

Orderings on monoids

X - any set

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

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

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

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

$$(s_i)_{i=1}^n \quad s_1 \succ s_2 \succ \dots \succ s_i \succ s_{i+1} \succ \dots$$

Proposition:

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

Proof (Axiom of choice).

If \prec is linear on X then it induces a linear ordering on X^n .

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

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

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

Lemma: if \prec is linear (well-) ordering on X
then \prec is linear (well-) ordering on X^* .

(Lex)

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

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

then $u \prec w$ if either holds

- 1) $k < l$ & $u_i = w_i \quad 1 \leq i \leq k$ (u is a prefix
of w)
- 2) $\exists 1 \leq i \leq \min(k, l)$ s.t.

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

Lemma: If \prec is linear ordering on X ,
then $\text{lex}(\prec)$ is linear ordering on X^* .

Note: this is not a well-ordering: when $a \prec b$, then
 $ab \succ a^2b \succ \dots \succ a^n b \succ \dots$

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

$u \prec w$ if

- $|u| < |w|$, or
- $|u| = |w|$ and $u \text{ lex}(\prec) w$.

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

Proof: Exercise.

Defn:

Ordering \prec on X^* is translation invariant

iff $\boxed{u \prec w \Rightarrow \forall A, B \in X^* \quad A u B \prec A w B}$.

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

Proof:

If $|u| < |w| \Rightarrow |xu| < |xw| \text{ s.t. } |u_x| < |w_x|$

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

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

u_x and w_x 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 $\varepsilon < u$ 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 \prec .

Lex ordering :-

$(A, \prec_A), (B, \prec_B)$: $\prec_A \in \prec_{\mathcal{L}}$ are rewriting orderings.

$\prec_A \circ \prec_B$ is an order on $(A \cup B)^*$

$$u = a_0 \cdot b_1 \cdot \dots \cdot b_k \cdot a_1 \quad c_j, a_i \in A^* \\ w = c_0 \cdot d_1 \cdot \dots \cdot d_l \cdot c_1 \quad | d_j, b_i \in B$$

$$u \prec w \Leftrightarrow b_1 \dots b_k \prec_B d_1 \dots d_l$$

$$\text{or } b_1 \dots b_k = d_1 \dots d_l$$

$$\text{and } (a_0, \dots, a_k) \prec_A (c_0, \dots, c_l)$$

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

Lemma: if \prec_A & \prec_B are rewriting orderings

then $\prec_A \circ \prec_B$ is a rewriting ordering on $(A \cup B)^*$.

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

$$a \xrightarrow{\text{def}} ab \prec a^2 b \prec b a b \prec b^2 a b \prec b^2 a^{\text{def}} b$$

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 \prec is a reduction ordering on S^*

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

\Rightarrow contains the minimal element U

U is the canonical form for u w.r.t. \prec

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

$u \stackrel{?}{=} v \rightarrow \overline{u} \stackrel{?}{=} \overline{v} \Rightarrow$ 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

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

↳ with $U = \overline{U}$.

Let $M = \text{Mon}(A|R)$ a f.p. monoid.

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

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

An ordered pair will be called a rewriting rule:

Defn:

(R, \prec) is a rewriting system when

every element of \overline{R} is a rule.

\overline{R} a generating set

for a $\tilde{\approx}$
congruence.

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

Replace the occurrence of a in w by b .
 $\leadsto w_1$

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

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

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

$$\forall x \in I, \forall y \in M \quad \underbrace{xy \in I}_{\text{right ideal}} \quad \overbrace{\exists y \in I}^{\text{left ideal}}$$

Ex: $u \subset X^*$

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

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

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

Then U is the unique minimal generating set for I .

Proof:

Let $N(U)$ - the ideal generated by U .

By defn. $N(U) \subset I$.

Let $u \in I$ and pick any minimal v-a subword of u s.t. $v \in I$. Then $v \in U$ and $u \in N(U)$.

$$\Rightarrow I \subset N(U).$$

Let V - generating set for I . pick $u \in U$.

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

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

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

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

↓ with the
dfn. of U .

□

Suppose (R, \prec) is a rws.

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

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

If $u \in N(\mathcal{L}) \Rightarrow u = a \cdot b \cdot b : a, b \in A^*$
i.e. $b \in \mathcal{L}$.

$b \rightarrow^r r \in R$.

then $a \cdot b \cdot b >_R a \cdot b \cdot r$.

since $b \sim_R r \Rightarrow \underbrace{a \cdot b \cdot b}_{u=u_0} >_R \underbrace{a \cdot b \cdot r}_{u=u_1}$.

