

# Inducción y recursión

Lógica computacional

13 de marzo de 2024

## 1. Preliminares

Antes de empezar con el tema, que seguro es nuevo o al menos tiene aspectos nuevos para todos ustedes, debemos de partir de un suelo en común, las bases. Algunas no las cubriremos pues confiamos en que sus profesores de semestres pasados las dejaron muy claras, pero si no pueden acercarse, mandar un correo y podemos apoyarles en la medida de lo posible.

Hay dos conceptos que seguro ya vieron, pero que nos interesa regresar a ellos pues queremos ver algunos detalles específicos y además serán utilizados durante el curso (además de que de ahí salen ejercicios y debemos dejarles algo para que hagan ustedes). Estos son los de la inducción y la recursión.

En primer lugar hay algunas funciones que se definen de esta forma y que en esta materia tendrán importancia, tanto de forma inductiva como recursiva. Pero además durante el resto de la carrera necesitarán de estos conceptos y seguramente durante su desempeño profesional les serán útiles, ya más adelante les comentaré al respecto.

### 1.1. Relaciones

Empecemos con las ideas básicas:

**Definición 1** *Dados dos conjuntos  $A$  y  $B$  (posiblemente vacíos), su producto Cartesiano, denotado por  $A \times B$ , es el conjunto de parejas ordenadas:*

$$\{\langle a, b \rangle \mid a \in A, b \in B\}.$$

Definición que se puede ampliar a más conjuntos, digamos  $A_1, A_2, \dots, A_n$ , donde el producto Cartesiano es el conjunto de  $n$ -tuplas ordenadas  $\langle a_1, a_2, \dots, a_n \rangle$ . De esta forma podemos definir

**Definición 2** *Una relación binaria entre  $A$  y  $B$  es cualquier subconjunto  $R$  (posiblemente vacío) de  $A \times B$ .*

Ya en esta definición hay un *spoiler*, ya que le llamo  $R$ , esto deriva en lo que llamamos una relación.

**Definición 3** *Dada una relación  $R$  entre los conjuntos  $A$  y  $B$ , el conjunto*

$$\{x \in A \mid \exists y \in B \langle x, y \rangle \in R\},$$

*es llamado el dominio de  $R$ ,  $\text{dom}(R)$ . El conjunto*

$$\{y \in B \mid \exists x \in A \langle x, y \rangle \in R\},$$

*es llamado el rango de  $R$ ,  $\text{rango}(R)$*

Para ahorrar espacio podemos escribir  $\langle x, y \rangle \in R$  como  $xRy$ .

## Funciones parciales, totales y composición

Si se dan cuenta, estamos poniendo en un lenguaje formal algunas cuestiones matemáticas que ya han usado desde hace años, seguro desde su primer curso de matemáticas en primaria. Recuerden que estamos en lo de las bases comunes, así que sean pacientes con el exceso de definiciones. Ahora vamos con una definición de las funciones a partir de las relaciones.

**Definición 4** Una relación  $R$  entre dos conjuntos  $A$  y  $B$  es funcional si y sólo si, para toda  $x \in A$ , y  $y, z \in B$ ,  $(x, y) \in R$  y  $(x, z) \in R$  implica que  $y = z$ .

**Definición 5** Una función parcial es la tripleta  $f = \langle A, G, B \rangle$ , donde  $A$  y  $B$  son conjuntos arbitrarios (posiblemente vacíos) y  $G$  una relación funcional (posiblemente vacía) entre  $A$  y  $B$ , llamada la gráfica de  $f$ .

Que también suele escribirse la función parcial como  $f : A \rightarrow B$ , el elemento único en el rango de  $f$  tal que  $(x, y) \in \text{graf}(f)$  se denota por  $f(x)$ . Una función total es aquella función para la cual  $\text{dom}(f) = A$ .

Y para no dejarlo, vamos a hacer más abstracto algo que ya usan desde hace años, pero sigan la corriente, estamos formalizando todo, como si fuéramos a una fiesta elegante.

**Definición 6** Dadas dos relaciones binarias,  $R$  entre  $A$  y  $B$ , y  $S$  entre  $B$  y  $C$ , su composición escrita como  $R \cdot S$  es una relación entre  $A$  y  $C$  definida por el siguiente conjunto de parejas ordenadas

$$\{(a, c) \mid \exists b \in B, (a, b) \in R \text{ y } (b, c) \in S\}$$

Con esto podemos definir uno de esos factores que nos resultan útiles para algunas propiedades algebraicas de los conjuntos, la identidad, en este caso la relación identidad ( $I_A$ ) definida como  $\{(x, x) \mid x \in A\}$ , que es una función total. De manera similar podemos definir la relación *conversa* que al pasarlo a términos de relaciones funcionales derivará en la función inversa.

## Inyecciones, suprayecciones y biyecciones

Va un carrusel de definiciones

**Definición 7** Una función  $f : A \rightarrow B$  es inyectiva (uno a uno) si y sólo si para toda  $(x, y) \in A$ ,  $f(x) = f(y)$  implica que  $x = y$

**Definición 8** Una función  $f : A \rightarrow B$  es suprayectiva (sobre) si y sólo si para toda  $y \in B$ , hay alguna  $x \in A$  tal que  $f(x) = y$ . Es decir, el rango de  $f$  es  $B$ .

