BLOCK SYSTEMS FOR THE $\mathrm{SL}(2,\mathbb{Z})$-ACTION ON ORBITS OF PRIMITIVE ORIGAMIS, AND MAXIMAL VEECH GROUPS IN $\mathcal{H}(2)$ AND $\mathcal{H}(1,1)$

KOREA SUPERINTELLIGENCE LABS

Abstract. An origami is a pair (h,v) of permutations of n symbols generating a transitive group, taken up to simultaneous conjugation; $\mathrm{SL}(2,\mathbb{Z})$ acts through $T(h,v)=(h,vh^{-1})$ and $S(h,v)=(hv^{-1},v)$, and the stabiliser of an origami is its Veech group. Jeffreys and Matheus recently constructed several block systems for this action on a single orbit — for an orbit with monodromy group $\mathrm{Sym}(n)$, the partition into the three classes of the parity pair $(\operatorname{sgn}h,\operatorname{sgn}v)$ — and called that material "of independent interest", but did not ask whether the systems they build are all of them. We answer this, per orbit, in the two hyperelliptic strata. For every $\mathrm{SL}(2,\mathbb{Z})$-orbit of primitive n-square origamis in $\mathcal{H}(2)$ with $3\le n\le 21$, and in $\mathcal{H}(1,1)$ with n odd and $5\le n\le 15$, the only block systems are the two trivial ones together with the parity partition, whose blocks are equinumerous. On the orbits where the monodromy lies in $\mathrm{Alt}(n)$ the parity partition degenerates and the action is therefore *primitive*: the Veech group of such an origami is a maximal subgroup of $\mathrm{SL}(2,\mathbb{Z})$, hence of $\mathrm{PSL}(2,\mathbb{Z})$. A negative control one stratum over shows that this is a fact about the hyperelliptic strata and not a formality: an $\mathcal{H}(4)$ orbit with 120 origamis and constant parity pair carries a further block system and is imprimitive. We also correct a remark of the same paper: contrary to its closing sentence, $(ST)^2$ does appear in the Veech group of a primitive origami in $\mathcal{H}(2)$, with an explicit 7-square witness, and we locate the failure exactly by the paper's own block dynamics. All statements are formally verified in Lean 4; the searches behind them are exhaustive and are described.

1. Introduction

Origamis, the two moves, and Veech groups. Let $n\ge 1$. Following [7], an *origami* with n squares is built from a pair (h,v) of permutations of $\{1,\dots,n\}$ that act transitively: one glues the right edge of the i-th unit square to the left edge of the $h(i)$-th, and its top edge to the bottom edge of the $v(i)$-th. The result is a translation surface covering the unit-square torus, and two pairs give the same origami exactly when they are *simultaneously conjugate*, $(h,v)\sim(ghg^{-1},gvg^{-1})$ for $g\in\mathrm{Sym}(n)$, this being a relabelling of the squares. The group $\langle h,v\rangle\le\mathrm{Sym}(n)$ is the *monodromy group*, and the origami is *primitive* when the monodromy group is primitive as a permutation group; equivalently, when the origami is not a cover of another origami other than itself and the unit-square torus.

The zeros of the abelian differential are read off the commutator $c(h,v)=hvh^{-1}v^{-1}$: a cycle of $c(h,v)$ of length m is a cone point, a zero of order $m-1$. Thus $\mathcal{H}(2)$ is the locus where $c(h,v)$ is a single 3-cycle, $\mathcal{H}(1,1)$ the locus where it is a product of two disjoint transpositions, and $\mathcal{H}(4)$ the locus where it is a single 5-cycle.

The group $\mathrm{SL}(2,\mathbb{Z})$ acts on origamis. It is generated by $T=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $S=\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$, and [7, §2] records the corresponding maps on pairs of permutations:

$$T(h,v)=(h,\ v\,h^{-1}),\qquad S(h,v)=(h\,v^{-1},\ v).\tag{1}$$

Both descend to simultaneous-conjugacy classes and preserve transitivity, primitivity and the stratum (Proposition 2.1). We write $\mathrm{SL}(X)\le\mathrm{SL}(2,\mathbb{Z})$ for the stabiliser of an origami X under this action and call it, as is standard, the *Veech group* of X; the orbit of X is in $\mathrm{SL}(2,\mathbb{Z})$-equivariant bijection with the coset space $\mathrm{SL}(2,\mathbb{Z})/\mathrm{SL}(X)$, so for each of the finite orbits below $|\mathcal{O}|$ is the index of $\mathrm{SL}(X)$. The identification of this combinatorial stabiliser with the Veech group of the underlying translation surface, and an algorithm computing the latter, are Schmithüsen's [14]: her main theorem identifies the Veech group of an origami with "the image of a certain subgroup of $\mathrm{Aut}^+(F_2)$ in $\mathrm{SL}(2,\mathbb{Z}) \cong \mathrm{Out}^+(F_2)$", and from [4, Thm. 5.5] she deduces there that it has finite index in $\mathrm{SL}(2,\mathbb{Z})$. Neither fact is used below: $\mathrm{SL}(X)$ is *defined* here as the stabiliser, and every index quoted is the length of an orbit this paper computes and certifies complete.

Block systems, and the question this paper answers. For a group G acting on a set Ω, [7, §3] calls a partition $\mathcal{B}$ of Ω a *block system* when for all $\Delta \in \mathcal{B}$ and all $g \in G$ either $g(\Delta) = \Delta$ or $g(\Delta) \cap \Delta = \emptyset$, and calls a transitive action *primitive* when the only block systems are $\{\Omega\}$ and the partition into singletons. We use the standard reading of that definition throughout: a G-invariant partition, i.e. a system of imprimitivity. For a transitive action such a partition is determined by the part containing a fixed base point, and conversely the G-translates of any block through the base point form one, so classifying the possible parts at one point classifies the block systems.

Section 3 of [7] *constructs* block systems for the action of $\mathrm{SL}(2,\mathbb{Z})$ on a single orbit $\mathcal{O}$ of origamis. The one we meet everywhere below is theirs: if $|\mathcal{O}| \geq 3$ and the monodromy group of the origamis in $\mathcal{O}$ is $\mathrm{Sym}(n)$, then

$$\varepsilon(h,v) = \big(\operatorname{sgn} h,\ \operatorname{sgn} v\big) \in (\mathbb{Z}/2)^2 \setminus \{0\} \tag{2}$$

takes all three values on $\mathcal{O}$, and its three fibres $B_1 = \{h \notin \mathrm{Alt}(n), v \in \mathrm{Alt}(n)\}$, $B_2 = \{h \notin \mathrm{Alt}(n), v \notin \mathrm{Alt}(n)\}$, $B_3 = \{h \in \mathrm{Alt}(n), v \notin \mathrm{Alt}(n)\}$ form a block system [7, Prop. 3.3]; the induced action of $\mathrm{SL}(2,\mathbb{Z})$ on $\{B_1, B_2, B_3\}$ factors through $\mathrm{SL}(2,\mathbb{Z}/2) \cong \mathrm{Sym}(3)$, with $T = (B_1\, B_2)$ and $S = (B_2\, B_3)$ [7, Fig. 3.4]. A second construction of the same section [7, Prop. 3.6] applies to orbits on which $-I$ acts without fixed points, and pairs each origami with its image under $-I$. The authors describe the section as "of independent interest" [7, §1.5] and use it as a source of coverings between orbit graphs; they never ask whether the systems they construct are *all* the block systems, and they attach no block system at all to the orbits whose monodromy lies in $\mathrm{Alt}(n)$, where their mechanism produces nothing.

That gap is what this paper closes, in the two strata where the orbits are under control.

