

MATHEMATICS 300 — SPRING 2010

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

(February 13, 2010)

1 THE BASIC LOGICAL RULES FOR FORMAL MATHEMATICAL PROOFS

TAUTOLOGIES AND CONTRADICTIONS. Before we list the basic rules, we need to discuss the concepts of “tautology” and “contradiction.”

Definition of “tautology”: A **tautology** is a propositional form \mathcal{F} that has the value “true” for every assignment of truth values to the propositional variables that occur in \mathcal{F} .

Definition of “instance of a tautology”: An **instance of a tautology** is a sentence that is obtained from a tautology \mathcal{T} by plugging in sentences for the propositional variables occurring in \mathcal{T} .

Definition of “contradiction”: A **contradiction** is a propositional form \mathcal{C} that has the value “false” for every assignment of truth values to the propositional variables that occur in \mathcal{C} .

Definition of “instance of a contradiction”: An **instance of a contradiction** is a sentence that is obtained from a contradiction \mathcal{C} by plugging in sentences for the propositional variables that occur in \mathcal{C} .

Examples:

- (1) The propositional form

$$A \vee (\sim A)$$

is a tautology.

- (2) The propositional form

$$(A \wedge (A \implies B)) \implies B$$

is a tautology. (Reason: how can $(A \wedge (A \implies B)) \implies B$ be false? For this to happen, B has to be false and $A \wedge (A \implies B)$ has to be true. For $A \wedge (A \implies B)$ to be true, A and $A \implies B$ have to be true. But then B has to be true, because if B was false, then $A \implies B$ would be false, since A is true. So B has to be both false and true, which is impossible.)

- (3) The statement

Obama will be reelected in 2012 or he will not

is an instance of a tautology, because it is of the form $A \vee (\sim A)$, and $A \vee (\sim A)$ is a tautology.

(4) The statement

$$a > 0 \vee (\sim a > 0)$$

is an instance of a tautology. because it is of the form $A \vee (\sim A)$, and $A \vee (\sim A)$ is a tautology.

(5) The statement

$$1 + 1 = 2$$

is true, but it is *not* an instance of a tautology, because it is of the form A , and A is not a tautology.

(6) The statement

If (a) you are a senior citizen, and (b) if you are
a senior citizen then you are entitled to a discount,
then you are entitled to a discount

is an instance of a tautology. because it is of the form $(A \wedge (A \implies B)) \implies B$, and $(A \wedge (A \implies B)) \implies B$ is a tautology.

(7) The propositional form

$$A \wedge (\sim A)$$

is a contradiction.

(8) The statement

Obama will be reelected and he will not be reelected

is an instance of a contradiction, because it is of the form $A \wedge (\sim A)$, and $A \wedge (\sim A)$ is contradiction.

(5) The statement

$$1 + 1 = 4$$

is false, but it is *not* an instance of a contradiction, because it is of the form A , and A is not a contradiction.

THE RULES OF LOGIC. And now we can get started listing the 14 basic rules of logic. You should think of these rules as being like “permitted moves” in a game like chess. That is, each rule gives you things that you are *allowed* to do, but this doesn’t mean that you have to do what the rule says.

The first ten rules correspond to the five *propositional connectives*

$$\sim, \vee, \wedge, \implies, \iff,$$

as follows:

- For each of the propositional connectives other than \sim there are two rules, a “use” rule and a “prove” rule, adding up to a total of eight..
- In addition, there is the *tautology proof rule* and the *proof by contradiction rule*.

1. The **tautology proof rule**. At any point in a proof, you are allowed to bring in, as a new step, any proposition which is an instance of a tautology.

2. The **proof by contradiction rule**. Let \mathcal{A} and \mathcal{C} be sentences, such that \mathcal{C} is a contradiction.

