Writing more proofs

Misha Lavrov

ARML Practice 3/16/2014 and 3/23/2014

Warm-up

Using the quantifier notation on the reference sheet, and making any further definitions you need to, write the following:

"You can fool all the people some of the time, and some of the people all the time, but you cannot fool all the people all the time."

Warm-up

Using the quantifier notation on the reference sheet, and making any further definitions you need to, write the following:

"You can fool all the people some of the time, and some of the people all the time, but you cannot fool all the people all the time."

Let $\mathbb{P}$ be the set of all people, $\mathcal{T}$ the set of all times, and $F(p,t)$ the statement that person p can be fooled at time t. Then

$$
\begin{aligned}
&(\forall p \in \mathbb{P}\ \exists t \in \mathcal{T} : F(p,t)) \\
\wedge\ &(\exists p \in \mathbb{P}\ \forall t \in \mathcal{T} : F(p,t)) \\
\wedge\ &\neg(\forall p \in \mathbb{P}\ \forall t \in \mathcal{T} : F(p,t)).
\end{aligned}
$$

Proving things: a case study

Problem

Prove that the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

diverges.

Proving things: a case study

Problem

Prove that the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

diverges.

Proof idea.

Round down $\frac{1}{3} + \frac{1}{4}$ to $\frac{1}{4} + \frac{1}{4}$, $\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}$ to $\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}$, and so on. □

Key points to hit

- It's good to be specific about the rounding: $\frac{1}{n}$ rounds down to $\frac{1}{2^k}$ chosen so that $2^{k-1} < n \leq 2^k$.

  This makes it easy to show that there are 2^{k-1} terms that round down to $\frac{1}{2^k}$, contributing a total of $\frac{1}{2}$.
- One possible punchline: $1 + \frac{1}{2} + \frac{1}{2} + \cdots$ diverges, and the harmonic series is at least as large.
- Better (fewer infinities): The first 2^k terms of the harmonic series total at least $1 + \frac{k}{2}$, which can be arbitrarily large.

What is divergence, anyway?

Say we have the infinite series $a_1 + a_2 + a_3 + \cdots$. We call $S_n = \sum_{k=1}^{n} a_k$ the n-th partial sum.

What is divergence, anyway?

Say we have the infinite series $a_1 + a_2 + a_3 + \cdots$. We call $S_n = \sum_{k=1}^{n} a_k$ the n-th partial sum.

When all the a_k are positive, the infinite series diverges if and only if the sequence of partial sums tends to infinity. This happens iff:

- The partial sums become arbitrarily large if we take sufficiently many terms.
- Which is to say, for all M there is an index n such that S_n exceeds M.
- $\forall M \, \exists n : S_n > M$.

What is divergence, anyway?

Say we have the infinite series $a_1 + a_2 + a_3 + \cdots$. We call $S_n = \sum_{k=1}^{n} a_k$ the n-th partial sum.

When all the a_k are positive, the infinite series diverges if and only if the sequence of partial sums tends to infinity. This happens iff:

- The partial sums become arbitrarily large if we take sufficiently many terms.
- Which is to say, for all M there is an index n such that S_n exceeds M.
- $\forall M\ \exists n : S_n > M$.

When a series contains negative numbers, things are more complicated: e.g.,

$$1 - 1 + 1 - 1 + 1 - 1 + \cdots .$$

Proving a dependence

We want to prove that $\forall M \, \exists n : S_n > M$, where $S_n = \sum_{k=1}^{n} \frac{1}{k}$.
How?

Proving a dependence

We want to prove that $\forall M \, \exists n : S_n > M$, where $S_n = \sum_{k=1}^{n} \frac{1}{k}$.
How?

Let M be any real number.

Proving a dependence

We want to prove that $\forall M\ \exists n : S_n > M$, where $S_n = \sum_{k=1}^{n} \frac{1}{k}$.
How?

Let M be any real number. Take $n = 2^{2M}$.

Proving a dependence

We want to prove that $\forall M \; \exists n : S_n > M$, where $S_n = \sum_{k=1}^{n} \frac{1}{k}$.
How?

