NEW ZEALAND JOURNAL OF MATHEMATICS
Volume 52 (2022), 827–844
https://doi.org/10.53733/193

TWO NEW PROOFS OF THE FACT THAT TRIANGLE GROUPS ARE DISTINGUISHED BY THEIR FINITE QUOTIENTS

Marston Conder

(Received 14 December, 2021)

Dedicated to the memory of my good friend and colleague Sir Vaughan Jones

Abstract. In a 2016 paper by Alan Reid, Martin Bridson and the author, it was shown using the theory of profinite groups that if Γ is a finitely-generated Fuchsian group and Σ is a lattice in a connected Lie group, such that Γ and Σ have exactly the same finite quotients, then Γ is isomorphic to Σ. As a consequence, two triangle groups $\Delta(r,s,t)$ and $\Delta(u,v,w)$ have the same finite quotients if and only if (u,v,w) is a permutation of (r,s,t). A direct proof of this property of triangle groups was given in the final section of that paper, with the purpose of exhibiting explicit finite quotients that can distinguish one triangle group from another. Unfortunately, part of the latter direct proof was flawed. In this paper two new direct proofs are given, one being a corrected version using the same approach as before (involving direct products of small quotients), and the other being a shorter one that uses the same preliminary observations as in the earlier version but then takes a different direction (involving further use of the 'Macbeath trick').

1. Introduction

For any positive integers r, s and t, the ordinary (r,s,t) *triangle group* is the abstract group $\Delta(r,s,t)$ with presentation $\langle\, x,y,z \mid x^r = y^s = z^t = xyz = 1\,\rangle$.

In a recent paper [**2**], it was shown that if Γ is a finitely-generated Fuchsian group and Σ is a lattice in a connected Lie group, such that Γ and Σ have exactly the same finite quotients, then Γ is isomorphic to Σ. As a consequence, two triangle groups $\Delta(r,s,t)$ and $\Delta(u,v,w)$ have the same finite quotients if and only if (u,v,w) is a permutation of (r,s,t). The main theorems in the first seven sections of [**2**], including these, were proved using the theory of profinite groups, without reference to explicit finite quotients. A second proof of the fact concerning triangle groups was given in the final section of [**2**], with the purpose of exhibiting explicit finite quotients that can distinguish one triangle group from another.

Unfortunately, this second proof (given as the proof of Theorem 8.1 in [**2**]) was flawed. In particular, Lemma 8.11 is incorrect, even when restricted to triples (r,s,t) and (u,v,w) that survive Lemmas 8.3, 8.4, 8.5 and 8.7, Proposition 8.6 and Corollaries 8.8 and 8.10, as it fails for the triples $(15,105,126)$ and $(21,30,315)$ with $(q_2,q_2) = (7,45)$, as well as for similar triples. Also there were gaps in the argument used in the proof of Theorem 8.1. The situation is somewhat more complicated than was indicated. In particular, the use of direct products of two quotients each isomorphic to $\mathrm{PSL}(2,p)$ for some prime p did not cover all possibilities remaining after simpler methods were applied. Please note, however, that the main findings of [**2**] are unaffected by these flaws, as Section 8 of [**2**] is independent of the earlier sections.

Here we must sincerely thank Frankie Chan, who pointed out the problems with Lemma 8.11, and provided an effective version of Theorem 8.1 of [**2**] in his recent PhD thesis [**3**], while developing an algorithm for distinguishing finite quotients between cocompact triangle groups and lattices of constant-curvature symmetric 2-spaces, with specific attention paid to the case where these lattices are Fuchsian groups.

In this paper we give two new direct proofs of Theorem 8.1 of [**2**], without requiring Lemma 8.11. The first one is rather intricate, showing how the approach involving direct products of quotients isomorphic to $\mathrm{PSL}(2,p)$ for some prime p can be undertaken correctly and extended in some exceptional cases (by using quotients that are direct products of the form $\mathrm{PSL}(2,p_1) \times \mathrm{PSL}(2,p_2) \times A$ where A is cyclic, in those cases).

The second proof is quite a lot shorter, using certain smooth quotients of triangle groups $\Delta(k,l,m)$, where k, l and m divide either r, s and t, or u, v and w (in some order). This is an approach we considered earlier and were able to use successfully to deal with the vast majority of triple pairs, but completed only with the help of a key observation made by Frankie Chan in [**3**] for the remaining pairs, and again we owe a debt of gratitude to him for that.

Here we note that both proofs show that any two non-isomorphic hyperbolic triangle groups $\Delta(r,s,t)$ and $\Delta(u,v,w)$ can be distinguished by finite quotients that are abelian, dihedral, isomorphic to $\mathrm{PSL}(2,p)$ for some prime p, or a direct product $\mathrm{PSL}(2,p_1) \times \mathrm{PSL}(2,p_2) \times A$ where p_1 and p_2 are distinct primes and A is cyclic (or trivial), or an extension of a homocyclic abelian group by one of the preceding groups.

Before giving the two new proofs, we repeat and extend some of the background to this topic, in order to make the paper self-contained.

2. Further Background

Each triangle group $\Delta(r,s,t)$ is called *spherical*, *Euclidean* or *hyperbolic* according to whether the quantity $1/r + 1/s + 1/t$ is greater than, equal to or less than 1, respectively. Note that $\Delta(r,s,t)$ is isomorphic to $\Delta(u,v,w)$ if and only if the triple (u,v,w) is a permutation of the triple (r,s,t).

The spherical triangle groups are $\Delta(1,n,n)$, $\Delta(2,2,n)$, $\Delta(2,3,3)$, $\Delta(2,3,4)$ and $\Delta(2,3,5)$, which are isomorphic to C_n (cyclic), D_n (dihedral of order $2n$), A_4, S_4 and A_5, respectively. The Euclidean triangle groups are $\Delta(2,3,6)$, $\Delta(2,4,4)$ and $\Delta(3,3,3)$, each which is an extension of a free abelian group of rank 2 by a cyclic group (C_6, C_4 and C_3, respectively). In particular, the spherical triangle groups are finite, while the Euclidean triangle groups are infinite but soluble. See [**4**] for further details. In contrast, all hyperbolic triangle groups are infinite and insoluble, and have a wealth of finite quotients (see [**5**] for example).

The latter categorisation makes the spherical and Euclidean triangle groups easy to distinguish from others by their finite quotients, and so we will focus our attention on the hyperbolic ones, namely those with $1/r + 1/s + 1/t < 1$.

As in [**2**], we define a finite group G to be (k,l,m)-*generated* if G can be generated by elements a, b and c of (precise) orders k, l and m such that $abc = 1$. In this case we say that G is a *smooth* quotient of the triangle group $\Delta(k,l,m)$, noting that the corresponding epimorphism from $\Delta(k,l,m)$ to G preserves the orders of the canonical generators of $\Delta(k,l,m)$, and has torsion-free kernel. For any hyperbolic triple (k,l,m), the set of (k,l,m)-generated groups is non-empty because of the residual finiteness of the hyperbolic triangle group $\Delta(k,l,m)$, but in most cases $\Delta(k,l,m)$ can also have 'non-smooth' quotients, in which the orders of the canonical generators of $\Delta(k,l,m)$ are not preserved.

We will make use of the following important but relatively straightforward observation, the proof of which we leave as an exercise for the reader:

Lemma 2.1. *For any integers k, l and m, all greater than 1, let Δ be the triangle group $\Delta(k,l,m)$. Then the abelianisation $\Delta/\Delta' = \Delta/[\Delta,\Delta]$ of Δ is isomorphic to the direct product $C_e \times C_d$, where $e = \mathrm{lcm}(\gcd(k,l),\gcd(k,m),\gcd(l,m))$ and $d = \gcd(k,l,m)$, and also $de = klm\,\mathrm{lcm}(k,l,m)$. Moreover, $\Delta/[\Delta,\Delta]$ is (k',l',m')-generated, where $k' = \gcd(k,lm)$, $l' = \gcd(l,km)$ and $m' = \gcd(m,kl)$.*

Also a theorem below by Macbeath [**6**] on triangle-generation of the finite simple groups $\mathrm{PSL}(2,q)$ is critical to this work:

Theorem 2.2. *Let (k,l,m) be any hyperbolic triple other than $(2,5,5)$, $(3,4,4)$, $(3,3,5)$, $(3,5,5)$ or $(5,5,5)$. Then for any given odd prime p, the group $\mathrm{PSL}(2,p^f)$ is (k,l,m)-generated if and only if p^f is the smallest power of p for which $\mathrm{PSL}(2,p^f)$ contains elements of orders k, l and m.*

The triples $(2,5,5)$, $(3,4,4)$, $(3,3,5)$, $(3,5,5)$ and $(5,5,5)$, together with the spherical triples and the triple $(3,3,3)$, were called *exceptional* by Macbeath. Note that the spherical group $\Delta(2,3,5) \cong A_5 \cong \mathrm{PSL}(2,5)$ is also $(2,5,5)$-, $(3,3,5)$-, $(3,5,5)$- and $(5,5,5)$-generated, while the spherical group $\Delta(2,3,4) \cong S_4$ is also $(3,4,4)$-generated.

