K3 surfaces of Picard rank one and degree two

Andreas-Stephan Elsenhans and Jörg Jahnel

Universität Göttingen, Mathematisches Institut, Bunsenstraße 3–5,
D-37073 Göttingen, Germany*
elsenhan@wwwuser.gwdg.de, ~jjahnel@wwwuser.gwdg.de

Abstract. We construct explicit examples of K3 surfaces over $\mathbb{Q}$ which are of degree 2 and geometric Picard rank 1. We construct, particularly, examples of the form $w^2 = \det M$ where M is a (3×3)-matrix of ternary quadratic forms.

1 Introduction

A K3 surface is a simply connected, projective algebraic surface with trivial canonical class. If $S \subset \mathbf{P}^n$ is a K3 surface then its degree is automatically even. For every even number $d > 0$, there exists a K3 surface $S \subset \mathbf{P}^n$ of degree d.

Examples 1. A K3 surface of degree two is a double cover of $\mathbf{P}^2$, ramified in a smooth sextic. K3 surfaces of degree four are smooth quartics in $\mathbf{P}^3$. A K3 surface of degree six is a smooth complete intersection of a quadric and a cubic in $\mathbf{P}^4$. And, finally, K3 surfaces of degree eight are smooth complete intersections of three quadrics in $\mathbf{P}^5$.

The Picard group of a K3 surface is isomorphic to $\mathbb{Z}^n$ where n may range from 1 to 20. It is generally known that a generic K3 surface over $\mathbb{C}$ is of Picard rank one. This does, however, not yet imply that there exists a K3 surface over $\mathbb{Q}$ the geometric Picard rank of which is equal to one. The point is, genericity means that there are countably many exceptional subvarieties in moduli space.

It seems that the first explicit examples of K3 surfaces of geometric Picard rank one have been constructed as late as in 2005 [vL]. All these examples are of degree four.

The goal of this article is to provide explicit examples of K3 surfaces over $\mathbb{Q}$ which are of geometric Picard rank one and degree two.

* The computer part of this work was executed on the Sun Fire V20z Servers of the Gauß Laboratory for Scientific Computing at the Göttingen Mathematisches Institut. Both authors are grateful to Prof. Y. Tschinkel for the permission to use these machines as well as to the system administrators for their support.

For that, let first $\mathscr{S}$ be a K3 surface over a finite field $\mathbb{F}_q$. Then, we have the first Chern class homomorphism

$$c_1\colon\ \mathrm{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_q}) \longrightarrow H^2_{\text{ét}}(\mathscr{S}_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_l(1))$$

into l-adic cohomology at our disposal. There is a natural operation of the Frobenius on $H^2_{\text{ét}}(\mathscr{S}_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_l(1))$. All eigenvalues are of absolute value 1. The Frobenius operation on the Picard group is compatible with the operation on cohomology.

Every divisor is defined over a finite extension of the ground field. Consequently, on the subspace $\mathrm{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_q})\otimes_{\mathbb{Z}}\overline{\mathbb{Q}}_l \hookrightarrow H^2_{\text{ét}}(\mathscr{S}_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_l(1))$, all eigenvalues are roots of unity. Those correspond to eigenvalues of the Frobenius operation on $H^2_{\text{ét}}(\mathscr{S}_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_l)$ which are of the form $q\zeta$ for ζ a root of unity.

We may therefore estimate the rank of the Picard group $\mathrm{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_q})$ from above by counting how many eigenvalues are of this particular form. It is conjectured that this estimate is always sharp but we avoid to make use of this.

Estimates from below may be obtained by explicitly constructing divisors. Under certain circumstances, it is possible, that way, to determine $\mathrm{rk}\,\mathrm{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_q})$, exactly.

Our general strategy is to use reduction modulo p. We apply the inequality

$$\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) \leq \mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{F}}_p})$$

which is true for every smooth variety S over $\mathbb{Q}$ and every prime p of good reduction [Fu, Example 20.3.6, 19.3.1.iii) and iv))]. Having constructed an example with $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{F}}_3}) = \mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{F}}_5}) = 2$, we use the same technique as in [vL] to deduce $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) = 1$.

Remark 2. Let S be a K3 surface over $\mathbb{Q}$ of degree two and geometric Picard rank one. Then, S cannot be isomorphic, not even over $\overline{\mathbb{Q}}$, to a K3 surface $S' \subset \mathbf{P}^3$ of degree 4.

Indeed, $\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) = \mathbb{Z}\cdot\langle\mathscr{L}\rangle$ and $\deg S = 2$ mean that the intersection form on $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ is given by $\langle\mathscr{L}^{\otimes n}, \mathscr{L}^{\otimes m}\rangle := 2nm$. The self-intersection numbers of divisors on $S_{\overline{\mathbb{Q}}}$ are of the form $2n^2$ which is always different from 4.

2 Lower bounds for the Picard rank

In order to estimate the rank of the Picard group from below, we need to explicitly construct divisors. Calculating discriminants, it is possible to show that the corresponding divisor classes are linearly independent.

Notation 3. Let k be an algebraically closed field of characteristic $\neq 2$. In the projective plane $\mathbf{P}^2_k$, let a smooth curve B of degree 6 be given by $f_6(x, y, z) = 0$. Then, $w^2 = f_6(x, y, z)$ defines a K3 surface $\mathscr{S}$ in a weighted projective space. We have a double cover $\pi\colon \mathscr{S} \to \mathbf{P}^2$ ramified at $\pi^{-1}(B)$.

Construction 4. i) One possible construction with respect to our aims is to start with a branch curve "$f_6 = 0$" which allows a tritangent line G. The pull-back of G to the K3 surface $\mathscr{S}$ is a divisor splitting into two irreducible components. The corresponding divisor classes are linearly independent.

ii) A second possibility is to use a conic which is tangent to the branch sextic in six points.

Both constructions yield a lower bound of 2 for the rank of the Picard group.

