Minimal Criminal Arguments

Tyler Baylson, Zane Billings & Justin Kearse

25 October, 2019

Abstract

Proof using a minimum counterexample, or informally, a minimal criminal, argument, is a versatile proof technique which can be applied to disparate problems in pure mathematics, as well as to some problems in applied mathematics. We provide a definition, explanation, and algorithm for minimal criminal arguments, and additionally supply several examples where a minimal criminal argument is used. Examples include problems from number theory and physics.

Contents

1 Introduction

Proof using a minimum counterexample, or informally a minimal criminal argument, is a specific type of proof by contradiction which can be applied to proofs of propositions about totally ordered sets. The set of all possible counterexamples to a statement is considered to be a subset of all possible objects the statement applies to, and the least counterexample (using the order on the set) is considered. In these proofs, this minimal counterexample can be shown to either not exist at all, or not actually be the true minimum of the set. Either of these results proves that the set of all counterexamples must be empty, and thus there are no counterexamples to the original statement.

2 Method

While minimal criminal arguments can be used for a wide variety of proofs, all of these proofs generally follow the same general structure. Given some totally ordered set and a statement which we want to show is true for all members of this totally ordered set, we employ a contradiction argument. The contradiction argument aims to show that the statement has no counterexamples, and relies on the Well-Ordering Principle (or one of its equivalencies).

2.1 The Well-Ordering Principle

Theorem 1 (Well-Ordering Principle)**.** *Every nonempty set of nonnegative integers contains a least element. [1]*

The Well-Ordering Principle is equivalent to the Axiom of Choice [2], and as such no proof is given and the Well-Ordering Principle can be taken as an axiom. Using a minimal criminal argument relies on the truth of the Well-Ordering Principle: the least element of the set of counterexamples to a statement is considered, and without the Well-Ordering Principle, the existence of a least element in every set of counterexamples (all subsets of the natural numbers) would be extremely difficult to show, whereas the Well-Ordering Principle guarantees the existence of this element.

2.2 General Algorithm

Suppose we have some statement P, which we want to prove is true for all natural numbers $\mathbb{N}$ (this can generalize to well-ordered sets, but the natural numbers are the most common and easiest set to think about).

The first step in constructing a minimal criminal argument is to begin an argument by contradiction. So, we assume that there exists at least one natural number n^* such that $P(n^*)$ is false. That is, there is at least one counterexample to P. So, let $C \subset \mathbb{N}$ be the set of all natural numbers for which P is false. By the Well-Ordering Principle (or one of its equivalencies), C must have a least element, since $C \subset \mathbb{N}$. So, we consider the least element of C, which we will call n_0.

Then, the next step in forming a minimal criminal argument is to use the premises of the problem to derive a contradiction involving this minimum counterexample, n_0. Typically, the contradiction in a minimal criminal argument is in one of two forms.

1. The existence of the least element $n_0 \in C$ implies the existence of some $n_k \in C$ such that $n_k < n_0$, which contradicts the assumption that n_0 is the least element of C; or

2. In fact, the element n_0 cannot actually be a member of C, and the statement $P(n_0)$ is true, which contradicts our assumption about the truth value of $P(n_0)$.

The element n_0 is called the "minimal criminal" informally because assuming n_0 to be the minimum counterexample leads to a contradiction. Either of these contradictions leads to the conclusion that the set C does not have a least element, and thus by the Well-Ordering Principle, the set C must be empty.

Since the set of counterexamples C is empty, the statement $P(n)$ is true for all natural numbers n, exactly what we wanted to prove.

3 Relating Minimal Criminal to Mathematical Induction

If you review the minimal criminal technique closely, you will see that there is a very conspicuous relationship to mathematical induction. To see what is happening, note that these proofs start off with a statement that is true for everything, by assertion. In principle, we only need one counterexample, and the minimal criminal technique assumes such a counterexample exists. Further, it defines a set C of all such counterexamples. From the Well-Ordering Principle, we are guaranteed a *least* counterexample.