- (i) If you have started a subproof P' of a proof P with “Assume $\sim \mathcal{A}$ ” and have obtained \mathcal{C} in a step of P' , then you can exit P' and go to \mathcal{A} in P .

$$\begin{array}{l} \text{From} \\ \text{you can go to} \end{array} \left\{ \begin{array}{l} \vdots \\ \text{Assume } \sim \mathcal{A} \\ \vdots \\ \mathcal{C} \end{array} \right. \mathcal{A}$$

- (ii) If you have started a subproof P' of a proof P with “Assume \mathcal{A} ” and have obtained \mathcal{C} in a step of P' , then you can exit P' and go to $\sim \mathcal{A}$ in P .

$$\begin{array}{l} \text{From} \\ \text{you can go to} \end{array} \left\{ \begin{array}{l} \vdots \\ \text{Assume } \mathcal{A} \\ \vdots \\ \mathcal{C} \end{array} \right. \sim \mathcal{A}$$

3. **Rule \wedge_{use}** , or “rule for using a conjunction.” Let \mathcal{A} and \mathcal{B} be sentences.

(i) If you have $\mathcal{A} \wedge \mathcal{B}$ in a previous step of a proof, then you can go to \mathcal{A} :

From $\left\{ \begin{array}{l} \vdots \\ \mathcal{A} \wedge \mathcal{B} \\ \vdots \end{array} \right.$
you can go to \mathcal{A}

(ii) If you have $\mathcal{A} \wedge \mathcal{B}$ in a previous step of a proof, then you can go to \mathcal{B} :

From $\left\{ \begin{array}{l} \vdots \\ \mathcal{A} \wedge \mathcal{B} \\ \vdots \end{array} \right.$
you can go to \mathcal{B}

4. **Rule \wedge_{prove}** , or “**rule for proving a conjunction.**” Let \mathcal{A} and \mathcal{B} be sentences. If you have \mathcal{A} and \mathcal{B} in previous steps of a proof, then you can go to $\mathcal{A} \wedge \mathcal{B}$:

From $\left\{ \begin{array}{l} \vdots \\ \mathcal{A} \\ \vdots \\ \mathcal{B} \\ \vdots \end{array} \right.$
you can go to $\mathcal{A} \wedge \mathcal{B}$

5. **Rule \implies_{use}** , also known as **modus ponens**, or the “**rule for using an implication**”. Let \mathcal{A} and \mathcal{B} be sentences. If you have \mathcal{A} and $\mathcal{A} \implies \mathcal{B}$ in previous steps of a proof, then you can go to \mathcal{B} .

From $\left\{ \begin{array}{l} \vdots \\ \mathcal{A} \implies \mathcal{B} \\ \vdots \\ \mathcal{A} \\ \vdots \end{array} \right.$
you can go to \mathcal{B}

6. **Rule \implies_{prove}** , also known as the “**deduction rule**”, or “**rule for proving an implication**,” Let \mathcal{A} and \mathcal{B} be sentences. If you have started a subproof P' of a proof P with “Assume \mathcal{A} ” and have obtained \mathcal{B} in a step of

P' , then you can get out of P' and go to $\mathcal{A} \implies \mathcal{B}$ in P :

From $\left\{ \begin{array}{l} \vdots \\ \text{Assume } \mathcal{A} \\ \vdots \\ \mathcal{B} \end{array} \right.$
you can go to $\mathcal{A} \implies \mathcal{B}$

7. **Rule \vee_{use}** , also known as the “rule for using a disjunction,” or **rule of proof by cases**. Let \mathcal{A} , \mathcal{B} , \mathcal{C} , be sentences. If you have $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A} \implies \mathcal{C}$, $\mathcal{B} \implies \mathcal{C}$, in previous steps, then you can go to \mathcal{C} .

From $\left\{ \begin{array}{l} \vdots \\ \mathcal{A} \vee \mathcal{B} \\ \vdots \\ \mathcal{A} \implies \mathcal{C} \\ \vdots \\ \mathcal{B} \implies \mathcal{C} \\ \vdots \end{array} \right.$
you can go to \mathcal{C}

7a. **Another version of the proof by cases rule**. Let \mathcal{A} , \mathcal{B} , \mathcal{C} , be sentences. If, in a proof P ,

- (a) you have $\mathcal{A} \vee \mathcal{B}$,
- (b) you started a subproof P' of P with “Assume \mathcal{A} ” and obtained \mathcal{C} in a step of P' ,
- (c) you started a subproof P'' of P with “Assume \mathcal{B} ” and obtained \mathcal{C} in a step of P'' ,

then you can go back to P and write C as a step of P .