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 the rewriting process

we arrive at a word $v \in A^* \setminus N(\mathcal{L})$.

which is said to be irreducible 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:

- $U \rightarrow W$ or $U \xrightarrow{R} W$ when W is the result of applying a single rule from R .
- $U \hookrightarrow W$ or $U \xrightarrow{* R} W$ when there exists a (finite) sequence of rewritings leading from U to W :

$$U = U_0 \rightarrow U_1 \rightarrow U_2 \rightarrow \dots \rightarrow U_n = W.$$

Ex:

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

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

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

$$\underline{baa} \rightarrow b$$

$$\begin{aligned} \underline{baa} &\rightarrow abbb\underline{ba} \rightarrow abbb\underline{abb}bb \rightarrow \\ &\rightarrow abbb\underline{abb}bb \rightarrow ab\underline{abb}bb \\ &\rightarrow ab\underline{abb}bb \rightarrow \underline{aba} \rightarrow \underline{aa}bb \downarrow \\ &\qquad\qquad\qquad b^4. \end{aligned}$$

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

Proposition:

$$u \xrightarrow[R]{*} v \Rightarrow uw \xrightarrow[R]{*} uv$$

• If R generates \sim & R is an rew \Rightarrow

$$u \sim v \Leftrightarrow u \xleftarrow{*} u_1 \xleftarrow{*} \dots \xleftarrow{*} u_n = v$$

$$u \xrightarrow{*} u_1 \xrightarrow{*} u_2 \xrightarrow{*} u_3 \xrightarrow{*} \dots \xrightarrow{*} v$$

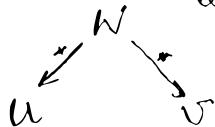
Properties:

- $u \sim v \Rightarrow \exists Q \text{ s.t. } \dots$



(Church-Rosser)

- If

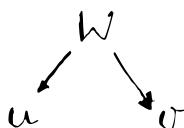


$\Rightarrow \exists Q \text{ s.t. }$

(Confluence)

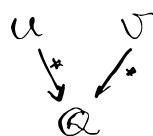


- If



$\Rightarrow \exists Q \text{ s.t. }$

(local confluence)



Proposition:

If Church-Rosser property holds for R

\Rightarrow every congruence class of $\sim = \langle R \rangle$

contains a unique element of

$$J^* \setminus N(L)$$

the canonical form

Proof: Suppose, u, v - irreducible and $u \sim v$

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

Proposition: Let (R, \prec) be a rws w.r.t. a rw-ordering \prec .
 Church-Rosser, confluence and local confluence
 are equivalent for (R, \prec) .

Proof:

$\text{Ch-}R \Rightarrow \text{confluence}$

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

By $\text{ch-}R \exists Q$ s.t. $u \xrightarrow{*} Q \xleftarrow{*} v$
 i.e. R is confluent.

confluence $\rightarrow \text{Ch-}R$

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

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

Induction on k :

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

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

$k=2$

$$u \xrightarrow{*} u_1 \xrightarrow{*} u_2 = v \Rightarrow Q = u_1$$

$$\begin{array}{ccc} \nearrow \searrow & \Rightarrow Q = v \\ R & \Leftrightarrow & \Rightarrow Q = u \end{array}$$

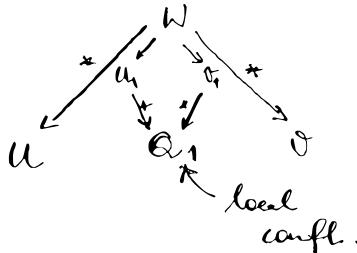
$$u \xleftarrow{*} u_1 \xrightarrow{*} u_2 \Rightarrow \text{by confluence}$$

$$\begin{array}{c} u_1 \xleftarrow{*} u \\ u \xrightarrow{*} v \\ A \end{array}$$

confluence \Rightarrow local confluence (trivial)

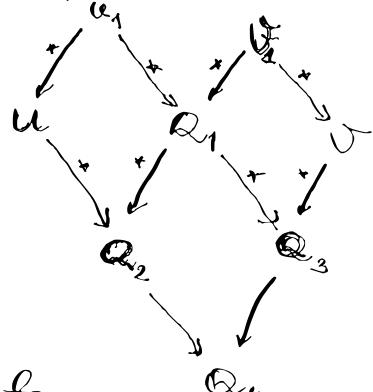
local confluence \Rightarrow confluence

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



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

since $u_1 \prec W \Rightarrow$ by confluence



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

□

Corollary: If (R, \prec) is a confluent ws

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, \prec) is reduced if
- 1) each rhs of rule in R is irreducible
 - 2) no word is lhs of two rules in R
 - 3) no lhs is a subword of another lhs in R .

Equivalently:

R is reduced iff \forall rewrite $P \rightarrow Q \in R$

both P and Q are irreducible wrt.

$$R \setminus \{P \rightarrow Q\}.$$

Proposition:

Let \prec be a re-ordering on S^* . Every congruence relation on S^* is generated by a unique, reduced, confluent rws (R, \prec) .

□

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

Proposition: Let (R, \prec) be a confluent rws on S^* .

Let $P = \{\text{lhs of } R \text{ which don't contain other lhs as a proper subword}\}$

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

then $RC(S, \prec, R) = \{P \rightarrow \tilde{P} : P \in P\}$.

□

