

## 2. Nociones sobre Teoría de Conjuntos y Lógica

Para llevar a cabo nuestro propósito de especificar formalmente los problemas y demostrar rigurosamente la correctitud de nuestros programas, introduciremos algunas nociones sobre Teoría de Conjuntos y Lógica. Los conceptos y notación dados nos permitirán unificar la notación que utilizaremos en las especificaciones y las demostraciones de correctitud de programas.

### 2.1. Conjuntos, Relaciones, Funciones

Un *conjunto* es una colección de objetos distintos, o elementos como normalmente son llamados. Por ejemplo: el conjunto  $\{3,5\}$  consiste de los enteros 3 y 5 y es el mismo conjunto que  $\{5,3\}$ .

$\{\}$  representa al conjunto vacío, es decir, aquel que no contiene elementos. También se representa por  $\emptyset$ .

La notación anterior describe a un conjunto de manera explícita o por extensión, listando todos sus elementos. También podemos describir un conjunto de manera implícita o por comprensión:

$$\{i: \text{existe un natural } j \text{ tal que } i=2^j\}$$

La *cardinalidad o tamaño* de un conjunto es el número de elementos del conjunto, y se denota por  $|A|$  o  $\text{card}(A)$ . Así  $\text{card}(\{3,5\})=2$

Luego definiremos más formalmente lo que es una operación, sin embargo damos algunas operaciones que todos conocemos sobre conjuntos:

Operaciones entre conjuntos: Unión, Intersección, Diferencia.

Operaciones que producen un valor booleano (verdadero o falso): la igualdad entre conjuntos, la pertenencia ( $a \in A$ ), la no pertenencia ( $a \notin A$ ), la inclusión ( $A \subseteq B$ )

Operaciones que producen un número: Si  $A$  es un conjunto de números entonces  $\min A$  es el menor elemento de  $A$  y  $\max A$  es el mayor elemento de  $A$ .

El *conjunto de partes de un conjunto*  $A$ , denotado por  $2^A$ , es el conjunto cuyos elementos son todos los subconjuntos de  $A$ ,  $2^A = \{B : B \subseteq A\}$ . Una *partición de un conjunto*  $A$  es un conjunto cualquiera  $P = \{A_1, A_2, \dots, A_n\}$  tal que para todo  $i$  entre 1 y  $n$  se cumple que  $A_i \subseteq A$  y cualesquiera dos elementos de  $P$ ,  $A_i$  y  $A_j$ , con  $i$  distinto de  $j$ , tienen intersección vacía y la unión de todos es el conjunto  $A$ .

#### Relaciones y Funciones

Sean  $A$  y  $B$  dos conjuntos. El *producto cartesiano* de  $A$  y  $B$ , denotado por  $A \times B$ , es el conjunto de los pares ordenados  $(a,b)$  donde  $a \in A$  y  $b \in B$ :

$$A \times B = \{(a,b): a \in A \text{ y } b \in B\}$$

La cardinalidad de  $A \times B$  es  $|A| * |B|$

Una *relación binaria* en los conjuntos  $A$  y  $B$  es un subconjunto de  $A \times B$ . Si  $R$  es una relación y  $(a,b) \in R$ , entonces también escribimos  $a R b$ . El *dominio de  $R$* , denotado  $\text{dom}(R)$ , es el conjunto de los elementos  $a$  de  $A$  para los cuales existe un par  $(a,b)$  en  $R$ , el *rango de  $R$* , denotado  $\text{rango}(R)$ , es el conjunto de los elementos  $b$  de  $B$  para los cuales existe un par  $(a,b)$  en  $R$ .

Por ejemplo, sea  $P$  el conjunto de los seres humanos. Una relación en  $P \times P$  es la relación progenitor:

Progenitor =  $\{(a,b): a \in P \text{ y } b \in P \text{ y } a \text{ es progenitor de } b\}$

Sea  $N$  el conjunto de los números naturales. Una relación en  $N \times N$  es la relación sucesor:

Sucesor =  $\{(i, i+1): i \in N\}$

La relación identidad en  $A \times A$ , denotada por  $I$ , es la relación:

$I = \{(a,a): a \in A\}$

Una relación en  $A \times B$  puede que no contenga pares  $(a,b)$  para algún  $a$  en  $A$ , en este caso decimos que la relación es *parcial*. Por otro lado, decimos que la relación es *total* si existe al menos un par  $(a,b)$  para cada  $a$  en  $A$ . Si para cada  $b$  en  $B$  existe un par  $(a,b)$  en la relación decimos que  $R$  es *sobre*  $B$ .

