Deciding Conjugacy of a Rational Relation

C.Aiswarya, Amaldev Manuel, Saina Sunny

Chennai Mathematical Institute, IIT Goa

Abstract

A relation over free monoid is conjugate if every pair in the relation is conjugate, or cyclic shift of each other. We show that checking whether a rational relation is conjugate is decidable.

When is a pair of words conjugate?

Two words u and v are conjugate if there exists words x, y such that $u = xy$ and $v = yx$.

$$\begin{pmatrix} listen \\ enlist \end{pmatrix} \qquad \begin{pmatrix} was \\ saw \end{pmatrix}$$

Conjugate Not Conjugate

Another characterization given by Lyndon and Schutzenberger in 1962 is two words are conjugate if and only if there exists a word z such that $uz = zv$. Moreover,

$$z \in (xy)^* x \text{ where } u = xy \text{ and } v = yx$$

When is a Kleene closure of a set conjugate?

A set of pairs G has a *common witness* z if either

$$\forall (u, v) \in G, uz = zv \text{ or } \forall (u, v) \in G, zu = vz$$

Theorem 1 *Let G be an arbitrary set of conjugate pairs of words. The following are equivalent.*

1. *G^* is conjugate.*
2. *G^* has a common witness z.*
3. *G has a common witness z.*
4. *Roots of G has a common witness z.*

$$\left\{\begin{pmatrix} ab \\ ba \end{pmatrix}, \begin{pmatrix} ac \\ ca \end{pmatrix}\right\}^* \qquad \left\{\begin{pmatrix} ab \\ ba \end{pmatrix}, \begin{pmatrix} ca \\ ac \end{pmatrix}\right\}^*$$

Conjugate Not Conjugate

a is a common witness No common witness

When is a sumfree set conjugate?

A *sumfree* set M is an expression that does not use union $(+)$ in the top level, i.e,

$$M = (u_0, v_0) G_1{}^* (u_1, v_1) G_2^* \cdots G_k{}^* (u_k, v_k), k > 0$$

where $G_1, G_2, \ldots, G_k$ are arbitrary sets of pairs.

Theorem 2 *Let M be a sumfree set of the form $(u_0, v_0) G^* (u_1, v_1)$. The following are equivalent.*

1. *M is conjugate.*
2. *$G \cup \{(u_1 u_0, v_1 v_0)\}$ has a common witness z.*
3. *M has a common witness z_m which is obtained by word equation involving z, u_0, u_1, v_0, v_1.*

$$\begin{pmatrix} b \\ a \end{pmatrix} \left\{\begin{pmatrix} ac \\ ca \end{pmatrix}\right\}^* \begin{pmatrix} ab \\ bb \end{pmatrix} \text{ has a common witness } b = u_0 z v_0^{-1} = baa^{-1}$$

where

$$\left\{\begin{pmatrix} ac \\ ca \end{pmatrix}, \begin{pmatrix} abb \\ bba \end{pmatrix}\right\} \text{ has a common witness } z = a$$

Theorem 3 *Let M be a sumfree set. The following are equivalent.*

1. *M is conjugate.*
2. *Each singleton redux of M (where all but one Kleene star is substituted with (ϵ, ϵ)) has a common witness z.*
3. *M has a common witness z.*

$$\begin{pmatrix} b \\ a \end{pmatrix} \left\{\begin{pmatrix} ac \\ ca \end{pmatrix}\right\}^* \begin{pmatrix} ab \\ b \end{pmatrix} \left\{\begin{pmatrix} bab \\ bab \end{pmatrix}\right\}^* \begin{pmatrix} \epsilon \\ b \end{pmatrix} \text{ has a common witness } b$$

which lies in the intersection of the common witnesses of the singleton reduces

$$\begin{pmatrix} b \\ a \end{pmatrix} \left\{\begin{pmatrix} ac \\ ca \end{pmatrix}\right\}^* \begin{pmatrix} ab \\ bb \end{pmatrix} \text{ and } \begin{pmatrix} bab \\ ab \end{pmatrix} \left\{\begin{pmatrix} bab \\ bab \end{pmatrix}\right\}^* \begin{pmatrix} \epsilon \\ b \end{pmatrix}$$

