Orderings on monoids

Let $M = \langle S | R \rangle$ be a monoid

Let $< \subset X \times X$ be transitive. It is a

- linear ordering if $\forall s, t \in X$
  either $s < t$, $s = t$ or $t < s$.

  (we write $s \leq t$ to denote $s < t$ or $s = t$)

- well-ordering if it is linear and no infinite decreasing sequence exists i.e.

$$(s_i)_{i=1}^{\infty} \quad s_1 > s_2 > \dots > s_i > s_{i+1} > \dots .$$

Proposition:
In a well ordered set X every non-empty subset has a least element.

Proof (Axiom of choice).

If $<$ is linear on S, then it induces a linear ordering on S^n:

$$(s_1, \dots, s_n) < (t_1, \dots, t_n) \iff$$

$$\exists\, 1 \leq i \leq n \text{ s.t. } \begin{cases} s_j = t_j \text{ for } j < i \\ s_i < t_i \end{cases}$$

Lemma: if $<$ is linear (well-) ordering on S, then $<$ is linear (well-) ordering on S^*.

Defn: A (left-to-right) lexicographical ordering (Lex) on X^* is defined as follows:

If $u = u_1 \cdots u_k \quad u_i \in X$
$w = w_1 \cdots w_l \quad w_i \in X$ } written in letters

then $u < w$ if either holds

1) $k < l$ & $u_i = w_i \quad 1 \le i \le k$ (u is a prefix of w)

2) $\exists\ 1 \le i \le \min(k,l)$ s.t.

$$\begin{cases} u_j = w_j & 1 \le j < i \\ u_i < w_i \end{cases}$$

Lemma: If $<$ is linear ordering on X, then $\mathrm{Lex}(<)$ is linear ordering on X^*.

Defn: A Length-lexicographical ordering (lenlex) on X^* is defined as follows:

$u < w$ if

- $k < l$, or
- $k = l$ and u $\mathrm{Lex}(<)$ w.

Lemma: if $\prec$ is linear (well-) ordering on X, then $\mathrm{Lenlex}(\prec)$ is linear (well-)ordering on X^*

Proof: Exercise.

Defn:

Ordering $\prec$ on X^* is *translation invariant*

iff $\quad u \prec w \Rightarrow \forall_{A,B \in X^*} \; AuB \prec AwB.$

Proposition: $\mathrm{Lenlex}(\prec)$ is translation invariant on X^*.

Proof:

If $|u| < |w| \Rightarrow |xu| < |xw|$ & $|ux| < |wx|$

If $|u| = |w| \Rightarrow \exists\, i$ s.t. u and w differ first on i-th letter.

$\Rightarrow$ xu and xw differ first on $(i+1)$-th one (in the same way)

ux and wx differ first on i-th one (in the same way)

□

Defn: Translation invariant well-ordering on X^*

$=:$ rewriting ordering on X^*.

Prop: In rewriting ordering $\varepsilon \prec u$ for all $u \in X^+$

Proof:

Canonical forms:

Let $M = \langle S | R \rangle \cong M/_{\sim}$

$[u] = [w] \Leftrightarrow u \sim w$

Aim: choose a simplest element from each congruence class of words in M.

If $\prec$ is a reduction ordering on S^*

each $[u] = \{ v \in S^* : v \sim u \}$ is non-empty

$\Rightarrow$ contains the minimal element $\bar{u}$

$\bar{u}$ is the canonical form for u w.r.t. $\prec$

$\Rightarrow$ relies on the axiom of choice $\Rightarrow$ non-constructive

$u \overset{?}{=} v \rightsquigarrow \bar{u} \overset{?}{=} \bar{v}$ $\Rightarrow$ solving the word problem.

($\bar{u}, \bar{v}$: canonical forms)

Proposition: If u is the canonical form for an element of M, then subwords of u are canonical forms as well.

