 \pmod{p}.$$

Since $\alpha, \gamma \in \mathbb{Z}_p^\times$, it follows from the congruence above that $2 \equiv (\alpha/\gamma)^2 \pmod{p}$, which is a contradiction to the fact that $p \equiv 5 \pmod{8}$. Thus $P_1 \in \mathbb{Z}_p^\times$. Since $2, b, d, \gamma$ and P_1 are in \mathbb{Z}_p^\times , we obtain that

$$(n+1)\alpha^2 bd + \gamma Q_1 \equiv 0 \pmod{p}.$$

Since $\gamma Q_1 \equiv -bdP_1 \pmod{p}$ and $b, d \in \mathbb{Z}_p^\times$, we deduce from this congruence that

$$(n+1)\alpha^2 \equiv P_1 \equiv (\alpha^2 - 2\gamma^2) \pmod{p}.$$

Since $\alpha, \gamma \in \mathbb{Z}_p^\times$, it follows that $n \equiv -2(\gamma/\alpha)^2 \pmod{p}$, which is a contradiction to (A6). Thus the system (16) has a solution $(x, z) = (1, 0)$. By Hensel's lemma, \mathcal{C} is locally solvable at p .

Step 2. \mathcal{C} is locally solvable at 2.

We will use Theorem 4.5 with the exponent $\delta = 1$ to prove the local solvability of \mathcal{C} at 2. We consider the system of equations

$$(21) \quad \begin{cases} F(x, z) \equiv 0 \pmod{2^3}, \\ \frac{\partial F}{\partial x}(x, z) \equiv 0 \pmod{2}, \\ \frac{\partial F}{\partial x}(x, z) \not\equiv 0 \pmod{2^2}. \end{cases}$$

We see from (17) and the definitions of P_1 and Q_1 that

$$F(1, 0) = 2p^3(\gamma(4bd\gamma - 4b^2\bar{\beta} - d^2p\bar{\beta}) + bd(\alpha^2 + 2p\bar{\beta}^2 - 2\gamma^2))^2.$$

Since β is in \mathbb{Z}_2^\times and $p \neq 2$, we see that $\bar{\beta}$ is also in \mathbb{Z}_2^\times . Since $b, d, p, \alpha, \bar{\beta}, \gamma \in \mathbb{Z}_2^\times$, we see that

$$-d^2p\bar{\beta}\gamma + bd\alpha^2 \equiv 0 \pmod{2}.$$

Let v_2 denote the 2-adic valuation. We see that

$$\begin{aligned} v_2(\gamma(4bd\gamma - 4b^2\bar{\beta} - d^2p\bar{\beta}) + bd(\alpha^2 + 2p\bar{\beta}^2 - 2\gamma^2)) \\ = v_2((4\gamma(bd\gamma - b^2\bar{\beta}) + 2bd(p\bar{\beta}^2 - \gamma^2)) + (-d^2p\bar{\beta}\gamma + bd\alpha^2)) \\ \geq \min(v_2(4\gamma(bd\gamma - b^2\bar{\beta}) + 2bd(p\bar{\beta}^2 - \gamma^2)), v_2(-d^2p\bar{\beta}\gamma + bd\alpha^2)) \geq 1. \end{aligned}$$

Hence $F(1, 0) \equiv 0 \pmod{2^3}$. On the other hand, we know from (18) that

$$\frac{\partial F}{\partial x}(1, 0) \equiv 0 \pmod{2}.$$

Since n is odd, $(2n + 2) \equiv 2(n + 1) \equiv 0 \pmod{2^2}$. Hence, it follows from (18) that

$$\frac{\partial F}{\partial x}(1, 0) \equiv 2d^2p^4\bar{\beta}P_1Q_1 \pmod{2^2}.$$

By (A4) and the definitions of P_1 and Q_1 , we know that

$$d^2p^4\bar{\beta}P_1Q_1 \not\equiv 0 \pmod{2}.$$

Hence we deduce that $(\partial F/\partial x)(1, 0) \not\equiv 0 \pmod{2^2}$. Thus the system (21) has a solution $(x, z) = (1, 0)$. By Hensel's lemma, \mathcal{C} is locally solvable at 2, and hence our contention follows. \square

Remark 4.7. Assume (A1)–(A3), (A5) and (S). Following closely the proof of Corollary 4.6, we note that the following are true:

- (1) If $\alpha, \beta, \gamma \in \mathbb{Z}_2^\times$ and n is odd, then \mathcal{C} is locally solvable at 2.
- (2) If $\alpha, \gamma, d \in \mathbb{Z}_p^\times, \beta \in \mathbb{Z}_p, n \geq 2$ and $n \not\equiv -2(\gamma/\alpha)^2 \pmod{p}$, then \mathcal{C} is locally solvable at p .

We now prove a sufficient condition under which certain hyperelliptic curves of genus $n \equiv 2 \pmod{4}$ satisfy CHP and NZC.

Corollary 4.8. *We maintain the same notation as in Theorem 4.1 and Corollary 4.6. Assume (A1)–(A5) and (S). Assume further that the following are true:*

$$(B1) \quad bd - \bar{\beta}\gamma \equiv 0 \pmod{4}.$$

$$(B2) \quad n \not\equiv -2(\gamma/\alpha)^2 \pmod{p}, \quad n \geq 2 \text{ and } n \equiv 2 \pmod{4}.$$

Let \mathcal{C} be the smooth projective model defined by (13). Then \mathcal{C} satisfies CHP and NZC.

Proof. By Theorem 4.1 and Remark 4.7, it suffices to prove that \mathcal{C} is locally solvable at 2. We will use Theorem 4.5 with the exponent $\delta = 2$ to prove the local solvability of \mathcal{C} at 2. We consider the system of equations

$$(22) \quad \begin{cases} F(x, z) \equiv 0 \pmod{2^5}, \\ \frac{\partial F}{\partial x}(x, z) \equiv 0 \pmod{2^2}, \\ \frac{\partial F}{\partial x}(x, z) \not\equiv 0 \pmod{2^3}, \end{cases}$$

where $F(x, z)$ denotes the polynomial in the variables x, z defined in (16). Since $\alpha \in \mathbb{Z}_2^\times$, we know that $\alpha \equiv 1 \pmod{4}$ or $\alpha \equiv 3 \pmod{4}$. Hence $\alpha^2 \equiv 1 \pmod{4}$. Similarly we know that $\bar{\beta}^2, \gamma^2, b^2, d^2 \equiv 1 \pmod{4}$. Since $p \equiv 5 \pmod{8}$, it follows that

$$P_1 \equiv 1 \pmod{4},$$

$$Q_1 \equiv -\bar{\beta} \pmod{4}.$$

By (B1), we know that

$$\gamma Q_1 + bd P_1 \equiv bd - \bar{\beta}\gamma \equiv 0 \pmod{4},$$

and hence we deduce from (17) that $F(1, 0) \equiv 0 \pmod{2^5}$.

Since $n \equiv 2 \pmod{4}$, there is a nonnegative integer l such that $n = 4l + 2$. We know that

$$\begin{aligned} 4b^2 P_1 (d^2 P_1 + 2\bar{\beta} Q_1) + 2d^2 P_1 (2b^2 P_1 + p\bar{\beta} Q_1) \\ = 8b^2 d^2 P_1^2 + 8b^2 \bar{\beta} P_1 Q_1 + 2pd^2 \bar{\beta} P_1 Q_1. \end{aligned}$$

Hence, it follows from (18) that

$$\frac{\partial F}{\partial x}(1, 0) \equiv 2\alpha^2 Q_1^2 + 2pd^2 \bar{\beta} P_1 Q_1 \equiv 2 - 2\bar{\beta}^2 \equiv 0 \pmod{2^2}.$$

Similarly, one sees that

$$\frac{\partial F}{\partial x}(1, 0) \equiv 5(8l + 6)\alpha^2 Q_1^2 + 10pd^2 \bar{\beta} P_1 Q_1 \pmod{2^3}.$$

Since $\alpha, \bar{\beta}, \gamma, b, d \in \mathbb{Z}_2^\times$, we deduce that $\alpha^2, \bar{\beta}^2, \gamma^2, b^2, d^2 \equiv 1 \pmod{2^3}$. Since $p \equiv 5 \pmod{2^3}$ and $bd\gamma - b^2\bar{\beta} \equiv 0 \pmod{2}$, it follows from the definitions of P_1 and Q_1 that

$$\begin{aligned} P_1 &\equiv 1 \pmod{2^3}, \\ Q_1 &\equiv 4(bd\gamma - b^2\bar{\beta}) - 5\bar{\beta} \equiv -5\bar{\beta} \pmod{2^3}. \end{aligned}$$

Thus we see that

$$\frac{\partial F}{\partial x}(1, 0) \equiv 30 - 250\bar{\beta}^2 \equiv 4 \not\equiv 0 \pmod{2^3}.$$

Therefore the system (22) has a solution $(x, z) = (1, 0)$. By Hensel's lemma, \mathcal{C} is locally solvable at 2, which proves our contention. \square

5. Infinitude of sextuples $(p, b, d, \alpha, \beta, \gamma)$

By Corollaries 4.6 and 4.8, we know that in order to construct algebraic families of hyperelliptic curves satisfying CHP and NZC, we need to find certain sextuples of rational functions in $\mathbb{Q}(T)$ that parametrize sextuples $(p, b, d, \alpha, \beta, \gamma)$ satisfying (A1)–(A5), (S) and (B1). In this section, we show how to produce infinitely many sextuples $(p, b, d, \alpha, \beta, \gamma)$ satisfying (A1)–(A5) and (B1) from the known ones.

Lemma 5.1. *Let (p, b, d) be a triple of integers satisfying (A1) and (A2). Assume that there is a triple $(\alpha_0, \beta_0, \gamma_0) \in \mathbb{Q}^3$ satisfying (A3)–(A5) and (B1). Let $(u_0, v_0, t_0) \in \mathbb{Z}^3$ be a point on the conic $Q_1^{(\alpha_0, \beta_0, \gamma_0)}$ such that $u_0v_0t_0 \neq 0$ and $\gcd(u_0, v_0, t_0) = 1$, where the conic $Q_1^{(\alpha_0, \beta_0, \gamma_0)}$ is defined by*

$$Q_1^{(\alpha_0, \beta_0, \gamma_0)} : pU^2 - V^2 - \beta_0 P_0 Q_0 T^2 = 0$$

with

$$\begin{aligned} P_0 &= p\alpha_0^2 + 2\beta_0^2 - 2p\gamma_0^2, \\ Q_0 &= 4bdp\gamma_0 - 4b^2\beta_0 - d^2p\beta_0. \end{aligned}$$

Let $A, B \in \mathbb{Q}$ be rational numbers, and assume that the following are true:

- (C1) $A, B \in \mathbb{Z}_2$ and $B^2 - pA^2 \in \mathbb{Z}_2^\times$.
- (C2) $A \in \mathbb{Z}_p$ and $B \in \mathbb{Z}_p^\times$.
- (C3) $u := u_0 + AC \neq 0$ and $v := v_0 + BC \neq 0$, where

$$(23) \quad C := \frac{2pu_0A - 2v_0B - 4p^3\alpha_0\beta_0t_0^2Q_0}{B^2 - pA^2 + 4p^5\beta_0t_0^2Q_0}.$$

Define

$$\alpha := \alpha_0 + 2p^2C, \quad \beta := \beta_0, \quad \gamma := \gamma_0.$$

Then the triple $(\alpha, \beta, \gamma) \in \mathbb{Q}^3$ satisfies (A3)–(A5) and (B1).