La *relación secuenciación* de dos relaciones  $R$  en  $A \times B$  y  $S$  en  $B \times C$ , denotada por  $R.S$ , es la relación en  $A \times C$  definida por:

$$a R . S c \text{ si y sólo si Existe } b \text{ tal que } a R b \text{ y } b S c$$

Por ejemplo, la relación  $(\text{Progenitor} . \text{Progenitor})$  es la relación Abuelo =  $\{(a,c): a \text{ es abuelo de } c\}$

La secuenciación es *asociativa*:  $(R.S).T = R.(S.T)$  por lo que podemos omitir los paréntesis y escribir  $R.S.T$ .  $R^i$  denota la relación  $R$  secuenciada con ella misma  $i$ -veces, cuando  $R$  es una relación en  $A \times A$ .  $R^0$  representa a la relación identidad.

De igual forma la *relación inversa* de una relación  $R$  en  $A \times B$  es una relación, denotada por  $R^{-1}$  en  $B \times A$  y definida por  $\{(b,a): (a,b) \in R\}$

Una relación  $R$  en  $A \times A$  es *reflexiva* si  $I \subseteq R$ , es *simétrica* si siempre que el par  $(a,b)$  esté en  $R$  se tiene que el par  $(b,a)$  está en  $R$ , es *transitiva* si siempre que el par  $(a,b)$  esté en  $R$  y el par  $(b,c)$  esté en  $R$  se tiene que el par  $(a,c)$  está en  $R$ .

Una función  $f$  de  $A$  en  $B$  es una relación en  $A \times B$  donde para cada  $a \in A$  existe a lo sumo un par  $(a,b)$  y se denota por:

$$f : A \rightarrow B$$

Por ser una relación, a una función aplican todos los conceptos dados sobre relaciones. Cada par de una función lo podemos escribir de la forma  $(a, f(a))$ ,  $f(a)$  es llamado el valor de la función  $f$  para el argumento  $a$ . Diremos que la función  $f$  no está definida para un elemento  $a$  de  $A$  si  $f$  no contiene el par  $(a,b)$  cualquiera sea  $b$  en  $B$ .

La relación sucesor es una función. Así  $\text{sucesor}(1)=2$ ,  $\text{sucesor}(i)=i+1$ .

Una *operación n-aria* es una función del producto cartesiano de  $n$  conjuntos en un conjunto, decimos que la operación es de *aridad*  $n$ . Por ejemplo, si  $P(A)$  representa el conjunto de todos los subconjuntos de un conjunto  $A$ , entonces la función que asigna a cada par  $X, Y$  de elementos de  $P(A)$ , la unión de  $X$  e  $Y$  es una operación binaria de  $P(A) \times P(A)$  en  $P(A)$ , el valor de la operación unión aplicada a  $X$  e  $Y$  la denotamos usualmente por  $X \cup Y$ , y decimos que  $\cup$  es el *operador* unión. Decimos que  $X$  e  $Y$  son los operandos de la operación unión.

### Secuencias, números enteros y reales

Una *secuencia* es una función total de  $A=\{0, 1, 2, \dots, n-1\}$  en  $B$ , donde  $B$  es cualquier conjunto y  $n$  cualquier número natural. Por ejemplo la función  $S=\{(0,b_0), (1,b_1), (2,b_2), \dots, (n-1,b_{n-1})\}$  es una secuencia y decimos que es de largo  $n$ , denotamos el largo de una secuencia  $s$  por *largo(s)* o por  $|s|$ , y vemos que en general el largo de una secuencia es igual a la cardinalidad de su dominio.

Hay otra forma de denotar una secuencia, por ejemplo, la secuencia  $S$  anterior también la podemos denotar de la siguiente forma:  $s = \langle b_0, b_1, \dots, b_{n-1} \rangle$ . Decimos que el primer elemento de la secuencia es  $b_0$ , el segundo elemento es  $b_1$ , y en general el elemento  $i$ -ésimo de la secuencia es  $b_{i-1}$ . También denotaremos los elementos de una secuencia en la forma  $s[i]$ , donde  $s[0]$  es el primer elemento, etc. Cuando el dominio de una secuencia sea vacío diremos que la secuencia es vacía y la denotamos por  $\langle \rangle$ .