Tritangent. Assume, the line G is a tritangent to the sextic given by $f_6 = 0$. This means, the restriction of f_6 to $G \cong \mathbf{P}^1$ is a section of $\mathscr{O}(6)$, the divisor of which is divisible by 2 in $\mathrm{Div}(G)$. As G is of genus 0, this implies $f_6|_G$ is the square of a section $f \in \Gamma(G, \mathscr{O}(3))$. The form f_6 may, therefore, be written as $f_6 = \widetilde{f}^2 + lq_5$ for l a linear form defining G, $\widetilde{f}$ a cubic form lifting f, and a quintic form q_5.

Consequently, the restriction of π to $\pi^{-1}(G)$ is given by an equation of the form $w^2 = f^2(s,t)$. Hence, we have $\pi^*(G) = D_1 + D_2$ where D_1 and D_2 are the two irreducible divisors given by $w = \pm f(s,t)$. Both curves are isomorphic to G. In particular, they are projective lines.

The adjunction formula shows $-2 = D_1(D_1 + K) = D_1^2$. Analogously, one sees $D_2^2 = -2$. Finally, we have $G^2 = 1$. It follows that $(D_1 + D_2)^2 = 2$ which yields $D_1 D_2 = 3$. Thus, for the discriminant, we find

$$\mathrm{Disc}\langle D_1, D_2\rangle = \begin{vmatrix} -2 & 3 \\ 3 & -2 \end{vmatrix} = -5 \neq 0$$

guaranteeing $\mathrm{rk}\,\mathrm{Pic}(\mathscr{S}) \geq 2$.

Remark 5. We note explicitly that this argument works without modification if two or all three points of tangency coincide.

Conic tangent in six points. If C is a conic tangent to the branch curve "$f_6 = 0$" in six points then, for the same reasons as above, we have $\pi^*(C) = C_1 + C_2$ where C_1 and C_2 are irreducible divisors. Again, C_1 and C_2 are isomorphic to C and, therefore, of genus 0. This shows $C_1^2 = C_1^2 = -2$.

We have another divisor at our disposal, the pull-back $D := \pi^*(G)$ of a line in $\mathbf{P}^2_k$. $G^2 = 1$ implies that $D^2 = 2$. Further, we have $GC = 2$ which implies $D(C_1 + C_2) = 4$ and $DC_1 = 2$. For the discriminant, we obtain

$$\mathrm{Disc}\langle C_1, D\rangle = \begin{vmatrix} -2 & 2 \\ 2 & 2 \end{vmatrix} = -8 \neq 0.$$

Consequently, $\mathrm{rk}\,\mathrm{Pic}(\mathscr{S}) \geq 2$ in this case, too.

Remark 6. There is no further refinement of $\langle C_1, D\rangle$ to lattice in $\mathrm{Pic}(\mathscr{S})$ of discriminant (-2). Indeed, the self-intersection number of a curve on a K3 surface is always even. Hence, the discriminant of an arbitrary rank two lattice in $\mathrm{Pic}(\mathscr{S})$ is of the shape $\left|\begin{smallmatrix} 2a & c \\ c & 2b \end{smallmatrix}\right| = 4ab - c^2$ for $a, b \in \mathbb{Z}$. The quadratic form on the right hand side does not represent integers which are 1 or 2 modulo 4.

The discriminant of the lattice spanned by C_1 and C_2 turns out to be $\mathrm{Disc}\langle C_1, C_2\rangle = \left|\begin{smallmatrix} -2 & 6 \\ 6 & -2 \end{smallmatrix}\right| = -32 \neq 0$ which would be completely sufficient for our purposes.

Remark 7. Further tritangents or further conics which are tangent in six points lead to even larger Picard groups.

Detection of tritangents. The property of a line of being a tritangent may easily be written down as an algebraic condition. Therefore, tritangents may be searched for, in practice, by investigating a Gröbner base.

More precisely, a general line in $\mathbf{P}^2$ can be described by a parametrization

$$g_{a,b}\colon t \mapsto [1 : t : (a+bt)] \,.$$

$g_{a,b}$ is a (possibly degenerate) tritangent of the sextic given by $f_6 = 0$ if and only if $f_6 \circ g_{a,b}$ is a perfect square in $\overline{\mathbb{F}}_q[t]$. This means,

$$f_6(g_{a,b}(t)) = (c_0 + c_1 t + c_2 t^2 + c_3 t^3)^2$$

is an equation which encodes the tritangent property of $g_{a,b}$. Comparing coefficients, this yields a system of seven equations in c_0, c_1, c_2, and c_3 which is solvable if and only if $g_{a,b}$ is a tritangent.

The latter may be understood as well as a system of equations in a, b, c_0, c_1, c_2, and c_3 encoding the existence of a tritangent of the form above. Corresponding to this system of equations, there is an ideal $I \subseteq \mathbb{F}_q[a,b,c_0,c_1,c_2,c_3]$ given explicitly by seven generators.

The remaining one-dimensional family of lines may be treated analogously using the parametrizations $g_a\colon t \mapsto [1 : a : t]$ and $g\colon t \mapsto [0 : 1 : t]$. Similarly, this leads to ideals $I' \subseteq \mathbb{F}_q[a,c_0,c_1,c_2,c_3]$ and $I'' \subseteq \mathbb{F}_q[c_0,c_1,c_2,c_3]$.

Thus, there is a simple method to find out whether the sextic given by $f_6 = 0$ has a tritangent or not.

Algorithm 8 (Given a sextic form f_6 over $\mathbb{F}_q$, this algorithm decides whether the curve given by $f_6 = 0$ has a tritangent**).**

i) Compute a Gröbner base for the ideal $I \subseteq \mathbb{F}_q[a,b,c_0,c_1,c_2,c_3]$, described above.

ii) Compute a Gröbner base for the ideal $I' \subseteq \mathbb{F}_q[a,c_0,c_1,c_2,c_3]$.

iii) Compute a Gröbner base for the ideal $I'' \subseteq \mathbb{F}_q[c_0,c_1,c_2,c_3]$.

iv) If it turns out that actually all three ideals are equal to the unit ideal then output that the curve given has no tritangent. Otherwise, output that a tritangent was detected.

