Deciding Conjugacy of a Rational Relation

Amaldev Manuel
School of Mathematics and Computer Science
IIT GOA

Joint work with C. Aiswarya (CMI) and Saina Sunny (IIT GOA)

Rational Relations

- A binary relation over monoids A^* and B^* is a subset of $A^* \times B^*$.
- A relation is **rational** if it can built out of finite subsets of $A^* \times B^*$ using the operations **union**, **product** and **Kleene star**.

Rational Relations

- A binary relation over monoids A^* and B^* is a subset of $A^* \times B^*$.
- A relation is ***rational*** if it can built out of finite subsets of $A^* \times B^*$ using the operations union, product and Kleene star.
- Example:

$$\{(u, v) \mid u \in \{a, b, c\}^*, v \in \{b, c\}^*, v = u[a|b]\}$$

Rational Relations

- A binary relation over monoids A^* and B^* is a subset of $A^* \times B^*$.
- A relation is ***rational*** if it can built out of finite subsets of $A^* \times B^*$ using the operations union, product and Kleene star.
- Example:

$$\{(u, v) \mid u \in \{a, b, c\}^*, v \in \{b, c\}^*, v = u[a|b]\}$$

$$\equiv$$

$$((a, b) + (b, b) + (c, c))^*$$

Conjugacy of a Relation

- A pair (u, v) is *conjugate* if there exist words x and y such that $u = xy$ and $v = yx$.
- In other words, u and v are cyclic shifts of each other.

  Example: $(ab, ba), (abb, bab)$.

Conjugacy of a Relation

- A pair (u, v) is *conjugate* if there exist words x and y such that $u = xy$ and $v = yx$.
- In other words, u and v are cyclic shifts of each other.

  Example:$(ab, ba), (abb, bab)$.
- Pair (x, y) is called a *cut* of (u, v). There can be several cuts for a pair.

  Example: $(abab, baba)$ have cuts (a, bab) and (aba, b).

Conjugacy of a Relation

- A pair (u, v) is *conjugate* if there exist words x and y such that $u = xy$ and $v = yx$.

  Example:$(ab, ba), (abb, bab)$.

- Pair (x, y) is called a *cut* of (u, v). There can be several cuts for a pair.

  Example: $(abab, baba)$ have cuts (a, bab) and (aba, b).

- A *set of pairs (or a relation) is conjugate* if each pair in the set is conjugate.

Conjugacy of Rational Relations

- If two rational relations R_1 and R_2 are conjugate, then
    - union of R_1 and R_2 is conjugate,

Conjugacy of Rational Relations

- If two rational relations R_1 and R_2 is conjugate, then
  - union of R_1 and R_2 is conjugate,
  - product of R_1 and R_2 need not be conjugate,

Example : $R_1 = \{(ab, ba)\}$ and $R_2 = \{(ca, ac)\}$

$R_1 \cdot R_2 = \{(abca, baac)\}$ is not conjugate.

Conjugacy of Rational Relations

- If two rational relations R_1 and R_2 is conjugate, then
  - union of R_1 and R_2 is conjugate,
  - product of R_1 and R_2 need not be conjugate, and
  - kleene star of R_1 also need not be conjugate.

Example : $R_1 = \{(ab, ba), (ca, ac)\}$

Deciding Conjugacy of a Rational Expression of Pairs

- Express the rational relation as a rational expression (E).
- Every rational expression is equivalent to a sum of sumfree expressions ($E = E_1 + E_2 + \cdots + E_k, k \geq 1$).

$$E_1 \cdot E_2 = (e+\cdots+f)(g+\cdots+h) = (e\cdot g + \cdots + f\cdot h)$$

$$E^* = (e+\cdots+f)^* = (e^* \ldots f^*)^*$$

$$E_1 + E_2 = e+\cdots+f+g+\cdots+h$$

- E is conjugate if each sumfree expressions $E_1, E_2, \ldots, E_k$ are conjugate.
- Check the existence of a common witness for each sumfree expression.

When is Kleene star of a set of pairs conjugate?

Given: A set of pairs $G = \{(u_i, v_i) \mid i \in I\}$ where I is a countable set.

Question: Are all the pairs obtained by concatenation conjugates?

sure of G: $\langle G \rangle = \{(u_{i_1} u_{i_2} \cdots u_{i_n} , v_{i_1} v_{i_2} \cdots v_{i_n}) \mid n \geq 1, i_j \in$

When is Kleene star of a set of pairs conjugate?

Given: A set of pairs $G = \{(u_i, v_i) \mid i \in I\}$ where I is a countable set.

Question: Are all the pairs obtained by concatenation conjugates?

sure of G: $\langle G \rangle = \{(u_{i_1} u_{i_2} \cdots u_{i_n}, v_{i_1} v_{i_2} \cdots v_{i_n}) \mid n \geq 1, i_j \in$

exists

→ Conjugate PCP Problem - Undecidable [4].

When are two words conjugate?

Second Theorem of Lyndon-Schützenberger[1]: Let u and v be two words. TFAE:

1. u and v are conjugate words.
2. There exists a word z such that $uz = zv$.
3. There exists words z, x and y such that $u = xy$, $v = yx$ and $z \in (xy)^*x$.

When are two words conjugate?

Second Theorem of Lyndon-Schützenberger[1]: Let u and v be two words. TFAE:

1. u and v are conjugate words.
2. There exists a word z such that $uz = zv$.
3. There exists words z, x and y such that $u = xy$, $v = yx$ and $z \in (xy)^*x$.

Witness of pair (u, v)

When are two words conjugate?

Second Theorem of Lyndon-Schützenberger[1]: Let u and v be two words. TFAE:

1. u and v are conjugate words.
2. There exists a word z such that $uz = zv$.
3. There exists words z, x and y such that $u = xy$, $v = yx$ and $z \in (xy)^*x$.

Witness of pair (u, v)

- z is an *inner witness* of (u, v) if $uz = zv$ and $z \in (xy)^*x$.
- z is an *outer witness* of (u, v) if $zu = vz$ and $z \in (yx)^*y$.
- z is a *witness* of (u, v) if z is either an inner or an outer witness of (u, v)

Witness of Set of Pairs (Common witness)

$$G = \{(u_i, v_i) \mid i \in I$$

z is a *common inner witness* of G if z is an inner witness of each pair in G.

z is a *common outer witness* of G if z is an outer witness of each pair in G.

$$z \in \bigcap_{i \in I} (x_i y_i)^* x_i$$

$$z \in \bigcap_{i \in I} (y_i x_i)^* y_i$$

z is a *common witness* of G if z is either a common inner or a common outer witness of G

Example of Common witnesses

Consider set $P = \{(ab, ba), (ac, ca)\}$

(ab, ba) has inner witnesses $(ab)^*a$ and outer witnesses $(ba)^*b$.

(ac, ca) has inner witnesses $(ac)^*a$ and outer witnesses $(ca)^*c$.

Example of Common witnesses

Consider set $P = \{(ab, ba), (ac, ca)\}$

(ab, ba) has inner witnesses $(ab)^*a$ and outer witnesses $(ba)^*b$.

(ac, ca) has inner witnesses $(ac)^*a$ and outer witnesses $(ca)^*c$.

P has one common inner witness $(ab)^*a \cap (ac)^*a = a$.

P does not have any common outer witness since $(ba)^*b \cap (ca)^*c = \emptyset$.

Example of Common witnesses

- The set $\{(ab, ba), (ac, ca)\}$ has a unique common witness a.
- The set $\{(ab, ba), (abab, baba)\}$ has infinitely many common inner witnesses $(ab)^*a$ and infinitely many common outer witnesses $(ba)^*b$.
- The set $\{(ab, ba), (ba, ab)\}$ has no common witness since $(ab)^*a \cap (ba)^*b = \emptyset$.

