Economics 204 Summer/Fall 2016
Lecture 1–Monday July 25, 2016

Section 1.2. Methods of Proof

We begin by looking at the notion of proof. What is a proof? "Proof" has a formal definition in mathematical logic, and a formal proof is long and unreadable. In practice, you need to learn to recognize a proof when you see one.

We will begin by discussing four main methods of proof that you will encounter frequently:

- deduction
- contraposition
- induction
- contradiction

We look at each in turn.

Proof by Deduction:

A proof by deduction is composed of a list of statements, the last of which is the statement to be proven. Each statement in the list is either

- an axiom: a fundamental assumption about mathematics, or part of definition of the object under study; or
- a previously established theorem; or
- follows from previous statements in the list by a valid rule of inference

Example: Prove that the function $f(x) = x^2$ is continuous at $x = 5$.

Recall from one-variable calculus that $f(x) = x^2$ is continuous at $x = 5$ means

$$\forall \varepsilon > 0 \ \exists \delta > 0 \text{ s.t. } |x - 5| < \delta \Rightarrow |f(x) - f(5)| < \varepsilon$$

That is, "for every $\varepsilon > 0$ there exists a $\delta > 0$ such that whenever x is within δ of 5, $f(x)$ is within ε of $f(5)$."

To prove the claim, we must systematically verify that this definition is satisfied.

Proof: Let $\varepsilon > 0$ be given. Let

$$\delta = \min\left\{1, \frac{\varepsilon}{11}\right\} > 0$$

Why??

Suppose $|x-5| < \delta$. Since $\delta \leq 1$, $4 < x < 6$, so $9 < x+5 < 11$ and $|x+5| < 11$. Then

$$\begin{aligned} |f(x) - f(5)| &= |x^2 - 25| \\ &= |(x+5)(x-5)| \\ &= |x+5||x-5| \\ &< 11 \cdot \delta \\ &\leq 11 \cdot \frac{\varepsilon}{11} \\ &= \varepsilon \end{aligned}$$

Thus, we have shown that for every $\varepsilon > 0$, there exists $\delta > 0$ such that $|x-5| < \delta \Rightarrow |f(x) - f(5)| < \varepsilon$, so $f(x) = x^2$ is continuous at $x = 5$. ■

Proof by Contraposition:

First recall some basics of logic.

$\neg P$ means "P is false."

$P \wedge Q$ means "P is true *and* Q is true."

$P \vee Q$ means "P is true *or* Q is true (or possibly both)."

$\neg P \wedge Q$ means $(\neg P) \wedge Q$; $\neg P \vee Q$ means $(\neg P) \vee Q$.

$P \Rightarrow Q$ means "whenever P is satisfied, Q is also satisfied."

Formally, $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$.

The *contrapositive* of the statement $P \Rightarrow Q$ is the statement

$$\neg Q \Rightarrow \neg P$$

These are logically equivalent, as we prove below.

Theorem 1 *$P \Rightarrow Q$ is true if and only if $\neg Q \Rightarrow \neg P$ is true.*

Proof: Suppose $P \Rightarrow Q$ is true. Then either P is false, or Q is true (or possibly both). Therefore, either $\neg P$ is true, or $\neg Q$ is false (or possibly both), so $\neg(\neg Q) \vee (\neg P)$ is true, $\neg Q \Rightarrow \neg P$ is true.

Conversely, suppose $\neg Q \Rightarrow \neg P$ is true. Then either $\neg Q$ is false, or $\neg P$ is true (or possibly both), so either Q is true, or P is false (or possibly both), so $\neg P \vee Q$ is true, so $P \Rightarrow Q$ is true. ■

So to prove a statement $P \Rightarrow Q$, it is equivalent to prove the contrapositive $\neg Q \Rightarrow \neg P$. See de la Fuente for an example of the use of proof by contraposition.

Proof by Induction:

We illustrate with an example.

Theorem 2 *For every* $n \in \mathbf{N}_0 = \{0, 1, 2, 3, \ldots\}$,

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

i.e. $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Proof:
Base step $n = 0$: The left hand side (LHS) above $= \sum_{k=1}^{0} k =$ the empty sum $= 0$. The right hand side (RHS) $= \frac{0 \cdot 1}{2} = 0$ so the claim is true for $n = 0$.

