EXPERIMENTS WITH THE TRANSCENDENTAL BRAUER-MANIN OBSTRUCTION

ANDREAS-STEPHAN ELSENHANS AND JÖRG JAHNEL

Abstract. We report on our experiments and theoretical investigations concerning weak approximation and the transcendental Brauer-Manin obstruction for special Kummer surfaces.

1. Introduction

1.1. Consider a projective variety S over the field $\mathbb{Q}$ of rational numbers. It is said that S fulfills weak approximation when the following is true. For every finite set $\{p_1, \ldots, p_l\}$ of prime numbers and every vector

$$(x_0, x_1, \ldots, x_l) \in S(\mathbb{R}) \times S(\mathbb{Q}_{p_1}) \times \cdots \times S(\mathbb{Q}_{p_l}),$$

there exists a sequence of $\mathbb{Q}$-rational points that simultaneously converges versus x_i in the p_i-adic topology for $i = 1, \ldots, l$ and versus x_0 with respect to the real topology. In a more formal language, this means that the set $S(\mathbb{Q})$ of the rational points on S is dense in the set $S(\mathbb{A}_\mathbb{Q})$ of all adelic points.

Even for Fano varieties, which are generally expected to have many rational points, weak approximation is not always fulfilled. Popular counterexamples are due to Sir Peter Swinnerton-Dyer [SD], L. J. Mordell [Mo], J. W. S. Cassels and M. J. T. Guy [CG], and many others.

For varieties of intermediate type, e.g. $K3$ surfaces, the situation is yet more obscure. In fact, to prove the much weaker statement that $\#S(\mathbb{Q}) = \infty$ is usually a formidable task in its own [LKL]. It seems therefore that proving weak approximation, even for a single surface, is presently out of reach and that experiments are asked for.

1.2. To test weak approximation experimentally is, however, an ill-posed problem, at least from the strictly formal point of view. The reason is that weak approximation is not a finite phenomenon. It is strongly infinite in nature.

An interesting situation occurs when a certain "obstruction" is responsible for the failure of weak approximation. This means that $S(\mathbb{Q}_p)$ breaks somehow regularly into open-closed subsets, each of which behaves uniformly as far as approximation by $\mathbb{Q}$-rational points is concerned. As $S(\mathbb{Q}_p)$ is compact, it is clear that finitely many subsets $U_1, \ldots, U_k \subset S(\mathbb{Q}_p)$ will suffice. When such a behaviour appears, we speak of a *colouring* and call the subsets the *colours* of $S(\mathbb{Q}_p)$.

Date: February 12, 2012.

2010 *Mathematics Subject Classification.* Primary 11D41; Secondary 11Y50, 11G35, 14J28.

Key words and phrases. Kummer surface, Weak approximation, Transcendental Brauer-Manin obstruction, Multivariate paging.

1.3. It is well-known that a class $\alpha \in \mathrm{Br}(S)$ in the Grothendieck-Brauer group of S induces such a colouring. For a point $x \in S(\mathbb{Q}_p)$, its colour is obtained as $\mathrm{inv}_{\mathbb{Q}_p}(\alpha|x) \in \mathbb{Q}/\mathbb{Z}$. If α is of order N then not more than N colours may occur.

As a result, a failure of weak approximation may appear. Indeed, for a $\mathbb{Q}$-rational point, one must have $\sum_p \mathrm{inv}_{\mathbb{Q}_p}(\alpha|x) = 0$, but the same need not be true for an adelic point. This phenomenon is called the Brauer-Manin obstruction [Ma].

There is a canonical filtration on $\mathrm{Br}(S)$, which causes a distinction between *algebraic* and *transcendental* Brauer classes. Correspondingly, the are the algebraic and the transcendental Brauer-Manin obstruction.

The algebraic Brauer-Manin obstruction is rather well understood. At least on $S(\mathbb{Q}_p)_{\text{good}} \subseteq S(\mathbb{Q}_p)$, the p-adic points with good reduction, it yields extremely regular colourings [CKS, EJ3]. For example, a colouring by two colours is possible only when there is an unramified two-sheeted covering $\pi\colon X \to S(\mathbb{Q}_p)_{\text{good}}$. The two colours are then given by the subsets $\{x \in S(\mathbb{Q}_p) \mid \pi^{-1}(x) = \emptyset\}$ and $\{x \in S(\mathbb{Q}_p) \mid \#\pi^{-1}(x) = 2\}$.

Explicit computations of the algebraic Brauer-Manin obstruction have been done for many classes of varieties. Most of the examples were Fano. For instance, we gave a systematic treatment of the (algebraic) Brauer-Manin obstruction for cubic surfaces in [EJ2, EJ4]. Concerning $K3$ surfaces, computations for diagonal quartic surfaces are due to M. Bright [Br]. Further, it is known that there is no algebraic Brauer-Manin obstruction on a generic Kummer surface as well as on the generic case of a Kummer surface associated to the product of two elliptic curves [SZ, Proposition 1.4.ii)].

1.4. The transcendental Brauer-Manin obstruction is much less understood and seems to be by far more difficult, at least at present. Observe, for example, that the whole Ph.D. thesis of Th. Preu [Pr] is devoted to the computation of the transcendental Brauer-Manin obstruction for single diagonal quartic surface.

Somehow an exception is provided by the case of the Kummer surfaces $S := \mathrm{Kum}(E \times E')$ for two elliptic curves E and E'. Here, the Brauer group, which is typically purely transcendental, was described in detail by A. N. Skorobogatov and Yu. G. Zarhin in [SZ].

1.5. For that reason, in this article, we will deal with Kummer surfaces, defined over $\mathbb{Q}$, of this particular type. To keep the theory simple, we will restrict ourselves to the case that both curves have their full 2-torsion defined over the base field. We may start with equations of the form $y^2 = x(x-a)(x-b)$ and $y^2 = x(x-a')(x-b')$ with $a, b, a', b' \in \mathbb{Q}$ for E and E'. Then $S := \mathrm{Kum}(E \times E')$ is given by

$$z^2 = x(x-a)(x-b)u(u-a')(u-b')\,. \tag{1}$$

The goal of the article is to report on our experiments and theoretical investigations concerning weak approximation and the transcendental Brauer-Manin obstruction for Kummer surfaces of this particular type.

Remark 1.6. To be precise, equation (1) defines a model of the Kummer surface with 16 singular points of type A_1. In the minimal regular model, the singularities are replaced by projective lines. As $\mathrm{Br}(\mathbf{P}^1_k) = \mathrm{Br}(k)$, the evaluation of a Brauer class on a projective line is automatically constant. Thus, we may work as well with the singular model.

2. The transcendental Brauer group

Generalities.

2.1. The cohomological Grothendieck-Brauer group of an algebraic variety S over a field k is equipped with a canonical three-step filtration, defined by the Hochschild-Serre spectral sequence.

i) $\operatorname{Br}_0(S) \subseteq \operatorname{Br}(S)$ is the image of $\operatorname{Br}(k)$ under the natural map. One has $\operatorname{Br}_0(S) \cong \operatorname{Br}(k)$, at least when S has a k-rational point. $\operatorname{Br}_0(S)$ does not contribute to the Brauer-Manin obstruction.

ii) The quotient $\operatorname{Br}_1(S)/\operatorname{Br}_0(S)$ is isomorphic to $H^1(\operatorname{Gal}(k^{\mathrm{sep}}/k), \operatorname{Pic}(S_{k^{\mathrm{sep}}}))$. This subquotient is called the algebraic part of the Brauer group. For k a number field, it is responsible for the algebraic Brauer-Manin obstruction.

iii) Finally, $\operatorname{Br}(S)/\operatorname{Br}_1(S)$ injects into $\operatorname{Br}(S_{k^{\mathrm{sep}}})$. This quotient is called the transcendental part of the Brauer group. Nevertheless, every Brauer class that is not algebraic is usually said to be transcendental. For k a number field, the corresponding obstruction is a transcendental Brauer-Manin obstruction.