Una operación binaria entre secuencias es la *concatenación*, denotada por  $\parallel$ . Si  $B = \langle b_0, b_1, \dots, b_{n-1} \rangle$  y  $C = \langle c_0, c_1, \dots, c_{m-1} \rangle$  son dos secuencias entonces  $B \parallel C$  es la secuencia  $\langle b_0, b_1, \dots, b_{n-1}, c_0, c_1, \dots, c_{m-1} \rangle$  la cual tiene largo  $n+m$ . Note que el elemento  $n+1$  de esta secuencia es  $c_0$ , el elemento  $n+2$  es  $c_1$ , etc.

La operación *primero* aplicada a una secuencia nos dá el primer elemento de la secuencia, así  $\text{primero}(\langle 1,2,3 \rangle)=1$ . La operación *resto* aplicada a una secuencia  $s$  de largo  $n$  nos devuelve la secuencia de largo  $n-1$ , cuyo  $i$ -ésimo elemento,  $1 \leq i \leq n$ , es el  $(i+1)$ -ésimo elemento de  $s$ , así  $\text{resto}(\langle 1,2,3 \rangle)=\langle 2,3 \rangle$ . Note que las operaciones primero y resto no están definidas para la secuencia vacía.

## Números

Normalmente utilizaremos los siguientes conjuntos:

El conjunto de los números enteros  $Z$ :  $\{\dots, -2, -1, 0, 1, 2, \dots\}$

El conjunto de los números naturales  $N$ :  $\{0, 1, 2, 3, \dots\}$

El conjunto de los números reales que denotaremos por  $\mathcal{R}$ .

Las siguientes operaciones toman por operandos números enteros o reales:

|                             |   |
|-----------------------------|---|
| $+, -, *$                   | suma, resta, multiplicación                               |
| $/$                         | división; produce un número real                          |
| $<, >, =, \geq, \leq, \neq$ | operadores de comparación; producen verdadero o falso     |
| $\text{abs}(x)$ ó $ x $     | valor absoluto  |
| $\lceil x \rceil$           | menor entero mayor o igual que $x$                        |
| $\lfloor x \rfloor$         | mayor entero menor o igual que $x$ (parte entera de $x$ ) |

Las siguientes operaciones, **div** y **mod**, tienen sólo enteros como operandos:

Dados dos números enteros  $x \geq 0$ ,  $y > 0$ , el cociente y resto de la división entera de  $x$  entre  $y$  son los números enteros  $q$  y  $r$ , respectivamente, que satisfacen:

$$x = y * q + r, 0 \leq r < y$$

|                    |   |
|--------------------|---|
| $x \text{ div } y$ | denotará el cociente de la división entera de $x$ entre $y$ . |
| $x \text{ mod } y$ | denotará el resto de la división entera de $x$ entre $y$ .    |
|                    | Note que $x \text{ mod } y = x - y * (x \text{ div } y)$      |

Ejercicios: Guías de Estructuras Discretas I. Autor: Pedro Borges.

- 1) Capítulo 2, ejercicios 1, 2, 3, 4, 12 con lógica, 13ª con lógica.
- 2) Capítulo 4: 4, 13.
- 3) Capítulo 5: 5

## 2.2. Proposiciones y Predicados

### Proposiciones

Una proposición es una expresión sobre un conjunto de *variables lógicas o booleanas*, es decir, variables que sólo pueden tomar los valores “verdadero” ó “falso” (denotaremos “verdadero” por V, y “falso” por F). Estas expresiones se definen como sigue:

- 1) V y F son proposiciones.
- 2) Una variable lógica (o identificador) es una proposición.
- 3) Si  $a$  es una proposición entonces  $(\neg a)$  es una proposición.
- 4) Si  $a$  y  $b$  son proposiciones entonces así lo son  $(a \wedge b)$ ,  $(a \vee b)$ ,  $(a \Rightarrow b)$ ,  $(a \equiv b)$

Ejemplo de proposiciones:  $\forall, ((\neg a) \vee (a \wedge b)), ((a \vee b) \vee (F \vee x))$

Como vemos en la sintaxis anterior, se han definido cinco operadores sobre valores de tipo booleano, uno de aridad 1 y cuatro de aridad 2 (binarios):

Negación: (no a), o  $(\neg a)$   
 Conjunción: (a y b), o  $(a \wedge b)$   
 Disyunción: (a o b), o  $(a \vee b)$   
 Implicación: (a implica b), o  $(a \Rightarrow b)$ , b es el antecedente y c la consecuencia  
 Equivalencia: (a es equivalente a b), o  $(a \equiv b)$

Evaluación de proposiciones.