Y una función es *biyectiva* si es uno a uno y sobre.

## 1.2. Imagen directa, imagen inversa y secuencias

Más definiciones, no se agobien, es sólo para que todo quede bien definido, pero seguro estos son conceptos que ya tienen claros o al menos los han manejado con una cierta noción.

**Definición 9** Dada una función (parcial)  $f : A \rightarrow B$ , para todo subconjunto  $X$  de  $A$ , la imagen directa (imagen) de  $X$  bajo  $f$  es el conjunto

$$\{y \in B \mid \exists x \in X, f(x) = y\}, \quad (1)$$

Denotada como  $f(X)$ . Para todo subconjunto  $Y$  de  $B$ , la imagen inversa de  $Y$  sobre  $f$  es el conjunto

$$\{x \in A \mid \exists y \in Y, f(x) = y\} \quad (2)$$

denotada como  $f^{-1}(Y)$

**Definición 10** Dados dos conjuntos  $I$  y  $X$ , una secuencia  $I$ -indexada (o simplemente secuencia) es cualquier función  $A : I \rightarrow X$ , denotado  $(A_i)_{i \in I}$ .  $I$  es el conjunto índice. Si  $X$  es un conjunto de conjuntos,  $(A_i)_{i \in I}$  es una familia de conjuntos.

## 1.3. Vamos todos a contar

Todo esto anterior es para saber, de manera formal, qué es lo que hacemos cuando contamos. Lo que hacemos es definir una secuencia. Pero algunas de las definiciones anteriores nos pueden dar más detalles de la secuencia que usamos para contar.

Cuando aprendemos a contar en la infancia lo hacemos con los dedos, lo que hacemos es asociar los objetos contados con los números naturales. En ese sentido decimos que un conjunto  $A$  es:

- *Numerable* si y sólo si o  $A = \emptyset$  o si hay una suprayección  $h : \mathbb{N} \rightarrow A$
- *Infinitamente numerable* si y sólo si hay una biyección  $h : \mathbb{N} \rightarrow A$
- *No numerable* de cualquier otra forma.

Siendo más quisquillosos podemos hablar de los enteros positivos, que estarán definidos como  $\mathbb{N}_+$ , el subconjunto de los naturales positivos  $\{1, 2, \dots, n\}$  se denota como  $[n]$ . De esta forma  $[0]$  sería el conjunto vacío. Decimos que un conjunto  $A$  es finito si y sólo si existe una biyección  $h : [n] \rightarrow A$  para alguna  $n \in \mathbb{N}$ . Ese natural  $n$  es la cardinalidad del conjunto  $A$ , se escribe  $|A|$ .

Si hablamos de secuencias y el conjunto índice son los naturales, la secuencia  $(A_i)_{i \in I}$  es una secuencia contable, en el caso de que  $I$  sea  $[n]$  para algún  $n \in \mathbb{N}$  entonces es una secuencia finita.

## 1.4. Relaciones de equivalencia

**Definición 11** ■ Una relación binaria  $R \subset A \times A$  es reflexiva si y sólo si para toda  $x \in A$ ,  $(x, x) \in R$ .

- La relación  $R$  es simétrica si y sólo si para toda las  $x, y \in A$ ,  $(x, y) \in R$  implica que  $(y, x) \in R$ .

- La relación  $R$  es transitiva si y sólo si para todas las  $x, y, z \in A$ ,  $(x, y) \in R$  y  $(y, z) \in R$  implica que  $(x, z) \in R$ .
- Si la relación  $R$  cumple las tres características anteriores, entonces es una relación de equivalencia

**Definición 12** Dada una relación de equivalencia  $R$  sobre un conjunto  $A$  para toda  $x \in A$ , el conjunto  $\{y \in A \mid (x, y) \in R\}$  es la clase de equivalencia de  $x$  módulo  $R$  y se escribe como  $[x]_R$ .

Piensen en los enteros que entran en la clase de equivalencia del 2 módulo 3: 2, 5, 8, 11,....

Si juntamos todas las clases de equivalencia de los enteros módulo 3 volvemos a formar todos los enteros, pero además ningún elemento está en dos clases a la vez.

- El conjunto de clases de equivalencia módulo  $R$  es el cociente de  $A$  por  $R$ ,  $A/R$
- $A/R$  es también llamada una *partición* de  $A$ , cualesquiera dos clases de equivalencia son no vacías y disjuntas. Su unión es  $A$  misma.
- La función suprayectiva  $h_R : A \rightarrow A/R$  es la *función canónica* respecto a  $R$ .

Dada cualquier relación  $R$  sobre un conjunto  $A$ , las potencias de  $R$  son:

- $R^0 = I_A$ ,
- $R^1 = R$ ,
- $R^{n+1} = R^n \cdot R$

La unión  $R^+ = \bigcup_{n \geq 1} R^n$  es la *cerradura transitiva* de  $R$  y es la relación transitiva más pequeña sobre  $A$  que contiene a  $R$ . Por otro lado  $R^* = \bigcup_{n \geq 0} R^n$  es la *cerradura reflexiva y transitiva*.

