

Well, this is precisely what a computer algebra system is supposed to do. The way is based on the observation that all computations really take place in a finite extension of the prime field. Now, there is a little lemma to be proved that says you can always do this extension in two steps:

- (a) Pass to a purely transcendental extension. This field obviously has a computationally effective arithmetic.
- (b) Move on to an algebraic extension of finite degree – this can be done since finitely generated algebraic extensions are finite. Those extensions can be represented as matrix algebras over their base field. Hence they, too, are computationally effective.

These considerations have two consequences:

Theorem 3.38. *A finitely generated linear group has a solvable word problem.* **q.e.d.**

Theorem 3.39 (Mal'cev). *A finitely generated linear group has a faithful representation over a pure transcendental extension of the prime field.*

Proof. There is only a finite extension missing. This, however, can be realized as a matrix algebra. **q.e.d.**

This technique is known as “restriction of scalars”.

3.2 Burnside's Problem

Definition 3.40. A group G is periodic if there is a number $N \in \mathbb{N}$ such that for all $g \in G$.

$$g^N = 1.$$

The number N is called the exponent of G .

General Burnside Problem 3.41. *Are there no finitely generated, infinite torsion groups?*

Burnside Problem 3.42. *Are there no finitely generated, infinite periodic groups?*

Restricted Burnside Problem 3.43. *Are there only finitely many finite groups with a given exponent and a given bound on the number of generators?*

The answers are “no”, “no”, and “yes”. Grigorchuk’s Group provides an example for the General Burnside Problem.

Definition 3.44. A general Burnside group is a finitely generated, infinite torsion group.

It is not at all easy to come up with examples of finitely generated, infinite torsion groups since these are subject to rather strong restrictions.

Theorem 3.45. *Finitely generated, virtually solvable torsion groups are finite.*

Proof. Let us ignore the word “virtually” for a while. First observe that finitely generated abelian torsion groups are finite. Being abelian is the same as being step-1-solvable. Of course, we proceed by induction.

Let $N \hookrightarrow G \twoheadrightarrow Q$ be a short exact sequence with Q abelian, N step- s -solvable, and G finitely generated and torsion. It follows that Q is finitely generated and torsion and, therefore, finite. Hence N has finite index and is finitely generated, too. As a subgroup of G , it is clearly torsion. By induction, N is finite. Hence G is finite-by-finite whence finite. This completes the induction.

Now, we know that finitely generated solvable torsion groups are finite. So suppose G is torsion, finitely generated, and

virtually solvable. Then the solvable subgroup of finite index is finitely generated and torsion. Hence it is finite. But if G has a finite subgroup of finite index, G is finite. **q.e.d.**

Corollary 3.46. *A general Burnside group does not satisfy the Tits alternative, i.e., it neither contains a non-abelian free group, nor is it virtually solvable.*

Proof. Since a torsion free group cannot contain a non-abelian free subgroup, we are reduced to the virtually solvable case. **q.e.d.**

Corollary 3.47 (Burnside-Schur-Kaplanski). *Finitely generated linear torsion groups are finite.*

Remark 3.48. Of course, this is sort of a a mock proof of the Burnside-Schur-Kaplanski theorem: Tits' proof that linear groups satisfy the Tits alternative uses results from representation theory that come close to give the Burnside-Schur-Kaplanski result directly.

Theorem 3.49. *The First Grigorchuk group \mathcal{G}_1 is a general Burnside group. In particular it is neither linear nor virtually solvable.*

As \mathcal{G}_1 is finitely generated by construction, we have to prove that it is infinite [3.51] and torsion [3.52].

Lemma 3.50. *Let $\mathcal{G}_1(1) := \ker(\mathcal{G}_1 \rightarrow \text{Aut}(T_2^\bullet(1)))$ be the stabilizer of the level 1 subtree. The inclusion*

$$\mathcal{G}_1(1) \hookrightarrow \text{Aut}(T_2^\bullet) \times \text{Aut}(T_2^\bullet)$$

induces an inclusion

$$\mathcal{G}_1(1) \hookrightarrow \mathcal{G}_1 \times \mathcal{G}_1$$

which is "surjective in each coordinate", i.e., for each element $\xi_0 \in \mathcal{G}_1$ there is an element $\xi_1 \in \mathcal{G}_1$ such that $(\xi_0, \xi_1) \in \mathcal{G}_1(1)$.