Remark 9. There are a few obvious refinements.

i) For example, given the Gröbner bases, it is easy to calculate the lengths of the quotient rings $\mathbb{F}_q[a,b,c_0,c_1,c_2,c_3]/I$, $\mathbb{F}_q[a,c_0,c_1,c_2,c_3]/I'$, and $\mathbb{F}_q[c_0,c_1,c_2,c_3]/I''$. Each of them is twice the number of the corresponding tritangents.

ii) Usually, from the Gröbner bases, the tritangents may be read off, directly.

Remark 10. We ran Algorithm 8 using `Magma`. The time required to compute a Gröbner base as needed over a finite field is usually a few seconds.

Remark 11. The existence of a tritangent is a codimension one condition. Over small ground fields, one occasionally finds tritangents on randomly chosen examples.

Searching for conics tangent in six points. A non-degenerate conic in $\mathbf{P}^2$ allows a parametrization of the form

$$c\colon t \mapsto [(c_0 + c_1 t + c_2 t^2) : (d_0 + d_1 t + d_2 t^2) : (e_0 + e_1 t + e_2 t^2)] \, .$$

With the sextic given by $f_6 = 0$, all intersection multiplicities are even if and only if $f_6 \circ c$ is a perfect square in $\overline{\mathbb{F}}_q[t]$. This may easily be checked by factoring $f_6 \circ c$.

Algorithm 12 (Given a sextic form f_6 over $\mathbb{F}_q$, this algorithm decides whether the curve given by $f_6 = 0$ allows a conic defined over $\mathbb{F}_q$ which is tangent in six points)**.**

i) In a precomputation, generate a list of parametrizations, one for each of the $q^2(q^3 - 1)$ non-degenerate conics defined over $\mathbb{F}_q$.

ii) Run through the list. For each parametrization, factorize the univariate polynomial $f_6 \circ c$ into irreducible factors. If it turns out to be a perfect square then output that a conic which is tangent in six points has been found.

Remarks 13. a) For very small q, this algorithm is extremely efficient. We need it only for $q = 3$ and 5.

b) A general method, analogous to the one for tritangents, to find conics defined over $\overline{\mathbb{F}}_q$ does not succeed. The required Gröbner base computation becomes too large.

3 An upper bound for the geometric Picard rank

In this section, we consider a K3 surface $\mathscr{S}$ over a finite field $\mathbb{F}_p$. A method to understand the operation of the Frobenius ϕ on the l-adic cohomology $H^2_{\text{ét}}(\mathscr{S}_{\overline{\mathbb{F}}_p}, \overline{\mathbb{Q}}_l) \cong \overline{\mathbb{Q}}_l^{22}$ works as follows.

The Lefschetz trace formula. Count the points on $\mathscr{S}$ over $\mathbb{F}_{p^d}$ and apply the Lefschetz trace formula [Mi] to compute the trace of the Frobenius $\phi_{\mathbb{F}_{p^d}} = \phi^d$. In our situation, this yields

$$\mathrm{Tr}(\phi^d) = \#\mathscr{S}(\mathbb{F}_{p^d}) - p^{2d} - 1 \, .$$

We have $\mathrm{Tr}(\phi^d) = \lambda_1^d + \dots + \lambda_{22}^d =: \sigma_d(\lambda_1, \dots, \lambda_{22})$ when we denote the eigenvalues of ϕ by $\lambda_1, \dots, \lambda_{22}$. Newton's identity [Ze]

$$s_k(\lambda_1, \dots, \lambda_{22}) = \frac{1}{k} \sum_{r=0}^{k-1} (-1)^{k+r+1} \sigma_{k-r}(\lambda_1, \dots, \lambda_{22}) s_r(\lambda_1, \dots, \lambda_{22})$$

shows that, doing this for $d = 1, \dots, k$, one obtains enough information to determine the coefficient $(-1)^k s_k$ of t^{22-k} of the characteristic polynomial f_p of ϕ.

Remark 14. Observe that we also have the functional equation

$$(*) \qquad p^{22} f_p(t) = \pm t^{22} f_p(p^2/t)$$

at our disposal. It may be used to convert the coefficient of t^i into the one of t^{22-i}.

Algorithms for counting points. The number $\#\mathscr{S}(\mathbb{F}_q)$ of points may be determined as the sum

$$\sum_{[x:y:z]\in\mathbf{P}^2(\mathbb{F}_q)} \left[1 + \chi\big(f_6(x,y,z)\big)\right].$$

Here, χ is the quadratic character of $\mathbb{F}_q^*$. The sum is well-defined since $f_6(x, y, z)$ is uniquely determined up to a sixth-power residue. To count the points naively, one would need $q^2 + q + 1$ evaluations of f_6 and χ.

Here, an obvious possibility for optimization arises. We may use symmetry: If f_6 is defined over $\mathbb{F}_p$ then the summands for $[x : y : z]$ and $\phi([x : y : z])$ are equal.

Algorithm 15 (Point counting)**.**

i) Precompute a list which contains exactly one representative for each Galois orbit of $\mathbb{F}_q$. Equip each member y with an additional marker s_y indicating the size of its orbit.

ii) Let $[0 : y : z]$ run through all $\mathbb{F}_q$-rational points on the projective line and add up the values of $[1 + \chi\big(f_6(0, y, z)\big)]$ to a sum Z.

iii) In an iterated loop, let y run through the precomputed list and z through the whole of $\mathbb{F}_q$. Add up Z and all values of $s_y{\cdot}[1 + \chi\big(f_6(1, y, z)\big)]$.

Remark 16. Over $\mathbb{F}_{p^d}$, we save a factor of about d as, on the affine chart "$x \neq 0$", we put in for y only values from a fundamental domain of the Frobenius.

