Eli Annoni

Algorithm Analysis: partial prod 32 Informal Proof

Goal is to prove that at the beginning of each loop invariant:

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

Basis: Before the first iteration where $i=0$, c is also 0, which clearly satisfies the above equation.

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

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

$= \sum_{k<i} (bs[k] \cdot d + as'[k]) \cdot B^k + sum \cdot B^i$ [adding sum]

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

$= \sum_{k<i} (bs[k] \cdot d + as'[k]) B^k + (bs[k] \cdot d + as'[k]) B^i + C \cdot B^i$ [partial distribution]

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

$= \sum_{k<i} as[k] \cdot B^k + (bs[i] \cdot d + as'[i]) C^i$ [Inductive Hypothesis Substitution]

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

because sum >> 32 = sum // B, and (uint32_t) sum = sum % B.

So, $\sum_{k<i} (bs[k] \cdot d + as[k]) B^k + (sum >> 32 \cdot B + (uint32\_t)\, sum) \cdot B^i$ [substitute sum]

since c = sum >> 32, and as[i] = (uint32_t) sum

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

$= \sum_{k<i} as[k] \cdot B^k + C \cdot B^{i+1} + as[i] B^i$ [IH substitution and distribution]

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

Then, once i increments, the top of the loop will then be:

$$= \sum_{k<i} as[k] \cdot B^k + c \cdot B^i$$

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

□