Massachusetts Institute of Technology | Handout 12
6.042J/18.062J: Mathematics for Computer Science | February 19, 1998 (soln to prob 6
revised 2/27)
Professor Albert R. Meyer

Problem Set 2 Solutions

Problem 1. Prove: For all $x, n \in \mathbb{N} : x+1 | x^{2n+1}+1$.

Proof by induction on n with

$$P(n) ::\equiv \forall x \in \mathbb{N} : x+1 | x^{2n+1}+1.$$

Base Case: $n = 0$. Then $2n+1 = 1$ and $P(0)$ is true since $x+1|x^1+1$.

Inductive Step: Assume $P(n)$, so $x^{2n+1}+1 = p(x+1)$ for some integer p. We need to show that $x+1|x^{2(n+1)+1}+1$.

$$\begin{aligned} x^{2(n+1)+1}+1 &= x^2x^{2n+1}+1 \\ &= x^2(x^{2n+1}+1) - x^2 + 1 \\ &= x^2p(x+1) - (x-1)(x+1) \\ &= (x^2p - (x-1))(x+1). \end{aligned}$$

So $x+1$ is indeed a factor of $x^{2(n+1)+1}+1$. ■

Problem 2. Prove that

$$1 \cdot 1! + 2 \cdot 2! + ... + n \cdot n! = (n+1)! - 1,$$

for all $n \in \mathbb{N}$.

Proof by induction on n.

Base Case: $n = 0$. True since L.H.S. = 0 = R.H.S.

Inductive Step: Assuming the inductive hypothesis, we have

$$\begin{aligned} 1 \cdot 1! + 2 \cdot 2! + ... + n \cdot n! + (n+1) \cdot (n+1)! &= (n+1)! - 1 + (n+1) \cdot (n+1)! \\ &= (n+1)!(1+n+1) - 1 \\ &= (n+2)! - 1 \end{aligned}$$

as desired.

Problem 3. For $n \in \mathbb{N}$, define numbers u_n by the equations:

$$u_0 = 2, u_1 = 3, u_{n+2} = 3u_{n+1} - 2u_n.$$

Guess a general formula for u_n and use mathematical induction to prove your answer.

We claim, $u_n = 2^n + 1$ for all $n \in \mathbb{N}$. We can prove it by strong induction on n.

Base Cases: $n = 0, 1$. Then $u_0 = 2 = 2^0 + 1$ and $u_1 = 3 = 2^1 + 1$ as required.

Inductive Step: We may assume $n \geq 1$ and $u_k = 2^k + 1$ for all $k \leq n$. We shall show $u_{n+1} = 2^{n+1} + 1$. Since $n - 1 \geq 0$, the value of u_{n+1} is determined by the recurrence formula, namely,

$$\begin{aligned}
u_{n+1} &= 3u_n - 2u_{n-1} \\
&= 3(2^n + 1) - 2(2^{n-1} + 1) \\
&= 3 \cdot 2^n - 2 \cdot 2^{n-1} + 1 \\
&= 3 \cdot 2^n - 2^n + 1 \\
&= 2 \cdot 2^n + 1 \\
&= 2^{n+1} + 1
\end{aligned}$$

∎

Problem 4. A set of lines in the plane is said to be in *general position* when no two of the lines are parallel, and no three intersect at a common point. Let R_n be the number of regions into which n lines in general position divide the plane. For example, $R_0 = 1, R_1 = 2, R_2 = 4$. Explain, informally but clearly, why $R_{n+1} = R_n + (n+1)$. Find a simple formula for R_n and prove your result by induction.

A set of n lines in a general position divides the plane into R_n regions. When the $(n+1)^{st}$ line is added to the plane such that the resulting set of lines is in a general position, the new line has to intersect the previous n lines, splitting in two each region above a point of intersection, and also splitting in two the region below the lowest point of intersection. This splits $n + 1$ regions into $2(n + 1)$ regions, with a net increase of $n + 1$ regions. Therefore $R_{n+1} = R_n + (n + 1)$.

A general formula for R_n is $\frac{n(n+1)}{2} + 1$, as we prove by induction.

Base Case: $n = 0$. There is one region, namely the whole plane, and so thew number of regions equals R_0.