Las operaciones de negación, conjunción, disyunción, implicación y equivalencia se definen de manera natural (desde el punto de vista lógico o de sentido común), como sigue:

| a | b | $\neg a$ | $(a \wedge b)$ | $(a \vee b)$ | $(a \Rightarrow b)$ | $(a \equiv b)$ |
|---|---|----------|----------------|--------------|---------------------|----------------|
| V | V | F        | V              | V            | V                   | V              |
| V | F | F        | F              | V            | F                   | F              |
| F | V | V        | F              | V            | V                   | F              |
| F | F | V        | F              | F            | V                   | V              |

Podemos evaluar expresiones booleanas de acuerdo a esta tabla. Por ejemplo: evaluemos la proposición  $((a \wedge (b \Rightarrow c)) \vee \neg c)$  para  $a=F, b=V, c=F$ . Reemplazamos en la expresión los valores de verdad de las variables y obtenemos  $((F \wedge (V \Rightarrow F)) \vee \neg F) = V$ .

Podemos omitir paréntesis de acuerdo a las siguientes reglas de precedencia de operadores:

- a) Secuencias del mismo operador son evaluadas de derecha a izquierda (ver David Gries). Por ejemplo:  $a \Rightarrow b \Rightarrow c \Rightarrow d$  es lo mismo que  $(a \Rightarrow (b \Rightarrow (c \Rightarrow d)))$ . Como veremos más adelante, los otros tres operadores binarios ( $\wedge, \vee, \equiv$ ) son asociativos, por lo que no importará por donde comience la evaluación.
- b) El orden de evaluación de operadores consecutivos diferentes es:
  - negación (prioridad más alta),
  - conjunción y disyunción, la misma prioridad,
  - implicación y equivalencia, la misma prioridad.
 Por ejemplo:  $b \Rightarrow c \Rightarrow d \wedge e$  es lo mismo que  $b \Rightarrow (c \Rightarrow (d \wedge e))$   
 $a \vee b \wedge c$  no sabremos cómo evaluarla.

Podemos convertir expresiones en español a forma de proposicional:

Por ejemplo la frase “Si llueve y me quedo en casa no me mojaré” la podemos convertir en una proposición de la siguiente forma:

Buscamos, si se puede, algunas proposiciones atómicas:

Llueve: a

Me quedo en casa: b

Me mojo: c

Y la frase en español quedaría en la forma:  $(a \wedge b) \Rightarrow \neg c$

Ejercicios: pag. 17 Gries, números 1, 2, 3, 4.

Una *Tautología* es una proposición que es verdad cualesquiera sean los valores de verdad de las variables que intervienen en ella. Por ejemplo  $(a \vee \neg a)$  es una tautología.

La lista siguiente son tautologías:

Leyes Conmutativas:

$$(E1 \wedge E2) \equiv (E2 \wedge E1)$$

$$(E1 \vee E2) \equiv (E2 \vee E1)$$

$$(E1 \equiv E2) \equiv (E2 \equiv E1)$$

Leyes Asociativas:

$$((E1 \wedge E2) \wedge E3) \equiv (E1 \wedge (E2 \wedge E3))$$

$$((E1 \vee E2) \vee E3) \equiv (E1 \vee (E2 \vee E3))$$

$$((E1 \equiv E2) \equiv E3) \equiv (E1 \equiv (E2 \equiv E3))$$

Leyes distributivas:

$$(E1 \vee (E2 \wedge E3)) \equiv ((E1 \vee E2) \wedge (E1 \vee E3))$$

$$(E1 \wedge (E2 \vee E3)) \equiv ((E1 \wedge E2) \vee (E1 \wedge E3))$$

Leyes de De Morgan

$$\neg(E1 \wedge E2) \equiv (\neg E1 \vee \neg E2)$$

$$\neg(E1 \vee E2) \equiv (\neg E1 \wedge \neg E2)$$

Ley de Doble Negación:

$$\neg(\neg E1) \equiv E1$$

Ley del Tercero Excluido:

$$E1 \vee \neg E1 \equiv V$$

Ley de la Contradicción:

$$E1 \wedge \neg E1 \equiv F$$

Ley de la Implicación:

$$(E1 \Rightarrow E2) \equiv \neg E1 \vee E2$$

Ley de la Equivalencia:

$$(E1 \equiv E2) \equiv (E1 \Rightarrow E2) \wedge (E2 \Rightarrow E1)$$

Leyes de simplificación de la disyunción:

