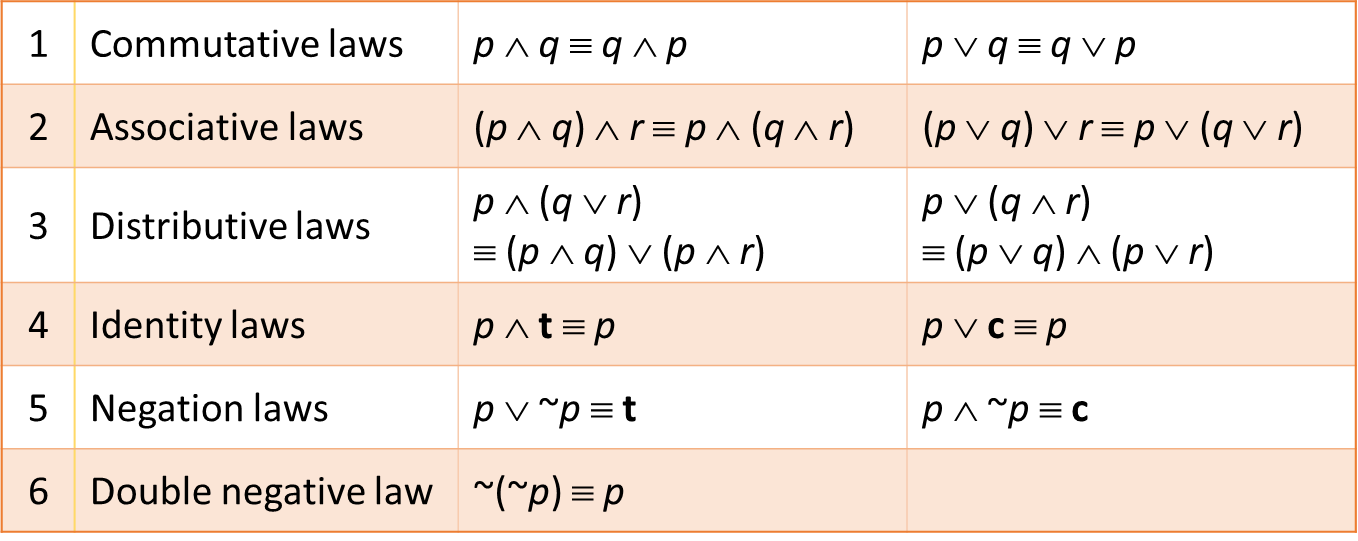
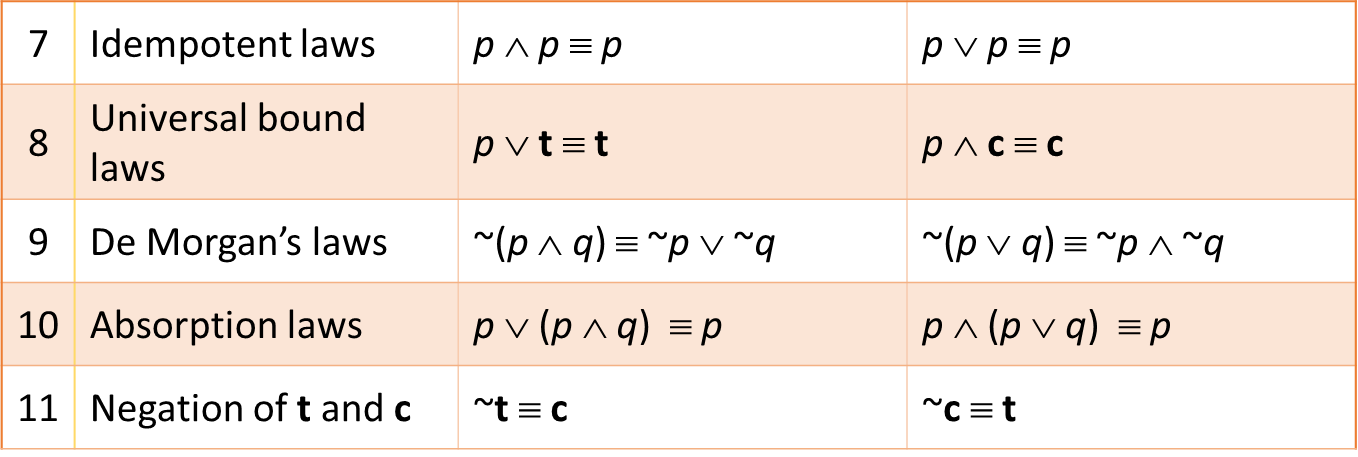
CS1231

