Deciding Conjugacy of a Rational Relation

(extended abstract)

C. Aiswarya[1,2][0000−0002−4878−7581], Amaldev Manuel[3][0000−0002−4953−7920]⋆, and Saina Sunny[3][0009−0005−1366−0168]

[1] Chennai Mathematical Institute, India
[2] CNRS, ReLaX, IRL 2000, India
[3] Indian Institute of Technology Goa, India

Abstract. A relation on the free monoid is conjugate if each pair of words in the relation is conjugate, i.e., cyclic shifts of each other. We show that checking whether a rational relation is conjugate is decidable. This extended abstract outlines the proof of this fact. A result of independent interest is a generalisation of the classical Lyndon-Schützenberger theorem from word combinatorics that equates conjugacy of a pair of words (u, v) and the existence of a word z (called a *witness*) such that $uz = zv$.

A full version of the paper, with details of the proof, can be found on arXiv [1].

Keywords: Rational relations · Finite state transducers · Conjugacy of words · Combinatorics of words.

1 Conjugacy of a Relation

Conjugacy of two elements u and v in a group can be defined as any of the following equivalent cases:

1. $uz = zv$ for some z,
2. $u = xy$ and $v = yx$ for some x, y.

The conjugacy problem asks if a given pair of elements in a finitely presented group (typically infinite) is conjugate. It along with the word and isomorphism problems constitute the classical triad of decision problems on groups identified by Dehn in 1912 [15]. Dehn's prescient choice turned out to be instrumental not only in mathematics, but also to the theory of semigroups/monoids and automata in computer science. It turns out that the above conditions are equivalent for free monoids as well (i.e., when u, v, z, x, y are taken to be words over some finite alphabet). This is the well-known second theorem of Lyndon-Schützenberger. But unlike in the case of groups where condition (1) is taken to be the definition of conjugacy, in the case of monoids condition (2) is taken as the definition of conjugacy. Hence the statement reads the following way.

⋆ Supported by the DST SERB MATRICS grant for the project *Deciding closeness of finite state transducers* [MTR/2022/000628]

Theorem 1 (Proposition 1.3.4 of [14]). *A pair of nonempty words (u, v) is conjugate iff there exists a word z such that $uz = zv$. Moreover, $z \in (xy)^*x$ where x and y are such that $u = xy$ and $v = yx$.*

The conjugacy problem is solvable in polynomial time over free monoids and free groups. We consider a generalisation of the problem to a finitely-presented possibly infinite set of pairs. Let A be a finite alphabet. A relation $R \subseteq A^* \times A^*$ over the free monoid A^* is conjugate if each pair $(u, v) \in R$ is conjugate. Consider the following decision version: *Given a relation R over A^*, is it conjugate?*. Of particular interest is when R is automata-definable because of motivations detailed later. First, we recall the class of rational relations. The family of *rational subsets* of a monoid M is the smallest class containing $\varnothing$, all singleton subsets of M and closed under union, product and Kleene closure. A natural way to present a rational subset of M is as a rational expression: $\varnothing, m \in M$ are rational expressions, and if E_1, E_2 are rational expressions then $E_1 \cdot E_2$, $E_1 + E_2$, and E_1^* are also rational expressions. A rational relation over A^* is a rational subset of the product monoid $A^* \times A^*$. Coincidentally, rational relations are precisely those that are defined by nondeterministic finite state transducers.

Example 1. The rational expression $E_1 = (\epsilon, a)(ab, ba)^*(a, \epsilon)$ denotes the set of pairs $\{((ab)^n a, a(ba)^n) \mid n \geqslant 0\}$. The expression $E_2 = ((a, aa) + (b, \epsilon))^*$ represents $\{(u, v) \mid v$ is obtained from u by duplicating a's and discarding b's$\}$. The expression E_1 is conjugate, and in fact is a subset of identity relation. However, E_2 is not conjugate.

A strong justification for the above problem comes from the theory of word transducers. Checking a number of properties of word transducers, for instance sequentiality (can the given transducer be determinised?) or finite sequentiality (is the given transducer equivalent to a disjoint union of deterministic transducers?), bounded edit-distance [2] (is the edit-distance between the respective outputs of the given tranducers bounded?) etc. amounts to checking conjugacy of the rational relations defined by the strongly connected components of the transducer and certain specific properties of the underlying acyclic graph of strongly connected components. Loosely speaking, conjugacy of the relations defined by the strongly connected components imply that the loops of the transducer are pumpable. Historically, decidability of these properties were shown by tailor-made procedures, for instance *twinning property* of Choffrut for sequentiality [5], *weak twinning* for finite sequentiality [7,11,13]. However, there is no general procedure to decide conjugacy of rational relations.

Our main result is summarised by the following theorem.

