Groupe de Hotz

Langages formels, calculabilité, complexité

Oscar Blumberg

1 Objectif

De même qu'étant donnés deux espaces topologiques il est difficile de dire si ils sont ou non homéomorphes, il est difficile (au sens non décidable) de déterminer l'équivalence de deux grammaires algébriques. L'objectif est, comme en topologie algébrique, d'associer à ces grammaires des invariants qui passent au langage.

Nous allons ici construire un groupe $\mathcal{H}(G)$ associé à une grammaire G tel que, si les grammaires sont réduites :

$$L(G) = L(G') \Rightarrow \mathcal{H}(G) = \mathcal{H}(G')$$

$\mathcal{H}(G)$ nous sera en fait donné sous la forme d'une *présentation de groupe*. Déterminer si deux présentations représentent deux groupes isomorphes est encore un problème en général indécidable. Cependant, des arguments algébriques simples permettent souvent de dire que les deux groupes ne sont pas isomorphes, et donc que les grammaires n'engendrent pas le même langage.

On dispose donc d'un outil qui permet *parfois* de répondre simplement à la question d'équivalence des grammaires.

2 Groupe de Hotz

2.1 Construction

Définition Le groupe libre sur un alphabet A sera noté $F(A)$ et l'inverse de $u \in F(A)$ sera noté $\overline{u}$.

Soit $G = (A, V, P)$ une grammaire, nous allons faire agir G sur $F(A + V)$.

Groupe de Hotz On étends la définition de $\rightarrow_G$ à $F(A+V)$ en rajoutant les productions $\overline{S} \rightarrow \overline{u}$ pour tout $S \rightarrow u \in P$ (i.e. on pose $P = P \cup \overline{P}$). Pour $u, v \in F(A + V)$, on note $u \sim_G v$ la clotûre réflexive transitive de $\rightarrow_G$.

Enfin, on note $\mathcal{H}(G) = F(A + V)/_{\sim_G}$ le groupe de Hotz de G et $[u]_G$ le classe d'équivalence de $u \in F(A + V)$ dans $\mathcal{H}(G)$.

Remarque On est en fait entrain de redefinir une présentation de groupe :

$$\mathcal{H}(G) = < A + V | \{S\overline{u}, S \to u \in P\} >$$

En effet, on identifie ainsi tous les mots de $F(A+V)$ qui sont dans la même orbite sous l'« action » de G. Cela revient à construire le groupe dans lequel seules les relations suivantes, et celles qui en découlent par les proprietées de groupe, sont valables :

$$S = u \text{ pour tout } S \to u \in P$$

D'un point de vue plus algébrique, on quotiente $F(A+V)$ par son plus petit sous groupe distingué contenant $R = \{S\overline{u}, S \to u \in P\}$

2.2 Calcul pratique

En pratique le plus intuitif est de se placer du point de vue des présentations et de reconnaître, idéalement le groupe, ou simplement des caracteristiques algébriques du groupe, à partir des relations auquelles on à le droit.

Exemple Soit $G = (\{a, b\}, \{S\}, \{S \to aSb + \varepsilon\})$. On a $[ab]_G = [S]_G$ et $[S]_G = [\varepsilon]_G$.

$\mathcal{H}(G)$ est donc un groupe à 3 générateurs a, b et S vérifiants les relations suivantes :
- $ab = S$
- $S = 1$

donc, $\mathcal{H}(G)$ est en fait engendré par un unique élément a et $\mathcal{H}(G) =< \{a\}|\emptyset >= F(\{a\}) = \mathbb{Z}$ car les autres relations deviennent intutiles.

Exemple Prenons $G = (A, \{S\}, \{S \to \sum_{x \in A} xSx + \sum_{x \in A} x\})$ qui reconnaît les palindromes non vides sur un alphabet A. Ici toutes les lettres sont égales dans $\mathcal{H}(G)$. Notons a cette classe d'équivalence. On a alors :
- $S = a$
- $S = aSa$

i.e. $a = a^3$. Enfin $\mathcal{H}(G) =< \{a\}, \{a^2\} >= \mathbb{Z}/_{2\mathbb{Z}}$

Exemple Soit $G = (\{a, b\}, \{S, A\}, \{S \to bSb + A, A \to aA + \varepsilon\})$ qui engendre $\{b^p a^q b^p | p, q \geq 0\}$. On a comme relations :
- $S = bSb = A$
- $A = aA = 1$

donc $S = A = a = 1$ et $b^2 = 1$, c'est à nouveau $\mathbb{Z}/_{2\mathbb{Z}}$.