What is classified, and what is open. The $\mathrm{SL}(2,\mathbb{Z})$-orbits of primitive origamis have been classified in only two settings, and [7] says so in as many words: "the $\mathrm{SL}(2,\mathbb{Z})$-orbits of primitive origamis have only been classified in $\mathcal{H}(2)$ and in the Prym loci in $\mathcal{H}(4)$ and $\mathcal{H}(6)$" [7, §1.1]. In $\mathcal{H}(2)$, combining [5], [12] and [11], a primitive origami with $n \geq 3$ squares lies in a single orbit when $n = 3$ or $n \geq 4$ is even, and in one of exactly two orbits $\mathcal{G}_n^A$ and $\mathcal{G}_n^B$ when $n \geq 5$ is odd, with

$$|\mathcal{G}_n^A| = \tfrac{3}{16}(n-1)\,\psi(n), \qquad |\mathcal{G}_n^B| = \tfrac{3}{16}(n-3)\,\psi(n), \qquad \psi(n) := n^2 \prod_{p|n,\ p\ \text{prime}} \big(1 - p^{-2}\big). \tag{3}$$

Here $\mathcal{G}_n^B$ is the smaller orbit, and it is the one whose monodromy lies in $\mathrm{Alt}(n)$; the labelling is pinned by the example of [7, §4.1] and is verified in Proposition 6.1. In the Prym loci of $\mathcal{H}(4)$ and $\mathcal{H}(6)$ the orbits were classified by Lanneau and Nguyen [9, 10].

In $\mathcal{H}(1,1)$ the picture is conjectural in general. Zmiaikou [16] conjectured, on computational evidence, that for $n \geq 7$ there are exactly two orbits of primitive n-square origamis in $\mathcal{H}(1,1)$, of cardinalities

$$\mathcal{A}_n(1,1) = \tfrac{1}{24}(n-3)(n-5)\,\psi(n), \qquad \mathcal{S}_n(1,1) = \tfrac{1}{8}(n-1)(n-3)\,\psi(n) \tag{4}$$

for odd n — these being the orbits with monodromy $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$ respectively — and of cardinalities $\frac{1}{24}n(n-2)\psi(n)$ and $\frac{1}{8}(n-2)(n-4)\psi(n)$ for even n. For *odd* n the two cardinalities are a theorem, and [7, §6] records the reason: for odd n every primitive origami of $\mathcal{H}(1,1)$ carries one of exactly two HLK-invariants (Duryev [2, Thm. 3.1], quoted there), and Kappes and Möller [8] computed the sizes of the two invariant classes,

$$t_{d,1,0} = \frac{(d-3)(d-5)}{12d}\big|\mathrm{PSL}(2,\mathbb{Z}/d\mathbb{Z})\big|, \qquad t_{d,1,1} = \frac{(d-1)(d-3)}{4d}\big|\mathrm{PSL}(2,\mathbb{Z}/d\mathbb{Z})\big| \tag{5}$$

for odd $d \geq 5$, which [7, §6] observes "are the formulae conjectured by Zmiaikou". Here d is the number of squares, our n. The same section adds: "To the best of our knowledge, the case $n = 1$ for even d (also conjectured by Zmiaikou) is still open" — in that sentence the letter n is the source's torsion parameter, fixed at 1 throughout the case we need, and the number of squares is again d, so what it calls open is the even-square case. Nothing below is claimed for an even number of squares in $\mathcal{H}(1,1)$.

Results. Everything is derived from (1) and the definitions above by finite computations whose completeness is itself proved; Section 8 says what was delegated to computation and Sections 3–7 say, statement by statement, which exhaustive search each rests on. Write $\mathcal{O}$ for an $\mathrm{SL}(2,\mathbb{Z})$-orbit of primitive n-square origamis, and call $\mathcal{O}$ *ε-constant* when $\langle h, v\rangle \leq \mathrm{Alt}(n)$ for one, equivalently every, origami in it (Proposition 2.1(v)).

Theorem 1.1 (Theorem 3.1). *Let $3 \leq n \leq 21$ and let $\mathcal{O}$ be an $\mathrm{SL}(2,\mathbb{Z})$-orbit of primitive n-square origamis in $\mathcal{H}(2)$. Then the block systems of the $\mathrm{SL}(2,\mathbb{Z})$-action on $\mathcal{O}$ are exactly: the partition into singletons, the partition into the fibres of ε, and $\{\mathcal{O}\}$. If $\mathcal{O}$ is ε-constant — that is, n is odd and $\mathcal{O} = \mathcal{G}_n^B$ — the middle partition is $\{\mathcal{O}\}$ and the action is **primitive**; otherwise the fibres of ε are three blocks of $|\mathcal{O}|/3$ origamis each, except at $n = 3$, where they are the three singletons and the action is again primitive.*

Theorem 1.2 (Theorem 4.1). *The same conclusion holds in $\mathcal{H}(1,1)$ for every odd n with $5 \leq n \leq 15$: the ε-constant orbit $\mathcal{A}_n$ (of cardinality $16, 72, 240, 560, 960$ at $n = 7, 9, 11, 13, 15$) is primitive, and the orbit $\mathcal{S}_n$ (of cardinality $24, 144, 432, 1200, 2520, 4032$ at $n = 5, 7, 9, 11, 13, 15$) has the partition into the fibres of ε, with three blocks of $|\mathcal{S}_n|/3$ origamis, as its unique non-trivial block system.*

In both theorems the orbits listed are all the orbits at each n in the range: in $\mathcal{H}(2)$ by the classification (3) with the cardinality check of Theorem 3.2, and in $\mathcal{H}(1,1)$ by Proposition 4.2, which uses (5) and not Zmiaikou's conjecture. The consequence for Veech groups is Corollary 5.1: the Veech group of a primitive origami in $\mathcal{G}_n^B$ or in $\mathcal{A}_n$ is a *maximal* subgroup of $\mathrm{SL}(2,\mathbb{Z})$, and its image is maximal in $\mathrm{PSL}(2,\mathbb{Z})$; that of an origami in the other orbit has exactly one intermediate subgroup, of index 3. Section 7 exhibits an $\mathcal{H}(4)$ orbit where both conclusions fail, which is what makes the two theorems statements about the hyperelliptic strata rather than about origamis in general.

The third result is a correction to [7].

Theorem 1.3 (Theorem 6.2). *The remark of* [7, §4.1] *ends: "Notice that $(ST)^2$ does not seem to appear in the Veech group of any primitive origami in $\mathcal{H}(2)$." This is false. The word $(ST)^2$ fixes 2 origamis of $\mathcal{G}_5^B$, 4 of $\mathcal{G}_7^B$ and 4 of $\mathcal{G}_{11}^B$. An explicit witness is $X_7 = \big((1\,2)(3\,4)(5\,6\,7),\ (1\,3\,5\,7\,2\,4\,6)\big)$, a primitive 7-square origami in $\mathcal{H}(2)$ lying in $\mathcal{G}_7^B$, whose Veech group contains $(ST)^2$ and contains neither ST nor $(TS)^2$.*

Every other entry of that remark is reproduced exactly for $n \leq 13$, with one omission which we record. The failure is localised by the paper's own machinery: by [7, Prop. 3.3, Fig. 3.4] the word $(ST)^2$ acts on $\{B_1, B_2, B_3\}$ as a fixed-point-free 3-cycle, so it can fix no origami in an orbit that is not ε-constant — which leaves exactly the orbits $\mathcal{G}_n^B$, and that is where it occurs. No theorem of [7] depends on the sentence, which is explicitly heuristic; what it changes is the conjectural picture of which pseudo-Anosov elements occur.

Relation to other work. We have not found either dichotomy in the literature, and state that as the outcome of a search rather than as a claim of novelty. Two neighbours should be named. First, W. Y. Chen [1] computes exactly this invariant, by machine, for a different family. His moduli stacks $\mathcal{M}(G)$ parametrise G-covers of elliptic curves branched at most above the origin — in the square-tiling dictionary he sets out, the regular origamis with deck group G — and letting G run over the 36 smallest non-abelian finite simple groups gives 860 components of the stacks $\mathcal{M}(G)^{\mathrm{abs}}$, of which he reports that "719 components are primitive covers of $\mathcal{M}(1)$, in the sense that they admit no nontrivial intermediate covers", classifying the intermediate covers of the remaining 141. A connected cover of the modular stack $\mathcal{M}(1)$ corresponds to a subgroup of $\mathrm{SL}(2,\mathbb{Z})$ and its intermediate covers to the intermediate subgroups, so "primitive cover of $\mathcal{M}(1)$" says that the subgroup — for a cover coming from an origami, its Veech group — is maximal. His family is disjoint from ours and the words "maximal subgroup" do not occur in [1], but the question type is in the literature. Second, Meiri and Puder [13] prove that an analogous action — the Markoff triples modulo a prime — is symmetric or alternating, hence primitive. That is a different family and is not phrased in terms of Veech groups, but it is the natural template for proving Theorems 1.1 and 1.2 for all n rather than for a certified range.