Induction step: Suppose

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \text{ for some } n \geq 0$$

We must show that

$$\sum_{k=1}^{n+1} k = \frac{(n+1)((n+1)+1)}{2}$$

$$\begin{aligned}
\text{LHS} &= \sum_{k=1}^{n+1} k \\
&= \sum_{k=1}^{n} k + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \text{ by the Induction hypothesis} \\
&= (n+1)\left(\frac{n}{2} + 1\right) \\
&= \frac{(n+1)(n+2)}{2} \\
\text{RHS} &= \frac{(n+1)((n+1)+1)}{2} \\
&= \frac{(n+1)(n+2)}{2} \\
&= \text{LHS}
\end{aligned}$$

so by mathematical induction, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for all $n \in \mathbf{N}_0$. ■

Proof by Contradiction:

A proof by contradiction proves a statement by assuming its negation is true and working until reaching a contradiction. Again we illustrate with an example.

Theorem 3 *There is no rational number q such that $q^2 = 2$.*

Proof: Suppose $q^2 = 2$, $q \in \mathbf{Q}$. We can write $q = \frac{m}{n}$ for some integers $m, n \in \mathbf{Z}$. Moreover, we can assume that m and n have no common factor; if they did, we could divide it out.[1]

$$2 = q^2 = \frac{m^2}{n^2}$$

Therefore, $m^2 = 2n^2$, so m^2 is even.

We claim that m is even. If not[2], then m is odd, so $m = 2p + 1$ for some $p \in \mathbf{Z}$. Then

$$\begin{aligned} m^2 &= (2p+1)^2 \\ &= 4p^2 + 4p + 1 \\ &= 2(2p^2 + 2p) + 1 \end{aligned}$$

which is odd, contradiction. Therefore, m is even, so $m = 2r$ for some $r \in \mathbf{Z}$.

$$\begin{aligned} 4r^2 &= (2r)^2 \\ &= m^2 \\ &= 2n^2 \\ n^2 &= 2r^2 \end{aligned}$$

so n^2 is even, which implies (by the argument given above) that n is even. Therefore, $n = 2s$ for some $s \in \mathbf{Z}$, so m and n have a common factor, namely 2, contradiction. Therefore, there is no rational number q such that $q^2 = 2$. ■

Section 1.3 Equivalence Relations

Definition 4 A *binary relation* R from X to Y is a subset $R \subseteq X \times Y$. We write xRy if $(x, y) \in R$ and "not xRy" if $(x, y) \notin R$. $R \subseteq X \times X$ is a *binary relation on* X.

Example: Suppose $f : X \to Y$ is a function from X to Y. The binary relation $R \subseteq X \times Y$ defined by

$$xRy \iff f(x) = y$$

[1] This is actually a subtle point. We are using the fact that the expression of a natural number as a product of primes is unique.

[2] This is a proof by contradiction within a proof by contradiction!

is exactly the graph of the function f. A function can be considered a binary relation R from X to Y such that for each $x \in X$ there exists exactly one $y \in Y$ such that $(x, y) \in R$.

Example: Suppose $X = \{1, 2, 3\}$ and R is the binary relation on X given by $R = \{(1, 1), (2, 1), (2, 2), (3, 1), (3, 2), (3, 3)\}$. This is the binary relation "is weakly greater than," or $\geq$.

Definition 5 A binary relation R on X is

(i) *reflexive* if $\forall x \in X, xRx$

(ii) *symmetric* if $\forall x, y \in X, xRy \Leftrightarrow yRx$

(iii) *transitive* if $\forall x, y, z \in X, (xRy \wedge yRz) \Rightarrow xRz$

Definition 6 A binary relation R on X is an *equivalence relation* if it is reflexive, symmetric and transitive.

Definition 7 Given an equivalence relation R on X, write

$$[x] = \{y \in X : xRy\}$$

$[x]$ is called the *equivalence class containing* x.

The set of equivalence classes is the *quotient* of X with respect to R, denoted X/R.

Example: The binary relation $\geq$ on $\mathbf{R}$ is not an equivalence relation because it is not symmetric.

Example: Let $X = \{a, b, c, d\}$ and $R = \{(a, a), (a, b), (b, a), (b, b), (c, c), (c, d), (d, c), (d, d)\}$. R is an equivalence relation (why?) and the equivalence classes of R are $\{a, b\}$ and $\{c, d\}$. $X/R = \{\{a, b\}, \{c, d\}\}$

The following theorem shows that the equivalence classes of an equivalence relation form a *partition* of X: every element of X belongs to exactly one equivalence class.

Theorem 8 *Let R be an equivalence relation on X. Then $\forall x \in X, x \in [x]$.*

Given $x, y \in X$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

Proof: If $x \in X$, then xRx because R is reflexive, so $x \in [x]$.

Suppose $x, y \in X$. If $[x] \cap [y] = \emptyset$, we're done. So suppose $[x] \cap [y] \neq \emptyset$. We must show that $[x] = [y]$, i.e. that the elements of $[x]$ are exactly the same as the elements of $[y]$.