Proof. $\mathcal{G}_1(1)$ contains (in fact it is generated by) the elements

$$(\sigma, \beta), (\sigma, \gamma), (\sigma, \delta), (\beta, \sigma), (\gamma, \sigma), (\delta, \sigma)$$

and therefore surjects onto \mathcal{G}_1 , e.g., by projection onto the first coordinate. **q.e.d.**

Corollary 3.51. \mathcal{G}_1 is infinite.

Proof. $\mathcal{G}_1(1)$ is a proper subgroup of \mathcal{G}_1 . However, a finite group cannot have a proper subgroup that surjects onto the bigger group. **q.e.d.**

Proposition 3.52. \mathcal{G}_1 is a 2-group, i.e., every element has finite order which is a power of 2.

Proof. This is done by induction on a “complexity”, a refined version of word length. First observe that, since all generators of \mathcal{G}_1 are involutions, we can represent each element as a word in the generators without using inverses. Moreover, (3.4) implies that we can use word in which the swap alternates with the other generators. Finally, since the order of an element is unaffected by conjugation, we may assume that the word length is ≤ 1 or even. Let us call those words cyclicly reduced.

For each cyclicly reduced word w let $C_\sigma(w)$ denote the number of occurrences of σ in w . Define C_β , C_γ , and C_δ analogously. The complexity of w to be the tuple

$$C(w) := [C_\sigma(w); C_\beta(w), C_\gamma(w), C_\delta(w)].$$

We order complexities lexicographically. Note that for cyclicly reduced words the σ -count closely reflects the length of the word. And for $C_\sigma(w) \geq 1$, we have $C_\sigma(w) = C_\beta(w) + C_\gamma(w) + C_\delta(w)$ unless $w = \sigma$.

The induction starts with

$$C(w) \in \{[0; 0, 0, 1], [0; 0, 1, 0], [0; 1, 0, 0], [1; 0, 0, 0]\}.$$

These cases correspond to the generators which are involutions.

Now assume that w has a higher complexity. We distinguish two cases:

$C_\sigma(w)$ is even: Then $w = (w_1, w_2)$ for two word whose σ -count is at most $\frac{C_\sigma(w)}{2}$. Hence induction applies.

$C_\sigma(w)$ is odd: Now we will consider w^2 . This word has an even σ -count whence we have

$$w^2 = (w_1, w_2)$$

and our aim is to show that w_1 and w_2 have a smaller complexity than w .

We have subcases:

$C_\delta(w) > 0$: In this case, $C_\sigma(w_i) < C_\sigma(w)$. The reason is $\delta = (1, \beta)$ and $\sigma\delta\sigma = (\beta, 1)$. The 1-components do the shortening.

$C_\delta(w) = 0$: In this case, no cancellations occur. The word w_i will be cyclicly reduced right away, and we can track where the letters come from. It transpires that β -letters in w give rise to γ -letters in the w_i and γ -letters in w will provide δ -letters in the w_i . Hence, we have

$$C(w_i) = [C_\sigma(w); 0, C_\beta(w), C_\gamma(w)] < [C_\sigma(w); C_\beta(w), C_\gamma(w), 0].$$

This completes the induction.

q.e.d.

Remark 3.53. Let us explicitly write out the low complexity cases:

- $\sigma\delta$ has order 4. Hence $\langle \sigma, \delta \rangle$ is a dihedral group of order 8.
- $\sigma\gamma$ has order 8. Hence $\langle \sigma, \gamma \rangle$ is a dihedral group of order 16.
- $\sigma\beta$ has order 16. Hence $\langle \sigma, \beta \rangle$ is a dihedral group of order 32.

3.3 Subgroup Structure

Definition 3.54. Let us define the following elements:

$$t := \sigma\beta\sigma\beta = (\gamma\sigma, \sigma\gamma)$$

$$v := (\beta\sigma\delta\sigma)^2 = (t, 1)$$

$$w := (\sigma\beta\sigma\delta)^2 = (1, t)$$

Darn Technical Computation 3.55. We have the following conjugacy identities:

$$\begin{array}{lll} \beta t \beta = \sigma \beta \sigma \beta = t^{-1} & \beta w \beta = t^{-1} \delta t \delta = t^{-1} w^{-1} t & \beta v \beta = v^{-1} \\ \sigma t \sigma = t^{-1} & \sigma w \sigma = w & \sigma v \sigma = w \\ \delta t \delta = w^{-1} t & \delta w \delta = w^{-1} & \delta v \delta = \beta \sigma \delta \sigma \delta \beta \delta \sigma \delta \sigma = v. \end{array}$$

In the last identity, we used $\sigma\delta\sigma\delta = \delta\sigma\delta\sigma$.