Vamos a un ejercicio:

1. Dada una relación  $R$  sobre un conjunto  $A$ , prueba que  $R$  es transitiva si y sólo si  $R \cdot R \subset R$ .

*De izquierda a derecha:* Asumimos  $R$  es transitiva, por definición 11  $R$  es transitiva si y sólo si para todas  $x, y, z \in A$ , que  $(x, y) \in R$  y  $(y, z) \in R$  implican que  $(x, z) \in R$ . Es decir que si  $(a, c) \in R$  existe una  $b$  tal que  $(a, b) \in R$  y  $(b, c) \in R$ . Pero si recuerdan esta es la definición 6 de la composición de relaciones, si  $(a, b) \in R$  y  $(b, c) \in R$  entonces  $(a, c) \in R \cdot R$  y como  $(a, c) \in R$ , entonces  $R \cdot R \subset R$ .

*De derecha a izquierda:* Es similar, por definiciones.

## 1.5. Órdenes parciales y totales

Nos vamos acercando poco a poco a lo que es el tema de esta sección, pero necesitamos tener claras las definiciones. Van unas pocas más.

**Definición 13** Una relación  $R$  sobre un conjunto  $A$  es antisimétrica si y sólo si para toda  $x, y \in A$ ,  $(x, y) \in R$  y  $(y, x) \in R$  implica que  $x = y$

**Definición 14** ■ Una relación  $R$  sobre  $A$  es un orden parcial si y sólo si  $R$  es reflexiva, transitiva y antisimétrica.

- Dado un orden parcial  $R$  en  $A$ , la pareja  $\langle A, R \rangle$  es llamado un conjunto parcialmente ordenado. Un orden parcial se denota por el símbolo  $\leq$ .
- Dado un orden parcial  $\leq$  en  $A$ , dado cualquier subconjunto  $X$  de  $A$ ,  $X$  es una cadena si y sólo si para todos  $x, y \in X$ , o  $x \leq y$  o  $y \leq x$ .
- Un orden parcial  $\leq$  en un conjunto  $A$  es un orden total (u orden lineal) si y sólo si  $A$  es una cadena.
- Dado un orden parcial  $\geq$  en un conjunto  $A$ , dado cualquier  $X \subset A$ , un elemento  $b \in A$  es una cota inferior de  $X$  si y sólo si para toda  $x \in X$ ,  $b \leq x$ . Por el otro extremo  $m \in A$  es una cota superior si y sólo si para toda  $x \in X$ ,  $x \leq m$ . Noten que  $b$  y  $m$  son elementos de  $A$  pero no necesariamente de  $X$ .
- Un elemento  $b \in X$  es el mínimo de  $X$  si y sólo si para toda  $x \in X$ ,  $b \leq x$ . Un elemento  $m \in X$  es el máximo de  $X$  si y sólo si para toda  $x \in X$ ,  $x \leq m$ . Estos valores son únicos.
- Dado un subconjunto  $X$  de  $A$ , un elemento  $b \in X$  es minimal en  $X$  si y sólo si para toda  $x \in X$ ,  $x \leq b$  implica que  $x = b$ . Un elemento  $m \in X$  es maximal en  $X$  si para toda  $x \in X$ ,  $m \leq x$  implica  $m = x$ . Estos valores no son únicos.
- Un elemento  $m \in A$  es la mínima cota superior de un subconjunto  $X$ , si y sólo si el conjunto de cotas superiores de  $X$  no es vacío y  $m$  es el elemento menor en este conjunto. Un elemento  $b \in A$  es la máxima cota inferior de  $X$ , si y sólo si el conjunto de cotas inferiores de  $X$  no es vacío y  $b$  es el elemento mayor en este conjunto.

## 2. Conjuntos bien fundados e inducción completa

Como hasta este punto han visto puras definiciones tomaré una pausa para hablarse de una mujer relacionada con este tema que empezaremos a tratar. Si caminan por los pasillos de la facultad de ciencias, en una de sus escaleras hayaran el mural de Emmy Noether (quizá no se parece mucho, y no le dieron el tiempo suficiente a la persona que hizo el trabajo creativo, pero es valioso que se reconozca el trabajo de la científica). A esta matemática se le deben algunos de los conceptos que trataremos en este capítulo. Nacida el 23 de marzo de 1882 en Erlangen, región bávara alemana, su investigación fue variada y extensa. En física es famosa por el teorema de Noether, relacionado a las conservaciones de magnitudes físicas con simetrías en el formalismo matemático. Para el caso tratado aquí lo relevante es su labor en el álgebra abstracta. Fue una de las primeras mujeres en poder matricularse en la universidad de Baviera donde tomó clases con Karl Schwarzschild (también muy conocido en la física y astrofísica), Minkowski, Klein y Hilbert.

Por varios años ya tras titularse dio clases en la universidad de Erlangen sin recibir sueldo, entre que suplía a su padre y que no tenían contemplado darle un sueldo de profesora a una mujer. Hilbert y Klein insistieron en que se le dejara ingresar como profesora a la universidad de Gotinga, pero una parte de la facultad se negó, un tanto ante el *qué dirán*. A esto Hilbert respondió: “No veo por qué el sexo de un candidato pueda ser un argumento en contra de su admisión como **privatdozent**. Después de todo, somos una universidad, no un establecimiento de baños”.



Figura 1: Amalie Emmy Noether, imagen de dominio público.

