Distinguishing triangle groups by their finite quotients

Marston Conder
University of Auckland

m.conder@auckland.ac.nz

[Answer to question by Martin Bridson and Alan Reid]

Riemann surface actions

Let X be a compact Riemann surface of genus g, and let G be the group of all conformal automorphisms of X.

Then X is isomorphic to the quotient space $\mathcal{U}/\Lambda$ of the upper half-plane $\mathcal{U}$ via its fundamental group Λ, and G is isomorphic to Γ/Λ, where Γ is the normalizer of Λ in $\mathrm{PSL}(2,\mathbb{R})$, the group of all orientation-preserving isometries of $\mathcal{U}$.

The groups Γ and Λ are called Fuchsian groups, which by definition are co-compact discrete subgroups of $\mathrm{PSL}(2,\mathbb{R})$. The group Λ is also called a surface-kernel group.

Fuchsian groups and signatures

Every Fuchsian group Γ has a finite presentation in terms of (say) r elliptic generators $x_1, x_2, \ldots, x_r$ and 2γ hyperbolic generators $a_1, b_1, \ldots, a_\gamma, b_\gamma$, subject to the defining relations

$$x_1{}^{m_1} = x_2{}^{m_2} = \cdots = x_r{}^{m_r} = [a_1, b_1] \ldots [a_\gamma, b_\gamma]\, x_1 \ldots x_r = 1.$$

The presentation can be encoded by the signature of Γ, which is $\sigma(\Gamma) = (\gamma; m_1, m_2, \ldots, m_r)$.

If the surface-kernel group Λ is the fundamental group of a compact Riemann surface of genus g, then $r = 0$ and $\gamma = g$, so that Λ has signature $(g; -)$.

Riemann-Hurwitz formula

The area of a fundamental region for the Fuchsian group Γ with signature $(\gamma; m_1, m_2, \dots, m_r)$ is $\mu(\Gamma) = 2\pi\xi(\Gamma)$, where

$$\xi(\Gamma) = 2\gamma - 2 + \sum_{i=1}^{r}\left(1 - \frac{1}{m_i}\right).$$

If $\Lambda \leq \Gamma$ with finite index, then $\mu(\Lambda) = |\Gamma : \Lambda| \cdot \mu(\Gamma)$, or, equivalently, $\xi(\Lambda) = |\Gamma : \Lambda| \cdot \xi(\Gamma)$. In particular, if $G = \Gamma/\Lambda$ is the conformal automorphism group of a compact Riemann surface of genus g, then $\xi(\Lambda) = 2g - 2$ and therefore

$$2g - 2 = |G|\left(2\gamma - 2 + \sum_{i=1}^{r}\left(1 - \frac{1}{m_i}\right)\right).$$

This is known as the Riemann-Hurwitz formula.

Triangle groups

The 'group order to genus' ratio is $\dfrac{|G|}{2g-2} = \dfrac{|\Gamma:\Lambda|}{\xi(\Lambda)} = \dfrac{1}{\xi(\Gamma)}$.

For genus $g > 1$, this ratio is maximised when $\xi(\Gamma)$ takes its minimum positive value, which is $\frac{1}{84}$, and occurs when the group Γ has signature $(0;\, 2, 3, 7)$. This is Hurwitz's theorem (and then quotients of Γ are called Hurwitz groups).

More generally, a Fuchsian group with signature $(0;\, k, l, m)$ is called a triangle group, and has defining presentation

$$\Delta(k, l, m) = \langle\ x, y, z \mid x^k = y^l = z^m = xyz = 1\ \rangle.$$

Big question (by Martin Bridson & Alan Reid)

If Γ and Σ are Fuchsian groups that have exactly the same finite quotients, then are Γ and Σ isomorphic?

In other words, is every Fuchsian group determined up to isomorphism by its finite quotients?

Important case: What about triangle groups?

Preliminaries

Let Γ be the (r, s, t) triangle group, with presentation

$$\Delta(r, s, t) = \langle\ x, y, z \mid xyz = x^r = y^s = z^t = 1\ \rangle.$$

We can assume $r \leq s \leq t$ (by permutation and/or inversion of the three generators).

Also the (r, s, t) triangle group Γ is called

- spherical (genus 0) if $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} > 1$
- euclidean (genus 1) if $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} = 1$
- hyperbolic (genus $g > 1$) if $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$.

