


Deciding Conjugacy of a Rational Relation

C. Aiswarya 

Chennai Mathematical Institute, India and IRL ReLaX, CNRS France

aiswarya@cmi.ac.in

Amaldev Manuel

Indian Institute of Technology Goa

amal@iitgoa.ac.in

Saina Sunny 

Indian Institute of Technology Goa

saina19231102@iitgoa.ac.in

Abstract

A rational relation is conjugate if every pair of related words are conjugates. It is shown that checking whether a rational relation is conjugate is decidable. For this, we generalise the Lyndon-Schützenberger’s theorem from word combinatorics. A consequence of the generalisation is that a set of pairs generated by a sumfree rational expression is conjugate if and only if there is a word witnessing the conjugacy of all the pairs.

2012 ACM Subject Classification Theory of computation → Quantitative automata; Mathematics of computing → Combinatorics on words

Keywords and phrases Rational relations, Finite state transducers, Conjugacy of words, Combinatorics of words

Contents

1	Introduction	2
1.1	Rational Sets and Relations	2
1.2	Conjugacy of Words and Relations	3
1.3	Sumfree Expressions	3
1.4	Conjugacy of a Sumfree Expression	4
1.5	Related Work	6
1.6	Organisation of the Paper	6
2	Tools from Combinatorics of Words	7
2.1	Primitive and Periodic words	7
2.2	Characterisation of Conjugacy and the Uniqueness of Cuts	8
3	Common Witness Theorems	10
3.1	Common Witness Theorem for Kleene Closure	10
3.2	Common Witness Theorem for Monoid Closure	14
4	Auxillary Results for Case Analysis	16
4.1	Cut Lemma and its Corollaries	16
4.2	Equal Length Lemma	19
5	Existence of Common Witness for Kleene Closure	21
5.1	For a Finite Set of Pairs	21
5.2	For an Infinite Set of Pairs	25

6	Existence of Common Witness for Monoid Closure	25
6.1	Common Witness of a Singleton Redux	25
6.2	Common Witness of a Sumfree Set	37
7	Computing Witness of a Sumfree Expression	44
8	Conclusion	47

1 Introduction

We begin by recalling the definitions of rational relations and expressions and introduce the conjugacy problem of rational relations. The general problem is then reduced to determining conjugacy of sumfree expressions. Subsequently, it is argued that decidability follows from two specific questions (Question 11 and Question 14). We conclude the section by giving an overview of our results and related work.

1.1 Rational Sets and Relations

A monoid \mathbf{M} is a set M with an associative binary operation that has an identity. For convenience, we speak of the monoid operation as a multiplication (\cdot) and denote the identity by 1. For example, the set of all finite words over an alphabet A , denoted as A^* , forms a monoid with concatenation as the operation and the empty word ϵ as the identity. The product operation can be extended to subsets of M as

$$X \cdot Y = \{x \cdot y \mid x \in X, y \in Y\} . \quad (1)$$

Since the operation is associative, we can define X^i without any ambiguity. For instance, defined inductively, $X^0 = \{1\}$, and $X^i = X^{i-1} \cdot X$, for $i > 0$. Similarly, the *Kleene closure* of X , denoted as X^* , is the closure of X under finite products, i.e.,

$$X^* = X^0 \cup X^1 \cup \dots \quad (2)$$

► **Definition 1** (Rational Subset). *The family of rational subsets of \mathbf{M} is the smallest class containing all the finite subsets of M and closed under union, product and Kleene closure.*

A natural way to present a rational subset is as an expression.

► **Definition 2** (Rational Expression). *A rational expression over the monoid \mathbf{M} is defined recursively: $\emptyset, 1, m \in M$ 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.*

The *language* of a rational expression E , denoted as $L(E) \subseteq M$, is defined as follows.

$$\begin{array}{llll} L(\emptyset) & = & \emptyset & L(1) & = & \{1\} \\ L(m) & = & \{m\} & L(E_1 \cdot E_2) & = & L(E_1) \cdot L(E_2) \\ L(E_1 + E_2) & = & L(E_1) \cup L(E_2) & L(E_1^*) & = & L(E_1)^* \end{array}$$

It is easy to prove that rational expressions define precisely the class of rational subsets of \mathbf{M} . Two rational expressions are *equivalent* (denoted by \equiv) if they define the same sets.

► **Definition 3** (Rational Relation). *A binary relation over two free monoids A^* and B^* is a subset of the product monoid $A^* \times B^*$. It is rational if it is a rational subset of $A^* \times B^*$.*

► **Example 4.** [13] Let monoid $M = \{a\}^* \times \{b, c\}^*$. The set $R_1 = (a, b)^*(\epsilon, c)^* = \{(a^n, b^n c^m) \mid n, m \geq 0\}$ is a rational subset of M . The set $R_2 = (\epsilon, b)^*(a, c)^* = \{(a^n, b^m c^n) \mid n, m \geq 0\}$ is also a rational subset of M .

Rational relations are precisely those computable by a 2-tape 1-way finite automata, or equivalently by a nondeterministic finite state transducer [9, 15]. The first systematic study of such relations was established by Elgot and Mezei [5]. A recent survey on transducers can be found in [12].

The class of rational relations are closed neither under intersection nor under complement. For instance in the above example $R_1 \cap R_2 = \{(a^n, b^n c^n) \mid n \geq 0\}$ is not a rational subset of M ([13], Example 1.3). Several algorithmic problems, such as universality, equivalence, and intersection emptiness, are undecidable [7, 14]. However, a notable subclass of rational relations is the class of rational functions that admits a decidable equivalence problem [1].

1.2 Conjugacy of Words and Relations

► **Definition 5** (Conjugate Word). *A pair of words (u, v) is conjugate, denoted as $u \sim v$, if there exist words x and y (possibly empty) such that $u = xy$ and $v = yx$. In other words, u and v are cyclic shifts of one another.*

For example, $(aaab, aaba)$ is a conjugate pair with $x = a$ and $y = aab$. It is not difficult to see that conjugacy relation is an equivalence relation on the set of words.

Let A and B be two finite alphabets. We say, a set of pairs from (or a relation over) $A^* \times B^*$ is *conjugate* if each pair in the set is conjugate. In this work we address the following question.

► **Question 6** (Conjugacy Problem). *Given a rational relation over the product monoid $A^* \times B^*$, is it conjugate?*

We assume that the input is given as a rational expression over the monoid $A^* \times B^*$. Furthermore, if there is a pair in the relation containing a letter in the symmetric difference of A and B , then the pair as well as the relation is not conjugate. Since this can be easily checked, the nontrivial part of the problem is when the alphabets are identical, i.e., when $A = B$. Therefore we assume that the given rational relation is over $A^* \times A^*$ for a fixed finite alphabet A .

The objective of this paper is to address the decidability of conjugacy problem for a rational relation. We present a proof that conjugacy of a rational relation can be decided.

1.3 Sumfree Expressions

A rational expression is *sumfree* if it does not use the sum (i.e., $+$). The set of sumfree expressions can be defined formally as a hierarchy.

Fix a monoid $\mathbf{M} = (M, \cdot, 1)$. Given a class \mathcal{C} of expressions over \mathbf{M} , the *Kleene closure* of \mathcal{C} , denoted as \mathcal{KC} , is the smallest class of expressions containing \mathcal{C} and closed under Kleene star, i.e.,

$$\mathcal{KC} = \mathcal{C} \cup \{E^* \mid E \in \mathcal{C}\}.$$

The *monoid closure* of \mathcal{C} , denoted as \mathcal{MC} , is the smallest class containing \mathcal{C} that is closed under concatenation, i.e.,

$$\mathcal{MC} = \mathcal{C} \cup \{E_1 \cdots E_k \mid E_i \in \mathcal{C} \text{ for each } 1 \leq i \leq k \text{ and } k \in \mathbb{N}\}.$$

► **Definition 7** (Sumfree expression). *The family \mathcal{F} of sumfree expressions is defined inductively. Let $\mathcal{F}_0 = \{\emptyset, 1\} \cup M$ and $\mathcal{F}_{i+1} = \mathcal{MK}\mathcal{F}_i$ for each $i \geq 0$. We define*

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

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

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

A rational expression is in *Sumfree Normal Form* (SNF) if it is a finite sum of sumfree expressions. The following lemma is standard.

► **Lemma 8.** *Every rational expression is effectively equivalent to one in sumfree normal form.*

Proof. Let E be a rational expression over the monoid \mathbf{M} . We obtain an equivalent expression by induction on the structure of E . For the base case, if E is \emptyset or 1 or $m \in M$, then E is already sumfree.

Next assume that E_1 and E_2 are rational expressions. By induction hypothesis, $E_1 \equiv \alpha_1 + \cdots + \alpha_k$ and $E_2 \equiv \beta_1 + \cdots + \beta_\ell$ such that α_i, β_j , $1 \leq i \leq k$, $1 \leq j \leq \ell$, are sumfree expressions.

If $E = E_1 + E_2$, then by substituting for E_1 and E_2 , we get an equivalent expression of the desired form.

If $E = E_1 \cdot E_2$, then by substituting E_1 and E_2 we get $E \equiv (\alpha_1 + \cdots + \alpha_k) \cdot (\beta_1 + \cdots + \beta_\ell)$. Distributing the monoid operation over the union, we get $E \equiv (\alpha_1 \beta_1 + \cdots + \alpha_1 \beta_\ell) + \cdots + (\alpha_k \beta_1 + \cdots + \alpha_k \beta_\ell)$, that is in the required form.

Finally, if $E = E_1^*$, then by repeatedly applying the rational identity $(X+Y)^* = (X^*Y^*)^*$, where X, Y are rational expressions, we get $E = E_1^* \equiv (\alpha_1 + \alpha_2 + \cdots + \alpha_k)^* = (\alpha_1^* \alpha_2^* \cdots \alpha_k^*)^*$. ◀

Rewriting a rational expression as a sum of sumfree expressions may result in an exponential blow-up. For example, the equivalent expression in SNF for $(a+b)^n$, $n > 0$ over the monoid $\{a, b\}^*$ has at least 2^n summands.

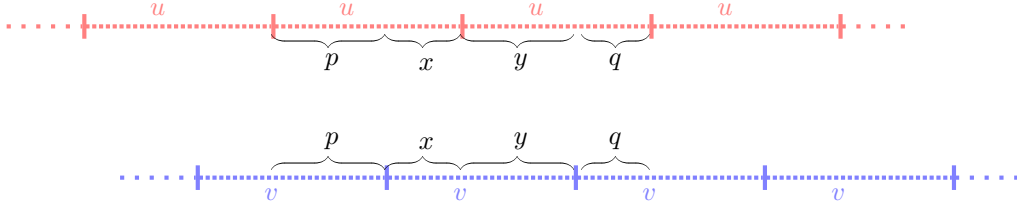
By Lemma 8, we can assume without loss of generality that a given rational expression is in SNF.

1.4 Conjugacy of a Sumfree Expression

► **Proposition 9.** *Let $E = E_1 + \cdots + E_k$, $k \geq 1$ be a rational expression over $A^* \times A^*$ in SNF. Then E is conjugate if and only if each of E_1, \dots, E_k is conjugate.*

Proof. Since each $L(E_i) \subseteq L(E)$, for $1 \leq i \leq k$, if E is conjugate then each E_i is conjugate as well. For the other direction, assume that E_1, \dots, E_k define conjugate relations. Then each pair in $L(E)$ belongs to some $L(E_i)$, for $1 \leq i \leq k$, and hence it is conjugate. Since all pairs in $L(E)$ are conjugate, E is conjugate by definition. ◀

Therefore, to solve the conjugacy problem it suffices to solve it for sumfree expressions. We use pairs of lowercase Greek letters (α, β) with suitable modifications to denote pairs



■ **Figure 1** v as infix of uu .

of words over $A^* \times A^*$. Clearly \emptyset and (ϵ, ϵ) are conjugates. For an expression of the form (α, β) , it is straightforward to check conjugacy. Thus 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 show that if the problem is decidable for \mathcal{F}_i , $i \geq 0$, 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 . Let E be an expression in \mathcal{F}_i and hence $E^* \in \mathcal{KF}_i$. Since $L(E) \subseteq L(E^*)$,

► **Proposition 10.** *The expression E^* is conjugate only if E is conjugate.*

Because conjugacy is decidable for \mathcal{F}_i , we can check whether E is conjugate. Therefore, to show the decidability of conjugacy for \mathcal{KF}_i it suffices to show the decidability of the following question.

► **Question 11 (Conjugacy of Kleene Closures).** Given a conjugate sumfree expression E , is E^* conjugate?

Next assume that conjugacy is decidable for \mathcal{KF}_i . Let $E = (\alpha_0, \beta_0)E_1^*(\alpha_1, \beta_1) \cdots E_k^*(\alpha_k, \beta_k)$ be an expression in \mathcal{MKF}_i where E_1^*, \dots, E_k^* are from \mathcal{KF}_i . Analogous to the case of Kleene closures, E is conjugate only if E_1^*, \dots, E_k^* are conjugate, as the next lemma shows.

► **Lemma 12.** *If the expression $E = (\alpha_0, \beta_0)F^*(\alpha_1, \beta_1)$ is conjugate, then F^* is conjugate.*

Proof. If F^* is an empty set, then it is conjugate. Otherwise, assume that (u, v) is a nonempty pair in $L(F^*)$. Therefore, (u^ℓ, v^ℓ) for each $\ell \geq 0$ 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 that in turn leads to nonconjugacy of E .

Let k be the total length of $|\alpha_0 + \beta_0 + \alpha_1 + \beta_1|$. Consider the pair $(\alpha_0, \beta_0)(u^\ell, v^\ell)(\alpha_1, \beta_1)$ where $\ell = 2^k$ (some value much larger than 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 portion 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 $|u| = |v|$, length of p and length of y are the same, that 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 generalize the above lemma to the general form of sumfree expressions.

► **Corollary 13.** *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 $E_1^*, E_2^*, \dots, E_k^*$ is conjugate.*

Proof. If E is conjugate, then for each $i \in \{1, \dots, k\}$,

$$(\alpha_0 \cdots \alpha_{i-1}, \beta_0 \cdots \beta_{i-1})E_i^*(\alpha_i \cdots \alpha_k, \beta_i \cdots \beta_k) \subseteq E$$

is conjugate. Therefore, from Lemma 12 we get that each of E_1^*, \dots, E_k^* is conjugate. ◀

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

► **Question 14 (Conjugacy of Monoid Closures).** Given conjugate sumfree expressions E_1^*, \dots, 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 11 and Question 14 can be effectively answered. We use the notion of a *common witness*. 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 *common witness* of a conjugate set of pairs is either an inner witness of all the pairs in the set or an outer witness of all the pairs in the set (further elaborated in Definition 35).

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

1. Let G be an arbitrary conjugate set of pairs. The set G^* is conjugate if and only if G has a common witness (Theorem 42).
2. Let G_1^*, \dots, G_k^* be arbitrary conjugate sets of 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 49).

► **Remark 15.** Note that the assumption of conjugacy of the sets G, G_1^*, \dots, 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 (Since Proposition 10 and Corollary 13 also holds for arbitrary sets).

Item 2 is a generalisation of Item 1, and its proof relies on Item 1. Both theorems are generalisations of a classical theorem of Lyndon-Schützenberger (recalled in the next section).

When G, G_1^*, \dots, G_k^* are rational sumfree expressions of pairs, the above theorems are *effective*, that is a common witness, if exists, is computable in polynomial time (Section 7). Hence, we have the following decidability result.

► **Theorem 16 (Main Theorem).** *It is decidable to check if a rational relation is conjugate.*

1.5 Related Work

A problem much related to Theorem 42 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 [8]. 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 to infinite sets, though with no comparison to ours, is considered in [3], 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.

1.6 Organisation of the Paper

In Section 2, we revisit the standard tools from combinatorics of words required to state and prove our main theorems. We present the common witness theorems for addressing Question 11 and Question 14, along with the proofs of the easier directions in Section 3. However, the difficult directions require a detailed case analysis. To simplify the analysis, we

use some auxiliary results presented in Section 4. Using those results, we complete the proof of common witness theorems for Kleene closure and monoid closure in Section 5 and Section 6 respectively. We outline the decision procedure for computing the witness in Section 7. This section can be read independently of Sections 4, 5 and 6. In Section 8, we state some future directions and conclude.

2 Tools from Combinatorics of Words

We recall some standard notions from combinatorics on words and introduce some new definitions and associated facts (Definition 17, Definition 29, Proposition 30 and Proposition 31).

The set of all finite nonempty words over A is denoted by A^+ . The unique infinite word $u \cdot u \cdots$ (ω -times) is denoted by u^ω . A word u is called a *factor* (respectively *prefix*, *suffix*) of a word v , if there exist words $x, y \in A^*$ such that $v = xuy$ (respectively $v = uy$, $v = xu$). Let $u[i..j]$ denote the factor of u from index i to j where $1 \leq i \leq j \leq |u|$. Let u^r denote the word obtained by reversing the word u and for $i \geq 0$ let $lshift_i(u)$ denote the word obtained after i left cyclic shifts of a word u .

If u and v are words such that u is a prefix of v , the *left quotient* of v by u , denoted by $u^{-1}v$, is the word x such that $v = ux$. Similarly, the *right quotient* of $v = xu$ by u , denoted as vu^{-1} , is the word x .

► **Definition 17** (Mutual Quotient). *If u and v are words such that one of them is a prefix of another, we define the mutual left quotient between u and v as*

$$[u, v]_L = \begin{cases} u^{-1}v & \text{if } u \text{ is a prefix of } v \\ v^{-1}u & \text{if } v \text{ is a prefix of } u \end{cases}$$

Similarly, the mutual right quotient of two words u and v such that one of them is suffix of another, denoted by $[u, v]_R$, is vu^{-1} if u is a suffix of v and uv^{-1} if v is a suffix of u .

For example, $[abaa, ab]_L = aa = [ab, abaa]_L$.

2.1 Primitive and Periodic words

A word u is said to be a *power* of a word v if u is obtained by concatenating v a certain number of times, i.e.,

$$u = v^n \text{ for some } n \geq 1.$$

► **Definition 18** (Primitive word). *A word $u \in A^+$ is primitive if it cannot be expressed as a power of any strictly smaller word.*

For example, aba is primitive but $abab$ is not. The following fact is easy to verify.

► **Proposition 19.** *If u is primitive, then u^r is also primitive.*

A word ρ is called a *primitive root* of a word u if $u = \rho^n$ for $n \geq 1$ and ρ is a primitive word.

Following theorem relates primitivity and commutativity.

► **Theorem 20** (First Theorem of Lyndon-Schützenberger ([11], Lemma 3)). *Two words $u, v \in A^*$ commute, i.e., $uv = vu$, if and only if they are powers of a same word.*

The above theorem has an interesting corollary about primitive root of a word.

► **Corollary 21** ([10], Proposition 1.3.1). *Every word u has a unique primitive root, denoted by ρ_u .*

► **Proposition 22.** *The primitive root of a word can be computed in time polynomial in the length of the word.*

Proof. For a word w , we can compute the smallest $i \in \{1, \dots, |w|\}$ such that $\text{lshift}_i(w) = w$ in time quadratic to $|w|$. If i divides $|w|$, then $w[1 \dots i]$ is the primitive root of word w . ◀

Let $w = a_1 a_2 \dots a_n$ where $a_i \in A, n \geq 1$. We say that $1 \leq p < n$ is a *period* of w if $a_i = a_{i+p}$ for $i \in 1, \dots, n - p$. For example, the word *abababa* has periods 2, 4, and 6. Below is a fundamental periodicity result of words by Fine and Wilf.

► **Theorem 23** (Fine and Wilf ([4], Theorem 5)). *If a word has two periods p and q , and it is of length at least $p + q - \gcd(p, q)$, then it also has a period $\gcd(p, q)$.*

Below is a reformulation of the above theorem.

► **Corollary 24** ([4], Theorem 5). *Let u and v be two nonempty words. They are powers of the same word if and only if the words u^ω and v^ω have a common prefix of length $|u| + |v| - \gcd(|u|, |v|)$.*

2.2 Characterisation of Conjugacy and the Uniqueness of Cuts

Given below is a complete characterisation of conjugacy.

► **Theorem 25** (Second Theorem of Lyndon-Schützenberger ([10], Proposition 1.3.4)). *Two words u and v are conjugate iff there exists a word z such that*

$$uz = zv . \quad (3)$$

More precisely, Equation (3) holds iff there exist words x and y such that

$$u = xy, v = yx, z \in (xy)^*x . \quad (4)$$

If we switch the words u and v in the above theorem, we get that v and u are conjugates if and only if there exists a word z' such that $z'u = vz'$ where $v = yx, u = xy$ and $z' \in (yx)^*y$. Therefore if (u, v) is a conjugate pair, then there exist words z, z' such that $uz = zv$ and $z'u = vz'$.

The following proposition connects conjugate words and their primitive roots.