2.2. For S, the Kummer surface corresponding to the product of two elliptic curves, the transcendental Brauer group of S is well understood due to the work [SZ] of A. N. Skorobogatov and Yu. G. Zarhin. For us, the following result will be sufficient.

Proposition (Skorobogatov/Zarhin)**.** *Let $E\colon y^2 = x(x-a)(x-b)$ and $E'\colon v^2 = u(u-a')(u-b')$ be two elliptic curves over a field k of characteristic zero. Suppose that their 2-torsion points are defined over k and that E and E' are not isogenous to each other.*

Further, let $S := \operatorname{Kum}(E \times E')$ be the corresponding Kummer surface. Then,

$$\operatorname{Br}(S)_2/\operatorname{Br}(k)_2 = \operatorname{im}(\operatorname{Br}(S)_2 \to \operatorname{Br}(S_{\overline{k}})_2) \cong \ker(\mu\colon \mathbb{F}_2^4 \to (k^*/k^{*2})^4)\,,$$

where μ is given by the matrix

$$M_{aba'b'} := \begin{pmatrix} 1 & ab & a'b' & -aa' \\ ab & 1 & aa' & a'(a'-b') \\ a'b' & aa' & 1 & a(a-b) \\ -aa' & a'(a'-b') & a(a-b) & 1 \end{pmatrix}. \qquad (2)$$

□

2.3. Consider the case that k is algebraically closed. Then, induced by the Kummer sequence, there is the short exact sequence

$$0 \to \operatorname{Pic}(S)/2\operatorname{Pic}(S) \to H^2_{\text{ét}}(S, \mu_2) \to \operatorname{Br}(S)_2 \to 0\,.$$

We have $\dim_{\mathbb{F}_2} \operatorname{Pic}(S)/2\operatorname{Pic}(S) = 16 + \dim_{\mathbb{F}_2} \operatorname{NS}(E \times E')/2\operatorname{NS}(E \times E') = 18$ and $\dim_{\mathbb{F}_2} H^2_{\text{ét}}(S, \mu_2) = 22$. This explains $\operatorname{Br}(S)_2 \cong \mathbb{F}_2^4$. More canonically, there are isomorphisms

$$\operatorname{Br}(S)_2 \cong H^2_{\text{ét}}(E \times E', \mu_2)/(H^2_{\text{ét}}(E, \mu_2) \oplus H^2_{\text{ét}}(E', \mu_2)) \cong \operatorname{Hom}(E[2], E'[2])\,.$$

Remark 2.4. For k any field of characteristic zero, the assumption that the 2-torsion points are defined over k therefore implies that $\operatorname{Gal}(\overline{k}/k)$ operates trivially on $\operatorname{Br}(S_{\overline{k}})_2$. We see explicitly that $\operatorname{Br}(S)_2 \subsetneqq \operatorname{Br}(S_{\overline{k}})_2^{\operatorname{Gal}(\overline{k}/k)} \cong \mathbb{F}_2^4$, in general.

2.5. Assume k to be algebraically closed. For $f, g \in k(S)$, we denote by (f, g) the quaternion algebra

$$k(S)\{I, J\}/(I^2 - f, J^2 - g, IJ + JI)$$

over $k(S)$. Cohomologically, f and g define classes in $H^1(\mathrm{Gal}(\overline{k(S)}/k(S)), \mu_2)$ via the Kummer sequence. The Brauer class of (f, g) is the cup product in

$$\begin{aligned} H^2(\mathrm{Gal}(\overline{k(S)}/k(S)), \mu_2^{\otimes 2}) &= H^2(\mathrm{Gal}(\overline{k(S)}/k(S)), \mu_2) \\ &\subseteq H^2(\mathrm{Gal}(\overline{k(S)}/k(S)), \overline{k(S)}^*) \end{aligned}$$

of these two classes. The symbol $(.\,,.)$ is thus bilinear and symmetric.

Fact 2.6. *Let k be an algebraically closed field, $\operatorname{char} k = 0$, $a, b, a', b' \in k$, and S be as in Proposition 2.2. Then, in terms of the canonical injection $\mathrm{Br}(S) \hookrightarrow \mathrm{Br}(k(S))$, a basis of $\mathrm{Br}(S)_2$ is given by the four quaternion algebras*

$$A_{\mu,\nu} := ((x - \mu)(x - b), (u - \nu)(u - b')), \qquad \mu = 0, a,\ \nu = 0, a'.$$

Thereby, the standard vectors in $\mathbb{F}_2^4$ correspond to these four algebras. More precisely, e_1 corresponds to $A_{a,a'}$, e_2 to $A_{a,0}$, e_3 to $A_{0,a'}$, and e_4 to $A_{0,0}$.

Proof. This is [SZ, Lemma 3.6] together with [SZ, formula (20)]. □

Remark 2.7. Using bilinearity, for nine of the 15 non-trivial classes, we find a description as a single quaternion algebra similar to the type above. For the six classes corresponding to the vectors $(1, 0, 0, 1)$, $(0, 1, 1, 0)$, $(1, 1, 1, 0)$, $(1, 1, 0, 1)$, $(1, 0, 1, 1)$, and $(0, 1, 1, 1)$, we need at least two such algebras.

Remark 2.8 (Isomorphy, Twisting). The automorphisms $\mathbf{P}^1 \to \mathbf{P}^1$, $x \mapsto x - \mu$ for $\mu = a, b$ show that we may replace (a, b) by $(-a, b - a)$ or $(-b, a - b)$ without changing S. Similarly for (a', b').

Further, the twist $E^{(\lambda)}\colon \lambda y^2 = x(x - a)(x - b)$ is isomorphic to the elliptic curve, given by $Y^2 = X(X - \lambda a)(X - \lambda b)$. Hence, replacing (a, b) by $(\lambda a, \lambda b)$ for λ a square does not change S either. Finally, S remains unchanged when both curves are twisted with the same value λ.

Thus, when $k = \mathbb{Q}$, we may assume without restriction that $a, b, a', b' \in \mathbb{Z}$, $\gcd(a, b) = 1$, and $\gcd(a', b')$ is square-free. The assumption that $M_{aba'b'}$ has a non-trivial kernel then ensures that $\gcd(a', b') = 1$, too.

2.9 (The isogenous case)**.** When $E_{\overline{k}}$ and $E'_{\overline{k}}$ are isogenous, only minor modifications occur. The isogeny causes $\mathrm{NS}(E_{\overline{k}} \times E'_{\overline{k}})/2\,\mathrm{NS}(E_{\overline{k}} \times E'_{\overline{k}})$ to be larger than of rank two. Hence, the homomorphism $\mathbb{F}_2^4 \cong \mathrm{Hom}(E[2], E'[2]) \to \mathrm{Br}(S_{\overline{k}})_2$ is only a surjection, not a bijection.

Over an algebraically non-closed field, the situation is as follows. If E and E' are isogenous over k then $\dim_{\mathbb{F}_2} \mathrm{Pic}(S)/2\,\mathrm{Pic}(S) > 2$. As the additional generator evaluates trivially, one finds it in $\ker M_{aba'b'}$ [SZ, Lemma 3.6]. Thus, the map $\ker M_{aba'b'} \twoheadrightarrow \mathrm{Br}(S)_2/\mathrm{Br}(k)_2$ has a non-trivial kernel.

