TOKYO J. MATH.
VOL. 40, NO. 1, 2017

Certain Forms Violate the Hasse Principle

Dong Quan Ngoc NGUYEN

University of Notre Dame

(Communicated by N. Suwa)

Abstract. A family of smooth geometrically irreducible curves violates the Hasse principle if they have local points everywhere, but they possesses no global points. In this paper, we show how to construct non-constant algebraic families of forms of degree $4k$ that violate the Hasse principle. Some examples of non-constant algebraic families of forms of degrees 12 and 24 that violate the Hasse principle are given to illustrate the method.

1. Introduction

A family of smooth geometrically irreducible curves $(\mathcal{C}_\alpha)_\alpha$ over $\mathbb{Q}$ is said to be counterexamples to the Hasse principle if $\mathcal{C}_\alpha(\mathbb{Q}) = \emptyset$ but $\mathcal{C}_\alpha(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ for each α. Equivalently, we also say that the curves $(\mathcal{C}_\alpha)_\alpha$ violate the Hasse principle. The failure for the Hasse principle on these curves is said to be explained by the Brauer–Manin obstruction if $\mathcal{C}_\alpha(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$ for each α. See, for example, Jahnel [8] for an account of the Brauer–Manin obstruction. It is well-known that the Hasse principle for curves fail in general. The first counterexamples of cubic forms to the Hasse principle were discovered by Selmer [10]; for example, Selmer [10] showed that the ternary cubic form defined by $3x^3 + 4y^3 + 5z^3 = 0$ is a counterexample to the Hasse principle.

Bhargava [1] proved that for each $n \geq 1$, a positive proportion of hyperelliptic curves $z^2 = F(x)$ of genus n over $\mathbb{Q}$, when ordered by height, fails the Hasse principle. Bhargava [1] further showed that the failure can be explained by the Brauer–Manin obstruction. One can ask whether a similar asymptotic result holds when hyperelliptic curves are replaced by forms of degree ≥ 3 over $\mathbb{Q}$. In this direction, Bhargava [2] proved that a positive proportion of ternary cubic forms over $\mathbb{Z}$, when ordered by the heights of their coefficients, fails the Hasse principle. It is not known whether a similar asymptotic result hold when ternary cubic forms are replaced by a more general form of degree ≥ 3.

In this paper, we are interested in the following weaker question.

QUESTION. For each integer $n \geq 3$, does there exist a family of forms of degree $n \geq 3$ that are counterexamples to the Hasse principle?

Received December 18, 2015; revised November 12, 2016

For $n = 3$, Bhargava [2] answers this question in the affirmative as a special case of his result, but does not explicitly describe such ternary cubic forms. An explicit algebraic family of cubic curves is given in the work of Poonen [9]. In [5], the author constructed an arithmetic family of quartic forms over $\mathbb{Q}$ that are counterexamples to the Hasse principle, which affirmatively answers the question when $n = 4$. Fujiwara and Sudo [7] produced many forms of degree n with $n \equiv 5 \pmod{10}$ that violate the Hasse principle. In [6], the author proved that there are algebraic families of degree n with $n \equiv 2 \pmod{4}$ that violate the Hasse principle.

The present work is a continuation of our previous work [6]. We will show how to construct non-constant algebraic families of forms of degree n with $n \equiv 0 \pmod{4}$ that are counterexamples to the Hasse principle. As an illustration, we explicitly construct a non-constant algebraic family of forms of degree 12 and a non-constant algebraic family of forms of degree 24 that violate the Hasse principle.

Our paper is organized as follows. In Section 2, we prove that for $k \in \mathbb{Z}_{\geq 0}$, $m, n \in \mathbb{Z}_{>0}$ with $(k+1)n > m$, under certain conditions, there exist hyperelliptic curves of genus $2(k+1)n - 1$ that are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction (see Theorem 2.3). These curves are of the form

$$z^2 = A(Bx^{2(k+1)n} + C)^2 + (Dx^{2m} + E)^2 \tag{1}$$

for certain choices of parameters A, B, C, D, E. In Section 3, we prove that under certain conditions, there exist forms $(\mathcal{X}_\zeta)_\zeta$ of degree $4(k+1)n$ parameterized by certain rational numbers ζ such that each form $\mathcal{X}_\zeta$ admits a morphism to a hyperelliptic curve of genus $2(k+1)n - 1$. The latter is among the hyperelliptic curves of the form (1) in Theorem 2.3. It thus follows from Theorem 2.3 that the form $\mathcal{X}_\zeta$ of degree $4(k+1)n$ is a counterexample to the Hasse principle (see Theorem 3.1). In Section 4, we show that under certain conditions, there exist algebraic families of forms of degree $4(k+1)n$ for a given non-negative integer k and a given positive integer n (see Theorem 4.2). Using this result, we explicitly construct a non-constant algebraic family of forms of degree 12 and a non-constant algebraic family of degree 24 that are counterexamples to the Hasse principle (see Examples 4.4 and 4.6).

2. Certain hyperelliptic curves violating the Hasse principle

In this section, for a prime $p \equiv 1 \pmod{8}$, a triple (k, m, n) of integers with $k \geq 0$, $m \geq 1$ and $n \geq 1$, we explicitly construct certain curves $\mathcal{D}$ of genus $2(k+1)n - 1$ that are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction. These curves play a key role in constructing forms over $\mathbb{Q}$ that are counterexamples to the Hasse principle.

We begin by proving the following lemma.

LEMMA 2.1. *Let p be a prime. Let $(\alpha, \beta, \gamma, \lambda) \in \mathbb{Z}^4$ be a quadruple of non-zero integers, and let k, m, n be integers such that $k \geq 0$, $m \geq 1$ and $n \geq 1$. Set*

$$d := \alpha^m \lambda^{2(k+1)m}(p(\alpha+\beta))^{(k+1)n} + (-1)^{m+1}\beta^m \gamma^{2(k+1)n}(p\alpha + (p+1)\beta)^{(k+1)n}, \tag{2}$$

and assume that the following are true:

(A1) $(k+1)n > m$, *and* $d \neq 0$.

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

$$P_{p,\alpha,\beta,\lambda,\gamma}(x) := p(\alpha\lambda^{2(k+1)}x^{2(k+1)n} + \beta)^2 + \big((p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta)\big)^2$$

is separable, that is, $P_{p,\alpha,\beta,\lambda,\gamma}(x)$ *has exactly* $4(k+1)n$ *distinct roots over* $\mathbb{C}$.

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

$$\mathcal{C} : z^2 = P_{p,\alpha,\beta,\lambda,\gamma}(x)\,, \tag{3}$$

and let $\mathbb{Q}(\mathcal{C})$ *be the function field of* $\mathcal{C}$. *Let* $\mathcal{A} \in \mathrm{Br}(\mathbb{Q}(\mathcal{C}))$ *be the class of the quaternion algebra defined by*

$$\mathcal{A} = \big(p, (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z\big)\,. \tag{4}$$

Then the element $\mathcal{A}$ *belongs to the subgroup* $\mathrm{Br}(\mathcal{C})$ *of* $\mathrm{Br}(\mathbb{Q}(\mathcal{C}))$. *Furthermore*,

$$\mathcal{B} := \big(p, (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) - z\big)$$

and

$$\mathcal{F} := \left(p, \frac{(p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z}{x^{2(k+1)n}}\right)$$

all represent the same class as $\mathcal{A}$ *in* $\mathrm{Br}(\mathbb{Q}(\mathcal{C}))$.

PROOF. The defining equation of $\mathcal{C}$ can be written in the form

$$\begin{aligned}\big((p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z\big)\big((p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) - z\big)\\ = -p(\alpha\lambda^{2(k+1)}x^{2(k+1)n} + \beta)^2\,,\end{aligned} \tag{5}$$

and thus

$$\begin{aligned}&\big((p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z\big)\big((p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) - z\big)\\ &= \mathrm{Norm}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}\big(\sqrt{p}(\alpha\lambda^{2(k+1)}x^{2(k+1)n} + \beta)\big)\,.\end{aligned}$$

Thus we deduce that $\mathcal{A} + \mathcal{B} = 0$. Furthermore, we know that $\mathcal{A} - \mathcal{F} = (p, x^{2(k+1)n}) = 0$. Since $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{F}$ belong to the 2-torsion part of $\mathrm{Br}(\mathbb{Q}(\mathcal{C}))$, it follows that $\mathcal{A} = \mathcal{B} = \mathcal{F}$.

Let U_1 be the largest open subvariety of $\mathcal{C}$ in which the rational function $F := (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z$ neither has a zero nor pole, and let U_2 be the largest open subvariety of $\mathcal{C}$ in which the rational function $G := (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) - z$ neither has a zero nor pole. Since $\mathcal{A} = \mathcal{B}$, $\mathcal{A}$ belongs to $\mathrm{Br}(U_1)$ and $\mathrm{Br}(U_2)$. We prove that in the affine part of $\mathcal{C}$, the locus where both F and G have a zero is empty. Assume the contrary, and let (X, Z) be a common zero of F and G. Then it follows from (5) that

$$\alpha\lambda^{2(k+1)}X^{2(k+1)n} + \beta = 0\,,$$

and thus

$$\alpha\lambda^{2(k+1)}X^{2(k+1)n} = -\beta\,. \tag{6}$$

On the other hand, we know that

$$2((p\alpha + (p+1)\beta)\gamma^2X^{2m} - p(\alpha+\beta)) = F + G = 0\,,$$

and thus

$$(p\alpha + (p+1)\beta)\gamma^2X^{2m} = p(\alpha+\beta)\,. \tag{7}$$

Hence it follows from (6) and (7) that

$$\begin{aligned}(\gamma^{2(k+1)n}(p\alpha + (p+1)\beta)^{(k+1)n})(\alpha^m\lambda^{2(k+1)m})X^{2(k+1)nm}\\ = (-1)^m\beta^m\gamma^{2(k+1)n}(p\alpha + (p+1)\beta)^{(k+1)n}\\ = \alpha^m\lambda^{2(k+1)m}(p(\alpha+\beta))^{(k+1)n}\,,\end{aligned}$$

and thus

$$d = \alpha^m\lambda^{2(k+1)m}(p(\alpha+\beta))^{(k+1)n} + (-1)^{m+1}\beta^m\gamma^{2(k+1)n}(p\alpha + (p+1)\beta)^{(k+1)n} = 0\,,$$

which contradicts (A1).