Number of Common witnesses

Proposition: Let G be a set of pairs. Then one of the following is true:

- G has no common witness.
- G has exactly one common witness.
- G have infinitely many common witnesses.

Theorem (Infinitary Version of Lyndon-Schützenberger Theorem)

Theorem : Let $G = \{(u_i, v_i) \mid i \in I\}$ be a set of conjugate pairs. Then the following are equivalent.

1. $\langle G \rangle$ is conjugate.
2. $\langle G \rangle$ has a common witness z.
3. G has a common witness z.
4. Roots of G has a common witness z.

Roots of a Set

- A word is *primitive* if it cannot be expressed as a power of a smaller word.

  Example: aba is a primitive word but $abab$ is not.

- *Primitive root* of a word u is the primitive word ρ_u such that $u = \rho_u^n$ for some $n \geq 1$.

  Example: ab is the primitive root of $abab$.

Roots of a Set

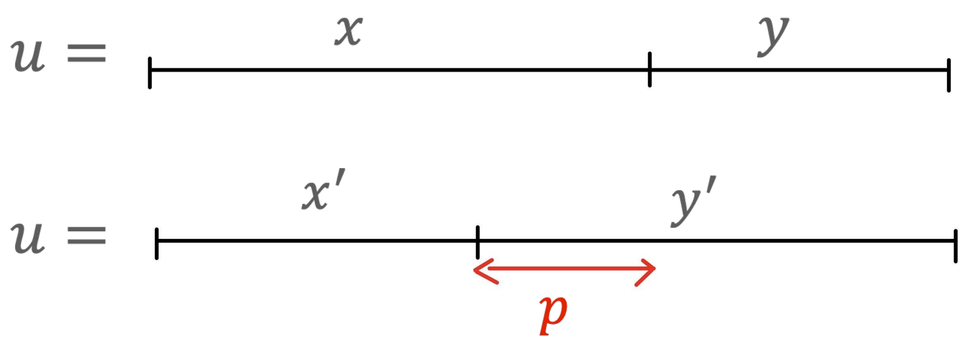
- A word is *primitive* if it cannot be expressed as a power of a smaller word.
- *Primitive root* of a word u is the primitive word ρ_u such that $u = \rho_u^n$ for some $n \geq 1$.
- *Primitive root of a pair* (u, v) is (ρ_u, ρ_v).
- *Roots of a set* P is the set of all primitive root of each pair in P.

Example: roots of the set $\{(ab, ba), (abab, baba), (bab, abb)\}$ is $\{(ab, ba), (bab, ab$

Why roots are important?

- A distinct conjugate primitive pair has a unique cut.

Assume (u, v) has two non empty cuts (x, y) and (x', y').



$$v = yx = yx'p$$

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

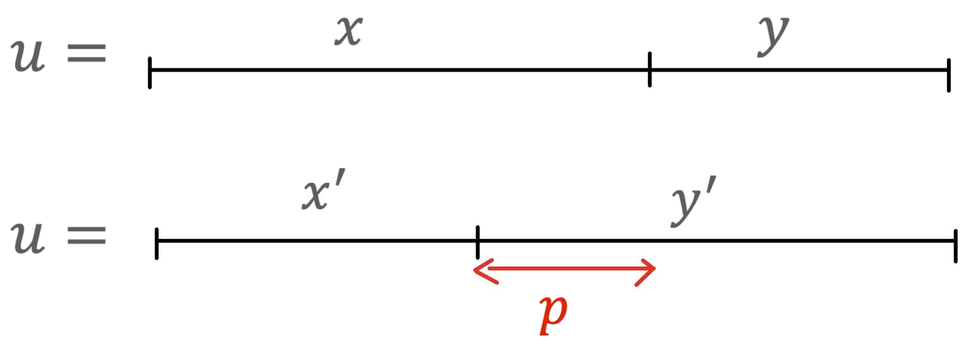
Nonempty words yx' and p commutes. Hence v is a power of a smaller word.

(First Lyndon-Schützenberger Theorem: Two words x and y commute iff they are power of a same word)

Why roots are important?

- A distinct conjugate primitive pair has a unique cut.

Assume (u, v) has two non empty cuts (x, y) and (x', y').



$$v = yx = yx'p$$

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

Nonempty words yx' and p commutes. Hence v is a power of a smaller word.

- If $u = v$, the only possible cuts are (u, ϵ) and (ϵ, u).

Why roots are important? - Cut Lemma

Cut Lemma:

- Assume (u, v) is a conjugate primitive pair with the cut (x, y). The following equalities cannot hold for any nonempty words x', x'', y', y'' such that $x = x'x''$ and $y = y'y''$.
  - $xy = x''yx'$
  - $xy = y''xy'$
  - $yx = y''xy'$
  - $yx = x''yx'$

Why roots are important? - Cut Lemma

Cut Lemma:

- Assume (u, v) is a conjugate primitive pair with the cut (x, y). The following equalities cannot hold for any nonempty words x', x'', y', y'' such that $x = x'x''$ and $y = y'y''$.
  - $xy = x''yx'$
  - $xy = y''xy'$
  - $yx = y''xy'$
  - $yx = x''yx'$

Since $(xy, yx) = (x''yx', yx'x'')$, there exist a different nonempty cut (x'', yx') for (u, v) .

Why roots are important? - Cut Lemma

Consequences of Cut Lemma:

- Any cut of the pair (u^n, v^n) for $n \geq 1$ is of the form $((xy)^*x, (yx)^*y)$, where (u, v) is a primitive pair with the cut (x, y).

$$u^n = xvxv \cdots x$$

$$v^n = vxvx \cdots v$$

Why roots are important? - Cut Lemma

Consequences of Cut Lemma:

- Any cut of the pair (u^n, v^n) for $n \geq 1$ is of the form $((xy)^*x, (yx)^*y)$, where (u, v) is a primitive pair with the cut (x, y).

Corollary:

- z is a witness of (u, v) iff z is a witness of (ρ_u, ρ_v).
- z is a witness of a set G iff z is a witness of roots of G.

Why roots are important? - Equal Length Lemma

Equal Length Lemma:

- Let (u_1, v_1) and (u_2, v_2) be conjugate primitive pairs of equal length, 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 $y_1 = y_2$.
- Can be extended to any number of pairs.

Why roots are important? - Equal Length Lemma

Equal Length Lemma:

- Let (u_1, v_1) and (u_2, v_2) be conjugate primitive pairs of equal length, 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 $y_1 = y_2$.
- Can be extended to any number of pairs.

Corollary:

- If $\langle G \rangle$ is conjugate and all the pairs in roots of G are of equal length, then roots of G has a common witness (either x_i's are equal or y_i's are equal).

Theorem (Infinitary Version of Lyndon-Schützenberger Theorem)

Theorem : Let $G = \{(u_i, v_i) \mid i \in I\}$ be a set of conjugate pairs. Then the following are equivalent.

1. $\langle G \rangle$ is conjugate.
2. $\langle G \rangle$ has a common witness z.
3. G has a common witness z.
4. Roots of G has a common witness z.

We prove $(4) \Longrightarrow (3) \Longrightarrow (2) \Longrightarrow (1) \Longrightarrow (4)$

Theorem (Infinitary Version of Lyndon-Schützenberger Theorem)

Theorem : Let $G = \{(u_i, v_i) \mid i \in I\}$ be a set of conjugate pairs. Then the following are equivalent.

1. $\langle G \rangle$ is conjugate.
2. $\langle G \rangle$ has a common witness z.
3. G has a common witness z.
4. Roots of G has a common witness z.

