Discrete Math

Basic of Proof

Last updated: Saturday 19th December, 2015 01:20

A good chunk of this class will be about proof. This is most likely to be the first place you learn about mathematical proof. You may have taken some math courses or even calculus before. But this is something different. This class is all about reasoning which is in fact the real heart of math.

Let us start consider what exactly is a proof. The formal definition of proof would not do us any good. To understand what a proof is we must understand the "feeling" when we have proved something. This can be shown with the following five card trick.

The Five Card Trick

Magic show is like mathematical theorem. Theorem claims that something is true. Magic just put the truth right in front of our eyes and left us wonder how that works. Proving is like fully understanding how the magic works. As you read this trick, keep in mind that what we want you to understand that feeling when we have fully understood something.

Here is what the audience will see in the trick

- A volunteer pick 5 cards showed it to the magician.
- The magician then look at these 5 cards and return one card to volunteer. The rest of the cards are laid out on a table.
- A random stranger comes in inpsect the cards on the table and tell the card the magician return to the volunteer?

So, the first question we have would be how did the stranger figure out the suit? If you have seen it for a few times, I'm sure you will figure out that it is as simple as the suit of the first card.

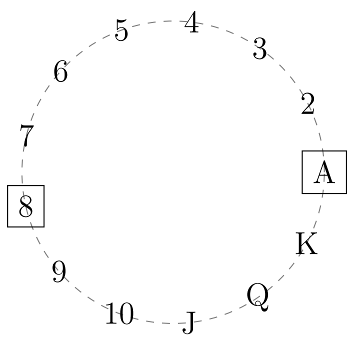
Does this mean that we fully understand the suit part of the trick? Of course not. Even though we know that the strager figure out the suit from from the first card. How can the magician guarantee that he will have two cards of the same suit such that to leave one on the table and another to hand back to the volunteer?

- You will learn this later. It is called the pigeon hole principle. There are 4 suit and since the volunteer pick 5 cards you are guarantee to have at least one suit that has at least two cards.

Again, we are not done yet. We still have the question of the rank left. The stranger gets the rank correct too. If you think about it, it must be the other three cards that the magician laid out on the table. Of course, the magician has no control over the rank of the 3 cards. So, the only tool of communication available to the magician would be the ordering of the three cards on the table High(H), Medium(M) and Low(L).

However, there are only $3 \times 2 \times 1 = 6$ way to arrange HML. Yet, there are 13 rank. This alone is not enough for the magician and the stranger to communicate. As in most proof, we guess, we fail and we guess again.

Here is the important part. The card that the magician return is always the double suit card. If we arrange the rank of cards in a circle then pick any two points the shortest distance between the two cards is at most $\frac{13-1}{2} = 6$.



This means that we can use the first card as the base then use the other three card to communicate the shift we can really convey information about 13 cards.

Therefore, to perform this trick all you need to do is to agree before hand which arrangement of HML means which number from 1 to 6. The one I use in the class is

LMH	1
LHM	2
MLH	3
MHL	4
HLM	5
HML	6

Also you will need to communicate which way to shift the card. For example, if the cards the volunteer pick are

$$3\clubsuit, 2\heartsuit, A\spadesuit, 5\spadesuit, 7\diamondsuit$$

From this, we want the stranger to do $A\spadesuit + 4$ to get $5\spadesuit$. Therefore, we should return $5\spadesuit$ to the volunteer. After that I should arrange the card on the table to represent $A\spadesuit + 4$ which is $A\spadesuit + MHL$. Therefore the card on the table would be(if you have same number you and rank the suit in someway ex: slave ranking).

$$A\spadesuit, 3\clubsuit, 7\diamondsuit, 2\heartsuit$$

When the stranger comes in and look at the table, it is clear to him that the suit of the hidden card has to be $\spadesuit$. Plus the amount of shift he needs to do is MHL=4. Thus, the stranger then do the arithmetic $A\spadesuit + 4 = 5\spadesuit$.

With all this, we feel that we have completed the understanding of the magic. We can actually replicate the magic. No question left to ask. It is important we keep questioning ourselves if there is anything left to ask – Did we just fool ourself?

