The Higman Embedding Theorem

Reading group on the Boone–Higman Conjecture

Alexis Marchand

February 1, 2024

The goal of these notes is to characterise *recursively presented groups* from a combinatorial group-theoretic perspective. We will do so following Rotman [1, Chapter 13]. As a first step, we will need to construct (semi)groups with unsolvable word problem.

1 From Turing machines to semigroups

Consider a Turing machine $\mathcal{T}$, with alphabet $\mathcal{A} = \{s_j\}_j$, states $\mathcal{Q} = \{q_j\}_j$, blank symbol s_0, halting state q_0 and starting state q_1. The Turing machine $\mathcal{T}$ has instructions of the form

$$q_i s_j s_k q_\ell \quad \text{or} \quad q_i s_j L q_\ell \quad \text{or} \quad q_i s_j R q_\ell.$$

We encode $\mathcal{T}$ in a semigroup $U(\mathcal{T})$, with generators $\mathcal{Q} \cup \mathcal{A} \cup \{q\} \cup \{h\}$, where q and h are abstract symbols not contained in any of the other sets. The semigroup $U(\mathcal{T})$ has the following relations:

- $q_i s_j = q_\ell s_k$ if $\mathcal{T}$ contains an instruction $q_i s_j s_k q_\ell$,
- $q_i s_j s_k = s_j q_\ell s_k$ if $\mathcal{T}$ contains an instruction $q_i s_j R q_\ell$,
- $q_i s_j h = s_j q_\ell s_0 h$ if $\mathcal{T}$ contains an instruction $q_i s_j R q_\ell$,
- $s_k q_i s_j = q_\ell s_k s_j$ if $\mathcal{T}$ contains an instruction $q_i s_j L q_\ell$,
- $h q_i s_j = h q_\ell s_0 s_j$ if $\mathcal{T}$ contains an instruction $q_i s_j L q_\ell$,
- $q_0 s_k = q_0$,
- $s_k q_0 h = q_0 h$,
- $h q_0 h = q$.

An element $h w_1 q_i x w_2 h$ should be interpreted as representing the configuration of $\mathcal{T}$ in the state q_i, with the word $w_1 x w_2$ on the tape, with the head on x, and with h representing an infinite blank word. The relations of $U(\mathcal{T})$ encode the transitions of $\mathcal{T}$.

Hence, the language accepted by $\mathcal{T}$ is characterised in terms of the algebra of the semigroup $U(\mathcal{T})$:

Proposition 1. *Let $\mathcal{T}$ be a Turing machine and $w \in \mathcal{A}^*$. Then $\mathcal{T}$ accepts w if and only if*

$$hq_1wh \overset{U(\mathcal{T})}{=} q.$$

2 (Semi)groups with unsolvable word problem

The formalism of §1 allows one to construct semigroups with certain algorithmic properties, starting from well-chosen Turing machines.

Theorem 2 (Markov–Post '47). *There is a finitely presented semigroup with unsolvable word problem.*

Proof. Pick a Turing machine $\mathcal{T}$ whose set E of accepted words is not recursive — note that E is recursively enumerable since it is recognised by $\mathcal{T}$. If one could solve the word problem for $U(\mathcal{T})$, then by Proposition 1, one could decide whether or not a given word is in E, since $w \in E$ if and only if $hq_1wh = q$ in $U(\mathcal{T})$. Therefore, E would be recursive, which is a contradiction. □

Remark 3. The finitely presented semigroup U constructed in the proof of Theorem 2 has the following properties:

- It is generated by $\mathcal{Q} \cup \mathcal{A} \cup \{q\} \cup \{h\}$,
- Its relators are of the form $\alpha q_j \beta = \gamma q_k \delta$ for some words $\alpha, \beta, \gamma, \delta \in (\mathcal{A} \cup \{h\})^*$,
- There is no decision process to determine, for given words $v, w \in \mathcal{A} \cup \{h\}$ and state $q_i \in \mathcal{Q}$, whether or not $vq_iw = q$ in Γ.

We can now readily construct a group, rather than a semigroup, with unsolvable word problem.