From $\left\{ \begin{array}{l} \vdots \\ \mathcal{A} \vee \mathcal{B} \\ \vdots \\ \text{Assume } \mathcal{A} \\ \vdots \\ \mathcal{C} \\ \vdots \\ \text{Assume } \mathcal{B} \\ \vdots \\ \mathcal{C} \end{array} \right.$
you can go to \mathcal{C}

8. **Rule \vee_{prove}** , also called the “rule for proving a disjunction.” Let \mathcal{A} and \mathcal{B} be sentences.

- (i) If you have proved $(\sim \mathcal{A}) \implies \mathcal{B}$ in a previous step, then you can go to $\mathcal{A} \vee \mathcal{B}$:

From $\left\{ \begin{array}{l} \vdots \\ (\sim \mathcal{A}) \implies \mathcal{B} \\ \vdots \end{array} \right.$
you can go to $\mathcal{A} \vee \mathcal{B}$

- (ii) If you have proved $(\sim \mathcal{B}) \implies \mathcal{A}$ in a previous step, then you can go to $\mathcal{A} \vee \mathcal{B}$.

From $\left\{ \begin{array}{l} \vdots \\ (\sim \mathcal{B}) \implies \mathcal{A} \\ \vdots \end{array} \right.$
you can go to $\mathcal{A} \vee \mathcal{B}$

9. **Rule \iff_{use}** , also known as the “rule for using a biconditional.” Let \mathcal{A} and \mathcal{B} be sentences.

- (i) If you have \mathcal{A} and $\mathcal{A} \iff \mathcal{B}$ in previous steps then you can go to \mathcal{B} :

From $\left\{ \begin{array}{l} \vdots \\ \mathcal{A} \\ \vdots \\ \mathcal{A} \iff \mathcal{B} \\ \vdots \end{array} \right.$
you can go to \mathcal{B}

(ii) If you have \mathcal{B} and $\mathcal{A} \iff \mathcal{B}$ in previous steps then you can go to \mathcal{A} :

From $\left\{ \begin{array}{l} \vdots \\ \mathcal{B} \\ \vdots \\ \mathcal{A} \iff \mathcal{B} \\ \vdots \end{array} \right.$
 you can go to \mathcal{A}

10. **Rule \iff_{prove}** , also known as the “rule for proving a biconditional.” Let \mathcal{A} and \mathcal{B} be sentences. If you have $\mathcal{A} \implies \mathcal{B}$ and $\mathcal{B} \implies \mathcal{A}$ in previous steps then you can go to $\mathcal{A} \iff \mathcal{B}$ in your proof:

From $\left\{ \begin{array}{l} \vdots \\ \mathcal{A} \implies \mathcal{B} \\ \vdots \\ \mathcal{B} \implies \mathcal{A} \\ \vdots \end{array} \right.$
 you can go to $\mathcal{A} \iff \mathcal{B}$

TERMS AND FREE VARIABLES. Before we state the four rules corresponding to the quantifiers (Rules \forall_{use} , \forall_{prove} , \exists_{use} and \exists_{prove}), we need to know what a *term* is, and we will also have to explain what a *free variable* is.

At each moment in a proof, some letter variables will have assigned values (which may be “arbitrary”) and others will not. A letter variable is *bound* if it has an assigned value and *free* if it not bound.

For example, if we say “let $x = 3$ ” or “let x be arbitrary”, then from that moment on x is bound, and we can no longer take x to be something else. The variable x can be unbound (i. e., made to become free again) by undoing the declaration of value, but this is usually only done when we need to use it with some other value. (For example, we may say “Let x be an arbitrary even integer,” and then go on until we no longer need this, and then we may say “Now let x be an arbitrary odd integer.” This makes the variable free for a brief moment, and then immediately gives it another value.) This can lead to all kinds of confusions, so I highly recommend that you do not reuse letter variables with different values within a proof.