Remark 5.2. In order to use Theorem 4.1 to show the existence of algebraic families of hyperelliptic curves satisfying CHP and NZC, one of the crucial steps is to describe a parametrization of triples (α, β, γ) such that the conics associated to these triples in (A3) has a nontrivial rational point. Assuming the existence of one triple $(\alpha_0, \beta_0, \gamma_0)$ satisfying (A3)–(A5) and (B1), Lemma 5.1 shows how to construct families of triples (α, β, γ) satisfying the same conditions as the triple $(\alpha_0, \beta_0, \gamma_0)$.

Proof. We first prove that (α, β, γ) satisfies (A4). Since $A \in \mathbb{Z}_p$, $B \in \mathbb{Z}_p^\times$ and the triple $(\alpha_0, \beta_0, \gamma_0)$ satisfies (A4), it follows that $B^2 - pA^2 + 4p^5\beta_0t_0^2Q_0 \in \mathbb{Z}_p^\times$. Hence by (23) and (C2), we see that $C \in \mathbb{Z}_p$. Thus $\alpha = \alpha_0 + 2p^2C \in \mathbb{Z}_p$. Hence it follows that

$$\alpha \equiv \alpha_0 \not\equiv 0 \pmod{p},$$

which proves that $\alpha \in \mathbb{Z}_p^\times$. By assumption, one knows that the triple $(\alpha_0, \beta_0, \gamma_0)$ satisfies (A4). Since $\beta = \beta_0$ and $\gamma = \gamma_0$, we deduce that $\beta, \gamma \in \mathbb{Z}_2^\times$, $\beta \in \mathbb{Z}_p$ and $\gamma, d \in \mathbb{Z}_p^\times$. Hence it remains to prove that $\alpha \in \mathbb{Z}_2^\times$. By assumptions and (C1), we know that $Q_0 \in \mathbb{Z}_2$ and $B^2 - pA^2 \in \mathbb{Z}_2^\times$. Hence it follows that

$$B^2 - pA^2 + 4p^5\beta_0t_0^2Q_0 \equiv B^2 - pA^2 \not\equiv 0 \pmod{2}.$$

Thus $B^2 - pA^2 + 4p^5\beta_0t_0^2Q_0 \in \mathbb{Z}_2^\times$, and hence we deduce that $C \in \mathbb{Z}_2$. Thus,

$$\alpha = \alpha_0 + 2p^2C \equiv \alpha_0 \not\equiv 0 \pmod{2}.$$

Therefore $\alpha \in \mathbb{Z}_2^\times$, and hence (α, β, γ) satisfies (A4).

Now we prove that (α, β, γ) satisfies (A3). By what we have proved above, we know that $\alpha, \beta, \gamma \in \mathbb{Z}_2^\times$. This implies that $\alpha, \beta, \gamma \neq 0$. Let P and Q be the rational numbers defined by (11) and (12), respectively. One knows that $Q = Q_0 \neq 0$. Since $\alpha, \beta, \gamma \in \mathbb{Z}_2^\times$, it follows that $P \in \mathbb{Z}_2$. Hence we deduce that

$$P \equiv p\alpha^2 \not\equiv 0 \pmod{2},$$

which proves that $P \in \mathbb{Z}_2^\times$. Note that $P \neq 0$ since $P \in \mathbb{Z}_2^\times$.

Let $\mathcal{Q}_1 \subset \mathbb{P}_{\mathbb{Q}}^2$ be the conic defined by

$$\mathcal{Q}_1 : pU^2 - V^2 - \beta PQT^2 = 0.$$

We prove that the point $\mathbf{P} := (u, v, t) \in \mathbb{Q}^3$ belongs to $\mathcal{Q}_1(\mathbb{Q})$, where u and v are defined in (C3) and $t := t_0$. Indeed, since $\beta = \beta_0$, $\gamma = \gamma_0$ and $Q = Q_0$, we deduce from (11) that

$$\begin{aligned} -\beta PQT^2 &= -\beta_0t_0^2Q_0(p(\alpha_0 + 2p^2C)^2 + 2\beta_0^2 - 2p\gamma_0^2) \\ &= -(4p^5\beta_0t_0^2Q_0)C^2 - (4p^3\alpha_0\beta_0t_0^2Q_0)C - (\beta_0P_0Q_0)t_0^2. \end{aligned}$$

Hence

$$\begin{aligned} pu^2 - v^2 - \beta P Q t^2 &= p(u_0 + AC)^2 - (v_0 + BC)^2 - (4p^5 \beta_0 t_0^2 Q_0) C^2 \\ &\quad - (4p^3 \alpha_0 \beta_0 t_0^2 Q_0) C - (\beta_0 P_0 Q_0) t_0^2 \\ &= (pA^2 - B^2 - 4p^5 \beta_0 t_0^2 Q_0) C^2 \\ &\quad + (2pu_0 A - 2v_0 B - 4p^3 \alpha_0 \beta_0 t_0^2 Q_0) C + (pu_0^2 - v_0^2 - \beta_0 P_0 Q_0 t_0^2). \end{aligned}$$

Since (u_0, v_0, t_0) belongs to $\mathcal{Q}_1^{(\alpha_0, \beta_0, \gamma_0)}(\mathbb{Q})$, we see that

$$pu_0^2 - v_0^2 - \beta_0 P_0 Q_0 t_0^2 = 0.$$

Hence it follows from (23) that

$$\begin{aligned} pu^2 - v^2 - \beta P Q t^2 \\ = (pA^2 - B^2 - 4p^5 \beta_0 t_0^2 Q_0) C^2 + (2pu_0 A - 2v_0 B - 4p^3 \alpha_0 \beta_0 t_0^2 Q_0) C = 0. \end{aligned}$$

Thus $P \in \mathcal{Q}_1(\mathbb{Q})$. Since \mathcal{Q}_1 is a nonsingular conic in $\mathbb{P}_{\mathbb{Q}}^2$, $\mathcal{Q}_1(\mathbb{Q}) \neq \emptyset$ and $uvt \neq 0$, it follows that (α, β, γ) satisfies (A3).

We now prove that (α, β, γ) satisfies (A5). Indeed, we have shown that (α, β, γ) satisfies (A3), (A4). This implies that $\alpha, \beta, \gamma \in \mathbb{Z}_p$. By Lemma 4.3, we know that there is a rational number $\bar{\beta} \in \mathbb{Q}$ such that $\beta = p\bar{\beta}$ and $\bar{\beta} \in \mathbb{Z}_p$. Similarly, since $(\alpha_0, \beta_0, \gamma_0)$ satisfies (A3) and (A4), there is a rational number $\bar{\beta}_0$ such that $\beta_0 = p\bar{\beta}_0$ and $\bar{\beta}_0 \in \mathbb{Z}_p$. Since $\beta = \beta_0$, we deduce that $\bar{\beta} = \bar{\beta}_0$.

Let P_1 and Q_1 be the rational numbers defined in Remark 4.4 and let $P_1^{(0)}$ and $Q_1^{(0)}$ be the rational numbers defined by the same equations as P_1, Q_1 with $(\alpha_0, \bar{\beta}_0, \gamma_0)$ in the role of $(\alpha, \bar{\beta}, \gamma)$. By assumption, one knows that the triple $(\alpha_0, \beta_0, \gamma_0)$ satisfies (A5), that is,

$$\gamma_0 Q_1^{(0)} + bdP_1^{(0)} \equiv 0 \pmod{p^2}.$$

We will prove that

$$\gamma Q_1 + bdP_1 \equiv 0 \pmod{p^2}.$$

Indeed, one can check that

$$P_1 = \alpha^2 + 2p\bar{\beta}^2 - 2\gamma^2 = 4p^4 C^2 + 4p^2 \alpha_0 C + P_1^{(0)}$$

and $Q_1 = Q_1^{(0)}$. Since $\alpha, \bar{\beta}, \gamma$ are in \mathbb{Z}_p , we deduce that $P_1 \in \mathbb{Z}_p$. Recall that $C \in \mathbb{Z}_p$. Hence

$$P_1 = 4p^4 C^2 + 4p^2 \alpha_0 C + P_1^{(0)} \equiv P_1^{(0)} \pmod{p^2},$$

and thus we deduce that

$$\gamma Q_1 + bdP_1 \equiv \gamma_0 Q_1^{(0)} + bdP_1^{(0)} \equiv 0 \pmod{p^2}.$$

Therefore (α, β, γ) satisfies (A5).

Finally, since $(\alpha_0, \beta_0, \gamma_0)$ satisfies (B1), we see that

$$bd - \bar{\beta}\gamma = bd - \bar{\beta}_0\gamma_0 \equiv 0 \pmod{4}.$$

Thus (α, β, γ) satisfies (B1), which proves our contention. \square

Lemma 5.3. *Let (p, b, d) be a triple of integers satisfying (A1) and (A2). Assume that there is a triple $(\alpha_0, \beta_0, \gamma_0) \in \mathbb{Q}^3$ satisfying (A3)–(A5) and (B1). Let $(u_0, v_0, t_0) \in \mathbb{Z}^3$ be a point on the conic $\mathcal{Q}_1^{(\alpha_0, \beta_0, \gamma_0)}$ such that $u_0v_0t_0 \neq 0$ and $\gcd(u_0, v_0, t_0) = 1$, where P_0, Q_0 and the conic $\mathcal{Q}_1^{(\alpha_0, \beta_0, \gamma_0)}$ are defined as in Lemma 5.1. Let \mathbf{I} be the set defined by*

$$\mathbf{I} := \{(A, B) \in \mathbb{Q}^2 : (A, B) \text{ satisfies (C1)–(C3) in Lemma 5.1}\}.$$

Then \mathbf{I} is of infinite cardinality.