Let

$$H := \frac{(p\alpha + (p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta) + z}{x^{2(k+1)n}}\,,$$

and denote by $\infty = (X_\infty : Y_\infty : Z_\infty)$ be a point at infinity of $\mathcal{C}$. We know that $Y_\infty = 0$ and $Z_\infty = \pm p^{1/2}\alpha\lambda^{2(k+1)}X_\infty^{2(k+1)n}$, where $X_\infty \neq 0$. Since $(k+1)n > m$, we deduce that

$$\begin{aligned}H(\infty) &= \frac{(p\alpha + (p+1)\beta)\gamma^2X_\infty^{2m}Y_\infty^{2(k+1)n-2m} - p(\alpha+\beta)Y_\infty^{2(k+1)n} + Z_\infty}{X_\infty^{2(k+1)n}}\,,\\ &= \pm p^{1/2}\alpha\lambda^{2(k+1)} \neq 0\,,\end{aligned}$$

and therefore H is regular and non-vanishing at the points at infinity of $\mathcal{C}$.

Let U_3 be the largest open subvariety of $\mathcal{C}$ in which the rational function H neither has a zero nor pole. Since $\mathcal{A} = \mathcal{F}$, we deduce that $\mathcal{A}$ belongs to $\mathrm{Br}(U_3)$. By what we have shown, it follows that $\mathcal{C} = U_1 \cup U_2 \cup U_3$. Since $\mathcal{A}$ belongs to $\mathrm{Br}(U_i)$ for $i = 1, 2, 3$, we deduce that $\mathcal{A}$ belongs to $\mathrm{Br}(\mathcal{C})$. Therefore our contention follows. □

THEOREM 2.2. *We maintain the same notation and assumptions as in Lemma* 2.1. *Assume that p is a prime such that $p \equiv 1 \pmod 8$. Assume further that* (A1), (S) *in Lemma* 2.1 *are true, and that the following are true*:

(A2) $\gcd(\alpha, p) = 1$, $\gcd(\beta, p) = 1$, $\gcd(\gamma, p) = 1$ *and* $\gcd(\lambda, p) = 1$.

(A3) *l is a quadratic residue in $\mathbb{F}_p^\times$ for any odd prime l dividing α.*

(A4) *β is a quadratic non-residue in $\mathbb{F}_p^\times$.*

(A5) *l is a quadratic residue in $\mathbb{F}_p^\times$ for any odd prime l dividing λ.*

(A6) *l is a quadratic residue in $\mathbb{F}_p^\times$ for any odd prime l dividing d.*

Let $\mathcal{C}$ be the smooth projective model of the affine curve in Lemma 2.1. *Then $\mathcal{C}(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$.*

PROOF. Let $\mathbb{Q}(\mathcal{C})$ be the function field of $\mathcal{C}$, and let $\mathcal{A}$ be the class of the quaternion algebra defined by (4) in Lemma 2.1. For any $P_l \in \mathcal{C}(\mathbb{Q}_l)$, we will prove that

$$\mathrm{inv}_l(\mathcal{A}(P_l)) = \begin{cases} 0 & \text{if } l \neq p \\ 1/2 & \text{if } l = p\,. \end{cases} \tag{8}$$

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

Suppose that l is an odd prime such that $l \neq p$ and p is not a square in $\mathbb{Q}_l^\times$. By (A3) and (A5), we deduce that $\alpha \not\equiv 0 \pmod{l}$ and $\lambda \not\equiv 0 \pmod{l}$. We consider the following cases:

Case 1. $v_l(x) \geq 0$.

Assume that

$$\begin{cases} (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z & \equiv 0 \pmod{l} \\ (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) - z & \equiv 0 \pmod{l}\,. \end{cases} \tag{9}$$

It follows that

$$(p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) \equiv 0 \pmod{l}\,,$$

and thus

$$(p\alpha + (p+1)\beta)\gamma^2 x^{2m} \equiv p(\alpha+\beta) \pmod{l}\,. \tag{10}$$

Furthermore, it follows from (9) and (5) that

$$\alpha\lambda^{2(k+1)} x^{2(k+1)n} + \beta \equiv 0 \pmod{l}\,,$$

and hence

$$\alpha\lambda^{2(k+1)} x^{2(k+1)n} \equiv -\beta \pmod{l}\,. \tag{11}$$

Thus it follows from (10) and (11) that

$$\begin{aligned} &\alpha^m \lambda^{2(k+1)m} (p\alpha + (p+1)\beta)^{(k+1)n} \gamma^{2(k+1)n} x^{2(k+1)mn} \\ &\quad \equiv \alpha^m \lambda^{2(k+1)m} (p(\alpha+\beta))^{(k+1)n} \pmod{l} \end{aligned}$$

and

$$\begin{aligned} &\alpha^m \lambda^{2(k+1)m} (p\alpha + (p+1)\beta)^{(k+1)n} \gamma^{2(k+1)n} x^{2(k+1)mn} \\ &\quad \equiv (-1)^m \beta^m (p\alpha + (p+1)\beta)^{(k+1)n} \gamma^{2(k+1)n} \pmod{l}\,. \end{aligned}$$

Thus we deduce from the last two congruences that

$$\alpha^m \lambda^{2(k+1)m} (p(\alpha+\beta))^{(k+1)n} \equiv (-1)^m \beta^m (p\alpha + (p+1)\beta)^{(k+1)n} \gamma^{2(k+1)n} \pmod{l}\,,$$

and therefore

$$d = \alpha^m \lambda^{2(k+1)m} (p(\alpha+\beta))^{(k+1)n} + (-1)^{m+1}\beta^m (p\alpha + (p+1)\beta)^{(k+1)n} \gamma^{2(k+1)n} \equiv 0 \pmod{l}.$$

By (A6), we deduce that l is a quadratic residue in $\mathbb{F}_p^\times$, and thus it follows from the quadratic reciprocity law that p is a square in $\mathbb{Q}_l^\times$, which is a contradiction. Thus at least one of $(p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z$ and $(p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) - z$ is non-zero modulo l, say U. Thus the Hilbert symbol $(p, U)_l$ is 1, and therefore $\mathrm{inv}_l(\mathcal{A}(P_l))$ is 0.

Case 2. $\varepsilon := v_l(x) < 0$.

By (A3) and (A5), $\alpha \not\equiv 0 \pmod{l}$ and $\lambda \not\equiv 0 \pmod{l}$. Hence

$$v_l\big(p\alpha^2\lambda^{4(k+1)}x^{4(k+1)n}\big) = 4(k+1)n\varepsilon\,,$$

and thus it follows from (A1) and (3) that

$$v_l(z) = \frac{v_l(z^2)}{2} = \frac{v_l\left(p\alpha^2\lambda^{4(k+1)}x^{4(k+1)n}\right)}{2} = 2(k+1)n\varepsilon\,.$$

We have that

$$\begin{aligned} v_l((p\alpha+(p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta)) &\geq \min\big(v_l(p(\alpha+\beta)), v_l((p\alpha+(p+1)\beta)\gamma^2x^{2m})\big) \\ &\geq \min\big(0, v_l(p\alpha+(p+1)\beta) + 2v_l(\gamma) + 2mv_l(x)\big) \\ &\geq \min(0, 2m\varepsilon) \\ &= 2m\varepsilon \ \ (\text{since } 2m\varepsilon < 0) \\ &> 2(k+1)n\varepsilon = v_l(z) \ \ (\text{since } (k+1)n > m)\,. \end{aligned}$$

Hence we deduce that

$$v_l((p\alpha+(p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta) + z) = v_l(z) = 2(k+1)n\varepsilon\,,$$

which is an even integer. Using Theorem 5.2.7 in [4], we see that the Hilbert symbol $(p, (p\alpha+(p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta)+z)_l$ is 1. Thus $\mathrm{inv}_l(\mathcal{A}(P_l))$ is 0.

Suppose that $l = p$. If $v_p(x) < 0$, then it follows from (A2) and (3) that

$$\begin{aligned} 2v_p(z) &= v_p(z^2) = v_p\big(p\alpha^2\lambda^{4(k+1)}x^{4(k+1)n}\big) \\ &= v_p(p) + v_p\big(\alpha^2\lambda^{4(k+1)}x^{4(k+1)n}\big) = 1 + 4(k+1)nv_p(x)\,, \end{aligned}$$

which is a contradiction since the left-hand side is an even integer whereas the right-hand side is an odd integer.

