

# Algoritmos y Estructuras de Datos II

Tomás Agustín Hernández



# 1. Especificación

## Consideraciones importantes / Reminders

- Utilizar operadores luego: Si estoy en LPO (Lógica de Primer Orden) utilizar los operadores luego si vemos que hay una posible indefinición como una división, o ingresar a una lista a un índice. Recordar que el para todo y un existe, aunque esté acotado por un rango, los cuantificadores predicen IGUAL para todos los valores. Entonces, aunque diga que  $x$  es positivo, también probará dividir inclusive por 0 y estallará.
- Recordar las condiciones bidireccionales
  - Si por algún motivo tengo que armar una “lista”, como, por ejemplo, los divisores de un número  $x$  tengo que indicar que, si el número divide a  $x$ , entonces ese número está en res, pero además todos los valores que están en res DIVIDEN a  $x$ . Es una condición bidireccional.
  - Otro ejemplo puede ser que tenga que considerar el máximo de una lista, si todos los valores  $y$  que están en la lista son menores que res entonces significa que res también pertenece a esa lista original.
- Recordar el significado de los cuantificadores con dos variables al mismo tiempo: En la lógica se ejecutan todos de uno a la vez. Es decir, si tengo que poner un para todo adentro de un para todo entonces hago un para todo solo con dos variables y listo.
- Recordar que cuando en un procedimiento llamo a un predicado y ese predicado devuelve algo de un para todo, existe (básicamente un valor de verdad) tengo que castear ese valor en el procedimiento porque son dos mundos distintos. Ej: asegura:  $\text{res} = \text{True} \iff \text{predicado}$
- Los predicados y funciones auxiliares no describen problemas. Son herramientas sintácticas para descomponer predicados.
  - Los procedimientos pueden llamar a funciones auxiliares o predicados. Un procedimiento no puede llamar a otro procedimiento.
  - Los predicados pueden llamar a predicados o auxiliares.
  - Las auxiliares solo pueden llamar auxiliares.
- No usamos nunca  $==$  en especificación, usamos siempre  $=$  y estamos comparando, no asignando.
- No existe el guardar o asignar en el mundo de la lógica. No puedo guardar en una lista en un índice específico porque si un valor. Para esto solemos usar que  $x$  valor pertenecerá a esta lista, por ejemplo.
- Si tengo un algoritmo que cumple una funcionalidad específica con un require más débil, puedo poner el require más restrictivo y va a funcionar igual pero NO al revés.

## Fórmulas compuestas

Decimos que una fórmula es compuesta a una fórmula que tiene más de una operación y esa operación necesita realizarse antes de conocer su valor.

- $(p \wedge q) \vee m$
- $((p \wedge q) \vee m) \implies n$

## Fórmula atómica

Decimos que una fórmula es atómica si se puede inferir su valor con una, o ninguna operación. Es irreducible.

- $p$
- $p \wedge q$

## Fórmulas bien definidas

Decimos que una fórmula está bien definida cuando el orden que hay que hacer las operaciones es clara. Es decir, cuando cada operación toma dos variables proposicionales, y al realizar la operación termina siendo una fórmula atómica.

- $p \wedge q \vee r$  está mal formada. No se especifica si primero se realiza el  $\wedge$  o el  $\vee$ .
- $(p \wedge q) \vee r$  está bien formada.
- $p \wedge q \wedge r \wedge m$  está bien formada porque son todas conjunciones.
- $p \vee q \vee r \vee m$  está bien formada porque son todas disyunciones.

