Ch 1. The Foundations: Logic and Proofs

Methods of Proof

Sungwon Kang

Acknowledgement

- [Rosen 19] Kenneth H. Rosen, for Discrete Mathematics & Its Applications (8th Edition), Lecture slides
- [Hunter 11] David J. Hunter, Essentials of Discrete Mathematics, 2nd Edition, Jones & Bartlett Publishers, 2011, Lecture Slides

Ch 1. The Foundations: Logic and Proofs

1.1 Propositional Logic
1.2 Applications of Propositional Logic
1.3 Propositional Equivalences
1.4 Predicates and Quantifiers
1.5 Nested Quantifiers
1.6 Rules of Inference
1.7 Introduction to Proofs
1.8 Proof Methods and Strategy

Methods of Proof

Note that any of the inference rules of Gentzen's Natural Deduction can be used as a method of proof.

1. Deduction
2. Direct proof
3. Proof by contraposition
4. Proof by contradiction
5. Disproof by giving a counterexample
6. . . .

1. Deduction

- Used to prove a conditional “A $\rightarrow$ B”.

$\longrightarrow$ - intro rule (or Deduction Theorem)
Σ , A |- B logically implies Σ |- A $\longrightarrow$ B

[redacted]

A common application of Deduction

[redacted]

To prove a statement of the form $(\forall x)(P(x) \to Q(x))$, begin your proof with a sentence of the form by applying $\forall$-Elim

Let x be [an element of the domain], and suppose $P(x)$.

Then Q(x) is proved and by the Deduction Theorem, “P(x) $\to$ Q(x)” is true and by $\forall$-intro, we are done.

Example

Definition

An integer x *divides* an integer y if there is some integer k such that $y = kx$. written "x | y"

Axiom

If a and b are integers, so are $a + b$ and $a \cdot b$.

Prove the following.

> *For all integers a, b, and c, if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

Prove the following.

For all integers a, b, and c, if $a \mid b$ *and* $a \mid c$*, then* $a \mid (b + c)$.

Proof.

[redacted]

Prove the following.

> *For all integers a, b, and c, if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