Algorithm

1. Every rational relation can be expressed as a rational expression (E) over pairs of words.
   $((a, aa) + (b, b))^*$ represents $\{(u, v) \mid v \text{ is obtained from } u \text{ by duplicating } a\text{'s}\}$.
2. The union operation preserves conjugacy while, product and Kleene star do not.
   $$E_1 = \begin{pmatrix} ab \\ ba \end{pmatrix}, E_2 = \begin{pmatrix} ca \\ ac \end{pmatrix}$$
   $E_1 + E_2$ is conjugate, while $E_1 \cdot E_2$ as well as $(E_1 + E_2)^*$ are not.
3. Every rational expression is equivalent to a sum of sumfree expressions $E \equiv e_1 + e_2 + \cdots + e_k, k \geq 1$ where each e_i is a sumfree expression.
   $$E_1 + E_2 \equiv (e + \cdots + f) + (g + \cdots + h)$$
   $$E_1^* \equiv (e + \cdots + f)^* \equiv (e^* \cdots f^*)^*$$
   $$E_1 \cdot E_2 \equiv (e + \cdots + f) \cdot (g + \cdots + h) \equiv e \cdot g + \cdots + f \cdot h$$
   (Exponential blow up both in number of summands and size of individual summands)
4. E is conjugate if each sumfree expressions are conjugate.
5. Check the conjugacy of each sumfree expression.
   (a) Each sumfree expression is of the form $(u_0, v_0) e_1^* (u_1, v_1) e_2^* \cdots e_k^* (u_k, v_k), k \geq 0$
   (b) A sumfree expression is conjugate iff it has a common witness.
6. Computing a witness of a given sumfree expression, if one exists, can be done in polynomial time. However, converting a rational expression into a sum of sumfree expressions may result in an exponential blow-up. Thus, the algorithm is of exponential time.

Common Witness Computation

Given a sumfree expression M, we compute its witness set bottom up.

1. Start from the innermost Kleene star – check conjugacy of a pair of word
2. Given the witness set of each Kleene star in M, we can compute the witness set of M in time $\mathcal{O}(m \cdot (m + n)^2)$ where m is the size of the expression and n is the maximum size among the given witnesses.
3. M is not conjugate if there is no common witness at any level of Kleene star.

Complexity: The length of a witness of a sumfree expression is bounded by the length of the expression. Thus, the common witnesses of a sumfree expression can be computed in $\mathcal{O}(h \cdot m^3)$ where h is a star height of the expression and m is the length of the expression.

Applications

Below properties of word transducers amounts to checking conjugacy of rational relations

1. sequentiality — can the given transducer be determinised? (Choffrut 1977)
2. finite sequentiality — is the given transducer equivalent to a disjoint union of deterministic transducers? (Choffrut-Schutzenberger 1986, Jecker-Filiot 2018)
3. bounded edit-distance — is the edit-distance between the respective outputs of the given tranducers bounded? (Aiswarya-Manuel-S. 2024)

Future Work

1. Existence of an automata-theoretic proof.
2. It remains to find the precise complexity of this problem.
3. Conjugacy problem of more general classes — regular functions, polyregular functions.
4. Conjugacy problem over free groups.

References

[1] Christian Choffrut. "Une Caracterisation des Fonctions Sequentielles et des Fonctions Sous-Sequentielles en tant que Relations Rationnelles". In: *Theor. Comput. Sci.* 5.3 (1977), pp. 325–337.
[2] Christian Choffrut and Marcel Paul Schützenberger. "Décomposition de Fonctions Rationnelles". In: *STACS 86*. Vol. 210. LNCS. Springer, 1986, pp. 213–226.
[3] Ismaël Jecker and Emmanuel Filiot. "Multi-Sequential Word Relations". In: *Int. J. Found. Comput. Sci.* 29.2 (2018), pp. 271–296.
[4] C. Aiswarya, Amaldev Manuel, and Saina Sunny. "Edit Distance of Finite State Transducers". In: *ICALP 2024*. Vol. 297. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024, 125:1–125:20.
[5] Roger C Lyndon, Marcel-Paul Schützenberger, et al. "The equation aM= bN cP in a free group". In: *Michigan Math. J* 9.4 (1962), pp. 289–298.