Focusing on the least counterexample gives us two ways to counter the counterexample. If you can take that least element and demonstrate that it actually isn't the least counterexample, this implies that there are no counterexamples.

Where this connects to mathematical induction is a very foundational part of the induction process. If you recall, induction begins with a statement that is true for a first element x_0. If the statement is provably true for a next element $x_{(i+1)}$ when it is true for an (arbitrary) element x_i, or better yet when it is provably true for this next element $x_{(i+1)}$ when it is true for *all* previous elements up to and including x_i, then induction very simply yields that the truth for x_0 implies that it is true for $x_1, x_2, \ldots$ *ad infinitum*.

You will notice, induction is dependent on being true for some first element. Without this, induction has no starting point from which to guarantee the truth of later elements.

Minimal criminal is related to induction by the specific targeting of the least counterexample to a statement. Where induction takes a first element and then guarantees truth for all later elements, the minimal criminal's disruption of the first counterexample guarantees there cannot be any such counterexamples.

4 Example Proofs using a Minimal Criminal Argument

The minimal criminal technique can be used to prove conjectures from several areas of pure mathematics, including number theory and algebra, and can also be used in applied mathematics. We present several diverse examples of proofs where a minimal criminal argument is useful.

4.1 Irrationality of the Square Root of 2

The proof that the number $\sqrt{2}$ is irrational using coprimality is extremely famous and well-known to most mathematicians. However, several proofs of the statement exist, and one such proof employs a minimal criminal argument which is arguably just as elegant as the well-known proof.

Claim 1. *The square root of 2, $\sqrt{2}$, cannot be written as a ratio of integers (i.e. $\sqrt{2}$ is irrational).*

Proof. We begin by supposing that instead, $\sqrt{2}$ is a rational number. Let $\frac{p}{q}$ be the least fraction such that $\sqrt{2} = \frac{p}{q}$ (since we have assumed that $\sqrt{2}$ is a rational number), where p and q are both natural numbers with $q \neq 0$ (since $\sqrt{2}$ is positive, both p and q must be positive as well).

Then, we have that $2 = \frac{p^2}{q^2}$ and hence $2q^2 = p^2$. This implies that p^2 is an even number, and thus that p is an even number. Since p is even, we can say $p = 2m$, where m is some integer. So we see that $2q^2 = (2m)^2 = 4m^2$, and that $q^2 = 2m^2$. This implies that q^2 is even, and thus that q itself is even, so we can say that $q = 2n$ for some integer n.

Hence, we can say $\sqrt{2} = \frac{2m}{2n} = \frac{m}{n}$. But, since we cancelled out a factor, m must be less than p and n must be less than q. 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 smallest fraction equation to $\sqrt{2}$, making $\sqrt{2}$ irrational. □

4.2 Every fraction is reducible

Using a minimal criminal argument, we can show that every fraction can be reduced to lowest terms.

Claim 2 (Lowest form fractions)**.** *For any positive integers m and n, the fraction $\frac{m}{n}$ can be written in lowest terms, that is, in the form $\frac{m'}{n'}$, where m' and n' are positive integers with no common prime factors.*

Proof. First, suppose the negation is true: Let C be the nonempty set of numerators such that $\frac{m}{n}$ cannot be written in lowest terms, for some positive integers m, n. Let m_0 be the smallest such element of C. Then, by the definition of C, there exists a positive integer n_0 such that $\frac{m_0}{n_0}$ cannot be written in lowest terms.

This means m_0 and n_0 have a common prime factor, $p > 1$. We can multiply $\frac{m_0}{n_0}$ by $1 = \frac{\frac{1}{p}}{\frac{1}{p}}$ to give us $\frac{\frac{m_0}{p}}{\frac{n_0}{p}}$. Since $\frac{m_0}{n_0}$ cannot be written in lowest terms, neither can $\frac{\frac{m_0}{p}}{\frac{n_0}{p}}$. Therefore, $\frac{m_0}{p} \in C$.

