## Logical Equivalence Laws

1. $p \wedge T \equiv p$, $p \vee F \equiv p$ — Identity Laws
2. $p \vee \mathbf{T} \equiv \mathbf{T}$, $p \wedge \mathbf{F} \equiv \mathbf{F}$ — Domination Laws
3. $p \vee p \equiv p$, $p \wedge p \equiv p$ — Idempotent Laws
4. $\neg(\neg p) \equiv p$ — Double Negation
5. $p \vee q \equiv q \vee p$, $p \wedge q \equiv q \wedge p$ — Commutatve
6. $(p \vee q) \vee r \equiv p \vee (q \vee r)$, $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ — Associative
7. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$, $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ — Distributive
8. $\neg(p \wedge q) \equiv \neg p \vee \neg q$, $\neg(p \vee q) \equiv \neg p \wedge \neg q$ — DeMorgan's
9. $p \vee (p \wedge q) \equiv p$, $p \wedge (p \vee q) \equiv p$ — Absorption
10. $p \vee \neg p \equiv \mathbf{T}$, $p \wedge \neg p \equiv \mathbf{F}$ — Negation
11. $\neg \forall x\, P(x) \equiv \exists x\, \neg P(x)$, $\neg \exists x\, P(x) \equiv \forall x\, \neg P(x)$ — De Morgans (Quantifiers)
12. $p \to q \equiv \neg p \vee q$ — Implication Breakout
13. $p \to q \equiv \neg q \to \neg p$ — Contrapositives

## Natural Deduction Rules:

### 5 intro rules

$\wedge$-intro $\dfrac{p,\ q}{p \wedge q}$

$\vee$-intro $\dfrac{p}{p \vee q}$ / $\dfrac{q}{p \vee q}$

$\to$-intro $\dfrac{\boxed{\begin{array}{c} p \\ \vdots \\ q \end{array}}}{p \to q}$

$\leftrightarrow$-intro $\dfrac{\boxed{\begin{array}{c} p \\ \vdots \\ q \end{array}} \quad \boxed{\begin{array}{c} q \\ \vdots \\ p \end{array}}}{p \leftrightarrow q}$

$\neg$-intro $\dfrac{\boxed{\begin{array}{c} p \\ \vdots \\ F \end{array}}}{\neg p}$

### 7 elim rules

$\wedge$-elim $\dfrac{p \wedge q}{p}$ / $\dfrac{p \wedge q}{q}$

$\vee$-elim $\dfrac{\boxed{\begin{array}{c} p \\ \vdots \\ r \end{array}} \quad \boxed{\begin{array}{c} q \\ \vdots \\ r \end{array}} \quad p \vee q}{r}$

$\to$-elim $\dfrac{p,\ p \to q}{q}$

$\leftrightarrow$-elim $\dfrac{p \leftrightarrow q,\ p}{q}$ / $\dfrac{p \leftrightarrow q,\ q}{p}$

$\neg$-elim $\dfrac{p,\ \neg p}{F}$

$\neg\neg$-elim $\dfrac{\neg\neg p}{p}$

F-elim $\dfrac{F}{p}$

### Quantifier Rules

$\forall$-elim $\dfrac{\forall P(x)}{P(t)}$

$\exists$-intro $\dfrac{P(t)}{\exists x\, P(x)}$

$\forall$-intro $\dfrac{\boxed{\begin{array}{c} x_0 \\ \vdots \\ P(x_0) \end{array}}}{\forall x\, P(x)}$

$\exists$-elim $\dfrac{\exists x\, P(x),\ \boxed{\begin{array}{c} x_0 \quad P(x_0) \\ \vdots \\ q \end{array}}}{q}$

## Things to Remember:

- Do $\forall$-elim inside correct assumption box w/ same variable name that's needed
- Check line numbers — make sure to include ALL necessary citations for each step of natural deduction
- 2 Assumption Boxes will never end on the same line
- Distributive law WORKS BOTH WAYS
- For proof by contradiction for $p \to q$, assume $p$ is true and $q$ is false; then show that $p$ is false based on $q$ being true, creating contradiction.
- Check Work!! ⚠

