Computación Bio-inspirada

PRELIMINARES

David Orellana Martín
Mario de J. Pérez Jiménez

Dpto. Ciencias de la Computación e Inteligencia Artificial
E.T.S. Ingeniería Informática
Universidad de Sevilla

marper@us.es

http://www.cs.us.es/~marper/

Máster Universitario en Lógica, Computación e Inteligencia Artificial
Curso 2021-2022

Teoría de Zermelo-Fraenkel

Teoría intuitiva de conjuntos: G. Cantor (desarrollada entre 1873 y 1896).

Aparición de paradojas en la teoría de Cantor:

* C. Burali-Forti (1897): afectaba al conjunto de los ordinales.
* B. Russell (1901): afectaba a la relación de pertenencia.

Para resolver este escollo, algunos matemáticos optaron por la axiomatización.

* E. Zermelo (1908): Primer sistema de axiomas de la teoría de conjuntos.
* A. Fraenkel (1922): Complementa y "precisa" el sistema axiomático de Zermelo (en esa tarea, Th. Skolem realizó importantes contribuciones).

Teoría de Zermelo-Fraenkel

Los objetos matemáticos de esta teoría son **conjuntos**.

Conceptos primitivos o indefinibles en la teoría:

* Concepto de **conjunto**.
* Concepto de **pertenencia** ($a \in b$: el conjunto a es un elemento del conjunto b).

Sean a y b conjuntos. Notaremos $\mathbf{a} \notin \mathbf{b}$ para indicar que a **no es un elemento** de b

Fórmula $\theta(x)$ sobre un conjunto a:

- Si $b \in a$, entonces $\theta(b)$ es una proposición (verdadera o falsa).
- $\{x \mid \theta(x)\}$: conjunto cuyos elementos son los conjuntos x tales que la proposición $\theta(x)$ es verdadera.

Abreviaremos la expresión “ **si y sólo si** ” escribiendo “ **sii** ”.

Teoría de Zermelo-Fraenkel

Algunos axiomas de la teoría de Z-F que destacamos:

Axioma de extensionalidad: dos conjuntos a y b son iguales ($a = b$) **sii** poseen los mismos elementos: $\forall x\,(x \in a \longleftrightarrow x \in b)$.
Si los conjuntos a y b **no son iguales** entonces se notará $a \neq b$.

Axioma del conjunto vacío: existe un conjunto que carece de elementos (se denotará por $\emptyset$ y se denomina **conjunto vacío**),

Axioma del par no ordenado: para cada par de conjuntos a y b existe un conjunto c cuyos únicos elementos son a y b. Se notará $c = \{a, b\}$

- ⋆ El **par ordenado**, de primera componente el conjunto a y segunda componente el conjunto b, notaremos (a, b), es el conjunto $\{\{a\}, \{a, b\}\}$.
- ⋆ Dados los conjuntos a, b, c y d se tiene que $(a, b) = (c, d)$ **sii** $a = c$ y $b = d$.

Teoría de Zermelo-Fraenkel

Axioma de la unión: dado un conjunto a, existe un conjunto (que se notará $\bigcup \mathbf{a}$) cuyos elementos son, exactamente, los elementos de los conjuntos que son elementos de a. Es decir, $\bigcup \mathbf{a} = \{x \mid \exists y\,(y \in a \wedge x \in y\}$.
En el caso particular $a = \{b, c\}$, el conjunto $\bigcup \mathbf{a}$ se notará $\mathbf{b} \cup \mathbf{c}$. Por tanto, se verificará que $\mathbf{b} \cup \mathbf{c} = \{x \mid x \in b \vee x \in c\}$.

Axioma del conjunto de partes: para cada conjunto a existe un conjunto $\mathcal{P}(a)$ cuyos elementos son todos los <u>subconjuntos</u> de a.

- ⋆ Se dice que un conjunto b es un **subconjunto** de a (y se notará $\mathbf{b} \subseteq \mathbf{a}$) si se verifica que $\forall x\,(x \in b \rightarrow x \in a)$.
- ⋆ Se dice que un conjunto b es un **subconjunto estricto** (o propio) de a (y se notará $\mathbf{b} \subsetneq \mathbf{a}$) si se verifica que $b \subseteq a$ y $b \neq a$.