If $v_p(x) > 0$, then it follows that $v_p(x) \geq 1$. Since $\alpha \not\equiv 0 \pmod{p}$, $\beta \not\equiv 0 \pmod{p}$ and $\lambda \not\equiv 0 \pmod{p}$, we see that

$$v_p\big(p(\alpha\lambda^{2(k+1)}x^{2(k+1)n} + \beta)^2\big) = v_p(p) + v_p\big((\alpha\lambda^{2(k+1)}x^{2(k+1)n} + \beta)^2\big)$$

$$
\begin{aligned}
&= 1 + 2v_p\big(\alpha\lambda^{2(k+1)}x^{2(k+1)n} + \beta\big)\\
&= 1 + 2\min\big(v_p(\alpha\lambda^{2(k+1)}x^{2(k+1)n}), v_p(\beta)\big)\\
&= 1 + 2\min\big(2(k+1)nv_p(x), 0\big)\\
&= 1 + 2\cdot 0 \ \ (\text{since } v_p(x) \geq 1)\\
&= 1\,.
\end{aligned}
$$

On the other hand, we see that

$$
\begin{aligned}
&v_p\Big(\big((p\alpha + (p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta)\big)^2\Big)\\
&\quad = 2v_p\Big((p\alpha + (p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta)\Big)\\
&\quad \geq 2\min\Big(v_p\big((p\alpha + (p+1)\beta)\gamma^2x^{2m}\big), v_p\left(p(\alpha+\beta)\right)\Big)\\
&\quad \geq 2\min\big(v_p(p\alpha + (p+1)\beta) + 2mv_p(x), 1 + v_p(\alpha+\beta)\big)\\
&\quad \geq 2\min\big(2mv_p(x), 1\big) \ \ \big(\text{since } v_p(p\alpha + (p+1)\beta) \geq 0 \text{ and } v_p(\alpha+\beta) \geq 0\big)\\
&\quad = 2 \ \ (\text{since } 2mv_p(x) \geq 2m \geq 2 > 1)\,.
\end{aligned}
$$

Hence we deduce from (3) that

$$
\begin{aligned}
2v_p(z) &= v_p(z^2)\\
&= \min\Big(v_p\big(p(\alpha\lambda^{2(k+1)}x^{2(k+1)n} + \beta)^2\big),\\
&\qquad v_p\Big(\big((p\alpha + (p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta)\big)^2\Big)\Big)\\
&= \min\Big(1, v_p\Big(\big((p\alpha + (p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta)\big)^2\Big)\Big)\\
&= 1 \ \ \Big(\text{since } v_p\Big(\big((p\alpha + (p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta)\big)^2\Big) \geq 2\Big)\,,
\end{aligned}
$$

which is a contradiction since the left-hand side is an even integer whereas the right-hand side is odd. This contradiction establishes that $v_p(x) = 0$, and hence x is a unit in $\mathbb{Z}_p^{\times}$. By (3), we see that $v_p(z) \geq 0$.

Taking (5) modulo p, we deduce that

$$(p\alpha + (p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta) - z \equiv 0 \pmod{p}$$

or

$$(p\alpha + (p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta) + z \equiv 0 \pmod{p}\,.$$

We consider the following two cases:

Case I. $(p\alpha + (p+1)\beta)\gamma^2x^{2m} - p(\alpha+\beta) - z \equiv 0 \pmod{p}$.

We see that $z \equiv (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) \pmod{p}$, and hence it follows that

$$\begin{aligned}&(p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z \\ &\quad \equiv 2((p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta)) \equiv 2\beta\gamma^2 x^{2m} \not\equiv 0 \pmod{p}.\end{aligned}$$

Using Theorem 5.2.7 in [4], we deduce from (A4) that the local Hilbert symbol

$$\big(p, (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z\big)_p = \left(\frac{2\beta\gamma^2 x^{2m}}{p}\right) = \left(\frac{2\gamma^2 x^{2m}}{p}\right)\left(\frac{\beta}{p}\right) = -1\,,$$

and therefore $\mathrm{inv}_p(\mathcal{A}(P_p)) = 1/2$. *Case II.* $(p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) + z \equiv 0 \pmod{p}$.

We see that $-z \equiv (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) \pmod{p}$, and hence it follows that

$$\begin{aligned}&(p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) - z \\ &\quad \equiv 2((p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta)) \equiv 2\beta\gamma^2 x^{2m} \not\equiv 0 \pmod{p}\,.\end{aligned}$$

Using Theorem 5.2.7 in [4], we deduce from (A4) that the local Hilbert symbol

$$\big(p, (p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta) - z\big)_p = \left(\frac{2\beta\gamma^2 x^{2m}}{p}\right) = \left(\frac{2\gamma^2 x^{2m}}{p}\right)\left(\frac{\beta}{p}\right) = -1\,.$$

Since $\mathcal{A}$ and $\mathcal{B}$ represent the same class in $\mathrm{Br}(\mathbb{Q}(\mathcal{C}))$, where $\mathcal{B}$ is the Azumaya algebra defined in Lemma 2.1, we deduce that $\mathrm{inv}_p(\mathcal{A}(P_p)) = 1/2$.

Therefore $\sum_l \mathrm{inv}_l \mathcal{A}(P_l) = 1/2$ for any adelic point $(P_l)_l \in \mathcal{C}(\mathbb{A}_\mathbb{Q})$. Hence $\mathcal{C}(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$. □

We now prove the main theorem in this section.

THEOREM 2.3. *We maintain the same notation and assumptions as in Theorem* 2.2. *Let* $\lambda = \gamma = 1$ *in Theorem* 2.2, *and let* d *be the integer defined by* (2) *with both of* λ *and* γ *replaced by* 1, *that is*, d *is of the form*

$$d = \alpha^m (p(\alpha+\beta))^{(k+1)n} + (-1)^{m+1}\beta^m (p\alpha + (p+1)\beta)^{(k+1)n}\,. \tag{12}$$

Set

$$q := \beta^2 + p(\alpha+\beta)^2\,. \tag{13}$$

Assume (A1)–(A6), *and* (S) *in Theorem* 2.2, *and assume further that the following is true.*

(A7) *let* l *be any odd prime dividing* q. *Then* $(k+1)n - m \not\equiv 0 \pmod{l}$.

Let $\mathcal{D}$ *be the smooth projective model of the affine curve defined by*

$$\mathcal{D} : z^2 = p(\alpha x^{2(k+1)n} + \beta)^2 + \big((p\alpha + (p+1)\beta)x^{2m} - p(\alpha+\beta)\big)^2\,. \tag{14}$$

Then $\mathcal{D}$ *is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction.*

REMARK 2.4. Note that condition (S) in Theorem 2.3 is equivalent to saying that the polynomial $P_{p,\alpha,\beta,1,1}(x) \in \mathbb{Q}[x]$ defined by

$$P_{p,\alpha,\beta,1,1}(x) = p(\alpha x^{2(k+1)n} + \beta)^2 + \big((p\alpha + (p+1)\beta)x^{2m} - p(\alpha+\beta)\big)^2$$

is separable.

REMARK 2.5. When $\lambda = 1$ and $\gamma = 1$, we see that $\gcd(\gamma, p) = \gcd(\lambda, p) = 1$, and (A5) is trivially true. Hence it suffices to only assume that (S), (A1)–(A4), (A6), and (A7) are true in Theorem 2.3.

REMARK 2.6. Substituting $\gamma = \lambda = 1$ into the defining equation (3) of $\mathcal{C}$, we see that (3) becomes the defining equation (14) of $\mathcal{D}$. Hence it follows from Theorem 2.2 and the assumptions in Theorem 2.3 that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$.

PROOF OF THEOREM 2.3. By Remark 2.6, $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$. Hence it suffices to prove that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$. Since $\mathcal{D}$ is a proper scheme over $\mathbb{Q}$, we know that

$$\mathcal{D}(\mathbb{A}_{\mathbb{Q}}) = \prod_{p \text{ primes}} \mathcal{D}(\mathbb{Q}_p)\,.$$

(For the proof of this fact, see, for example, Jahnel [8, Lemma 1.9, p.121].) Thus in order to prove that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$, one only needs to show that $\mathcal{D}(\mathbb{Q}_p) \neq \emptyset$ for all primes p including $p = \infty$, i.e., $\mathcal{D}$ is everywhere locally solvable. We consider the following cases:

Case 1. *l is an odd prime such that p is a square in $\mathbb{Q}_l^{\times}$.*

We see that the curve $\mathcal{D}_*$ defined by

$$\mathcal{D}_* : z^2 = p(\alpha x^{2(k+1)n} + \beta y^{2(k+1)n})^2 + y^{4(k+1)n-4m}\big((p\alpha + (p+1)\beta)x^{2m} - p(\alpha+\beta)y^{2m}\big)^2\,.$$

is an open subscheme of $\mathcal{D}$. One can check that the point $P_1 := (x : y : z) = (1 : 0 : \alpha\sqrt{p}) \in \mathcal{D}_*(\mathbb{Q}_l) \subset \mathcal{D}(\mathbb{Q}_l)$, and hence it follows that $\mathcal{D}$ is locally solvable at l.

Case 2. *l is an odd prime such that q is a square in $\mathbb{Q}_l^{\times}$.*

By the definition of q, we see that the point $P_2 := (x, z) = (1, \sqrt{q})$ lies on $\mathcal{D}$. Since $\sqrt{q} \in \mathbb{Q}_l^{\times}$, it follows that $P_2 \in \mathcal{D}(\mathbb{Q}_l)$.

