Halting Problem

Assume H(P,I), which able to tell that any P with any input I loops or halts, exists.

So H it should be able to tell us whether P with input P (itself) loops or halts as well.

Let K(P) take the output of H(P,P).

- If H(P,P) has "loop forever" as output, then K(P) halts.
- If H(P,P) has "halt" as output, then K(P) loops forever.

So what if we use K as input to K itself.

Substitute K in, you see the contradiction.

Resolution

This is another use of the tautology

$$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$$

The part $q \vee r$ is called **resolvent**.

Example: Show that the hypothesis "Jojo is running or it is not raining" and "It is raining or Doppio is playing football" imply that "Jojo is running or Doppio is playing football"

Answer:

We can present these sentences by substituting:

- p = It is raining
- q = Jojo is running
- r = Doppio is playing football

in the above tautology. We can conclude $q \vee r$ straightforwardly.

Example: Show that $(p \wedge q) \vee r$ and $r \rightarrow s$ imply $(p \vee s)$.

Answer:

1. $(p \wedge q) \vee r$ is $(p \vee r)$ and $(q \vee r)$.
2. $r \rightarrow s$ is $\neg r \vee s$.
3. So now we have $(p \vee r)$ and $(\neg r \vee s)$.
   By resolution, we can say that $(p \vee s)$.

Fallacies

Proof that use wrong tautology! I'll name two:

- use $[(p \rightarrow q) \wedge q] \rightarrow p$:**fallacy of affirming the conclusion**
- use $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$:**fallacy of denying the hypothesis**

Proof by cases

Example: Show that $|xy| = |x||y|$ where x and y are real numbers.

Answer: proof stages are as follows:

1. Let p be "x and y are real numbers". p is equivalent to $p_1 \vee p_2 \vee p_3 \vee p_4$:
   - p_1 is "$x \geq 0 \wedge y \geq 0$".
   - p_2 is "$x \geq 0 \wedge y < 0$".
   - p_3 is "$x < 0 \wedge y \geq 0$".
   - p_4 is "$x < 0 \wedge y < 0$".
2. let q be "$|xy| = |x||y|$".

3. We must show that $p_1 \rightarrow q$, $p_2 \rightarrow q$, $p_3 \rightarrow q$, and $p_4 \rightarrow q$:

   - $p_1 \rightarrow q$: $xy \geq 0$, therefore $|xy| = xy = |x||y|$.
   - $p_2 \rightarrow q$: $xy \leq 0$, therefore $|xy| = -xy = x(-y) = |x||y|$.
   - $p_3 \rightarrow q$: $xy \leq 0$, therefore $|xy| = -xy = -x(y) = |x||y|$.
   - $p_4 \rightarrow q$: $xy \geq 0$, therefore $|xy| = xy = (-x)(-y) = |x||y|$.

Example: Show that the 3 following statements:

- p_1: n is an even integer.
- p_2: $n - 1$ is an odd integer.
- p_3: n^2 is an even integer.

are equivalent.

Answer: We show this by showing $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, and $p_3 \rightarrow p_1$.

To show $p_1 \rightarrow p_2$, we use direct proof.

Say, n is even, therefore:

$$\begin{aligned} n &= 2k \\ n-1 &= 2k-1 \\ &= 2(k-1)+1 \end{aligned}$$

which is the form of an odd integer, i.e. $2m+1$.

To show that $p_2 \rightarrow p_3$, we use direct proof. Suppose $n-1$ is odd

$$\begin{aligned} n-1 &= 2m+1 \\ n &= 2m+2 \\ n^2 &= (2m+2)^2 \\ &= 4m^2+8m+4 \\ &= 2(m^2+4m+2) \end{aligned}$$

Thus it can be seen that n^2 must be even.

To show $p_3 \rightarrow p_1$, we use an indirect proof, assume n is not even, we mus show that n^2 is not even.

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

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

which is a form of an odd integer. Thus we have the whole proof.