Proof Techniques:

Direct, Contrapositive, Induction & Strong Induction, Contradiction

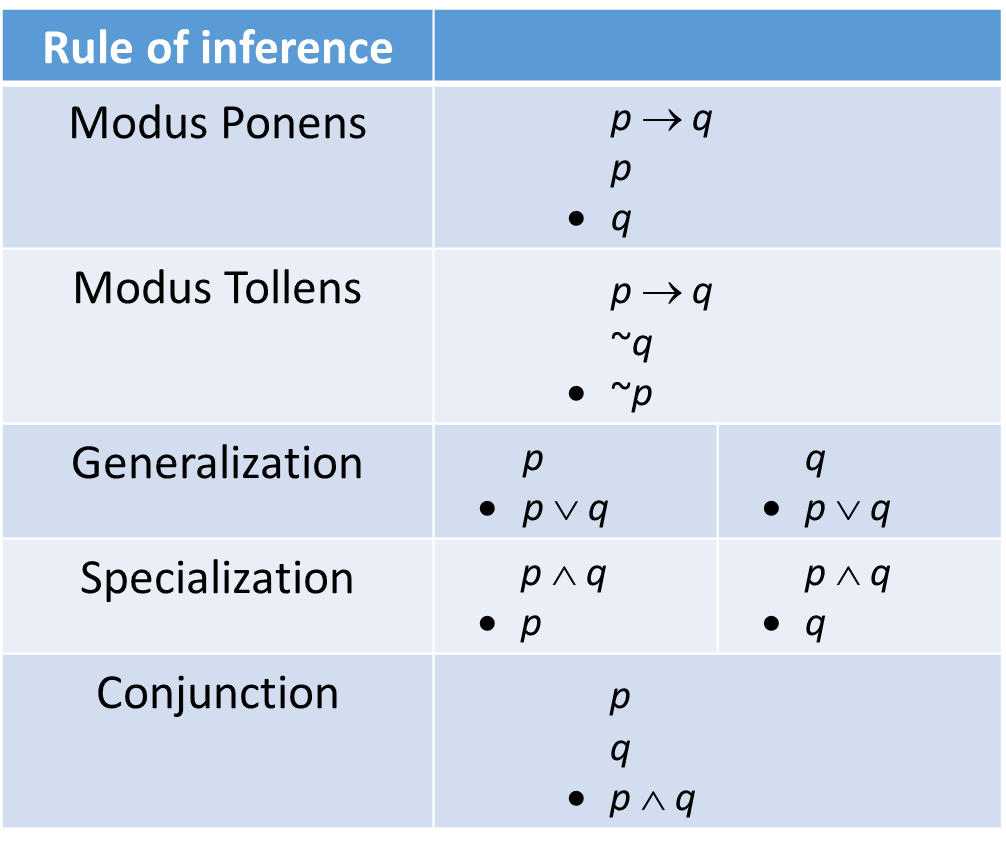
Propositional Logic:

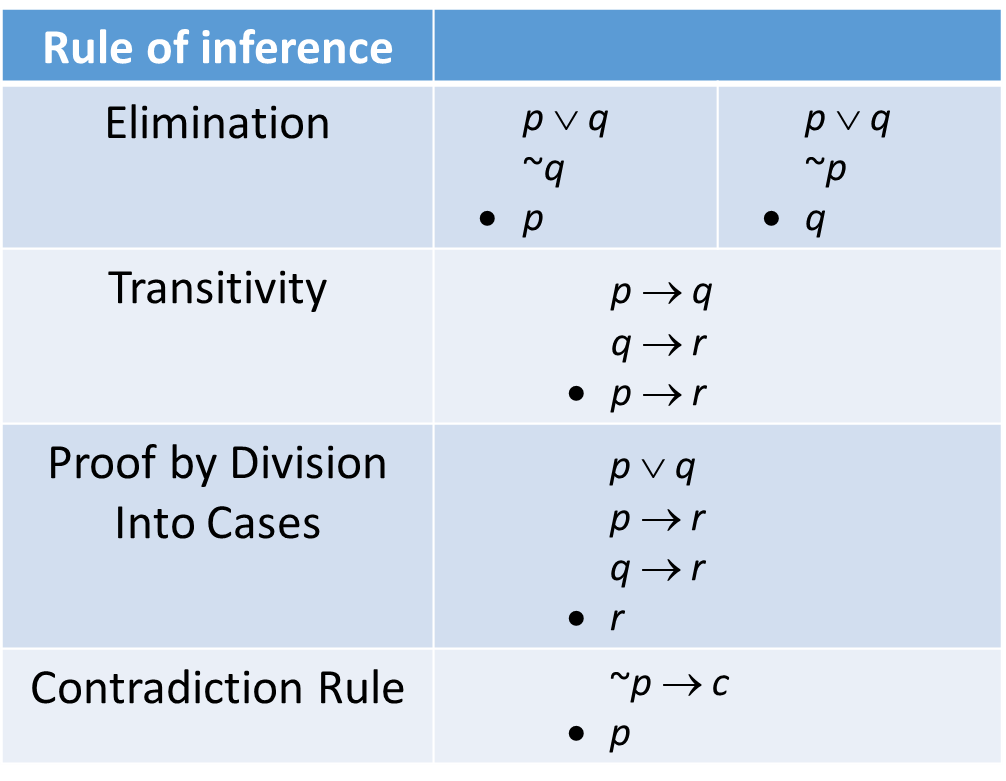
Impt Tables:



