The Brauer-Manin Obstruction and Cyclic Algebras

Thomas Wright

Abstract
Borrowing from a classical construction for counterexamples to the Hasse principle, we show that for a certain family of affine varieties which do not satisfy the Hasse principle, the Brauer-Manin obstruction is not satisfied. The approach is elementary and requires little algebraic geometry.

1. Introduction
Questions about the veracity of the Hasse Principle have been a major focus of number theorists and algebraic geometers alike for a number of years. Recently, questions have focused on the applicability of the Brauer-Manin obstruction to various counterexamples to the Hasse Principle. It is this question which we address in the current paper.

Recall that the Hasse Principle is the idea that a variety which has solutions everywhere locally has solutions globally as well. We begin with a construction from [3, p. 72] which violates the Hasse Principle:

\[ V : (x_1^2 + x_2^2 + \ldots + x_n^2)^{k} - 2(y_0^2 + y_1^2 + \ldots y_n^2)^2 = 0. \]

This equation has solutions in every local field \( \mathbb{Q}_p \) (including \( \mathbb{Q}_\infty = \mathbb{R} \)), but it does not have solutions in \( \mathbb{Q} \).

Although it has not appeared explicitly in literature, it is obvious that this can be generalized to

\[ V : (x_1^2 + x_2^2 + \ldots + x_n^2)^{k} - a(y_0^2 + y_1^2 + \ldots y_n^2)^k = 0 \]

if \( a \in \mathbb{N} \) is not a \( k \)-th power, or, indeed, to any

\[ V : X^k - aY^k = 0 \]

where \( a \) is not a \( k \)-th power, \( X \) is a positive definite form in \( \mathbb{Q}[x_1, \ldots, x_n] \) which represents every integer primitively (i.e. not all of the \( x_i \) have a common factor) and \( Y \in \mathbb{Q}[y_1, \ldots, y_l] \) is zero only if all of the \( y_i \) are zero. Note that this construction can create either a projective or affine variety; moreover, the construction provides counterexamples to the Hasse principle of arbitrary even degree and arbitrary number of variables, provided the former is \( \geq 4 \) and the latter is \( \geq 6 \).

For our study of the Brauer-Manin obstruction, we consider the affine variety given by

\[ V : (x_1^2 + x_2^2 + \ldots + x_n^2 + 1)^2 - ay_0^2 = 0, \]

where \( a \in \mathbb{N} \) is not a square. We show that, under certain assumptions, \( V \) does not have the Brauer-Manin obstruction.

Recent work on the Hasse Principle has focused largely on algebraic geometric techniques. This paper, by contrast, approaches the problem from a largely number-theoretic perspective with minimal algebraic geometry. In particular, we use the fact that an element in the Brauer group of \( \mathbb{Q}_p \) must be a cyclic algebra generated by some \( u \in \mathbb{Q}_p^\times \). As such, we construct the

2000 Mathematics Subject Classification Primary 11S45; Secondary 14G05.
pre-image of this algebra under a certain mapping; subsequently, we show that, under this same mapping, this pre-image maps to an element that is not in the Brauer group, thereby deriving a contradiction. In section 4, we use this to prove the following:

**Theorem 4.1.** Let $V$ be as above. Then $V$ does not satisfy the Brauer-Manin obstruction.

2. Background: The Brauer-Manin Obstruction

It was Manin’s observation that many of the known examples of the failure of the Hasse principle can be realized by examining the Brauer groups coming from these varieties. In particular, for a variety $V$, we have the following commutative diagram:

$$
\begin{array}{ccc}
V(\mathbb{Q}) & \xrightarrow{\cdot_v A} & V(\mathbb{Q}_v) \\
\downarrow^{ev_A} & & \downarrow^{ev_A} \\
0 & \longrightarrow & Br(\mathbb{Q}) \\
& & \oplus_v Br(\mathbb{Q}_v) \\
& & \xrightarrow{i} \mathbb{Q}/\mathbb{Z} \\
& & \longrightarrow 0
\end{array}
$$

where $Br$ is the Brauer group, $A$ is an algebra in $Br(V)$, and, for $z \in V(k)$, $ev_A(z)$ is the map sending $A$ to an algebra in $Br(k)$ by sending $x_i$ to $z_i$. Note that the bottom row is exact, and hence $i$ is the canonical homomorphism (generally referred to as the invariant map).