Choose $z \in [x] \cap [y]$. Then $z \in [x]$, so xRz. By symmetry, zRx. Also $z \in [y]$, so yRz. By symmetry again, zRy. Now choose $w \in [x]$. By definition, xRw. Since zRx and R is transitive, zRw. By symmetry, wRz. Since zRy, wRy by transitivity again. By symmetry, yRw, so $w \in [y]$, which shows that $[x] \subseteq [y]$.
Similarly, $[y] \subseteq [x]$, so $[x] = [y]$.$\blacksquare$

Section 1.4 Cardinality

Definition 9 Two sets A, B are *numerically equivalent* (or *have the same cardinality*) if there is a bijection $f : A \to B$, that is, a function $f : A \to B$ that is 1-1 ($a \neq a' \Rightarrow f(a) \neq f(a')$), and onto ($\forall b \in B\ \exists a \in A$ s.t. $f(a) = b$).

Roughly speaking, if two sets have the same cardinality then elements of the sets can be uniquely matched up and paired off.

A set is either finite or infinite. A set is *finite* if it is numerically equivalent to $\{1, \ldots, n\}$ for some n. A set that is not finite is *infinite*.

For example, the set $A = \{2, 4, 6, \ldots, 50\}$ is numerically equivalent to the set $\{1, 2, \ldots, 25\}$ under the function $f(n) = 2n$. In particular, this shows that A is finite. The set $B = \{1, 4, 9, 16, 25, 36, 49 \ldots\} = \{n^2 : n \in \mathbf{N}\}$ is numerically equivalent to $\mathbf{N}$ and is infinite.

An infinite set is either countable or uncountable. A set is *countable* if it is numerically equivalent to the set of natural numbers $\mathbf{N} = \{1, 2, 3, \ldots\}$. An infinite set that is not countable is called *uncountable*.

Example: The set of integers $\mathbf{Z}$ is countable.

$$\mathbf{Z} = \{0, 1, -1, 2, -2, \ldots\}$$

Define $f : \mathbf{N} \to \mathbf{Z}$ by

$$\begin{aligned}
f(1) &= 0 \\
f(2) &= 1 \\
f(3) &= -1 \\
&\vdots \\
f(n) &= (-1)^n \left\lfloor \frac{n}{2} \right\rfloor
\end{aligned}$$

where $\lfloor x \rfloor$ is the greatest integer less than or equal to x. It is straightforward to verify that f is one-to-one and onto.

Notice $\mathbf{Z} \supset \mathbf{N}$ but $\mathbf{Z} \neq \mathbf{N}$; indeed, $\mathbf{Z} \setminus \mathbf{N}$ is infinite! So statements like "One half of the elements of $\mathbf{Z}$ are in $\mathbf{N}$" are not meaningful.

Theorem 10 *The set of rational numbers* $\mathbf{Q}$ *is countable.*

"Picture Proof":

$$
\begin{aligned}
\mathbf{Q} &= \left\{ \frac{m}{n} : m, n \in \mathbf{Z}, n \neq 0 \right\} \\
&= \left\{ \frac{m}{n} : m \in \mathbf{Z}, n \in \mathbf{N} \right\}
\end{aligned}
$$

$$
\begin{array}{cc|ccccccccc}
 & & & & & & m & & & & \\
 & & 0 & & 1 & & -1 & & 2 & & -2 \\
\hline
 & 1 & 0 & \rightarrow & 1 & & -1 & \rightarrow & 2 & & -2 \\
 & & & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
 & 2 & 0 & & \frac{1}{2} & & -\frac{1}{2} & & 1 & & -1 \\
 & & \downarrow & \nearrow & & \swarrow & & \nearrow & & & \\
n & 3 & 0 & & \frac{1}{3} & & -\frac{1}{3} & & \frac{2}{3} & & -\frac{2}{3} \\
 & & & \swarrow & & \nearrow & & & & & \\
 & 4 & 0 & & \frac{1}{4} & & -\frac{1}{4} & & \frac{1}{2} & & -\frac{1}{2} \\
 & & \downarrow & \nearrow & & & & & & & \\
 & 5 & 0 & & \frac{1}{5} & & -\frac{1}{5} & & \frac{2}{5} & & -\frac{2}{5}
\end{array}
$$

Go back and forth on upward-sloping diagonals, omitting the repeats:

$$
\begin{aligned}
f(1) &= 0 \\
f(2) &= 1 \\
f(3) &= \frac{1}{2} \\
f(4) &= -1 \\
&\vdots
\end{aligned}
$$

$f : \mathbf{N} \rightarrow \mathbf{Q}$, f is one-to-one and onto.

Notice that although $\mathbf{Q}$ appears to be much larger than $\mathbf{N}$, in fact they are the same size.