Alphabets, words & Monoids.

Let X - set. (finite)

Defn:

A word over X is a finite sequence $W = (x_1, \dots, x_k)$ of elements from X.

$\varepsilon = ()$ (the empty word)

X^* - the set of all words over X

$Mon(X) := (X^*, \cdot, \varepsilon)$ monoid of words over alphabet X.

$|W| = k$ - the length of W

If $W = A \cdot B \cdot C$ for $A, B, C \in X^*$

then
- A is prefix of W
- B is subword of W
- C is suffix of W.

If $W = (x_1, \dots, x_k) = x_1 x_2 \cdot \ldots \cdot x_k$, then any of $x_2 \cdot \ldots \cdot x_k x_1$, $x_3 \cdot \ldots \cdot x_k x_1 x_2$ etc is cyclic permutation of W.

$(M, \cdot, e)$ - monoid, then $S \subseteq M$ is a submonoid iff
- $\varepsilon \in S$
- $\forall a, b \in S \quad a \cdot b \in S$.

Lemma:

An intersection of submonoids is a submonoid.

Let $Y \subset M$ be a subset.

Defn:

A monoid generated by Y, $\mathrm{Mon}\langle Y\rangle$ is the intersection $\bigcap S$ of all submonoids containing Y.

Lemma: If $Y = \{y_1, \dots, y_n\}$ then

$$\mathrm{Mon}\langle Y\rangle = \{ w : w = \prod_k y_{i_k} \}.$$

Defn: If $a \in M$ & $\exists A \in M$ s.t.

$aA = Aa = \varepsilon \Rightarrow$ we call a a unit.

If $Y \subset$ units of $M \Rightarrow \mathrm{Mon}\langle Y \cup Y^{-1}\rangle$ is a group

$\mathrm{Grp}\langle Y\rangle = \mathrm{Mon}\langle Y \cup Y^{-1}\rangle$.

Defn: M is finitely generated iff

$M = \mathrm{Mon}\langle Y\rangle$ for a finite $Y \subset M$.

Proposition: (von Dyck 1882).

If G is generated (as a group) by n elts, it is generated (as a monoid) by $(n+1)$ elts:

If G is generated (as a group) by $x_1, \dots, x_n$ then G is generated (as monoid) by $x_1, \dots, x_n, y$

$$y = \prod_i x_i^{-1}.$$

A Monoid is *cyclic* if it is generated by a set of cardinality 1.

Proposition: If M - finitely generated monoid
$\Rightarrow$ every generating set contains a finite generating subset.

Proof: Let $M = Mon\langle X \rangle$, X - finite

Let Y be an infinite generating set for M.

write $x_i \in X$ as a word w_i over Y

$|w_i|$ - finite

+ finite nr. of x_i $\Rightarrow$ the union of all letters $y \in Y$ that appear in all w_i is finite

$\rightarrow$ this set $Z \subset Y$ generates M.

(the same happens for groups).

Defn: $f: M \to N$ is a homomorphism if $f(1_M) = f(1_N)$ & $f(xy) = f(x)f(y)$ $\forall x, y \in M$.

Note: If M is a group $\Rightarrow$ $f(M)$ is a subgroup of N.

__Defn:__ $Mon\langle X\rangle$ (X^*) is called the __free monoid__ generated by X.

__Proposition:__

let X - set, M - monoid

for every $f: X \to M$

there exists exactly one $\bar{f}: X^* \to M$ homomorphism

extending f:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "i"'] & M \\ X^* \arrow[ur, "\exists!\bar{f}"'] & \end{tikzcd}.$$

__Proof:__

$x \in X,\ y \in X^* \Rightarrow \bar{f}(xy) = f(x)\bar{f}(y)$, $\bar{f}(\varepsilon) = 1$

