UBA - Facultad de Ciencias Exactas y Naturales - Departamento de Computación- Algoritmos y Estructura de Datos I

Primer parcial - 10/5/2019

Nro. de orden:
LU:
Apellidos:
Nombres:
Nro. de hojas que adjunta:

1	2	3		4			TOTAL
a	a	a	b	a	b	c	
						25	96

(A)

Aclaraciones: Se permite tener UNA hoja A4 con anotaciones durante el parcial. Cualquier decisión de interpretación que se tome debe ser aclarada y justificada. Para aprobar se requieren al menos 60 puntos.
Entregar cada ejercicio en una hoja separada, numerada y que incluya el nro. de orden.

Ejercicio 1. [20 puntos]

a) **[20 puntos]** Especificar la func: CantSubSeqCumple(A: $seq\langle\mathbb{Z}\rangle$) que devuelve la cantidad de subsecuencias de A (con longitud distinta a 0) que cumplen que la suma de sus elementos son divisibles por el tamaños de la misma subsecuencia más uno.

Por ejemplo,

- Si A=[7,2,0], todas las subsecuencias de A que cumplen q la longitud sea distinta de 0, son, [[7],[2],[0],[7,2],[2,0],[7,2,0]], las que cumplen que la suma de sus elementos son divisibles por el tamano más uno son: [2], [0], [7,2]. [2] cumple pués suma 2, que es divisible por el tamano más uno, que tambien es 2. Con [0] sucede lo mismo, y por último, [7,2] suma 9, que es divisile por el tamano más uno, que es 3.

Ejercicio 2. [20 puntos]

a) **[20 puntos]** Especificar el proc dameLaUnicaSubSeqQueCumple(in A: $seq\langle\mathbb{Z}\rangle$, out res: $seq\langle\mathbb{Z}\rangle$) **que devuelve la única subquecuencia no vacía de** A **que cumple que la suma de sus elementos es divisible por su tamaño más uno. Por ejemplo: si la entrada es** [5,2,11], la unica subsecuencia que cumple la propiedad es [2]. Por otro lado, la entrada [5,1,2] **no es una entrada valida pues**, la subsecuencia que cumple no es única (pues cumplen: [2] que es divisible por 2, [1,2] que la suma, 3, **es divisible por 3 y tambien** [5,1] que la suma es 6 y es divisible por 3). **Para resolver este problema se puede usar el predicado del ejercicio 1a.**

Ejercicio 3. [25 puntos] Dada la siguiente especificación junto con el siguiente programa:

proc swap3k (inout S: $seq\langle\mathbb{Z}\rangle$) {

Pre $\{S = S_0 \wedge |S| \ mod\ 2 = 0\}$

Post $\{|S| = |S_0| \wedge$

$(\forall j : \mathbb{Z})((0 \leq j < |S|/2 \wedge j \ mod\ 3 = 0) \rightarrow_L (S[j] = S_0[|S_0| - j - 1] \wedge S[|S| - j - 1] = S_0[j])) \wedge$

$(\forall j : \mathbb{Z})((0 \leq j < |S|/2 \wedge j \ mod\ 3 \neq 0) \rightarrow_L (S[j] = S_0[j] \wedge S[|S| - j - 1] = S_0[|S_0| - j - 1]))\}$

}

```
i := 0;
while (i < |S|/2) do
  if (i mod 3 == 0) then
    aux := S[i]
    S[i] := S[|S| - i - 1]
    S[|S| - i - 1] := aux
  endif;
  i:=i+1
endwhile
```

a) **[10 puntos]**Proponer el invariante del ciclo en palabras.

b) **[15 puntos]**Escribir el invariante con lógica, Pc y Qc

Ejercicio 4. [35 puntos]