Corollary of Cut Lemma

We prove $(4) \Longrightarrow (3) \Longrightarrow (2) \Longrightarrow (1) \Longrightarrow (4)$

Theorem (Infinitary Version of Lyndon-Schützenberger Theorem)

Theorem : Let $G = \{(u_i, v_i) \mid i \in I\}$ be a set of conjugate pairs. Then the following are equivalent.

1. $\langle G \rangle$ is conjugate.
2. $\langle G \rangle$ has a common witness z.
3. G has a common witness z.
4. Roots of G has a common witness z.

From Second theorem of Lyndon-Schützenberger

We prove $(4) \Longrightarrow (3) \Longrightarrow (2) \Longrightarrow (1) \Longrightarrow (4)$

Theorem (Infinitary Version of Lyndon-Schützenberger Theorem)

Theorem : Let $G = \{(u_i, v_i) \mid i \in I\}$ be a set of conjugate pairs. Then the following are equivalent.

1. $\langle G \rangle$ is conjugate.
2. $\langle G \rangle$ has a common witness z.
3. G has a common witness z.
4. Roots of G has a common witness z.

Prove for finite number of pairs and later extend to infinite pairs.

We prove $(4) \Longrightarrow (3) \Longrightarrow (2) \Longrightarrow (1) \Longrightarrow (4)$

$\langle G \rangle$ is conjugate $\Longrightarrow$ Roots of G has a common witness

Strategy: extensive case analysis.

Main Lemmas Used:

- Cut Lemma
- Equal Length Lemma
- Conjugate Fine and Wilf Theorem [2]

> For any two words u and v, 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.

$\langle G \rangle$ is conjugate $\Longrightarrow$ Roots of G has a common witness

- Let G be a finite set of k pairs.
- When $k = 1$,
  - G contains only one pair (u, v) and by assumption it is conjugate.
  - From Lyndon-Schützenberger theorem, (u, v) has a witness.
  - Roots of $G = \{(\rho_u, \rho_v)\}$ has witnesses same as that of (u, v).

$\langle G \rangle$ is conjugate $\Longrightarrow$ Roots of G has a common witness

- Let G be a finite set of k pairs.
- When $k > 1$,
  - Let $\approx$ be the equivalence relation on G whereby

    $(u, v) \approx (u', v')$ if ρ_u is conjugate to $\rho_{u'}$
  - Assume $\approx$ has d equivalence classes.

$\langle G \rangle$ is conjugate $\Longrightarrow$ Roots of G has a common witness

- Let G be a finite set of k pairs.
- When $k > 1$,
  - Let $\approx$ be the equivalence relation on G whereby

    $(u, v) \approx (u', v')$ if ρ_u is conjugate to
  - Assume $\approx$ has d equivalence classes.
  - If $d = 1$, then the primitive roots of all pairs in G are conjugates to each other.

↓

All pairs in roots of G are of equal length and $\langle G \rangle$ is conjugate.

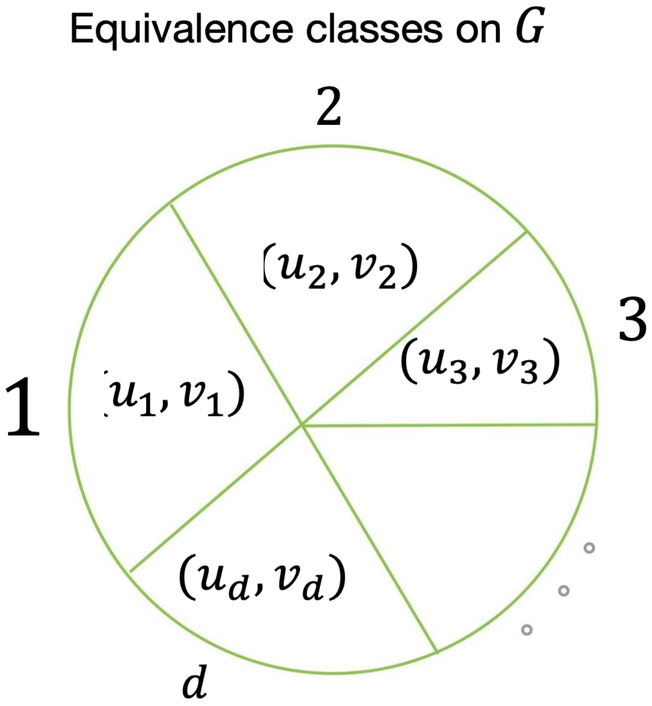
↓

Roots of G has a common witness using Equal length Lemma.

$\langle G \rangle$ is conjugate $\Longrightarrow$ Roots of G has a common witness

- Let G be a finite set of k pairs.
- When $k > 1$,
  - Let $\approx$ be the equivalence relation on G whereby

    $(u, v) \approx (u', v')$ if ρ_u is conjugate to $\rho_{u'}$
  - Assume $\approx$ has d equivalence classes.
  - Assume $d > 1$,



Choose d pairs $(u_1, v_1), (u_2, v_2), \ldots (u_d, v_d)$ from each equivalence class.

We construct a pair $(u, v) \in (u_1, v_1)^* (u_2, v_2)^* \cdots (u_d, v_d)^* \subseteq \langle G \rangle$.

Show that (u, v) is conjugate only if roots of G has a common witness.

$\langle G \rangle$ is conjugate $\Longrightarrow$ Roots of G has a common witness

- Proved when G is a finite set of pairs.
- When G is an infinite set of pairs:

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.

$\langle G \rangle$ is conjugate $\rightarrow$ Closure of every finite subset G_f is conjugate $\rightarrow$ Roots of G_f, G_f has a common witness

By Compactness Theorem, G has a common witness $\rightarrow$ Roots of G has a common witness

Theorem (Infinitary Version of Lyndon-Schützenberger Theorem)

Theorem : Let $G = \{(u_i, v_i) \mid i \in I\}$ be a set of conjugate pairs. Then the following are equivalent.

1. $\langle G \rangle$ is conjugate.
2. $\langle G \rangle$ has a common witness z.
3. G has a common witness z.
4. Roots of G has a common witness z.

We prove $(4) \Longrightarrow (3) \Longrightarrow (2) \Longrightarrow (1) \Longrightarrow (4)$ ✓ ✓ ✓ ✓

Theorem (Infinitary Version of Lyndon-Schützenberger Theorem)

Theorem : Let $G = \{(u_i, v_i) \mid i \in I\}$ be a set of conjugate pairs. Then the following are equivalent.

1. $\langle G \rangle$ is conjugate.
2. $\langle G \rangle$ has a common witness z.
3. G has a common witness z.
4. Roots of G has a common witness z.

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

Common Witness Theorem of a Sumfree Expression

Theorem: A sumfree expression of pairs is conjugate if and only if it has a common witness.

- This does not generalise to arbitrary regular expression.
- Example : $(ab, ba)^* + (ba, ab)^*$ is an infinite conjugate set but does not have a common witness.

