Large orbits on Markoff-type K3 surfaces over finite fields

Evan M. O’Dorney

November 17, 2022

Abstract

We study the surface $W_k : x^2 + y^2 + z^2 + x^2 y^2 z^2 = kxyz$ in $(\mathbb{P}^1)^3$, a tri-involutive K3 (TIK3) surface. We explain a phenomenon noticed by Fuchs, Litman, Silverman, and Tran: over a finite field of order $\equiv 1 \mod 8$, the points of $W_k$ do not form a single large orbit under the group $\Gamma$ generated by the three involutions fixing two coordinates and a few other obvious symmetries, but rather admit a partition into two $\Gamma$-invariant subsets of roughly equal size. The phenomenon is traced to an explicit double cover of the surface.

1 Introduction

A surface $W$ defined by a general $(2,2,2)$-form on $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ is a K3 surface, possibly singular, admitting three involutions $\sigma_x, \sigma_y, \sigma_z$ that fix two coordinates and flip the third to the other root of the appropriate quadratic equation. In [5], Fuchs, Litman, Silverman and Tran call these tri-involutive K3 (TIK3) surfaces and ask the natural question of the orbit structure of the $F_q$-points of such a $W$ under the group $C_2 \ast C_2 \ast C_2$ generated by the $\sigma_i$. For such a large group, in the absence of additional structure, one normally conjectures that for $q$ large, the points form a single large orbit and possibly some very small orbits.

A TIK3 surface is given by $W_k : x^2 + y^2 + z^2 + x^2 y^2 z^2 = kxyz$, whose $\mathbb{Z}$-points arise in Diophantine approximation, has an action by $S_3 \times (C_2 \times C_2) \cong S_4$ by permuting the coordinates and negating an even number of them. In 1879, Markoff [6] showed that the $\mathbb{Z}$-points $M(\mathbb{Z})$ form a single orbit under the group $\Gamma$ generated by all the symmetries named. In 1991, Baragar [11] conjectured that, after removing the singular point $(0,0,0)$, $M(\mathbb{F}_p)$ consists of one $\Gamma$-orbit for all primes $p$. In 2016, Bourgain, Gamburd, and Sarnak [3, 2] have proved that all orbits but one have size $O_\varepsilon(q^\varepsilon)$ for all $\varepsilon > 0$. Recently, Chen [13] announced a proof that Baragar’s conjecture holds (that is, there is only one nonsingular $\Gamma$-orbit) for all but finitely many $p$.

An even richer symmetry group occurs for the family $W_k : x^2 + y^2 + z^2 + x^2 y^2 z^2 = kxyz$, in which one can also reciprocate an even number of the coordinates. Via numerical experiments, the authors of [5] found that the case $k = \pm 4, q \equiv 1 \mod 8$ is exceptional in that there are two largest orbits of roughly equal size. They conjecture that there is an algebro-geometric reason for this aberration and that it is the only one in its family:

Conjecture 1 ([5, §13]). Let $q$ be an odd prime power. Let $\Gamma$ be the subgroup of automorphisms of $W_k$ generated by the involution $\sigma_z$, the finite-order symmetries $(x, y, z) \mapsto (x, -y, -z)$ and $(x, y, z) \mapsto (x, y^{-1}, z^{-1})$, and the permutations of the coordinates. Then the large $\Gamma$-orbits of the $\mathbb{F}_q$-points of $W_k$ are as follows:

(a) For $k = \pm 4$ or $\pm 4 \sqrt{-1}$, if $q \equiv 1 \mod 8$, there are two orbits of size $\frac{1}{2}q^2 + o(q^2)$.
(b) In all other cases, there is one orbit of size $q^2 + o(q^2)$.

All other orbits are necessarily of size $o(q^2)$.
2 Main theorem

In this paper, we focus our attention on $W_4$. (The surfaces $W_k$ and $W_{-k}$ are isomorphic via negating the coordinates, and if the ground field contains a square root $i$ of $-1$, then $W_k$ and $W_{ik}$ are also isomorphic via multiplying all coordinates by $-i$.) Incidentally, over $\mathbb{R}$, the variety

$$W_4 : x^2 + y^2 + z^2 + x^2y^2z^2 = 4xyz$$

is an equality case of the four-term AM–GM inequality

$$\frac{x^2 + y^2 + z^2 + x^2y^2z^2}{4} \geq \sqrt[4]{x^2 \cdot y^2 \cdot z^2 \cdot x^2y^2z^2} = |xyz|.$$

In particular, $W_4$ has no real points other than the eight singular points, which are $(0, 0, 0)$, $(0, \infty, \infty)$, $(1, 1, 1)$, $(1, -1, -1)$, and their images under permutations of coordinates. There is also an extra symmetry of $W_4$ given by the linear fractional transformation $t \mapsto (1 + t)/(1 - t)$ on each coordinate. This symmetry will not be needed in this note; adjoining it to $\Gamma$ does not change our results.

