ANÁLISIS LÓGICO
INDUCCIÓN Y RECURSIÓN

Francisco Hernández Quiroz

Departamento de Matemáticas
Facultad de Ciencias, UNAM
E-mail: fhq@ciencias.unam.mx
Página Web: www.matematicas.unam.mx/fhq

Facultad de Ciencias

Resumen

En este capítulo se estudiarán los conjuntos inductivos y las funciones recursivas definidas en éstos.
Dichos conjuntos y funciones serán los elementos básicos de todos los lenguajes que se verán en el resto del curso.

Definiciones “circulares”

- Es muy común definir un conjunto de manera “circular”. Por ejemplo, las fórmulas del cálculo de proposiciones:
  “Si ϕ y ψ son proposiciones, entonces $\neg\phi$ y $\phi \vee \psi$ son proposiciones”.
- Si la definición anterior fuera realmente circular, sería incorrecta.
- En realidad, lo que se hace es definir el conjunto anterior de manera *inductiva*.
- Una definición inductiva parte de un conjunto básico y de un conjunto de funciones que generan nuevos elementos a partir del conjunto básico.

Nota: En algunos textos se llama *recursivas* a estas definiciones. Esto es un error terminológico.

Conjuntos inductivos

Definición

- *Sea $A \subseteq U$ un conjunto y sea $F = \{f_i^n : U^n \to U\}$ un conjunto de funciones. Decimos que A es cerrado bajo F sii $\forall f_k^n \in F$ y $\forall a_1, \ldots a_n \in A$ resulta que $f_k^n(a_1, \ldots, a_n) \in A$.*
- *Sea $X \subseteq U$. Entonces, un conjunto $Y \subseteq U$ es inductivo en X bajo F sii $X \subseteq Y$ y Y es cerrado bajo F.*

De todos los conjuntos inductivos en X nos interesa uno en particular al que llamaremos la *cerradura inductiva*. Existen dos métodos para definirla.

Cerradura inductiva

Sea $X \subseteq U$ y sea $F = \{f_i^n : U^n \to U\}$ un conjunto de funciones.

Definición

La cerradura inductiva de X bajo F, construida de abajo hacia arriba, es:

$$\begin{aligned} X_0 &= X \\ X_{i+1} &= X_i \cup \{f_k^n(x_1, \ldots, x_n) \mid f_k^n \in F \wedge x_1, \ldots, x_n \in X_i\} \\ X_+ &= \bigcup_{i \in \mathbb{N}} X_i. \end{aligned}$$

Sea $\mathcal{X}$ la familia de conjuntos inductivos en X bajo F. La cerradura inductiva de X bajo F, construida de arriba hacia abajo es el conjunto

$$X^+ = \bigcap_{Y \in \mathcal{X}} Y.$$

Equivalencia

Teorema

Ambas definiciones son equivalentes, es decir $X_+ = X^+$.

Demostración. Es claro que X_+ es inductivo en X y, dado que X^+ es la intersección de los conjuntos inductivos en X, se tiene que $X^+ \subseteq X_+$. La otra contención se demostrará por inducción matemática:

- Caso base. $X_0 = X \subseteq X^+$.
- Hipótesis inductiva. $X_i \subseteq X^+$.
- Por demostrar que $X_{i+1} \subseteq X^+$. Pero esto último se sigue del hecho de que X^+ es cerrado. Por inducción, $\forall n \in \mathbb{N}\,.\, X_n \subseteq X^+$. Entonces $X_+ \subseteq X^+$. □

Ejemplo 1

El cálculo de proposiciones se puede ahora construir de la siguiente forma. Sea $\Sigma = \{p, q, r, p_1, \ldots\} \cup \{(,)\} \cup \{\vee, \neg\}$ un alfabeto y sea $\neg_S : \Sigma^* \to \Sigma^*$ y $\vee_S : \Sigma^* \times \Sigma^* \to \Sigma^*$ las funciones definidas de la siguiente forma:

$$\begin{aligned} \neg_S(\alpha) &= \neg\alpha \\ \vee_S(\alpha, \beta) &= (\alpha \vee \beta). \end{aligned}$$

Sea $P_a = \{p, q, r, p_1, \ldots\}$ el conjunto básico. El conjunto fórmulas del cálculo de proposiciones, P, se puede definir usando los dos métodos:

$$\begin{aligned} P_0 &= P_a \\ P &= P_+ = P^+ \\ P^+ &= \bigcap_{Y \in \mathcal{P}} Y, \end{aligned}$$

donde $\mathcal{P}$ es la familia de conjuntos inductivos en P_a.