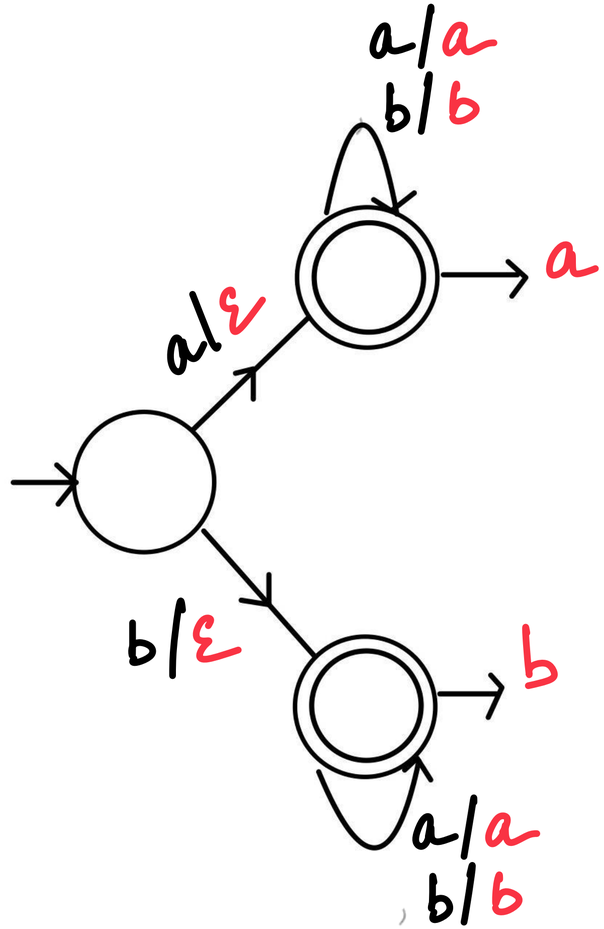
Deciding Conjugacy of a Rational Relation

- Express the rational relation as a rational expression (E).
- Every rational expression is equivalent to a sum of sumfree expressions ($E = E_1 + E_2 + \cdots + E_k, k \geq 1$).
- E is conjugate if each sumfree expressions $E_1, E_2, \ldots, E_k$ are conjugate.
- Check the existence of a common witness for each sumfree expression.

Application : Comparing Transducers

Finite State Transducers

- Finite state automata that reads an input word and produces zero or more output words.
- Example: $aw \mapsto wa$ and $bw \mapsto wb$
- Functional Transducers*:* every input has at most one output.



Comparing Transducers

- Functional Equivalence - decidable [7]
- Can we meaningfully compare two inequivalent transducers?
    - On any input, the respective outputs are “approximately” the same?
    - Convert one output to another using few “edits”?

Comparing Transducers

- Functional Equivalence
- Can we meaningfully compare two inequivalent transducers?
    - On any input, the respective outputs are “approximately” the same?
    - Convert one output to another using few “edits”?
    - Edits? - Ex: substitute a letter with another, insert a letter, or delete a letter.
    - The number of such edits needed can indicate some “distance” between the words.

Levenshtein Edit Distance

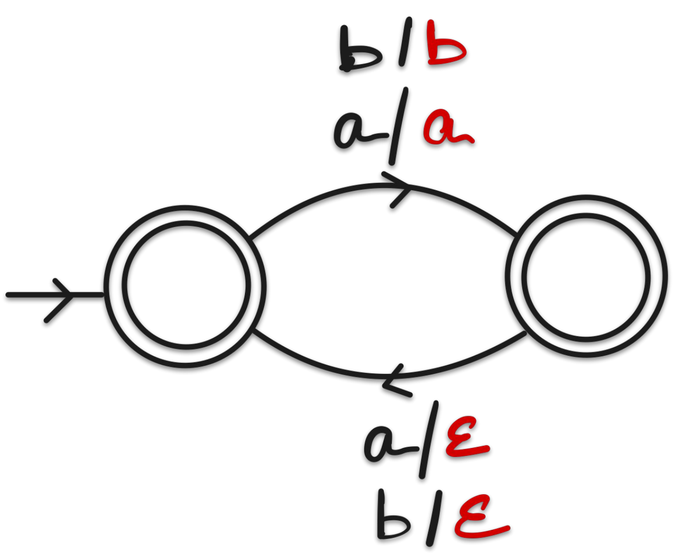
- Levenshtein edit distance between two words u and v is the minimum number of insertions,deletions and substitutions required to convert u to v.

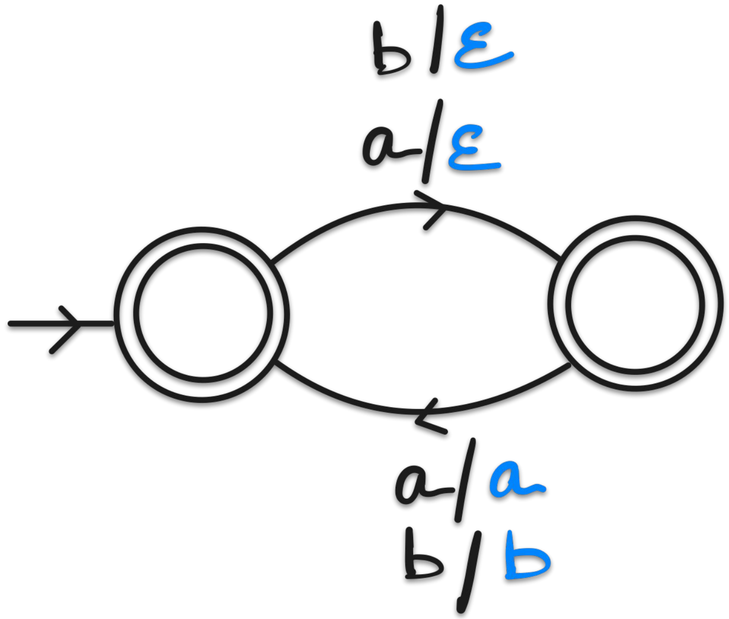
Levenshtein Edit Distance

- Levenshtein edit distance between two words u and v is the minimum number of insertions,deletions and substitutions required to convert u to v.

- Two transducers T_1 and T_2 are close w.r.t Levenshtein edit distance, if there exist a number k such that on any input , the output of T_1 can be converted to output of T_2 with at most k edits.

T_1 and T_2 are not close - Example



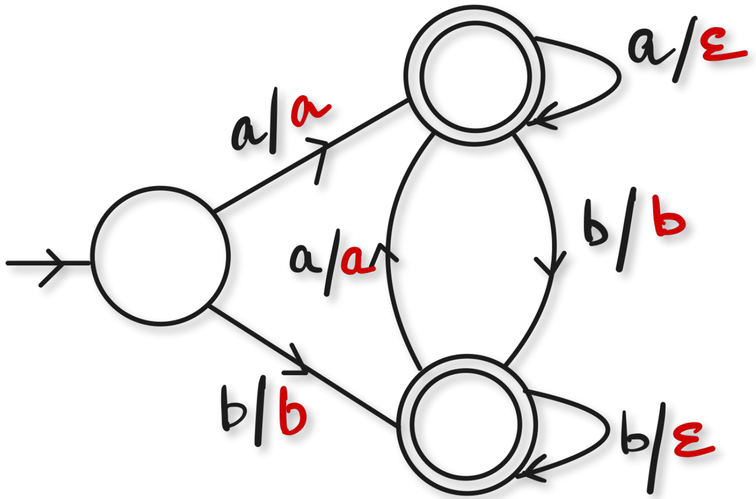


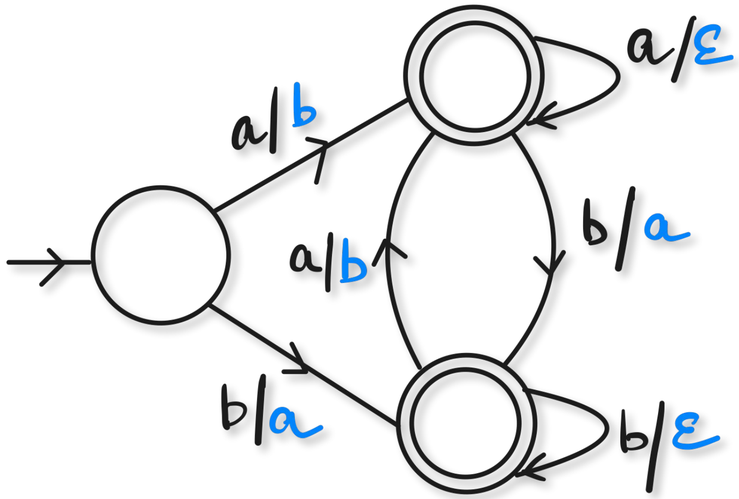
T_1: Output letters at odd positions

T_2:Output letters at even positions

$$(ab)^n \rightarrow (a^n, b^n)$$

T_1 and T_2 are close - Example





- For each block of a, outputs a
- For each block of b, outputs b

- For each block of a, outputs b
- For each block of b, outputs a

$$aaabbabbba \rightarrow (ababa, babab)$$

Levenshtein Edit Distance

- Levenshtein edit distance between two words u and v is the minimum number of insertions,deletions and substitutions required to convert u to v.

