From pregroups to groups

Andrew Duncan

December 15th, 2008

Outline

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution $^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity $[1x] = [x1] = x$ for all x;

Inverses $[x^\varepsilon x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;

Associativity $[xy]$ & $[yz]$ defined then
$[[xy]z]$ defined iff $[x[yz]]$ defined
and then $[[xy]z] = [x[yz]]$;

Uniformity If (w, x) & (x, y) & $(y, z) \in D$ then
either $(w, [xy]) \in D$ or $([xy], z) \in D$.

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution $^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity $[1x] = [x1] = x$ for all x;

Inverses $[x^{\varepsilon} x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;

Associativity $[xy]$ & $[yz]$ defined then
$[[xy]z]$ defined iff $[x[yz]]$ defined
and then $[[xy]z] = [x[yz]]$;

Uniformity If (w, x) & (x, y) & $(y, z) \in D$ then
either $(w, [xy]) \in D$ or $([xy], z) \in D$.

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution $^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity	$[1x] = [x1] = x$ for all x;
Inverses	$[x^{\varepsilon}x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;
Associativity	$[xy]$ & $[yz]$ defined then $[[xy]z]$ defined iff $[x[yz]]$ defined and then $[[xy]z] = [x[yz]]$;
Uniformity	If (w, x) & (x, y) & $(y, z) \in D$ then either $(w, [xy]) \in D$ or $([xy], z) \in D$.

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution $^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity $[1x] = [x1] = x$ for all x;

Inverses $[x^{\varepsilon}x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;

Associativity $[xy]$ & $[yz]$ defined then $[[xy]z]$ defined iff $[x[yz]]$ defined and then $[[xy]z] = [x[yz]]$;

Uniformity If (w, x) & (x, y) & $(y, z) \in D$ then either $(w, [xy]) \in D$ or $([xy], z) \in D$.

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution $^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity $[1x] = [x1] = x$ for all x;

Inverses $[x^{\varepsilon}x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;

Associativity $[xy]$ & $[yz]$ defined then
$[[xy]z]$ defined iff $[x[yz]]$ defined
and then $[[xy]z] = [x[yz]]$;

Uniformity If (w, x) & (x, y) & $(y, z) \in D$ then
either $(w, [xy]) \in D$ or $([xy], z) \in D$.

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution $^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity $[1x] = [x1] = x$ for all x;

Inverses $[x^{\varepsilon} x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;

Associativity $[xy]$ & $[yz]$ defined then
$[[xy]z]$ defined iff $[x[yz]]$ defined
and then $[[xy]z] = [x[yz]]$;

Uniformity If (w, x) & (x, y) & $(y, z) \in D$ then
either $(w, [xy]) \in D$ or $([xy], z) \in D$.

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution $^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity $[1x] = [x1] = x$ for all x;

Inverses $[x^{\varepsilon} x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;

Associativity $[xy]$ & $[yz]$ defined then
$[[xy]z]$ defined iff $[x[yz]]$ defined
and then $[[xy]z] = [x[yz]]$;

Uniformity If (w, x) & (x, y) & $(y, z) \in D$ then
either $(w, [xy]) \in D$ or $([xy], z) \in D$.

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution $^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity $[1x] = [x1] = x$ for all x;

Inverses $[x^{\varepsilon}x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;

Associativity $[xy]$ & $[yz]$ defined then
$[[xy]z]$ defined iff $[x[yz]]$ defined
and then $[[xy]z] = [x[yz]]$;

Uniformity If (w, x) & (x, y) & $(y, z) \in D$ then
either $(w, [xy]) \in D$ or $([xy], z) \in D$.

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution $^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity $[1x] = [x1] = x$ for all x;

Inverses $[x^{\varepsilon} x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;

Associativity $[xy]$ & $[yz]$ defined then
$[[xy]z]$ defined iff $[x[yz]]$ defined
and then $[[xy]z] = [x[yz]]$;

Uniformity If (w, x) & (x, y) & $(y, z) \in D$ then
either $(w, [xy]) \in D$ or $([xy], z) \in D$.

Pregroups

A **pregroup** consists of a set P together with

1. a designated element 1;
2. an involution ${}^{-1}$ defined on P;
3. a set $D \subseteq P \times P$;
4. a function $m : D \to P$;

such that, writing $[xy]$ to mean $(x, y) \in D$ and $m(x, y) = [xy]$

Identity	$[1x] = [x1] = x$ for all x;
Inverses	$[x^{\varepsilon} x^{-\varepsilon}] = 1$, for all x, $\varepsilon = \pm 1$;
Associativity	$[xy]$ & $[yz]$ defined then $[[xy]z]$ defined iff $[x[yz]]$ defined and then $[[xy]z] = [x[yz]]$;
Uniformity	If (w, x) & (x, y) & $(y, z) \in D$ then either $(w, [xy]) \in D$ or $([xy], z) \in D$.