► **Proposition 26** ([4], Lemma 1). *If u and v are conjugates, then their primitive roots ρ_u and ρ_v respectively are also conjugate. In particular, the exponents are equal, i.e., $u = \rho_u^n$ and $v = \rho_v^n$ for some $n \geq 1$.*

The theorem of Fine and Wilf (Corollary 24) can be adapted to yield primitive roots that are conjugates.

► **Theorem 27** (Conjugate Fine and Wilf ([4], Theorem 5)). *Let $\ell(u, v)$ denote the maximal common factor of words u and v . For any two words $u, v \in A^+$, if u^ω and v^ω have a common factor of length at least $|u| + |v| - \gcd(|u|, |v|)$, then the primitive roots of u and v are conjugates, i.e., we have*

$$\ell(u^\omega, v^\omega) \geq |u| + |v| - \gcd(|u|, |v|) \Rightarrow \rho_u \sim \rho_v .$$

Like primitivity, conjugacy can also be decided easily.

► **Proposition 28.** *Deciding if a pair of words is conjugate can be done in quadratic time.*

Proof. Let (u, v) be a pair of words. We can check if there exists an $i \in \{1, \dots, |u|\}$ such that $\text{lshift}_i(u) = v$ in time quadratic to the length of u . ◀

► **Definition 29 (Cut).** *A cut of a conjugate pair (u, v) is a pair of words (x, y) such that $u = xy$ and $v = yx$. Alternatively, we say that u has a cut at position $|x|$, or equivalently, v has a cut at position $|y|$.*

If either x or y is the empty word, then we say the cut is empty. Otherwise the cut is nonempty.

For example, the pair $(aabb, bbaa)$ has a cut (aa, bb) . There can be several cuts for a conjugate pair. For instance, the pair $(abab, baba)$ has cuts (a, bab) and (aba, b) .

If u and v are conjugates and one of them is primitive, by Proposition 26, the other is also primitive. A pair (u, v) is primitive if both u and v are primitive words. For such pairs, their cuts are also special.

► **Proposition 30 (Uniqueness of Cuts of Primitive Pairs).** *Let (u, v) be a distinct conjugate primitive pair. Then (u, v) has a unique cut (x, y) , i.e., there exists unique words x and y such that $u = xy$ and $v = yx$.*

Proof. By definition, if pair (u, v) is conjugate, then there exist a cut (x, y) such that $u = xy$ and $v = yx$. Since u and v are distinct, x and y have to be nonempty. It suffices to show that x and y are unique if u and v are primitive.

For the sake of contradiction, assume that (x, y) is not unique, i.e., there exists a different cut (x', y') for (u, v) , i.e., $u = x'y'$, $v = y'x'$ and $x' \neq x, y' \neq y$. WLOG, assume that $|x| > |x'|$. Therefore there exists a nonempty word p such that $x = x'p$ and $y' = py$. Substituting for x in v , we get

$$v = yx = yx'p$$

and substituting for y' in v , we obtain

$$v = y'x' = pyx'.$$

Therefore yx' and p commutes. By the first theorem of Lyndon-Schützenberger (Theorem 20), they are powers of the same word. Since p and yx' are nonempty words, v is a power of some smaller word. Hence v is not primitive and it is a contradiction. ◀

In the case where $u = v$ and u being primitive, two possible cuts are (u, ϵ) and (ϵ, v) , i.e., the empty cuts. Imagine there is a nonempty cut (x, y) . Since $u = v$, it follows that $xy = yx$. Using the first theorem of Lyndon-Schützenberger (Theorem 20), u and v are powers of a smaller word and hence not primitive. Therefore, when u is primitive and $u = v$, the only possible cuts are the empty cuts.

► **Proposition 31.** *If (x, y) is a cut of the conjugate pair (u, v) , then (u^r, v^r) is also conjugate with the cut (y^r, x^r) .*

Proof. Since (x, y) is a cut of (u, v) , $u = xy$ and $v = yx$. Hence, $u^r = y^r x^r$ and $v^r = x^r y^r$. Thus, (u^r, v^r) is conjugate with the cut (y^r, x^r) . ◀

3 Common Witness Theorems

In this section, it is shown that an infinite set of pairs that is generated by a sumfree set is conjugate if and only if there is a word witnessing its conjugacy. This is an infinitary analogue of Theorem 25.

3.1 Common Witness Theorem for Kleene Closure

Lyndon-Schützenberger theorem characterises conjugacy of a pair of words. We generalise the notion in Theorem 25 to an infinite set of pairs closed under concatenation. The question we ask is:

“Given an arbitrary set of pairs G , whether G^* , i.e., the Kleene closure (Equation (2)) of G , is conjugate?”

We have already seen from the second theorem of Lyndon-Schützenberger (Theorem 25) that if two words u and v are conjugates, then there exist words z, z' such that $uz = zv$ and $z'u = vz'$. This leads to the following notion.

► **Definition 32** (Inner and Outer Witness). *Given a conjugate pair (u, v) , the word z is an inner witness of (u, v) if $uz = zv$. Similarly, z is an outer witness of (u, v) if $zu = vz$.*

An inner witness of a pair (u, v) is an outer witness of the pair (v, u) . A conjugate pair has infinitely many inner and outer witnesses by Theorem 25.

► **Example 33.** The pair (aba, baa) has inner witnesses $(aba)^*a$ and outer witnesses $(baa)^*ba$.

We say that a pair of words has a *witness* if it has either an inner witness or an outer witness.

► **Proposition 34.** *Powers of a conjugate pair is also conjugate. Furthermore, if a pair (u, v) is conjugate with a witness z , then (u^n, v^n) for $n \geq 1$ is also conjugate with the same witness z .*

Proof. If (u, v) is conjugate, by Theorem 25, there exists a word z such that $uz = zv$ (that is z is an inner witness of (u, v)). By induction on n , we prove $\forall n \geq 1 \ u^n z = zv^n$. It is true when $n = 1$. For all $n > 1$,

$$\begin{aligned} u^n z &= u^{n-1} u z \\ &= u^{n-1} z v && \text{(Since } uz = zv \text{)} \\ &= z v^{n-1} v && \text{(Inductive Hypothesis)} \\ &= z v^n \end{aligned}$$

Symmetrically we can prove that $z' u^n = v^n z'$, for any outer witness z' of (u, v) . Hence if (u, v) is conjugate with a witness z , then (u^n, v^n) for $n \geq 1$ is also conjugate, with the same witness z . ◀

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

► **Definition 35** (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 can be obtained from Theorem 25.

► **Proposition 36.** *Let $P = \{(u_i, v_i) \mid i \in I\}$ be a set of pairs of words. The following are equivalent.*

1. z is a common inner witness of P .
2. There exists a cut (x_i, y_i) of each pair (u_i, v_i) such that $z \in \bigcap_{i \in I} (x_i y_i)^* x_i$.
3. $z \in \bigcap_{i \in I} \bigcup_{j \in \{1, \dots, k_i\}} (x_{i,j} y_{i,j})^* x_{i,j}$ where $\{(x_{i,1}, y_{i,1}), \dots, (x_{i,k_i}, y_{i,k_i})\}$ is the set of all cuts of (u_i, v_i) .

The statement for common outer witness is analogous.

Proof. We prove $(3) \Rightarrow (2) \Rightarrow (1) \Rightarrow (3)$. $(3) \Rightarrow (2)$ is obvious. $(2) \Rightarrow (1)$ follows from Theorem 25. We show $(1) \Rightarrow (3)$. Suppose z is a common inner witness of P , i.e., z is an inner witness of each pair in P . Hence $u_i z = z v_i$ for each $i \in I$. Let $\{(x_{i,1}, y_{i,1}), \dots, (x_{i,k_i}, y_{i,k_i})\}$ be the set of all cuts of (u_i, v_i) . Using Theorem 25, there exists a cut (x_i, y_i) for (u_i, v_i) such that $z \in (x_i y_i)^* x_i$. This implies that z also belongs to the set $\bigcup_{j \in \{1, \dots, k_i\}} (x_{i,j} y_{i,j})^* x_{i,j}$. Therefore,

$$z \in \bigcap_{i \in I} \bigcup_{j \in \{1, \dots, k_i\}} (x_{i,j} y_{i,j})^* x_{i,j}.$$

The case when P has a common outer witness is symmetric. ◀

► **Example 37.** 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 $(abab)^* a$.

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 38.** 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 36, 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 $(ba)^* b \cap (ca)^* c = \emptyset$.

The set $\{(ab, ba), (abab, baba)\}$ has both common inner witnesses

$$(ab)^* a = (ab)^* a \cap ((abab)^* aba \cup (abab)^* a)$$

and common outer witnesses

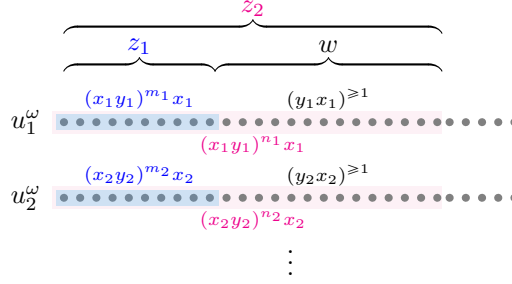
$$(ba)^* b = (ba)^* b \cap ((baba)^* b \cup (baba)^* bab).$$

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

Next we analyse the number of common witnesses a set of primitive pairs can have.

► **Lemma 39.** *The following are equivalent for a conjugate set of primitive pairs P .*

1. P has more than one common witness.



■ **Figure 2** When there are at least two common inner witnesses z_1, z_2 .

2. P has infinitely many common witnesses.
3. P is a singleton set.

Proof. (2) \Rightarrow (1) is obvious. (3) \Rightarrow (1) is straightforward because when a P consists of only one conjugate primitive pair with a cut, say (x, y) , it has inner witnesses x and xyx (in fact $(xy)^*x$). Hence P has more than one witness.

We show (1) \Rightarrow (2) and (1) \Rightarrow (3). Suppose a set of pairs P has two common inner witnesses, say z_1 and z_2 . Since P is a set of primitive pairs, each pair $(u_i, v_i) \in P$ either has a unique cut, denoted as (x_i, y_i) , using Proposition 30 (when $u_i \neq v_i$) or two empty cuts, namely (ϵ, u_i) and (u_i, ϵ) (if $u_i = v_i$). For the latter case, the inner witnesses obtained using cut (ϵ, u_i) is a superset of inner witnesses obtained using (u_i, ϵ) . Hence, we can choose cut $(x_i, y_i) = (\epsilon, u_i)$ for pair (u_i, v_i) when $u_i = v_i$. Therefore, as stated in Proposition 36, both z_1 and z_2 belongs to $\bigcap_{i \in I} (x_i y_i)^* x_i$.

Without loss of generality, assume that $|z_1| < |z_2|$. As depicted in Figure 2, a common factor $w \in \bigcap_{i \in I} (y_i x_i)^{\geq 1}$ exists for each u_i^ω that can be repeated one after another in u_i^ω to get longer and longer common inner witnesses. By symmetry, when P has two common outer witnesses, we get infinitely many common outer witnesses.

Let us assume that the P has a common inner witness z_1 and a common outer witness z_2 , where $z_1 \neq z_2$. For each distinct primitive pair in P , there exists a unique cut. However, for identical primitive pairs, we fix a cut based on the values of z_1 and z_2 . We consider two cases: either $z_1, z_2 \neq \epsilon$, or exactly one of z_1 and z_2 is equal to ϵ .

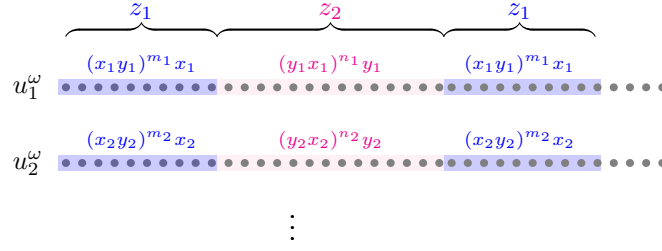
In the case where $z_1, z_2 \neq \epsilon$, for primitive pairs (u_i, v_i) such that $u_i = v_i$, we can choose either of the two empty cuts as (x_i, y_i) , resulting in $z_1 \in (x_i y_i)^* x_i$ and $z_2 \in (y_i x_i)^* y_i$.

In the second case, if $z_1 = \epsilon$, we select the cut $(x_i, y_i) = (\epsilon, u_i)$. This choice ensures that $z_1 \in (x_i y_i)^* x_i$ and $z_2 \in (y_i x_i)^* y_i$ (since $z_2 \neq \epsilon$). Similarly, if $z_2 = \epsilon$, we choose the cut $(x_i, y_i) = (u_i, \epsilon)$.

Consequently, we can conclude that z_1 belongs to $\bigcap_{i \in I} (x_i y_i)^* x_i$ and z_2 belongs to $\bigcap_{i \in I} (y_i x_i)^* y_i$. As shown in Figure 3, concatenating $z_1 \cdot z_2 \cdot z_1$ in u_i^ω , we get one more common inner witness z_3 for P . By the above argument, P has infinitely many common witnesses. This completes the proof of (1) \Rightarrow (2).

In both the cases, we get that $(x_1 y_1)^\omega = (x_2 y_2)^\omega = \dots$ and $(y_1 x_1)^\omega = (y_2 x_2)^\omega = \dots$. Hence from Fine and Wilf Corollary 24, all u_i 's has the same primitive root. Similarly, all v_i 's has the same primitive root. This proves (1) \Rightarrow (3). ◀

For the lemma stated above, it is worth noting that even if we relax the condition that each pair must be primitive, the lemma still holds (Corollary 56). However, the proof of this extended version requires an additional lemma, that is shown later.



■ **Figure 3** When there are 1 common inner witness z_1 and 1 common outer witness z_2 .

If G^* has a common witness, then each pair in G^* has a witness and is conjugate. Hence G^* is conjugate. We prove the converse, namely, if G^* is conjugate, then it has a common witness. To prove this direction, we need the notion of primitive roots of a conjugate set of pairs.

► **Definition 40** (Primitive Root of a Conjugate Set of Pairs). *The primitive root of a conjugate pair (u, v) is the pair (ρ_u, ρ_v) . By Proposition 26, ρ_u is conjugate to ρ_v and there exists an $n \geq 1$ such that $(u, v) = (\rho_u^n, \rho_v^n)$, when u and v are conjugate.*

The primitive root of a conjugate set of pairs $G = \{(u_i, v_i) \mid i \in I\}$, denoted by $R(G)$, is the set of all primitive roots of each pair in G .

$$R(G) = \{(\rho_{u_i}, \rho_{v_i}) \mid i \in I\}.$$

► **Example 41.** $\{(ab, ba), (bab, abb)\}$ is the primitive root of the set $\{(abab, baba), (bab, abb)\}$.

Let G be a conjugate set of pairs. The set $R(G)^*$ is a superset of G^* , but not necessarily the other way round — In the above example, G^* does not contain the set $\{((ab)^n, (ba)^n) \mid n \text{ is odd}\} \subseteq R(G)^*$.

The below theorem characterises conjugacy of a freely generated set of pairs of words.

► **Theorem 42** (Common Witness Theorem for Kleene Closure). *Let G be an arbitrary conjugate set of 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. We prove $(4) \Rightarrow (3) \Rightarrow (2) \Rightarrow (1) \Rightarrow (4)$. The directions $(4) \Rightarrow (3) \Rightarrow (2) \Rightarrow (1)$ is proved for common inner witness; the proof for common outer witness is symmetric. The only nontrivial direction is $(1) \Rightarrow (4)$ that is proved in Section 5. Let $G = \{(u_i, v_i) \mid i \in I\}$ be a conjugate set of pairs.

(4) \Rightarrow (3) Assume $R(G) = \{(\rho_{u_i}, \rho_{v_i}) \mid i \in I\}$ has a common inner witness z . Therefore, z is an inner witness of all pairs in $R(G)$, i.e., $\rho_{u_i} z = z \rho_{v_i}$ for each $i \in I$. From Proposition 34, we obtain z is also an inner witness of powers of (ρ_{u_i}, ρ_{v_i}) . Since each pair $(u_i, v_i) \in G$ is conjugate, from Proposition 26, there exists an $m \geq 1$ such that $(u_i, v_i) = (\rho_{u_i}^m, \rho_{v_i}^m)$. Because $\rho_{u_i}^m z = z \rho_{v_i}^m$, word z is also an inner witness for pair (u_i, v_i) . Thus, G has a common inner witness.

(3) \Rightarrow (2) Suppose there exists a common inner witness z of the set G . Hence $u_i z = z v_i$ for each $i \in I$. Let (u, v) be any arbitrary element from G^* . By definition, $(u, v) =$

$(u_{i_1}u_{i_2}\cdots u_{i_n}, v_{i_1}v_{i_2}\cdots v_{i_n})$ for some $n \geq 1$ and $i_j \in I$ for $j \in \{1, \dots, n\}$. By induction on n , we equate $uz = zv$ as follows.

$$\begin{aligned}
 uz &= u_{i_1} \cdots u_{i_{n-1}} u_{i_n} z \\
 &= u_{i_1} \cdots u_{i_{n-1}} z v_{i_n} && \text{(Since } u_{i_n} z = z v_{i_n} \text{)} \\
 &= z v_{i_1} \cdots v_{i_{n-1}} v_{i_n} && \text{(Inductive Hypothesis)} \\
 &= zv
 \end{aligned}$$

Hence z is a common inner witness of set G^* . Therefore G^* has a common witness.

(2) \Rightarrow (1) Follows from Theorem 25. ◀

► **Corollary 43.** *Let E be a rational expression of pairs. E^* is conjugate if and only if E^* has a common witness.*

Below is an illustration of the common witness theorem for a set of pairs that is not rational.

► **Example 44.** 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^* .

3.2 Common Witness Theorem for Monoid Closure

Next we prove the common witness theorem for monoid closures, i.e., sumfree sets of the form

$$M = (\alpha_0, \beta_0) G_1^* (\alpha_1, \beta_1) G_2^* \cdots (\alpha_{k-1}, \beta_{k-1}) G_k^* (\alpha_k, \beta_k), k \geq 0.$$

where $G_1^*, G_2^*, \dots, G_k^*$ are arbitrary conjugate sets of pairs. We show that such a set is conjugate if and only if it has common witness. Note that this does not generalise to arbitrary sets of pairs, in particular, rational sets using sum.

► **Example 45.** $(ab, ba)^* + (ba, ab)^*$ is an infinite conjugate set that does not have a common witness.

► **Definition 46** (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 (ϵ, ϵ) .*

A singleton redux of M is a set obtained by substituting all but one of the G_i^ 's by (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 $1 \leq i \leq k$.*

► **Example 47.** $M = (a, a)(baa, aba)^*(b, a)(aab, baa)^*(a, b)$ has redux (aba, aab) . 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 and that is in the intersection of the common witnesses of the singleton reduxes of the set.

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

1. M is conjugate.
2. There exist a common witness z of $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$.
3. M has a common witness z_m such that one of the following cases is true:
 - (a) If z is a unique common inner witness of $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$, then M has a unique common witness $z_m = [\alpha_0z, \beta_0]_R = [\alpha_1, z\beta_1]_L$. Moreover, if $|\alpha_0z| \geq |\beta_0|$ or equivalently $|\alpha_1| \leq |z\beta_1|$, then z_m is an inner witness, otherwise it is an outer witness.
 - (b) If z is a unique common outer witness of $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$, then M has a unique common witness $z_m = [\alpha_0, \beta_0z]_R = [z\alpha_1, \beta_1]_L$. Moreover, if $|z\alpha_1| \geq |\beta_1|$ or equivalently $|\alpha_0| \leq |\beta_0z|$, then z_m is an outer witness, otherwise it is an inner witness.
 - (c) If G and $(\alpha_1\alpha_0, \beta_1\beta_0)$ have infinitely many common witnesses, then M is a set of powers of the primitive root of its redux. Thus, M has infinitely many witnesses.

The proof of the above proposition as well as the the proof of the general case below are given in Section 6.

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 are conjugate. From Proposition 48, 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 49** (Common Witness Theorem for Monoid Closure). Let M be a sumfree set. The following are equivalent.

1. M is conjugate.
2. There exists a word z that is a common witness of each of the singleton reduxes.
3. M has a common witness z .

► **Example 50.** Let $M = (\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$ be a sumfree set with one Kleene star where

$$\begin{pmatrix} \alpha_0 \\ \beta_0 \end{pmatrix} = \begin{pmatrix} ab \\ b \end{pmatrix}, G = \left\{ \begin{pmatrix} bab \\ abb \end{pmatrix} \right\}, \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} b \\ ab \end{pmatrix}.$$

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 48 (c), M is a set of powers of the primitive root of the redux, i.e., $M = (abb, bab)^+$. Therefore, M has infinitely many witnesses same as those of (abb, bab) .