Let M be any real number. Take $n = 2^{2M}$. Then

$$\begin{aligned} S_n &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{2M}} \\ &= 1 + \left(\frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \cdots + \left(\frac{1}{2^{2M-1}+1} + \cdots + \frac{1}{2^{2M}}\right) \\ &> 1 + \underbrace{\frac{1}{2} + \frac{1}{2} + \cdots + \frac{1}{2}}_{2M \text{ times}} = M + 1 > M. \end{aligned}$$

Therefore the harmonic series diverges.

Proving a dependence

We want to prove that $\forall M\ \exists n : S_n > M$, where $S_n = \sum_{k=1}^{n} \frac{1}{k}$. How?

Let M be any real number. Take $n = 2^{2M}$. Then

$$\begin{aligned} S_n &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{2M}} \\ &= 1 + \left(\frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \cdots + \left(\frac{1}{2^{2M-1}+1} + \cdots + \frac{1}{2^{2M}}\right) \\ &> 1 + \underbrace{\frac{1}{2} + \frac{1}{2} + \cdots + \frac{1}{2}}_{2M \text{ times}} = M + 1 > M. \end{aligned}$$

Therefore the harmonic series diverges.

[Therefore for any M, there is some n such that $S_n > M$, so S_n tends to infinity, and therefore the harmonic series diverges.]

Exercises

1. "There are arbitrarily large numbers of the form $111\ldots11$ which are divisible by 7."
   - Rephrase this statement as "For all ..., there exists ... such that ...."
   - Then prove it. (Hint: $111111 = 15873 \cdot 7$.)
2. The infinite series $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots$ converges to $\frac{\pi^2}{6}$. This is obviously kind of tricky to prove, so we won't.
   - Prove that $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots \leq 2$. (Hint: a similar approach works.)
   - What would you need to show to prove that the sequence of partial sums DOES NOT tend to infinity, using the formal definition?
3. A number x is even if $x = 2y$ for some y, and odd if $x = 2y + 1$ for some y. Prove that all numbers are either even or odd.

Various kinds of mathematical statements

- $\exists x$: "Odd numbers exist".

  To prove this, you give an example of an odd number.

- $\forall x$: "All numbers are equal to themselves".

  To prove this, you say "Let n be any number", and then prove that $n = n$.

Various kinds of mathematical statements

- $\exists x$: "Odd numbers exist".

  To prove this, you give an example of an odd number.

- $\forall x$: "All numbers are equal to themselves".

  To prove this, you say "Let n be any number", and then prove that $n = n$.

- $\forall x \; \exists y$: See previous slides.

- $\exists x \; \forall y$: "There is a number x such that $x + y = y$ for all y."

  To prove this, you pick an x, and then do the $\forall$ proof.

Various kinds of mathematical statements

- $\exists x$: "Odd numbers exist".

  To prove this, you give an example of an odd number.

- $\forall x$: "All numbers are equal to themselves".

  To prove this, you say "Let n be any number", and then prove that $n = n$.

- $\forall x \, \exists y$: See previous slides.

- $\exists x \, \forall y$: "There is a number x such that $x + y = y$ for all y."

  To prove this, you pick an x, and then do the $\forall$ proof.

- $\forall x \, \exists y \, \forall z$ "For all x, there is a y such that $(x + y) + z = z$ for all z."

- ...

Proving things about sets

This is an exercise in unpacking notation. (You should have a reference sheet for all the notation I will use.) For example:

Theorem

$A \cap B \subseteq A$.

Proving things about sets

This is an exercise in unpacking notation. (You should have a reference sheet for all the notation I will use.) For example:

Theorem

$A \cap B \subseteq A$.

Proof.

First of all, $A \cap B \subseteq A$ means "for all $x \in A \cap B$, $x \in A$."

Proving things about sets

This is an exercise in unpacking notation. (You should have a reference sheet for all the notation I will use.) For example:

Theorem

$A \cap B \subseteq A$.

Proof.

First of all, $A \cap B \subseteq A$ means "for all $x \in A \cap B$, $x \in A$."

Suppose $x \in A \cap B$. Then $x \in A$ and $x \in B$.
Therefore $x \in A$.

Proving things about sets

This is an exercise in unpacking notation. (You should have a reference sheet for all the notation I will use.) For example:

Theorem

$A \cap B \subseteq A$.