- Two transducers T_1 and T_2 are close w.r.t Levenshtein edit distance, if there exist a number k such that on any input , the output of T_1 can be converted to output of T_2 with at most k edits.

T_1 and T_2 are close iff all the cycles in $T_1 \times T_2$ are conjugates.

Future Work

- Computing the complexity of deciding conjugacy of a rational relation.
- Comparing two transducers based on the structural similarity of their outputs.
- Repair Problem: Given two functional transducers T_1 and T_2, does there exist a functional transducer T such that T_2 can be obtained as a cascading composition of T_1 and T.

References

1. Lothaire, M., Combinatorics on words, Addison-Wesley, 1983.

2. Christian Choffrut and Juhani Karhumaki . Combinatorics of words, Handbook of Formal Languages, volume 1,pages 329-438, 1997.

3. Roger C Lyndon, Marcel-Paul Schützenberger, et al. The equation am=bn cp in a free group. Michigan Math. J, 9(4):289-298, 1962.

4. Vesa Halava, Tero Harju, and Esa Sahla. The conjugate post correspondence problem. CoRR, 2021.

5. Calvin C Elgot and Jorge E Mezei . On relations defined by generalised finite automata. IBM Journal of Research and development, 9(1):47-68, 1965.

6. Christian Choffrut. Minimising subsequential transducers: a survey. Theoretical Computer Science, 2003.

7. Gurari . The equivalence problem for deterministic two-way sequential transducers is decidable. SIAM Journal on Computing, 1982

Thank you

Appendix

Rational Relations

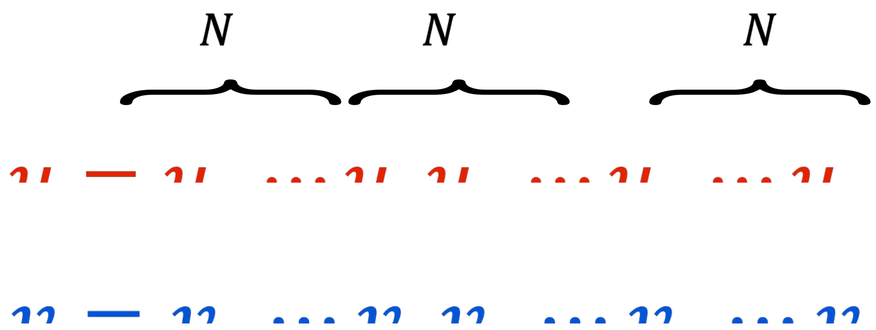
- A binary relation over two free monoids A^* and B^* is a subset of $A^* \times B^*$
- A relation is rational if it can built out of finite subsets of $A^* \times B^*$ using the operations union, product and Kleene star.

$$X \cdot Y = \{(u_1 u_2, v_1 v_2) \mid (u_1, v_1) \in X, (u_2, v_2)$$

$$X^* = X^0 \cup X^1 \cup \cdots$$

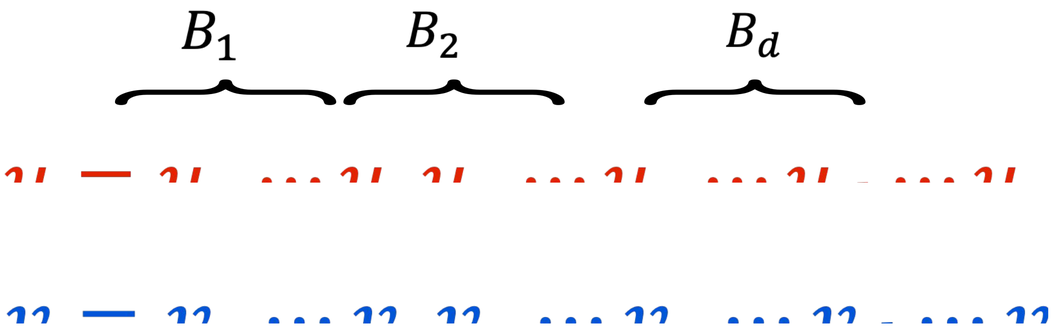
where X^i *is defined inductively as* $X^0 = (\epsilon, \epsilon)$, *and* $X^i = X^{i-1} \cdot X$, *for* $i > 0$

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness



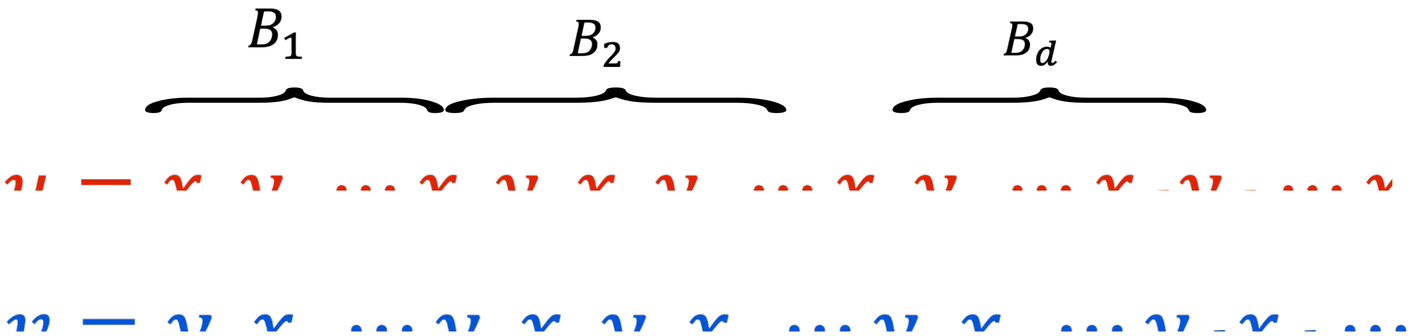
Where $N > 2\ell$ (Fine and Wilf index of any two pairs

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness



- Since (u, v) is conjugate, there exist a cut (p, q).
- We do a case analysis on all possible cuts in u.
  - Cut in u within first block B_1.
  - Cut in u within the last block B_d.
  - Cut is within the block B_j where $1 < j < k$.