Dado el siguiente programa, invariante , Pc y Qc

- $P_c : S = S_0 \wedge (i = 0)$
- $Q_c : |S| = |S_0| \wedge$
  $(\forall j : \mathbb{Z})((0 \leq j < |S| \wedge_L S[j] \ mod\ 2 = 0) \rightarrow_L S[j] = S_0[j]/2)$
- $I : |S| = |S_0| \wedge (0 \leq i \leq |S|) \wedge$
  $(\forall j : \mathbb{Z})((0 \leq j < i \wedge_L S[j] \ mod\ 2 = 0) \rightarrow_L S[j] = S_0[j]/2) \wedge$
  $(\forall j : \mathbb{Z})((i \leq j < |S|) \rightarrow_L S[j] = S_0[j])$

```
i := 0;
while (i < |s|) do
  if ( s[i] mod 2 == 0 ) then
       s[i] := s[i] / 2;
  else
       skip
  endif
  i:=i+1;
endwhile
```

realizar los siguientes pasos de la demostración:

a) **[5 puntos]** $P_c \implies I$

b) **[5 puntos]** $(I \wedge \neg B) \implies Q_c$

c) **[25 puntos]** $\{I \wedge B\}S\{I\}$

6)

1) aux CantSubSeqCumple (A: seq<Z>): Z =

$$\sum_{j=1}^{|A|}\sum_{i=0}^{|A|-1} \text{if } (|subseq(A,i,j)| > 0 \land \underline{sumaSeq}(subseq(A,i,j)) \bmod |subseq(A,i,j)|+1 = 0) \text{ then } 1 \text{ else } 0 \text{ fi};$$

aux $\underline{sumaseq}(S: seq\langle \mathbb{Z}\rangle): \mathbb{Z} = \sum_{k=0}^{|S|-1} S[k]$;

2) proc dameLaUnicaSubSeqQueCumple (in A: seq<Z>, out res: seq<Z>) {

Pre { cantSubseqCumple (A) = 1 }

Post { $0 < |res| \leq |A| \land_L \underline{esSubseqDe}(res, A) \land \underline{sumaseq}(res) \bmod |res|+1 = 0$ }

pred $\underline{esSubseqDe}$ (res: seq<Z>, A: seq<Z>) {

$(\exists i: \mathbb{Z})(\exists j: \mathbb{Z})((0 \leq i < j \land i < j \leq |A|) \land_L |res| = subseq(A,i,j))$

}

SIN LOS PALITOS!

}

3) Antes de comenzar el ciclo, i vale 0, y el ciclo termina cuando $i \geq \frac{|S|}{2}$. Por lo tanto, como el invariante debe valer antes y después de cada ejecución del ciclo, i debe estar entre cero y $\frac{|S|}{2}$. ✓

La variable aux es interna al ciclo, y como el invariante solo predica sobre el estado al iniciar y al finalizar el ciclo, no es necesario incluirla. ✓

El ciclo va recorriendo las posiciones de la secuencia en espejo e intercambiando las que son múltiplo de 3 (contando desde el principio y desde el final). Por este motivo, si en determinada iteración la posición que se evalúa en la guarda del if no es múltiplo de 3, la secuencia queda igual. También queda igual en las posiciones que aún no recorrió el ciclo. ✓

Si la posición es múltiplo de 3, se intercambian los valores y en este caso sí se produce un cambio en S.

Entonces, el invariante sería ✓

$(|S| = |S_0| \land |S| \bmod 2 = 0 \land 0 \leq i \leq \frac{|S|}{2}) \land_L$ (las caracteristicas de la secuencia y los valores posibles de i) ✓

$(\forall j: \mathbb{Z})((0 \leq j < i \land j \bmod 3 = 0) \to_L (S[j] = S_0[|S_0|-j-1] \land S[|S|-j-1] = S_0[j])) \land$ ✓

lo que les ocurre a las posiciones que son múltiplo de 3, que se intercambian

$(\forall j: \mathbb{Z})((0 \leq j < i \land j \bmod 3 \neq 0) \to_L (S[j] = S_0[j] \land S[|S|-j-1] = S_0[|S_0|-j-1])) \land$ ✓

lo que les ocurre a las posiciones que no son múltiplo de 3, que quedan igual

$(\forall j: \mathbb{Z})(i \leq j < \frac{|S|}{2} \to_L (S[j] = S_0[j] \land S[|S|-j-1] = S_0[|S_0|-j-1]))$ ✓

las posiciones que aún no recorrió el ciclo quedan igual

Por lo tanto:

$I \equiv \left(|s|=|s_0| \wedge |s| \bmod 2 = 0 \wedge 0 \le i \le \frac{|s|}{2}\right) \wedge_L (\forall j:\mathbb{Z})((0\le j<i \wedge j \bmod 3 = 0) \to_L$
$(s[j]=s_0[|s_0|-j-1] \wedge s[|s|-j-1]=s_0[j])) \wedge (\forall j:\mathbb{Z})((0\le j<i \wedge j \bmod 3 \neq 0) \to_L$
$(s[j]=s_0[j] \wedge s[|s|-j-1]=s_0[|s_0|-j-1])) \wedge (\forall j:\mathbb{Z})(i \le j < \frac{|s|}{2} \to_L$
$(s[j]=s_0[j] \wedge s[|s|-j-1]=s_0[|s_0|-j-1]))$ ✓

$P_c \equiv i=0 \wedge s=s_0 \wedge |s| \bmod 2 = 0$ ✓

$Q_c \equiv |s|=|s_0| \wedge_L i=\frac{|s|}{2} \wedge (\forall j:\mathbb{Z})((0\le j<\frac{|s|}{2} \wedge j \bmod 3 = 0) \to_L (s[j]=s_0[|s_0|-j-1] \wedge$
$s[|s|-j-1]=s_0[j])) \wedge (\forall j:\mathbb{Z})((0\le j<\frac{|s|}{2} \wedge j \bmod 3 \neq 0) \to_L (s[j]=s_0[j] \wedge$
$s[|s|-j-1]=s_0[|s_0|-j-1]))$ ✓

$P_c \Rightarrow I$

$\overline{s=s_0} \wedge \overline{i=0} \Rightarrow \overline{|s|=|s_0|} \wedge \overline{0\le i\le |s|} \wedge_L (\forall j:\mathbb{Z})((0\le j<i \wedge_L s_0[j] \bmod 2 = 0)$
$\to_L s[j]=\frac{s_0[j]}{2}) \wedge (\forall j:\mathbb{Z})(i\le j<|s| \to_L s[j]=s_0[j])$

- $s=s_0 \Rightarrow |s|=|s_0|$ ✓
- $i=0 \Rightarrow 0\le i\le |s|$ ✓

Supongo $i=0$: $(\forall j:\mathbb{Z})((0\le j<0 \wedge_L s_0[j] \bmod 2 = 0) \to_L s[j]=\frac{s_0[j]}{2}) \wedge (\forall j:\mathbb{Z}((0\le j<|s|)$
$\to_L s[j]=s_0[j]) \equiv true \wedge s=s_0$ ✓

$s=s_0 \wedge i=0 \Rightarrow true \wedge s=s_0$ ✓

$I \wedge \neg B \Rightarrow Q_c$

$|s|=|s_0| \wedge 0\le i\le|s| \wedge i\ge|s| \wedge_L (\forall j:\mathbb{Z})((0\le j<i \wedge_L s[j] \bmod 2 = 0) \to_L s[j]=\frac{s_0[j]}{2})$
$\wedge (\forall j:\mathbb{Z})(i\le j<|s| \to_L s[j]=s_0[j]) \equiv |s|=|s_0| \wedge i=|s| \wedge_L (\forall j:\mathbb{Z})((0\le j<|s| \wedge_L$
$s_0[j] \bmod 2 = 0) \to_L s[j]=\frac{s_0[j]}{2}) \wedge (\forall j:\mathbb{Z})(|s|\le j<|s| \to s[j]=s_0[j]) \equiv$
$\equiv |s|=|s_0| \wedge i=|s| \wedge_L (\forall j:\mathbb{Z})((0\le j<|s| \wedge s_0[j] \bmod 2 = 0) \to_L s[j]=\frac{s_0[j]}{2}) \wedge true$ ✓

