Orderings on monoids

First discuss solving the word problem in free groups as minimizing length.

X - any set

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 $s<$ 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 X then it induces a linear ordering on X^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 X then $<$ is linear (well-) ordering on X^n.

Defn: A (left-to-right) <u>lexicographical ordering</u> (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^*.

Note: this is not a well-ordering: when $a < b$, then
$ab > a^2b > \ldots > a^n b > \ldots$

Defn: A <u>Length - lexicographical</u> ordering (LenLex) on X^* is defined as follows:

$U < W$ if

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

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

Proof: Exercise.

Defn:
Ordering $<$ on X^* is translation invariant iff $u < w \Rightarrow \forall A, B \in X^* \quad AuB < AwB.$

Proposition: $\mathrm{LenLex}(<)$ 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)

$\square$

Defn: Translation invariant well-ordering on X^* $=:$ rewriting ordering on X^*.

Prop: In rewriting ordering $\varepsilon < u$ for all $u \in X^*$

Proof: suppose that $\exists W < \varepsilon \Rightarrow W^2 < W < \varepsilon$

$\Rightarrow \varepsilon > W > W^2 > \dots$ is infinite, descending contradicting well-order of $<$.

Wreath ordering:

$(A^*, <_A), (B^*, <_B)$: $<_A$ & $<_B$ are rewriting orderings.

$<_A \wr <_B$ is an order on $(A \sqcup B)^*$

$u = A_0 \cdot b_1 \dots A_{k-1} b_k A_k$ $\quad$ $C_j, A_i \in A^*$

$W = C_0 \cdot d_1 \dots C_{l-1} d_l C_l$ $\quad$ $d_j, b_i \in B$

$u <_2 W \iff b_1 \dots b_k <_B d_1 \dots d_l$

or $b_1 \dots b_k = d_1 \dots d_l$

and $(A_0, \dots, A_k) <_A (C_0, \dots, C_k)$

on Lex order on $(A^*)^{k+1}$.

Lemma: if $<_A$ & $<_B$ are rewriting orderings then $<_A \wr <_B$ is a rewriting ordering on $(A \sqcup B)^*$.

Ex: $A = \{a\}$, $B = \{b\}$

$a^{100} <_2 ab <_2 a^2 b <_2 bab <_2 b^2 ab <_2 b^2 a^{100} b$

Canonical forms:

Let $M = \langle S \mid R \rangle \cong M/_\sim$

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

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

If $<$ is a reduction ordering on S^*

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

$\Rightarrow$ contains the minimal element U

$\boxed{U \text{ is the canonical form for } u \text{ w.r.t. } <}$

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

$u \overset{?}{=} v \rightsquigarrow \underbrace{\bar{u} \overset{?}{=} \bar{v}}_{\text{canonical forms}} \Rightarrow$ solving the word problem.

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

Proof: if $U = A \cdot V \cdot B$ and V is not canonical

$\Rightarrow U = A \cdot V \cdot B > A \cdot \bar{V} B$ for $\bar{V}$ canonical for V.
by bi-invariance of $>$

$\lightning$ with $U = \bar{u}$.

Let $M = \mathrm{Mon}\langle A \mid R\rangle$ a f.p. monoid.

Suppose that $<_A$ is a rewriting order. Then the set of pairs $R = \{(a_i, b_i)\}_i$ can be oriented so that $a_i < b_i$. By reflexivity $\sim_R$ is unchanged.

Instead of (a, b) or $a = b$ we will be writing $a \to b$ to signify the order.

<u>An ordered pair</u> will be called a <u>rewriting rule</u>.

<u>Defn:</u>

$(R, <)$ is a <u>rewriting system</u> when every element of $\underline{\underline{R}}$ is a rwrule.

a generating set for a $\tilde{}$ congruence.

If $w \in A^*$, then find the first occurence of a (s.t. $a \to b \in R$) in w.

Replace <u>the occurence</u> of a in w by b.

$\rightsquigarrow w_1$

Observe: $w > w_1$ (by defn. of R).

Find next occurence of a, replace by b, to obtain w_2. $w > w_1 > w_2$. itd.

