CS30 (Discrete Math in CS), Summer 2021 : Lecture 8 Supp

Topic: Induction

Disclaimer: These notes have not gone through scrutiny and in all probability contain errors. Please discuss in Piazza/email errors to deeparnab@dartmouth.edu

---

Minimal Counterexample: A Different look at Induction

There is a different, and equivalent, at looking at mathematical induction proofs which, at times, may be more suitable. This is more of a "proof by contradiction" viewpoint. One assumes the assertion is false, picks the *minimal counterexample* to the statement at hand, and then tries to argue a contradiction. To make things concrete, let is give a "different" proof of something we saw in class.

Theorem 1. Every natural number ≥ 2 can be written as a product of primes and 1.

Proof. Suppose not. Let n be the minimal counter example to the statement, that is, it is *smallest* number which *cannot* be written as a product of primes and 1. Then n cannot be a prime, for a prime is a product of primes and 1. So, $n = a \times b$ for two numbers a and b which are $< n$. Since n is the *minimal counter example*, both a and b can be expressed as a product of primes and 1. And thus, so can n which is a contradiction to n being a counterexample. □

Indeed, the above is the *same* proof. But the mental image one has can differ. Let's give another example. In the UGP, you are asked to prove this by induction.

Theorem 2. Suppose a finite number of players play a round-robin tournament, with everyone playing everyone else exactly once. Each match has a winner and a loser (no ties). We say that the tournament has a *cycle* of length m if there exist m distinct players $(p_1, p_2, \ldots, p_m)$ such that p_1 beats p_2, p_2 beats p_3, $\cdots$, p_{m-1} beats p_m, and p_m beats p_1. Clearly this is possible only for $m \geq 3$. If a tournament has at least one cycle, then it has a cycle of length *exactly* 3.

Proof. Let us consider a tournament with a cycle, and consider among all cycles in the tournament, any one with the smallest length. Let this be $C = (p_1, p_2, \ldots, p_m)$ with length m. If $m = 3$, we are done. Therefore, suppose, for contradiction's sake, $m > 3$. Now consider the players p_1 and p_3. Since there are no ties, either p_1 beats p_3 or p_3 beats p_1. If p_3 beats p_1, then (p_1, p_2, p_3) is a shorter cycle (indeed its length is 3). If p_1 beats p_3, then $(p_1, p_3, p_4, \ldots, p_m)$ is a shorter cycle of length $m - 1$. This contradicts that C was a *smallest cycle*. Thus, $m = 3$. □

The Well-Ordering Principle and PMI

What we have used before, implicitly and rather matter-of-fact-ly, is the following *axiom* called the well-ordering principle (WOP).

$$\text{Any } \textit{non-empty} \text{ subset } S \subseteq \mathbb{N} \text{ has a minimum element } x \in S. \qquad \text{(WOP)}$$

An element $x \in S$ is minimum if for all $y \in S \setminus x$, we have $x < y$.

Remark: *Note that S needs to be non-empty. More importantly, note that if $S \subseteq \mathbb{Z}$, then the above statement is* false*; consider the set S to be of all negative integers. Finally, note if $S \subseteq \mathbb{Q}_+$, that is, if it is a subset of* positive *rationals, then the statement would be* false *too. Indeed, let S be the set of all rationals* strictly *greater than 0. Do you see why S doesn't have a minimum?*

In both the above applications, we have used this principle on a subset generated by the counterexamples. In the prime factorization example, S was the subset of numbers which cannot be written as a product of primes and 1. In the tournament example, S was the lengths of the smallest cycles in tournaments which have cycles but none of length 3. The fact that S was not empty was assumed for contradiction's sake. And then the minimal element was used for obtaining a contradiction.

Let us end by showing that the WOP can be used to *prove* the principle of mathematical induction (PMI). Recall, the principle of mathematical (strong) induction (PMI) states that

Theorem 3 (Induction)**.** Given predicates $P(1), P(2), P(3), \ldots$, *if*

- $P(1)$ is true (**base case**); and
- For all $k \in \mathbb{N}$, $(P(1) \wedge P(2) \wedge \cdots \wedge P(k)) \Rightarrow P(k+1)$ (**inductive case**);

then, $\forall n \in \mathbb{N} : P(n)$ is true.

Proof. Suppose not. That is, the base case and the inductive case holds, but $P(n)$ is false for some non-negative integer n. Indeed, let $S \subseteq \mathbb{N}$ be the subset of non-negative integers n for which $P(n)$ is false. By our supposition, S is *non-empty*. Therefore, by WOP, S has a minimal element x.

Now $x > 1$ because $P(1)$, as we know by the base-case, is true. Thus the set $\{1, 2, \ldots, x-1\}$ is *not* empty. Furthermore, since $1, 2, \ldots, x-1$ are all strictly $< x$, and x is the minimum element of S, *none* of these elements can be in S. Therefore, $P(1)$, $P(2)$, $\ldots$, $P(x-1)$ are all *true*. Thus, $P(1) \wedge \cdots \wedge P(x-1)$ is true. The inductive case then implies $P(x)$ is true. But this contradicts the fact that $x \in S$. Thus our supposition is false, and hence PMI is true. □