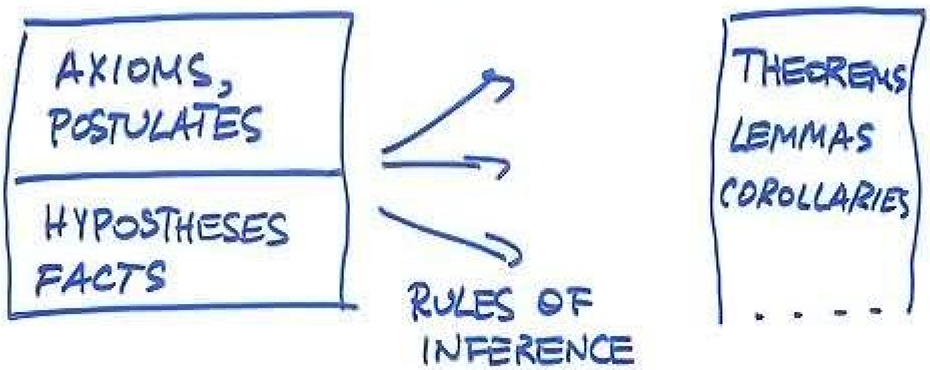
LEC. 12 09/22/99

# PROOFS

SYSTEMATIC METHOD OF ESTABLISHING TRUTH




AXIOMS, POSTULATES: BASIC ASSUMPTIONS ABOUT UNDERLYING MATHEMATICAL STRUCTURES (COMMUTATIVITY OF ADDITION, MULTIPLICATION, LAWS OF EQUALITY, ORDERS, ETC.)

HYPOTHESES: ASSUMPTIONS MADE FOR A PARTICULAR THEOREM (LET $p, q$ BE RELATIVELY PRIME INTEGERS. THEN...)

FACTS: PREVIOUSLY PROVED THEOREMS

THEOREMS, LEMMAS, COROLLARIES: CONCLUTIONS

RULES OF INFERENCE: CORRECT METHODS OF REASONING.

**TABLE 1 Rules of Inference.**

| *Rule of Inference* | *Tautology* | *Name* |
|---|---|---|
| $p$<br>$\therefore p \vee q$ | $p \rightarrow (p \vee q)$ | Addition |
| $p \wedge q$<br>$\therefore p$ | $(p \wedge q) \rightarrow p$ | Simplification |
| $p$<br>$q$<br>$\therefore p \wedge q$ | $\cancel{((p) \wedge (q)) \rightarrow (p \wedge q)}$<br>$p \Rightarrow (q \Rightarrow (p \wedge q))$ | Conjuction |
| $p$<br>$p \rightarrow q$<br>$\therefore q$ | $[p \wedge (p \rightarrow q)] \rightarrow q$ | Modus ponens |
| $\neg q$<br>$p \rightarrow q$<br>$\therefore \neg p$ | $[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$ | Modus tollens |
| $p \rightarrow q$<br>$q \rightarrow r$<br>$\therefore p \rightarrow r$ | $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$ | Hypothetical syllogism |
| $p \vee q$<br>$\neg p$<br>$\therefore q$ | $[(p \vee q) \wedge \neg p] \rightarrow q$ | Disjunctive syllogism |

## DEDUCTION THEOREM:

$T$ IS PROVABLE FROM HYPOTHESES $H_1, H_2, \dots H_n$ $\Longleftrightarrow$ $H_1 \wedge H_2 \wedge \dots \wedge H_n \rightarrow T$ IS VALID

EXAMPLE: $p$ := YOU SEND ME E-MAIL
$q$ := I WILL FINISH WRITING THE PROGRAM
$r$ := I WILL GO TO SLEEP EARLY
$s$ := I WILL WAKE UP FEELING REFRESHED

HYPOTHESES: $p \rightarrow q$, $\neg p \rightarrow r$, $r \rightarrow s$

THE GOAL: $\neg q \rightarrow s$

ARGUMENT:

1. $p \rightarrow q$ — HYP
2. $\neg q \rightarrow \neg p$ — CONTRAPOSITIVE OF 1
3. $\neg p \rightarrow r$ — HYP
4. $\neg q \rightarrow r$ — SYLLOGISM, FROM 2, 3
5. $r \rightarrow s$ — HYP
6. $\neg q \rightarrow s$ — SYLLOGISM, FROM 4, 5

FALLACY: INCORRECT REASONING

EXAMPLE: $\dfrac{p \rightarrow q,\ q}{p}$ FALLACY OF AFFIRMING THE CONCLUSION

cf: $\dfrac{p \rightarrow q,\ p}{q}$ - modus ponens

EXAMPLE: $n \equiv 1 \pmod 3 \sim p$

$n^2 \equiv 1 \pmod 3 \sim q$

$p \to q$ IS TRUE

ASSUME $q$. THEN $p$?