La inducción bien fundada también es conocida como inducción noetheriana, justo por la labor de la matemática al respecto. Este tipo de inducción sucede en conjuntos parcialmente ordenados, que tienen un orden bien fundado. Dado un orden parcial  $\leq$  sobre un conjunto  $A$ , el *orden estricto*  $<$  asociado con  $\leq$  se define como:

$$x < y \text{ si y sólo si } x \leq y \text{ y } x \neq y. \quad (3)$$

Un conjunto parcialmente ordenado  $\langle A, \leq \rangle$  está *bien fundado* si y sólo si no tiene infinitas secuencias decrecientes  $(x_i)_{i \in \mathbb{N}}$ , es decir, secuencias tales que  $x_{i+1} < x_i$  para toda  $i \geq 0$ .

**Lema 1** *Dado un conjunto parcialmente ordenado  $\langle A, \leq \rangle$ ,  $\langle A, \leq \rangle$  es un conjunto bien fundado si y sólo si todo subconjunto no vacío de  $A$  tiene un elemento minimal.*

*De izquierda a derecha:* Suponemos que  $\langle A, \leq \rangle$  es bien fundado, como lo hace el libro [1] es por contradicción, suponiendo que cualquier subconjunto  $X \subset A$  y que no tiene un elemento minimal, entonces para cualquier  $x \in X$  existe una  $y \in X$  tal que  $y < x$ , no hay un minimal  $x \in X$ . Como  $X$  no es vacío existe  $x_0 \in X$ , y de ser cierto lo anterior entonces existe  $x_1 \in X$  tal que  $x_1 < x_0$ . Si aplicamos este argumento de manera recursiva llegamos a que tenemos una secuencia infinita decreciente, pero eso es una contradicción con nuestra suposición inicial de que el conjunto es bien fundado. Es necesario que  $X$  tenga un minimal.

*De derecha a izquierda:* Suponemos que todo subconjunto no vacío de  $A$  tiene un minimal. Si una secuencia infinita decreciente  $(x_i)$  existe en  $A$ , debe tener a fuerzas, por la primera suposición, un minimal, pero esto contradice el hecho de que  $x_{k+1} < x_k$ .  $\square$ .

Ahora sí, el momento más esperado del día **definiremos el principio de inducción completa o estructural**.

**Definición 15** *Sea  $\langle A, \leq \rangle$  un conjunto ordenado parcialmente bien fundado, y sea  $P$  una propiedad del conjunto  $A$ , es decir, la función  $P : A \rightarrow \{\text{false}, \text{true}\}$ . Decimos que  $P(x)$  se cumple si  $P(x) = \text{true}$ . Para probar que una propiedad  $P$  se cumple para toda  $z \in A$ , basta con mostrar que para toda  $x \in A$ :*

- **Hipótesis inductiva:** si  $x$  es minimal o  $P(y)$  es cierto para toda  $y < x$
- entonces  $P(x)$  se cumple.

El **paso inductivo** es que para toda  $x$ , el primer inciso implica el segundo. De manera formal:

$$(\forall x \in A)[(\forall y \in A)(y < x \supset P(y)) \supset P(x)] \supset (\forall z \in A)P(z) \quad (4)$$

Nótese que  $x$  es minimal,  $P(x)$  es el o los *casos base*.

**Lema 2** *El principio de inducción completa se cumple para todo conjunto bien fundado.*

Y de nueva cuenta el autor de la ya tan citada obra en estas notas lo hace por contradicción:

*Prueba:* Supongamos el principio de inducción completa es falso, entonces

$$(\forall x \in A)[(\forall y \in A)(y < x \supset P(y)) \supset P(x)], \quad (5)$$

es verdadero, pero  $(\forall z \in A)P(z)$  es falso, es decir  $(\exists z \in A)(P(z) = \text{false})$  es verdadero. En ese caso el conjunto

$$X = \{x \in A \mid P(x) = \text{false}\}, \quad (6)$$

es no vacío. Como  $A$  es bien fundado,  $X$  tiene algún minimal  $b$ . Como 5 es verdadero para toda  $x \in A$ , sea  $x = b$

$$[(\forall y \in A)(y < b \supset P(y)) \supset P(b)], \quad (7)$$

es verdadero. Si  $b$  además es minimal en  $A$ , no hay  $y \in A$  tal que  $y < b$ , entonces

$$(\forall y \in A)(y < b \supset P(y)), \quad (8)$$

es cierto de manera trivial (*tribilín*) y entonces  $P(b) = \text{true}$  lo que contradice que  $b \in X$ . De otra forma, para toda  $y \in A$  tal que  $y < b$ ,  $P(y) = \text{true}$ , ya que  $y$  pertenecería a  $X$  y  $b$  ya no sería minimal. Pero entonces

$$(\forall y \in A)(y < b \supset P(y)), \quad (9)$$

también sería cierto y 7 implica que  $P(b) = \text{true}$ , contradiciendo el hecho de que  $b \in X$ . Por lo tanto inducción completa es válida para conjuntos bien fundados  $\square$ .

## 2.1. Ejercicios

Veamos un ejercicio de inducción.

**Proposición:** Todo entero  $n \geq 2$  es un producto de números primos.

**Demostración:** Para  $n \geq 2$  denotamos  $P(n)$  como el enunciado “ $n$  es un número primo o el producto de dos números primos”.

**Base inductiva.**  $P(2)$  es verdadero ya que 2 es un número primo.

**Hipótesis inductiva.** Suponemos  $n \geq 2$  y  $P(n)$  verdadera para  $2 \leq k \leq n$ . Probamos que  $P(n+1)$  es verdadero.