Theorem 2. *Conjugacy of rational relations is decidable.*

The decidability hinges on a couple of crucial definitions. The first is that of a sumfree expression: a rational expression is sumfree if it does not use sum (i.e., $+$). Formally, they can be defined as a hierarchy. Given a class $\mathcal{C}$ of expressions over the monoid M, the *Kleene closure* of $\mathcal{C}$, denoted as $\mathcal{KC}$, is the class of expressions $\mathcal{KC} = \mathcal{C} \cup \{E^* \mid E \in \mathcal{C}\}$. Similarly, the *monoid closure* of $\mathcal{C}$, denoted as $\mathcal{MC}$, is the class of expressions $\mathcal{MC} = \mathcal{C} \cup \{E_1 \cdots E_k \mid E_i \in \mathcal{C}, i \in \{1, \ldots, k\}, k \in \mathbb{N}\}$. The family $\mathcal{F}$ of sumfree expressions is given by: $\mathcal{F}_0 = M \cup \{\varnothing\}$ and $\mathcal{F}_{i+1} = \mathcal{MKF}_i$ for each $i \geqslant 0$, and

$$\mathcal{F} = \bigcup_{i \geqslant 0} \mathcal{F}_i \ .$$

The *star height* of an expression E is the smallest $k \in \mathbb{N}$ such that E belongs to $\mathcal{F}_k$.

Over the free monoid A^*, the set of expressions $\mathcal{F}_0$ is $A^* \cup \{\varnothing\}$ and $\mathcal{KF}_0$ is the set of expressions $\mathcal{F}_0 \cup \{w^* \mid w \in A^*\}$ (for convenience we assume that $\varnothing$ is not used in any other expression other than $\varnothing$ itself). It is not difficult to see that $\mathcal{MKF}_0$ is the set of expressions $\mathcal{KF}_0 \cup \{u_1 v_1^* u_2 v_2^* \cdots u_k v_k^* u_{k+1} \mid u_i, v_i \in A^*, k \in \mathbb{N}\}$.

Every rational expression is effectively equivalent to a sum of sumfree expressions (called sumfree normal form (SNF)), by inductively rewriting the expression using the identities $(a+b)^* = (a^*b^*)^*$ and $(a+b)\cdot(c+d) = ac+ad+bc+bd$. This fact is the rational-expression analogue of the factorisation forest theorem of Simon, a deep result from the theory of finite semigroups [17]. Rewriting a rational expression in SNF may result in an exponential blow-up, both in the number of summands and the size of each summand.

Example 2. For the expression $E = (a + b)^n$ for some $n > 0$, it can be shown that any equivalent expression in SNF will have at least 2^n summands. For $E' = \$(E\#)^* \subseteq \{\$, \#, a, b\}^*$, any equivalent SNF expression will have at least one summand of exponential size, and the expression $E \cdot E'$ in SNF will have exponentially many summands of exponential size.

The union operation of rational relations, unlike the product and Kleene closure, preserves conjugacy, i.e., if R_1 and R_2 are conjugate, then $R_1 \cup R_2$ is also conjugate. Therefore for proving Theorem 2 it suffices to decide the conjugacy of a rational relation given by a sumfree expression.

The second crucial definition is the notion of a common witness of a relation, inherited from Lyndon-Schützenberger's theorem. A *witness* of a conjugate pair (u, v) is a word z such that either $uz = zv$ (*inner witness*) or $zu = vz$ (*outer witness*). A word z is a *common inner (resp. outer) witness* of a relation, if for every pair (u, v) in the relation, z is an inner witness (*resp.* outer witness) of (u, v). By Theorem 1, if a relation has a common witness then it is conjugate. However, the converse is easily shown to be false.

We show that a sumfree rational relation is conjugate if and only if it has a common witness, i.e., either a common inner witness or a common outer witness, (but not necessarily both). This characterisation of conjugacy is a main contribution of our paper. It is in fact a generalisation of the Lyndon-Schützenberger theorem characterising conjugacy of two words.

There are two interesting questions regarding common witnesses:

I. *Is there a common witness for the relation R?*
II. *Given a word z, is it a common witness of R?*

Question II proves to be comparatively more tractable, as it can be reduced to verifying whether the rational relation $R' = \{(uz, zv) \mid (u, v) \in R\}$ (or, $R' = \{(zu, vz) \mid (u, v) \in R\}$) consists of only identical pairs [16]. In fact, the decidability of the twinning property of a transducer is connected to Question II.

Question I, on the other hand, is more difficult *a priori* as we do not have a bound on the size of a possible common witness. We provide a decision procedure for Question I. This is another main contribution of the article. Our characterisation of conjugacy via common witness, together with this procedure, yields an algorithm for deciding conjugacy.

1.1 Related Work

A problem much related is the *Conjugate Post Correspondence problem*: given a finite set of pairs G, does there exist of a pair $(u, v) \in G^*$ such that u and v are conjugate? This problem is shown to be undecidable by reduction to the word problem of a special type of semi-Thue systems [10]. In Section 3, we show that the universal version of this problem — checking if all the pairs in G^* are conjugate — is decidable.

A generalisation of Lyndon-Schützenberger's theorem to infinite sets, though with no comparison to ours, is considered in [4][12], where solutions to the language equation $XZ = ZY$, where X, Y, Z are sets of words, are given for special cases. The general solution is still open.