In particular, $\langle t, v, w \rangle$ is normal in \mathcal{G}_1 .

Moreover, we have

$$\beta\beta\beta = \beta$$

$$\sigma\beta\sigma = t\beta$$

$$\delta\beta\delta = \beta$$

In particular $\langle \beta, t, v, w \rangle$ is normal in \mathcal{G}_1 .

Definition 3.56. We put

$$B := \langle \beta, t, v, w \rangle$$

$$K := \langle t, v, w \rangle$$

Lemma 3.57. Let $\pi_s : \mathcal{G}_1 \rightarrow \text{Aut}(T_2^\bullet(s))$ be the canonical projection. Then

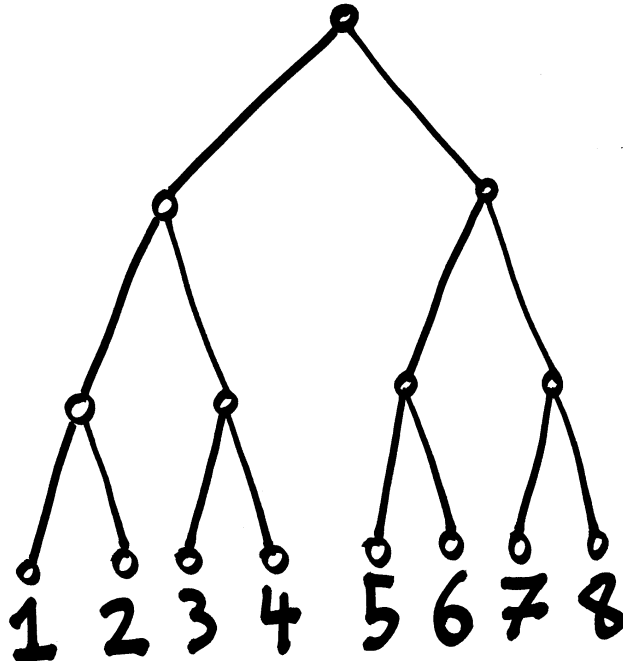
$$|\pi_3(\mathcal{G}_1)| = 128$$

$$|\pi_3(B)| = 16$$

$$|\pi_3(K)| = 8$$

In particular, the index of B in \mathcal{G}_1 is at least 8 and the index of K in B is at least 2.

Proof.



We embed $\text{Aut}(T_2^*(3))$ in $\text{Perm}(1, \dots, 8)$ and compute the images of the generators σ , β , and δ :

$$\sigma \mapsto (1, 5)(2, 6)(3, 7)(4, 8)$$

$$\beta \mapsto (1, 3)(2, 4)(5, 6)$$

$$\delta \mapsto (5, 6)$$

It requires a finite amount of work to check that the image is isomorphic to

$$(C_2 \wr C_2) \wr C_2.$$

The order of this group is 128.

For the elements t , v , and w , we have

$$t \mapsto (1, 4, 2, 3)(5, 7, 6, 8)$$

$$v \mapsto (1, 2)(3, 4)$$

$$w \mapsto (5, 6)(7, 8)$$

Now the amount of work for determining the images of K and B is finite, too.

q.e.d.

Another Technical Computation 3.58. We write v , and w as products of conjugates of t and t^{-1} .

$$\begin{aligned} w &= t\delta t^{-1}\delta \\ v &= \sigma w \sigma \end{aligned}$$

So v and w lie in the normal span of t .

Proposition 3.59. The subgroup B has index 8 in \mathcal{G}_1 and is the normal subgroup generated by β .

Proof. We know that B is normal and therefore contains the normal closure of β . To prove the other inclusion, we observe that t lies clearly in the normal span of β . We already saw (3.58) that u and v lie in the normal closure of t .

