CPSC 406 Assignment 1

Vinny Caffaro

Part 1) $c + \sum_{k<i} as[k] = \sum_{k<i} (as'[k] + bs[k])$

* Basis: Let $i=0$

- If $i=0$, we are at top of loop, and $c=0$

$$0 + \sum_{k<0} as[k] = \sum_{k<0} (as'[k] + bs[k])$$

$$0 = 0 \qquad \text{[def. of summation]}$$

- For the ith iteration of the loop:

* First assigment of sum (s)

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

* After assignment of c and as[i]

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

$$= \sum_{k<i} (as'[k]+bs[k]) B^k + ((sum >> 32) + (uint32\_t\ sum)) B^i$$

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

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

* End of Loop

* Start of loop $i+1$

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

Part2) Proof of partial prod32

$$c + \sum_{k<i} as[k] = \sum_{k<i} \left(as'[k] + (bs[k] * d)\right)$$

Basis: $i = 0$

$$0 + \sum_{k<0} as[k] = \sum_{k<0} \left(as'[k] + (bs[k] * d)\right)$$

$$0 \stackrel{\checkmark}{=} 0$$

$$\sum_{k<i} (prod\_bd[k]) + prod\_c \cdot B = \sum_{k<i} \left(prod\_c + (bs[k] * d)\right)$$

*After assignment of temp

$$\sum_{k<i} (prod\_bd[k]) + prod\_c \cdot B = \sum_{k<i} (temp)$$

$$\sum_{k<i} (prod\_bd[k]) + prod\_c \cdot B = \sum_{k<i} \left((temp \gg 32) \cdot B + ((uint32\_t)temp)\right)$$

$$\sum_{k<i} (prod\_bd[k]) + prod\_c \cdot B = \sum_{k<i} \left((prod\_c) \cdot B + prod\_bd[k]\right)$$

$$\sum_{k<i} (prod\_bd[k]) + prod\_c \cdot B \stackrel{\checkmark}{=} \sum_{k<i} (prod\_bd[k]) + prod\_c \cdot B$$

Prod_bd stores the product of b & d, so our unmodified addto32 code proved in Part 1 should compute:

$$c + \sum_{k<i} as[k] = \sum_{k<i} \left(as'[k] + prod\_bd[k]\right)$$

Part 3) $\sum_{k<i} c[k] = \sum_{j<sz\_b} \left(\left(\sum_{k<i} a[k]\right) * b[j]\right)$

* On the nth iteration $(j<n)$

$$\sum_{j<n}\left(\left(\sum_{k<i} a[k]\right) * b[j]\right) = \sum_{j<n}\left(\sum_{k<i}\left(prod\_temp32[k] \cdot B^{j}\right)\right) \quad [1]$$

$$= \sum_{j<n}\left(\sum_{k<i} prod\_shifted32[k]\right) \quad [2]$$

$$= \sum_{k<i} c[k] \quad [3]$$

* [1]: Part 2 proves that partialprod32(prod-temp, a, b[j]) computes $\sum_{k<i} prod\text{-}temp += \sum_{k<i}\left((a[k]) * b[j]\right)$

* [2]: For loop computes: $\sum_{k<i} prod\_shifted = \sum_{k<i}\left(prod\_temp[k] * B^{i}\right)$

* [3]: Part 2 proves that addto32(c, prod_shifted) computes $\sum_{k<i} c[k] += \sum_{k<i} prod\_shifted[k]$