- Si  $n+1$  es primo ya la hicimos.

- De lo contrario sabemos que  $2 \leq k \leq n < n + 1$ , entonces existen  $x, y \leq n$ , y  $n + 1 = xy$ , como  $x, y \leq n$  entonces  $P(x)$  y  $P(y)$  existen, por lo tanto  $n + 1$  es producto de primos y  $P(n + 1)$  existe.

**Teorema 1** (Principio de inducción Noetheriana) Sea  $(A, \preceq)$  un conjunto bien fundado. Para probar que una propiedad  $P(x)$  es verdadera para todos los elementos  $x$  en  $A$  es suficiente probar las siguientes propiedades:

- (a) **Base inductiva:**  $P(x)$  es verdad para todos los elementos minimales de  $A$ .
- (b) **Paso inductivo** Para cada no minimal  $x$  en  $A$ , si  $P(y)$  es verdad para toda  $y \prec x$  (**hipótesis inductiva**), entonces  $P(x)$  es verdad.

Para darles un ejemplo no me detendré en el caso del triángulo de Pascal, pero sí en el factorial que antes hicimos. Más que un ejercicio es un ejemplo ilustrativo.

**Ejemplo:** Demuestra que el factorial es una función total.

Recordemos que nuestra función factorial está definida de la siguiente forma:

$$\begin{aligned} f(0) &= 0! = 1 \\ f(x) &= x(x-1)!, \quad x > 0 \text{ y } x \in \mathbb{N}. \end{aligned}$$

Entonces aplicamos la inducción:

- **Base inductiva:** Estamos trabajando en los naturales más el 0 ( $\mathbb{N}_0$ ), el minimal es el 0 y por la definición de la función  $f(0) = 0! = 1$ , ya está.
- **Hipótesis inductiva:** Supongamos es cierto para  $n > 0$  con  $n \in \mathbb{N}_0$ , en ese caso tenemos que  $f(n) = n!$ .
- **Paso inductivo:** Probemos que se cumple para  $n + 1$ . Para este caso por definición  $f(n+1) = (n+1)n!$ , como supusimos que  $n!$  está valuado por consiguiente  $(n+1)n!$  está valuado también, es solo una multiplicación de naturales que da un natural  $\square$ .

## 2.2. Orden lexicográfico

**Definición 16** Sea un conjunto parcialmente ordenado  $\langle A, \leq \rangle$ , el orden lexicográfico  $<_L$  en  $A \times A$  inducido por  $\leq$  se define: para todas  $x, y, x', y' \in A$ ,

$$(x, y) <_L (x', y') \text{ si y sólo si} \tag{10}$$

$$x = x' \text{ y } y = y', \text{ o} \tag{11}$$

$$x < x' \text{ o} \tag{12}$$

$$x = x' \text{ y } y < y'. \tag{13}$$

**Lema 3** Si  $\langle A, \leq \rangle$  es un conjunto parcialmente ordenado y bien fundado, el orden lexicográfico en  $A \times A$  es también bien fundado.

**Demostración:** Otra vez, de acuerdo al autor del ya citado libro, lo hace por contradicción. Suponemos que hay una secuencia infinita decreciente  $(\langle x_i, y_i \rangle)_{i \in \mathbb{N}}$  en  $A \times A$ . Entonces



1. Hay un número infinito de distintas  $x_i$ : en este caso la sucesión es infinita y por definición  $\langle A, \leq \rangle$  no es bien fundado.
2. Sólo hay un número finito de distintas  $x_i$ : existe una  $k$  tal que para toda  $i \geq k$   $x_i = x_{i+1}$ , como supusimos al principio y ya que la  $x$  no puede decrecer, entonces  $(y_i)_{i \geq k}$  es una secuencia decreciente en  $A$ , contradiciendo que  $\langle A, \leq \rangle$  es bien fundado.

No queda de otra que  $\leq_L$  sea bien fundado  $\square$ .

**Definición 17** Sea  $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ , el conjunto de los enteros no negativos. La función de Ackermann se define como:

$$A(x, y) = \begin{cases} \text{if } (x == 0) \text{ then return } y + 1; \\ \text{else if } (y == 0) \text{ then return } A(x - 1, 1); \\ \text{else return } A(x - 1, A(x, y - 1)); \end{cases}$$

¿Es  $A(x, y)$  una función total? Es decir a cada par en  $\mathbb{N}_0 \times \mathbb{N}_0$  ¿le corresponde un valor entero no negativo?

*Demostración:* Sea  $\sqsubseteq$  lo que denota el orden lexicográfico en  $\mathbb{N}_0 \times \mathbb{N}_0$  de la forma:

$$(m_1, m_2) \sqsubseteq (n_1, n_2) \text{ si y sólo si } \begin{cases} m_1 < n_1, \\ m_1 = n_1 \text{ y } m_2 \leq n_2 \end{cases}$$

Entonces  $(\mathbb{N}_0 \times \mathbb{N}_0, \sqsubseteq)$  es un conjunto bien fundado con elemento minimal  $(0, 0)$ .