We also make use of the fact that if the finite group G is (k,l,m)-generated, then G is a group of conformal automorphisms of a compact Riemann surface S of genus g, where

$$2 - 2g = |G|\left(\tfrac{1}{k} + \tfrac{1}{l} + \tfrac{1}{m} - 1\right)$$

as a consequence of the Riemann-Hurwitz formula. The kernel K of the corresponding smooth homomorphism from $\Delta(k,l,m)$ onto G is the fundamental group of S, and is itself a Fuchsian group, with signature $(2g;-)$. In particular, if $g \geq 1$ then K is generated by $2g$ elements $a_1, b_1, \ldots, a_g, b_g$ subject to a single defining relation $[a_1,b_1]\ldots[a_g,b_g] = 1$. Now for any positive integer n, the subgroup $K'K^{(n)}$ generated by the derived subgroup K' and the nth powers of all elements of K is characteristic in K and hence normal in $\Delta(k,l,m)$, and the quotient $\Delta(k,l,m)/K'K^{(n)}$ is then isomorphic to an extension by G of an abelian subgroup $K/K'K^{(n)}$ of rank $2g$ and exponent n (and order n^{2g}). This observation is often known as 'the Macbeath trick'.

Hence for any (k,l,m)-generated group G, we can construct an infinite family of smooth quotients of $\Delta(k,l,m)$, to help distinguish $\Delta(k,l,m)$ from other triangle groups.

In what follows, we will also require some information about the groups $\mathrm{PSL}(2,p)$, for p prime. When p is odd, the orders of the elements of $\mathrm{PSL}(2,p)$ are precisely the divisors of p, $\frac{p-1}{2}$ and $\frac{p+1}{2}$ (see [**7**, Chapter 3.6] for example). The integers p, $\frac{p-1}{2}$

and $\frac{p+1}{2}$ are pairwise coprime, so the order of any non-trivial element of $\mathrm{PSL}(2,p)$ divides exactly one of them.

Next, define the *L_2-set* of a triple (k,l,m) to be the (unique) set of pairwise coprime positive integers whose least common multiple is the same as that of $\{k,l,m\}$ and which has the property that each of k,l and m divides exactly one member of that set. For example, if k,l and m are themselves pairwise coprime, then the L_2-set of the triple (k,l,m) is just $\{k,l,m\}$, while if $\gcd(k,lm)=1$ but $\gcd(l,m)>1$ then its L_2-set is $\{k,\mathrm{lcm}(l,m))\}$, and if $\gcd(k,l)>1$ and $\gcd(l,m)>1$ then its L_2-set is $\{\mathrm{lcm}(k,l,m))\}$. Note that every maximal prime-power divisor of $\mathrm{lcm}(k,l,m)$ divides exactly one member of the L_2-set.

Accordingly, we have the following corollary of Macbeath's theorem (Theorem 2.2):

Corollary 2.3.

(a) *If (k,l,m) is a hyperbolic triple and p is an odd prime, then the group* $\mathrm{PSL}(2,p)$ *is (k,l,m)-generated if and only if every member of the L_2-set of the triple (k,l,m) is equal to p or a divisor of $\frac{p\pm1}{2}$.*

(b) *Let (k,l,m) be any triple of integers greater than* 1*. Then 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 smooth finite quotient G of the (k,l,m) triangle group such that G has no element of order q. Similarly, for every integer $q>1$ that is coprime to* 6 *and to every member of the L_2-set of (k,l,m), there exists a smooth finite quotient G of the (k,l,m) triangle group such that G has no non-trivial element of order dividing q. Moreover, when the triple (k,l,m) is hyperbolic, in both cases G can be taken as* $\mathrm{PSL}(2,p)$ *for some prime $p>5$.*

(c) *If two triples of integers greater than* 1 *have the same least common multiple but different L_2-sets, then the corresponding triangle groups have different sets of smooth quotients.*

Proof. Part (a) is an immediate consequence of Theorem 2.2.

Both cases of part (b) are easy for all non-hyperbolic triples and exceptional triples: we can take $G=D_m$ for $(k,l,m)=(2,2,m)$ whenever $m\geq 2$, or $G=A_4$ for $(k,l,m)=(2,3,3)$, or $G=S_4$ for $(k,l,m)=(2,3,4)$ or $(3,4,4)$, or $G=A_5$ for $(k,l,m)=(2,3,5)$, $(2,5,5)$, $(3,3,5)$, $(3,5,5)$ or $(5,5,5)$, or $G=C_6$ for $(k,l,m)=(2,3,6)$, or $G=C_4$ for $(k,l,m)=(2,4,4)$, or $G=C_3$ for $(k,l,m)=(3,3,3)$. For any non-exceptional hyperbolic triple (k,l,m), we can take $G=\mathrm{PSL}(2,p)$, where p is a prime such that $p\equiv\pm1$ modulo twice each of the members of the L_2-set of (k,l,m), but $p\not\equiv\pm1$ modulo $2q$ in the first case, and $p\not\equiv\pm1$ modulo h for every prime divisor h of q in the second case. In both cases, the existence of such a prime p is guaranteed by the Chinese Remainder Theorem and Dirichlet's theorem on primes in arithmetic progression.

Finally, for part (c), the L_2-set of one of the two triples must contain an integer $q>3$ that does not divide any of the members of the L_2-set of the other triple, and then the assertion follows from part (b). □

3. Main Theorem and Preliminary Steps for its New Proofs

We can now begin to prove the following, in which we use the notation $(r, s, t) \simeq (u, v, w)$ to mean that (r, s, t) is a permutation of (u, v, w).

Theorem 3.1. *If $\Gamma = \Delta(r, s, t)$ and $\Sigma = \Delta(u, v, w)$ are triangle groups having exactly the same finite quotients, then $(r, s, t) \simeq (u, v, w)$ and so $\Gamma \cong \Sigma$.*

As a first step, we may suppose that (r, s, t) and (u, v, w) are hyperbolic triples. Next, we present a key observation that generalises part of Lemma 8.4 of [**2**], followed by combination of the remainder of Lemmas 8.3 to 8.5 and 8.7 of [**2**] and some further helpful properties.

Lemma 3.2. *Under the given assumptions, $\Gamma = \Delta(r, s, t)$ and $\Sigma = \Delta(u, v, w)$ have the same (k, l, m)-generated quotients, for every triple (k, l, m) of integers greater than* 1.

Proof. This follows easily from the assumption that Γ and Σ have exactly the same finite quotients. □

Lemma 3.3. *Under the given assumptions,*

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

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

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

(d) $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} = \frac{1}{u} + \frac{1}{v} + \frac{1}{w}$,

(e) *a finite group is (r, s, t)-generated if and only if it is (u, v, w)-generated,*

(f) *$rst = uvw$, and $\mathrm{lcm}(r, s, t) = \mathrm{lcm}(u, v, w)$, and $rs + rt + st = uv + uw + vw$,*

(g) *$v^2(s - u)(w - s) = s^2(v - r)(t - v)$, and similarly for every permutation of (r, s, t) and every permutation of (u, v, w),*

(h) *if $r \le s \le t$ and $u \le v \le w$, and (r, s, t) and (u, v, w) have no common entry, then either $r < u \le v < s \le t < w$ or $u < r \le s < v \le w < t$, and*

(i) *the triples (r, s, t) and (u, v, w) have the same L_2-set.*

Proof. Parts (a) to (c) follow immediately from Lemma 2.1.

For part (d), we may suppose without loss of generality that $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} \le \frac{1}{u} + \frac{1}{v} + \frac{1}{w}$, and let G be any (r, s, t)-generated finite quotient of Γ. Then G is also a quotient of Σ. So now let u', v' and w' be divisors of u, v and w (respectively) chosen such that G is (u', v', w')-generated, and $\frac{1}{u'} + \frac{1}{v'} + \frac{1}{w'}$ is as small as possible subject to those conditions. Then in particular, $\frac{1}{u'} + \frac{1}{v'} + \frac{1}{w'} \ge \frac{1}{u} + \frac{1}{v} + \frac{1}{w} \ge \frac{1}{r} + \frac{1}{s} + \frac{1}{t}$.

Next, for any n coprime to $|G|$, the largest quotient of Γ that is an extension of an abelian group of exponent n by G has order $n^{2g}|G|$, where $2-2g = |G|(\frac{1}{r} + \frac{1}{s} + \frac{1}{t} - 1)$, by comments made in the previous section. On the other hand, the largest quotient of Σ that is an extension of an abelian group of exponent n by G is a smooth quotient of the (u', v', w') triangle group and so has order $n^{2g'}|G|$, where $2-2g' = |G|(\frac{1}{u'} + \frac{1}{v'} + \frac{1}{w'} - 1)$. Since Γ and Σ have the same quotients, we find that $g' = g$, so $\frac{1}{u'} + \frac{1}{v'} + \frac{1}{w'} = \frac{1}{r} + \frac{1}{s} + \frac{1}{t}$. The final observation in the previous paragraph now gives us $\frac{1}{u} + \frac{1}{v} + \frac{1}{w} = \frac{1}{r} + \frac{1}{s} + \frac{1}{t}$, as required.

The latter also implies that $(u', v', w') = (u, v, w)$, and hence that G is (u, v, w)-generated. The converse holds by the same argument, with the roles of (r, s, t) and (u, v, w) reversed, and this proves (e).

For part (f), let p be any prime divisor of rst, and let p^α, p^β and p^γ be the largest powers of p dividing r, s and t, ordered in such a way that $\alpha \le \beta \le \gamma$. Then p^α must be the largest power of p dividing $\gcd(r, s, t)$, while p^β is the largest power of p dividing $\mathrm{lcm}(\gcd(r, s), \gcd(r, t), \gcd(s, t))$, and p^γ is the largest power of p dividing $\mathrm{lcm}(r, s, t)$. Also $p^{\alpha+\beta+\gamma}$ is the largest power of p dividing rst, and so $p^{\alpha+\beta}$ is the largest power of p dividing $\frac{rst}{\mathrm{lcm}(r,s,t)}$. Furthermore, either $\gamma = \beta$, or p^γ is the largest power of p dividing the denominator of $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} = \frac{rs+rt+st}{rst}$ when the latter is expressed in reduced form. (To verify the last claim, note that $rs + rt + st$ is divisible by $p^{\alpha+\beta}$ but not $p^{\alpha+\beta+1}$ when $\alpha \le \beta < \gamma$.)

