Notes: The lecture notes reference [L1s12] means Lecture 1 Slide 12.

Syntax and Trees

Definition 1 (Abstract Syntax Tree). *An* **abstract syntax tree** *is a concise tree representation of a linear notation.* [L1s4]

The process of converting a linear notation to a syntax tree is called **parsing**. *Parsing depends on the "relative stickness" of operators, called* **precedence**. [L1s12-13]

Definition 2 (Assignment). *The values of the variables can be captured in an* **assignment**, *which is a table that maps each variable to a value. An assignment that makes a logical formula true is called a* **satisfying assignment** *of that formula.* [L1s18]

Definition 3 (Recursive Definition of Arithmetic Expressions). *If α and β are arithmetic expressions, then the following are all arithmetic expressions:*

- *A number*
- *A variable name;*
- $-\alpha$
- $\alpha + \beta$
- $\alpha - \beta$
- $\alpha * \beta$
- α / β
- α^β

[L1s22]

Propositional Logic

Definition 4 (Propositional Connectives). *In propositional logic, the* **truth values** *are T for "true" and F for "false". The operators are* **propositional connectives**, *such as $\neg$ for "NOT", $\wedge$ for "AND" and $\vee$ for "OR".* [L2s5]

Definition 5 (Recursive Definition of Propositional Logic Formula). *If α and β are propositional logic formulas, the following are all propositional logic formulas:*

- *One of the truth values T or F*
- *A variable (typically P, Q)*
- $\neg\alpha$
- $\alpha \wedge \beta$
- $\alpha \vee \beta$

The order of precedence of the connectives is: $\neg$, $\wedge$, $\vee$. [L2s6,7]

The assignment of truth values to variables in a propositional logic formula is called a **truth assignment**. [L2s9]

Definition 6 (Satisfiability of Propositional Formulas). **The satisfiability problem (or "SAT")** *is, given a propositional formula* t*, does there exist a satisfying truth assignment* a*.* [L2s10]

Definition 7 (Truth Table). **Truth tables** *enumerate values of a propositional logical formula for all of the possible values of the propositional variables appearing in it.* [L2s11]

Definition 8 (Tautology). *A* **tautology** *is a propositional formula that is always true. I.e., the entire column for the sentence in the truth table is "T".* [L2s15]

Theorem 1 (Propositional Connective Laws). [L2s17-18]

Identity	*Name*
$\neg\neg P \equiv P$	*double negation*
$P \wedge T \equiv P$ $P \vee F \equiv P$	*identity*
$P \wedge F \equiv F$ $P \vee T \equiv T$	*domination*
$P \wedge \neg P \equiv F$ $P \vee \neg P \equiv T$	*inverse laws*
$P \wedge P \equiv P$ $P \vee P \equiv P$	*idempotence*
$P \wedge Q \equiv Q \wedge P$ $P \vee Q \equiv Q \vee P$	*commutativity*
$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$ $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$	*associativity*
$(P \vee Q) \wedge R \equiv (P \wedge R) \vee (Q \wedge R)$ $(P \wedge Q) \vee R \equiv (P \vee R) \wedge (Q \vee R)$	*distributivity*
$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$	*De Morgan's laws*

Theorem 2 (Duality). *If you swap $\wedge$ and $\vee$ and T and F in an identity, you get another identity.* [L2s18]

Definition 9 (Implication). $P \to Q \equiv \neg P \vee Q$. [L2s19]

Given an implication $P \to Q$, there are several related implications:

implication	name
$Q \to P$	converse
$\neg P \to \neg Q$	inverse
$\neg Q \to \neg P$	contrapositive

Important equivalence identities:

identity	note
$P \to Q \equiv \neg Q \to \neg P$	(statement $\equiv$ contrapositive)
$Q \to P \equiv \neg P \to \neg Q$	(converse $\equiv$ inverse)

[L2s25]

Definition 10 (Biconditionals). $P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$.

$P \leftrightarrow Q$ is true exactly when P and Q have the same truth value. In English, biconditionals are indicated by "P if and only if Q", "P iff Q.", "P is necessary and sufficient for Q" etc. [L2s26]

Theorem 3. *$P \leftrightarrow Q$ is satisfiable.* [L3s6]

Theorem 4 (Distributive Law of Implications).