Now, consider the set

$$V(\mathbb{Q}_k)^{Br} = \{ z \in V(\mathbb{Q}_k) | i(ev_A(z)) = 1 \ \forall \ A \in Br(V) \}.$$  

Let $z \in V(\mathbb{Q}_k)$ be in the image of $V(\mathbb{Q})$. Then, by the commutativity of the diagram, $z \in V(\mathbb{Q}_k)^{Br}$. So

$$V(\mathbb{Q}) \subseteq V(\mathbb{Q}_k)^{Br} \subseteq V(\mathbb{Q}_k).$$

If $V$ violates the Hasse principle, it is often because $V(\mathbb{Q}_k) \neq \emptyset$ but $V(\mathbb{Q}_k)^{Br} = \emptyset$. This is known as the Brauer-Manin obstruction to the Hasse Principle.

3. Background: Cyclic Algebras

In order to understand whether or not our examples satisfy the Brauer-Manin obstruction from a number-theoretic perspective, we require a well-known result about the structure of central simple algebras over a local field.

Define a cyclic algebra over $K$ as follows. Let $L$ be a cyclic extension of $K$ such that $[L:K] = m$, and let $\sigma$ be a generator for the Galois group $Gal(L/K)$. Moreover, let $u \in K^\times$ and let $b$ be some element with the defining relations

$$b^m = u,$$

$$xb = bx^\sigma$$

for $x \in L$.

The $K$-algebra generated by $L$, $u$, and $\sigma$ is called a cyclic algebra, and is often denoted by $(L|K,u,\sigma)$ [11].

As it turns out, these play an extremely important role in Brauer groups of both local fields and number fields. We discuss the former here:

**Brauer Groups of Local Fields.** Let $A \in Br(\mathbb{Q}_p)$. Then $A$ is a central simple algebra over $\mathbb{Q}_p$. Moreover, $A$ is a cyclic algebra of dimension $m^2$ over $\mathbb{Q}_p$.

**Proof.** See [10, p. 226]
4. The Brauer-Manin Obstruction for $V$

We would like to use the language of cyclic algebras to talk about the Brauer-Manin obstruction. The ultimate goal, of course, is the following theorem:

**Theorem 4.1.** Let

$$V : (x_1^2 + x_2^2 + \ldots + x_{n-1}^2 + 1)^2 - ay_0^2 = 0$$

be an affine variety over $Q$. Then $V$ does not satisfy the Brauer-Manin obstruction.

We begin with the aforementioned variety. Clearly, we can assume that $a$ is square-free (otherwise, if $a = a's^2$, we replace $y_0$ with $y_0s$ and proceed with $a'$ instead of $a$). We wish to show that, under the evaluation map, elements in $V(Q_A)$ map to elements in $Br(Q_p)$ contained in the image of $Br(Q)$. It follows, then, that the Brauer-Manin obstruction does not apply because $i(ev_A(z))$ would equal 1 for every $z \in V(Q_A)$ and $A \in Br(V)$.

First, since $V$ is an affine variety, we know that $Br(V)$ is the ring of Azumaya algebras over

$$R = \frac{Q[y_0, x_1, x_2, \ldots, x_{n-1}]}{< (x_1^2 + x_2^2 + \ldots + x_{n-1}^2 + 1)^2 - ay_0^2>}.$$ 

Let $b \in A \in Br(V)$ be an element in an algebra $A$ over $R$ such that $b$ is not in the base ring. Since the algebra is finitely generated, there exists a minimal polynomial

$$a_m b^n + a_{m-1} b^{n-1} + \ldots + a_1 b + a_0 = 0$$

where the $a_i \in A$ are such that $a_i$ has no $b$-component for each $i$. In particular, since the algebra must be free, $a_n$ must be in $Q$; otherwise, $b^m$ is a torsion element.