Hence the largest powers of p dividing r,s and t are determined by the quantities $\gcd(r, s, t)$, $\frac{rst}{\mathrm{lcm}(r,s,t)}$ and $\frac{1}{r} + \frac{1}{s} + \frac{1}{t}$. By parts (a), (b) and (d), 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. As this holds for all p, the stated identities follow easily.

Part (g) follows from expanding and simplifying $v^2(s-u)(w-s)-s^2(v-r)(t-v)$ using the identities $rst = uvw$ and $rs + rt + st = uv + uw + vw$ from part (f), and noting that those two identities are invariant under all permutations of (r, s, t) and/or (u, v, w).

To prove part (h), let us suppose that $r < u$, so that $r = \min\{r, s, t, u, v, w\}$. Then since (r, s, t) and (u, v, w) have no common entry, we have only the following five possibilities, with others ruled out by the identity $rst = uvw$:

$$r \le s < u \le v \le w < t, \text{ or } r < u < s < v \le w < t, \text{ or } r < u \le v < s \le t < w,$$
$$\text{or } r < u \le v < s < w < t, \text{ or } r < u \le v \le w < s \le t.$$

The first, second, fourth and fifth of these possibilities can be eliminated, however, as they imply $v^2(s - u)(w - s) < 0 < s^2(v - r)(t - v)$, which contradicts part (g). The analogous argument works also when $u < r$.

Finally, part (i) follows immediately from part (c) of Corollary 2.3. □

At this stage we have enough to prove what happens in certain special cases, some of which were covered by Lemma 8.6 and Corollaries 8.8 and 8.10 of [**2**].

Proposition 3.4. *If u, v and w have divisors u', v' and w', all greater than 1, such that at least one of r, s and t is coprime to each of 6, u', v' and w', then there exists a finite group that is a quotient of $\Delta(u, v, w)$ but not a quotient of $\Delta(r, s, t)$. In particular, this holds when one of r, s and t is a power of some prime $p > 3$ such that none of u, v and w is a power of p. Also the analogous statements hold when (r, s, t) and (u, v, w) are interchanged.*

Proof. Suppose $k \in \{r, s, t\}$ is coprime to 6, u', v' and w'. Then by part (b) of Corollary 2.3, there exists a smooth finite quotient G of the triangle group $\Delta(u', v', w')$ such that G has no non-trivial element of order dividing k, and so G is a quotient of $\Delta(u, v, w)$ but cannot be a quotient of $\Delta(r, s, t)$. The rest follows easily. □

Proposition 3.5. *Theorem* 3.1 *holds in each of the following cases* (*or its equivalent form when* r, s *and* t *are permuted, or* (r, s, t) *and* (u, v, w) *are interchanged*):

(a) (r, s, t) *is one of the exceptional triples* $(2, 5, 5)$, $(3, 4, 4)$, $(3, 3, 5)$, $(3, 5, 5)$, $(5, 5, 5)$;

(b) (r, s, t) *and* (u, v, w) *have a common entry*;

(c) *two or more of* (r, s, t) *are even*;

(d) *one of* r, s, t *is coprime to each of the other two*;

(e) *one of* r, s, t *is a power of* 2;

(f) *one or more of* r, s, t, u, v *and* w *is equal to* $\gcd(r, s, t)$.

Proof. First, case (a) follows from parts (a) and (f) of Lemma 3.3, because $(2, 5, 5)$ is the only hyperbolic triple with $rst = 50$, and $(3, 4, 4)$ is the only hyperbolic triple with $rst = 48$, $\operatorname{lcm}(r, s, t) = 12$ and $\gcd(r, s, t) = 1$, and $(3, 3, 5)$ is the only hyperbolic triple with $rst = 45$, and $(3, 5, 5)$ is the only hyperbolic triple with $rst = 75$, and finally, $(5, 5, 5)$ is the only hyperbolic triple with $rst = 125$.

For case (b), 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 $r + s = u + v$. Hence r and s are the zeroes of the same quadratic $x^2 - bx + c$ as u and v (namely with $b = u + v$ and $c = uv$), so $\{r, s\} = \{u, v\}$, and then $(r, s, t) \simeq (u, v, w)$. The same argument works for all other coincidences between entries of (r, s, t) and (u, v, w).

Case (c) follows from the fact that for every integer $m \geq 2$, the only triangle group having the dihedral group D_m of order $2m$ as a smooth quotient is $\Delta(2, 2, m)$. For suppose that two or more of r, s and t are even. Then $\operatorname{lcm}(\gcd(r, s), \gcd(r, t), \gcd(s, t))$ is even, and therefore so is $\operatorname{lcm}(\gcd(u, v), \gcd(u, w), \gcd(v, w))$, and hence two or more of u, v and w are even. Also if all three of r, s and t are even, then $\gcd(r, s, t)$ is even, and then so is $\gcd(u, v, w)$, and hence all three of u, v and w are even. Now let $m = \max(r, s, t, u, v, w)$ if all three of r, s and t are even, or otherwise let m be the largest odd integer among r, s, t, u, v and w. Then the dihedral group D_m is a $(2, 2, m)$-generated quotient of Γ or Σ, and hence must also be a $(2, 2, m)$-generated quotient of the other. By definition of m, and the fact mentioned at the start of this paragraph, it follows that m appears in both triples (r, s, t) and (u, v, w), and hence by case (b) we know that $(r, s, t) \simeq (u, v, w)$.

In case (d), suppose first that $\gcd(r, st) = 1$. Then the L_2-set of (r, s, t) is either $\{r, s, t\}$ or $\{r, st\}$, and is the same as the L_2-set of (u, v, w), by part (i) of Lemma 3.3. It follows that each of u, v and w divides r or st. If one of them divides r and the other two divide st, then since $\gcd(r, st) = 1$, one of them is equal to r and then $(r, s, t) \simeq (u, v, w)$ by case (b). On the other hand, suppose two of them divide r, while the other one divides st and hence is coprime to the other two. Then $A = \operatorname{lcm}(\gcd(u, v), \gcd(u, w), \gcd(v, w))$ divides r, while $B = \operatorname{lcm}(\gcd(r, s), \gcd(r, t), \gcd(s, t)) = \gcd(s, t)$ which divides st, and then because $\gcd(r, st) = 1$, and $A = B$ (by part (c) of Lemma 3.3), we find $A = B = 1$, and so $\gcd(s, t) = 1$. Thus r, s and t are pairwise coprime, and it follows that the L_2-sets of (r, s, t) and (u, v, w) are both equal to $\{r, s, t\}$, and therefore $(r, s, t) \simeq (u, v, w)$. The other two possibilities $\gcd(s, rt) = 1$ and $\gcd(t, sr) = 1$ can be handled in the same way.

Case (e) now follows immediately from cases (c) and (d).

Finally, for case (f), suppose that $d = \gcd(r, s, t) = r$, say, with $r \le s \le t$ and $u \le v \le w$. If (r, s, t) and (u, v, w) have no common entry, then $r < u \le v < s \le t < w$ by part (h) of Lemma 3.3, and then $uvw = rst = dst$, so $st = \frac{uvw}{d}$, and then because $t \ge s \ge v+1$ it follows that $rs+rt+st = d(s+t)+\frac{uvw}{d} \ge 2d(v+1)+\frac{uvw}{d}$. Now if $u \ge 3d$, then $rs + rt + st > \frac{uvw}{d} \ge 3vw > uv + uw + vw$, while on the other hand, if $u < 3d$ then $u = 2d$, and therefore $2d(v + 1) = u(v + 1) > uv$ and $\frac{uvw}{d} = 2vw \ge uw+vw$, which together imply that $rs+rt+st \ge 2d(v+1)+\frac{uvw}{d} > uv + uw + vw$, another contradiction. Thus (r, s, t) and (u, v, w) have a common entry, and case (b) applies. □

4. The First New Proof, using Direct Products

For our first new proof of Theorem 3.1, we may suppose that (r, s, t) and (u, v, w) are non-exceptional hyperbolic triples for which $\Gamma = \Delta(r, s, t)$ and $\Sigma = \Delta(u, v, w)$ have exactly the same finite quotients, and hence satisfy the conclusions of Lemma 3.3 but not the principal hypothesis of Proposition 3.4, and do not satisfy any of the sufficient conditions (b) to (f) given in Proposition 3.5.

In particular, we suppose that (r, s, t) and (u, v, w) have no entry in common, no entry that is a power of 2, no entry equal to $\gcd(r, s, t)$, and no more than one even entry each, and also that no element of one of the triples is coprime to each of the other two, and no element of one of the triples is coprime to 6 and to proper divisors of the elements of the other triple. Furthermore, we let $M = \mathrm{lcm}(r, s, t) = \mathrm{lcm}(u, v, w)$, the maximal prime-power divisors of which will be a key to what follows.