The Universal Group

The *universal group* $U(P)$ of a pregroup P is the group

$$\langle P | m(x,y) = xy, \forall (x,y) \in D \rangle.$$

Stallings: "Group Theory and 3-dimensional Manifolds" (1971)
A word $p_1 \cdots p_n \in P^*$ is **reduced** if $(p_i, p_{i+1}) \notin D$, for $i = 1, \ldots, n-1$.

Theorem (Stallings)

All reduced words representing an element $g \in U(P)$ have the same length.

Corollary

P embeds in $U(P)$.

The Universal Group

The *universal group* $U(P)$ of a pregroup P is the group

$$\langle P | m(x,y) = xy, \forall (x,y) \in D \rangle.$$

Stallings: "Group Theory and 3-dimensional Manifolds" (1971)
A word $p_1 \cdots p_n \in P^*$ is **reduced** if $(p_i, p_{i+1}) \notin D$, for $i = 1, \ldots, n-1$.

Theorem (Stallings)

All reduced words representing an element $g \in U(P)$ have the same length.

Corollary

P embeds in $U(P)$.

The Universal Group

The *universal group* $U(P)$ of a pregroup P is the group

$$\langle P | m(x,y) = xy, \forall (x,y) \in D \rangle.$$

Stallings: "Group Theory and 3-dimensional Manifolds" (1971)
A word $p_1 \cdots p_n \in P^*$ is **reduced** if $(p_i, p_{i+1}) \notin D$, for $i = 1, \ldots, n-1$.

Theorem (Stallings)

All reduced words representing an element $g \in U(P)$ have the same length.

Corollary

P embeds in $U(P)$.

The Universal Group

The *universal group* $U(P)$ of a pregroup P is the group

$$\langle P | m(x,y) = xy, \forall (x,y) \in D \rangle.$$

Stallings: "Group Theory and 3-dimensional Manifolds" (1971)
A word $p_1 \cdots p_n \in P^*$ is **reduced** if $(p_i, p_{i+1}) \notin D$, for $i = 1, \ldots, n-1$.

Theorem (Stallings)

All reduced words representing an element $g \in U(P)$ have the same length.

Corollary

P embeds in $U(P)$.

Examples

1. Suppose that
   - $x^{-1} = x$ only if $x = 1$ and
   - D contains exactly $(1, p)$, $(p, 1)$, $(p^{\pm 1}, p^{\mp 1})$, for all $p \in P$,

   then $U(P)$ is free of rank $(|P| - 1)/2$.
2. Let A and B be groups with $A \cap B = C$. Set $P = A \cup B$ and $D = (A \times A) \cup (B \times B)$. Then $U(P) \cong A *_C B$.
3. HNN extensions.
4. The fundamental group of a graph of groups is the universal group of a pregroup (Rimlinger, Hoare).

Examples

1. Suppose that
   - $x^{-1} = x$ only if $x = 1$ and
   - D contains exactly $(1, p)$, $(p, 1)$, $(p^{\pm 1}, p^{\mp 1})$, for all $p \in P$,

   then $U(P)$ is free of rank $(|P| - 1)/2$.
2. Let A and B be groups with $A \cap B = C$. Set $P = A \cup B$ and $D = (A \times A) \cup (B \times B)$. Then $U(P) \cong A *_C B$.
3. HNN extensions.
4. The fundamental group of a graph of groups is the universal group of a pregroup (Rimlinger, Hoare).

Examples

1. Suppose that
   - $x^{-1} = x$ only if $x = 1$ and
   - D contains exactly $(1, p)$, $(p, 1)$, $(p^{\pm 1}, p^{\mp 1})$, for all $p \in P$,

   then $U(P)$ is free of rank $(|P| - 1)/2$.
2. Let A and B be groups with $A \cap B = C$. Set $P = A \cup B$ and $D = (A \times A) \cup (B \times B)$. Then $U(P) \cong A *_C B$.
3. HNN extensions.
4. The fundamental group of a graph of groups is the universal group of a pregroup (Rimlinger, Hoare).

Examples

1. Suppose that
   - $x^{-1} = x$ only if $x = 1$ and
   - D contains exactly $(1, p)$, $(p, 1)$, $(p^{\pm 1}, p^{\mp 1})$, for all $p \in P$,

   then $U(P)$ is free of rank $(|P| - 1)/2$.
2. Let A and B be groups with $A \cap B = C$. Set $P = A \cup B$ and $D = (A \times A) \cup (B \times B)$. Then $U(P) \cong A *_C B$.
3. HNN extensions.
4. The fundamental group of a graph of groups is the universal group of a pregroup (Rimlinger, Hoare).

