

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 $s < t$ 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 X then it induces
a linear ordering on X^n .

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

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

Lemma: if $<$ is linear (well-) ordering on X
then $<$ is linear (well-) ordering on X^n .

(Lex)
Defn: $<$ (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 $U < W$ if either holds

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

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

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

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

Defn: $<$ length-lexicographical ordering (lexlex)
on X^* is defined as follows:

$U < W$ if

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

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

Proof: Exercise.

Defn:

Ordering $<$ on X^* is translation invariant

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

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

Proof:

$\exists!$ $|u| < |w| \Rightarrow |xu| < |xw| \ \& \ |u_x| < |w_x|$

$\exists!$ $|u| = |w| \Rightarrow \exists i$ st. u and w 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^* □
 \equiv 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 $<$.

Weak ordering:

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

$<_A \geq <_B$ is an order on $(A \cup B)^*$

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

$W = C_0 \cdot d_1 \dots C_{k-1} d_k C_k$ $\left\{ \begin{array}{l} d_j, b_i \in B \end{array} \right.$

$u <_2 W \Leftrightarrow b_1 \dots b_k <_B d_1 \dots d_k$

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

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

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

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

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:

$$\text{Let } M = \langle \mathcal{A}^* / R \rangle \cong M / \sim$$

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

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

If $<$ is a reduction ordering on \mathcal{A}^*

each $[u] = \{v \in \mathcal{A}^* : v \sim u\}$ is non-empty
 \Rightarrow contains the minimal element U

U is the canonical form for u w.r.t. $<$

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

$u \equiv v \rightsquigarrow \bar{u} \stackrel{?}{=} \bar{v} \Rightarrow$ solving the word problem.
 $\uparrow \uparrow$
canonical forms

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

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

\downarrow with $u = \bar{u}$.

Let $\mathcal{M} = \text{Mon} \langle A | R \rangle$ a f.p. monoid.

Suppose that $<_R$ 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 \approx_R 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:
 $(R, <)$ is a rewriting system when every element of \overline{R} is a rule.
 \overline{R} a generating set for a \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 .
 $w \rightsquigarrow w_1$

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

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

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

$$\forall x \in I, \forall y \in M \quad \underline{xy \in I} \text{ or } \underline{yx \in I}$$

right 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 $\mathcal{N}(U)$ - the ideal generated by U .

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

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

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

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

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

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
defn. of U .

□

Notation:

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

$$u = u_0 \rightarrow u_1 \rightarrow u_2 \rightarrow \dots \rightarrow u_n = W.$$

Ex:

$$\mathcal{I} = \{x, y, x^{-1}, y^{-1}\}, \quad \mathcal{R} = \{xX \Rightarrow \varepsilon, Xx \Rightarrow \varepsilon, \\ yY \Rightarrow \varepsilon, Yy \Rightarrow \varepsilon\}.$$

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

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

baa \rightarrow b

baa \rightarrow abbbba \rightarrow abbbabbbb \rightarrow
 \rightarrow abbabbbb \rightarrow ababbb
 \rightarrow ababbbbb \rightarrow aba \rightarrow aabbbb
 \downarrow
 b^4

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

Proposition:

• $u \xrightarrow[\mathcal{R}]{} v \Rightarrow u w \xrightarrow[\mathcal{R}]{} u v$

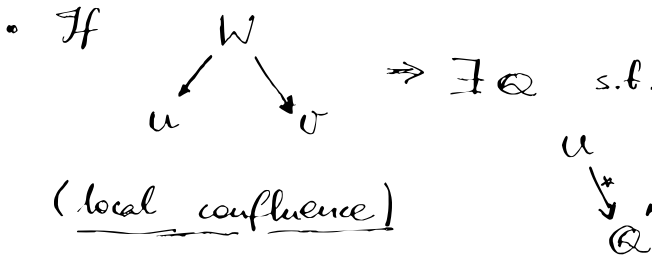
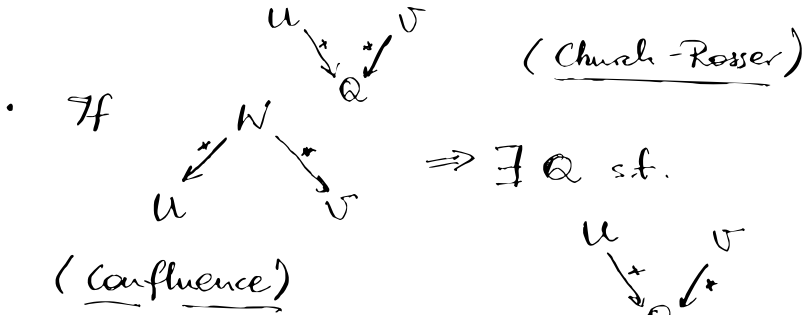
• If \mathcal{R} generates \sim & \mathcal{R} is an rws \Rightarrow

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



Properties:

- $u \sim v \Rightarrow \exists Q$ s.t.



Proposition:

If Church-Rosser property holds for R

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

contains a unique element of

\uparrow $S^*(N(L))$
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 $(R, <)$ be a rews. w.r.t. a rew-ordering τ .

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

Proof:

Ch-R \Rightarrow confluence

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

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

confluence \rightarrow 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 .

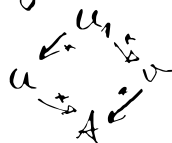
$k=2$

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

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

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

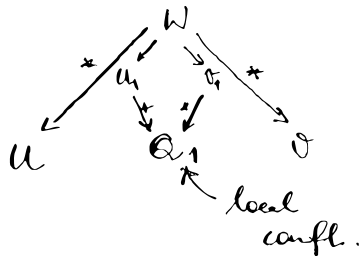
$u \xrightarrow{*} u_1 \xrightarrow{*} u_2 \Rightarrow$ by confluence



confluence \Rightarrow local confluence (trivial)

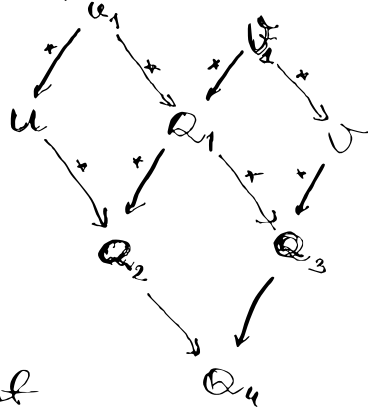
local confluence \Rightarrow confluence

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 rew

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 rews $(R, <)$ 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 rule $P \rightarrow Q \in R$
both P and Q are irreducible wrt.

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

Proposition:

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

□

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

Proposition: Let $(R, <)$ be a confluent rews on S^* .

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

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

then $RC(S, <, R) = \{P \rightarrow \bar{P} : P \in \mathcal{P}\}$.

□

