Application: word problems

Peter Mayr

Computability Theory, February 10, 2021

Rewriting systems

Book, Otto. String-rewriting Systems. 1993.

Example

Presentation of a monoid (semigroup with 1):

$$\langle \underbrace{a, b}_{\text{generators } \Sigma} \ : \ \underbrace{ab \overset{\rightarrow}{=} 1, ba \overset{\rightarrow}{=} 1}_{\text{relations}} \rangle$$

operation is concatenation

$a\underbrace{ba}_{1}a \overset{\rightarrow}{=} a1a = aa$

$abaa \overset{*}{\longleftrightarrow}_R baaa$

$[u]_R$ is the equivalence class of $u \in \Sigma^*$ w.r.t. $\overset{*}{\longleftrightarrow}_R$

$\Sigma^*/\overset{*}{\longleftrightarrow}_R = \{ [a^n], [b^n] : n \in \mathbb{N} \}$

Definition

- A **string rewriting system (SRS)** R over a finite alphabet Σ is a subset of $\Sigma^* \times \Sigma^*$ (rewriting rules).
- For $u, v \in \Sigma^*$

  $$u \to_R v$$

  if $\exists (\ell, r) \in R \; \exists x, y \in \Sigma^* : \; u = x\ell y, v = xry.$
- $\overset{*}{\leftrightarrow}_R$ is the reflexive, transitive, symmetric closure of $\to_R$. Then $\overset{*}{\leftrightarrow}_R$ is a congruence on the free monoid $(\Sigma^*, \cdot)$.
- $M_R := \Sigma^* / \overset{*}{\leftrightarrow}_R$ is the monoid **presented by** $\langle \Sigma : \; R \rangle$.

Word problem for semigroups

Word problem for SRS R on Σ

Input: $u, v \in \Sigma^*$
Question: Is $u \overset{*}{\leftrightarrow}_R v$?

Theorem (Post 1947)

There exist a finite SRS with undecidable word problem (c.e. but not computable).

Proof idea

Encode DTM as SRS in the following.

DTM as SRS

Let $M = (Q, \Sigma, \Gamma, s, t, r, \delta)$ be a DTM with bi-infinite tape.

Consider a configuration $(q, \ \dots \sqcup a_\ell \dots a_r \sqcup \dots, \ n)$ as string

state   tape content   position

$$h \underbrace{a_\ell \dots a_{n-1}}\, q \underbrace{a_n \dots a_r}\, h$$

delimiter

over $\Omega := Q \mathbin{\dot\cup} \Gamma \mathbin{\dot\cup} \{h, \underbrace{t_1, t_2}_{\text{copies of } t}\}$.

Define SRS $S(M)$. For $a, a', b \in \Gamma, q, q' \in Q$ let

1. $qa \to a'q'$ if $\delta(q, a) = (q', a', +1)$
2. $qh \to a'q'h$ if $\delta(q, \sqcup) = (q', a', +1)$
3. $bqa \to q'ba'$ if $\delta(q, a) = (q', a', -1)$
4. $hqa \to hq' \sqcup a'$ if $\delta(q, a) = (q', a', -1)$

encoding transitions on configuration.

5. $t \to t_1$
6. $t_1 a \to t_1$
7. $a t_1 h \to t_1 h$
8. $h t_1 h \to t_2$

Once in accepting state t, deletes the tape

Rewriting configurations

Lemma

For $u, v, u', v' \in \Gamma^*$ and $q, q' \in Q$ TFAE:

1. $(q,\ \sqcup uv \sqcup,\ \text{position of } v_1) \vdash_M^* (q',\ \sqcup u'v' \sqcup,\ \text{position of } v_1')$
2. $\exists m, n \in \mathbb{N} :\ huqvh \xrightarrow{*}_{S(M)} h\sqcup^m u'q'v'\sqcup^n h$

Proof.

1. $\Rightarrow$ 2. is clear by definition of the rewriting rules 1-4.
2. $\Rightarrow$ 1. follows since in item 2. only rules 1-4 are applied as no t_1, t_2 are introduced. □

Corollary

Let $x \in \Sigma^*$. Then $hsxh \xrightarrow{*}_{S(M)} t_2$ iff $x \in L(M)$.

starting config

accepting config

Proof.

t_2 can only be introduced from an accepting configuration via rules 5-8. Almost done. But $\Leftrightarrow$ is not a one-way street. □

Reducing equivalence to rewriting

Lemma

Let $w \in \Omega^*$. Then $w \overset{*}{\leftrightarrow}_{S(M)} t_2$ iff $w \overset{*}{\rightarrow}_{S(M)} t_2$.

Proof. $\Leftarrow$ easy

$\Rightarrow$: Assume $w \overset{*}{\leftrightarrow}_{S(M)} t_2$.

- Either $w = t_2$ or $w = huqvh$ for some $u, v \in \Gamma^*, q \in Q \cup \{t_1\}$ since no rule changes the number of "states" $Q \cup \{t_1, t_2\}$.
- Consider a **shortest path** connecting $w \neq t_2$ and t_2 via the symmetric closure $\leftrightarrow = \leftarrow \cup \rightarrow$:

$$w = huqvh = w_0 \leftrightarrow w_1 \leftrightarrow \cdots \leftrightarrow w_k = t_2$$

- Then $w_{k-1} = ht_1h \rightarrow t_2 = w_k$.
- Let $\ell \in \mathbb{N}$ minimal such that w_ℓ contains t_1. Then

$$w_{\ell-1} = hu_{\ell-1}tv_{\ell-1}h \rightarrow hu_{\ell-1}t_1v_{\ell-1}h = w_\ell.$$

- Clearly $w_{\ell-1} \overset{*}{\rightarrow} t_2$.

- It remains to show $w \xrightarrow{*} w_{\ell-1}$.
- Note that $w_{\ell-2} \rightarrow w_{\ell-1}$ since M stops when reaching t.
- Let $m \in \mathbb{N}$ maximal such that

$$w \xrightarrow{*} w_{m-1} \leftarrow w_m \rightarrow w_{m+1} \xrightarrow{*} w_{\ell-1}$$

- Then $w_{m-1} = w_{m+1}$ represents the unique successor configuration of w_m.
- We can skip w_m above to get a shorter path from w to t_2.
- Hence our minimal path from w to t_2 cannot contain any $\leftarrow$. Thus $w \xrightarrow{*} t_2$. $\square$

SRS are equivalent to DTM

Corollary

Let $x \in \Sigma^*$. Then $hsxh \overset{*}{\leftrightarrow}_{S(M)} t_2$ iff $x \in L(M)$.

Note

- The language of any DTM many-one reduces to the word problem of the corresponding SRS.
- Conversely word problems can clearly be solved by NTM.
- SRS are a **Turing complete** model of computation (exactly as powerful as DTM, λ-calculus, ...).

Word problem for semigroups is undecidable

For a DTM with not computable language (e.g. AP), the corresponding SRS is not computable either. We proved:

Theorem (Post 1947)

There exist a finite SRS with undecidable word problem (c.e. but not computable).

Note

- Non-trivial properties of finite SRS are undecidable (Rice's Theorem).
- Undecidability of the word problem for groups follows with similar ideas but much harder details (Novikov 1955).
- 1-relator groups have decidable word problem (Magnus 1932).
- Matiyasevich (1967) gave an undecidable SRS with 2 generators and 3 relations.
- Open: Are 1-relator SRS decidable?
  1-relator inverse monoids have undecidable word problem