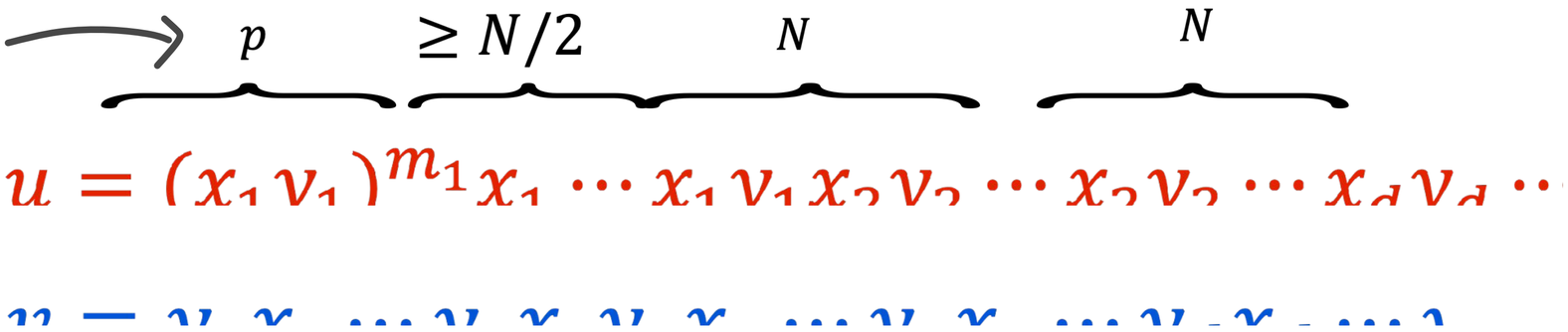
(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness



- Substituting (u_i, v_i) with powers of $(x_i y_i, y_i x_i)$.
- When the cut is in the first block B_1
  - Within the first half of the block B_1
  - Within the second half of the block B_1

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness

By Cut Lemma



- When the cut in u within the first half of the first block B_1.
- $|p| \leq N/2$

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness

By Cut Lemma

$$u = \overbrace{(x_1 y_1)^{m_1}}^{p} \overbrace{x_1 (y_1 x_1)^{n_1}}^{q_1} \overbrace{y_1 x_2 y_2 \cdots x_2 y_2 \cdots x_d y_d}^{N} \cdot \overbrace{\quad}^{N}$$

$$v = \underbrace{(y_1 x_1)^{n_1}}_{q_1} y_1 x_1 \cdots y_1 x_1 y_2 x_2 \cdots y_2 x_2 \cdots y_d x_d \cdots$$

- When the cut in u within the first half of the first block B_1.
- $|p| \leq N/2$

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness

By Cut Lemma

$$u = \overbrace{(x_1 y_1)^{m_1}}^{p} \overbrace{x_1 (y_1 x_1)^{n_1}}^{q_1} \overbrace{y_1 x_2 y_2 \cdots x_2 y_2 \cdots x_d y_d}^{N} \cdot \overbrace{\quad}^{N}$$

$$v = \underbrace{(y_1 x_1)^{n_1}}_{q_1} \underbrace{y_1 (x_1 y_1)^{m_1}}_{p} x_1 y_2 x_2 \cdots y_2 x_2 \cdots y_d x_d \cdot$$

- When the cut in u within the first half of the first block B_1.
- $|p| \leq N/2$

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness

$$u = \overbrace{(x_1 y_1)^{m_1} x_1 (y_1 x_1)^{n_1} y_1}^{p\ q_1} \overbrace{(x_2 y_2)^{m_2} x_2 (y_2 x_2)^{n_2} y_2}^{p\ q_2} \cdots \overbrace{(x_d y_d)^{m_d} x_d}^{p\ q_d}$$

$$v = \underbrace{(y_1 x_1)^{n_1} y_1}_{q_1} \underbrace{(x_1 y_1)^{m_1} x_1}_{p} \underbrace{(y_2 x_2)^{n_2} y_2}_{q_2} \underbrace{(x_2 y_2)^{m_2} x_2}_{p} \cdots \underbrace{(y_d x_d)^{n_d} y_d}_{q_d\ p}$$

- When the cut in u within the first half of the first block B_1.
- $|p| \leq N/2$

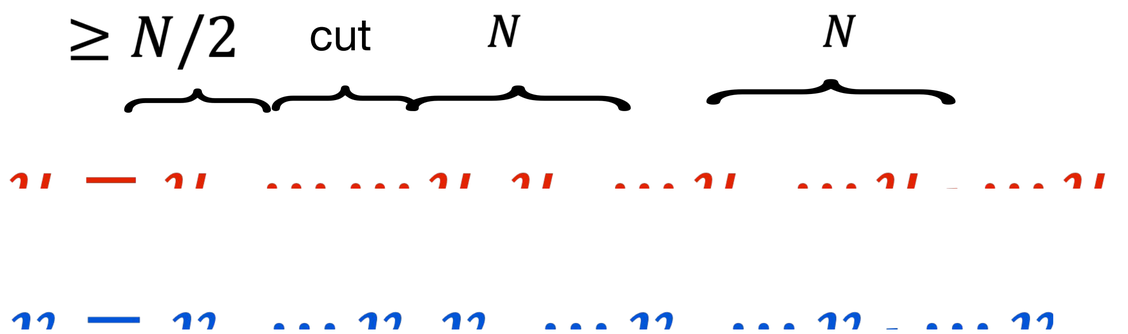
(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness

$$u = \overbrace{(x_1y_1)^{m_1}x_1}^{p}\overbrace{(y_1x_1)^{n_1}y_1}^{q_1}\overbrace{(x_2y_2)^{m_2}x_2}^{p}\overbrace{(y_2x_2)^{n_2}y_2}^{q_2}\cdots\overbrace{(x_dy_d)^{m_d}x_d}^{p}\overbrace{(y_dx_d)^{n_d}y_d}^{q_d}$$

$$v = \underbrace{(y_1x_1)^{n_1}y_1}_{q_1}\underbrace{(x_1y_1)^{m_1}x_1}_{p}\underbrace{(y_2x_2)^{n_2}y_2}_{q_2}\underbrace{(x_2y_2)^{m_2}x_2}_{p}\cdots\underbrace{(y_dx_d)^{n_d}y_d}_{q_d}\underbrace{(x_dy_d)^{m_d}x_d}_{p}$$

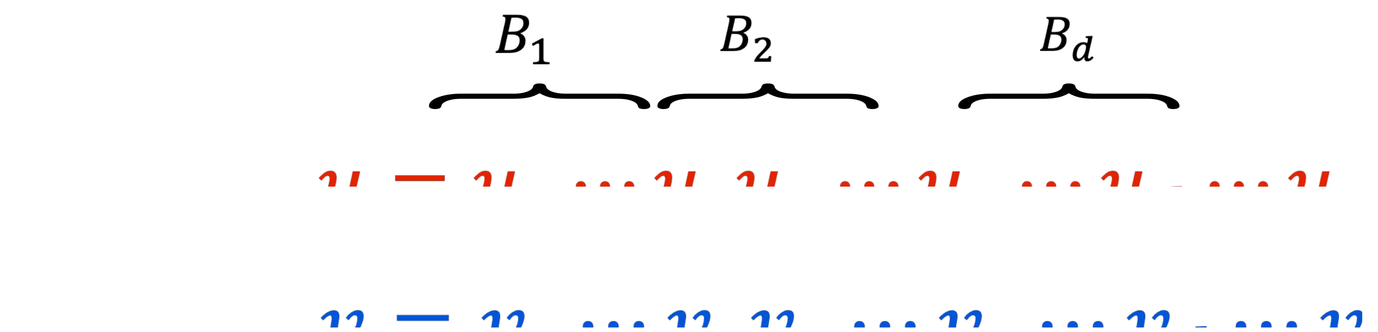
- When the cut in u within the first half of the first block B_1.
- $p = (x_1y_1)^{m_1}x_1 = (x_2y_2)^{m_2}x_2 = \cdots = (x_dy_d)^{m_d}x_d$
- Thus, Roots of G has a common witness.

