Minimal Criminal Proofs

Tyler Baylson, Zane Billings, Justin Kearse

Western Carolina University

October 24, 2019

Abstract

The least counterexample, or colloquially the "minimal criminal", is a technique for proving mathematical concepts. It ties in with functionality comparable to induction, and works by evaluating the *least* proposed counterexample. As such, this technique is useful in sets that have some ordered arrangement.

Outline

1. Technique
2. Example: Fundamental Theorem of Arithmetic
3. How it works
4. More Examples
   - The square root of 2 is irrational
   - Fibonacci Numbers
   - Freefall cannot break terminal velocity

Introduction

- Suppose we have an ordered set, such as the integers greater than zero.
- Also, suppose we have a statement P that may be true for everything in the set.
- If it isn't true for everything, then we can collect things for which it doesn't hold.

- Suppose we have an ordered set, such as the integers greater than zero.
- Also, suppose we have a statement P that may be true for everything in the set.
- If it isn't true for everything, then we can collect things for which it doesn't hold.
- Since the set is ordered, it is only logical that there is some *least* element where P doesn't hold.

The Well-Ordering Principle

Every nonempty set of nonnegative integers has a smallest element.

Technique

- State what you are trying to prove, as "$P(n)$ is true for all $n \in \mathbb{N}$".
- Set up a set C of counterexamples, $C = \{n \in \mathbb{N} | P(n) \text{ is false}\}$.
  Note: "$P(n)$ is false" is equivalent to other statements!
- Assume C is not empty.
- By the Well-Ordering Principle, there must be a smallest element $n_0 \in C$.
- Work out a contradiction - either show:
  - there is a smaller element $n_k < n_0$ such that $n_0 \in C \Rightarrow n_k \in C$, or
  - in fact, the element $n_0 \notin C$.
- Conclude that C is empty, thus there is no counterexample, and $P(n)$ is true for all $n \in \mathbb{N}$.

The contradiction is the reason for the name "minimal criminal"!

Fundamental Theorem of Arithmetic: Existence

Theorem

Every natural number $n > 1$ can be factored into a product of primes.

Fundamental Theorem of Arithmetic: Existence

Theorem

Every natural number $n > 1$ can be factored into a product of primes.

Proof.

- Suppose not. Let $X \subset \mathbb{N}$ be the set of all natural numbers which cannot be factored into a product of primes. Then, by the well-ordering principal, X has a least element, say n.

Fundamental Theorem of Arithmetic: Existence

Theorem

Every natural number $n > 1$ can be factored into a product of primes.

Proof.

- Suppose not. Let $X \subset \mathbb{N}$ be the set of all natural numbers which cannot be factored into a product of primes. Then, by the well-ordering principal, X has a least element, say n.
- We see that n itself cannot be prime. So, n must be composite, and thus $n = ab$ for some natural numbers a and b, both less than n.

Fundamental Theorem of Arithmetic: Existence

Theorem

Every natural number $n > 1$ can be factored into a product of primes.

Proof.

- Suppose not. Let $X \subset \mathbb{N}$ be the set of all natural numbers which cannot be factored into a product of primes. Then, by the well-ordering principal, X has a least element, say n.
- We see that n itself cannot be prime. So, n must be composite, and thus $n = ab$ for some natural numbers a and b, both less than n.
- Since n is the least natural number which cannot be factored into a product of primes, a and b can both be factored into a product of primes. But then, n must be a product of primes, and this is a contradiction!

Fundamental Theorem of Arithmetic: Existence

Theorem

Every natural number $n > 1$ can be factored into a product of primes.

Proof.

- Suppose not. Let $X \subset \mathbb{N}$ be the set of all natural numbers which cannot be factored into a product of primes. Then, by the well-ordering principal, X has a least element, say n.
- We see that n itself cannot be prime. So, n must be composite, and thus $n = ab$ for some natural numbers a and b, both less than n.
- Since n is the least natural number which cannot be factored into a product of primes, a and b can both be factored into a product of primes. But then, n must be a product of primes, and this is a contradiction!