Nothing is claimed outside the certified ranges: an independent unverified computation observed the same dichotomy up to $n = 21$ in $\mathcal{H}(2)$ and odd $n = 15$ in $\mathcal{H}(1,1)$ and no further, so the verified and the unverified ranges coincide. Section 9 reproduces, as a check on the encoding, an orbit census every value of which is already tabulated in the database of [15], and which agrees with the tables of [16] wherever those reach — with the single exception recorded in Remark 9.4.

Acknowledgement of the source. Every definition, quoted conjecture and quoted classification here is taken from the LaTeX source of [7] (v1) and is reproduced in the form it has there.

2. Origamis, the two moves, and their invariants

Throughout, α is a set and $\mathrm{Sym}(\alpha)$ its symmetric group; for the counting statements $\alpha = \{1,\dots,n\}$. We write a pair of permutations as $x = (h, v)$, and

$$T(x) = (h, vh^{-1}), \quad S(x) = (hv^{-1}, v), \quad T^{-1}(x) = (h, vh), \quad S^{-1}(x) = (hv, v),$$
$$c(x) = hvh^{-1}v^{-1}, \qquad g\cdot x = (ghg^{-1}, gvg^{-1}) \ \ (g \in \mathrm{Sym}(\alpha)).$$

Proposition 2.1. *Let α be any set and $x = (h, v) \in \mathrm{Sym}(\alpha)^2$.*

(i) *For every $g \in \mathrm{Sym}(\alpha)$, $T(g\cdot x) = g\cdot T(x)$ and $S(g\cdot x) = g\cdot S(x)$.*
(ii) *$c(T(x)) = c(x)$ and $c(S(x)) = c(x)$; moreover $c(g\cdot x) = g\, c(x)\, g^{-1}$.*
(iii) *$\langle T(x)_1, T(x)_2\rangle = \langle h, v\rangle = \langle S(x)_1, S(x)_2\rangle$ as subgroups of $\mathrm{Sym}(\alpha)$.*
(iv) *$T^{-1}(T(x)) = x$ and $S^{-1}(S(x)) = x$, and likewise in the other order.*
(v) *If α is finite, then $\mathrm{sgn}(T(x)_1) = \mathrm{sgn}(T(x)_2) = 1$ if and only if $\mathrm{sgn}(h) = \mathrm{sgn}(v) = 1$, and the same for S; conjugation changes neither sign.*

Proof. All five are identities in $\mathrm{Sym}(\alpha)$. For (ii), $c(T(x)) = h(vh^{-1})h^{-1}(vh^{-1})^{-1} = hvh^{-1}v^{-1} = c(x)$ and $c(S(x)) = (hv^{-1})v(hv^{-1})^{-1}v^{-1} = hvh^{-1}v^{-1}$. For (iii), $v = (vh^{-1})h$ and $h = (hv^{-1})v$, so each pair generates the other. For (v), the sign is a homomorphism, so $\mathrm{sgn}(vh^{-1}) = \mathrm{sgn}(v)\mathrm{sgn}(h)$. Parts (i) and (iv) are direct expansions. ☐

By (i), T and S descend to simultaneous-conjugacy classes, so "an origami" is a well-defined object on which $\mathrm{SL}(2,\mathbb{Z})$ acts and one may compute with one representative of each class; by (ii) and (iii) the stratum, transitivity, primitivity and the monodromy group are constant along an orbit. Part (v) says that the parity pair (2) transforms under the induced action of $\mathrm{SL}(2,\mathbb{Z}/2)$, which fixes $(0,0)$ and permutes the three non-zero vectors; in particular "$\langle h, v\rangle \le \mathrm{Alt}(\alpha)$" is an orbit invariant. It is the machine-checkable stand-in for the labels $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$: it separates the orbits without identifying the monodromy group.

Canonical forms and orbit certificates. For a transitive pair x and a base point s, the breadth-first order of $\{1,\dots,n\}$ generated from s by applying h and v is a bijection, and relabelling x along it is a simultaneous conjugation; doing this from every base point and keeping the lexicographically least result gives a map can constant on simultaneous-conjugacy classes of transitive pairs. Set $\mathrm{mv}(x) = \{\mathrm{can}(Tx), \mathrm{can}(Sx), \mathrm{can}(T^{-1}x), \mathrm{can}(S^{-1}x)\}$ and let $\mathrm{Reach}(x)$ be the set reachable from x under iterated mv; since T and S generate $\mathrm{SL}(2,\mathbb{Z})$, this is the $\mathrm{SL}(2,\mathbb{Z})$-orbit of x in canonical representatives.

Proposition 2.2. *Let* $\mathrm{orb}(x)$ *be the list produced by breadth-first saturation of* $\{x\}$ *under* mv *with a fixed finite fuel. Then every element of* $\mathrm{orb}(x)$ *lies in* $\mathrm{Reach}(x)$ *and* $x \in \mathrm{orb}(x)$*; and if* L *is any list with* $x \in L$ *and* $\mathrm{mv}(y) \subseteq L$ *for all* $y \in L$*, then* $\mathrm{Reach}(x) \subseteq L$*. Consequently, if* $\mathrm{orb}(x)$ *is closed under* mv *then* $\mathrm{Reach}(x) = \mathrm{orb}(x)$ *exactly, and* $|\mathrm{orb}(x)|$ *is the cardinality of the* $\mathrm{SL}(2,\mathbb{Z})$*-orbit of* x*.*

Proof. The first assertion is an induction on the fuel: the saturation only ever appends images under mv of elements already present, and the initial list is $\{x\}$. The second is an induction on the definition of Reach. The consequence is their conjunction. □

Proposition 2.2 is what turns a computation into a theorem: closure is a finite Boolean check, and no statement below assumes that a search terminated having seen everything.

Seeds, uniformly in n. Every orbit reached below is reached from a formula, not from a stored pair or a random search.

Proposition 2.3. *Let* α *be a finite set,* $h \in \mathrm{Sym}(\alpha)$ *and* $a \in \alpha$*. Then*

$$[h,\,(a\ h(a))] = (h(a)\ h^2(a)) \cdot (h(a)\ a), \qquad [h,\,(a\ h^2(a))] = (h(a)\ h^3(a)) \cdot (a\ h^2(a)),$$

where $[x,y] = xyx^{-1}y^{-1}$ *and* $(\cdot\ \cdot)$ *denotes a transposition. If* $a, h(a), h^2(a)$ *are distinct the first commutator is a* 3*-cycle, so* $(h,(a\ h(a)))$ *lies in* $\mathcal{H}(2)$*; if* $a, h(a), h^2(a), h^3(a)$ *are distinct the second has cycle type* $(2,2)$*, so* $(h,(a\ h^2(a)))$ *lies in* $\mathcal{H}(1,1)$*. If moreover* h *is a cycle of full support then* $\langle h,(a\ h(a))\rangle = \mathrm{Sym}(\alpha)$*, and* $\langle h,(a\ h^2(a))\rangle = \mathrm{Sym}(\alpha)$ *when* $|\alpha|$ *is odd; in particular both pairs are primitive origamis.*

Proof. Both identities follow from $h\,(x\ y)\,h^{-1} = (h(x)\ h(y))$. In the first, the two transpositions share the point $h(a)$, so their product is a 3-cycle; in the second they are disjoint under the stated hypothesis, so the product has type $(2,2)$. The two closure statements are the classical facts that a full-support cycle together with a transposition of adjacent points, or with a transposition $(a\ h^k(a))$ with k coprime to $|\alpha|$, generates the symmetric group. □

Concretely, with $h_n = (1\,2\,\cdots\,n)$ we use the seeds

$$\mathcal{G}_n^A,\ \mathcal{G}_n:\ (h_n,(1\,2)); \qquad \mathcal{G}_n^B:\ (h_n,(1\,2\,3)); \qquad \mathcal{S}_n:\ (h_n,(1\,3)); \qquad \mathcal{A}_n:\ (h_n,(2\,5\,4\,3\,6)),$$

each put in canonical form; the parity of the second coordinate selects the orbit, by Proposition 2.1(v) and because h_n is even for odd n. For the negative control of Section 7 we use the $\mathcal{H}(4)$ seed $(h_n,(1\,2\,4))$.