Examples

1. Suspose that
   - $x^{-1} = x$ only if $x = 1$ and
   - D contains exactly $(1, p)$, $(p, 1)$, $(p^{\pm 1}, p^{\mp 1})$, for all $p \in P$,

   then $U(P)$ is free of rank $(|P| - 1)/2$.
2. Let A and B be groups with $A \cap B = C$. Set $P = A \cup B$ and $D = (A \times A) \cup (B \times B)$. Then $U(P) \cong A *_C B$.
3. HNN extensions.
4. The fundamental group of a graph of groups is the universal group of a pregroup (Rimlinger, Hoare).

Examples

1. Suppose that
   - $x^{-1} = x$ only if $x = 1$ and
   - D contains exactly $(1, p)$, $(p, 1)$, $(p^{\pm 1}, p^{\mp 1})$, for all $p \in P$,

   then $U(P)$ is free of rank $(|P| - 1)/2$.
2. Let A and B be groups with $A \cap B = C$. Set $P = A \cup B$ and $D = (A \times A) \cup (B \times B)$. Then $U(P) \cong A *_C B$.
3. HNN extensions.
4. The fundamental group of a graph of groups is the universal group of a pregroup (Rimlinger, Hoare).

Rewriting Systems

A *rewriting relation* over a set X: $\Longrightarrow \subseteq X \times X$.

- $\stackrel{*}{\Longrightarrow}$: the reflexive and transitive closure of $\Longrightarrow$;
- $\stackrel{*}{\Longleftrightarrow}$: its symmetric, reflexive, and transitive closure.

The relation $\Longrightarrow \subseteq X \times X$ is called:

- *confluent*, if $y \stackrel{*}{\Longleftarrow} x \stackrel{*}{\Longrightarrow} z$ implies $y \stackrel{*}{\Longrightarrow} w \stackrel{*}{\Longleftarrow} z$ for some w;
- *terminating*, if every infinite chain

$$x_0 \stackrel{*}{\Longrightarrow} x_1 \stackrel{*}{\Longrightarrow} \cdots x_{i-1} \stackrel{*}{\Longrightarrow} x_i \stackrel{*}{\Longrightarrow} \cdots$$

  becomes stationary;
- *convergent*, if it is confluent and terminating.

Rewriting Systems

A *rewriting relation* over a set X: $\Longrightarrow \subseteq X \times X$.

- $\stackrel{*}{\Longrightarrow}$: the reflexive and transitive closure of $\Longrightarrow$;
- $\stackrel{*}{\Longleftrightarrow}$: its symmetric, reflexive, and transitive closure.

The relation $\Longrightarrow \subseteq X \times X$ is called:

- *confluent*, if $y \stackrel{*}{\Longleftarrow} x \stackrel{*}{\Longrightarrow} z$ implies $y \stackrel{*}{\Longrightarrow} w \stackrel{*}{\Longleftarrow} z$ for some w;
- *terminating*, if every infinite chain

$$x_0 \stackrel{*}{\Longrightarrow} x_1 \stackrel{*}{\Longrightarrow} \cdots x_{i-1} \stackrel{*}{\Longrightarrow} x_i \stackrel{*}{\Longrightarrow} \cdots$$

  becomes stationary;
- *convergent*, if it is confluent and terminating.

Rewriting Systems

A *rewriting relation* over a set X: $\Longrightarrow \subseteq X \times X$.

- $\overset{*}{\Longrightarrow}$: the reflexive and transitive closure of $\Longrightarrow$;
- $\overset{*}{\Longleftrightarrow}$: its symmetric, reflexive, and transitive closure.

The relation $\Longrightarrow \subseteq X \times X$ is called:

- *confluent*, if $y \overset{*}{\Longleftarrow} x \overset{*}{\Longrightarrow} z$ implies $y \overset{*}{\Longrightarrow} w \overset{*}{\Longleftarrow} z$ for some w;
- *terminating*, if every infinite chain

$$x_0 \overset{*}{\Longrightarrow} x_1 \overset{*}{\Longrightarrow} \cdots x_{i-1} \overset{*}{\Longrightarrow} x_i \overset{*}{\Longrightarrow} \cdots$$

  becomes stationary;
- *convergent*, if it is confluent and terminating.

Rewriting Systems

A *rewriting relation* over a set X: $\Longrightarrow \subseteq X \times X$.

- $\stackrel{*}{\Longrightarrow}$: the reflexive and transitive closure of $\Longrightarrow$;
- $\stackrel{*}{\Longleftrightarrow}$: its symmetric, reflexive, and transitive closure.

The relation $\Longrightarrow \subseteq X \times X$ is called:

- *confluent*, if $y \stackrel{*}{\Longleftarrow} x \stackrel{*}{\Longrightarrow} z$ implies $y \stackrel{*}{\Longrightarrow} w \stackrel{*}{\Longleftarrow} z$ for some w;
- *terminating*, if every infinite chain

$$x_0 \stackrel{*}{\Longrightarrow} x_1 \stackrel{*}{\Longrightarrow} \cdots x_{i-1} \stackrel{*}{\Longrightarrow} x_i \stackrel{*}{\Longrightarrow} \cdots$$

  becomes stationary;
- *convergent*, if it is confluent and terminating.