So, X cannot have a least element and thus must be empty, and every natural number greater than one can be factored as a product of primes. $\square$

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ has a unique factorization into primes.

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ has a unique factorization into primes.

Euclid's Lemma

Let p be a prime and let $a, \ b$ be natural numbers. If p divides ab, then p divides a or p divides b.

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ has a unique factorization into primes.

Euclid's Lemma

Let p be a prime and let $a,\ b$ be natural numbers. If p divides ab, then p divides a or p divides b.

Proof.

- Let s be the smallest number which can be written as two distinct products of primes, say $p_1 p_2 \ldots p_n$ and $q_1 q_2 \ldots q_n$.

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ has a unique factorization into primes.

Euclid's Lemma

Let p be a prime and let a, b be natural numbers. If p divides ab, then p divides a or p divides b.

Proof.

- Let s be the smallest number which can be written as two distinct products of primes, say $p_1 p_2 \dots p_n$ and $q_1 q_2 \dots q_n$.
- Since q_1 and $q_2 \dots q_n$ are both less than s, they both have a unique prime factorization.

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ *has a unique factorization into primes.*

Proof.

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ has a unique factorization into primes.

Proof.

- Furthermore, since p_1 divides s, p_1 divides $q_1 q_2 \ldots q_n$. By Euclid's lemma, p_1 divides one of these q_i, say q_1 WLOG.

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ has a unique factorization into primes.

Proof.

- Furthermore, since p_1 divides s, p_1 divides $q_1 q_2 \ldots q_n$. By Euclid's lemma, p_1 divides one of these q_i, say q_1 WLOG.
- Since p_1 and q_1 are both prime, this means $p_1 = q_1$.

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ has a unique factorization into primes.

Proof.

- Furthermore, since p_1 divides s, p_1 divides $q_1 q_2 \ldots q_n$. By Euclid's lemma, p_1 divides one of these q_i, say q_1 WLOG.
- Since p_1 and q_1 are both prime, this means $p_1 = q_1$.
- Thus, by the cancellation property of the natural numbers, we see that $p_2 p_3 \ldots p_n = q_2 q_3 \ldots q_n = t$, where $t \in \mathbb{N}$.

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ has a unique factorization into primes.

Proof.

- Furthermore, since p_1 divides s, p_1 divides $q_1 q_2 \ldots q_n$. By Euclid's lemma, p_1 divides one of these q_i, say q_1 WLOG.
- Since p_1 and q_1 are both prime, this means $p_1 = q_1$.
- Thus, by the cancellation property of the natural numbers, we see that $p_2 p_3 \ldots p_n = q_2 q_3 \ldots q_n = t$, where $t \in \mathbb{N}$.
- So, t is strictly less than s, but we see that t has two distinct prime factorizations.

Fundamental Theorem of Arithmetic: Uniqueness

Theorem

Furthermore, every natural number $n > 1$ has a unique factorization into primes.

Proof.

- Furthermore, since p_1 divides s, p_1 divides $q_1 q_2 \ldots q_n$. By Euclid's lemma, p_1 divides one of these q_i, say q_1 WLOG.
- Since p_1 and q_1 are both prime, this means $p_1 = q_1$.
- Thus, by the cancellation property of the natural numbers, we see that $p_2 p_3 \ldots p_n = q_2 q_3 \ldots q_n = t$, where $t \in \mathbb{N}$.
- So, t is strictly less than s, but we see that t has two distinct prime factorizations.

So, s is not the least natural number with two unique prime factorizations and thus, every natural number greater than one has a unique prime factorization. $\square$

How it works

Note that we start off with a statement that is true for everything, by assertion.

In principle, we only need one counterexample.

Picking specifically the least one opens two ways to counter the counterexample:

- Showing n_0 is not a counterexample implies there are no counterexamples.
- Showing n_0 is not the least violates the least element assumption.
  recall: by the WOP, "every nonempty set $(\dots)$ has a least element",
  therefore there cannot be any counterexample elements.