$$E1 \vee E1 \equiv E1$$

$$E1 \vee V \equiv V$$

$$E1 \vee F \equiv E1$$

$$E1 \vee (E1 \wedge E2) \equiv E1$$

Leyes de simplificación de la conjunción:

$$E1 \wedge E1 \equiv E1$$

$$E1 \wedge V \equiv E1$$

$$E1 \wedge F \equiv F$$

$$E1 \wedge (E1 \vee E2) \equiv E1$$

Ley de identidad:

$$E1 \equiv E1$$

Regla de Sustitución: Si  $e1 \equiv e2$  es una tautología y  $E(p)$  es una proposición donde aparece la variable  $p$ , entonces  $E(e1) \equiv E(e2)$  y  $E(e2) \equiv E(e1)$  son tautologías.

Regla de Transitividad: Si  $e1 \equiv e2$  y  $e2 \equiv e3$  son tautologías entonces  $e1 \equiv e3$  es una tautología.

Ejemplo de demostración de tautologías utilizando las leyes y reglas:

Demostrar que  $(b \Rightarrow c) \equiv (\neg c \Rightarrow \neg b)$  es una tautología

$$(b \Rightarrow c)$$

$$\equiv \neg b \vee c \quad (\text{por la ley de implicación})$$

$$\equiv c \vee \neg b \quad (\text{por la ley conmutativa})$$

$$\equiv \neg \neg c \vee \neg b \quad (\text{por la ley de negación y regla de sustitución})$$

$$\equiv \neg c \Rightarrow \neg b \quad (\text{por la ley de implicación})$$

Así  $(b \Rightarrow c) \equiv (\neg c \Rightarrow \neg b)$  es una tautología por la regla de transitividad.

Los pasos de la demostración deben leerse como sigue: partiendo del hecho que  $(b \Rightarrow c)$  es verdadero (lo cual es una suposición) se tiene que  $\neg b \vee c$  es verdadero pues  $(b \Rightarrow c) \equiv \neg b \vee c$  es una tautología (si  $V \equiv x$  es verdadero entonces  $x$  debe ser verdadero), etc.

Ejercicios: pag. 26 y 27 del Gries, números 1, 3, 4, 5, 6(b,e)

### Predicados:

Una proposición, como  $p \vee (q \wedge s)$ , la podemos ver como una función de  $\{V,F\}^3$  en  $\{V,F\}$ . Por ejemplo para  $p=V$ ,  $q=F$  y  $s=V$  el valor de la proposición es  $V$ .  $(V,F,V)$  se denomina *estado* de las variables  $p$ ,  $q$  y  $s$ . Para cada estado tendremos un valor de verdad para la proposición.

Ahora queremos extender la noción de estado para permitir a las variables contener valores de otros tipos, como enteros, conjuntos, etc. Con este fin en mente, la noción de una proposición será generalizada de dos maneras, dando lugar a los *predicados*:

- 1) En una proposición, una variable booleana podrá ser reemplazada por cualquier expresión que tenga valor  $V$  ó  $F$ , por ejemplo:  $x > y$ .
- 2) Definiremos los cuantificadores existencial ( $\exists$ ) y universal ( $\forall$ ), lo cual conllevará a explicar las nociones de identificadores libres y ligados y al alcance de las variables en las expresiones.

Consideremos la expresión  $(x > y)$ , donde  $x$  e  $y$  son de tipo entero. Cuando evaluamos la expresión para valores particulares de  $x$  e  $y$ , obtenemos un valor  $V$  ó  $F$ . Por lo tanto esta expresión puede reemplazar cualquier identificador en una proposición. Por ejemplo, reemplazando  $p$  en  $p \vee (q \wedge s)$  por  $(x > y)$ , obtenemos:

$$(x > y) \vee (q \wedge s)$$

La expresión que resulta de reemplazar una variable booleana en una proposición por una expresión que al evaluarla dé  $V$  ó  $F$ , se denomina *predicado*. Note que una proposición es un caso particular de predicado. Otros predicados válidos son:

$$\begin{aligned} & ((x > y) \wedge (z < y)) \vee (x+y \geq z) \\ & (x > y \wedge z < y) \vee x+y \geq z \end{aligned}$$

La segunda expresión muestra que tantos paréntesis no serán necesarios, pues consideraremos que los operadores lógicos tendrán prioridad más baja que los operadores relacionales (como  $<$ ) y los aritméticos.