Ejemplo 2 I

Los conjuntos definidos por medio de la notación Backus-Naur se pueden transformar en conjuntos inductivos.
Las expresiones aritméticas del conjunto *EA* se definen así:

$$A ::= N \mid X \mid A + A \mid A \times A \mid A - A$$

donde $A \in EA$ y N es un entero ($\mathbb{Z}$) y X una localidad (Loc). Estos dos conjuntos se pueden definir inductivamente:

$$N ::= 0 \mid \text{suc}(N) \mid \text{pred}(N),$$

con suc y pred las funciones de sucesor y predecesor, respectivamente. Las localicades se definirán así:

$$\text{Loc} ::= X \mid Y \mid Z \mid X_N \mid Y_N \mid Z_N$$

Ejemplo 2 II

con $N \in \mathbb{Z}$.
Este último conjunto *no* es inductivo en realidad (su construcción se realiza en un solo paso).
Para EA, se comienza con un conjunto básico: $EA_0 = \mathbb{Z} \cup \text{Loc}$ y un conjunto de funciones:

$$\begin{aligned} +_S(\alpha, \beta) &= \alpha + \beta \\ \times_S(\alpha, \beta) &= \alpha \times \beta \\ -_S(\alpha, \beta) &= \alpha - \beta. \end{aligned}$$

y se obtienen así las expresiones aritméticas $EA = EA_+ = EA^+$.

Relaciones binarias

Si dos elementos a, b de un conjunto están en una relación R se escribirá $(a, b) \in R$, $a\ R\ b$ o $R(a, b)$.

Definición

Sea A un conjunto y sea $R \subseteq A \times A$. Se dice que R es:

1. Reflexiva *sii* $\forall a \in A\ .\ R(a, a)$.
2. Simétrica *sii* $\forall a, b \in A\ .\ R(a, b) \Rightarrow R(b, a)$.
3. Antisimétrica *sii* $\forall a, b \in A\ .\ R(a, b) \wedge R(b, a) \Rightarrow a = b$.
4. Transitiva *sii* $\forall a, b, c \in A\ .\ R(a, b) \wedge R(b, c) \Rightarrow R(a, c)$.
5. Total *sii* $\forall a, b \in A\ .\ a \neq b \Rightarrow R(a, b) \vee R(b, a)$.

Cerraduras reflexivas y transitivas

Dada una relación R en $A \times A$ se puede construir sus cerraduras transitiva y reflexiva y transitiva, denotadas por R^+ y R^*, respectivamente:

$$\begin{aligned} R^0 &= \{(a, a) \mid a \in A\} \\ R^1 &= R \\ R^{n+1} &= R^n \cup \{(a, c) \mid \exists b\ .\ (a, b) \in R^n \wedge (b, c) \in R^n\} \\ R^+ &= \bigcup_{n \in \mathbb{N}} R^{n+1} \\ R^* &= \bigcup_{n \in \mathbb{N}} R^n \end{aligned}$$

Órdenes

En matemáticas hay un tipo de relaciones muy comunes llamadas órdenes. Sin embargo, los órdenes vienen en distintos sabores.

Definición

- *Una relación R es un* pre-orden *(o cuasi orden) sii es reflexiva y transitiva.*
- *Un* orden parcial *(o poset, por el inglés partially ordered set) es una relación reflexiva, transitiva y antisimétrica.*
- *Un* orden total *o* lineal *es simplemente una relación total. Obsérvese cómo no se supone que tenga ninguna otra propiedad.*

Ejemplos

- El orden parcial más conocido es $\leq$ en $\mathbb{N}$.
- En el mismo conjunto, $<$ es un orden total.
- Un ejemplo de pre-orden en $\mathcal{P}(\mathbb{N})$ es *el preorden inferior o de Hoare*:

$$A \sqsubseteq_L B \qquad \text{sii} \qquad \forall a \in A \,.\, \exists b \in B \,.\, a \leq b,$$

Se tiene que $\{0,1,2\} \sqsubseteq_L \{1,2\}$ y $\{1,2\} \sqsubseteq_L \{0,1,2\}$ pero $\{0,1,2\} \neq \{1,2\}$.

Se usarán con frecuencia los símbolos $\prec$ y $\succ$ para denotar relaciones de orden arbitrarias.

Órdenes en n-adas

Una relación de orden en un conjunto A se puede extender a A^n al menos de dos formas:

1. Orden lexicográfico. Sea $\prec \subseteq A \times A$ un orden. La relación $\prec_{lex} \subseteq (A \times A) \times (A \times A)$ se define así:

$$(a,b) \prec_{lex} (a',b') \qquad \text{sii} \qquad \begin{array}{l} a \prec a' \quad \text{o} \\ a = a' \quad \text{y} \quad b \prec b'. \end{array}$$

   La definición anterior se extiende a A^n de la misma forma en que se extiende el concepto de par ordenado a n-adas arbitrarias.
2. Orden por coordenadas. $\prec_{coor}$ es la siguiente relación:

$$(a,b) \prec_{coor} (a',b') \qquad \text{sii} \qquad a \prec a' \quad \text{y} \quad b \prec b',$$

   que se extiende del mismo modo a n-adas arbitrarias.