Inductive Step: Assuming $R_n = \frac{n(n+1)}{2} + 1$, we need to show that $R_{n+1} = \frac{(n+1)(n+2)}{2} + 1$.

$$\begin{aligned}R_{n+1} &= R_n + (n+1) \\ &= \frac{n(n+1)}{2} + 1 + (n+1) \\ &= (n+1)(\frac{n}{2}+1)+1 \\ &= \frac{(n+1)(n+2)}{2} + 1\end{aligned}$$

as desired.

Problem 5. Prove that any finite set of size $n > 0$ has exactly 2^{n-1} subsets of even size. For example, $\{1,2\}$ has two subsets of even size: $\emptyset$ and $\{1,2\}$. *Hint*: Let e be an element of a set S of size $n+1$. An even size subset of S which does not contain e corresponds to an even size subset of $S - \{e\}$; an even size subset of S which does contain e corresponds to an odd size subset of $S - \{e\}$. So $\text{Even}(n+1) = \text{Even}(n) + \text{Odd}(n)$.

(Proof by induction.) Let $\text{Even}(n)$ be the number of even-size subsets of a set of size n. Then we have to show $\forall n > 0 : \text{Even}(n) = 2^{n-1}$. To do this, we let $\text{Odd}(n)$ be the number of odd-size subsets of a set of size n, and we prove by induction a somewhat stronger fact:

Induction hypothesis: $P(n) ::\equiv [\text{Even}(n) = 2^{n-1} \wedge \text{Odd}(n) = 2^{n-1}]$.

Base Case: $n = 1$. There is one even-size subset, namely the empty set, and one odd-size subset, namely the whole set. So $\text{Even}(1) = \text{Odd}(1) = 1 = 2^{1-1}$. So $P(1)$ is true.

Inductive Step: Let A be a set of size $n+1$. Let e be an element of A. The number of even-size subsets in A which do not contain e is equal to the number of even-size subsets in $A - \{e\}$. Also, the number of even-size subsets of A which do contain e is equal to the number of odd-size subsets in $A - \{e\}$. Since the set $A - \{e\}$ is of size n, we have the following recurrence

$$\text{Even}(n+1) = \text{Even}(n) + \text{Odd}(n).$$

Similarly, the number of odd-size subsets of A which do not contain e is equal to the number of odd-size subsets in $A - \{e\}$, and the number of odd-size subsets of A which do contain e is equal to the number of even-size subsets of $A - \{e\}$, so

$$\text{Odd}(n+1) = \text{Odd}(n) + \text{Even}(n).$$

By induction we have that $\text{Even}(n) = 2^{n-1}$ and $\text{Odd}(n) = 2^{n-1}$. So

$$\text{Even}(n+1) = 2^{n-1} + 2^{n-1} = 2^n,$$

and

$$\text{Odd}(n+1) = 2^{n-1} + 2^{n-1} = 2^n,$$

which proves $P(n+1)$. ∎

Problem 6. Pinpoint, and illustrate with a counterexample, *exactly* where the following proofs go awry.

(a) Claim 1: $(\forall \text{real } x)(\forall n \in \mathbb{N}) : x^n = 1$.

Proof by strong induction on n:

(Base case, $n = 0$) $x^n = x^0 = 1$ by definition of "zeroth power" of a real number.

(Strong Induction hypothesis) For all $k \leq n : x^k = 1$.

We must show that $x^{n+1} = 1$. By the strong inductive hypothesis, with $k = n$ and $k = 1$, we have $x^n = 1$ and $x^1 = 1$. So,

$$x^{n+1} = x^n x^1 = 1 \times 1 = 1.$$

■

The proof of the induction step is not correct when $n = 0$. In this case, $k = 1$ is not $\leq n$, so we cannot assume by strong induction that $x^1 = 1$, which of course it is not when $x \neq 1$.

(b) Claim 2: For any positive integers $p, n, x_1, x_2, \ldots, x_n$, if $p | x_1 x_2 \ldots x_n$, then $p | x_i$ for some $1 \leq i \leq n$.

(Refined 2/27/98 by ARM):

Proof by strong induction on n.