### Evaluación de predicados:

La evaluación de un predicado es similar a la evaluación de una proposición. Todas las variables son reemplazadas por sus valores (que llamamos el estado de las variables), estos valores serán de los tipos a los que corresponda cada variable (entero, lógico, etc.). Luego se procede a evaluar la expresión resultante de reemplazar las variables por sus valores. Por lo que un predicado lo podemos ver como una función cuyo conjunto de partida es el producto cartesiano de los conjuntos de valores de las variables y el conjunto de llegada es  $\{V, F\}$ . Por ejemplo: el predicado  $x > y \vee (q \wedge s)$  en el estado  $x = 3, y = 4, q = F, s = F$ , tiene el valor de  $3 > 4 \vee (F \wedge F) = F$

Ejercicios: 1, 2, 3(g,h,i,j) pag. 70 de Gries.

### Cuantificadores Existencial y Universal

#### Cuantificador Existencial:

Sean  $m$  y  $n$  dos enteros con  $m \leq n$ . Consideremos el predicado:

$$(1) \quad E_m \vee E_{m+1} \vee \dots \vee E_{n-1}$$

donde cada  $E_i$  es un predicado. (1) es verdad en cada estado en el cual al menos uno de los  $E_i$  es verdad, y falso en caso contrario. Podemos expresar este hecho utilizando el cuantificador existencial  $\exists$  de la siguiente forma:

$$(2) \quad (\exists i: m \leq i < n: E_i)$$

Los valores  $i$  que satisfacen  $m \leq i < n$  se llama *el rango del identificador cuantificado  $i$* . (2) se lee como sigue: “Existe al menos un entero  $i$  tal que  $i$  está entre  $m$  y  $(n-1)$  inclusive, para el cual se cumple  $E_i$ ”

Ejemplo:  $(\exists i: m \leq i < n: x * i > 0)$ , y se lee: existe al menos un entero  $i$  entre  $m$  y  $n-1$  tal que  $x*i$  es mayor que 0

Por la definición anterior se tiene que:

$$\begin{aligned} (\exists i: m \leq i < m: E_i) &\equiv F \quad (\text{la disyunción de cero predicados es falso}) \\ \text{Para } k \geq m, (\exists i: m \leq i < k+1: E_i) &\equiv (\exists i: m \leq i < k: E_i) \vee E_k \end{aligned}$$

#### Cuantificador Universal:

Sean  $m$  y  $n$  dos enteros con  $m \leq n$ . Consideremos el predicado:

$$(3) \quad E_m \wedge E_{m+1} \wedge \dots \wedge E_{n-1}$$

donde cada  $E_i$  es un predicado. (3) es verdad en cada estado en el cual todos los  $E_i$  son verdad para ese estado, y falso en caso contrario. Podemos expresar este hecho utilizando el cuantificador universal  $\forall$  de la siguiente forma:

$$(4) \quad (\forall i: m \leq i < n: E_i)$$

El conjunto de valores que satisfacen  $m \leq i < n$  se llama *el rango* del *identificador cuantificado*  $i$ . (4) se lee como sigue: “Para todo entero  $i$  tal que  $i$  está entre  $m$  y  $(n-1)$  inclusive, se cumple  $E_i$ ”

Ejemplo:  $(\forall i: m \leq i < n: x * i > 0)$ , y se lee: para todo  $i$  entre  $m$  y  $n-1$  se tiene que  $x*i$  es mayor que 0

Por la definición anterior se tiene que:

$(\forall i: m \leq i < m: E_i) \equiv V$  (la conjunción de cero predicados es verdadero)

Para  $k \geq m$ :  $\forall i: m \leq i < k+1: E_i) \equiv (\forall i: m \leq i < k: E_i) \wedge E_k$

Podemos definir el cuantificador universal en términos del cuantificador existencial. Por ejemplo, para  $m = 3$  y  $n = 8$ :

$(\forall i: 3 \leq i < 8: E_i)$

$\equiv E_3 \wedge E_4 \wedge E_5 \wedge E_6 \wedge E_7$  (por definición de la notación  $\forall \dots$ )

$\equiv \neg \neg (E_3 \wedge E_4 \wedge E_5 \wedge E_6 \wedge E_7)$  (ley de negación)

$\equiv \neg (\neg E_3 \vee \neg E_4 \vee \neg E_5 \vee \neg E_6 \vee \neg E_7)$  (ley de De Morgan)

$\equiv \neg (\exists i: 3 \leq i < 8: \neg E_i)$  (definición del existencial)

Ejemplo de uso de los cuantificadores:

Existe un teorema matemático que dice que existen números primos arbitrariamente grandes. Este teorema lo podemos expresar más formalmente como sigue:

$(\forall n: 0 < n: (\exists i: n < i: \text{primo}(i)))$  implícitamente  $n$  e  $i$  son enteros, podría ser necesario explicitarlo en el rango!!.

donde  $\text{primo}(i) = (1 < i \wedge (\forall j: 1 < j < i: i \bmod j \neq 0))$

Ejercicios: pag. 75 Gries, número 6.

