CSE 311 Notes

Contents

1 Inference Rules

1.1 Eliminate $\wedge$

$$\frac{A \wedge B}{\therefore A, B}$$

1.2 Eliminate $\vee$

$$\frac{A \vee B, \neg A}{\therefore B}$$

1.3 Introduce $\wedge$

$$\frac{A; B}{\therefore A \wedge B}$$

1.4 Introduce $\vee$

$$\frac{A}{\therefore A \vee B}$$

1.5 Direct Proof

$$\frac{A \Rightarrow B}{\therefore A \Rightarrow B}$$

Assuming A, show that $A \Rightarrow B$ is true

1.6 Modus Ponens

$$\frac{p \Rightarrow q,\ p}{\therefore q}$$

1.7 Introduce $\exists$

$$\frac{P(c)\ for\ some\ c}{\therefore \exists x\ P(x)}$$

1.8 Introduce $\forall$

$$\frac{P(c)\ for\ any\ arbitrary\ c}{\therefore \forall x\ P(x)}$$

1.9 Eliminate $\exists$

$$\frac{\exists x\ P(x)}{\therefore P(c)\ for\ some\ specific\ c}$$

1.10 Eliminate $\forall$

$$\frac{\forall x\ P(x)}{\therefore P(c)\ for\ any\ c}$$

2 Elementary Equivalences

2.1 Identity

$Q \wedge T \equiv Q$

$Q \vee F \equiv Q$

2.2 Domination

$Q \vee T \equiv T$

$Q \wedge F \equiv F$

2.3 Idempotent

$Q \vee Q \equiv Q$

$Q \wedge Q \equiv Q$

2.4 Commutative

$Q \vee R \equiv R \vee Q$

$Q \wedge R \equiv R \wedge Q$

2.5 De Morgan's Laws

$\neg(Q \wedge R) \equiv \neg Q \vee \neg R$

$\neg(Q \vee R) \equiv \neg Q \wedge \neg R$

2.6 Inverse De Morgan's Laws

$Q \vee R \equiv \neg(\neg Q \wedge \neg R)$

$Q \wedge R \equiv \neg(\neg Q \vee \neg R)$

2.7 Associative

$(Q \vee R) \vee S \equiv Q \vee (R \vee S)$

$(Q \wedge R) \wedge S \equiv Q \wedge (R \wedge S)$

2.8 Distributive

$Q \wedge (R \vee S) \equiv (Q \wedge R) \vee (Q \wedge S)$

$Q \vee (R \wedge S) \equiv (Q \vee R) \wedge (Q \vee S)$

2.9 Absorption

$Q \vee (Q \wedge R) \equiv Q$

$Q \wedge (Q \vee R) \equiv Q$

2.10 Negation

$Q \vee \neg Q \equiv T$

$Q \wedge \neg Q \equiv F$

2.11 Double Negation

$\neg(\neg Q) \equiv Q$

2.12 Law of Implication

$Q \Rightarrow R \equiv \neg Q \vee R$

2.13 Law of Biconditional

$Q \Leftrightarrow R \equiv (Q \Rightarrow R) \wedge (R \Rightarrow Q)$

3 Set Theory

3.1 Sets

A set is a collection of distinct objects, such as $\{1, 2, 3\}$ and $\varnothing$

- A set has no repeated elements
- $\{1\}$ is distinct from $\{\{1\}\}$
  - 1 is an element of $\{1\}$ but not of $\{\{1\}\}$

3.2 Null Set

The null set $\varnothing$ is the set containing nothing, equivalent to $\{\}$

- The null set is a subset of every set
- The null set is not necessarily an element of a set
- $\varnothing$ is distinct from $\{\varnothing\}$

3.3 Subsets

A set A is a subset of a set B, $A \subseteq B$, if all elements of A are also elements of B

- $A \subseteq B$ if $\forall x,\ x \in A \Rightarrow x \in B$

3.4 Equivalent Sets

A set A is equivalent to B, $A = B$, if all elements of A are also elements of B and vice-versa