Certifying that there is no other block system. Fix an orbit $\mathcal{O}$, listed as O with $V = |O|$, and read the four maps T, S, T^{-1}, S^{-1} off it as maps on indices $\{0,\dots,V-1\}$. A partition of $\mathcal{O}$ invariant under those four maps — by (1) exactly a block system for $\mathrm{SL}(2,\mathbb{Z})$ — is the same thing as an equivalence relation compatible with them, that is, a *congruence*. Let $\mathrm{Gen}(a_0,b_0)$ be the least congruence relating a_0 and b_0, defined inductively by the seed pair, reflexivity, symmetry, transitivity, and closure under the four maps.

Proposition 2.4.
- (i) *If* l *is any congruence with* $l(a_0) = l(b_0)$*, then* $\mathrm{Gen}(a_0,b_0)(a,b)$ *implies* $l(a) = l(b)$*.*
- (ii) *Let a* derivation log *be a finite list of instructions — assert reflexivity, symmetrise a stored pair, compose two stored pairs, apply one of the four maps to a stored pair — replayed against the four maps. Whatever the log contains, every pair it produces is related by* $\mathrm{Gen}(a_0,b_0)$*.*
- (iii) *Let* π *be the labelling of* O *by the parity pair* (2)*. Suppose that for every index* $j \neq 0$ *there is a log whose replay from* $(0,j)$ *covers the whole of* $\{k : \pi(k) = \pi(0)\}$ *when* $\pi(j) = \pi(0)$*, and the whole of* $\{0,\dots,V-1\}$ *otherwise. Then for* every *congruence* l *the class of* 0 *is* $\{0\}$*, or* $\{k : \pi(k) = \pi(0)\}$*, or everything.*

(iv) *If in addition the index maps are checked to be the four moves and to land in range, (iii) transports back to $\mathcal{O}$: for every block system of the* $\mathrm{SL}(2,\mathbb{Z})$*-action on* $\mathcal{O}$*, the block containing a given origami* s *is* $\{s\}$*, or* $\{z \in \mathcal{O} : \varepsilon(z) = \varepsilon(s)\}$*, or* $\mathcal{O}$*. If the parity labelling is checked to be a congruence, the middle partition really is a block system.*

Proof. (i) is induction on the derivation, using that every derived index stays below V. (ii) is induction on the log, every instruction being given a total meaning: an unjustified composition falls back to a reflexive pair and an out-of-range read to $(0,0)$, so a bug in the process that writes the log can only make the check fail, never make it lie. For (iii): if some $j \neq 0$ in the class of 0 has $\pi(j) \neq \pi(0)$ then its target is everything and (i) forces the class of 0 to be everything; otherwise the class is contained in $\{k : \pi(k) = \pi(0)\}$ and, if it is not $\{0\}$, contains it by the same argument. (iv) is the translation of a labelling of O into a labelling of $\mathcal{O}$ and back. □

The logs themselves are produced by an unverified union–find search — Atkinson's minimal-block closure, instrumented to emit one instruction per step it takes — and are replayed and checked in the same evaluation, so by (ii) nothing about the search has to be trusted. For one orbit the work is V minimal-congruence searches, each $O(V\alpha(V))$ instructions plus its replay: $O(V^2)$.

We package one orbit as $\mathrm{cert}(n,\kappa,s) = (V, p_0, \texttt{true})$, where $V = |\mathcal{O}|$, p_0 is the number of origamis in $\mathcal{O}$ with the same parity pair as the seed s, and the Boolean asserts: s is a canonical primitive origami of the stratum κ; the computed list is closed under the four moves and contains s, hence is the whole orbit by Proposition 2.2; the index maps are the four moves and land in range; the parity labelling is a congruence; and every $j \neq 0$ carries a replay-checked derivation covering its target. A certificate with $p_0 = V$ is a primitivity statement, one with $p_0 = V/3$ a uniqueness statement.

3. The block dichotomy in $\mathcal{H}(2)$

Theorem 3.1. *Let* $3 \le n \le 21$ *and let* $\mathcal{O}$ *be one of the orbits listed in Table 1. Then every block system of the* $\mathrm{SL}(2,\mathbb{Z})$*-action on* $\mathcal{O}$ *is the partition into singletons, the partition into the fibres of* ε*, or* $\{\mathcal{O}\}$*; and the partition into the fibres of* ε *is a block system. In the column* $\mathcal{G}_n^B$ *the parity pair is constant, so the fibre partition is* $\{\mathcal{O}\}$ *and the action is primitive; in the other column the fibres of* ε *are three blocks of* $|\mathcal{O}|/3$ *origamis each, except at* $n = 3$ *where they are three singletons and the action is again primitive.*

	$\mathcal{G}_n$ or $\mathcal{G}_n^A$		$\mathcal{G}_n^B$			$\mathcal{G}_n$ or $\mathcal{G}_n^A$		$\mathcal{G}_n^B$	
n	$\lvert\mathcal{O}\rvert$	$\lvert B_1\rvert$	$\lvert\mathcal{O}\rvert$	$\lvert B_1\rvert$	n	$\lvert\mathcal{O}\rvert$	$\lvert B_1\rvert$	$\lvert\mathcal{O}\rvert$	$\lvert B_1\rvert$
3	3	1			13	378	126	315	315
4	9	3			14	648	216		
5	18	6	9	9	15	504	168	432	432
6	36	12			16	1008	336		
7	54	18	36	36	17	864	288	756	756
8	108	36			18	1296	432		
9	108	36	81	81	19	1215	405	1080	1080
10	216	72			20	1944	648		
11	225	75	180	180	21	1440	480	1296	1296
12	360	120							

Table 1. The 28 certified orbits in $\mathcal{H}(2)$. $|B_1|$ is the number of origamis in the orbit whose parity pair agrees with that of the seed. $|B_1| = |\mathcal{O}|$ means the parity pair is constant and the action is primitive; $|B_1| = |\mathcal{O}|/3$ means the parity partition is the unique non-trivial block system.

Proof sketch. For each of the 28 orbits of Table 1 a certificate $\mathrm{cert}(n,[3],s) = (|\mathcal{O}|, |B_1|, \texttt{true})$ was evaluated, with s the seed of Proposition 2.3 for that column. Each such evaluation is exhaustive in two respects: it saturates the orbit from the seed under the four maps and checks the returned list is closed, which by Proposition 2.2 makes it the whole orbit; and it runs, for each of the $|\mathcal{O}|-1$ indices $j \neq 0$, a minimal-congruence search whose derivation log is then replayed and checked to cover the target set of Proposition 2.4(iii). The conclusion is then Proposition 2.4(iv) applied to that certificate. No orbit outside the table, and no n outside $3 \leq n \leq 21$, is claimed. The equalities $|\mathcal{O}| = 3|B_1|$ and $|B_1| = |\mathcal{O}|$ are read off the certified pairs in the table. □

Besides the uniqueness, one small thing in the theorem is not in [7]: the equinumerosity of B_1, B_2, B_3, hence $3 \mid |\mathcal{O}|$ for every orbit that is not ε-constant. It follows from the Sym(3)-dynamics of [7, Fig. 3.4], and the certificates return it directly.

It remains to know that the orbits of Table 1 are all the orbits. For odd n this is the classification (3) together with the matching of the certified cardinalities against $|\mathcal{G}_n^A|$ and $|\mathcal{G}_n^B|$. For even n the classification says there is a single orbit, but [7] states no cardinality there, so a check is needed that the seed reaches it and not some smaller invariant set. The count of *all* primitive n-square origamis in $\mathcal{H}(2)$ supplies the missing number:

$$\Phi(n) = \tfrac{3}{8}(n-2)\,\psi(n), \tag{6}$$

which for odd n is exactly $|\mathcal{G}_n^A| + |\mathcal{G}_n^B|$. The formula is *not* Hubert and Lelièvre's, as it is sometimes cited: it is Eskin, Masur and Schmoll's, recorded in [3, §4] as a remark after their asymptotic count of primitive degree-n covers in the minimal stratum. Hubert and Lelièvre quote it from them — [5] attributes it to [3] outright, and [6] states it as an external theorem — and what *they* conjectured, and what [12] and [11] then settled, is the finer split (3) of $\Phi(n)$ into the two odd-n orbits.