Rewriting Systems

A *rewriting relation* over a set X: $\Longrightarrow \subseteq X \times X$.

- $\stackrel{*}{\Longrightarrow}$: the reflexive and transitive closure of $\Longrightarrow$;
- $\stackrel{*}{\Longleftrightarrow}$: its symmetric, reflexive, and transitive closure.

The relation $\Longrightarrow \subseteq X \times X$ is called:

- *confluent*, if $y \stackrel{*}{\Longleftarrow} x \stackrel{*}{\Longrightarrow} z$ implies $y \stackrel{*}{\Longrightarrow} w \stackrel{*}{\Longleftarrow} z$ for some w;
- *terminating*, if every infinite chain

  $$x_0 \stackrel{*}{\Longrightarrow} x_1 \stackrel{*}{\Longrightarrow} \cdots x_{i-1} \stackrel{*}{\Longrightarrow} x_i \stackrel{*}{\Longrightarrow} \cdots$$

  becomes stationary;
- *convergent*, if it is confluent and terminating.

Rewriting Systems

A *rewriting relation* over a set X: $\Longrightarrow \subseteq X \times X$.

- $\stackrel{*}{\Longrightarrow}$: the reflexive and transitive closure of $\Longrightarrow$;
- $\stackrel{*}{\Longleftrightarrow}$: its symmetric, reflexive, and transitive closure.

The relation $\Longrightarrow \subseteq X \times X$ is called:

- *confluent*, if $y \stackrel{*}{\Longleftarrow} x \stackrel{*}{\Longrightarrow} z$ implies $y \stackrel{*}{\Longrightarrow} w \stackrel{*}{\Longleftarrow} z$ for some w;
- *terminating*, if every infinite chain

  $$x_0 \stackrel{*}{\Longrightarrow} x_1 \stackrel{*}{\Longrightarrow} \cdots x_{i-1} \stackrel{*}{\Longrightarrow} x_i \stackrel{*}{\Longrightarrow} \cdots$$

  becomes stationary;
- *convergent*, if it is confluent and terminating.

Rewriting system over a monoid

A *rewriting system* over a monoid M is a relation $S \subseteq M \times M$.

It defines the rewriting relation $\underset{S}{\Longrightarrow} \subseteq M \times M$ by

$$x \underset{S}{\Longrightarrow} y, \text{ if } x = p\ell q, \; y = prq \text{ for some } (\ell, r) \in S.$$

The relation $\overset{*}{\underset{S}{\Longleftrightarrow}} \subseteq M \times M$ is a congruence;

write M/S for the quotient monoid.

If $S \subseteq \Gamma^* \times \Gamma^*$ is a finite convergent string rewriting system (i.e $\underset{S}{\Longrightarrow}$ is a ....) then then the monoid M/S has decidable word problem.

Rewriting system over a monoid

A *rewriting system* over a monoid M is a relation $S \subseteq M \times M$.

It defines the rewriting relation $\underset{S}{\Longrightarrow} \subseteq M \times M$ by

$$x \underset{S}{\Longrightarrow} y, \text{ if } x = p\ell q,\ y = prq \text{ for some } (\ell, r) \in S.$$

The relation $\overset{*}{\underset{S}{\Longleftrightarrow}} \subseteq M \times M$ is a congruence;

write M/S for the quotient monoid.

If $S \subseteq \Gamma^* \times \Gamma^*$ is a finite convergent string rewriting system (i.e $\underset{S}{\Longrightarrow}$ is a ....) then then the monoid M/S has decidable word problem.

Rewriting system over a monoid

A *rewriting system* over a monoid M is a relation $S \subseteq M \times M$.

It defines the rewriting relation $\underset{S}{\Longrightarrow} \subseteq M \times M$ by

$$x \underset{S}{\Longrightarrow} y, \text{ if } x = p\ell q,\ y = prq \text{ for some } (\ell, r) \in S.$$

The relation $\overset{*}{\underset{S}{\Longleftrightarrow}} \subseteq M \times M$ is a congruence;

write M/S for the quotient monoid.

If $S \subseteq \Gamma^* \times \Gamma^*$ is a finite convergent string rewriting system (i.e $\underset{S}{\Longrightarrow}$ is a ....) then then the monoid M/S has decidable word problem.

Rewriting system over a monoid

A *rewriting system* over a monoid M is a relation $S \subseteq M \times M$.