Mínimos, máximos, etc.

Conviene dar nombre a algunos elementos especiales de un conjunto ordenado:

Definición

Sea $\prec$ una relación en $A \times A$ y sea $X \subseteq A$. Se dice que $x \in X$ es un:

1. mínimo *sii* $\forall y \in X \,.\, x \neq y \Rightarrow x \prec y$.
2. máximo *sii* $\forall y \in X \,.\, x \neq y \Rightarrow y \prec x$.
3. minimal *sii* $\neg\exists y \in X \,.\, x \neq y \wedge y \prec x$.
4. maximal *sii* $\neg\exists y \in X \,.\, x \neq y \wedge x \prec y$.

Ejemplos

Sea $A = \{0,1,2\}$.

- Si se ordena $\mathcal{P}(A)$ con la relación $\subseteq$ entonces $\emptyset$ y A son el mínimo y el máximo de $\subseteq$.
- En cambio, $\mathcal{P}(A) - \{\emptyset\}$ no tiene mínimo, pero si tres minimales: $\{0\}$, $\{1\}$ y $\{2\}$.
- Por su parte, $\mathcal{P}(A) - \{A\}$ no tiene máximo, pero sí tres maximales:

$$\{0,1\}, \{0,2\} \text{ y } \{1,2\}.$$

Un caso extraño

- En un orden parcial, un mínimo es un minimal, pero esto no es necesariamente el caso en un preorden.
- Más adelante se verán otros órdenes en los que los mínimos son siempre minimales.

Cadenas

Definición

Sea $\prec$ un orden en $U \times U$ y sea $C \subseteq U$.

- *Decimos que C es una cadena sii $\forall x, y \in C$ es el caso que $x \prec y$ o $y \prec x$.*
- *Una cadena descendente infinita es una cadena C tal que $\forall x \in C$, $\exists y \in C$ tal que $y \prec x$.*
- *De manera dual, una cadena infinita ascendente C tiene la propiedad de que $\forall x \in C$, $\exists y \in C$ tal que $x \prec y$.*

Obsérvese cómo una cadena $C \subseteq X$ es un subconjunto de X que visto de manera aislada forma un orden total.

Órdenes bien fundados

Las cadenas descendentes nos permiten caracterizar los órdenes bien fundados.

Definición

Sea $\prec \subseteq U \times U$ una relación. Decimos que $\prec$ es un bien fundada sii no existen cadenas infinitas descendentes en U.

Ejemplo 1

- $<$ en $\mathbb{N}$.
  Si denotamos por $\prec_{suc}$ la relación inducida por suc : $\mathbb{N} \to \mathbb{N}$

  $$x \prec_{suc} y \qquad \text{sii} \qquad y = \text{suc}(x),$$

  esta relación también es bien fundada.
  Por cierto, a diferencia de $<$, $\prec_{suc}$ *no* es transitiva.

Ejemplo 2

- Relaciones entre cadenas de símbolos.
  - Un alfabeto es un conjunto no vacío finito Σ.
  - Una cadena α es un sucesión finita (posiblemente vacía) de símbolos de Σ.
  - La cadena vacía se representa con el símbolo ϵ.
  - El conjunto de cadenas es Σ^* y el de cadenas no vacías es Σ^+.
  - La relación $\prec_{pre}$ está determinada por la regla:

$$\alpha \prec_{pre} \beta \qquad \text{sii} \qquad \exists\gamma \,.\, \beta = \alpha\gamma \wedge \gamma \neq \epsilon.$$

Puede verificarse que $\prec_{pre}$ es un orden bien fundado y que su mínimo en Σ^* es ϵ.
Σ^+ no tiene mínimo sino varios minimales: los elementos de Σ.

Más sobre relaciones bien fundadas

Teorema

Sea $\prec$ una relación bien fundada. Entonces:

(a) *$\prec$ no es reflexiva ni simétrica;*
(b) *su cerradura transitiva es bien fundada;*
(c) *los órdenes lexicográfico y por coordenadas basados en $\prec$ son bien fundados;*
(d) *$\prec^*$ es un orden parcial.*