## Cuantificadores

- Para todo:  $\forall$ 
  - *Garantiza la conjunción* :  $p(1) \wedge p(2) \wedge p(3) \cdots \wedge p(m)$ . Todos los casos deben ser true para que el cuantificador sea true.
  - Se acompaña por un  $\longrightarrow$  a la hora de predicar sobre los elementos.
  - $(\forall i : \mathbb{Z})(0 \leq i < |s| \longrightarrow s[i] \bmod 2 = 0)$ . Todos los elementos de la lista son divisibles por 2.
  - Estructura:  $\forall + \text{rango} + \longrightarrow_L$
- Existe:  $\exists$ 
  - *Garantiza la disyunción* :  $p(1) \vee p(2) \vee p(3) \cdots \vee p(m)$ . Con un caso true el cuantificador es true.
  - Se acompaña por un  $\wedge$  a la hora de predicar sobre los elementos.
  - $(\exists i : \mathbb{Z})(0 \leq i < |s| \wedge s[i] \geq 0)$ . Existe algún elemento en la lista que es mayor o igual a 0.
  - $\exists + \text{rango} + \wedge_L$

## Equivalencias entre fórmulas

Decimos que dos fórmulas son equivalentes  $\iff$  los valores de la tabla de verdad al aplicar la operación arroja el mismo resultado.

## Valuaciones

Las valuaciones surgen en base a la tabla de verdad. Las valuaciones serian darle valor a las variables proposicionales y ver el resultado de la operación. Solo hacen referencias a fórmulas atómicas.

## Tautologías, contradicciones y contingencias

- Una fórmula es tautología  $\iff$  el resultado de la operación en cada fila arroja siempre V.
- Una fórmula es contradicción  $\iff$  el resultado de la operación en cada fila arroja siempre F.
- Una fórmula es contradicción  $\iff$  el resultado de la operación en cada fila arroja siempre V y F.

## Relaciones de fuerza entre fórmulas

Decimos que una fórmula es más fuerte que la otra  $\iff$  una fórmula es más restrictiva que la otra, o está incluida en la otra.

En el mundo de la lógica, decimos que A es más fuerte que B  $\iff A \implies B$

- Si  $(A \implies B)$  y  $(B \implies A)$  son tautologías, entonces A y B son equivalentes.
- Si  $(A \implies B)$  es tautología y  $(B \not\implies A)$  no es tautología, entonces decimos que A es más fuerte que B.
- Si  $(A \not\implies B)$  y  $(B \not\implies A)$  son contingencias, entonces no existe relación de fuerza entre A y B.

Algunos ejemplos:

- $|s| = 0 \implies |s| \geq 0$ . En este caso vemos que  $|s| = 0$  es más fuerte que  $|s| \geq 0$  pues  $|s| = 0$  está incluido en  $|s| \geq 0$ . Por lo tanto,  $A \implies B$
- $|s| = 0 \implies |s| \geq 3$ . En este caso vemos que  $|s| = 0$  no es más fuerte que  $|s| \geq 3$  pues  $|s| = 0$  no está incluido en  $|s| \geq 3$ . Por lo tanto,  $A \not\implies B$
- $2 \leq i < |s| \implies 1 \leq i < |s|$ . En este caso  $A \implies B$ , pues  $i = 2$  está incluido en el rango de B. Por lo tanto,  $A \implies B$
- $0 \leq i < |s| \implies 1 \leq i < |s|$ . En este caso  $A \not\implies B$ , pues el 0 de A no es parte de B. Por lo tanto,  $A \not\implies B$

## Tipos de parámetros en especificacion

- in: Solo nos interesa el valor de entrada de una variable. No la vamos a modificar. Ya están inicializados
- out: Donde se retornará el resultado. No nos importa el valor inicial ni tampoco determina nada en nuestra función.
- inout: Necesitamos el valor original aunque lo terminamos modificando y devolviendo.

## Lógica trivaluada

También llamada lógica secuencial porque se procesa de izquierda a derecha; Nos introduce los conceptos de  $\wedge_L \vee_L \longrightarrow_L$  y el valor de indefinido  $\perp$ .

Se termina de evaluar una expresión cuando se puede deducir el valor de verdad.