How it works

Corresponding information: Mathematical induction

- Suppose a statement is true for a first element x_0.
- Suppose also the statement is provably true for a next element x_{i+1} when it is true for an element x_i.
- Or, suppose it is provably true for a next element x_{i+1} when it is true for all previous elements $x_0, x_1, x_2, \ldots, x_i$.
- Thus we see it is true for $x_0, x_1, x_2, \ldots$ *ad infinitum*.

Induction hinges upon being true for some first element!

The minimal criminal technique disrupts the first element.

The square root of 2 is irrational

claim

The square root of 2, $\sqrt{2}$ is irrational.

Proof.

The square root of 2 is irrational

claim

The square root of 2, $\sqrt{2}$ is irrational.

Proof.

- Suppose instead that $\sqrt{2}$ is a rational number. Let $\frac{p}{q}$ be the least fraction such that $\sqrt{2} = \frac{p}{q}$.

The square root of 2 is irrational

claim

The square root of 2, $\sqrt{2}$ is irrational.

Proof.

- Suppose instead that $\sqrt{2}$ is a rational number. Let $\frac{p}{q}$ be the least fraction such that $\sqrt{2} = \frac{p}{q}$.
- So we have that $2 = \frac{p^2}{q^2}$ and thus $2q^2 = p^2$, which means p^2 and thus p are even numbers.

The square root of 2 is irrational

claim

The square root of 2, $\sqrt{2}$ is irrational.

Proof.

- Suppose instead that $\sqrt{2}$ is a rational number. Let $\frac{p}{q}$ be the least fraction such that $\sqrt{2} = \frac{p}{q}$.
- So we have that $2 = \frac{p^2}{q^2}$ and thus $2q^2 = p^2$, which means p^2 and thus p are even numbers.
- Then, $p = 2m$, where m is some integer. So we see that $2q^2 = (2m)^2 = 4m^2$, and $q^2 = 2m^2$, so q^2 and thus q are even also. So we can say that $q = 2n$ for some integer n

The square root of 2 is irrational

claim

The square root of 2, $\sqrt{2}$ is irrational.

Proof.

- Suppose instead that $\sqrt{2}$ is a rational number. Let $\frac{p}{q}$ be the least fraction such that $\sqrt{2} = \frac{p}{q}$.
- So we have that $2 = \frac{p^2}{q^2}$ and thus $2q^2 = p^2$, which means p^2 and thus p are even numbers.
- Then, $p = 2m$, where m is some integer. So we see that $2q^2 = (2m)^2 = 4m^2$, and $q^2 = 2m^2$, so q^2 and thus q are even also. So we can say that $q = 2n$ for some integer n
- Hence, we can say $\sqrt{2} = \frac{2m}{2n} = \frac{m}{n}$. But this is a contradiction!

The square root of 2 is irrational

claim

The square root of 2, $\sqrt{2}$ is irrational.

Proof.

- Suppose instead that $\sqrt{2}$ is a rational number. Let $\frac{p}{q}$ be the least fraction such that $\sqrt{2} = \frac{p}{q}$.
- So we have that $2 = \frac{p^2}{q^2}$ and thus $2q^2 = p^2$, which means p^2 and thus p are even numbers.
- Then, $p = 2m$, where m is some integer. So we see that $2q^2 = (2m)^2 = 4m^2$, and $q^2 = 2m^2$, so q^2 and thus q are even also. So we can say that $q = 2n$ for some integer n
- Hence, we can say $\sqrt{2} = \frac{2m}{2n} = \frac{m}{n}$. But this is a contradiction!

This contradicts our assumption that $\frac{p}{q}$ is the smallest fraction equal to $\sqrt{2}$, and thus we can say that there is no fraction equivalent to $\sqrt{2}$. $\square$

Fibonacci Numbers

Claim.

The n^{th} Fibonacci number is at most 2^n for all natural numbers n.

Fibonacci Numbers

Claim.

The n^{th} Fibonacci number is at most 2^n for all natural numbers n.