An isogeny defined over a proper field extension l/k causes the same effect over l, but not over k. As $\mathrm{Pic}(S)/2\,\mathrm{Pic}(S) \subsetneq \mathrm{Pic}(S_l)/2\,\mathrm{Pic}(S_l)$, it may, however, happen that a Brauer class is annihilated by the extension l/k. I.e., that a vector in $\ker M_{aba'b'}$ describes an *algebraic* Brauer class. By the Hochschild-Serre spectral sequence, we have $H^2_{\text{ét}}(S, \mu_2)/\mathrm{Br}(k)_2 \subseteq H^2_{\text{ét}}(S_{\overline{k}}, \mu_2)$. Hence, there are no other algebraic 2-torsion Brauer classes than these.

The transcendental Brauer-Manin obstruction.

Fact 2.10. *Let k be a local field of characteristic zero. For two elliptic curves $E\colon y^2 = x(x-a)(x-b)$ and $E'\colon v^2 = u(u-a')(u-b')$ over k with k-rational 2-torsion, consider $S := \mathrm{Kum}(E \times E')$, given explicitly by*

$$z^2 = x(x-a)(x-b)u(u-a')(u-b')\,.$$

Let $\alpha \in \mathrm{Br}(S)$ be a Brauer class, represented by an Azumaya algebra over $k(S)$ of the type $\bigotimes_i A_{\mu_i\nu_i}$.

Then, the local evaluation map $\mathrm{ev}_\alpha\colon S(k) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is given by

$$(x,u;z) \mapsto \mathrm{ev}_\alpha((x,u;z)) = \sum_i ((x-\mu_i)(x-b),(u-\nu_i)(u-b'))_k\,.$$

Here, $(.\,,.)_k$ denotes the k-Hilbert symbol [BS, Ch. 1, §6].

Proof. By definition, $\mathrm{ev}_\alpha((x,u;z)) = \mathrm{inv}(\alpha|_{(x,u;z)})$. Further, $\alpha|_{(x,u;z)}$ is the Azumaya algebra $\bigotimes_i((x-\mu_i)(x-b),(u-\nu_i)(u-b'))$ over k. Now observe that the quaternion algebra (f,g) splits if and only if g is a norm from $k(\sqrt{f})$. This is tested by the norm residue symbol $(g,k(\sqrt{f})/k)$, which agrees with the classical Hilbert symbol $(f,g)_k$. □

Remarks 2.11. i) For us, the Hilbert symbol takes values in $(\frac{1}{2}\mathbb{Z}/\mathbb{Z},+)$. This differs from the classical setting, where the values are in $(\{\pm 1\},\,\cdot\,)$.

ii) According to Proposition 2.2, $\mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \subseteq \mathbb{F}_2^4$. Further, by Fact 2.6, we have an explicit basis, which is given by Azumaya algebras. I.e., for each class in $\mathrm{Br}(S)_2/\mathrm{Br}(k)_2$, we chose a lift to $\mathrm{Br}(S)_2$.

For k a local field, this lift is normalized such that $\mathrm{ev}_\alpha((\infty,\infty,\ .\ )) = 0$. Indeed, for x close to ∞ in k, $(x-\mu)(x-b)$ is automatically a square.

2.12. The evaluation map is constant near the singular points.

Lemma. *Let $p > 2$ be prime, $a,b,a',b' \in \mathbb{Z}_p$ such that $\gcd(a,b) = \gcd(a',b') = 1$ and $E\colon y^2 = x(x-a)(x-b)$ as well as $E'\colon v^2 = u(u-a')(u-b')$ be elliptic curves, not isogenous to each other. Put*

$$l := \max(\nu_p(a),\nu_p(b),\nu_p(a-b)) + \max(\nu_p(a'),\nu_p(b'),\nu_p(a'-b'))\,.$$

Consider the surface S over $\mathbb{Q}_p$, given by $z^2 = x(x-a)(x-b)u(u-a')(u-b')$. Then, for every $\alpha \in \mathrm{Br}(S)_2$, the evaluation map $S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is constant on the subset

$$\{(x,u;z) \in S(\mathbb{Q}_p) \mid \nu_p(x) < 0 \text{ or } \nu_p(u) < 0 \text{ or } x \equiv \mu, u \equiv \nu \pmod{p^{l+1}},\ \mu = 0,a,b,\ \nu = 0,a',b'\}\,.$$

Proof. Consider the Hilbert symbol $((x-a)(x-b),(u-a')(u-b'))_p$, first. Using the equation of the surface, we see that

(3)
$$((x-a)(x-b),(u-a')(u-b'))_p = ((x-a)(x-b),-xu)_p = (-xu,(u-a')(u-b'))_p.$$

We distinguish three cases. In all cases, observe that a Hilbert symbol is clearly zero, when at least one of its entries is a square.

First case. Negative valuation.
It is clear that $\nu_p(x) < 0$ implies $(x-a)(x-b)$ is a square and that $\nu_p(u) < 0$ implies that $(u-a')(u-b')$ is a square.

Second case. $x \equiv \mu, u \equiv \nu \pmod{p^{l+1}}$ for $(\mu, \nu) = (0, \nu)$ or $(\mu, 0)$.
First, let $x \equiv 0 \pmod{p^{l+1}}$. Then, $(x-a)(x-b) \equiv ab \pmod{p^{l+1}}$. As $\nu_p(ab) = \nu_p(a) + \nu_p(b) = \max(\nu_p(a), \nu_p(b)) \leq l$, both numbers belong to the same square class. Analogously, $u \equiv 0 \pmod{p^{l+1}}$ implies $(u-a')(u-b') \equiv a'b' \pmod{p^{l+1}}$ such that $(u-a')(u-b')$ is in the square class of $a'b'$.

Third case. $x \equiv \mu, u \equiv \nu \pmod{p^{l+1}}$ for $(\mu, \nu) = (a, a')$, (a, b'), (b, a'), or (b, b').
Suppose, for example that $x \equiv a \pmod{p^{l+1}}$ and $u \equiv a' \pmod{p^{l+1}}$. Then, $(-xu) \equiv (-aa') \pmod{p^{l+1}}$ such that $(-xu)$ is in the square class of $(-aa')$. The other cases yield the square classes of $(-ab')$, $(-ba')$, and $(-bb')$.

Consequently, the evaluation map is constant on the set described if and only if the vector

$$(1, ab, a'b', -aa')^t \in (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^4$$

is zero. This is exactly the first column of the matrix $M_{aba'b'}$, cf. formula (2).

For the Hilbert symbols $((x-a)(x-b), u(u-b'))_p$, $(x(x-b), (u-a')(u-b'))_p$, and $(x(x-b), u(u-b'))_p$, the calculations are completely analogous. They lead to the second, third, and fourth column of $M_{aba'b'}$.

To summarize, we see that, for a combination of Hilbert symbols, the evaluation map is constant exactly when it represents a Brauer class. □

Remark 2.13. For $p = 2$, the condition has to be strengthened to $\nu_2(x) < -2$ or $\nu_p(u) < -2$ or $x \equiv \mu, u \equiv \nu \pmod{2^{l+3}}$. The proof is essentially the same.

Proposition 2.14. *Let $E\colon y^2 = x(x-a)(x-b)$ and $E'\colon v^2 = u(u-a')(u-b')$ be two elliptic curves over a local field k, not isogenous to each other. Suppose that $a, b, a', b' \in k$. Further, let $S := \mathrm{Kum}(E \times E')$ be the corresponding Kummer surface.*

Suppose that either $k = \mathbb{R}$ or k is a p-adic field and both E and E' have good reduction. Then, for every $\alpha \in \mathrm{Br}(S)$, the evaluation map $\mathrm{ev}_\alpha\colon S(k) \to \mathbb{Q}/\mathbb{Z}$ is constant.

Proof. *First case.* $k = \mathbb{R}$.
Suppose without restriction that $a > b > 0$ and $a' > b' > 0$. Then, it will suffice to prove the assertion for representatives of e_2 and e_3. I.e., for $((x-a)(x-b), u(u-b'))_\mathbb{R}$ and $(x(x-b), (u-a')(u-b'))_\mathbb{R}$. Cf. the proof of Proposition 2.18.b) below.