Case 3. *l is an odd prime such that pq is a square in $\mathbb{Q}_l^{\times}$.*

We see that the point $P_3 := (x, z) = (0, \sqrt{pq}) \in \mathcal{D}(\mathbb{Q}_l)$, and thus $\mathcal{D}$ is locally solvable at l.

Case 4. *$l = 2$.*

By assumption, one knows that $p \equiv 1 \pmod 8$. Hence $\sqrt{p} \in \mathbb{Q}_2^{\times}$. Thus the point P_1 defined in *Case 1* belongs to $\mathcal{D}(\mathbb{Q}_2)$. Therefore $\mathcal{D}$ is locally solvable at 2.

Case 5. *$l = p$.*

By the definition of q, we see that

$$q = \beta^2 + p(\alpha+\beta)^2 \equiv \beta^2 \pmod p\,,$$

and hence q is a square in $\mathbb{Q}_p^\times$. Thus p is among the odd primes in *Case 2*, and therefore $P_2 \in \mathcal{D}(\mathbb{Q}_p)$.

Case 6. l is any odd prime such that l divides q.

If l divides α, then it follows from (A3) that l is a square in $\mathbb{F}_p^\times$, and hence we deduce from the quadratic reciprocity law that p is a square in $\mathbb{Q}_l^\times$. Thus the point P_1 defined in *Case 1* belongs to $\mathcal{D}(\mathbb{Q}_l)$, which proves that $\mathcal{D}$ is locally solvable at l.

Assume now that $\alpha \not\equiv 0 \pmod{l}$. We consider the following system of equations

$$\begin{cases} F(x,z) &= p(\alpha x^{2(k+1)n}+\beta)^2+((p\alpha+(p+1)\beta)x^{2m} \\ &\quad - p(\alpha+\beta))^2 - z^2 \equiv 0 \pmod{l} \\ \dfrac{\partial F}{\partial x}(x,z) &= 4(k+1)np\alpha x^{2(k+1)n-1}(\alpha x^{2(k+1)n}+\beta) \\ &\quad + 4m(p\alpha+(p+1)\beta)x^{2m-1}((p\alpha+(p+1)\beta)x^{2m} \\ &\quad - p(\alpha+\beta)) \not\equiv 0 \pmod{l}. \end{cases} \tag{15}$$

We see that

$$F(1,0) = q \equiv 0 \pmod{l}$$

and

$$\begin{aligned} \frac{\partial F}{\partial x}(1,0) &= 4(k+1)np\alpha(\alpha+\beta) + 4m(p\alpha+(p+1)\beta)\beta \\ &= 4\big(p(\alpha+\beta)(m\beta+(k+1)n\alpha)+m\beta^2\big). \end{aligned}$$

Since $q = \beta^2 + p(\alpha+\beta)^2 \equiv 0 \pmod{l}$, it follows that $\beta^2 \equiv -p(\alpha+\beta)^2 \pmod{l}$. Hence we deduce that

$$\begin{aligned} \frac{\partial F}{\partial x}(1,0) &\equiv 4\big(p(\alpha+\beta)(m\beta+(k+1)n\alpha) - mp(\alpha+\beta)^2\big) \\ &\equiv 4p\alpha(\alpha+\beta)((k+1)n-m) \pmod{l}. \end{aligned}$$

We prove that $4p\alpha(\alpha+\beta) \not\equiv 0 \pmod{l}$. By the assumption above, we know that $\alpha \not\equiv 0 \pmod{l}$. By the definition of q and (A2), we know that $q = \beta^2 + p(\alpha+\beta)^2 \equiv \beta^2 \not\equiv 0 \pmod{p}$, and hence it follows that p does not divide q. Thus we deduce that $p \not\equiv 0 \pmod{l}$. We assume that $\alpha+\beta \equiv 0 \pmod{l}$. Hence it follows from (13) that

$$\beta^2 \equiv \beta^2 + p(\alpha+\beta)^2 = q \equiv 0 \pmod{l},$$

and thus $\alpha \equiv (\alpha+\beta) - \beta \equiv 0 \pmod{l}$, contradiction. Therefore we have shown that $4p\alpha(\alpha+\beta) \not\equiv 0 \pmod{l}$. Furthermore, we see from (A7) that $(k+1)n - m \not\equiv 0 \pmod{l}$, and thus

$$\frac{\partial F}{\partial x}(1,0) \equiv 4p\alpha(\alpha+\beta)((k+1)n-m) \not\equiv 0 \pmod{l}.$$

Therefore we deduce that $(x, z) = (1, 0)$ is a solution to the system (15). By Hensel's lemma, we deduce that $\mathcal{D}$ is locally solvable at l.

Case 7. $l = \infty$.

Since $pq \geq 0$, we see that the point $P_3 = (x, z) = (0, \sqrt{pq}) \in \mathcal{D}(\mathbb{R})$. Hence $\mathcal{D}$ is locally solvable at ∞.

Therefore, by what we have shown, $\mathcal{D}$ is everywhere locally solvable, and hence our contention follows. □

EXAMPLE 2.7. Let $p = 17$, $(k, m, n) = (0, 1, 3)$, and let $(\alpha, \beta, \lambda, \gamma) = (1, 5, 1, 1)$. Then $d = 7186423$ is a prime such that d is a square in $\mathbb{F}_{17}^{\times}$. We see that $q = 637 = 7^2 \cdot 13$. We know that $(k+1)n - m = 2 \not\equiv 0 \pmod 7$ and $(k+1)n - m = 2 \not\equiv 0 \pmod{13}$. Thus (A7) holds. By computation, we easily see that (A1)–(A6) are true. On the other hand, we see that the polynomial $P_{17,1,5,1,1}(x) \in \mathbb{Q}[x]$ defined by

$$P_{17,1,5,1,1}(x) = 17(x^6 + 5)^2 + (107x^2 - 102)^2$$

is separable. Thus (S) holds.

Let $\mathcal{D}_{(17,1,5)}^{(0,1,3)}$ be the smooth projective model of the affine curve defined by

$$\mathcal{D}_{(17,1,5)}^{(0,1,3)} : z^2 = 17(x^6 + 5)^2 + (107x^2 - 102)^2 .$$

It then follows from Theorem 2.3 that $\mathcal{D}_{(17,1,5)}^{(0,1,3)}$ is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction.

3. The Hasse principle for certain forms

In this section, we will use the curves $\mathcal{D}$ in Theorem 2.3 to construct forms $\mathcal{X}$ of degree n with $n \equiv 0 \pmod 4$ that are counterexamples to the Hasse principle. The next theorem is the main result in this section.

THEOREM 3.1. *Let p be a prime such that $p \equiv 1 \pmod 8$. Let α, β be non-zero integers, and let d and q be the integers defined by* (12) *and* (13), *respectively. Let k, m, n be integers such that $k \geq 0$, $m \geq 1$ and $n \geq 1$. Assume that* (A1)–(A7), *and* (S) *in Theorem* 2.3 *are true. Let $(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8)$ be an octuple of non-negative integers, and let $\zeta \in \mathbb{Q}$ be a non-zero rational number. Assume further that the following are true*:

(C1) $2(k+1)n - 1 = (2n_1 + 1)n_2$ *and* $2n_1 + 1 = n_3 + n_4$.

(C2)

$$\begin{cases} n_1 \geq 2 \\ n_2, n_3, n_4, n_5, n_6, n_7 \geq 1 \\ n_8 \geq 0 , \end{cases} \tag{16}$$

and

$$\begin{cases} n_1 > n_5 \\ n_1 > n_6 \\ n_1 > n_7 + n_8 \\ n_5 > n_8 \\ n_6 > n_8\,. \end{cases} \tag{17}$$

(C3) $\zeta \in \mathbb{Z}_l$ *for any odd prime* l *dividing* q.

Let $(\Delta, \Psi, \Sigma, \Lambda) \in \mathbb{Q}^4$ *be the quadruple defined by*

$$\begin{cases} \Delta = \zeta \\ \Psi = -\alpha^{2(n_1-n_5)} p^{n_1-n_5} \zeta \\ \Sigma = -(pq)^{n_1-n_6} \zeta \\ \Lambda = q^{n_5-n_8} \left(\alpha^{2(n_1-n_5)} p^{n_1-n_5} + p^{n_1-n_6} q^{n_1-n_5} - q^{n_1-n_5}\right) \zeta\,, \end{cases} \tag{18}$$

and set

$$\begin{aligned} Q(x, y, z) := {} & x^{2n_1+1} - x^{n_3} y^{n_4} + y^{2n_1+1} + \Psi x^{2(n_1-n_5)} z^{2n_5+1} \\ & + \Sigma y^{2(n_1-n_6)} z^{2n_6+1} + \Lambda x^{2(n_1-n_7-n_8)} y^{2n_7} z^{2n_8+1} + \Delta z^{2n_1+1}. \end{aligned} \tag{19}$$

Let $\mathcal{X} \subset \mathbb{P}^2$ *be the form of degree* $4(k+1)n$ *defined by*

$$\begin{aligned} \mathcal{X} : (Q(x, y, z))^{2n_2} z^2 = {} & p(\alpha x^{2(k+1)n} + \beta y^{2(k+1)n})^2 \\ & + y^{4(k+1)n-4m}\left((p\alpha + (p+1)\beta)x^{2m} - p(\alpha+\beta)y^{2m}\right)^2. \end{aligned} \tag{20}$$

Then $\mathcal{X}$ *is a counterexample to the Hasse principle.*

REMARK 3.2.

(i) By (18), $\Lambda = -q^{n_5-n_8}\Psi - q^{n_6-n_8}\Sigma - q^{n_1-n_8}\Delta$.