Demostración: (a) Si $\prec$ fuera reflexiva, entonces es muy fácil formar una cadena infinita descendente a partir de un solo elemento:

$$\cdots \prec a \prec a.$$

Del mismo modo, si $\prec$ fuera simétrica, basta con tomar dos elementos a y b tales que $a \prec b$:

$$\cdots \prec b \prec a \prec b,$$

para tener otra cadena infinita.
(b) Supongamos que la relación $\prec$ es bien fundada. Si tenemos una cadena

$$\cdots \prec^+ a_i \prec^+ \cdots \prec^+ a_0,$$

y suponemos que es descendente infinita, entonces para todo i existen $a_{i_0} = a_i, \ldots, a_{i_m} = a_{i+1}$ tales que

$$a_{i_m} \prec \cdots \prec a_i$$

es decir, la misma cadena de $\prec^+$ se puede transformar en una cadena de $\prec$, por lo que tenemos una cadena infinita descendente en $\prec$, lo cual es una contradicción.
(c) Sea C una cadena en $A \times A$ con el orden $\prec_{coor}$:

$$\cdots \prec_{coor} (a_1, b_1) \prec_{coor} (a_0, b_0).$$

Si esta cadena fuera infinita, sería posible construir dos cadenas infinitas en $\prec$

$$\cdots \prec b_1 \prec b_0 \qquad \text{y} \qquad \cdots \prec a_1 \prec a_0,$$

por lo que C no puede ser infinita descendente. En cuanto a $\prec_{lex}$, considérese la siguiente cadena descendente infinita:

$$\cdots \prec_{lex} (a_1, b_1) \prec_{lex} (a_0, b_0).$$

En consecuencia, es posible construir una cadena en $\prec$ usando el siguiente método: el primer elemento es a_0, el segundo es el primer a_i tal que $a_0 \neq a_i$.

Si no existe tal elemento, entonces, por la definición de $\prec_{lex}$ tenemos una cadena descendente infinita en $\prec$

$$\cdots \prec b_1 \prec b_0,$$

lo cual no es posible. Por otro lado, suponer que podemos encontrar un número infinito de diferentes a_i nos lleva a otra cadena infinita

$$\cdots \prec a_1 \prec a_0,$$

lo que tampoco es posible. Por lo tanto, $\prec_{lex}$ tampoco contiene cadenas infinitas descendentes.
(d) Es claro que la cerradura transitiva y reflexiva tiene dos de las propiedades de un orden parcial. La antisimetría viene del hecho de que si tenemos que $a \prec^* b$ y $b \prec^* a$ y no fuera el caso que $a = b$, se podría formar una cadena descendente infinita en $\prec$ siguiendo el método de (a).

Relaciones bien fundadas: la otra versión I

El teorema siguiente nos da una caracterización alternativa de las relaciones bien fundadas.

Teorema

Una relación $\prec$ es bien fundada en $A \times A$ sii todo $X \subseteq A$ $(X \neq \emptyset)$ tiene un minimal.

Demostración. Supongamos que $\prec$ es bien fundada y que $\emptyset \neq X \subseteq A$. Ahora bien, si X no tiene un elemento minimal, entonces

$$\forall m \in X \,.\, \exists b \in X \,.\, b \prec m.$$

Iterando este razonamiento, podemos construir una cadena descendente infinita de elementos en X, lo cual es una contradicción.

Relaciones bien fundadas: la otra versión II

Si ahora suponemos que todo subconjunto no vacío de A tiene un minimal y además tenemos una cadena descendente

$$\cdots \prec a_i \prec \cdots \prec a_0,$$

basta con que tomemos el conjunto de elementos en la cadena que por hipótesis debe de tener un elemento minimal y, en consecuencia, la cadena no puede descender infinitamente.

Principio de inducción

Sea P una propiedad de elementos de A y sea $\prec \subseteq A \times A$. La siguiente afirmación se conoce como el principio de inducción:

$$(\forall a \in A \,.\, P(a)) \Leftrightarrow (\forall a \in A \,.((\forall b \in A \,.\, b \prec a \Rightarrow P(b)) \Rightarrow P(a))).$$

Este principio se aplica en conjuntos donde $\prec$ es un orden bien fundado:

Teorema

Sea $\prec \subseteq A \times A$ una relación bien fundada y sea $P : A \to \{V, F\}$ un predicado. Entonces el principio de inducción vale.

Demostración del teorema del principio de inducción I

La implicación $\Rightarrow$ es inmediata.
Supongamos ahora, por reducción al absurdo, que

$$\exists a \in A. \neg P(a).$$

Sea $Q = \{a \in A \mid \neg P(a)\}$ y, dado que $\prec$ es bien fundada, entonces existe un elemento minimal m de Q.
Aquí hay dos opciones:

(i) $\exists b \in A \,.\, b \prec m$;

(ii) $\neg\exists b \in A \,.\, b \prec m$.

Demostración del teorema del principio de inducción II

En el primer caso,

$$b \prec m \Rightarrow P(b)$$

y, dada la hipótesis principal, tenemos $P(m)$, lo que contradice la suposición.
En el segundo, el enunciado

$$((\forall b \in A \,.\, b \prec a \Rightarrow P(b))$$

sería verdadero por vacuidad, y como $P(m)$ es falso, entonces todo el enunciado sería falso. Pero sabemos que no existiría $a \in A$ tal que $P(A)$ y, en consecuencia,

$$(\forall a \in A \,.\, P(a))$$

sería falso también, con lo que tendríamos la otra implicación.