$\mathcal{R}$ can be understood as the set of pairs: (lhs=rhs)

since $=$ is reflexive we can orient every pair

assuming that $rhs < lhs$, hence

$\mathcal{R}$ is generated by oriented pairs

$lhs \Rightarrow rhs$

↖ rewriting rule w.r.t $\prec$. (rwrule)

$\Rightarrow$

Defn:

$(\mathcal{R}, \prec)$ is a rewriting system when

every element of $\mathcal{R}$ is a rwrule.

↖ a generating set for a $\sim$ congruence.

Suppose $(\mathcal{R}, \prec)$ is a RWS.

Let $\mathcal{L} = \{ u : \exists w : u \Rightarrow w \in \mathcal{R} \}$

$N(\mathcal{L})$ = the ideal of S^* generated by $\mathcal{L}$.

If $u \in N(\mathcal{L}) \Rightarrow u = alb$ for $l \in \mathcal{L}$; $a, b \in S^*$

and $arb \prec alb$ for $l \Rightarrow r \in \mathcal{R}$.

since $l \sim r \rightarrow u = alb \sim arb =: v$

repeat this as long as you can

This has to end since $\prec$-well-ordering.

At the end of this rewriting process we arrive at a word $W \in \mathcal{J}^* \setminus \mathcal{N}(\mathcal{L})$ which is said to be irreducible w.r.t $\mathcal{R}$.

Note: If w is in canonical form $\Rightarrow$ $w \in \mathcal{J}^* \setminus \mathcal{N}(\mathcal{L})$. (but not the other way)!!!

Notation:

- $u \to w$ or $u \xrightarrow{\mathcal{R}} w$ when w is the result of applying a single rewrule from $\mathcal{R}$.
- $u \xrightarrow{*} w$ or $u \xrightarrow[\mathcal{R}]{*} w$ when there exists a (finite) sequence of rewritings leading from u to w:

$$u = u_0 \to u_1 \to u_2 \to \dots \to u_n = w.$$

Ex:

$\mathcal{J} = \{x, y, x^{-1}, y^{-1}\}$, $\mathcal{R} = \{xx^{-1} \Rightarrow \varepsilon,\ x^{-1}x \Rightarrow \varepsilon,\ yy^{-1} \Rightarrow \varepsilon,\ y^{-1}y \Rightarrow \varepsilon\}$.

$u = xyx^{-1}xy^{-1}xy^{-1}yx^{-1}y$

Ex: $\Sigma = \{a, b\}$, $R = \{a^2 \Rightarrow \varepsilon,\ b^5 \Rightarrow \varepsilon,\ ba \Rightarrow ab^4\}$.

$baa \longrightarrow \varepsilon$

$baa \longrightarrow abbbba \longrightarrow abbbabbbb \longrightarrow$

$\longrightarrow abbabbbbbbbb \longrightarrow abbabb$

$\longrightarrow ababbbbbb \longrightarrow aba \longrightarrow aabbbb$

$\downarrow$

b^4.

- How to make the process of rewriting independent on the choices here?
- What are conditions on $(R, \prec)$ which guarantees this independence?

Proposition:

- $u \xrightarrow[R]{*} v \Rightarrow uw \xrightarrow[R]{*} uv$
- If R generates $\sim$ & R is an rws $\Rightarrow$

$u \sim v \iff u \overset{*}{\leftrightarrow} u_1 \overset{*}{\leftrightarrow} \dots \overset{*}{\leftrightarrow} u_k = v$

$u \searrow u_1 \swarrow u_2 \searrow u_3 \swarrow \dots \searrow v$

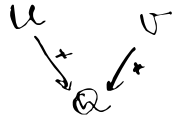
Properties:

- $u \sim v \Rightarrow \exists\, Q \in S^*$ s.t.

(Church-Rosser)

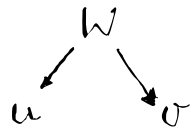
- If

$\Rightarrow \exists\, Q$ s.t.

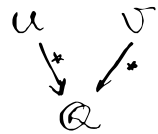


(confluence)

- If



$\Rightarrow \exists\, Q$ s.t.