For interested readers, we also give an indication of the relative numbers of triple-pairs in each situation considered, among the set $\mathcal{T}$ of 542970 distinct triple-pairs $\{(r, s, t), (u, v, w)\}$ satisfying the hypotheses two paragraphs above, with $2 \le r < u \le v < s \le t < w$ and $rst = uvw \le 12000000d^3$, where $d = \gcd(r, s, t) = \gcd(u, v, w)$. (Here we note that dropping the condition given in Proposition 3.4 would add another 830030 triple-pairs, which gives an indication of the importance of that condition.)

We consider four separate cases, which depend on the distribution of the maximal prime-power divisors of M among the divisors of the integers r, s, t, u, v and w, and we derive contradictions in all four cases. To do this, we consider a wider class of finite quotients of Γ and Σ, namely direct products of the form $G = Q_1 \times Q_2$ or $Q_1 \times Q_2 \times A$, where each Q_i is $\mathrm{PSL}(2, p_i)$ for some prime p_i, and A is abelian (indeed cyclic of order $d = \gcd(r, s, t)$).

In the first three of our four cases, Q_1 and Q_2 will be determined by a 'factorisation' of one of the triples, say (r, s, t), as a kind of product of two triples (r_1, s_1, t_1) and (r_2, s_2, t_2) of integers greater than 1, with the following properties:

(a) $\mathrm{lcm}(r_1, r_2) = r$ and $\mathrm{lcm}(s_1, s_2) = s$ and $\mathrm{lcm}(t_1, t_2) = t$,

(b) Q_1 and Q_2 are smooth quotients of the triangle groups $\Delta(r_1, s_1, t_1)$ and $\Delta(r_2, s_2, t_2)$, respectively, so that $Q_1 \times Q_2$ is a smooth quotient of $\Gamma = \Delta(r, s, t)$, but

(c) at least one of u, v and w is not the order of some element of $Q_1 \times Q_2$, and therefore

(d) $Q_1 \times Q_2$ is not a smooth quotient of $\Sigma = \Delta(u, v, w)$.

In the fourth case, we do the same but using three triples (r_1, s_1, t_1), (r_2, s_2, t_2) and (r_3, s_3, t_3), and a smooth abelian quotient A of $\Delta(r_3, s_3, t_3)$, such that $\mathrm{lcm}(r_1, r_2, r_3) = r$ and $\mathrm{lcm}(s_1, s_2, s_3) = s$ and $\mathrm{lcm}(t_1, t_2, t_3) = t$, but at least one of u, v and w is not the order of some element of $Q_1 \times Q_2 \times A$. In this case $Q_1 \times Q_2 \times A$ is a smooth quotient of Γ but not one of Σ. (In fact we take $A = C_d$ and $(r_3, s_3, t_3) = (d, d, d)$, where $d = \gcd(r, s, t)$.)

The first two cases cover the vast majority of the triple-pairs in our set $\mathcal{T}$ of 'small' triples, but each of them has a special sub-case which despite involving no triple-pairs from $\mathcal{T}$, appeared to need special treatment. (It may be possible to simplify the proof for those two cases by a more thorough application of the condition $rs + rt + st = uv + uw + vw$.)

Case (1): Suppose that some maximal prime-power divisor of $M = \mathrm{lcm}(r, s, t)$ greater than 3 divides just one of r, s and t, and hence also divides just one of u, v and w.

In this case, let q be the largest such maximal prime-power divisor of M.

By swapping the triples (r, s, t) and (u, v, w) and/or re-ordering each one if necessary, we may suppose that q divides both t and w but divides none of r, s, u and v, and that $\frac{t}{q} < \frac{w}{q}$, noting that $t \neq w$ because (r, s, t) and (u, v, w) have no entry in common.

When this happens, let $m = q$, let p be the prime divisor of m, so that $m = p^\gamma$, say, and let $m' = \frac{M}{q}$. Then $mm' = M$ and $\gcd(m, m') = 1$, with $m = q > 1$ and also $m' \geq \frac{w}{q} > 1$. Furthermore, $t \neq p$, for otherwise $t = m = q$, and so t is coprime to each of r and s.

Next, let (r_1, s_1, t_1) and (r_2, s_2, t_2) be the triples defined for each $x \in \{r, s, t\}$ as follows:

- $x_1 = x$ and $x_2 = p$ if x divides m, or
- $x_1 = m$ and $x_2 = \frac{x}{m}$ if x is a proper multiple of m (in which case $x = t$), or
- $x_1 = x$ and x_2 is a small prime divisor of x if x divides m' (so p does not divide x), or
- $x_1 = \gcd(x, m')$ and $x_2 = \gcd(x, m)$ if $1 < \gcd(x, m) < m$ and $\gcd(x, m') > 1$.

Then clearly $x_1 > 1$ and $x_2 > 1$ and $\mathrm{lcm}(x_1, x_2) = x$ for all $x \in \{r, s, t\}$. Moreover, each x_i is a divisor of either m or m', and in particular, $t_1 = m$ and $t_2 = \frac{t}{m}$ or p, but on the other hand, none of r_2, s_2 and t_2 is divisible by m. (To see this, note that if x divides m, and $p = x_2 = m$, then $x = m = p$ and so $t = x = p$, but we showed above that $t \neq p$.)

Hence the L_2-set of (r_1, s_1, t_1) is $\{m, b\}$ or $\{m, b, c\}$ where b and c are divisors of m', while the prime-power $m = p^\gamma$ divides no member of the L_2-set of (r_2, s_2, t_2).

In fact, the L_2-set $\mathcal{L}$ of (r_2, s_2, t_2) has one of the following forms, where α satisfies $1 \leq \alpha < \gamma$, and k and l are prime divisors of m':

(a) $\{p^\alpha\}$ or $\{p^\alpha, \frac{t}{m}\}$, if p divides r and s,

(b) $\{p^\alpha, \frac{t}{m}\}$ or $\{p^\alpha, k\}$ or $\{p^\alpha, \frac{t}{m}, k\}$, if p divides just one of r and s,

(c) $\{\frac{t}{m}\}$ or $\{\frac{t}{m}, k\}$ or $\{\frac{t}{m}, k, l\}$, if p divides neither r nor s.

(Note that in case (c), we cannot have $t_2 = p$, again because t is not coprime to r and s.)

Now if $\frac{w}{m}$ divides no element of the L_2-set of (r_2, s_2, t_2), then primes p_1 and p_2 can be found such that $Q_1 = \mathrm{PSL}(2, p_1)$ and $Q_2 = \mathrm{PSL}(2, p_2)$ are (r_1, s_1, t_1)- and (r_2, s_2, t_2)-generated, but Q_2 contains no element of order divisible by m or $\frac{w}{m}$. It then follows that $Q_1 \times Q_2$ is (r, s, t)-generated, but $Q_1 \times Q_2$ contains no element of order divisible by $m\frac{w}{m} = w$, and hence $Q_1 \times Q_2$ cannot be (u, v, w)-generated, a contradiction.

(For example, when $(r, s, t) = (21, 270, 441)$ and $(u, v, w) = (27, 63, 1470)$, with $M = 2 \cdot 27 \cdot 5 \cdot 49$, we take $m = q = 49$ and $m' = 270$, and then $(r_1, s_1, t_1) = (3, 270, 49)$ and $(r_2, s_2, t_2) = (7, 2, 9)$, with L_2-sets $\{49, 270\}$ and $\{2, 7, 9\}$, and we can choose p_2 so that $Q_2 = \mathrm{PSL}(2, p_2)$ has elements of order 14 and 9 but no element of order $m = 49$ or $\frac{w}{m} = 30$, and so $Q_1 \times Q_2$ has no element of order $49 \cdot 30 = 1470 = w$.)

Case (1) special sub-case: To complete case (1), we show that no element of the L_2-set of (r_2, s_2, t_2) is divisible by $\frac{w}{m}$. This is the most intricate part of the proof.

Assume the contrary. Then since $\frac{w}{m}$ divides neither p^α nor $\frac{t}{m}$, it must divide k or l, and so we may suppose that $w = mk$, where k is a prime divisor of m' but not one of $\frac{t}{m}$ and hence not one of t. Also because $k \in \mathcal{L}$ we may suppose from the definition of (r_2, s_2, t_2) that at least one of r and s divides m' and is divisible by k (but not by p). Moreover, if every $x \in \{r, s\}$ with this property were divisible by another prime divisor k' of m', then we could re-define x_2 as k', and thereby alter $\mathcal{L}$ so it contains no element divisible by $k = \frac{w}{m}$. Hence we may suppose that one of r and s, say r, is a power of k.

Next, because k is coprime to t, but r is not coprime to both s and t, we find that s is divisible by k as well. Also $\gcd(r, s)$ is divisible by k, so k is odd (because r and s cannot both be even), and $\gcd(u, v, w) = \gcd(r, s, t) = 1$ because r is coprime to t, and then since $\gcd(r, s) = k$ we find by part (c) of Lemma 3.3 that exactly two of u, v and w are divisible by k. Hence we may suppose without loss of generality that v is divisible by k, but u is not. In particular, if we let k^λ be the largest power of k dividing $M = \mathrm{lcm}(r, s, t)$, then the k-part of v is k^λ, and the k-parts of r and s are k and k^λ in some order.

Now assume for the moment that s is coprime to p (and hence to m), and let $f = \gcd(s, t)$. Then $f > 1$, because t is coprime to k and hence to r, and so cannot be coprime to s. But then f is odd (as it divides both s and t), so $f \geq 3$, and f is coprime to p (as f divides s), and so $km = w > t \geq mf \geq 3m$, which implies that $k \geq 5$. Moreover, f must divide two of u, v and w, but is coprime to w, so f divides v, which then cannot be a power of k. Hence Proposition 3.4 applies to r, because r $(= k$ or $k^\lambda)$ is coprime to 6 while none of u, v and w is a power of k. This contradiction shows that $\gcd(p, s) > 1$, and puts us in case (b) of the possibilities for the set $\mathcal{L}$.