## Table 7

(1) $p \to q \equiv \neg p \vee q$

(2) $p \to q \equiv \neg q \to \neg p$

(3) $p \vee q \equiv \neg p \to q$

(4) $p \wedge q \equiv \neg(p \to \neg q)$

(5) $\neg(p \to q) \equiv p \wedge \neg q$

(6) $(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$

(7) $(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$

(8) $(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

(9) $(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

## Proofs with Words

- Direct
- Contrapositive
- Contradiction
- Casework
- Counter example

- Cite definitions all the time - make explicit
- Say @ start what kind of proof it is
- "Seeking a contradiction, assume ..."
- "Let x be an arbitrary integer..."
- To prove $a \equiv b \equiv c$, prove CYCLE: $a \to b$, $b \to c$, $c \to a$.
- When proving rational / irrational, set $x = p/q$, with $\gcd(p, q) = 1$. For other things too, say "first instance of" or other specific to create contradiction later.

1. When proving logical equivalences, do NOT write both sides of equation.
- Edge / 0 cases in proofs
- For equivalent, must be able to start at any / get to any.

## Modular Arithmetic

- $a \equiv b \pmod m \Rightarrow a - b = m \cdot k$, $k \in \mathbb{Z}$
- m unique (mod m) values
- Addition, Subtraction, Multiplicatn normal; Division Hard
- $a^{-1}(a) \equiv 1 \bmod m$
  - → if $a^{-1}$ exists, is unique ($a, m$ relatively prime)
  - → otherwise, 0 or MULTIPLE SOLS

- Proposition: Statement abt world w/ truth value
  - paradox / not well-defined ⇒ not a prop
  - every prop has negation
- Predicate: Statement w/ unspecified variables that becomes proposition once defined
  - Can define variables OR put $\forall$ / $\exists$
- Quantifiers: order matters when different!

- Tautology: A compound prop that is always true
- Contradiction: A compound prop that is always false
- Satisfiable: A compound prop that has a possible assignment of truth values to make it True.
- Consistent System: System specifications do not contain conflicting requirements that could be used to derive contradiction.

## FME ($3^{26}$ mod 15)

$3^{26} = (3^{13})^2$ $\qquad 3^3 \equiv -3 \bmod 15$

$3^{13} = 3 \cdot 3^{12}$ $\qquad 3^6 \equiv (-3)^2 \bmod 15 \equiv -6$

$3^{12} = (3^6)^2$ $\qquad 3^{12} \equiv (-6)^2 \bmod 15 \equiv 6$

$3^6 = (3^3)^2$ $\qquad 3^{13} \equiv 3 \bmod 15$

$3^{26} = 3^2 \bmod 15 \equiv \boxed{9}$

- if p then q
- p only if q
- q unless not p
- q whenever p
- if p, q
- q if p
- q when p
- p implies q
- p is sufficient for q
- q follows from p
- q is necessary for p
- a necessary condition for p is q
- A sufficient condition for q is p

| p | q | p → q |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

be careful inside quantifiers of F → F case !!

$p \leftrightarrow q \equiv p \equiv q$

$\wedge$: and $\quad \vee$: or $\quad \oplus$: XOR ($\neg \leftrightarrow$) $\quad$ but $\equiv$ and

## Extended Euclidean Algo

- $59x \equiv 3 \bmod 73$

| | | |
|---|---|---|
| gcd (73, 59) | 73 − 59 = 14 | 3 − 2 = 1 |
| gcd (59, 14) | 59 − 4(14) = 3 | 3 − (14 − 4·3) = 1 |
| gcd (14, 3) | 14 − 4·3 = 2 | 5·3 − 14 = 1 |
| gcd (3, 2) | 3 − 2 = 1 | 5[59 − 4(14)] − 14 = 1 |
| gcd (2, 1) | | 5·59 − 21·14 = 1 |
| | | 5·59 − 21(73−59) = 1 |
| | | 26·59 − 21·73 = 1 |