Proof. Let B_0 be an integer such that $\gcd(B_0, 2p) = 1$. For each $x \in \mathbb{Z}$, define $B = 2px + B_0$. We see that $B \in \mathbb{Z}_2^\times$ and $B \in \mathbb{Z}_p^\times$. The latter implies that $B \neq 0$. Let $A = 0$, and let C be the rational number defined by (23). Define

$$u := u_0 + AC = u_0,$$

$$v := v_0 + BC.$$

By assumption, we know that $u = u_0 \neq 0$. Assume that $v = 0$. Since $B \neq 0$, it follows from (23) and the definition of v that

$$C = -\frac{v_0}{B} = \frac{-2v_0B - 4p^3\alpha_0\beta_0t_0^2Q_0}{B^2 + 4p^5\beta_0t_0^2Q_0}.$$

Hence we deduce that B is a zero of the quadratic polynomial $\mathcal{B}(T) \in \mathbb{Q}[T]$, where $\mathcal{B}(T)$ is defined by

$$(24) \quad \mathcal{B}(T) := v_0T^2 + (4p^3\alpha_0\beta_0t_0^2Q_0)T - 4p^5\beta_0v_0t_0^2Q_0.$$

Hence, upon letting T_1 and T_2 be the zeros of $\mathcal{B}(T)$, we deduce that $(0, B)$ satisfies (C3) if and only if $B \neq T_1$ and $B \neq T_2$. The latter holds if and only if $x \neq (T_1 - B_0)/(2p)$ and $x \neq (T_2 - B_0)/(2p)$. This implies that if $T_1, T_2 \notin \mathbb{Z}$, then $(0, B)$ automatically satisfies (C3) for any integer $x \in \mathbb{Z}$. Furthermore we see that $B^2 - pA^2 = B^2 \in \mathbb{Z}_2^\times$. Hence $(0, B)$ satisfies (C1) and (C2). Thus \mathbf{J} is a subset of \mathbf{I} , where \mathbf{J} is defined by

$$\mathbf{J} := \left\{ (0, B) : x \in \mathbb{Z}, x \neq \frac{T_1 - B_0}{2p} \text{ and } x \neq \frac{T_2 - B_0}{2p} \right\}.$$

Since \mathbf{J} is of infinite cardinality, so is \mathbf{I} . Hence our contention follows. \square

Using Lemmas 5.1 and 5.3, we prove the main result in this section.

Lemma 5.4. *There are infinitely many sextuples $(p, b, d, \alpha, \beta, \gamma)$ satisfying (A1)–(A5) and (B1).*

Proof. Assume that there is a sextuple $(p, b, d, \alpha_0, \beta_0, \gamma_0)$ satisfying (A1)–(A5) and (B1). Let $(u_0, v_0, t_0) \in \mathbb{Z}^3$ be a point on the conic $Q_1^{(\alpha_0, \beta_0, \gamma_0)}$ such that $u_0 v_0 t_0 \neq 0$ and $\gcd(u_0, v_0, t_0) = 1$, where P_0, Q_0 and the conic $Q_1^{(\alpha_0, \beta_0, \gamma_0)}$ are defined as in Lemma 5.1. Let J be the set defined in the proof of Lemma 5.3. We construct an infinite sequence $(0, B_n)_{n \in \mathbb{Z}_{\geq 0}}$ of elements of J as follows.

Let $(0, B_1)$ be an arbitrary element of J , and assume that the elements $(0, B_i)$ of J with $1 \leq i \leq n$ are already constructed. Since J is infinite, we can choose an element $(0, B_{n+1})$ of J such that $B_{n+1} \neq B_i$ for $1 \leq i \leq n$ and B_{n+1} is not a zero of any of the polynomials $H_i(T)$ for $1 \leq i \leq n$, where for each $1 \leq i \leq n$,

$$(25) \quad H_i(T) = (v_0 B_i + 2p^3 \alpha_0 \beta_0 t_0^2 Q_0)T + 2p^3 \alpha_0 \beta_0 t_0^2 Q_0 B_i - 4p^5 \beta_0 v_0 t_0^2 Q_0 \in \mathbb{Q}[T].$$

Indeed, we see that $2p^3 \alpha_0 \beta_0 t_0^2 Q_0 B_i - 4p^5 \beta_0 v_0 t_0^2 Q_0 \neq 0$ for every $1 \leq i \leq n$; otherwise, there is an integer $1 \leq i \leq n$ such that

$$\alpha_0 B_i = 2p^2 v_0.$$

Hence $\alpha_0 B_i \notin \mathbb{Z}_p^\times$, which is a contradiction since α_0 and B_i are in \mathbb{Z}_p^\times . Hence $H_i(T)$ is nonzero and of degree at most 1 for each $1 \leq i \leq n$. Thus $H_i(T)$ has at most one zero in \mathbb{Z} for each $1 \leq i \leq n$; hence, excluding these n zeros (if existing) and the integers B_i for $1 \leq i \leq n$ out of the infinite set J , one can choose an element $(0, B_{n+1})$ as desired. Therefore we have inductively constructed an infinite sequence $\{(0, B_n)\}_{n \geq 1}$ of elements of J . We contend that for any two distinct members $(0, B_m)$ and $(0, B_n)$ of the sequence with $m < n$, the triples $(\alpha_m, \beta_0, \gamma_0)$ and $(\alpha_n, \beta_0, \gamma_0)$ are distinct, that is, $\alpha_m \neq \alpha_n$, where

$$\alpha_m := \alpha_0 + 2p^2 C_{(m)}, \quad \alpha_n := \alpha_0 + 2p^2 C_{(n)},$$

and $C_{(m)}, C_{(n)}$ are defined as in (23) with $(0, B_m)$ and $(0, B_n)$ in the role of (A, B) , respectively. Assume the contrary, that is, $\alpha_m = \alpha_n$. It follows that

$$\frac{-2v_0 B_m - 4p^3 \alpha_0 \beta_0 t_0^2 Q_0}{B_m^2 + 4p^5 \beta_0 t_0^2 Q_0} = C_{(m)} = C_{(n)} = \frac{-2v_0 B_n - 4p^3 \alpha_0 \beta_0 t_0^2 Q_0}{B_n^2 + 4p^5 \beta_0 t_0^2 Q_0}.$$

Hence we deduce that

$$2(B_n - B_m)((v_0 B_m + 2p^3 \alpha_0 \beta_0 t_0^2 Q_0)B_n + 2p^3 \alpha_0 \beta_0 t_0^2 Q_0 B_m - 4p^5 \beta_0 v_0 t_0^2 Q_0) = 0.$$

Since $B_n \neq B_m$, we deduce that B_n is a zero of $H_m(T)$, where $H_m(T)$ is defined by (25), which is a contradiction to the choice of B_n . Thus we have shown that there are infinitely many sextuples $(p, b, d, \alpha, \beta, \gamma)$ satisfying (A1)–(A5) and (B1) provided that there exists one sextuple $(p, b, d, \alpha_0, \beta_0, \gamma_0)$ satisfying (A1)–(A5) and (B1). On the other hand, in the proof of Theorem 6.8(i) below, we will show

that the sextuple $(p, b, d, \alpha_0, \beta_0, \gamma_0) = (29, 1, 3, 7, 261, 15)$ satisfies (A1)–(A5) and (B1), and hence our contention follows. \square

6. Algebraic families of hyperelliptic curves violating the Hasse principle

Let n be an integer such that $n > 5$ and $n \not\equiv 0 \pmod{4}$. In this section, using the results in the last section, we will show how to construct algebraic families of hyperelliptic curves of genus n satisfying CHP and NZC. We begin by proving:

Lemma 6.1. *Let S be a finite set of primes, and let $G(t) \in \mathbb{Q}(t)$ be a nonzero rational function. Let Z be the finite set of rational zeros and poles of $G(t)$, that is, Z consists of the rational numbers $z \in \mathbb{Q}$ for which $G(z)$ is either zero or infinity. For any $z \in Z$, let a_z, b_z be integers such that $b_z \neq 0$, $\gcd(a_z, b_z) = 1$ and $z = a_z/b_z$. Assume that the following is true:*

(D) *Let z be any element in Z such that $a_z \neq 0$. Then $a_z \not\equiv 0 \pmod{l}$ for each prime $l \in S$.*

Then there is a rational function $F(t) \in \mathbb{Q}(t)$ such that the following are true:

- (1) $F(t_*) \in \mathbb{Z}_l^\times$ for each prime $l \in S$ and each $t_* \in \mathbb{Q}$; and
- (2) $G(F(t_*))$ is defined (that is, not infinity) and nonzero for each $t_* \in \mathbb{Q}$.

Proof. We consider two cases:

Case 1. Z is nonempty.

By the Chinese remainder theorem, there exists an integer ϵ such that $\epsilon \equiv 2 \pmod{4}$ and ϵ is a quadratic nonresidue in \mathbb{F}_l^\times for each odd prime $l \in S$ with $l \neq 2$. Let p_0 be an odd prime such that:

- (i) $p_0 \notin S$;
- (ii) $b_z \not\equiv 0 \pmod{p_0}$ for every $z \in Z$; and
- (iii) for any element z in Z such that $a_z \neq 0$, we have $a_z \not\equiv 0 \pmod{p_0}$.