In particular, s must be divisible by p^α, and so p is odd (because t is divisible by p as well), and also p^α divides exactly one of u and v (because it divides s and t and w but not r).

Thus $(r, s, t) = (k, k^\lambda p^\alpha s', mt')$ or $(k^\lambda, kp^\alpha s', mt')$ for some positive integers s' and t', both coprime to k and m, and $(u, v, w) = (p^\alpha u', k^\lambda v', km)$ or $(u', p^\alpha k^\lambda v', km)$ for some positive integers u' and v', both coprime to k and m. Also $k^{1+\lambda} p^\alpha s' m t' = rst = uvw = p^\alpha k^{1+\lambda} u' v' m$ and therefore $s't' = u'v'$.

Moreover, $\gcd(r,s) = k$ and $\gcd(r,t) = 1$ and $\gcd(s,t) = p^\alpha \gcd(s',t')$, the least common multiple of which is $kp^\alpha \gcd(s',t')$, while $\gcd(u,v) = \gcd(u',v')$, and either $\gcd(u,w) = p^\alpha$ and $\gcd(v,w) = k$, or $\gcd(u,w) = 1$ and $\gcd(v,w) = p^\alpha$, with least common multiple $kp^\alpha \gcd(u',tv)$. Hence by part (c) of Lemma 3.3 we find that $\gcd(s',t') = \gcd(u',v')$. In particular, it follows that if $\gcd(s',t') = 1$ then u is divisible by p^α, for otherwise $u = u'$ which is coprime to each of v and w.

We can now complete this sub-case by considering possibilities for s' and t'.

Case (i): Suppose $s't' = 1$. Then $u'v' = s't' = 1$ and so $s' = t' = u' = v' = 1$, which gives $(r,s,t) = (k, k^\lambda p^\alpha, m)$ and $(u,v,w) = (p^\alpha, k^\lambda, km)$ because $u > 1$, and then also $\lambda > 1$, because $r \neq v$ and $u > 1$. Next, dividing the identity $rs+rt+st = uv+uw+vw$ by kp^α gives $k^\lambda + p^{\gamma-\alpha} + k^{\lambda-1}m = k^{\lambda-1} + k^\lambda p^{\gamma-\alpha} + m$, and it follows that $k^\lambda \equiv k^{\lambda-1} \bmod p^{\gamma-\alpha}$ and $p^{\gamma-\alpha} \equiv m \bmod k^{\lambda-1}$, and therefore $k \equiv 1 \bmod p^{\gamma-\alpha}$ and $1 \equiv p^\alpha \bmod k^{\lambda-1}$. Accordingly, we find that $p^\alpha > k^{\lambda-1} \geq k > p^{\gamma-\alpha}$, which gives $\alpha > \gamma - \alpha > 0$, and so $\alpha > 1$.

Now we can define $(u_1,v_1,w_1) = (p^\alpha, k^\lambda, m)$ and $(u_2,v_2,w_2) = (p,k,k)$, so that $y_1 > 1$ and $y_2 > 1$ and $\operatorname{lcm}(y_1,y_2) = y$ for all $y \in \{u,v,w\}$, and the L_2-sets of (u_1,v_1,w_1) and (u_2,v_2,w_2) are $\{k^\lambda, m\}$ and $\{k,p\}$, respectively. Hence there exist primes p_1 and p_2 such that $Q_1 = \mathrm{PSL}(2,p_1)$ and $Q_2 = \mathrm{PSL}(2,p_2)$ are (u_1,v_1,w_1)- and (u_2,v_2,w_2)-generated, respectively, but Q_1 contains no element of order $k^\lambda p^\alpha$, and Q_2 contains no element of order k^λ or p^α (since $\lambda > 1$ and $\alpha > 1$). It follows that $Q_1 \times Q_2$ is (u,v,w)-generated, but contains no element of order $k^\lambda p^\alpha = s$, so cannot be (r,s,t)-generated, a contradiction.

Case (ii): Suppose $s't' > 1$. Here the situation depends on whether $k = 3$ or $k > 3$.

If $k > 3$, then v cannot be a proper multiple of k^λ, for otherwise Proposition 3.4 would apply to r ($= k$ or k^λ), and therefore $v = k^\lambda$ (and $v' = 1$), and p^α divides u. Then since $r \neq v$ we find that $(r,s,t) = (k, k^\lambda p^\alpha s', mt')$ while $(u,v,w) = (p^\alpha s't', k^\lambda, km)$, and $\lambda > 1$.

If $s' = 1$, then $t' > 1$, and we can take $(u_1,v_1,w_1) = (p^\alpha, k^\lambda, m)$ and $(u_2,v_2,w_2) = (t',k,k)$, with L_2-sets $\{k^\lambda, m\}$ and $\{k,t'\}$, and accordingly there exist primes p_1 and p_2 such that $Q_1 = \mathrm{PSL}(2,p_1)$ and $Q_2 = \mathrm{PSL}(2,p_2)$ are (u_1,v_1,w_1)- and (u_2,v_2,w_2)-generated, but Q_1 has no element of order $k^\lambda p^\alpha$ (even if $\alpha = 1$), and Q_2 has no element of order k^λ or p^α. It follows that $Q_1 \times Q_2$ is (u,v,w)-generated, but contains no element of order $k^\lambda p^\alpha = s$, and so $Q_1 \times Q_2$ cannot be (r,s,t)-generated, a contradiction.

Hence $s' > 1$. But now we can take $(u_1,v_1,w_1) = (p^\alpha s't', k^\lambda, m)$ and $(u_2,v_2,w_2) = (p,k,k)$, as in case (i) above, with L_2-sets $\{k^\lambda, ms't'\}$ and $\{k,p\}$, and there exist primes p_1 and p_2 such that $Q_1 = \mathrm{PSL}(2,p_1)$ and $Q_2 = \mathrm{PSL}(2,p_2)$ are (u_1,v_1,w_1)- and (u_2,v_2,w_2)-generated, but Q_1 has no element of order $k^\lambda s'$, and Q_2 has no element of order k^λ or $p^\alpha s'$, and again $Q_1 \times Q_2$ is (u,v,w)-generated, but has no element of order $k^\lambda p^\alpha s' = s$, so cannot be (r,s,t)-generated, another contradiction.

On the other hand, suppose $k = 3$. Then $p > 3$, so $s \geq kp^\alpha > 3$, and since $t < w = 3m$, we have $t = m$ or $2m$, and then $u'v' = s't' = s'$ or $2s'$, with s' coprime to 3 ($= k$) and p.

Now if $t = m = p^\gamma$, then $t' = 1$, so $u'v' = s't' = s' > 1$. Also if $u \neq p^\alpha$, then none of u, v and w is a power of p, in which case Proposition 3.4 applies to t, and therefore $u = p^\alpha$ (with $u' = 1$) and $v = k^\lambda v' = k^\lambda s'$. Accordingly, we have

$(r,s,t) = (3, 3^\lambda p^\alpha s', m)$ or $(3^\lambda, 3p^\alpha s', m)$, and $(u,v,w) = (p^\alpha, 3^\lambda s', 3m)$. Hence we can take $(u_1,v_1,w_1) = (p^\alpha, 3^\lambda, m)$ and $(u_2,v_2,w_2) = (p, s', 3)$, with L_2-sets $\{3^\lambda, m\}$ and $\{3, p, s'\}$, and find there are primes p_1 and p_2 such that $Q_1 = \mathrm{PSL}(2, p_1)$ and $Q_2 = \mathrm{PSL}(2, p_2)$ are (u_1,v_1,w_1)- and (u_2,v_2,w_2)-generated, but Q_1 has no element of order $3p$, $3s'$ or ps', and Q_2 has no element of order $3s'$ or ps'. It follows that $Q_1 \times Q_2$ has no element of order $3ps'$ and hence no element of order s, so again $Q_1 \times Q_2$ is (u,v,w)-generated but not (r,s,t)-generated, another contradiction.

Thus $t = 2m = 2p^\gamma$, with $t' = 2$, and then s is odd, so $\gcd(s',t') = 1$, and it follows that u is divisible by p^α, by observations made before case (i) above. Accordingly, we have $(r,s,t) = (3, 3^\lambda p^\alpha s', 2m)$ or $(3^\lambda, 3p^\alpha s', 2m)$, where $p > 3$, and s' is coprime to 2, 3 and p, while $(u,v,w) = (p^\alpha u', 3^\lambda v', 3m)$ and $2s' = u'v'$. Also u' is even, for otherwise u' divides s' and then $u = p^\alpha u'$ strictly divides $s = 3^\lambda p^\alpha s'$ or $3p^\alpha s'$, so Proposition 3.4 applies to u. Hence we can write s' as gh where $g = \gcd(s', u')$ and $h = \gcd(s', v')$, and then we have $(r,s,t) = (3, 3^\lambda p^\alpha gh, 2m)$ or $(3^\lambda, 3p^\alpha gh, 2m)$ and $(u,v,w) = (2p^\alpha g, 3^\lambda h, 3m)$.