Fibonacci numbers

$$F_0 = 1$$

$$F_1 = 1$$

$$F_n = F_{n-1} + F_{n-2}$$

Fibonacci Numbers

Claim.

The n^{th} Fibonacci number is at most 2^n for all natural numbers n.

Fibonacci numbers

$$F_0 = 1$$

$$F_1 = 1$$

$$F_n = F_{n-1} + F_{n-2}$$

The first 10 terms of this sequence are $1, 1, 2, 3, 5, 8, 13, 21, 34, 55$.

Fibonacci Numbers

Claim.

The n^{th} Fibonacci number is at most 2^n for all natural numbers n.

Fibonacci numbers

$$F_0 = 1$$

$$F_1 = 1$$

$$F_n = F_{n-1} + F_{n-2}$$

The first 10 terms of this sequence are $1, 1, 2, 3, 5, 8, 13, 21, 34, 55$.

Example

n	0	1	2	3	4	5
F_n	1	1	2	3	5	8
2^n	1	2	4	8	16	32

Fibonacci Numbers

Claim

.

$$F_n \leq 2^n \; \forall n \in \mathbb{N}.$$

Fibonacci Numbers

Claim

.

$$F_n \leq 2^n \ \forall n \in \mathbb{N}.$$

Proof.

Suppose not.

Fibonacci Numbers

Claim

.

$$F_n \leq 2^n \ \forall n \in \mathbb{N}.$$

Proof.

Suppose not.

- Then, let x be the smallest such number where this is not true. That is, x is the smallest number such that $F_x = F_{x-1} + F_{x-2} > 2^n$. Assume $x \geq 2$ (from the table constructed, we can make this assumption).

Fibonacci Numbers

Claim

.

$$F_n \leq 2^n \ \forall n \in \mathbb{N}.$$

Proof.

Suppose not.

- Then, let x be the smallest such number where this is not true. That is, x is the smallest number such that $F_x = F_{x-1} + F_{x-2} > 2^n$. Assume $x \geq 2$ (from the table constructed, we can make this assumption).
- Then, since x is the smallest number breaking the claim and $x-1$ and $x-2$ are both less than x, we have $F_{x-1} \leq 2^{x-1}$ and $F_{x-2} \leq 2^{x-2}$.

Fibonacci Numbers

Claim

.

$$F_n \leq 2^n \ \forall n \in \mathbb{N}.$$

Proof.

So we have the following.

$$F_x = F_{x-1} + F_{x-2}$$
$$F_x \leq 2^{x-1} + 2^{x-2} = 2^{x-2}(2+1) = 2^{x-2}(3)$$
$$F_x < 2^{x-2}\left(2^2\right) = 2^x$$

Fibonacci Numbers

Claim

.

$$F_n \leq 2^n \ \forall n \in \mathbb{N}.$$

Proof.

So we have the following.

$$F_x = F_{x-1} + F_{x-2}$$
$$F_x \leq 2^{x-1} + 2^{x-2} = 2^{x-2}(2+1) = 2^{x-2}(3)$$
$$F_x < 2^{x-2}\left(2^2\right) = 2^x$$

But, this contradicts our original assumption! So there is no least element breaking the claim, and thus the claim is true for all natural numbers. □

Example: Freefall cannot break terminal velocity

Suppose the contrary is true, that an object in freefall can meet or exceed terminal velocity.

Presuming the object started with a 0 velocity, there must be some first moment t where it meets or exceeds terminal velocity (v_∞). Therefore at the moment prior, it is slower than v_∞, and accelerates to a velocity $\geq v_\infty$.

Let us designate the moment prior as $t - \delta$ for an infinitely small $\delta > 0$.

We can model freefall with the differential equation $\frac{dv}{dt} = \sum F = F_g + F_R$, where F_g is the constant force of gravity g and F_R is the air resistance. F_R increases as an object accelerates, thus $F_R = k^* v$, and opposes F_g. Combined, we have $\frac{dv}{dt} = g - kv$, where $v > 0$ is in the downward direction.