Concerning e_2, $((x-a)(x-b), u(u-b'))_\mathbb{R} = \frac{1}{2}$ would mean that $(x-a)(x-b) < 0$ and $u(u-b') < 0$. Hence, $b < x < a$ and $0 < u < b'$. But then $x(x-a)(x-b)u(u-a')(u-b') < 0$ such that there is no real point on S corresponding to (x, u). For e_3, the argument is analogous.

Second case. $k = \mathbb{Q}_p$.
Assume without reduction that $a, b, a', b' \in \mathbb{Z}_p$. Good reduction implies $p \nmid a, b$, $a \not\equiv b \pmod{p}$, and the analogous conditions for a' and b'. In particular, $p > 2$.

Again, we consider the Hilbert symbol $((x-a)(x-b), (u-a')(u-b'))_p$, first. In order to be non-zero, for a Hilbert symbol, it is necessary that at least one of its entries is of odd p-adic valuation. This enforces $x, u \in \mathbb{Z}_p$. Further, two of the nine congruences $x \equiv 0, a, b \pmod{p}$, $u \equiv 0, a', b' \pmod{p}$ must be fulfilled. Indeed, otherwise for at least one of the three representations given in (3), we see that the Hilbert symbol is zero. For the Hilbert symbols $((x-a)(x-b), u(u-b'))_p$, $(x(x-b), (u-a')(u-b'))_p$, and $(x(x-b), u(u-b'))_p$, the argument is analogous.

Consequently, for a Brauer class that is normalized to $\mathrm{ev}_\alpha((\infty, \infty, \ .\ )) = 0$, the evaluation map $\mathrm{ev}_\alpha \colon S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is zero, except possibly for the points reducing to one of the singularities. But for these, Lemma 2.12 is applicable. Observe that, because of the good reduction, we have $l = 0$. □

Algorithm 2.15. Let the parameters $a, b, a', b' \in \mathbb{Z}$, a Brauer class $\alpha \in \mathrm{Br}(S)_2$ as a combination of Hilbert symbols, and a prime number p be given. Then this algorithm determines the colouring of $S(\mathbb{Q}_p)$ defined by $\mathrm{ev}_\alpha \colon S(\mathbb{Q}_p) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, for S the surface given by $z^2 = x(x-a)(x-b)u(u-a')(u-b')$.

i) Calculate $l := \max(\nu_p(a), \nu_p(b), \nu_p(a-b)) + \max(\nu_p(a'), \nu_p(b'), \nu_p(a'-b'))$.

ii) Initialize three lists S_0, S_1, and S_2, the first two being empty, the third containing all triples (x_0, u_0, p) for $x_0, u_0 \in \{0, \ldots, p-1\}$. A triple (x_0, u_0, p^e) shall represent the subset $\{(x, u; z) \in S(\mathbb{Q}_p) \mid \nu_p(x - x_0) \geq e, \nu_p(u - u_0) \geq e\}$.

iii) Run through S_2. For each element (x_0, u_0, p^e), test whether the corresponding set is non-empty. Otherwise, delete it and continue.

If $e \geq l+1$, $\nu_p(x-\mu) \geq l+1$ for some $\mu \in \{0, a, b\}$ and $\nu_p(u-\nu) \geq l+1$ for a $\nu \in \{0, a', b'\}$ then move (x_0, u_0, p^e) to S_0 and continue.

Then, test naively, using the Hilbert symbols, whether the elements in the corresponding set all have the same evaluation. If this test succeeds then move (x_0, u_0, p^e) to S_0 or S_1, accordingly, and continue.

Otherwise, replace (x_0, u_0, p^e) by the p^2 triples $(x_0 + ip^e, u_0 + jp^e, p^{e+1})$ for $i, j \in \{0, \ldots, p-1\}$ and continue.

iv) If S_2 is empty then output S_0 and S_1 and terminate. Otherwise, go back to step iii).

Example 2.16. Consider the Kummer surface S over $\mathbb{Q}$, given by

$$z^2 = x(x-1)(x-25)u(u+25)(u+36)\,.$$

Then, weak approximation is violated on S.

Proof. This is caused by the transcendental Brauer-Manin obstruction. In fact, the matrix (2) is

$$M = \begin{pmatrix} 1 & 25 & 900 & 25 \\ 25 & 1 & -25 & -275 \\ 900 & -25 & 1 & -24 \\ 25 & -275 & -24 & 1 \end{pmatrix} \mathrel{\widehat{=}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -11 \\ 1 & -1 & 1 & -6 \\ 1 & -11 & -6 & 1 \end{pmatrix},$$

having the kernel $\langle e_1 \rangle$. Hence, there is a transcendental Brauer class on S, represented by the quaternion algebra $((x-1)(x-25), (u+25)(u+36))$.

Now, the argument is completely elementary. For every $(x, u; z) \in S(\mathbb{Q}_p)$ with $z \neq 0$, one has

$$\sum_p ((x-1)(x-25), (u+25)(u+36))_p = 0\,,$$

according to the sum formula for the Hilbert symbol. The bad primes of the elliptic curves $y^2 = x(x-1)(x-25)$ and $y^2 = x(x+25)(x+36)$ are $2, 3, 5$, and 11. Hence, the sum is actually only over these four primes.

Our implementation of Algorithm 2.15 shows that the local evaluation map is constant at the primes 2, 3, and 11, but not at 5. Hence, 5-adic points such that $((x-1)(x-25),(u+25)(u+36))_5 = \frac{1}{2}$ may not be approximated by $\mathbb{Q}$-rational ones.

Examples for such 5-adic points are those with $(x,u) = (17,5)$. Indeed, $17 \cdot (17-1) \cdot (17-25) \cdot 5 \cdot (5+25) \cdot (5+36) = -535\,296 \cdot 5^2$ is a 5-adic square, but $(17-1) \cdot (17-25) = -128$ is a non-square and $\nu_5((5+25) \cdot (5+36)) = 1$ is odd. □

Remarks 2.17. i) The constancy of the local evaluation maps at 3 and 11 and the non-constancy at 5 also follow from the criterion, formulated as Theorem 2.21 below.

ii) In the colouring obtained on $S(\mathbb{Q}_5)$, all the points such that $x,u \not\equiv 0 \pmod 5$ have colour zero. This is very different from the colourings, typically obtained from an algebraic Brauer class. The reader should compare the situation described in [CKS], where, on the cone over an elliptic curve, three sets of equal sizes appear.

Ranks, Normal Form, Asymptotics.

Proposition 2.18. *Let $E\colon y^2 = x(x-a)(x-b)$ and $E'\colon v^2 = u(u-a')(u-b')$ be two elliptic curves over a field k of characteristic zero. Suppose that $a,b,a',b' \in k$ and that E and E' are not isogenous to each other. Further, let $S := \mathrm{Kum}(E \times E')$ be the corresponding Kummer surface.*

a) *Then,* $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \leq 4$ *and* $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \neq 3$.

Thereby, $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 = 4$ *is possible only when* (-1) *is a square in* k.

b) *Let p be a prime number and $k = \mathbb{Q}_p$. If both E and E' have good reduction then* $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2$ *is even.*

Finally, if $k = \mathbb{R}$ *then* $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 = 2$.

Proof. a) The inequality $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \leq 4$ follows directly form Proposition 2.2. Further, dimension three would imply that $M_{aba'b'}$ is of rank one. But this is impossible for symmetric matrix having zeroes on the diagonal.