Axioma del infinito: existe un conjunto $\mathbb{N}$ (denominado **conjunto de los números naturales**) tal que: (a) $\emptyset \in \mathbb{N}$; y (b) $\forall x\,(x \in \mathbb{N} \rightarrow x \cup \{x\} \in \mathbb{N})$.

El conjunto de los números naturales

Existencia del **conjunto de los números naturales** (axioma del infinito).

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, ...\}$$

El conjunto $\mathbb{N}$ se puede describir, de **manera recursiva**, como sigue:

- ⋆ 0 es el conjunto vacío.
- ⋆ Para cada número natural n se tiene que $n + 1 = n \cup \{n\}$.

Es decir:

- ⋆ $0 \stackrel{def}{=} \emptyset$.
- ⋆ $1 \stackrel{def}{=} 0 \cup \{0\} = \{0\}$.
- ⋆ $2 \stackrel{def}{=} 1 \cup \{1\} = \{0, 1\}$.
- ⋆ $3 \stackrel{def}{=} 2 \cup \{2\} = \{0, 1, 2\}$.
- ⋆ ....

Qué son los números naturales

Los números naturales son los siguientes

- 0 **es el conjunto vacío**.
- Para cada número natural $n \neq 0$ se tiene que:
    - n es **un** conjunto.
    - n es **un** conjunto que consta, exactamente, de n elementos.
    - n es **el conjunto** cuyos elementos son, exactamente: $0, 1, \dots n-1$; es decir: $n = \{0, 1, \dots n-1\}$.

RGNC

Tuplas ordenadas

Par ordenado (a, b): también se denomina 2-tupla ordenada.

A partir de aquí, se define, **manera recursiva**, las n-tuplas ordenadas, para cada $n \geq 3$, como sigue:

- ⋆ $(x_1, x_2, x_3) \stackrel{def}{=} (x_1, (x_2, x_3))$.
- ⋆ $(x_1, x_2, x_3, x_4) \stackrel{def}{=} (x_1, (x_2, x_3, x_4))$.
- ⋆ $(x_1, x_2, x_3, x_4, x_5) \stackrel{def}{=} (x_1, (x_2, x_3, x_4, x_5))$.
- ⋆ ....

En general: $(x_1, x_2, \ldots, x_n) \stackrel{def}{=} (x_1, (x_2, \ldots, x_n))$, para cada $n \geq 3$.

Así se tiene el concepto de n-tupla ordenada $(x_1, \ldots, x_n)$, para cada $n \geq 2$.

Operaciones con conjuntos

Sean a y b dos conjuntos arbitrarios:

- ⋆ **Unión**: $a \cup b = \{x \mid x \in a \vee x \in b\}$
- ⋆ **Intersección**: $a \cap b = \{x \mid x \in a \wedge x \in b\}$
  - ∗ Dos conjuntos a y b se dicen que son **disjuntos sii** $a \cap b = \emptyset$.
- ⋆ **Diferencia**: $a \setminus b = \{x \mid x \in a \wedge x \notin b\}$
- ⋆ **Complementario**: Si $b \subseteq a$, el complementario de b en a es $a \setminus b$.
- ⋆ **Conjunto de las partes** de a: $\mathcal{P}(a) = \{x \mid x \subseteq a\}$.
- ⋆ **Producto cartesiano** de a y b (¡en ese orden!):

$$a \times b = \{(x_1, x_2) \mid x_1 \in a \wedge x_2 \in b\}$$

Para cada número natural $n \geq 2$, si $a_1, \ldots, a_n$ son conjuntos entonces se define $a_1 \times \ldots \times a_n = \{(x_1, \ldots, x_n) \mid x_1 \in a_1 \wedge \ldots \wedge x_n \in a_n\}$.

Se define $a^1 = a$ y $a^n = a \times \overset{(n)}{\ldots} \times a$, para cada número natural $n \geq 2$.