(ii) Since $\zeta \neq 0$, we see from (18) that $\Delta\Psi\Sigma\Lambda \neq 0$.

PROOF. We first prove that $\mathcal{X}$ is everywhere locally solvable. It suffices to consider the following cases:

Case 1. l *is an odd prime such that* p *is a square in* $\mathbb{Q}_l^\times$.

Since $Q(1, 0, \alpha\sqrt{p}) = 1$, the point $P_1 = (x, y, z) = (1, 0, \alpha\sqrt{p})$ belongs to $\mathcal{X}(\mathbb{Q}_l)$, which proves that $\mathcal{X}$ is locally solvable at l.

Case 2. l *is an odd prime such that* q *is a square in* $\mathbb{Q}_l^\times$.

Since $Q(1, 1, \sqrt{q}) = 1$, the point $P_2 = (x, y, z) = (1, 1, \sqrt{q})$ belongs to $\mathcal{X}(\mathbb{Q}_l)$, which proves that $\mathcal{X}$ is locally solvable at l.

Case 3. l *is an odd prime such that* pq *is a square in* $\mathbb{Q}_l^\times$.

Since $Q(0, 1, \sqrt{pq}) = 1$, the point $P_3 = (x, y, z) = (0, 1, \sqrt{pq})$ belongs to $\mathcal{X}(\mathbb{Q}_l)$, which proves that $\mathcal{X}$ is locally solvable at l.

Case 4. $l = 2$.

By assumption, we know that $p \equiv 1 \pmod 8$, and hence $\sqrt{p} \in \mathbb{Q}_2^\times$. Thus the point P_1 defined in *Case 1* belongs to $\mathcal{X}(\mathbb{Q}_2)$. Therefore $\mathcal{X}$ is locally solvable at 2.

Case 5. $l = p$.

By the definition of q, we know that $q = \beta^2 + p(\alpha+\beta)^2 \equiv \beta^2 \pmod p$, and hence it follows that q is a square in $\mathbb{Q}_p^\times$. Thus p is among the odd primes in *Case 2*, and therefore the point P_2 in *Case 2* belongs to $\mathcal{X}(\mathbb{Q}_p)$.

Case 6. *l is any odd prime such that l divides q.*

If l divides α, then it follows from (A3) that l is a square in $\mathbb{F}_p^\times$, and hence we deduce from the quadratic reciprocity law that p is a square in $\mathbb{Q}_l^\times$. Thus the point P_1 in *Case 1* belongs to $\mathcal{X}(\mathbb{Q}_l)$, which proves that $\mathcal{X}$ is locally solvable at l.

Assume now that $\alpha \not\equiv 0 \pmod l$. Set

(21)
$$\begin{aligned} F(x,y,z) &= p(\alpha x^{2(k+1)n} + \beta y^{2(k+1)n})^2 \\ &\quad + y^{4(k+1)n-4m}\big((p\alpha + (p+1)\beta)x^{2m} - p(\alpha+\beta)y^{2m}\big)^2 - z^2\,(Q(x,y,z))^{2n_2}\,, \end{aligned}$$

and consider the system of equations defined by

$$\begin{cases} F(x,y,z) & \equiv 0 \pmod l \\ \dfrac{\partial F}{\partial x}(x,y,z) & \not\equiv 0 \pmod l\,. \end{cases} \tag{22}$$

By (C3), we know that $\zeta \in \mathbb{Z}_l$, and hence $Q(x,y,z) \in \mathbb{Z}_l[x,y,z]$. By (21), and since $q = \beta^2 + p(\alpha+\beta)^2$, we deduce that

$$F(1,1,0) = q \equiv 0 \pmod l\,. \tag{23}$$

We see that

$$\begin{aligned} \frac{\partial F}{\partial x}(x,y,z) &= 4(k+1)np\alpha x^{2(k+1)n-1}(\alpha x^{2(k+1)n} + \beta y^{2(k+1)n}) \\ &\quad + 4m(p\alpha + (p+1)\beta)x^{2m-1}y^{4(k+1)n-4m} \\ &\quad \times \big((p\alpha + (p+1)\beta)x^{2m} - p(\alpha+\beta)y^{2m}\big) \\ &\quad - z^2\left(2n_2\frac{\partial Q}{\partial x}(x,y,z)\,(Q(x,y,z))^{2n_2-1}\right)\,. \end{aligned} \tag{24}$$

Note that since $q = \beta^2 + p(\alpha+\beta)^2 \equiv 0 \pmod l$, it follows that $\beta^2 \equiv -p(\alpha+\beta)^2 \pmod l$. Therefore we deduce from (24) that

$$\begin{aligned} \frac{\partial F}{\partial x}(1,1,0) &\equiv 4\big(p(\alpha+\beta)(m\beta + (k+1)n\alpha) - mp(\alpha+\beta)^2\big) \\ &\equiv 4p\alpha(\alpha+\beta)((k+1)n - m) \pmod l\,. \end{aligned} \tag{25}$$

Using exactly the same arguments as in *Case 6* of the proof of Theorem 2.3, we know that $4p\alpha(\alpha+\beta) \not\equiv 0 \pmod{l}$. On the other hand, by (A7) in Theorem 2.3, $(k+1)n - m \not\equiv 0 \pmod{l}$. Thus it follows from (25) that

$$\frac{\partial F}{\partial x}(1,1,0) \not\equiv 0 \pmod{l}\,. \tag{26}$$

Therefore it follows from (23) and (26) that $(x, y, z) = (1, 1, 0)$ is a solution to the system (22). By Hensel's lemma, we deduce that $\mathcal{X}$ is locally solvable at l.

Case 7. $l = \infty$.

Since $\sqrt{p} \in \mathbb{R}$, we see that the point P_1 in *Case 1* belongs to $\mathcal{X}(\mathbb{R})$. Therefore $\mathcal{X}$ is locally solvable at ∞.

By what we have shown above, $\mathcal{X}$ is everywhere locally solvable.

We now prove that $\mathcal{X}$ has no rational points. Let $\mathcal{D}$ be the smooth projective model of the affine curve defined by (14) in Theorem 2.3, and let $\phi : \mathcal{X} \to \mathcal{D}$ be the rational map defined by

$$\begin{aligned} \phi : \mathcal{X} &\longrightarrow \mathcal{D} \\ (x : y : z) &\longmapsto \left(x : y : z(Q(x, y, z))^{n_2}\right)\,. \end{aligned}$$

If $x = y = z(Q(x, y, z))^{n_2} = 0$, then by (19), $z(\Delta z^{2n_1+1})^{n_2} = 0$. Since $\Delta = \zeta \neq 0$, we deduce that $z = 0$. Thus ϕ is *regular* at every point of $\mathcal{X}(\bar{\mathbb{Q}})$, and therefore ϕ is a $\mathbb{Q}$-morphism. Recall from Theorem 2.3 that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$. In particular, this implies that $\mathcal{D}(\mathbb{Q}) = \emptyset$, and thus $\mathcal{X}(\mathbb{Q}) = \emptyset$. □

4. Certain algebraic families of forms violating the Hasse principle

In this section, using Theorem 3.1 in Section 3, we will construct certain algebraic families of forms of degree n with $n \equiv 0 \pmod{4}$ that are counterexamples to the Hasse principle.

The next lemma shows the existence of certain rational functions over $\mathbb{Q}$ that only take values in $\cap_{l\in\mathbf{S}}\mathbb{Z}_l$ for a given finite set $\mathbf{S}$ of odd primes. Lemma 4.1 below is a special case of Lemma 4.2 in [6].

LEMMA 4.1. *Let* $\mathbf{S}$ *be a finite set of odd primes, and let* $\mathbb{Q}(T)$ *be the field of rational functions in the variable* T *over* $\mathbb{Q}$. *Then there exist infinitely many rational functions* $F(T) \in \mathbb{Q}(T)$ *that satisfy the following conditions*:

(i) $F(T_\star) \neq 0$ *for every rational number* $T_\star \in \mathbb{Q}$;
(ii) *for each odd prime* $l \in \mathbf{S}$, $F(T_\star)$ *belongs to* $\mathbb{Z}_l$ *for every rational number* $T_\star \in \mathbb{Q}$.

PROOF. By the Chinese Remainder Theorem, there exist infinitely many integers ε such that ε is a quadratic non-residue in $\mathbb{F}_l^\times$ for each $l \in \mathbf{S}$. Take such an integer ε, and define

$$F(T) = \frac{1}{T^2 - \varepsilon} \in \mathbb{Q}(T)\,.$$

Following the ideas in the proof of Lemma 4.2 in [6], one can show that $F(T)$ satisfies (i) and (ii) in Lemma 4.1. □

THEOREM 4.2. *Let p be a prime such that $p \equiv 1 \pmod 8$. Let k, m, n be integers such that $k \geq 0, m \geq 1$ and $n \geq 1$. Let α, β be non-zero integers, and let d and q be the integers defined by* (12) *and* (13), *respectively. Assume that* (A1)–(A7), *and* (S) *in Theorem* 2.3 *are true. Let $(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8)$ be an octuple of non-negative integers such that* (C1) *and* (C2) *in Theorem* 3.1 *hold. Then there are algebraic families of forms of degree $4(k+1)n$ that are counterexamples to the Hasse principle.*

PROOF. Set

$$\mathbf{S} = \{l \mid l \text{ is an odd prime dividing } q\}.$$

Applying Lemma 4.1 for the set $\mathbf{S}$, we deduce that there exist infinitely many rational functions $F(T)$ in $\mathbb{Q}(T)$ that satisfy the following conditions:

(i) $F(T_\star) \neq 0$ for every rational number $T_\star \in \mathbb{Q}$; and
(ii) for each odd prime $l \in \mathbf{S}$, $F(T_\star)$ belongs to $\mathbb{Z}_l$ for every rational number $T_\star \in \mathbb{Q}$.