Now suppose the (r, s, t) triangle group Γ and the $(u, v.w)$ triangle group Σ have exactly the same finite quotients.

Some properties of hyperbolic triangle groups

If $\frac{1}{r}+\frac{1}{s}+\frac{1}{t}<1$, then the (r,s,t) triangle group Δ is

- infinite
- insoluble
- residually finite [i.e. the intersection of all subgroups of finite index in Δ is trivial]
- SQ-universal [i.e. every countable group is a subgroup of some quotient of Δ]

Observation 1

If Γ is spherical, then [by Maschke] we know that Γ is cyclic, dihedral, tetrahedral, octahedral or icosahedral.

In fact:

- $\Gamma \cong C_t$ if $(r,s,t) = (1,t,t)$,
- $\Gamma \cong D_t$ if $(r,s,t) = (2,2,t)$,
- $\Gamma \cong A_4$ if $(r,s,t) = (2,3,3)$,
- $\Gamma \cong S_4$ if $(r,s,t) = (2,3,4)$,
- $\Gamma \cong A_5$ if $(r,s,t) = (2,3,5)$.

Conversely, if Γ is finite, then Γ is spherical.

Corollary 1: If Γ is spherical, then so is Σ, and $\Gamma \cong \Sigma$.

Observation 2

If Γ is toroidal, then Γ is infinite and soluble, with free abelian derived group $\Gamma' = [\Gamma, \Gamma]$ and finite abelian quotient $\Gamma/[\Gamma, \Gamma]$.

In fact:

- $\Gamma/[\Gamma,\Gamma] \cong C_6$ if $(r,s,t) = (2,3,6)$,
- $\Gamma/[\Gamma,\Gamma] \cong C_2 \times C_4$ if $(r,s,t) = (2,4,4)$,
- $\Gamma/[\Gamma,\Gamma] \cong C_3 \times C_3$ if $(r,s,t) = (3,3,3)$.

Conversely, if Γ is infinite and soluble, then Γ is toroidal.

Corollary 2: If Γ is toroidal, then so is Σ, and $\Gamma \cong \Sigma$.

So from now on, we may suppose that Γ and Σ are both hyperbolic. In particular, Γ and Σ are infinite but insoluble.

Observation 3

The abelianisation of the (r,s,t) triangle group Γ is $C_d \times C_e$ where $d = \gcd(r,s,t)$, $e = \mathrm{lcm}(\gcd(r,s),\gcd(r,t),\gcd(s,t))$, and $de = rst/\mathrm{lcm}(r,s,t)$.

[For example, the abelianisation of $\Delta(4,6,28)$ is $C_2 \times C_4$.]

Corollary 3:

(a) $\gcd(r,s,t) = \gcd(u,v,w)$,

(b) $\frac{rst}{\mathrm{lcm}(r,s,t)} = \frac{uvw}{\mathrm{lcm}(u,v,w)}$, and

(c) $\mathrm{lcm}(\gcd(r,s),\gcd(r,t),\gcd(s,t))$
$= \mathrm{lcm}(\gcd(u,v),\gcd(u,w),\gcd(v,w))$.

Observation 4

Let us say that a group G is (r,s,t)-generated if G can be generated by elements a, b and c of orders r, s and t respectively such that $abc = 1$ ... or in other words, if G is a smooth quotient Γ/Λ of the (r,s,t)-triangle group Γ.

Moreover, for any triple (r,s,t), the set of (r,s,t)-generated groups is non-empty. The latter follows from the known fact that every hyperbolic triangle group is residually finite (or from Macbeath's theorem, to come).

Corollary 4: The groups Γ and Σ have exactly the same sets of (r,s,t)-generated quotients and (u,v,w)-generated quotients, and each of these sets is non-empty.

Macbeath's theorem [A.M. Macbeath (1969)]

Let (r, s, t) be a hyperbolic triple other than $(2, 5, 5)$, $(3, 4, 4)$, $(3, 3, 5)$, $(3, 5, 5)$ or $(5, 5, 5)$. Then for any odd prime p, the group PSL$(2, p^f)$ is (r, s, t)-generated if and only if p^f is the smallest power of p for which PSL$(2, p^f)$ contains elements of orders r, s and t.

The five triples above, together with the spherical triples and the triple $(3, 3, 3)$, were called exceptional by Macbeath.