Vocabulary

To make writing proof short and make it easier to communicate with other people let us first learn some vocabulary.

Basic Set Notation

In this class, we will be dealing with set a lot.

Set is loosely a collection of things the order doesn't matter. For example,

$$A = \{\text{cat, dog, mouse}\} \tag{1}$$
$$B = \{1, 2, 3\} \tag{2}$$
$$C = \{a \in I^+ | a \text{ is odd}\} \tag{3}$$
$$D = \{x \in \mathbb{R} | x^2 - 2x + 1 = 0\} \tag{4}$$

There are also simple set operation that is union and intersection. The union of the two set A and B is a set that contains all the elements in A and all the elements in B. For example,

$$\{1, 2, 3\} \cup \{2, 3, 4\} = \{1, 2, 3, 4\}$$

The intersection of two set, A and B, is a set that contains all the element that presents in both set A and B. For example,

$$\{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}$$

Proof

This class also deal with proofing stuff a lot. We are going to give a loose definition of proof here as a method of ascertaining the truth.

Def: A **proposition** is a statement that is true or false.

A proposition doesn't have to be true. It can be false. We don't even need to know the answer whether it is true or false. All we need to know is that it is either true or false.

Example of something that is a proposition:

$$2 + 3 = 5$$
$$2 + 3 = 1$$

Example of statement that is not a proposition:

What is love$\heartsuit$?

What is the meaning of life universe and everything? (42 By the way)

This statement is false.

Here are some example to give you an idea of proof:

Example 1:
Theorem: There are xxx students in this class.
Proof: I just counted. $\square$

Example 2:
Theorem: If $x > 2$ then $x^2 > 4$.
Proof:

$$x > 2$$
$$x \cdot x > 2 \cdot x > 2 \cdot 2 \quad \square$$

Example 3:
Theorem: If $x \geq 2$ then $x^2 > 5$.
Proof: False. Counter example $x = 2$, $x^2 = 4 < 5$. $\square$

Sometime counter example is not so easy to find

Example 4:
Theorem: For $n \in I$ if $n > 0$ then n^2+n+41 is a prime.
False counter example of n=41.

Predicate and Qualifier

Def: A **predicate** is a proposition whose truth value depends on the value of the variable. You can think about this as a function that takes in a value then return true/false.

For example,

$$n^2 + n + 41 \text{ is a prime.}$$

is a predicate since the truth value of the statement depends on the variable n.

The previous theorm contains qualifier and proposition.

$$\underset{\text{quantifier}}{\underset{\uparrow}{\forall}} n \in I, n \geq 0 \quad \underbrace{n^2 + n + 41\text{is a prime}}_{\text{Proposition}}$$

The symbol $\forall$ reads for all. The proposition above is true if and only if the predicate that follows is true for every single number $n \in I$. Thus since $n = 41$ doesn't make it true. The proposition above is false.

There is a related symbol for requiring just element in the set to give make it true.

$$\underset{\text{quantifier}}{\underset{\uparrow}{\exists}} n \in I, n \geq 0 \quad \underbrace{n^2 + n + 41\text{is a prime}}_{\text{Proposition}}$$

The statement above reads for some(there exists) an integer n such that the following predicate is true. The proposition is true if we can find just a number to make the predicate true. The above propositiion is true since $n = 0$ make the predicate true.

Example 5:
There exists a real number x such that the square is less than one.

$$\exists x \in \mathbb{R} \text{ such that } x^2 < 1$$

Example 6:
All real number x has the square less than one.

$$\forall x \in \mathbb{R}, x^2 < 1$$

Example 7:
There exists a male student in this room

$$\exists x \in \text{Student}, x \text{ is Male}$$

Example 8: Euler Conjecture
Theorem: $a^5 + b^5 + c^5 + d^5 = e^5$ has no integer solution

$$\forall a, b, c, d, e \in I^+, a^5 + b^5 + c^5 + d^5 \neq e^5$$

The theorem is actually false since

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

But it took 200 years to find it. One of the shortest paper ever.[a]

[a] http://www.ams.org/journals/bull/1966-72-06/S0002-9904-1966-11654-3/S0002-9904-1966-11654-3.pdf

Example 9:
Another euler conjecture. $a^4 + b^4 + c^4 = d^4$ has no integer solution. This is also false. The first solution is

$$\begin{aligned} a &= 95800 \\ b &= 217519 \\ c &= 414560 \\ d &= 422481 \end{aligned}$$

Example 10:
$313(x^3 + y^3) = z^3$ has no positive integer solution.
This is also false but the first z is more than 1,000 digit.