Take such a rational function $F(T)$, and let $\Delta(T), \Psi(T), \Sigma(T), \Lambda(T)$ be rational functions in $\mathbb{Q}(T)$ defined by

$$\begin{aligned}
\Delta(T) &= F(T), \\
\Psi(T) &= -\alpha^{2(n_1-n_5)} p^{n_1-n_5} F(T), \\
\Sigma(T) &= -(pq)^{n_1-n_6} F(T), \\
\Lambda(T) &= q^{n_5-n_8}\big(\alpha^{2(n_1-n_5)} p^{n_1-n_5} + p^{n_1-n_6} q^{n_1-n_5} - q^{n_1-n_5}\big) F(T),
\end{aligned}$$

and set

$$\begin{aligned}
Q(x, y, z)(T) = {} & x^{2n_1+1} - x^{n_3} y^{n_4} + y^{2n_1+1} + \Psi(T) x^{2(n_1-n_5)} z^{2n_5+1} \\
& + \Sigma(T) y^{2(n_1-n_6)} z^{2n_6+1} + \Lambda(T) x^{2(n_1-n_7-n_8)} y^{2n_7} z^{2n_8+1} + \Delta(T) z^{2n_1+1}.
\end{aligned}$$

For each rational number $T_\star$, let $\mathcal{X}_{T_\star} \subset \mathbb{P}^2$ be the form of degree $4(k+1)n$ defined by

$$\begin{aligned}
\mathcal{X}_{T_\star} : (Q(x, y, z)(T_\star))^{2n_2} z^2 = {} & p(\alpha x^{2(k+1)n} + \beta y^{2(k+1)n})^2 \\
& + y^{4(k+1)n-4m}\big((p\alpha + (p+1)\beta) x^{2m} - p(\alpha+\beta) y^{2m}\big)^2.
\end{aligned}$$

Take an arbitrary rational number $T_\star \in \mathbb{Q}$. Since $F(T)$ satisfies (i) and (ii) above, the condition (C3) in Theorem 3.1 is satisfied with $F(T_\star)$ in the role of ζ. Applying Theorem 3.1 with $F(T_\star)$ in the role of ζ, we deduce that $\mathcal{X}_{T_\star}$ is a counterexample to the Hasse principle. Hence each member in the algebraic family $\big(\mathcal{X}_{T_\star}\big)_{T_\star \in \mathbb{Q}}$ is a counterexample to the Hasse principle, which completes our proof. □

REMARK 4.3.

(i) Note that Theorem 4.2 does not imply that for each integer $k \geq 0$, and each integer $n \geq 1$, there exists an algebraic family of forms of degree $4(k+1)n$ that are counterexamples to the Hasse principle.

(ii) Note that once one can choose integers $k \geq 0, m \geq 1, n \geq 1, \alpha \neq 0, \beta \neq 0$ for which conditions (A1)–(A7) and (S) are satisfied, it is not difficult to show the existence of the octuples of non-negative integers $(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8)$ that satisfy conditions (C1) and (C2) in Theorem 3.1. Thus Theorem 4.2 really means that for each prime $p \equiv 1 \pmod 8$, if one can choose integers $k \geq 0, m \geq 1, n \geq 1, \alpha \neq 0, \beta \neq 0$ for which conditions (A1)–(A7) and (S) are satisfied, then one can construct algebraic families of forms of degree $4(k+1)n$ that are counterexamples to the Hasse principle.

(iii) For a given prime $p \equiv 1 \pmod 8$, using the Chinese Remainder Theorem, and Dirichlet's theorem on primes in arithmetic progressions, it is not difficult to show that there are infinitely many tuples of integers (k, m, n, α, β) with $k \geq 0, m \geq 1, n \geq 1, \alpha \neq 0, \beta \neq 0$ for which conditions (A1)–(A7) are satisfied. The only difficulty is to show among those tuples, there exists at least one tuple that satisfies condition (S) in Lemma 2.1, which is equivalent to showing the existence of one tuple for which the polynomial $P_{p,\alpha,\beta,\lambda,\gamma}(x)$ is separable, where

$$P_{p,\alpha,\beta,\lambda,\gamma}(x) = p(\alpha\lambda^{2(k+1)}x^{2(k+1)n} + \beta)^2 + \big((p\alpha + (p+1)\beta)\gamma^2 x^{2m} - p(\alpha+\beta)\big)^2.$$

For sufficiently large integers k, m, n, it seems a non-trivial question to determine whether the polynomial $P_{p,\alpha,\beta,\lambda,\gamma}(x)$ is separable for a general couple of integers (α, β).

4.1. Examples of algebraic families of forms of degree $4n$ with n odd. In this subsection, we will construct an explicit non-constant algebraic family of forms of degree 12 that are counterexamples to the Hasse principle. Although we restrict ourself to constructing only one non-constant algebraic family of forms of degree 12, the method presented here can be easily extended to construct algebraic forms of degree $4n$ for other odd values of n.

Throughout this subsection, we maintain the same notation as in Theorem 2.3, Theorem 3.1 and Lemma 4.1.

EXAMPLE 4.4. We set $p = 17$, $k = 0$, and $m = 1$ as in Example 2.7. Let $n = 3$, and let

$$(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8) = (2, 1, 1, 4, 1, 1, 1, 0).$$

Let $(\alpha, \beta) = (1, 5)$. Then $d = 7186423$ is a prime such that d is a square in $\mathbb{F}_{17}^{\times}$. Thus (A6) holds. We see that $q = 637 = 7^2 \cdot 13$. We know that $(k+1)n - m = 2 \not\equiv 0 \pmod 7$ and $(k+1)n - m = 2 \not\equiv 0 \pmod{13}$. Thus (A7) holds. By computation, we easily see that

(A1)–(A5) are true. Furthermore the polynomial defined by

$$17(x^6+5)^2+(107x^2-102)^2 \in \mathbb{Q}[x]$$

is separable over $\mathbb{C}$, and thus condition (S) in Theorem 2.3 is satisfied. On the other hand, it is not difficult to check that conditions (C1), (C2) are satisfied.

Since $q = 637 = 7^2 \cdot 13$, we see that $\mathbf{S} = \{7, 13\}$. Set $\varepsilon = 5$, and define

$$F(T) := \frac{1}{T^2-5} \in \mathbb{Q}(T)\,.$$

For each rational number $T_\star \in \mathbb{Q}$, we see from Lemma 4.1 that $(C3)$ is satisfied with $F(T_\star)$ in the role of ζ.

Let $\Delta(T)$, $\Psi(T)$, $\Sigma(T)$, $\Lambda(T)$ be the rational functions defined by

$$\begin{aligned}
\Delta(T) &= F(T) = \frac{1}{T^2-5}\,,\\
\Psi(T) &= -\alpha^{2(n_1-n_5)}p^{n_1-n_5}F(T) = -\frac{17}{T^2-5}\,,\\
\Sigma(T) &= -(pq)^{n_1-n_6}F(T) = -\frac{10829}{T^2-5}\,,\\
\Lambda(T) &= q^{n_5-n_8}\left(\alpha^{2(n_1-n_5)}p^{n_1-n_5}+p^{n_1-n_6}q^{n_1-n_5}-q^{n_1-n_5}\right)F(T) = \frac{6503133}{T^2-5},
\end{aligned}$$

and let

$$\begin{aligned}
Q(x,y,z)(T) :=\ & x^5-xy^4+y^5-\frac{17}{T^2-5}x^2z^3-\frac{10829}{T^2-5}y^2z^3\\
&+\frac{6503133}{T^2-5}x^2y^2z+\frac{1}{T^2-5}z^5\,.
\end{aligned}$$

For each rational number $T_\star \in \mathbb{Q}$, let $\mathcal{X}^{(17)}_{(0,1,3),T_\star} \subset \mathbb{P}^2$ be the form of degree 12 defined by

$$\mathcal{X}^{(17)}_{(0,1,3),T_\star} : (Q(x,y,z)(T_\star))^2 z^2 = 17(x^6+5y^6)^2+y^8(107x^2-102y^2)^2\,.$$

Note that the defining equation of $\mathcal{X}^{(17)}_{(0,1,3),T_\star}$ can be written in the form

$$\begin{aligned}
\mathcal{X}^{(17)}_{(0,1,3),T_\star} :\ & \left(x^5-xy^4+y^5-\frac{17}{T_\star^2-5}x^2z^3-\frac{10829}{T_\star^2-5}y^2z^3\right.\\
&\left.+\frac{6503133}{T_\star^2-5}x^2y^2z+\frac{1}{T_\star^2-5}z^5\right)^2 z^2\\
=\ & 17(x^6+5y^6)^2+y^8(107x^2-102y^2)^2\,.
\end{aligned} \tag{27}$$

By Theorem 3.1, we deduce that each member in the *algebraic* family $\left(\mathcal{X}^{(17)}_{(0,1,3),T_\star}\right)_{T_\star\in\mathbb{Q}}$ is a counterexample to the Hasse principle.