Remarque L'exemple précedent nous montre déjà que la caracterisation n'est pas complète. Autrement dit, la réciproque du théorème n'est pas vraie : il existe en fait une infinité de grammaire engendrant des langages distincts et ayant le même groupe de Hotz.

3 Invariance par changement de grammaire

On va montrer le résultat principal associé au groupe de Hotz : quand G est réduite, $\mathcal{H}(G)$ ne dépends pas de la grammaire G mais uniquement de $L(G)$.

Proposition 3.1 *Soit $G = (A, V, P)$ une grammaire réduite.*

Soit H_L le plus petit sous groupe distingué de $F(A)$ contenant $\{u\overline{v}|u, v \in L\}$.

Soit H_G le plus petit sous groupe distingué de $F(A+V)$ contenant $\{S\overline{u}|S \to u \in P\}$.

On a l'isomorphisme suivant $\mathcal{H}(G) = F(A+V)/_{H_G} \simeq F(A)/_{H_L}$.

Preuve G étant réduite, chaque variable $X \in V$ engendre au moins un élement dans $L_G(X)$ que nous noterons $\varphi(X)$. Posons $\varphi(a) = a$ pour $a \in A$ et prolongeons φ en un morphisme de groupe : $F(A+V) \to F(A)$.

Par projection $p : F(A) \to F(A)/_{H_L}$ on obtient $\tilde{\varphi} = \varphi \circ p : F(A+V) \to F(A)/_{H_L}$. On va en fait montrer que $\ker\tilde{\varphi} = H_G$.

On a bien $H_L \subset (H_G \cap F(A))$. En effet si $u, v \in L$, $S \to_G u$ et $S \to_G v$ donc $S\overline{u} \in H_G$ et $S\overline{v} \in H_G$. Enfin $\overline{S\overline{u}}S\overline{v} = u\overline{v} \in H_G$. Donc une famille génératrice de H_L est dans $(H_G \cap F(A))$. Or φ étant injectif, $\ker\tilde{\varphi} = \varphi^{-1}(H_L) \subset \varphi^{-1}(H_G \cap F(A)) \subset H_G$ car $H_G \cap F(A) \subset \varphi(H_G)$.

Montrons maintenant que $H_G \subset \ker\tilde{\varphi}$. Soit $T \to u \in P$. T étant utile car G est réduite il existe $x, y \in A^*$ tels que $x\varphi(T)y \in L$ et $x\varphi(u)y \in L$. On a alors :

$$\varphi(xTy\overline{xuy}) = (x\varphi(T)y)(\overline{x\varphi(u)y}) \in H_L$$

donc $x\varphi(T)\overline{\varphi(u)}\overline{x} \in H_L$ donc $\varphi(T)\overline{\varphi(u)} = \varphi(T\overline{u}) \in H_L$, ce qui donne finalement :

$$\tilde{\varphi}(T\overline{u}) = \varepsilon$$

donc $\ker\tilde{\varphi} = H_G$.

Par le théorème de factorisation de morphismes on a $F(A+V)/_{\ker\tilde{\varphi}} \simeq F(A)/_{H_L}$ ce qui conclut.

Remarque $F(A)/_{H_L}$ est en fait également une présentation : $< A, \{u\overline{v}|u, v \in L\} >$. On quotiente donc par la relation d'équivalence la plus petite envoyant tous les mots du langage dans la même classe (et compatible avec les lois de groupe).

Ce groupe est appellé le groupe d'effondrement de L.

Le théorème est alors immédiat :

Théorème 3.2 (Hotz) *Si G et G' sont réduites et que $L(G) = L(G')$:*

$$\mathcal{H}(G) \simeq F(A)/_{H_{L(G)}} = F(A)/_{H_{L(G')}} \simeq \mathcal{H}(G')$$

4 Conclusion

Cet outil est très agréable a manipuler puisqu'il permet de simplifier grandement l'étude le grammaire : énormement de simplifications apparaissent rapidement lorsqu'on s'autorise a utiliser les axiomes de groupes.

C'est un phénomène à double tranchants car en pratique, on se retrouve souvent, du moins sur les quelques exemples que j'ai essayés, avec un groupe très simple : un groupe libre (eventuellement d'ordre 0 ou 1) ou parfois un groupe cyclique fini, ce qui permet rarement de conclure. Le groupe de Hotz se comporte peut-être mieux dans le cas de grammaires plus complèxes.