$P_1 \to (P_2 \wedge P_3) \equiv (P_1 \to P_2) \wedge (P_1 \to P_3)$ [L3s5]

Theorem 5 (Tautology and Satisfiability). *ϕ is tautology iff its truth table has all T's iff the truth table for $\neg\phi$ has all F's.*
In other words, $P \leftrightarrow P$ is a tautology, and $\neg(P \leftrightarrow P)$ is unsatisfiable. [L3s7]

First-Order Logic

Definition 11 (First Order Logic). *First-order logic is usually defined with two levels of syntax (two types of trees):* **terms***, which represent individuals (e.g., non-boolean values), and* **formulas***, which represent properties or relationships (e.g. boolean expressions.)* [L3s10]

Definition 12 (Predicates). ***Predicates*** *are boolean (true/false) functions that have terms as arguments. They can be written using normal functional notation, e.g.,* $P(x, y)$*, or using* **infix** *(e.g.,* $1 + 2$*),* **prefix** *(e.g.,* -1*), and* **postfix** *operators (e.g.,* $3!$*).* [L3s12]

Definition 13 (Quantifiers). *First order logic has two quantifiers: the* **universal quantifier** $\forall$ *("every") and the* **existential quantifier** $\exists$ *("exists").*

Note that quantifiers go with **variables***, which are terms that represent non-Boolean values. (e.g., "*$\forall x$*").* [L3s13]

Theorem 6. $\forall$ *is "AND over everything",* $\exists$ *is "OR over everything."* [L3s15]

For *finite sets*, quantified expressions can be rewritten by substituting all possible values for the quantified variables and ANDing or ORing the results together (depending on whether the quantifier is $\forall$ or $\exists$).

E.g., if we're quantifying over the integers in the range $0 \ldots 2$

$\forall x\ \mathsf{P}(x) = \mathsf{P}(0) \wedge \mathsf{P}(1) \wedge \mathsf{P}(2)$ $\qquad$ $\exists x\ \mathsf{P}(x) = \mathsf{P}(0) \vee \mathsf{P}(1) \vee \mathsf{P}(2)$

Definition 14 (Recursive Definition of Terms). *Let* γ_1*,* γ_2*, ... be terms. A term can be any of the following:*

- *A variable, e.g.,* x*.*
- *A function application:* $f(\gamma_1, \gamma_2, \ldots, \gamma_n)$*.*
- *A constant, e.g.* 0*.*

[L3s16]

Definition 15 (Recursive Definition of Formulas). *Let* α*,* β*, ... be formulas and* γ_1*,* γ_2*, ... be terms. A formula can be:*

- *One of the truth values T or F.*
- *A predicate, e.g.,* $\gamma_1 \leq \gamma_2$*,* $\gamma_1 = \gamma_2$*.*
- *Quantified formulas:* $\forall x\ (\alpha)$ *and* $\exists x\ (\alpha)$

[L3s17]

Definition 16 (Restricted Quantifiers). *Quantifiers that apply to individuals with a particular property are* **restricted quantifiers** *(also known as* **Aristotelian forms***):*

"All P's are Q's"	$\forall x\ (P(x) \rightarrow Q(x))$
"Some P's are Q's"	$\exists x\ (P(x) \wedge Q(x))$

Note that $\exists x\ (P(x) \rightarrow Q(x))$ *is incorrect.* [L3s19]

Definition 17 (Vacious Truth Sentences). *$\forall x\ (P(x) \to Q(x))$ is true if $P(x)$ is never true. When this occurs, the sentence is said to be* **vacuously true**. [L3s23]

Theorem 7. *Swapping two adjacent quantifiers of the same kind does not change the meaning of the sentence:*

$$\begin{array}{lcl} \forall x \forall y\ (R(x,y)) & \equiv & \forall y \forall x\ (R(x,y)) \\ \exists x \exists y\ (R(x,y)) & \equiv & \exists y \exists x\ (R(x,y)) \end{array}$$ [L3s25]