Now, we know by the statement about Brauer groups for local fields that any element of the Brauer group over $Q_p$ must be cyclic, i.e. after the evaluation map, if $b$ maps to $b'$, the minimal polynomial for $b'$ must be $(b')^m = u$. So all of the $a_i$ must map to zero except for $a_n$, which is a rational number, and $a_0$, which maps to $u$. We claim that this implies $a_0$ is a constant polynomial (i.e. $a_0 \in Q$). This means that the evaluation map sends $a_0$ to the same rational number $u$ for every $p$. From this, it follows that $ev_A(z)$ is in the image of $Br(Q)$, and hence the invariant map goes to 1 for every $A$ and $z$.

5. A Proof that $a_0 \in Q$

Here, we prove that $a_0 \in Q$. Specifically, we show that, if $a_0 \not\in Q$ then there exists a point $z \in V(Q_A)$ and a $p$ such that such that $a_0$ evaluates to zero in $Q_p$. From this, since we know that an algebra over $Q_p$ must be cyclic, we have that

$$ev_A(z) : a_0 b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0 \mapsto a_0 (b')^n,$$

which means that $(b')^n = 0$. Hence, the algebra $ev_z(A)$ has a non-trivial ideal given by $b'[ev_z(A)]$, contradicting the fact that $ev_z(A)$ is a central simple algebra. First, however, we show that if $f$ and $g$ are non-constant polynomials, there exists a $p_0$ such that $f$ and $g$ both have roots in $Q_{p_0}$. In fact, we prove the much stronger result that there are infinitely many such $p_0$. We will apply this later by letting $f$ be a polynomial related to the minimal polynomial of $b$ given above and letting $g$ be the minimal polynomial of $\sqrt{a}$.

**Lemma 5.1.** For all monic non-constant $f, g \in Z[x] \subset Z_p[x]$ with respective degrees $m, n$, there exist infinitely many primes $p$ such that the product $f \cdot g(x)$ factors into linear terms in $Z_p[x]$. In particular, $f$ and $g$ will each have roots in $Z_p$. 

Proof. This follows from applying the theorem of Frobenius in [14, p. 31] to the polynomial $f \cdot g(x)$. □

We now apply this to prove Theorem 4.1.

**Theorem 5.2.** For a non-constant $a_0$, $a_0$ maps to 0 for some $p$.

Proof. As stated before, we know that $Br(V) = Br(R)$, where $R$ is as defined previously. Since $g_0^* \in \mathbb{Q}(x_1, ..., x_{n-1})$ and $a_0 \in R$ (since $a_0$ is assumed to be in the base ring), this means that $a_0$ can be written as

$$a_0 = c_0 + c_1 y_0$$

for $c_i \in \mathbb{Q}(x_1, ..., x_{n-1})$, and for any point on $V$, we have

$$y_0 = \pm \frac{x_1^2 + \cdots + x_{n-1}^2 + 1}{\sqrt{a}}.$$ 

So

$$a_0 = c_0 \pm c_1 \frac{x_1^2 + \cdots + x_{n-1}^2 + 1}{\sqrt{a}}.$$ 

Now, consider the equation

$$c_0^2 - \frac{1}{\alpha} c_1^2 (x_1^2 + \cdots + x_{n-1}^2 + 1)^2 = 0.$$ 

We can assume that either $c_0$ is not a constant or $c_1$ is not zero (or both); otherwise, $a_0 \in \mathbb{Q}$. This means that the left-hand side of this equation is not a non-zero constant. Choose an $x_i$ which appears in this expression on the left hand side; WLOG, we will assume that this is $x_1$. Then we can rewrite the left side as a polynomial in $x_1$ over the ring $\mathbb{Q}[x_1, ..., x_{n-1}]$, i.e.