Defn: Ideal of M - monoid is a set $I \subset M$ s.t.

$$\forall x \in I, \forall y \in M \quad \underbrace{xy \in I}_{\text{right ideal}} \ \& \ yx \in I$$

Ex: $\mathcal{U} \subset X^*$

$I = \{ w \in X^* : \text{a subword of } w \text{ belongs to } \mathcal{U} \}$

Ex: Right ideal:

$w \in X^*$

$I = \{ w \cdot u : u \in X^* \}$.

A generating set for $I \subset M$ is a subset Y s.t.

$$I = MYM = \{ ayb : a \in M, b \in M, y \in Y \}$$

A Minimal generating set for I is a generating set not properly contained in any other generating set.

Note: • we may have many minimal generating sets (see: cyclic groups).

• we might have no min. generating sets

However:

Proposition:

Let $I \subset X^*$ be an ideal. Let

$$\mathcal{U} = \{ u \in I : \text{no proper subword of } u \text{ is in } I \}.$$

Then $\mathcal{U}$ is the unique minimal generating set for I.

Proof:

Let $N(\mathcal{U})$ – the ideal generated by $\mathcal{U}$.

By defn. $N(\mathcal{U}) \subset I$.

Let $u \in I$ and pick any minimal v – a subword of u s.t. $v \in I$. then $v \in \mathcal{U}$ and $u \in N(\mathcal{U})$.

$$\Rightarrow I \subset N(\mathcal{U}).$$

Let $\mathcal{V}$ – generating set for I. pick $u \in \mathcal{U}$.

since $u \in \mathcal{U} \subset I \Rightarrow u = avb$ s.t. $v \in \mathcal{V}$.
$(a, b \in M)$.

If $|a| = |b| = 0 \Rightarrow u = v \in \mathcal{V}$.

If any of $|a|, |b| > 0$, then

$v \in I$ and v is a proper subword of u.

$\lightning$ with the dfn. of $\mathcal{U}$.

$\square$

Suppose $(R, <)$ is a rws.

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

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

If $u \in N(\mathcal{L}) \Rightarrow u = a \cdot l \cdot b$: $a, b \in A^*$
$l \in \mathcal{L}$.
$l \to r \in R$.

then $alb > arb$.

since $l \sim_R r \Rightarrow \underbrace{alb}_{u=u_0} \sim_R \underbrace{arb}_{u_1}$.

Repeat as long as $u_i \in N(\mathcal{L})$:

$$u = u_0 > u_1 > u_2 > \dots > u_r = v$$

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

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

Notation:

- $U \to W$ or $U \xrightarrow[R]{} W$ when W is the result of applying a single rwrule from R.

- $U \xrightarrow{*} W$ or $U \xrightarrow[R]{*} W$ when there exists a (finite) sequence of rewritings leading from U to W:

$$U = U_0 \longrightarrow U_1 \longrightarrow U_2 \longrightarrow \cdots \longrightarrow U_n = W.$$

Ex:

$S = \{x, y, X, Y\}$, $R = \{xX \Rightarrow \varepsilon,\ Xx \Rightarrow \varepsilon,$
$yY \Rightarrow \varepsilon,\ Yy \Rightarrow \varepsilon\}.$

$U = x y x^{-1} x y^{-1} x y^{-1} y x^{-1} y$

Ex: $S = \{a,b\}$, $R = \{a^2 \Rightarrow \varepsilon,\ b^6 \Rightarrow \varepsilon,\ ba \Rightarrow ab^4\}$.

$\underline{baa} \to b$

$\underline{ba}a \to abbb\underline{ba} \to abbb\underline{a}bbbb \to$

$\to abba\underline{bbbbbbbb} \to ab\underline{ba}bb$

$\to aba\underline{bbbbbb} \to a\underline{ba} \to \underline{aa}bbbb$

$\downarrow$

b^4.