Finally, $rs+rt+st = 3^{\lambda+1}p^\alpha gh + 6m + 3^\lambda p^\alpha 2ghm$ or $3^{\lambda+1}p^\alpha gh + 3^\lambda 2m + 6p^\alpha ghm$, while $uv + uw + vw = 3^\lambda p^\alpha 2gh + 3mp^\alpha 2g + 3^{\lambda+1}mh$, and in each case dividing by $3p^\alpha$ and then taking residues mod p gives $3^\lambda gh \equiv 3^{\lambda-1}2gh \bmod p$, so p divides $3^{\lambda-1}gh(3-2) = 3^{\lambda-1}gh$, which is impossible.

Case (2): Suppose that some maximal prime-power divisor q of $M = \mathrm{lcm}(r,s,t)$ divides just one of r, s and t, and just one of u, v and w, but the largest such q is 2 or 3.

Here we may suppose that q divides t and w, but divides none of r, s, u and v, while every maximal prime-power divisor of M greater than 3 divides at least two of r, s and t, and least two of u, v and w. Also neither t nor w can be equal to q, for otherwise case (d) of Proposition 3.5 would hold, and so each of them is a proper multiple of q.

We claim that t and w are not divisible by the same maximal prime-power divisors of M. Assume the contrary, and that (say) $t < w$. Then w has a non-trivial prime-power divisor $k \neq q$ such that k does not divide t. If $k > q$ then k cannot be a maximal prime-power divisor of M (for otherwise by assumption k would divide t), and so k strictly divides some maximal prime-power divisor of M, which then divides both u and v. But this implies that k divides all three of u, v and w, and so divides $\gcd(u,v,w) = \gcd(r,s,t)$, a contradiction (again since k does not divide t). Hence the only possibility is $k = 2$, giving $q = 3$, and then $(t, w) = (3c, 6c\}$ for some odd c. Also one of r and s must be even, say s, so $s = 2b$ for some b coprime to 6. Now $6rbc = rst = uvw = 6uvc$, and so $rb = uv$, which is coprime to 6, and yet $2rb \equiv rs \equiv rs + rt + st \equiv uv + uw + vw \equiv uv \equiv rb \bmod 3$, from which it follows that 3 divides $2rb - rb = rb$, a contradiction.

Hence we may suppose that there exists a maximal prime-power divisor m of M that divides w but not t. Then since m does not divide t, it divides r and s, so cannot be even, and as it does not divide $\gcd(r,s,t) = \gcd(u,v,w)$, it divides just one of u and v, say v. It follows that $m \neq 3$, for otherwise $q = 2$ and then u is coprime to 6 while r, s and t are divisible by 3, 3 and 2, so Proposition 3.4 applies to u. Thus m is odd and $m > 3$.

With this choice of m, again let $m' = \frac{M}{m}$, so $mm' = M$ and $\gcd(m, m') = 1$. This time m' is divisible by $\frac{w}{m}$ and hence by q, and so $\gcd(t, m')$ is divisible by q, giving $\gcd(t, m') > 1$.

Now let p be the prime divisor of m, and let $(r_1, s_1, t_1) = (m, m, \gcd(t, m'))$, and let $r_2 = p$ or $\frac{r}{m}$, depending on whether or not $r = m$, and let $s_2 = p$ or $\frac{s}{m}$, depending on whether or not $s = m$, and let t_2 be $\gcd(t, m)$ or the smallest prime divisor of $\frac{t}{q}$, depending on whether or not $\gcd(t, m) > 1$. Then $x_1 > 1$ and $x_2 > 1$ and $\mathrm{lcm}(x_1, x_2) = x$ for all $x \in \{r, s, t\}$. Note also that $r_2 \neq p$ and $s_2 \neq p$ when $m = p$, because otherwise r or s is equal to p and then Proposition 3.4 applies to r or s.

Next, the L_2-set of (r_1, s_1, t_1) is $\{m, \gcd(t, m')\}$, while the L_2-set of (r_2, s_2, t_2) contains no element divisible by m or q, and hence no element of order $\frac{w}{m} = q\,\frac{w}{qm}$, since none of r_2, s_2 and t_2 is divisible by m or q. It follows that unless $\frac{w}{m} = 2$ or 3, there exist primes p_1 and p_2 such that $Q_1 = \mathrm{PSL}(2, p_1)$ and $Q_2 = \mathrm{PSL}(2, p_2)$ are (r_1, s_1, t_1)- and (r_2, s_2, t_2)-generated, respectively, but Q_1 contains no element of order mq, and Q_2 contains no element of order divisible by m or $\frac{w}{m}$. When that happens, $Q_1 \times Q_2$ is (r, s, t)-generated but has no element of order $m\frac{w}{m} = w$, and so $Q_1 \times Q_2$ cannot be (u, v, w)-generated, a contradiction.

(For example, when $(r, s, t) = (175, 1225, 1470)$ and $(u, v, w) = (245, 3675, 350)$, with $M = 2 \cdot 3 \cdot 25 \cdot 49$, we take $q = 2$, $m = 25$ and $m' = 294$, and then $(r_1, s_1, t_1) = (25, 25, 294)$ and $(r_2, s_2, t_2) = (7, 49, 5)$, with L_2-sets $\{25, 294\}$ and $\{5, 49\}$, and we can choose p_2 so that $\mathrm{PSL}(2, p_2)$ has elements of order 5 and 49 but no element of order $m = 25$ or $\frac{w}{m} = 14$.)

Case (2) special sub-case: To complete case (2), we suppose that $\frac{w}{m} = 2$ or 3. Then we have $w = qm = 2m$ or $3m$, while every maximal prime-power divisor of M not in $\{2, q, m\}$ divides both u and v. So now let B be the product of those other maximal prime-power divisors of M. Then B is odd and divides both u and v, while q does not divide u or v, and since m divides at least two of u, v and w, we may suppose without loss of generality that $v = mB$ and $u = p^\alpha B$ for some $\alpha \geq 0$.

It follows that $(r, s, t) = (mr', ms', qp^\alpha t')$ for some divisors r', s' and t' of B, while $(u, v, w) = (p^\alpha B, mB, qm)$. Then from $qp^\alpha m^2 r's't' = rst = uvw = qp^\alpha m^2 B^2$ we find that $r's't' = B^2$. Also each of r', s' and t' must be greater than 1, since for example if $r' = 1$ then $s't' = B^2$ and so $s' = t' = B$, but then $s = mB = v$, which is impossible. Moreover, $p^\alpha < m$, for otherwise $t = qp^\alpha t' \geq qm = w$.

Now if $\alpha > 0$, then we can take $(u_1, v_1, w_1) = (B, B, q)$ and $(u_2, v_2, w_2) = (p^\alpha, m, m)$, which have L_2-sets $\{q, B\}$ and $\{m\}$ respectively, and then find primes p_1 and p_2 such that $Q_1 = \mathrm{PSL}(2, p_1)$ and $Q_2 = \mathrm{PSL}(2, p_2)$ are (u_1, v_1, w_1)- and (u_2, v_2, w_2)-generated, but so that Q_1 has no element of order qt', and Q_2 has no element of order $p^\alpha t'$ or $p^\alpha q$. It then follows that $Q_1 \times Q_2$ is (u, v, w)-generated, but has no element of order $qp^\alpha t' = t$ and so cannot be (r, s, t)-generated, a contradiction.

Thus $\alpha = 0$, which gives $u = B$ and $t = qt'$. In particular, $u = B$ is coprime to $qm = w$, and so $\gcd(r, s, t) = \gcd(u, v, w) = 1$. (It also follows that B is divisible by 3, for otherwise Proposition 3.4 applies to u, with r, s and t being divisible by m, m and q, and hence in particular, $q = 2$; but we do not need to know these things.)

Next, consider the maximal prime-power divisors of M that divide B. Every such divisor k is coprime to at least one of r', s' and t', because $1 = \gcd(r,s,t) = \gcd(r',s',t')$, and so must divide exactly two of them. It follows that there exist pairwise coprime odd positive integers f, g and h such that $(r',s',t') = (fg,fh,gh)$, namely $f = \gcd(r',s')$, $g = \gcd(r',t')$ and $h = \gcd(s',t')$, so that $B = fgh$. Moreover, $g > 1$, for otherwise we find that $v = mB = mfgh = mfh = ms' = s$, and similarly $h > 1$. Also $f > 1$, for otherwise $(r,s,t) = (mg,mh,qgh)$ and $(u,v,w) = (gh,mgh,qm)$ and then since at least two of m, g and h are coprime to 3 and hence to 6, we find that Proposition 3.4 applies to r or s or u.

But now it follows that we can take $(r_1,s_1,t_1) = (mf,mf,gh)$ and $(r_2,s_2,t_2) = (g,h,q)$, which have L_2-sets $\{mf,gh\}$ and $\{q,g,h\}$ respectively, and then find primes p_1 and p_2 such that $Q_1 = \mathrm{PSL}(2,p_1)$ and $Q_2 = \mathrm{PSL}(2,p_2)$ are (r_1,s_1,t_1)- and (r_2,s_2,t_2)-generated, but Q_1 has no element of order mfg or mfh, and Q_2 has no element of order mf or gh. Then $Q_1 \times Q_2$ is (r,s,t)-generated, but has no element of order $mfgh = mB = v$ and so cannot be (u,v,w)-generated, a final contradiction.

Remarks: Cases (1) and (2) considered above apply to 535695 and 6507 of the 542695 triple-pairs in the set $\mathcal{T}$ given earlier, leaving just 768 of those triple-pairs to be covered.

For the remaining possibilities, we may suppose that every maximal prime-power divisor k of M divides two or more of r, s and t, and two or more of u, v and w. In particular, every such k is odd, and therefore M is odd, so each of r, s, t, u, v and w is odd.