2 Conjugacy of Sumfree Expressions

We now proceed to solve the conjugacy problem for sumfree expressions. We use pairs of lowercase Greek letters (α, β) with suitable modifications to denote pairs of words over $A^* \times A^*$. Clearly $\varnothing$ and (ϵ, ϵ) are conjugates. For an expression of the form (α, β), it is straightforward to check conjugacy. Thus, the conjugacy problem is decidable for the class of expressions $\mathcal{F}_0$.

To show the decidability of the conjugacy problem for the whole family $\mathcal{F}$, it suffices to show that if the problem is decidable for $\mathcal{F}_i$, $i \geqslant 0$, then it is also decidable for $\mathcal{KF}_i$ and $\mathcal{F}_{i+1} = \mathcal{MKF}_i$. Then by induction on i, the decidability extends to the whole family $\mathcal{F}$.

Assume that conjugacy is decidable for $\mathcal{F}_i$. Assume that $E \in \mathcal{F}_i$. Since $L(E) \subseteq L(E^*)$, if the expression E^* is conjugate then necessarily E is conjugate. Because conjugacy is decidable for $\mathcal{F}_i$, we can check this necessary condition. Therefore, to show the decidability of conjugacy for $\mathcal{KF}_i$, it suffices to show the decidability of the following question.

Question 1 (Conjugacy of Kleene Closures). Given a conjugate sumfree expression E, is E^* conjugate?

Next, assume that the conjugacy is decidable for $\mathcal{KF}_i$. Let

$$E = (\alpha_0, \beta_0) E_1^* (\alpha_1, \beta_1) \cdots E_k^* (\alpha_k, \beta_k)$$

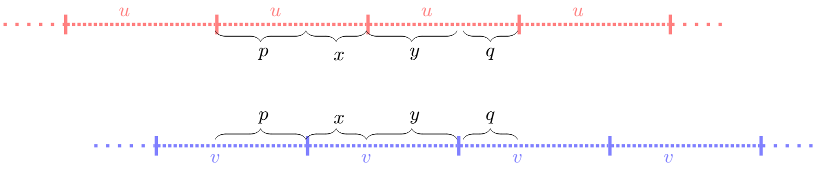

Fig. 1. v as infix of uu.

be an expression in $\mathcal{MKF}_i$ where $E_1^*, \ldots, E_k^*$ are from $\mathcal{KF}_i$. Analogous to the case of Kleene closures, E is conjugate only if $E_1^*, \ldots, E_k^*$ are conjugate, as the next lemma shows.

Lemma 1. *If the expression $E = (\alpha_0, \beta_0)F^*(\alpha_1, \beta_1)$ is conjugate, then F^* is conjugate.*

Proof. If F^* contains only the empty pair, then it is conjugate. Otherwise, assume that (u, v) is a nonempty pair in $L(F^*)$. Therefore, (u^ℓ, v^ℓ) for each $\ell \geqslant 0$ is also in $L(F^*)$. We can safely assume that $|u| = |v|$, otherwise each iteration will increase the difference in length between u^ℓ and v^ℓ, leading to nonconjugacy of E.

Let $k = |\alpha_0| + |\beta_0| + |\alpha_1| + |\beta_1|$. Consider the pair $(\alpha_0, \beta_0)(u^\ell, v^\ell)(\alpha_1, \beta_1)$ where ℓ is some value much larger than k, say 2^k. Since ℓ is much larger than k and $(\alpha_0 u^\ell \alpha_1, \beta_0 v^\ell \beta_1)$ is conjugate, there exist large factors of u^ℓ and v^ℓ that match as shown in Figure 1. Since $|u| = |v|$, we can infer that u is a factor of vv, and v is a factor of uu.

Since v is an infix of uu, the following holds as shown in Figure 1. There exist words x, y, p, and q such that $v = xy$ and $u = px = yq$. Since $|u| = |v|$, the length of p and the length of y are the same, which implies $p = y$ (since $u = px = yq$). Therefore, $u = yx$. Hence u and v are conjugate words. Since the pair (u, v) was arbitrary, F^* is conjugate.

We can generalise the above lemma to the general form of sumfree expressions.

Corollary 1. *If the expression $E = (\alpha_0, \beta_0)E_1^*(\alpha_1, \beta_1) \cdots E_k^*(\alpha_k, \beta_k)$ is conjugate, then each of $E_1^*, E_2^*, \ldots, E_k^*$ is conjugate.*

Since the conjugacy of $\mathcal{KF}_i$ is decidable, we can check whether $E_1^*, \ldots, E_k^*$ are conjugate expressions. Thus, to show the decidability of $\mathcal{MKF}_i$, it suffices to show the decidability of the following question.

Question 2 (Conjugacy of Monoid Closures). Given conjugate sumfree expressions $E_1^*, \ldots, E_k^*$, is the expression $E = (\alpha_0, \beta_0)E_1^*(\alpha_1, \beta_1) \cdots E_k^*(\alpha_k, \beta_k)$ conjugate?

We show that Question 1 and Question 2 can be effectively answered. The idea is to use the notion of common witness that we mentioned in the beginning.