A *term* is an expression that denotes a thing, object or entity. For example, “2” is a term, “ $1 + 2$ ” is a term, “ $a^2 + 3 + b$ ” is a term, “ $(a^2 + 3) \cdot b$ ” is a term, “ $\{x \in \mathbb{R} : x^2 > a\}$ ” is a term. But expressions such as “ $2 = 1 + 1$ ” or “ $a > 2$ ” or “ $a = +$ ” are not terms. (“ $2 = 1 + 1$ ” and “ $a > 2$ ” are sentences, and “ $a = +$ ” is just meaningless.) A term may contain letters as well as numbers or other fixed constants such as \emptyset .

A term for which all the letters or variable symbols have been assigned a value before is called a *constant term* (or *bound term*, if you prefer).

For example, “2” and “1+2” are constant terms, “ a^2+3+b ” and “ $(a^2+3)\cdot b$ ” are constant terms, if a and b have been assigned values before, and “ $\{x \in \mathbb{R} : x^2 > a\}$ ” is a constant term, if a has been assigned a value before. (Why don’t I require x to have been assigned a value before? Because it’s a dummy variable!)

THE RULES FOR \forall and \exists . There will be two rules for each of the quantifiers, a use rule and a prove rule. This will give us a total of four rules for the two quantifiers. Together with the ten rules we had before, we will end up with fourteen rules.

In stating our rules for the quantifiers, we will use the following notation:

- Whenever we write $\mathcal{A}(x)$, it will be understood that $\mathcal{A}(x)$ is a statement where x is a variable and there is no quantifier involving x .
- If t is a constant term then $\mathcal{A}(t)$ (which you can read as “ \mathcal{A} with t plugged in for x ”, or “ \mathcal{A} of t ”) is the statement that you get from $\mathcal{A}(x)$ by substituting t for x in **all** the occurrences of x in $\mathcal{A}(x)$.

For example, $\mathcal{A}(x)$ could be “ $(x+a)^2 = x^2 + 2ax + a^2$ ”, and t could be “ $b-a$ ”, in which case $\mathcal{A}(t)$ would be “ $((b-a)+a)^2 = (b-a)^2 + 2a(b-a) + a^2$ ”.

11. **Rule \forall_{use}** , also known as the “rule for using a universal statement,” or **specialization rule**.

- (i) If you have $(\forall x)\mathcal{A}(x)$ in a previous step, you can go to $\mathcal{A}(t)$:

$$\begin{array}{l} \text{From} \\ \text{you can go to} \end{array} \left\{ \begin{array}{l} \vdots \\ (\forall x)\mathcal{A}(x) \\ \vdots \end{array} \right. \mathcal{A}(t)$$

- (ii) If S is a set, and you have $(\forall x \in S)\mathcal{A}(x)$ and $t \in S$ in previous steps, then you can go to $\mathcal{A}(t)$:

$$\begin{array}{l} \text{From} \\ \text{you can go to} \end{array} \left\{ \begin{array}{l} \vdots \\ (\forall x \in S)\mathcal{A}(x) \\ \vdots \\ t \in S \\ \vdots \end{array} \right. \mathcal{A}(t)$$

An example for Rule \forall_{use} . If you know that “All Rutgers professors are very smart”, and “H. Sussmann is a Rutgers professor,” you can conclude that “H. Sussmann is very smart.”

12. **Rule \forall_{prove}** , also known as the “rule for proving a universal statement”, or **universal generalization rule**.

- (i) Suppose you are in a proof P (which may be itself be a subproof of some other proof) and you have started a subproof P' of P by saying “Let a be arbitrary,” and that until that point a had never appeared in P . Suppose that in P' you got to $\mathcal{A}(a)$. Then you can get out of P' and go to $(\forall x)\mathcal{A}(x)$ in P :

From $\left\{ \begin{array}{l} \vdots \\ \text{Let } a \text{ be arbitrary} \\ \vdots \\ \mathcal{A}(a) \end{array} \right.$
you can go to $(\forall x)\mathcal{A}(x)$.