Theorem 8 (Precedence of Logic Connectives). *The precedence order of logical connectives is $\forall x$ and $\exists x$ and $\neg$ (all equal precedence), $\wedge$, $\vee$, $\to$, $\leftrightarrow$.*

$\to$ is right-associative, so $P \to Q \to R$ is $P \to (Q \to R)$. All the other connectives are left-associative. [L4s6]

Theorem 9 (DeMorgan's Laws for Quantifiers). [L4s16]

$$\begin{array}{lcl} \neg\forall x\ P(x) & \equiv & \exists x\ \neg P(x) \\ \neg\exists x\ P(x) & \equiv & \forall x\ \neg P(x) \end{array}$$

Theorem 10 (DeMorgan's Laws for Restricted Quantifiers). [L4s18]

$$\begin{array}{lcl} \neg\forall x\ (P(x) \to Q(x)) & \equiv & \exists x\ (P(x) \wedge \neg Q(x)) \\ \neg\exists x\ (P(x) \wedge Q(x)) & \equiv & \forall x\ (P(x) \to \neg Q(x)) \end{array}$$

Definition 18 (Free and Bound Variables). *ν is a* **bound variable** *in $\forall\nu\ P$ and $\exists\nu\ P$. A* **free variable** *is an unbound variable (i.e., it is not acted upon by a quantifier).* [L4s19]

Theorem 11 (Distributive Laws for Quantifiers). *These laws always work*

$$\begin{array}{lcl} \forall x\ (P(x) \wedge Q(x)) & \equiv & (\forall x\ P(x)) \wedge (\forall x\ Q(x)) \\ \exists x\ (P(x) \vee Q(x)) & \equiv & (\exists x\ P(x)) \vee (\exists x\ Q(x)) \end{array}$$

In general, $\forall$ does not *distribute over $\vee$ and $\exists$ does* not *distribute over $\wedge$. But, if x* does not occur free in P,

$$\begin{array}{lcl} \forall x\ (P \vee Q(x)) & \equiv & P \vee (\forall x\ Q(x)) \\ \exists x\ (P \wedge Q(x)) & \equiv & P \wedge (\exists x\ Q(x)) \end{array}$$ [L4s20]

Theorem 12 (Substitution Property). *Let β and γ be terms. Let $\alpha[\beta]$ be a term in which β appears, and let $\alpha[\gamma]$ be the term where β is replaced by γ.*

If $\beta = \gamma$, then $\alpha[\beta] = \alpha[\gamma]$. [L4s22]

Theorem 13 (Equality properties). *Other properties of equality besides substitution:*

- **reflexivity:** $\forall x\ (x = x)$
- **symmetry:** $\forall x, y\ (x = y \rightarrow y = x)$
- **transitivity:** $\forall x, y, z\ (x = y \wedge y = z \rightarrow x = z)$.

The quantifiers is often omitted with the mathematical convention of **implicit quantification**. [L4s24]

Proofs

Definition 19 (Big-Oh). *If f and g are two functions from real numbers to real numbers, we say $f(n)$ is $O(g(n))$ if*

$\exists c\ \exists n_0\ \forall n(n > n_0 \rightarrow 0 \leq f(n) \leq cg(n))$ [L5s7]

Definition 20 (Proof). *A* **proof** *is a demonstration of a theorem which is a mathematical truth (***axiom***). A proof begins with a set of initial assumptions that are explicitly stated (***premises***) or implicitly assumed as a known truth. A series of* **conclusions** *are drawn from these assumptions and previous conclusions. The theorem is the last of these conclusions.* [L5s9,11]

A **formal proof** *is a proof that is performed using a mathematically precise logical language and rules of inference.* [L5s10]

Definition 21 (Even and Odd). [L5s16]

$Even(n) : \exists k\ (n = 2k)$
$Odd(n) : \exists k\ (n = 2k + 1)$

Theorem 14 (Properties of Even and Odd Integers).