Theorem 3.2. *For every $3 \leq n \leq 21$ the orbits of Table 1 exhaust the primitive locus: at $n = 3$ and at even n the single certified orbit has $\Phi(n)$ elements, and at odd $n \geq 5$ the two certified orbits have $\Phi(n)$ elements between them. Moreover $\Phi(n) = |\mathcal{G}_n^A| + |\mathcal{G}_n^B|$ at every odd n in that range. Consequently Theorem 3.1 describes every $\mathrm{SL}(2,\mathbb{Z})$-orbit of primitive n-square origamis in $\mathcal{H}(2)$ for $n \leq 21$.*

Proof sketch. The formula (6) is Eskin–Masur–Schmoll's and is not claimed here; what is checked is the identification. The orbit lengths reported by the 28 certificates of Theorem 3.1 are summed and compared with (6), evaluated in integer arithmetic at each n of the range; the comparison uses no further search. The final sentence combines this with the classification (3): a single orbit of the full cardinality is the whole primitive locus, and two orbits whose sizes add to it are both of them. □

Remark 3.3. Two controls accompany Theorem 3.2: at every odd n of the range neither certified orbit *alone* has $\Phi(n)$ elements, so the sum is doing real work; and the two nearest wrong closed forms $\frac{3}{8}(n-1)\psi(n)$ and $\frac{3}{8}(n-3)\psi(n)$ disagree with Φ at every $3 \leq n \leq 21$, so the match is not an accident of the shape of the formula.

4. The block dichotomy in $\mathcal{H}(1,1)$

Theorem 4.1. *Let n be odd with $5 \leq n \leq 15$ and let $\mathcal{O}$ be one of the orbits listed in Table 2. Then every block system of the $\mathrm{SL}(2,\mathbb{Z})$-action on $\mathcal{O}$ is the partition into singletons, the partition into the fibres of ε, or $\{\mathcal{O}\}$; and the partition into the fibres of ε is a block system. On $\mathcal{A}_n$ the parity pair is constant, so the action is* ***primitive****; on $\mathcal{S}_n$ the fibres of ε are three blocks of $|\mathcal{S}_n|/3$ origamis each, and form the unique non-trivial block system.*

Proof sketch. Identical in shape to Theorem 3.1: one certificate $\mathrm{cert}(n,[2,2],s) = (|\mathcal{O}|, |B_1|, \texttt{true})$ per orbit, with s the corresponding seed of Proposition 2.3; the orbit is saturated from the seed and checked closed, and each of the $|\mathcal{O}|-1$ indices $j \neq 0$ carries a replay-checked derivation covering its

	$\mathcal{S}_n$		$\mathcal{A}_n$	
n	$\lvert\mathcal{O}\rvert$	$\lvert B_1\rvert$	$\lvert\mathcal{O}\rvert$	$\lvert B_1\rvert$
5	24	8	empty	
7	144	48	16	16
9	432	144	72	72
11	1200	400	240	240
13	2520	840	560	560
15	4032	1344	960	960

TABLE 2. The 11 certified orbits in $\mathcal{H}(1,1)$ at odd $n \leq 15$. The cardinalities are exactly $\mathcal{S}_n(1,1)$ and $\mathcal{A}_n(1,1)$ of (4); at $n = 5$ one has $\mathcal{A}_5(1,1) = 0$.

target. The largest single search is the $\mathcal{S}_{15}$ orbit, where 4031 minimal-congruence searches are run over a 4032-element orbit. □

That these are all the orbits at each odd n in the range does *not* need Zmiaikou's conjecture, and it is worth writing the argument out, because the classification statement one would like to quote does not exist: as noted in Section 1, [7] says the orbits of primitive origamis have been classified only in $\mathcal{H}(2)$ and in the Prym loci.

Proposition 4.2. *Let n be odd, $5 \leq n \leq 15$. The two orbits of Table 2 are all the $\mathrm{SL}(2,\mathbb{Z})$-orbits of primitive n-square origamis in $\mathcal{H}(1,1)$.*

Proof. For odd n, [7, §6] records — reading off Duryev's [2, Thm. 3.1] — that every primitive n-square origami in $\mathcal{H}(1,1)$ carries one of exactly two HLK-invariants, namely $(3,[1,1,1])$ and $(1,[3,1,1])$, so the primitive locus is partitioned into two classes; the invariant is $\mathrm{SL}(2,\mathbb{Z})$-invariant, so each orbit lies in one class. Kappes and Möller [8] computed the two class cardinalities (5), and with $|\mathrm{PSL}(2,\mathbb{Z}/d\mathbb{Z})| = \frac{1}{2}d\,\psi(d)$ for odd $d \geq 3$ these are literally $\mathcal{A}_d(1,1)$ and $\mathcal{S}_d(1,1)$ — the observation [7, §6] makes when it says these are Zmiaikou's conjectured formulas. Table 2 exhibits one orbit of cardinality exactly $\mathcal{S}_n(1,1)$ and, for $n \geq 7$, one of cardinality exactly $\mathcal{A}_n(1,1)$. An orbit contained in a class and of the class's full cardinality is that class; hence each class is a single orbit and there are exactly two. At $n = 5$ one has $\mathcal{A}_5(1,1) = 0$ and only the class $\mathcal{S}_5$ is non-empty, and the argument degenerates correctly. □

Duryev's theorem is stated for the loci $\Omega W_{d^2}[n]$ of [7, §6]; the case used here is $n = 1$ and d odd, where it says that the number of integer Weierstrass points is 1 or 3 and is locally constant, which is the two-class statement above. We have checked that reading against [2] itself and not only against the quotation in [7]; the numbering is that of [2] in the arXiv version cited, whose Theorem 3.1 is the one meant.

Nothing above is claimed for even n in $\mathcal{H}(1,1)$, where [7, §6] says the cardinality statement "is still open" and where the argument of Proposition 4.2 is unavailable.

5. Consequences for Veech groups

Corollary 5.1. *Let X be a primitive n-square origami lying in $\mathcal{G}_n^B$ with n odd, $5 \leq n \leq 21$, or in $\mathcal{A}_n$ with n odd, $7 \leq n \leq 15$; or let X be one of the three origamis of $\mathcal{G}_3$. Then the Veech group $\mathrm{SL}(X)$ is a* maximal *subgroup of $\mathrm{SL}(2,\mathbb{Z})$. If instead X lies in one of the remaining orbits of Tables 1 and 2, then $\mathrm{SL}(X)$ has exactly one subgroup strictly between it and $\mathrm{SL}(2,\mathbb{Z})$, and that subgroup has index 3 in $\mathrm{SL}(2,\mathbb{Z})$.*

Proof. The orbit of X is $\mathrm{SL}(2,\mathbb{Z})/\mathrm{SL}(X)$ as an $\mathrm{SL}(2,\mathbb{Z})$-set, and for a transitive action the blocks through the base point correspond to the subgroups between the stabiliser and the whole group, the block being the orbit of the intermediate subgroup and the number of blocks its index in $\mathrm{SL}(2,\mathbb{Z})$.

So Theorems 3.1 and 4.1 say precisely that $\mathrm{SL}(X)$ is maximal in the first case, and in the second that the only intermediate subgroup is the one whose orbit is the parity block $B_1 \ni X$, of index $|\mathcal{O}|/|B_1| = 3$. □

The correspondence used here is the classical one between block systems and intermediate subgroups; it is the one step of the argument that is not part of the formal development, the machine-checked statements being about invariant partitions of the orbit.

Remark 5.2. Both statements descend to $\mathrm{PSL}(2,\mathbb{Z})$. Every translation surface of genus two is hyperelliptic, so $-I$ lies in the Veech group of every origami in $\mathcal{H}(2)$ and $\mathcal{H}(1,1)$ and the action factors through $\mathrm{PSL}(2,\mathbb{Z})$; consequently the maximal subgroups above are maximal in $\mathrm{PSL}(2,\mathbb{Z})$ as well. That $-I = (TS^{-1}T)^2$ fixes every origami of the $\mathcal{H}(2)$ and $\mathcal{H}(1,1)$ orbits at $n = 7$ is checked directly in Proposition 7.1(ii), where it also fails, as it must, one stratum over.