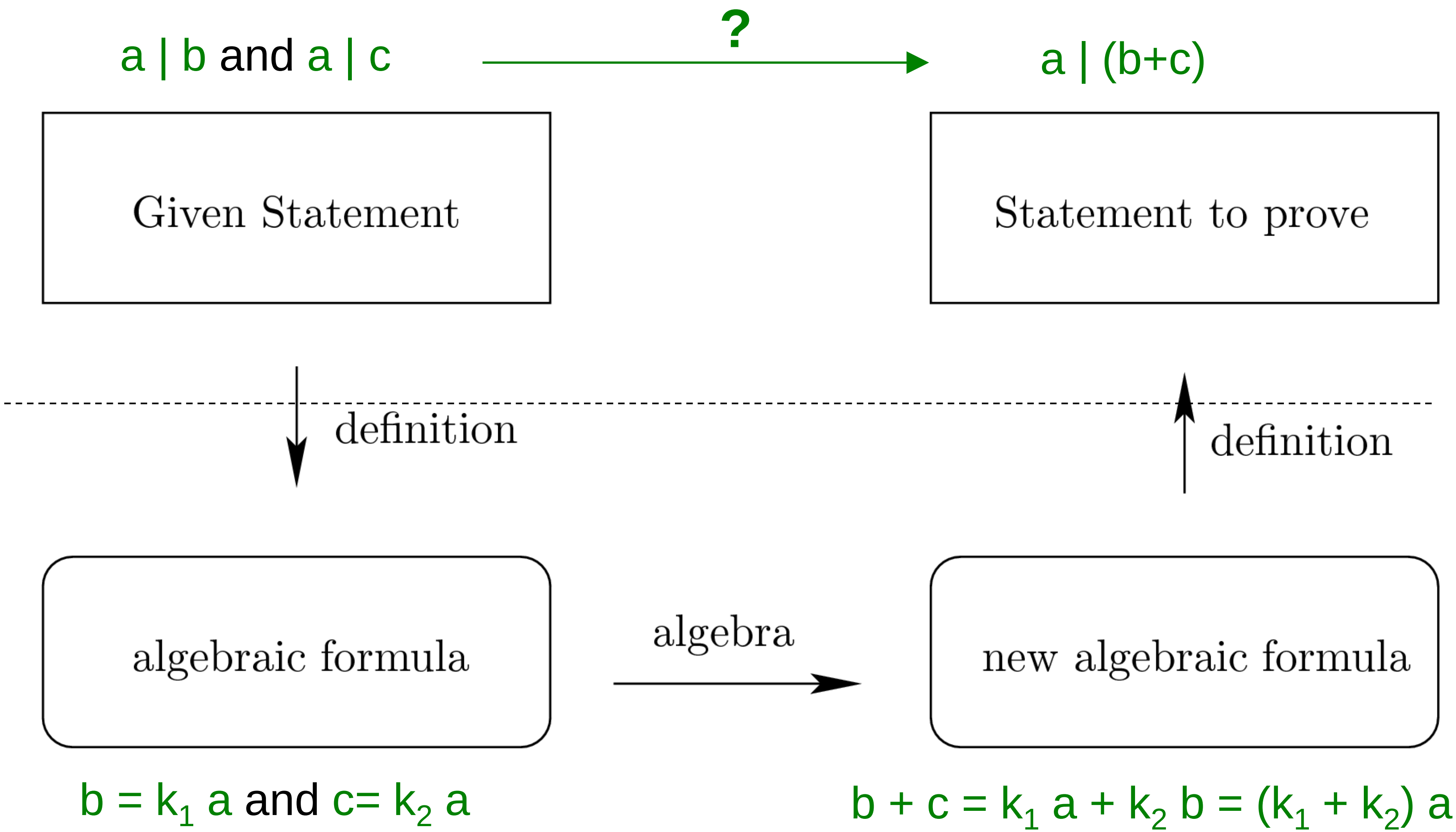
Proof.

Let integers a, b, and c be given, and suppose $a \mid b$ and $a \mid c$. Then, by the definition of $\mid$, there is some integer k_1 such that $b = k_1 a$ and there is some integer k_2 such that $c = k_2 a$. Therefore,

$$b + c = k_1 a + k_2 a = (k_1 + k_2)a.$$

By the closure axiom, $k_1 + k_2$ is an integer, so $a \mid (b + c)$, again by the definition of $\mid$. $\square$

The structure of an algebraic proof



2. Direct Proof

Recall that this is Not a Propositional Logic connective but a "meta-language" symbol and is read "logically implies."

In order to prove $A \Rightarrow C$, we can prove a sequence of results:

$$A \Rightarrow B_1 \Rightarrow B_2 \Rightarrow \cdots \Rightarrow B_n \Rightarrow C$$

This is the logic of a *direct proof*.

Prove the following statement.

For all real numbers x, *if* $x > 1$, *then* $x^2 > 1$.

Proof.

[redacted]

Prove the following statement.

For all real numbers x, if $x > 1$, then $x^2 > 1$.

Proof.

Let x be a real number, and suppose $x > 1$. Multiplying both sides of this inequality by a positive number preserves the inequality, so we can multiply both sides by x to obtain $x^2 > x$. Since $x > 1$, we have $x^2 > x > 1$, or $x^2 > 1$, as required. $\square$

3. Proof by contraposition

To prove a formula of the form “A $\to$ B”, prove its contrapositive instead.

A common application of proof by contraposition

To prove a statement of the form $(\forall x)(P(x) \to Q(x))$, begin your proof with a sentence of the form

Let x be [an element of the domain], and suppose $\neg Q(x)$.

A proof by contraposition is then a sequence of justified conclusions culminating in $\neg P(x)$.

Example 1.

Suppose x and y are positive real numbers such that the geometric mean $\sqrt{xy}$ is different from the arithmetic mean $\frac{x+y}{2}$. Prove that $x \neq y$.

