Minimal Counterexample Technique

S. Kumaresan
kumaresa@gmail.com

17 August, 2020

Abstract

We explain the basic idea of the technique and illustrate with examples from Number theory, linear algebra and three basic results in the theory of finite groups.

It is well-known that the Principle of (Mathematical) Induction and the Well-ordering Principle are equivalent. So, in theory, it should be possible to offer a proof of any result proved using the former by employing the latter principle. The basic idea of such an approach runs as follows.

Assume that $A \subset \mathbb{N}$ is a nonempty subset. Assume that we wish to show that each $n \in A$ has a property "P". We prove this by contradiction. The set $S \subset A$ of the numbers $n \in A$ for which the result is false is non-empty. By the well-ordering principle, S has a least element. Let $m \in S$ be the least element. Let $k \in A$ be any number such that $k < m$ or k is a proper factor of m. Then $k \notin S$. Using this we somehow show that $m \notin S$! This contradiction shows that no such m exists. In other words, $S = \emptyset$. Note that this proves that each element of A has the required property P.

The natural number m in the discussion above is called a *minimal counterexample.*

Observe that in some sense the technique seems to be a 'reverse process' of the induction argument.

Let us illustrate this approach with a simple example.

Theorem 1. *Let $n \in N$ be such that $n > 1$. Then there exists a prime $p \in \mathbb{N}$ which divides n.*

Proof. Let $A = \{n \in \mathbb{N} : n > 1\}$. Let the property P be defined as "the existence of a prime divisor". Let S be the set of natural numbers $n \in A$ which do not have any prime divisor. If $S = \emptyset$, we are through. So, we assume that $S \neq \emptyset$. By the well-ordering principle, there exists $m \in S$ which is the least element of S. Note that $m > 1$.

What does this entail? If $1 < k < m$, then k has a prime divisor.

Now either m has a proper divisor or not. If m has a proper divisor, say, d, then $1 < d < m$. Hence there exists a prime p which divides d and hence m, a contradiction. If m has no proper divisor, it means that if k divides m, then $k = 1$ or $k = m$. That is, m is a prime and hence the prime m divides m, again a contradiction. We therefore conclude no such m exist. In other words, S must be empty. □

Using the same idea, you may prove the following result. We leave it as an easy exercise for the reader.

Theorem 2. *Let $n > 1$ be a natural number. Then n is a product of primes.* □

Let us now illustrate the technique in Linear Algebra. We intentionally formulate the result in a 'qualitative manner' rather than a quantitative way.

Theorem 3. *Any (finite) set of nonzero eigenvectors corresponding to distinct eigenvalues of a linear map on a (finite dimensional) vector space is linearly independent.*

Proof. Let us understand the statement. Let $T\colon V \to V$ be a linear map on a vector space V (over a field K). Let v_j, $1 \leq j \leq n$, be a set of nonzero vectors in V such that there exist scalars $\lambda_j \in K$ such that $Tv_j = \lambda_j v_j$, $1 \leq j \leq n$. We further assume that $\lambda_i = \lambda_j$ iff $i = j$. Then we are required to show that the set $\{v_j : 1 \leq j \leq n\}$ is linearly independent.

How do we form the subset $A \subset \mathbb{N}$ as in the idea above? Let $n \in \mathbb{N}$. Then $n \in A$ iff *any* set of n nonzero eigenvectors of T corresponding to distinct eigenvalues of T are linearly independent.

Let S be the set of those n which are not in A. If S were nonempty, let $m \in S$ be the least element. What does this mean? If $1 \leq k < m$ and if there exist k nonzero vectors $v_1, \dots, v_k$ and k distinct scalars $\lambda_1, \dots, \lambda_k$ such that $Tv_j = \lambda_j v_j$ for $1 \leq j \leq k$, then the set $\{v_j : 1 \leq j \leq k\}$ is linearly independent.

Let $c_j \in K$ be such that $c_1 v_1 + \cdots + c_m v_m = 0$ with at least one $c_j \neq 0$. Can any c_j be zero? If $c_j = 0$, then we have $k = m - 1 < m$ nonzero vectors $\{v_i : 1 \leq i \leq m, i \neq j\}$ such that $c_1 v_1 + \cdots + c_{j-1} v_{j-1} + c_{j+1} v_{j+1} + \cdots + c_m v_m = 0$, with at least one c_i nonzero. Thus, $\{v_i : 1 \leq i \leq m, i \neq j\}$ is a set of $m - 1$ eigenvectors with distinct eigenvalues which are linearly dependent, that is, $m - 1 \in S$. This contradicts the minimality of m. So, we conclude that $c_j \neq 0$ for $1 \leq j \leq m$.

