Lecture 1

Monday, May 4, 2020 10:15 AM

Good morning and welcome to my first ever Zoom class.

<u>Def</u> An equivalence relation R on a set S is a set of pairs $R \subseteq S \times S$ s.t. [write xRy for $(x,y) \in R$]

(i) xRx (ref)

(ii) $xRy \Rightarrow yRx$ (symm)

(iii) xRy & $yRz \Rightarrow xRz$ (trans)

$[x] := \{y \mid xRy\}$ equivalence class

The set of equivalence classes forms a <u>partition</u> of S.

$S/R \to$ the set of equivalence classes.

<u>Partial order</u> : "comparison"

A binary relation on a set S

$\leq^{\sigma}$

(i) $x \leq x$

(ii) $x \leq y$ & $y \leq x \Rightarrow x = y$

(iii) $x \leq y$ & $y \leq z \Rightarrow x \leq z$.

(iv) if $\forall x, y$ $x \leq y$ or $y \leq x$ total order

WELL-FOUNDED ORDER :

$x < y$ means $x \leq y$ but $x \neq y$

Given a p.o. set $(S, \leq)$ & $U \subseteq S$, we say $u \in U$ is a minimal element of U if $\forall v < u$ $v \notin U$.

Def A poset $(S, \leq)$ is said to be well-founded if every non-empty subset U has a minimal element.

Ex: The non-negative integers $\mathbb{N}$

Ex 1. The non-negative ...

Ex 2. The positive rationals, not well founded.

Ex 3. Pairs $\mathbb{N}\times\mathbb{N}$ $(m,n) \leq (m',n')$

if $m < m'$ OR $m = m'$ & $n \leq n'$.

KEY FACT: An order is well founded if and only if there are no infinite strictly decreasing sequences (chain)

$$x_1 > x_2 > x_3 > \cdots$$

An order that is both total & well-founded is called a well order.

ZERMELO'S Thm: Every set can be given a well order assuming the axiom of choice.

Principle of Induction:

"predicate" $P(\cdot)$ S: set

$U := \{x \in S \mid P(x)\}$

$(S, \leq)$ is <u>inductive</u> if

$\forall P \quad \underline{\forall x \in S\left(\left(\forall y < x.\, P(y)\right) \Rightarrow P(x)\right)}$
$\Longrightarrow \forall x\, P(x)$

Not every order is inductive.

<u>Thm</u> An order is inductive <u>if and only if</u> it is well founded.

<u>Proof</u>: $WF \Rightarrow Ind$ $\quad (S, \leq)$ is WF

<u>Assume</u> $\forall x \in S\left(\forall y < x\, P(y)\right) \Rightarrow P(x)$

Assume $V := \{s \in S \mid \neg P(s)\}$ is not empty. So it has a minimal element v_0.

$\forall y < v_0 \quad y \notin V$ i.e. $P(y)$

but the assumption then $\Rightarrow P(v_0)$ $\otimes$

so $V = \phi$ i.e. $\forall x\ P(x)$ ☺

Ind $\Rightarrow$ WF Assume $U \subseteq S$ has no minimal element. $P(x) := x \notin U$.

$\forall x\ (\forall y < x\ P(y)) \Rightarrow P(x)$

But now IND says $\forall x\ P(x)$ i.e. $U = \phi$ & hence $(S, \leq)$ is well founded.

Emmy Noether

$\Sigma = \{a, b\}$ $\Sigma^* = \{\varepsilon, a, b, aa, ab, \cdots\}$
under lexicographic ordering this is <u>not</u> well founded.

<u>Lecture I Part II</u>

Σ : a <u>finite</u> set called an <u>alphabet</u>

$\Sigma = \{a, b\}$ $\Sigma = \{0, 1\}$

Σ^* : set of <u>finite</u> sequences

(words)

$\Sigma^* = \{\varepsilon, a, b, aa, ab, ba, bb, \ldots\}$

$L \subseteq \Sigma^*$ is called a <u>language</u>.

We will explore ways of <u>describing</u> a language & alg. for <u>testing</u> whether a word belongs to a language.

def A <u>monoid</u> is a set S with a binary operation $\cdot$ & a unit e:

(i) $\forall x, y, z \in S \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$

(ii) $\forall x \in S \quad x \cdot e = e \cdot x = x$

if (iii) $\forall x, y \quad x \cdot y = y \cdot x$ then we get a special kind of monoid called a <u>commutative</u> <u>monoid</u>.

Σ^* with concatenation & ε is a monoid; it is <u>NOT</u> commutative.

$aab \cdot ba = aabba$

(iv) $\forall x,y,z$ if $xy = xz \Rightarrow y = z$
CANCELLATIVE MONOID

<u>Def</u> If M_1 & M_2 are monoids &
$h: M_1 \to M_2$ satisfies
$h(x \cdot y) = h(x) \cdot h(y)$ &
$h(e_1) = e_2$
h is a HOMOMORPHISM.

---

suppose M is <u>any</u> monoid
& suppose $f: \Sigma \to M$ is <u>any</u>
function then $\exists$ a <u>unique</u>
<u>homomorphism</u> $f^*: \Sigma^* \to M$

s.t.
$$\begin{tikzcd} \Sigma \arrow[r, "\eta"] \arrow[dr, "f"'] & \Sigma^* \arrow[d, "f^*"] \\ & M \end{tikzcd}$$

$f = f^* \circ \eta$ where $\eta(a) = a \; \forall a \in \Sigma$.

