Some Basic Logic

Henry Liu, 25 October 2010

In the solution to almost every olympiad style mathematical problem, a very important part is existence of accurate proofs. Therefore, the student should be competent with the strict rules of mathematical logic. These rules can be easily ignored, and errors often appear, ranging from proving an inequality, to a proof by contradiction.

Very often, phrases like 'if and only if', 'contradiction', 'necessary and sufficient', and symbols like '$\Rightarrow$', '$\iff$', '$\exists$' keep appearing. What exactly do they mean? In this set of notes, we shall discuss the exact meaning of these and other related terms.

1. Statements and Notations

1.1 Statements

Definition 1 *A* (mathematical) statement *is a mathematical sentence which can only be true or false.*

Example. Here are some examples of mathematical statements.

- 40 is divisible by 5.
- $\angle ABC = \angle XYZ$.
- $\sqrt{2}$ is rational.
- $x \leq y$.

Note that the first statement is true, the third is false, and the other two can be either true or false.

1.2 Quantifiers and some other notations

There are some basic quantifiers and notations which are worth knowing.

Definition 2

(a) '$\exists$' means 'there exists', and '$\exists!$' means 'there exists a unique'.

(b) '$\forall$' means 'for all'.

(c) '$\ni$' means 'such that'.

If A and B are mathematical statements, then,

(d) '$A \Rightarrow B$', or '$B \Leftarrow A$', means 'A implies B'.

(e) '$A \iff B$' means 'A implies B, and B implies A'.

In (d), there are some other ways of saying 'A $\Rightarrow$ B':

- 'A only if B';
- 'B if A';
- 'A is a sufficient condition for B';
- 'B is a necessary condition for A'.

In (e), A and B are said to be *equivalent statements*. Essentially, A and B are different ways of saying the same thing. Other ways of saying 'A $\iff$ B':

- 'A if and only if B', or 'A iff B' in short;
- 'B is a necessary and sufficient condition for A'.

Also, note that 'A $\Rightarrow$ B' and 'A $\iff$ B' are also statements; they are *compound statements*. The statement 'B $\Rightarrow$ A' is the *converse* of the statement 'A $\Rightarrow$ B'.

Example. The following are true mathematical statements.

- $\forall\, n \in \mathbb{N}\ \exists\, p \in \mathbb{N} \ni p > n$ and p is prime.
- $x^2 - 4x - 5 = 0 \Rightarrow x = -1$ or $x = 5$.
- $\forall\, n \in \mathbb{N}\ \exists!\, k \in \mathbb{N} \cup \{0\} \ni 2^k$ divides n, but 2^{k+1} does not divide n.

The following are false mathematical statements.

- $q \in \mathbb{Q} \iff q \in \mathbb{Z}$.
- $\exists$ polynomial $p(x) \ni p(x)$ is cubic and it has no real root.

The following mathematical statements can be true or false.

- $\angle ABC = \angle XYZ \iff \angle DEF = \angle PQR$.
- $\exists!$ vertex v in a graph $G \ni \deg(v) = 3$.

2. Proofs

2.1 Implications, and 'If and only if'

A common mistake in proofs involving statements is the direction of the implications being the wrong way round. This is especially common in inequalities problems, but it can also occur in problems in other areas.

Example. Consider the following problem. *Let x, y, z be positive real numbers. Prove that*

$$(x + y + z)(xy + yz + zx) \geq 9xyz.$$

When does equality hold?

Now consider the following 'solution'.

"$(x+y+z)(xy+yz+zx) \geq 9xyz$. So, multiplying out the LHS,

$$\begin{aligned} & xy^2+xz^2+yz^2+yx^2+zx^2+zy^2+3xyz &\geq& \quad 9xyz \\ \Rightarrow \quad & xy^2+xz^2+yz^2+yx^2+zx^2+zy^2-6xyz &\geq& \quad 0 \\ \Rightarrow \quad & x(y^2+z^2-2yz)+y(z^2+x^2-2zx)+z(x^2+y^2-2xy) &\geq& \quad 0 \\ \Rightarrow \quad & x(y-z)^2+y(z-x)^2+z(x-y)^2 &\geq& \quad 0 \end{aligned}$$

Each term on the LHS of the last line is non-negative. So the original inequality is true, and the result follows.

Equality holds when $y-z=z-x=x-y=0 \Rightarrow x=y=z$."