Let us apply $(T - \lambda_1 I)$ on both sides of the equation $\sum_j c_j v_j = 0$ to obtain

$$c_2(\lambda_2 - \lambda_1)v_2 + \cdots + (c_m(\lambda_m - \lambda_1)v_m = 0.$$

Note that each of the coefficients on the right side expression is non-zero. (Why?) The argument above shows that this contradicts the minimality of m. Hence no such m exists. In other words, $S = \emptyset$. □

Please go through the proof once again. In order to explain in detail, the proof looks longer than necessary but the idea and its execution are simple.

Now let us explain how the minimal counterexample technique offers simple and elegant proofs of some of the well-known results in the theory of finite groups. I understand that this technique was systematically used by Feit and Thompson in their work on Finite groups.

As earlier, let us give a rough sketch how the argument will go in the minimal counterexample technique in group theory.

Let P be a result about finite groups. Let A be a nonempty subset of natural numbers. We wish to prove that the result is true for each group G whose order $n \in A$. We assume that this is false. Then the set $S \subset A$ of those numbers n, for which we can find a group G with $|G| = n$ but the result is not true, is not empty. Note that $\emptyset \neq S \subset A$. Let m the least element of S. Then there is a group G such that $|G| = m$ but the result is false for G. Such a G is called a *minimal counterexample* for the result. It follows that if $H \leq G$ is a proper subgroup or if G/K is a proper quotient group, each of their orders is greater than 1 and less than $|G|$. If these orders are in A, then the result is true for H and G/K. We use this information to arrive at a contradiction. Usually we show that the result is true for G! Hence $S = \emptyset$ or the result is true for all $n \in A$.

Do not worry, if you find what went above is vague. The first application (Theorem 4) is the best example to understand this technique.

All the results below depend on the class equation. Let us quickly review the facts without proof. Let G be a group. For any $x \in G$, let $C(x) := \{gxg^{-1} : g \in G\}$ be the conjugacy class of x. Let

$$C_G(x) := \{g \in G : gxg^{-1} = x, \text{ that is, } gx = xg\},$$

be the centralizer of x in G. One knows that if G is finite, then $|G| = |C(x)| \cdot |C_G(x)|$. In particular each of $|C(x)|$ and $|C_G(x)|$ are divisors of $|G|$. (It might have occurred to you that we are going to exploit this in minimal counterexample technique!) One knows that given two conjugacy classes $C(x)$ an $C(y)$, either they are disjoint or they are the same. Hence the set of distinct conjugacy classes partition G. Let C_i, $1 \leq i \leq m$ be the set of all pairwise disjoint distinct conjugacy classes in G. We then have the class equation for G:

$$\begin{aligned} G &= C_1 \cup \cdots \cup C_m, \qquad \text{(disjoint union)} \\ |G| &= |C_1| + \cdots + |C_m|. \end{aligned}$$

Fix $x_i \in C_i$ and let $H_i := C_G(x_i)$. Note that the conjugacy class $C(x) = \{x\}$ iff $x \in Z(G)$, the centre of G. Hence we observe that the numbers of conjugacy classes which are singletons is the order $|Z(G)|$.

With the preliminaries over, we give the first illustration of the minimal counterexample technique in finite group theory.

Theorem 4 (Cauchy's theorem for Abelian Groups)**.** *Let G be a finite abelian group. Let p be a prime divisor of $|G|$. Then there exists $a \in G$ such that the order $o(a) = p$.*

Proof. Let us assume that the result is false. Then there exists a minimal counter example G. That is, p divides $|G|$ but there exists no element (in G) of order p and if K is any such group then $|G| \leq |K|$.

Let $e \neq a \in G$. Can it happen that p divides $o(a)$? That is, $o(a) = pk$ for some $k \in \mathbb{N}$. Let $g := a^k$. Then we know $o(g) = p$, a contradiction. So, we conclude that p does not divide $o(a)$, for any $a \in G$.