- $A = B$ if $\forall x,\ x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in A$

3.5 Complementary Sets

The complement of a set A^c or $\overline{A}$ is the set of all elements not in A

3.6 Symmetric Difference

The symmetric difference of two sets A and B, $A \oplus B$, is the set of elements which are in either set but not in both

- $A \oplus B = \{x \mid x \in A \oplus x \in B\}$

3.7 Meta Theorem

Any relationship between sets defined by $\cup, \cap, -^C$ can be translated into a propositional logic defined by $\vee, \wedge, \neg$

3.8 Power Set

The power set of a set A is the set of all subsets of A, including the empty set and A itself

- $P(A) = \{S \mid S \subseteq A\}$
- $P(\varnothing) = \{\varnothing\}$
- $P(\{x, y\}) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$

Power set manipulation

- $\{x, y\} \in P(A) \;\equiv\; x, y \in A$
- $\{x, y\} \in P(A) \;\equiv\; \{x, y\} \subseteq A$

3.9 Cartesian Product

The Cartesian product of two sets A and B is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

- The Cartesian product is not commutative, $(a, b) \neq (b, a)$

3.10 Bit Representation of Sets

Given $U = u_1, u_2, ..., u_n$, the bit representation of the set $B \subseteq U$ is a string of bits where the i-th bit is 1 if $u_i \in B$ and 0 if $u_i \notin B$

- $U = \{1, 2, 3, 4, 5\}$
- $B = \{2, 4\}$
- $B \subseteq U = 0\ 1\ 0\ 1\ 0$

The bit string (i.e. $0\ 1\ 0\ 1\ 0$) is also known as the characteristic vector of set B

3.11 Recursively Defined Sets

Each element in a set is defined by its preceding elements. Recursive definitions are comprised of:

- Basis step: Some specific element in S
- Recursive step: Given some existing named elements in S, some new object constructed from these elements is also in S

3.12 String Sets

- An alphabet Σ is any finite set of characters
- The set Σ^* of strings over the alphabet Σ is defined by
  - Basis step: $\varepsilon \in \Sigma$, where ε is the empty string
  - Recursive step: if $w \in \Sigma^*$ and $a \in \Sigma$, then $wa \in \Sigma^*$

4 Arithmetic Operations

4.1 Divisibility

a divides b

For $a \in \mathbb{Z},\ b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \Leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$$

4.2 Division Theorem

a divided by b

For $a \in \mathbb{Z},\ d \in \mathbb{Z}$ with $d > 0$:

There exists unique integers q, r with $0 \leq r < d$ such that $a = dq + r$

4.3 Modular Arithmetics

a is congruent to b modulo m

For $a, b, m \in \mathbb{Z}$ with $m > 0$:

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b)$$

Let $a, b, m \in \mathbb{Z}$ with $m > 0$:

$$a \equiv b \pmod{m} \Leftrightarrow a \,\%\, m = b \,\%\, m$$

Let m be a positive integer

$$a \equiv b \pmod{m}\ \wedge\ c \equiv d \pmod{m} \Rightarrow (a + c) \equiv (b + d) \pmod{m}$$

Let m be a positive integer

$$a \equiv b \pmod{m}\ \wedge\ c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$$

4.4 Euclidean Algorithm

$$\gcd(a, b) = \gcd(b, a \,\%\, b)$$
$$\gcd(a, 0) = a$$

Example:

$$\begin{aligned}
\gcd(660, 126) &= \gcd(126, 660 \,\%\, 126) &&= \gcd(126, 30) \\
&= \gcd(30, 126 \,\%\, 30) &&= \gcd(30, 6) \\
&= \gcd(6, 30 \,\%\, 6) &&= \gcd(6, 0) \\
&= 6
\end{aligned}$$

$$\begin{array}{llll}
660 & = & 5 & * \quad 126 + 30 \\
126 & = & 4 & * \quad 30 + 6 \\
30 & = & 5 & * \quad 6 + 0
\end{array}$$