Theorem 4 (Novikov–Boone '55). *There exists a finitely presented group with unsolvable word problem.*

Proof. We start with the semigroup U constructed in the proof of Theorem 2. It has generators $\mathcal{Q} \cup \mathcal{A} \cup \{q\} \cup \{h\}$, and relators $\{\alpha_i q_{j_i} \beta_i = \gamma_i q_{k_i} \delta_i\}_{i \in I}$ (see Remark 3). From this, we construct a group G^{nb}, with generators $\mathcal{Q} \cup \mathcal{A} \cup \{q\} \cup \{h\} \cup \{r_i\}_{i \in I} \cup \{x\} \cup \{t\} \cup \{k\}$, and with the following relators:

- $s_j^{-1} x s_j = x^2$ and $h^{-1} x h = x^2$,
- $s_j^{-1} r_i s_j = x r_i x$,

- $r_i^{-1}\left(\bar{\alpha}_i q_{j_i} \beta_i\right) r_i = \bar{\gamma}_i q_{k_i} \delta_i$,
- $[t, r_i] = [t, x] = [k, r_i] = [k, x] = \left[k, q^{-1} t q\right] = 1$.

Claim. Given words $v, w \in (\mathcal{A} \cup \{h\})^*$, and a state $q_i \in \mathcal{Q}$, consider $\sigma = \bar{v} q_i w$ and $\sigma^* = v q_i w$. Then

$$\left[k, \sigma^{-1} t \sigma\right] \overset{G^{nb}}{=} 1 \Longleftrightarrow \sigma^* \overset{U}{=} q.$$

We omit the proof of the claim — one can prove it most easily by considering Van Kampen diagrams, see Rotman [1, pp. 372-379].

Admitting the claim, it follows that an algorithm solving the word problem for G^{nb} would also be able to decide whether or not a word of the form $v q_i w$ is equal to q in σ^*, contradicting Remark 3. $\square$

Remark 5. The construction of group G^{nb} in the proof of Theorem 4 is really a sequence of HNN-extensions and free products:

- Start from the infinite cyclic group $G_0 = \langle x \rangle$.
- Construct successive HNN-extensions with stable letters $\mathcal{A} \cup \{h\}$ to obtain G_1.
- Take a free product with the free group on $\mathcal{Q} \cup \{q\}$, then take successive HNN-extensions with stable letters $\{r_i\}_{i \in I}$, to obtain G_2.
- Take an HNN-extension with stable letter t to obtain G_3.
- Take an HNN-extension with stable letter k to obtain G^{nb}.

3 The Higman Embedding Theorem

Standing assumption. In a group presentation $\langle S \mid R \rangle$, the generating set S will always be assumed to be finite and every relator $r \in R$ will be assumed to be a positive word over S — this can be achieved for example by replacing S with $S \cup S^{-1}$.

Definition 6. A group Γ is *recursively presented* if one of the following two equivalent conditions holds:

(i) Γ admits a presentation $\Gamma = \langle S \mid R \rangle$, where R is a recursively enumerable subset of S^*.

(ii) Γ admits a finite (symmetric) generating set S for which the set

$$\left\{ w \in S^* \;\middle|\; w \overset{\Gamma}{=} 1 \right\}$$

is recursively enumerable.

The main theorem of these notes is the following:

Theorem 7 (Higman '61)**.** *For a finitely generated group Γ, the following are equivalent:*

(i) Γ *is recursively presented.*

(ii) Γ *embeds in a finitely presented group.*

Proof of Theorem 7. For the implication (ii) $\Rightarrow$ (i), it suffices to note that the property of being recursively presented descends to subgroups (this is clear from characterisation (ii) in Definition 6), and that finitely presented groups are recursively presented.

We now prove (i) $\Rightarrow$ (ii). Let $\langle S \mid R\rangle$ be a presentation of Γ for which the set $R \subseteq S^*$ is recursively enumerable. Let $\mathcal{T}$ be a Turing machine on the alphabet $\mathcal{A} = S$ enumerating R, and let $U(\mathcal{T})$ be the associated semigroup, as described in §1. From the semigroup $U(\mathcal{T})$, construct a finitely presented group $G^{nb}(\mathcal{T})$, with generators $\mathcal{Q} \cup \mathcal{A} \cup \{q\} \cup \{h\} \cup \{r_i\}_{i\in I} \cup \{x\} \cup \{t\} \cup \{k\}$ following the same process as in the proof of the Novikov–Boone Theorem (Theorem 4). The claim in the proof of Theorem 4, together with Proposition 1, tell us that, given a word $w \in \mathcal{A}^*$, if we set $\sigma = h^{-1}q_1wh$ and $\sigma^* = hq_1wh$, then

$$w \in R \Longleftrightarrow \sigma^* \overset{U(\mathcal{T})}{=} q \Longleftrightarrow \left[k, \sigma^{-1}t\sigma\right] \overset{G^{nb}(\mathcal{T})}{=} 1.$$