Funciones

- ⋆ Una **relación** es un conjunto de **pares ordenados**.
- ⋆ Una **función** f es una relación tal que
$$\forall x \forall y \forall z \,(\,(x,y) \in f \wedge (x,z) \in f \implies y = z\,)$$
- ⋆ Una **función** f es **inyectiva** si satisface la siguiente condición:
$$\forall x \forall y \forall z \,(\,(x,y) \in f \wedge (z,y) \in f \implies x = z\,)$$
- ⋆ El **dominio** de una función f es el conjunto:
$$dom(f) = \{x \mid \exists y\,((x,y) \in f)\}$$
- ⋆ El **rango** de f es el conjunto:
$$rang(f) = \{x \mid \exists y\,((y,x) \in f)\}$$
- ⋆ Si f es una función y $a \in dom(f)$, entonces existe un único $b \in rang(f)$ tal que $(a,b) \in f$. Notaremos $f(a) = b$ para expresar que $(a,b) \in f$.
- ⋆ Si $x \in dom(f)$, notaremos $f(x)\downarrow$ (f está definida en x).
- ⋆ Si $x \notin dom(f)$, notaremos $f(x)\uparrow$ (f no está definida en x).
- ⋆ $[f = g] \iff [\mathrm{dom}(f) = \mathrm{dom}(g) \wedge \forall x \in dom(f)\ (f(x) = g(x))]$.

Tipos de funciones

Sean A y B dos conjuntos.

⋆ Una **función total** f de A en B (notaremos $f : A \longrightarrow B$) es una función que verifica: $dom(f) = A$ y $rang(f) \subseteq B$.

- Una **aplicación** f de A en B es una función total f de A en B.

⋆ Una **función parcial** f de A en B (notaremos $f : A - \rightarrow B$) es una función que verifica: $dom(f) \subseteq A$ y $rang(f) \subseteq B$.

- Toda función total de A en B es una función parcial de A en B.
- Existen funciones parciales de A en B que no son funciones totales de A en B (por ejemplo: la función f de $\mathbb{N}$ en $\mathbb{N}$ definida por $f(x) =$ raíz cuadrada de x. Se tiene que $f(10) \uparrow$).

⋆ Una función parcial f de A en B es:

- **sobreyectiva** (o suprayectiva) si $rang(f) = B$.
- **biyectiva** si es total, inyectiva y sobreyectiva.

Si A un conjunto, la **función identidad** sobre A es la función $Id_A : A \rightarrow A$, definida por $Id_A(x) = x$.

Composición de funciones

Sean $f : A \dashrightarrow B$ y $g : B \dashrightarrow C$. La **composición** de f y g (¡en ese orden!) es la función parcial h de A en C definida así:

$$h = \{(x, y) \in A \times C : \ \exists z \in B\,(\, f(x) = z \ \wedge \ g(z) = y\}$$

Gráficamente,

$$\begin{array}{ccccccc} A & \overset{f}{\dashrightarrow} & B & \overset{g}{\dashrightarrow} & C & & \\ x & \mapsto & f(x) & \mapsto & g(f(x)) & & (= h(x)) \end{array}$$

Notación: $h = g \circ f$.

Función inversa

Si f es una **función** entonces se define el **conjunto** $f^{-1} = \{(x, y) \mid (y, x) \in f\}$.

- ⋆ El conjunto f^{-1} **no tiene por qué** ser una función.
- ⋆ f^{-1} es una función **sii** f es inyectiva (**función inversa** de f). Además, en este caso se tiene que $(f^{-1})^{-1} = f$.

Proposición: Sea f una función total de A en B.

- f^{-1} es una aplicación de B en A **sii** f es biyectiva.
- Si f es biyectiva, entonces $f \circ f^{-1} = Id_B$ y $f^{-1} \circ f = Id_A$.

Imagen directa e imagen inversa por una función

Sea f una función parcial de un conjunto A en un conjunto B.

