CS 30: Discrete Math in CS (Winter 2019): Lecture 16 Supplement

Date: 1st February, 2019 (Friday)
Topic: A "proof" of 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

---

Well-Ordering Principle and proof of the Principle of Mathematical Induction.
To recapitulate, the principle of mathematical (strong) induction (PMI) states that 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.

The "proof" of PMI may seem *obvious*. Indeed, one can take it as an *axiom*; a ground truth which one must assume to build other truths (read theorems). Or, you may assume another *equally obvious sounding* principle as an *axiom*, and *prove* PMI as a theorem. This principle is very useful to know, and is called the *well ordering principle* (WOP).

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

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?*

This is quite a useful principle. We first show a proof of PMI, and then show how one can use WOP directly to prove a statement we already proved by induction.

Proof of PMI. Suppose PMI were false. 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. ∎

Prime Factorization. We prove the following statement

$$\text{For all positive integer } n \geq 2, \quad n \text{ can be factored into a product of primes.} \tag{1}$$

Suppose not, and let $S \subseteq \mathbb{N}$ be the set of numbers ≥ 2 which *can't* be factored as a product of primes. By supposition, S is non-empty. Let x be the minimal element in S. Now, x can't be a prime; it is trivially a product of primes. Thus, $x = n \cdot m$ for some two natural numbers $2 \leq n, m < x$. Since both are $< x$, they can't lie in S. Thus, n can be expressed as a product of primes, and so can m. And thus, $x = n \cdot m$ can be expressed as a product of primes contradicting $x \in S$. Thus, the supposition must be wrong, implying (1).