- (ii) Suppose that S is a set, you are in a proof P (which may be itself be a subproof of some other proof) and you have started a subproof P' of P by saying “Let $a \in S$ be arbitrary,” and that until that point a had never appeared in P . Suppose that in P' you got to $\mathcal{A}(a)$. Then you can get out of P' and go to $(\forall x \in S)\mathcal{A}(x)$ in P .

From $\left\{ \begin{array}{l} \vdots \\ S \text{ is a set} \\ \vdots \\ \text{Let } a \in S \text{ be arbitrary} \\ \vdots \\ \mathcal{A}(a) \end{array} \right.$
you can go to $(\forall x \in S)\mathcal{A}(x)$.

An example for Rule \forall_{prove} . If you start with “Let a be an arbitrary integer”, and prove that $6|a^3 - a$, then you can conclude that $(\forall x \in \mathbb{Z})(6|x^3 - x)$.

13. **Rule \exists_{use}** , also known as the “rule for using an existential statement,” or the **picking a witness rule**.

- (i) Suppose you have proved $(\exists x)\mathcal{A}(x)$. Then you can introduce a constant w and stipulate that $\mathcal{A}(w)$, by saying “pick a witness w for $(\exists x)\mathcal{A}(x)$, so $\mathcal{A}(w)$, provided that the symbol w has not been assigned a value before.

From $\left\{ \begin{array}{l} \vdots \\ (\exists x)\mathcal{A}(x) \\ \vdots \end{array} \right.$
you can go to Pick a witness w for $(\exists x)\mathcal{A}(x)$, so $\mathcal{A}(w)$.

- (ii) Suppose you have proved $(\exists x \in S)\mathcal{A}(x)$. Then you can introduce a constant w and stipulate that $w \in S \wedge \mathcal{A}(w)$, by saying “pick a witness w for $(\exists x \in S)\mathcal{A}(x)$, so $w \in S \wedge \mathcal{A}(w)$, provided that the symbol w has not been assigned a value before.

From
$$\left\{ \begin{array}{l} \vdots \\ (\exists x \in S)\mathcal{A}(x) \\ \vdots \end{array} \right.$$
 you can go to Pick a witness w for $(\exists x \in S)\mathcal{A}(x)$, so $w \in S \wedge \mathcal{A}(w)$.

Examples for Rule \exists_{use} . Once we have established that somebody will win the next election, we can give a name to the person who will win, for example by calling him/her “the winner.”

Once we have established that $(\exists x \in \mathbb{R})(x^3 - x = 0)$, we can say “pick a real number a which is a solution of $x^3 - x = 0$, so $a^3 - a = 0$.”

14. **Rule \exists_{prove}** , also known as the “rule for proving an existential statement,” or the **proof by giving an example rule**, or, perhaps easiest to remember, the **using a witness rule**.

- (i) Suppose you have proved $\mathcal{A}(t)$. Then you can go to $(\exists x)\mathcal{A}(x)$.
- (ii) Suppose you have proved $t \in S \wedge \mathcal{A}(t)$. Then you can go to $(\exists x \in S)\mathcal{A}(x)$.

Examples for Rule \exists_{prove} . If you have found a cow, and called her “Clarabella”, then from the fact that “Clarabella is a cow” you can go to the assertion that $(\exists x)(x \text{ is a cow})$, that is, to “there are cows.”

Once you have shown that $\sqrt{2} \in \mathbb{R}$ and $\sqrt{2}$ is irrational, you can conclude that $(\exists x \in \mathbb{R})(x \text{ is irrational})$, that is, that there are irrational numbers.

A comment. In the previous example, we proved that cows exist by the simple procedure of giving an example of a cow. Similarly, we showed that irrational numbers exist by giving one example of an irrational number.

Some students claim that they have been told somewhere, maybe by some teacher, that “you cannot prove things by giving examples.” This is plain silly, besides being awfully vague. Their key point here is that, if you were told something like this, whoever told you did not use the word “things.” Some “things” can be proved by giving examples, others cannot. More precisely: *existential statements can be proved by giving examples*, as we have just done. But *universal statements cannot be proved by giving examples*. For example, I cannot establish that all cows are white by showing you one (or two, or ten thousand) white cows. And I cannot prove that all real numbers are rational by giving you one (or two, or ten thousand) rational numbers.