Because $\frac{m_0}{p} < m_0$, we contradict the statement that m_0 is the smallest element in C. Since the assumption that C is nonempty leads to a contradiction, C must be empty. Thus, there are no numerators of fractions that can't be written in lowest terms, and hence there are no such fractions at all. □

4.3 Fundamental Theorem of Arithmetic

One of the most famous minimal criminal proofs is arguably Euclid's proof of the Fundamental Theorem of Arithmetic.

Theorem 2 (Fundamental Theorem of Arithmetic)**.** *Every natural number greater than one can be written as a unique product of prime numbers, up to the reordering of the numbers. [3]*

Proofs in number theory which work with nonnegative integers tend to be extremely convenient places to apply a minimal criminal argument, as the nonnegative integers have an obvious and natural total order. We begin the proof by constructing the set of counterexamples, and then we show that this set must be empty, implying the statement is true for all natural numbers greater than one.

Claim 3. *First, every natural number greater than one can be written as a product of primes (if we write the natural number n as a product of primes, we call this the prime factorization of n).*

Proof. Suppose not. Then, there is some set, say S, which is a subset of the natural numbers greater than one, containing all of these numbers which cannot be written as a product of primes. By the Well-Ordering Principle, S has a smallest element, say n. That is, n is the smallest natural number greater than one which cannot be written as a product of primes.

If n were prime, then n would already be written as a product of primes by definition, so n must not be prime. Thus, $n = ab$ for some a and b, both natural numbers greater than one. Then, a and b are both strictly less than n. Since n is by assumption the least element which cannot be written as a product of primes, so both a and b can be written as a product of primes. But then, ab is also a product of primes, and thus n can be written as a product of primes. So, n is actually not in the set of counterexamples. Since the set of counterexamples no longer has a least element, this set must be empty as a consequence of the Well-Ordering Principle. Thus, every natural number greater than one can be written as a product of prime numbers. □

Furthermore, all natural numbers greater than one have exactly one unique prime factorization. In order to show that prime factorization of each of these numbers is unique, we will again employ a minimal criminal argument. However, we will need one additional tool, concerning the divisibility of products, to prove this statement. Apostol provides an excellent and terse proof in the given reference.

Theorem 3 (Euclid's Lemma)**.** *Let a and b be nonnegative integers and let p be a prime number such that p divides ab. Then, p divides a or p divides b. [1]*

Claim 4. *Every natural number greater than one has a **unique** prime factorization.*

Proof. Again, to show this is true, first suppose not. Let x be the least natural number greater than one which has at least two prime factorizations. Then, $x = p_1p_2 \dots p_n = q_1q_2 \dots q_m$, where p_i and q_i are prime numbers, and m and n are natural numbers.

Now, since $x = p_1p_2 \dots p_n = q_1q_2 \dots q_m$, we can say that p_1 divides x, and furthermore that p_1 divides the product $q_1q_2 \dots q_m$. By Euclid's Lemma, p_1 must divide at least one of these q_i, say q_1 for convenience without loss of generality. But, since p_1 and q_1 are both prime, if p_1 divides q_1, then $p_1 = q_1$.

Then, by the cancellation property of the integers we see that $p_2p_3 \dots p_n = q_2q_3 \dots q_m = y$, where y is some natural number greater than one. Since all of the factors are natural numbers, y must be strictly less than x since we have canceled out a factor. This number y is then both strictly less than x and has two prime factorizations. This violates our assumption that x is the least element with more than one prime factorization, which implies that all natural numbers greater than one must have a unique prime factorization. □

4.4 Fibonacci Numbers

Another example of proof by minimal counterexample involves the famous Fibonacci sequence.