We present two common witness theorems that address the above questions:

1. Let G be an arbitrary set of conjugate pairs. The set G^* is conjugate if and only if G has a common witness (Theorem 3).
2. Let $G_1^*, \ldots, G_k^*$, $k > 0$, be arbitrary sets of conjugate pairs. The set

$$(\alpha_0, \beta_0) G_1^* (\alpha_1, \beta_1) \cdots G_k^* (\alpha_k, \beta_k),$$

called a *sumfree set*, is conjugate if and only if it has a common witness (Theorem 4).

Remark 1. Note that the assumption of conjugacy of the sets $G, G_1^*, \ldots, G_k^*$ is not necessary. However, if they are not conjugate then the corresponding sets will neither have a common witness nor be conjugate, and the statements will be vacuously true.

Item 2 is a generalisation of Item 1, and its proof relies on Item 1. Both theorems are generalisations of the Lyndon-Schützenberger theorem.

In both the theorems above, the common witness for the bigger expression can be computed in polynomial time from those of the subexpressions. When $G, G_1^*, \ldots, G_k^*$ are rational sumfree expressions of pairs, the above theorems are *effective*, that is a common witness, if it exists, is computable in polynomial time in the length of the expression (Section 4). Hence, we have the decidability result — Theorem 2.

3 Common Witness Theorems

In this section, it is shown that an infinite set of pairs generated by a sumfree set is conjugate if and only if a word is witnessing its conjugacy.

3.1 Common Witness and its Characterisations

A word u is *primitive* if it cannot be expressed as a power of any strictly smaller word. For example, aba is primitive, but $abab$ is not. A word ρ is called a *primitive root* of a word u if $u = \rho^n$ for $n \geqslant 1$ and ρ is a primitive word. Every word u has a unique primitive root, denoted by ρ_u ([14], Proposition 1.3.1). We lift the notion of primitive root to a pair and a relation as follows: $R(u, v) = (\rho_u, \rho_v)$, and $R(G) = \{R(u, v) \mid (u, v) \in G\}$. For instance, if $G = \{(abab, baba), (bb, abb)\}$, then $R(G) = \{(ab, ba), (b, abb)\}$.

Recall from Theorem 1 that a pair of words (u, v) is conjugate, then there exists a word z such that $uz = zv$ where $u = xy$, $v = yx$ and $z \in (xy)^*x$. By symmetry of conjugacy, there also exists a word z' such that $z'u = vz'$ where $z' \in (yx)^*y$. We call z (resp. z') in the above characterisation as an *inner witness* (resp. *outer witness*) of the pair (u, v) (since z is appended to the inner ends). Given a conjugate pair (u, v), the set of all inner witnesses of (u, v) is $\{z \mid uz = zv\} = \cup_{\{(x,y) \mid u = xy, v = yx\}} (xy)^* x$. Similarly, the set of all outer witnesses of (u, v) is $\{z \mid zu = vz\} = \cup_{\{(x,y) \mid u = xy, v = yx\}} (yx)^* y$. For example, the pair (aba, baa) has inner witnesses $(aba)^* a$ and outer witnesses $(baa)^* ba$.

There is a connection between a conjugate pair and its primitive root. It is known that if a pair (u, v) is conjugate, then their primitive root (ρ_u, ρ_v) is also conjugate. Moreover, $(u, v) = (\rho_u, \rho_v)^n$ for some $n \geqslant 1$ (Lemma 1 of [6]). In fact, their witnesses are the same.

Proposition 1. *A word z is an inner (resp. outer) witness of a conjugate pair (u, v) iff z is an inner (resp. outer) witness of the primitive root (ρ_u, ρ_v).*

We generalise the notion of a witness of a pair to a set of pairs.

Definition 1 (Common Witness). *A word is a* common inner witness *of a set of pairs P if it is an inner witness of each pair in P. Similarly, a word is a* common outer witness *of P if it is an outer witness of each pair in P.*

A set of pairs has a common witness *if it has either a common inner witness or a common outer witness.*

The structure of a common witness of a set of pairs is obtained from Theorem 1.

Proposition 2. *Let P be a set of pairs of words. The following are equivalent.*

1. *z is a common inner witness of P.*
2. *$z \in \bigcap_{(u,v)\in P} \bigcup_{\{(x,y) \mid u=xy, v=yx\}} (xy)^* x$.*

The statement for common outer witness is analogous.

Example 3. Consider the set $P = \{(ab, ba), (abab, baba)\}$. The pair (ab, ba) has a unique cut (a, b), and the pair $(abab, baba)$ has two cuts: (a, bab) and (aba, b). The word a is a common inner witness of P since a belongs to both $(ab)^*a$ and $(abab)^*a$ (using the first cut). Similarly, aba is also a common inner witness of P since aba belongs to both $(ab)^*a$ and $(abab)^*aba$ (using the second cut). Notice that aba is not in the intersection of $(ab)^*a$ and $(abab)^*a$.

Proposition 1 connecting witness of a conjugate pair and its root can be lifted to a set of conjugate pairs and its root as follows.