For each $z \in Z$, we define

$$(26) \quad D_z := p_0 b_z \operatorname{sign}(a_z) \prod_{w \in Z \setminus \{z\}} \max(1, |a_w|) \in \mathbb{Z},$$

where $\operatorname{sign}(\cdot)$ denotes the usual sign function of \mathbb{R} , that is, $\operatorname{sign}(x) = 1$ if $x \geq 0$, and $\operatorname{sign}(x) = -1$ if $x < 0$. We see that $|D_z| \geq p_0 \geq 3$ for each $z \in Z$. This implies that $|D_z - 1| \geq 1$ for every $z \in Z$. We will prove that the rational function $F(t) \in \mathbb{Q}(t)$, defined by

$$(27) \quad F(t) := \left(p_0 \prod_{z \in Z} \max(1, |a_z|) \right) \left(1 + \frac{4 \prod_{l \in S, l \neq 2} l \prod_{z \in Z} (D_z - 1)}{t^2 - p_0^2 \epsilon} \right),$$

satisfies (1) and (2) in Lemma 6.1. Indeed, take any rational number t_* , and write $t_* = t_1/t_2$, where $t_1, t_2 \in \mathbb{Z}$, $t_2 \neq 0$ and $\gcd(t_1, t_2) = 1$. For each prime l , denote by v_l the l -adic valuation of \mathbb{Q}_l . For each prime $l \in \mathcal{S}$ with $l \neq 2$, one knows that

$$v_l\left(\frac{1}{t_*^2 - p_0^2\epsilon}\right) = v_l(t_2^2) - v_l(t_1^2 - t_2^2 p_0^2\epsilon).$$

Assume that $t_1^2 - t_2^2 p_0^2\epsilon \equiv 0 \pmod{l}$. Since $p_0 \neq l$ and ϵ is a quadratic nonresidue in \mathbb{F}_l^\times , it follows that $t_1 \equiv t_2 \equiv 0 \pmod{l}$, which is a contradiction. Hence we deduce that $v_l(t_1^2 - t_2^2 p_0^2\epsilon) = 0$. Thus we see that

$$v_l\left(\frac{1}{t_*^2 - p_0^2\epsilon}\right) = v_l(t_2^2) \geq 0.$$

Therefore $\frac{1}{t_*^2 - p_0^2\epsilon} \in \mathbb{Z}_l$, and hence we deduce that

$$1 + \frac{4 \prod_{l \in \mathcal{S}, l \neq 2} l \prod_{z \in \mathcal{Z}} (D_z - 1)}{t_*^2 - p_0^2\epsilon} \in 1 + l\mathbb{Z}_l.$$

By assumption (D) and the choice of p_0 , one knows that $p_0 \prod_{z \in \mathcal{Z}} \max(1, |a_z|) \in \mathbb{Z}_l^\times$. Hence it follows that for each prime $l \in \mathcal{S}$ with $l \neq 2$, $\mathbf{F}(t_*) \in \mathbb{Z}_l^\times$ for every $t_* \in \mathbb{Q}$. Thus we have shown that if $2 \notin \mathcal{S}$, then $\mathbf{F}(t)$ satisfies (1) in Lemma 6.1. Hence it remains to show that if $2 \in \mathcal{S}$, then $\mathbf{F}(t_*) \in \mathbb{Z}_2^\times$ for every $t_* \in \mathbb{Q}$.

Let us first assume that t_1 is even. Hence t_2 is odd, and then one sees that $t_1^2 - t_2^2 p_0^2\epsilon \equiv 2 \pmod{4}$. Thus $v_2(t_1^2 - t_2^2 p_0^2\epsilon) = 1$. Hence it follows that

$$v_2\left(\frac{2}{t_*^2 - p_0^2\epsilon}\right) = 1 + v_2(t_2^2) - v_2(t_1^2 - t_2^2 p_0^2\epsilon) = 0,$$

which implies that $2/(t_*^2 - p_0^2\epsilon) \in \mathbb{Z}_2$ for all $t_* \in \mathbb{Q}$.

Now assume that t_1 is odd. Since ϵ is even, one sees that $t_1^2 - t_2^2 p_0^2\epsilon$ is odd. Hence it follows that

$$v_2\left(\frac{2}{t_*^2 - p_0^2\epsilon}\right) = 1 + v_2(t_2^2) - v_2(t_1^2 - t_2^2 p_0^2\epsilon) = 1 + v_2(t_2^2) \geq 1.$$

Thus we have shown that $2/(t_*^2 - p_0^2\epsilon) \in \mathbb{Z}_2$ for all $t_* \in \mathbb{Q}$. By the definition of $\mathbf{F}(t)$ and assumption (D), we deduce that $\mathbf{F}(t_*) \in \mathbb{Z}_2^\times$ for all $t_* \in \mathbb{Q}$. Hence the rational function $\mathbf{F}(t)$ satisfies Lemma 6.1(1).

Now we prove that $\mathbf{F}(t)$ satisfies Lemma 6.1(2). Since z is a rational zero or pole of $\mathbf{G}(t)$ for each $z \in \mathcal{Z}$, we see that if $\mathbf{F}(t_*) \neq z$ for every $z \in \mathcal{Z}$ and all $t_* \in \mathbb{Q}$, then $\mathbf{G}(\mathbf{F}(t_*))$ is defined, namely, not infinity, and nonzero for all $t_* \in \mathbb{Q}$.

Assume that there is a rational number $t_* \in \mathbb{Q}$ such that $\mathbf{F}(t_*) = z$ for some $z = a_z/b_z \in \mathcal{Z}$. We consider two subcases:

Subcase 1. $a_z \neq 0$.

We see that $\max(1, |a_z|) = |a_z|$. Hence it follows that

$$D_z \left(1 + \frac{4 \prod_{l \in S, l \neq 2} l \prod_{w \in Z} (D_w - 1)}{t_*^2 - p_0^2 \epsilon} \right) = 1.$$

Upon multiplying both sides by $t_*^2 - p_0^2 \epsilon$ and simplifying, we deduce that

$$t_*^2 = p_0^2 \epsilon - 4D_z \prod_{l \in S, l \neq 2} l \prod_{w \in Z \setminus \{z\}} (D_w - 1).$$

Hence it follows from (26) that

$$t_*^2 = p_0 \left(p_0 \epsilon - 4b_z \operatorname{sign}(a_z) \prod_{w \in Z \setminus \{z\}} \max(1, |a_w|) \prod_{l \in S, l \neq 2} l \prod_{w \in Z \setminus \{z\}} (D_w - 1) \right).$$

This implies that $t_* \in \mathbb{Z}$ and $t_* \equiv 0 \pmod{p_0}$. Hence $v_{p_0}(t_*^2) = 2v_{p_0}(t_*) \geq 2$. Thus,

$$p_0 \epsilon - 4b_z \operatorname{sign}(a_z) \prod_{w \in Z \setminus \{z\}} \max(1, |a_w|) \prod_{l \in S, l \neq 2} l \prod_{w \in Z \setminus \{z\}} (D_w - 1) \equiv 0 \pmod{p_0}.$$

Hence

$$4b_z \operatorname{sign}(a_z) \prod_{w \in Z \setminus \{z\}} \max(1, |a_w|) \prod_{l \in S, l \neq 2} l \prod_{w \in Z \setminus \{z\}} (D_w - 1) \equiv 0 \pmod{p_0}.$$

By (26), one knows that $D_w \equiv 0 \pmod{p_0}$ for every $w \in Z$. Hence

$$\prod_{w \in Z \setminus \{z\}} (D_w - 1) \equiv (-1)^{m-1} \pmod{p_0}.$$

Thus we deduce that

$$(-1)^{m-1} 4b_z \operatorname{sign}(a_z) \prod_{w \in Z \setminus \{z\}} \max(1, |a_w|) \prod_{l \in S, l \neq 2} l \equiv 0 \pmod{p_0},$$

which is a contradiction to the choice of p_0 . Therefore $\mathbf{F}(t_*) \neq z$ for all $t_* \in \mathbb{Q}$.

Subcase 2. $a_z = 0$.

We see that $\mathbf{F}(t_*) = a_z/b_z = 0$. Hence we deduce from the definition of $\mathbf{F}(t_*)$ that

$$t_*^2 = p_0^2 \epsilon - 4 \prod_{l \in S, l \neq 2} l \prod_{w \in Z} (D_w - 1).$$

This implies that $t_* \in \mathbb{Z}$. Hence we deduce that

$$t_*^2 = p_0^2 \epsilon \pmod{l}$$

for each prime $l \in S$ with $l \neq 2$. Since ϵ is a quadratic nonresidue in \mathbb{F}_l^\times , it follows that $t_* \equiv p_0 \equiv 0 \pmod{l}$, which is a contradiction to the choice of p_0 . Thus, in any event, $\mathbf{F}(t_*) \neq z$ for all $t_* \in \mathbb{Q}$. Therefore $\mathbf{F}(t_*)$ satisfies Lemma 6.1(2).

Case 2. $\mathbf{Z} = \emptyset$.

In this case, let ϵ be the same as in Case 1, and let p_0 be an odd prime such that $p_0 \notin \mathbf{S}$. Let $F(t) \in \mathbb{Q}(t)$ be the rational function defined by

$$(28) \quad F(t) := 1 + \frac{4 \prod_{l \in \mathbf{S}, l \neq 2} l}{t^2 - p_0^2 \epsilon}.$$

Using the same arguments as in Case 1, one can show that $F(t)$ satisfies (1) and (2) in Lemma 6.1. □

Lemma 6.2. *Let $D(t) \in \mathbb{Q}(t)$ be a nonzero rational function of the form*

$$D(t) = \frac{at^4 + bt^2 + c}{dt^4 + et^2 + f},$$

where a, b, c, d, e, f are integers. Let q be an odd prime. Assume that there exists an integer t_0 such that

$$\begin{aligned} at_0^4 + bt_0^2 + c &\equiv 0 \pmod{q}, \\ at_0^4 + bt_0^2 + c &\not\equiv 0 \pmod{q^2}, \\ dt_0^4 + et_0^2 + f &\not\equiv 0 \pmod{q}. \end{aligned}$$

Then there exists a rational function $\Gamma(t) \in \mathbb{Q}(t)$ such that for all $t_* \in \mathbb{Q}$, $D(\Gamma(t_*))$ belongs to $q\mathbb{Z}_q$, but does not belong to $q^2\mathbb{Z}_q$.

Proof. Let ϵ be an integer such that ϵ is a quadratic nonresidue in \mathbb{F}_q^\times . Let q_0 be an odd prime such that $q_0 \neq q$. We will show that the rational function $\Gamma(t) \in \mathbb{Q}(t)$, defined by

$$(29) \quad \Gamma(t) = t_0 + \frac{q^2}{t^2 - q_0^2 \epsilon},$$

satisfies the assertions in Lemma 6.2.

Since ϵ is not a square in \mathbb{F}_q^\times , it follows that $t_*^2 - q_0^2 \epsilon$ is nonzero for each $t_* \in \mathbb{Q}$, and hence $\Gamma(t_*)$ is well defined, namely, not infinity for all $t_* \in \mathbb{Q}$.

We now prove that $\Gamma(t_*)$ belongs to $t_0 + q^2\mathbb{Z}_q$ for all $t_* \in \mathbb{Q}$. Indeed, take any rational number t_* , and write $t_* = t_1/t_2$, where t_1, t_2 are integers such that $t_2 \neq 0$ and $\gcd(t_1, t_2) = 1$. We see that

$$v_q\left(\frac{1}{t_*^2 - q_0^2 \epsilon}\right) = v_q\left(\frac{t_2^2}{t_1^2 - q_0^2 \epsilon t_2^2}\right) = v_q(t_2^2) - v_q(t_1^2 - q_0^2 \epsilon t_2^2).$$

If $t_2 \equiv 0 \pmod{q}$, then it follows that $t_1 \not\equiv 0 \pmod{q}$. Hence we deduce that

$$v_q(t_1^2 - q_0^2 \epsilon t_2^2) = \min(v_q(t_1^2), v_q(q_0^2 \epsilon t_2^2)) = \min(0, v_q(t_2^2)) = 0,$$

and thus

$$v_q\left(\frac{1}{t_*^2 - q_0^2\epsilon}\right) = v_q(t_2^2) - v_q(t_1^2 - q_0^2\epsilon t_2^2) = 2v_q(t_2) \geq 2.$$

Therefore $1/(t_*^2 - q_0^2\epsilon)$ belongs to \mathbb{Z}_q , and hence it follows from (29) that $\Gamma(t_*)$ belongs to $t_0 + q^2\mathbb{Z}_q$.