(Base case, $n = 1$) When $n = 1$, we have $p | x_1$, therefore we can let $i = 1$ and conclude $p | x_i$.

(Induction case) Now assuming the claim holds for all $k \leq n$, we must prove it for $n + 1$.

So suppose $p | x_1 x_2 \ldots x_{n+1}$. Let $y_n = x_n x_{n+1}$, so $x_1 x_2 \ldots x_{n+1} = x_1 x_2 \ldots x_{n-1} y_n$. Since the righthand side of this equality is a product of n terms, we have by induction that p divides one of them. If $p | x_i$ for some $i < n$, then we have the desired i. Otherwise $p | y_n$. But since y_n is a product of the two terms x_n, x_{n+1}, we have by strong induction that p divides one of them. So in this case $p | x_i$ for some $i = n$ or $i = n + 1$. ■

The statement "we have by strong induction that p divides one of them" is the place where the proof breaks down: it appeals to strong induction to justify applying the induction hypothesis for $2 = k \leq n$. But the base case was $n = 1$, so we can't assume $2 \leq n$. Note that the reasoning above is fine for every $n \geq 2$, so the whole proof would be fine if we had an argument to prove the claim for $n + 1 = 2$. But of course we can't prove it for $n + 1 = 2$ because it isn't true: let $p = 6, x_1 = 2, x_2 = 3$. Even though the reasoning is fine for every $n \geq 2$, the fact that it failed for $n = 1$ let us deduce a patently false result.

Problem 7. Define *constant-free one-occurrence* Boolean formulas, *1BF*'s for short, inductively as follows:

- a variable is a 1BF.
- if F is a 1BF, then so is $\neg F$,
- if F and G are 1BF's with no variables in common, then $F \wedge G$ and $F \rightarrow G$ are 1BF's.

A *Boolean assignment*, A, is a mapping from variables to truth values. The *complement* of assignment A is the assignment B such that $B(x) = \neg A(x)$ for all variables x in the domain of A.

Prove by induction that for all 1BF's, F, there is a Boolean assignment A for the variables of F such that F is true under assignment A and false under the complement of A.

We prove the theorem by strong induction on the length of the 1BF F, with induction hypothesis $P(n)$:

$$\forall F : \text{length}(F) = n \Rightarrow [\exists A : (F \text{ is true under } A) \wedge (F \text{ is false under} \overline{A})]$$

where F ranges over 1BF's and A ranges over Boolean assignments. Here we use the notation $\overline{A}$ for the complement of assignment A.

Base Case: $n = 1$. If F is a 1BF of length 1 it must be a variable. Then the desired assignment is any A such that $A(F) = \text{true}$.

Inductive Step: Now assume $P(k)$ for all $k \leq n$. To show $P(n+1)$, let F be a length $n+1$ 1BF for $n \geq 1$. There are three cases:

1. $F = \neg G$, where G is a 1BF with length $\leq n$. By inductive hypothesis, there is an assignment A_0 such that G is true under A_0 and false under $\overline{A_0}$. Then the desired assignment A will be $\overline{A_0}$.
2. $F = G \wedge H$, where G and H are formulas of length $\leq n$. By inductive hypothesis there is an assignment A_0 such that G is true under A_0 and false under $\overline{A_0}$. Also, there is an assignment A_1 such that H is true under A_1 and false under $\overline{A_1}$. Now let A be the assignment which agrees with A_0 on the variables of G and with A_1 on the variables of H. Such an A exists because F is a 1BF, so no variable occurs in both G and H. Now under A both G and H are true, and therefore $G \wedge H$ is true. Likewise, $\overline{A}$ makes $G \wedge H$ false as required.
3. $F = G \rightarrow H$, where G and H are formulas of length $\leq n$. As in the previous case, there is an assignment $A_0(A_1)$ such that $G(H)$ is true under $A_0(A_1)$ and false under $\overline{A_0}(\overline{A_1})$. So this time we let A be the assignment which agrees with $\overline{A_0}$ on the variables of G and with A_1 on the variables of H. Now under A, G is false and H is true, so $G \implies H$ is true; under $\overline{A}$, G is true and H is false, so $G \implies H$ is false, as required.

■