This 'solution' is absurd because it has taken the chain of implications in the wrong direction. It is wrong to say something like "We would like to prove A. A implies B, which implies C, which implies D, which is true. Hence A is true." This is incorrect. The correct thing to do, of course, is to argue the opposite way. So, the correct version should be "We want to prove A. But B implies A. But C implies B. But D implies C. But D is true. So A is true." Furthermore, looking for equivalent statements is a good idea.

So, the correct version of the above should be the following.

"We have

$$\begin{aligned} & (x+y+z)(xy+yz+zx) &\geq& \quad 9xyz \\ \iff \quad & xy^2+xz^2+yz^2+yx^2+zx^2+zy^2+3xyz &\geq& \quad 9xyz \\ \iff \quad & xy^2+xz^2+yz^2+yx^2+zx^2+zy^2-6xyz &\geq& \quad 0 \\ \iff \quad & x(y^2+z^2-2yz)+y(z^2+x^2-2zx)+z(x^2+y^2-2xy) &\geq& \quad 0 \\ \iff \quad & x(y-z)^2+y(z-x)^2+z(x-y)^2 &\geq& \quad 0 \end{aligned}$$

The LHS of the last line is non-negative, so the last inequality is true. But it is equivalent to the original inequality, so the original inequality is true as well."

Also, the corrected version of dealing with the case of equality is the following.

"Equality holds if and only if $y-z=z-x=x-y=0$, or equivalently, $x=y=z$."

What was previously written about the case of equality is again, incorrect.

Even the following shorter argument in proving this result is correct.

"By the AM-GM inequality, we have $x+y+z \geq 3(xyz)^{1/3}$, and $xy+yz+zx \geq 3(xyz)^{2/3}$. Multiplying these two gives the result. Equality holds iff $x=y=z$ and $xy=yz=zx$, ie: iff $x=y=z$."

This solution is good because we started with two statements, both being true, and deduced what we wanted to prove from them. In the case of equality, we derived '$x=y=z$' because this is equivalent to saying '$x=y=z$ and $xy=yz=zx$'.

We often see problems of the following form:

"Prove that A if and only if B."

What exactly does this mean? For those who lack the knowledge of what we have discussed so far, they may get confused at what exactly the problem is asking. There are two tasks at hand: prove that A implies B, *and* that B implies A.

It is a common and regrettable mistake to prove just one of the two implications.

Example. Here is a classic example. *Prove that a number $n \in \mathbb{N}$ is divisible by 3 if and only if the sum of its digits (in base 10) is divisible by 3.*

The correct way to proceed is the following.

Let n have k digits, say, $n =$ '$a_{k-1}a_{k-2}\cdots a_1a_0$' is the base 10 representation of n. That is, the digits of n (in base 10) are the a_i.

Firstly, suppose that n is divisible by 3. Then

$$\begin{aligned} n = \sum_{i=0}^{k-1} a_i 10^i \;&\equiv\; 0 \pmod 3 \\ \Rightarrow (a_{k-1} + \cdots + a_0) + \sum_{i=0}^{k-1} a_i(10^i - 1) \;&\equiv\; 0 \pmod 3. \end{aligned}$$

Now, since $10 \equiv 1 \pmod 3$, we have $10^\ell \equiv 1 \pmod 3$ for every non-negative integer ℓ. It follows that

$$\sum_{i=0}^{k-1} a_i(10^i - 1) \equiv 0 \pmod 3, \tag{1}$$

and hence $a_{k-1} + \cdots + a_0 \equiv 0 \pmod 3$, as required.

Conversely, let $a_{k-1} + \cdots + a_0 \equiv 0 \pmod 3$. Again, (1) is true. We have

$$n = \sum_{i=0}^{k-1} a_i 10^i = (a_{k-1} + \cdots + a_0) + \sum_{i=0}^{k-1} a_i(10^i - 1) \equiv 0 \pmod 3,$$

as required.

In the above proof, the classic mistake is to prove only one of the two implications. One must be careful of the task when the a problem says 'if and only if'.

2.2 The converse

Whenever a statement 'A $\Rightarrow$ B' is true, its converse may or may not be true. Sometimes, a problem may be of the form 'Prove that A $\Rightarrow$ B', and then it asks 'Is the converse true?'. If one wants to claim that the converse is false, then only a counterexample needs to be provided. Otherwise, if one wants to claim that the converse is true, then a proof is required. Often (but not always), the converse involved in such a problem is false, and one should try hard to think of a counterexample first.

Example. Consider the following problem. *Let $ABCD$ be a quadrilateral inscribed in a circle of radius r, and let the diagonals AC and BD meet at X.*

Prove that, if AC is perpendicular to BD, then

$$AX^2 + BX^2 + CX^2 + DX^2 = 4r^2.$$

Is the converse true?