Further, $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 = 4$ requires $M_{aba'b'}$ to be the zero matrix. In particular, aa' and $(-aa')$ both have to be squares in k. This implies that (-1) is a square, too.

b) The assumption of good reduction implies $p > 2$. Further, $a, b, a-b$ as well as $a', b', a'-b'$ are p-adic units. Then, being a square in $\mathbb{Q}_p$ or not is tested by the Legendre symbol. $M_{aba'b'}$ is essentially a symmetric matrix with entries in $\mathbb{F}_2$, having zeroes on the diagonal. As such a matrix is antisymmetric, its rank is even.

At last, consider the case that $k = \mathbb{R}$. Here, applying one of the automorphisms of $\mathbf{P}^1 \times \mathbf{P}^1$, $(x,u) \mapsto (x-\mu, u-\nu)$ for $\mu = 0,a,b,$ $\nu = 0,a',b'$, if necessary, we may assume that $a > b > 0$ and $a' > b' > 0$. Then,

$$M_{aba'b'} = \begin{pmatrix} + & + & + & - \\ + & + & + & + \\ + & + & + & + \\ - & + & + & + \end{pmatrix}$$

has kernel $\langle e_2, e_3 \rangle$. □

2.19 (Normal form)**.** Let $a,b,a',b' \in \mathbb{Q}^*$, $a \neq b$, $a' \neq b'$, and S be the Kummer surface $z^2 = x(x-a)(x-b)u(u-a')(u-b')$. Fix a non-trivial transcendental Brauer class $\alpha \in \mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q})_2$. Then, there are two types.

Type 1. α may be expressed by a single Hilbert symbol.
There are nine cases for the kernel vector of $M_{aba'b'}$. A suitable automorphism of $\mathbf{P}^1 \times \mathbf{P}^1$ transforms the surface to one with kernel vector e_1.

Then, $ab, a'b', (-aa') \in \mathbb{Q}^{*2}$. As we may suppose $\gcd(a, b) = \gcd(a', b') = 1$, we have the normal form that $a > b$, $a' < b'$, and

$$a, b, (-a'), (-b') \in \mathbb{Q}^{*2}\,.$$

Up to the involution $(a, b, a', b') \mapsto (-a', -b', -a, -b)$ this normal form is unique. Geometrically, this involution means to interchange the two elliptic curves and to twist both by (-1).

Type 2. To express α, two Hilbert symbols are necessary.
There are six cases for the kernel vector of $M_{aba'b'}$. A suitable automorphism of $\mathbf{P}^1 \times \mathbf{P}^1$ transforms the surface to one with kernel vector $e_2 + e_3$. Then $aa', bb', (a - b)(a' - b') \in \mathbb{Q}^{*2}$.

Remarks 2.20 (asymptotics). i) Let $N > 0$. Then, the number of pairs (a, b) such that a and b are perfect squares, $a < b$, and $a, b - a < N$ is asymptotically CN for $C := \frac{1}{2}[\log(\sqrt{2} + 1) + \sqrt{2} - 1]$. Indeed, the Stieltjes integral

$$\int_1^N \sqrt{x + N} - \sqrt{x}\; d\sqrt{x}$$

has exactly this behaviour. Assuming that isogenies are rare, we obtain that the number of surfaces over $\mathbb{Q}$ with integer coefficients of absolute value $\leq N$ and a 2-torsion Brauer class of type 1 is asymptotically $\frac{1}{2}(6/\pi^2)^2 C^2 N^2 \approx 0{,}077\,544 N^2$.

ii) On the other hand, a 2-torsion Brauer class of type 2 leads to a $\mathbb{Q}$-rational point on the intersection of three quadrics in $\mathbf{P}^6$. The Manin conjecture leads to the naive expectation of a growth of the type $cN \log^l N$.

iii) The number of all Kummer surfaces of the form considered and with coefficients up to N is $O(N^4)$. Thus, only a very small fraction has a non-trivial 2-torsion Brauer class.

Even less surfaces should have odd torsion in their Brauer group. Indeed, for l-torsion, one must have $\mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}(E[l], E'[l]) \neq 0$ [SZ, Proposition 3.3]. Consequently, $\#E(\mathbb{F}_p) \equiv \#E'(\mathbb{F}_p) \pmod{l}$ for every prime $p \neq l$ that is good for both E and E'. Based on this, our computations show that, up to $N = 200$, no surface has an l-torsion Brauer class for $l \geq 5$. Further, at most eight pairs of j-invariants allow a 3-torsion Brauer class.

iv) It is possible over $\mathbb{Q}$ to have a two dimensional 2-torsion Brauer group. For this, in the normal form of type 1, one needs that $a-b$ and $b'-a'$ are perfect squares, too. Further, these surfaces have four normal forms instead of two, as there are two Brauer classes of type 1. Corresponding to a pair of Pythagorean triples, we therefore have two Kummer surfaces, differing from each other by a twist by (-1). The asymptotics of Pythagorean triples [BV] shows that there are asymptotically $\frac{4}{\pi^4} \log^2(1+\sqrt{2})N \approx 0{,}031\,899N$ surfaces over $\mathbb{Q}$ with integer coefficients of absolute value $\leq N$ and a Brauer group of dimension two.

v) Some actual numbers are listed in the table below. Compare the description of the sample, given in 4.2.

Table 1. Surfaces with a 2-torsion Brauer class

bound	dimension 2	dimension 1, type 1	dimension 1, type 2
		(among them algebraic classes)	(none is algebraic)
50	0	183 (1)	38
100	0	766 (2)	98
200	2	3049 (3)	367
500	12	18825 (4)	1457
1000	20	77249 (8)	4398
2000	42	305812 (11)	12052

Trivial evaluation.

Theorem 2.21 (A criterion)**.** *Let $p > 2$ be a prime number and $0 \neq a, b, a', b' \in \mathbb{Z}_p$ such that $\gcd(a, b) = \gcd(a', b') = 1$, $a \neq b$, and $a' \neq b'$. Let S be the Kummer surface, given by $z^2 = x(x - a)(x - b)u(u - a')(u - b')$. Assume that e_1 is a kernel vector of the matrix $M_{aba'b'}$ and let $\alpha \in \operatorname{Br}(S)_2$ be the corresponding Brauer class.*

i) *Suppose $a \equiv b \pmod p$ or $a' \equiv b' \pmod p$. Then, the evaluation map $\operatorname{ev}_\alpha \colon S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is constant.*

ii) *If $a \not\equiv b \pmod p$, $a' \not\equiv b' \pmod p$, and one the four numbers is divisible by p then the evaluation map $\operatorname{ev}_\alpha \colon S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is non-constant.*

Proof. *First step.* Preparations.
We are interested in the Hilbert symbol $((x-a)(x-b), (u-a')(u-b'))_p$. Suppose that S is normalized such that $a, b, (-a'), (-b') \in \mathbb{Q}_p^{*2}$, $a \equiv b \pmod p$, and $a'/b' \in \mathbb{Z}_p$.

A $\mathbb{Q}_p$-rational point on S corresponds to a pair of points on the elliptic curves $\lambda y^2 = x(x-a)(x-b)$ and $\lambda v^2 = u(u-a')(u-b')$ for common value of λ. The Hilbert symbol then simplifies to $(\lambda x, \lambda u)_p$.

Second step. 2-descent.
By 2-descent, cf. [Si, Proposition X.1.4], $E\colon Y^2 = X(X - a)(X - b)$ has a point in the square class of x if and only if the system

$$\begin{aligned} xz_1^2 - tz_2^2 &= a \\ xz_1^2 - xtz_3^2 &= b \end{aligned}$$

is solvable. Eliminating t, we obtain $x^2z_1^2z_3^2 - xz_1^2z_2^2 = axz_3^2 - bz_2^2$ or

$$(xz_3^2 - z_2^2)(xz_1^2 - b) = (a - b)xz_3^2.$$

Division by $(-b)xz_3^2$ yields $(1 - \frac{z_2^2}{z_3^2}\frac{1}{x})(1 - \frac{z_1^2}{b}x) = 1 - \frac{a}{b}$. In other words, E has a point in the square class of x if and only if $(1 - v^2x)(1 - \frac{w^2}{b}x) = 1 - \frac{a}{b}$ is solvable.