Considere  $x = \text{true} \wedge y = \perp \wedge z = \text{false}$

- $x \vee_L y$ : Como el  $\vee_L$  necesita uno solo para ser verdadero, entonces como  $x$  ya es  $\text{true}$  entonces toda la fórmula es verdadera.
- $x \wedge_L y$ : Como el  $\wedge_L$  necesita que ambas variables sean verdaderas, evalúa indefinido y el programa estalla.
- $\neg x \longrightarrow_L y$ : Como el  $\longrightarrow_L$  solo es falso si el antecedente es  $\text{true}$  y el consecuente  $\text{false}$ , como en este caso el antecedente ya es  $\text{false}$ , toda la implicación es verdadera.
- $(x \wedge z) \wedge_L y$ : Como el  $\wedge_L$  necesita que ambas fórmulas sean  $\text{true}$ , en este caso, como  $(x \wedge z)$  es  $\text{false}$ , entonces ya toda la fórmula es falsa. Nótese que el  $\wedge$  de la condición interna no contiene el luego porque jamás se indefinirá.
- $(\forall i : \mathbb{Z})(0 \leq i < |s| \longrightarrow_L s[i] \geq 0)$  Nótese que aquí usamos un  $\longrightarrow_L$  porque podría ser que la lista esté indefinida o no exista el valor en  $s[i]$

## Predicados

- Viven en el mundo de la lógica.
- Nos sirven para poder modularizar nuestras especificaciones.
- Solamente devuelven valores de verdad  $\text{True}$  y  $\text{False}$  y es necesario castearlos en caso de querer devolver  $\text{bool}$  como tipo de dato.
- Los predicados pueden llamar a otros predicados o funciones auxiliares.
- Pueden utilizar cuantificadores.
- No tienen requiere ni asegura.
- No admite parámetros  $\text{in}$ ,  $\text{out}$ ,  $\text{inout}$ .

Ejemplo cuando tenemos que transformar el valor de verdad a tipo de dato:

```
pred divisiblePorDos (n:  $\mathbb{Z}$ ) {  
     $n \bmod 2 = 0$   
}  
  
proc esMultiploDeDos (in n:  $\mathbb{Z}$ ) : Bool  
    requiere {true}  
    asegura { $res = \text{true} \iff \text{divisiblePorDos}(n)$ }
```

Ejemplo usando un predicado sin necesidad de transformar el valor de verdad a tipo de dato:

```
pred todosSonPares (l:  $\text{seq}(\mathbb{Z})$ ) {  
     $(\forall i : \mathbb{Z}) (0 \leq i < |l| \longrightarrow_L l[i] \bmod 2 = 0)$   
}  
  
proc todosPares (in l:  $\text{seq}(\mathbb{Z})$ ) : Bool  
    requiere { $\text{todosSonPares}(l)$ }
```

## Funciones Auxiliares

- Son reemplazos sintácticos.
- Nos ayudan a modularizar las especificaciones.
- No pueden ser recursivas.
- Solo hacen cuentas.
- No pueden utilizar cuantificadores.
- Pueden llamar a predicados.
- Devuelven un tipo de dato.
- No tienen requiere ni asegura.
- No admite parámetros in, out, inout.

```
aux sumar (n:  $\mathbb{Z}$ , m:  $\mathbb{Z}$ ) :  $\mathbb{Z} = n + m$  ;  
aux sumarTodos (s:  $seq\langle\mathbb{Z}\rangle$ ) :  $\mathbb{Z} = \sum_{i=0}^{|s|-1} s[i]$  ;
```

## Aridad

Decimos que una función es de aridad  $n$  cuando la función recibe  $n$  cantidad de parámetros.

## Variables Ligadas y Libres

Las variables son ligadas  $\iff$  están dentro de un cuantificador mientras que son libres cuando no lo están.

- $(\forall i : \mathbb{Z})(0 \leq i < |s| \longrightarrow_L n \geq s[i])$  i es una variable ligada mientras que n y s son variables libres.
- $(\exists j : \mathbb{Z})(0 \leq j < |s| \wedge_L n \geq s[j])$  j es una variable ligada mientras que n y s son variables libres.
- $(\forall i : \mathbb{Z})(0 \leq i < |s| \longrightarrow_L n \geq s[i]) \wedge P(i)$  Ojo acá. i es una variable ligada, pero la i que está fuera del cuantificador  $P(i)$  no está ligada. Esta última debería ser renombrada para no tener problemas y confusiones.