Podemos cuantificar sobre otros rangos que no sean los números enteros. Por ejemplo, si  $P(p)$  representa la expresión “ $p$  es una persona” y  $M(x)$  representa la expresión “ $x$  es mortal” entonces la expresión “todas las personas son mortales” se puede expresar por  $(\forall p: P(p): M(p))$ .

Supongamos que hemos probado que el predicado  $\max(n, -n) = \text{abs}(n)$ , donde  $\max$  es la función máximo entre dos números y  $\text{abs}$  la función valor absoluto, es una tautología en los

números enteros, es decir, en cada estado de la variable  $n$  la igualdad es verdadera. Por lo tanto es verdadero para todo entero  $n$ , por lo que el predicado siguiente es verdadero:

$$(\forall n : n \in \mathbb{Z} : \max(n, -n) = \text{abs}(n))$$

si en el contexto podemos sobreentender que  $n$  está en los enteros, podemos escribir:

$$(\forall n : \max(n, -n) = \text{abs}(n)), \text{ es decir, no especificar el rango.}$$

Cualquier tautología  $E$  es equivalente al mismo predicado  $E$  pero con todas sus variables libres  $i_1, i_2, \dots, i_m$  cuantificadas universalmente, es decir, es equivalente a  $(\forall i_1, i_2, \dots, i_m : E)$ . Por ejemplo:  $m \leq 0 \vee m > 0$  es equivalente a  $\forall m (m \leq 0 \vee m > 0)$

### Variables libres y ligadas:

El predicado:

$$(5) \quad (\forall i : m \leq i < n : x * i > 0)$$

afirma que  $x$  multiplicado por cualquier entero entre  $m$  y  $n-1$  (inclusive) es mayor que cero. Vemos que esto es verdad si y sólo si  $x$  y  $m$  son mayores que cero o  $x$  es menor que cero y  $n$  es a lo sumo 0. Por lo tanto (5) es equivalente a:

$$(6) \quad (x > 0 \wedge m > 0) \vee (x < 0 \wedge n \leq 0)$$

(cuando decimos (5) es equivalente a (6) queremos decir que  $(5) \equiv (6)$  es una tautología). Por lo tanto el valor de verdad de (5) depende del estado de las variables  $x, m, n$ , pero no de  $i$ . más aún, el significado de (5) no cambia si reemplazamos  $i$  por  $j$ . Diremos que  $x, n, m$  son *variables libres* del predicado (5) (ó (6)), y la variable  $i$  es una *variable ligada* en (5), y ella está ligada al cuantificador  $\forall$ .

Ejercicios: pag. 79 Gries.

### Otros cuantificadores:

Sea  $X$  un conjunto y  $\oplus$  una operación binaria sobre  $X$  conmutativa, asociativa y con elemento neutro  $e$ , es decir para todo  $x, y, z$  en  $X$ :

$$x \oplus y = y \oplus x$$

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z$$

$$e \oplus x = x \oplus e$$

Para la secuencia  $x(i), 0 \leq i$ , y  $n$  un número natural, la expresión  $x(0) \oplus x(1) \oplus \dots \oplus x(n-1)$  la escribimos como  $(\oplus i : 0 \leq i < n : x(i))$ .

Y tenemos:

$$(\oplus i : 0 \leq i < 0 : x(i)) = e$$

$$(\oplus i : 0 \leq i < n+1 : x(i)) = (\oplus i : 0 \leq i < n : x(i)) \oplus x(n)$$

La última línea puede ser acompañada con la nota “separación de  $i=n$ ”.

En general, esta cuantificación es de la forma:  $(\oplus x : R(x) : F(x))$ , donde  $x$  es una lista de variables,  $R$  es un predicado con variables libres  $x$ , llamado el *rango de la cuantificación*, y  $F$  es llamado el *término*.

Tenemos entonces que  $(\oplus x : \text{falso} : F(x)) = e$ , el elemento neutro de  $\oplus$ .