$$c_0^2 - \frac{1}{\alpha} c_1^2 (x_1^2 + \cdots + x_{n-1}^2 + 1)^2 = d_m x_1^m + d_{m-1} x_1^{m-1} + \cdots + d_1 x_1 + d_0,$$

where the $d_i \in \mathbb{Q}[x_1, ..., x_{n-1}]$. Since $d_m = d_m(x_2, ..., x_{n-1})$ is not constantly zero, there exist $(z_2, ..., z_{n-1}) \in \mathbb{Q}^{n-2}$ such that $d_m(z_2, ..., z_{n-1})$ is not zero (otherwise, there exists a non-zero affine variety which is everywhere zero in $\mathbb{A}_\mathbb{Q}^{n-2}$, which is impossible). If we plug in these $z_i$ for the various $x_i$, we have

$$d_m' x_1^m + d_{m-1}' x_1^{m-1} + \cdots + d_1' x_1 + d_0',$$

where each $d_i' \in \mathbb{Q}$. We will assume that these $d_i'$ are integers (if not, we can multiply through by the greatest common denominator, since we will set this equation equal to zero). Making the substitution $x_1' = \frac{x_1}{d_m}$ and multiplying the above through by $(d_m')^{m-1}$, we have that setting the above equal to zero will be the same as setting

$$(x_1')^m + d_{m-1}'(x_1')^{m-1} + \cdots + d_1' x_1 + d_0'$$

equal to zero. Call the above polynomial $f(x_1')$.

From Lemma 5.1, there exists a $p_0$ such that the equations

$$f(x_1') = 0, \quad g(y) = y^2 - a = 0$$

have solutions in $\mathbb{Q}_{p_0}$, which means that $\sqrt{a} \in \mathbb{Q}_{p_0}$. Let $z_1 \in \mathbb{Q}_{p_0}$ be a solution such that $f(z_1) = 0$. Since $f(x_1')$ was a polynomial derived from

$$c_0^2 - \frac{1}{\alpha} c_1^2 (x_1^2 + \cdots + x_{n-1}^2 + 1)^2,$$
this shows that the equation
\[ c_0^2 = \frac{1}{a} c_1^2 (x_1^2 + \ldots + x_{n-1}^2 + 1)^2 \]
has a solution in \( \mathbb{Q}_{p_0} \) given by \((z_1, z_2, \ldots, z_{n-1}, \pm \frac{x_1^2 + \ldots + x_{n-1}^2 + 1}{\sqrt{a}})\). This means that
\[ c_0 = \mp c_1 \frac{x_1^2 + \ldots + x_{n-1}^2 + 1}{\sqrt{a}} = -c_1 y_0, \]
or
\[ c_0 + c_1 y_0 = 0 \]
has the same solution. Thus, for the point \((z_1, z_2, \ldots, z_{n-1}, \pm \frac{x_1^2 + \ldots + x_{n-1}^2 + 1}{\sqrt{a}})\), we have that \(a_0\) maps to 0. But then \(ev_A((z_1, z_2, \ldots, z_{n-1}, \pm \frac{x_1^2 + \ldots + x_{n-1}^2 + 1}{\sqrt{a}}))\) is a non-simple algebra, contradicting the fact that it is contained in the Brauer group of \( \mathbb{Q}_p \). Therefore, \(a_0\) must be in \( \mathbb{Q} \), which means that \(ev_A(z)\) is in the image of \( Br(\mathbb{Q}) \) for any \( z \). So \( i(ev_A(z)) = 1 \) for every \( z \) and every \( A \), proving Theorem 5.2 and, consequently, Theorem 4.1.

References
2. B.J. BIRCH, 'Homogeneous forms of odd degree in a large number of variables', Mathematische Annalen, 4 (1957), 102-105.

Thomas Wright
Department of Mathematics
Johns Hopkins University
3400 North Charles St.
Baltimore, MD 21218
USA
wright@math.jhu.edu