Cuando tenemos variables ligadas **no** podemos hacer nada sobre ellas, entre esas cosas, no podemos reemplazarlas porque no dependen de nosotros sino de los cuantificadores.

## Cuantificadores anidados

Anidamos cuantificadores cuando el rango de las variables es exactamente el mismo.

- $(\forall i, j : \mathbb{Z})(0 \leq i, j < |s| \longrightarrow_L n \geq s[i][j]) \equiv (\forall i : \mathbb{Z})((0 \leq i < |s| \longrightarrow_L (\forall j : \mathbb{Z})(0 \leq j < |s| \longrightarrow_L n \geq s[i][j])))$

## Estado

Llamamos estado a los valores de las variables en un punto de ejecución específico. El estado de un programa es importante porque muta al asignar valores a las variables. Cuando necesitamos hablar del estado de una variable en un instante específico, hablamos de **metavariables**

## Metavariables

Llamamos metavariable a una variable en un instante dado. Es útil cuando tenemos que predicar como cambio el valor de una variable con respecto al inicial.

Cuando tenemos que utilizar metavariables, sea S una variable cualquiera podemos referirnos al instante de tiempo de S como  $S_t$  donde t indica el momento.

Notación  $S = S_0$

```
proc multiplicarPorDosAImpares (inout l:  $seq\langle\mathbb{Z}\rangle$ )  
  requiere  $\{l = l_0\}$   
  asegura  $\{|l| = |l_0|\}$   
  asegura  $\{(\forall i : \mathbb{Z})(0 \leq i < |s| \longrightarrow_L if(s_0[i] \bmod 2 \neq 0) then (s[i] = s_0[i] * 2) else (s[i] = s_0[i]) fi)\}$ 
```

Nota: Cuando utilizamos metavariables tenemos que indicar que al modificar algo directamente, si no modificamos todo el

conjunto de valores tenemos que indicar que los demás permanecen inalterados. En este caso, como estamos editando los valores, no tendría sentido que la lista salga con mayor longitud, es por eso que garantizamos que no cambia.

Otra manera de resolver el ejemplo anterior es utilizando `old(s)`

```
proc multiplicarPorDosAImpares (inout l: seq(Z))
  asegura {|l| = |old(l)|}
  asegura {(∀i : Z)(0 ≤ i < |s| →L if(old(s)[i] mod 2 ≠ 0) then (s[i] = old(s)[i] * 2) else (s[i] = old(s)[i]) fi)}
```

## Correctitud de un Programa

Decimos que un programa  $S$  es correcto respecto a una especificación si se cumple la precondition  $P$ , el programa termina su ejecución y se cumple la postcondición  $Q$ .

### Tripla de Hoare

Notación para indicar que  $S$  es correcto respecto a la especificación  $(P, Q)$

$$\{P\} S \{Q\}$$

### SmallLang

Es un lenguaje que nos permitirá poder validar la correctitud de un programa. Solo tiene dos operaciones:

- $x := E \equiv$  asignación
- `skip`  $\equiv$  no hace nada

Nota:  $E$  es una expresión cualquiera. Un valor, una función, cualquier cosa.

### Estructuras de Control en SmallLang

- Secuencia de pasos:  $S1; S2$  es un programa  $\iff S1$  y  $S2$  son dos programas.
- Condicionales: `if B then S1 else S2 endif` es un programa  $\iff B$  es una condición lógica (guarda) y  $S1$  y  $S2$  son programas.
- Ciclo: `while B do S endwhile` es un programa  $\iff B$  es una condición lógica y  $S$  un programa.

### Validez de una tripla de Hoare

$\{x \geq 4\} x := x + 1 \{x \geq 7\}$  Donde,

- $P = \{x \geq 4\}$
- $S = x := x + 1$
- $Q = \{x \geq 7\}$

¿Vale que  $\{P\} S \{Q\}$ ? Solo vale  $\iff x \geq 6$  por lo tanto, como la precondition  $P$  falla en los casos de  $x = 4$ ,  $x = 5$  podemos decir que la tripla de Hoare no es válida.