**Theorem 2.** Let $\Gamma$ be the subgroup of the automorphisms of $W_4$ generated by those mentioned above:

- The transpositions $\tau_{yz}, \tau_{xz}, \tau_{xy}$ of two coordinates;
- The nontrivial automorphism $\sigma_x$ fixing $y$ and $z$;
- The sign change $s_x$ that negates $y$ and $z$;
- The transformation $r_x$ that reciprocates $y$ and $z$.

(Observe that conjugates like $\sigma_y = \tau_{xy} \circ \sigma_x \circ \tau_{xy}^{-1}$ also belong to $\Gamma$.) If $q \equiv 1 \mod 8$, then there is a partition $W_4(\mathbb{F}_q) = U_1 \sqcup U_2$ into two disjoint $\Gamma$-invariant subsets, each of roughly the same size $\frac{1}{2}q^2 + O(q^{3/2})$. In particular, every $\Gamma$-orbit has size at most $\frac{1}{2}q^2 + O(q^{3/2})$.

**Proof.** To prove this theorem, we produce a $\Gamma$-invariant function on the $\mathbb{F}_q$-points of $W_4$. As the condition $q \equiv 1 \mod 8$ suggests, this invariant will be defined over the 8th cyclotomic field $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$.

Let $\Delta_x$ be the discriminant of the equation

$$f = f(x, y, z) = x^2 + y^2 + z^2 + x^2y^2z^2 - 4xyz$$

of $W_4$ considered as a quadratic in $x$. Note that $\Delta_x$ is reducible over $\mathbb{Z}[i]$:

$$\Delta_x = (4yz)^2 - 4(1 + y^2z^2)(y^2 + z^2)$$

$$= 4 \left(y(1 - z^2) + iz(1 - y^2)\right) \cdot \left(y(1 - z^2) - iz(1 - y^2)\right).$$

We denote by $\Delta_{yz}$ the first factor

$$\Delta_{yz} = y(1 - z^2) + iz(1 - y^2)$$

of the discriminant. We claim that it is our desired invariant:

**Lemma 3.** Let $F$ be a field, $2 \neq 0 \in F$, containing all 8th roots of unity. The class $\Delta$ of $\Delta_{yz}$, in the multiplicative group

$$F(W_4)^\times / \left(F(W_4)^\times\right)^2$$

of the function field $F(W_4)$ modulo squares, is invariant under the group $\Gamma$.

**Proof.** Invariance under $\sigma_x$ is clear since $\sigma_x$ preserves the $y$ and $z$ coordinates. Invariance under $s_x$ and $r_x$ is clear using $i \in F$:

$$s_x^*(\Delta_{yz}) = -\Delta_{yz} = i^2 \cdot \Delta_{yz}, \quad r_x^*(\Delta_{yz}) = \left(\frac{1}{yz}\right)^2 \Delta_{yz}.$$

It remains to show that $\Delta$ is invariant under the transpositions $\tau_{uv}$ of coordinates. Denote by $\Delta_{yz}, \Delta_{xz},$ etc. the corresponding expressions where the indicated variables are substituted in place of $y$ and $z$ in $\Delta_{yz}$.  

First consider $\tau_{yz}$, that is, compare $\Delta_{yz}$ and $\Delta_{zy}$. Their product is

$$\Delta_{yz} \cdot \Delta_{zy} = (y(1 - z^2) + iz(1 - y^2)) \cdot (z(1 - y^2) + iy(1 - z^2))$$

$$= (y(1 - z^2) + iz(1 - y^2)) \cdot i(y(1 - z^2) - iz(1 - y^2))$$

$$= \frac{i}{4} \Delta_x.$$ 

Now $\Delta_x = (x - \sigma_x^2(x))^2$ is a square in the function field. Also $i = \zeta_8^2$ is a square, so $\Delta_{yz}$ and $\Delta_{zy}$ define the same class in $F(W_4)^\times / (F(W_4)^\times)^2$.