We show that the algebraic family $\left(\mathcal{X}^{(17)}_{(0,1,3),T_\star}\right)_{T_\star\in\mathbb{Q}}$ is non-constant, i.e., there exist rational numbers $T_\star^{(1)}, T_\star^{(2)} \in \mathbb{Q}$ such that $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(1)}}$ and $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(2)}}$ are non-isomorphic. The latter can be proved if one can show the existence of rational numbers $T_\star^{(1)}, T_\star^{(2)} \in \mathbb{Q}$ such that

(i) both $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(1)}}$ and $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(2)}}$ are nonsingular projective curves of degree 12 and genus 55;

(ii) there exists a prime $\wp$ at which both $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(1)}}$ and $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(2)}}$ have good reduction, and the sets $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(1)}}(\mathbb{F}_\wp)$, $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(2)}}(\mathbb{F}_\wp)$ are different.

Set $T_\star^{(1)} = 0$, and $T_\star^{(2)} = 1$. Then $\mathcal{X}^{(17)}_{(0,1,3),0}$, and $\mathcal{X}^{(17)}_{(0,1,3),1}$ are the forms of degree 12 defined by

$$\begin{aligned}\mathcal{X}^{(17)}_{(0,1,3),0} : &\left(x^5 - xy^4 + y^5 + \frac{17}{5}x^2z^3 + \frac{10829}{5}y^2z^3 - \frac{6503133}{5}x^2y^2z - \frac{1}{5}z^5\right)^2 z^2\\ &= 17(x^6+5y^6)^2 + y^8(107x^2 - 102y^2)^2\,,\end{aligned}$$

and

$$\begin{aligned}\mathcal{X}^{(17)}_{(0,1,3),1} : &\left(x^5 - xy^4 + y^5 + \frac{17}{4}x^2z^3 + \frac{10829}{4}y^2z^3 - \frac{6503133}{4}x^2y^2z - \frac{1}{4}z^5\right)^2 z^2\\ &= 17(x^6+5y^6)^2 + y^8(107x^2 - 102y^2)^2\,.\end{aligned}$$

We know that both $\mathcal{X}^{(17)}_{(0,1,3),0}$, and $\mathcal{X}^{(17)}_{(0,1,3),1}$ are non-singular projective curves of degree 12 and genus 55; furthermore they have good reduction at $\wp = 11$.

By computation, the set of all points of $\mathcal{X}^{(17)}_{(0,1,3),0}$ over $\mathbb{F}_{11}$ is given by

$$\begin{aligned}\mathcal{X}^{(17)}_{(0,1,3),0}(\mathbb{F}_{11}) = \{&(0:1:1), (4:2:1), (0:3:1), (0:7:1), (8:7:1), (0:8:1),\\ &(6:8:1), (2:10:1)\}\,.\end{aligned}$$

The set of all points of $\mathcal{X}^{(17)}_{(0,1,3),1}$ over $\mathbb{F}_{11}$ is given by

$$\begin{aligned}\mathcal{X}^{(17)}_{(0,1,3),1}(\mathbb{F}_{11}) = \{&(0:3:1), (10:5:1), (10:6:1), (0:7:1), (3:7:1), (0:8:1), (5:8:1),\\ &(0:9:1), (7:9:1)\}\,.\end{aligned}$$

Hence

$$\mathcal{X}^{(17)}_{(0,1,3),0}(\mathbb{F}_{11}) \neq \mathcal{X}^{(17)}_{(0,1,3),1}(\mathbb{F}_{11})\,,$$

which proves that $\mathcal{X}^{(17)}_{(0,1,3),0}$, and $\mathcal{X}^{(17)}_{(0,1,3),1}$ are non-isomorphic. Thus the algebraic family $\left(\mathcal{X}^{(17)}_{(0,1,3),T_\star}\right)_{T_\star\in\mathbb{Q}}$ is non-constant.

REMARK 4.5. In order to find a prime $\wp$ at which both $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(1)}}$ and $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(2)}}$ have good reduction, and the sets $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(1)}}(\mathbb{F}_\wp)$, $\mathcal{X}^{(17)}_{(0,1,3),T_\star^{(2)}}(\mathbb{F}_\wp)$ are different, we used the computational algebra software MAGMA [3] to search for small primes $\wp$ satisfying these conditions.

4.2. Examples of algebraic families of forms of degree $4n$ with n even. In this subsection, we will show how to construct algebraic families of forms of degree $4n$ that are counterexamples to the Hasse principle, where n is an even integer such that $n \geq 6$. Throughout this subsection, we will keep the same notation as in Theorem 2.3, Theorem 3.1 and Lemma 4.1.

Fix $k = 0$, and let m be a positive integer. Throughout this subsection, assume that $n \geq 1$ is even. Let d be the integer defined by (12). Reducing d modulo p, we see that

$$d \equiv (-1)^{m+1}\beta^{n+m} \pmod{p},$$

and since $p \equiv 1 \pmod 8$, it follows that

$$\left(\frac{d}{p}\right) = \left(\frac{(-1)^{m+1}\beta^{n+m}}{p}\right) = \left(\frac{\beta^{n+m}}{p}\right). \tag{28}$$

Here $\left(\frac{\cdot}{\cdot}\right)$ denotes the Jacobi symbol. Note that in order to use Theorem 3.1 to produce algebraic forms of degree $4n$ that are counterexamples to the Hasse principle, we need to assume that conditions (A1)–(A7), and (S) are satisfied.

Assume now that (A1)–(A7), and (S) are satisfied. By (A4), we see that β is a quadratic non-residue in $\mathbb{F}_p^\times$. We contend that $n + m$ is even; otherwise, we deduce that β^{n+m} is a quadratic non-residue in $\mathbb{F}_p^\times$, and hence it follows from (28) that d is a quadratic non-residue in $\mathbb{F}_p^\times$. By (A6) and since $p \equiv 1 \pmod 8$, we know that d is a quadratic residue in $\mathbb{F}_p^\times$, which is a contradiction. Thus $n + m$ is an even integer, and therefore m is an even integer.

We contend that $n + m \equiv 0 \pmod 4$. Assume the contrary, i.e., $n + m = 2(2h + 1)$ for some integer h. By (12), and since m, n are even, we see that

$$\begin{aligned} d &= \alpha^m\big(p(\alpha+\beta)\big)^n - \beta^m\big(p\alpha + (p+1)\beta\big)^n \\ &= \big(\alpha^{m/2}\big(p(\alpha+\beta)\big)^{n/2} + \beta^{m/2}\big(p\alpha + (p+1)\beta\big)^{n/2}\big) \\ &\quad \times \big(\alpha^{m/2}\big(p(\alpha+\beta)\big)^{n/2} - \beta^{m/2}\big(p\alpha + (p+1)\beta\big)^{n/2}\big). \end{aligned}$$

By (A6), and since 2 is quadratic residue in $\mathbb{F}_p^\times$, d_+ is a quadratic residue in $\mathbb{F}_p^\times$, where

$$d_+ = \alpha^{m/2}(p(\alpha+\beta))^{n/2} + \beta^{m/2}(p\alpha + (p+1)\beta)^{n/2}.$$

On the other hand, reducing d_+ modulo p shows that

$$d_+ \equiv \beta^{(n+m)/2} = \beta^{2h+1} \pmod{p}.$$

Since β is a quadratic non-residue, it follows from the last congruence that d_+ is not a square in $\mathbb{F}_p^\times$, which is a contradiction. Therefore $n + m \equiv 0 \pmod 4$.

We contend that $n \geq 6$ and $m \geq 2$. Indeed, (A1) implies that $n > m \geq 1$. Since m, n are even, $m \geq 2$ and $n \geq 4$. If $n = 4$, then $m = 2$. Thus $n + m = 6 \not\equiv 0 \pmod 4$, which is a contradiction. Therefore m, n are even integers such that $n \geq 6$, and $m \geq 2$.

For the rest of this subsection, assume further that $m = n - 4 \geq 2$. With this choice of n and m, $n - m = 4 \not\equiv 0 \pmod l$ for any odd prime l dividing q. Therefore (A7) is trivially satisfied.

In order to use Theorem 3.1 to produce algebraic families of forms of degree $4n$ for an even integer $n \geq 6$ that are counterexamples to the Hasse principle, it suffices to find couples (α, β) such that (A2), (A3), (A4), and (S) hold, and such that $|d_+|$ and $|d_-|$ are primes, where $|\cdot|$ is the usual absolute value, and

$$d_+ = \alpha^{m/2}(p(\alpha+\beta))^{n/2} + \beta^{m/2}(p\alpha + (p+1)\beta)^{n/2},$$
$$d_- = \alpha^{m/2}(p(\alpha+\beta))^{n/2} - \beta^{m/2}(p\alpha + (p+1)\beta)^{n/2}.$$

With this choice of d_+, d_-, we contend that (A6) is satisfied. Indeed, reducing d_+ and d_- modulo p, we see that

$$d_+ \equiv \beta^{(n+m)/2} \pmod p,$$
$$d_- \equiv -\beta^{(n+m)/2} \pmod p.$$

Since $(n + m)/2$ is even and -1 is a square in $\mathbb{F}_p^\times$, d_+ and d_- are quadratic residues in $\mathbb{F}_p^\times$. Since $d = d_+d_-$, (A6) is satisfied.

Once we can obtain quadruples (α, β, d, q) that satisfy (A1)–(A7), and (S), we can follow Theorem 3.1 and Lemma 4.1 to construct algebraic families of forms of degree $4n$ for an even integer $n \geq 6$ that are counterexamples to the Hasse principle. As an illustration, we will construct a non-constant algebraic family of forms of degree 24 such that each member in the algebraic family is a counterexample to the Hasse principle.