This is called a <u>universal</u>
property; & Σ^* is called the <u>free</u>

monoid generated by Σ.

Ex Let S be any set & let $[S \to S]$ be the set of functions from S to itself. Then with $\circ$ as the operation & the id f^n as the unit we get a monoid.

Def A deterministic finite automaton (DFA) is a 5-tuple

$$A = (S, s_0 \in S, \Sigma, \delta : S \times \Sigma \to S, F \subseteq S)$$

This "reads" words from Σ^* & moves from state to state

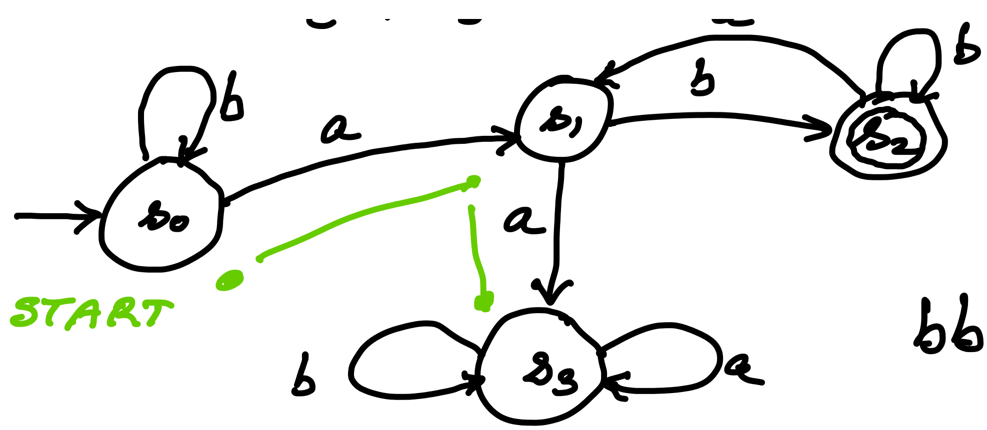
S: states s_0: start state

Σ: alphabet, δ: transition f^n

F: accepting states.

A reads a word from Σ^* and either accepts it or rejects it.

$\Sigma = \{a, b\}$



bbaab X

$\delta(s_0, a) = s_1$
$\delta(s_0, b) = s_0$

e.g. abbababb ✓

Formalizing acceptance:

$$\delta^* : S \times \Sigma^* \to S$$

by induction on length of $w \in \Sigma^*$
$|w|$: length of w

$$\delta^*(s, \varepsilon) = s$$
$$\delta^*(s, w \cdot a) = \delta(\underbrace{\delta^*(s, w)}_{s}, a) \quad \forall a \in \Sigma$$

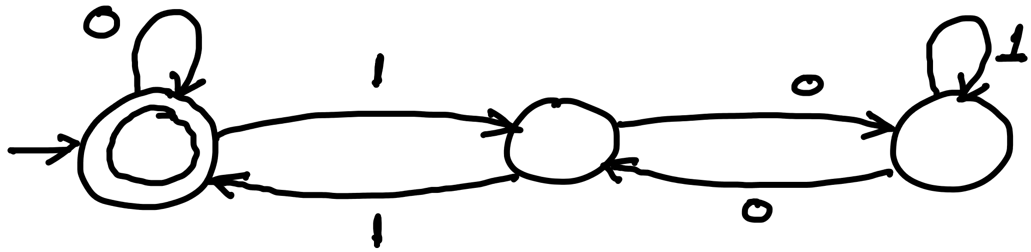
$$L(A) = \{ w \in \Sigma^* \mid \delta^*(s_0, w) \in F \}$$

↳ the language <u>accepted</u> by OR <u>recognized</u> by A.

<u>Def</u> A language recognized by

a DFA is called a <u>regular language</u>.

$\Sigma = \{0, 1\}$



$L(A) = \{0, \varepsilon, 1001, 0011, 1100, 10101, \dots\}$

$\Sigma = \{a, b\}$

$L(A) = \{w \mid w$ has an equal number of a's & b's$\}$

No DFA can do this!

Let M be a <u>finite</u> monoid.

Let F be a (finite) subset of M.

Let $h: \Sigma^* \to M$ be a homo.

$L(M, F, h) := \{w \in \Sigma^* \mid h(w) \in F\}$

Thm. A language is regular iff it

<u>Thm</u> A language is regular iff it is recognized by some triple (M, E, h).

<u>Def</u> Given $L \subseteq \Sigma^*$ we define $\equiv_L$ an equivalence relation:

$$x \equiv_L y \text{ if } \forall z \in \Sigma^*$$
$$xz \in L \iff yz \in L$$

<u>FACT</u> $x \equiv_L y$ & $u \equiv_L v$ then
$$xu \equiv_L yv$$
Such a relation is called a <u>congruence</u> <u>relation</u>.

$\Sigma^* / \equiv_L$ is a well-defined monoid.

Regular languages have nice properties that can be investigated by studying this m