A second possibility for optimization is to use decoupling: Suppose, f_6 is decoupled, i.e., it contains only monomials of the form $x^i y^{6-i}$ or $x^i z^{6-i}$. Then, on the affine chart "$x \neq 0$", the form f_6 may be written as $f_6(1, y, z) = g(y) + h(z)$. If f_6 is defined over $\mathbb{F}_p$ then we still may use symmetry. The ranges of g and h are invariant under the operation of Frobenius. There is an algorithm as follows.

Algorithm 17 (Point counting – decoupled situation)**.**

i) For the function g, generate a list A of its values. For each $u \in A$, store the number $n_A(u)$ indicating how many times it is adopted by g.

ii) For the function h, generate a list B of its values. For each $v \in B$, store the number $n_B(v)$ indicating how many times it is adopted by h.

iii) Modify the table for g. For each orbit $F = \{u_1, \ldots, u_e\}$ of the Frobenius, delete all elements except one, say u_1. Multiply $n_A(u_1)$ by $\#F$.

iv) Tabulate the quadratic character χ.

v) Let $[0 : y : z]$ run through all $\mathbb{F}_q$-rational points on the projective line and add up the values of $[1 + \chi\big(f_6(0, y, z)\big)]$ to a sum Z.

vi) Use the table for χ and the tables built up in steps i) through iii) to compute the sum

$$\sum_{u \in A} \sum_{v \in B} \chi(u + v) \cdot n_A(u) \cdot n_B(v).$$

vii) Add $q^2 + Z$ to the number obtained.

Remarks 18. i) The tables for g and h may be built up in $O(q \log q)$ steps.

ii) Statistically, after steps i) and ii) the sizes of A and B are approximately $(1-1/e) \cdot q = (1-1/e) \cdot p^d$. Step iii) reduces the size of A almost to $(1-1/e) \cdot p^d/d$. After all the preparations, we therefore expect about $(1 - 1/e)^2 \cdot q^2/d$ additions to be executed in step vi).

The advantage of a decoupled situation is, therefore, not only that evaluations of the polynomial f_6 in $\mathbb{F}_{p^d}$ get replaced by additions. Furthermore, the expected number of additions is only about 40% of the number of evaluations of f_6 required by Algorithm 15.

Remark 19. We implemented the point counting algorithms in `C`. The optimization realized in Algorithm 15 allows to determine the number of $\mathbb{F}_{3^{10}}$-rational points on $\mathscr{S}$ within half an hour on an AMD Opteron processor.

In a decoupled situation, the number of $\mathbb{F}_{5^9}$-rational points may be counted within two hours by Algorithm 17. In a few cases, we determined the numbers of points over $\mathbb{F}_{5^{10}}$. This took around two days. Using Algorithm 15, the same counts would have taken around one day or 25 days, respectively.

This shows, using the methods above, we may effectively compute the traces of $\phi_{\mathbb{F}_{p^d}} = \phi^d$ for $d = 1, \ldots, 9, (10)$.

Remark 20. In Algorithm 17, the sum calculated in step vi) is nothing but $\sum_{w \in \mathbb{F}_q} \chi(w) \cdot (n_A * n_B)(w)$. It might be on option to compute the convolution $n_A * n_B$ using FFT. We expect that, concerning running times, this might lead to a certain gain. On the other hand, such an algorithm would require a lot more space than Algorithm 17.

This possible use of FFT could be of interest from a theoretical point of view. It is well-known that, in most applications, FFT is used on large cyclic groups. Here, however, the group is $(\mathbb{F}_{p^d}, +) \cong (\mathbb{Z}/p\mathbb{Z})^d$ for p very small.

An upper bound for $\operatorname{rk} \operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p})$ having counted till $d = 10$.

We know that f_p, the characteristic polynomial of the Frobenius, has a zero at p since the pull-back of a line in $\mathbf{P}^2$ is a divisor defined over $\mathbb{F}_p$. Suppose, we determined $\operatorname{Tr}(\phi^d)$ for $d = 1, \ldots, 10$. Then, we may use the following algorithm.

Algorithm 21 (Upper bound for $\operatorname{rk}\operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p})$)**.**

i) First, assume the minus sign in the functional equation $(*)$. Then, f_p automatically has coefficient 0 at t^{11}. Therefore, the numbers of points counted suffice in this case to determine f_p, completely.

ii) Then, assume that, on the other hand, the plus sign is present in $(*)$. In this case, the data collected immediately allow to compute all coefficients of f_p, except that at t^{11}. Use the known zero at p to determine that final coefficient.

iii) Use the numerical test, provided by Algorithm 23 below, to decide which sign is actually present.

iv) Factor $f_p(pt)$ into irreducible polynomials. Check which of the factors are cyclotomic polynomials, add their degrees, and output that sum as an upper bound for $\operatorname{rk}\operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p})$. If step iii) had failed then work with both candidates for f_p and output the maximum.

Verifying $\operatorname{rk}\operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p}) = 2$ having counted till $d = 9$, only.
Assume, $\mathscr{S}$ is a K3 surface over $\mathbb{F}_p$ given by Construction 4.i) or ii). We, therefore, know that the rank of the Picard group is at least equal to 2. We assume that the divisor constructed by pull-back splits already over $\mathbb{F}_p$. This ensures p is a double zero of f_p.

Suppose, we determined $\operatorname{Tr}(\phi^d)$ for $d = 1, \ldots, 9$. Then, there is the following algorithm.

Algorithm 22 (Verifying $\operatorname{rk}\operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p}) = 2$)**.**

i) First, assume the minus sign in the functional equation $(*)$. This forces another zero of f_p at $(-p)$. The data collected are then sufficient to determine f_p, completely. Algorithm 23 below may indicate a contradiction. Otherwise, output `FAIL` and terminate prematurely. (In this case, we could still find an upper bound for $\operatorname{rk}\operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p})$ which is, however, at least equal to 4.)

ii) As we have the plus sign in $(*)$, the data immediately suffice to compute all coefficients of f_p, with the exception of those at t^{10}, t^{11}, and t^{12}. The functional equation yields a linear relation for the three remaining coefficients of f_p. From the known double zero at p, one computes another linear condition.

iii) Let n run through all natural numbers such that $\varphi(n) \leq 20$. (The largest such n is 66.)