We modify slightly the successive presentations defined in Remark 5 to simplify the equation $\left[k, \sigma^{-1}t\sigma\right] = 1$:

- G_2 is defined as in Remark 5.
- G_3 is the HNN-extension of G_2 with stable letter t_0, with relations

  $$\left[t_0, \left(q_1^{-1}h\right) r_i \left(q_1^{-1}h\right)^{-1}\right] = \left[t_0, \left(q_1^{-1}h\right) x \left(q_1^{-1}h\right)^{-1}\right] = 1.$$

  Note that this is just another presentation of the group G_3 of Remark 5, with $t_0 = \left(q_1^{-1}h\right) t \left(q_1^{-1}h\right)^{-1}$.
- $G^{nb}(\mathcal{T})$ is the HNN-extension of G_3 with stable letter k_0, with relations

  $$\left[k_0, hr_ih^{-1}\right] = \left[k_0, hxh^{-1}\right] = \left[k_0, \left(hq^{-1}h^{-1}q_1\right) t_0 \left(hq^{-1}h^{-1}q_1\right)^{-1}\right] = 1.$$

  This is again another presentation of $G^{nb}(\mathcal{T})$, with $k_0 = hkh^{-1}$.

Now we have, given $w \in \mathcal{A}^*$,

$$w \in R \Longleftrightarrow \left[k_0, w^{-1}t_0w\right] \overset{G^{nb}(\mathcal{T})}{=} 1. \qquad (*)$$

Take a disjoint copy $\mathcal{A}' = \left\{s'_j\right\}_{j\in J}$ of the alphabet $\mathcal{A} = \{s_j\}_{j\in J}$, and construct the following groups:

- G_4 is the free product $G^{nb}(\mathcal{T}) * \Gamma$, where the generators of Γ are labelled using letters of $\mathcal{A}'$.

- G_5 is the HNN-extension of G_4 with stable letters $\{\tau_j\}_{j\in J}$, with relations

$$[\tau_j, s_k] = [\tau_j, s'_k] = 1 \qquad \text{and} \qquad \tau_j^{-1} k_0 \tau_j = k_0 {s'_j}^{-1}.$$

- G_6 is the HNN-extension of G_5 with stable letter d, with relations

$$[d, k_0] = 1 \qquad \text{and} \qquad d^{-1} s_j \tau_j d = s_j.$$

- G_7 is the HNN-extension of G_6 with stable letter σ, with relations

$$[\sigma, k_0] = [\sigma, s_j] = 1 \qquad \text{and} \qquad \sigma^{-1} t_0 \sigma = t_0 d.$$

Remark 8. The fact that the above constructions are all HNN-extensions requires some justification (one needs to check that there are pairs of isomorphic subgroups inducing each extension). In fact, most of the HNN-extensions arising in the construction (but not the last one) have free edge groups. We do not go into more details here — we refer the reader to [1, pp. 382-388] instead.

It then follows that there are embeddings

$$\Gamma \hookrightarrow G^{nb}(\mathcal{T}) * \Gamma = G_4 \hookrightarrow G_5 \hookrightarrow G_6 \hookrightarrow G_7.$$

It remains to prove the

Claim. The group G_7 is finitely presented.

Proof of the claim. Looking back at the construction of $G_1, \dots, G_7$, we observe that the group $G^{nb}(\mathcal{T})$ is finitely presented (this boils down to the Turing machine $\mathcal{T}$ being given by a finite amount of data only, as for the Novikov–Boone Theorem). The group G_4 is obtained from $G^{nb}(\mathcal{T})$ by adding finitely many generators and the possibly infinite set of relators $R' = \left\{ s'_{j_1} \cdots s'_{j_\ell} \mid s_{j_1} \cdots s_{j_\ell} \in R \right\}$. The groups G_5, G_6, G_7 are obtained from G_4 by adding finitely many generators and relations.

Therefore, the resulting presentation of G_7 has finitely many generators, and its set of relations is $R' \cup \Lambda$ for a finite set Λ. Hence, it suffices to show that each relation in R' is a consequence of relations in Λ.

Pick a relation $w \in R$. Consider the word $w' \in R'$ obtained by replacing each letter s_j in w with s'_j. Our goal is to deduce that $w' = 1$ from the relations in the finite set Λ. Since $w \in R$, ($*$) gives

$$\left[k_0, w^{-1} t_0 w\right] \overset{G_7}{=} 1.$$

Conjugating by σ and using the relations of G_7 yields

$$\left[k_0, w^{-1} \left(t_0 d\right) w\right] = 1.$$

The above two equalities say that $w k_0 w^{-1}$ commutes with t_0 and with $t_0 d$, so it commutes with d.