Remark 5.3. The index-3 subgroup of Corollary 5.1 can be named, though we state that only as an observation, it being outside the formal development. The map $(h, v) \mapsto (\operatorname{sgn} h, \operatorname{sgn} v)$ identifies B_1, B_2, B_3 with the three non-zero vectors of $\mathbb{F}_2^2$; by Proposition 2.1(v) the moves act on those vectors by $T\colon (a, b) \mapsto (a, a + b)$ and $S\colon (a, b) \mapsto (a + b, b)$, so the action factors through a surjection $\rho\colon \mathrm{SL}(2,\mathbb{Z}) \twoheadrightarrow \mathrm{SL}(2,\mathbb{F}_2) \cong \mathrm{Sym}(3)$ whose kernel is the principal congruence subgroup $\Gamma(2)$. The intermediate subgroup is therefore the ρ-preimage of a point stabiliser: an index-3 subgroup containing $\Gamma(2)$, hence a congruence subgroup of level 2. There are exactly three such subgroups — $\Gamma_0(2)$, $\Gamma^0(2)$ and the theta group Γ_θ, corresponding to the three subgroups of order 2 in $\mathrm{Sym}(3)$ — and they are conjugate in $\mathrm{SL}(2,\mathbb{Z})$, the conjugation action being transitive on the three transpositions; which of them occurs depends on which block contains the chosen origami. The second half of Corollary 5.1 then reads: the only subgroup strictly between such a Veech group and $\mathrm{SL}(2,\mathbb{Z})$ is a congruence group.

6. A correction: $(ST)^2$ in $\mathcal{H}(2)$ Veech groups

Section 4.1 of [7] lists, from computation, the primitive $\mathcal{H}(2)$ origamis fixed by each of the eight hyperbolic words of length at most four in T and S, and closes with:

> "Computations suggest that these are the only primitive origamis in $\mathcal{H}(2)$ fixed by any of these words. Notice that $(ST)^2$ does not seem to appear in the Veech group of any primitive origami in $\mathcal{H}(2)$." [7, §4.1]

Words act on origamis through (1), with ST the matrix product, that is $X \mapsto S(T(X))$. The convention matters, and is pinned by the source's own data.

Proposition 6.1. *The two origamis* $\big((1\,2\,3\,4\,5), (3\,4\,5)\big)$ *and* $\big((3\,4\,5), (1\,2\,3\,5\,4)\big)$ *that* [7, §4.1] *lists as fixed by* ST *are fixed by* $X \mapsto S(T(X))$ *and are not fixed by* $X \mapsto T(S(X))$*; and both lie in the* 9*-element orbit* $\mathcal{G}_5^B$*, whose monodromy lies in* $\mathrm{Alt}(5)$.

So the source's $\mathcal{G}_n^B$ is the smaller, Alt-monodromy orbit of (3), as used throughout.

Theorem 6.2. *The closing sentence quoted above is false. Over all* $\mathrm{SL}(2,\mathbb{Z})$*-orbits of primitive* n*-square origamis in* $\mathcal{H}(2)$ *with* $n \le 13$*, the numbers of origamis fixed by the eight words are given by Table 3; in particular* $(ST)^2$ *fixes* 2 *origamis of* $\mathcal{G}_5^B$, 4 *of* $\mathcal{G}_7^B$ *and* 4 *of* $\mathcal{G}_{11}^B$*. An explicit witness is*

$$X_7 = \big((1\,2)(3\,4)(5\,6\,7),\ (1\,3\,5\,7\,2\,4\,6)\big),$$

a primitive 7*-square origami in* $\mathcal{H}(2)$ *with both permutations even, hence in* $\mathcal{G}_7^B$*, whose Veech group contains* $(ST)^2$ *and contains neither* ST *nor* $(TS)^2$*. Every other assertion of the remark is reproduced exactly in that range, with one omission:* ST^2 *and* S^2T *each fix one origami of* $\mathcal{G}_3$ *as well, which the remark's list does not mention.*

orbit	ST	ST^2	S^2T	S^2T^2	ST^3	S^3T	$(ST)^2$	$(TS)^{-1}ST$
$\mathcal{G}_3$	0	1	1	3	0	0	0	0
$\mathcal{G}_4$	0	1	1	2	0	0	0	0
$\mathcal{G}_5^A$	0	1	1	2	0	0	0	0
$\mathcal{G}_5^B$	2	0	0	0	0	0	2	2
$\mathcal{G}_7^A$	0	1	1	2	0	0	0	0
$\mathcal{G}_7^B$	0	0	0	0	1	1	4	0
$\mathcal{G}_9^B$	0	0	0	0	1	1	0	0
$\mathcal{G}_{11}^B$	0	0	0	0	0	0	4	0
all other orbits, $n \leq 13$	0	0	0	0	0	0	0	0

TABLE 3. Origamis fixed by the eight hyperbolic words of [7, §4.1], over the 16 orbits of $\mathcal{H}(2)$ with $n \leq 13$.

Proof sketch. For each of the 16 orbits with $n \leq 13$ the orbit is saturated from the seed of Proposition 2.3 and checked closed, so by Proposition 2.2 the list is the whole orbit; then for each of the eight words the origamis it fixes are counted by exhaustive scan of that list. This is 16×8 exhaustive counts, and Table 3 is their value. For X_7 the assertions — primitivity, membership in $\mathcal{H}(2)$, evenness of both permutations, membership in the 36-element orbit $\mathcal{G}_7^B$, and the three fixed-point assertions — are separate evaluations at that pair, so the counterexample does not depend on the canonical form being correct: it was additionally re-verified by brute force over all $7! = 5040$ relabellings with the canonical form switched off. $\square$

The failure is exactly where the source's own machinery predicts it can be.

Proposition 6.3. *On $\mathcal{G}_7^A$ the parity pair never takes the degenerate value, and T and S act on the three parity blocks as $(B_1\, B_2)$ and $(B_2\, B_3)$, which is* [7, Fig. 3.4]. *Consequently $(ST)^2$ acts on $\{B_1, B_2, B_3\}$ with no fixed block.*

Since a word fixing an origami must fix its block, $(ST)^2$ can fix no origami of an orbit that is not ε-constant: the orbits $\mathcal{G}_n$ with n even and $\mathcal{G}_n^A$ with n odd are excluded by [7, Prop. 3.3] itself, and the only orbits left are the $\mathcal{G}_n^B$ — which is exactly where Table 3 finds it. Running the same argument over all eight words, ST, ST^3, S^3T, $(TS)^{-1}ST$ and $(ST)^2$ act as fixed-point-free 3-cycles, while $ST^2 = S$ fixes B_1, $S^2T = T$ fixes B_3 and S^2T^2 is the identity; so [7, §4.1], which rules out ST, ST^3, S^3T and $(TS)^{-1}ST$ on the even-n and A orbits, under-uses its own proposition by exactly one word, and that word is the one its closing sentence over-generalises. At $n = 5$ the failure is already forced by the remark's own ST line, since $ST \in \mathrm{SL}(X)$ implies $(ST)^2 \in \mathrm{SL}(X)$; at $n = 7$ and $n = 11$ it is not, ST fixing nothing there.

Remark 6.4. No theorem of [7] depends on the sentence: it is explicitly heuristic ("Computations suggest", "does not seem to"), and the surrounding results do not use the absence of $(ST)^2$. What the correction changes is the conjectural picture of which pseudo-Anosov elements arise as Veech group elements of small primitive origamis, and it removes what would otherwise look like an asymmetry between $(ST)^2$ and the other words of its length.

7. Controls

The dichotomy of Sections 3 and 4 is a statement about two hyperelliptic strata, and the following says that it is not a formality of the certificate.