Proof that $\bar{f}$ is a homomorphism:

$$\overline{f(u\cdot w)} = \bar{f}(x \cdot u' \cdot w) \quad \text{where} \quad u = x_1 u'$$

$$= f(x_1)\cdot \bar{f}(u'\cdot w) = \ldots =$$

$$= f(x_1)\cdot f(x_2)\cdot \bar{f}(u''\cdot w) =$$

$$= f(x_1)\cdot \bar{f}(x_2) = \bar{f}(u)\cdot \bar{f}(w).$$

$\square$

Presentations:

<u>Defn:</u> A <u>congruence</u> on M (monoid) is a bi-invariant equivalence relation on $M \times M$

i.e.
$\forall x, y, z \in M \quad x \sim y \Rightarrow xz \sim yz \ \& \ zx \sim zy.$

<u>Ex:</u>
Let $f : M \to N$ be a homomorphism of monoids
$x \sim_f y := f(x) = f(y)$ is a congruence on M

<u>Proposition:</u>
Every congruence $\sim$ on M is of the form $\sim_f$ for some $f : M \to N$.

<u>Proof:</u>
Let Q be the set of eq. classes of $\sim$.
on Q define multiplication as
$[x] \cdot [y] = [xy]$ <u>Claim: this is well defined:</u>

$\left.\begin{array}{l} x, x' \in [x] \\ y, y' \in [y] \end{array}\right\} \Rightarrow x'y' \in [xy]$

$x \sim x' \Rightarrow x'y' \sim xy'$
$y \sim y' \Rightarrow xy' \sim xy$

Q with this relation becomes a monoid with $[1]$ as identity.

$\square$

<u>Defn:</u> Q is called the quotient monoid or $M/\sim$; $x \mapsto [x]$ is a monoid homomorphism.

Ex: $f =$ 

$f^5 = f \qquad M = \mathrm{Mon}\langle f \rangle$ order: 5

$\sim$ on M:

$\underbrace{\{1\}}_{1}, \underbrace{\{f, f^3\}}_{u}, \underbrace{\{f^2, f^4\}}_{u^2}$ $\sim$ classes

$f \sim f^3 \Rightarrow f f \sim f f^3$ ✓

$f^3 \cdot f^3 = f^6 = f^2$

$f^3 \cdot f = f^4$.

$M/_\sim = \{1, u, u^2\}$

$u^3 = u$.

Proposition: let M - monoid, $S \subset M \times M$ - subset. intersection $\sim_S$ of all congruences containing S is a congruence.

Proof: the intersection is not-empty since "full congruence" $\to M \times M \supset \sim_S$

$\forall s, t \in S \quad s \sim_S t$.

Let $x \sim_S y \Rightarrow \forall \equiv$ ← congruence relation containing S

we have $x \equiv y$ and hence $xz \equiv yz$ & $zx \equiv zy$.

but that also means that $xz \sim_S yz$ & $zx \sim_S zy$.

$\square$

Defn: $\sim_S$ is the congruence generated by S.

Proposition:

Let M - monoid, $S \subset M \times M$ & $\sim_S$ the congruence generated by S.

$\pi : M \longrightarrow M/_{\sim_S}$ be the canonical quotient map.

Let $f : M \longrightarrow N$
a homomorphism of monoids s.t.
$f(s) = f(t) \quad \forall (s,t) \in S$.

$$\Rightarrow \quad \begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & N \\ M/_{\sim_S} \arrow[ur, dashed, "\exists ! \overline{f}"'] & \end{tikzcd} \quad \text{s.t. } f = \overline{f} \circ \pi.$$

Proof: Existence:

$f \rightsquigarrow \sim_f \; ; \; S \subset \sim_f \Rightarrow \sim_S \subset \sim_f$.

$\Rightarrow \overline{f}([x]_{\sim_S}) = [x]_{\sim_f}$ is well defined.