Proof.

First of all, $A \cap B \subseteq A$ means "for all $x \in A \cap B$, $x \in A$."

Suppose $x \in A \cap B$. Then $x \in A$ and $x \in B$.
Therefore $x \in A$.

Therefore $\forall x \in A \cap B : x \in A$, which means $A \cap B \subseteq A$. □

Exercises in sets

Prove the following:

1. $A \subseteq A \cup B$.
2. $\emptyset \subseteq A$.
3. $A \cup \emptyset = A$.
4. $A \subseteq (A - B) \cup B$.
5. $(A - B) \cap (B - A) = \emptyset$.
6. Let $A \Delta B$ denote $(A - B) \cup (B - A)$. Prove that

$$(A \Delta B) \Delta (B \Delta C) \Delta (A \Delta C) = \emptyset.$$

Second warmup

1. Prove that if $\sqrt{2}$ is an integer, then it is odd.

2. Prove that if $\sqrt{2}$ is rational, then it is an integer.

Second warmup

1. Prove that if $\sqrt{2}$ is an integer, then it is odd.

   Since $1 < 2 < 4$, we have $\sqrt{1} < \sqrt{2} < \sqrt{4}$, so $1 < \sqrt{2} < 2$, and therefore $\sqrt{2}$ is not an integer. Therefore it is true that if $\sqrt{2}$ is an integer, it is odd.

2. Prove that if $\sqrt{2}$ is rational, then it is an integer.

Second warmup

1. Prove that if $\sqrt{2}$ is an integer, then it is odd.

   Since $1 < 2 < 4$, we have $\sqrt{1} < \sqrt{2} < \sqrt{4}$, so $1 < \sqrt{2} < 2$, and therefore $\sqrt{2}$ is not an integer. Therefore it is true that if $\sqrt{2}$ is an integer, it is odd.

2. Prove that if $\sqrt{2}$ is rational, then it is an integer.

   It suffices to prove that $\sqrt{2}$ is irrational.

   Suppose $\sqrt{2} = \frac{p}{q}$, where p and q are integers. Then $p^2 = 2q^2$. But the highest power of 2 dividing p^2 is even, while the highest power of 2 dividing $2q^2$ is odd. This is a contradiction, so $\sqrt{2}$ cannot be rational.

A simple induction proof

Theorem

For $n \geq 4$, $n! > 2^n$.

Proof.

Let $n = 4$; then $n! = 24 > 16 = 2^n$.

If $n > 4$ and $(n-1)! > 2^{n-1}$, then

$$n! = n \cdot (n-1)! > n \cdot 2^{n-1} > 2 \cdot 2^{n-1} = 2^n.$$

By induction, we have $n! > 2^n$ for all $n \geq 4$. □

The AM-GM inequality

Theorem (AM-GM)

For real numbers $a_1, \ldots, a_n \geq 0$*, if* $\mathrm{AM} = \frac{a_1 + \cdots + a_n}{n}$ *and* $\mathrm{GM} = (a_1 \cdot a_2 \cdots a_n)^{1/n}$*, then* $\mathrm{AM} \geq \mathrm{GM}$*.*

Proof outline.

We prove three things:

1. That $\mathrm{AM} \geq \mathrm{GM}$ for $n = 2$.
2. That the n case implies the $2n$ case.
3. That the n case implies the $n - 1$ case.

These implications give us a path to any value of n from the base case of 2 (though this claim needs proof). For example, to prove $n = 17$, we go

$$2 \Rightarrow 4 \Rightarrow 3 \Rightarrow 6 \Rightarrow 5 \Rightarrow 10 \Rightarrow 9 \Rightarrow 18 \Rightarrow 17.$$

By induction, $\mathrm{AM} \geq \mathrm{GM}$ for all n. □

The AM-GM inequality

1. Check that AM $\geq$ GM for $n = 2$.

   Start with $(\sqrt{a_1} - \sqrt{a_2})^2 \geq 0$. This means $a_1 + a_2 - 2\sqrt{a_1 a_2} \geq 0$, or $\frac{a_1+a_2}{2} \geq \sqrt{a_1 a_2}$.