Proposition 3. *The common witnesses of a set of conjugate pairs G and its root $R(G)$ are the same, i.e., a word z is a common inner (resp. outer) witness of G iff z is a common inner (resp. outer) witness of $R(G)$.*

When a set is not conjugate, clearly it has no common witness. However, even when a set is conjugate, it may have both common inner and outer witnesses, or only common inner witness, or only common outer witness, or neither of them as shown below.

Example 4. Consider the set $P = \{(ab, ba), (ac, ca))\}$. The pair (ab, ba) has inner witnesses $(ab)^*a$ and outer witnesses $(ba)^*b$. Similarly, the pair (ac, ca) has inner witnesses $(ac)^*a$ and outer witnesses $(ca)^*c$. According to Proposition 2, the set P has a unique common inner witness $a = (ab)^*a \cap (ac)^*a$, but it does not have any common outer witness since $(ba)^*b \cap (ca)^*c = \varnothing$.

The set $\{(ab, ba), (abab, baba)\}$ has both common inner witnesses $(ab)^*a = (ab)^*a \cap ((abab)^*aba \cup (abab)^*a)$ as well as common outer witnesses $(ba)^*b = (ba)^*b \cap ((baba)^*b \cup (baba)^*bab)$.

However, the set $\{(ab, ba), (ba, ab)\}$ has no common witnesses since $(ab)^*a \cap (ba)^*b = \varnothing$.

Proposition 4. *Let G be a set of pairs of words. The following are equivalent.*

1. *G has more than one common witness.*
2. *G has infinitely many common witnesses.*
3. *G has infinitely many common inner witnesses.*
4. *G has infinitely many common outer witnesses.*
5. *All the pairs in G have the same primitive root.*

Therefore, a set of pairs can have no common witness, a unique common witness, or infinitely many common witnesses.

3.2 Common Witness Theorem for Kleene Closure

We generalise the notion in Theorem 1 to an infinite set of pairs closed under concatenation. The question we ask is: "Given an arbitrary set of pairs G, is G^* conjugate?"

If G^* has a common witness, then each pair in G^* has a witness and thus, G^* is conjugate. We prove the converse, namely, if G^* is conjugate, then it has a common witness. The below theorem characterises the conjugacy of a freely generated set of pairs of words.

Theorem 3 (Common Witness Theorem for Kleene Closure). *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. *$R(G)$ has a common witness z.*

Proof (sketch). We prove (4) ⇒ (3) ⇒ (2) ⇒ (1) ⇒ (4).

(4) ⇒ (3) Follows from Proposition 3.

(3) ⇒ (2) WLOG assume that z is a common inner witness of the set G. Hence $\forall (u, v) \in G$, $uz = zv$. Let (u', v') be any arbitrary element from G^*, i.e., $(u', v') = (u_1 \cdots u_n, v_1 \cdots v_n)$ for some $n \geqslant 1$ and $(u_i, v_i) \in G$ for $1 \leqslant i \leqslant n$. By induction on n, we equate $u'z = zv'$ as follows. Thus, z is a common inner witness of G^*.

$$\begin{aligned} u'z &= u_1 \cdots u_{n-1} u_n z \\ &= u_1 \cdots u_{n-1} z v_n && \text{(Since } u_n z = z v_n\text{)} \\ &= z v_1 \cdots v_{n-1} v_n && \text{(Inductive Hypothesis)} \\ &= z v' \end{aligned}$$

(2) ⇒ (1) Follows from Theorem 1.

(1) ⇒ (4) The proof idea is to first prove when G is finite by case analysis and then extend it for a countably infinite set of pairs using a compactness argument — If every finite subset of an infinite set of pairs G has a common witness, then G has a common witness.

As a corollary, we get that E^* is conjugate iff E is conjugate for any rational expression of pairs E. Below is an instance of the common witness theorem for a set of pairs that is not rational.

Example 5. Let $G = \{(ab^p, b^p a) \mid p \text{ is a prime number}\}$. The set G has a common inner witness $a \in \bigcap_{p\in\mathbb{N},\ p \text{ is a prime}} (ab^p)^* a$. It is also easy to verify that G^* is conjugate and a is a common inner witness of G^*.

3.3 Common Witness Theorem for Monoid Closure

Next, we give the common witness theorem for monoid closures, i.e., sumfree sets of the form $(\alpha_0, \beta_0){G_1}^*(\alpha_1, \beta_1){G_2}^* \cdots (\alpha_{k-1}, \beta_{k-1}){G_k}^*(\alpha_k, \beta_k), k > 0$ where $G_1^*, G_2^*, \ldots, G_k^*$ are arbitrary sets of conjugate pairs. It is shown that such a set is conjugate if and only if it has a common witness. Note that this does not generalise to arbitrary sets of pairs, in particular, rational sets using sum.

Example 6. $(ab, ba)^* + (ba, ab)^*$ is an infinite conjugate set with *no* common witness.