Now, we determine the index of B . Since B is normal, this amounts to compute the size of the group \mathcal{G}_1/B . Since β dies in this quotient, δ and γ become equal whence \mathcal{G}_1/B is actually a factor of $\langle \sigma, \delta \rangle$ which has order 8. Hence the index of B is at most 8. We saw in (3.57) that the index is at least 8. **q.e.d.**

Exercise 3.60. Put $D := \langle (\sigma, \delta), (\delta, \sigma) \rangle \leq \mathcal{G}_1 \times \mathcal{G}_1$. Show that the image of $\mathcal{G}_1(1)$ in $\mathcal{G}_1 \times \mathcal{G}_1$ is

$$(B \times B) \rtimes D$$

where the action is conjugation in each component. Infer that $\mathcal{G}_1(1)$ has index 8 in $\mathcal{G}_1 \times \mathcal{G}_1$.

Proposition 3.61. The subgroup K has index 16 in \mathcal{G}_1 and is the normal closure of t . Moreover, K contains $\mathcal{G}_1(3)$ as a subgroup of index 8.

Proof. It follows from (3.58) that K is the normal closure of t . In (3.57) we saw that its index in B is at least 2. Hence it suffices to show that B/K has order ≤ 2 . This, however, is clear as the quotient is generated by the image of β which has order 2.

It follows that K is actually the preimage of its order 8-image in $\text{Aut}(T_2^*(3))$ which implies that $\mathcal{G}_1(3)$ is a normal subgroup of K of index 8. **q.e.d.**

The subgroup K is very important because this is the fractal part of \mathcal{G}_1 whose self-similarity is at the heart of virtually all theorems about the First Grigorchuk Group.

Proposition 3.62. *$K \times K$ is a subgroup of K of index 4.*

Proof. Of course, we are referring to the inclusion of $\mathcal{G}_1(1) \hookrightarrow \mathcal{G}_1 \times \mathcal{G}_1$ from (3.50). So first, we observe

$$w = \sigma\beta\sigma\delta\sigma\beta\sigma\delta = (\gamma, \sigma)(1, \beta)(\gamma, \sigma)(1, \beta) = (1, t).$$

From this we get $1 \times K \leq K$ as follows: For any $\xi \in \mathcal{G}_1$, there is at least one partner $\zeta \in \mathcal{G}_1$ such that $(\zeta, \xi) \in \mathcal{G}_1(1)$. Hence, we have

$$(\zeta, \xi)(1, t)(\zeta, \xi)^{-1} = (1, \xi t \xi^{-1}) \in K.$$

As conjugation by σ swaps the coordinates, we also have $K \times 1 \leq K$. Hence $K \times K \leq K$.

As for the index, we quote (3.60). We know that K has index 8 in $\mathcal{G}_1(1)$ which has index 8 in $\mathcal{G}_1 \times \mathcal{G}_1$. This accounts for an index of 64. On the other hand, $K \times K$ has index $256 = 16^2$ in $\mathcal{G}_1 \times \mathcal{G}_1$. Hence it is of index 4 in K . **q.e.d.**

Corollary 3.63. *\mathcal{G}_1 does not have polynomial growth.*

Proof. Clearly \mathcal{G}_1 and K have the same growth. On the other hand, K contains an isomorphic copy of itself of infinite index. This contradicts polynomial growth by (1.74). **q.e.d.**

3.3.1 Finite 2-groups

Proposition 3.64. *Let $H \leq K$ be a subgroup. Then K contains an isomorphic copy of $H \wr C_2$.*

Proof. Here is the idea: Since $H \times H \leq K \times K \leq K$ we have a copy of $H \wr C_2$ inside \mathcal{G}_1 , namely

$$(H \times H) \rtimes \langle \sigma \rangle.$$

Unfortunately, $\sigma \notin K$. This is the problem we have to fix.

We need an element in K that acts somewhat like σ . So, note that K contains the following element:

$$\begin{aligned} \tilde{\sigma} &:= t^4 \\ &= (\gamma\sigma, \sigma\gamma)^4 \\ &= ((\sigma\delta, \delta\sigma), (\delta\sigma, \sigma\delta))^2 \\ &= (((\beta, \beta), (\beta, \beta)), ((\beta, \beta), (\beta, \beta))) \\ &= ((((\sigma, \gamma), (\sigma, \gamma)), ((\sigma, \gamma), (\sigma, \gamma))), (((\sigma, \gamma), (\sigma, \gamma)), ((\sigma, \gamma), (\sigma, \gamma)))) \in \mathcal{G}_1(4). \end{aligned}$$

This is an element of order 2 and spans a copy of C_2 .

