Predicate Calculus Validity

Propositional validity

$$(A \rightarrow B) \vee (B \rightarrow A)$$

True ***no matter what*** the truth values of *A* and *B* are

Predicate calculus validity

$$\forall z\, [Q(z) \wedge P(z)] \rightarrow [\forall x. Q(x) \wedge \forall y. P(y)]$$

True ***no matter what***

- the Domain is,
- or the predicates are.

That is, logically correct, independent of the specific content.

Arguments with Quantified Statements

Universal instantiation:

$$\forall x, P(x)$$
$$\therefore\ P(a)$$

Universal modus ponens:

$$\forall x, P(x) \rightarrow Q(x)$$
$$P(a)$$
$$\therefore\ Q(a)$$

Universal modus tollens:

$$\forall x, P(x) \rightarrow Q(x)$$
$$\neg Q(a)$$
$$\therefore\ \neg P(a)$$

Universal Generalization

valid rule

$$\frac{A \rightarrow R(c)}{A \rightarrow \forall x.R(x)}$$

providing c is independent of *A*

Informally, if we could prove that R(c) is true for an arbitrary c
(in a sense, c is a "variable"), then we could prove the for all statement.

e.g. given any number c, 2c is an even number

=> for all x, 2x is an even number.

Remark: Universal generalization is often difficult to prove, we will introduce mathematical induction to prove the validity of for all statements.

Valid Rule?

$$\forall z\,[Q(z) \vee P(z)] \rightarrow [\forall x.Q(x) \vee \forall y.P(y)]$$

Proof: Give **countermodel**, where

$\forall z\,[Q(z) \vee P(z)]$ is true,

but $\forall x.Q(x) \vee \forall y.P(y)$ is false.

Find a domain,
and a predicate.

In this example, let domain be integers,

$Q(z)$ be true if z is an even number, i.e. Q(z)=even(z)

$P(z)$ be true if z is an odd number, i.e. P(z)=odd(z)

Then $\forall z\,[Q(z) \vee P(z)]$ is true, because every number is either even or odd.

But $\forall x.Q(x)$ is not true, since not every number is an even number.

Similarly $\forall y.P(y)$ is not true, and so $\forall x.Q(x) \vee \forall y.P(y)$ is not true.

Valid Rule?

$$\forall z \in D \quad [Q(z) \wedge P(z)] \rightarrow [\forall x \quad Q(x) \wedge \forall y\, P(y)]$$

Proof: Assume $\forall z\, [Q(z) \wedge P(z)]$.

So $Q(z) \wedge P(z)$ holds for all z in the domain D.

Now let c be some element in the domain D.

So $Q(c) \wedge P(c)$ holds (by instantiation), and therefore $Q(c)$ by itself holds.

But c could have been any element of the domain D.

So we conclude $\forall x.Q(x)$. (by generalization)

We conclude $\forall y.P(y)$ similarly (by generalization). Therefore,

$$\forall x.Q(x) \wedge \forall y.P(y)$$ QED.

This Lecture

Now we have learnt the basics in logic.

We are going to apply the logical rules in proving mathematical theorems.

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

Basic Definitions

An integer n is an even number
if there exists an integer k such that $n = 2k$.

An integer n is an odd number
if there exists an integer k such that $n = 2k+1$.

Proving an Implication

Goal: If P, then Q. (P implies Q)

Method 1: Write assume P, then show that Q logically follows.

Claim: If $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$

Reasoning: When x=0, it is true.

When x grows, 4x grows faster than x^3 in that range.

Proof: $-x^3 + 4x + 1 = x(2-x)(2+x) + 1$

When $0 \leq x \leq 2$, $x(2-x)(2+x) \geq 0$ $\square$

Direct Proofs

The sum of two even numbers is even.

Proof

$$x = 2m, y = 2n$$

$$x+y = 2m+2n$$

$$= 2(m+n)$$

The product of two odd numbers is odd.

Proof

$$x = 2m+1, y = 2n+1$$

$$xy = (2m+1)(2n+1)$$

$$= 4mn + 2m + 2n + 1$$

$$= 2(2mn+m+n) + 1.$$

Divisibility

a "divides" b $(a|b)$:

$b = ak$ for some integer k

$5|15$ because $15 = 3\times5$

$n|0$ because $0 = n\times0$

$1|n$ because $n = 1\times n$

$n|n$ because $n = n\times1$

A number $p > 1$ with no positive integer divisors other than 1 and itself is called a **prime**. Every other number greater than 1 is called **composite**.

2, 3, 5, 7, 11, and 13 are prime,

4, 6, 8, and 9 are composite.