Example: Freefall cannot break terminal velocity

Minimal element: some first moment where $v_t \geq v_\infty$

Freefall model: $\frac{dv}{dt} = g - kv$

Note: $\frac{dv}{dt} = \lim_{\Delta \to 0} \frac{v_t - v_{(t-\Delta)}}{\Delta}$, thus we equate $\frac{dv}{dt} = \frac{v_t - v_{(t-\delta)}}{\delta}$, from which we derive:

$$\frac{dv}{dt}\delta = v_t - v_{(t-\delta)} \qquad v_{(t-\delta)} + \frac{dv}{dt}\delta = v_t \qquad v_{(t-\delta)} = v_t - \frac{dv}{dt}\delta$$

Also, for later brevity we derive v_∞ as follows:
At terminal velocity v_∞, the velocity is stable, i.e. $\frac{dv}{dt} = 0$. Thus:

$$0 = g - kv_\infty$$
$$kv_\infty = g$$
$$v_\infty = \frac{g}{k}$$

We have two cases:

- $v_t = v_\infty$
- $v_t > v_\infty$

Example: Freefall cannot break terminal velocity

Minimal element: some first moment where $v_t \geq v_\infty$

Freefall model: $\frac{dv}{dt} = g - kv$ $\quad v_{(t-\delta)} = v_t - \frac{dv}{dt}\delta$ $\quad v_\infty = \frac{g}{k}$

We have two cases:

- $\mathbf{v_t = v_\infty}$. Since $v_t = v_\infty$, then $\frac{dv}{dt} = 0$, and we have:

$$\begin{aligned} v_{(t-\delta)} &= v_t - \frac{dv}{dt}\delta \\ &= v_t - 0 \cdot \delta \\ &= v_t - 0 \\ &= v_t \\ &= v_\infty \end{aligned}$$

Well, that contradicts our *first moment* assumption. Let's try $v_t > v_\infty$.

Example: Freefall cannot break terminal velocity

Minimal element: some first moment where $v_t \geq v_\infty$

Freefall model: $\frac{dv}{dt} = g - kv$ $\quad v_{(t-\delta)} = v_t - \frac{dv}{dt}\delta$ $\quad v_\infty = \frac{g}{k}$

We have two cases: $\cancel{v_t = v_\infty}$

- $\mathbf{v_t > v_\infty}$. Since $v_t > v_\infty$, then:

$$
\begin{aligned}
kv_t &> kv_\infty \\
-kv_t &< -kv_\infty \\
g - kv_t &< g - kv_\infty \\
g - kv_t &< g - k\left(\frac{g}{k}\right) \\
\frac{dv}{dt} &< 0 \\
\\
\frac{dv}{dt}\delta &< 0 \\
-\frac{dv}{dt}\delta &> 0
\end{aligned}
$$

and we have:

$$
\begin{aligned}
v_{(t-\delta)} &= v_t - \frac{dv}{dt}\delta \\
&= v_t + \left(-\frac{dv}{dt}\delta\right) \\
&> v_t + 0 \\
&> v_t \\
&> v_\infty
\end{aligned}
$$

This, too, contradicts our *first moment* assumption!. (Or, alternately, freefall)

Example: Freefall cannot break terminal velocity

Minimal element: some first moment where $v_t \geq v_\infty$

Freefall model: $\frac{dv}{dt} = g - kv$ $\qquad v_{(t-\delta)} = v_t - \frac{dv}{dt}\delta$ $\qquad v_\infty = \frac{g}{k}$

We have two cases:

- $\cancel{v_t = v_\infty}$
- $\cancel{v_t > v_\infty}$

Thus in both cases, we have a contradiction. Our only conclusion therefore is that our minimal element cannot exist, i.e. there are no "first moments" where a free-falling object breaks terminal velocity, thus proving that a free-falling object cannot break terminal velocity. $\square$

Minimal Criminal Proofs

Tyler Baylson, Zane Billings, Justin Kearse

Western Carolina University

October 24, 2019

References