If $t_2 \not\equiv 0 \pmod{q}$, then $v_q(t_2^2) = 0$. We contend that $t_1^2 - q_0^2\epsilon t_2^2 \not\equiv 0 \pmod{q}$. Assume the contrary, that is, $t_1^2 - q_0^2\epsilon t_2^2 \equiv 0 \pmod{q}$. Since $t_2 \not\equiv 0 \pmod{q}$ and $q_0 \neq q$, we deduce that

$$\epsilon \equiv \left(\frac{t_1}{q_0 t_2}\right)^2 \pmod{q},$$

which contradicts the choice of ϵ . This establishes that $t_1^2 - q_0^2\epsilon t_2^2 \not\equiv 0 \pmod{q}$, and thus

$$v_q\left(\frac{1}{t_*^2 - q_0^2\epsilon}\right) = v_q(t_2^2) - v_q(t_1^2 - q_0^2\epsilon t_2^2) = 0.$$

Therefore $1/(t_*^2 - q_0^2\epsilon)$ belongs to \mathbb{Z}_q^\times , and hence it follows from (29) that $\Gamma(t_*)$ belongs to $t_0 + q^2\mathbb{Z}_q$.

Since $\Gamma(t_*)$ belongs to $t_0 + q^2\mathbb{Z}_q$, we see that

$$\begin{aligned} a(\Gamma(t_*))^4 + b(\Gamma(t_*))^2 + c &\equiv at_0^4 + bt_0^2 + c \equiv 0 \pmod{q}, \\ a(\Gamma(t_*))^4 + b(\Gamma(t_*))^2 + c &\equiv at_0^4 + bt_0^2 + c \not\equiv 0 \pmod{q^2}, \\ d(\Gamma(t_*))^4 + e(\Gamma(t_*))^2 + f &\equiv dt_0^4 + et_0^2 + f \not\equiv 0 \pmod{q}. \end{aligned}$$

The last congruence shows that

$$\frac{1}{c(\Gamma(t_*))^4 + d(\Gamma(t_*))^2 + e}$$

belongs to \mathbb{Z}_q^\times , and hence we deduce that for every $t_* \in \mathbb{Q}$,

$$D(\Gamma(t_*)) = \frac{a(\Gamma(t_*))^4 + b(\Gamma(t_*))^2 + c}{d(\Gamma(t_*))^4 + e(\Gamma(t_*))^2 + f}$$

belongs to $q\mathbb{Z}_q$, but does not belong to $q^2\mathbb{Z}_q$. Thus our contention follows. \square

The next two examples will be used in proving the main theorem in this section.

Example 6.3. Let $D_1(T) \in \mathbb{Q}(T)$ be the rational function defined by

$$(30) \quad D_1(T) := \frac{45588894173298T^4 - 1641200890885920T^2 + 14770814323798008}{-5477180725633679T^4 + 197178506122812676T^2 - 1774606555105302716},$$

and define

$$(31) \quad \mathbf{D}_1^*(T) := 7 + 1682\mathbf{D}_1(T) \\ = \frac{-38340254920051483T^4 + 1380250355610428708T^2 - 12422263806891130444}{5477180725633679T^4 - 197178506122812676T^2 + 1774606555105302716}.$$

Let $T_0 = 0$, and let $q = 31$. Since

$$12422263806891130444 = 2^2 \cdot 7^3 \cdot 31 \cdot 433 \cdot 3299 \cdot 10589 \cdot 19309,$$

it follows that

$$v_q(-12422263806891130444) = v_{31}(-12422263806891130444) = 1,$$

and we deduce that for $T = T_0 = 0$ the numerator of the fraction in (31) is divisible by q , but not by q^2 . Since

$$1774606555105302716 = 2^2 \cdot 7^2 \cdot 47 \cdot 192640746320593,$$

we see that for $T = T_0 = 0$ the denominator in (31) is not divisible by q .

Let $\epsilon = 3$, and let $q_0 = 5$. Following the proof of Lemma 6.2, we define the rational function $\Gamma_1(T) \in \mathbb{Q}(T)$ by (29), that is,

$$(32) \quad \Gamma_1(T) := T_0 + \frac{q^2}{T^2 - q_0^2\epsilon} = \frac{961}{T^2 - 75}.$$

Applying Lemma 6.2 with $\mathbf{D}_1^*(T)$ in the role of $\mathbf{D}(t)$, we deduce that for all $T_* \in \mathbb{Q}$, $\mathbf{D}_1^*(\Gamma_1(T_*))$ belongs to $31\mathbb{Z}_{31}$, but does not belong to $31^2\mathbb{Z}_{31}$, where

$$(33) \quad \mathbf{D}_1^*(\Gamma_1(T)) = \frac{\Sigma_{1,1}(T)}{\Sigma_{1,2}(T)} \in \mathbb{Q}(T)$$

with

$$(34) \quad \Sigma_{1,1}(T) = -12422263806891130444T^8 + 3726679142067339133200T^6 \\ + 855438785181123078355868T^4 - 170240958125426027001880200T^2 \\ - 25922975674046723162225380003$$

and

$$(35) \quad \Sigma_{1,2}(T) = 1774606555105302716T^8 - 532381966531590814800T^6 \\ - 122205519918242118687196T^4 + 24320125111216714469579400T^2 \\ + 3703283999134302153081910439.$$

Example 6.4. Let $\mathbf{D}_2(T) \in \mathbb{Q}(T)$ be the rational function defined by

$$(36) \quad \mathbf{D}_2(T) := \frac{-64380401708754T^4 + 2317693623118880T^2 - 20859235062503544}{407097080892401T^4 - 14655494912126204T^2 + 131899454209147204},$$

and define

$$(37) \quad \mathbf{D}_2^*(T) := 133 + 1682\mathbf{D}_2(T) \\ = \frac{-54143923915434895T^4 + 1949179850773171028T^2 - 17542605965314382876}{407097080892401T^4 - 14655494912126204T^2 + 131899454209147204}.$$

Let $T_0 = 0$, and let $q = 11$. Since

$$17542605965314382876 = 2^2 \cdot 7 \cdot 11 \cdot 56956512874397347,$$

it follows that for $T = T_0$ the numerator in (37) is divisible by 11, but not by 11^2 . Since

$$131899454209147204 \equiv 8 \not\equiv 0 \pmod{11},$$

for $T = T_0$ the denominator in (37) is not divisible by 11.

Let $\epsilon = 7$, and let $q_0 = 3$. Following the proof of Lemma 6.2, we define the rational function $\Gamma_2(T) \in \mathbb{Q}(T)$ by (29), that is,

$$(38) \quad \Gamma_2(T) := T_0 + \frac{q^2}{T^2 - q_0^2\epsilon} = \frac{121}{T^2 - 63}.$$

Applying Lemma 6.2 with $\mathbf{D}_2^*(T)$ in the role of $\mathbf{D}(t)$, we deduce that for all $T_* \in \mathbb{Q}$, $\mathbf{D}_2^*(\Gamma_2(T_*))$ belongs to $11\mathbb{Z}_{11}$, but does not belong to $11^2\mathbb{Z}_{11}$, where

$$(39) \quad \mathbf{D}_2^*(\Gamma_2(T)) = \frac{\Sigma_{2,1}(T)}{\Sigma_{2,2}(T)} \in \mathbb{Q}(T)$$

with

$$(40) \quad \Sigma_{2,1}(T) = -17542605965314382876T^8 + 4420736703259224484752T^6 \\ - 389221676262826716788116T^4 + 13950123258644442355341240T^2 \\ - 174687125980796870729105719$$

and

$$(41) \quad \Sigma_{2,2}(T) = 131899454209147204T^8 - 33238662460705095408T^6 \\ + 2926482501528191763292T^4 - 104888292579475114826088T^2 \\ + 1313439132893945928914009.$$

The next result is a mild generalization of Theorem 2.1 of [Dong Quan 2014]. The only difference between these two theorems is that in the latter, a, b, c, d, e are assumed to be integers, whereas here we only assume that a, b, c, d, e belong to \mathbb{Z}_p . Upon examining closely the proof of [loc. cit.], we see that it is sufficient to assume that a, b, c, d, e are in \mathbb{Z}_p , and hence Theorem 6.5 follows immediately from the proof of that result.

Theorem 6.5 (separability criterion [Dong Quan 2014]). *Let n, m, k be positive integers, and let a, b, c, d, e be rational numbers such that $a \neq 0$. Let p be an odd prime such that a, b, c, d, e belong to \mathbb{Z}_p and $a \equiv 0 \pmod{p}$. Let $F(x) \in \mathbb{Q}[x]$ be the polynomial defined by*

$$(42) \quad F(x) := ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e).$$

Define

$$n_1 := (m+k)(v_p(a) - v_p(bd)) + m + k - 1,$$

$$n_2 := (m+k)(v_p(a) - v_p(b)) + m - 1,$$

$$n_3 := (m+k)(v_p(a) - v_p(d)) + k - 1,$$

$$n_4 := (m+k)v_p(a) - 1,$$

$$n_5 := v_p(a) - v_p(bd) + m + k - 1.$$

Suppose that the following are true:

$$(S1) \quad n > m + k - 1 \text{ and } n > \max(n_1, n_2, n_3, n_4, n_5).$$

$$(S2) \quad ce \not\equiv 0 \pmod{p}, km \not\equiv 0 \pmod{p}, \text{ and } b^k e^m + (-1)^{m+k+1} c^k d^m \not\equiv 0 \pmod{p}.$$

Then F is separable, that is, it has exactly $2n + 2$ distinct roots in \mathbb{C} . \square

Using Theorem 6.5, we prove the following corollaries that are crucial in constructing algebraic families of curves violating the Hasse principle.