It's a homomorphism:

$\overline{f}([1]_{\sim_S}) = [1]_{\sim_f}$ ✓

$\overline{f}([x]_{\sim_S} \cdot [y]_{\sim_S}) = \overline{f}([xy]_{\sim_S}) =$

$= [xy]_{\sim_f} = [x]_{\sim_f} \cdot [y]_{\sim_f} = \overline{f}([x]_{\sim_S}) \cdot \overline{f}([y]_{\sim_S})$. ✓

Let X - alphabet, $S \subset X^* \times X^*$.

<u>Defn:</u> $\mathrm{Mon}\langle X \mid S\rangle := X^*/_{\sim_S}$

(X, S) - monoid presentation for $X^*/_{\sim_S}$

Let M

- M - finitely generated iff $M \cong \mathrm{Mon}\langle X \mid S\rangle$ for some $|X| < \infty$.
- M - ——— presented iff $M \cong \mathrm{Mon}\langle X \mid S\rangle$ for some $|X| < \infty$, $|S| < \infty$.

<u>Ex:</u> $X = \{a, b\}$, $R = \{\underset{(1)}{(ab, ba)}, \underset{(2)}{(a^4, a^2)}, \underset{(3)}{(b^3, a^3)}\}$

$\mathrm{Mon}\langle X \mid R\rangle = ?$

$[w] \overset{(1)}{=} [a^i b^j] \quad i, j \geq 0$

by (2) $\quad 0 \leq i \leq 3$

by (3) $\quad 0 \leq j \leq 2$

$$\begin{array}{ccc} \varepsilon & b & b^2 \\ a & ab & ab^2 \\ a^2 & a^2b & a^2b^2 \\ a^3 & a^3b & a^3b^2 \end{array} \longrightarrow \begin{cases} f: 0\ldots n \to 0\ldots n & f^4 = f^2 \\ g: 0\ldots n \to 0\ldots n & g^3 = f^3 \\ f \circ g = g \circ f & \end{cases}$$

at most 12 elts

$$f = \begin{cases} 0 \to 1 \to 2 \to 3 \\ 4 \to 5 \to 6 \to 7 \\ 8 \to 9 \to 10 \to 11 \end{cases} \qquad g = \begin{cases} 0 \to 4 \to 8 \\ 1 \to 5 \to 9 \\ 2 \to 6 \to 10 \\ 3 \to 7 \to 11 \end{cases}$$

you may check that

<u>$f^i \circ g^j$ are all different</u>

$\Rightarrow M$ contains 12 elts.

Ex: $X = \{a, b\}$ $R = \{(ab^3a, b), (ba^2b, a)\}$

Prove that $[a]^6 = [\varepsilon]$.

<u>Proposition</u>: let $R \subset S \subset X^* \times X^*$ for an alphabet X. The map

$$\mathrm{Mon}\langle X | R\rangle \longrightarrow \mathrm{Mon}\langle X | S\rangle$$

$$[\omega]_{\sim_R} \longrightarrow [\omega]_{\sim_S}$$

is an epimorphism.

$\square$

X - a finite set

$X^{\pm 1} = X \times \{-1, 1\}$

$(X^{\pm 1})^*$ - free monoid over $X^{\pm}$

$R = \{((x,1)(x,-1), \varepsilon), ((x,-1)(x,1), \varepsilon)\}_{x \in X}$

$\mathrm{Mon}\langle X^{\pm 1} | R\rangle = (X^{\pm 1})^* / \sim_R$ is called the <u>free group generated by X</u>.

<u>Proposition</u>:

- $\mathrm{Mon}\langle X^{\pm 1} | R\rangle$ is a group
- for every map $X \xrightarrow{f} G$ ← group
  $\exists!\, \bar{f} : \mathrm{Mon}\langle X^{\pm 1} | R\rangle \longrightarrow G$ homomorphism "extending" f.