(local confluence)

Proposition:

If Church-Rosser property holds for R

$\Rightarrow$ every congruence class of $\sim = \langle R \rangle$ contains a unique element of $S^* \setminus N(\mathcal{L})$

↑ the canonical form

Proof: $u, v \in S^* \setminus N(\mathcal{L})$, $u \sim v$

by Ch-R $\exists\, Q : u \xrightarrow{*}_R Q \xleftarrow{*}_R v \Rightarrow u = Q = v$. □

Proposition Let $(R, <)$ be a rws. wrt. a rw-ordering $<$.
Church-Rosser, confluence and local confluence
are equivalent for $(R, <)$.

Proof:

Ch-R $\Rightarrow$ confluence

If $u \overset{*}{\leftarrow} w \overset{*}{\rightarrow} v \Rightarrow u \sim w \sim v \Rightarrow u \sim v$.

By ch-R $\exists Q$ s.t. $u \overset{*}{\rightarrow} Q \overset{*}{\leftarrow} v$

i.e. R is confluent.

---

confluence $\rightarrow$ Ch-R

Suppose $u \sim v$. Then there exists a seq.

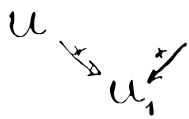
$$u = u_0 \overset{*}{\leftrightarrow} u_1 \overset{*}{\leftrightarrow} \dots \overset{*}{\leftrightarrow} u_k = v.$$

Induction on k:

$k = 1 \Rightarrow u \overset{*}{\rightarrow} v$, or $v \overset{*}{\rightarrow} u$

i.e Q is the smallest of u, v.

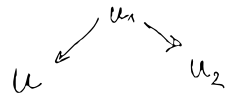
$k = 2$



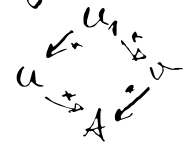
$\Rightarrow Q = u_1$

$\Rightarrow Q = v$

$\Rightarrow Q = u$



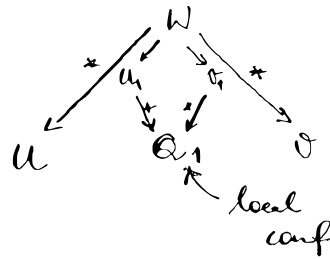
$\Rightarrow$ by confluence



confluence $\Rightarrow$ local confluence (trivial)

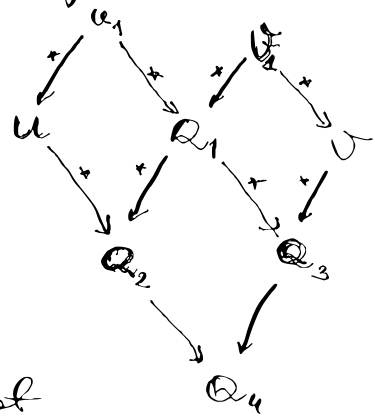
local confluence $\Rightarrow$ confluence

If confluence fails at (W, u, v).



we assume that W is the smallest word for which confluence fails.

since $u_1 < W \Rightarrow$ by confluence



$\Rightarrow$ confluence does not fail at (W, u, v).

□

Corollary: If $(R, <)$ is a confluent rws the result of rewriting u with R depends only on u, R and doesn't depend on the choices made in the process.

Defn a RWS $(R, <)$ is reduced if

1) each rhs of rewrule in R is irreducible
2) no word is lhs of two rewrules in R
3) no lhs is a subword of another lhs in R.

Equivalently:

R is reduced iff $\forall$ rewrule $P \to Q \in R$ both P and Q are irreducible wrt. $R \setminus \{P \to Q\}$.

Proposition:

Let $<$ be a rw-ordering on S^*. Every congruence relation on S^* is generated by a unique, reduced, confluent RWS $(R, <)$.

□

We will denote it by $RC(S, <, R)$.

Proposition: Let $(R, <)$ be a confluent RWS on S^*.
Let $P = \{$lhs of R which don't contain other lhs as a proper subword$\}$

for a word W let $\overline{W}$ denote the result of rewriting W using R.

then $RC(S, <, R) = \{P \to \overline{P} : P \in P\}$.

□