Importance of Operations:

NOT>(AND=OR)>(IMPLIES==IF AND ONLY IF (BICONDITIONAL))

Valid and Invalid Arguments:



**DEFINITIONS:**

**Divisibility (Definiton 1.3.1):**

**If n and d are integers and d≠ 0**

n is divisible by d iff n equals d times some integer

i.e.

**Even and Odd Numbers (Definition 1.6.1):**

An integer as even iff it is twice some other integer. It is odd iff it is twice some other integer+1

**Prime Numbers (Definition 4.2.1):**

An integer n is prime or composite according to the following:

**Lower Bound:**

**Greatest Common Divisor (Definition 4.5.1):**

]

**Co-prime (Definition 4.5.3):**

**Least Common Multiple (Definition 4.6.1):**

**Modular congruence (Definition 4.7.1):**

**Multiplicative inverse modulo n (Definition 4.7.2):**

**Second-order Linear Homogeneous Recurrence Relation with Constant Co-efficients:**

**Set Theory Definitions:**

**Empty Set (Definition 6.3.1):**

**Set Equality (Definition 6.3.2):**

**Power Set (Definition 6.3.4):**

**Union (Definition 6.4.1):**

**Intersection (Definition 6.4.3):**

**Disjoint Sets (Definition 6.4.5):**

**Mutually Disjoint (Definition 6.4.6):**

**Partition (Definition 6.4.7):**

**Non-symmetric difference (A-B) (Definition 6.4.8):**

**Symmetric-Difference (Definition 6.4.9):**

**Complement (Definition 6.4.10):**

**Cartesian product (Definition 8.1.3 &8.1.4 (general)):**

**Relation (Definition 8.2.1 & 8.2.7(generalized))**

**Domain, Range, Co-domain (Definition 8.2.2 to 8.2.4):**

(**Proposition 8.2.5)**

**Inverse Relation (Definition 8.2.6):**

t)

**Composition (Definition 8.2.9):**

**Reflexivity, Symmetry and Transitivity of Relations (8.3.1 to 8.3.3):**

(8.3.3))

**Definition 8.3.4 (Equivalence Relation):**

**Definition 8.3.5 (Equivalence Class):**

**Definition 8.5.1 (Transitive Closure):**

**Definition 8.6.2 (Partial Order):**

**Definition 8.6.3 (Comparable):**

**Definition 8.6.4 (Total Order):**

**Definitions 8.6.5-8.6.8 (Minimax definitions):**

**Definition 8.6.9.**

**Definition 7.1.1 (Function):**

**Definition 7.1.2-7.1.5:**

**Definition 7.2.1-7.2.3(Injective, Surjective, Bijective, Identity):**

/--/

//

**Counting and Probability:**

**Sample Space:**

**Probability:**

**r-Combinations:**

**Let *n* and *r* be non-negative integers with *r* ≤ *n*.**

**An *r*-combination of a set of *n* elements is a subset of *r* of the *n* elements.**

**Expected Value:**

**Conditional probability:**

**Independent Events:**

**Pairwise Independent:**

**GRAPH THEORY:**

**Graph:**

**Degree:**

**Trails, Walks, Paths, Circuits, Closed walks, closed circuits, Simple circuits:**

**Isomorphic Graph:**

--

**Trees:**

A **weighted graph** is a graph for which each edge has an associated positive real number **weight** . The sum of the weights of all the edges is the **total weight** of the graph.

A **minimum spanning tree** for a connected weighted graph is a spanning tree that has the least possible total weight compared to all other spanning trees for the graph.