► **Example 51.** 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

$$\begin{pmatrix} \alpha_0 \\ \beta_0 \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}, G_1 = \left\{ \begin{pmatrix} ac \\ ca \end{pmatrix} \right\}, \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} ab \\ b \end{pmatrix}, G_2 = \left\{ \begin{pmatrix} bab \\ bab \end{pmatrix} \right\}, \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \epsilon \\ b \end{pmatrix}.$$

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,

$$M_1 = \begin{pmatrix} \alpha_0 \\ \beta_0 \end{pmatrix} G_1^* \begin{pmatrix} \alpha_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} \begin{pmatrix} ac \\ ca \end{pmatrix}^* \begin{pmatrix} ab \\ bb \end{pmatrix}$$

and,

$$M_2 = \begin{pmatrix} \alpha_0\alpha_1 \\ \beta_0\beta_1 \end{pmatrix} G_2^* \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} bab \\ ab \end{pmatrix} \begin{pmatrix} bab \\ bab \end{pmatrix}^* \begin{pmatrix} \epsilon \\ b \end{pmatrix}.$$

The set $G_1 \cup \{(\alpha_1\alpha_2\alpha_0, \beta_1\beta_2\beta_0)\} = \{(ac, ca)\} \cup \{(abb, bba)\} = \{(ac, ca), (abb, bba)\}$ has a unique common inner witness, say $z_1 = a = (ac)^*a \cap (abb)^*a$ and no common outer witness since $(ca)^*c \cap (bba)^*bb = \emptyset$. By Proposition 48 (a), the unique common inner witness of the singleton redux M_1 of M is $[\alpha_0z_1, \beta_0] = [ba, a]_R = b$.

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 set of powers of the primitive root of the redux using Proposition 48 (c), i.e., $M_2 = (bab, abb)^+$. Thus M_2 have infinitely many common inner witnesses $(bab)^*b$ and common outer witnesses $(abb)^*ab$.

By Theorem 49, 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 Auxillary Results for Case Analysis

For proving common witness theorems, we require a detailed case analysis. To ease the analysis, we establish two lemmas, namely, the *Cut Lemma* and the *Equal Length Lemma*.

4.1 Cut Lemma and its Corollaries

Simply stated, the content of the cut lemma is that a primitive word cannot be equal to any of its nontrivial cyclic shifts, i.e., $u \neq lshift_i(u)$, $1 \leq i < |u|$ for any primitive word u . However, the statement of the lemma is given in a fashion that is suitable for case analysis.

► **Lemma 52** (Cut Lemma). *Assume (u, v) is a conjugate primitive pair.*

I. *If (u, v) is a distinct pair with the unique cut (x, y) , then the following equalities cannot hold for any nonempty words x', x'', y', y'' such that $x = x'x''$ and $y = y'y''$.*

- (a) $xy = x''yx'$
- (b) $xy = y''xy'$
- (c) $yx = y''xy'$
- (d) $yx = x''yx'$
- (e) $xy = yx$

II. *In the special case when $u = v$, there are two empty cuts (u, ϵ) and (ϵ, u) . In both cases, the equality $u = u''u'$ cannot hold for any nonempty words u', u'' such that $u = u'u''$.*

Proof. Consider the case when (u, v) is a distinct pair with the unique nonempty cut (x, y) . It suffices to show that if any of the equalities hold, there exists a different nonempty cut of the primitive pair (u, v) contradicting Proposition 30.

1. In the case of I. (a), the other nonempty cut is (x'', yx') since $(xy, yx) = (x''yx', yx'x'')$.
2. In the case of I. (b), the other nonempty cut is $(y''x, y')$ since $(xy, yx) = (y''xy', y'y''x)$.
3. When I. (c) is true, we obtain a different nonempty cut (xy', y'') because $(xy, yx) = (xy'y'', y''xy')$.
4. If I. (d) holds, the other nonempty cut is $(x', x''y)$ since $(xy, yx) = (x'x''y, x''yx')$.
5. If I. (e) holds, the other nonempty cut is (y, x) since $(xy, yx) = (yx, xy)$ and $x \neq y$ (since $u \neq v$).

Consider the special case when $u = v$. If the equality $u = u''u'$ holds, then we obtain $u = u'u'' = u''u'$. Therefore, u' and u'' commutes. Since u' and u'' are nonempty words, u is a power of some smaller word using Theorem 20. Hence u is not primitive and it is a contradiction. ◀

In the rest of the subsection we discuss a number of consequences of Cut Lemma. The following proposition conveys that the cut of the primitive root decides the cuts of its power.

► **Proposition 53.** *Let (u, v) is a distinct conjugate primitive pair with the unique cut (x, y) . Any cut of the pair (u^n, v^n) for $n \geq 1$ is of the form $((xy)^*x, (yx)^*y)$.*

Proof. Let $(u', v') = (u^n, v^n)$ for some $n \geq 1$. The lemma is trivially true for $n = 1$ by the uniqueness of cut of primitive pairs by Proposition 30.

Consider the case when $n \geq 2$. Substituting for $u = xy$ and $v = yx$ in u' and v' ,

$$u' = \overbrace{u \cdots u}^{n \text{ times}} = xy \cdots xy$$

$$v' = v \cdots v = yx \cdots yx$$

We show that cut in u' will always be at the end of some x and all other cases leads to one of Cases I. (a) to I. (e) of Cut Lemma.

Case 1: When the cut is at the end of y

I.e., there exists a cut (p, q) for (u', v') such that $p \in (xy)^+$. Then

$$u' = \overbrace{xy \cdots xy}^p \overbrace{xy \cdots xy}^q \quad (5)$$

$$v' = yx \cdots yxyx \cdots yx = qp = \overbrace{xy \cdots xy}^q \overbrace{xy \cdots xy}^p \quad (6)$$

Equating the suffixes of v' of length $|xy|$ in both side of the Equation (6), we deduce $xy = yx$, i.e., $u = v$. It satisfies Case I. (e) of Cut Lemma. Hence a contradiction.

Case 2: When the cut is strictly within some x or y

We will make a further case analysis: when there is an xy present before the cut, and when there is an xy present after the cut (since $n \geq 2$).

Suppose the cut in u' is in the i^{th} xy for $i > 1$, i.e., there is an xy present before the cut.

1. When the cut is within x , i.e., there exists a cut (p, q) of (u', v') such that $p \in (xy)^+x'$ where x' is a nonempty proper prefix of x and $x = x'x''$ for some word x'' . Now,

$$u' = \cdots \overbrace{x'x''yx'}^p \overbrace{x''y \cdots}^q \quad (7)$$

$$v' = yx'x'' \cdots yx'x'' = qp = \overbrace{x''y \cdots}^q \overbrace{x'x''yx'}^p \quad (8)$$

As before, equating the suffixes of v' of length $|xy|$ on both sides of Equation (8), we obtain

$$yx = yx'x'' = x''yx'$$

Here x' and x'' satisfies Case I. (d) of Cut Lemma. Hence a contradiction.

2. When the cut is within y , i.e., there exists a cut (p, q) of (u', v') such that $p \in (xy)^+xy'$ where y' is a nonempty prefix of y and $y = y'y''$ for some word y'' . Then,

$$u' = \cdots \overbrace{xy'y''xy'}^p \overbrace{y'' \cdots}^q \quad (9)$$

$$v' = y'y''x \cdots y'y''x = qp = \overbrace{y'' \cdots}^q \overbrace{xy'y''xy'}^p \quad (10)$$

On both sides of the Equation (10), equating the suffixes of v' of length $|xy|$, we get

$$yx = y'y''x = y''xy'$$

that is Case I. (c) of **Cut Lemma**. Hence a contradiction.

The case when there is an xy after the cut is symmetric and leads to Cases I. (a) and I. (b) of **Cut Lemma**.

Since we have eliminated all of other scenarios, the only possible cuts of the pair (u', v') are of the form $((xy)^*x, (yx)^*y)$. ◀

Using Proposition 53, we relate the witnesses of a pair and its primitive root.

► **Proposition 54.** *Let (u, v) be a conjugate pair with the primitive root (ρ_u, ρ_v) . The following are equivalent for a word z .*

1. z is a witness of (u, v) .
2. z is a witness of (ρ_u, ρ_v) .

Proof. From Proposition 34, we get $(2) \Rightarrow (1)$.

Next we prove $(1) \Rightarrow (2)$. From Proposition 26, if (u, v) is conjugate then (ρ_u, ρ_v) is conjugate as well. In the case where $u = v$, it follows that $\rho_u = \rho_v$. Consequently, any witness z for the pair (u, v) belongs to the set u^* that is a subset of ρ_u^* . Thus, z serves as a witness for the pair (ρ_u, ρ_v) as well, since ρ_u^* consists of witnesses for (ρ_u, ρ_v) .

Consider the case when $u \neq v$. It follows that $\rho_u \neq \rho_v$. According to Proposition 30, the pair (ρ_u, ρ_v) has a unique cut, denoted as (x, y) . From Proposition 53, all cuts of (u, v) are of the form $((xy)^*x, (yx)^*y)$. From Theorem 25, an inner witness of (u, v) belongs to

$$((xy)^*x(yx)^*y)^*(xy)^*x = (xy)^*x$$

and hence is an inner witness of (ρ_u, ρ_v) . The proof for outer witness is symmetric. ◀

From the above theorem we get the following corollary for a set of pairs of words.

► **Corollary 55.** *A set of pairs G has a common-witness z if and only if $R(G)$ has a common-witness z .*

Proof. We proved (\leftarrow) in $(4) \Rightarrow (3)$ of Theorem 42. Next we prove the direction (\rightarrow) . Let z be a common witness of the set G . For any arbitrary pair $(u, v) \in G$, z is a witness of (u, v) . From Proposition 54, z is also a witness for its primitive root. Since each pair in $R(G)$ is a primitive root of some pair in G , all pairs in $R(G)$ have z as a witness. Therefore, z is a common witness for $R(G)$. ◀

Using above corollary, we can extend Lemma 39 for a set of pairs of words (not necessarily primitive pairs).

► **Corollary 56.** *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. All the pairs in G have the same primitive root.

Proof. (2) \Rightarrow (1) is obvious. We show (3) \Rightarrow (1). If each pair in G is a power of a same primitive root, then $R(G)$ is a singleton set. Lemma 39 implies that $R(G)$ has infinitely many common witnesses. This implies G has infinitely many common witnesses using Corollary 55.

Now it suffices to show (1) \Rightarrow (2) and (1) \Rightarrow (3). If the set G has two common witnesses, namely z_1 and z_2 , then according to Corollary 55, z_1 and z_2 are also common witnesses of $R(G)$. Since $R(G)$ has more than one common witness, it follows that $R(G)$ is a singleton set by Lemma 39. Hence it has infinitely many common witnesses. Additionally, since witnesses of $R(G)$ are also witnesses of G (as per Corollary 55), it implies that G itself has infinitely many common witnesses. \blacktriangleleft

4.2 Equal Length Lemma

Equal length lemma can be summarised as follows: Let $G = \{(u_1, v_1), \dots, (u_k, v_k)\}$, $k > 1$ be a set of conjugate primitive pairs of *identical length*, i.e., $|u_1| = \dots = |u_k|$. If G^* is conjugate then either $x_1 = \dots = x_k$ or $y_1 = \dots = y_k$ where (x_i, y_i) is a cut of (u_i, v_i) for $1 \leq i \leq k$ (Proposition 58).

► **Lemma 57 (Equal Length Lemma).** *Let $(u_1, v_1), (u_2, v_2)$ be two conjugate primitive pairs of equal length (i.e., $|u_1| = |u_2|$) and let (x_1, y_1) and (x_2, y_2) be their unique cuts respectively. Any pair $(u_1, v_1)^{\ell_1} (u_2, v_2)^{\ell_2}$ where $\ell_2 \gg \ell_1 > 2$, is conjugate only if either $x_1 = x_2$ or $y_1 = y_2$.*

Proof. Let $(u, v) = (u_1, v_1)^{\ell_1} (u_2, v_2)^{\ell_2}$ such that $\ell_1 > 2$ and $\ell_2 \gg \ell_1$ ($\ell_2 > \ell_1 + 2$ suffices).

$$\begin{aligned} u &= \underbrace{u_1 \cdots u_1}_{\ell_1 \text{ times}} \underbrace{u_2 u_2 \cdots u_2 u_2}_{\ell_2 \text{ times}} \\ v &= v_1 \cdots v_1 v_2 v_2 \cdots v_2 v_2 \end{aligned}$$

If (u, v) is conjugate, then they have a cut say (p, q) . There are two possibilities for a cut of (u, v) : when the cut in u is within $u_1^{\ell_1} u_2$ or it is after $u_1^{\ell_1} u_2$.

In both the cases we show that either $x_1 = x_2$, or $y_1 = y_2$ or both.

Case 1: When the cut in u is within $u_1^{\ell_1} u_2$

In this case, the cut in v is within the suffix $v_2^{\ell_1+1}$ since the $|u_1| = |u_2| = |v_2|$ and $\ell_2 \gg \ell_1$. Substituting (u_1, v_1) and (u_2, v_2) with $(x_1 y_1, y_1 x_1)$ and $(x_2 y_2, y_2 x_2)$,

$$\begin{aligned} u &= x_1 y_1 \cdots x_1 y_1 x_2 y_2 \cdots x_2 y_2 = pq \\ v &= y_1 x_1 \cdots y_1 x_1 \cdots y_2 x_2 \underbrace{y_2 x_2}_{\text{cut region}} \cdots = qp \end{aligned}$$

Since $\ell_2 \gg \ell_1$, there exist atleast one $y_2 x_2$ before the cut in v . We compare the suffixes of q in both u and v . Since q ends with $x_2 y_2$ in u , the cut in v should be at the end of a y_2 by Cases I. (a), I. (b), I. (e) and II. of Cut Lemma.

Hence p can be of the form x_2 or $(x_2 y_2)^+ x_2$ depending upon if the cut in v is within the last $y_2 x_2$ or not.

$$\begin{aligned} u &= x_1 y_1 \cdots x_1 y_1 x_2 y_2 \cdots x_2 y_2 = pq \\ v &= \underbrace{y_1 x_1 \cdots y_1 x_1 \cdots y_2 x_2 y_2}_q \underbrace{x_2 \cdots}_p \end{aligned}$$

Suppose $p \in (x_2y_2)^+x_2$, then equating the prefixes of p in u and v of length $|x_2y_2| = |x_1y_1|$ (Since $|u_1| = |u_2|$), we obtain $x_2y_2 = x_1y_1$. Substituting this in u ,

$$\begin{aligned} u &= x_1y_1 \cdots x_1y_1x_1y_1 \cdots x_1y_1 = pq \\ v &= \underbrace{y_1x_1 \cdots y_1x_1 \cdots y_2x_2y_2}_q \underbrace{x_2y_2 \cdots x_2}_p \end{aligned}$$

Now we compare the prefixes of q in u and v . Since q starts with y_1x_1 in v , from Cases **I. (c)**, **I. (d)**, **I. (e)** and **II. of Cut Lemma**, the cut in u should be at the end of x_1 . Therefore, $p \in (x_1y_1)^+x_1$ in u . Also, $p \in (x_2y_2)^+x_2$ in v . Since $|x_1y_1| = |x_2y_2|$ and $|x_1|, |x_2| < |x_1y_1|$, we can deduce $p = (x_1y_1)^ix_1 = (x_2y_2)^ix_2$ for some i . Hence, $x_1 = x_2$. Therefore, it implies $y_1 = y_2$ since $x_1y_1 = x_2y_2$ and hence, (u_1, v_1) and (u_2, v_2) are identical.

Suppose $p = x_2$ in v . Here, p in u is within the first x_1y_1 since $|x_1y_1| = |x_2y_2|$. Moreover $p = x_1$ since the only possible cut in u will be at the end of x_1 by Cases **I. (c)**, **I. (d)**, **I. (e)** and **II. of Cut Lemma** (comparing the prefixes of q in u and v). Hence $x_1 = x_2$.

Case 2: Cut in u is after $u_1^{\ell_1}u_2$

This case is symmetric. For the sake of completeness we prove it.

Substituting (u_1, v_1) and (u_2, v_2) with (x_1y_1, y_1x_1) and (x_2y_2, y_2x_2) ,

$$\begin{aligned} u &= x_1y_1 \cdots x_1y_1 \cdots x_2y_2 \overbrace{x_2y_2}^{\text{cut region}} \cdots = pq \\ v &= y_1x_1 \cdots y_1x_1y_2x_2 \cdots y_2x_2 = qp \end{aligned}$$

Note that there is at least one x_2y_2 before the cut. We compare the suffixes of p in u and v . Since p ends with y_2x_2 in v , the cut in u should be at the end of x_2 by Cases **I. (c)**, **I. (d)**, **I. (e)** and **II. of Cut Lemma**.

$$\begin{aligned} u &= \underbrace{x_1y_1 \cdots x_1y_1 \cdots x_2y_2x_2}_p \underbrace{\cdots y_2}_q \\ v &= y_1x_1 \cdots y_1x_1y_2x_2 \cdots y_2x_2 = qp \end{aligned}$$

Hence q is of the form y_2 or $(y_2x_2)^+y_2$ depending upon if the cut in u is within the last x_2y_2 or not.

If $q \in (y_2x_2)^+y_2$, then comparing the prefixes of q of length $|y_2x_2| = |y_1x_1|$ (Since $|v_1| = |v_2|$) in u and v , we obtain $y_2x_2 = y_1x_1$. Substituting this in v ,

$$\begin{aligned} u &= \underbrace{x_1y_1 \cdots x_1y_1 \cdots x_2y_2x_2}_p \underbrace{\cdots y_2}_q \\ v &= y_1x_1 \cdots y_1x_1y_1x_1 \cdots y_1x_1 = qp \end{aligned}$$

We compare the prefixes of p in u and v . Since p starts with x_1y_1 in u , the cut in v should be at the end of y_1 using Cases **I. (a)**, **I. (b)**, **I. (e)** and **II. of Cut Lemma**. Therefore, $q \in (y_1x_1)^+y_1$ in v and $q \in (y_2x_2)^+y_2$ in u . Hence, as before we can deduce that $y_1 = y_2$. It also implies $x_1 = x_2$ since $y_1x_1 = y_2x_2$ and thus (u_1, v_1) and (u_2, v_2) are identical.

If $q = y_2$. The cut in v is within first y_1x_1 . In fact, $q = y_1$ since the only possible cut in u will be at the end of y_1 by Cases **I. (a)**, **I. (b)**, **I. (e)** and **II. of Cut Lemma** (comparing the prefixes of p in u and v). Hence $y_1 = y_2$. ◀

Using Equal Length Lemma we characterise the conjugacy of the closure of a set of conjugate primitive pairs of equal length.

► **Proposition 58.** *Let G be a set of conjugate pairs such that all pairs in $R(G)$ are of equal length pairs. Let (x_i, y_i) be the unique cut of the primitive pair $(u_i, v_i) \in R(G)$. If G^* is conjugate then either $x_1 = x_2 = \dots$ or $y_1 = y_2 = \dots$.*

Proof. Proof is by induction on the number of pairs in $R(G)$.

1. *Base Case:* When $R(G)$ has only 2 pairs, i.e., $R(G) = \{(u_1, v_1), (u_2, v_2)\}$. There exist ℓ_1, ℓ_2 such that $\ell_2 \gg \ell_1 > 2$ and $(u_1, v_1)^{\ell_1} (u_2, v_2)^{\ell_2} \in G^*$ and hence it is conjugate. From **Equal Length Lemma** we get either $x_1 = x_2$ or $y_1 = y_2$.
2. *Inductive Case:* Let us assume that the statement is true for k equal length pairs in $R(G)$, i.e., $R(G) = \{(u_1, v_1), \dots, (u_k, v_k)\}$. By induction hypothesis, G^* is conjugate only if $x_1 = \dots = x_k$ or $y_1 = \dots = y_k$. WLOG, assume $x_1 = \dots = x_k$. We aim to prove for $k+1$ pairs. Let $G' \supseteq G$ be such that G'^* is conjugate and $R(G') = R(G) \cup \{(u_{k+1}, v_{k+1})\}$ where (u_{k+1}, v_{k+1}) is a conjugate primitive pair of identical length to that of pairs in $R(G)$. Let (x_{k+1}, y_{k+1}) be the cut of (u_{k+1}, v_{k+1}) . There exists the set of pairs

$$\{(u_i, v_i)^{\ell_i} (u_{k+1}, v_{k+1})^{\ell_{k+1}} \mid \ell_{k+1} \gg \ell_i > 2, 1 \leq i \leq k\} \subset G'^*$$

that is conjugate. Therefore, the pairs (u_i, v_i) and (u_{k+1}, v_{k+1}) satisfy either $x_i = x_{k+1}$ or $y_i = y_{k+1}$ by **Equal Length Lemma**. There are two cases:

- (a) Suppose there exist an i such that $x_i = x_{k+1}$. Since $i \in \{1, \dots, k\}$ and $x_1 = \dots = x_k$, we conclude $x_1 = \dots = x_k = x_{k+1}$ as required.
- (b) Otherwise $y_i = y_{k+1}$ for all i . Then it follows that $y_1 = \dots = y_k = y_{k+1}$.

◀

5 Existence of Common Witness for Kleene Closure

In this section, we prove the direction (1) \Rightarrow (4) of Theorem 42 recalled in the following lemma.