Demostraciones por inducción

El principio de inducción nos da una estrategia para demostrar una propiedad P en un conjunto A con una relación bien fundada $\prec$;

1. Se demuestra que todos los elementos minimales cumplen P.
2. Se asume como hipótesis inductiva

$$\forall b \in A \,.\, b \prec a \Rightarrow P(b).$$

3. Se demuestra que entonces $P(a)$.

Más adelante habrá oportunidad de usar esta estrategia.

Definiciones de funciones

- Una forma muy común de definir funciones en conjuntos es por enumeración.
- Por ejemplo, la función identidad en el conjunto $\{1, 2\}$ se puede expresar como un conjunto de pares ordenados:

$$\{(1, 1), (2, 2)\}.$$

- No obstante, con conjuntos de gran tamaño esto es poco práctico.
- Cuando contamos con una regla que nos permite calcular el valor de una función en un elemento dado es mejor usar una ecuación:

$$f(x) = x^2$$

o varias ecuaciones

$$\begin{aligned} 0! &= 1 \\ (n+1)! &= n! \times (n+1) \end{aligned}$$

Funciones recursivas

- El último ejemplo ilustra además una posibilidad más: las definiciones recursivas, donde la función definida aparece no del lado izquierdo *y* del lado derecho de la ecuación.
- Sin embargo, es muy fácil cometer "errores" en las definiciones recursivas:

$$g(x) = g(x+1)$$

  es una "función" que nunca nos da un resultado.
- Este ejemplo es muy obvio, pero en general no es posible decir si una función recursiva con dominio y contradominio en los naturales da siempre un resultado o no.
- Un problema adicional es cuando se puede obtener más de un resultado, dependiendo del orden en que se apliquen las ecuaciones que definen la función.

Ejemplos I

Supóngase que se desea evaluar las expresiones aritméticas *EA* tal y como se definieron en la sección anterior.

- Se partirá de una asignación de valores a las localidades por medio de una función $e : \text{Loc} \to \mathbb{Z}$, es decir, se supondrá que para toda $X \in \text{Loc}$, $e(X)$ ya está dado.
- También se tendrá que $e(n) = n$, para todo $n \in \mathbb{Z}$. Ahora hay que extender e al conjunto de elementos de *EA*:

$$\begin{aligned} e(X) &= m \quad \text{ya está dado } \forall X \in \text{Loc} \\ e(n) &= n \quad \forall n \in \mathbb{Z} \\ e(\alpha + \beta) &= e(\alpha) +_{\mathbb{Z}} e(\beta) \\ e(\alpha \times \beta) &= e(\alpha) \times_{\mathbb{Z}} e(\beta) \\ e(\alpha - \beta) &= e(\alpha) -_{\mathbb{Z}} e(\beta) \end{aligned}$$

Ejemplos II

donde $+_{\mathbb{Z}}$, $\times_{\mathbb{Z}}$ y $-_{\mathbb{Z}}$ son las operaciones de suma, multiplicación y resta en los enteros y no los símbolos sintácticos respectivos.

Con estas ecuaciones, queremos evaluar la expresión

$$2 + 3 \times 2.$$

Como las ecuaciones no establecen ningún orden especial para la evaluación de las expresiones, existen dos posibilidades:

$$\begin{aligned} e(2 + 3 \times 2) &= e(2) +_{\mathbb{Z}} e(3 \times 2) = 2 +_{\mathbb{Z}} (e(3) \times_{\mathbb{Z}} e(2)) \\ &= 2 +_{\mathbb{Z}} (3 \times_{\mathbb{Z}} 2) = 2 +_{\mathbb{Z}} 6 = 8 \end{aligned}$$

y también

$$\begin{aligned} e(2 + 3 \times 2) &= e(2 + 3) \times_{\mathbb{Z}} e(2) = (e(2) +_{\mathbb{Z}} e(3)) \times_{\mathbb{Z}} 2 \\ &= (2 +_{\mathbb{Z}} 3) \times_{\mathbb{Z}} 2 = 5 \times_{\mathbb{Z}} 2 = 10 \end{aligned}$$

Definiciones correctas

- Aunque no hay condiciones necesarias para saber si una función recursiva está bien definida, la definición 3.1 y el teorema 3.2 nos dan condiciones suficientes.
- El concepto clave es la generación libre de un conjunto inductivo.