If *G* is a weighted graph and *e* is an edge of *G*, then ***w*(*e*)** denotes the weight of *e* and ***w*(*G*)** denotes the total weight of *G*

**Theorems:**

**Theorem 4.1.1:**

**Proposition 4.2.2:**

**Theorem 4.2.3:**

*are any integers such that p |*

**Theorem 4.3.1 (Epp):**

**Theorem 4.3.3 (Epp)**:

**Theorem 4.3.4 (Epp):**

**Theorem 4.3.5 (Epp):**

**Proposition 4.7.3 (Epp):**

**Theorem 4.7.4 (Epp):**

**Theorem 4.3.2 (Well Ordering Principle):**

**Proposition 4.3.3:**

**Theorem 4.4.1 (Quotient Remainder Theorem):**

**Theorem 4.5.2(Bezout’s Identity):**

**Proposition 4.5.4**

**Theorem 8.4.1 (Epp) (Modular Equivalences)**

**Theorem 8.4.3 (Epp):**

**Corollary 8.4.4 (Epp):**

**Theorem 4.7.3 (Existence of Multiplicative Inverse)**

**Corollary 4.7.4 (Special case: n is prime):**

**Theorem 8.4.9 (Epp)**

**Theorem 5.1.1 (Epp)**

**Theorem 5.8.3(Epp) Distinct Roots Theorem:**

**Theorem 5.8.5(Epp)**

**Theorem 6.2.1 (Epp):**

**Theorem 6.2.2 (Epp):**

**Theorem 6.2.3 (Epp):**

**Theorem 6.2.4 (Epp):**

**Proposition 6.3.3 & Corollary 6.2.5(Epp):**

**Proposition 6.4.2:**

then

**Proposition 6.4.4:**

then

**Proposition 8.2.9 and 8.2.10:**

**Theorem 8.3.1**

**Lemma 8.3.2 &8.3.3 (Epp):**

**Theorem 8.3.4 (Epp):**

**Proposition 8.5.2:**

**Proposition 7.2.4 (Existence of )**

**Proposition 7.3.1 (Composition):**

**Proposition 7.3.3**

**Theorem 9.1.1:**

**Theorem 9.2.1 (The Multiplication Rule):**

**Theorem 9.2.2 (Permutations of n objects):**

**Theorem 9.2.3 r-Permutations from a set of n elements**

**Theorem 9.3.1 The Addition Rule**

**Theorem 9.3.2 The Difference Rule**

**Theorem 9.3.3 The Inclusion-Exclusion Principle**

**Generalized Pigeonhole Principle (Contrapositive):**

*For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if k < n/m, then there is some y ∈ Y such that y is the image of at least k + 1 distinct elements of X.*

*For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if for each y ∈ Y, f –1(y) has at most k elements, then X has at most km elements; in other words, n ≤ km.*

**Theorem 9.4.2**

--

**Theorem 9.5.1**

**Theorem 9.5.2**

**Theorem 9.6.1**

**Pascal’s Formula(Theorem 9.7.1):**

**Binomial Theorem (Theorem 9.7.2):**

**Probability Axioms:**

**Theorem 9.9.1-9.9.3:**

**Bayes’ Theorem:**

**Theorem 10.1.1 (Handshake Theorem):**

**Corollary 10.1.2:**

**Propostition 10.1.3:**

**Lemma 10.2.1:**

**Theorem 10.2.2:**

**Theorem 10.2.3:**

**Theorem 10.2.4:**

**Corollary 10.2.5:**

**Proposition 10.2.6**

**Adjacency Matrices:**

(Theorem 10.3.2)

**Theorem 10.4.1 (Isomorphism)**

**Theorem 10.4.2 Graph Isomorphism invariants:**

**Lemma 10.5.1:**

**Theorem 10.5.2:**

**Lemma 10.5.3:**

**Theorem 10.5.4:**

**Theorem 10.6.1: Full Binary Tree**

**Theorem 10.6.2**

**Proposition 10.7.1**

F1. *Commutative Laws* For all real numbers *a* and *b*,  
*a* + *b* = *b* + *a* and *ab* = *ba.*  
F2. *Associative Laws* For all real numbers *a, b,* and *c,*  
*(a* + *b)* + *c* = *a* + *(b* + *c)* and *(ab)c* = *a(bc).*  
F3. *Distributive Laws* For all real numbers *a, b,* and *c,*  
*a(b* + *c)* = *ab* + *ac* and *(b* + *c)a* = *ba* + *ca.*  
F4. *Existence of Identity Elements* There exist two distinct real numbers, denoted 0  
and 1, such that for every real number *a,*  
0 + *a* = *a* + 0 = *a* and 1 · *a* = *a* · 1 = *a.*  
F5. *Existence of Additive Inverses* For every real number *a*, there is a real number,  
denoted −*a* and called the **additive inverse** of *a,* such that  
*a* + *(*−*a)* = *(*−*a)* + *a* = 0*.*  
F6. *Existence of Reciprocals* For every real number *a* = 0*,* there is a real number,  
denoted 1*/a* or *a*−1*,* called the **reciprocal** of *a,* such that  
*a* · = · *a* = 1  
  