It defines the rewriting relation $\underset{S}{\Longrightarrow} \subseteq M \times M$ by

$$x \underset{S}{\Longrightarrow} y, \text{ if } x = p\ell q,\ y = prq \text{ for some } (\ell, r) \in S.$$

The relation $\underset{S}{\overset{*}{\Longleftrightarrow}} \subseteq M \times M$ is a congruence;

write M/S for the quotient monoid.

If $S \subseteq \Gamma^* \times \Gamma^*$ is a finite convergent string rewriting system (i.e $\underset{S}{\Longrightarrow}$ is a ....) then then the monoid M/S has decidable word problem.

Rewriting system over a monoid

A *rewriting system* over a monoid M is a relation $S \subseteq M \times M$.

It defines the rewriting relation $\underset{S}{\Longrightarrow} \subseteq M \times M$ by

$$x \underset{S}{\Longrightarrow} y, \text{ if } x = p\ell q, \; y = prq \text{ for some } (\ell, r) \in S.$$

The relation $\overset{*}{\underset{S}{\Longleftrightarrow}} \subseteq M \times M$ is a congruence;

write M/S for the quotient monoid.

If $S \subseteq \Gamma^* \times \Gamma^*$ is a finite convergent string rewriting system (i.e $\underset{S}{\Longrightarrow}$ is a ....) then then the monoid M/S has decidable word problem.

Pre-perfect rewriting systems

Definition

A rewriting system $S \subseteq \Gamma^* \times \Gamma^*$ is called *pre-perfect*, if:

i.) S is confluent.

ii.) If $\ell \longrightarrow r \in S$, then $|\ell| \geq |r|$.

iii.) If $\ell \longrightarrow r \in S$ with $|\ell| = |r|$, then $r \longrightarrow \ell \in S$, too.

- A convergent length-reducing system is pre-perfect,
- If a confluent system satisfies $|\ell| \geq |r|$ for all $\ell \longrightarrow r \in S$, then we can add symmetric rules in order to make it pre-perfect.
- Includes non-terminating and infinite systems.
- Leads to a (PSPACE-)decision algorithm for the word problem (for finite systems).

Pre-perfect rewriting systems

Definition

A rewriting system $S \subseteq \Gamma^* \times \Gamma^*$ is called *pre-perfect*, if:

i.) S is confluent.

ii.) If $\ell \longrightarrow r \in S$, then $|\ell| \geq |r|$.

iii.) If $\ell \longrightarrow r \in S$ with $|\ell| = |r|$, then $r \longrightarrow \ell \in S$, too.

- A convergent length-reducing system is pre-perfect,
- If a confluent system satisfies $|\ell| \geq |r|$ for all $\ell \longrightarrow r \in S$, then we can add symmetric rules in order to make it pre-perfect.
- Includes non-terminating and infinite systems.
- Leads to a (PSPACE-)decision algorithm for the word problem (for finite systems).

Pre-perfect rewriting systems

Definition

A rewriting system $S \subseteq \Gamma^* \times \Gamma^*$ is called *pre-perfect*, if:

i.) S is confluent.

ii.) If $\ell \longrightarrow r \in S$, then $|\ell| \geq |r|$.

iii.) If $\ell \longrightarrow r \in S$ with $|\ell| = |r|$, then $r \longrightarrow \ell \in S$, too.

- A convergent length-reducing system is pre-perfect,
- If a confluent system satisfies $|\ell| \geq |r|$ for all $\ell \longrightarrow r \in S$, then we can add symmetric rules in order to make it pre-perfect.
- Includes non-terminating and infinite systems.
- Leads to a (PSPACE-)decision algorithm for the word problem (for finite systems).

Pre-perfect rewriting systems

Definition
A rewriting system $S \subseteq \Gamma^* \times \Gamma^*$ is called *pre-perfect*, if:

i.) S is confluent.

ii.) If $\ell \longrightarrow r \in S$, then $|\ell| \geq |r|$.

iii.) If $\ell \longrightarrow r \in S$ with $|\ell| = |r|$, then $r \longrightarrow \ell \in S$, too.

- A convergent length-reducing system is pre-perfect,
- If a confluent system satisfies $|\ell| \geq |r|$ for all $\ell \longrightarrow r \in S$, then we can add symmetric rules in order to make it pre-perfect.
- Includes non-terminating and infinite systems.
- Leads to a (PSPACE-)decision algorithm for the word problem (for finite systems).

Pre-perfect rewriting systems

Definition

A rewriting system $S \subseteq \Gamma^* \times \Gamma^*$ is called *pre-perfect*, if:

i.) S is confluent.

ii.) If $\ell \longrightarrow r \in S$, then $|\ell| \geq |r|$.

iii.) If $\ell \longrightarrow r \in S$ with $|\ell| = |r|$, then $r \longrightarrow \ell \in S$, too.