Generación libre

Definición

Sean A un conjunto, $X \subseteq A$ y $F = \{f_i^n : A^n \to A\}$ un conjunto de funciones. Se dice que X_+ (o X^+) es generado libremente por X y F sii se cumplen las siguientes condiciones:

(i) *La restricción de toda $f^n \in F$ a X_+^n es inyectiva.*

(ii) *Para todas f_k^m y $f_i^n \in F$, si $f_k^m \neq f_i^n$ entonces $f_k^m(X_+) \cap f_i^n(X_+) = \emptyset$.*

(iii) *Los elementos de X son realmente básicos, es decir, para toda $f_i^n \in F$ y para todas $x_1, \ldots, x_n \in X_+$, se tiene que $f_i^n(x_1, \ldots, x_n) \notin X$.*

Ejemplos I

En el caso de *EA*, el conjunto no se generó libremente, pues no se cumple con la condición (ii). Por ejemplo, la expresión $2 + 3 \times 2$ se puede generar de dos maneras, a saber, $+_S(2, 3 \times 2)$ y $\times_S(2 + 3, \times 2)$, por lo que las imágenes de $+_S$ y $\times_S$ no son ajenas. Este problema es muy común cuando se trata de evaluar operaciones con más de un argumento. La solución más general consiste en encerrar entre paréntesis las expresiones generadas por las funciones de tal forma que se impone un orden de evaluación. De esta manera, se redefinen las funciones para expresiones aritméticas:

$$\begin{aligned} +_S(\alpha, \beta) &= (\alpha + \beta) \\ \times_S(\alpha, \beta) &= (\alpha \times \beta) \\ -_S(\alpha, \beta) &= (\alpha - \beta) \end{aligned}$$

y la ambigüedad desaparece. Se deja como ejercicio para el lector que la nueva definición cumple con las condiciones (i)–(iii) de la definición 3.1.

Ejemplos II

En cuanto a las listas, la definición que se dio no cumple ni con (i) ni con (ii):

$$\begin{aligned} l{+\!+}[\,] &= [\,]{+\!+}l = l \\ 0 :: [\,] &= [\,]{+\!+}[0] \end{aligned}$$

Aquí el problema es la función ++. Una nueva definición de listas en la que la única función constructora es :: resuelve el problema (y el lector puede verificarlo en un ejercicio fácil).

Generación libre y homomorfismos

Este teorema permite definir funciones recursivas en conjuntos generados libre e inductivamente:

Teorema

Sea X_+ un conjunto generado libremente por X y el conjunto de funciones F y sea $B \neq \emptyset$ un conjunto cualquiera acompañado por un conjunto de funciones $G = \{g_i^n : B^n \to B\}$.
Sea $\delta : F \to G$ una función tal que $\delta(f_i^n) = g_i^m$ implica que $n = m$.
Finalmente, sea $h : X \to B$ una función. Entonces, existe una única $\hat{h} : X_+ \to B$ tal que:

(i) *Para todo $x \in X$. $\hat{h}(x) = h(x)$*

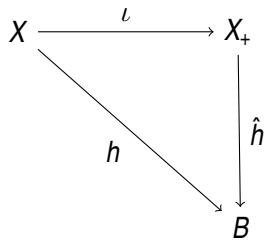
(ii) *Para toda $f_k^n \in F$ y para todas $x_1, \ldots, x_n \in X_+$ se tiene que*

$$\hat{h}(f_i^n(x_1, \ldots, x_n)) = g_k^m(\hat{h}(x_1), \ldots, \hat{h}(x_n)),$$

donde $\delta(f_i^n) = g_k^m$

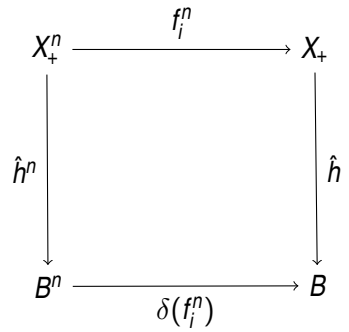
Versión diagramática I

- En álgebra, una función como $\hat{h}$ se conoce como un *homomorfismo*.
- Los homomorfismos se pueden explicar por medio de *diagramas conmutativos*.
- Sea $\iota : X \to X_+$ la función inclusión (*i.e.*, $\forall x \in X \,.\, \iota(x) = x$). Entonces, según la cláusula (i):



Versión diagramática II

En pocas palabras, para llegar al vértice marcado con B partiendo del vértice X se puede ir directamente a través de h o indirectamente a través de i, primero, y $\hat{h}$, después, y el resultado será el mismo.
La cláusula (ii) del teorema dice, a su vez:



Un lema útil I

Antes de demostrar el teorema anterior, veamos el siguiente lema.

Lema

Sea X_+ un conjunto generado libre e inductivamente por X y F. Para toda $f_k^n \in F$, si $x_1, \ldots, x_n \in X_i$, entonces $f_k^n(x_1, \ldots, x_n) \notin X_i$.