EXAMPLE 4.6. Let $p = 17, k = 0, m = 2$, and $n = 6$, and set

$$(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8) = (5, 1, 1, 10, 4, 4, 1, 3).$$

Let $(\alpha, \beta) = (1, 20)$. Then $d_+ = 1117151953$ and $d_- = -1026153367$ satisfy the following:

(i) $|d_+| = 1117151953, |d_-| = 1026153367$ are primes;
(ii) d_+ and d_- are squares in $\mathbb{F}_{17}^\times$.

Since $d = d_+d_- = -1146369238021575751$, (A6) is satisfied.

We see that $q = 7897 = 53 \cdot 149$. We know that $(k + 1)n - m = 4 \not\equiv 0 \pmod{53}$ and $(k + 1)n - m = 4 \not\equiv 0 \pmod{149}$. Thus (A7) holds. By computation, we easily see that (A1)–(A5) are true. Furthermore the polynomial defined by

$$17(x^{12} + 20)^2 + (377x^4 - 357)^2 \in \mathbb{Q}[x]$$

is separable over $\mathbb{C}$, and thus (S) is satisfied. On the other hand, it is easy to see that (C1), (C2) hold.

Since $q = 7897 = 53 \cdot 149$, $\mathbf{S} = \{53, 149\}$. Set $\varepsilon = 3$. Following Lemma 4.1, one obtains the rational function $F(T) \in \mathbb{Q}(T)$ defined by

$$F(T) = \frac{1}{T^2 - 3} \in \mathbb{Q}(T)\,.$$

For each $T_\star \in \mathbb{Q}$, it follows from Lemma 4.1 that (C3) is satisfied with $F(T_\star)$ in the role of ζ. Let $\Delta(T)$, $\Psi(T)$, $\Sigma(T)$, $\Lambda(T)$ be the rational functions defined by

$$\Delta(T) = F(T) = \frac{1}{T^2 - 3}\,,$$

$$\Psi(T) = -\alpha^{2(n_1-n_5)} p^{n_1-n_5} F(T) = -\frac{17}{T^2 - 3}\,,$$

$$\Sigma(T) = -(pq)^{n_1-n_6} F(T) = -\frac{134249}{T^2 - 3},$$

$$\Lambda(T) = q^{n_5-n_8}\left(\alpha^{2(n_1-n_5)} p^{n_1-n_5} + p^{n_1-n_6} q^{n_1-n_5} - q^{n_1-n_5}\right) F(T) = \frac{997935993}{T^2 - 3}\,.$$

Set

$$Q(x, y, z)(T) := x^{11} - xy^{10} + y^{11} - \frac{17}{T^2 - 3}x^2z^9 - \frac{134249}{T^2 - 3}y^2z^9 + \frac{997935993}{T^2 - 3}x^2y^2z^7 + \frac{1}{T^2 - 3}z^{11}\,.$$

For each $T_\star \in \mathbb{Q}$, let $\mathcal{X}^{(17)}_{(0,2,6),T_\star} \subset \mathbb{P}^2$ be the form of degree 24 defined by

$$\mathcal{X}^{(17)}_{(0,2,6),T_\star} : (Q(x, y, z)(T_\star))^2 z^2 = 17(x^{12} + 20y^{12})^2 + y^{16}(377x^4 - 357y^4)^2\,.$$

By Theorem 3.1, each member in the algebraic family $\left(\mathcal{X}^{(17)}_{(0,2,6),T_\star}\right)_{T_\star\in\mathbb{Q}}$ is a counterexample to the Hasse principle.

We show that the algebraic family $\left(\mathcal{X}^{(17)}_{(0,2,6),T_\star}\right)_{T_\star\in\mathbb{Q}}$ is non-constant, i.e., there exist rational numbers $T_\star^{(1)}, T_\star^{(2)} \in \mathbb{Q}$ such that $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(1)}}$ and $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(2)}}$ are non-isomorphic. The latter can be proved if one can show the existence of rational numbers $T_\star^{(1)}, T_\star^{(2)} \in \mathbb{Q}$ such that

(i) both $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(1)}}$ and $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(2)}}$ are nonsingular projective curves of degree 12 and genus 55;

(ii) there exists a prime $\wp$ at which both $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(1)}}$ and $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(2)}}$ have good reduction, and the sets $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(1)}}(\mathbb{F}_\wp)$, $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(2)}}(\mathbb{F}_\wp)$ are different.

Set $T_\star^{(1)} = 0$ and $T_\star^{(2)} = 2$. Then $\mathcal{X}^{(17)}_{(0,2,6),0}$ and $\mathcal{X}^{(17)}_{(0,2,6),2}$ are the forms of degree 24 defined by

$$\mathcal{X}^{(17)}_{(0,2,6),0} : \left(x^{11} - xy^{10} + y^{11} + \frac{17}{3}x^2z^9 + \frac{134249}{3}y^2z^9 - 332645331x^2y^2z^7 - \frac{1}{3}z^{11}\right)^2 z^2$$
$$= 17(x^{12} + 20y^{12})^2 + y^{16}(377x^4 - 357y^4)^2\,,$$

and

$$\mathcal{X}^{(17)}_{(0,2,6),2} : (x^{11} - xy^{10} + y^{11} - 17x^2z^9 - 134249y^2z^9 + 997935993x^2y^2z^7 + z^{11})^2 z^2$$
$$= 17(x^{12} + 20y^{12})^2 + y^{16}(377x^4 - 357y^4)^2\,,$$

We know that both $\mathcal{X}^{(17)}_{(0,2,6),0}$ and $\mathcal{X}^{(17)}_{(0,2,6),2}$ are nonsingular projective curves of degree 24 and genus 253; furthermore they have good reduction at $\wp = 11$.

By computation, the points $(0 : 3 : 1)$, $(5 : 4 : 1)$, $(6 : 4 : 1)$, $(0 : 8 : 1)$, $(5 : 8 : 1)$, $(6 : 8 : 1)$, $(0 : 10 : 1)$, $(2 : 10 : 1)$, $(9 : 10 : 1)$ are all the points of $\mathcal{X}^{(17)}_{(0,2,6),0}$ over $\mathbb{F}_{11}$. On the other hand, the set of points of $\mathcal{X}^{(17)}_{(0,2,6),2}$ over $\mathbb{F}_{11}$ consists of the points $(0 : 2 : 1)$, $(3 : 2 : 1)$, $(8 : 2 : 1)$, $(0 : 3 : 1)$, $(0 : 4 : 1)$, $(1 : 5 : 1)$, $(10 : 5 : 1)$, $(0 : 8 : 1)$, $(1 : 8 : 1)$, $(10 : 8 : 1)$. Thus

$$\mathcal{X}^{(17)}_{(0,2,6),0}(\mathbb{F}_{11}) \neq \mathcal{X}^{(17)}_{(0,2,6),2}(\mathbb{F}_{11})\,,$$

which proves that the algebraic family $\left(\mathcal{X}^{(17)}_{(0,2,6),T_\star}\right)_{T_\star\in\mathbb{Q}}$ is non-constant.

REMARK 4.7. In order to find a prime $\wp$ at which both $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(1)}}$ and $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(2)}}$ have good reduction, and the sets $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(1)}}(\mathbb{F}_\wp)$, $\mathcal{X}^{(17)}_{(0,2,6),T_\star^{(2)}}(\mathbb{F}_\wp)$ are different, we used the computational algebra software MAGMA [3] to search for small primes $\wp$ satisfying these conditions.

ACKNOWLEDGEMENTS. I am extremely grateful to the referee for reading my paper very carefully, and giving many very useful comments that greatly help improve the exposition of my paper. The computations in this paper were carried out using the computational algebra software MAGMA [3].

References

[1] M. BHARGAVA, Most hyperelliptic curves over $\mathbb{Q}$ have no rational points, Preprint (2013). Available at http://arxiv.org/pdf/1308.0395.pdf.

[2] M. BHARGAVA, A positive proportion of plane cubics fail the Hasse principle, Preprint (2014). Available at http://arxiv.org/pdf/1402.1131v1.pdf.

[3] W. BOSMA, J. CANNON and C. PLAYOUST, The Magma algebra system. I. The user language, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[4] H. COHEN, *Number Theory, Volume I: Tools and Diophantine equations*, Graduate Texts in Math. **239**, Springer-Verlag (2007).

[5] N. N. DONG QUAN, On the Hasse principle for certain quartic hypersurfaces, Proc. Amer. Math. Soc. **139** (2011), no. 12, 4293–4305.

[6] N. N. DONG QUAN, The Hasse principle for certain hyperelliptic curves and forms, Quarterly Journal of Mathematics **64** (2013), no. 1, 253–268.

[7] M. FUJIWARA and M. SUDO, Some forms of odd degree for which the Hasse principle fails, Pacific J. Math. **67** (1976), no. 1, 161–169.

[8] J. JAHNEL, *Brauer groups, Tamagawa measures, and rational points on algebraic varieties*, Mathematical Surveys and Monographs, **198**, American Mathematical Society, Providence, RI, 2014.

[9] B. POONEN, An explicit family of genus-one curves violating the Hasse principle, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 263–274.

[10] E. S. SELMER, The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362.

Present Address:
DEPARTMENT OF APPLIED AND COMPUTATIONAL MATHEMATICS AND STATISTICS,
UNIVERSITY OF NOTRE DAME,
NOTRE DAME, INDIANA 46556, USA.
e-mail: dongquan.ngoc.nguyen@nd.edu