Third step. Application to the Kummer surface S.
As $\lambda y^2 = x(x - a)(x - b)$ is equivalent to $y'^2 = \lambda x(\lambda x - \lambda a)(\lambda x - \lambda b)$ and $b, (-b')$ are squares, we see that S has a point with coordinates in the square classes of x and u if and only if

$$\begin{aligned} (1 - v^2\lambda x)(1 - w^2x) &= 1 - \tfrac{a}{b} \\ (1 - v'^2\lambda u)(1 + w'^2u) &= 1 - \tfrac{a'}{b'} \end{aligned}$$

has a solution.

Now let $(x, u; z) \in S(\mathbb{Q}_p)$ be any point with $z \neq 0$. Then, Lemma 2.23.i) shows $(-u, \lambda u)_p = 0$. Further, by Lemma 2.23.iii), x or λx is a square in $\mathbb{Q}_p$. In the case $\lambda x \in \mathbb{Q}_p^{*2}$, the assertion $(\lambda x, \lambda u)_p = 0$ is clearly true. If $x \in \mathbb{Q}_p^{*2}$ then $0 = (-u, \lambda u)_p = (\lambda, \lambda u)_p = (\lambda x, \lambda u)_p$.

ii) Without restriction, assume that $p^2 | a$ and $a'/b' \in \mathbb{Z}_p$. We claim, for $\lambda = -1$, there is a point on S such that $x = p$ and $2 | \nu_p(u)$, thereby $(-u)$ being a non-square.

Indeed, it is obvious that $(-p)(p-a)(p-b) \in \mathbb{Q}_p^{*2}$. Further, by Hensel's Lemma, it suffices to find a pair $(U_1, U_2) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ of non-squares such that $(1 - U_1)(1 - U_2) = 1 - \frac{\overline{a}'}{\overline{b}'}$. For this, a counting argument applies. In fact, each $U_1 \in \mathbb{F}_p \backslash \{0, 1, \frac{\overline{a}'}{\overline{b}'}\}$ uniquely determines its partner. As this set contains $\frac{p-1}{2}$ non-squares and only $\frac{p-5}{2}$ squares, the assertion follows. □

Remarks 2.22. i) It might seem strange to use a descent type argument over a local field. It seems to us, however, that a direct argument is neither more elegant nor shorter.

ii) Using the descent argument above, we also recover the constancy of the evaluation map in the case of good reduction. Indeed, Lemma 2.23.ii) implies that x or λx is a square or both have even valuation. The first two cases are dealt with as above. Otherwise, λ is a square and one has to show $2 | \nu_p(u)$. But this is implied by Lemma 2.23.ii) when looking at the second equation.

Lemma 2.23. *Let $p > 2$ be a prime number and $A, B \in \mathbb{Q}_p^*$, $Q \in \mathbb{Q}_p^{*2}$. Suppose that the equation $(1 - Av^2)(1 - Bw^2) = 1 - Q$ is solvable in $\mathbb{Q}_p^* \times \mathbb{Q}_p^*$.*

i) *Then, $(A, B)_p = 0$.*

ii) *If $Q \in \mathbb{Z}_p^*$ then $A \in \mathbb{Q}_p^{*2}$, or $B \in \mathbb{Q}_p^{*2}$, or both, A and B, are of even valuation.*

iii) *If $Q \in \mathbb{Z}_p^*$ and $Q \equiv 1 \pmod p$ then $A \in \mathbb{Q}_p^{*2}$, or $B \in \mathbb{Q}_p^{*2}$.*

Proof. i) We have that $Av^2 + Bw^2 - AB(vw)^2$ is a square. When all three summands are of the same valuation, they must be units. The assertion is then clearly true. Otherwise, at most two of the three summands have minimal valuation. Then, their sum is a square, too. According to the definition of the Hilbert symbol [BS, page 55], $(A, B)_p = 0$, $(A, -AB)_p = 0$, or $(B, -AB)_p = 0$. These three are equivalent to each other.

ii) We have $\nu_p(1 - Q) \geq 0$. On the other hand, when both A and B are non-squares then $\nu_p(1 - Av^2), \nu_p(1 - Bw^2) \leq 0$. This implies equality, hence $Av^2, Bw^2 \in \mathbb{Z}_p$. Both must be units as $Av^2 + Bw^2 - AB(vw)^2 \in \mathbb{Z}_p^*$ is a square.

iii) If A and B were both non-squares then $\nu_p(1 - Av^2) \leq 0$ and $\nu_p(1 - Bw^2) \leq 0$. As $\nu_p(1 - Q) > 0$, this is a contradiction. □

2.24. Experiments with Algorithm 2.15 show surprisingly often that there are non-trivial Brauer classes with trivial evaluation. The reason is the following fact.

Fact 2.25. *Let $p > 2$ be a prime number and $E\colon y^2 = x(x-a)(x-b)$ and $E'\colon v^2 = u(u-a')(u-b')$ be two elliptic curves over $\mathbb{Q}_p$. Suppose that E and E' are not isogenous to each other and that $a, b, a', b' \in \mathbb{Q}_p$. Let, finally S be the corresponding Kummer surface. Then,*

i) *If $\dim \mathrm{Br}(S)_2 / \mathrm{Br}(\mathbb{Q}_p)_2 = 1$ or 2 then there is a non-zero $\alpha \in \mathrm{Br}(S)_2$ such that ev_α is the zero map.*

ii) *Let $\dim \mathrm{Br}(S)_2 / \mathrm{Br}(\mathbb{Q}_p)_2 = 4$. Then, the subspace of classes with constant evaluation map is of dimension 3 when both, E and E', have bad reduction. Otherwise, the dimension is 2.*

Proof. i) The assumption implies that E or E' has bad reduction. Applying an automorphism of $\mathbf{P}^1 \times \mathbf{P}^1$, we may assume that $a, b \in \mathbb{Z}_p$, $p \nmid a, b$, and $a \equiv b \pmod{p}$. Then, $ab \in \mathbb{Q}_p^{*2}$. The upper left 2×2-block of $M_{aba'b'}$ is zero. If the block $\left(\begin{smallmatrix} a'b' & aa' \\ -aa' & a'(a'-b') \end{smallmatrix}\right)$, occurring in the upper right and lower left, has full rank then $\ker M_{aba'b'} = 0$, a contradiction. Otherwise, there is a Brauer class represented by a vector from $\langle e_1, e_2 \rangle$. By Theorem 2.21.i), its evaluation map is constant.

ii) If both E and E' have bad reduction then we may assume $a \equiv b \pmod{p}$ and $a' \equiv b' \pmod{p}$ such that the Brauer classes corresponding to $\langle e_1, e_2, e_3 \rangle$ have constant evaluation maps. However, ev_{e_4} is non-constant by virtue of Theorem 2.21.ii).

Otherwise, Theorem 2.21 implies that the Brauer classes corresponding to $\langle e_1, e_2 \rangle$ have constant evaluation maps, while those of e_3, e_4, and $e_3 + e_4$ are non-constant. □

Remark 2.26. Our experiments show that, over $\mathbb{Q}_2$, dimension one is possible with a non-trivial evaluation map. This occurs, for example, for $(a, b) = (3, -20)$ and $(a', b') = (5, -16)$. Dimension two is possible with a one- or two-dimensional trivial part.