- *Every integer is either even or odd.* [L5s16]
- *No integer is both even and odd.* [L6s23]
- *If n is odd, then n^2 is odd: $\forall n\ (Odd(n) \rightarrow Odd(n^2))$* [L5s28]
- *$n^3 + n$ is even, for every integer n.* [L5s31]
- *n is even iff n^2 is even for every integer n: $\forall n\ (Even(n^2) \leftrightarrow Even(n))$* [L6s11]

Definition 22 (Rational Numbers). *Every* **rational number** *can be written in the form p/q where:*

- *p and q are integers.*
- *$q \neq 0$.*
- *The only positive integer that evenly divides p and q is 1.*

[L6s25]

Theorem 15. *Between every two distinct rational numbers, there is another rational number.* [L5s33]

Theorem 16 (Irrationality of $\sqrt{2}$). $\sqrt{2}$ *is irrational.* [L6s26]

Sets

Definition 23 (Sets). *A* **set** *is an unordered collection of distinct objects. The* **empty set***, written* $\emptyset$*, is the set that contains no objects.* [L7s8]

Sets can be finite or infinite. Common infinite sets:

- The **natural numbers,** $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- The **integers,** $\mathbb{Z} = \{\ldots - 2, -1, 0, 1, 2, \ldots\}$.
- The **rational numbers,** $\mathbb{Q} = \{p/q \mid \text{where } p \text{ and } q \text{ are integers and } q \neq 0\}$
- The **reals,** $\mathbb{R}$ (rationals, plus π, e, $\sqrt{2}$, etc.)

[L7s10]

Definition 24 (Set Membership). *We denote the predicate of whether an object is a* **member** *of a set as* $x \in S$*. (pronounced: "x is a member of S" or "x is in S")*

The notation $x \notin S$ *is an abbreviation for* $\neg(x \in S)$*.* [L7s11]

Definition 25 (Set Equality). *Another predicate on sets is* $=$*.* $S_1 = S_2$ *if both sets have exactly the same members, regardless of order and repetition.* [L7s13]

Theorem 17 (Axiom of Extensionality). $\forall S_1, S_2, x\ ((x \in S_1 \leftrightarrow x \in S_2) \rightarrow S_1 = S_2)$ [L7s14]

Definition 26 (Subset). A *is a* **subset** *of* B *if every member of* A *is also a member of* B*. If* A *is a subset of* B *then* B *is a* **superset** *of* A *(*$B \supseteq A$*.* [L7s15]

A *is a* **proper subset** *of* B *(*$A \subset B$ *or* $A \subsetneq B$*) if it is a subset but* $A \neq B$*.* [L7s16]

Theorem 18. *The empty set is a subset of every other set.* [L7s17]

Theorem 19. $S_1 = S_2$ *iff* $S_1 \subseteq S_2$ *and* $S_2 \subseteq S_1$*.* [L7s18]

Theorem 20. *There is at most one empty set.* [L7s18]

Theorem 21 (Russell's Paradox). *Let R be the set of all sets that do not contain themselves, i.e. $R = \{S \mid S \notin S\}$. The set R does not exist.* [L7s22]

Definition 27 (Set Intersection). *$A \cap B$ (set intersection) is the set of all values that are in both A and B, i.e. $A \cap B = \{x \mid x \in A \land x \in B\}$.* [L7s26-28]

Theorem 22 (Properties of Intersection). [L7s29]

- $\emptyset \cap A = \emptyset$
- $A \cap A = A$ *(idempotency)*
- $A \cap B = B \cap A$ *(commutativity)*
- $(A \cap B) \cap C = A \cap (B \cap C)$ *(associativity)*
- $A \cap B = B$ *iff* $B \subseteq A$

Definition 28 (Set Union). *$A \cup B$ is the set of all values that are in A or in B.* [L7s30]

Theorem 23 (Properties of Union). [L7s31]

- $\emptyset \cup A = A$
- $A \cup A = A$ *(idempotency)*
- $A \cup B = B \cup A$ *(commutativity)*
- $(A \cup B) \cup C = A \cup (B \cup C)$ *(associativity)*
- $A \cup B = B$ *iff* $A \subseteq B$

Theorem 24 (Distributive Laws of Union and Intersection). [L7s32]

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \end{aligned}$$

Definition 29 (Set Difference). *$A - B$ is the set of values in A that are not in B. Alternate notation: $A \backslash B$.* [L7s34]