- ⋆ Si $C \subseteq A$ entonces la **imagen directa** de C por f es el conjunto
  $$f[C] = \{y \in B \mid \text{Existe } x \in dom(f) \cap C \text{ tal que } f(x) = y\}$$
- ⋆ Si $D \subseteq B$ entonces la **imagen inversa** de D por f es el conjunto
  $$f^{-1}[D] = \{x \in A \mid x \in dom(f) \text{ y } f(x) \in D\}$$

Familia de conjuntos

Sea I un conjunto no vacío.

- ⋆ Una **familia de conjuntos, con conjunto de índices I**, es una función F cuyo dominio es I (los elementos de I se denominan **índices** de la familia).
  - ∗ La familia F se representará así: $\{F(i) \mid i \in I\}$.
  - ∗ Si $I = \{1, \dots, n\}$, con $n \in \mathbb{N} \setminus \{0\}$, entonces la familia F se representará así: $\{F(1), \dots, F(n)\}$.
- ⋆ Sea F una familia de conjuntos, con conjunto de índices I.
  - ∗ La **unión** de los conjuntos de la familia F, que se notará $\bigcup_{i \in I} F(i)$, es el conjunto $\{x \mid \exists i\, (i \in I \wedge x \in F(i))\}$.
  - ∗ La **intersección** de los conjuntos de la familia F, que se notará $\bigcap_{i \in I} F(i)$, es el conjunto $\{x \mid \forall i\, (i \in I \rightarrow x \in F(i))\}$.

Familia de conjuntos

Sea F una familia de conjuntos, con conjunto de índices $I \neq \emptyset$.

- ⋆ Se dice que F es una **familia de conjuntos disjuntos dos a dos** si satisface la siguiente propiedad:
  - ∗ Para cada $i, j \in I$ tales que $i \neq j$, se tiene que los conjuntos $F(i)$ y $F(j)$ de la famila, son disjuntos.
- ⋆ Se dice que F es un **recubrimiento de un conjunto A** si satisface la siguiente propiedad: $A \subseteq \bigcup_{i \in I} F(i)$.
- ⋆ Se dice que F es una **partición de un conjunto A** si satisface:
  - ∗ F es una familia de subconjuntos de A.
  - ∗ F es un recubrimiento de A.
  - ∗ F es una familia de conjuntos disjuntos dos a dos.

Sucesiones de elementos de un conjunto

Sucesión finita de elementos de un conjunto A: es una aplicación de un número natural $n \in \mathbb{N}$ en el conjunto A.

- ⋆ El número natural n se denomina **longitud** de la sucesión.
- ⋆ La sucesión finita de longitud 0 será la función vacía.
- ⋆ Una sucesión finita, f, de longitud $n+1$ se representará así: $f(0)\, f(1) \dots f(n)$.

Toda sucesión finita de elementos de un conjunto A, de longitud $n \in \mathbb{N}$, es una familia de conjuntos (que son elementos de A), cuyo conjunto de índice es n.

Sucesión infinita de elementos de un conjunto A: es una aplicación del conjunto $\mathbb{N}$ de los números naturales en el conjunto A.

- ⋆ Una sucesión infinita, f, se representará así: $f(0)\, f(1) \dots$.

Toda sucesión infinita de elementos de un conjunto A es una familia de conjuntos (que son elementos de A), cuyo conjunto de índice es $\mathbb{N}$.

Conjuntos infinitos

Un conjunto A es **infinito sii** existe un subconjunto estricto B de A tal que es **equipotente** a A (es decir, existe una aplicación biyectiva de B en A).

- ⋆ El conjunto $\mathbb{N}$ es infinito: existe una biyección entre dicho conjunto y el subconjunto de los números pares.

Un conjunto A es **numerable sii** existe una aplicación biyectiva de $\mathbb{N}$ en A.

Ejemplos:

- ⋆ El conjunto $\mathbb{N}^2$ es numerable: se prueba que la función $J : \mathbb{N}^2 \to \mathbb{N}$ definida por $J(x, y) = \frac{(x+y)(x+y+1)}{2} + x$ es **biyectiva**.
- ⋆ Para cada $k \geq 2$, el conjunto $\mathbb{N}^k$ es numerable.
- ⋆ El conjunto $\mathbb{Q}$ de los números racionales es numerable.
- ⋆ El conjunto $\mathbb{R}$ de los números reales **no** es numerable.
- ⋆ El intervalo $[0, 1) \subseteq \mathbb{R}$ **no** es numerable.
- ⋆ $\mathcal{P}(\mathbb{N})$ **no** es numerable.