Note that $A_5 \cong$ PSL$(2, 5)$ is $(2, 5, 5)$-, $(3, 3, 5)$-, $(3, 5, 5)$- and $(5, 5, 5)$-generated, while the group S_4 is $(3, 4, 4)$-generated.

Observation 5

If $G = \Gamma/\Lambda$ is the smallest (r, s, t)-generated quotient of Γ, then Λ is a Fuchsian group with signature $(2g; -)$, being the fundamental group of a Riemann surface S of genus g, where $2-2g = |G|\left(\frac{1}{r}+\frac{1}{s}+\frac{1}{t}-1\right)$, by Riemann-Hurwitz.

In particular, Λ/Λ' is free abelian of rank $2g$.

It follows that for any positive integer n coprime to $|G|$, the largest quotient of Γ that is an extension of an abelian group of exponent n by the group G is the quotient $\Gamma/\Lambda'\Lambda^n$, which has order $n^{2g}|G|$.

Corollary 5: $\frac{1}{r}+\frac{1}{s}+\frac{1}{t}=\frac{1}{u}+\frac{1}{v}+\frac{1}{w}$ [Pf: Same g for both.]

Observation 6

For any prime divisor p of rst, let p^α, p^β and p^γ be the largest powers of p dividing r, s and t, ordered so that $\alpha \leq \beta \leq \gamma$. Then:

(a) p^α is the largest power of p dividing $\gcd(r, s, t)$,

(b) p^γ is the largest power of p dividing $\mathrm{lcm}(r, s, t)$,

(c) $p^{\alpha+\beta+\gamma}$ is the largest power of p dividing rst,

(d) $p^{\alpha+\beta}$ is the largest power of p dividing $\frac{rst}{\mathrm{lcm}(r,s,t)}$.

Furthermore, either $\beta = \gamma$, or p^γ is the largest power of p dividing the reduced denominator of $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} = \frac{rs+rt+st}{rst}$.

Corollary 6a: $rst = uvw$, and $\text{lcm}(r, s, t) = \text{lcm}(u, v, w)$, and $rs + rt + st = uv + uw + vw$.

Proof. For any prime divisor p of rst, the largest powers of p dividing r,s and t are determined by the quantities $\gcd(r, s, t)$, $\frac{rst}{\text{lcm}(r,s,t)}$ and $\frac{1}{r} + \frac{1}{s} + \frac{1}{t}$. By Corollaries 3 and 5, these three quantities are the same for the triple (u, v, w), and hence the largest powers of p dividing u, v and w are equal to those for r,s and t (in some order). The rest follows easily. $\square$

Corollary 6b: If (r, s, t) is one of the exceptional hyperbolic triples $(2, 5, 5)$, $(3, 4, 4)$, $(3, 3, 5)$, $(3, 5, 5)$ or $(5, 5, 5)$, then $(r, s, t) = (u, v, w)$.

Proof. Each such triple (r, s, t) is uniquely determined by rst (plus $\text{lcm}(r, s, t)$ and $\gcd(r, s, t)$ in the case of $(3, 4, 4)$). $\square$

Corollary 6c: If the triples (r, s, t) and (u, v, w) have an entry in common, then $(r, s, t) = (u, v, w)$.

Proof. Suppose for example that $t = w$.

Then $rs = \frac{rst}{t} = \frac{uvw}{w} = uv$, and then since $rs + (r + s)t = rs+rt+st = rst(\frac{1}{r}+\frac{1}{s}+\frac{1}{t}) = uvw(\frac{1}{u}+\frac{1}{v}+\frac{1}{w}) = uv+uw+vw = uv + (u + v)w$, we find that $r + s = u + v$.

It is now an elementary exercise to deduce from $rs = uv$ and $r + s = u + v$ that $\{r, s\} = \{u, v\}$.

The same argument works for all other coincidences. $\square$

Observation 7

If Γ has a dihedral group D_m as a quotient, then its abelianisation has even order, so at least two of r, s and t are even.

Corollary 7: If at least two of r, s and t are even, then $(r, s, t) = (u, v, w)$.

Proof. By comparison of abelianisations, at least two of u, v and w are even. Now let $m = \max(t, w)$ if all three of r, s and t are even, or let m be the largest odd integer among r, s, t, u, v and w otherwise. Then D_m is a quotient of Γ or Σ, and hence must also be a quotient of the other. It follows that m appears in both triples (r, s, t) and (u, v, w), and so by Corollary 6c, we have $(r, s, t) = (u, v, w)$. $\square$

Do we have enough yet?