Definition 1 (Fibonacci numbers)**.** The sequence of Fibonacci numbers is defined by the following recursive relationship.

$$F_0 = 1;\ F_1 = 1;\ F_n = F_{n-1} + F_{n-2} \text{ for } n > 1.$$

The first few Fibonacci numbers are displayed in the table below.

n	0	1	2	3	4	5	6
$F(n)$	1	1	2	3	5	8	13

Table 1: The values of n and $F(n)$ for $n \in [0, 6]$.

We make the following claim about the sequence of Fibonacci numbers, which can be proven with a minimal criminal argument.

Claim 5. *The n^{th} Fibonacci number, F_n, is at most 2^n for all natural numbers n.*

Proof. Suppose that the claim is not true, i.e. that there is some Fibonacci number F_n such that $F_n > 2^n$.

Let x be the smallest number such that $F_x > 2^x$. From Table 1, we see that $F_0 = 2^0$ and $F_1 < 2^1$, so assume $x \geq 2$. By the definition of the Fibonacci numbers, we have that

$$F_x = F_{x-1} + F_{x-2},$$

and all of these terms are guaranteed to be defined since $x \geq 2$. Since x is the smallest index such that $F_x > 2^x$, we have that

$$F_{x-1} \leq 2^{x-1}; \text{ and } F_{x-2} \leq 2^{x-2},$$

which implies that

$$F_x = F_{x-1} + F_{x-2} \leq 2^{x-1} + 2^{x-2}.$$

So, we see that

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

Therefore, we have that

$$F_x > 2^x$$

by assumption, but we have just calculated that

$$F_x < 2^x,$$

which is clearly a contradiction! So we see that x does not actually satisfy the desired condition, implying that the claim is true for all natural numbers. □

4.5 Terminal Velocity

In the previous examples we used the natural numbers, however this technique is not exclusive to them. As stated, this technique can be applied to propositions on totally ordered sets, so we feature the next proof regarding an object's velocity through time to show how it can be leveraged.

Claim 6. *The velocity of a freefalling object cannot break terminal velocity.*

In this claim, we will be investigating the relationship of velocity through time, where our order will be in the forward progression of time. Before diving into this proof, we need to identify three things:

- a mathematical model of how velocity changes through time
- a relationship between one moment's velocity and the previous moment's velocity, and
- a definition of terminal velocity

Since we are considering an object in freefall, we can borrow from the discipline of physics to model our object's velocity, denoted v. We will use the convention that $v > 0$ indicates velocity in the downward direction, that $t - \delta$ is the time of our moment prior to t for some infinitely small $\delta > 0$, and presume the object started with a 0 velocity. At any given time, our object is subjected to multiple forces, and the imbalance thereof causes our object to change velocity. Particularly for freefall, our object experiences two forces: the force of gravity accelerating the object towards the ground, as well as the force of air resistance as it passes through the atmosphere. The force of

air resistance opposes the current velocity of the object, and it increases as the object accelerates, giving us $F_R = k * v$, for some $k \in \mathbb{R}$. Thus we can model the change in velocity with the equation:

$$\frac{dv}{dt} = \sum F = F_g + F_R = g - kv \tag{1}$$

Next, to relate the velocity between a given moment and the exact previous moment, we will invoke the limit definition of the derivative. Since we use our infinitely small δ we equate the limit definition to a specific formula. Then, for our purposes we solve it for the term $v_{(t-\delta)}$. This give us:

$$\frac{dv}{dt} = \lim_{\Delta \to \infty} \frac{v_t - v_{(t-\Delta)}}{t-(t-\Delta)} = \lim_{\Delta \to \infty} \frac{v_t - v_{(t-\Delta)}}{\Delta} \quad \text{becomes} \quad \frac{dv}{dt} = \frac{v_t - v_{(t-\delta)}}{\delta} \quad \text{and thus} \quad v_{(t-\delta)} = v_t - \frac{dv}{dt}\delta \tag{2}$$

Finally, we observe that terminal velocity is defined as the velocity v_∞ which an object tends to over time, and in particular make the observation that terminal velocity is stable. To give this with an equation:

$$\frac{dv}{dt} = g - kv_\infty = 0 \tag{3}$$

We then proceed with our proof by minimal criminal.