**Ejercicio:** Se tiene una función  $f : \mathbb{N} \rightarrow \mathbb{N}$  definida como:

$$f(x) = \begin{cases} x - 10 & \text{si } x > 100 \\ f(f(x + 11)) & \text{de otra manera.} \end{cases}$$

Demuestra por inducción bien fundada respecto al orden  $<$  que:

$$f(x) = \begin{cases} x - 10 & \text{si } x > 101 \\ 91 & \text{de otra manera.} \end{cases}$$

Un programa de Haskell para que vean que es cierto lo que dice:

```
funC x | x > 100 = x-10
      | otherwise = funC (funC (x+11))
```

### 3. Trabajando sobre funciones

Ya hablamos de relaciones, nos centramos en las relaciones de orden parciales para definir la recursión total, pero si recuerdan también hablo de funciones y gráficas ¿cómo podemos ampliar os conceptos a estas relaciones particulares?

**Definición 18** Un orden parcial en funciones parciales se define como:  $f \subseteq g$  si y sólo si  $\text{graf}(f)$  es un subconjunto de  $\text{graf}(g)$ . Decimos que  $g$  es una extensión de  $f$  y que  $f$  es una restricción de  $g$ .

Un lema útil:

**Lema 4** Sea  $(f_n)_{n \geq 0}$  una secuencia de funciones parciales  $f_n : A \rightarrow B$  tal que  $f_n \subseteq f_{n+1}$  para toda  $n \geq 0$ . Entonces  $g = (A, \cup \text{graf}(f_n), B)$  es una función parcial. Más aún,  $g$  es la mínima cota superior de la secuencia  $(f_n)$ .

## 4. Cadenas

Seré telegráfico en esta sección, pues seguro estas definiciones ya las vieron una y otra vez. Partimos de un conjunto  $A$  que incluso podría ser infinito:

- Una *cadena* es cualquier secuencia finita  $u : [n] \rightarrow A$ , donde  $n \in \mathbb{N}$ .
- Al conjunto  $A$  se le suele llamar un *alfabeto*.
- Dada la cadena  $u : [n] \rightarrow A$ ,  $n$  es la longitud de  $u$ ,  $|u|$ .
- La cadena vacía corresponde a  $n = 0$ ,  $\epsilon$ .
- El conjunto de todas las cadenas sobre  $A$  se denota  $A^*$ .
- Si  $u : [n] \rightarrow A$  es una cadena,  $n > 0$ , para toda  $i \in [n]$ ,  $u(i) = u_i$  es un elemento de  $A$ .
- Las cadenas pueden concatenarse (no daré definición, ver la bibliografía).
- Luego vienen las definiciones de prefijo, sufijo, subcadena y subfijo propio, pueden verlas pero me parece pueden ya estar más que claras.

## 5. Árboles

Los árboles son una estructura útil para acomodar conjuntos de datos, relacionarlos y agilizar la búsqueda.

### 5.1. Dominio de árboles

**Definición 19** Un dominio de árbol  $D$  es un subconjunto no vacío de cadenas en  $\mathbb{N}_+^*$  que satisface las condiciones:

- Para cada  $u \in D$  todo prefijo de  $u$  también está en  $D$ .
- Para cada  $u \in D$ , para todo  $i \in \mathbb{N}_+$ , si  $u_i \in D$ , entonces para toda  $j$ ,  $1 \leq j \leq i$ ,  $u_j$  también está en  $D$ .

Un ejemplo es el dominio de árbol  $\{\epsilon, 1, 2, 11, 21, 22, 221, 222, 2211\}$ .

**Definición 20** Dado un conjunto  $\Sigma$  de etiquetas, un  $\Sigma$ -árbol (o simplemente árbol) es una función total  $t : D \rightarrow \Sigma$  donde  $D$  es un dominio de árbol.

Noten que el dominio del árbol muestra que es un conjunto de cadenas ordenadas, el árbol tal cual es este mismo arreglo ordenado pero con cualquier etiqueta en sus elementos. El orden de cierta forma está implícito aunque puede tener cualquier etiqueta. El dominio se denota como  $\text{dom}(t)$ , cada cadena  $u \in \text{dom}(t)$  es llamada un nodo.

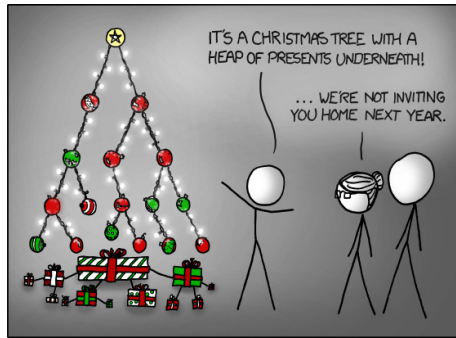


Figura 2: Imagen de xkcd con licencia CC-BY-NC.

**Definición 21** El rango o ramificación  $d(u)$  del nodo  $u$  es la cardinalidad del conjunto  $\{i | ui \in \text{dom}(t)\}$ .

- Un árbol de rango 0 es una *hoja*.
- El nodo con dirección  $\epsilon$  es la *raíz* del árbol.
- Un árbol  $t$  es finito si su dominio  $\text{dom}(t)$  es finito.
- Dado un nodo  $u$  en  $\text{dom}(t)$ , todo nodo de la forma  $ui$  en  $\text{dom}(t)$  con  $i \in \mathbb{N}_+$  es un hijo de  $u$ .

