Inducción y recursión

Lógica computacional

8 de febrero de 2024

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 las 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.

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 le conjunto de parejas ordenadas:*

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

Definición que se puede ampliar a más conjuntos, digamos $A_1, A_2, ..., A_n$, donde el producto Cartesiano es el conjunto de eneadas ordenadas $\langle a_1, a_2, ..., a_n\rangle$. 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 *espoiler*, 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, $dom(R)$. El conjunto*

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

es llamado el rango *de R, $rango(R)$*

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 Bson 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 $f : A \to B$, el elemento único en el rango de f tal que $(x, y) \in graf(f)$ se denota por $f(x)$. Una función total es aquella función para la cual $dom(f) = A$.

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 resultán 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 $f : A \to B$ 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 $f : A \to B$ 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.

0.1. 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) $f : A \to B$, para todo subconjunto X de A, la* imagen directa *(*imagen*) de X bajo f es el conjunto*

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

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

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

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

Definición 10 *Dados dos conjuntos I y X, una* secuencia I-indexada *(o simplemente* secuencia*) es cualquier función $A : I \to X$, 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.*

0.2. 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 $h : \mathbb{N} \to B$
- *Infinitamente numerable* si y sólo si hay una biyección $h : \mathbb{N} \to A$
- *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 $\{1, 2, ..., n\}$ 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 $h : [n] \to A$ 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. 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 suprayectica $h_R : A \to A/R$ 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.

Órdenes parciales y totales

Nos vamos acercando poco a poco a lo que es el tema de esta sección, pero requerimos 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* elemento menor *de X si y sólo si para toda $x \in X$, $b \leq x$. Un elemento $m \in X$ es el* elemento mayor *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 ordenadas, que tienen un orden bien fundado. Dado un orden parcial $\leq$ sobre un conjunto A, el *orden estricto* $<$ asociado con $\leq$ se define como:

$$x < y \text{ si y sólo si } x \leq y \text{ y } x \neq y. \tag{3}$$

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 $P : A \to \{\mathbf{false}, \mathbf{true}\}$. Decimos* *que $P(x)$ se cumple si $P(x) = \mathtt{true}$. 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:

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

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

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

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

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

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

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

es verdadero. Si b además es minimal en A, na hay $y \in A$ tal que $y < b$, entonces

$$(\forall y \in A)(y < b \supset P(y)), \tag{8}$$

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

$$(\forall y \in A)(y < b \supset P(y)), \tag{9}$$

también sería cierto y 7implica que $P(y) = \mathtt{true}$, 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.

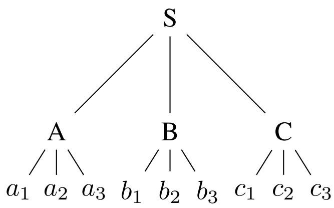

Figura 2: Árbol ternario.

- 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.

Considera la siguiente función que actúa sobre árboles ternarios de naturales ($A_3(a,b,c)$ es un árbol con ramas a, b, c):

$$\begin{aligned}
card(n) =& 1 \; n \in \mathbb{N} \\
card(A_3(a,b,c)) =& card(a) + card(b) + card(c) \\
prof(n) =& 1 \; n \in \mathbb{N} \\
prof(A_3(a,b,c)) =& \text{máximo}\{prof(a), prof(b), prof(c)\} + 1
\end{aligned}$$

Demuestra por inducción bien fundada que $card(a) \leq 3^{prof(a)}$

Base inductiva: $card(a) = 1$ si $a \in \mathbb{N}$, para el mismo caso $prof(n) = 1$. $card(a) = 1 \leq 3 = 3^1 = 3^{card(a)}$. **Hipótesis inductiva:** Suponemos que es cierto para $card(A(\square, \square, \square)) = 3^{prof(A)}$. Por demostrar que es cierto para $B(A, S, T)$.

$$\begin{aligned}
card(B(A,S,T)) =& card(A) + card(S) + card(T) \\
\leq& 3^{prof(A)} + card(S) + card(T) \\
\leq& 3^{prof(A)} + 3^{prof(S)} + 3^{prof(T)} \\
\leq& 3(3^{\text{máximo}\{prof(A), prof(S), prof(T)\}}) \\
=& 3^{\text{máximo}\{prof(A), prof(S), prof(T)\}+1} = 3^{prof(B(A,S,T))}
\end{aligned}$$

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 $x, y, x', y' \in A$,*

$$(x,y) <_L (x',y') \text{ si y sólo sí} \tag{10}$$
$$x = x' \text{ y } y = y', \text{ o} \tag{11}$$
$$x < x' \text{ o} \tag{12}$$
$$x = x' \text{ y } y < y'. \tag{13}$$

Referencias

[1] Gallier, Jean. "Logic for computer science. Foundations of automatic theorem proving" University of Pensylvania (2003) 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.