Proposition 7.1. (i) The dichotomy fails one stratum over. *The* $\mathrm{SL}(2,\mathbb{Z})$*-orbit of primitive 7-square origamis in $\mathcal{H}(4)$ reached from $\big((1\,2\,\cdots\,7), (1\,2\,4)\big)$ has* 120 *elements and constant parity pair, and the certificate of Section 2 returns* `false` *on it — not for a bookkeeping* *reason: the seed is a canonical primitive origami of* $\mathcal{H}(4)$. *The reason is exhibited: the* 60 *pairs* $\{X, -I\cdot X\}$ *are a genuine block system of that orbit, with a block of size* 2 *at the seed, so that orbit is imprimitive.*

(ii) And why the two strata differ. $-I = (TS^{-1}T)^2$ *fixes every origami of the* $\mathcal{H}(2)$ *orbits* $\mathcal{G}_7^A$ *and* $\mathcal{G}_7^B$ *and of the* $\mathcal{H}(1,1)$ *orbit* $\mathcal{S}_7$, *and no origami of that* $\mathcal{H}(4)$ *orbit.*

(iii) The obvious coarser guess is not a block system. *The two-class partition of* $\mathcal{G}_7^A$ *by* $\operatorname{sgn} h$ *alone is not invariant, while the parity pair is, with three classes of* 18 *in an orbit of* 54.

(iv) Non-vacuity. *Both trivial partitions of* $\mathcal{G}_7^A$ *are block systems, so both outer branches of the trichotomy are attainable.*

(v) The encoding is guarded. *A non-canonical seed — the raw pair* $\big((1\,2\,\cdots\,7),(1\,2)\big)$ *— makes the certificate return* `false`, *and so does a seed of the wrong stratum, in either direction between* $\mathcal{H}(2)$ *and* $\mathcal{H}(1,1)$.

Both directions of the bridge between the decidable check and the statement "is a block system" are proved, so the `false` *outcomes in (i), (iii) and (v) are genuine refutations and not merely uninformative computations.*

Part (i) is the source's own second construction: [7, §3] builds the system $\{X, -I\cdot X\}$ precisely on orbits where $-I$ acts without fixed points, which by (ii) is what distinguishes $\mathcal{H}(4)$ from the two genus-two strata. An unverified sweep over $\mathcal{H}(4)$ seeds with $6 \le n \le 13$ finds all three behaviours — orbits with both block systems, orbits with only $\{X, -I\cdot X\}$, and orbits that behave exactly like $\mathcal{H}(2)$ — so no dichotomy of the present shape can hold there; certifying the $\mathcal{H}(4)$ picture is a separate project.

8. Verification

Every statement in this paper has been formally verified in Lean 4 (toolchain `v4.32.0`) against *Mathlib*; the development contains no `sorry`, and the repository reference is to be added at submission. The division of labour is as follows. Propositions 2.1, 2.2, 2.3 and 2.4 are proved without computation — the first and third for an arbitrary type of squares, at the level of Mathlib's permutation groups — and use no axioms beyond `propext`, `Classical.choice` and `Quot.sound`. What is delegated to compiled evaluation, through Lean's `native_decide`, is exactly the finite searches: one Boolean per orbit for the $28 + 11$ block certificates behind Theorems 3.1 and 4.1, in which the orbit saturation, the closure test, the faithfulness of the index maps, the parity congruence and all $|\mathcal{O}| - 1$ derivation replays are fused into a single evaluation; one Boolean per orbit for the 16 word-counting certificates of Theorem 6.2, and one per witness for Proposition 6.1 and for X_7; one per item for the controls of Proposition 7.1; and one per closed-form comparison, the formulas (3), (4) and (6) being evaluated in integer arithmetic separately from any search. Theorem 3.2 is the only statement combining many certificates at once — all 28 in $\mathcal{H}(2)$ — and it introduces no evaluation of its own, the passage from the certified orbit lengths to (6) being kernel arithmetic. The whole certified development costs about 2.5 hours of CPU in Lean's interpreter and never exceeds 1.5 gigabytes of memory, the largest single item being the $\mathcal{S}_{15}$ orbit of Table 2 at about half an hour. Independently, every value in Tables 1, 2 and 3 was first produced over exactly the same ranges by an implementation in Python sharing no code with the formal development, and the census of Section 9 by one in C; both agree with it everywhere. The Python side stops exactly where the certified side does — $n = 21$ in $\mathcal{H}(2)$ and odd $n = 15$ in $\mathcal{H}(1,1)$ — so no unverified range extends past a verified one.

9. Appendix: the certified census

The census of primitive origamis and of orbit cardinalities recorded below is the calibration on which the encoding used above rests, and one of its values disagrees with the literature. The values themselves are not new. The origami database shipped with [15] tabulates every one of them, its coverage of each stratum running well past any n reached here. So does Zmiaikou's thesis [16] over the ranges its tables cover: Table B.3 (p. 131) gives the two $\mathcal{H}(1,1)$ orbit lengths at every $7 \le n \le 17$, Table B.2 (p. 130) the orbits of $\mathcal{H}(1,1)$ for $n \le 6$, and Table B.1 (p. 129) the orbits of $\mathcal{H}(4)$ at $n = 5$ and $n = 6$ — the last being where the one disagreement of Remark 9.4 lies.

Theorem 9.1. *Up to simultaneous conjugation:*

(i) *the numbers of primitive n-square origamis in $\mathcal{H}(2)$ are $3, 9, 27, 36, 90$ for $n = 3, \ldots, 7$, falling into $1, 1, 2, 1, 2$ orbits of cardinalities $\{3\}$, $\{9\}$, $\{18, 9\}$, $\{36\}$, $\{54, 36\}$; at $n = 3$ the three origamis are $\big((2\,3), (1\,2\,3)\big)$, $\big((2\,3), (1\,2)\big)$, $\big((1\,2\,3), (2\,3)\big)$, the three vertices of the graph of* [7, Fig. 2.1]*;*

(ii) *in $\mathcal{H}(1,1)$ there is no primitive origami with 2 or 3 squares, there are exactly 4 with 4 squares and 24 with 5, each forming a single orbit, and exactly 48 with 6 squares, forming two orbits of 24;*

(iii) *there are exactly 160 primitive 7-square origamis in $\mathcal{H}(1,1)$, falling into exactly two orbits, of cardinalities 16 and 144, the first being the ε-constant one; and $\mathcal{A}_7(1,1) = 16$, $\mathcal{S}_7(1,1) = 144$;*

(iv) *the numbers of primitive n-square origamis in $\mathcal{H}(4)$ are $40, 225, 775$ for $n = 5, 6, 7$, falling into $4, 7, 6$ orbits of cardinalities*

$$\{3, 10, 12, 15\}, \qquad \{10, 15, 15, 15, 20, 30, 120\}, \qquad \{30, 40, 105, 120, 120, 360\}.$$

Proof sketch. Each line is a complete enumeration: a simultaneous conjugation moves h to any permutation of its cycle type, so it suffices to run over the $p(n)$ cycle types and, for each, over all $n!$ choices of v, filtering by the cycle type of $c(h, v)$, by transitivity and by primitivity, then reducing to canonical form and removing duplicates — that is, $p(n) \cdot n!$ candidate pairs, 840 at $n = 5$ and 75 600 at $n = 7$. The orbit decomposition is Proposition 2.2 applied to one seed per orbit, together with the checks that each computed orbit is contained in the enumeration, that the enumeration is covered by the orbits, and that the sizes sum to the total — which is what forces the list of orbits to be complete. □

Theorem 9.2. *There are $\mathrm{SL}(2,\mathbb{Z})$-orbits of primitive n-square origamis of the following cardinalities: in $\mathcal{H}(2)$, 108 at $n = 8$ and the pairs $(108, 81)$ at $n = 9$ and $(225, 180)$ at $n = 11$, which are $(|\mathcal{G}_n^A|, |\mathcal{G}_n^B|)$ as given by* (3)*, that formula being matched also at $n = 5, 7$; in $\mathcal{H}(1,1)$, 96 and 144 at $n = 8$, 72 and 432 at $n = 9$, 240 and 432 at $n = 10$, 240 and 1200 at $n = 11$, 480 and 960 at $n = 12$, 560 and 2520 at $n = 13$, 1008 and 2160 at $n = 14$, 960 and 4032 at $n = 15$, in each pair the ε-constant orbit first, and all of them equal to the values $\mathcal{A}_n(1,1)$ and $\mathcal{S}_n(1,1)$ conjectured in* [16]*; and in $\mathcal{H}(4)$, $25, 90, 135$ at $n = 9$, $10, 135, 450$ at $n = 10$ and $180, 200, 420$ at $n = 11$.*

Proof sketch. Each cardinality is a breadth-first saturation from one seed, certified closed and hence a complete orbit by Proposition 2.2; the number of orbits is not asserted at any of these n, and at $n = 12, 14$ in $\mathcal{H}(1,1)$ a complete enumeration is out of reach ($p(12) \cdot 12! \approx 3.7 \cdot 10^{10}$). The comparisons with (3) and (4) are evaluations of the closed forms in integer arithmetic, independent of the searches. □

The even values $n = 8, 10, 12, 14$ in $\mathcal{H}(1,1)$ lie outside the range where (5) applies, so Theorem 9.2 confirms four cells of the half of Zmiaikou's conjecture that [7, §6] calls open — as a derivation from the definitions rather than as a new number: all four are printed in [16, Table B.3] and all appear in [15], as do the $\mathcal{H}(4)$ values, which agree with that database row for row.