**Ejercicio:** Sea  $T$  un árbol binario con altura  $h$  y  $n$  nodos. Entonces  $n \leq 2^{h+1} - 1$ .

**Respuesta:** Hacemos inducción sobre  $h$ , la altura del árbol. **Caso base:** El caso base es cuando  $h = 0$ , en ese caso hay un nodo, es decir  $n = 1$ , y dado que  $h = 0$  entonces  $2^{h+1} - 1 = 2^1 - 1 = 1$ ,  $n = 1 \leq h = 1$ , de manera estricta  $1 = 1$ , lo cumple.

**Paso inductivo:** Suponemos que se cumple para toda  $h > 0$ , debemos demostrar que se cumple para  $h + 1$ . Debemos verlo por casos

- **Caso 1:**  $T$  consiste de una raíz más un subárbol  $X$ .  $x$  tiene una altura  $h - 1$  (es el árbol sin la raíz). De tal forma que  $h$  máximo  $2^h - 1$  nodos, así que  $T$  contiene máximo  $2^h$  nodos, que es menor que  $2^{h+1} - 1$  ya que  $2^{h+1} - 1 = 2 * 2^h - 1$  que sin importar cuanto vale  $h$  cumple  $2^h \leq 2^{h+1} - 1$ .
- **Caso 2:**  $T$  consiste de una raíz y dos subárboles  $X$  y  $Y$ , los cuales tienen alturas  $p$  y  $q$  respectivamente, tales que  $p, q < h$ . Por el paso inductivo sabemos que  $X$  y  $Y$  cumplen la relación, es decir que  $X$  tiene a lo más  $2^{p+1} - 1$  nodos y  $Y$  a lo más  $2^{q+1} - 1$  nodos. Pero como  $p, q < h$  entonces ambos árboles tienen una cantidad de nodos tales que  $\leq 2^h - 1$ . El número total de nodos es la suma de los nodos de  $X$  y  $Y$  más la raíz, es decir que el número total de nodos es  $\leq 1 + (2^p - 1) + (2^q - 1) \leq 1 + 2(2^h - 1) = 1 + 2^{h+1} - 2 = 2^{h+1} - 1$ . Así que el número total de nodos de  $T$  es  $\leq 2^{h+1} - 1$ .  $\square$

## 5.2. Inducción estructural sobre árboles

Cuando se puede establecer un orden entre nodos, por ejemplo si el árbol se llena con números naturales, y el padre siempre tiene un valor mayor que los hijos, se

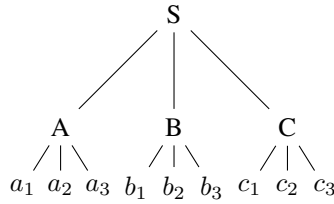


Figura 3: Árbol ternario.

dice que el árbol tiene una propiedad de pila (*heap*). Para verlo concentremos nuestra atención en un árbol binario.

**Proposición:** Si un árbol binario tiene la propiedad de pila entonces el valor en su raíz es cuando menos tan grande como cualquier valor en los nodos del árbol.

Sea  $v(a)$  el valor en uno de los nodos del árbol, para demostrarlo se usa la estructura recursiva de un árbol.

**Caso base:** Si el árbol contiene un sólo nodo, la raíz, es claro que se cumple.

**Paso inductivo:** Suponemos es cierto para los árboles  $X$  y  $Y$ , con ello probamos que es cierto para el árbol  $T$  que consiste en un nodo raíz y los subárboles  $X$  y  $Y$ . Sea  $r$  la raíz de  $T$  y  $p$  y  $q$  los hijos de esta raíz, es decir, la raíz de los árboles  $X$  y  $Y$  respectivamente. Como suponemos que  $T$  tiene la propiedad de pila entonces se cumple  $v(r) \geq v(p)$  y  $v(r) \geq v(q)$ .

Ahora sea  $x$  cualquier nodo del árbol  $T$ , probamos que  $v(r) \geq v(x)$  por casos:

- $x = r$  es el caso obvio.
- $x$  es un nodo en el subárbol  $X$ , por la hipótesis inductiva  $v(p) \geq v(x)$  y como sabemos que  $v(r) \geq v(p)$  entonces se cumple  $v(r) \geq v(x)$ .
- $x$  es un nodo en el subárbol  $Y$ , por la hipótesis inductiva  $v(q) \geq v(x)$  y como sabemos que  $v(r) \geq v(q)$  entonces se cumple  $v(r) \geq v(x)$ . □

## 6. Definiciones inductivas

Una definición inductiva tiene la siguiente estructura:

- Definición de los átomos, los elementos que son la base del objeto, pueden ser variables, letras, números.
- Especificación de las condiciones de cerradura, es decir que si al operar los átomos con ciertas operaciones los resultados vuelven a caer en la definición.
- La determinación de que los conjuntos así definidos son la expresión más pequeña de los conjuntos que pueden definirse así.

Para ponerlo en términos más formales:

**Definición 22** Sea  $A$  un conjunto y  $X$  un subconjunto de  $A$ , sea  $F$  un conjunto de funciones  $f : A^n \rightarrow A$ , con aridad  $n > 0$ <sup>1</sup>. Decimos que un conjunto  $Y$  es inductivo en

<sup>1</sup>La aridad se refiere a la cantidad de argumentos que acepta la función, si es 1 es una función unitaria, 2 binaria, 3 ternaria, etc.