3. A point search algorithm for special Kummer surfaces

3.1. Our surfaces are double covers of $\mathbf{P}^1 \times \mathbf{P}^1$, given by equations of the form

$$z^2 = f_{ab}(x, y) f_{a'b'}(u, v) \, .$$

Here, f_{ab} is the binary quartic form $f_{ab}(x, y) := xy(x - ay)(x - by)$. Thus, a point $([x : y], [u : v]) \in (\mathbf{P}^1 \times \mathbf{P}^1)(\mathbb{Q})$ leads to a point on the surface if and only if the square classes of $f_{ab}(x, y)$ and $f_{a'b'}(u, v)$ coincide or one of them is zero.

We will call the solutions with $f_{ab}(x, y)$ or $f_{a'b'}(u, v)$ zero the trivial solutions of the equation. Obviously, there is a huge number of trivial solutions. Our aim is to describe an efficient algorithm that searches for non-trivial solutions and does not care about the trivial ones. In its simplest version, our algorithm works as follows.

Algorithm 3.2 (Point search)**.** Given a two lists $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$, this algorithm will simultaneously search for the solutions of all equations of the form

$$w^2 = f_{a_i b_i}(x, y) f_{a_j b_j}(u, v) \, .$$

It will find those with $|x|, |y|, |u|, |v| \leq B$.

i) Compute a bound L for the linear factors by putting

$$L := B(1 + \max\{|a_i|, |b_i| \mid i = 1, \ldots, k\}) \, .$$

ii) Store the square-free parts of the integers in $[1, \ldots, L]$ in an array T.

iii) Enumerate in an iterated loop representatives for all points $[x : y] \in \mathbf{P}^1(\mathbb{Q})$ with $x, y \in \mathbb{Z}$, $|x|, |y| \leq B$, and $x, y \neq 0$.

iv) For each point $[x : y]$ enumerated, run a loop over $i = 1, \ldots, k$ to compute the four linear factors x, y, $x - a_i y$, and $x - b_i y$ of f_{a_i, b_i}.

v) Store the square-free parts of the factors in $m_1, \ldots, m_4$. Use table T here.

vi) Put $p_1 := \frac{m_1}{\gcd(m_1,m_2)} \frac{m_2}{\gcd(m_1,m_2)}$, $p_2 := \frac{m_3}{\gcd(m_3,m_4)} \frac{m_4}{\gcd(m_3,m_4)}$, and

$$p_3 := \tfrac{p_1}{\gcd(p_1,p_2)} \tfrac{p_2}{\gcd(p_1,p_2)} \, .$$

Thus, p_3 is a representative of the square class of $f_{a_i b_i}(x, y)$.

vii) Store the quadruple $(x, y, i, h(p_3))$ into a list. Here, h is a hash-function.

viii) Sort the list by the last component.

ix) Split the list into parts. Each part corresponds to a single value of $h(p_3)$. At this point, we have detected all collisions of the hash-function.

x) Run in an iterated loop over all the collisions and check whether $((x, y, i, h(p_3)), (x', y', i', h(p'_3)))$ corresponds to a solution $([x : y], [x' : y'])$ of the equation $w^2 = f_{a_i b_i}(x, y) f_{a_{i'} b_{i'}}(x', y')$. Output all the solutions found.

Remarks 3.3. i) For practical search bounds B, the first integer overflow occurs when we multiply $\frac{p_1}{\gcd(p_1,p_2)}$ and $\frac{p_2}{\gcd(p_1,p_2)}$. But we can think of this reduction modulo 2^{64} as being a part of our hash-function. Note that the final check of $w^2 = f_{a_i b_i}(x, y) f_{a_{i'} b_{i'}}(x', y')$ can be done without using multi-precision integers by dividing out the gcd's of the values of the eight linear factors.

ii) One disadvantage of Algorithm 3.2 is obvious. It requires by far more memory than available. We solved this problem by the introduction of what we call a *multiplicative paging*. This is an approach motivated by the simple, additive paging as described in [EJ1]. In addition, our memory-optimized point search algorithm is based on the following observation.

Lemma 3.4. *Let p be a good prime. Then, for each pair (x, y) with $\gcd(x, y) = 1$, at most one of the factors x, y, $(x - ay)$, and $(x - by)$ is divisible by p.* □

Algorithm 3.5 (Point search using multivariate paging)**.** i) Compute L and the table of square-class representatives as in Algorithm 3.2.

ii) Compute the upper bound $C := 2 \max\{|a_i|, |b_i| \mid i = 1, \ldots, k\}$ for the possibly bad primes.

iii) Initialize an array of Booleans of length L. Use the value `false` for the initialization. We will call this array the markers of the factors already treated.

iv) In a loop, run over all good primes below L. Start with the biggest one and stop when the upper bound C is reached. For each prime p_p, execute the steps below. We call p_p the *page prime*.

• Run over all multiples m of p_p not exceeding L and such that the p_p-adic valuation is odd. For each m, do the following.

•• Check whether m is marked as already treated. In this case, continue with the next m.

•• Test whether x, y, $x - a_i y$, or $x - b_i y$ can represent this value. Here, use the constraints $|x|, |y| \leq B$ and $i \in \{1, \ldots, k\}$.

•• For each possible representation with $\gcd(x, y) = 1$, check whether x, y, $x - a_i y$, or $x - b_i y$ is marked as already treated. Otherwise, store the quadruples $(x, y, i, h(p_3))$ into a list.

•• Mark the value of m as treated and continue with the next m.

• As in Algorithm 3.2, construct all solutions by inspecting the collisions of the hash-function.

v) Up to now, all solutions were found such that w has at least one prime factor bigger than the bad-primes bound. To get the remaining ones, use the initial algorithm but skip all values of x, y that are marked as treated factors. Further, skip step iv) if m_3 or m_4 is marked as treated.

Remark 3.6. The last step computes all solutions in smooth numbers. It is an experimental observation that this step takes only a small fraction of the running time, but gives a large percentage of the solutions. When initializing the markers for treated factors in an appropriate way, one can modify the algorithm such that only the solutions in smooth numbers are found.

4. Some experiments

4.1 (Colouring by covering—A search for regular colourings)**.** As noticed in 1.3, on various types of surfaces [Br, EJ3], the (algebraic) Brauer-Manin obstruction leads to very regular colourings. Carrying this knowledge over to the special Kummer surfaces, given by $S\colon w^2 = f_4(x,y)g_4(u,v)$, one is led to test the following. For a $\mathbb{Q}$-rational point with $w \neq 0$, write $\lambda w_1^2 = f_4(x,y)$ and $\lambda w_2^2 = g_4(u,v)$ and expect the colour to be given by the square class of λ.

For p-adic points, this defines a colouring with four ($p > 2$), respectively eight ($p = 2$) colours. At the infinite place, the colour is given by the sign of λ. Motivated by [Br, EJ3], we assume that the p-adic colour of a rational point has a meaning only when p divides the conductor of one of the elliptic curves used to construct S. Further, we restricted ourselves to the square classes of even p-adic valuation (for the primes of bad reduction). This does not exclude all rational points reducing to the singular locus at a bad prime.

Thus, we get a colouring of the $\mathbb{Q}$-rational points with 2^k colours for a surface with k relevant odd primes. Weak approximation would imply that the colour-map is a surjection. In the case of a visible obstruction, we would expect that at most half of the possible colours are in the image of the colour map.

For a systematic test, we used the 184 elliptic curves with odd conductor and $|a|, |b| < 100$. This led to 16836 surfaces. The following table gives an overview of the number of colours that occurred.