► **Lemma 59.** *For a set of pairs G , if G^* is conjugate then $R(G)$ has a common witness.*

We prove the lemma when G is finite by case analysis and then extend it for a countably infinite set of pairs using a compactness argument.

5.1 For a Finite Set of Pairs

We now prove the common witness theorem for a finite set.

► **Lemma 60.** *Let G be a finite set of k pairs. If G^* is conjugate then $R(G)$ as well G has a common witness.*

Proof. When $k = 1$, G has only one pair (u, v) and by assumption it is conjugate. By Theorem 25, (u, v) has a witness. From Proposition 54, we obtain that the witnesses of $R(G) = \{(\rho_u, \rho_v)\}$ are same as that of (u, v) .

Next we assume that $k > 1$. Let \approx be the equivalence relation on G whereby $(u, v) \approx (u', v')$ if $\rho_u \sim \rho_{u'}$, i.e., the primitive roots of the pairs are conjugates. Assume that \approx has d equivalence classes. Clearly $1 \leq d \leq k$. We do a cases analysis on whether $d = 1$ or otherwise.

If \approx has only one equivalence class, then the primitive roots of all the pairs in G are conjugates. Consequently, their lengths are identical. Since G^* is conjugate and all the pairs in $R(G)$ have identical lengths, by Proposition 58, $R(G)$ has a common witness.

Now we assume that $d > 1$. Choose d pairs $(u_1, v_1), (u_2, v_2), \dots, (u_d, v_d)$ from each equivalence class. We construct a pair $(u, v) \in (u_1, v_1)^* (u_2, v_2)^* \cdots (u_d, v_d)^* \subseteq G^*$ and show that (u, v) is conjugate only if $R(G)$ has a common witness.

Let m be the least common multiple of $|u_1|, \dots, |u_d|$. Let $\ell_{ij} = |u_i| + |u_j| - \gcd(|u_i|, |u_j|) > 0$ for $1 \leq i, j \leq d$ and $i \neq j$. Let $\ell = \max \{\ell_{ij} \mid 1 \leq i, j \leq d, i \neq j\}$. Let N be a multiple of m that is $> 2\ell$.

Let $(u, v) = (u_1, v_1)^{j_1} (u_2, v_2)^{j_2} \cdots (u_d, v_d)^{j_d}$ such that $j_1, \dots, j_d > 2$ and $|u_i^{j_i}| = N$ for each $1 \leq i \leq d$.

$$\begin{aligned} u &= \overbrace{u_1 \cdots u_1}^N \overbrace{u_2 \cdots u_2}^N \cdots \overbrace{u_d \cdots u_d}^N \\ v &= v_1 \cdots v_1 v_2 \cdots v_2 \cdots v_d \cdots v_d \end{aligned}$$

Since (u, v) is conjugate, it has a cut, say (p, q) . Substituting each pair in (u, v) with their primitive roots, we get

$$\begin{aligned} u &= \rho_{u_1} \cdots \rho_{u_1} \rho_{u_2} \cdots \rho_{u_2} \cdots \rho_{u_d} \cdots \rho_{u_d} = pq \\ v &= \rho_{v_1} \cdots \rho_{v_1} \rho_{v_2} \cdots \rho_{v_2} \cdots \rho_{v_d} \cdots \rho_{v_d} = qp \end{aligned}$$

Let (x_i, y_i) be the unique cut of (ρ_{u_i}, ρ_{v_i}) for $1 \leq i \leq d$. Let B_1, B_2, \dots, B_d represent the blocks in u , and let B'_1, B'_2, \dots, B'_d represent the blocks in v .

The cut in u can be either within the first block B_1 , or the last block B_d , or anywhere between the first and the last blocks in u . We do a case analysis on all the possible cuts of (u, v) and show that there exists a common witness of $R(G)$ in each of the cases.

Case 1: When the cut in u is in the first block B_1

We make a further case analysis depending upon if the cut is within the first half or the second half of the first block.

Suppose the cut in u is within the first half of the block, i.e., p is of length at most $N/2$. In this case, since the length of each block are equal, the cut in v is within the second half of the last block B'_d , i.e., p is a suffix of v of length at most $N/2$.

$$\begin{aligned} u &= \overbrace{\rho_{u_1} \cdots \rho_{u_1}}^p \overbrace{\rho_{u_1} \rho_{u_2} \cdots \rho_{u_2} \cdots \rho_{u_d} \cdots \rho_{u_d}}^q \\ v &= \underbrace{\rho_{v_1} \cdots \rho_{v_1} \rho_{v_2} \cdots \rho_{v_2} \cdots \rho_{v_d} \cdots \rho_{v_d}}_q \underbrace{\rho_{v_d}}_p \end{aligned}$$

We obtain

$$q = p^{-1}(B_1 B_2 \cdots B_d) = (B'_1 B'_2 \cdots B'_d) p^{-1}.$$

▷ **Claim 61.** The following holds for each $1 \leq i \leq d$.

1. B_i is of the form pq_i and B'_i is of the form $q_i p$, and
2. p is of the form $(x_i y_i)^{m_i} x_i$ and q_i is of the form $(y_i x_i)^{m_i} y_i$ for some $m_i \geq 0$.

Proof. Proof is by induction on i .

1. *Base Case:* when $i = 1$. We compare the prefixes of q in u and v . Since $|p| \leq N/2$, the prefix of q in u must begin within the first block B_1 . Also, there must be at least one

occurrence of the factor $\rho_{u_1} = x_1 y_1$ following the cut. Since q in v starts with $\rho_{v_1} = y_1 x_1$, the cut should be at the end of x_1 by Cases **I. (c)**, **I. (d)**, **I. (e)** and **II.** of **Cut Lemma**. Hence $p = (x_1 y_1)^{m_1} x_1$ for some integer $m_1 \geq 0$. Consequently, the prefix of q in the block B_1 , denoted as q_1 , is of the form $y_1 (x_1 y_1)^{n_1}$, for some $n_1 > 0$. After matching q_1 in v , we observe that a factor equal to p appears in the suffix of the block B'_1 , as shown below.

$$\begin{aligned} u &= \overbrace{(x_1 y_1)^{m_1} x_1}^p \overbrace{y_1 (x_1 y_1)^{n_1}}^{q_1} \overbrace{\rho_{u_2} \cdots \rho_{u_2} \cdots \rho_{u_d} \cdots \rho_{u_d}}^{q_1^{-1} q} \\ v &= \underbrace{y_1 (x_1 y_1)^{n_1}}_{q_1} \underbrace{(x_1 y_1)^{m_1} x_1}_{=p} \rho_{v_2} \cdots \rho_{v_2} \cdots \rho_{v_d} \cdots \rho_{v_d} = qp \end{aligned}$$

2. *Inductive Case:* Assume the claim is true for first i blocks where $1 \leq i < k$.

$$\begin{aligned} u &= \overbrace{(x_1 y_1)^{m_1} x_1}^p \overbrace{y_1 (x_1 y_1)^{n_1}}^{q_1} \cdots \overbrace{(x_i y_i)^{m_i} x_i}^p \overbrace{y_i (x_i y_i)^{n_i}}^{q_i} \overbrace{\rho_{u_{i+1}} \cdots \rho_{u_{i+1}} \cdots \rho_{u_d} \cdots \rho_{u_d}}^{q'' = (q_1 p \cdots q_{i-1} p q_i)^{-1} q} = pq \\ v &= \underbrace{y_1 (x_1 y_1)^{n_1}}_{q_1} \underbrace{(x_1 y_1)^{m_1} x_1}_p \cdots \underbrace{y_i (x_i y_i)^{n_i}}_{q_i} \underbrace{(x_i y_i)^{m_i} x_i}_p \rho_{v_{i+1}} \cdots \rho_{v_{i+1}} \cdots \rho_{v_d} \cdots \rho_{v_d} = qp \end{aligned}$$

Let q'' denote the remaining suffix of q in u after the i -th block B_i . We obtain $q'' = (q_1 p \cdots q_{i-1} p q_i)^{-1} q$. By comparing the prefixes of q'' in u and v , we get that the suffix of the block B'_i in v , that is equal to p , matches within the first half of the block B_{i+1} in u since $|p| < N/2$. Moreover, the matching should end at x_{i+1} by Cases **I. (c)**, **I. (d)**, **I. (e)** and **II.** of **Cut Lemma**. Hence $p = (x_{i+1} y_{i+1})^{m_{i+1}} x_{i+1}$ for some integer $m_{i+1} \geq 0$. Consequently, the remaining suffix of the block B_{i+1} , denoted by q_{i+1} , is of the form $(y_{i+1} x_{i+1})^{n_{i+1}} y_{i+1}$ for some integer $n_{i+1} > 0$. After matching q_{i+1} in B'_{i+1} , we observe that a factor equal to p appears in the suffix of the block B'_{i+1} . Hence, $B_{i+1} = p q_{i+1}$ and $B'_{i+1} = q_{i+1} p$.

◀

From the above claim, it follows that $q = q_1 p q_2 p \cdots p q_d$ and

$$p = (x_1 y_1)^{m_1} x_1 = (x_2 y_2)^{m_2} x_2 = \cdots = (x_d y_d)^{m_d} x_d$$

for $m_1, \dots, m_d \geq 0$. Since above equation holds for any two pairs between the equivalence classes, from Proposition 36 we obtain p is a common inner witness of $R(G)$.

Next we assume the cut in u is in the second half of B_1 . We compare the prefixes of q in u and v and deduce that there exist a common factor of length at least $N/2 > \ell > \ell_{12}$ between block B'_1 and block B_2 . From Theorem 27, ρ_{v_1} is conjugate to ρ_{u_2} , that is in turn is conjugate to ρ_{v_2} . From transitivity of conjugacy, ρ_{v_1} is conjugate to ρ_{v_2} , which contradicts the fact that (u_1, v_1) and (u_2, v_2) belong to different equivalence classes. Hence cut in second half of B_1 is not possible.

Case 2: When the cut in u is in the last block B_d

We make a further case analysis depending upon if the cut in u is in the first half or second half of the last block B_d . The proof is symmetric to that of the previous case.

Suppose the cut in u is within the suffix of the block B_d of length $N/2$.

$$\begin{aligned} u &= \overbrace{\rho_{u_1} \cdots \rho_{u_1} \rho_{u_2} \cdots \rho_{u_2} \cdots \rho_{u_d} \cdots}^p \overbrace{\cdots \rho_{u_d}}^q \\ v &= \underbrace{\rho_{v_1} \cdots}_{q} \underbrace{\rho_{v_1} \rho_{v_2} \cdots \rho_{v_2} \cdots \rho_{v_d} \cdots \rho_{v_d}}_p \end{aligned}$$

Consider the pair (u^r, v^r) , where u^r, v^r are the reverses of the words u and v respectively. Since (u, v) is conjugate with the cut (p, q) , from Proposition 31 we obtain that the pair (u^r, v^r) is also conjugate with cut (q^r, p^r) .

$$\begin{aligned} u^r &= \overbrace{\rho_{u_d}^r \cdots \rho_{u_d}^r \rho_{u_{d-1}}^r \cdots \rho_{u_{d-1}}^r}^{q^r} \cdots \overbrace{\rho_{u_1}^r \cdots \rho_{u_1}^r}^{p^r} \\ v^r &= \overbrace{\rho_{v_d}^r \cdots \rho_{v_d}^r \rho_{v_{d-1}}^r \cdots \rho_{v_{d-1}}^r}^{p^r} \cdots \overbrace{\rho_{v_1}^r \cdots \rho_{v_1}^r}^{q^r} \end{aligned}$$

Since (x_i, y_i) is the unique cut of (ρ_{u_i}, ρ_{v_i}) , from Proposition 31 and Proposition 19, we get that the unique cut of $(\rho_{u_i}^r, \rho_{v_i}^r)$ is (y_i^r, x_i^r) for $1 \leq i \leq k$.

This reduces to Case 1 where the cut in u^r is in the first half of the first block. Therefore, there exist integers $m_1, m_2, \dots, m_k \geq 0$ such that

$$q^r = (y_1^r x_1^r)^{m_1} y_1^r = (y_2^r x_2^r)^{m_2} y_2^r = \cdots = (y_d^r x_d^r)^{m_k} y_d^r.$$

Since $((y_i^r x_i^r)^{m_i} y_i^r)^r = (y_i x_i)^{m_i} y_i$, we obtain

$$q = (y_1 x_1)^{m_1} y_1 = (y_2 x_2)^{m_2} y_2 = \cdots = (y_d x_d)^{m_d} y_d.$$

From the above equation, that is valid for any two pairs belonging to the equivalence classes, we can deduce from Proposition 36 that q is a common outer witness of $R(G)$.

Next assume that the cut in u is in the first half of the last block B_k . We compare the suffixes of p in u and v and deduce that there exist a common factor of length at least $N/2 > \ell > \ell_{(d-1)d}$ between the block B_{d-1} and the block B'_d . As before, from Theorem 27, ρ_{v_d} is conjugate to $\rho_{u_{d-1}}$, that is in turn conjugate to $\rho_{v_{d-1}}$. Since conjugacy is transitive, this implies that ρ_{v_d} is conjugate to $\rho_{v_{d-1}}$, which contradicts the fact that (u_d, v_d) and (u_{d-1}, v_{d-1}) belong to different equivalence classes. Therefore, the cut in first half of B_d is not possible.

Case 3: When the cut in u is within the block B_j for $1 < j < d$

WLOG, assume that the cut in u is within the first half of the block B_j . In this case the cut in v will be within the second half of the block B_{d-j+1} .

$$\begin{aligned} u &= \overbrace{\rho_{u_1} \cdots \rho_{u_1} \cdots \rho_{u_j} \cdots}^p \cdots \overbrace{\rho_{u_j} \cdots \rho_{u_d} \cdots \rho_{u_d}}^q \\ v &= \overbrace{\rho_{v_1} \cdots \rho_{v_1} \cdots \rho_{v_{d-j+1}} \cdots}^q \cdots \overbrace{\rho_{v_{d-j+1}} \cdots \rho_{u_d} \cdots \rho_{u_d}}^p \end{aligned}$$

By matching q in u and v , we get ρ_{v_1} and ρ_{u_j} shares a common factor of length at least $N/2 > \ell > \ell_{1j}$ and hence they are conjugates to each other by Theorem 27. Since ρ_{u_j} is conjugate to ρ_{v_j} , by transitivity of conjugacy we obtain ρ_{v_1} and ρ_{v_j} are conjugates. This contradicts the fact that (u_1, v_1) and (u_j, v_j) belongs to different equivalence classes. Hence cut in B_j where $1 < j < d$ is not possible.

Hence, for a finite set of pairs G , G^* is conjugate only if $R(G)$ has a common witness. By Corollary 55, we also conclude that G has a common witness. \blacktriangleleft

Hence, we proved Lemma 59 for the finite case.

5.2 For an Infinite Set of Pairs

We now extend Lemma 59 from a finite set to an infinite set of pairs.

► **Lemma 62** (Compactness Theorem). *Let G be an infinite set of pairs. If every finite subset of G has a common witness, then G has a common witness.*

Proof. From Corollary 56, if a set has a witness, it has exactly one common witness or infinitely many common witnesses. Given that every finite subset of G has a common witness, there are two possible cases: a finite subset of G with a unique witness exists, or every finite subset of G has infinitely many witnesses.

1. Assume that there exists a finite subset G_f of G with exactly one common witness, say z . We claim that z is a common witness of G as well. By assumption, the finite set $G_f \cup \{(u, v)\}$ has a common witness, for any pair $(u, v) \in G$. Moreover, the witness for this set must be z ; otherwise, it contradicts the uniqueness of the witness of G_f . This implies that z is a witness for any pair in G . Hence z is a common witness of G .
2. Next we assume that every finite subset of G has infinitely many common witnesses. Take any pair (u_i, v_i) and (u_j, v_j) from G . The set $\{(u_i, v_i), (u_j, v_j)\}$ is a finite set with infinitely many witnesses by assumption. Therefore, from Corollary 56, both (u_i, v_i) and (u_j, v_j) have the same primitive root. Since primitive roots are unique by Corollary 21, the primitive root of every pair in G is the same. From Proposition 54, the witnesses of the primitive root is same as that of the witnesses of each pair in G . Hence, G has a common witness.

◀

The proof of Lemma 59 is a straightforward corollary of the Compactness Theorem. If G^* is conjugate, then the closure of every finite subset of G is also conjugate. From Lemma 60, every finite subset of G has a common witness. Using Compactness Theorem, G has a common witness. From Corollary 55, we conclude that $R(G)$ has a common witness.

This concludes the proof of Common Witness Theorem (Theorem 42).

6 Existence of Common Witness for Monoid Closure

In this section, we prove the equivalence between conjugacy and the presence of a common witness in sumfree sets. We begin by proving Proposition 48 for sumfree sets that contain only one Kleene star. Subsequently, we establish Theorem 49 that extends the result to general sumfree sets.

6.1 Common Witness of a Singleton Redux

We prove Proposition 48 by showing $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1)$. It is trivial that $(3) \Rightarrow (1)$, i.e., if a sumfree set M has a common witness, then M is conjugate.

Now we proceed to prove $(1) \Rightarrow (2)$, namely, if a sumfree set $M = (\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$ is conjugate, then there exists a common witness of $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$. We first prove this direction when G is just a singleton set and later generalise it to any arbitrary set of pairs G .

► **Proposition 63.** *Let (u, v) be a nonempty conjugate pair. If the pair $(\alpha_0, \beta_0)(u, v)^{4n}(\alpha_1, \beta_1)$, for some n such that $n|u| \geq |\alpha_0| + |\alpha_1| + |\beta_0| + |\beta_1|$, is conjugate then there exists a common witness of $\{(u, v), (\alpha_1\alpha_0, \beta_1\beta_0)\}$.*

Proof. Consider the pair $(u', v') = (\alpha_0, \beta_0)(u, v)^{4n}(\alpha_1, \beta_1)$. Let (x, y) denote the cut of the primitive root of the conjugate pair (u, v) . Thus, (u, v) can be expressed as a power of (xy, yx) .

We now examine the possible cuts of (u', v') in u' and show that in each case, a common witness of $\{(u, v), (\alpha_1\alpha_0, \beta_1\beta_0)\}$ exists.

Case 1: When the cut in u' is within α_0

I.e., there exists a cut (p, q) for (u', v') such that $p = \alpha'_0$ is a prefix of α_0 and $\alpha_0 = \alpha'_0\alpha''_0$ for some word α''_0 . Substituting (u, v) with powers of (xy, yx) ,

$$\begin{aligned} u' &= \overbrace{\alpha'_0}^p \overbrace{\alpha''_0 xy \cdots xy \alpha_1}^q \\ v' &= \beta_0 yx \cdots yx \beta_1 \end{aligned}$$

Comparing prefixes of q in u' and v' , we obtain three possible cases for β_0 .

- (a) β_0 is a proper prefix of α''_0 : After matching β_0 with the prefix of q in u' , we find that the remaining suffix of α''_0 matches with the prefix of the block $yx \cdots yx$ in v' . Since the total length of the block $yx \cdots yx$ is greater than $4|\alpha_0|$, it follows that α''_0 must end within the first half of the block. Furthermore, using Cases **I. (a)**, **I. (b)**, **I. (e)** and **II.** of **Cut Lemma**, it should end after a y since there exists an xy after α''_0 in u' . Thus, we can express α''_0 as

$$\alpha''_0 = \beta_0(yx)^m y \quad (11)$$

for some integer $m \geq 0$. Continuing to match q in u' and v' , we obtain

$$u' = \alpha'_0 \alpha''_0 \overbrace{xy \cdots x}^=(yx)^m y \alpha_1 = pq \quad (12)$$

$$v' = \underbrace{\beta_0(yx)^m y}_{\alpha''_0} \underbrace{xy \cdots x}_= \beta_1 = qp = \alpha''_0 \overbrace{xy \cdots x}^=(yx)^m y \alpha_1 \alpha'_0 \quad (13)$$

By equating the sets for v' on both sides of Equation (13), we get

$$\beta_1 = (yx)^m y \alpha_1 \alpha'_0. \quad (14)$$

Concatenating Equation (11) and Equation (14), we obtain

$$(yx)^m y \alpha_1 \alpha_0 = \beta_1 \beta_0 (yx)^m y.$$

From Theorem 25, we get $(yx)^m y$ is a outer witness for $(\alpha_1\alpha_0, \beta_1\beta_0)$, and it is also a outer witness of (u, v) using Proposition 54. Therefore, $(yx)^m y$ is a common outer witness of $\{(u, v), (\alpha_1\alpha_0, \beta_1\beta_0)\}$.