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness



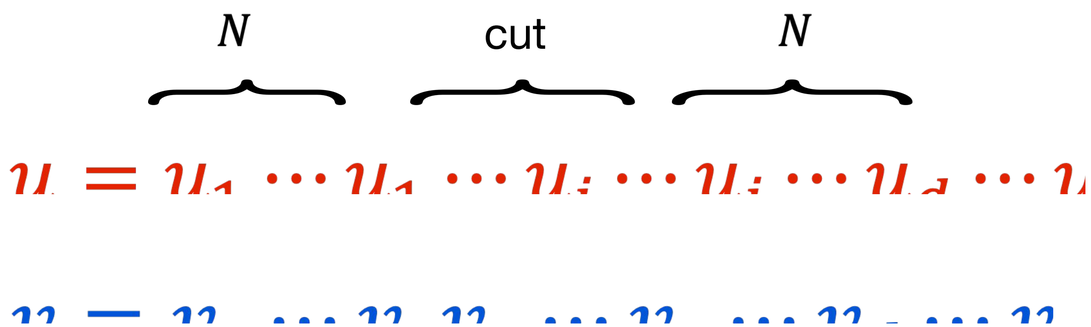
- When the cut in u within the second half of the first block B_1.
- Block of v_1's and u_1's share a common factor of length atleast $N/2 > \ell$.
- From Conjugate Fine and Wilf Theorem, ρ_{v_1} is conjugate to ρ_{u_1}.
- Contradicts that (u_1, v_1) and (u_2, v_2) belongs to different equivalence classes.

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness



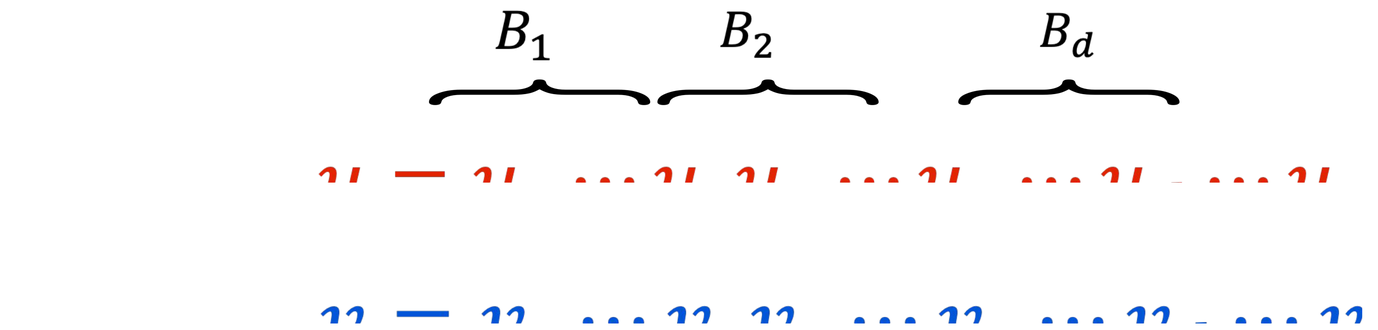
- Since (u, v) is conjugate, there exist a cut (p, q).
- We do a case analysis on all possible cuts in u.
  - Cut in u within first block B_1.
  - Cut in u within the last block B_d : symmetric
  - Cut is within the block B_j where $1 < j < k$.

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness



- When the cut in u is within the block B_j for $1 < j < k$.
- Block of v_1's and u_j's share a common factor of length atleast $N/2 > \ell$.
- From Conjugate Fine and Wilf Theorem, ρ_{v_1} is conjugate to ρ_{u_j}.
- Contradicts that (u_1, v_1) and (u_j, v_j) belongs to different equivalence classes.

(u, v) is conjugate $\Longrightarrow$ Roots of G has a common witness



- Since (u, v) is conjugate, there exist a cut (p, q).
- We do a case analysis on all possible cuts in u.
  - Cut in u within first block B_1.
  - Cut in u within the last block B_d : symmetric
  - Cut is within the block B_j where $1 < j < k$.

Proof of Compactness Theorem

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.

- There are two cases:
  - There exists a finite subset with unique common witness, say z.
  - Every finite subset has infinitely many witnesses.

Proof of Compactness Theorem

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.**

- Case 1: There exists a finite subset G_f with unique common witness, say z.
  - For any pair (u, v) in G, the finite subset $G_f \cup \{(u, v)\}$ has common witness.
  - Infact z is the common witness of $G_f \cup \{(u, v)\}$.
  - Therefore, z is a witness of any pair in G.
  - Thus, z is a common witness of G.

Proof of Compactness Theorem

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.**

- Case 2: Every finite subset has infinitely many witnesses.
  - Take any two pairs (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 common witnesses.
  - Both (u_i, v_i) and (u_j, v_j) have same primitive root.
  - Primitive root of any pair in G is the same. Hence G have common witnesses same as that of the witnesses of its primitive root.

Metric on words

A metric on words over the alphabet A is a function $d: A^* \times A^* \to [0, \infty]$ such that for any words u, v and w in A^*

- $d(u,u) = 0$
- $d(u,v) = d(v,u)$
- $d(u,v) \leq d(u,w) + d(w,v)$

Example: discrete metric

$$d(u,v) = \begin{cases} 0 & if\, u = v \\ \infty & otherwise \end{cases}$$

Closeness and k- closeness of Transducers

Transducers T_1 and T_2 are k-close, $k \geq 0$, w.r.t metric d if $d(T_1, T_2) \leq k$.

Transducers T_1 and T_2 are close if they are k-close for some $0 \leq k < \infty$, i.e., $d(T_1, T_2) < \infty$.

Are T_1 and T_2 close (or k-close) w.r.t a metric d?

Distance Problem

- Closeness and k-closeness are respectively a boundedness and upperbounded problem on distance.

Proposition:

Let d be an integer-valued metric. The distance problem w.r.t d is computable if and only if k-closeness and closeness problems w.r.t d are decidable.

Some Metrics

- Discrete Metric

$$d_\infty(u,v) = \begin{cases} 0 & if\, u = v \\ \infty & otherwise \end{cases}$$

Closeness w.r.t to discrete metric ≡ Equivalence of two transducers.

If T_1 and T_2 have different domain

or

$d_\infty(T_1, T_2) = \infty$

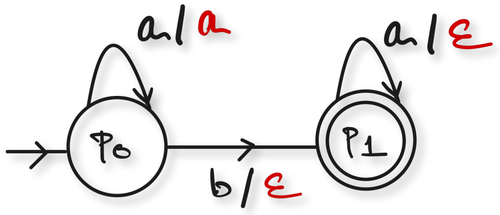
If there exist a word w such that $T_1(w) \neq T_2(w)$

Some Metrics

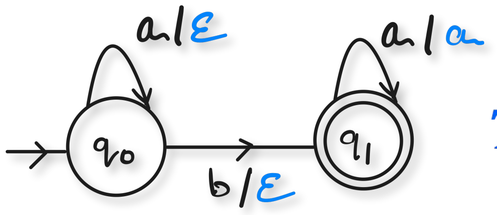
- Discrete Metric
- Levenshtein Edit Distance - insertions, deletion and substitutions
- Conjugacy Distance - cyclic shifts
- Hamming Distance - substitutions
- Transposition Distance - swapping adjacent letters
- Longest Common Subsequence - insertions and deletions
- Damerau Levenshtein Edit distance - insertion, deletion, substitution and transpositions

Closeness w.r.t Levenshtein or Conjugacy Distance

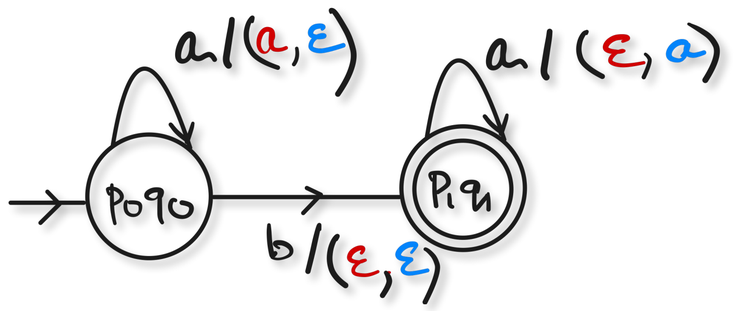
- Given two transducers: T_1, T_2
- Check if their domains are identical – Equivalence of DFAs
- Construct a Cartesian product of T_1 and T_2



