LEC. 12 09/22/99

PROOFS

SYSTEMATIC METHOD OF ESTABLISHING TRUTH

AXIOMS, POSTULATES	RULES OF INFERENCE →	THEOREMS, LEMMAS, COROLLARIES, ...
HYPOSTHESES, FACTS		

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.

-81-

3.1 Methods of Proof 165

TABLE 1 Rules of Inference.

Rule of Inference	Tautology	Name
p / $\therefore p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ / $\therefore p$	$(p \wedge q) \to p$	Simplification
p / q / $\therefore p \wedge q$	~~$[(p) \wedge (q)] \to (p \wedge q)$~~ $p \to (q \to (p \wedge q))$	Conjuction
p / $p \to q$ / $\therefore q$	$[p \wedge (p \to q)] \to q$	Modus ponens
$\neg q$ / $p \to q$ / $\therefore \neg p$	$[\neg q \wedge (p \to q)] \to \neg p$	Modus tollens
$p \to q$ / $q \to r$ / $\therefore p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Hypothetical syllogism
$p \vee q$ / $\neg p$ / $\therefore q$	$[(p \vee q) \wedge \neg p] \to q$	Disjunctive syllogism

-82-

DEDUCTION THEOREM:

T IS PROVABLE FROM HYPOTHESES $H_1, H_2, \ldots H_n$ $\Longleftrightarrow$ $H_1 \wedge H_2 \wedge \cdots \wedge H_n \to T$ 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: $p \to q$, $\neg p \to r$, $r \to s$

THE GOAL: $\neg q \to s$

ARGUMENT:

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

FALLACY: INCORRECT REASONING

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

cf. $\dfrac{p \to q,\ p}{q}$ - modus ponens.

-83-

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

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

$p \to q$ IS TRUE

ASSUME q. THEN p?

$\dfrac{p \to q,\ q}{p}$?

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

F 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: $\dfrac{P(c) \text{ FOR ARBITRARY } c}{\forall x P(x)}$

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

$B(x)$ ~ "X IS A BIRD", $F(x)$ ~ "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.

-84-

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

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

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

LET n BE EVEN; $n = 2k$, $3n+2 = 3 \cdot 2k + 2 = 2(3k+1)$
EVEN.

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

PROOF BY CONTRADICTION:
$$\frac{\dfrac{\neg P / z \ , \ \neg P / \neg z}{\neg P / z \wedge \neg z}}{P}$$

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

$\neg P$: $\sqrt{2}$ IS RATIONAL $\implies \sqrt{2} = \frac{m}{n}$ $\underbrace{\gcd(m,n)=1}_{z}$

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

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

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

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

$$\frac{\neg P / z \quad \neg P / \neg z}{P}$$

EXAMPLE. "THE FOLLOWING ARE EQUIVALENT
1. p_1
2. p_2
⋮
n. p_n "

$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n$. SUFFICES TO ESTABLISH
$p_1 \to p_2 \to p_3 \to \cdots \to p_n \to p_1$

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

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

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

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

$\exists x$ ($x+i$ IS COMPOSITE FOR $i = 1, 2, \ldots 100$)
$x := (101)! + 1$ 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 $p \nmid 2, 3, 4, \ldots, n \implies p > n$. NONCONSTRUCTIVE
NO SPECIFIC p IS GIVEN

HW 3.1: 2b,e 12 18 54