Origami and the product replacement algorithm

Jan-Christoph Schlage-Puchta
Gabriela Weitze-Schmitthüsen

University Rostock
KIT Karlsruhe

4.7.2013

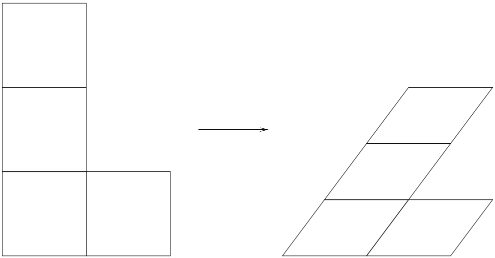
Origami

A *translational surface* is a two dimensional manifold which has an atlas, such that changes of charts are translations.
An *Origami* of size d is

- A d-sheated covering of a puctured Torus;
- Two permutations in S_d generating a transitive group
- A set of d squares, glued together along corresponding sides, such that the resulting surface is connected

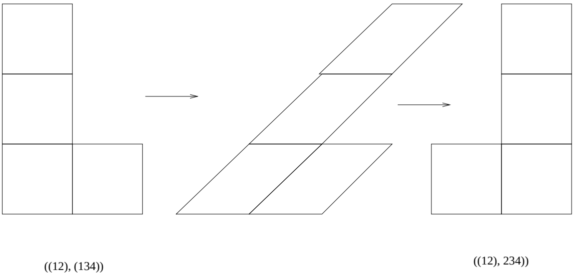
Origami give translational surfaces/higher genus curves which are not much more complicated then the torus/elliptic curves.

The action of $\mathrm{Sl}_2(\mathbb{R})$



An origami defines a map from $\mathrm{Sl}_2(\mathbb{R})/\mathrm{Sl}_2(\mathbb{Z})$ to the space of curves with given topological data.

The action of $\mathrm{Sl}_2(\mathbb{Z})$



$\mathrm{Sl}_2(\mathbb{Z})$ acts on the set of origami. The stabilizer of an origami is the *Veechgroup* of the origami. The orbit of this action corresponds to different descriptions of isomorphic curves.

The product replacement algorithm

Problem: Given a finite group G, choose elements from G at random.
Application: Las-Vegas-algorithms
Define random walk on

$$X = \{(x_1, \ldots, x_k) \in G^k | \langle x_1, \ldots, x_k \rangle = G\}$$

by choosing $i \neq j$ at random, and replacing x_i by $x_i x_j$.
Experimentally the distribution quickly converges to something close to an equidistribution, however, proving anything is quiet difficult.

Product replacement and Origami

Let $\pi, \sigma \in S_d$ be permutations generating a transitive permutation groups.

- (π, σ) defines an origami, which defines an orbit of the action under $\mathrm{Sl}_2(\mathbb{Z})$;
- (π, σ) defines a generating pair of a transitive subgroup of S_d, which defines a connected component of the product replacement algorithm.

These notions coincide:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \hat{=} (x, y) \mapsto (xy, y), \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \hat{=} (x, y) \mapsto (y, x)$$

Reason: $\mathrm{Out}(F_2) \cong \mathrm{Sl}_2(\mathbb{Z})$

Motivation

Groups help Curves:
Finite group theory well developed, Combinatorics allows for easy constructions
Curves help Groups:
Curves have additional structure, might yield non-obvious invariants

Curves with many automorphisms

Theorem (Hurwitz, 1896)

1. *A curve of genus $g \geq 2$ has at most $84(g-1)$ automorphisms.*
2. *There exists a curve of genus $g \geq 2$ with $84(g-1)$ automorphisms if and only if there exists a $(2,3,7)$-generated group of order $84(g-1)$.*

Theorem (S-P&W-S, 2013)

1. *A translational surface of genus $g \geq 2$ has at most $4(g-1)$ automorphisms.*
2. *If C is a translational surface with maximal automorphism group then C is a branched covering of an elliptic curves with all branching orders 1 or 2;*
3. *There exists a translational surface of genus $g \geq 2$ with $4(g-1)$ automorphisms if and only if $(g-1, 6) > 1$.*

Proof:

$p : X \to X/\mathrm{Aut}(X)$ defines a normal covering. Since p is normal, all branching orders over some point are equal. Computation using Riemann-Hurwitz-formula yields that $X/\mathrm{Aut}(X)$ has genus 1, one branch point, and all branching orders equal 2.
Hence X is an origami.
Branch points of X correspond to cycles of $[\pi, \sigma]$. Hence translational surfaces with maximal automorphism group correspond to normal subgroups $N \triangleleft F_2$ such that $F_2/N = \langle a, b\rangle$ where $[a, b]$ has order 2.

Proof, continued:

Theorem

There exists a 2-generated group $G = \langle a, b \rangle$ of order n, such that $[a, b]$ has order 2, if and only if n is divisible by 8 or 12.

Proof.

Existence: Direct product of cyclic groups with generalized quaternion groups or A_4.
Necessity: If neither by 8 nor 12 divide $|G|$, then G is solvable.
Let H be a $2'$-Hall group of G. If $4 \nmid |G|$, then H is normal, thus $G' \leq H$, hence $|G'|$ is odd.
If $(|G|, 24) = 4$, then $(G : N_G(H))$ divides $(G : H) = 4$.
Counting orbits of the action of H on its conjugates yields:
$(G : N_G(H)) - 1$ is non-negative linear combination of prime divisors of $|H|$. Hence H is normal, and $|G'|$ is odd. □

Congruence subgroups

A principal congruence subgroup of $\mathrm{Sl}_2(\mathbb{Z})$ is the kernel of the map $\mathrm{Sl}_2(\mathbb{Z}) \to \mathrm{Sl}_2(\mathbb{Z}/q\mathbb{Z})$ for some integer q. A congruence subgroup is a subgroup containing some principal congruence subgroup.
A subgroup Δ is totally non-congruence, if $\Delta \to \mathrm{Sl}_2(\mathbb{Z}/q\mathbb{Z})$ is surjective for all q.
Congruence subgroups are rare: There are $\mathcal{O}(n^{c \log n})$ congruence subgroups of index n, compared with $n!^{1/6+o(1)}$ subgroups.
But: Veechgroups are not random subgroups, constructions yield congruence subgroups.

Theorem (Hubert-Lelièvre)

There exists precisely one origami with genus 2 and one branch point of order 2, whose Veechgroup is congruence.

Theorem (S-P&W-S)

For any given branching data there exists an origami realizing these branching orders, which have totally non-congruence Veechgroup.

Translates to: There exist $\pi, \sigma \in S_d$, such that

- $\langle \pi, \sigma \rangle$ acts transitive;
- $[\pi, \sigma]$ has prescribed cycle structure;
- For each prime number p there exists (π', σ') in the orbit of (π, σ), such that $p \nmid o(\pi')o(\sigma')$.

Theorem (S-P&W-S)

Almost all origami have totally non-congruence Veechgroup.

For the proof study $\pi, \pi\sigma, \pi\sigma^2, \ldots$ using representation theory.
Proof mimics Romanov's theorem on integers of the form $p + 2^a$.