- (b) The case when $\beta_0 = \alpha''_0$:

$$u' = \alpha'_0 \alpha''_0 \overbrace{xy \cdots xy}^= \alpha_1 = pq \quad (15)$$

$$v' = \underbrace{\beta_0}_{\alpha''_0} \underbrace{yx \cdots yx}_= \beta_1 = qp = \alpha''_0 \overbrace{xy \cdots xy}^= \alpha_1 \alpha'_0 \quad (16)$$

Equating v' on both sides of the Equation (16), we get that $xy = yx$ and

$$\beta_1 = \alpha_1 \alpha'_0. \quad (17)$$

Appending the equation $\beta_0 = \alpha''_0$ to Equation (17), we get $\alpha_1 \alpha_0 = \beta_1 \beta_0$. Hence $(\alpha_1 \alpha_0, \beta_1 \beta_0)$ is conjugate with ϵ as a witness. Since $xy = yx$, we can also deduce that (u, v) is an identical pair with ϵ as a witness. Therefore, ϵ is a common witness of $\{(u, v), (\alpha_1 \alpha_0, \beta_1 \beta_0)\}$.

- (c) α''_0 is a proper prefix of β_0 : Since the total length of block $xy \cdots xy$ is at least $4|\beta_0|$, it follows that β_0 must end within the first half of the block of xy . Moreover, it should end after an x by Cases I. (c), I. (d), I. (e) and II. of Cut Lemma since there is at least one yx after β_0 in v' . Therefore,

$$\beta_0 = \alpha''_0(xy)^m x \quad (18)$$

for some integer $m \geq 0$. Continuing with the analysis, we have:

$$u' = \alpha'_0 \overbrace{\alpha''_0(xy)^m x}^{\beta_0} \overbrace{yx \cdots y}^{\beta_0} \alpha_1 = pq \quad (19)$$

$$v' = \beta_0 \underbrace{yx \cdots y}_{=} (xy)^m x \beta_1 = qp = \overbrace{\alpha''_0(xy)^m x}^{\beta_0} \overbrace{yx \cdots y}^{\beta_0} \alpha_1 \alpha'_0 \quad (20)$$

By equating the sets for v' on both sides of Equation (20), we get

$$(xy)^m x \beta_1 = \alpha_1 \alpha'_0. \quad (21)$$

Concatenating Equation (18) and Equation (21), we obtain

$$\alpha_1 \alpha_0 (xy)^m x = (xy)^m x \beta_1 \beta_0.$$

From Theorem 25, we get $(xy)^m x$ is an inner witness of $(\alpha_1 \alpha_0, \beta_1 \beta_0)$, and it is also an inner witness for (u, v) using Proposition 54. Thus, $(xy)^m x$ is a common inner witness of $\{(u, v), (\alpha_1 \alpha_0, \beta_1 \beta_0)\}$.

Case 2: When the cut in u' is within the block of $(u, v) \cdots (u, v)$

A cut (p, q) exists such that p ends within the block of (u, v) 's. There are two cases based on whether the cut in u' is within the first half or the second half of the block of $(u, v) \cdots (u, v)$.

- (a) When p ends within the first half of the block of (u, v) 's:

$$\begin{aligned} u' &= \alpha_0 \overbrace{xy \cdots xy}^{\text{cut region } \geq 2n \text{ times}} \overbrace{xy \cdots xy}^{\beta_0} \alpha_1 = pq \\ v' &= \beta_0 yx \cdots yxyx \cdots yx \beta_1 = qp \end{aligned}$$

We compare the prefixes of q in u' and v' . Since the length of the remaining half of the block of xy 's is still greater than $2n|u| > 2|\beta_0|$, it follows that β_0 in v' matches within the block of xy 's in u' and there is at least one xy occurring after it. Moreover, it ends after an x by Cases I. (c), I. (d), I. (e) and II. of Cut Lemma, as there is at least one yx in v' after β_0 . Therefore,

$$p\beta_0 = \alpha_0(xy)^m x \quad (22)$$

for some integer $m \geq 0$.

$$u' = \overbrace{\alpha_0(xy)^m x}^{p\beta_0} \overbrace{yx \cdots y}^{\quad} \alpha_1 = pq \quad (23)$$

$$v' = \beta_0 \underbrace{yx \cdots y}_{\quad} (xy)^m x \beta_1 = qp = \beta_0 \overbrace{yx \cdots y}^{\quad} \alpha_1 p \quad (24)$$

By equating the sets for v' on both sides of Equation (24), we get

$$\begin{aligned} (xy)^m x \beta_1 = \alpha_1 p &\Rightarrow (xy)^m x \beta_1 \beta_0 = \alpha_1 p \beta_0 && \text{(Appending } \beta_0) \\ &\Rightarrow (xy)^m x \beta_1 \beta_0 = \alpha_1 \alpha_0 (xy)^m x && \text{(Substituting Equation (22))} \end{aligned}$$

Therefore we obtain,

$$\alpha_1 \alpha_0 (xy)^m x = (xy)^m x \beta_1 \beta_0 .$$

From Theorem 25, $(xy)^m x$ is an inner witness of $(\alpha_1 \alpha_0, \beta_1 \beta_0)$, and it is also an inner witness for (u, v) using Proposition 54. Therefore, $(xy)^m x$ is a common inner witness of $\{(u, v), (\alpha_1 \alpha_0, \beta_1 \beta_0)\}$.

- (b) When p ends within the second half of the block of (u, v) 's:

$$\begin{aligned} u' &= \alpha_0 \overbrace{xy \cdots xy}^{\geq 2n \text{ times cut region}} \overbrace{xy \cdots xy}^{\quad} \alpha_1 = pq \\ v' &= \beta_0 yx \cdots yxyx \cdots yx \beta_1 = qp \end{aligned}$$

We compare the suffixes of p in u' and v' . Since the suffix of p within the block xy is still greater than $2n|u| > 2|\beta_1|$, it follows that the suffix β_1 in v' matches within the block of xy 's in u' and there is at least one xy occurring before it. Moreover, it starts with a y by Cases I. (c), I. (d), I. (e) and II. of Cut Lemma since there is at least one yx before β_1 . Hence,

$$\beta_1 q = (yx)^m y \alpha_1 \quad (25)$$

for some integer $m \geq 0$.

$$u' = \alpha_0 \overbrace{xy \cdots x}^{\quad} \overbrace{(yx)^m y \alpha_1}^{\beta_1 q} = pq \quad (26)$$

$$v' = \beta_0 (yx)^m y \underbrace{xy \cdots x}_{\quad} \beta_1 = qp = q \alpha_0 \overbrace{xy \cdots x}^{\quad} \beta_1 \quad (27)$$

By equating v' on both sides of the Equation (27), we get

$$\begin{aligned} \beta_0 (yx)^m y = q \alpha_0 &\Rightarrow \beta_1 \beta_0 (yx)^m y = \beta_1 q \alpha_0 && \text{(Concatenating } \beta_1 \text{ on the left side)} \\ &\Rightarrow \beta_1 \beta_0 (yx)^m y = (yx)^m y \alpha_1 \alpha_0 && \text{(Substituting Equation (25))} \end{aligned}$$

Therefore, we obtain

$$(yx)^m y \alpha_1 \alpha_0 = \beta_1 \beta_0 (yx)^m y .$$

From Theorem 25, we get $(yx)^m y$ is an outer witness of $(\alpha_1 \alpha_0, \beta_1 \beta_0)$, and it is also an outer witness for (u, v) using Proposition 54. Therefore, $(yx)^m y$ is a common outer witness of $\{(u, v), (\alpha_1 \alpha_0, \beta_1 \beta_0)\}$.

Case 3: When the cut in u' is within α_1

I.e., there exist a cut (p, q) for (u', v') such that $q = \alpha_1''$ is a suffix of α_1 and $\alpha_1 = \alpha_1' \alpha_1''$ for some word α_1' .

$$\begin{aligned} u' &= \overbrace{\alpha_0 xy \cdots xy \alpha_1'}^p \overbrace{\alpha_1''}^q \\ v' &= \beta_0 yx \cdots yx \beta_1 \end{aligned}$$

This case is symmetric to *Case 1*, where the cut in u' is within α_0 . \blacktriangleleft

► **Corollary 64.** *If a set $M = (\alpha_0, \beta_0)(u, v)^*(\alpha_1, \beta_1)$ is conjugate then there exist a common witness of $\{(u, v), (\alpha_1 \alpha_0, \beta_1 \beta_0)\}$.*

Proof. Since M is conjugate, as stated in Lemma 12, (u, v) is also conjugate. Furthermore, the pair $(\alpha_0, \beta_0)(u, v)^{4n}(\alpha_1, \beta_1) \in M$ is conjugate, where $n|u| \geq 2 \cdot (\text{length of the redux of } M)$. From Proposition 63, we conclude that there exists a common witness of $\{(u, v), (\alpha_1 \alpha_0, \beta_1 \beta_0)\}$. \blacktriangleleft

Now we extend the above corollary to an arbitrary set G . First, we prove the following lemma.

► **Lemma 65.** *Let $M = (\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$ be a conjugate sumfree set. If there exist a pair $(u, v) \in G$ such that the set $\{(u, v), (\alpha_1 \alpha_0, \beta_1 \beta_0)\}$ has a unique common witness z , then z is a common witness of G .*

Proof. Let (u', v') be any pair in G . We show that z is a witness of (u', v') . Consider the set $M' = (\alpha_0, \beta_0)(u, v)^*(u', v')^*(\alpha_1, \beta_1)$, that is a subset of the set M and thus conjugate. We show that there exists a pair in M' such that it is conjugate only if z is a witness of (u', v') . We divide into two cases depending upon if the primitive roots of (u, v) and (u', v') are conjugates to each other, i.e., $\rho_u \sim \rho_{u'}$ or not.

Let m be the least common multiple of $|u|$ and $|u'|$, and let $\ell = |u| + |u'| - \gcd(u, u')$ be the Fine and Wilf index of u and u' . Let C denote the length of the redux of M . Let n be the smallest number such that $nm \geq \max(C, \ell)$. Let (x, y) and (x', y') be the unique cut of the primitive roots of (u, v) and (u', v') respectively.

Case 1: When $\rho_u \sim \rho_{u'}$

We have $|xy| = |x'y'|$ in this case. Since G^* is conjugate, there exist l_1, l_2 such that $l_2 \gg l_1 > 2$ and $(xy, yx)^{l_1}(x'y', y'x')^{l_2}$ is conjugate. From **Equal Length Lemma**, either $x = x'$ or $y = y'$.

Consider a pair $(\bar{u}, \bar{v}) \in M'$ as follows.

$$\begin{aligned} \bar{u} &= \alpha_0 \overbrace{u \cdots u}^{2nm} \overbrace{u' \cdots u'}^{8nm} \alpha_1 \\ \bar{v} &= \beta_0 v \cdots v v' \cdots v' \beta_1 \end{aligned}$$

As M' is conjugate, (\bar{u}, \bar{v}) is conjugate with some cut, say (p, q) . We do a case analysis on the cuts possible and show that z is also a witness of (u', v') . There are two cases to consider: when the cut p in \bar{u} ends within the first $2nm$ length of the block $u' \cdots u'$, or after it.

Substituting (u, v) with powers of (xy, yx) and (u', v') with powers of (x', y') , we get

$$\begin{aligned} \bar{u} &= \alpha_0 \overbrace{xy \cdots xy}^{2nm} \overbrace{x'y' \cdots x'y'}^{2nm} \overbrace{x'y' \cdots x'y'}^{6nm} \alpha_1 \\ \bar{v} &= \beta_0 yx \cdots yx y'x' \cdots y'x'y'x' \cdots y'x'y'x' \beta_1 \end{aligned}$$

1. When the cut p in \bar{u} ends atmost within the first $2nm$ length of block $x'y' \cdots x'y'$.

$$\begin{aligned}\bar{u} &= \overbrace{\alpha_0 xy \cdots xy x'y' \cdots x'y'}^{\text{cut region}} \overbrace{x'y' \cdots x'y'}^{\geq 6nm} \alpha_1 = pq \\ \bar{v} &= \beta_0 yx \cdots yx y'x' \cdots y'x'y'x' \cdots y'x'\beta_1 = qp\end{aligned}$$

In this case, the total length of p is less than $5nm$. As the total length of the block consisting of $y'x'$ is at least $8nm$, the cut in \bar{v} is at most within the suffix of the block $y'x' \cdots y'x'$. We compare the suffixes of q in \bar{u} and \bar{v} . Since the length of the remaining block of $y'x'$ before the cut is still greater than $3nm$, we conclude that α_1 in \bar{u} matches at most within the block $y'x'$'s in \bar{v} .

$$\bar{v} = \beta_0 yx \cdots yx y'x' \cdots \underbrace{y'x'\beta_1}_{=\alpha_1 p} = qp$$

There are 3 possible cases for $\alpha_1 p$.

- (a) $\alpha_1 p$ is a proper suffix of β_1 : We continue comparing the suffixes of q , and deduce that β_1 starts within the block of $x'y'$'s, and there is at least one occurrence of $x'y'$ before it. Moreover, by Cases **I. (c)**, **I. (d)**, **I. (e)** and **II. of Cut Lemma**, we determine that β_1 starts from y' since there is at least one $y'x'$ preceding β_1 in \bar{v} . Therefore, we can express β_1 as

$$\beta_1 = (y'x')^{m_2} y' \alpha_1 p \quad (28)$$

for some integer $m_2 \geq 0$. Let $w' = (y'x')^{m_2} y'$. Continuing the matching of q in \bar{u} and \bar{v} ,

$$\begin{aligned}\bar{u} &= \alpha_0 xy \cdots xy \overbrace{x' \cdots x'}^{\text{=}} w' \alpha_1 = pq \\ \bar{v} &= \beta_0 yx \cdots yx w' \underbrace{x' \cdots x'}_{\text{=}} \underbrace{\beta_1}_{w' \alpha_1 p} = qp\end{aligned}$$

On matching further, we get a factor of w' in \bar{v} that needs to be matched within the block of xy 's. There are two cases for w' depending on whether $m_2 = 0$ or not.

Suppose $w' = y'$. In this case, w' in \bar{v} must match with the suffix of xy in \bar{u} since $|xy| = |x'y'|$. Given that there is at least one occurrence of yx before w' in \bar{v} , we can apply Cases **I. (c)**, **I. (d)**, **I. (e)** and **II. of Cut Lemma** to conclude that $w' = y' = y$. Proceeding with further matchings, we obtain

$$\begin{aligned}\bar{u} &= \underbrace{\alpha_0}_{p\beta_0 y} \underbrace{x \cdots x}_{\text{=}} \underbrace{y x' \cdots x'}_{\text{=}} y' \alpha_1 = pq \\ \bar{v} &= \beta_0 y \underbrace{x \cdots x}_{\text{=}} \underbrace{y' x' \cdots x'}_{\text{=}} \beta_1 = qp\end{aligned}$$

Therefore, we have $p = \alpha_0(\beta_0 y)^{-1}$. Substituting it in the Equation (28), we obtain

$$y' \alpha_1 \alpha_0 = \beta_1 \beta_0 y. \quad (29)$$

Since $y = y'$, it follows from Equation (29) that y, y' is an outer witness of $(\alpha_1 \alpha_0, \beta_1 \beta_0)$ using Theorem 25. Also, y and y' are outer witnesses of (u, v) and (u', v') respectively,

using Proposition 54. Overall, we obtain that y, y' is a common outer witness of $\{(u, v), (u', v'), (\alpha_1\alpha_0, \beta_1\beta_0)\}$.

Since z is the unique common witness of $\{(u, v), (\alpha_1\alpha_0, \beta_1\beta_0)\}$, $z = y = y'$ is a witness of (u', v') .

Suppose $w' \in (y'x')^+y'$. By matching w' in \bar{v} with the suffix of the block $xy \cdots xy$ in \bar{u} , we obtain $xy = x'y'$ since $|xy| = |x'y'|$. It also follows that $yx = y'x'$ because either $x = x'$ or $y = y'$. Therefore, the primitive roots of (u, v) and (u', v') are the same. Thus, z is also a witness for (u', v') .

- (b) The case when $\alpha_1p = \beta_1$: Further matching q in \bar{u} and \bar{v} we get $x'y' = y'x'$ and $xy = yx$. Thus, (u, v) and (u', v') are identical pairs with ϵ as a common witness. Let's consider the sets of \bar{u} and \bar{v} :

$$\begin{aligned}\bar{u} &= \alpha_0 \overbrace{xy \cdots xyx'y' \cdots x'y'}^{\quad} \alpha_1 = pq \\ \bar{v} &= \beta_0 \underbrace{yx \cdots yxy'x' \cdots y'x'}_{\quad} \underbrace{\beta_1}_{=\alpha_1p} = qp\end{aligned}$$

On further matching, we obtain

$$p = \alpha_0(\beta_0)^{-1}. \quad (30)$$

Substituting Equation (30) in the equation $\alpha_1p = \beta_1$, we obtain $\alpha_1\alpha_0 = \beta_1\beta_0$. Thus, ϵ is a common witness for $\{(u, v), (u', v'), (\alpha_1\alpha_0, \beta_1\beta_0)\}$. Since z is the unique witness of (u, v) and $(\alpha_1\alpha_0, \beta_1\beta_0)$, we conclude that $z = \epsilon$. Therefore, z is a witness of (u', v') .

- (c) β_1 is proper suffix of α_1p : We continue by comparing the suffixes of q in \bar{u} and \bar{v} . Since $|\alpha_1p| \leq C + 5nm \leq 6nm$ and the total length of the block of $y'x'$'s is at least $8nm$, α_1p starts within the $y'x'$'s, and there is at least one occurrence of $x'y'$ before that. Furthermore, it starts from x' by using Cases I. (a), I. (b), I. (e) and II. of Cut Lemma, as there exists at least one $x'y'$ before α_1 in \bar{u} . Thus, we get

$$\alpha_1p = (x'y')^{m_2}x'\beta_1 \quad (31)$$

for some integer $m_2 \geq 0$. Let $w' = (x'y')^{m_2}x'$.

$$\begin{aligned}\bar{u} &= \alpha_0xy \cdots xyw' \overbrace{y' \cdots y'}^{\quad} \alpha_1 \\ \bar{v} &= \beta_0yx \cdots yx \underbrace{y' \cdots y'}_{\quad} \underbrace{w'\beta_1}_{\alpha_1p}\end{aligned}$$

On matching further, a factor w' in \bar{u} to be matched within the block of yx 's in \bar{v} . There are two cases of w' depending upon if $m_2 = 0$ or not.

Let us consider the case when $w' = x'$. In this scenario, w' in \bar{u} must match with the suffix of yx in \bar{v} since $|xy| = |x'y'|$. Given that there is at least one occurrence of xy before w' in \bar{u} , we can apply Cases I. (a), I. (b), I. (e) and II. of Cut Lemma to conclude that $w' = x' = x$. By further matching, we obtain:

$$\begin{aligned}\bar{u} &= \overbrace{\alpha_0x}^{p\beta_0} \overbrace{y \cdots y}^{\quad} \overbrace{x'y' \cdots y'}^{\quad} \alpha_1 \\ \bar{v} &= \beta_0 \underbrace{y \cdots y}_{\quad} x \underbrace{y' \cdots y'}_{\quad} x' \beta_1\end{aligned}$$

We have $p = \alpha_0 x \beta_0^{-1}$. Substituting it in the Equation (31), we obtain

$$\alpha_1 \alpha_0 x = x' \beta_1 \beta_0. \quad (32)$$

Since $x = x'$, it follows from Equation (32) that x, x' is an inner witness of $(\alpha_1 \alpha_0, \beta_1 \beta_0)$ using Theorem 25. Also, x and x' are inner witnesses of (u, v) and (u', v') respectively, using Proposition 54. Overall, we obtain that x, x' is a common inner witness of $\{(u, v), (u', v'), (\alpha_1 \alpha_0, \beta_1 \beta_0)\}$.

Since z is the unique common witness of $\{(u, v), (\alpha_1 \alpha_0, \beta_1 \beta_0)\}$, $z = x = x'$ is a witness of (u', v') .

Suppose $w' \in (x'y')^+ x'$. By matching w' in \bar{u} with the suffix of the block $yx \cdots yx$ in \bar{v} , we obtain $yx = y'x'$ since $|yx| = |y'x'|$. It also follows that $xy = x'y'$ because either $x = x'$ or $y = y'$. Therefore, the primitive roots of (u, v) and (u', v') are the same. Thus, z is also a witness for (u', v') .

2. When the cut in \bar{u} ends after the first $2nm$ length of the block $x'y' \cdots x'y'$.

$$\begin{aligned} \bar{u} &= \alpha_0 xy \cdots xy \overbrace{x'y' \cdots x'y'}^{\geq 2nm} \overbrace{x'y' \cdots x'y'}^{\text{cut region}} \cdots x'y' \alpha_1 \\ \bar{v} &= \beta_0 yx \cdots yx y'x' \cdots y'x'y'x' \cdots y'x' \beta_1 \end{aligned}$$

We compare the suffixes of p in \bar{u} and \bar{v} . In \bar{v} , β_1 starts matching within the block of $x'y'$'s in \bar{u} since the length of β_1 is at most C , that is less than or equal to nm , and the length of the block of $x'y'$'s before the cut is at least $2nm$.

$$\bar{u} = \alpha_0 xy \cdots xy x'y' \cdots \overbrace{\cdots x'y'}^{\beta_1 q} \alpha_1$$

There are three possible cases for $\beta_1 q$, that are symmetric to the three cases for $\alpha_1 p$ discussed earlier:

- (a) $\beta_1 q$ is a proper suffix of α_1 .
- (b) $\beta_1 q = \alpha_1$
- (c) α_1 is a proper suffix of $\beta_1 q$.