Demostración. Se aplicará inducción sobre i.
Caso base: $i = 0$. Por la condición (iii) de la definición, es verdad que $\forall f_k^n \in F$ y $x_1, \ldots, x_n \in X_0$ se tiene que $f_k^n(x_1, \ldots, x_n) \notin X_0$.
Hipótesis inductiva: $\forall f_k^n \in F,\ x_1, \ldots, x_n \in X_i \,.\, f_k^n(x_1, \ldots, x_n) \notin X_i$. Se debe demostrar que lo mismo vale en X_{i+1}. Para esto, hay que considerar una función f_k^n y elementos $x_1, \ldots, x_n \in X_{i+1} - X_i$ (pues si los elementos estuvieran también en X_i, quedarían cubiertos por la hipótesis inductiva).

Un lema útil II

Supóngase que $f_k^n(x_1, \ldots, x_n) = x$ y que $x \in X_{i+1}$. Entonces, por definición de X_{i+1}, hay dos opciones

(a) $x \in X_i$;
(b) existen $g_q^m \in F$ y $y_1, \ldots, y_m \in X_i$ tales que $x = g_q^m(y_1, \ldots, y_m)$.

La opción (a) es imposible, pues contradiría la hipótesis inductiva. Pero (b) contradiría la condición (i) de la definición si $f_k^n = g_q^m$ o la condición (ii) si $f_k^n \neq g_q^m$.
En cualquiera de los casos, no es posible que $x \in X_{i+1}$ y, por inducción matemática, esto vale para toda X_n. □

Demostración del teorema del homomorfismo único I

Con el lema 3.3 ya se puede demostrar el teorema 3.2:

Demostración de 3.2. Considérese la siguiente sucesión de funciones:

$$\begin{aligned} h_0 &= h \\ h_{i+1} &= h_i \cup \{(f_i^n(x_1,\ldots,x_n), g_k^n(h_i(x_1),\ldots,h_i(x_n))) \mid x_1,\ldots,x_n \in \mathrm{dom}(h_i)\} \\ \hat{h} &= \bigcup_{i\in\mathbb{N}} h_i \end{aligned}$$

Obsérvese primero que, dado que X_* es generado libremente, $\mathrm{dom}(h_i) \subseteq X_i$. Por otro lado, queremos demostrar que $\hat{h}$ es en realidad una función, es decir, si $(x,y) \in \hat{h}$ y $(x,z) \in \hat{h}$, entonces $y = z$. Lo haremos por inducción.
Caso base: $x \in X$. En este caso, como X_* es generado libremente, no existen $f_q^m \in F$ ni $x_1,\ldots,x_m \in X_*$ tales que $x = f_q^m(x_1,\ldots,x_n)$. Como

Demostración del teorema del homomorfismo único II

$h_0(x) = h(x)$ y no asignamos ningún nuevo valor a x en las futuras h_i ($i \geq 1$), entonces $\hat{h}(x)$ tiene una asignación única.
Hipótesis inductiva: $\forall m \leq i+1$ tenemos que si $x \in X_m$ y $(x,y) \in \hat{h}$ y $(x,z) \in \hat{h}$, entonces $y = z$. Sea ahora $x \in X_{i+1} - X_i$. Es decir, por las condiciones (i) y (ii) de 3.1, existen $x_1,\ldots,x_n \in X_i$ y $f_q^n \in F$ únicos tales que $f_q^n(x_1,\ldots,x_n) = x$. El lema 3.3 nos dice que $f_q^n(x_1,\ldots,x_n) \notin X_i$ y por esta razón, h_i no está definida en x. Entonces, tenemos que aplicar la definición de $\hat{h}$,

$$\begin{aligned} \hat{h}(x) &= y = g_k^n(h_i(x_1),\ldots,h_i(x_n)) \\ \hat{h}(x) &= z = g_k^n(h_i(x_1),\ldots,h_i(x_n)) \end{aligned}$$

Pero por hipótesis inductiva, $\hat{h}$ es una función en $x_1,\ldots,x_n$ y, por tanto, $y = z$. Es decir, $\hat{h}$ también es una función en $x \in X_{i+1}$ y, por inducción, lo es en todo X_*.