Example 11: Four color theorem
Every map can be color with 4 color such that no adjacent area has the same color.

There are many failed attempt on this but in the alst 30 years or so people are able to use computer to check almost every case. But that is considered not elegant. Right now, there is a short proof in 2008.

Example 12:
Every even integer is a sum of two prime numbers.

$$\forall x \in \underset{\substack{\uparrow \\ \text{Even integer}}}{\mathbb{E}}, \exists a, b \in \underset{\substack{\uparrow \\ \text{Prime}}}{\mathbb{P}} \text{ such that } a + b = x$$

This remains unproven for several hundred years already.

The above example is an example of using multiple quantifier together. We must be a bit more careful than usual when using more than one quantifier. For example, the proposition,

$$\forall x \in I, \exists y \in I \text{ such that } x + y = 1,$$

is true since for every integer x we can find an integer $y = 1 - x$ such that the sum is 1.

However, the proposition,

$$\exists y \in I \text{ such that } x + y = 1 \forall x \in I$$

is not true. The proposition is asking for whether there is one y that can add to any x such that the sum is always 1. This is not true since

- Let x_1 be the first solution, $y + x_1 = 1$
- Consider $x_2 = x_1 + 1$
- The proposition require also that $y + x_2 = 1$
- But

$$\begin{aligned} y + x_2 &= y + (x_1 + 1) \\ &= (y + x_1) + 1 \\ &= 1 + 1 = 2. \end{aligned}$$

- Threfore, $y + x_2 \neq 1$. The proposition is false.

Logical Operators

Let P be a proposition. There are couple things we can do with propositions.

Not

We can consider the negate($\sim$) of the proposition. For example,

This car is red

The negate is just

This car not red

We can also write a truth table for the negation

P	$\sim P$
T	F
F	T

And

The and($\wedge$) operator requires that both propositions to be true. For example,

This car is red *and* has 4 doors

This will be true if the car is red and has 4 doors. A car that is blue but has 4 doors is not qualified.

The truth table for and operator is shown below

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Or

The or($\vee$) operator requires that at least one of the proposition is true.

The car is red *or* has 4 door.

The above proposition is true if the car is 2 door red car.

The truth table for or operator is shown below

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Imply

The imply/if-then($\rightarrow$) operator indicate an inferral or a promise of some kind.

If you pay attention in class, you will get an A.

This statement is false only if you pay attention in class but you didn't get an A. Of course, the predicate above is still true if there is a student in the class that never pay atten but get an A. But, please please do the homework.

The truth table for imply operator is shown below

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Equivalent

The equivalent/if-and-only-if/iff($\iff$) indicates the equivalence of the truth value of the two proposition.

You will get an A if and only if you pay attention in class.

The proposition above means that if you pay attention in class you will get an A and if you don't then you won't.

The truth tale for iff is shown below

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

Combination of those

We can combine all these operator as well. Let us show the first identity:

$$(P \rightarrow Q) \wedge (Q \rightarrow P) = P \iff Q$$

To show that the above proposition is true we need to show that it is true of all value of P and Q. So, the simplest way is to just check all the cases:

P	Q	$P \to Q$	$Q \to P$	$(P \to Q) \wedge (Q \to P)$	$P \iff Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	F	F	F
F	F	T	T	T	T

The above truth table shows that the last two column which are the value of the left hand side(LHS) statement and the value of the right hand side(RHS) are the same for all cases.

Therefore,

$$(P \to Q) \wedge (Q \to P) = P \iff Q$$

As an exercise, you should show that

$$P \to Q = \sim Q \to \sim P$$

You will learn this later it is called contrapositive.