$(26 \cdot 59 - \cancel{21 \cdot 73}) \bmod 73 \equiv 1 \bmod 73$

$26 \cdot 59 \bmod 73 \equiv 1 \bmod 73$

$26(59)\, x \equiv 26(3) \bmod 73$

$x \equiv 78 \bmod 73$

$\boxed{x \equiv 5 \bmod 73}$

if-then with $\forall$ to talk about some of domain and with $\exists$ to talk about some of domain

S(x): student in class $\qquad$ C(x): studied calculus

Every student in this class has studied calculus $\forall x\,(S(x) \to C(x))$

Some student in this class has studied calculus $\exists x\,(S(x) \wedge C(x))$

Logic Puzzles: Write down $2^n$ truth table of possibilities, see which consistent.

$\exists y\, \forall(x)\, P(x, y) \to \forall x\, \exists y\, P(x, y)$

restrictive; single y to satisfy each x value

not as restrictive; can have diff y for each x-val

# Sample Natural Deduction Proofs:

$$\frac{\neg(a \wedge b)}{\neg a \vee \neg b}$$

| | | |
|---|---|---|
| 1. | $\neg(a \wedge b)$ | Premise |
| 2. | $\neg(\neg a \vee \neg b)$ | Assumptn |
| 3. | $a$ | Assumption |
| 4. | $b$ | Assumption |
| 5. | $(a \wedge b)$ | $\wedge$-intro (4, 3) |
| 6. | F | $\neg$-elim (5, 1) |
| 7. | $\neg b$ | $\neg$-intro (4 - 7) |
| 8. | $\neg a \vee \neg b$ | $\vee$-intro (7) |
| 9. | F | $\neg$-elim (2, 8) |
| 10. | $\neg a$ | $\neg$-intro (3-9) |
| 11. | $\neg a \vee \neg b$ | $\vee$-intro (10) |
| 12. | F | $\neg$-elim (2, 11) |
| 13. | $\neg\neg(\neg a \vee \neg b)$ | $\neg$-intro (2-12) |
| 14. | $\neg a \vee \neg b$ | $\neg\neg$-elim (13) |

$$\frac{\forall x\, \exists y\, [P(x) \rightarrow Q(y)], \quad \exists x\, P(x)}{\exists y\, Q(y)}$$

| | | |
|---|---|---|
| 1. | $\forall x\, \exists y\, [P(x) \rightarrow Q(y)]$ | Premise |
| 2. | $\exists x\, P(x)$ | Premise |
| 3. | $x_0 \quad P(x_0)$ | Arbitrary x / Assumption |
| 4. | $\exists y\, [P(x_0) \rightarrow Q(y)]$ | $\forall$-elim (1) |
| 5. | $y_0 \quad P(x_0) \rightarrow Q(y_0)$ | Arbitray y / Assumptn |
| 6. | $Q(y_0)$ | $\rightarrow$-elim (3, 5) |
| 7. | $Q(y_0)$ | $\exists$-elim (4, 5-6) |
| 8. | $Q(y_0)$ | $\exists$-elim (2, 3-7) |
| 9. | $\exists y\, Q(y)$ | $\exists$-intro (8) |

$$\overline{p \vee \neg p}$$

| | | |
|---|---|---|
| 1 | $\neg(p \vee \neg p)$ | Assumption |
| 2. | $p$ | Assumption |
| 3. | $p \vee \neg p$ | $\vee$-intro (2) |
| 4. | F | $\neg$-elim (1, 3) |
| 5. | $\neg p$ | $\neg$-intro (2-4) |
| 6. | $p \vee \neg p$ | $\vee$-intro (5) |
| 7. | F | $\neg$-elim (1, 6) |
| 8. | $\neg\neg(p \vee \neg p)$ | $\neg$-intro (1-7) |
| 9. | $(p \vee \neg p$ | $\neg\neg$-elim (8) |

$$\begin{array}{l} \forall x(P(x) \rightarrow \neg Q(x)) \\ \underline{\exists x(P(x) \wedge Q(x))} \\ \therefore\ \forall x R(x) \end{array}$$