$X$  si y sólo si  $X$  es subconjunto de  $Y$  y  $Y$  es cerrado bajo las funciones en  $F$ , es decir, para toda función  $f : A^n \rightarrow A$  en  $F$ , para toda  $y_1, y_2, \dots, y_n \in Y$ ,  $f(y_1, y_2, \dots, y_n) \in Y$  también.

EL mismo conjunto  $A$  es inductivo en  $X$ . La intersección de todos los conjuntos inductivos en  $X$  también está cerrado bajo  $F$ , se le llama la cerradura inductiva de  $X$  y se representa como  $X^+$ .

Podemos definir la secuencia de conjuntos  $(X_i)_{i \geq 0}$  de manera inductiva como:

- $X_0 = X$  y
- $X_{i+1} = X_i \cup \{f(x_1, \dots, x_n) \mid f \in F, x_1, \dots, x_n \in X_i, n = r(f)\}$
- Es claro que  $X_i \subseteq X_{i+1}$  para toda  $i \geq 0$ . Sea

$$X_+ = \bigcup_{i \geq 0} X_i. \quad (14)$$

Esta definición de la cerradura inductiva es por abajo, la de líneas arriba es por arriba, pero son equivalentes, la demostración puede consultarse en [1].

**Un ejemplo coloquial:** podemos definir a un *sadwich* (emparedado si quieren evitar el anglicismo) de forma inductiva:

1. Cualquier cosa que vaya entre dos panes es un emparedado.
2. Si tenemos un emparedado  $e_1$  y un emparedado  $e_2$ , si a ambos los ponemos entre dos panes también forman un emparedado (piensen en esos emparedados con varias capas, claro que esto abre la posibilidad a tener emparedados de aire).
3. Nada que no pueda hacerse con los pasos anteriores es un emparedado.

**Ejercicio:** Define el lenguaje de los términos agradables, aquellos formados por las letras  $a, b, c, d$  (una letra ya es en sí un término agradable, la cosa es ver las posibles combinaciones con los corchetes y el operador), los corchetes bien anidados  $[]$  (bien anidado quiere decir que todo corchete que se abra debe cerrarse, y no puede cerrarse un corchete sin tener uno abierto a la izquierda) y la operación binaria  $\cdot$  que se escribe como  $[a \cdot b]$ .

## 6.1. Conjuntos libremente generados

**Definición 23** Sea  $A$  un conjunto,  $X$  un subconjunto de  $A$ ,  $F$  un conjunto de funciones en  $A$  y  $X_+$  la cerradura inductiva de  $X$  bajo  $F$ . Decimos que  $X_+$  es libremente generado por  $X$  y  $F$  si se cumplen las siguientes condiciones:

- La restricción de toda función  $f : A^m \rightarrow A$  en  $F$  a  $X_+^m$  es inyectiva.
- Para toda  $f : A^m \rightarrow A$ ,  $g : A^n \rightarrow A$  en  $F$ ,  $f(X_+^m)$  es disjunta<sup>2</sup> de  $g(X_+^n)$  cuando  $f \neq g$ .
- Para toda  $f : A^m \rightarrow A$  en  $F$  y toda  $(x_1, \dots, x_m) \in X_+^m$ ,  $f(x_1, \dots, x_m) \notin X$ , es decir, los elementos son realmente básicos.

<sup>2</sup>Disjunta se refiere a que  $f(X_+^m) \cap g(X_+^n) = \emptyset$

**Ejemplo:** El grupo de los enteros positivos  $(\mathbb{Z}, \text{Sum}())$ , donde el grupo generador es  $S = \{1\}$  es libremente generado. La función  $\text{Sum}()$  sumará una unidad al argumento dado, así  $\text{Sum}(1)$  dará el siguiente natural (al cual no nombraremos 2 porque imaginemos que tiene derechos de autor, solo le llamaremos  $\text{Sum}(1)$ ). El siguiente natural será  $\text{Sum}(\text{Sum}(1))$ , que de nueva cuenta ya se figuran quien es pero no le daremos ese nombre. La función es inyectiva, a cada elemento del dominio  $(1, \text{Sum}(1), \dots, \text{Sum}^n(1), \dots)$  le asocia un sólo elemento del codominio. En este caso no hay más funciones así que podemos asegurar las disyunción, y no hay manera de que alguna  $\text{Sum}^i(1)$  nos regrese al mismo generador 1.

**Ejercicio:** ¿Como ampliarías la definición de los naturales positivos para incluir una operación más, la multiplicación? Considera que tienes la cerradura inductiva, pero si no te convence también puedes probarlo ¿necesitas un nuevo conjunto generador?

## Referencias

- [1] Gallier, Jean. “Logic for computer science. Foundations of automatic theorem proving” University of Pennsylvania (2003) [https://www.researchgate.net/publication/31634432\\_Logic\\_for\\_computer\\_science\\_foundations\\_of\\_automatic\\_theorem\\_proving\\_JH\\_Gallier](https://www.researchgate.net/publication/31634432_Logic_for_computer_science_foundations_of_automatic_theorem_proving_JH_Gallier)
- [2] Lemus, Vladimir. “Notas para el curso de programación funcional para la física computacional”, <https://git.disroot.org/vladomiro/notas-tsfc>.
- [3] <https://courses.engr.illinois.edu/cs173/fa2010/Lectures/trees.pdf> Consultada el 14 de febrero de 2024.