- A convergent length-reducing system is pre-perfect,
- If a confluent system satisfies $|\ell| \geq |r|$ for all $\ell \longrightarrow r \in S$, then we can add symmetric rules in order to make it pre-perfect.
- Includes non-terminating and infinite systems.
- Leads to a (PSPACE-)decision algorithm for the word problem (for finite systems).

A rewriting system for $U(P)$

Define $S \subseteq P^* \times P^*$ by

$$\begin{array}{rcll} 1 & \longrightarrow & \varepsilon & (= \text{the empty word}) \\ ab & \longrightarrow & [ab] & \text{if } (a,b) \in D \\ ab & \longleftrightarrow & [ac][c^{-1}b] & \text{if } (a,c),\ (c^{-1},b) \in D \end{array}$$

Proposition (Diekert, AD, Miasnikov, '08)

- *P^*/S defines $U(P)$.*
- *The system S is strongly confluent and therefore pre-perfect.*
- *Stallings' normal form theorem for $U(P)$ follows easily.*
- *Normal forms for free products with amalgamation and HNN-extensions also follow from specialisations of the rewriting system to these cases.*

A rewriting system for $U(P)$

Define $S \subseteq P^* \times P^*$ by

$$\begin{array}{rcll} 1 & \longrightarrow & \varepsilon & (= \text{the empty word}) \\ ab & \longrightarrow & [ab] & \text{if } (a,b) \in D \\ ab & \longleftrightarrow & [ac][c^{-1}b] & \text{if } (a,c),\ (c^{-1},b) \in D \end{array}$$

Proposition (Diekert, AD, Miasnikov, '08)

- *P^*/S defines $U(P)$.*
- *The system S is strongly confluent and therefore pre-perfect.*
- *Stallings' normal form theorem for $U(P)$ follows easily.*
- *Normal forms for free products with amalgamation and HNN-extensions also follow from specialisations of the rewriting system to these cases.*

A rewriting system for $U(P)$

Define $S \subseteq P^* \times P^*$ by

$$\begin{array}{rcll} 1 & \longrightarrow & \varepsilon & (= \text{the empty word}) \\ ab & \longrightarrow & [ab] & \text{if } (a,b) \in D \\ ab & \longleftrightarrow & [ac][c^{-1}b] & \text{if } (a,c), (c^{-1},b) \in D \end{array}$$

Proposition (Diekert, AD, Miasnikov, '08)

- *P^*/S defines $U(P)$.*
- *The system S is strongly confluent and therefore pre-perfect.*
- *Stallings' normal form theorem for $U(P)$ follows easily.*
- *Normal forms for free products with amalgamation and HNN-extensions also follow from specialisations of the rewriting system to these cases.*

A rewriting system for $U(P)$

Define $S \subseteq P^* \times P^*$ by

$$\begin{array}{rcll} 1 & \longrightarrow & \varepsilon & (= \text{the empty word}) \\ ab & \longrightarrow & [ab] & \text{if } (a,b) \in D \\ ab & \longleftrightarrow & [ac][c^{-1}b] & \text{if } (a,c),\, (c^{-1},b) \in D \end{array}$$

Proposition (Diekert, AD, Miasnikov, '08)

- *P^*/S defines $U(P)$.*
- *The system S is strongly confluent and therefore pre-perfect.*
- *Stallings' normal form theorem for $U(P)$ follows easily.*
- *Normal forms for free products with amalgamation and HNN-extensions also follow from specialisations of the rewriting system to these cases.*

A rewriting system for $U(P)$

Define $S \subseteq P^* \times P^*$ by

$$\begin{array}{rcll} 1 & \longrightarrow & \varepsilon & (= \text{the empty word}) \\ ab & \longrightarrow & [ab] & \text{if } (a,b) \in D \\ ab & \longleftrightarrow & [ac][c^{-1}b] & \text{if } (a,c),\ (c^{-1},b) \in D \end{array}$$

Proposition (Diekert, AD, Miasnikov, '08)

- *P^*/S defines $U(P)$.*
- *The system S is strongly confluent and therefore pre-perfect.*
- *Stallings' normal form theorem for $U(P)$ follows easily.*
- *Normal forms for free products with amalgamation and HNN-extensions also follow from specialisations of the rewriting system to these cases.*

Given G and an isomorphism $\theta : H \to K$, where H and K are subgroups of G, let t be a symbol not in G and let X and Y be right transversals for H and K in G.

Set

$$P = G \cup GtY \cup Gt^{-1}X$$

and

$$D = G \times G \cup G \times GtY \cup G \times Gt^{-1}X \cup GtY \times G \cup Gt^{-1} \times G \cup S_A \cup S_B,$$

where

$$S_A = \{(ht^{-1}c, gtd) | g, h \in G, c \in X, d \in Y, cg \in A\} \text{ and}$$
$$S_B = \{(gtd, ht^{-1}c) | g, h \in G, d \in Y, c \in X, dh \in B\}.$$

Then P is a pregroup and $U(P) = H$.