| | | | |
|---|---|---|---|
| 1. | $\forall x\, [P(x) \rightarrow \neg Q(x)]$ | Premise | ✓ |
| 2. | $\exists x\, (P(x) \wedge Q(x))$ | Premise | ✓ |
| 3. | $x_0 \quad P(x_0) \wedge Q(x_0)$ | Arbitrary x (2) | ✓ |
| 4. | $P(x_0) \rightarrow \neg Q(x_0)$ | $\forall$-elim (1) | ✓ |
| 5. | $P(x_0)$ | $\wedge$-elim (3) | ✓ |
| 6. | $Q(x_0)$ | $\wedge$-elim (3) | ✓ |
| 7. | $\neg Q(x_0)$ | $\rightarrow$-elim (5, 4) | ✓ |
| 8. | F | $\neg$-elim (6, 7) | ✓ |
| 9. | F | $\exists$-elim (2, 3-8) | ✓ |
| 10. | $\forall x\, R(x)$ | F-elim (9) | ✓ |

+7

$L(x, y)$ : x eats lunch w/ y
$C(x, y)$ : x has class w/ y
$R(x, y)$ : x is roommates w/ y
} UM Students

a) $\forall x\, \forall y\, [(C(x,y) \wedge R(x,y)) \rightarrow L(x,y)]$

Every pair of UM students that have a class w/ each other and are roommates, eat lunch together.

b) $\exists x\, \forall y\, [((x \neq y) \wedge C(x,y)) \rightarrow \neg L(x,y)]$

There is at least one UM studen who does not have lunch w/ any of their classmates.

c) $\forall x\, \exists y\, [((x \neq y) \wedge C(x,y) \vee R(x,y)) \wedge \neg L(x,y)]$

For every UM student, there exists someone who they are either roommates or classmates with and they don't eat lunch with.

$I(x)$ : x has internet connection
(x: students in class)

"Everyone except one student has an internet connection in class."

$\exists x\, \neg I(x) \wedge \forall y\, (x \neq y \rightarrow I(y))$

$$\frac{\neg p \wedge q}{\therefore \neg(p \vee \neg q)}$$

| | | | |
|---|---|---|---|
| 1. | $\neg p \wedge q$ | Premise | ✓ |
| 2. | $p \vee \neg q$ | Assumption | ✓ |
| 3. | $p$ | Assumption | ✓ |
| 4. | $\neg p$ | $\wedge$-elim (1) | ✓ |
| 5. | F | $\neg$-elim (3, 4) | ✓ |
| 6. | $\neg q$ | Assumption | ✓ |
| 7. | $q$ | $\wedge$-elim (1) | ✓ |
| 8. | F | $\neg$-elim (6, 7) | ✓ |
| 9. | F | $\vee$-elim(2, 3-5, 6-8) | ✓ |
| 10. | $\neg(p \vee \neg q)$ | $\neg$-intro (2-9) | ✓ |

## ① Prove that $\sqrt{2}$ is irrational

Seeking contradiction, $\sqrt{2} = a/b$, $\gcd(a,b) = 1$.

$\frac{a^2}{b^2} = 2 \rightarrow a^2 = 2b^2$. Thus $a^2$ is even.

Prove if $a^2$ is even then a is even by contrapositive.

Then $a = 2k$; $(2k)^2 = 2b^2$; $b^2 = 2k^2$.

Same proof by contrapositive; b is even.

As a, b both even, $\gcd(a, b) \neq 1$ (CONTRADICTION!)

Thus, $\sqrt{2}$ is not rational.

## ② Infinitely Many Primes:

Seeking a contradiction, assume there are finitely many primes. Then, we could list them all in increasing order: $P_1, P_2, \ldots, P_n$

$Q = (P_1 P_2 P_3 \ldots P_n) + 1$ Product of all prims + 1.

$Q \equiv 1 \bmod p_i \quad \forall\, i \in [1, n]$

$\rightarrow$ Q is one more than a multiple of any of those primes

Q cannot be prime as it is greater than $p_n$.

Thus, Q must be the product of prims, yet no prime $P_1, P_2, \ldots P_n$ divides Q. This creates a contradiction

Thus, we conclude that the assumption was false, and therefore there must be infinitely many primes.