Esto que acabamos de hacer se llama demostrar la correctitud de un programa, y acabamos de demostrar que la precondition  $P$  para el programa  $S$  es demasiado débil pues no nos garantiza que llegaremos a  $Q$  cumpliendo  $P$ .

Existe una manera formal que nos permite conocer la precondition más débil de un algoritmo.

## Predicado def(E)

Dada una expresión E, llamamos def(E) a las condiciones para que E esté definida. Todas las constantes están definidas, por lo tanto  $\text{def}(x) \equiv \text{True}$ . La idea es ir separando en términos e ir colocando las definiciones necesarias para esa operación específica.

- $\text{def}(x + 1) \equiv \text{def}(x) \wedge \text{def}(1) \equiv \text{True} \wedge \text{True} \equiv \text{True}$
- $\text{def}(x/y) \equiv \text{def}(x) \wedge (\text{def}(y) \wedge y \neq 0) \equiv \text{True} \wedge (\text{True} \wedge y > 0) \equiv y \neq 0$
- $\text{def}(\sqrt{x}) \equiv (\text{def}(x) \wedge x \geq 0)$
- $\text{def}(a[i] + 3) \equiv (\text{def}(a) \wedge \text{def}(i)) \wedge_L 0 \leq i < |a| \wedge \text{def}(3) \equiv (\text{True} \wedge \text{True}) \wedge_L 0 \leq i < |a| \wedge \text{True} \equiv 0 \leq i < |a|$

## Predicado $Q_E^x$

Cuando hablamos de este predicado hablamos de reemplazar las ocurrencias de x por E en el programa. Solo se reemplazan las ocurrencias libres, no las ligadas.

## Axiomas

- Axioma 1:  $\text{wp}(x := E, Q) \equiv \text{def}(E) \wedge_L Q_E^x$
- Axioma 2:  $\text{wp}(\text{skip}, Q) \equiv Q$
- Axioma 3:  $\text{wp}(S1; S2, Q) \equiv \text{wp}(S1, \text{wp}(S2, Q))$
- Axioma 4:  $\text{wp}(S, Q) \equiv \text{def}(B) \wedge_L ((B \wedge \text{wp}(S1, Q)) \vee (\neg B \wedge \text{wp}(S2, Q)))$

## Axioma 1 con secuencias

El axioma 1 nos sirve para asignar una expresión a una variable; Sin embargo, si tenemos que guardar algo en una secuencia debemos utilizar el setAt.

- $\text{wp}(b[i] := E, Q)$   
 $\equiv \text{def}(\text{setAt}(b, i, E)) \wedge_L Q_{\text{setAt}(b, i, E)}^{b[i]}$   
 $\equiv (\text{def}(b) \wedge \text{def}(i) \wedge \text{def}(E)) \wedge_L 0 \leq i < |b| \wedge_L Q_{\text{setAt}(b, i, E)}^{b[i]}$   
 $\equiv 0 \leq i < |b| \wedge_L Q_{\text{setAt}(b, i, E)}^{b[i]}$   
 $\equiv \text{setAt}(b, i, E)[j] = \{E \text{ si } i = j, b[j] \text{ si } i \neq j\}$

TODO: Luego mostrar un ejercicio y aclarar que por cada condición se separan n cuantificadores.

## Precondición más débil (Weakest Precondition)

Es la precondición más débil que se necesita para poder ejecutar un algoritmo y satisfacer la postcondición Q.

Notación:  $\text{wp}(S, Q)$  donde S es el programa y Q la postcondición.

Teorema: Una tripla de Hoare  $\{P\} S \{Q\}$  es válida  $\iff P \longrightarrow_L \text{wp}(S, Q)$ .

Sea el siguiente enunciado, calcule la precondición más debil.