No!

There are 3581 pairs of distinct triples $\{(r,s,t),(u,v,w)\}$ with

(a) $r \le s \le t$ and $u \le v \le w$,

(b) $rst = uvw \le$ 12,000,000,

(c) $\gcd(r,s,t) = \gcd(u,v,w)$ and $\operatorname{lcm}(r,s,t) = \operatorname{lcm}(u,v,w)$,

(d) $rs + rt + st = uv + uw + vw$, and

(e) at most one of r,s,t being even.

e.g. take $(5,14,21)$ and $(7,7,30)$, or $(4,11,105)$ and $(5,7,132)$.

Observation 8

Define the L_2-set of a triple (k, l, m) to be the (unique) set of pairwise coprime positive integers such that
(a) their LCM is the same as the LCM of $\{k, l, m\}$, and
(b) each of k, l and m divides exactly one member of the set
— e.g. the L_2-set of $(6, 15, 19)$ is $\{19, 30\}$.

If the triple (k, l, m) is non-exceptional, then by Macbeath's theorem, PSL$(2, p)$ is (k, l, m)-generated iff each member of the L_2-set of (k, l, m) is equal to p or a divisor of $\frac{p\pm1}{2}$.

Corollary 8a: If the triples (r, s, t) and (u, v, w) are non-exceptional, then they have the same L_2-set.

Corollary 8b: If one of r, s, t is coprime to each of the other two, then $(r, s, t) = (u, v, w)$. In particular, if Γ is perfect, then $(r, s, t) = (u, v, w)$.

Proof. Suppose that $(r, s, t) \neq (u, v, w)$, and also, say, that $\gcd(r, st) = 1$. (The other two cases are similar.) Then since $uvw = rst$ (by Corollary 6a) and each of u, v and w is distinct from r, s and t (by Corollary 6c), at least one of u, v and w divides neither r nor st, and hence is of the form cd where c and d are non-trivial divisors of r and st respectively. It follows that the L_2-sets of (r, s, t) and (u, v, w) are distinct, contradiction. $\square$

Thus any two non-isomorphic perfect triangle groups are distinguished by their finite quotients.

Observation 9

For every triple (k, l, m) such that $k, l, m > 1$ and at most one of k, l, m is even, and for every integer $q > 3$ that does not divide any of the members of the L_2-set of (k, l, m), there exists a finite quotient G of the (k, l, m) triangle group such that G has no element of order q. [The proof is easy.]

Corollary 9: The integers u, v and w do not have non-trivial divisors u', v' and w' such that one of r, s and t is coprime to each of $6, u', v'$ and w'.

Proof. If $q \in \{r, s, t\}$ is coprime to $6, u', v'$ and w', then there exists a finite quotient G of the (u', v', w') triangle group such that G has no non-trivial element of order dividing q. But then G is a quotient of $\Delta(u, v, w)$ but not $\Delta(r, s, t)$. $\square$

Application/example

Consider the triples $(17, 162, 459)$ and $(27, 34, 1377)$.

Note that 17 divides 459, 34 and 1377, and if we 'suppress' it (by dividing through by 17), then we obtain the two sub-triples $(1, 162, 27)$ and $(27, 2, 81)$.

Now $\mathsf{PSL}(2, 163)$ is a quotient of $\Delta(27, 2, 81)$, and hence one of $\Delta(27, 34, 1377)$, but because it has no element of order 17, it cannot be a quotient of $\Delta(17, 162, 459)$.

Thus $\Delta(17, 162, 459) \ncong \Delta(27, 34, 1377)$.

Note: Equivalently, only the latter has $C_{17} \times \mathsf{PSL}(2, 163)$ as a smooth quotient.

Summary of where we're at:

The observations made so far are sufficient to distinguish most triangle groups from each other, using just abelian, dihedral and 2-dimensional projective quotients (and extensions of abelian groups by the latter).

But these are not completely sufficient.

For example, consider the triples $(15, 42, 63)$ and $(21, 21, 90)$, which satisfy the conclusions of Corollaries 3, 5 and 6a, but do not satisfy the hypothesis of Corollary 8b and do not admit the kinds of divisors met in Corollary 9.