Proof.

Suppose x and y are positive real numbers such that the geometric mean $\sqrt{xy}$ is different from the arithmetic mean $\frac{x+y}{2}$. Prove that $x \neq y$.

Proof.

(By contraposition.) Let x and y be positive real numbers, and suppose $x = y$. Then

$$\begin{aligned} \sqrt{xy} &= \sqrt{x^2} && \text{since } x = y \\ &= x && \text{since } x \text{ is positive} \\ &= \frac{x+x}{2} && \text{using arithmetic} \\ &= \frac{x+y}{2} && \text{since } x = y \end{aligned}$$

$\square$

Example 2.

Theorem

The sum of the measures of the angles of any triangle equals 180°.

Definition

Two lines are parallel if they do not intersect.

Prove:

> *If two lines are cut by a transversal such that a pair of interior angles are supplementary, then the lines are parallel.*

Prove: *If two lines are cut by a transversal such that a pair of interior angles are supplementary, then the lines are parallel.*

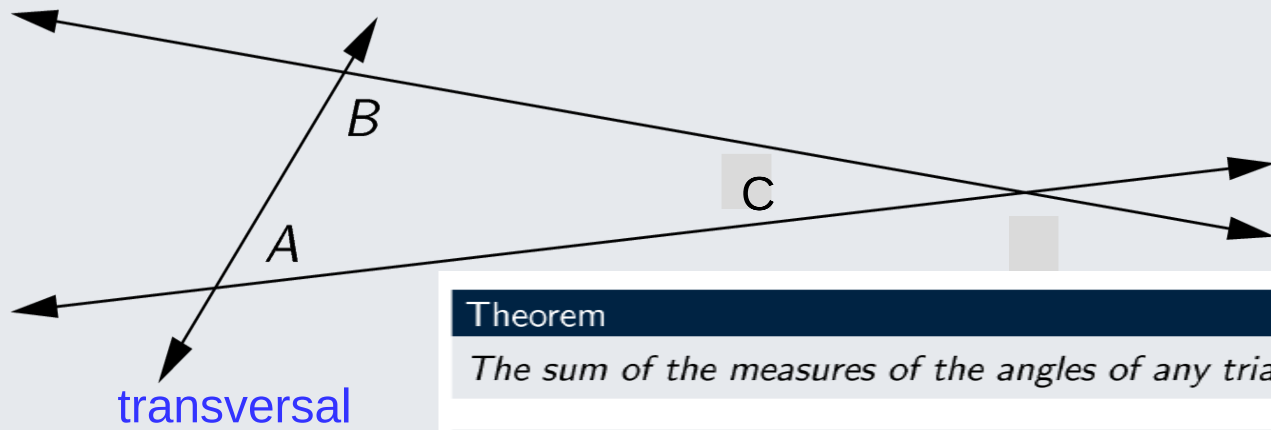
If two lines are cut by a transversal such that a pair of interior angles are supplementary, then the two lines do not intersect.

Definition

Two lines are parallel if they do not intersect.

Prove: *If two lines intersect, then a transversal will not cut them such that a pair of interior angles are supplementary.*

Proof If two lines intersect, then a transversal will make a triangle with them and, by the theorem, the sum of the three interior angles equals 180 degrees. Thus the pair of interior angles A and B are not supplementary.



Theorem

The sum of the measures of the angles of any triangle equals 180°.

Definition

Two lines are parallel if they do not intersect.

4. Proof by contradiction

To prove a statement A by contradiction, begin your proof with the following sentence.

Suppose, to the contrary, that $\neg A$.

Then argue, as in a direct proof, until you reach a contradiction.

contradiction

The above is the same as Gentzen's $\neg$-intro rule(proof by contradiction).

$$\frac{\Sigma, A \vdash B, \neg B}{\Sigma \vdash \neg A}$$

Example

Lemma

Let n be an integer. If n^2 is even, then n is even.

Proof.

To present a rigorous proof,
assume the definitions and the theorem in the following slide.