2. Go from n to $2n$.

3. Go from n to $n - 1$.

The AM-GM inequality

1. Check that AM $\geq$ GM for $n = 2$.
2. Go from n to $2n$.

   Split the $2n$ inequality into two halves:

$$\frac{a_1 + \cdots + a_{2n}}{2n} = \frac{\frac{a_1+\cdots+a_n}{n} + \frac{a_{n+1}+\cdots+a_{2n}}{n}}{2}$$
$$\geq \frac{(a_1 \cdots a_n)^{1/n} + (a_{n+1} \cdots a_{2n})^{1/n}}{2}$$
$$\geq \left((a_1 \cdots a_n)^{1/n} \cdot (a_{n+1} \cdots a_{2n})^{1/n}\right)^{1/2}$$
$$= (a_1 \cdots a_{2n})^{1/2n}.$$

3. Go from n to $n - 1$.

The AM-GM inequality

1. Check that AM $\geq$ GM for $n = 2$.
2. Go from n to $2n$.
3. Go from n to $n - 1$.

   Let $\text{AM} = \frac{a_1 + \cdots + a_{n-1}}{n-1}$, and set $a_n = \text{AM}$. Then:

$$\begin{aligned} \text{AM} = \frac{a_1 + \cdots + a_n}{n} &\geq (a_1 \cdots a_{n-1} \cdot \text{AM})^{1/n} \\ \text{AM}^n &\geq (a_1 \cdots a_{n-1}) \cdot \text{AM} \\ \text{AM}^{n-1} &\geq (a_1 \cdots a_{n-1}) \\ \text{AM} &\geq (a_1 \cdots a_{n-1})^{1/n}. \end{aligned}$$

Induction exercises

1. Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ by induction on n.
2. (Recall that the Fibonacci numbers are defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.) Prove that F_{3n} is even for all n.
3. Prove that for all natural numbers n and for all real x, $(1 + x)^n \geq 1 + nx$. (This also holds for all real $n \geq 0$ when $x \geq -1$, a fact known as Bernoulli's inequality.)
4. Prove that for $n \geq 6$, $n! > n^3$.

Proving things with bijections

Theorem

$$\binom{n}{k} = \binom{n}{n-k}$$

Proof idea.

$\binom{n}{k}$ counts subsets of $\{1, 2, \ldots, n\}$ with k elements. $\binom{n}{n-k}$ counts subsets with $n - k$ elements. We can pair these up, by pairing the subset A, where $|A| = k$, with the subset $\{1, 2, \ldots, n\} - A$. Therefore the number of each type of subset is the same. □

The general technique is to prove $|X| = |Y|$ for two sets X, Y by finding a bijection $f : X \to Y$.

What is a bijection?

A bijection must satisfy two constraints:

1. It hits everything: $\forall y \in Y \ \exists x \in X : f(x) = y$.

What is a bijection?

A bijection must satisfy two constraints:

1. It hits everything: $\forall y \in Y \; \exists x \in X : f(x) = y$.

   Let B be a subset of $\{1, 2, \ldots, n\}$ of size $n - k$. Then $A = \{1, 2, \ldots, n\} - B$ is a subset of size k such that $f(A) = B$.

What is a bijection?

A bijection must satisfy two constraints:

1. It hits everything: $\forall y \in Y\ \exists x \in X : f(x) = y$.

   Let B be a subset of $\{1, 2, \ldots, n\}$ of size $n - k$. Then $A = \{1, 2, \ldots, n\} - B$ is a subset of size k such that $f(A) = B$.

2. It hits nothing twice: $\forall x_1, x_2 \in X : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

What is a bijection?

A bijection must satisfy two constraints:

1. It hits everything: $\forall y \in Y\ \exists x \in X : f(x) = y$.

   Let B be a subset of $\{1, 2, \ldots, n\}$ of size $n - k$. Then $A = \{1, 2, \ldots, n\} - B$ is a subset of size k such that $f(A) = B$.

2. It hits nothing twice: $\forall x_1, x_2 \in X : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

   Let A_1, A_2 be two subsets of size k. If $\{1, \ldots, n\} - A_1 = \{1, \ldots, n\} - A_2$, then $A_1 = A_2$. (Exercise!)