For such triples, we need to consider further types of quotients, so we turn to other direct products.

Example

Consider the triples $(5, 35, 42)$ and $(7, 10, 105)$.

We can think of $(5, 35, 42)$ as a kind of 'product' of the triples $(5, 5, 6)$ and $(5, 7, 7)$, and then see that the direct product $\mathrm{PSL}(2, 11) \times \mathrm{PSL}(2, 29)$ is $(5, 35, 42)$-generated.

But on the other hand, elements of $\mathrm{PSL}(2, 11)$ have orders dividing 5, 6 and 11, while elements of $\mathrm{PSL}(2, 29)$ have orders dividing 14, 15 and 29, and so the direct product $\mathrm{PSL}(2, 11) \times \mathrm{PSL}(2, 29)$ has no element of order 105. Hence $\mathrm{PSL}(2, 11) \times \mathrm{PSL}(2, 29)$ is not $(7, 10, 105)$-generated.

Thus $\Delta(5, 35, 42) \ncong \Delta(7, 10, 105)$.

Observation 10

Suppose (r_1, s_1, t_1) and (r_2, s_2, t_2) are sub-triples such that $r = \text{lcm}(r_1, r_2)$, $s = \text{lcm}(s_1, s_2)$ and $t = \text{lcm}(t_1, t_2)$. If G and H are finite groups that are (r_1, s_1, t_1)- and (r_2, s_2, t_2)-generated, say by element triples (x_1, y_1, z_1) and (x_2, y_2, z_2), then some subgroup of $G \times H$ is (r, s, t)-generated, by the triple $((x_1, x_2), (y_1, y_2), (z_1, z_2))$.

Corollary 10: If q_1 and q_2 are coprime positive integers, each greater than 3, such that $q_1 q_2$ divides at least one of u, v and w, then either $q_1 q_2$ divides at least one of r, s and t, or otherwise one of r, s and t is prime and equal to q_1 or q_2.

[Proof uses quotients of the form $G \times \text{PSL}(2, p)$ for some p.]

Theorem [2011, not yet published]

If Γ and Σ are triangle groups having exactly the same finite homomorphic images, then $\Gamma \cong \Sigma$.

Proof. Assume the theorem is false. Let (r, s, t) and (u, v, w) be distinct triples such that $\Gamma = \Delta(r, s, t)$ and $\Sigma = \Delta(u, v, w)$ have exactly the same finite quotients.

WLOG assume $w = \max\{r, s, t, u, v, w\}$. By Corollary 6c, we have $r \leq s \leq t < w$, so w cannot divide r, s or t.

If w is a prime-power, then w divides $\mathrm{lcm}(r, s, t) = \mathrm{lcm}(u, v, w)$ and so divides at least one of r, s, t, contradiction. Hence w is composite, say $w = q_1 q_2$, with $1 < q_1 < q_2 < w$.

Now $q_1 q_2 = w$ divides none of r, s and t, and so Corollary 10 applies, giving a contradiction unless q_1 and q_2 cannot be chosen such that each is each is greater than 3, and neither is both prime and equal to one (or more) of r, s and t.

An easy number-theoretic exercise then shows that

(a) $q_1 = 2$ and q_2 is an odd prime-power, or

(b) $q_1 = 3$ and q_2 is a prime-power, or

(c) one of q_1 and q_2 is prime and equal to r, s or t, and the other is a prime-power, or

(d) $w = 6p$ where $p > 3$ is a prime equal to r, s or t.

We can eliminate each of these four cases in turn, using the earlier results [in about a third of a page for each case].

Final note

Recall there are 3581 pairs of distinct triples $\{(r,s,t),(u,v,w)\}$ with

(a) $r \leq s \leq t$ and $u \leq v \leq w$,

(b) $rst = uvw \leq 12{,}000{,}000$,

(c) $\gcd(r,s,t) = \gcd(u,v,w)$ and $\mathrm{lcm}(r,s,t) = \mathrm{lcm}(u,v,w)$,

(d) $rs + rt + st = uv + uw + vw$, and

(e) at most one of r, s, t being even.

All of these 3581 pairs can be eliminated using Corollary 8b (the 'coprime' test) or Corollary 10 (on direct products), except for **one** pair, viz. $\{(17,162,459),(27,34,1377)\}$, which we eliminated using Corollary 9 (by 'suppressing' $r = 17$).