Definition

An integer n is even if $n = 2k$ for some integer k.

Definition

An integer n is odd if $n = 2k + 1$ for some integer k.

Theorem

For all integers n, $\neg(n \textit{ is even}) \Leftrightarrow (n \textit{ is odd})$.

Lemma

Let n be an integer. If n^2 is even, then n is even.

Proof.

What is your proof strategy?

Lemma

Let n be an integer. If n^2 is even, then n is even.

Proof.

Suppose <u>n^2 is even</u>. –(1)
Now to prove n is even, let's assume that <u>n is not even</u> – (2)
to use proof by contradiction. Then n is odd by the theorem below
and $n = 2*p + 1$ for some p.
Therefore $n^2 = (2*p+1)^2 = 4*p^2 + 4*p + 1 = 2*(2*P^2 +2*p) + 1$.
So n^2 is odd. Then, by the theorem below,
<u>n^2 must not be even.</u> –(3)
So we have a contradiction (1) and (3) due to the assumption (2).
Therefore (2) must be false and n must be even, as was to be proved.

Theorem

For all integers n, $\neg(n \text{ is even}) \Leftrightarrow (n \text{ is odd})$.

5. Disproof by giving a counterexample

A particular value of x that shows a statement of the form

$$(\forall x)P(x)$$

to be false is called a *counterexample* to the statement. A counterexample shows that the negation

$$(\exists x)\neg P(x)$$

is true.

Find a counterexample to the following statement.

For all sequences of numbers $a_1, a_2, a_3, \ldots$, if $a_1 < a_2 < a_3 < \cdots$, then some a_i must be positive.

Solution

Find a counterexample to the following statement.

> *For all sequences of numbers $a_1, a_2, a_3, \ldots$, if $a_1 < a_2 < a_3 < \cdots$, then some a_i must be positive.*

Solution

We need an example of a sequence that satisfies the "if" part of the statement and violates the "then" part. In other words, we need to find an increasing sequence that is always negative. Something with a horizontal asymptote will work: $a_n = -1/n$ is one example. Note that $-1 < -1/2 < -1/3 < \cdots$, but all the terms are less than zero.

Example. Let's assume that the domain of x be {1,2}.
P(x) can have one of the following interpretations:

	(1)	(2)	(3)	(4)
P(1)	T	T	F	F
P(2)	T	F	T	F

$\forall$x P(x) will be true only in case (1).
If we can find a model in which P is interpreted such that (2) or (3) or (4) is the case, then $\forall$x P(x) has been disproved.

☛ This approach can be generalized as in the next slide.

To prove that $\forall y \exists x\, P(x,y) \Rightarrow \exists x \forall y\, P(x,y)$ is invalid,

☛ Construct a **model** in which the premises are true and the conclusion is false.

Counterexample 1 (Finite & minimal domain).

The domain of x and y is {1,2}
P(x, y) has the following interpretation:

P(1,1)	T
P(1,2)	F
P(2,1)	F
P(2,2)	T

A model that makes $\forall y \exists x\, P(x,y)$ true and $\exists x \forall y\, P(x,y)$ false:

Counterexample 2 (Infinite domain).

$$\forall y \exists x\, (x > y) \overset{?}{\Rightarrow} \exists x \forall y\, (x > y)$$

In the domain $\mathbb{Z}$, if $P(x,y)$ is interpreted as $x > y$, then $\forall y \exists x\, (x > y)$ is true but $\exists x \forall y\, (x > y)$ is false.

Therefore, $\forall y \exists x\, P(x,y) \Rightarrow \exists x \forall y\, P(x,y)$ is invalid
And our failure to prove is not due to our lack of ingenuity
but it is due to the impossibility of deriving a proof
with any **sound** formal predicate logic system such as Gentzen's Natural Deduction

Quiz 09-1

Suppose that there are only two predicates P(x,y) and Q(x,y) to consider for modeling a given problem.

Assume that the domain of the variables x and y is {1,2}. How many different interpretations are possible?

(a) 16

(b) 64

(c) 256

(d) 1024

.