4.5 Bézout's Theorem

If a and b are positive integers:

Then there exists integers u and v such that $\gcd(a, b) = ua + vb$

Example (continuing 4.4):

$126 = 4 * 30 + 6$

$6 = 126 - 4 * 30$

$660 = 5 * 126 + 30$

$30 = 660 - 5 * 126$

$6 = 126 - 4 * (660 - 5 * 126)$

$6 = 126 - 4 * 660 + 20 * 126$

$6 = 21 * 126 - 4 * 660$

4.6 Modular Inverse

For a, b that satisfies $\gcd(a, b) = ua + vb = 1$, the modular inverse of $a \pmod b$ is $u \,\%\, b$, where $ua = 1 \pmod b$

4.7 Fast Modular Exponentiation

If $a \,\%\, m \equiv a \pmod m$ and $b \,\%\, m \equiv b \pmod m$ then $ab \,\%\, m = ((a \,\%\, m)(b \,\%\, m)) \,\%\, m$

- $a^{2n} \,\%\, m = (a^n \,\%\, m)^2 \,\%\, m$
- $a^{2n+r} \,\%\, m = ((a^{2n} \,\%\, m)(a^r \,\%\, m)) \,\%\, m$

5 Languages

5.1 Language

A language is a set of strings that satisfies special syntactic properties

5.2 Regex

A regular expression is a sequence of characters that specifies a search pattern used to parse strings

Operators:

- ^...$ start/end of string
- [abc] only *a* or *b* or *c*
- [^abc] not *a* nor *b* nor *c*
- [a-z] characters *a* to *z*
- [0-9] numbers *0* to *9*
- ab *a* followed by *b*
- (a|b) only *a* or *b*
- a* zero or more repetitions of *a*
- a+ one or more repetitions of *a*
- a? optional inclusion of *a*

5.3 Context-Free Grammars

A Context-Free Grammar (CFG) is a language defined by a finite set of substitution rules involving:

- A start symbol S
- A finite set V of variables that can be replaced
- An alphabet Σ of terminal symbols

Rules that define a variable A are written as $A \rightarrow w_1 \mid w_2 \mid ... \mid w_k$, where w_i is a string of variables or terminals

5.4 Relations

A relation R from set A to set B is a subset of $A \times B$

- If $(a, b) \in R$, where R is a relation from some set A to some set B, we can write $a\ R\ b$
- A relation R on a set A is a subset of $A \times A$

5.5 Equivalence Relations

An equivalence relation is a relation that has the properties

- Reflexive: $\forall a \in A,\ a\ R\ a$
- Symmetric: $\forall a, b \in A,\ a\ R\ b \Leftrightarrow b\ R\ a$
- Antisymmetric: $\forall a, b \in A,\ a\ R\ b \Leftrightarrow \neg(b\ R\ a)$
- Transitive: $\forall a, b, c \in A,\ (a\ R\ b \wedge b\ R\ C) \Rightarrow a\ R\ c$

5.6 Composition Relations

Let R be a relation from A to B
Let S be a relation from B to C

The composition of R and S, denoted $R \circ S$ is the relation from A to C defined by
$R \circ S = \{(a, c) \mid \exists b \text{ such that } (a, b) \in R \wedge (b, c) \in S\}$

5.7 Finite Automata

A finite automata is a language defined by a directed graph. It consists of:

- States, represented as nodes
  - Has a start state, accepting state (final state) and rejecting state (non-final state)
- Transitions on input symbols, represented as edges
- Recognized languages, represented as paths

5.8 Deterministic Finite Automata

- There is only one state transition for each symbol in the alphabet
- The next possible state is distinctly set
- There is no ambiguity in which state transition is next
- Subset of NFAs

5.9 Nondeterministic Finite Automata

- There can be multiple state transitions for each symbol in the alphabet
- There can be many next possible states
- There may be ambiguity in which state transition is next
- Superset of DFAs