We conclude that z is a witness of the pair (u', v') in all three cases.

Case 2: When $\rho_u \not\sim \rho_{u'}$

Consider a pair $(\bar{u}, \bar{v}) \in M'$ as follows.

$$\begin{aligned} \bar{u} &= \alpha_0 \overbrace{u \cdots u}^{6nm} \overbrace{u' \cdots u'}^{6nm} \alpha_1 \\ \bar{v} &= \beta_0 v \cdots v v' \cdots v' \beta_1 \end{aligned}$$

Since M' is conjugate, the pair (\bar{u}, \bar{v}) is conjugate with some cut (p, q) . To analyze the cuts and demonstrate that z is also a witness of (u', v') , we consider three main cases:

- The cut p in \bar{u} is positioned within the initial $2nm$ length of the block $u \cdots u$. (When p is short)
- The cut p in \bar{u} is located within the suffix starting from the last $2nm$ length of the block $u' \cdots u'$. (When q is short).
- The cut p is located between the remaining portion, i.e., the portion following the first $2nm$ length of the block u 's and before the last $2nm$ length of the block u' 's.

Substituting (u_i, v_i) with powers of $(x_i y_i, y_i x_i)$ we get,

$$\begin{aligned}\bar{u} &= \alpha_0 \overbrace{xy \cdots xy}^{2nm} \overbrace{xy \cdots xy}^{4nm} \overbrace{x'y' \cdots x'y'}^{4nm} \overbrace{x'y' \cdots x'y'}^{2nm} \alpha_1 \\ \bar{v} &= \beta_0 yx \cdots yxyx \cdots yxy'x' \cdots y'x'xy'x' \cdots y'x'\beta_1\end{aligned}$$

1. When p is short, i.e., when the cut in \bar{u} is within first $2nm$ length of the block u 's.

$$\bar{u} = \overbrace{\alpha_0 xy \cdots xy}^{\text{cut region}} \overbrace{xy \cdots xy}^{\geq 4nm} \overbrace{x'y' \cdots x'y'}^{\geq 6nm} \alpha_1$$

In this case, we perform a further analysis based on whether the cut in \bar{u} is within α_0 or within the block $xy \cdots xy$.

Let's consider the scenario where the cut p is within α_0 , i.e., $p = \alpha'_0$ is a prefix of α_0 and $\alpha_0 = \alpha'_0 \alpha''_0$, for some word α''_0 . Next, we compare the prefixes of q in \bar{u} and \bar{v} . We can further divide this analysis into three cases:

- β_0 is a proper prefix of α''_0 .
- $\beta_0 = \alpha''_0$.
- α''_0 is a proper prefix of β_0 .

In the last case, we also consider the scenario where the cut is within the block $xy \cdots xy$. We examine these cases and show that z is a witness of (u', v') in every situation.

- (a) When the cut is within α_0 and β_0 is a proper prefix of α''_0 . We continue to match the prefixes of q in \bar{u} and \bar{v} . After matching β_0 with the prefix of q in \bar{u} , we find that the remaining suffix of α''_0 matches with the prefix of the block $yx \cdots yx$ in \bar{v} . Since the total length of the block $yx \cdots yx$ is far greater than $|\alpha_0|$ and there exists a xy after α''_0 in \bar{u} , it should end at a y using Cases **I. (a)**, **I. (b)**, **I. (e)** and **II.** of **Cut Lemma**. Thus, we can express α''_0 as

$$\alpha''_0 = \beta_0 (yx)^m y \tag{33}$$

for some integer $m \geq 0$. Let $w = (yx)^m y$. Continuing to match q in \bar{u} and \bar{v} , we obtain

$$\begin{aligned}\bar{u} &= \alpha'_0 \alpha''_0 \overbrace{x \cdots x}^w w x' y' \cdots x' y' \alpha_1 \\ \bar{v} &= \underbrace{\beta_0 w}_{\alpha''_0} \underbrace{x \cdots x}_{=}' y' x' \cdots y' x' \beta_1\end{aligned}$$

Furthermore, a factor equal to w in \bar{u} must be matched with a prefix of the block $y'x'$'s in \bar{v} . Given that the length of w is smaller than the length of α_0 , i.e., $|w| < |\alpha_0| < nm$, we can conclude that w matches within the block $y'x'$'s. By applying Cases **I. (a)**, **I. (b)**, **I. (e)** and **II.** of **Cut Lemma**, we determine that w ends at y' since there is at least one occurrence of $x'y'$ following w in \bar{u} . Let $w' = (y'x')^{m_2} y'$ for some $m_2 \geq 0$, and it follows that $w = w'$. On further matching, we obtain

$$\begin{aligned}\bar{u} &= \alpha_0 \overbrace{x \cdots x}^w \overbrace{x' \cdots x'}^{w'} w' \alpha_1 = pq \\ \bar{v} &= \beta_0 w \underbrace{x \cdots x}_{=}' \underbrace{w' \cdots x'}_{=}' \beta_1 = qp\end{aligned}$$

We have,

$$\beta_1 = w' \alpha_1 p. \tag{34}$$

By substituting $p = \alpha'_0$ and appending the Equation (33) in Equation (34), we can deduce that $w'\alpha_1\alpha_0 = \beta_1\beta_0w$. Since we know that $w = w'$, it follows that $w\alpha_1\alpha_0 = \beta_1\beta_0w$ and $w'\alpha_1\alpha_0 = \beta_1\beta_0w'$. Therefore, w, w' is an outer witness of $(\alpha_1\alpha_0, \beta_1\beta_0)$ using Theorem 25. Also, $w \in (yx)^*y$ and $w' \in (y'x')^*y'$ are outer witnesses of (u, v) and (u', v') respectively, using Proposition 54. Since $w = w'$, we get w, w' is a common outer witness of $\{(u, v), (u', v'), (\alpha_1\alpha_0, \beta_1\beta_0)\}$.

Since we know that z is the unique common witness for $\{(u, v), (\alpha_1\alpha_0, \beta_1\beta_0)\}$, $z = w = w'$ is a witness of (u', v') .

- (b) When the cut p is within α_0 and $\beta_0 = \alpha'_0$: We observe that through further matchings in q , we obtain $xy = yx$ and $x'y' = y'x'$. Consequently, (u, v) and (u', v') form an identical pair with ϵ as a witness. This scenario is equivalent to the previous case where $w = w' = \epsilon$.
- (c) The remaining cases involve either the cut being within α_0 and α'_0 being a proper suffix of β_0 , or the cut being located within the first $2nm$ length of the block $xy \cdots xy$. In both cases, as the length of the remaining half of xy 's is still greater than $nm \geq |\beta_0|$, we can match the prefixes of q in \bar{u} and \bar{v} to determine that β_0 ends within the block xy 's. Furthermore, using Cases I. (c), I. (d), I. (e) and II. in Cut Lemma, β_0 should end after an x because there exists a yx after β_0 in \bar{v} . Thus, we can express $p\beta_0$ as

$$p\beta_0 = \alpha_0w \quad (35)$$

where $w = (xy)^{m_1}x$ for some integer $m_1 \geq 0$. On matching further, we obtain

$$\begin{aligned} \bar{u} &= \overbrace{\alpha_0w}^{p\beta_0} \overbrace{y \cdots y}^{=} x'y' \cdots x'y' \alpha_1 \\ \bar{v} &= \beta_0 \overbrace{y \cdots y}^{=} w y' x' \cdots y' x' \beta_1 \end{aligned}$$

Note that the maximum length of w is atmost $3nm$ (that is equal to $|p| + |\beta_0|$). Given that the total length of the block $x'y' \cdots x'y'$ is at least $6nm$, we can conclude that w matches within the block $x'y'$'s and ends after an x' . This can be inferred from Cases I. (c), I. (d), I. (e) and II. in Cut Lemma, as there exists a $y'x'$ after w in \bar{v} . Let $w' = (x'y')^{m_2}x'$, where $m_2 \geq 0$, and we have $w = w'$.

$$\begin{aligned} \bar{u} &= \alpha_0w \overbrace{y \cdots y}^{=} \overbrace{w' y' \cdots y'}^{=} \alpha_1 \\ \bar{v} &= \beta_0 \overbrace{y \cdots y}^{=} \overbrace{w y' \cdots y'}^{=} w' \beta_1 \end{aligned}$$

We have,

$$w'\beta_1 = \alpha_1p. \quad (36)$$

By substituting p of Equation (35) in the Equation (36), we can deduce that $\alpha_1\alpha_0w = w'\beta_1\beta_0$. Since we know that $w = w'$, it follows that $\alpha_1\alpha_0w = w\beta_1\beta_0$ and $\alpha_1\alpha_0w' = w'\beta_1\beta_0$. From Theorem 25, we get w, w' is an inner witness of $(\alpha_1\alpha_0, \beta_1\beta_0)$. Also, $w \in (xy)^*x$ and $w' \in (x'y')^*x'$ are inner witnesses of (u, v) and (u', v') respectively, using Proposition 54. Since $w = w'$, we get w, w' is a common inner witness of $\{(u, v), (u', v'), (\alpha_1\alpha_0, \beta_1\beta_0)\}$.

Since we know that z is the unique common witness of $\{(u, v), (\alpha_1\alpha_0, \beta_1\beta_0)\}$, we can conclude that $z = w = w'$ is a witness of (u', v') .

2. When q is short, i.e., when the cut p in \bar{u} is positioned within the suffix starting from the last $2nm$ length of the block $u' \cdots u'$. This situation is symmetric to the previous case where p is short, and we can analyze it similarly.
3. Suppose \bar{u} has a long cut on either side, meaning that the cut p is located between the remaining portion, i.e., the portion following the first $2nm$ length of the block u 's and before the last $2nm$ length of the block u' 's. In this case, the block of xy 's and the block of $x'y'$'s have a common factor of length at least nm , that is greater than or equal to ℓ (the fine and Wilf index of u and u'). According to Theorem 27, it follows that xy and $x'y'$ are conjugates.

Hence, the primitive roots of (u, v) and (u', v') are conjugates, which contradicts our assumption that $\rho_u \not\sim \rho_{u'}$.

Therefore, z is a witness of any pair in G . Hence, z is a common witness of G . ◀

► **Proposition 66.** *If a set $M = (\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$ is conjugate then one of the following is true:*

1. G has infinitely many witnesses: In this case, each pair in G shares the same primitive root that has a common witness with $(\alpha_1\alpha_0, \beta_1\beta_0)$.
2. G has a unique common witness z : There exist a pair in G that has a unique common witness with $(\alpha_1\alpha_0, \beta_1\beta_0)$, that is equal to z . Hence, z is the only common witness of $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$.

Proof. Given that $(\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$ is conjugate, we can deduce that G^* is conjugate by Lemma 12. Furthermore, according to Corollary 43, G^* is conjugate if and only if G has a common witness. Considering Corollary 56, there are two possibilities for G : it either has a unique common witness or infinitely many common witnesses.

Assume that G has infinitely many common witnesses. From Corollary 56, G is a set of powers of a primitive root, say (ρ, ρ') . The common witnesses of G are the same as that of the witnesses of (ρ, ρ') using Corollary 55. Since M is conjugate, $(\alpha_0, \beta_0)(\rho^n, \rho'^n)^*(\alpha_1, \beta_1)$ is conjugate for some $n \geq 1$. From Corollary 64, there exists a common witness of $\{(\rho^n, \rho'^n), (\alpha_1\alpha_0, \beta_1\beta_0)\}$. Furthermore, according to Proposition 54, the witness of (ρ, ρ') is the same as the witness of (ρ^n, ρ'^n) . Therefore, we can conclude that there exists a common witness of $\{(\rho, \rho'), (\alpha_1\alpha_0, \beta_1\beta_0)\}$, and thus of $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$.

Next we assume that G has a unique common witness. We know that each pair in G has a common witness with $(\alpha_1\alpha_0, \beta_1\beta_0)$ using Corollary 64. Moreover, we claim that there exists a pair $(u, v) \in G$ such that (u, v) and $(\alpha_1\alpha_0, \beta_1\beta_0)$ share a *unique* common witness. Suppose not, i.e., every pair in G has infinitely many common witnesses with $(\alpha_1\alpha_0, \beta_1\beta_0)$. Consequently, each pair in G can be expressed as a power of the primitive root of $(\alpha_1\alpha_0, \beta_1\beta_0)$. Hence, G itself has infinitely many common witnesses by Corollary 56, a contradiction.

From Lemma 65, we obtain that the unique common witness of (u, v) and $(\alpha_1\alpha_0, \beta_1\beta_0)$ is a common witness of G . Thus, the unique common witness of G is the common witness of the set $G \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$. ◀

The remaining direction to prove is $(2) \Rightarrow (3)$ in Proposition 48. This direction states that if there exists a common witness for both G and $(\alpha_1\alpha_0, \beta_1\beta_0)$ for a given set $M = (\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$, then M has a common witness. It is a straightforward corollary of the below lemma.

► **Lemma 67.** *Let $M = (\alpha_0, \beta_0)G^*(\alpha_1, \beta_1)$ be a sumfree set. If there exists a common witness z for both G and $(\alpha_1\alpha_0, \beta_1\beta_0)$, then one of the following cases is true:*

- (a) If z is a unique common inner witness, then M has a unique common witness $z_m = [\alpha_0 z, \beta_0]_R = [\alpha_1, z\beta_1]_L$. Moreover, if $|\alpha_0 z| \geq |\beta_0|$ or equivalently $|\alpha_1| \leq |z\beta_1|$, then z_m is an inner witness, otherwise it is an outer witness.
- (b) If z is a unique common outer witness, then M has a unique common witness $z_m = [\alpha_0, \beta_0 z]_R = [z\alpha_1, \beta_1]_L$. Moreover, if $|z\alpha_1| \geq |\beta_1|$ or equivalently $|\alpha_0| \leq |\beta_0 z|$, then z_m is an outer witness, otherwise it is an inner witness.
- (c) If G and $(\alpha_1\alpha_0, \beta_1\beta_0)$ have infinitely many common witnesses, then M is a set of powers of the primitive root of its redux. Thus, M has infinitely many witnesses.

Proof. Case (a): When z is a common inner witness of G and $(\alpha_1\alpha_0, \beta_1\beta_0)$

The following equations hold:

$$\alpha_1\alpha_0z = z\beta_1\beta_0 \quad (37)$$

$$uz = zv \text{ for any pair } (u, v) \in G^* \quad (38)$$

We claim that $z_m = [\alpha_0 z, \beta_0]_R = [\alpha_1, z\beta_1]_L$ is a common witness for M . There are two cases depending upon whether β_0 is a suffix of $\alpha_0 z$ or vice-versa in Equation (37).

- (a) When β_0 is a suffix of $\alpha_0 z$ or equivalently, when α_1 is a prefix of $z\beta_1$. We get $z_m = \alpha_0 z \beta_0^{-1} = \alpha_1^{-1} z \beta_1$. We show that z_m is a common inner witness for M .
For any $(u, v) \in G^*$,

$$\begin{aligned} \alpha_0 u \alpha_1 z_m &= \alpha_0 u z \beta_1 && \text{(Substituting } \alpha_1 z_m = z \beta_1) \\ &= \alpha_0 z v \beta_1 && (z \text{ is an inner witness of } (u, v)) \\ &= z_m \beta_0 v \beta_1 && \text{(Substituting } \alpha_0 z = z_m \beta_0) \end{aligned}$$

- (b) When $\alpha_0 z$ is a suffix of β_0 or equivalently $z\beta_1$ is a prefix of α_1 . We get $z_m = \beta_0(\alpha_0 z)^{-1} = (z\beta_1)^{-1}\alpha_1$. We show that z_m is a common outer witness for M .
For any $(u, v) \in G^*$,

$$\begin{aligned} z_m \alpha_0 u \alpha_1 &= z_m \alpha_0 u z \beta_1 z_m && \text{(Substituting } \alpha_1 = z \beta_1 z_m) \\ &= z_m \alpha_0 z v \beta_1 z_m && (z \text{ is an inner witness of } (u, v)) \\ &= \beta_0 v \beta_1 z_m && \text{(Substituting } z_m \alpha_0 z = \beta_0) \end{aligned}$$

Case (b): When z is a common outer witness of G and $(\alpha_1\alpha_0, \beta_1\beta_0)$

Therefore, the following equations hold:

$$z\alpha_1\alpha_0 = \beta_1\beta_0z \quad (39)$$

$$zu = vz \text{ for any pair } (u, v) \in G^* \quad (40)$$

We claim that $z_m = [\alpha_0, \beta_0 z]_R = [z\alpha_1, \beta_1]_L$ is a witness for M . There are two cases depending upon if α_0 is a suffix of $\beta_0 z$ or vice-versa in Equation (39).

- (a) When α_0 is a suffix of $\beta_0 z$ or equivalently, β_1 is a prefix of $z\alpha_1$. We get $z_m = \beta_0 z \alpha_0^{-1} = \beta_1^{-1} z \alpha_1$. We show that z_m is a common outer witness for M .

For any $(u, v) \in G^*$,

$$\begin{aligned}
 z_m \alpha_0 u \alpha_1 &= \beta_0 z u \alpha_1 && \text{(Substituting } z_m \alpha_0 = \beta_0 z) \\
 &= \beta_0 v z \alpha_1 && (z \text{ is an outer witness of } (u, v)) \\
 &= \beta_0 v \beta_1 z_m && \text{(Substituting } z \alpha_1 = \beta_1 z_m)
 \end{aligned}$$

- (b) If $\beta_0 z$ is a suffix of α_0 or equivalently, $z \alpha_1$ is a prefix of β_1 . Therefore, $z_m = \alpha_0 (\beta_0 z)^{-1} = (z \alpha_1)^{-1} \beta_1$. We show that z_m is a common inner witness for M .

For any $(u, v) \in G^*$,

$$\begin{aligned}
 \alpha_0 u \alpha_1 z_m &= z_m \beta_0 z u \alpha_1 z_m && \text{(Substituting } \alpha_0 = z_m \beta_0 z) \\
 &= z_m \beta_0 v z \alpha_1 z_m && (z \text{ is an outer witness of } (u, v)) \\
 &= z_m \beta_0 v \beta_1 && \text{(Substituting } z \alpha_1 z_m = \beta_1)
 \end{aligned}$$

Therefore, if there exists a common witness z for G and $(\alpha_1 \alpha_0, \beta_1 \beta_0)$, there also exists a common witness z_m for M .

▷ **Claim 68.** If z is a unique common witness for G and $(\alpha_1 \alpha_0, \beta_1 \beta_0)$ then z_m is the unique common witness of M .

Proof. Since G and $(\alpha_1 \alpha_0, \beta_1 \beta_0)$ have a unique witness z , as stated in the second item of Proposition 66, there exists a pair (u, v) in G that has a unique common witness with $(\alpha_1 \alpha_0, \beta_1 \beta_0)$, that is equal to z .

Let z'_m be any common witness for M . Thus, z'_m is a common witness for the pair $P = (\alpha_0, \beta_0)(u, v)^{4n}(\alpha_1, \beta_1) \in M$, where n is the smallest number such that $n|u| \geq \max\{2 \cdot \text{length of the redux}, z'_m\}$. According to Proposition 63, for any cut in P , there exists a common witness for (u, v) and $(\alpha_1 \alpha_0, \beta_1 \beta_0)$. Since (u, v) and $(\alpha_1 \alpha_0, \beta_1 \beta_0)$ have a unique witness z , there is only one unique cut for P , as any other cut would lead to a new common witness. Therefore, $z'_m = z_m$. ◀

Case (c): When $G \cup \{(\alpha_1 \alpha_0, \beta_1 \beta_0)\}$ has infinitely many witnesses

According to Corollary 56, it is a set of powers of the same primitive root, let us say (ρ, ρ') . Therefore, $G^*(\alpha_1, \beta_1)(\alpha_0, \beta_0)$ is a set of powers of (ρ, ρ') and is conjugate. Since M is a cyclic shift of $G^*(\alpha_1, \beta_1)(\alpha_0, \beta_0)$ and is also conjugate, it is a set of powers of a primitive root, let us say (ρ_m, ρ'_m) , that is a cyclic shift of (ρ, ρ') . Moreover, α_1 (resp. β_1) is an inner (resp. outer) witness of (ρ, ρ_m) (resp. (ρ', ρ'_m)). We observe that (ρ_m, ρ'_m) is the primitive root of the redux of M . Hence, M is a set of powers of the primitive root of its redux. ◀

6.2 Common Witness of a Sumfree Set

We prove $(1) \Rightarrow (2), (3) \Rightarrow (1)$ and $(2) \iff (3)$ in Theorem 49. $(3) \Rightarrow (1)$ is obvious. We show $(2) \iff (3)$ first.

