CS21001 Discrete Structures, Autumn 2007

Tutorial 6: August 30, 2007

---

1 **(a)** Let $H_n = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}$ denote the n-th harmonic number. Prove by induction on n that $H_1 + H_2 + \cdots + H_n = (n+1)H_n - n$ for all $n \in \mathbb{N}$.

Solution [Basis] For $n = 0$, both sides evaluate to 0.

[Induction] Suppose for some $n \geqslant 0$, we have $H_1 + H_2 + \cdots + H_n = (n+1)H_n - n$. Then $H_1 + H_2 + \cdots + H_{n+1} = (H_1 + H_2 + \cdots + H_n) + H_{n+1} = (n+1)H_n - n + H_{n+1} = (n+1)\left(H_{n+1} - \frac{1}{n+1}\right) - n + H_{n+1} = (n+2)H_{n+1} - (n+1)$.

(b) Why can't you prove $H_1 + H_2 + \cdots + H_n = (n+1)H_n - n + 1$ by induction on n?

Solution The induction basis does not hold.

2 Assume that the well-ordering principle of $\mathbb{N}$ holds. Prove the principle of weak mathematical induction.

Solution Let $P(n)$ be a proposition involving a variable $n \in \mathbb{N}$. It is given that $P(0)$ is true, and whenever $P(n)$ is true, so also is $P(n+1)$. We have to show that $P(n)$ is true for all $n \in \mathbb{N}$. Let S be the subset of $\mathbb{N}$, containing the integers n for which $P(n)$ is false. We need to show that S is empty. Suppose not, i.e., S is non-empty. But then S contains a minimum element by the well-ordering principle. Call this minimum element n. Clearly, $n > 0$, since $P(0)$ is true by hypothesis. Also by the choice of n, we have $n - 1 \notin S$ (but $n - 1 \in \mathbb{N}$). Therefore, $P(n-1)$ is true, and so $P((n-1)+1) = P(n)$ is also true, a contradiction to the fact that $n \in S$.

3 Suppose that we want to prove by induction on n the fact that $P(n)$ is true for all $n \in \mathbb{N}$. How many basis cases do you have to prove in each of the following cases?

(a) $\forall n \geqslant 0 \left[P(n) \rightarrow P(n+5)\right]$.

Solution Five, namely, $P(0)$, $P(1)$, $P(2)$, $P(3)$, and $P(4)$.

(b) $\forall n \geqslant 0 \left[P(n) \wedge P(n+2) \rightarrow P(n+3)\right]$.

Solution Three, namely, $P(0)$, $P(1)$, and $P(2)$.

(c) $\forall n \geqslant 1 \left[P(\lfloor n/2 \rfloor) \rightarrow P(n)\right]$.

Solution One, i.e., $P(0)$ only.

(d) $\forall n \geqslant 1 \left[P(n-1) \wedge P(n-2) \wedge \cdots \wedge P(\lfloor n/2 \rfloor) \rightarrow P(n)\right]$.

Solution Again one ($P(0)$) only.

4 Prove that the set A of all finite subsets of $\mathbb{N}$ is countable.

Solution [First solution] For $k \in \mathbb{N}$, denote by A_k the set of all subsets of $\mathbb{N}$ of size k. We have $A = \bigcup_{k \in \mathbb{N}} A_k$. So it suffices to show that each A_k is countable. For the proof note that if we plan to list the elements of finite subsets of $\mathbb{N}$ of size k in the increasingly sorted order, then we can identify A_k with a subset of $\mathbb{N}^k$ which is a countable set.

[Second solution] Let $p_0 = 2, p_1 = 3, p_2 = 5, p_3 = 7, \ldots$ be the sequence of prime numbers. (We know that there are infinitely many primes, and the set of primes, being a subset of $\mathbb{N}$, is countable.) Define a map $f : A \rightarrow \mathbb{N}$ as $f(\{a_1, a_2, \ldots, a_n\}) = p_{a_1} p_{a_2} \cdots p_{a_n}$. By unique factorization of integers, f is injective.

[Note that the function f in the second solution is not surjective. Indeed, $\mathrm{Im}(f)$ consists precisely of all square-free positive integers. But this does not matter. In order to prove a set A to be countable, it suffices to supply an injective map $A \rightarrow \mathbb{N}$. If A is infinite, there anyway exists an injective map $\mathbb{N} \rightarrow A$.]

Additional exercises

5 Find the flaw in the following proof:

Theorem: All horses are of the same color.

Proof Let there be n horses. We proceed by induction on n. If $n = 1$, there is nothing to prove. So assume that $n > 1$ and that the theorem holds for any group of $n - 1$ horses. From the given n horses discard one, say the first one. Then all the remaining $n - 1$ horses are of the same color by the induction hypothesis. Now put the first horse back and discard another, say the last one. Then the first $n - 1$ horses have the same color again by the induction hypothesis. So all the n horses must have the same color as the ones that were not discarded either time. •

6 **(a)** Prove that $\mathbb{N}$ is well-ordered assuming that the principle of weak mathematical induction holds.
(b) Prove that the principle of weak mathematical induction is equivalent to the principle of strong mathematical induction. That is, if you assume any of the two, you can prove the other.

7 Let $P(m, n)$ be a predicate involving two variables $m, n \in \mathbb{N}$. Suppose that the following are true.

(1) $P(0, 0)$ is true.
(2) For all $m, n \in \mathbb{N}$, the truth of $P(m, n)$ implies the truth of $P(m + 1, n)$ and also of $P(m, n + 1)$.

Prove that $P(m, n)$ is true for all $m, n \in \mathbb{N}$.

8 Let F_n, $n \in \mathbb{N}$, denote the sequence of Fibonacci numbers (i.e., $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geqslant 2$). Prove the following assertions by induction on n.

(a) $F_n = \frac{\phi^n - (1-\phi)^n}{\sqrt{5}}$ for all $n \in \mathbb{N}$, where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio.
(b) $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$ for all $n \geqslant 1$.
(c) $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ for all $n \geqslant 1$.
(d) $F_{m+1}F_n + F_mF_{n-1} = F_{m+n}$ for all $m \geqslant 0$, $n \geqslant 1$.
(e) $\gcd(F_n, F_{n+1}) = 1$ for all $n \geqslant 0$.
(f) $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ for all $m, n \in \mathbb{N}$, not both zero.

9 Let A be a finite set. Prove that the set of all functions $A \to \mathbb{N}$ is countable.

10 Prove that the set of all valid C programs is countable.

11 **(a)** Let $\mathbb{Z}[X]$ denote the set of polynomials in one indeterminate X and with integer coefficients. Prove that $\mathbb{Z}[X]$ is countable.
(b) Let k be a fixed positive integer. Prove that the set $\mathbb{Z}[X_1, X_2, \ldots, X_k]$ of multivariate polynomials with integer coefficients is countable.
(c) Prove that the set $\mathbb{Z}[X_1, X_2, \ldots, X_k, \ldots]$ of polynomials with countably infinite indeterminates and with integer coefficients is countable.

12 A real or complex number α is called *algebraic* if $f(\alpha) = 0$ for some non-zero polynomial $f(X)$ with integer coefficients. Let $\mathbb{A}$ denote the set of all algebraic numbers. We have $\mathbb{A} \subseteq \mathbb{C}$.

(a) Prove that $\mathbb{A}$ is countable.
(b) Conclude that there are uncountably many transcendental numbers.