Note: instead of $\mathcal{A} \times \{-1, 1\}$

we will often write:

$$\mathcal{A} = \{x_1, \dots, x_n\} \qquad \bar{A} = A \cup \mathcal{A}'$$
$$\mathcal{A}' = \{X_1, \dots, X_n\}$$

$$\underbrace{R = \{(x_i X_i, \varepsilon), (X_i x_i, \varepsilon)\}_{i=1}^{n}}_{FGRel(\mathcal{A})} \subset \bar{\mathcal{A}}^* \times \bar{\mathcal{A}}^*$$

Defn $w \in \bar{\mathcal{A}}^*$ is freely reduced if w contains no subword $x_i X_i$ or $X_i x_i$ $\forall i$.

Defn: If $S \subset \bar{\mathcal{A}}^* \times \bar{\mathcal{A}}^*$ then

$$Grp\langle \mathcal{A} \mid S \rangle := Mon\langle \bar{\mathcal{A}} \mid FGRel(\mathcal{A}) \cup S \rangle.$$

$(\mathcal{A}, S)$ - group presentation.

Proposition:

If $Mon\langle \mathcal{A} \mid S \rangle$ is a group then

$$Mon\langle \mathcal{A} \mid S \rangle \cong Grp\langle \mathcal{A} \mid S \rangle.$$

$\square$

Let $M = \mathrm{Mon}\langle A \mid R\rangle$.

$\sim_R$ - the congruence on A^* generated by R.

if $(u,v) \in \sim_R$ then we say that

(u,v) is a <u>consequence</u> of R.

<u>Proposition:</u>

1) If (u,v) is a consequence of R, then

$$\mathrm{Mon}\langle A ; R\rangle \cong \mathrm{Mon}\langle A \mid R \cup \{(u,v)\}\rangle.$$

2) If $(u,v) \in R$ is a consequence of $R \setminus \{(u,v)\}$ then

$$\mathrm{Mon}\langle A \mid R\rangle \cong \mathrm{Mon}\langle A \mid R \setminus \{(u,v)\}\rangle.$$

3) If $u \in A^*$ and $y \notin A \Rightarrow$

$$\mathrm{Mon}\langle A \mid R\rangle \cong \mathrm{Mon}\langle A \cup \{y\} \mid R \cup \{(y,u)\}\rangle.$$

4) Suppose that $(y,u) \in R$ s.t.

- $|y| = 1$
- y is not a subword of u.

Let $B = A \setminus \{y\}$ and let $f : A^* \longrightarrow B^*$ be a homomorphism given by

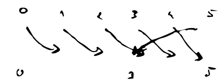
$$\begin{cases} f(a) = a & \text{if } a \in B \\ f(y) = u \end{cases}$$

$$\mathrm{Mon}\langle A \mid R\rangle \cong \mathrm{Mon}\langle B \mid S\rangle$$

$$S = \{(f(a), f(b))\}_{(a,b) \in R,\ (a,b) \neq (y,u)}.$$

Example: $\mathcal{A} = \{x\}$, $\mathcal{R} = \{(x^6, x^3)\}$

$\mathrm{Mon}\langle \mathcal{A} \mid \mathcal{R} \rangle$ has order 6



$$\mathrm{Grp}\langle \mathcal{A} \mid \mathcal{R} \rangle = \mathrm{Mon}\langle \{x, X\} \mid \underbrace{\{(xX, \varepsilon), (Xx, \varepsilon), (x^6, x^3)\}}_{\mathcal{S}} \rangle$$

$$x^6 \sim x^3$$

$$X^3 x^6 \sim X^3 x^3$$

$x^3 \sim \varepsilon$ is a consequence of $\mathcal{S}$

$$\overset{(1)}{=} \mathrm{Mon}\langle \{x, X\} \mid \{(xX, \varepsilon), (Xx, \varepsilon), (x^6, x^3), (x^3, \varepsilon)\} \rangle =$$

$$\overset{(2)}{=} \mathrm{Mon}\langle \{x, X\} \mid \{(xX, \varepsilon), (Xx, \varepsilon), (x^3, \varepsilon)\} \rangle$$