Corollary 6.6. *We maintain the same notation as in Example 6.3. Let $\mathbf{D}_1(T)$, $\mathbf{D}_1^*(T)$, $\Gamma_1(T) \in \mathbb{Q}(T)$ be the rational functions defined by (30), (31), (32), respectively. Let n be a positive integer such that $n > 5$. For each rational number $T_* \in \mathbb{Q}$, let $\mathcal{P}_{1,T_*}(x) \in \mathbb{Q}[x]$ be the polynomial of degree $2n + 2$ given by*

$$(43) \quad \mathcal{P}_{1,T_*}(x) := 118579927725(\mathbf{D}_1^*(\Gamma_1(T_*)))^2 x^{2n+2} \\ + (2(29(\mathbf{D}_1^*(\Gamma_1(T_*)))^2 + 123192)x^2 - 16689645) \\ \times (261(29(\mathbf{D}_1^*(\Gamma_1(T_*)))^2 + 123192)x^2 - 33379290),$$

where the composition rational function $\mathbf{D}_1^*(\Gamma_1(T))$ of $\mathbf{D}_1^*(T)$ and $\Gamma_1(T)$ is given by (33). Then for all $T_* \in \mathbb{Q}$, the polynomial $\mathcal{P}_{1,T_*}(x)$ is separable, that is, it has exactly $2n + 2$ distinct roots in \mathbb{C} .

Proof. Throughout the proof, we maintain the same notation as in Theorem 6.5. Take any rational number $T_* \in \mathbb{Q}$, and define

$$a := 118579927725(\mathbf{D}_1^*(\Gamma_1(T_*)))^2,$$

$$b := 2(29(\mathbf{D}_1^*(\Gamma_1(T_*)))^2 + 123192),$$

$$c := -16689645,$$

$$d := 261(29(\mathbf{D}_1^*(\Gamma_1(T_*)))^2 + 123192),$$

$$e := -33379290.$$

Let $p = 31$, and let $m = k = 1$. Since $118579927725 \equiv 27 \not\equiv 0 \pmod{31}$, $123192 \equiv 29 \not\equiv 0 \pmod{31}$, it follows from Example 6.3 that

$$\begin{aligned} v_p(a) &= v_{31}(118579927725(\mathbf{D}_1^*(\Gamma_1(T_*)))^2) = 2v_{31}(\mathbf{D}_1^*(\Gamma_1(T_*))) = 2, \\ v_p(b) &= v_{31}(2(29(\mathbf{D}_1^*(\Gamma_1(T_*)))^2 + 123192)) = v_{31}(123192) = 0, \\ v_p(d) &= v_{31}(261(29(\mathbf{D}_1^*(\Gamma_1(T_*)))^2 + 123192)) = v_{31}(123192) = 0. \end{aligned}$$

We see that

$$\begin{aligned} n_1 &:= (m+k)(v_p(a) - v_p(bd)) + m+k-1 = 2v_p(a) + 1 = 5, \\ n_2 &:= (m+k)(v_p(a) - v_p(b)) + m-1 = 2v_p(a) = 4, \\ n_3 &:= (m+k)(v_p(a) - v_p(d)) + k-1 = 2v_p(a) = 4, \\ n_4 &:= (m+k)v_p(a) - 1 = 2v_p(a) - 1 = 3, \\ n_5 &:= v_p(a) - v_p(bd) + m+k-1 = 2+1 = 3, \end{aligned}$$

and hence

$$\max(n_1, n_2, n_3, n_4, n_5) = 5.$$

By assumption, we know that

$$n > 5 = \max(n_1, n_2, n_3, n_4, n_5),$$

and hence condition (S1) is satisfied.

It is obvious that $km = 1 \not\equiv 0 \pmod{31}$ and

$$ce = (-16689645) \cdot (-33379290) \equiv 25 \not\equiv 0 \pmod{31}.$$

Furthermore, since $\mathbf{D}_1^*(\Gamma_1(T_*))$ belongs to $31\mathbb{Z}_{31}$, we deduce that

$$\begin{aligned} b^k e^m + (-1)^{m+k+1} c^k d^m &= be - cd \\ &= (2(29(\mathbf{D}_1^*(\Gamma_1(T_*)))^2 + 123192))(-33379290) \\ &\quad - (-16689645)(261(29(\mathbf{D}_1^*(\Gamma_1(T_*)))^2 + 123192)) \\ &\equiv 2 \cdot 123192 \cdot (-33379290) + 16689645 \cdot 261 \cdot 123192 \\ &\equiv 12 \not\equiv 0 \pmod{31}. \end{aligned}$$

Therefore condition (S2) is satisfied, and hence the polynomial $\mathcal{P}_{1, T_*}(x)$ is separable. Since T_* is an arbitrary rational number, our contention follows. \square

Corollary 6.7. *We maintain the same notation as in Example 6.4. Let $\mathbf{D}_2(T)$, $\mathbf{D}_2^*(T)$, $\Gamma_2(T) \in \mathbb{Q}(T)$ be the rational functions defined by (36), (37), (38), respectively. Let n be a positive integer such that $n > 5$. For each rational number $T_* \in \mathbb{Q}$,*

let $\mathcal{P}_{2,T_*}(x) \in \mathbb{Q}[x]$ be the polynomial of degree $2n + 2$ given by

$$(44) \quad \mathcal{P}_{2,T_*}(x) := 84898109(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 x^{2n+2} \\ + (2(29(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 - 40600)x^2 + 49619) \\ \times (261(29(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 - 40600)x^2 + 99238),$$

where the composition rational function $\mathbf{D}_2^*(\Gamma_2(T))$ of $\mathbf{D}_2^*(T)$ and $\Gamma_2(T)$ is given by (39). Then for all $T_* \in \mathbb{Q}$, the polynomial $\mathcal{P}_{2,T_*}(x)$ is separable, that is, it has exactly $2n + 2$ distinct roots in \mathbb{C} .

Proof. Throughout the proof, we maintain the same notation as in Theorem 6.5. Take any rational number $T_* \in \mathbb{Q}$, and define

$$a := 84898109(\mathbf{D}_2^*(\Gamma_2(T_*)))^2, \\ b := 2(29(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 - 40600), \\ c := 49619, \\ d := 261(29(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 - 40600), \\ e := 99238.$$

Let $p = 11$, and let $m = k = 1$. Since $84898109 \equiv 10 \not\equiv 0 \pmod{11}$, $40600 \equiv 10 \not\equiv 0 \pmod{11}$, it follows from Example 6.4 that

$$v_p(a) = v_{11}(84898109(\mathbf{D}_2^*(\Gamma_2(T_*)))^2) = 2v_{11}(\mathbf{D}_2^*(\Gamma_2(T_*))) = 2, \\ v_p(b) = v_{11}(2(29(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 - 40600)) = v_{11}(40600) = 0, \\ v_p(d) = v_{31}(261(29(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 - 40600)) = v_{11}(40600) = 0.$$

We see that

$$n_1 := (m + k)(v_p(a) - v_p(bd)) + m + k - 1 = 2v_p(a) + 1 = 5, \\ n_2 := (m + k)(v_p(a) - v_p(b)) + m - 1 = 2v_p(a) = 4, \\ n_3 := (m + k)(v_p(a) - v_p(d)) + k - 1 = 2v_p(a) = 4, \\ n_4 := (m + k)v_p(a) - 1 = 2v_p(a) - 1 = 3, \\ n_5 := v_p(a) - v_p(bd) + m + k - 1 = 2 + 1 = 3,$$

and hence

$$\max(n_1, n_2, n_3, n_4, n_5) = 5.$$

By assumption, we know that

$$n > 5 = \max(n_1, n_2, n_3, n_4, n_5),$$

and hence condition (S1) is satisfied.

It is obvious that $km = 1 \not\equiv 0 \pmod{11}$ and

$$ce = 49619 \cdot 99238 \equiv 8 \not\equiv 0 \pmod{11}.$$

Since $\mathbf{D}_2^*(\Gamma_2(T_*))$ belongs to $11\mathbb{Z}_{11}$, we deduce that

$$\begin{aligned} b^k e^m + (-1)^{m+k+1} c^k d^m &= be - cd \\ &= (2(29(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 - 40600))(99238) \\ &\quad - (49619)(261(29(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 - 40600)) \\ &\equiv 2 \cdot (-40600) \cdot 99238 - (49619) \cdot 261 \cdot (-40600) \\ &\equiv 8 \not\equiv 0 \pmod{11}. \end{aligned}$$

Therefore condition (S2) is satisfied, and hence the polynomial $\mathcal{P}_{2,T_*}(x)$ is separable. Since T_* is an arbitrary rational number, our contention follows. \square

For the rest of this section, let

$$\begin{aligned} \mathbf{A}_1 &:= \{n \in \mathbb{Z} : n > 5, n \not\equiv 0 \pmod{4} \text{ and } n \not\equiv 21 \pmod{29}\}, \\ \mathbf{A}_2 &:= \{n \in \mathbb{Z} : n > 5, n \not\equiv 0 \pmod{4} \text{ and } n \not\equiv 8 \pmod{29}\}. \end{aligned}$$

We see that

$$(45) \quad \mathbf{A}_1 \cup \mathbf{A}_2 = \{n \in \mathbb{Z} : n > 5 \text{ and } n \not\equiv 0 \pmod{4}\}.$$

We now prove the main theorem in this section.

Theorem 6.8. *For each $n \in \mathbf{A}_1$ and each rational number $T_* \in \mathbb{Q}$, let $\mathcal{P}_{1,T_*}(x) \in \mathbb{Q}[x]$ be the polynomial of degree $2n + 2$ defined by (43). For each $n \in \mathbf{A}_2$ and each rational number $T_* \in \mathbb{Q}$, let $\mathcal{P}_{2,T_*}(x) \in \mathbb{Q}[x]$ be the polynomial of degree $2n + 2$ defined by (44). Then:*

- (i) *For each $n \in \mathbf{A}_1$ and each rational number $T_* \in \mathbb{Q}$, the hyperelliptic curve $\mathcal{C}_{n,T_*,(29,1,3)}^{(7,261,15)}$ of genus n satisfies CHP and NZC, where $\mathcal{C}_{n,T_*,(29,1,3)}^{(7,261,15)}$ is the smooth projective model of the affine curve defined by*

$$\mathcal{C}_{n,T_*,(29,1,3)}^{(7,261,15)} : z^2 = \mathcal{P}_{1,T_*}(x).$$

- (ii) *For each $n \in \mathbf{A}_2$ and each rational number $T_* \in \mathbb{Q}$, the hyperelliptic curve $\mathcal{C}_{n,T_*,(29,1,3)}^{(133,29,27)}$ of genus n satisfies CHP and NZC, where $\mathcal{C}_{n,T_*,(29,1,3)}^{(133,29,27)}$ is the smooth projective model of the affine curve defined by*

$$\mathcal{C}_{n,T_*,(29,1,3)}^{(133,29,27)} : z^2 = \mathcal{P}_{2,T_*}(x).$$

Remark 6.9. By (45) and Theorem 6.8, Theorem 1.1 follows immediately.