Definition 2 (Redux, Singleton Redux). *Let M be the sumfree set*

$$(\alpha_0, \beta_0){G_1}^*(\alpha_1, \beta_1){G_2}^* \cdots (\alpha_{k-1}, \beta_{k-1}){G_k}^*(\alpha_k, \beta_k)\ .$$

The redux *of M is the pair $(\alpha_0\alpha_1 \cdots \alpha_k, \beta_0\beta_1 \cdots \beta_k)$ obtained by substituting each G_i^* by the empty pair (ϵ, ϵ). A* singleton redux *of M is a set obtained by substituting all but one of the G_i^*'s by the empty pair (ϵ, ϵ). They are of the form $(\alpha_0 \cdots \alpha_{i-1}, \beta_0 \cdots \beta_{i-1}){G_i}^*(\alpha_i \cdots \alpha_k, \beta_i \cdots \beta_k)$ where $1 \leqslant i \leqslant k$.*

Example 7. Consider the set $M = (a, a)(baa, aba)^*(b, a)(aab, baa)^*(a, b)$. The redux of M is (aba, aab), and its singleton reduxes are $(a, a)(baa, aba)^*(ba, ab)$ and $(ab, aa)(aab, baa)^*(a, b)$.

If a sumfree set has a common witness, it is conjugate. We prove the converse, i.e., if a sumfree set is conjugate, then it has a common witness which is in the intersection of the common witnesses of the singleton reduxes of the set. Towards this, we need the following definition.

Definition 3 (Prefix Delay and Suffix Delay). *If u and v are words such that one of them is a prefix (resp. suffix) of another, we define the* prefix delay *(resp.* suffix delay*), denoted as $[u, v]_L$ (resp. $[u, v]_R$) between u and v as*

$$[u, v]_L = \begin{cases} u^{-1}v & \textit{if } u \textit{ is a prefix of } v \\ v^{-1}u & \textit{if } v \textit{ is a prefix of } u \end{cases} \quad [u, v]_R = \begin{cases} vu^{-1} & \textit{if } u \textit{ is a suffix of } v \\ uv^{-1} & \textit{if } v \textit{ is a suffix of } u \end{cases}$$

Following is the common witness theorem for a sumfree set with only one Kleene star, i.e., $M = (\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$. In short, it states that such a set is conjugate if and only if it has a common witness that is determined by the common witnesses of $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$.

Proposition 5. *Let $M = (\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$ be a sumfree set with nonempty redux. The following are equivalent.*

1. *M is conjugate.*
2. *There exists a common witness of $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$.*
3. *M has a common witness. Furthermore,*
   (a) *If the set $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$ has a unique common inner witness, say z', then M has a unique common witness $z = [\alpha_0 z', \beta_0]_R = [\alpha_1, z'\beta_1]_L$. Moreover, if $|\alpha_0 z'| \geqslant |\beta_0|$ or equivalently $|\alpha_1| \leqslant |z'\beta_1|$, then z is a common inner witness, otherwise it is a common outer witness.*
   (b) *If the set $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$ has a unique common outer witness, say z', then M has a unique common witness $z = [\alpha_0, \beta_0 z']_R = [z'\alpha_1, \beta_1]_L$. Moreover, if $|z'\alpha_1| \geqslant |\beta_1|$ or equivalently $|\alpha_0| \leqslant |\beta_0 z'|$, then z is a common outer witness, otherwise it is a common inner witness.*
   (c) *If $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$ has infinitely many common witnesses, then M is a subset of powers of the primitive root of its redux. Thus, M has infinitely many common witnesses.*

Example 8. Let $M = (\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$ be a sumfree set with one Kleene star where

$$(\alpha_0, \beta_0) = (ab, b), G = \{(bab, abb)\}, (\alpha_1, \beta_1) = (b, ab).$$

The redux of M is $(\alpha_0\alpha_1, \beta_0\beta_1) = (abb, bab)$. The set $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\} = \{(bab, abb)\} \cup \{(bab, abb)\} = \{(bab, abb)\}$ and, hence it has infinitely many common witnesses. By Proposition 5 3c, M is a subset of powers of the primitive root of the redux, i.e., $M = (abb, bab)^+$. Therefore, M has infinitely many witnesses, the same as those of (abb, bab).

A singleton redux of a sumfree set is nothing but a sumfree set with only one Kleene star. Given any sumfree set M, if M is conjugate, each of its singleton reduxes is conjugate. From Proposition 5, a singleton redux of M has a common witness. Further, we prove that M has a common witness that is the common witness of each of its singleton reduxes. The below theorem characterises the conjugacy of a general sumfree set.

Theorem 4 (Common Witness Theorem for Monoid Closure). *Let M be a sumfree set. The following are equivalent.*

1. *M is conjugate.*
2. *Each of the singleton reduxes of M has a common witness z.*
3. *M has a common witness z.*

Example 9. Let $M = (\alpha_0, \beta_0)G_1^*(\alpha_1, \beta_1)G_2^*(\alpha_2, \beta_2)$ be a sumfree set with two Kleene star where $(\alpha_0, \beta_0) = (b, a), G_1 = \{(ac, ca)\}, (\alpha_1, \beta_1) = (ab, b), G_2 = \{(bab, bab)\}, (\alpha_2, \beta_2) = (\epsilon, b)$. The redux of M is $(\alpha_0\alpha_1\alpha_2, \beta_0\beta_1\beta_2) = (bab, abb)$. The set M has two singleton reduxes,

$$M_1 = (\alpha_0, \beta_0)G_1^*(\alpha_1\alpha_2, \beta_1\beta_2) = (b, a)(ac, ca)^*(ab, bb), \text{ and}$$

$$M_2 = (\alpha_0\alpha_1, \beta_0\beta_1)G_2^*(\alpha_2, \beta_2) = (bab, ab)(bab, bab)^*(\epsilon, b).$$