Now for the moment, assume that $\gcd(r,s,t) = \gcd(u,v,w) = 1$. Then each prime divisor k of r must be coprime to one of s and t, say s, and furthermore, if $m = k^\lambda$ is the maximum power of k dividing M, then m must divide r and t but be coprime to s. The analogous argument works for each of s, t, u, v and w, and hence every one of r, s, t, u, v and w is a product of maximal prime-power divisors of M. Next, let x be the smallest one of r, s, t, u, v and w that is not divisible by 3, and suppose without loss of generality that $x \in \{u,v,w\}$. Then x is coprime to 6, and cannot be a multiple of any of r, s and t, and so each of r, s and t is divisible by some odd prime that does not divide x, but in that case Proposition 3.4 applies to x, a contradiction.

Thus $\gcd(r,s,t) = \gcd(u,v,w) > 1$, and in particular, no two of r, s and t are coprime, and the same holds for u, v and w.

Case (3): Suppose that no maximal prime-power divisor q of $M = \mathrm{lcm}(r,s,t)$ divides just one of r, s and t (or just one of u, v and w), but that some such q divides exactly two of r, s and t, and is coprime to the third.

In this case, q is coprime to $\gcd(r,s,t) = \gcd(u,v,w)$, and hence also q divides two of u, v and w and is coprime to the third. By swapping the triples (r,s,t) and (u,v,w) and/or re-ordering each one if necessary, we may suppose that $\gcd(r,q) = \gcd(u,q) = 1$, so that s, t, v and w are the elements of $\{r,s,t,u,v,w\}$ divisible by q. Also we may suppose also that w is the largest of these.

Now let $m = q$ and $m' = \frac{M}{q}$, and define the triples (r_1,s_1,t_1) and (r_2,s_2,t_2) as follows:

- $s_1 = m$ and $s_2 = \frac{s}{m} = \gcd(s,m')$,

- $t_1 = \frac{t}{m} = \gcd(t, m')$ and $t_2 = m$, and
- $r_1 = \gcd(r, t_1)$ and $r_2 = \gcd(r, s_2)$.

Clearly $s_1 = m > 1$ and $t_2 = m > 1$, and $s = s_1 s_2$ and $t = t_1 t_2$. Also $s_2 = \gcd(s, m') > 1$, for otherwise $s = m$ and then $\gcd(r, s) = 1$, which contradicts the observation made above that $\gcd(r, s, t) > 1$. Similarly $t_1 = \gcd(t, m') > 1$. Thus $s = ms_2 > m$ and $t = mt_1 > m$, and so $s \geq 3m$ and $t \geq 3m$, and it follows that $w > 3m$.

Next, every maximal prime-power divisor of M divides s or t (or both) and hence every maximal prime-power divisor of r divides $\frac{s}{m} = s_2$ or $\frac{t}{m} = t_1$, and so $\mathrm{lcm}(r_1, r_2) = r$. Moreover, $r_1 = \gcd(r, t_1) = \gcd(r, t_1 m) = \gcd(r, t) > 1$, and similarly $r_2 = \gcd(r, s_2) > 1$.

The L_2-set of (r_1, s_1, t_1) is $\{m, t_1\}$ since $r_1 = \gcd(r, t_1)$ divides t_1, which is coprime to m, and similarly, the L_2-set of (r_2, s_2, t_2) is $\{m, s_2\}$.

It follows that there exist primes p_1 and p_2 such that $Q_1 = \mathrm{PSL}(2, p_1)$ and $Q_2 = \mathrm{PSL}(2, p_2)$ are (r_1, s_1, t_1)- and (r_2, s_2, t_2)-generated, but each of Q_1 and Q_2 has no element of order k such that k divides $M = mm'$ and is strictly divisible by m.

In particular, $Q_1 \times Q_2$ is (r, s, t)-generated. But on the other hand, the only orders of elements of $Q_1 \times Q_2$ that are divisors of M and strictly divisible by m are divisors of ms_2 $(= s)$ or $t_1 m$ $(= t)$, or perhaps $3m$, and then because w is greater than $3m$, s and t, it follows that $Q_1 \times Q_2$ has no element of order w, and so $Q_1 \times Q_2$ is not (u, v, w)-generated, a contradiction.

(For example, when $(r, s, t) = (105, 585, 819)$ and $(u, v, w) = (315, 117, 1365)$, with $M = 9 \cdot 5 \cdot 7 \cdot 13$, we can take $m = 13$ and $m' = 315$, and then $(r_1, s_1, t_1) = (21, 13, 63)$ and $(r_2, s_2, t_2) = (15, 45, 13)$, with L_2-sets $\{13, 63\}$ and $\{13, 45\}$, and we can choose p_1 and p_2 so that $Q_1 \times Q_2$ has no element of order $w = 13 \cdot 105$.)

Remarks: This case applies to 766 of the 542695 triple-pairs in our set $\mathcal{T}$, leaving just $768 - 766 = 2$ triple-pairs in $\mathcal{T}$ that need to be covered by case (4). A computation using MAGMA [**1**] shows that in these two cases, there is no direct product of the form $\mathrm{PSL}(2, p_1) \times \mathrm{PSL}(2, p_2)$ that is a smooth quotient of one of $\Delta(r, s, t)$ and $\Delta(u, v, w)$ but not the other, and thereby explains why we need to consider direct products of three quotients for some triple-pairs.

Case (4): Suppose that every maximal prime-power divisor of $M = \mathrm{lcm}(r, s, t)$ divides exactly two of r, s and t but is not coprime to the third (and hence also divides exactly two of u, v and w but is not coprime to the third).

In this case, every prime divisor of M divides all six of r, s, t, u, v and w, and hence divides $d = \gcd(r, s, t) = \gcd(u, v, w) > 1$. On the other hand, none of those six is equal to d, because otherwise case (j) of Proposition 3.5 applies. Also by swapping and/or re-ordering the triples (r, s, t) and (u, v, w), we may suppose that $w = \max(\{r, s, t, u, v, w\})$.

Now let D be the product of all maximal prime-power divisors of M that divide d, let X be the set of all maximal prime-power divisors of M that do not divide d, and let E be their product. Then D divides d, and $M = DE$ with $\gcd(D, E) = 1$. Also every $q \in X$ divides exactly two of r, s and t but does not divide the third, and divides exactly two of u, v and w but does not divide the third. Moreover, no

$q \in X$ can be prime, for otherwise q divides d. Hence every $q \in X$ is of the form p^α for some odd prime p and some $\alpha \geq 2$, and in particular, $3 \notin X$.

Also let X_1 be the set of all $q \in X$ that divide r and s but not t, let X_2 be the set of all $q \in X$ that divide r and t but not s, let X_3 be the set of all $q \in X$ that divide s and t but not r, and let m_1, m_2 and m_3 be the product of the members of X_1, X_2 and X_3, respectively. Then $E = m_1m_2m_3$, with m_1, m_2 and m_3 pairwise coprime, and it is easy to see that $r = \mathrm{lcm}(m_1m_2, d) = m_1m_2r'$ for some r' dividing d, while $s = \mathrm{lcm}(m_1m_3, d) = m_1m_3s'$ for some s' dividing d, and $t = \mathrm{lcm}(m_2m_3, d) = m_2m_3t'$ for some t' dividing d.

Next, let $(r_1, s_1, t_1) = (m_1, m_1, m_3)$, $(r_2, s_2, t_2) = (m_2, m_3, m_2)$ and $(r_3, s_3, t_3) = (d, d, d)$. Then $x_i > 1$ for all $x \in \{r, s, t\}$ and all i, and $\mathrm{lcm}(r_1, r_2, r_3) = \mathrm{lcm}(m_1m_2, d) = r$, and $\mathrm{lcm}(s_1, s_2, s_3) = \mathrm{lcm}(m_1m_3, d) = s$, and $\mathrm{lcm}(t_1, t_2, t_3) = \mathrm{lcm}(m_2m_3, d) = t$.

The L_2-sets of (r_1, s_1, t_1) and (r_2, s_2, t_2) are $\{m_1, m_3\}$ and $\{m_2, m_3\}$, and it follows that there exist primes p_1 and p_2 such that $Q_1 = \mathrm{PSL}(2, p_1)$ and $Q_2 = \mathrm{PSL}(2, p_2)$ are (r_1, s_1, t_1)- and (r_2, s_2, t_2)-generated respectively, but Q_1 has no element of order k where k divides E but does not divide m_1 or m_3, and Q_2 has no element of order k where k divides E but does not divide m_2 or m_3. Then since $3 \notin X$, it follows that if $Q_1 \times Q_2$ has an element of order k where k is a product of members of X, then k divides m_1m_2, m_1m_3 or m_3m_2.

Now $Q_1 \times Q_2$ is (m_1m_2, m_1m_3, m_2m_3)-generated, and hence if $A = C_d$, which is (d, d, d)-generated, then also $Q_1 \times Q_2 \times A$ is (r, s, t)-generated.

On the other hand, $w = mw' = \mathrm{lcm}(m, d)$ for some product m of members of X and some divisor w' of d, and as $\frac{w}{d} > \frac{x}{d}$ for all $x \in \{r, s, t\}$, we know that m cannot divide any of m_1m_2, m_1m_3 and m_3m_2, and it follows that $Q_1 \times Q_2$ has no element of order m.

Thus $Q_1 \times Q_2 \times A$ has no element of order $\mathrm{lcm}(m, d) = w$, and hence $Q_1 \times Q_2 \times A$ cannot be (u, v, w)-generated, a final contradiction.

