Capítulo IV:
FUNCIONES RECURSIVAS

IV.3: CODIFICACIONES

Mario de J. Pérez Jiménez
Grupo de investigación en Computación Natural
Dpto. Ciencias de la Computación e Inteligencia Artificial
Universidad de Sevilla

Lógica Matemática

Curso 2010-11

La sucesión de números primos.

Consideremos la siguiente función $p : \mathbb{N} \to \mathbb{N}$ definida así:

$$p(n) = \begin{cases} 0 & \text{si} \quad n = 0 \\ \text{el } n\text{–ésimo primo} & \text{si} \quad n \geq 1 \end{cases}$$

La función p proporciona la sucesión de números primos (para $n \geq 1$). Notaremos $p(n) = p_n$.

Proposición. La función p es primitiva recursiva.

Para demostrar este resultado hay que usar el siguiente lema de Euclides:

- **Lema**. $\forall n \, (p_{n+1} \leq 1 + p_n!)$.

Entonces basta describir la función p como sigue:

$$\begin{cases} p(0) & = & 0 \\ p(n+1) & = & \mu y \leq (1 + p(n)!) \; (primo(y) \land y > p(n)) \end{cases}$$

Codificaciones

Definición (sucesiones finitas).
Una codificación de $\mathbb{N}^p$ a partir de $\mathbb{N}$, es una función total $f : \mathbb{N}^p \longrightarrow \mathbb{N}$ que verifica:

- f es **PR** e inyectiva.
- Para cada $i, 1 \leq i \leq p$, la función total, $g_i : \mathbb{N} \longrightarrow \mathbb{N}$ definida por

$$g_i(x) = \begin{cases} a_i & si\ x \in rang(f) \wedge x = f(a_1, ..., a_p) \\ 0 & e.c.o.c. \end{cases}$$

  es **PR**.

Definición: (sucesiones de longitud arbitraria)
Sea $\mathbb{N}' = \{\varepsilon\} \cup \mathbb{N} \cup \mathbb{N}^2 \cup ... \cup \mathbb{N}^k \cup ...$ (donde ε es la sucesión vacía). Diremos que una función total $f : \mathbb{N}' \longrightarrow \mathbb{N}$, codifica $\mathbb{N}'$ a partir de $\mathbb{N}$, si para cada $p \geq 1$ la restricción de f a $\mathbb{N}^p$ es una codificación de $\mathbb{N}^p$ a partir de $\mathbb{N}$.

La función par

La función par es la función total $J : \mathbb{N}^2 \longrightarrow \mathbb{N}$ definida por

$$J(x, y) = 2^x \cdot (2y + 1) \dot{-} 1$$

- La función J es **PR** y biyectiva.
- Para todo $x, y \in \mathbb{N}$ se verifica que $x \leq J(x, y)$, $y \leq J(x, y)$.
- Existen $K, L : \mathbb{N} \longrightarrow \mathbb{N}$ tales que si $z = \langle x, y \rangle$, entonces

  $$K(z) = x; \quad L(z) = y; \qquad z = J(K(z), L(z)\rangle$$

  K y L son funciones `decodificadoras` de la función par.
- Las funciones K y L son **PR**.

Nota. Usando la función par podemos codificar $\mathbb{N}^3$ a partir de $\mathbb{N}$:

$$(x, y, z) \longrightarrow J(x, J(y, z))$$

Y, en general, $\mathbb{N}^p$ a partir de $\mathbb{N}$, para cada $p \geq 3$.

La codificación de Gödel

Sea $\{p_n : n \geq 1\}$ la sucesión de números primos y $[\,\cdots\,] : \mathbb{N}' \longrightarrow \mathbb{N}$ la función definida así:

$$\begin{cases} [\varepsilon] & = 1 \\ [a_1, \dots, a_n] & = p_1^{a_1} \dots p_n^{a_n} \end{cases}$$

Diremos que $[a_1, \dots, a_n]$ es el número de Gödel de la sucesión finita $a_1, \dots, a_n$.

Propiedades:

- La función $[\,\cdots\,]$ codifica $\mathbb{N}'$ a partir de $\mathbb{N}$.
- Para cada i $(1 \leq i \leq n)$ se verifica que $a_i \leq [a_1, \dots, a_n]$.
- La función $[\,\cdots\,]$ **no** es inyectiva.
- rang($[\,\cdots\,]$)$= \mathbb{N} - \{0\}$.
- Cada número natural codifica infinitas sucesiones, ya que

$$[a_1, \dots, a_n] = [a_1, \dots, a_n, 0] = [a_1, \dots, a_n, 0, 0] = \dots$$

- En general se tiene que $[a_1, \dots, a_n] \neq [0, a_1, \dots, a_n]$.

La función componente (I)

Para cada número natural $x \geq 2$ existen unos únicos números naturales $a_1, \ldots, a_n$ verificando que $a_n > 0$ y $x = p_1^{a_1} \cdot \cdots \cdot p_n^{a_n}$ (es decir, tal que $x = [a_1, ..., a_n]$).