The set $G_1 \cup \{(\alpha_1\alpha_2\alpha_0, \beta_1\beta_2\beta_0)\} = \{(ac, ca), (abb, bba)\}$ has a unique common inner witness, say $z_1 = a = (ac)^*a \cap (abb)^*a$ and no common outer witness since $(ca)^*c \cap (bba)^*bb = \varnothing$. By Proposition 5 3a, the unique common inner witness of the singleton redux M_1 is $[\alpha_0 z_1, \beta_0]_R = [ba, a]_R = b$.

The set $G_2 \cup \{(\alpha_2\alpha_0\alpha_1, \beta_2\beta_0\beta_1)\} = \{(bab, bab)\}$ has infinitely many common witnesses. Thus, the singleton redux M_2 is a subset of powers of the primitive root of the redux using Proposition 5 3c, i.e., $M_2 = (bab, abb)^+$. Thus M_2 has infinitely many common inner witnesses $(bab)^*b$ and common outer witnesses $(abb)^*ab$.

By Theorem 4, M has a unique common inner witness $b \cap (bab)^*b = b$, that equals to the intersection of the common inner witness of its singleton reduxes M_1 and M_2.

4 Computing Witness of a Sumfree Expression

In this section, we give a decision procedure to compute the common witness of a sumfree expression, if it exists. The set of common witnesses (abbreviated as the *witness set*) of a sumfree expression is either empty, singleton, or infinite. Whenever there are infinitely many common witnesses for an expression, the witnesses are the same as those of its primitive root (Proposition 4). In that case, we compute the primitive root as their finite representation.

The following proposition shows that there is a bound to the size of the unique common witness of two conjugate pairs if it exists, which aids in computing the common witness of two pairs in polynomial time.

Proposition 6. *If two conjugate pairs (u_1, v_1) and (u_2, v_2) have a unique common witness z, then $|z| \leqslant 2 \cdot \max(|u_1|, |u_2|)$.*

The witness set of a sumfree expression is equal to the intersection of witness sets of each of its singleton reduxes. So first, we compute the witness set of a singleton redux.

Lemma 2. *Let $M = (\alpha_0, \beta_0)E^*(\alpha_1, \beta_1)$ be a sumfree expression. Given the witness set of E, we can compute the witness set of M in time $\mathcal{O}((m+n)^2)$ where m is the size of the expression M, and n is the size of the witness of E.*

Proof (sketch). If the redux of M is the empty word, then the witness set of M is equal to the witness set of E by Theorem 3. Now if M has a nonempty redux, M has a common witness iff $E \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$ has a common witness by Proposition 5. If it exists, the common witness of M can be computed from the common witness of $E \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$ using Proposition 5 3a, 3b, 3c.

Using the above algorithm, we compute the common witness of a general sumfree expression.

Lemma 3. *Let M be a sumfree expression. 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.*

Proof (sketch). From Theorem 4, the witness set of M is the intersection of the witness sets of its singleton reduxes. The idea is that we compute the witness set of each singleton reduxes, if it exists, using Lemma 2. Assume M has a nonempty redux. If all the singleton reduxes have infinitely many witnesses, then M is a subset of powers of the primitive root of the redux of M by Proposition 53c and thus, M has infinitely many common witnesses. If there exists a singleton redux with a unique common witness, say z, then for all other singleton reduxes of M with a unique witness z', check if $z = z'$ (for all other singleton reduxes z is already a witness by virtue of being a witness of the redux of M). If so, z is the unique common witness of M; otherwise, M has no common witness. The case where M has an empty redux is similar.

Computation of the Witness Set: Given a sumfree expression M, we compute its witness set bottom-up. We start from the innermost Kleene star. It is a pair of words (u, v). First, we check if (u, v) is conjugate. If yes, then there are infinitely many common witnesses for $(u, v)^*$, namely the witnesses of its primitive root, otherwise M has no witness. This step can be done in a time polynomial in the length of (u, v). Now, we recursively use Lemma 3 to compute the common witness of the expression under the Kleene star in each level. If there is no common witness for any level of Kleene star expression, then M is not conjugate. To find out the complexity of the decision procedure, it suffices to estimate the maximum length of a witness involved in the computation.