Proposition 9.3. *The census computation is guarded: the canonical form is invariant under simultaneous conjugation over all 120 relabellings of all 24 primitive 5-square origamis of $\mathcal{H}(1,1)$, and so are the two moves; a non-transitive pair whose commutator has the right cycle type is excluded; primitivity is not vacuous ($4 \to 10$ at $n = 4$ and $48 \to 88$ at $n = 6$ in $\mathcal{H}(1,1)$ without it); a mis-transcribed move takes the two $n = 7$ seeds of $\mathcal{H}(1,1)$ out of the stratum; one generator alone gives orbits of size 7 inside orbits of sizes 16 and 144; and neither $n = 7$ orbit of $\mathcal{H}(1,1)$ is the whole stratum while the two together are.*

Remark 9.4 (one disagreement with the literature). Table B.1 of [16] (p. 129) lists the $\mathrm{SL}(2,\mathbb{Z})$-orbits of 5- and 6-square origamis in $\mathcal{H}(4)$ with a representative, an orbit length and a monodromy group for each. At $n=5$ the four lengths printed are $3,12,10,15$, which is Theorem 9.1(iv) as a multiset. At $n=6$ seven orbits are printed, of lengths $10,15,15,15,20,30,60$: the first six agree and the seventh does not, ours being 120. The discrepancy is not one of convention — the printed lengths sum to 165, whereas $10+15+15+15+20+30+120=225$ is the number of primitive 6-square origamis in $\mathcal{H}(4)$ returned by the complete enumeration, which together with the orbit decomposition and the certificate of its completeness is part of Theorem 9.1(iv). Outside the formal development we also computed the orbit of the representative printed in the disagreeing row, $\sigma=(1\,2\,3)$, $\tau=(2\,4)(3\,5\,6)$ in the notation of [16], which is our (h,v), and found it to have 120 elements; the database [15] also gives $10,15,15,15,20,30,120$ here. We take the printed 60 to be a misprint. It is the only entry of [16] we compare against that disagrees.

Only the second half of Remark 9.4 — the orbit of the representative printed in the disagreeing row — was computed outside the formal development. The enumeration it is compared with, including the certificate of its own completeness, is machine-checked, and it is the enumeration that carries the correction.

Remark 9.5. At $n=6$ in $\mathcal{H}(1,1)$ the two cardinalities of Theorem 9.1(ii) agree with the conjectured values, $\mathcal{A}_6(1,1)=\mathcal{S}_6(1,1)=24$, but the *labels* fail: a computation outside the formal development gives the monodromy groups as $\mathrm{Alt}(6)$ and a primitive subgroup of $\mathrm{Sym}(6)$ of order 120, not $\mathrm{Sym}(6)$. This is [16, Thm. 3.21], "for each integer $n\neq 6$, the monodromy group of any primitive n-square-tiled surface from $\mathcal{H}(1,1)$ is either $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$", whose proof names the $n=6$ exception as an index-6 subgroup of $\mathrm{Sym}(6)$; the two orbits are the two primitive rows of [16, Table B.2, p. 130], which otherwise lists all five $\mathrm{SL}(2,\mathbb{Z})$-orbits of 6-square origamis in $\mathcal{H}(1,1)$, primitive or not. It explains why Zmiaikou's conjecture is posed for $n\geq 7$.

References

[1] W. Y. Chen, *Noncongruence modular curves as Hurwitz spaces*, arXiv:2510.12003v1 [math.NT] (13 October 2025), doi:10.48550/arXiv.2510.12003. Survey article, intended for conference proceedings; the counts and the sentence quoted above are those of v1, the only version.

[2] E. Duryev, *Teichmüller curves in genus two: square-tiled surfaces and modular curves*, Geom. Topol. **28** (2024), no. 9, 3973–4056, doi:10.2140/gt.2024.28.3973; arXiv:1905.09312. The result numbering used above (Theorem 3.1) is that of arXiv:1905.09312v2, against which we checked it.

[3] A. Eskin, H. Masur and M. Schmoll, *Billiards in rectangles with barriers*, Duke Math. J. **118** (2003), no. 3, 427–463, doi:10.1215/S0012-7094-03-11832-3; arXiv:math/0107204.

[4] E. Gutkin and C. Judge, *Affine mappings of translation surfaces: geometry and arithmetic*, Duke Math. J. **103** (2000), no. 2, 191–213, doi:10.1215/S0012-7094-00-10321-3.

[5] P. Hubert and S. Lelièvre, *Prime arithmetic Teichmüller discs in* $\mathcal{H}(2)$, Israel J. Math. **151** (2006), no. 1, 281–321, doi:10.1007/BF02777365; arXiv:math/0401056. Version 1 of the preprint circulated under the title *Square-tiled surfaces in* $\mathcal{H}(2)$, which is how it is occasionally cited; the two are the same paper.

[6] P. Hubert and S. Lelièvre, *Noncongruence subgroups in* $\mathcal{H}(2)$, Int. Math. Res. Not. **2005**, no. 1, 47–64, doi:10.1155/IMRN.2005.47; arXiv:math/0410595.

[7] L. Jeffreys and C. Matheus, *Euler characteristics of* $\mathrm{SL}(2,\mathbb{Z})$*-orbit graphs of origamis*, arXiv:2602.21984v1 [math.GT] (25 February 2026), doi:10.48550/arXiv.2602.21984. Preprint; all section and result numbers quoted above are those of v1, the only version.

[8] A. Kappes and M. Möller, *Cutting out arithmetic Teichmüller curves in genus two via Theta functions*, Comment. Math. Helv. **92** (2017), no. 2, 257–309, doi:10.4171/CMH/412.

[9] E. Lanneau and D.-M. Nguyen, *Teichmüller curves generated by Weierstrass Prym eigenforms in genus 3 and genus 4*, J. Topol. **7** (2014), no. 2, 475–522, doi:10.1112/jtopol/jtt036.

[10] E. Lanneau and D.-M. Nguyen, *Weierstrass Prym eigenforms in genus four*, J. Inst. Math. Jussieu **19** (2020), no. 6, 2045–2085, doi:10.1017/S1474748019000057.

[11] S. Lelièvre and E. Royer, *Orbitwise countings in* $\mathcal{H}(2)$ *and quasimodular forms*, Int. Math. Res. Not. **2006**, Art. ID 42151, 30 pp., doi:10.1155/IMRN/2006/42151.

[12] C. McMullen, *Teichmüller curves in genus two: discriminant and spin*, Math. Ann. **333** (2005), no. 1, 87–130, doi:10.1007/s00208-005-0666-y.

[13] C. Meiri and D. Puder, *The Markoff group of transformations in prime and composite moduli*, Duke Math. J. **167** (2018), no. 14, 2679–2720, doi:10.1215/00127094-2018-0024. With an appendix by D. Carmon.

[14] G. Schmithüsen, *An algorithm for finding the Veech group of an origami*, Experiment. Math. **13** (2004), no. 4, 459–472, doi:10.1080/10586458.2004.10504555; arXiv:math/0401185.

[15] F. Chapoton, D. Davis, V. Delecroix, O. Fontaine, C. Fougeron, L. Jeffreys, S. Lelièvre, J. Rüth, I. Yakovlev and C. Zhang, `surface_dynamics` — a SageMath package, version 0.7.0 (12 February 2025), doi:10.5281/zenodo.14859632. The origami database referred to above is the SQLite file `origamis.db` of that release, one row per orbit.

[16] D. Zmiaikou, *Origamis and permutation groups*, Ph.D. thesis, Université Paris-Sud 11, 2011; NNT 2011PA112133, HAL tel-00648120. Page and table numbers quoted above are those of the deposited text.