Let H be the cyclic subgroup generated by a fixed $a \in G$, $a \neq e$. Then we claim that H is a proper subgroup of G. For, if $H = G$, the $p||G|$ whereas p does not divide $|H| = o(a)$. Thus, H is a proper subgroup of G.

Since G is abelian, H is normal in G. Hence the the quotient group G/H is also a proper quotient, that is, $(e) \neq G/H \neq G$. We know that $|G| = |G/H| \cdot |H|$. Now, p dives the left side and it does not divide $|H|$. Hence p divides $|G/H|$. Since G/H is abelian, whose order is divisible by p and is strictly less than $|G|$, the result is true for G/H. That is, there exists an element $gH \in G/H$ such that $o(gH) = p$. Note that if $m = o(g)$, then $g^m = e$ and hence $(gH)^m = g^m H = H$. Hence m is divisible by $p = o(gH)$. But this contradicts what we saw in the second paragraph of this proof. Hence we conclude that G is a not a counterexample and hence the result is true. □

Please go through the proof once again, review it in your mind without looking into this article. It will help you master the technique.

Theorem 5 (Cauchy)**.** *Let G be a finite group and p be prime divisor of $|G|$. Then there exists $g \in G$ such that $o(g) = p$.*

Proof. Without much ado, let G be a minimal counterexample. (Do you understand what this means? Take sometime to put your ideas in concrete terms!)

> Let $n = |G|$. Then p divided n and there is no element of order p in G. Furthermore, if K is any group with same properties, then $n \leq |K|$.

Let $H \leq G$ be any proper subgroup. Can p divide $|H|$? No, for if it did, then, since $|H| < |G|$, there exists $a \in H$ of order p. But $a \in G$ and $o_G(a) = o_H(a)$. (Do you understand the symbols, $o_G(a)$ and $o_H(a)$?) Hence we conclude that p does not divide the order of any proper subgroup H.

Now let us look $Z(G)$, the centre of G. It is a normal subgroup of G. If $Z(G) = G$, then by the last theorem there exists $g \in Z(G)$ with $o(g) = p$. Therefore, G is not a counterexample! We are forced to conclude that $Z(G)$ is a proper subgroup of G.

> **Caution:** Are you tempted to look at $G/Z(G)$ and argue as in the abelian case? What may not be in our favour? What if $Z(g) = \{e\}$?

Let us now make use of the class equation. Let $\{C_j : 1 \leq j \leq m\}$ be the set of distinct conjugacy classes. Without loss of generality, let us assume that $|C_j| = 1$ for $1 \leq j \leq k$. Note that $\cup_{j=1}^{k} C_j = Z(G)$. (Why?) We have

$$|G| = |Z(G)| + |C_{k+1}| + \cdots + |C_m|. \tag{1}$$

Let $x_j \in C_j$ and $H_j = C_G(x_j)$, the centralizer subgroup of x_j. Since p divides $|G|$ and p does not divide $|Z(G)|$, we conclude that there exists j such that $k + 1 \leq j \leq m$ and p does not divide $|C_j|$. Let $C = C_j$ and $H = H_j$ for simplicity.

Since $|G| = |C||H|$ and since $|C| > 1$, we find that $|H| < |G|$. Also, since p divides $|G|$ and it does not divide $|C|$,we conclude that p divides $|H|$. Since G is a minimal counterexample, the result is true for H. That, there exists $a \in H$ such that $o_H(a) = p$. Since $o_G(a) = o_H(a)$, we see that $a \in G$ is an element of order p. This contradicts the fact that G is a minimal counterexample! □

The next application is the first theorem of Sylow.

Theorem 6 (Sylow-I). *Let G be a finite group. Let p be a prime and $k \in \mathbb{N}$ such that p^k divides $|G|$. Then there exists a subgroup $H \leq G$ such that $|H| = p^k$.*

Proof. Let G be a minimal counterexample. I am sure by now you can figure out the meaning of this statement.

> Let G be a finite group such that $p^k||G|$ and G has no subgroup order p^k. Also, if K is group with $|K| < |G|$ and p^r divides $|K|$, then K has a subgroup H with $|H| = p^r$.

Let us consider $Z(G)$. There are two possibilities: either p divides $|Z(G)|$ or it does not.

Let p be a divisor of $|Z(G)|$. Then by Cauchy's theorem there exists $a \in Z(G)$ such that $o(a) = |H| = p$ where H is the cyclic subgroup generated by a. Note that H is normal in G.

