Demostración de PR de una función

Práctica 2 - Modelos de Cálculo

Rubén García
Javier Mier
Yuhua Zhan

1. Presentación de la función

El objetivo de esta práctica es demostrar de manera formal que la función $f : \mathbb{N}^2 \to \mathbb{N}$ definida por

$$mcd(n,m) = \begin{cases} 0 & \text{si } nm = 0 \\ \text{el máximo común divisor de } n \text{ y } m & \text{si } nm \neq 0, \end{cases}$$

2. Funciones PR

En este apartado se incluyen las funciones que son primitivas recursivas que ya han sido demostradas.

(a) La función cero: $z(n) = 0, \forall n \in \mathbb{N}$

(b) La función sucesor: $s(n) = n + 1, \forall n \in \mathbb{N}$

(c) La función proyección: $p_i^k(n_1, \ldots, n_k) = n_i, \forall k \in \mathbb{N}^*, n_1, \ldots, n_k \in \mathbb{N}, \forall i \in 1, \ldots, k$

(d) Composición de funciones: $f_1(\vec{n}) = g_1(h_0(\vec{n}), \ldots, h_l(\vec{n}))$

(e) Recursión primitiva:

$$\begin{cases} f_2(\vec{n}, 0) = g_2(\vec{n}) \\ f_2(\vec{n}, m+1) = h(\vec{n}, m, f_2(\vec{n}, m)) \end{cases}$$

Donde $\vec{n} = (n_1, \ldots, n_k)$

Otras funciones de las que se hacen uso y que también han sido demostradas durante las sesiones de teoría como PR son las siguientes:

- $suma(n,m) = n + m$
- $resta(n,m) = \begin{cases} n - m & \text{si } n > m \\ 0 & \text{si } n \leq m \end{cases}$

- $mult(n, m) = n * m$
- $resto(n, m) = \begin{cases} \text{el resto de dividir } m \text{ entre } n & \text{si } n \neq 0 \\ m & \text{si } n = 0 \end{cases}$
- $\overline{sg}(n) = \begin{cases} 1 & \text{si } n = 0 \\ 0 & \text{si } n \neq 0 \end{cases}$

3. Demostración de la función

En primer lugar, para poder demostrar que el máximo común divisor entre dos números sea una función PR, sería necesario encontrar una función PR que nos devuelva un número d si es divisor común entre dos números n y m, y 0 en caso contrario.

$$f(n, m, d) = \begin{cases} d & \text{si } resto(d, n) \text{ o } resto(d, m) \\ 0 & \text{en caso contrario} \end{cases}$$

Para saber si un número d es divisor de otro número cualquiera n, sabemos que el resto de la división del segundo entre el primero ha de ser 0 ($resto(d, n)$). Usando esto a nuestro favor, podemos saber que, si el resto de n entre d es 0 y el resto entre m y d es 0, el número d es divisor común de n y m ($suma(resto(d, n), resto(d, m))$). Con la función $\overline{sg}(n)$ podemos obtener un 1 cuando la suma de restos sea 0 y devolverá un 0 en cualquier otro caso. Multiplicando este resultado por el número d, podemos hacer que la función $f(n, m, d)$ devuelva el número d si es divisor común de n y m.

$$f(n, m, d) = mult(d, \overline{sg}(suma(resto(d, n), resto(d, m))))$$

Ajustándolo para que la entrada que reciben las funciones sean iguales a los parámetros recibidos por f, nos queda una función como la siguiente:

$$f(n, m, d) = mult(p_3^3(n, m, d), \overline{sg}(suma(resto(p_3^3(n, m, d), p_1^3(n, m, d)), resto(p_3^3(n, m, d), p_2^3(n, m, d)))))$$

$f(n, m, d)$ es PR por (c), (d) y porque $\overline{sg}$, $mult$, $suma$ y $resto$ son PR.

Una vez podemos conocer si un número es divisor común entre dos números distintos, para poder encontrar el MCD es necesario poder identificar el máximo entre dos números. Para saber el máximo entre dos números n y m; podemos aprovechar que, si m es mayor que n, la resta entre n y m es igual a 0[1], en caso contrario, si n es mayor que m, el resultado de la resta es $n - m$. Teniendo esto en cuenta, si al resultado de la resta le sumamos m, el resultado final es el mayor número de los dos. Si m es mayor que n, el resultado de la resta es 0, por lo que al sumarle m, el resultado final es m, el mayor de los dos; si n es mayor que m, el

[1]Esto es por como está definida la resta, ya que solo tratamos con números naturales, incluyendo el 0.

resultado de la resta es $n - m$, y al sumarle m, el resultado final es n, el mayor de los dos.

$$max(n, m) = \begin{cases} m, & \text{si } n \leq m \\ n, & \text{si } n > m \end{cases}$$

$$suma(resta(n, m), m)$$

$$suma(resta(n, m), p_2^2(n, m))$$

$max(n, m)$ es PR por (c), (d) y porque suma y resta son PR.

Ya teniendo demostrada la función que devuelve el máximo entre dos número, podemos crear una función de máximo acumulativo que nos permita encontrar el máximo de una colección de tamaño $p+1$. Si hacemos uso de la función f definida anteriormente, encontrar el máximo de esa colección de resultados sería equivalente a obtener el máximo común divisor de dos números n y m.

$$Max(n, m, p) = máximo\{f(n, m, 0), ..., f(n, m, p)\}$$

Aunque hemos demostrado anteriormente que $max(n, m)$ y $f(n, m, d)$ son funciones PR, es necesario demostrar que la función del máximo acumulativo $Max(n, m, p)$ también es PR. Podemos tratar de demostrarlo por recursión primitiva.

- Caso base:

  $$Max(n, m, 0) = g_2(n, m) = f(n, m, 0) = f(p_1^2(n, m), p_2^2(n, m), z(p_1^2(n, m)))$$

  Este caso es PR por (a), (c), (d) y porque f es PR.

- Caso inductivo:

  $$Max(n, m, p + 1) = h(n, m, p, Max(n, m, p)) = \text{máximo}\{f(n, m, 0), ..., f(n, m, p), f(n, m, p + 1)\} = max(Max(n, m, p), f(n, m, p + 1))$$

  Sustitución de $Max(n, m, p)$ por t

  $$h(n, m, p, t) = max(t, f(n, m, p + 1)) = max(p_4^4(n, m, p, t), f(p_1^4(n, m, p, t), p_2^4(n, m, p, t), p_3^4(n, m, p, t)))$$

  Este caso es PR por (b), (c), (d) y porque f es PR.

Como ambos casos son PR, podemos concluir que $Max(n, m, p)$ es PR por (a), (b), (c), (d), (e) y porque f es PR.

Nos quedaría comprobar que el máximo común divisor es una función PR. Como hemos mencionado anteriormente, la función del máximo acumulativo nos permite encontrar el divisor común más grande de n y m de una lista de $p + 1$ elementos (desde 0 hasta p). Como el resultado del mcd depende del producto de n y m, podemos hacer que el límite p de la lista sea la multiplicación de n y m, quedando la siguiente igualdad:

$$mcd(n, m) = Max(n, m, mult(n, m))$$

Podemos modificar la segunda mitad de la igualdad para que los parámetros recibidos por Max sean los mismos que los de la función mcd, es decir, que utilicen el mismo vector. El resultado de dicha modificación resulta en la identidad:

$$mcd(n, m) = Max(p_1^2(n, m), p_2^2(n, m), mult(n, m))$$

Con esto podemos concluir que la función mcd es PR por (c), (d) y porque Max y $mult$ son PR.