Length of the Witness of a Sumfree Expression: We claim that if a sumfree expression M is conjugate, then there exists a witness of length linear in size of M. If M has infinitely many witnesses, M is a set of powers of a primitive root by Proposition 4. Thus, there exists a witness of length less than that of the length of the primitive root. Next, suppose M has a unique common witness. In that case, there exists a subexpression E_i^* such that E_i^* has a unique common witness, and all Kleene stars appearing in E_i have infinitely many witnesses. Thus, all of them have a common witness of length at most $|E_i|$. Therefore, there is a singleton redux M_i of E_i^* that has a unique witness z_i. The size of z_i is linear in M_i and the size of the witnesses of subexpressions of E_i. Both are upper bounded by the size of M. Furthermore, the common witnesses for all subsequent levels are unique (if they exist), and their length is bounded by $|M|$.

Complexity of the Algorithm: Since the size of the common witness of M is linear in $|M|$, by Lemma 3, the overall complexity of computing a common witness of a sumfree expression is $\mathcal{O}(h \cdot m^3)$ where h is the *star height* of M and m is the length of the expression.

5 Conclusion

The current decision procedure proceeds through the analysis of rational expressions. In its essence, it is analogous to the boundedness checking of distance automata using factorisation trees [8], though explicit use of factorisation trees are avoided using sumfree rational expressions instead. An obvious question is the existence of an automata-theoretic proof. Factorisation forests remain the primary tool to settle boundedness questions on automata and by that standard the proof approach taken in this paper is natural and quite possibly the most intuitive.

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 presented in the paper is of exponential time. It remains to find the precise complexity of this problem.

It is natural to look at the conjugacy problem of more general classes, for instance functions definable by a deterministic two-way transducers (regular functions [9]), or by two-way pebble automata (polyregular functions [3]). The corresponding problem over free groups is another interesting problem.

References

1. Aiswarya, C., Manuel, A., Sunny, S.: Deciding conjugacy of a rational relation. CoRR **abs/2307.06777** (2023). https://doi.org/10.48550/arXiv.2307.06777
2. Aiswarya, C., Manuel, A., Sunny, S.: Edit distance of finite state transducers. In: ICALP 2024. LIPIcs, Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2024). https://doi.org/10.48550/arXiv.2404.16518, CoRRabs/.2404.16518, (To appear)
3. Bojanczyk, M.: Transducers of polynomial growth. In: LICS 2022. pp. 1–27. ACM (2022). https://doi.org/10.1145/3531130.3533326
4. Cassaigne, J., Karhumäki, J., Manuch, J.: On conjugacy of languages. RAIRO Theoretical Informatics and Applications **35**(6), 535–550 (2001). https://doi.org/10.1051/ita:2001130
5. Choffrut, C.: Une caractérisation des fonctions séquentielles et des fonctions sous-séquentielles en tant que relations rationnelles. Theoretical Computer Science **5**(3), 325–337 (1977). https://doi.org/10.1016/0304-3975(77)90049-4
6. Choffrut, C., Karhumäki, J.: Combinatorics of words. In: Handbook of Formal Languages, Volume 1: Word, Language, Grammar, pp. 329–438. Springer (1997). https://doi.org/10.1007/978-3-642-59136-5_6
7. Choffrut, C., Schützenberger, M.P.: Décomposition de fonctions rationnelles. In: STACS 86. Lecture Notes in Computer Science, vol. 210, pp. 213–226. Springer (1986). https://doi.org/10.1007/3-540-16078-7_78
8. Colcombet, T.: The factorisation forest theorem. In: Handbook of Automata Theory, pp. 653–693. European Mathematical Society Publishing House (2021). https://doi.org/10.4171/AUTOMATA-1/18
9. Engelfriet, J., Hoogeboom, H.J.: MSO definable string transductions and two-way finite-state transducers. ACM Transactions on Computational Logic **2**(2), 216–254 (2001). https://doi.org/10.1145/371316.371512

10. Finkel, O., Halava, V., Harju, T., Sahla, E.: On bi-infinite and conjugate post correspondence problems. RAIRO Theoretical Informatics and Applications **57**, 7 (2023). https://doi.org/10.1051/ITA/2023008
11. Jecker, I., Filiot, E.: Multi-sequential word relations. International Journal of Foundations of Computer Science **29**(2), 271–296 (2018). https://doi.org/10.1142/S0129054118400075
12. Karhumäki, J.: Combinatorial and computational problems on finite sets of words. In: MCU 2001. Lecture Notes in Computer Science, vol. 2055, pp. 69–81. Springer (2001). https://doi.org/10.1007/3-540-45132-3_4
13. Lombardy, S., Sakarovitch, J.: Sequential? Theoretical Computer Science **356**(1-2), 224–244 (2006). https://doi.org/10.1016/J.TCS.2006.01.028
14. Lothaire, M.: Combinatorics on words. Cambridge mathematical library, Cambridge University Press (1997). https://doi.org/10.1017/CBO9780511566097
15. Peifer, D.: Max Dehn and the origins of topology and infinite group theory. The American Mathematical Monthly **122**(3), 217–233 (2015). https://doi.org/10.4169/amer.math.monthly.122.03.217
16. Sakarovitch, J.: Elements of Automata Theory. Cambridge University Press (2009). https://doi.org/10.1017/CBO9781139195218
17. Simon, I.: Factorization forests of finite height. Theoretical Computer Science **72**(1), 65–94 (1990). https://doi.org/10.1016/0304-3975(90)90047-L