Simple Divisibility Facts

1. If $a \mid b$, then $a \mid bc$ for all c.
2. If $a \mid b$ and $b \mid c$, then $a \mid c$.
3. If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$ for all s and t.
4. For all $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.

Proof of (1)

$a \mid b$

$\Rightarrow \quad b = ak$

$\Rightarrow \quad bc = ack$

$\Rightarrow \quad bc = a(ck)$

$\Rightarrow \quad a|bc$

a "divides" b $\quad (a|b)$:

$b = ak$ for some integer k

Simple Divisibility Facts

1. If $a \mid b$, then $a \mid bc$ for all c.
2. If $a \mid b$ and $b \mid c$, then $a \mid c$.
3. If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$ for all s and t.
4. For all $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.

Proof of (2)

$a \mid b \Rightarrow b = ak_1$

$b \mid c \Rightarrow c = bk_2$

$\Rightarrow c = ak_1k_2$

$\Rightarrow a \mid c$

a "divides" b (a|b):

b = ak for some integer k

Simple Divisibility Facts

1. If $a \mid b$, then $a \mid bc$ for all c.
2. If $a \mid b$ and $b \mid c$, then $a \mid c$.
3. If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$ for all s and t.
4. For all $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.

Proof of (3)

$a \mid b \Rightarrow b = ak_1$

$a \mid c \Rightarrow c = ak_2$

$sb + tc$

$= sak_1 + tak_2$

$= a(sk_1 + tk_2)$

$\Rightarrow a \mid (sb+tc)$

a "divides" b ($a|b$):

$b = ak$ for some integer k

This Lecture

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

Proving an Implication

Goal: If P, then Q. (P implies Q)

Method 1: Write assume P, then show that Q logically follows.

Claim: If r is irrational, then √r is irrational.

How to begin with?

What if I prove "If √r is rational, then r is rational", is it equivalent?

Yes, this is equivalent;
proving "if P, then Q" is equivalent to proving "if not Q, then not P".

Rational Number

R is rational ⇔ there are integers a and b such that

numerator → a

$$r = \frac{a}{b}$$ and $b \neq 0$.

denominator → b

Is 0.281 a rational number? Yes, 281/1000

Is 0 a rational number? Yes, 0/1

If m and n are non-zero integers, is (m+n)/mn a rational number? Yes

Is the sum of two rational numbers a rational number? Yes, a/b+c/d=(ad+bc)/bd

Is x=0.12121212…… a rational number? Note that 100x-x=12, and so x=12/99.

Proving an Implication

Goal: If P, then Q. (P implies Q)

Method 2: Prove the ***contrapositive***, i.e. prove "not Q implies not P".

Claim: If r is irrational, then $\sqrt{r}$ is irrational.

Proof:

We shall prove the contrapositive –

"if $\sqrt{r}$ is rational, then r is rational."

Since $\sqrt{r}$ is rational, $\sqrt{r} = a/b$ for some integers a,b.

So $r = a^2/b^2$. Since a,b are integers, a^2, b^2 are integers.

Therefore, r is rational. □ Q.E.D.

(Q.E.D.) "which was to be demonstrated", or "quite easily done". ☺

Proving an "if and only if"

Goal: Prove that two statements P and Q are "**logically equivalent**",
that is, one holds if and only if the other holds.

Example:

An integer is even if and only if the its square is even.

Method 1: Prove P implies Q **and** Q implies P.

Method 1': Prove P implies Q **and** not P implies not Q.

Method 2: Construct a chain of if and only if statement.

Proof the Contrapositive

An integer is even if and only if its square is even.

Method 1: Prove P implies Q **and** Q implies P.

Statement: If m is even, then m^2 is even

Proof: $m = 2k$

$m^2 = 4k^2$

Statement: If m^2 is even, then m is even

Proof: $m^2 = 2k$

$m = \sqrt{(2k)}$

??

Proof the Contrapositive

An integer is even if and only if its square is even.

Method 1': Prove P implies Q **and** not P implies not Q.

Statement: If m^2 is even, then m is even

Contrapositive: If m is odd, then m^2 is odd.

Proof (the contrapositive):

Since m is an odd number, $m = 2k+1$ for some integer k.

So $m^2 = (2k+1)^2$

$= (2k)^2 + 2(2k) + 1$

So m^2 is an odd number.

This Lecture

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

Proof by Contradiction

$$\frac{\bar{P} \rightarrow \mathrm{F}}{P}$$

To prove P, you prove that not P would lead to ridiculous result,

and so P must be true.

You are working as a clerk.

If you have won the lottery, then you would not work as a clerk.

$\therefore$ You have not won the lottery.

Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.