Assume, in addition, that there is another zero of the form $p\zeta_n$. This yields further linear relations. Inspecting this system of linear equations, one either achieves a contradiction or determines all three remaining coefficients. In the latter case, Algorithm 23 may indicate a contradiction. Otherwise, output `FAIL` and terminate prematurely.

iv) Output that $\operatorname{rk}\operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p}) = 2$.

Algorithm 23 (A numerical test – Given a polynomial f, this test may prove that f is not the characteristic polynomial of the Frobenius).

i) Given $f \in \mathbb{Z}[t]$ of degree 22, calculate all its zeroes as complex floating point numbers.

ii) If at least one of them is of an absolute value clearly different from p then output that f can not be the characteristic polynomial of the Frobenius for any K3 surface over $\mathbb{F}_p$. Otherwise, output `FAIL`.

Remark 24. Consequently, the equality $\operatorname{rk}\operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p}) = 2$ may be effectively provable having determined $\operatorname{Tr}(\phi^d)$ for $d = 1, \ldots, 9$, only. This is of importance since point counting over $\mathbb{F}_{5^{10}}$ is not that fast, even in a decoupled situation.

Possible values of the upper bound. This approach will always yield an even number for the upper bound of the geometric Picard rank. Indeed, the bound we use is

$$\operatorname{rk}\operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p}) \leq \dim(H^2_{\text{ét}}(\mathscr{S}_{\overline{\mathbb{F}}_p}, \overline{\mathbb{Q}}_l)) - \#\{\text{ zeroes of } f_p \text{ not of the form } \zeta_n p\,\}\,.$$

The relevant zeroes come in pairs of complex conjugate numbers. Hence, for a K3 surface the bound is always even.

Remark 25. There is a famous conjecture due to John Tate [Ta] which implies that the canonical injection $c_1\colon\ \operatorname{Pic}(\mathscr{S}_{\overline{\mathbb{F}}_p}) \to H^2_{\text{ét}}(\mathscr{S}_{\overline{\mathbb{F}}_p}, \overline{\mathbb{Q}}_l(1))$ maps actually onto the sum of all eigenspaces for the eigenvalues which are roots of unity. Together with the conjecture of J.-P. Serre claiming that the Frobenius operation on étale cohomology is always semisimple, this would imply that the bound above is actually sharp.

It is a somewhat surprising consequence of the Tate conjecture that the Picard rank of a K3 surface over $\overline{\mathbb{F}}_p$ is always even. For us, this is bad news. The obvious strategy to prove $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 1$ for a K3 surface S over $\mathbb{Q}$ would be to verify $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{F}}_p}) = 1$ for a suitable place p of good reduction. The Tate conjecture, however, indicates that there is no hope for such an approach.

4 Proving $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 1$

Using the methods described above, on one hand, we can construct even upper bounds for the Picard rank. On the other hand, we can generate lower bounds by explicitly stating divisors. In an optimal situation, this may establish an equality $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{F}}_p}) = 2$.

How is it possible that way to reach Picard rank 1 for a surface S defined over $\mathbb{Q}$? For this, a technique due to R. van Luijk [vL, Remark 2] is helpful.

Lemma 26. *Assume that we are given a K3 surface $\mathscr{S}^{(3)}$ over $\mathbb{F}_3$ and a K3 surface $\mathscr{S}^{(5)}$ over $\mathbb{F}_5$ which are both of geometric Picard rank 2. Suppose further that the discriminants of the intersection forms on $\operatorname{Pic}(\mathscr{S}^{(3)}_{\overline{\mathbb{F}}_3})$ and $\operatorname{Pic}(\mathscr{S}^{(5)}_{\overline{\mathbb{F}}_5})$ are essentially different, i.e., their quotient is not a perfect square in $\mathbb{Q}$.*

Then, every K3 surface S over $\mathbb{Q}$ such that its reduction at 3 is isomorphic to $\mathscr{S}^{(3)}$ and its reduction at 5 is isomorphic to $\mathscr{S}^{(5)}$ is of geometric Picard rank one.

Proof. The reduction maps $\iota_p\colon \operatorname{Pic}(S_{\overline{\mathbb{Q}}}) \to \operatorname{Pic}(S_{\overline{\mathbb{F}}_p}) = \operatorname{Pic}(\mathscr{S}^{(p)}_{\overline{\mathbb{F}}_p})$ are injective [Fu, Example 20.3.6]. Observe here, $\operatorname{Pic}(S_{\overline{\mathbb{Q}}})$ is equal to the group of divisors on $S_{\overline{\mathbb{Q}}}$ modulo numerical equivalence.

This immediately leads to the bound $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) \leq 2$. Assume, by contradiction, that equality holds. Then, the reductions of $\operatorname{Pic}(S_{\overline{\mathbb{Q}}})$ are sublattices of maximal rank in both, $\operatorname{Pic}(S_{\overline{\mathbb{F}}_3}) = \operatorname{Pic}(\mathscr{S}^{(3)}_{\overline{\mathbb{F}}_3})$ and $\operatorname{Pic}(S_{\overline{\mathbb{F}}_5}) = \operatorname{Pic}(\mathscr{S}^{(5)}_{\overline{\mathbb{F}}_5})$.