Demostración del teorema del homomorfismo único III

Finalmente, se verá la unicidad de $\hat{h}$. Supóngase que $\hat{h}' : X_* \to B$ cumple con las condiciones (i) y (ii) del teorema. Demostraremos por inducción en X_* que $\hat{h}$ y $\hat{h}'$ son iguales.
Caso base: sea $x \in X_0$. Por la condición (i), $\hat{h}(x) = h(x) = \hat{h}'(x)$.
Hipótesis inductiva: $\forall m \leq i+1$, tenemos que si $x \in X_m$, entonces $\hat{h}(x) = \hat{h}'(x)$. Sea $x \in X_{i+1} - X_i$, es decir, existen $x_1,\ldots,x_n \in X_i$ y $f_q^n \in F$ únicos tales que $f_q^n(x_1,\ldots,x_n) = x$. Sea $\delta(f_q^n) = g_k^n$. Por la condición (ii):

$$\begin{aligned} \hat{h}(x) &= = \hat{h}(f_q^n(x_1,\ldots,x_n)) = g_k^n(\hat{h}(x_1),\ldots,\hat{h}(x_n)) \\ \hat{h}'(x) &= = \hat{h}'(f_q^n(x_1,\ldots,x_n)) = g_k^n(\hat{h}(x_1),\ldots,\hat{h}(x_n)) \end{aligned}$$

y, por hipótesis inductiva, $\hat{h}(x_1) = \hat{h}'(x_1),\ldots,\hat{h}(x_n) = \hat{h}'(x_n)$. En consecuencia, $\hat{h}(x) = \hat{h}'(x)$ y, por inducción, $\hat{h} = \hat{h}'$. □

Funciones recursivas 2

Como se recordará, la función de evaluación de expresiones aritméticas $e : EA \to \mathbb{Z}$ no funcionó con la definición original de EA. Sin embargo, este último conjunto se redefinió de forma que era generado libremente por $\mathbb{Z} \cup \mathrm{Loc}$ y las nuevas funciones $+_S$, $\times_S$ y $-_S$, por lo que el teorema 3.2 permite asegurar que la función de evaluación siguiente está bien definida:

$$\begin{aligned} \hat{e}(n) &= n \qquad \forall n \in \mathbb{Z} \\ \hat{e}(X) &= e(X) \qquad \forall x \in \mathrm{Loc} \\ \hat{e}((\alpha+\beta)) &= \hat{e}(\alpha) +_{\mathbb{Z}} \hat{e}(\beta) \\ \hat{e}((\alpha\times\beta)) &= \hat{e}(\alpha) \times_{\mathbb{Z}} \hat{e}(\beta) \\ \hat{e}((\alpha-\beta)) &= \hat{e}(\alpha) -_{\mathbb{Z}} \hat{e}(\beta) \end{aligned}$$

Más ejemplos

En cuanto a las listas de enteros generadas libremente por ::, también se pueden definir funciones recursivas de manera natural. Por ejemplo, se tiene la función long : $L(\mathbb{N}) \to \mathbb{N}$:

$$\begin{aligned} \text{long}([\,]) &= 0 \\ \text{long}(n :: l) &= 1 + \text{long}(l) \end{aligned}$$

Orden estructural

La generación libre también nos da un orden natural para estos conjuntos, como se muestra en la siguiente definición.

Definición

Sea X_+ un conjunto generado libre e inductivamente por el conjunto básico X y las funciones F y sean $\alpha, \beta \in X_+$. Entonces

$\alpha \prec_S \beta$ *sii* $\exists f_i^n \in F \wedge x_1, \ldots, x_{n-1} \in X_+ . \beta = f_i^n(x_1, \ldots, \alpha, x_{n-1})$.

$\prec_S$ se conoce como el orden sintáctico o estructural y es claramente una relación bien fundada. Por esta razón, se puede usar como base de un método de demostración llamado *inducción estructural*. Veamos un ejemplo.

Una aplicación I

Considérese nuevamente *EA*, con la nueva definición. A simple vista parece que toda expresión de *EA* tiene paréntesis balanceados, es decir, a un paréntesis que se abre corresponde siempre uno que se cierra. Esta conjetura se demostrará por inducción estructural. Sea $\alpha \in EA$
Caso base: $\alpha \in \mathbb{Z}$ o $\alpha \in$ Loc. Entonces, como las localidades y los enteros no incluyen paréntesis, la proposición es trivialmente cierta.
Hipótesis inductiva: α y β tienen paréntesis balanceados. Se debe demostrar ahora que $(\alpha + \beta)$, $(\alpha \times \beta)$ y $(\alpha - \beta)$ también tienen paréntesis balanceados, pues

$$\alpha, \beta \prec_S (\alpha + \beta), (\alpha \times \beta), (\alpha - \beta).$$

Supóngase que $(\alpha + \beta)$ tiene más paréntesis que se abren de los que se cierran. Dado que el primer paréntesis y el último de la expresión se cancelan mutuamente, entonces el problema debe estar en α o en β, lo que

Una aplicación II

contradice la hipótesis inductiva. Entonces, $(\alpha + \beta)$ tiene paréntesis balanceados. Con un razonamiento análogo se demuestran los casos de $(\alpha \times \beta)$ y $(\alpha - \beta)$. □