Método diagonal de Cantor: $\mathcal{P}(\mathbb{N})$ no es numerable

Caso contrario, $\mathcal{P}(\mathbb{N}) = \{A_0, A_1, A_2, \dots, A_n, \dots\}$.

- ⋆ Cada subconjunto B de $\mathbb{N}$ se puede identificar con una sucesión infinita compuesta de SÍES y NOES:

	0	1	2	...	n	...
B	SÍ	NO	NO	...	SÍ	...

En la posición j–ésima aparece SÍ cuando $j \in B$ y NO en caso contrario.

- ⋆ Formemos una tabla infinita con la información de los conjuntos A_j (de acuerdo con el criterio anterior). .

	0	1	2	..	n	..
A_0	SÍ	no	no	..	no	..
A_1	no	NO	sí	..	sí	..
A_2	sí	sí	NO	..	no	..
⋮	⋮	⋮	⋮	..	⋮	..
A_n	no	sí	no	..	SÍ	..
⋮	⋮	⋮	⋮	..	⋮	..

- ⋆ El conjunto $D \subseteq \mathbb{N}$ definido como sigue a través de la diagonal de la tabla (permutando SÍ y NO, entre sí)

	0	1	2	...	n	...
	NO	–	–	...	–	...
	–	SÍ	–	...	–	...
D	–	–	SÍ	...	–	...
	–	–	–	...	–	...
	–	–	–	...	NO	...
	–	–	–	...	–	...

Entonces $D \in \mathcal{P}(\mathbb{N})$ y D es un conjunto distinto de $A_0, A_1, A_2, \dots, A_n, \dots$. Lo que es una **contradicción**.

Método diagonal de Cantor: $[0,1)$ no es numerable

Recuérdese que $[0,1) = \{x \in \mathbb{R} : \ 0 \leq x < 1\}$

Veamos ahora que

- ⋆ Cada número real $x \in [0,1)$ se puede escribir en base 10 como: $0'a_0\, a_1\, a_2\, \dots$, en donde cada $a_k \in \{0,1,2,\dots,9\}$. Por tanto podemos identificar x con la sucesión $(a_0,\ a_1,\ a_2,\ \dots,a_n,\ \dots)$
- ⋆ Si el conjunto $[0,1)$ fuese numerable, entonces $[0,1) = \{x_0, x_1, x_2, \dots\}$. Ahora bien, cada x_j tendría una expresión decimal: $0'a_{j,0}\, a_{j,1}\, a_{j,2}\, \dots$.
- ⋆ Formemos una tabla infinita con las expresiones decimales de los x_j:

x_0	$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	..	$a_{0,n}$	..
x_1	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	..	$a_{1,n}$	..
x_2	$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	..	$a_{2,n}$	..
$\vdots$	$\vdots$	$\vdots$	$\vdots$	..	$\vdots$	..
x_n	$a_{n,0}$	$a_{n,1}$	$a_{n,2}$	..	$a_{n,n}$	..
$\vdots$	$\vdots$	$\vdots$	$\vdots$	..	$\vdots$	..

- ⋆ Definamos ahora el número real $d = 0'd_0\, d_1\, d_2\, \dots,\ d_n\, \dots$, en donde $d_j = \begin{cases} 0 & \text{si } a_{j,j} \neq 0 \\ 1 & \text{si } a_{j,j} = 0 \end{cases}$
- ⋆ Entonces $d \in [0,1)$ y para todo $j \in \mathbb{N}$, $x_j \neq d$; es decir, $d \notin \{x_0, x_1, x_2, \dots\} = [0,1)$. Lo que es una **contradicción**.

Predicados

Sea A un conjunto. Si $(x_1, \ldots, x_n) \in A^n$, $n \neq 0$, entonces notaremos $\vec{x} \in A^n$.

