S. KIMMEL

Announcements: Quiz, Equatio, Plickers, Questionnaire

Outline of Course

1. Writing Proofs
   - Induction ⟸ One of the most powerful tools in C.S. tool box
   - Constructive
   - Direct
   - Contradiction
   - Contrapositive

We'll start here, to whet your appetite

2. Important Math for C.S. (and life!)
   - counting & combinatorics
   - graphs
   - number theory
   - probability
   - growth of functions
   - finite state machines

Motivating Proofs

Q: When you write a program, how do you tell if it works correctly?

- Try examples
- Trace variable values
- Use debugging tools
- Think logically
- See if got an "A"

Better approach: **Proof**: formal method of arguing a statement is true

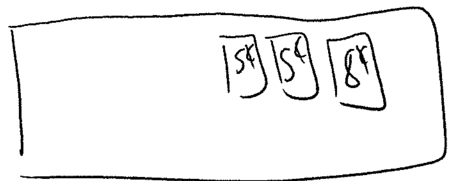
↑

"My program outputs correct value"

S. KIMMEL

Induction

Suppose you have unlimited 5¢ stamps and 8¢ stamps.
What postage values can you create?



18¢ ✓

What about 4¢? No!

What about 28¢?

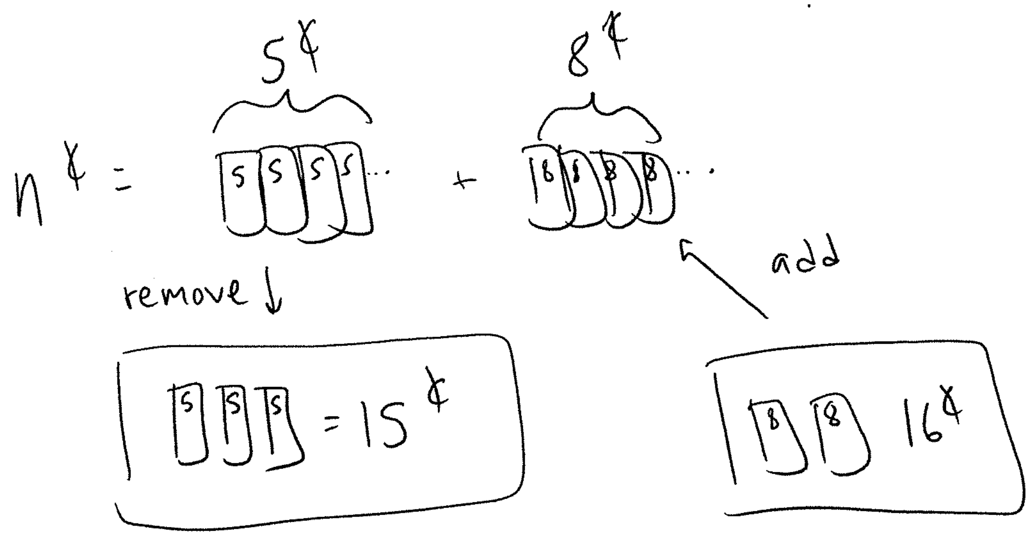
$\boxed{5}\boxed{5}\boxed{5}\boxed{5}\boxed{8}$

What about n¢?

S. KIMMEL

Induction: use old solution to get new solution

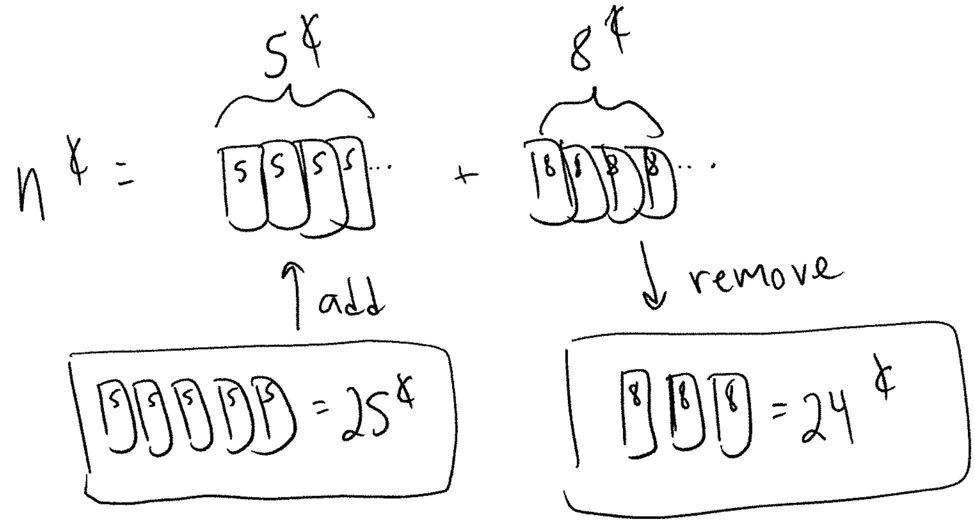
Suppose



$n¢ \to (n+1)¢$

Q:

Suppose



$n¢ \to (n+1)¢$

Consequence: If can create $n¢$ with at least 3 [5] or at least 3 [8], can create $n+1$ ¢

S. KIMMEL

$28¢ = 4 \cdot \boxed{5} + 1 \cdot \boxed{8}$

$29¢ = 1 \cdot \boxed{5} + 3 \cdot \boxed{8}$

$30¢ = 6\,\boxed{5}$

$31¢ = 3\,\boxed{5} + 2\,\boxed{8}$

$\vdots$

Q: If $85{,}693¢ = 5{,}761\,\boxed{5} + 7111 \cdot \boxed{8}$

then can create $85{,}694¢$ as

$\underline{5758}\,\boxed{5} + \underline{7113}\,\boxed{8}$

or

$\underline{5766}\,\boxed{5} + \underline{7108}\,\boxed{8}$

A) 5759 / 7114

B) 5764 / 7108

C) 5766 / 7108

D) 5758 / 7113

find first solution, & the rest fall into place

$\Downarrow$

* Any postage $\geq 28¢$ is possible

Start at $28¢ \rightarrow 29¢ \rightarrow 30¢ \ldots \quad 85{,}693¢ \ldots$

S.KIMMEL

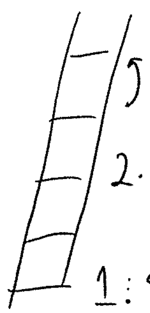
Principle of induction: solution to problem of size n gives solution to problem of size n+1.

Needed to have previous solution to get next solution!

Once you get 28¢ solution, we're good.

Inductive Metaphors

Ladder



2. Show how to move from one rung to next

1: Show how to get on first rung of ladder

Formal Inductive Proof

Proofs have a unique style/language
- Essay vs. Texting vs News article vs. lab notebook

all unique styles

This class → proof language.

Induction proof has a recipe, so a bit easier to start with than other proofs

S. KIMMEL

Inductive proof recipe:

(Set-up)

Let P(n) be the predicate <u>n¢ of postage can be formed from 5¢ and 8¢ stamps</u>.

We will prove, using induction on n, that P(n) is true for all $n \geq$ <u>28</u>.

(Base-case)

Base case: P(<u>28</u>) is true because ____________

(Inductive Case)

Inductive case: Let $k \geq$ <u>28</u> (base case #). Assume, for induction, that P(k) is true. That is, we assume <u>we can make k¢ postage out of 5¢ and 8¢ stamps</u>. Then we will prove P(k+1) is also true.

First note ____________

Then ____________

Plugging in ____________

Thus P(k+1) is true

Each sentence logically follows from previous

(Conclusion)

Therefore, by induction, P(n) is true for all $n \geq$ ___

S.KIMMEL

Notice:

- Complete sentences or equations
- "we"
- "Let" in setup

"#'s"

Q: Write inductive proof that $7^n - 1$ is a multiple of 6 for all integers $n \geq 0$.

(Hint: X is a multiple of 6 if $X = 6 \cdot m$ for some integer m.)

Let $P(n)$ be the predicate $7^n - 1$ is a multiple of 6. We will prove via induction that $P(n)$ is true for all $n \geq 0$.

Base Case: $P(0)$ is the statement $7^0 - 1$ is a multiple of 6.
$7^0 - 1 = 1 - 1 = 0 = 0 \cdot 6$, so the statement is true.

Inductive Case: Let $k \geq 0$. Assume, for induction, that $P(k)$ is true. That is, we assume $7^k - 1$ is a multiple of 6. This means $7^k - 1 = 6 \cdot m$ for some integer m. We will prove $P(k+1)$ is true. Note

$$7^{k+1} - 1 = (7^k - 1) \cdot 7 + 7 - 1 = (7^k - 1) \cdot 7 + 6$$

By our inductive assumption, $7^k - 1 = 6 \cdot m$. Thus

$$7^{k+1} - 1 = 6m \cdot 7 + 6 = 6(7 \cdot m + 1),$$

which is a multiple of 6. Thus $P(k)$ is true.

Alternative Inductive case:

Inductive Case: Let $k \geq 0$. Assume, for induction, that $P(k)$ is true. That is, we assume $7^k - 1$ is a multiple of 6. This means $7^k - 1 = 6 \cdot m$ for some integer m. We will prove $P(k+1)$ is true. If we multiply both sides by 7, we have

$$(7^k - 1)7 = 7^{k+1} - 7 = 6 \cdot 7 \cdot m$$

Then adding 6 to both sides, we have

$$7^{k+1} - 1 = 6 \cdot 7 \cdot m + 6 = 6(7m + 1).$$

Thus $7^{k+1} - 1$ is a multiple of 6, and $P(k+1)$ is true.

Therefore, by induction on n, $P(n)$ is true for all $n \geq 0$.