$\{I \wedge B\}\ S\ \{I\}$

quiero ver que $I \wedge B \Rightarrow wp(S, I)$

```
i := 0;
while (i<|s|) do                      B
    if (s[i] mod 2 == 0) then         c
        s[i] := s[i]/2;               T1      } S1
    else
        skip                          T2
    endif
    i := i+1;                         S2
endwhile
```

Voy a usar ~~los siguientes~~ estos reemplazos para simplificar la lectura

$$wp(S, I) \equiv wp(S_1 ; S_2 , I) \equiv wp(S_1 , \overbrace{wp(S_2, I)}^{E}) \equiv wp(S_1, E) \equiv$$

$$wp(\text{if } c \text{ then } T_1 \text{ else } T_2 \text{ endif}, E) \equiv def(c) \wedge_L [(c \wedge wp(T_1, E)) \vee$$

$$(\neg c \wedge wp(T_2, E))] \equiv 0 \leq i < |s| \wedge_L [(s[i] \bmod 2 = 0 \wedge wp(T_1, E)) \vee$$

$$(s[i] \bmod 2 \neq 0 \wedge wp(skip, E))] \equiv 0 \leq i < |s| \wedge_L [(s[i] \bmod 2 = 0 \wedge$$

$$\underbrace{wp(t_1, E)}_{1}) \vee (s[i] \bmod 2 \neq 0 \wedge \underbrace{E}_{2})]$$

(2) $$E \equiv wp(S_2, I) \equiv wp(i := i+1, I) \equiv def(i+1) \wedge_L I^{i}_{i+1} \equiv |s| = |s_0| \wedge$$

$$0 \leq i+1 \leq |s| \wedge_L (\forall j : \mathbb{Z})((0 \leq j < i+1 \wedge_L s_0[j] \bmod 2 = 0) \to_L s[j] = \frac{s_0[j]}{2}) \wedge$$

$$(\forall j : \mathbb{Z})(i+1 \leq j < |s| \to_L s[j] = s_0[j]) \equiv 0 \leq i < |s| \wedge_L (\forall j : \mathbb{Z})((0 \leq j \leq i \wedge_L$$

$$s_0[j] \bmod 2 = 0) \to_L s[j] = \frac{s_0[j]}{2}) \wedge (\forall j : \mathbb{Z})(i < j < |s| \to_L s[j] = s_0[j]))$$

(1) $$wp(t_1, E) \equiv wp(s[i] := \frac{s[i]}{2}, E) \equiv wp(s := setAt(s, i, \frac{s[i]}{2}), E) \equiv$$

$$0 \leq i < |s| \wedge_L E^{s}_{setAt(s, i, \frac{s_0[i]}{2})} \equiv 0 \leq i < |s| \wedge_L |s| = |s_0| \wedge \underbrace{[(\forall j : \mathbb{Z})((0 \leq j < i \wedge_L}_{\text{separo el caso } i=j\text{, que es el único}}$$

$$s_0[j] \bmod 2 = 0) \to_L s[j] = s_0[j]) \wedge \underbrace{((j = i \wedge s_0[i] \bmod 2 = 0) \to setAt(s, i, \frac{s[i]}{2})[i]}_{\text{afectado por el setAt}} =$$

$$\frac{s_0[i]}{2})] \wedge (\forall j : \mathbb{Z})(\underbrace{i < j < |s|}_{\substack{\text{el caso afectado por setAt} \\ \text{no está en el rango}}} \to_L s[j] = s_0[j])$$

$$\equiv 0 \leq i < |s| \wedge_L |s| = |s_0| \wedge (\forall j : \mathbb{Z})((0 \leq j < i \wedge_L s_0[j] \bmod 2 = 0) \to_L s[j] = s_0[j])$$

$$(\forall j : \mathbb{Z})(i < j < |s| \to_L s[j] = s_0[j]) \wedge (s_0[i] \bmod 2 \to s[i] = \frac{s_0[i]}{2})$$

por qué sacó i /2?