(Examples include the two triple-pairs $\{(28665, 266175, 621075), (47775, 53235, 1863225)\}$ and $\{(47775, 266175, 372645), (53235, 143325, 621075)\}$, not covered by cases (1) and (2), with $d = \gcd(r, s, t) = 1365 = 3 \cdot 5 \cdot 7 \cdot 13$ and $D = 1$ and $M = \mathrm{lcm}(r, s, t) = 3^3\, 5^2\, 7^2\, 13^2$ for both, and $(m_1, m_2, m_3) = (3^2, 7^2, 65^2)$ and $(5^2, 7^2, 39^2)$ respectively.)

This case completes the first new proof. □

5. The Second New Proof, using Divisor Triples

Again here we may suppose that (r, s, t) and (u, v, w) are non-exceptional hyperbolic triples for which $\Gamma = \Delta(r, s, t)$ and $\Sigma = \Delta(u, v, w)$ have exactly the same finite quotients, and hence satisfy the conclusions of Lemma 3.3, but not the principal hypothesis of Proposition 3.4, and do not satisfy any of the sufficient conditions (b) to (f) given in Proposition 3.5.

In particular, no element of one of the triples can be coprime to each of the other two, and it follows that the L_2-sets of the triples (r, s, t) and (u, v, w) are both equal to $\{M\}$, where $M = \mathrm{lcm}(r, s, t) = \mathrm{lcm}(u, v, w)$.

The approach we take is to show that for some triple (k, l, m), consisting of respective divisors of either r, s and t, or u, v and w, there exists a (k, l, m)-generated group Q that is a quotient of one of just one of Γ and Σ, which contradicts Lemma 3.2.

Just as in the first new proof, the choice of triple (k,l,m) depends on the distribution of the maximal prime-power divisors of M among the divisors of r, s, t, u, v and w. The group Q in each case is an extension of an abelian normal subgroup $N \cong C_n^{2g}$ by $G = \mathrm{PSL}(2,h)$, where $n > 1$ and h is a carefully chosen prime, and $2-2g = |G|\left(\frac{1}{k}+\frac{1}{l}+\frac{1}{m}-1\right)$ as described shortly after Theorem 2.2 in Section 2.

We proceed by considering two possibilities, each of which is a combination of two of the cases from the first new proof. Credit should go to Frankie Chan for the choice of (k,l,m) in the second possibility, even though it now seems obvious with the benefit of hindsight! Also the approach for both possibilities further underlines the value of the Macbeath trick.

Cases (1) and (2): Suppose that some maximal prime-power divisor of $M = \mathrm{lcm}(r,s,t)$ divides just one of r, s and t, and also so divides just one of u, v and w.

Let $q = p^\gamma$ be the smallest such maximal prime-power divisor of M, and also suppose without loss of generality that q divides t and w, and that $t < w$.

Now take $(k,l,m) = (u,v,\frac{w}{p})$. Then by our choice of $q = p^\gamma$ and the assumption that w is not coprime to both u and v, it follows that $\frac{w}{p}$ is not coprime to both u and v, and hence the L_2-set of (k,l,m) is $\{\frac{M}{p}\}$, where $\frac{M}{p}$ is not divisible by q.

Next, let h be an odd prime such that $\frac{h-1}{2}$ or $\frac{h+1}{2}$ is divisible by $\frac{M}{p}$, but not by q, and hence not by w or M. Then $G = \mathrm{PSL}(2,h)$ is a smooth quotient of the triangle group $\Delta(u,v,\frac{w}{p})$, and accordingly, so is an extension Q_n of C_n^{2g} by G for any positive integer n, where $2-2g = |G|\left(\frac{1}{u}+\frac{1}{v}+\frac{p}{w}-1\right)$. In particular, every such Q_n is a quotient of $\Sigma = \Delta(u,v,w)$, but has no element of order q (or w).

On the other hand, G is also a quotient of $\Gamma = \Delta(r,s,t)$, but we can show that Q_n is not, for every $n > 1$. For suppose the contrary. Then $G = \mathrm{PSL}(2,h)$ is (k,l,m)-generated for some divisors k, l and m of r, s and t, respectively, and then for any such triple (k,l,m), the third entry m must divide $\frac{t}{p}$ because G has no element of order q. Hence the largest conceivable value of f for which an extension of C_n^{2f} by G is a smooth quotient of $\Delta(k,l,m)$ is given by $2-2f = |G|\left(\frac{1}{r}+\frac{1}{s}+\frac{p}{t}-1\right)$. But now since $\frac{1}{r}+\frac{1}{s}+\frac{1}{t} = \frac{1}{u}+\frac{1}{v}+\frac{1}{w}$ and $t < w$, it follows that $2g-2f = (2-2f)-(2-2g) = |G|\left(\frac{p}{t}-\frac{1}{t}-\frac{p}{w}+\frac{1}{w}\right) = |G|(p-1)(\frac{1}{t}-\frac{1}{w}) > 0$, so $f < g$. Thus Q_n cannot be a smooth quotient of $\Delta(k,l,m)$, and hence cannot be a quotient of $\Delta(r,s,t)$, a contradiction.

Cases (3) and (4): Suppose that no maximal prime-power divisor of $M = \mathrm{lcm}(r,s,t)$ divides just one of r, s and t (or just one of u, v and w).

In this case, every maximal prime-power divisor of M divides two or all three of r, s and t, and at least one of them divides exactly two of r, s and t, since by assumption no entry of (r,s,t) is equal to $\gcd(r,s,t)$. The analogous properties hold also for the triple (u,v,w). Moreover, by the remarks following cases (1) and (2) in our first proof, we can suppose that $\gcd(r,s,t) = \gcd(u,v,w) > 1$.

So let $q = p^\gamma$ be the smallest maximal prime-power divisor of M that divides exactly two of r, s and t, and suppose without loss of generality that q divides s, t, v and w, and $r < u$.

Now let $(k,l,m) = (r,\frac{s}{p},\frac{t}{p})$. Then by our choice of $q = p^\gamma$ and because $\gcd(r,s,t) > 1$, we find that the L_2-set of (k,l,m) is $\{\frac{M}{p}\}$ once more, and that $\frac{M}{p}$ is not divisible by q.

Again let h be an odd prime such that $\frac{h-1}{2}$ or $\frac{h+1}{2}$ is divisible by $\frac{M}{p}$, but not by q, and hence not by v or w or M. Then $G = \mathrm{PSL}(2,h)$ is a smooth quotient of the triangle group $\Delta(r, \frac{s}{p}, \frac{t}{p})$, and accordingly, so is an extension Q_n of C_n^{2g} by G for any positive integer n, where this time $2-2g = |G|\left(\frac{1}{r}+\frac{p}{s}+\frac{p}{t}-1\right)$. In particular, every such Q_n is a quotient of $\Sigma = \Delta(r,s,t)$, but has no element of order q (or s or t).

On the other hand, G is also a quotient of $\Gamma = \Delta(u,v,w)$, but we can show that Q_n is not, for every $n > 1$. For otherwise $G = \mathrm{PSL}(2,h)$ is (k,l,m)-generated for some divisors k, l and m of u, v and w, respectively, and then for any such triple (k,l,m), the second and third entries must divide $\frac{v}{p}$ and $\frac{w}{p}$, as G has no element of order q. Hence the largest conceivable value of f for which an extension of C_n^{2f} by G is a smooth quotient of $\Delta(k,l,m)$ is given by $2-2f = |G|\left(\frac{1}{u}+\frac{p}{v}+\frac{p}{w}-1\right)$. But now since $\frac{p}{r}+\frac{p}{s}+\frac{p}{t} = \frac{p}{u}+\frac{p}{v}+\frac{p}{w}$ and $r < u$, it follows that $2g-2f = (2-2f)-(2-2g) = |G|\left(\frac{1}{u}-\frac{p}{u}-\frac{1}{r}+\frac{p}{r}\right) = |G|(p-1)(\frac{1}{r}-\frac{1}{u}) > 0$, so $f < g$. Thus Q_n cannot be a smooth quotient of $\Delta(k,l,m)$, and hence cannot be a quotient of $\Delta(u,v,w)$, a contradiction.

This completes the shorter proof. □

Acknowledgements

The author is grateful to the N.Z. Marsden Fund (via grant UOA2030) for supporting research that helped produce this paper, and also acknowledges the help of the Magma system [**1**] in investigating examples and testing conjectures.

References

[1] W. Bosma, J. Cannon and C. Playoust, *The* Magma *Algebra System I: The User Language*, J. Symbolic Computation **24** (1997), 235–265.

[2] M.R. Bridson, M.D.E. Conder and A.W. Reid, *Determining Fuchsian groups by their finite quotients*, Israel J. Math. 214 (2016), 1–41.

[3] F. Chan, *Finite Quotients of Triangle Groups*, PhD Thesis, Purdue University, August 2021.

[4] H.S.M. Coxeter and W.O.J. Moser, *Generators and Relations for Discrete Groups*, 4th ed., Springer, Berlin (1980).

[5] M. Larsen, A. Lubotzky and C. Marion, *Deformation theory and finite simple quotients of triangle groups I*, J. Eur. Math. Soc. (JEMS) 16 (2014), 1349–1375.

[6] A.M. Macbeath, *Generators of the fractional linear groups*, Proc. Sympos. Pure Math. **XII**, Amer. Math. Soc., (1969), 14–32.

[7] M. Suzuki, *Group Theory I*, Grundlehren der mathematischen Wissen. **247**, Springer-Verlag, (1982).

Department of Mathematics
University of Auckland
Private Bag 92019 Auckland
New Zealand
m.conder@auckland.ac.nz