More Proof by Cases

Example: Prove that if n is an integer not divisible by 2 or 3, then $n^2 - 1$ is divisible by 24

Divide n into cases:

1. $n = 6k$: ignore since this is divisible by 2 and 3.
2. $n = 6k + 1$: this is one case where we concern.
3. $n = 6k+2$: ignore since this is divisible by 2.
4. $n = 6k+3$: ignore since this is divisible by 3.
5. $n = 6k+4$: ignore since this is divisible by 2.
6. $n = 6k + 5$: this is one case where we concern.

For the case where $n = 6k + 1$,

$$\begin{aligned} n^2 - 1 &= (n-1)(n+1) \\ &= 6k(6k+2) \\ &= 6k(6k+2) \\ &= 12k(3k+1) \end{aligned}$$

Notice that $k(3k+1)$ is always even (try some example by yourself i.e. when k is odd and when k is even).

Thus there is a q that makes $k(3k+1) = 2q$, this will make the above $n^2 - 1 = 24q$, thus divisible by 24.

For the case where $n = 6k + 5$,

$$\begin{aligned} n^2 - 1 &= (n-1)(n+1) \\ &= (6k+4)(6k+6) \\ &= 12(k+1)(3k+2) \end{aligned}$$

Notice that $(k+1)(3k+2)$ is even (again, try it when k is odd and when k is even). Thus we get $n^2 - 1$ is divisible by 24 for all the cases we concern.

Example: Show that there are no integers x and y that makes $x^2 + 3y^2 = 8$.

Answer:

We know that $x^2 > 8$ when $|x| \geq 3$,and $3y^2 > 8$ when $|y| \geq 2$. Therefore

- x can only be $-2, -1, 0, 1, 2$
- y can only be $-1, 0, 1$

From these cases, possible values of x^2 are $0, 1, 4$, while possible values of $3y^2$ are 0 and 3. This means that the largest value of $x^2 + 3y^2$ is only 7, never 8. This completes the proof.

Nonconstructive Existence Proofs

Proof "for some", but not by finding working samples. It can be contradiction proof, etc.

Example: Show that there exist irrational numbers x and y, such that x^y is rational.

Answer:

We know that $\sqrt{2}$ is irrational. Use it!

If $\sqrt{2}^{\sqrt{2}}$ is rational, we will have the answer right away. That is $x = y = \sqrt{2}$.

If $\sqrt{2}^{\sqrt{2}}$ is irrational, we can have $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. In this case,

$$\begin{aligned} x^y &= (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} \\ &= (\sqrt{2})^2 \\ &= 2 \end{aligned}$$

In any case, there is, for sure, a situation that x^y is rational.

Uniqueness Proof

To show that x is unique:

1. show that x (with the desired property) exists.
2. show that if $y \neq x$, then y does not have that property.

Example: Show that if p is an integer, then there exists a unique integer q such that $p + q = 0$.

Answer:

If p is an integer, then it is obvious that there exists an integer $q = -p$ that makes $p + q = 0$. What we need to show next is that q is unique.

suppose r is an integer ($r \neq q$), and $p + r = 0$. We can derive:

$$\begin{aligned} p + q &= p + r \\ q &= r \end{aligned}$$

This contradicts the assumption. Therefore q is unique.

Beware of mistakes

Example: The proposition $1 = 2$ has the following incorrect proof step:

1. $a = b$: given
2. $a^2 = ab$: multiply both sides
3. $a^2 - b^2 = ab - b^2$: subtract b^2 from both sides
4. $(a - b)(a + b) = b(a - b)$: factor both sides
5. $a + b = b$: **divide both sides by $a - b$**
6. $2b = b$: replace a by b
7. $2 = 1$: divide both sides by b

The one in bold is wrong. Yes $a - b = 0$, it is divide by zero.

Example: The false theory "If $n^2 > 0$, then $n > 0$" has the following incorrect proof:

Assume $n^2 > 0$

Because $(n > 0) \rightarrow (n^2 > 0)$ is a tautology. We conclude from this that $n > 0$.

This is wrong. The inference rule is not used. This is fallacy of affirming the conclusion.

Example: The false theory "If n is not positive, then n^2 is not positive" has the following incorrect proof:

Assume n is not positive.