Given G and an isomorphism $\theta : H \to K$, where H and K are subgroups of G, let t be a symbol not in G and let X and Y be right transversals for H and K in G.
Set

$$P = G \cup GtY \cup Gt^{-1}X$$

and

$$D = G \times G \cup G \times GtY \cup G \times Gt^{-1}X \cup GtY \times G \cup Gt^{-1} \times G \cup S_A \cup S_B,$$

where

$$S_A = \{(ht^{-1}c, gtd) | g, h \in G, c \in X, d \in Y, cg \in A\} \text{ and}$$
$$S_B = \{(gtd, ht^{-1}c) | g, h \in G, d \in Y, c \in X, dh \in B\}.$$

Then P is a pregroup and $U(P) = H$.

Given G and an isomorphism $\theta : H \to K$, where H and K are subgroups of G, let t be a symbol not in G and let X and Y be right transversals for H and K in G.
Set

$$P = G \cup GtY \cup Gt^{-1}X$$

and

$$D = G \times G \cup G \times GtY \cup G \times Gt^{-1}X \cup GtY \times G \cup Gt^{-1} \times G \cup S_A \cup S_B,$$

where

$$S_A = \{(ht^{-1}c, gtd) | g, h \in G, c \in X, d \in Y, cg \in A\} \text{ and}$$
$$S_B = \{(gtd, ht^{-1}c) | g, h \in G, d \in Y, c \in X, dh \in B\}.$$

Then P is a pregroup and $U(P) = H$.

Given G and an isomorphism $\theta : H \to K$, where H and K are subgroups of G, let t be a symbol not in G and let X and Y be right transversals for H and K in G.
Set

$$P = G \cup GtY \cup Gt^{-1}X$$

and

$$D = G \times G \cup G \times GtY \cup G \times Gt^{-1}X \cup GtY \times G \cup Gt^{-1} \times G \cup S_A \cup S_B,$$

where

$$S_A = \{(ht^{-1}c, gtd) | g, h \in G, c \in X, d \in Y, cg \in A\} \text{ and}$$
$$S_B = \{(gtd, ht^{-1}c) | g, h \in G, d \in Y, c \in X, dh \in B\}.$$

Then P is a pregroup and $U(P) = H$.

Computability

Rabin's definition:
a map $i : G \to \mathbb{N}$ with $i(G)$ recursive is an *indexing*.

G is *computable* if G has an indexing such that the map
$m : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$(i(g), i(h)) \mapsto i(gh)$$

is recursive.

Rabin '67: A finitely generated group has solvable word problem iff it is computable.

Computability

Rabin's definition:
a map $i : G \to \mathbb{N}$ with $i(G)$ recursive is an *indexing*.

G is *computable* if G has an indexing such that the map
$m : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$(i(g), i(h)) \mapsto i(gh)$$

is recursive.

Rabin '67: A finitely generated group has solvable word problem iff it is computable.

Computability

Rabin's definition:
a map $i : G \to \mathbb{N}$ with $i(G)$ recursive is an *indexing*.

G is *computable* if G has an indexing such that the map
$m : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$(i(g), i(h)) \mapsto i(gh)$$

is recursive.

Rabin '67: A finitely generated group has solvable word problem iff it is computable.

Computable Pregroup

A pregroup P is *computable* if P has an indexing i such that

- $i \times i(D)$ is recursive and;
- $i \times i \times i(M)$ is recursive,

where

$$M = \{(a, b, c) | (a, b) \in D \text{ and } c = [ab]\}.$$

Proposition (Diekert, AD, Miasnikov)

If P is a computable pregroup then

1. *the word problem in $U(P)$ is solvable, relative to the generating set P and*
2. *$U(P)$ is a computable group.*

Computable Pregroup

A pregroup P is *computable* if P has an indexing i such that

- $i \times i(D)$ is recursive and;
- $i \times i \times i(M)$ is recursive,

where

$$M = \{(a, b, c) | (a, b) \in D \text{ and } c = [ab]\}.$$

Proposition (Diekert, AD, Miasnikov)

If P is a computable pregroup then

1. *the word problem in $U(P)$ is solvable, relative to the generating set P and*
2. *$U(P)$ is a computable group.*

Computable Pregroup

A pregroup P is *computable* if P has an indexing i such that

- $i \times i(D)$ is recursive and;
- $i \times i \times i(M)$ is recursive,

where

$$M = \{(a, b, c) | (a, b) \in D \text{ and } c = [ab]\}.$$

Proposition (Diekert, AD, Miasnikov)

If P is a computable pregroup then

1. *the word problem in $U(P)$ is solvable, relative to the generating set P and*
2. *$U(P)$ is a computable group.*