Un **predicado** n–ario, $n \neq 0$, θ sobre A es una aplicación de A^n en $\{0, 1\}$.

- ⋆ Si $\theta(\vec{x}) = 1$ para $\vec{x} \in A^n$, diremos que el predicado θ <u>se verifica</u> para $\vec{x}$. Caso contrario, diremos que el predicado θ <u>no se verifica</u> para $\vec{x}$.
- ⋆ Todo predicado n–ario, θ, sobre A determina un subconjunto de A^n definido así: $S_\theta = \{\vec{x} \in A^n \mid \theta(\vec{x}) = 1\}$.
- ⋆ Todo subconjunto de $B \subseteq A^n$ determina un predicado n–ario θ_B sobre A tal que $\theta_B(\vec{x}) = 1$ **sii** $\vec{x} \in B$.

La **función característica** de $B \subseteq A^n$ es el siguiente predicado sobre A^n:

$$C_B(\vec{x}) = \begin{cases} 1 & si\ \vec{x} \in B \\ 0 & si\ \vec{x} \in A^n \setminus B \end{cases}$$

La función característica del subconjunto B es el predicado n-ario asociado a B.

Operaciones con predicados

Sean θ y θ' predicados n–arios, $n \neq 0$, sobre un conjunto A. Se definen los siguientes predicados n–arios sobre A:

* $(\neg\theta)(\vec{x}) = 1 - \theta(\vec{x})$. Se notará $\neg\theta(\vec{x})$ en lugar de $(\neg\theta)(\vec{x})$
* $(\theta \vee \theta')(\vec{x}) = \text{máx}\ \{\theta(\vec{x}), \theta'(\vec{x})\}$. Se notará $\theta(\vec{x}) \vee \theta'(\vec{x})$ en lugar de $(\theta \vee \theta')(\vec{x})$.
* $(\theta \wedge \theta')(\vec{x}) = \text{mín}\ \{\theta(\vec{x}), \theta'(\vec{x})\}$. Se notará $\theta(\vec{x}) \wedge \theta'(\vec{x})$ en lugar de $(\theta \wedge \theta')(\vec{x})$.
* $\theta \rightarrow \theta' \overset{def}{=} (\neg\theta) \vee \theta'$.
* $\theta \leftrightarrow \theta' \overset{def}{=} (\theta \rightarrow \theta') \wedge (\theta' \rightarrow \theta)$.

Se verifican las siguientes relaciones:

* $S_{\theta \vee \theta'} = S_\theta \cup S_{\theta'}$.
* $S_{\theta \wedge \theta'} = S_\theta \cap S_{\theta'}$.
* $S_{\neg\theta} = A^n \setminus S_\theta$.

Cuantificación acotada

Sea $\theta(x_1, \ldots, x_n, y)$ un predicado $(n+1)$–ario sobre $\mathbb{N}$.

- ⋆ El predicado obtenido a partir de θ por **cuantificación existencial acotada** es el siguiente predicado $(n+1)$–ario sobre $\mathbb{N}$:

$$(\exists z)_{\leq y}\theta(\vec{x}, z) = \begin{cases} 1 & \text{si existe } z_0 \leq y \text{ tal que } \theta(\vec{x}, z_0) = 1. \\ 0 & \text{en caso contrario} \end{cases}$$

Obsérvese que $(\exists z)_{\leq y}\theta(\vec{x}, z) = \theta(\vec{x}, 0) \vee \theta(\vec{x}, 1) \vee \ldots \vee \theta(\vec{x}, y)$.

- ⋆ El predicado obtenido a partir de θ por **cuantificación universal acotada** es el siguiente predicado $(n+1)$–ario sobre $\mathbb{N}$:

$$(\forall z)_{\leq y}\theta(\vec{x}, z) = \begin{cases} 1 & \text{si para todo } z_0 \leq y \text{ se tiene } \theta(\vec{x}, z_0) = 1. \\ 0 & \text{en caso contrario} \end{cases}$$

Obsérvese que $(\forall z)_{\leq y}\ \theta(\vec{x}, z) = \theta(\vec{x}, 0) \wedge \theta(\vec{x}, 1) \wedge \ldots \wedge \theta(\vec{x}, y)$.