So, this question consists of two parts. The first part is to assume that AC is perpendicular to BD, and we would like to prove that $AX^2+BX^2+CX^2+DX^2 = 4r^2$.

Let E be the point such that AE be a diameter of the circle. Then $AE^2 = AB^2 + BE^2$. So, $4r^2 = AX^2 + BX^2 + BE^2$. Now, we claim that $BE = CD$. We have $\angle BAE = 90° - \angle BEA = 90° - \angle BCA = \angle CBD$. So, BE and CD subtend equal angles, and hence $BE = CD$. Now, we have $4r^2 = AX^2 + BX^2 + CD^2 = AX^2 + BX^2 + CX^2 + DX^2$, which is what we want.

For the second part, we must deal with the converse statement. We want to answer this: "Does $AX^2 + BX^2 + CX^2 + DX^2 = 4r^2$ imply that AC and BD are perpendicular?". If we want to show that this converse is false, then we just need to provide a counterexample. This indeed is the case here: let $ABCD$ be a rectangle which is not a square. Then $AX = BX = CX = DX = r$, and so $AX^2 + BX^2 + CX^2 + DX^2 = 4r^2$ holds. But AC and BD are not perpendicular. So, the converse statement is false.

2.3 Proof by contradiction

This is a method of proof which belongs to logic. The idea is that, when we want to prove that a certain mathematical statement is true, we firstly assume that it is false, see what the falsity can imply, and eventually hope to arrive at something which is absurd; the 'contradiction'.

Example. The following is a classic example which demonstrates proof by contradiction. *Prove that $\sqrt{2}$ is irrational.*

To prove that $\sqrt{2}$ is irrational, we start by assuming the contrary: that it is rational. So we can write $\sqrt{2} = p/q$, where $p, q \in \mathbb{N}$ and in lowest terms, so that $\mathrm{hcf}(p, q) = 1$. Then, $2 = p^2/q^2$, so $p^2 = 2q^2$. We see that p^2 is even, it follows that p is even. So write $p = 2P$ for some $P \in \mathbb{N}$. Then, $2q^2 = 4P^2$, so $q^2 = 2P^2$, and by the same argument, we have q is also even, say, $q = 2Q$. But now, we see that 2 divides both p and q, contradicting the fact that $\mathrm{hcf}(p, q) = 1$. Hence the original assumption was wrong, and $\sqrt{2}$ needs to be irrational in the first place.

Notice that the power of the proof by contradiction method is that, some problems such as "Prove that $\sqrt{2}$ is irrational" may otherwise be very difficult to prove directly.

Example. The previous example is very well-known, so here is another more original example. Consider the following problem.

Let ABC be a triangle, and let M be the midpoint of BC. Let P and Q be points on the sides AB and AC respectively, and let PQ meet AM at N. Suppose that N is the midpoint of PQ. Prove that PQ is parallel to BC.

We demonstrate how to use proof by contradiction to solve this problem. Assume the contrary; that PQ is not parallel to BC. Then, we can draw the line through N which is parallel to BC. Let this line meet AB and AC at R and S respectively. We have $R \neq P$ and $S \neq Q$. Now, it is easy to see that $\triangle AMB$ and $\triangle ANR$ are similar, so $BM/RN = AM/AN$. Similarly, $CM/SN = AM/AN$. So, $BM/RN = CM/SN$, hence $RN = SN$ since $BM = CM$. Now, $PRQS$ is a quadrilateral whose diagonals bisect each other, and so it is a parallelogram. So, we have PR and QS are parallel. This is absurd. So our original assumption that PQ and BC are not parallel was wrong, and they must be parallel in the first place.

Again, it seems a little bit more difficult to tackle this particular problem without a proof by contradiction.

Example. We finish with another classic example. We shall use proof by contradiction to prove a result that is over 2000 years old. *Prove that there are infinitely many primes.*

Assume the contrary, that there are only finitely many primes. Call these $p_1, p_2, \ldots, p_n$. We have $p_i \geq 2$ for every i. Now, consider the number $m = p_1 p_2 \cdots p_n + 1$. Since m leaves a remainder of 1 upon division by any prime p_i, it is a prime. However, $m \neq p_i$ for any i, since $m > p_i$ for every i. So, we have found a prime number m which is none of $p_1, p_2, \ldots, p_n$. This is absurd, so we cannot have finitely many primes $p_1, p_2, \ldots, p_n$ in the first place.