The intersection product is compatible with reduction. Therefore, the quotients $\operatorname{Disc}\operatorname{Pic}(S_{\overline{\mathbb{Q}}})/\operatorname{Disc}\operatorname{Pic}(\mathscr{S}^{(3)}_{\overline{\mathbb{F}}_3})$ and $\operatorname{Disc}\operatorname{Pic}(S_{\overline{\mathbb{Q}}})/\operatorname{Disc}\operatorname{Pic}(\mathscr{S}^{(5)}_{\overline{\mathbb{F}}_5})$ are perfect squares. This is a contradiction to the assumption. □

Remark 27. Suppose that $\mathscr{S}^{(3)}$ and $\mathscr{S}^{(5)}$ are K3 surfaces of degree two given by explicit branch sextics in $\mathbf{P}^2$. Then, using the Chinese Remainder Theorem, they can easily be combined to a K3 surface S over $\mathbb{Q}$.

Assume $\operatorname{rk}\operatorname{Pic}(\mathscr{S}^{(3)}_{\overline{\mathbb{F}}_3}) = 2$ and $\operatorname{rk}\operatorname{Pic}(\mathscr{S}^{(5)}_{\overline{\mathbb{F}}_5}) = 2$. If one of the two branch sextics allows a conic tangent in six points and the other a tritangent then the discriminants of the intersection forms on $\operatorname{Pic}(\mathscr{S}^{(3)}_{\overline{\mathbb{F}}_3})$ and $\operatorname{Pic}(\mathscr{S}^{(5)}_{\overline{\mathbb{F}}_5})$ are essentially different as shown in section 2.

5 An example

Examples 28. We consider two particular K3 surfaces.

i) By $\mathscr{X}^0$, we denote the surface over $\mathbb{F}_3$ given by the equation

$$w^2 = (y^3 - x^2y)^2 + (x^2 + y^2 + z^2)(2x^3y + x^3z + 2x^2yz + x^2z^2 + 2xy^3 + 2y^4 + z^4)\,.$$

ii) Further, let $\mathscr{Y}^0$ be the K3 surface over $\mathbb{F}_5$ given by

$$w^2 = x^5y + x^4y^2 + 2x^3y^3 + x^2y^4 + xy^5 + 4y^6 + 2x^5z + 2x^4z^2 + 4x^3z^3 + 2xz^5 + 4z^6\,.$$

Theorem 29. *Let S be any K3 surface over $\mathbb{Q}$ such that its reduction modulo 3 is isomorphic to $\mathscr{X}^0$ and its reduction modulo 5 is isomorphic to $\mathscr{Y}^0$. Then,* $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 1$.

Proof. We follow the strategy described in Remark 27. For the branch locus of $\mathscr{X}^0$, the conic given by $x^2 + y^2 + z^2 = 0$ is tangent in six points. The branch locus of Y_0 has a tritangent given by $z - 2y = 0$. It meets the branch locus at $[1:0:0]$, $[1:3:1]$, and $[0:1:2]$.

It remains necessary to show that $\operatorname{rk}\operatorname{Pic}(\mathscr{X}^0_{\overline{\mathbb{F}}_3}) \leq 2$ and $\operatorname{rk}\operatorname{Pic}(\mathscr{Y}^0_{\overline{\mathbb{F}}_5}) \leq 2$. To verify the first assertion, we ran Algorithm 21 together with Algorithm 15 for counting the points. For the second assertion, we applied Algorithm 22 and Algorithm 17. Note that, for $\mathscr{Y}^0$, the sextic form on the right hand side is decoupled. □

Corollary 30. *Let S be the K3 surface given by*

$$\begin{aligned} w^2 = {}& 11x^5y+7x^5z+x^4y^2+5x^4yz+7x^4z^2+7x^3y^3+10x^3y^2z+5x^3yz^2+4x^3z^3 \\ & + 6x^2y^4+5x^2y^3z+10x^2y^2z^2+5x^2yz^3+5x^2z^4+11xy^5+5xy^3z^2+12xz^5 \\ & + 9y^6 + 5y^4z^2 + 10y^2z^4 + 4z^6 \,. \end{aligned}$$

i) *Then,* $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 1$.

ii) *Further,* $S(\mathbb{Q}) \neq \emptyset$. $[2\,;\,0:0:1]$ *and* $[3\,;\,0:1:0]$ *are examples of* $\mathbb{Q}$*-rational points on* S.

Remark 31. a) For the K3 surface $\mathscr{X}^0$, the assumption of the negative sign leads to zeroes the absolute values of which range (without scaling) from 2.598 to 3.464. Thus, the sign in the functional equation is positive. For the decomposition of the characteristic polynomial f_p of the Frobenius, we find (after scaling to zeroes of absolute value 1)

$$\begin{aligned} (t-1)^2(3t^{20} + 2t^{19} + 2t^{18} + 2t^{17} + t^{16} - 2t^{13} - 2t^{12} - t^{11} - 2t^{10} \\ - t^9 - 2t^8 - 2t^7 + t^4 + 2t^3 + 2t^2 + 2t + 3)/3 \end{aligned}$$

with an irreducible polynomial of degree 20.

b) For the K3 surface $\mathscr{Y}^0$, the assumption of the negative sign leads to zeroes the absolute values of which range (without scaling) from 3.908 to 6.398. The sign in the functional equation is therefore positive. For the decomposition of the scaled characteristic polynomial of the Frobenius, we find

$$\begin{aligned} (t-1)^2(5t^{20} - 5t^{19} - 5t^{18} + 10t^{17} - 2t^{16} - 3t^{15} + 4t^{14} - 2t^{13} - 2t^{12} + t^{11} \\ + 3t^{10} + t^9 - 2t^8 - 2t^7 + 4t^6 - 3t^5 - 2t^4 + 10t^3 - 5t^2 - 5t + 5)/5 \,. \end{aligned}$$

c) For $\mathscr{X}^0$ and $\mathscr{Y}^0$, the sextics appearing on the right hand side are smooth. This was checked by a Gröbner base computation. The numbers of points and the traces of the Frobenius we determined are reproduced in table 1.

6 An example in determinantal form

Lemma 32. *Let M be a matrix of the particular shape*

$$M := \begin{pmatrix} l^2 & q & 0 \\ c & a & b \\ d & 0 & a \end{pmatrix} .$$

Here, l is supposed to be an arbitrary linear form. a, b, c, d, and q are arbitrary quadratic forms, q being non-degenerate and not a multiple of a.