**A - 2** Appendix A Properties of the Real Numbers  
T1. *Cancellation Law for Addition* If *a* + *b* = *a* + *c,* then *b* = *c*. (In particular, this  
shows that the number 0 of Axiom F4 is unique.)  
T2. *Possibility of Subtraction* Given *a* and *b,* there is exactly one *x* such that *a* + *x* = *b*.  
This *x* is denoted by *b* − *a*. In particular, 0 − *a* is the additive inverse of *a,* −*a*.  
T3. *b* − *a* = *b* + *(*−*a)*.  
T4. −*(*−*a)* = *a*.  
T5. *a(b* − *c)* = *ab* − *ac*.  
T6. 0· *a* = *a* · 0 = 0.  
T7. *Cancellation Law for Multiplication* If *ab* = *ac* and *a* = 0*,* then *b* = *c*. (In particular, this shows that the number 1 of Axiom F4 is unique.)  
T8. *Possibility of Division* Given *a* and *b* with *a* = 0, there is exactly one *x* such that  
*ax* = *b*. This *x* is denoted by *b/a* and is called the **quotient** of *b* and *a*. In particular,  
1*/a* is the reciprocal of *a*.  
T9. If *a* 0, then *b/a* = *b*· *a*−1.  
T10. If *a*  0, then *(a*−1*)*−1 = *a*.  
T11. *Zero Product Property* If *ab* = 0, then *a* = 0 or *b* = 0.  
T12. *Rule for Multiplication with Negative Signs*  
*(*−*a)b* = *a(*−*b)* = −*(ab), (*−*a)(*−*b)* = *ab,*  
and  
T13. *Equivalent Fractions Property*

T14. *Rule for Addition of Fractions*  
 *b*

T15. *Rule for Multiplication of Fractions*

T16. *Rule for Division of Fractions*  
The real numbers also satisfy the following axioms, called the **order axioms.** It is assumed  
that among all real numbers there are certain ones, called the **positive real numbers,** that  
satisfy properties Ord1–Ord3.  
  
Ord1. For any real numbers *a* and *b,* if *a* and *b* are positive, so are *a* + *b* and *ab*.  
Ord2. For every real number *a* 0*,* either *a* is positive or −*a* is positive but not both.  
Ord3. The number 0 is not positive.  
The symbols *<,>,* ≤*,* and ≥*,* and negative numbers are defined in terms of positive  
numbers.  
• **Definition**  
Given real numbers *a* and *b,*  
*a < b* means *b* + *(*−*a)* is positive. *b > a* means *a < b*.  
*a* ≤ *b* means *a < b* or *a* = *b*. *b* ≥ *a* means *a* ≤ *b*.  
If *a <* 0, we say that *a* is **negative.** If *a* ≥ 0*,* we say that *a* is **nonnegative.**  
From the order axioms Ord1–Ord3 and the above definition, all the usual rules for calculating with inequalities can be derived. The most important are collected as theorems  
T17–T27 as follows. In all these theorems the symbols *a, b, c,* and *d* represent arbitrary  
real numbers.  
T17. *Trichotomy Law* For arbitrary real numbers *a* and *b*, exactly one of the three relations *a < b, b < a,* or *a* = *b* holds.  
T18. *Transitive Law* If *a < b* and *b < c*, then *a < c*.  
T19. If *a < b*, then *a* + *c < b* + *c*.  
T20. If *a < b* and *c >* 0, then *ac < bc*.  
T21. If *a*  0, then *a*2 *>* 0.  
T22. 1 *>* 0.  
T23. If *a < b* and *c <* 0, then *ac > bc*.  
T24. If *a < b*, then −*a >* −*b*. In particular, if *a <* 0, then −*a >* 0.  
T25. If *ab >* 0, then both *a* and *b* are positive or both are negative.  
T26. If *a < c* and *b < d*, then *a* + *b < c* + *d*.  
T27. If 0 *< a < c* and 0 *< b < d*, then 0 *< ab < cd*