$$\frac{p \to q,\ q}{p} \quad ?$$

$(p \to q) \wedge q \Longrightarrow p$ IS NOT A TAUTOLOGY

F T T T T F F

CIRCULAR REASONING: A STATEMENT IS PROVED USING ITSELF

## RULES FOR QUANTIFIERS

UNIVERSAL INSTANTIATION: $\forall x P(x) \,/\, P(c)$

UNIVERSAL GENERALIZATION: $$\frac{P(c) \text{ FOR ARBITRARY } c}{\forall x\, P(x)}$$

EXISTENTIAL INSTANTIATION: $\exists x P(x) \,/\, P(c)$ FOR SOME $c$

EXISTENTIAL GENERALIZATION: $P(c) \,/\, \exists x P(x)$

EXAMPE: BIRDS CAN FLY. TWIGGY IS A BIRD. THEN T. CAN FLY

$B(x) \sim$ "X IS A BIRD", $F(x) \sim$ "X CAN FLY", $T$ = TWIGGY

1. $\forall x (B(x) \to F(x))$ HYPOTHESIS
2. $B(T) \to F(T)$ BY UNIVERSAL INSTANTIATION
3. $B(T)$ HYPOTHESIS
4. $F(T)$ BY MODUS PONENS, FROM 2,3.

DIRECT PROOF: $H / G \Rightarrow H \to G$

INDIRECT PROOF: $\neg G / \neg H \Rightarrow \neg G \to \neg H \Rightarrow H \to G$

$3n+2$ IS ODD $\to$ $n$ IS ODD ?

LET $n$ BE EVEN; $n = 2k$, $\underbrace{3n+2 = 3 \cdot 2k + 2 = 2(3k+1)}_{\text{EVEN.}}$

THEREFORE: IF $3n+2$ IS ODD THEN $n$ IS ODD.

PROOF BY CONTRADICTION:
$$\frac{\dfrac{\neg p / r \quad , \quad \neg p / \neg r}{\neg p / r \wedge \neg r}}{p}$$

<u>EXAMPLE:</u> $\sqrt{2}$ IS IRRATIONAL

$\neg p$: $\sqrt{2}$ IS RATIONAL $\Rightarrow \sqrt{2} = \frac{m}{n}$ $\underbrace{\gcd(m,n) = 1}_{r}$

$2 = \frac{m^2}{n^2} \Rightarrow 2n^2 = m^2 \Rightarrow m^2$ IS EVEN

IF $m$ WERE ODD, THEN $m = 2k+1$, $\underbrace{m^2 = 4k^2 + 4k + \underline{1}}_{\text{ALSO ODD}}$

THUS $m$ IS EVEN, $m = 2k$,

$2n^2 = 4k^2$, $n^2 = 2k^2$, $n^2$ IS EVEN, $n$ IS EVEN

$\Rightarrow \gcd(m,n) \geq 2 \Rightarrow \underbrace{\gcd(m,n) \neq 1}_{\neg r}$

$$\frac{\neg p / r \qquad \neg p / \neg r}{p}$$

EXAMPLE. "THE FOLLOWING ARE EQUIVALENT

1. $p_1$
2. $p_2$
⋮
n. $p_n$ "

$p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_n$. SUFFICES TO ESTABLISH

$p_1 \to p_2 \to p_3 \to \dots \to p_n \to p_1$

EXISTENCE PROOF: THEOREM IS $\exists x P(x)$

CONSTRUCTIVE, IF $P(a) \,/\, \exists x P(x)$

NONCONSTRUCTIVE: $\dfrac{\dfrac{\forall x \neg P(x) \,/\, \text{CONTRADICTION}}{\neg \forall x \neg P(x)}}{\exists x P(x)}$

NO SPECIFIC $a$ SUCH THAT $P(a)$ IS GIVEN

$\exists x$ ($x+i$ IS COMPOSITE FOR $i = 1, 2, \dots 100$)

$x := (101)! + 1$ CONSTRUCTIVE

$\exists p$ ($p$ IS A PRIME $\wedge\, p > 10^{10^{10}}$)

$n = 10^{10^{10}}$; $m = n! + 1$; $p$ - PRIME FACTOR OF $m$

THEN $p \nmid 2, 3, 4, \dots, n \Rightarrow p > n$. NONCONSTRUCTIVE

NO SPECIFIC $p$ IS GIVEN

HW 3.1: 2b,e 12 18 54