Then, $q(x, y, z) = 0$ defines a smooth conic meeting the sextic given by $\det(M(x, y, z)) = 0$ only with even multiplicities.

Proof. This may be seen by observing the congruence

$$\det(M) \equiv l^2a^2 \pmod{q} \,. \qquad \square$$

Examples 33. i) Let $\mathscr{X}$ be the K3 surface over $\mathbb{F}_3$ given by $w^2 = f_6(x,y,z)$ for

$$f_6(x,y,z) = \det\begin{pmatrix} l^2 & q & 0 \\ c & a & b \\ d & 0 & a \end{pmatrix} = \begin{cases} x^6{+}2x^5y{+}2x^5z{+}2x^4y^2{+}x^4yz{+}x^4z^2{+}x^3y^2z \\ {+}2x^3yz^2{+}2x^3z^3{+}x^2y^4{+}x^2y^3z{+}2x^2yz^3{+}xy^5{+}xy^4z \\ {+}xy^3z^2{+}xyz^4{+}xz^5{+}2y^6{+}2y^5z{+}2y^4z^2{+}y^3z^3{+}yz^5\,. \end{cases}$$

Here, we put

$$\begin{aligned} q &= x^2+y^2+z^2, & l &= 2x+y+z\,, \\ a &= x^2+xy+2z^2, & b &= xy+y^2+yz+2z^2, \\ c &= xy+2xz+z^2, & d &= 2xy+2xz+2y^2+2z^2. \end{aligned}$$

Then, the conic given by $q = 0$ meets the ramification locus such that all intersection multiplicities are even.

ii) Let $\mathscr{Y}$ be the K3 surface over $\mathbb{F}_5$ given by $w^2 = f_6(x,y,z)$ for

$$\begin{aligned} f_6(x,y,z) &= \det\begin{pmatrix} 0 & 2x^2+2xy+4y^2 & 4x^2+2xz \\ 4x^2+2xz+4z^2 & 0 & x^2+2xy+4y^2 \\ 2x^2+xy+4y^2 & x^2+2z^2 & 0 \end{pmatrix} \\ &= 4x^5y+x^4y^2+2x^3y^3+2x^2y^4+4y^6+x^5z+2x^4z^2+xz^5\,. \end{aligned}$$

There appears a degenerate tritangent G given by $x = 0$. It meets the branch sextic at $[0:0:1]$ with intersection multiplicity 6. The divisor $\pi^*(G)$ splits already over $\mathbb{F}_5$.

Remark 34. Over $\mathbb{F}_5$, we intended to construct examples of K3 surfaces of the form $w^2 = \det(M(x,y,z))$ where $M(x,y,z)$ is a (3×3)-matrix the entries of which are quadratic forms.

In order to be able to execute investigations over $\mathbb{F}_5$ in a reasonable amount of time, we needed a decoupled right hand side. This means, $f_6 := \det(M(x,y,z))$ must not contain monomials containing both y and z. In determinantal form, this may easily be achieved by choosing M of the particular structure

$$M(x,y,z) := \begin{pmatrix} 0 & q_1(x,y) & r_1(x,z) \\ r_2(x,z) & 0 & q_2(x,y) \\ q_3(x,y) & r_3(x,z) & 0 \end{pmatrix}.$$

Then, the determinant has the form $\det M = q_1q_2q_3 + r_1r_2r_3$.

Note that, in r_1, the monomial z^2 is missing. This causes that, in f_6, the coefficient of z^6 is equal to zero. Therefore, the line given by $x = 0$ meets the sextic "$\det M(x,y,z) = 0$" in only one point.

Theorem 35. *Let S be any K3 surface over $\mathbb{Q}$ such that its reduction modulo* 3 *is isomorphic to $\mathscr{X}$ and its reduction modulo* 5 *is isomorphic to $\mathscr{Y}$. Then,* $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 1$.

Proof. It remains necessary to show that $\operatorname{rk}\operatorname{Pic}(\mathscr{X}_{\overline{\mathbb{F}}_3}) \leq 2$ and $\operatorname{rk}\operatorname{Pic}(\mathscr{Y}_{\overline{\mathbb{F}}_5}) \leq 2$. To verify the first assertion, we ran Algorithm 21 together with Algorithm 15 for counting the points. For the second assertion, we applied Algorithm 22 and Algorithm 17. Note that, for $\mathscr{Y}$, the sextic form on the right hand side is decoupled. $\square$

Corollary 36. *Let S be the K3 surface given by*

$$\begin{aligned} w^2 &= \det \begin{pmatrix} 10x^2+10xy+10xz+10y^2+5yz+10z^2 & 7x^2+12xy+4y^2+70z^2 & 9x^2+12xz \\ 9x^2+10xy+2xz+4z^2 & 10x^2+10xy+5z^2 & 6x^2+7xy+4y^2+10yz+5z^2 \\ 12x^2+11xy+5xz+14y^2+5z^2 & 6x^2+12z^2 & 10x^2+10xy+5z^2 \end{pmatrix} \\ &= -80x^6 + 194x^5y - 424x^5z + 941x^4y^2 - 125x^4yz - 863x^4z^2 \\ &\quad + 3222x^3y^3 + 520x^3y^2z - 1735x^3yz^2 + 1040x^3z^3 \\ &\quad + 3292x^2y^4 + 1180x^2y^3z + 8370x^2y^2z^2 + 8510x^2yz^3 + 210x^2z^4 \\ &\quad + 1240xy^5 + 2200xy^4z + 10900xy^3z^2 + 7320xy^2z^3 + 2170xyz^4 + 976xz^5 \\ &\quad + 224y^6 + 560y^5z + 3800y^4z^2 + 8560y^3z^3 + 4890y^2z^4 + 2125yz^5 \,. \end{aligned}$$

i) *Then,* $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 1$.

ii) *Further,* $S(\mathbb{Q}) \neq \emptyset$. *For example,* $[0\,;\,0:0:1] \in S(\mathbb{Q})$.