Recall moreover that the relations of G_6 give $d^{-1}s_j\tau_j d = s_j$, which implies (since the τ_j commute with the s_j) that

$$dwd^{-1} = ww_\tau,$$

where w_τ is the word obtained from w by replacing each letter s_j with τ_j. It follows that

$$w^{-1}dw = w_\tau d.$$

But we have just seen that $\left[wk_0w^{-1}, d\right] = 1$, so $w^{-1}dw = k_0^{-1}\left(w^{-1}dw\right)k_0$, and therefore $w_\tau d = k_0^{-1}\left(w_\tau d\right)k_0$. But k_0 and d commute by the relations of G_6, so we obtain

$$[k_0, w_\tau] = 1. \tag{†}$$

Finally, the relations of G_5 give $k_0^{-1}\tau_j k_0 = \tau_j s'_j$, so that (since the s'_j and τ_j commute)

$$k_0^{-1}w_\tau k_0 = w_\tau w'.$$

Now (†) implies that $w' = 1$ as wanted. □

Remark 9. The proof of the above claim is summarised in the Van Kampen diagram of Figure 1.

We have shown that $\Gamma \hookrightarrow G_7$, and G_7 is finitely presented, which completes the proof. □

References

[1] Joseph J. Rotman, *An introduction to the theory of groups*, Third, Allyn and Bacon, Inc., Boston, MA, 1984. MR745804

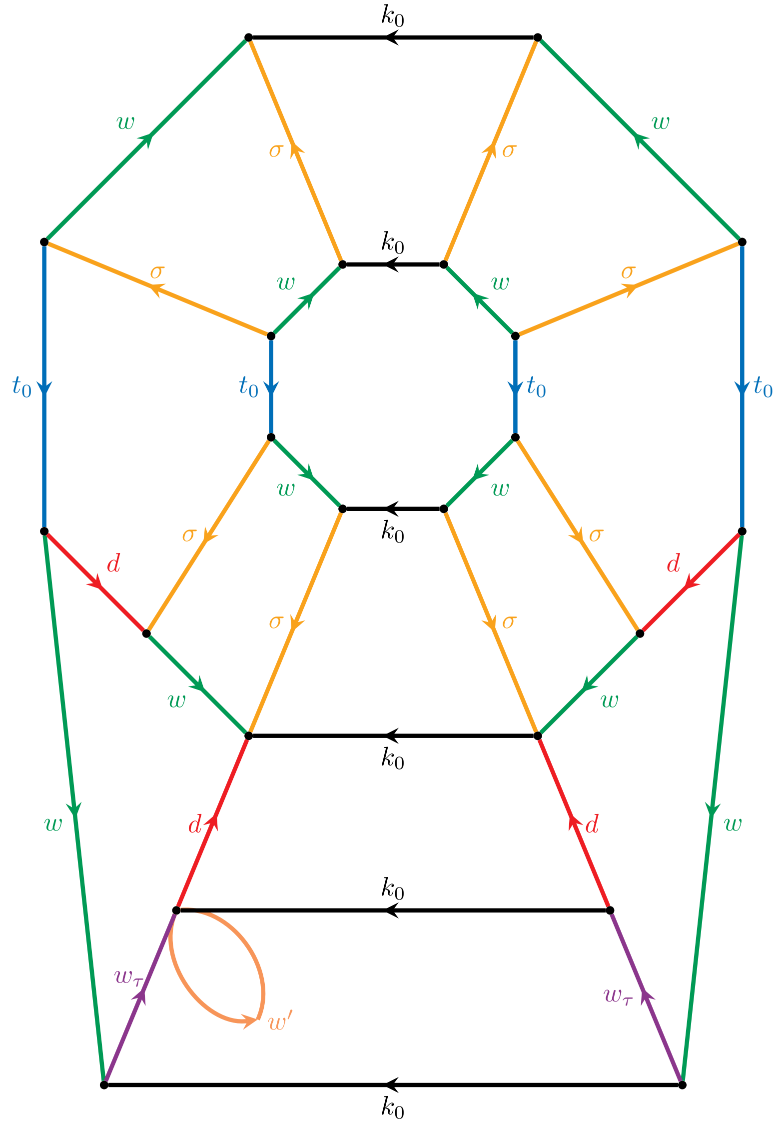

Figure 1: Van Kampen diagram showing that, given a word $w \in R$, the relation $w' = 1$ of G_7 follows from a finite set of relations.