Cuantificación no acotada

Sea $\theta(x_1, ..., x_n, y)$ un predicado $(n+1)$–ario sobre $\mathbb{N}$, con $n \neq 0$.

- ⋆ El predicado obtenido a partir de θ por **cuantificación <u>existencial</u> no acotada** es el siguiente predicado n–ario sobre $\mathbb{N}$:

$$(\exists z)\, \theta(\vec{x}, z) = \begin{cases} 1 & \text{si existe } z_0 \text{ tal que se verifica } \theta(\vec{x}, z_0) = 1. \\ 0 & \text{en caso contrario.} \end{cases}$$

- ⋆ El predicado obtenido a partir de θ por **cuantificación <u>universal</u> no acotada** es el siguiente predicado n–ario sobre $\mathbb{N}$:

$$(\forall z)\, \theta(\vec{x}, z) = \begin{cases} 1 & \text{si para todo } z_0 \text{ se verifica } \theta(\vec{x}, z_0) = 1. \\ 0 & \text{en caso contrario.} \end{cases}$$

El principio de minimización

Expresión sobre predicados. Sea $\theta(x)$ un predicado 1–ario sobre $\mathbb{N}$. Si $\exists x\ \theta(x)$ entonces $\exists m\ (\theta(m) \land \forall y < m\ (\neg\theta(y))$

- ⋆ Notación: $m = \mu x(\theta(x))$ (**m** es **el mínimo** de los x que verifican $\theta(x)$).

Expresión conjuntista. Sea $A \subseteq \mathbb{N}$ tal que $A \neq \emptyset$. Entonces $\exists m\ (m \in A \land \forall y < m\,(y \notin A))$

- ⋆ Notación: $m = min(A)$ (**m** es el **menor elemento** de A).

Ejercicio.

- ⋆ Probar que todo número natural $n \geq 2$ es divisible por un número primo.

  Indicación: considérese el conjunto $A = \{x \mid x > 1 \land x \text{ divide a } n\}$, pruébese que es no vacío y justifíquese que el menor elemento de ese conjunto es un número primo.

RGNC

El principio de inducción débil

Teorema: Sea $\theta(x)$ un predicado 1–ario sobre $\mathbb{N}$ tal que se verifica $\theta(0)$ y $\forall x\,(\theta(x) \longrightarrow \theta(x+1))$. Entonces se tiene que $\forall x\; \theta(x)$.

Corolario: Sean $\theta(x)$ un predicado 1–ario sobre $\mathbb{N}$ y $a \in \mathbb{N}$ tales que se verifica $\theta(a)$ y $\forall x \geq a\; (\theta(x) \longrightarrow \theta(x+1))$. Entonces se tiene que $\forall x \geq a\; (\theta(x))$.

Ejercicios.

- ⋆ Probar que para cada $n \in \mathbb{N}$ se tiene que $\displaystyle\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$
- ⋆ Probar que para cada $n \in \mathbb{N}$ se tiene que $\displaystyle\sum_{i=0}^{n} (2i+1) = (n+1)^2$

El principio de inducción fuerte

Teorema: Sea $\theta(x)$ un predicado 1–ario sobre $\mathbb{N}$ tal que se verifica $\theta(0)$ y $\forall x\,([\forall p \leq x\ \theta(p)] \longrightarrow \theta(x+1))$. Entonces se tiene que $\forall x\ \theta(x)$.

Corolario: Sean $\theta(x)$ un predicado 1–ario sobre $\mathbb{N}$ y $a \in \mathbb{N}$ tales que se verifica $\theta(a)$ y $\forall x \geq a\ ([\forall p \geq a(p \leq x \longrightarrow \theta(p))] \longrightarrow \theta(x+1))$. Entonces $\forall x \geq a\ (\theta(x))$.

Ejercicio.

- ⋆ Probar que todo número natural $n \geq 2$ se puede descomponer en un producto de números primos.