▷ **Lemma 69.** Given a sumfree set $M = (\alpha_0, \beta_0)G_1^*(\alpha_1, \beta_1)G_2^* \cdots G_k^*(\alpha_k, \beta_k)$. The following are equivalent.

1. z_m is a common witness of M .
2. z_m is a common witness of each of its singleton redux.

Proof. Let M_i be the singleton redux of M keeping only the Kleene star G_i^* , i.e., $M_i = (\alpha_0 \cdots \alpha_{i-1}, \beta_0 \cdots \beta_{i-1})G_i^*(\alpha_i \cdots \alpha_k, \beta_i \cdots \beta_k)$ for $i \in \{1, \dots, k\}$. The proof of (1) \Rightarrow (2) is trivial.

We prove (2) \Rightarrow (1). Assume z_m is a common inner witness of each M_i 's. For each i , let z_i denote the common witness of $G_i \cup \{(\alpha_i \cdots \alpha_k \alpha_0 \cdots \alpha_{i-1}, \beta_i \cdots \beta_k \beta_0 \cdots \beta_{i-1})\}$. There are 3 possible cases for z_i .

(a) z_i is a unique common inner witness. Therefore, for any pair $(u_i, v_i) \in G_i^*$,

$$u_i z_i = z_i v_i \quad (41)$$

$$\alpha_i \cdots \alpha_k \alpha_0 \cdots \alpha_{i-1} z_i = z_i \beta_i \cdots \beta_k \beta_0 \cdots \beta_{i-1} \quad (42)$$

$$z_m = \alpha_0 \cdots \alpha_{i-1} z_i (\beta_0 \cdots \beta_{i-1})^{-1} = (\alpha_i \cdots \alpha_k)^{-1} z_i \beta_i \cdots \beta_k \quad (\text{By Lemma 67 (a)}) \quad (43)$$

(b) z_i is a unique common outer witness. Therefore, for any pair $(u_i, v_i) \in G_i^*$,

$$z_i u_i = v_i z_i \quad (44)$$

$$z_i \alpha_i \cdots \alpha_k \alpha_0 \cdots \alpha_{i-1} = \beta_i \cdots \beta_k \beta_0 \cdots \beta_{i-1} z_i \quad (45)$$

$$z_m = \alpha_0 \cdots \alpha_{i-1} (\beta_0 \cdots \beta_{i-1} z_i)^{-1} = (z_i \alpha_i \cdots \alpha_k)^{-1} \beta_i \cdots \beta_k \quad (\text{By Lemma 67 (b)}) \quad (46)$$

(c) When $G_i \cup \{(\alpha_i \cdots \alpha_k \alpha_0 \cdots \alpha_{i-1}, \beta_i \cdots \beta_k \beta_0 \cdots \beta_{i-1})\}$ has infinitely many witnesses, by Corollary 56, it is a set of powers of the same primitive root say (ρ_i, ρ'_i) . Therefore z_i belongs to witnesses of (ρ_i, ρ'_i) . From Lemma 67 (c), the set M_i reduces to a set of powers of the primitive root of the redux $(\alpha_0 \cdots \alpha_k, \beta_0 \cdots \beta_k)$, say (ρ, ρ') . Note that $\alpha_i \cdots \alpha_k$ (*resp.* $\alpha_0 \cdots \alpha_{i-1}$) is an inner (*resp.* outer) witness of (ρ_i, ρ) . Similarly $\beta_i \cdots \beta_k$ (*resp.* $\beta_0 \cdots \beta_{i-1}$) is an inner (*resp.* outer) witness of (ρ'_i, ρ') .

We show that z_m is a common witness of M , i.e., for any arbitrary pair $(u_i, v_i) \in G_i^*$ (possibly empty), we prove $\alpha_0 u_1 \alpha_1 u_2 \alpha_2 \cdots \alpha_{k-1} u_k \alpha_k z_m = z_m \beta_0 v_1 \beta_1 v_2 \beta_2 \cdots \beta_{k-1} v_k \beta_k$. The proof is by induction on the number of singleton reduxes, $0 \leq i \leq k$.

Base Case:

When $i = 0$, it is vacuously true since z_m is a witness of the redux.

Inductive Case:

Assume for induction that it is true for the first $i - 1$ singleton reduxes, i.e.,

$$\alpha_0 u_1 \alpha_1 u_2 \alpha_2 \cdots u_{i-1} \alpha_{i-1} \cdots \alpha_k z_m = z_m \beta_0 v_1 \beta_1 v_2 \beta_2 \cdots v_{i-1} \beta_{i-1} \cdots \beta_k .$$

We prove it for the first i singleton reduxes, i.e., we show

$$\alpha_0 u_1 \alpha_1 u_2 \alpha_2 \cdots u_{i-1} \alpha_{i-1} u_i \alpha_i \cdots \alpha_k z_m = z_m \beta_0 v_1 \beta_1 v_2 \beta_2 \cdots v_{i-1} \beta_{i-1} v_i \beta_i \cdots \beta_k .$$

There are 3 possible cases for the common witness z_i of $G_i \cup \{(\alpha_i \cdots \alpha_k \alpha_0 \cdots \alpha_{i-1}, \beta_i \cdots \beta_k \beta_0 \cdots \beta_{i-1})\}$.

1. When z_i is a unique common inner witness. From Equation (43), $z_m = (\alpha_i \cdots \alpha_k)^{-1} z_i \beta_i \cdots \beta_k$.

$$\begin{aligned} & \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} u_i \alpha_i \cdots \alpha_k z_m \\ &= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} u_i z_i \beta_i \cdots \beta_k && (\text{Subs. } z_m) \\ &= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} z_i v_i \beta_i \cdots \beta_k && (u_i z_i = z_i v_i) \\ &= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} \alpha_i \cdots \alpha_k z_m (\beta_i \cdots \beta_k)^{-1} v_i \beta_i \cdots \beta_k && (\text{Subs. } z_i) \\ &= z_m \beta_0 v_1 \beta_1 \cdots v_{i-1} \beta_{i-1} \beta_i \cdots \beta_k (\beta_i \cdots \beta_k)^{-1} v_i \beta_i \cdots \beta_k && (\text{Inductive Hypothesis}) \\ &= z_m \beta_0 v_1 \beta_1 \cdots v_{i-1} \beta_{i-1} v_i \beta_i \cdots \beta_k && (\text{Simplifying}) \end{aligned}$$

2. When z_i is a unique outer witness. By Equation (46), $z_m = (z_i \alpha_i \cdots \alpha_k)^{-1} \beta_i \cdots \beta_k$.

$$\begin{aligned}
& \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} u_i \alpha_i \alpha_{i+1} \cdots \alpha_k z_m \\
&= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} u_i \alpha_i \alpha_{i+1} \cdots \alpha_k (z_i \alpha_i \cdots \alpha_k)^{-1} \beta_i \cdots \beta_k \quad (\text{Subs. } z_m) \\
&= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} u_i z_i^{-1} \beta_i \cdots \beta_k \quad (\text{Simplifying}) \\
&= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} z_i^{-1} v_i \beta_i \cdots \beta_k \quad (u_i = z_i^{-1} v_i z_i) \\
&= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} \alpha_i \cdots \alpha_k z_m (\beta_i \cdots \beta_k)^{-1} v_i \beta_i \cdots \beta_k \quad (\text{Subs. } z_i^{-1}) \\
&= z_m \beta_0 v_1 \beta_1 \cdots v_{i-1} \beta_{i-1} \beta_i \cdots \beta_k (\beta_i \cdots \beta_k)^{-1} v_i \beta_i \cdots \beta_k \quad (\text{Inductive Hypothesis}) \\
&= z_m \beta_0 v_1 \beta_1 \cdots v_{i-1} \beta_{i-1} v_i \beta_i \cdots \beta_k \quad (\text{Simplifying})
\end{aligned}$$

3. When z_i is a witness of the primitive root (ρ_i, ρ'_i) of $G_i \cup \{(\alpha_i \cdots \alpha_k \alpha_0 \cdots \alpha_{i-1}, \beta_i \cdots \beta_k \beta_0 \cdots \beta_{i-1})\}$ (The case where $G_i \cup \{(\alpha_i \cdots \alpha_k \alpha_0 \cdots \alpha_{i-1}, \beta_i \cdots \beta_k \beta_0 \cdots \beta_{i-1})\}$ have infinitely many witnesses). Here (u_i, v_i) is some m^{th} power of (ρ_i, ρ'_i) . Since z_m is a witness of a singleton redux, it is also a witness of the redux $(\alpha_0 \cdots \alpha_k, \beta_0 \cdots \beta_k)$, and hence a witness of its primitive root (ρ, ρ') . We also know that $\alpha_i \cdots \alpha_k$ is an inner witness of (ρ_i, ρ) and $\beta_i \cdots \beta_k$ is an inner witness of (ρ'_i, ρ') .

$$\begin{aligned}
& \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} u_i \alpha_i \alpha_{i+1} \cdots \alpha_k z_m \\
&= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} (\rho_i)^m \alpha_i \alpha_{i+1} \cdots \alpha_k z_m \quad (\text{Subs. } u_i) \\
&= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} \alpha_i \alpha_{i+1} \cdots \alpha_k (\rho)^m z_m \quad (\alpha_i \cdots \alpha_k \text{ is an i.w. of } (\rho_i, \rho)) \\
&= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} \alpha_i \alpha_{i+1} \cdots \alpha_k z_m (\rho')^m \quad (z_m \text{ is a witness of } (\rho, \rho')) \\
&= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} \alpha_i \alpha_{i+1} \cdots \alpha_k z_m (\beta_i \cdots \beta_k)^{-1} (\rho'_i)^m \beta_i \cdots \beta_k \quad (\beta_i \cdots \beta_k \text{ is an i.w. of } (\rho'_i, \rho')) \\
&= \alpha_0 u_1 \alpha_1 \cdots u_{i-1} \alpha_{i-1} \alpha_i \alpha_{i+1} \cdots \alpha_k z_m (\beta_i \cdots \beta_k)^{-1} v_i \beta_i \cdots \beta_k \quad (\text{Subs. } v_i = (\rho'_i)^m) \\
&= z_m \beta_0 v_1 \beta_1 \cdots v_{i-1} \beta_{i-1} \beta_i \cdots \beta_k (\beta_i \cdots \beta_k)^{-1} v_i \beta_i \cdots \beta_k \quad (\text{Inductive Hypothesis}) \\
&= z_m \beta_0 v_1 \beta_1 \cdots v_{i-1} \beta_{i-1} v_i \beta_i \cdots \beta_k \quad (\text{Simplifying})
\end{aligned}$$

Thus z_m is a common witness of M . ◀

We prove (1) \Rightarrow (2) in Theorem 49 in the case when a sumfree set contains only two Kleene stars. Later we extend it to an arbitrary number of Kleene stars.

► **Lemma 70.** *Let $M = (\alpha_0, \beta_0)G_1^*(\alpha_1, \beta_1)G_2^*(\alpha_2, \beta_2)$. If M is conjugate then there exists a common witness z such that z is a common witness for each of its singleton reduxes.*

Proof. Consider the singleton redux of M denoted as M_1 and M_2 . We have $M_1 = (\alpha_0, \beta_0)G_1^*(\alpha_1 \alpha_2, \beta_1 \beta_2)$ and $M_2 = (\alpha_0 \alpha_1, \beta_0 \beta_1)G_2^*(\alpha_2, \beta_2)$. Since M is conjugate, it follows that M_1 and M_2 are also conjugate. According to Proposition 48, both M_1 and M_2 has a common witness.

If both M_1 and M_2 have infinitely many common witnesses, we can conclude, based on the third item in Lemma 67, that both M_1 and M_2 are sets of powers of the primitive root of the redux of M . Thus, any witness for the primitive root of the redux is also a witness for both M_1 and M_2 using Proposition 54. Therefore, it holds true that when both M_1 and M_2 have infinitely many common witnesses.

Let us consider the scenario where exactly one of M_1 and M_2 has a unique witness. Without loss of generality, let us assume that M_1 has a unique witness, while M_2 has infinitely many witnesses. According to Lemma 67, we can conclude that M_2 is a set of powers of the primitive root of the redux. Consequently, the witnesses of M_2 are the same as the witnesses of the primitive root of the redux. Since the unique witness, say z , for M_1 is

also a witness for the redux, we can apply Proposition 54 to conclude that z is also a witness for the primitive root of the redux. Therefore, z is also a witness for M_2 .

If both M_1 and M_2 have a unique witness. From Lemma 67, G_1 has a unique common witness z_1 with $(\alpha_1\alpha_2\alpha_0, \beta_1\beta_2\beta_0)$. Moreover, From Proposition 66, there exist a pair $(u_1, v_1) \in G$ such that it has a unique common witness with $(\alpha_1\alpha_2\alpha_0, \beta_1\beta_2\beta_0)$ equal to z_1 . Similarly, there exists a pair $(u_2, v_2) \in G_2$ that has a unique common witness with $(\alpha_2\alpha_0\alpha_1, \beta_2\beta_0\beta_1)$, that is same as the unique witness of G_2 say z_2 .

Consider the set $M' = (\alpha_0, \beta_0)(u_1, v_1)^*(\alpha_1, \beta_1)(u_2, v_2)^*(\alpha_2, \beta_2)$, which is a subset of the sumfree set M and therefore M' is conjugate.

We construct a pair in M' and do a case analysis on its cuts. Our objective is to show that a nontrivial relation exists between z_1 , z_2 , and the redux for all possible cuts. By equating this relation, we can establish that the unique witnesses of M_1 and M_2 are identical.

Let m be the least common multiple of $|u_1|$ and $|u_2|$, and let C be the length of the redux. We choose n as the smallest number such that $nm \geq C$. Let (x_1, y_1) and (x_2, y_2) is the unique cut of the primitive root of (u_1, v_1) and (u_2, v_2) respectively.

Consider a pair $(u', v') \in M'$ as follows.

$$\begin{aligned} u' &= \alpha_0 \overbrace{u_1 \cdots u_1}^{2nm} \alpha_1 \overbrace{u_2 \cdots u_2}^{8nm} \alpha_2 \\ v' &= \beta_0 v_1 \cdots v_1 \beta_1 v_2 \cdots v_2 \beta_2 \end{aligned}$$

Since M' is conjugate, (u', v') is conjugate with some cut denoted as (p, q) . We do a case analysis based on the cuts possible and show that M_1 and M_2 share the same unique witness. There are two cases to consider: when the cut in u' occurs at most within the initial $2nm$ length of the block of $x_2y_2 \cdots x_2y_2$, or after it.

Substituting (u_i, v_i) with powers of (x_iy_i, y_ix_i) we get,

$$\begin{aligned} u' &= \alpha_0 \overbrace{x_1y_1 \cdots x_1y_1}^{2nm} \alpha_1 \overbrace{x_2y_2 \cdots x_2y_2}^{2nm} \overbrace{x_2y_2 \cdots x_2y_2}^{6nm} \alpha_2 \\ v' &= \beta_0 y_1x_1 \cdots y_1x_1 \beta_1 y_2x_2 \cdots y_2x_2 y_2x_2 \cdots y_2x_2 \beta_2 \end{aligned}$$

Case 1: When the cut p in u' ends at most within the first $2nm$ length of block $x_2y_2 \cdots x_2y_2$

$$\begin{aligned} u' &= \overbrace{\alpha_0 x_1y_1 \cdots x_1y_1 \alpha_1 x_2y_2 \cdots x_2y_2}^{\text{cut region}} \overbrace{x_2y_2 \cdots x_2y_2}^{\geq 6nm} \alpha_2 \\ v' &= \beta_0 y_1x_1 \cdots y_1x_1 \beta_1 y_2x_2 \cdots y_2x_2 y_2x_2 \cdots y_2x_2 \beta_2 \end{aligned}$$

In this case, the total length of p is less than $5nm$. As the total length of the block consisting of y_2x_2 is at least $8nm$, the cut in v' is at most within the suffix of the block $y_2x_2 \cdots y_2x_2$. We compare the suffixes of q in u' and v' . Since the length of the remaining block of y_2x_2 before the cut is still greater than $3nm$, we conclude that α_2 in u' matches at most within the y_2x_2 's in v' .

$$v' = \beta_0 y_1x_1 \cdots y_1x_1 \beta_1 y_2x_2 \cdots \underbrace{\cdots y_2x_2}_{=\alpha_2 p} \beta_2$$

There are 3 possible cases for $\alpha_2 p$.

- (a) $\alpha_2 p$ is a proper suffix of β_2 . We continue comparing the suffixes of q , and deduce that β_2 starts within the block of $x_2 y_2$'s, and there is at least one occurrence of $x_2 y_2$ before it. Moreover, by Cases I. (c), I. (d), I. (e) and II. of **Cut Lemma**, we determine that β_2 starts from y_2 since there is at least one $y_2 x_2$ preceding β_2 in v' . Therefore, we can express β_2 as $(y_2 x_2)^{m_2} y_2 \alpha_2 p$, where m_2 is an integer greater than or equal to 0. Let $w_2 = (y_2 x_2)^{m_2} y_2$. Continuing the matching of q in u' and v' ,

$$\begin{aligned} u' &= \alpha_0 x_1 y_1 \cdots x_1 y_1 \alpha_1 \overbrace{x_2 \cdots x_2}^{\beta_2} w_2 \alpha_2 = pq \\ v' &= \beta_0 y_1 x_1 \cdots y_1 x_1 \beta_1 w_2 \underbrace{x_2 \cdots x_2}_{w_2 \alpha_2 p} \beta_2 = qp \end{aligned}$$

On matching further, we deduce $p = \alpha_0 x_1 y_1 \cdots x_1 y_1 \alpha_1 (\beta_0 y_1 x_1 \cdots y_1 x_1 \beta_1 w_2)^{-1}$. By substituting it in the equation $w_2 \alpha_2 p = \beta_2$, we obtain

$$w_2 \alpha_2 \alpha_0 x_1 y_1 \cdots x_1 y_1 \alpha_1 = \beta_2 \beta_0 y_1 x_1 \cdots y_1 x_1 \beta_1 w_2 .$$

We deduce w_2 is an outer witness for $(\alpha_2 \alpha_0, \beta_2 \beta_0)(x_1 y_1, y_1 x_1) \cdots (x_1 y_1, y_1 x_1)(\alpha_1, \beta_1)$ using Theorem 25. Furthermore, w_2 is the unique outer witness for this set, as (u_1, v_1) and $(\alpha_1 \alpha_2 \alpha_0, \beta_1 \beta_2 \beta_0)$ share a unique common witness z_1 . By applying Lemma 67, we can equate w_2 accordingly. There are two cases to consider based on whether z_1 is a unique common inner or outer witness.

- a. When z_1 is a unique inner witness of (u_1, v_1) and $(\alpha_1 \alpha_2 \alpha_0, \beta_1 \beta_2 \beta_0)$.

$$w_2 = \beta_2 \beta_0 (\alpha_2 \alpha_0 z_1)^{-1} = (z_1 \beta_1)^{-1} \alpha_1 . \quad (47)$$

We obtain $w_2 \alpha_2 \alpha_0 \alpha_1 = \beta_2 \beta_0 \beta_1 w_2$ by solving Equation (47). Since $w_2 \in (y_2 x_2)^* y_2$, w_2 is a common outer witness of (x_2, y_2) and $(\alpha_2 \alpha_0 \alpha_1, \beta_2 \beta_0 \beta_1)$. Since z_2 is the unique common witness of (u_2, v_2) and $(\alpha_2 \alpha_0 \alpha_1, \beta_2 \beta_0 \beta_1)$, we get $w_2 = z_2$, which implies that z_2 is the unique common outer witness.

From Proposition 48, the unique witness of M_1 is $[\alpha_0 z_1, \beta_0]_R$ and the unique witness of M_2 is $[\beta_0 \beta_1 z_2, \alpha_0 \alpha_1]_R$. We show that they are equal as follows.

$$\begin{aligned} [\beta_0 \beta_1 z_2, \alpha_0 \alpha_1]_R &= [\beta_0 \beta_1 z_2, \alpha_0 z_1 \beta_1 z_2]_R \quad (\text{Since } z_1 \beta_1 z_2 = \alpha_1 \text{ in Equation (47)}) \\ &= [\beta_0, \alpha_0 z_1]_R \quad ([uw, vw]_R = [u, v]_R \text{ for any word } w, u \text{ and } v) \\ &= [\alpha_0 z_1, \beta_0]_R \quad ([u, v]_R = [v, u]_R \text{ for any word } u \text{ and } v) \end{aligned}$$

Thus the witness of M_1 and M_2 are the same.

- b. When z_1 is a unique outer witness of (u_1, v_1) and $(\alpha_1 \alpha_2 \alpha_0, \beta_1 \beta_2 \beta_0)$.

$$w_2 = \beta_2 \beta_0 z_1 (\alpha_2 \alpha_0)^{-1} = \beta_1^{-1} z_1 \alpha_1 . \quad (48)$$

We get $w_2 \alpha_2 \alpha_0 \alpha_1 = \beta_2 \beta_0 \beta_1 w_2$ by solving Equation (48). Since $w_2 \in (y_2 x_2)^* y_2$, w_2 is a common outer witness of (x_2, y_2) and $(\alpha_2 \alpha_0 \alpha_1, \beta_2 \beta_0 \beta_1)$. Since z_2 is the unique common witness of (u_2, v_2) and $(\alpha_2 \alpha_0 \alpha_1, \beta_2 \beta_0 \beta_1)$, we get $w_2 = z_2$, which implies z_2 is the unique common outer witness.