Definition 30 (Cardinality). *The number of members of a set S is its* **cardinality**, *written as $|S|$.* [L7s39]

Theorem 25. *If $A \subseteq B$, then $|A| \leq |B|$.* [L7s38]

Definition 31 (Powerset). *The* **powerset** *of a set A is the set of all subsets of A, $\mathscr{P}(A) = \{B \mid B \subseteq A\}$. $\mathscr{P}(A)$ is also written 2^A.* [L7s42]

Definition 32 (Set of Sets). *Let $\mathcal{C}$ be a set of sets. Then*

$\bigcap \mathcal{C}$ is the set of all values that are in every set $S \in \mathcal{C}$

$\bigcup \mathcal{C}$ is the set of all values that is in some set $S \in \mathcal{C}$. [L7s43]

Relations

Definition 33 (Tuples). *A* **tuple** *is an ordered list of values.* [L8s7]

Definition 34 (Cartesian Product). *The* **Cartesian product** *of sets A and B is the set of all pairs where the first element is from A and the second element from B: $A \times B = \{(x, y) \mid x \in A \land y \in B\}$.* [L8s8]

Definition 35 (Binary Relations). *If A and B are sets, a* **binary relation** R **from** A **to** B *is a subset of $A \times B$. A is the* **domain** *of the relation and B is the* **codomain***.* [L8s10]

Any set of pairs from two sets is a relation. $\emptyset$ is the minimum possible relation from A to B. $A \times B$ is the maximum possible relation from A to B. [L8s11]

If R is a relation from A to B and $(x, y) \in R$, we say "x is related to y by R." The standard notation for this is is: $x \; R \; y$. [L8s12]

Definition 36 (Set Operations on Relations). *Suppose R and S are relations from A to B. We define $\overline{R}$ to be $(A \times B) - R$ for these examples.*

$R \cap S$ is a relation from A to B.
$R \cup S$ is a relation from A to B. [L8s16]

Definition 37 (Endorelations). *An* **endorelation** *is a relation whose domain and codomain are the same. If R is a relation with domain and codomain A, we can say R* **is a relation on** *A.* [L8s17]

Example endorelations: [L8s17-20]

- $=, <, \leq, >, \geq$ on $\mathbb{R}$ (or $\mathbb{N}$, $\mathbb{Z}$, or $\mathbb{Q}$).
- Any set of pairs from the same set.
- Relation on $\mathbb{R}$: $\{(x, y) \mid x = y\}$ (equality)
- Relation on $\mathbb{R}$: $\{(x, y) \mid x^2 + y^2 = 1\}$ (unit circle)

Definition 38 (Properties on Endorelations).

Let R be an endorelation on A.

- *R is* **reflexive** *if* $\forall x \in A \; (x \; R \; x)$
- *R is* **symmetric** *if* $\forall x, y \in A \; (x \; R \; y \rightarrow y \; R \; x)$
- *R is* **transitive** *if* $\forall x, y, z \in A \; (x \; R \; y \land y \; R \; z \rightarrow x \; R \; z)$.

[L8s23-27]

Definition 39 (Directed Graph). *A* **directed graph** *(* **digraph** *for short) is an endorelation E on a set V. V is called the set of* **vertices** *(also called* **nodes***). E is called the set of* **directed edges** *(also called* **arcs***).* [L8s22]

Definition 40 (Equivalence Relation). *An endorelation R is an* **equivalence relation** *if it is* **reflexive***,* **symmetric***, and* **transitive***.* [L8s29]

Definition 41 (Partitions). *An equivalence relation on A is a* **partition** *of A. A partition of a set A is a set of sets $\{A_i\}$, where each $A_i \subseteq A$ and*

- $A_i \cap A_j = \emptyset$ *if $i \neq j$ (the sets are* **mutually exclusive***).*
- $\bigcup\{A_i\} = A$ *(the sets are* **collectively exhaustive***).*

[L8s30]

Theorem 26. $\|$ *is an equivalence relation on lines.* [L8s32]

Definition 42 (Congruence Relations). *A* **congruence relation** *(or just* **congruence***) is an equivalence relation that has a limited form of the substitutability for a defined set of operations.* [L8s34]