Proof. Let us consider some object in freefall that started with an initial velocity $v_0 = 0$. Suppose to the contrary that an object in freefall can meet or exceed terminal velocity. Therefore there is at least one moment where its velocity is at least v_∞. Considering these moments in the forward progression of time, we know that there must be some first moment t where the object meets or exceeds terminal velocity, i.e. $v_t \geq v_\infty$, due to the Well-Ordering Principle.

We therefore have two cases to consider: either $v_t = v_\infty$, or $v_t > v_\infty$.

For the first case, suppose that at this first moment, $v_t = v_\infty$. By equation 3, we then have that $\frac{dv}{dt} = 0$, and if we use this in equation 2, we see that $v_{(t-\delta)} = v_t - (0)\delta = v_t - 0 = v_t$. This gives us that $v_{(t-\delta)} = v_t = v_\infty$, which contradicts our assumption that t is the *first* moment.

Next we suppose that at this first moment, $v_t > v_\infty$. For this case our inequality stops us from running v_t through an equation to define $v_{(t-\delta)}$, but we can build up the inequality in a useful way. Using a careful sequence of multiplication and addition on both sides, we see $v_t > v_\infty$ becomes $kv_t > kv_\infty$, then $g - kv_t < g - kv_\infty$. By the substitution of equations 1 and 3, we then get $\frac{dv}{dt} < 0$, and continued multiplication yields $-\frac{dv}{dt}\delta > 0$. Since that is the case, we can break down equation 2 to show $v_{(t-\delta)} = v_t + (-\frac{dv}{dt}\delta)$, and therefore $v_{(t-\delta)} > v_t + 0$, which finally gives $v_{(t-\delta)} > v_t$. Lastly, since $v_t > v_\infty$ by assumption, then $v_{(t-\delta)} > v_t > v_\infty$. However, $v_{(t-\delta)} > v_\infty$ again contradicts our assumption that t is the *first* moment.

Therefore in both cases our assumption that there was a *first* moment of an object breaking terminal velocity led to the implication that there was a previous moment, which contradicts the first element in our counterexamples. As such, there are no such first elements where an object meets terminal velocity, and our only conclusion is that the claim is true, thus the velocity of a freefalling object cannot break terminal velocity. □

5 Conclusion

Minimal criminal arguments can be applied to several problems from diverse fields of mathematics, from basic principles of number theory to problems in applied physics. Minimal criminal arguments are justified by the Well-Ordering Principle (so do not use minimal criminal arguments when you work in a system where the Axiom of Choice is invalid). Using a minimal criminal argument typically involves several similar steps regardless of the field, and there is a straightforward algorithm to employing this type of argument.

References

[1] Tom Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, 1976.

[2] Gregory H. Moore. *Zermelo's axiom of choice: Its origins, development & influence.* Dover Publications, 1982.

[3] G.H. Hardy and E.M Wright. *An Introduction to the Theory of Numbers.* Oxford mathematics, sixth edition, 1938.

[4] Eric Lehman, Tom Leighton, and Albert Meyer. Chapter 3, course notes, 6.042j mathematics for computer science, fall 2010, 2010. Available at https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-042j-mathematics-for-computer-science-fall-2010/readings/MIT6_042JF10_chap03.pdf (2019/10/16).

[5] Chittu Tripathy and Albert Meyer. Lecture 6, proofs: The well ordering principle, compsci 230, summer 2013, 2013. Available at https://www2.cs.duke.edu/courses/summer13/compsci230/restricted/lectures/L06.pdf (2019/10/16).