$$\varepsilon \sim x^3$$

$$X \sim Xx^3 \sim x^2$$

$$\overset{(1)}{=} \mathrm{Mon}\langle \{x, X\} \mid \{(xX, \varepsilon), (Xx, \varepsilon), (x^3, \varepsilon), \underline{\underline{(X, x^2)}}\}$$

$$f : \{x, X\}^* \to \{x\}^*$$
$$x \longmapsto x$$
$$X \longmapsto x^2$$

$$\overset{(4)}{=} \mathrm{Mon}\langle \{x\} \mid \{(x^3, \varepsilon), (x^3, \varepsilon), (x^3, \varepsilon)\} \rangle$$

$$\overset{(2)}{=} \mathrm{Mon}\langle \{x\} \mid \{(x^3, \varepsilon)\} \rangle.$$

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

Problem: (the word problem)

given two words $u, v \in A^*$ decide

if $[u]_{\sim R} = [v]_{\sim R}$ or

if u and v represent the same element of M.

Theorem: The word problem is unsolvable

- in the category of finitely presented groups (P. Novikov 1955, W. Boone 1958)
- in the category of f. p. monoids (E. Post, A. Markov 1947)

- There exist a monoid with unsolvable word problem:

$A = \{a, b, c, d, e\}$ / Ex. due to G. S. Cejtin 1957.

$R = \{ ac = ca,\ ad = da,$
$bc = cb,\ bd = db,$
$ce = eca,\ de = edb,$
$cca = ccae \}$

What does exactly unsolvable mean?

Proposition:

Let $a, b \in A^*$ and $M = \mathrm{Mon}\langle A \mid R \rangle$

$a \sim b$ iff there exists a sequence of words

$$a = a_0, a_1, \dots, a_t = b \quad \text{s.t.}$$

$\forall i \; \exists x, y, p, q \in X^*$

$$a_i = xpy$$

$$a_{i+1} = xqy$$

and $(p, q) \in R$.

Proof:

write $a \equiv b$ when such seq. exists

← eq. relation

$a \equiv b \Rightarrow \forall x \quad ax \equiv bx$

hence $\equiv$ is a congruence.

- $R \subset \equiv$ - trivial
- by defn of $\sim_R$ we have $\sim_R \subset \equiv$
- if $a \equiv b \Rightarrow a \sim_R b \Rightarrow \equiv \subset \sim_R$

(by transitivity + congruence

$$\equiv \; = \; \sim_R .$$

Corollary:

- It is decidable to verify that $a \sim_{\mathcal{R}} b$.
- It is possible to list all words in

  $[a]_{\sim_{\mathcal{R}}}$ (filter by the number of rewrites)
- If $b \sim_{\mathcal{R}} a$ we will find it at some point
- undecidability of the word problem implies that it is <u>not</u> possible to list all words in $\mathcal{A}^* \setminus [a]_{\sim_{\mathcal{R}}}$.

<u>Other unsolvable problems:</u>

- conjugacy problem in $\mathrm{Grp}\langle \mathcal{A} \mid \mathcal{R} \rangle$:

  given $a, b \in \mathcal{A}^*$ decide if

  $[a]_{\sim_{\mathcal{R}}}$ and $[b]_{\sim_{\mathcal{R}}}$ are conjugate

  (word problem in grps: $x = y \iff xy^{-1} = 1$

  take $a = x^{-1}y$, $b = 1$.)

- <u>subgroup membership problem</u>:

  $G = \mathrm{Grp}\langle \mathcal{A} \mid \mathcal{R} \rangle$; $u_1, \dots, u_m \in \mathcal{A}^*$

  $H = \langle [u_1], \dots, [u_m] \rangle < G$.

  Problem: decide if $v \in G$ belongs to H.

- given a f.p. monoid decide whether it is
  - finite
  - infinite
  - trivial
  - a group

Groups with solvable word problem:

- Automatic groups
  includes: finite, hyperbolic, Coxeter, Braid groups
- Free (abelian or not) groups
- Polycyclic groups
- Finitely presented simple groups
- One relator groups