Se trata de definir el concepto de componentes del número de Gödel $[a_1, ..., a_n]$ de tal manera que si $x \geq 2$, entonces la componente i–ésima de $x = [a_1, ..., a_n]$ sea, precisamente, a_i (para $1 \leq i \leq n$).

En el caso que estamos considerando ($x \geq 2$) ¿qué propiedad caracteriza al número a_i en relación con $x = [a_1, ..., a_n]$?

Teniendo presente que $x = [a_1, ..., a_n] = p_1^{a_1} \cdot \cdots \cdot p_i^{a_i} \cdot \cdots \cdot p_n^{a_n}$ se deduce que:

- El número $p_i^{a_i}$ divide al número x.
- El número $p_i^{a_i+1}$ **no divide** a x.

Por tanto, a_i es el menor número t para el que p_i^{t+1} **no divide** a x. Además, ese número t debe ser menor o igual que x.

La función componente (II)

Estas consideraciones nos lleva proponer la siguiente definición:

- Para cada número natural $x \geq 2$ y cada número natural i, la componente i–ésima de x es el menor número $t \leq x$ tal que p_i^{t+1} **no** divide a x.
- Notaremos por $(x)_i = a_i$ la componente i–ésima de x.
- Además, convendremos que si $x = 0, 1$, entonces $(x)_i = 0$ para cada $i \in \mathbb{N}$ y que $(x)_0 = 0$ para cada $x \in \mathbb{N}$.

Así pues, la función componente está caracterizada por las condiciones:

$$(x)_i = \begin{cases} 0 & \text{si } x = 0, 1 \vee i = 0 \\ \mu t \leq x\ (\neg(p_i^{t+1} | x)) & \text{e.c.o.c.} \end{cases}$$

De la definición anterior resulta que:

- Si $x = p_1^{a_1} \cdot \dots \cdot p_n^{a_n} = [a_1, ..., a_n]$, entonces $(x)_i = 0$ para cada $i > n$.
- La función componente es **PR**.

La función β de Gödel

Teorema: Existe una función $\beta : \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que:

- β es primitiva recursiva.
- Para cada $n \in \mathbb{N}$ y cada sucesión finita $(a_0, \dots, a_n)$ existe $a \in \mathbb{N}$ tal que
$$\forall i \leq n \ (\beta(a, i) = a_i)$$
- $\forall i \in \mathbb{N} \ (\beta(0, i) = 0)$.
- $\forall i \in \mathbb{N} \ (\beta(a, i) \leq a \stackrel{\bullet}{-} 1)$.
- Si $a \neq 0$ entonces $\beta(a, i) < a$.
- El elemento a está acotado por una función primitiva recursiva.

Demostración: Tómese $a = [a_0, a_1, ..., a_n]$ y defínase $\beta(a, i) = (a)_{i+1}$.

La función longitud (I)

Recordemos que para cada número natural $x \geq 2$ existen unos únicos números naturales $a_1, \dots, a_n$ verificando que $a_n > 0$ y $x = p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$ (es decir, tal que $x = [a_1, ..., a_n]$).

Se trata de definir el concepto de longitud del número de Gödel $[a_1, ..., a_n]$ de tal manera que si $x \geq 2$ y $x = [a_1, ..., a_n]$, entonces su longitud sea n.

En el caso que estamos considerando ($x \geq 2$) ¿qué propiedad caracteriza al número n en relación con $x = [a_1, ..., a_n]$?

Teniendo presente que $x = [a_1, ..., a_n] = p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$ se deduce que:

- $(x)_n \neq 0$.
- Para cada i ($i \leq x \land i > n$) se tiene que $(x)_i = 0$.

Por tanto, n es el menor número t que verifica:

- $(x)_t \neq 0$.
- $\forall i \ (i \leq x \land i > n \to (x)_i = 0$.

La función longitud (II)

Estas consideraciones nos lleva proponer la siguiente definición:

- Para cada número natural $x \geq 2$, la longitud de x es el menor número $t \leq x$ tal que $(x)_t \neq 0$ y $\forall i\ (i \leq x \wedge i > t \rightarrow (x)_i = 0$.
- Notaremos por $Long(x)$ la longitud de x.
- Además, convendremos que si $x = 0, 1$, entonces $Long(x) = 0$.

Así pues, la función longitud está caracterizada por las condiciones:

$$Long(x) = \begin{cases} 0 & \text{si } x = 0, 1 \\ \mu t \leq x\ ((x)_t \neq 0 \wedge \forall i \leq x\ (i > t \rightarrow (x)_i = 0) & \text{e.c.o.c.} \end{cases}$$

De la definición anterior resulta que:

- Si $x = p_1^{a_1} \cdot \cdots \cdot p_n^{a_n} = [a_1, ..., a_n]$, con $a_n \neq 0$, entonces $Long(x) = n$.
- La función longitud es **PR**.