

## §1 05-04

### §1.1 Logistics

1. Potentially an oral final exam
2. Too many assignments to grade at the fast pace. Students will self grade their homeworks, and a few will be chosen at random to see if people are being honest in their self evaluation
3. All assignments are to be completed in Latex
4. Fact means he'll say it and not prove it.

### §1.2 Schedule

Lecture Schedule for COMP 598 Summer 2020			
Week 1	Lecture 1	4 May	Induction, strings, automata, monoids
	Lecture 2	5 May	NFA, Kleene theorem, regexp, Kleene algebra
	Lecture 3	6 May	Myhill-Nerode, minimization, duality
	Lecture 4	7 May	Pumping lemma
Week 2	Lecture 1	11 May	Temporal logic
	Lecture 2	12 May	Bisimulation
	Lecture 3	13 May	Learning automata
	Lecture 4	14 May	Weighted automata
Week 3	Lecture 1	18 May	Context-free languages, grammars and parsing
	Lecture 2	19 May	Pumping lemma for CFLs, DCFLs
	Lecture 3	20 May	Models of computation
	Lecture 4	21 May	$\lambda$ -calculus
Week 4	Lecture 1	25 May	Computability, reductions
	Lecture 2	26 May	Logic and unsolvability, arithmetic hierarchy
	Lecture 3	27 May	Fixed-point theory
	Lecture 4	28 May	Godel's and Tarski's theorems

**Definition 1.1** (Equivalence Relation). An equivalence relation  $R$  on a set  $S$  is a set of pairs  $R \subseteq S \times S$  such that (write  $xRy$  for  $(x, y) \in R$ )

1.  $xRx$
2.  $xRy \Rightarrow yRx$
3.  $xRy \wedge yRz \Rightarrow xRz$

**Definition 1.2** (Equivalence Relation).  $[x] := \{y | xRy\}$  is the equivalence class of  $x$ . The set of equivalence classes forms a partition of  $S$ . Prove this as an exercise.

**Definition 1.3** (Partial Order). Abstraction of comparison. Not all elements can be compared. A binary relation on a set  $S$ . Big difference is no symmetry.

1.  $x \leq x$
2.  $x \leq y \wedge y \leq x \Rightarrow x = y$

$$3. x \leq y \wedge y \leq z \Rightarrow x \leq z$$

Example of taking subsets and ordering them by inclusion. This is a typical partial ordering that is not total. The real numbers are a total ordering.

**Definition 1.4** (Well-founded order). Given a p.o.set (partially ordered set)  $(S, \leq)$  and  $U \subseteq S$ , we say that  $u \in U$  is a minimal element of  $U$  if  $\forall v < u, v \notin U$ . There can be infinitely many minimal elements, or none.

### Example 1.5

Negative integers has no minimal element

Non negative integers in which 0 is the smallest

Strictly positive rational numbers has no minimal element

A partially ordered set  $(S, \leq)$  is said to be well-founded if every non-empty subset  $U$  has (powerful word, an existential qualifier) a minimal element.

### Example 1.6

Examples - Non-negative integers These are well founded. - The positive rational numbers These are not well founded - Pairs  $N \times N$  where  $(m, n) \leq (m', n')$  if  $m < m' \vee (m = m' \wedge n \leq n')$ . Between (1, 17) and (2, 5) there are infinitely many elements, but do not be fooled there is still a minimal element.

**Fact 1.7.** An order is well founded if and only if there are no infinite strictly decreasing sequences (chain)  $x_1 > x_2 > x_3 > \dots$ .

An order that is both totally ordered and well-founded is called a well order.

### Theorem 1.8 (Zermelo's Theorem)

Every set can be given a well order assuming the axiom of choice. People don't want to believe this because no one can figure out how to write a well ordering of the real numbers.

**Note 1.9.** Zermelo's well ordering principle, axiom of choice, and zorn's lemma are equivalent. Zorn's lemma is something people don't want to give up.

## §1.3 Principle of Induction

**Definition 1.10** (Predicate). "predicate". you're in the set if you satisfy property of predicate. "predicate is a statement that may be true or false depending on the values of its variables". "The set defined by  $P(x)$  is written as  $x \text{ --- } P(x)$ , and is the set of objects for which  $P$  is true."

$(S, \leq)$  is inductive if  $\forall P, \forall x \in S, \forall y < x, P(y) \Rightarrow P(x)$

Not every order is inductive. Minimal element takes care of the base case. Which orders are inductive, and which are not?

**Theorem 1.11**

An order is inductive if and only if it is well founded.

*Proof.*

1. Assume  $V := \{s \in S \mid \neg P(s)\}$  is not empty. Which would contradict the principle of induction. Then  $\forall y < v_0, y \notin V$  and  $P(y)$ . But then this implies  $P(v_0)$ . So then  $V = \emptyset$ . i.e.  $\forall x P(x)$ .
2. Ind  $\Rightarrow$  Well founded. Assume  $U \subseteq S$  has no minimal element.  $P(x) := x \notin U$ .  $\forall x (\forall y < x P(y)) \Rightarrow P(x)$ . We know this because if all  $y$  is less than  $x$ , and  $y \notin U$  by the predicate, then  $x \notin U$  or else it would be a minimal element of  $U$ .

Induction says that  $\forall x P(x) \Rightarrow U = \emptyset$  and hence  $(S, \leq)$  is well founded because all sets have a minimal element. □

\*\* Emmy Noether  $\Sigma = \{a, b\}. \Sigma^* = \{\epsilon, a, b, aa, ab, \dots\}$

Under lexicographic ordering this is not well founded.

**§1.4 Strings**

A finite set is called an alphabet.  $\Sigma^*$  is a set of finite sequences. The number of such sequences is infinite.  $\epsilon$  is the symbol for the empty word. A subset of the set of sequences is called a language.

**Definition 1.12** (monoid). A monoid is a set  $S$  with a binary operation  $\cdot$  and a unit  $e$ .

1.  $\forall x, y, z \in S, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2.  $\forall x \in S, x \cdot e = e \cdot x = x$
3. Monoids are not necessarily commutative. If we have that  $\forall x, y, x \cdot y = y \cdot x$  then we get a special kind of monoid called a commutative monoid.
4. If there is an inverse operation, it is a group. Monoid's are a general form of group.

**Example 1.13**

1.  $\Sigma^*$  with concatenation and  $\epsilon$  is a monoid, but it is not commutative.  $aab \cdot ba = aabba$ .
2.  $\forall x, y, z$  if  $xy = xz \Rightarrow y = z$  is a cancellative monoid.