Now let us work on the subgroup H . Using $K \times K \leq K$, we descend to $K^{32} \leq K$ and find two isomorphic copies of H , namely,

$$H_0 := H \times 1 \times 1 \times \cdots \times 1 \leq K^{32}$$

and

$$H_1 := 1 \times H \times 1 \times \cdots \times 1 \leq K^{32}.$$

These copies commute, hence $H_0H_1 \cong H \times H$. Moreover,

$$\tilde{\sigma}H_0\tilde{\sigma} = H_1.$$

Hence we have

$$H \wr C_2 \cong (H_0H_1) \rtimes \langle \tilde{\sigma} \rangle \leq K$$

as desired. **q.e.d.**

Corollary 3.65. *Every finite 2-group embeds into \mathcal{G}_1 . In particular, \mathcal{G}_1 is not periodic.*

Proof. Every finite 2-group embeds into an iterated wreath product $((C_2 \wr C_2) \wr \cdots \wr C_2) \wr C_2$. This follows by induction from the following two facts:

1. [3.66] Every finite 2-group surjects onto C_2 .
2. [3.67] Every extension G of N by a finite group Q injects into $N \wr Q$. **q.e.d.**

Lemma 3.66. *Let G be a finite 2-group. Then there is a surjective homomorphism $G \twoheadrightarrow C_2$.*

Proof. We have $|G| = 2^N$. Consider the set

$$M := \{S \subset G \mid 2^{N-1} = |S|\}$$

and let G act on it by

$$gS = \{gs \mid s \in S\}.$$

It is obvious that G cannot fix an element of M . An easy induction proves that

$$|M| = \binom{2^N}{2^{N-1}} \equiv 2 \pmod{4}.$$

Since powers of 2 are the only possible sizes for orbits, the congruence shows that one of them has length 2. This induces the desired homomorphism. **q.e.d.**

Lemma 3.67. *Let $N \hookrightarrow G \twoheadrightarrow Q$ be a short exact sequence of groups with Q finite. Then there is an injective homomorphism $G \hookrightarrow N \wr Q$.*

Proof. Choose a set-theoretic section $\sigma: Q \rightarrow G$. It is easy to check that

$$g \mapsto ((\sigma(q) g \sigma(q\bar{g}))_{q \in Q}, \bar{g})$$

defines an injective homomorphism. Here \bar{g} denotes the image of g in the quotient Q . **q.e.d.**

Now, we can prove that \mathcal{G}_1 is not linear without quoting a big theorem.

Proposition 3.68. *A finitely generated linear torsion group G is periodic.*

Proof. Using Mal'cev's observation (3.39), we assume that $G \leq \text{GL}_n(k)$ where k is a purely transcendental extension of its prime field k_0 .

Consider $g \in G \leq \text{GL}_n(k)$ and let $\mu_g(t)$ be its minimal polynomial. We aim to show that only finitely many polynomials arise this way. This will imply the proposition since the order of an endomorphism only depends on its minimal polynomial.

Since g is torsion, we have, say, $g^n = 1$. Since every root of $\mu_g(t)$ is an eigenvalue for g , we find, that roots of $\mu_g(t)$ are roots of unity. Hence these roots are algebraic integers over k_0 . The coefficients of μ_g are elementary symmetric functions of the roots. Since k is a purely transcendental extension of k_0 , these coefficients belong to k_0 . For finite k_0 we are done now.

For $k_0 = \mathbb{Q}$, everything takes place inside \mathbb{C} . Thus, we can talk about absolute values. Roots of unity have absolute value 1. This implies a bound on the absolute values of coefficients of $\mu_g(t)$. On the other hand, these coefficients are integers, as we have seen. Therefore, we have only finitely many numbers from which to chose our coefficients. **q.e.d.**

Corollary 3.69. \mathcal{G}_1 is not linear.

3.3.2 Congruence Subgroups

Put $\mathcal{G}_1(s) := \ker(\mathcal{G}_1 \rightarrow \text{Aut}(T_2^\bullet(s)))$.

Observation 3.70. *Since every non-trivial tree automorphism has to act non-trivially on some finite subtree, we have*

$$\bigcap_{s \geq 1} \mathcal{G}_1(s) = 1.$$