CS054: Induction

The goal of this worksheet is to give you practice with induction: what can you do induction on? what cases will you have to prove and what will your IH be? which induction is the one you want? It's not for a grade—no need to turn it in! I'll post solutions, but you'll get the most out of it if you don't peek.

For all of these questions, I'm using math notation—$\forall$ for `forall` in Coq, $+$ for `plus` in Coq, etc. The questions are asking about the definitions we've made so far.

1. **Sample:** Suppose we want to prove that $\forall nm,\ n + m = m + n$.
   (a) What can we do induction on? **Answer:** n, m
   (b) For each possibility above, list (a) the goal you would have to prove in the base case, (b) the induction hypothesis you would get, and (c) the goal you would have to prove in the induction case.
   Answer for n:
   Base case: $0 + m = m + 0$
   IH: $n' + m = m + n'$
   Inductive case: $Sn' + m = m + Sn'$
   Answer for m:
   Base case: $n + 0 = 0 + n$
   IH: $n + m' = m' + n$
   Inductive case: $n' + Sm = Sm + n'$
   (c) Which of these inductions would work to prove the theorem? **Answer:** n, m

2. Suppose we want to prove that $\forall n,\ n - n = 0$.
   (a) What can we do induction on? _____n_____
   (b) For each possibility above, list (a) the goal you would have to prove in the base case, (b) the induction hypothesis you would get, and (c) the goal you would have to prove in the induction case.

   > **Solution: Answer for n:**
   > Base case: $0 - 0 = 0$
   > IH: $n' - n' = 0$
   > Inductive case: $Sn' - Sn' = 0$

   (c) Which of these inductions would work to prove the theorem? _____n_____

3. Suppose we want to prove that $\forall n,\ \mathsf{t} = \texttt{eqb}\ n\ n$.[1]
   (a) What can we do induction on? _____n_____
   (b) For each possibility above, list (a) the goal you would have to prove in the base case, (b) the induction hypothesis you would get, and (c) the goal you would have to prove in the induction case.

   > **Solution: Answer for n:**
   > Base case: $true = \texttt{eqb}\ 0\ 0$
   > IH: $true = \texttt{eqb}\ n'\ n'$
   > Inductive case: $true = \texttt{eqb}\ (Sn')\ (Sn')$

   (c) Which of these inductions would work to prove the theorem? _____n_____

[1] Many mathematicians will write `true` as t or $\mathtt{tt}$ or something similar; `false` would be rendered as f or $\mathtt{ff}$.

4. Suppose we want to prove that $\forall n,\ Sn = n + 1$.
   (a) What can we do induction on? _____ n _____
   (b) For each possibility above, list (a) the goal you would have to prove in the base case, (b) the induction hypothesis you would get, and (c) the goal you would have to prove in the induction case.

   Solution: Answer for n:
   Base case: $1 = 0 + 1$
   IH: $Sn' = n' + 1$
   Inductive case: $S(Sn') = Sn' + 1$

   (c) Which of these inductions would work to prove the theorem? _____ n _____

5. Suppose we want to prove that $\forall nm,\ n + Sm = S(n + m)$.
   (a) What can we do induction on? _____ n**,** m _____
   (b) For each possibility above, list (a) the goal you would have to prove in the base case, (b) the induction hypothesis you would get, and (c) the goal you would have to prove in the induction case.

   Solution: Answer for n:
   Base case: $0 + Sm = S(0 + m)$
   IH: $n' + Sm = S(n' + m)$
   Inductive case: $Sn' + Sm = S(Sn' + m)$
   Answer for m:
   Base case: $n + 1 = S(n + 0)$
   IH: $n + Sm' = S(n + m')$
   Inductive case: $n + S(Sm') = S(n + Sm')$

   (c) Which of these inductions would work to prove the theorem? _____ n _____

6. Suppose we want to prove that $\forall nmp,\ n * (m * p) = (n * m) * p$.
   (a) What can we do induction on? ____ n**,** m**,** p ____
   (b) For each possibility above, list (a) the goal you would have to prove in the base case, (b) the induction hypothesis you would get, and (c) the goal you would have to prove in the induction case.

   Solution: Answer for n:
   Base case: $0 * (m * p) = (0 * m) * p$
   IH: $n' * (m * p) = (n' * m) * p$
   Inductive case: $Sn' * (m * p) = (Sn' * m) * p$
   Answer for m:
   Base case: $n * (0 * p) = (n * 0) * p$
   IH: $n * (m' * p) = (n * m') * p$
   Inductive case: $n * (Sm' * p) = (n * Sm') * p$
   Answer for p:
   Base case: $n * (m * 0) = (n * m) * 0$
   IH: $n * (m * p') = (n * m) * p'$
   Inductive case: $n * (m * Sp') = (n * m) * Sp'$

   (c) Which of these inductions would work to prove the theorem? ____ n**,** m**,** p ____
   (d) Which of these inductions is easiest, i.e., requires the fewest other lemmas? _____ n _____
   (e) Why? **Because using n most closely follows the case analysis in the definitions.**

7. Suppose we want to prove $\forall n,\ n - 1 + 1 = n$.

   (a) What can we do induction on? _____n_____

   (b) For each possibility above, list (a) the goal you would have to prove in the base case, (b) the induction hypothesis you would get, and (c) the goal you would have to prove in the induction case.

   > **Solution: Answer for n:**
   > Base case: $0 - 1 + 1 = 0$
   > IH: $n' - 1 + 1 = n'$
   > Inductive case: $Sn' - 1 + 1 = Sn'$

   (c) Which of these inductions would work to prove the theorem? **none—it's false when $n = 0$**

8. Is there a difference between case analysis (`destruct`) and induction (`induction`) on $\mathbb{N}$ (`nat`)? If so, what is it? If not, why not?

   > **Solution:** These is a difference: doing induction gives you an induction hypothesis when $n = Sn'$.

9. Is there a difference between case analysis (`destruct`) and induction (`induction`) on booleans (`bool`)? If so, what is it? If not, why not?

   > **Solution:** There is no difference—because there are no subparts to booleans, there are no induction hypotheses to generate.

10. The induction principle for naturals is that to prove that $\forall n, P(n)$, it suffices to prove that $P(0)$ and $\forall n',\ P(n') \to P(Sn')$.

    We defined a version of binary numbers (`bin`) as follows:

```
Inductive bin : Type :=
  | BZ : bin           (* binary zero *)
  | T2 : bin -> bin    (* twice a binary number *)
  | T2P1 : bin -> bin. (* twice a binary number plus 1 *)
```

    What is the induction principle for binary numbers? (If you're not sure, go and finish `Day13_induction.v` first.)

> **Solution:** To prove $\forall b, P(b)$, it suffices to prove that $P(BZ)$, that $\forall b',\ P(b') \to P(T2\ b')$, and that $\forall b',\ P(b') \to P(T2P1\ b')$

11. What is the induction principle for binary trees `bt`?

> **Solution:** To prove $\forall t, P(t)$, it suffices to prove that $P(\texttt{empty})$, that $\forall lvr,\ P(l) \to P(r) \to P(\texttt{node}\ l\ v\ r)$.