What is a bijection?

A bijection must satisfy two constraints:

1. It hits everything: $\forall y \in Y\ \exists x \in X : f(x) = y$.

   Let B be a subset of $\{1, 2, \ldots, n\}$ of size $n - k$. Then $A = \{1, 2, \ldots, n\} - B$ is a subset of size k such that $f(A) = B$.

2. It hits nothing twice: $\forall x_1, x_2 \in X : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

   Let A_1, A_2 be two subsets of size k. If $\{1, \ldots, n\} - A_1 = \{1, \ldots, n\} - A_2$, then $A_1 = A_2$. (Exercise!)

A shortcut is to exhibit an inverse: a function $f^{-1} : Y \to X$ such that $\forall x \in X : f^{-1}(f(x)) = x$. This is also easy here.

Euler's identity on partitions

Theorem (Euler)

The number of ways to write n as a sum of odd numbers is equal to the number of ways to write n as a sum of distinct numbers. E.g.,

$$\begin{aligned} 7 &= 7 \\ &= 5+1+1 \\ &= 3+3+1 \\ &= 3+1+1+1+1 \\ &= 1+1+1+1+1+1+1 \end{aligned} \qquad \begin{aligned} 7 &= 7 \\ &= 5+2 \\ &= 6+1 \\ &= 4+3 \\ &= 4+2+1 \end{aligned}$$

(Note: these are also known as partitions of n, and the summands are called parts.)

Euler's identity on partitions

Proof

We construct a bijection f from the first kind of partition to the second kind.

Let λ be a partition of n into odd parts. For each odd k, let r_k be the number of times k occurs in λ.

Euler's identity on partitions

Proof

We construct a bijection f from the first kind of partition to the second kind.

Let λ be a partition of n into odd parts. For each odd k, let r_k be the number of times k occurs in λ.

Write r_k as a sum of distinct powers of 2:

$$r_k = 2^{a_{k,1}} + 2^{a_{k,2}} + \cdots + 2^{a_{k,\ell(k)}}.$$

Euler's identity on partitions

Proof

We construct a bijection f from the first kind of partition to the second kind.

Let λ be a partition of n into odd parts. For each odd k, let r_k be the number of times k occurs in λ.

Write r_k as a sum of distinct powers of 2:

$$r_k = 2^{a_{k,1}} + 2^{a_{k,2}} + \cdots + 2^{a_{k,\ell(k)}}.$$

Then we obtain $f(\lambda)$ by making the following replacement, for each k:

$$\underbrace{k + k + \cdots + k}_{r_k \text{ times}} \rightsquigarrow k \cdot 2^{a_{k,1}} + k \cdot 2^{a_{k,2}} + \cdots + k \cdot 2^{a_{k,\ell(k)}}.$$

Euler's identity on partitions

Proof

We construct a bijection f from the first kind of partition to the second kind.

Let λ be a partition of n into odd parts. For each odd k, let r_k be the number of times k occurs in λ.

Write r_k as a sum of distinct powers of 2:

$$r_k = 2^{a_{k,1}} + 2^{a_{k,2}} + \cdots + 2^{a_{k,\ell(k)}}.$$

Then we obtain $f(\lambda)$ by making the following replacement, for each k:

$$\underbrace{k + k + \cdots + k}_{r_k \text{ times}} \rightsquigarrow k \cdot 2^{a_{k,1}} + k \cdot 2^{a_{k,2}} + \cdots + k \cdot 2^{a_{k,\ell(k)}}.$$

Exercise: describe the inverse of f.

Exercises with bijections

1. Prove that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ using a bijection.
2. The Catalan numbers count the number of ways to parenthesize $a_1 + a_2 + \cdots + a_n$: e.g., for $n = 3$, we can write $((a_1 + a_2) + a_3)$ or $(a_1 + (a_2 + a_3))$; for $n = 4$, one of the possibilities is $((a_1 + (a_2 + a_3)) + a_4)$.

   Prove that the Catalan numbers also count the number of paths from $(1, 1)$ to (n, n) which go up or to the right at each step and also stay within region where $x \geq y$. For $n = 3$, we have the paths