Eli Annoni

Algorithm Analysis: addto32 Informal Proof

Prove that at the beginning of each loop invariant:

$$c + \sum_{k<i} as[k] \cdot B^k = \sum_{k<i} (as'[k] + bs[k]) \cdot B^k, \text{ where } B = 2^{32}, \text{ the base.}$$

Basis:

We know at the start that i is 0, and that before the first iteration, the equation is satisfied:

- $c + \sum_{k<i} as[k] \cdot B^k = \sum_{k<i} (as'[k] + bs[k]) \cdot B^k \rightarrow c + 0 = 0$

and since c is 0 at the start, this is true.

Inductive Hypothesis: Assume $c + \sum_{k<i} as[k] \cdot B^k = \sum_{k<i} (as'[k] + bs[k]) \cdot B^k$.

Inductive Step: Goal is to show that after an iteration, this invariant will remain the same as at the top of the loop.

First, the sum is added to the end of the previous equation:

~~$\sum_{k<i} (as'[k] + bs[k]) B^k + s \cdot B^i$~~

$= \sum_{k<i} (as'[k] + bs[k]) B^k + (as'[i] + bs[i] + c) \cdot B^i$ [substituting in for sum]

$= \sum_{k<i} (as'[k] + bs[k]) B^k + (as'[i] + bs[i]) B^i + c \cdot B^i$ [partially distribute B^i]

$= \sum_{k<i+1} (as'[i] + bs[i]) B^k + c \cdot B^i$ [consolidated summations]

$= \sum_{k<i} (as[k]) \cdot C^k + (as'[i] + bs[i]) C^i$ [I.H. substitution]

And sum = (sum >> 32) · B + (uint32_t) sum

because sum >> 32 = sum // B

(uint32_t) sum = sum % B

So, $\sum_{k<i} (as'[k] + bs[k]) B^k + (sum >> 32 \cdot B + (uint32\_t) sum) \cdot B^i$ [substituting sum for operations occurring after first line of for loop]

Then, since $C = sum >> 32$ and $as[i] = (uint32\_t) sum$,

So, $\sum_{k<i} (as'[k] + bs[k]) B^k + (C \cdot B^i + as[i]) \cdot B^i$ [substitution]

$= \sum_{k<i} (as[k]) B^k + C \cdot B^{i+1} + as[i] B^i$ [I.H. substitution]

$= \sum_{k<i+1} as[k] \cdot B^k + C \cdot B^{i+1}$ [Merge summations]

This is what is left at the end of the loop. Once i increments, the top of the loop will once again be:

$$\sum_{k<i} a[k] B^k + C \cdot B^i$$

This proves that this expression is invariant for each loop iteration.

□