From Proposition 48, the unique witness of M_1 is $[\beta_1 \beta_2, z_1 \alpha_1 \alpha_2]_L$ and the unique witness of M_2 is $[\beta_2, z_2 \alpha_2]_L$. We show that they are equal as follows.

$$\begin{aligned} [\beta_1 \beta_2, z_1 \alpha_1 \alpha_2]_L &= [\beta_1 \beta_2, \beta_1 z_2 \alpha_2]_L \quad (\text{Since } z_1 \alpha_1 = \beta_1 z_2 \text{ in Equation (48)}) \\ &= [\beta_2, z_2 \alpha_2]_L \quad ([wu, wv]_L = [u, v]_L \text{ for any word } w, u \text{ and } v) \end{aligned}$$

Thus the witness of M_1 and M_2 are the same.

- (b) $\alpha_2 p = \beta_2$. In this case by further matchings in q we get $x_2 y_2 = y_2 x_2$. Thus $u_2 = v_2$ and hence (u_2, v_2) is an identical cycle with ϵ as witness. It is the same as the above case where $w_2 = \epsilon$.
- (c) When β_2 is proper suffix of $\alpha_2 p$. β_1 is proper suffix of $\alpha_1 p$. We continue by comparing the suffixes of q in u' and v' . Since $|\alpha_2 p| \leq C + 5nm \leq 6nm$ and the total length of the block of $y_2 x_2$'s is at least $8nm$, $\alpha_2 p$ starts within the $y_2 x_2$'s, and there is at least one occurrence of $x_2 y_2$ before that. Furthermore, it starts from x_2 by using Cases I. (a), I. (b), I. (e) and II. of **Cut Lemma**, as there exists at least one $x_2 y_2$ before α_2 in u' . Thus, we can write $\alpha_2 p = (x_2 y_2)^{m_2} x_2 \beta_2$, where $m_2 \geq 0$. Let $w_2 = (x_2 y_2)^{m_2} x_2$.

$$\begin{aligned} u' &= \alpha_0 x_1 y_1 \cdots x_1 y_1 \alpha_1 w_2 \overbrace{y_2 \cdots y_2}^{\alpha_2 p} \alpha_2 \\ v' &= \beta_0 y_1 x_1 \cdots y_1 x_1 \beta_1 \underbrace{y_2 \cdots y_2}_{\alpha_2 p} \underbrace{w_2 \beta_2}_{\alpha_2 p} \end{aligned}$$

On matching further, we deduce $p = \alpha_0 x_1 y_1 \cdots x_1 y_1 \alpha_1 w_2 (\beta_0 y_1 x_1 \cdots y_1 x_1 \beta_1)^{-1}$. By substituting it in the equation $\alpha_2 p = (x_2 y_2)^{m_2} x_2 \beta_2$, we obtain

$$\alpha_2 \alpha_0 x_1 y_1 \cdots x_1 y_1 \alpha_1 w_2 = w_2 \beta_2 \beta_0 y_1 x_1 \cdots y_1 x_1 \beta_1 w_2.$$

We deduce w_2 is an inner witness for $(\alpha_2 \alpha_0, \beta_2 \beta_0)(x_1 y_1, y_1 x_1) \cdots (x_1 y_1, y_1 x_1)(\alpha_1, \beta_1)$ using Theorem 25. Furthermore, w_2 is the unique inner witness for this set, as (u_1, v_1) and $(\alpha_1 \alpha_2 \alpha_0, \beta_1 \beta_2 \beta_0)$ share a unique common witness z_1 . By applying Lemma 67, we can equate w_2 accordingly. There are two cases to consider based on whether z_1 is a unique common inner or outer witness.

- a. When z_1 is a unique inner witness of (u_1, v_1) and $(\alpha_1 \alpha_2 \alpha_0, \beta_1 \beta_2 \beta_0)$.

$$w_2 = \alpha_2 \alpha_0 z_1 (\beta_2 \beta_0)^{-1} = (\alpha_1)^{-1} z_1 \beta_1. \quad (49)$$

We deduce $\alpha_2 \alpha_0 \alpha_1 w_2 = w_2 \beta_2 \beta_0 \beta_1$ by solving Equation (49). Since $w_2 \in (x_2 y_2)^* x_2$, w_2 is a common inner witness of (x_2, y_2) and $(\alpha_2 \alpha_0 \alpha_1, \beta_2 \beta_0 \beta_1)$. Since z_2 is the unique common witness of (u_2, v_2) and $(\alpha_2 \alpha_0 \alpha_1, \beta_2 \beta_0 \beta_1)$, we get $w_2 = z_2$, which implies z_2 is the unique common inner witness.

From Proposition 48, the unique witness of M_1 is $[\alpha_0 z_1, \beta_0]_R$ and the unique witness of M_2 is $[\alpha_0 \alpha_1 z_2, \beta_0 \beta_1]_R$. We show that they are equal as follows.

$$\begin{aligned} [\alpha_0 \alpha_1 z_2, \beta_0 \beta_1]_R &= [\alpha_0 z_1 \beta_1, \beta_0 \beta_1]_R \quad (\text{Since } \alpha_1 z_2 = z_1 \beta_1 \text{ in Equation (49)}) \\ &= [\alpha_0 z_1, \beta_0]_R \quad ([uw, vw]_R = [u, v]_R \text{ for any word } w, u \text{ and } v) \end{aligned}$$

Thus the witness of M_1 and M_2 are the same.

- b. When z_1 is a unique outer witness of (u_1, v_1) and $(\alpha_1 \alpha_2 \alpha_0, \beta_1 \beta_2 \beta_0)$.

$$w_2 = \alpha_2 \alpha_0 (\beta_2 \beta_0 z_1)^{-1} = (z_1 \alpha_1)^{-1} \beta_1. \quad (50)$$

We obtain $\alpha_2 \alpha_0 \alpha_1 w_2 = w_2 \beta_2 \beta_0 \beta_1$ by solving Equation (50). Since $w_2 \in (x_2 y_2)^* x_2$, w_2 is a common inner witness of (x_2, y_2) and $(\alpha_2 \alpha_0 \alpha_1, \beta_2 \beta_0 \beta_1)$. Since z_2 is the unique common witness of (u_2, v_2) and $(\alpha_2 \alpha_0 \alpha_1, \beta_2 \beta_0 \beta_1)$, we get $w_2 = z_2$, which implies z_2 is the unique common inner witness.

From Proposition 48, the unique witness of M_1 is $[\beta_1\beta_2, z_1\alpha_1\alpha_2]_L$ and the unique witness of M_2 is $[\alpha_2, z_2\beta_2]_L$. We show that they are equal as follows.

$$\begin{aligned} [\beta_1\beta_2, z_1\alpha_1\alpha_2]_L &= [z_1\alpha_1z_2\beta_2, z_1\alpha_1\alpha_2]_L && \text{(Since } z_1\alpha_1z_2 = \beta_1 \text{ in Equation (50))} \\ &= [z_2\beta_2, \alpha_2]_L && ([wu, wv]_L = [u, v]_L \text{ for any word } w, u \text{ and } v) \\ &= [\alpha_2, z_2\beta_2]_L && ([u, v]_L = [v, u]_L \text{ for any word } u \text{ and } v) \end{aligned}$$

Thus the witness of M_1 and M_2 are the same.

Case 2: When the cut in u' ends after the first $2nm$ length of the block $x_2y_2 \cdots x_2y_2$

$$\begin{aligned} u' &= \alpha_0x_1y_1 \cdots x_1y_1\alpha_1 \overbrace{x_2y_2 \cdots x_2y_2}^{\geq 2nm} \overbrace{x_2y_2 \cdots x_2y_2\alpha_2}^{\text{cut region}} \\ v' &= \beta_0y_1x_1 \cdots y_1x_1\beta_1y_2x_2 \cdots y_2x_2y_2x_2 \cdots y_2x_2\beta_2 \end{aligned}$$

We compare the suffixes of p in u' and v' . In v' , β_2 starts matching within the block of x_2y_2 's in u' since the length of β_2 is at most C , which is less than or equal to nm , and the length of the block of x_2y_2 's before the cut is at least $2nm$.

$$u' = \alpha_0x_1y_1 \cdots x_1y_1\alpha_1x_2y_2 \cdots \overbrace{x_2y_2\alpha_2}^{\beta_2q}$$

There are three possible cases for β_2q , which are symmetric to the three cases for α_2p discussed earlier:

- (a) β_2q is a proper suffix of α_2 .
- (b) $\beta_2q = \alpha_2$.
- (c) α_2 is a proper suffix of β_2q .

◀

► **Theorem 71.** *If M is conjugate, then a common witness exists for the set of singleton reduses of M .*

Proof. Let M consist of k singleton reduses where $k \geq 1$. Suppose all singleton redux has infinitely many common witnesses. From the third item of Lemma 67, each singleton redux is a set of powers of the primitive root of the redux. Hence, any witness for the primitive root of the redux is a witness for any singleton redux of M . Therefore, a common witness exists for the set of singleton reduses of M .

Suppose there are ℓ singleton reduses with unique witnesses $z_{n_1}, z_{n_2}, \dots, z_{n_\ell}$, where $1 \leq \ell \leq k$.

We claim that $z_{n_1} = z_{n_2} = \dots = z_{n_\ell}$. For any two positions $i, j \in \{n_1, \dots, n_\ell\}$, since the subset of M obtained by keeping the Kleene star at positions i and j is conjugate, according to Lemma 70, $z_i = z_j$.

Thus, all the unique witnesses of the ℓ singleton reduses are the same, and let it be z . Since z is also a witness for the redux, as stated in Proposition 54, it is a witness for the primitive root of the redux. Therefore, z is also a witness for all singleton reduses with infinitely many witnesses, as they are sets of powers of the primitive root of the redux. Hence, z is a common witness of each singleton reduses of M . ◀

7 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. A sumfree expression can have no common witness, a unique common witness, or infinitely many common witnesses. Thus, the set of common witnesses (abbreviated as the *witness set*) 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 (Corollary 56). In that case we compute the primitive root as their finite representation.

The witness set of a sumfree expression is equal to the intersection of witness sets of each of its singleton reduses. So first, we show how to compute the witness set of a sumfree expression with only one Kleene star, in effect the witness set of a singleton redux. Using this procedure, we show how to compute the witness set of a general sumfree expression.

First we bound the size of the unique common witness of two conjugate primitive pairs, if it exists.

► **Proposition 72.** *If two conjugate primitive pairs (u_1, v_1) and (u_2, v_2) have a unique common witness z , then $|z| \leq 2 \cdot \max(|u_1|, |u_2|)$.*

Proof. Let z be a common inner witness. Therefore, $z = (x_1 y_1)^{n_1} x_1 = (x_2 y_2)^{n_2} x_2$ for some $n_1, n_2 \geq 0$ where (x_i, y_i) is the unique cut of pair (u_i, v_i) for $i \in \{1, 2\}$. We claim either n_1 or n_2 is less than 2. Suppose not, i.e., $n_1 \geq 2$ and $n_2 \geq 2$. Thus u_1^ω and u_2^ω share a common prefix of length at least $|u_1| + |u_2|$. From Corollary 24, they have the same primitive root. It implies that $x_1 y_1 = x_2 y_2$ since u_1 and u_2 are primitive words. Since $(x_1 y_1)^{n_1} x_1 = (x_2 y_2)^{n_2} x_2$, $x_1 y_1 = x_2 y_2$ and $|x_1|, |x_2| < |x_1 y_1|$, we obtain $n_1 = n_2$, and hence, $x_1 = x_2$. This implies $y_1 = y_2$ and hence, $y_1 x_1 = y_2 x_2$. Both (u_1, v_1) and (u_2, v_2) are the same word; thus, they have infinitely many common witnesses, that is a contradiction. Hence $|z| \leq 2 \cdot \max\{|u_1|, |u_2|\}$.

The case for common outer witness is symmetric. ◀

The above proposition holds true for any two conjugate pairs (not necessarily primitive) by Corollary 55.

The following proposition gives a decision procedure to compute the witness set of two conjugate primitive pairs.

► **Proposition 73.** *The witness set of two conjugate primitive pairs of words is computable in quadratic time.*

Proof. Let $G = \{(u_1, v_1), (u_2, v_2)\}$ be a set of two primitive conjugate pairs and let (x_i, y_i) be the cut of (u_i, v_i) for $i \in \{1, 2\}$. These cuts can be computed in quadratic time w.r.t. the length of u_1, u_2 by finding the smallest $i \in \{0, \dots, |u|\}$, such that $\text{lshift}_i(u) = v$.

According to Lemma 39, one of the following possibilities holds true for G : it has no common witness, a unique common witness, or infinitely many common witnesses. The following algorithm outlines the computation of the witness set of G :

1. Check if the primitive pairs are identical, i.e., verify if $u_1 = u_2$ and $v_1 = v_2$. If yes, then G has infinitely many common witnesses by Lemma 39. The witness is finitely represented by the primitive pair (u_1, v_1) . This step takes linear time w.r.t. the length of the primitive pairs.
2. If the pairs are not identical, then check if G has a unique common witness using Proposition 72 as follows: WLOG assume that $|u_1| > |u_2|$. According to Proposition 72,

if a unique common witness exists for G , its length is at most $2 \cdot \max(|u_1|, |u_2|) = 2 \cdot |u_1|$. Thus, it suffices to check whether $(x_1y_1)^\omega$ and $(x_2y_2)^\omega$ share equal prefixes of length $|x_1|$ or $|x_1y_1x_1|$, that also end in x_2 . If it is satisfied, then G has a unique common witness. This step can be performed in linear time w.r.t. the length of the primitive pairs.

3. If none of the above holds, then G has no common witness.

The overall complexity of the algorithm is quadratic w.r.t the length of the primitive pairs. ◀

► **Corollary 74.** *The witness set of two conjugate pairs can be computed in quadratic time.*

Proof. We can compute the primitive roots of the conjugate pairs in quadratic time by Proposition 22. From Corollary 55 (or, $3 \iff 4$ in Theorem 42), the common witnesses of a set of pairs are the same as that of its primitive root. Hence, using Proposition 73, we can compute the witness set of the conjugate pairs. ◀

Now we proceed to compute the common witness of a sumfree expression with only one Kleene star.

► **Lemma 75.** *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. From Proposition 48, M has a common witness iff $E \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$ has a common witness. The common witness of M is computed from the common witness of E and $(\alpha_1\alpha_0, \beta_1\beta_0)$.

The idea is to check if a common witness exists for $E \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$ using Proposition 66. If it exists, using that we compute the common witness for M . There are two possibilities for common witnesses of E :

1. E has a unique common inner (resp. outer) witness z . By Item 2 of Proposition 66, it suffices to check if z is a common inner (resp. outer) witness of $(\alpha_1\alpha_0, \beta_1\beta_0)$. This can be checked in $\mathcal{O}(m+n)$ time using Theorem 25. If so, z is the common witness of $E \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$. Now compute the common witness of M using Proposition 48(a) (resp. Proposition 48(b)). This can be computed in $\mathcal{O}(m+n)$ time. Otherwise, $E \cup \{(\alpha_1\alpha_0, \beta_1\beta_0)\}$ has no common witness and hence, M has no common witness by Proposition 48.
2. E has infinitely many common witnesses. In this case, the witnesses of E are the same as that of its primitive root, say (ρ, ρ') . From Item 1 of Proposition 66, it suffices to check if (ρ, ρ') and $(\alpha_1\alpha_0, \beta_1\beta_0)$ has a common witness. For this, first check if the primitive root of $(\alpha_1\alpha_0, \beta_1\beta_0)$ is equal to (ρ, ρ') . This step takes time $\mathcal{O}(m^2+n)$. We have two cases:
 - (a) If $(\alpha_1\alpha_0, \beta_1\beta_0)$ have same primitive root as that of E , then E and $(\alpha_1\alpha_0, \beta_1\beta_0)$ have infinitely many common witnesses by Corollary 56. In this case, M is a set of powers of the primitive root of the redux by Proposition 48(c). Thus M has infinitely many witnesses. Compute the primitive root of its redux using Proposition 22. This step takes $\mathcal{O}(m^2)$ time.
 - (b) Otherwise, compute the unique common witness of (ρ, ρ') and $(\alpha_1\alpha_0, \beta_1\beta_0)$ if it exists using Corollary 74. If so, we are back to Case 1; else M has no common witness. This step takes $\mathcal{O}((m+n)^2)$ time.

◀

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

► **Lemma 76.** *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. From Theorem 49, the witness set of M is the intersection of the witness sets of its singleton reduxes. The algorithm is as follows.

1. Check if the redux of M is conjugate using Proposition 28 (in time m^2). If yes, then compute the primitive root of the redux, say (ρ_m, ρ'_m) , using Proposition 22 (in time m^2). Otherwise, M has no common witness.
2. Check if each singleton redux of M has a common witness and compute it using Lemma 75. This step takes $\mathcal{O}(m \cdot (m + n)^2)$. If there is a singleton redux with no common witness, then M has no common witness by Theorem 49.
 - (a) If all the singleton reduxes have infinitely many witnesses, then M is a set of powers of the primitive root of the redux (ρ_m, ρ'_m) by Proposition 48(c). Thus M has infinitely many common witnesses.
 - (b) 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.

◀

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 using Proposition 28. 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 76 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, from Corollary 56, M is a set of powers of a primitive root. Therefore, there exists a witness of length that is 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 star appearing in E_i has infinitely many witnesses. Therefore, all of them have a common witness 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 size of M . Furthermore, the common witnesses for all subsequent levels is unique (if it exists) and its length is bounded by $|M|$.

Complexity of the Algorithm

Since the size of the common witness of M is linear in $|M|$, by Lemma 76, 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.

8 Conclusion

It is shown that the conjugacy problem of a rational relation is decidable. The decidability rests on the theorem that a sumfree expression of pairs is conjugate if and only if there exists a word that witnesses the conjugacy of all the pairs in the language of the expression.

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

It is also natural to look at the conjugacy problem of regular functions [6] (functions definable by a deterministic two-way transducer) as well as polyregular functions [2] (functions definable by a two-way pebble automaton).

References

- 1 Blattner and Head. The decidability of equivalence for deterministic finite transducers. *JCSS: Journal of Computer and System Sciences*, 19, 1979.
- 2 Mikolaj Bojanczyk. Transducers of polynomial growth. In *Proceedings of the 37th annual acm/ieee symposium on logic in computer science*, pages 1–27, 2022.
- 3 Julien Cassaigne, Juhani Karhumäki, and Ján Manuch. On conjugacy of languages. *RAIRO Theor. Informatics Appl.*, 35(6):535–550, 2001. doi:10.1051/ita:2001130.
- 4 Christian Choffrut and Juhani Karhumäki. Combinatorics of words. In Grzegorz Rozenberg and Arto Salomaa, editors, *Handbook of Formal Languages*, volume 1, pages 329–438. Springer-Verlag, 1997.
- 5 Calvin C Elgot and Jorge E Mezei. On relations defined by generalized finite automata. *IBM Journal of Research and development*, 9(1):47–68, 1965.
- 6 Joost Engelfriet and Hendrik Jan Hoogeboom. Mso definable string transductions and two-way finite-state transducers. *ACM Trans. Comput. Logic*, 2(2):216–254, April 2001.
- 7 Thomas V Griffiths. The unsolvability of the equivalence problem for λ -free nondeterministic generalized machines. *Journal of the ACM (JACM)*, 15(3):409–413, 1968.
- 8 Vesa Halava, Tero Harju, and Esa Sahla. The conjugate post correspondence problem. *CoRR*, abs/2111.04484, 2021.
- 9 J. Berstel. *Transductions and Context-Free Languages*. Teubner, Stuttgart, 1979.
- 10 M. Lothaire, editor. *Combinatorics on Words*. Addison-Wesley, Reading, MA, 1983.
- 11 Roger C Lyndon, Marcel-Paul Schützenberger, et al. The equation $a^M = b^N c^P$ in a free group. *Michigan Math. J.*, 9(4):289–298, 1962.
- 12 Anca Muscholl and Gabriele Puppis. The Many Facets of String Transducers (Invited Talk). In *STACS 2019*, volume 126 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:21, 2019. URL: <http://drops.dagstuhl.de/opus/volltexte/2019/10241>.

- 13 Jean-Éric Pin. Mathematical foundations of automata theory. *Lecture notes IRIF, Université Paris Cité*, 7:73, 2010.
- 14 Michael Rabin and Dana Scott. Finite automata and their decision problems. *IBM Journal of Research and Development*, 3:114–125, 04 1959.
- 15 Jacques Sakarovitch. *Elements of automata theory*. Cambridge University Press, 2009.