- $P = \{x \geq 4\}$
- $S = x := x + 1$
- $Q = \{x \geq 5\}$

$$P \longrightarrow_L \text{wp}(S, Q) \equiv \text{wp}(x := x + 1, x \geq 5) \equiv \text{def}(x + 1) \wedge_L Q_{x+1}^x \equiv \text{def}(x) \wedge_L \text{def}(1) \wedge_L x + 1 \geq 5 \\ \equiv \text{True} \wedge_L \text{True} \wedge_L x \geq 4 \equiv x \geq 4$$

Luego,  $\{x \geq 4\} \longrightarrow_L \{x \geq 4\}$  es true

Por lo tanto,  $\text{wp}(x := x + 1, x \geq 5) \equiv \{x \geq 4\}$

Finalmente, probamos que para poder satisfacer Q la precondición más debil que cumple P es cualquier  $x \geq 4$ .

Nota importante: Muchas veces puede ser que se nos solicite indicar que wp es incorrecta. Cuando se dice esto, significa que son precondiciones válidas pero hay algunas que no son la más débil.

## Precondición más débil en ciclos

Consideremos el siguiente ejemplo  $\{???\}S\{x = 0\}$  donde  $S$  es el siguiente programa

```
1 |   while(x>0) do
2 |       x := x-1
3 |   endwhile
```

Recordemos que esto es una tripla de Hoare, pero no podemos utilizar  $wp(S, Q)$  porque el programa es en base a ciclos. La precondición  $P$  más débil acá sería que  $x \geq 0$  porque para cumplir la postcondición  $Q$  me da igual si entra al ciclo o no. Eso tiene que quedar siempre claro, cuando estamos hablando en ciclos, si no entra al ciclo y satisface igual ya está.

### Predicado $H_k$

Definimos el predicado  $H_k$  para poder controlar la cantidad de iteraciones que hace un ciclo y poder calcular la precondición más débil.

- $H_0(Q) \equiv def(B) \wedge \neg B \wedge Q$
- $H_{k+1}(Q) \equiv def(B) \wedge B \wedge wp(S, H_k(Q))$  para  $k \geq 0$

### Axiomas

Definimos el Axioma 5 para poder verificar la correctitud de ciclos que hacen una cantidad de iteraciones fijas como

$$wp(\text{while } B \text{ do } S \text{ endwhile}, Q) \equiv (\exists_{i \geq 0})(H_i(Q))$$

¿Cual es el problema del Axioma 5 y el Predicado  $H_k$ ? El problema es que ambos nos sirven para poder validar la precondición de un ciclo que sabemos que finaliza luego de  $n$  iteraciones.

### Predicado $I$ - Invariante

Definimos el Invariante de un ciclo como un predicado que:

- Demuestra que el ciclo realmente funciona y nos ayuda a demostrar la correctitud parcial "si termina el ciclo... entonces se cumple  $Q$ "
- Vale antes de entrar al ciclo y luego de salir del ciclo.
- En cada iteración, el invariante debe volver a ser válido. En el medio de la iteración puede que deje de valer.
- Un buen invariante incluye el rango de la(s) variable(s) de control del ciclo.
- Un buen invariante tiene alguna afirmación sobre el acumulador del ciclo.

### Teorema del Invariante

Para poder probar que un ciclo es correcto, usamos el teorema del invariante.

- $P \equiv$  Las condiciones del requiere
- $P_c \equiv$  Las precondiciones que necesita el ciclo para poder ingresar, muchas veces son las líneas que están por encima del while y el requiere (¡no todas las del requiere!)
- $I \equiv$  Las condiciones que suceden antes y después de entrar al ciclo
- $B \equiv$  La guarda del ciclo
- $Q_c \equiv$  La postcondición del ciclo

Luego,

- $\{P\} S \{P_c\}$
- $P_c \implies I$
- $\{I \wedge B\} S \{I\}$
- $\{I \wedge \neg B\} \implies Q_c$

**Recordatorio:** Si aparece la  $S$  es que tenemos que calcular la  $wp$  porque es parte de la Tripla de Hoare.

**Recordatorio importante:** Para todo lo que es  $wp$  usamos SmallLang, es decir, cuando tenemos que validar la tripla de Hoare. En todos los demás casos usamos lógica.

Ej: No sería válido tener un if en un invariante.