Reemplazo en $wp(S, I)$

$$0 \leq i < |s| \wedge_L |s| = |s_0| \wedge [(s[i] \bmod 2 = 0 \wedge (\forall j : \mathbb{Z})((0 \leq j < i \wedge_L s_0[j] \bmod 2 = 0) \to_L$$

$$s[j] = \frac{s_0[j]}{2}) \wedge \underbrace{(s_0[i] \bmod 2 = 0 \to s[i] = \frac{s_0[i]}{2})}_{\equiv \text{True} \ \boxed{\text{porque?}}} \wedge (\forall j : \mathbb{Z})(i < j < |s| \to_L s[j] = s_0[j])$$

$$\vee (s_0[i] \bmod 2 \neq 0 \wedge (\forall j : \mathbb{Z})((0 \leq j \leq i \wedge_L s[j] \bmod 2 = 0) \to_L s[j] = \frac{s_0[j]}{2}) \wedge$$

$$(\forall j : \mathbb{Z})(i < j < |s| \to_L s[j] = s_0[j])]$$

sigue en hoja 4

(4)

$wp(S, I) \equiv 0 \leq i < |s| \wedge_L |s| = |s_0| \wedge [(s_0[i] \bmod 2 = 0 \wedge (\forall j : \mathbb{Z})((0 \leq j < i \wedge_L s_0[j] \bmod 2 = 0) \rightarrow_L s[j] = \frac{s_0[j]}{2}) \wedge (\forall j : \mathbb{Z})(i < j < |s| \rightarrow_L s[j] = s_0[j])$
$\vee (s_0[i] \bmod 2 \neq 0) \wedge (s_0[i] \bmod 2 \neq 0 \wedge (\forall j : \mathbb{Z})((0 \leq j \leq i \wedge_L s[j] \bmod 2 = 0) \rightarrow_L s[j] = \frac{s_0[j]}{2}) \wedge (\forall j : \mathbb{Z})(i < j < |s| \rightarrow_L s[j] = s_0[j]))]$

Separo en casos

Si $s_0[i] \bmod 2 = 0$:

$(\forall j : \mathbb{Z})(0 \leq j < i \wedge_L s_0[j] \bmod 2 = 0) \rightarrow_L s[j] = \frac{s_0[j]}{2}) \wedge$
$(\forall j : \mathbb{Z})(i < j < |s| \rightarrow_L s[j] = s_0[j])$

Si $s_0[i] \bmod 2 \neq 0$:

$(\forall j : \mathbb{Z})((0 \leq j < i \wedge_L s_0[j] \bmod 2 = 0) \rightarrow_L s[j] = \frac{s_0[j]}{2}) \wedge$

puedo sacar i porque no cumple con lo que sigue

$(\forall j : \mathbb{Z})(i < j < |s| \rightarrow_L s[j] = s_0[j])$

Uso la propiedad: $(p \wedge q) \vee (\neg p \wedge q) \Leftrightarrow \underbrace{(p \vee \neg p)}_{\equiv true} \wedge q$

$$\boxed{wp(S, I) \equiv 0 \leq i < |s| \wedge_L |s| = |s_0| \wedge (\forall j : \mathbb{Z})((0 \leq j < i \wedge_L s_0[j] \bmod 2 = 0) \rightarrow_L s[j] = \frac{s_0[j]}{2}) \wedge (\forall j : \mathbb{Z})(i < j < |s| \rightarrow_L s[j] = s_0[j])}$$

$I \wedge B \equiv |s_0| = |s| \wedge 0 \leq i < |s| \wedge (\forall j : \mathbb{Z})((0 \leq j < i \wedge_L s[j] \bmod 2 = 0) \rightarrow_L s[j] = s_0[j]/2) \wedge (\forall j : \mathbb{Z})(i \leq j < |s| \rightarrow_L s[j] = s_0[j]) \Rightarrow wp(S, I)$

~~establezco~~ $I \wedge B$ es más fuerte que $wp(S, I)$ porque es igual excepto por el caso de i, que I lo considera y $wp(S, I)$ no.