csci54 – discrete math & functional programming
induction

this week: continuing with proofs

- logic
  - propositional
  - predicate

- proof techniques
  - direct proofs
  - proof of the contrapositive
  - proof by example / disproof by counterexample
  - proof by contradiction
  - using cases

  - induction!

some definitions (recap)

- an integer k is <u>even</u> if and only if there exists an integer r such that k=2r
- an integer k is <u>odd</u> if and only if there exists an integer r such that k=2r+1
- k|m if and only if there exists an integer r such that m=kr. This is equivalent to saying that "m mod k = 0" or that "k evenly divides m".
- an integer k>1 is <u>prime</u> if the only positive integers that evenly divide k are 1 and k itself.
- an integer k>1 is <u>composite</u> if it is not prime.
- an integer k is a <u>perfect square</u> if and only if there exists an integer r such that $k=r^2$

What about . . .

- claim: given any non-negative integer n, the sum of integers up to n is n*(n+1)/2

- techniques we know:
  - direct proofs
  - proof of the contrapositive
  - proof by example / disproof by counterexample
  - proof by contradiction
  - using cases

(on summation notation)

- claim: given any non-negative integer n, the sum of the integers from 1 up to n is n*(n+1)/2
- could also write using summation notation:

What about . . .

- observations:
  - want to prove something is true for all elements of a set (the non-negative integers)
  - the set is ordered in the sense that we can talk about the smallest/first element, then the next one, then the next one, ...   (0, 1, 2, 3, ...)

Proofs by induction

Definition 5.1: Proof by mathematical induction.

Suppose that we want to prove that $P(n)$ holds for all $n \in \mathbb{Z}^{\geq 0}$. To give a *proof by mathematical induction* of $\forall n \in \mathbb{Z}^{\geq 0} : P(n)$, we prove two things:

1. the *base case:* prove $P(0)$.
2. the *inductive case*: for every $n \geq 1$, prove $P(n-1) \Rightarrow P(n)$.

Structure of a proof by induction

- claim: for all x, P(x)
- we prove the claim using a proof by induction on: x
- base case: P(x*) holds for the smallest x*

- inductive step: P(x') → P(x)
  - If we assume P(x') for some x' (inductive hypothesis)
  - We must show that for every way we can grow x' into some x, P(x') → P(x)
- therefore by the principle of mathematical induction: for all x, P(x)

Structure of a proof by induction

- claim: for all natural numbers n, P(n)
- we prove the claim using a proof by induction on: n
- base case: P(0)

- inductive step: P(n) → P(n+1)
  - If we assume P(n) for some n (inductive hypothesis)
  - We must show that for P(n) → P(n+1)
- therefore by the principle of mathematical induction: for all n, P(n)
- We will never **miss** a natural number with this induction scheme

Notes on writing proofs by induction

- we prove the claim using a proof by induction <...>
  - unless it's a direct proof should state the proof technique.
- base case
  - show true on the smallest element of the set
- inductive hypothesis (IHOP)
  - assume true for some value
- inductive step
  - wts: if IHOP is on n, then prove for n+1. if IHOP is on n-1, then prove for n.
  - some step in this part **must** refer back to the IHOP. otherwise it's definitely not a proof by induction (and may not be a proof at all)
- therefore by the principle of mathematical induction <...>
  - have a concluding line

Practice

For every positive integer, n + 1 <= n * 2

- we prove the claim using a proof by induction on n:
- base case: 1 + 1 <= 1 * 2

- inductive step:
  - inductive hypothesis (IH): n’ + 1 <= n’ * 2
  - Wts: (n’+1)+1 <= (n’+1)*2
  - (n’+1)+1 <= 2 * n’ + 2 * 1
  - We know n’+1 <= 2*n’ by the IH, so it suffices to show that 1 <= 2
- therefore by the principle of mathematical induction:
  - For all positive integers n, n + 1 <= n * 2

Example 5.2 from CDMCS

Practice

For every list and function, map f l has the same length as l

- we prove the claim using a proof by induction on l:
- base case: map f [] has the same length as [] (by the base cases of map and length)
- inductive step:
  - inductive hypothesis (IH): length (map f l') = length l'
  - Wts: length (map f (x:l')) = length (x:l')
  - map f (x:l') = (f x):(map f l')   (second case of map)
  - length (x:l') = 1 + length l' (second case of length)
  - length ((f x):(map f l')) = 1 + length (map f l') (same)
  - So we have: 1 + length l' = 1 + length l'

- Therefore, by induction, forall f and l, length (map f l) = length l

Practice

For every positive integer n, the sum from 1 up to n is equal to n*(n+1)/2.

- we prove the claim using a proof by induction on n:
- base case: for n=1, …
- inductive step: (for all n', if P(n') then P(n'+1))
  - inductive hypothesis (IH): for n=n'…
  - Wts: for n=n'+1, …
  - …
- therefore by the principle of mathematical induction:
  - For all positive integers n, the sum from 1 up to n is n*(n+1)/2.

Example 5.2 from CDMCS

Practice

- Identify the smallest positive integer p such that for all n >= p, $n! > 2^n$
- Prove that your choice of p is correct
  - statement needs to be true for all n
  - if p > 1, need to show that the statement is not true for p - 1

n! =
0! = 1! = 1

n! is read "n factorial"