T_1: Output a's before b



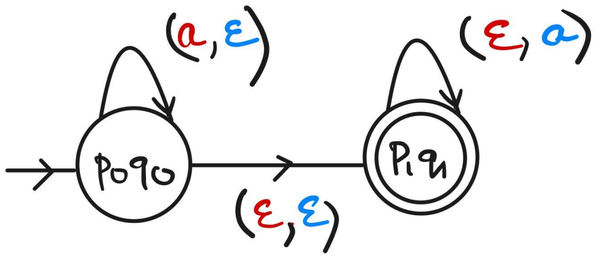
T_2: Output a's after b



Cartesian Product of T_1 and T_2

Closeness w.r.t Levenshtein or Conjugacy Distance

- Given two transducers: T_1, T_2
- Check if their domains are identical – Equivalence of DFAs
- Construct a Cartesian product of T_1 and T_2
- Construct a rational (or regular) expression for set of output pairs.



$(a, \epsilon)^*(\epsilon, \epsilon)(\epsilon, a)$

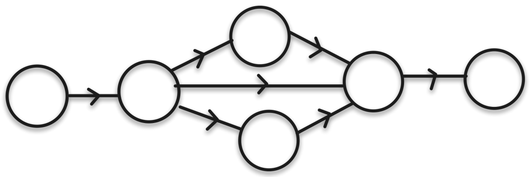
Closeness w.r.t Levenshtein or Conjugacy Distance

- Given two transducers: T_1, T_2
- Check if their domains are identical – Equivalence of DFAs
- Construct a Cartesian product of T_1 and T_2
- Construct a rational (or regular) expression for set of output pairs.
  - For **Conjugacy distance**: check Conjugacy of the rational expression.
  - For **Levenshtein distance**: check if there exists a k such that $d(u, v) \leq k$ for any pair (u, v) belonging to the expression.

Closeness w.r.t Levenshtein or Conjugacy Distance

- Given two transducers: T_1, T_2
- Check if their domains are identical – Equivalence of DFAs
- Construct a Cartesian product of T_1 and T_2
- Construct a rational (or regular) expression for set of output pairs.

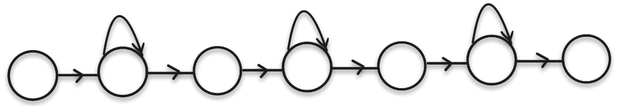
  - For Conjugacy distance: check Conjugacy of the rational expression.
  - For Levenshtein distance?
    - If the expression has no Kleene star - $d(T_1, T_2)$ is finite.



Closeness w.r.t Levenshtein or Conjugacy Distance

- Given two transducers: T_1, T_2
- Check if their domains are identical – Equivalence of DFAs
- Construct a Cartesian product of T_1 and T_2
- Construct a rational (or regular) expression for set of output pairs.

  - For Conjugacy distance: check Conjugacy of the rational expression.
  - For Levenshtein distance?
    - If the expression has no Kleene star - $d(T_1, T_2)$ is finite.
    - If it has Kleene star?



Cycles needs to be Conjugate

If $E = (\alpha_1, \beta_1)F^*(\alpha_2, \beta_2)$ has bounded distance then F^* is conjugate.

Cycles needs to be Conjugate

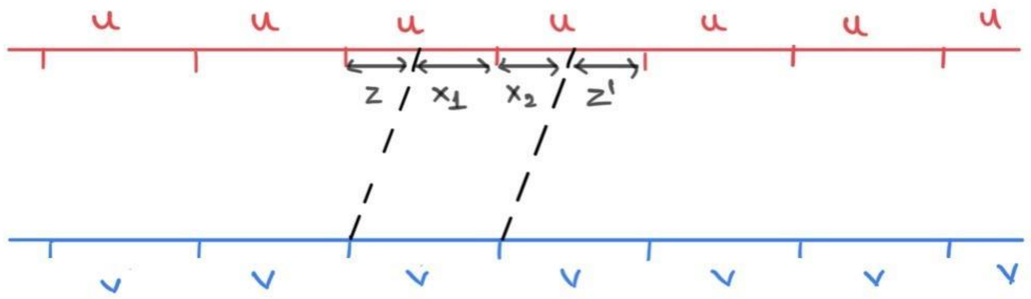
If $E = (\alpha_1, \beta_1)F^*(\alpha_2, \beta_2)$ has bounded distance then F^* is conjugate.

Assume E has bounded distance k.

Let (u, v) be a pair in F^*.

Consider pair $(\alpha_1, \beta_1)(u^\ell, v^\ell)(\alpha_2, \beta_2)$ where $\ell = 2^k$.

Since $\ell \gg k$ and $d((\alpha_1, \beta_1)(u^\ell, v^\ell)(\alpha_2, \beta_2)) \leq k$, there exists large portions of u's and v's that match.



Cycles needs to be Conjugate

If $E = (\alpha_1, \beta_1)F^*(\alpha_2, \beta_2)$ has bounded distance then F^* is conjugate.

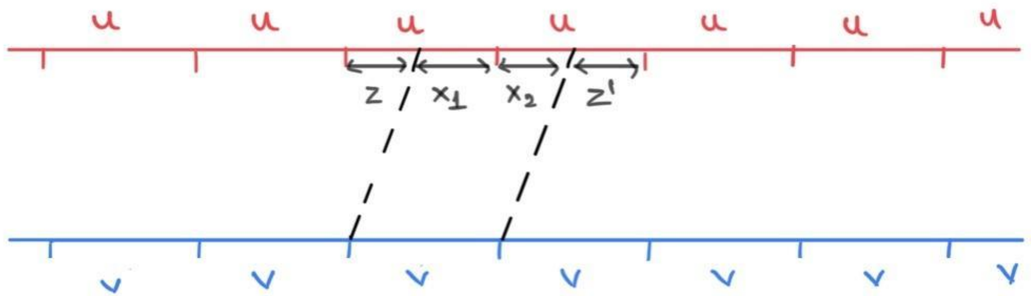
Assume E has bounded distance k.

Let (u, v) be a pair in F^*.

Consider pair $(\alpha_1, \beta_1)(u^\ell, v^\ell)(\alpha_2, \beta_2)$ where $\ell = 2^k$.

Since $\ell \gg k$ and $d((\alpha_1, \beta_1)(u^\ell, v^\ell)(\alpha_2, \beta_2)) \leq k$, there exists large portions of u's and v's that match.

$|u| = |v| \Longrightarrow v$ is a factor of uu .



As shown in fig, $v = x_1x_2$, $u = zx_1$ and $u = x_2z$.

Since $|u| = |v|$, $|z| = |x_2|$ that implies $z = x_2$ (since $u = zx_1 = x_2z$).

Closeness w.r.t Levenshtein or Conjugacy Distance

- Given two transducers: T_1, T_2
- Check if their domains are identical – Equivalence of DFAs
- Construct a Cartesian product of T_1 and T_2
- Construct a rational (or regular) expression for set of output pairs.

  - For **Conjugacy distance**: check Conjugacy of the rational expression.
  - For **Levenshtein distance**?
    - If the expression has no Kleene star - $d(T_1, T_2)$ is finite.
      - If it has Kleene star - Check if it is conjugate.