Remark 37. a) For $\mathscr{X}$, the assumption of the negative sign leads to zeroes the absolute values of which range (without scaling) from 2.609 to 3.450. Thus, we have the positive sign in the functional equation. The decomposition of the characteristic polynomial (after scaling to zeroes of absolute value 1) is

$$(t-1)^2(3t^{20}+t^{18}-2t^{17}-t^{15}+t^{13}-t^{12}+3t^{11}+3t^9-t^8+t^7-t^5-2t^3+t^2+3)/3$$

with an irreducible degree 20 polynomial. Therefore, the geometric Picard rank is equal to 2.

b) For $\mathscr{Y}$, the assumption of the negative sign leads to zeroes the absolute values of which range (without scaling) from 4.350 to 5.748. The sign in the functional equation is therefore positive. The decomposition of the scaled characteristic polynomial is

$$\begin{aligned} (t-1)^2(5t^{20} + 5t^{19} - 2t^{18} - 2t^{17} + 2t^{16} - 2t^{15} - 3t^{14} - 2t^{12} + 3t^{10} \\ - 2t^8 - 3t^6 - 2t^5 + 2t^4 - 2t^3 - 2t^2 + 5t + 5)/5 \,. \end{aligned}$$

Consequently, the geometric Picard rank is equal to 2.

c) We list the numbers of points and the traces of the Frobenius we determined in table 1.

Details on the experiments. i) Choosing l, a, b, c, d, and q randomly, we had generated a sample of 30 examples over $\mathbb{F}_3$. For each of them, by inspecting the ideal of the singular locus, we had checked that the branch sextic is smooth. Further, they had passed the tests described in section 2 to exclude the existence of a tritangent or a second conic tangent in six points.

For exactly five of the 30 examples, we found an upper bound of two for the geometric Picard rank. Example 33.i) reproduces one of them. The running time was around 30 minutes per example.

ii) We had randomly generated a series of 30 examples over $\mathbb{F}_5$ in which the branch locus is smooth and does neither allow a conic tangent in six points nor further tritangents.

For each of them, we determined the numbers of points over the fields $\mathbb{F}_{5^d}$ for $d \leq 9$. The method described in section 3 above showed $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{F}}_5}) = 2$ for two of the examples. For these, we further determined the numbers of points over $\mathbb{F}_{5^{10}}$. Example 33.ii) is one of the two.

The code was running for two hours per example which were almost completely needed for point counting. The time required to identify and factorize the characteristic polynomials of the Frobenii was negligible. The point counting over $\mathbb{F}_{5^{10}}$ took around two days of CPU time per example.

iii) The numbers of points counted and the traces of the Frobenius computed in the examples are listed in the table below.

Table 1. Numbers of points and traces of the Frobenius

	$\mathscr{X}^0$		$\mathscr{Y}^0$		$\mathscr{X}$		$\mathscr{Y}$	
d	$\#\mathscr{X}^0(\mathbb{F}_{3^d})$	$\mathrm{Tr}(\phi^d)$	$\#\mathscr{Y}^0(\mathbb{F}_{5^d})$	$\mathrm{Tr}(\phi^d)$	$\#\mathscr{X}(\mathbb{F}_{3^d})$	$\mathrm{Tr}(\phi^d)$	$\#\mathscr{Y}(\mathbb{F}_{5^d})$	$\mathrm{Tr}(\phi^d)$
1	14	4	41	15	16	6	31	5
2	92	10	751	125	94	12	721	95
3	758	28	15 626	0	838	108	15 751	125
4	6 752	190	392 251	1 625	6 742	180	391 701	1 075
5	59 834	784	9 759 376	-6 250	59 671	621	9 781 251	15 625
6	532 820	1 378	244 134 376	-6 250	533 818	2 376	244 155 751	15 125
7	4 796 120	13 150	6 103 312 501	-203 125	4 781 674	-1 296	6 103 878 126	362 500
8	43 068 728	22 006	152 589 156 251	1 265 625	43 081 390	34 668	152 589 507 501	1 616 875
9	387 421 463	973	3 814 704 296 876	7 031 250	387 322 075	-98 415	3 814 693 734 376	-3 531 250
10	3 487 077 812	293 410	95 367 474 609 376	42 968 750	3 486 694 249	-90 153	95 367 469 575 001	37 934 375

References

[Be] Beauville, A.: *Surfaces algébriques complexes,* Astérisque 54, Société Mathématique de France, Paris 1978

[EJ] Elsenhans, A.-S. and Jahnel, J.: *The Asymptotics of Points of Bounded Height on Diagonal Cubic and Quartic Threefolds,* Algorithmic number theory, Lecture Notes in Computer Science 4076, Springer, Berlin 2006, 317–332

[Fu] Fulton, W.: *Intersection theory,* Springer, Berlin 1984

[Li] Lieberman, D. I.: *Numerical and homological equivalence of algebraic cycles on Hodge manifolds,* Amer. J. Math. **90** (1968), 366–374

[vL] van Luijk, R.: *K3 surfaces with Picard number one and infinitely many rational points,* Algebra & Number Theory **1** (2007), 1–15

[Mi] Milne, J. S.: *Étale Cohomology,* Princeton University Press, Princeton 1980

[Pe] Persson, U.: *Double sextics and singular K3 surfaces,* Algebraic geometry, Sitges (Barcelona) 1983, Lecture Notes in Math. 1124, Springer, Berlin 1985, 262–328

[Ta] Tate, J.: *Conjectures on algebraic cycles in l-adic cohomology,* in: Motives, Proc. Sympos. Pure Math. 55-1, Amer. Math. Soc., Providence 1994, 71–83

[Ze] Zeilberger, D.: *A combinatorial proof of Newtons's identities,* Discrete Math. **49** (1984), 319