Proof. Throughout the proof of Theorem 6.8, we will use the same notation as in Theorem 4.1 and Lemma 5.1. We first prove that Theorem 6.8(i) holds.

Let $(p, b, d, \alpha_0, \beta_0, \gamma_0) = (29, 1, 3, 7, 261, 15)$. Let n be any integer such that $n \in A_1$. We see that $\bar{\beta}_0 = 9$. One can check that the sextuple $(p, b, d, \alpha_0, \beta_0, \gamma_0)$ satisfies (A1)–(A5) and (B1). Indeed, (A1), (A2), (A4), (A5) and (B1) are obvious. It remains to prove that $(p, b, d, \alpha_0, \beta_0, \gamma_0)$ satisfies (A3). By (11) and (12), we know that

$$P_0 = 124613, \quad Q_0 = -63945.$$

The conic $\mathcal{Q}_1^{(7,261,15)}$ in (A3) of Theorem 4.1 defined by

$$\mathcal{Q}_1^{(7,261,15)} : 29U^2 - V^2 + 2079746732385T^2 = 0$$

has a point $(u_0, v_0, t_0) = (166257, 3020031, 2)$, and hence $(p, b, d, \alpha_0, \beta_0, \gamma_0)$ satisfies (A3).

Let $S := \{2, 29\}$, and let $C_1(T)$ be the rational function in $\mathbb{Q}(T)$ defined by the same equation (23) of C with $(0, T)$ in the role of (A, B) , that is,

$$C_1(T) := \frac{-2v_0T - 4p^3\alpha_0\beta_0t_0^2Q_0}{T^2 + 4p^5\beta_0t_0^2Q_0} = \frac{-6040062T + 45588900213360}{T^2 - 5477180725633680}.$$

Let $G_1(T) \in \mathbb{Q}(T)$ be the rational function defined by

$$(46) \quad G_1(T) = v_0 + TC_1(T) \\ = \frac{-3020031T^2 + 45588900213360T - 16541255584016208244080}{T^2 - 5477180725633680}.$$

Since the numerator and denominator of $G_1(T)$ are irreducible polynomials over \mathbb{Q} , the set Z_1 of rational zeros and poles of $G_1(T)$ is empty. Hence, applying Lemma 6.1 for the triple $(S, G_1(T), Z_1)$, we know that $F_1(T)$ satisfies (1) and (2) in Lemma 6.1, where $F_1(T)$ is the rational function defined by (28) with $(p_0, \epsilon) = (3, 2)$ and $(S, G_1(T), Z_1)$ in the role of $(S, G(T), Z)$, that is,

$$F_1(T) := 1 + \frac{4 \prod_{l \in S, l \neq 2} l}{T^2 - p_0^2 \epsilon} = 1 + \frac{116}{T^2 - 18} = \frac{T^2 + 98}{T^2 - 18}.$$

Let $\Gamma_1(T) \in \mathbb{Q}(T)$ be the rational function defined by (32). Recall that

$$\Gamma_1(T) := \frac{961}{T^2 - 75}.$$

It is known that $\Gamma_1(T_*)$ is well-defined, namely, not infinity for all $T_* \in \mathbb{Q}$.

Take an arbitrary rational number $T_* \in \mathbb{Q}$, and let $(A, B) = (0, F_1(\Gamma_1(T_*)))$. By Lemma 6.1, we know that $(0, F_1(T_*))$ satisfies (C1) and (C2) in Lemma 5.1, and it thus follows that $(A, B) = (0, F_1(\Gamma_1(T_*)))$ also satisfies (C1) and (C2).

Let $D_1(\Gamma_1(T))$ be the rational function in $\mathbb{Q}(T)$ defined by the same equation (23) of C with $(0, F_1(\Gamma_1(T)))$ in the role of (A, B) , that is,

$$(47) \quad D_1(\Gamma_1(T)) := C_1(F_1(\Gamma_1(T))) \\ = \frac{45588894173298(\Gamma_1(T))^4 - 1641200890885920(\Gamma_1(T))^2 + 14770814323798008}{-5477180725633679(\Gamma_1(T))^4 + 197178506122812676(\Gamma_1(T))^2 - 1774606555105302716}.$$

Note that $(A, B) = (0, F_1(\Gamma_1(T_*)))$ satisfies (C1) and (C2). Hence, using the same arguments as in the proof of Lemma 5.1, one knows that $D_1(\Gamma_1(T_*)) \in \mathbb{Z}_{29}$.

We see that

$$u := u_0 + AD_1(\Gamma_1(T_*)) = u_0 = 166257 \neq 0.$$

Furthermore, it follows from Lemma 6.1(2), (46) and (47) that

$$v := v_0 + BD_1(\Gamma_1(T_*)) = G_1(F_1(\Gamma_1(T_*)))$$

is well-defined, namely, not infinity and nonzero. Hence $(A, B) = (0, F_1(\Gamma_1(T_*)))$ satisfies (C3) in Lemma 5.1.

Set

$$\alpha := \alpha_0 + 2p^2 D_1(\Gamma_1(T_*)) = 7 + 1682 D_1(\Gamma_1(T_*)) = D_1^*(\Gamma_1(T_*)), \\ \beta := \beta_0 = 261, \\ \gamma := \gamma_0 = 15,$$

where $D_1^*(\Gamma_1(T)) \in \mathbb{Q}(T)$ is the rational function defined by (33). Recall from there that

$$D_1^*(\Gamma_1(T)) = \frac{\Sigma_{1,1}(T)}{\Sigma_{1,2}(T)},$$

where $\Sigma_{1,1}(T)$, $\Sigma_{1,2}(T)$ are defined by (34), (35), respectively.

By Lemma 5.1, we know that (α, β, γ) satisfies (A1)–(A5) and (B1). By (11) and (12), we know that

$$P = 29(7 + 1682 D_1(\Gamma_1(T_*)))^2 + 123192 = 29(D_1^*(\Gamma_1(T_*)))^2 + 123192, \\ Q = Q_0 = -63945.$$

It is not difficult to see that the curve $C_{n, T_*, (29, 1, 3)}^{(7, 261, 15)}$ defined in Theorem 6.8(i) is the smooth projective model of the affine curve defined by (13).

By Corollary 6.6, we know that $\mathcal{P}_{1, T_*}(x)$ is separable, and hence we deduce that condition (S) in Theorem 4.1 is true. Since $D_1(\Gamma_1(T_*)) \in \mathbb{Z}_{29}$, we see that

$$-2\left(\frac{\gamma}{\alpha}\right)^2 \equiv 21 \pmod{29}.$$

Since $n \in A_1$, we deduce that

$$n \not\equiv -2\left(\frac{\gamma}{\alpha}\right)^2 \pmod{29}.$$

Thus (A6) holds if n is odd, and (B2) holds if $n \equiv 2 \pmod{4}$. By Corollaries 4.6 and 4.8, we deduce that for each $n \in A_1$, the curve $C_{n,T_*,(29,1,3)}^{(7,261,15)}$ satisfies CHP and NZC. Since T_* is an arbitrary rational number, Theorem 6.8(i) follows.

We now prove Theorem 6.8(ii). We will use the same notation as in the proof of part (i) as long as it does not cause any confusion. We will use the same arguments as in the proof of part (i) to construct an algebraic family of hyperelliptic curves of genus n satisfying CHP and NZC for each $n \in A_2$.

Let $(p, b, d, \alpha_0, \beta_0, \gamma_0) = (29, 1, 3, 133, 29, 27)$. Let n be any integer such that $n \in A_2$. We see that $\bar{\beta}_0 = 1$. One can check that the sextuple $(p, b, d, \alpha_0, \beta_0, \gamma_0)$ satisfies (A1)–(A5) and (B1). Indeed (A1), (A2), (A4), (A5) and (B1) are obvious. It remains to prove that the sextuple satisfies (A3). By (11) and (12), we know that

$$P_0 = 472381, \quad Q_0 = 1711.$$

The conic $Q_1^{(133,29,27)}$ in (A3) of Theorem 4.1 defined by

$$Q_1^{(133,29,27)} : 29U^2 - V^2 - 23439072839T^2 = 0$$

has a point $(u_0, v_0, t_0) = (728799, 3613777, 10)$, and thus $(p, b, d, \alpha_0, \beta_0, \gamma_0)$ satisfies (A3).

Let $S := \{2, 29\}$, and let $C_2(T) \in \mathbb{Q}(T)$ be the rational function defined by the same equation (23) of C with $(0, T)$ in the role of (A, B) , that is,

$$C_2(T) = \frac{-2v_0T - 4p^3\alpha_0\beta_0t_0^2Q_0}{T^2 + 4p^5\beta_0t_0^2Q_0} = \frac{-7227554T - 64380394481200}{T^2 + 407097080892400}.$$

Let $G_2(T) \in \mathbb{Q}(T)$ be the rational function defined by

$$(48) \quad G_2(T) = v_0 + TC_2(T) \\ = \frac{-3613777T^2 - 64380394481200T + 147115806769609459480}{T^2 + 407097080892400}.$$

Since the numerator and denominator of $G_2(T)$ are irreducible polynomials over \mathbb{Q} , the set Z_2 of rational zeros and poles of $G_2(T)$ is empty. Hence, applying Lemma 6.1 for the triple $(S, G_2(T), Z_2)$, we know that $F_2(T)$ satisfies (1) and (2) in Lemma 6.1, where $F_2(T)$ is the rational function defined by (28) with $(p_0, \epsilon) = (3, 2)$ and $(S, G_2(T), Z_2)$ in the role of $(S, G(T), Z)$, that is,

$$F_2(T) := 1 + \frac{4 \prod_{l \in S, l \neq 2} l}{T^2 - p_0^2 \epsilon} = 1 + \frac{116}{T^2 - 18} = \frac{T^2 + 98}{T^2 - 18}.$$

Let $\Gamma_2(T) \in \mathbb{Q}(T)$ be the rational function defined by (38). Recall that

$$\Gamma_2(T) := \frac{121}{T^2 - 63}.$$

It is known that $\Gamma_2(T_*)$ is well defined, namely, not infinity for each rational number $T_* \in \mathbb{Q}$.

Now take an arbitrary rational number $T_* \in \mathbb{Q}$, and let $(A, B) = (0, \mathbf{F}_2(\Gamma_2(T_*)))$. By Lemma 6.1, we know that $(0, \mathbf{F}_2(T_*))$ satisfies (C1) and (C2) in Lemma 5.1, and it thus follows that $(A, B) = (0, \mathbf{F}_2(\Gamma_2(T_*)))$ also satisfies (C1) and (C2).