Table 2. Regular colourings, numbers of points hit by $\mathbb{Q}$-rational points

#bad primes	2	3	4	5	6	7	8
#possible colours	8	16	32	64	128	256	512
#surfaces	4	182	1678	5777	7409	1726	60
#colours found $h = 1000$	8	15–16	26–32	32–64	33–127	31–157	27– 81
#colours found $h = 3000$	8	16	30–32	49–64	67–128	81–226	92–192
#colours found $h = 10000$	8	16	32	57–64	93–128	142–254	207–352
only smooth solutions	8	16	31–32	54–64	79–128	99–236	113–197
#colours found $h = 30000$	8	16	32	62–64	109–128	196–256	303–474
only smooth solutions	8	16	32	59–64	92–128	146–253	161–300
#colours found $h = 100000$	8	16	32	64	121–128	232–256	387–505
only smooth solutions	8	16	32	61–64	108–128	185–256	230–381

Our result is thus negative. It seems that there is no obstruction factoring over such a colouring. We expect, one would find $\mathbb{Q}$-rational points of all colours when further rising the search bound.

The running times were 18.5 hours for search bound 30000 and 275 hours for search bound 100000, but only 51 minutes for smooth solutions and bound 100000.

4.2 (Investigating the Brauer-Manin obstruction—A sample.)**.** We determined all Kummer surfaces of the particular form $z^2 = x(x-a)(x-b)u(u-a')(u-b')$ such that the parameters are of absolute value ≤ 200 and such that there is a transcendental 2-torsion Brauer class.

More precisely, we determined all $(a, b, a', b') \in \mathbb{Z}^4$ such that $\gcd(a, b) = 1$, $\gcd(a', b') = 1$, $a > b > 0$, $a - b, b \leq 200$, as well as $a' < b' < 0$, $a' - b', b' \geq -200$ and the matrix $M_{aba'b'}$ is degenerate. We made sure that (a, b, a', b') was not listed when $(-a', -b', -a, -b)$, $(a, a - b, a', a' - b')$, or $(-a', b' - a', -a, b - a)$ was already in the list. We ignored the quadruples, where (a, b) and (a', b') define the same elliptic curve.

This led to 3075 surfaces with a kernel vector of type 1, 367 surfaces with a kernel vector of type 2, and two surfaces with $\mathrm{Br}(S)_2$ of dimension two. The last correspond to $(25, 9, -169, -25)$ and $(25, 16, -169, -25)$. Among the 3075 surfaces, 26 actually have $\mathrm{Br}(S)_2 = 0$, due to a $\mathbb{Q}$-isogeny between the corresponding elliptic curves.

4.3 (The BM-relevant primes—p-adic point of view)**.** For every surface in the sample, using Algorithm 2.15 and Theorem 2.21, we determined all the BM-relevant primes. I.e., those for which ev_p is non-constant.

For each of the two surfaces with $\mathrm{Br}(S)_2$ of dimension two, one Brauer class works at 2 and 13, another at 5 and 13, and the third at all three.

Among the other surfaces, we found no relevant prime, six times, one relevant prime, 428 times, two 1577 times, three 1119 times, four 276 times, and five nine times. Finally, for $(361, 192, -196, -121)$, the Brauer class works at 2, 5, 7, 11, 13, and 19.

For three surfaces, it happened that the corresponding elliptic curves were isogenous over a proper extension of $\mathbb{Q}$. In these cases, the Brauer-Manin obstruction is algebraic. For two of the surfaces, it worked at one prime and at two for the last.

4.4 (The BM-relevant primes—$\mathbb{Q}$-rational points)**.** When the Brauer class α works at l primes $p_1, \ldots, p_l$, there are 2^l vectors consisting only of zeroes and $\frac{1}{2}$'s. By the Brauer-Manin obstruction, half of them are forbidden as values of $(\mathrm{ev}_{\alpha,p_1}(x), \ldots, \mathrm{ev}_{\alpha,p_l}(x))$ for $\mathbb{Q}$-rational points $x \in S(\mathbb{Q})$. Using the point search algorithm 3.5, we tested whether for every surface in the sample and each vector not forbidden, there is actually a rational point.

It turned that this was indeed the case. Thus, no further obstruction becomes visible via this colouring. However, in some of the cases, rather high search bounds were necessary. The following table shows, for the extreme case of six relevant primes, the number of vectors hit for several search bounds. Note that we also found 32 vectors when searching only for solutions in smooth numbers.

Table 3. Numbers of vectors in the case $(361, 192, -196, -121)$

bound	50	100	200	400	800	1600	3200	6400	12 800	25 600	50 000	100 000
vectors	7	13	18	21	24	27	30	30	31	31	31	32

For the other surfaces in the sample, lower search bounds were sufficient, but the differences were enormous. We summarize our observations in the table below.

Table 4. Search bounds to get all vectors by rational points

		bound N insufficient for								
#primes	#surfaces	$N = 50$	100	200	400	800	1600	3200	6400	12800
2	1577	267	33	6	-					
3	1119	633	177	18	-					
4	276	266	213	128	65	45	28	7	2	-
5	9	9	9	8	8	7	5	2	1	-

References

[BS] Borevich, Z. I. and Shafarevich, I. R.: *Number theory,* Academic Press, New York-London 1966

[BV] Benito, M. and Varona, J. L.: *Pythagorean triangles with legs less than n,* J. Comput. Appl. Math. **143** (2002), 117–126

[Br] Bright, M.: *The Brauer-Manin obstruction on a general diagonal quartic surface,* Acta Arith. **147** (2011), 291–302

[CG] Cassels, J. W. S. and Guy, M. J. T.: *On the Hasse principle for cubic surfaces,* Mathematika **13** (1966), 111–120

[CKS] Colliot-Thélène, J.-L., Kanevsky, D., and Sansuc, J.-J.: *Arithmétique des surfaces cubiques diagonales,* in: Diophantine approximation and transcendence theory (Bonn 1985), Lecture Notes in Math. 1290, Springer, Berlin 1987, 1–108

[EJ1] Elsenhans, A.-S. and Jahnel, J.: *The Diophantine equation $x^4 + 2y^4 = z^4 + 4w^4$,* Math. Comp. **75** (2006), 935–940

[EJ2] Elsenhans, A.-S. and Jahnel, J.: *On the Brauer-Manin obstruction for cubic surfaces,* J. Combinatorics and Number Theory **2** (2010), 107–128

[EJ3] Elsenhans, A.-S. and Jahnel, J.: *On the quasi group of a cubic surface over a finite field,* arXiv:1102.1278, To appear in: J. Number Theory

[EJ4] Elsenhans, A.-S. and Jahnel, J.: *On the order three Brauer classes for cubic surfaces,* Preprint

[LKL] Logan, A., McKinnon, D., and van Luijk, R.: *Density of rational points on diagonal quartic surfaces,* Algebra & Number Theory **4** (2010), 1–20

[Ma] Manin, Yu. I.: *Cubic forms,* North-Holland Publishing Co. and American Elsevier Publishing Co., Amsterdam-London and New York 1974

[Mo] Mordell, L. J.: *On the conjecture for the rational points on a cubic surface,* J. London Math. Soc. **40** (1965), 149–158

[Pr] Preu, T.: *Transcendental Brauer-Manin obstruction for a diagonal quartic surface,* Ph. D. thesis, Zürich 2010

[Si] Silverman, J. H.: *The arithmetic of elliptic curves,* Graduate Texts in Mathematics 106, Springer, New York 1986

[SD] Swinnerton-Dyer, Sir P.: *Two special cubic surfaces,* Mathematika **9** (1962), 54–56

[SZ] Skorobogatov, A. N. and Zarhin, Yu. G.: *The Brauer group of Kummer surfaces and torsion of elliptic curves,* arXiv:0911.2261, To appear in: J. reine angew. Math.

Mathematisches Institut, Universität Bayreuth, Universitätsstrasse 30, D-95440 Bayreuth, Germany

E-mail address: Stephan.Elsenhans@uni-bayreuth.de

URL: http://www.staff.uni-bayreuth.de/∼btm216

Département Mathematik, Universität Siegen, Walter-Flex-Strasse 3, D-57068 Siegen, Germany

E-mail address: jahnel@mathematik.uni-siegen.de

URL: http://www.uni-math.gwdg.de/jahnel