Los siguientes operadores son conmutativos, asociativos y poseen elemento neutro: la suma  $+$ , la multiplicación, el máximo  $\max$ , el mínimo  $\min$ , la conjunción  $\wedge$ , la disyunción  $\vee$ . El elemento neutro de  $+$ ,  $*$ ,  $\max$ ,  $\min$ ,  $\wedge$ ,  $\vee$  son respectivamente  $0$ ,  $1$ ,  $-\infty$ ,  $+\infty$ , verdadero, falso.

Utilizamos el símbolo  $\sum$  como símbolo de cuantificación de la suma de  $n$  números  $x(0) + x(1) + \dots + x(n-1)$ . Colocamos  $(\sum i : 0 \leq i < n : x(i))$  en lugar de  $(+ i : 0 \leq i < n : x(i))$ . De igual forma usamos  $\prod$  para denotar la cuantificación de la multiplicación en lugar de  $*$ :  $(\prod i : 0 \leq i < n : x(i))$ . Como ya vimos, utilizamos  $\forall$  y  $\exists$  para cuantificar respectivamente a  $\wedge$  y  $\vee$ .

Ejemplos:

$$(\sum i : 3 \leq i < 5 : i^2) = 3^2 + 4^2 = 25$$

$$(\sum x, y : 0 \leq x < 3 \wedge 0 \leq y < 3 : x*y) = 9$$

$$(\prod i : \text{falso} : x(i)) = 1$$

$$(\max i : 3 \leq i < 5 : i^2) = 16$$

Se tienen las siguientes propiedades:

a)  $\max$  y  $\min$  son distributivos uno respecto al otro:

$$x \min (\max i : R : F(i)) = (\max i : R : x \min F(i))$$

$$x \max (\min i : R : F(i)) = (\min i : R : x \max F(i))$$

b) Si  $R$  no es vacío:

$$x + (\max i : R : F(i)) = (\max i : R : x + F(i))$$

$$x + (\min i : R : F(i)) = (\min i : R : x + F(i))$$

c)  $(\max i : R \vee S : F(i)) = (\max i : R : F(i)) \max (\max i : S : F(i))$ , igual para  $\min$ .

Otro cuantificador es el *cuantificador de conteo*, denotado por  $\#$ . La función  $\# : \{\text{falso}, \text{verdadero}\} \rightarrow \{0, 1\}$ , se define como  $\#(\text{falso}) = 0$  y  $\#(\text{verdadero}) = 1$ . La expresión  $(\# i : R(i) : F(i))$ , donde  $F(i)$  es un predicado, se define como  $(\sum i : R(i) : \#(F(i)))$ , y representa el número de valores en el rango  $R$  para los cuales  $F$  es verdadero. En particular,  $(\# i : \text{falso} : F(i)) = 0$

Ejercicios: Página 49 Kaldewaij.

### Tautologías y Predicados más fuertes que otros:

Un predicado  $P$  es una tautología si para cualquier estado este es verdadero, la expresión “ $P$  es una tautología” la denotamos por  $[P]$ . Ejemplo, el predicado  $x > 0 \Rightarrow x \geq 0$  es una tautología y denotamos este hecho de la forma:  $[x > 0 \Rightarrow x \geq 0]$ .

Note que  $[x \geq 0 \Rightarrow x > 0]$  no se cumple, es decir  $x \geq 0 \Rightarrow x > 0$  no es una tautología.

Si  $[P \Rightarrow Q]$  entonces diremos que  $P$  es más fuerte que  $Q$  ó que  $Q$  es más débil que  $P$ . Ejemplo, como  $[x > 0 \Rightarrow x \geq 0]$  se cumple decimos que  $x > 0$  es más fuerte que  $x \geq 0$ . Se usa la expresión más fuerte en el sentido que el conjunto de estados que hacen verdad al antecedente de la implicación es un subconjunto (son menos estados) del conjunto de estados que hacen verdad al consecuente de la implicación.

Cuando en español decimos “el predicado  $Q$  se cumple **si** se cumple el predicado  $P$ ”, queremos decir que  $P \Rightarrow Q$  es una tautología. De igual forma, cuando decimos “ $Q$  se cumple **sólo si** se cumple  $P$ ”, queremos decir  $Q \Rightarrow P$  es una tautología. Por lo tanto cuando decimos “ $P$  se cumple **si y sólo si** se cumple  $Q$ ”, queremos expresar que  $P \equiv Q$  es una tautología.

Las leyes y reglas vistas para proposiciones (ley conmutativa, de De Morgan, etc.) se extienden de manera natural a predicados.

