How To Read and Do Mathematical Proofs

James A. Foster
Laboratory for Uphill Computing
Dept. of Computer Science
University of Idaho

September 26, 1996

Overview

- High level strategy
- Indicators for specific strategies
- Specific strategies
- Some good books

Notation

$\wedge$ And

$\vee$ Or

$\neg$ Not

$\forall$ For all (or "every")

$\exists$ There exists (or "some")

$\rightarrow$ If...Then (or "implies")

$\leftrightarrow$ If and only if

Your Task (High Level)

Show that conclusion C a necessary consequence of premises P and what you know K

1. Review definitions (Study)
2. How would you know C was true? (Ponder)
3. Is the theorem true? (Play)
4. Analyze P and C (Work)
5. Apply proof techniques (Work hard)
6. Re-write for legibility and clarity (Communicate)

Specific Strategies

Technique	*Indicator*
Forward-Backward	Any time
Construction	There is
Choose	For all, each, any
Induction	For all, each, any
Contrapositive	Not, no in C
Contradiction	Not, no, any time
Cases	Or
Compound	And, both
Inspiration	anytime

Forward-Backward

Indicator Any time

Strategy Work simultaneously from premise and conclusion

Thm: $\binom{n}{r} = \binom{n}{n-r}$

Forward-Backward Example

Thm: $\binom{n}{r} = \binom{n}{n-r}$
Proof: By definition,

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

But $r = n - (n - r)$. So

$$\begin{aligned} \frac{n!}{r!(n-r)!} &= \frac{n!}{(n-(n-r))!(n-r)!} \\ &= \binom{n}{n-r} \end{aligned}$$

where the last step is by definition. So, $\binom{n}{r} = \binom{n}{n-r}$.

Construction

Indicator "There is"

Strategy Build a witness and use it

Thm: The integers are denumerable.

Construction Example

Thm: The integers are denumerable.

Proof: We will produce an enumeration of the integers. Let

$$E(x) = \begin{cases} 2x - 1 & \text{if } x > 0 \\ 2|x| + 2 & \text{otherwise} \end{cases}$$

E clearly maps the integers to the natural numbers, since every integer is either greater than 0 or is not. E is $1:1$, since $x \neq y \rightarrow E(x) \neq E(y)$. Finally, E is onto, since every natural number is either even or odd. Therefore, E is the desired enumeration of the integers, showing that the integers are denumerable.

Choose

Indicator "For all, each, any"

Strategy Choose and use an *arbitrary* witness

Thm: The sum of any two odd integers is even

Choose Example

Thm: The sum of any two odd integers is even

Proof: Let x and y be two arbitrary odd integers. Then, by definition, $x = 2a + 1$ and $y = 2b + 1$ for two integers a and b. Now, let $c = a + b + 1$. Then

$$\begin{aligned} x + y &= 2a + 2b + 2 \\ &= 2c \end{aligned}$$

So, by definition, $x + y$ is even.

Induction

Indicator "For all, each, any" in a countable domain

Strategy Find base case, show how to express large instance in terms of smaller instance(s), show that if it holds for the small instance then it holds for the next larger one.

Thm: Prove that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Induction example

Thm: Prove that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof: For the base case, assume $n = 1$. Then

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

So the base case holds.

Now, show that if the theorem holds for $n = k$ then it holds for $n = k + 1$.

$$\begin{aligned} \sum_{i=1}^{k+1} &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

The first step is by definition of summation, the second by inductive assumption, and the third by algebraic manipulation. This completes the induction.

Contrapositive

Indicator "Not, no in C"

Strategy Assume "not C", prove "not P"

Thm: For real number p, q, if $\sqrt{pq} \neq \frac{p+q}{2}$ then $p \neq q$

Contrapositive Example

Thm: For real number p, q, if $\sqrt{pq} \neq \frac{p+q}{2}$ then $p \neq q$

Proof: Assume $p = q$. Then

$$\begin{aligned} \sqrt{pq} &= \sqrt{pp} \\ &= p \\ &= \frac{2p}{2} \\ &= \frac{p+p}{2} \\ &= \frac{p+q}{2} \end{aligned}$$

So $\sqrt{pq} = \frac{p+q}{2}$. Therefore, the theorem must hold by contrapositive.

Contradiction

Indicator "Not, no, any time" or desperation

Strategy Assume "not C", derive contradiction using P and K

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

Contradiction Example

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

We will need the following lemma:

Lemma: If x^2 is even, then so is x.

Proof: Let $x^2 = 2a$. Then $x^2 = x \cdot x = 2a$. So 2 must divide one of the multiplicands in x^2. So x must be even.

Contradiction Example (cont'd)

Proof of theorem: Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{p}{q}$ for some integers p and q which have no common factors. Then $\sqrt{2}^2 = 2 = \frac{p^2}{q^2}$, so

$$2q^2 = p^2$$

So, p^2 is even, which by the lemma implies that p is even. In other words, $p = 2a$ for some integer a.

This implies that $2 = \frac{(2a)^2}{q^2} = \frac{4a^2}{q^2}$, which implies that $2q^2 = 4a^2$ and that $q^2 = 2a^2$. So, q^2 is even, which by the lemma implies that q is even.

This means that both q and p are even, and so they have the common factor 2. This contradicts our assumption and proves the theorem.

Cases

Indicator "Or" or any time

Strategy Divide and conquer

Thm: There are irrational b and c such that b^c is rational.

Cases Example

Thm: There are irrational b and c such that b^c is rational.

Proof: Consider the number $\sqrt{2}^{\sqrt{2}}$.

Case 1: if $\sqrt{2}^{\sqrt{2}}$ is rational, then let $b = c = \sqrt{2}$.

Case 2: Suppose $\sqrt{2}^{\sqrt{2}}$ is irrational. Then let $b = \sqrt{2}^{\sqrt{2}}$ and $c = \sqrt{2}$. Now

$$\begin{aligned} b^c &= (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} \\ &= \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} \\ &= \sqrt{2}^2 \\ &= 2 \end{aligned}$$

So that b^c is rational.

These are the only two cases, so the theorem is true.

Compound proofs

Indicator "And, both"

Strategy Prove each part separately

Thm: There is exactly one even prime.

Compound Example

Thm: There is exactly one even prime.

Proof: 2 is an even prime, so there is at least one.

If p and q were both even primes, then both would have 2 as a divisor. But the only divisors of a prime are 1 and itself. So, both p and q must equal 2. So there are no other even primes than 2.

Inspiration

Indicator Any time

Strategy Change the Problem

Good Books

Some excellent books on doing proofs:

- Polya, G. *How to Solve It*, 2nd ed., Princeton, 1957.
- Solow, D. *How to Read and Do Proofs*, Wiley, 1990.
- Wickelgren, W. *How to Solve Problems*, Freeman, 1974.
- Polya, G. *Patterns of Plausible Inference*, 2nd ed., Princeton, 1968.
- Polya, G. *Induction and Analogy in Mathematics*, Princeton, 1973.
- Lakatos, I. *Proofs and Refutations*, Cambridge, 1976.