Computable Pregroup

A pregroup P is *computable* if P has an indexing i such that

- $i \times i(D)$ is recursive and;
- $i \times i \times i(M)$ is recursive,

where

$$M = \{(a, b, c) | (a, b) \in D \text{ and } c = [ab]\}.$$

Proposition (Diekert, AD, Miasnikov)

If P is a computable pregroup then

1. *the word problem in $U(P)$ is solvable, relative to the generating set P and*
2. *$U(P)$ is a computable group.*

Computable Pregroup

A pregroup P is *computable* if P has an indexing i such that

- $i \times i(D)$ is recursive and;
- $i \times i \times i(M)$ is recursive,

where

$$M = \{(a, b, c) | (a, b) \in D \text{ and } c = [ab]\}.$$

Proposition (Diekert, AD, Miasnikov)

If P is a computable pregroup then

1. *the word problem in $U(P)$ is solvable, relative to the generating set P and*
2. *$U(P)$ is a computable group.*

Conjugacy

Let $u = u_1 \cdots u_n \in P^*$ cyclically reduced of length n (reduced and $(u_n, u_1) \notin D$).

If $u = v_1 \cdots v_n$ then $v = v_i \cdots v_n v_1 \cdots v_{i-1}$ is a *cyclic permutation* of u over $U(P)$.

Lemma (D,D,M)

Let u be a cyclically reduced element of P^* and let v be a cyclic permutation of u. Then v is cyclically reduced. In particular, u and v have the same length.

Theorem (D,D,M)

Let u and v be cyclically reduced elements of P^* such that u is conjugate to v in $U(P)$. Then, we have:

1. *u and v have the same length.*
2. *If $u \notin P$, i.e., $n \geq 2$, then we can transform u into v by a sequence of cyclic permutations.*

Conjugacy

Let $u = u_1 \cdots u_n \in P^*$ cyclically reduced of length n (reduced and $(u_n, u_1) \notin D$).

If $u = v_1 \cdots v_n$ then $v = v_i \cdots v_n v_1 \cdots v_{i-1}$ is a *cyclic permutation* of u over $U(P)$.

Lemma (D,D,M)

Let u be a cyclically reduced element of P^* and let v be a cyclic permutation of u. Then v is cyclically reduced. In particular, u and v have the same length.

Theorem (D,D,M)

Let u and v be cyclically reduced elements of P^* such that u is conjugate to v in $U(P)$. Then, we have:

1. *u and v have the same length.*
2. *If $u \notin P$, i.e., $n \geq 2$, then we can transform u into v by a sequence of cyclic permutations.*

Conjugacy

Let $u = u_1 \cdots u_n \in P^*$ cyclically reduced of length n (reduced and $(u_n, u_1) \notin D$).

If $u = v_1 \cdots v_n$ then $v = v_i \cdots v_n v_1 \cdots v_{i-1}$ is a *cyclic permutation* of u over $U(P)$.

Lemma (D,D,M)

Let u be a cyclically reduced element of P^* and let v be a cyclic permutation of u. Then v is cyclically reduced. In particular, u and v have the same length.

Theorem (D,D,M)

Let u and v be cyclically reduced elements of P^* such that u is conjugate to v in $U(P)$. Then, we have:

1. *u and v have the same length.*
2. *If $u \notin P$, i.e., $n \geq 2$, then we can transform u into v by a sequence of cyclic permutations.*

Conjugacy

Let $u = u_1 \cdots u_n \in P^*$ cyclically reduced of length n (reduced and $(u_n, u_1) \notin D$).

If $u = v_1 \cdots v_n$ then $v = v_i \cdots v_n v_1 \cdots v_{i-1}$ is a *cyclic permutation* of u over $U(P)$.

Lemma (D,D,M)

Let u be a cyclically reduced element of P^* and let v be a cyclic permutation of u. Then v is cyclically reduced. In particular, u and v have the same length.

Theorem (D,D,M)

Let u and v be cyclically reduced elements of P^* such that u is conjugate to v in $U(P)$. Then, we have:

1. *u and v have the same length.*
2. *If $u \notin P$, i.e., $n \geq 2$, then we can transform u into v by a sequence of cyclic permutations.*

Conjugacy

Let $u = u_1 \cdots u_n \in P^*$ cyclically reduced of length n (reduced and $(u_n, u_1) \notin D$).

If $u = v_1 \cdots v_n$ then $v = v_i \cdots v_n v_1 \cdots v_{i-1}$ is a *cyclic permutation* of u over $U(P)$.

Lemma (D,D,M)

Let u be a cyclically reduced element of P^* and let v be a cyclic permutation of u. Then v is cyclically reduced. In particular, u and v have the same length.

Theorem (D,D,M)

Let u and v be cyclically reduced elements of P^* such that u is conjugate to v in $U(P)$. Then, we have:

1. *u and v have the same length.*
2. *If $u \notin P$, i.e., $n \geq 2$, then we can transform u into v by a sequence of cyclic permutations.*