Next look at $\tau_{xy}$, in other words compare $\Delta_{yz}$ and $\Delta_{zy}$. The product $\Delta_{yz} \cdot \Delta_{zy}$ has degree $(2,2,4)$ as a function of each variable separately, while $f$ has degree $(2,2,2)$, so it is natural to seek a quadratic $q(z) = az^2 + bz + c$ in $z$ alone such that we have the identity

$$\Delta_{xz} \Delta_{yz} + q(z) f(x, y, z) = g(x, y, z)^2$$

for some polynomial $g$ of degree $(1,1,2)$. Comparing the terms not involving $y$, we quickly find that $q(z) = \pm \frac{i}{2} (z^2 + 2z -1)$ (the $\pm$ signs are independent). A short computer computation shows that indeed

$$-2\Delta_{xz} \Delta_{yz} + (z^2 + 2z - 1)f = (xyz^2 + xyz - ixz - iy2 - z^2 + ix + iy - z)^2$$

as an identity in $\mathbb{Z}[i, x, y, z]$. Since $\sqrt{-2} = \zeta_8 + \zeta_8^3 \in F$, this shows the desired invariance under $\tau_{xy}$, completing the proof that $\Delta$ is $\Gamma$-invariant. \hfill \blacksquare

It is necessary to check that $\Delta$ is not constant, that is, $\Delta_{yz}$ is not a constant times a square in $F(W_4)$. To this end, note that $W_4$ contains the line $L = \{(iy, y, 0)\}$. We have $\Delta_{yz} \mid L = y$, which is not a square in $F(L)$.

We can use $\Delta$ to define a double cover of $W_4$. For a concrete construction, let $X_0$ be the subvariety of $(\mathbb{P}^1)^3$ defined by (the projectivization of) the following affine equations:

$$X_0 = \{(x, y, z, \delta_{xy}, \delta_{xz}, \delta_{y}, \delta_{yz}, \delta_{xz}, \delta_{zy}) : f(x, y, z) = 0 \text{ and } \delta_{uv}^2 = \Delta_{uv} \text{ for all distinct } u, v \in \{x, y, z\}\}.$$}

Then let $X$ be an irreducible component of $X_0$. Since the ratios of the $\Delta_{uv}$ are squares but the $\Delta_{uv}$ themselves are not, we see that the natural projection $\pi : X \to W_4$ is a double cover. We claim that $\pi$ is ramified only at the eight singular points. When $x, y, z$ are finite, ramification can only occur when all $\Delta_{uv}$ are zero. This happens only when $\Delta_x = \Delta_y = \Delta_z = 0$, that is, $(x, y, z)$ is a singular point. If $x = \infty$, then $y = \pm i/z$, so $\Delta_y$ is nonzero unless $y$ or $z$ is infinite, which occurs only at the singular points.

Let $U$ be the image of

$$\pi : X(\mathbb{F}_q) \to W_4(\mathbb{F}_q);$$

in other words, $U$ is the set of $(x, y, z) \in W_4(\mathbb{F}_q)$ such that some $\Delta_{uv}$ is a nonzero square, plus the singular points. Note that $U$ is $\Gamma$-invariant, since $\Delta$ is $\Gamma$-invariant. Moreover, $\pi$ is exactly 2-to-1 onto $U$, except at the eight singular points, which each have only one preimage. Thus, using the Weil conjectures for $X$, we have

$$|U| = \frac{|X(\mathbb{F}_q)| + 8}{2} = \frac{1}{2} q^2 + O\left(q^{3/2}\right),$$

yielding the desired splitting

$$W_4(\mathbb{F}_q) = U \sqcup (W_4(\mathbb{F}_q) \setminus U).$$

The implied constant is absolute and depends only on the topology of $X$ considered as a variety over $\mathbb{C}$, which we do not study here. \hfill \blacksquare

For $q \equiv 5 \mod 8$, the same proof yields:

**Theorem 4.** Let $q \equiv 5 \mod 8$ be a prime power. Let $\Gamma' \subset \Gamma$ be the subgroup of index 2 generated by $\sigma_x$, $s_x$, $\tau_x$, and the 3-cycle $\tau_{xy}$. Then there is a partition of the nonsingular points of $W_4(\mathbb{F}_q)$ into two disjoint $\Gamma'$-invariant subsets of the same size, which are interchanged by $\tau_{xy}$. In particular, every $\Gamma'$-orbit on $W_4(\mathbb{F}_q)$ has size at most $\frac{1}{2} q^2 + O\left(q^{3/2}\right)$. 

3
References

[1] Arthur Baragar. *The Markoff equation and equations of Hurwitz*. ProQuest LLC, Ann Arbor, MI, 1991. Thesis (Ph.D.)—Brown University.

[2] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Markoff surfaces and strong approximation: 1, 2016. Preprint, available at https://arxiv.org/abs/1607.01530

[3] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Markoff triples and strong approximation. *C. R. Math. Acad. Sci. Paris*, 354(2):131–135, 2016.

[4] William Chen. Nonabelian level structures, Nielsen equivalence, and Markoff triples, 2020. Preprint, available at https://arxiv.org/abs/2011.12940

[5] Elena Fuchs, Matthew Litman, Joseph H. Silverman, and Austin Tran. Orbits on K3 surfaces of Markoff type, 2022. Preprint, available at https://arxiv.org/abs/2201.12588

[6] A. Markoff. Sur les formes quadratiques binaires indéfinies. *Math. Ann.*, 15:381–406, 1879.