Let $\mathbf{D}_2(\Gamma_2(T))$ be the rational function in $\mathbb{Q}(T)$ defined by the same equation (23) of C with $(0, \mathbf{F}_2(\Gamma_2(T)))$ in the role of (A, B) , that is,

$$(49) \quad \begin{aligned} \mathbf{D}_2(\Gamma_2(T)) &:= \mathbf{C}_2(\mathbf{F}_2(\Gamma_2(T))) \\ &= \frac{-64380401708754(\Gamma_2(T))^4 + 2317693623118880(\Gamma_2(T))^2 - 20859235062503544}{407097080892401(\Gamma_2(T))^4 - 14655494912126204(\Gamma_2(T))^2 + 131899454209147204}. \end{aligned}$$

Note that $(A, B) = (0, \mathbf{F}_2(\Gamma_2(T_*)))$ satisfies (C1) and (C2). Hence, using the same arguments as in the proof of Lemma 5.1, one knows that $\mathbf{D}_2(\Gamma_2(T_*)) \in \mathbb{Z}_{29}$.

We see that

$$u := u_0 + A\mathbf{D}_1(\Gamma_1(T_*)) = u_0 = 728799 \neq 0.$$

Furthermore, it follows from Lemma 6.1(2), (48) and (49) that

$$v := v_0 + B\mathbf{D}_2(\Gamma_2(T_*)) = \mathbf{G}_2(\mathbf{F}_2(\Gamma_2(T_*)))$$

is defined, namely, not infinity and nonzero. Hence $(A, B) = (0, \mathbf{F}_2(\Gamma_2(T_*)))$ satisfies Lemma 5.1(C3).

Set

$$\alpha := \alpha_0 + 2p^2\mathbf{D}_2(\Gamma_2(T_*)) = 133 + 1682\mathbf{D}_2(\Gamma_2(T_*)) = \mathbf{D}_2^*(\Gamma_2(T_*)),$$

$$\beta := \beta_0 = 29,$$

$$\gamma := \gamma_0 = 27,$$

where $\mathbf{D}_2^*(\Gamma_2(T)) \in \mathbb{Q}(T)$ is the rational function defined by (39). Recall from there that

$$\mathbf{D}_2^*(\Gamma_2(T)) = \frac{\Sigma_{2,1}(T)}{\Sigma_{2,2}(T)},$$

where $\Sigma_{2,1}(T)$, $\Sigma_{2,2}(T)$ are defined by (40), (41), respectively.

By Lemma 5.1, we know that (α, β, γ) satisfies (A1)–(A5) and (B1). By (11) and (12), we know that

$$P = 29(133 + 1682\mathbf{D}_2(\Gamma_2(T_*)))^2 - 40600 = 29(\mathbf{D}_2^*(\Gamma_2(T_*)))^2 - 40600,$$

$$Q = Q_0 = 1711.$$

It is not difficult to see that the curve $C_{n,T_*,(29,1,3)}^{(133,29,27)}$ defined in Theorem 6.8(ii) is the smooth projective model of the affine curve defined by (13).

By Corollary 6.7, we know that $\mathcal{P}_{2,T_*}(x)$ is separable, and hence we deduce that condition (S) in Theorem 4.1 is true. Since $D_2(\Gamma_2(T_*)) \in \mathbb{Z}_{29}$, we see that

$$-2\left(\frac{\gamma}{\alpha}\right)^2 \equiv 8 \pmod{29}.$$

Since $n \in A_2$, we deduce that

$$n \not\equiv -2\left(\frac{\gamma}{\alpha}\right)^2 \pmod{29}.$$

Thus (A6) holds if n is odd, and (B2) holds if $n \equiv 2 \pmod{4}$. By Corollaries 4.6 and 4.8, we deduce that for each $n \in A_2$, the curve $C_{n,T_*,(29,1,3)}^{(133,29,27)}$ satisfies CHP and NZC. Since T_* is an arbitrary rational number, Theorem 6.8(ii) follows. \square

Acknowledgements

I am grateful to Emmanuel Kowalski for his encouragement. I thank the referee for useful comments. I was supported by a postdoctoral fellowship in the Department of Mathematics at the University of British Columbia during the writing of this paper.

References

- [Amer 1976] M. Amer, *Quadratische Formen über Funktionenkörpern*, thesis, Johannes Gutenberg University, Mainz, 1976.
- [Bhargava et al. 2013] M. Bhargava, B. H. Gross, and X. Wang, “Pencils of quadrics and the arithmetic of hyperelliptic curves”, preprint, 2013. arXiv 1310.7692
- [Borevich and Shafarevich 1966] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Pure and Applied Mathematics **20**, Academic Press, New York, 1966. MR 33 #4001 Zbl 0145.04902
- [Brumer 1978] A. Brumer, “Remarques sur les couples de formes quadratiques”, *C. R. Acad. Sci. Paris Sér. A* **286**:16 (1978), 679–681. MR 58 #16502 Zbl 0392.10021
- [Cohen 2007] H. Cohen, *Number theory, I: Tools and Diophantine equations*, Graduate Texts in Mathematics **239**, Springer, New York, 2007. MR 2008e:11001 Zbl 1119.11001
- [Colliot-Thélène and Poonen 2000] J.-L. Colliot-Thélène and B. Poonen, “Algebraic families of nonzero elements of Shafarevich–Tate groups”, *J. Amer. Math. Soc.* **13**:1 (2000), 83–99. MR 2000f:11067 Zbl 0951.11022
- [Colliot-Thélène et al. 1980] J.-L. Colliot-Thélène, D. F. Coray, and J.-J. Sansuc, “Descente et principe de Hasse pour certaines variétés rationnelles”, *J. Reine Angew. Math.* **320** (1980), 150–191. MR 82f:14020 Zbl 0434.14019
- [Coray and Manoil 1996] D. F. Coray and C. Manoil, “On large Picard groups and the Hasse principle for curves and $K3$ surfaces”, *Acta Arith.* **76**:2 (1996), 165–189. MR 97j:14038 Zbl 0877.14005
- [Corn 2007] P. Corn, “The Brauer–Manin obstruction on del Pezzo surfaces of degree 2”, *Proc. Lond. Math. Soc.* (3) **95**:3 (2007), 735–777. MR 2009a:14027 Zbl 1133.14022
- [Dong Quan 2014] N. N. Dong Quan, “From separable polynomials to nonexistence of rational points on certain hyperelliptic curves”, *J. Aust. Math. Soc.* **96**:3 (2014), 354–385. MR 3217721 Zbl 06324731

- [Iwaniec 1974] H. Iwaniec, “Primes represented by quadratic polynomials in two variables”, *Acta Arith.* **24**:5 (1974), 435–459. MR 49 #7210 Zbl 0271.10043
- [Lind 1940] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, thesis, University of Uppsala, 1940. MR 9,225c Zbl 0025.24802
- [Poonen 2001] B. Poonen, “An explicit algebraic family of genus-one curves violating the Hasse principle”, *J. Théor. Nombres Bordeaux* **13**:1 (2001), 263–274. MR 2002e:14036 Zbl 1046.11038
- [Poonen 2008] B. Poonen, “Rational points on varieties”, Lecture notes, MIT/UCB, 2008, <http://www-math.mit.edu/~poonen/papers/Qpoints.pdf>.
- [Reichardt 1942] H. Reichardt, “Einige im Kleinen überall lösbare, im Grossen unlösbare Diophantische Gleichungen”, *J. Reine Angew. Math.* **184** (1942), 12–18. MR 5,141c Zbl 0026.29701
- [Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026
- [Skorobogatov 2001] A. N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics **144**, Cambridge University Press, 2001. MR 2002d:14032 Zbl 0972.14015
- [Viray 2012] B. Viray, “Failure of the Hasse principle for Châtelet surfaces in characteristic 2”, *J. Théor. Nombres Bordeaux* **24**:1 (2012), 231–236. MR 2914907 Zbl 1285.11095

Received November 27, 2013.

NGUYEN NGOC DONG QUAN
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TEXAS AT AUSTIN
AUSTIN, TX 78712
UNITED STATES
dongquan.ngoc.nguyen@gmail.com

PACIFIC JOURNAL OF MATHEMATICS

msp.org/pjm

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Robert Finn
Department of Mathematics
Stanford University
Stanford, CA 94305-2125
finn@math.stanford.edu

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI
CALIFORNIA INST. OF TECHNOLOGY
INST. DE MATEMÁTICA PURA E APLICADA
KEIO UNIVERSITY
MATH. SCIENCES RESEARCH INSTITUTE
NEW MEXICO STATE UNIV.
OREGON STATE UNIV.

STANFORD UNIVERSITY
UNIV. OF BRITISH COLUMBIA
UNIV. OF CALIFORNIA, BERKELEY
UNIV. OF CALIFORNIA, DAVIS
UNIV. OF CALIFORNIA, LOS ANGELES
UNIV. OF CALIFORNIA, RIVERSIDE
UNIV. OF CALIFORNIA, SAN DIEGO
UNIV. OF CALIF., SANTA BARBARA

UNIV. OF CALIF., SANTA CRUZ
UNIV. OF MONTANA
UNIV. OF OREGON
UNIV. OF SOUTHERN CALIFORNIA
UNIV. OF UTAH
UNIV. OF WASHINGTON
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.


See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2015 is US \$420/year for the electronic version, and \$570/year for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2015 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 274 No. 1 March 2015

Unimodal sequences and “strange” functions: a family of quantum modular forms	1
KATHRIN BRINGMANN, AMANDA FOLSOM and ROBERT C. RHOADES	
Congruence primes for Ikeda lifts and the Ikeda ideal	27
JIM BROWN and RODNEY KEATON	
Constant mean curvature, flux conservation, and symmetry	53
NICK EDELEN and BRUCE SOLOMON	
The cylindrical contact homology of universally tight sutured contact solid tori	73
ROMAN GOLOVKO	
Uniform boundedness of S -units in arithmetic dynamics	97
HOLLY KRIEGER, AARON LEVIN, ZACHARY SCHERR, THOMAS TUCKER, YU YASUFUKU and MICHAEL E. ZIEVE	
A counterexample to the energy identity for sequences of α -harmonic maps	107
YUXIANG LI and YOUDE WANG	
Theory of newforms of half-integral weight	125
MURUGESAN MANICKAM, JABAN MEHER and BALAKRISHNAN RAMAKRISHNAN	
Algebraic families of hyperelliptic curves violating the Hasse principle	141
NGUYEN NGOC DONG QUAN	
F -zips with additional structure	183
RICHARD PINK, TORSTEN WEDHORN and PAUL ZIEGLER	
Mean values of L -functions over function fields	237
JEFFREY LIN THUNDER	



0030-8730(201503)274:1;1-3