> Why? We need to show that $gHg^{-1} = H$. But note that if $h \in H$, then $ghg^{-1} = hgg^{-1} = h$ and hence we see that $gHg^{-1} = H$.

Look at the quotient, G/H. Note that $|G| = |G/H| \cdot p$ and $|G/H| < |G|$ and p^{k-1} divides $|G/H|$. Hence G/H is not a counterexample and so there exists a subgroup $L \leq G/H$ with $|L| = p^{k-1}$. Let $\pi \colon G \to G/H$ be the quotient map $\pi(g) := gH$. Then it is easy to see that $K := \pi^{-1}(L)$ is a subgroup (of G) of order p^k.

> Let $\varphi \colon K/H \to L$ be defined by $\varphi(x) = xH$. Then it is well-defined since $\pi(xH) = H$ iff $x \in H$ in which case $xH = H$.
>
> It is also one one. Let $x, y \in K$. Then $\varphi(x) = xH = yH = \varphi(y)$ iff $x^{-1}y \in H$, in which case $xH = yH$. Also, if $gH \in L$, then $g \in K$ and hence $\varphi(g) = gH$. Thus the map φ is a bijection of K/H onto L. It follows that $|K| = |H||K| = p^k$.
>
> One can use the first homomorphism theorem also to conclude that $|K| = p^k$.

This contradicts the fact that G is a minimal counterexample. Hence we conclude that p does not divide $|Z(G)|$.

We now look at the class equation (1), as in the last theorem. Since p does not divide $|Z(G)|$, it follows that there exists a j such that p does not divide $|C_j|$. We let $C := C_j$ and by H the centralizer subgroup of some $x \in C$. Since $|G| = |C||H|$ we infer hat p^k divides $|H|$. Since $|C| > 1$, we see that $|H| < |G|$. Hence there exists a subgroup $K \leq H$ with $|H| = p^k$. But then H is also subgroup of G of the order p^k. This contradicts the fact that G is a minimal counterexample.

Hence we are forced to infer that no such example exists. In other words the theorem is true. □

We shall now prove that the converse of Lagrange's theorem holds for finite abelian groups.

Theorem 7. *Let G be a finite abelian group. Let m be a divisor of $|G|$. Then there exists a subgroup $H \leq G$ such that $|H| = m$.*

Proof. Let G be a minimal counterexample, say, m divides $|G|$ but we cannot find a subgroup order m. Note that $m > 1$.

If $m = p$, a prime, then the result follows from Theorem 4. If m is not a prime, let p be a prime divisor of m. Again, by Theorem 4, there exists a subgroup $H \leq G$ of order p. Consider the quotient group G/H. If we let $m = pk$, then k divides $|G/H|$. Hence there exists a subgroup $L \leq G/H$ such that $|L| = k$. We may argue as in the theorem of Sylow to find a subgroup $K \leq G$ such that $|K| = pk$. Thus G is not a counterexample. □

Remark 8. This may be considered as a collection of some personal remarks. I learned the minimal counterexample technique during early 70's when I was a student of M.Sc. I found a proof of the Cauchy's theorem for the abelian case using this technique in a book. Unfortunately, I do not remember the author's name or the title of the book. I tried to understand the proof in my own way and then found the proofs for the results above in number theory. I do not remember having read the general case of Cauchy's theorem. The first time I came across Sylow's theorems was after I joined TIFR. The then proofs were by induction. For more than three decades, I am fond of the proofs by group actions. Recently, when I was recording lectures on Group actions, I was reminded of the term "Minimal Counterexample". Slowly, I was able to put the pieces together and the result is this article.

I would appreciate if any reader of this article can find some (introductory, elementary) book on Algebra which talks of this technique. I understand that this was extensively used by Feit and Thompson in their work on Finite groups. Hence one is sure to find mention of the technique in specialized books on finite groups and their classification.

I will be more than delighted if someone uses this technique to prove either new results and give alternate proof of the results in a typical M.Sc. course. In principle, any result proved by induction should be amenable to this technique, though there could be technical issues.

I vaguely remember to have proved some result in the theory of representations of finite groups using the minimal counterexample technique.

The technique is not confined to finite groups.

Acknowledgment: I thank G. Santhanam and Bhaba Kumar Sarma for a careful reading of the first draft.