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

Proposition:

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

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

$$\begin{tikzcd}[column sep=small] u \arrow[dr] & & u_2 \arrow[dl] \arrow[dr] & & \cdots \arrow[dr] & \\ & u_1 & & u_3 & & v \end{tikzcd}$$

<u>Properties</u>:

- $U \sim V \Rightarrow \exists\, Q$ s.t.

$$\begin{tikzcd}[column sep=small] U \arrow[dr, "*"'] & & V \arrow[dl, "*"] \\ & Q & \end{tikzcd}$$

(<u>Church-Rosser</u>)

- If
$$\begin{tikzcd}[column sep=small] & W \arrow[dl, "*"'] \arrow[dr, "*"] & \\ U & & V \end{tikzcd} \Rightarrow \exists\, Q \text{ s.t. } \begin{tikzcd}[column sep=small] U \arrow[dr, "*"'] & & V \arrow[dl, "*"] \\ & Q & \end{tikzcd}$$

(<u>confluence</u>)

- If
$$\begin{tikzcd}[column sep=small] & W \arrow[dl] \arrow[dr] & \\ U & & V \end{tikzcd} \Rightarrow \exists\, Q \text{ s.t. } \begin{tikzcd}[column sep=small] U \arrow[dr, "*"'] & & V \arrow[dl, "*"] \\ & Q & \end{tikzcd}$$

(<u>local confluence</u>)

<u>Proposition</u>:

If Church-Rosser property holds for R

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

the canonical form

<u>Proof</u>: Suppose, U, V - irreducible and $U \sim V$

by Ch-R $\exists\, Q$: $U \xrightarrow[R]{*} Q \xleftarrow[R]{*} V \Rightarrow U = Q = V$.

$\square$

<u>Proposition</u> Let $(R,<)$ be a <u>rws</u> w.r.t. a rw-ordering $<$.

Church-Rosser, confluence and local confluence are equivalent for $(R,<)$.

<u>Proof:</u>

Ch-R $\Rightarrow$ confluence

If $u \xleftarrow{*} w \xrightarrow{*} v \Rightarrow u \sim w \sim v \Rightarrow u \sim v$.

By ch-R $\exists\, Q$ s.t. $u \xrightarrow{*} Q \xleftarrow{*} v$

i.e. R is confluent.

---

confluence $\to$ Ch-R

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

$u = u_0 \xleftrightarrow{*} u_1 \xleftrightarrow{*} \dots \xleftrightarrow{*} u_k = v$. (See previous lecture!)

<u>Induction on k:</u>

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

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

$k = 2$

$$\begin{tikzcd} u \arrow[dr, "*"] & & u_2 = v \arrow[dl, "*"'] \\ & u_1 & \end{tikzcd} \Rightarrow Q = u_1$$

$\searrow^{*} \ \nearrow^{*} \quad \Rightarrow Q = v$

$\nwarrow^{*} \ \swarrow^{*} \quad \Rightarrow Q = u$

$$\begin{tikzcd} & u_1 \arrow[dl, "*"'] \arrow[dr, "*"] & \\ u & & u_2 \end{tikzcd} \Rightarrow \text{by confluence}$$

$$\begin{tikzcd} & u_1 \arrow[dl, "*"'] \arrow[dr, "*"] & \\ u \arrow[dr, "*"'] & & v \arrow[dl, "*"] \\ & A & \end{tikzcd}$$

confluence $\Rightarrow$ local confluence (trivial)

local confluence $\Rightarrow$ confluence

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

$$\begin{tikzcd}[column sep=small]
 & & W \arrow[dll, "*"'] \arrow[dl] \arrow[dr] \arrow[drr, "*"] & & \\
 & u_1 \arrow[dr, "*"] & & v_1 \arrow[dl, "*"'] & \\
u & & Q_1 & & v
\end{tikzcd}$$

local confl.

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

since $u_1 < W \Rightarrow$ by confluence

$$\begin{tikzcd}[column sep=small]
 & u_1 \arrow[dl, "*"'] \arrow[dr, "*"] & & v_1 \arrow[dl, "*"'] \arrow[dr, "*"] & \\
u \arrow[dr, "*"] & & Q_1 \arrow[dl, "*"'] \arrow[dr, "*"] & & v \arrow[dl, "*"'] \\
 & Q_2 \arrow[dr] & & Q_3 \arrow[dl] & \\
 & & Q_4 & &
\end{tikzcd}$$

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

$\square$

<u>Corollary:</u> If $(R, <)$ is a confluent <u>rws</u> 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 rwrule in R is irreducible
2) no word is lhs of two rwrules in R
3) no lhs is a subword of another lhs in R.

Equivalently:

R is reduced iff $\forall$ rwrule $P \to Q \in R$ 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 $\mathcal{P} = \{$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 $RC(S,<,R) = \{ P \to \overline{P} : P \in \mathcal{P} \}$.

□