Proof (by contradiction):

- Suppose $\sqrt{2}$ was rational.
- Choose *m*, *n* integers without common prime factors (always possible)

  such that $\sqrt{2} = \dfrac{m}{n}$

- Show that *m* and *n* are both even, thus having a common factor 2,

  a **contradiction**!

Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.

Proof (by contradiction):

Want to prove both m and n are even.

$$\sqrt{2} = \frac{m}{n}$$

$$\sqrt{2}n = m$$

$$2n^2 = m^2$$

so *m* is even.

so can assume $m = 2l$

$$m^2 = 4l^2$$

$$2n^2 = 4l^2$$

$$n^2 = 2l^2$$

so *n* is even.

Infinitude of the Primes

Theorem. There are infinitely many prime numbers.

Proof (by contradiction):

Assume there are only finitely many primes.

Let $p_1, p_2, \ldots, p_N$ be all the primes.

We will construct a number N so that N is not divisible by any p_i.

By our assumption, it means that N is not divisible by any prime number.

On the other hand, we show that any number must be divisible by *some* prime.

It leads to a contradiction, and therefore the assumption must be false.

So there must be infinitely many primes.

Divisibility by a Prime

Theorem. Any integer $n > 1$ is divisible by a prime number.

- Let n be an integer.
- If n is a prime number, then we are done.
- Otherwise, $n = ab$, both are smaller than n.
- If a or b is a prime number, then we are done.
- Otherwise, $a = cd$, both are smaller than a.
- If c or d is a prime number, then we are done.
- Otherwise, repeat this argument, since the numbers are getting smaller and smaller, this will eventually stop and we have found a prime factor of n.

Idea of induction.

Infinitude of the Primes

Theorem. There are infinitely many prime numbers.

Proof (by contradiction):

Let $p_1, p_2, \ldots, p_N$ be all the primes.

Consider $p_1p_2\ldots p_N + 1$.

Claim: if p divides a, then p does not divide a+1.

Proof (by contradiction):

a = cp for some integer c

a+1 = dp for some integer d

=> 1 = (d-c)p, contradiction because p>=2.

So none of $p_1, p_2, \ldots, p_N$ can divide $p_1p_2\ldots p_N + 1$, a contradiction.

This Lecture

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

Proof by Cases

$$p \vee q$$
$$p \rightarrow r$$
$$q \rightarrow r$$
$$\therefore\ r$$

e.g. want to prove a nonzero number always has a positive square.

x is positive or x is negative

if x is positive, then $x^2 > 0$.

if x is negative, then $x^2 > 0$.

$\therefore\ x^2 > 0$.

The Square of an Odd Integer

$$\forall \text{ odd } n, \exists m, n^2 = 8m + 1?$$

Idea 0: find counterexample.

$3^2 = 9 = 8+1$, $5^2 = 25 = 3\times8+1$ …… $131^2 = 17161 = 2145\times8 + 1$, ………

Idea 1: prove that $n^2 - 1$ is divisible by 8.

$n^2 - 1 = (n-1)(n+1) = $??…

Idea 2: consider $(2k+1)^2$

$(2k+1)^2 = 4k^2+4k+1$

If k is even, then both k^2 and k are even, and so we are done.

If k is odd, then both k^2 and k are odd, and so k^2+k even, also done.

Trial and Error Won't Work!

Fermat (1637): If an integer n is greater than 2,

then the equation $a^n + b^n = c^n$ has no solutions in non-zero integers a, b, and c.

Claim: $313(a^3 + b^3) = c^3$ has no solutions in non-zero integers a, b, and c.

False. But smallest counterexample has more than 1000 digits.

Euler conjecture:

$a^4 + b^4 + c^4 = d^4$ has no solution for a,b,c,d positive integers.

Open for 218 years, until Noam Elkies found

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

The Square Root of an Even Square

Statement: If m^2 is even, then m is even

Contrapositive: If m is odd, then m^2 is odd.

Proof (the contrapositive):

Since m is an odd number, $m = 2l+1$ for some natural number l.

So $m^2 = (2l+1)^2$

$= (2l)^2 + 2(2l) + 1$

So m^2 is an odd number.

Proof by contrapositive.

Rational vs Irrational

Question: If a and b are irrational, can a^b be rational??

We know that $\sqrt{2}$ is irrational, what about $\sqrt{2}^{\sqrt{2}}$?

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational

Then we are done, $a=\sqrt{2}$, $b=\sqrt{2}$.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational

Then $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$, a rational number

So $a=\sqrt{2}^{\sqrt{2}}$, $b= \sqrt{2}$ will do.

So in either case there are a,b irrational and a^b be rational.

We don't (need to) know which case is true!

Summary

We have learnt different techniques to prove mathematical statements.

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

Next time we will focus on a very important technique, proof by induction.