Because $(n > 0) \rightarrow (n^2 > 0)$ is a tautology. We conclude from this that n^2 is not positive.

This is wrong. The inference rule is not used. This is fallacy of denying the hypothesis.

Example: The false theory "If x is a real number, then x^2 a positive real number" has the following incorrect proof:

Let p_1 be "x is positive", p_2 be "x is negative", and q be "x^2 is positive." We use proof by case:

1. $p_1 \rightarrow q$: obvious.
2. $p_2 \rightarrow q$: when x is negative, x^2 is positive anyway.

So, both cases are proven.

WRONG! We forget the case where $x = 0$, which will make the proposition false.

Circular Reasoning (fallacy of begging the question)

The statement is proven using itself. It is important not to make this mistake.

Example: The incorrect proof of "n is an even integer whenever n^2 is an even integer" is as follos:

Assume n^2 is an even integer, then $n^2 = 2k$ for some integer k. **Let $n = 2l$ for some integer l**. Therefore n is even.

Totally wrong, where does "Let $n = 2l$" come from? This is assuming what we

want to prove. (Or can be seen as an attempt to "Mua" the answer)

Proof Strategies

Forward Reasoning: This is what we do in direct and indirect proof.

Backward Reasoning: To prove q, we can find p that we can prove $p \rightarrow q$.

Example: Given two distinct positive real numbers a and b, their **arithmetic mean** is $\frac{(a+b)}{2}$ and their **geometric mean** is $\sqrt{ab}$. Show that

$$\frac{(a+b)}{2} > \sqrt{ab}$$

To show this, we can work backward from the wanted conclusion:

$$\begin{aligned} \frac{(a+b)}{2} &> \sqrt{ab} \\ \frac{(a+b)^2}{4} &> ab \\ (a+b)^2 &> 4ab \\ a^2+2ab+b^2 &> 4ab \end{aligned}$$

$$\begin{aligned} a^2 - 2ab + b^2 &> 0 \\ (a-b)^2 &> 0 \end{aligned}$$

$(a-b)^2 > 0$ only when $a \neq b$. This is the original condition. The proof is complete. We can now easily use forward reasoning.

Example: A stone pile contains 15 stones, two people take turn removing 1 or 2 or 3 stones at a time from the pile. Show that the first player can win the game no matter what the second player does.

Answer:

Work from the gameover stage, the pile has 1 or 2 or 3 stones for the first player.

The step before this win must be when there are 4 stones in the pile (just think of the case, say, 5 or 6 stones)

One step before must have 5 or 6 or 7 stones. (first player removes the stone to leave 4 remaining)

One step before, second player must remove stones from a pile size of 8 (so that

we can get 7,6,5 in the next step)

One step before, first player must remove stones from a pile of 9, or 10, or 11 stones.

One step before, the second player must remove stones from a pile of 12 stones.

One step before, the first player thus must remove 3 stones.

Thus the first player can win in any case.

Open Problem: Fermat's Last Theorem

$$x^n + y^n = z^n$$

has no solutions for x, y, z, with $x, y, z \neq 0$. Where n is an integer which > 2.

Fermat wrote that he proved it... but in fact didn't publish...Others look for this proof for over 300 years.

Eventually proven by **Andrew Wiles**, using theory of elliptic curves. He spent 10 years proving it -$''$_.

Open Problem: Goldbach's Conjecture

1742... He guessed that **every odd integer n, where $n > 5$, is the sum of three primes**. Euler told him this is the same as saying **every eveninteger n, where $n > 2$, is the sum of two primes**.

Supporting examples (e.g. $4 = 2+2, 10 = 7+3$) are found up to all positive even integers up to $4 * 10^{14}$. But no one has ever proven it yet.

Related proofs are found though:

- O.Ramare, 1995: every even positive integer greater than 2 is the sum of at most six primes.
- J. R. Chen, 1966: every sufficiently large positive integer is the sum of a prime and a number that is either prime or the product of two primes.
- H. Iwaniec, 1973: There are infinitely many positive integers n such that n^2+

1 is prime or the product of at most two primes.