Verificación Formal - Tarea 1

Ciro Iván García López

Octubre 2020

1. Árbol Binario.

Definición 1. Se define una lista (arreglo) inductivamente de la siguiente manera:

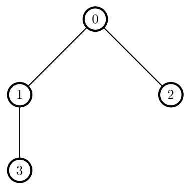
- Existe una lista vacía notada por NL.
- Si $x \in \mathbb{N}$ y L es una lista, entonces $[x, L]$ es una lista. Para una lista de esta forma, se llamará a x la cabeza de la lista y a L la cola.

Ejemplo 1. La lista $[1, 2, 3]$ está representada por $[1\ [2\ [3\ NL]]]$.

Definición 2. Se define un árbol binario de manera inductiva por:

- Existe un árbol vacío notado por NA.
- Si $e \in \mathbb{N}$ y AI, AD son árboles binarios, entonces $A = (e, AI, AD)$ es un árbol binario. Al elemento e se le llamará raíz de A.

Ejemplo 2. $A = (0\ (1\ (3\ NA\ NA)\ NA)\ (2\ NA\ NA))$ representa el siguiente árbol:



Definición 3. Se define la concatenación de dos listas L_1, L_2 como la operación que pega al final de la lista L_1 los elementos de la lista L_2. Se notará por $L_1 + +L_2$.

Definición 4. Aplanamiento de un árbol binario. Sea A un árbol binario, entonces:

$$Aplan(A) = \begin{cases} NL & \text{Si } A = NA \\ [e] + +Aplan(AI) + +Aplan(AD) & \text{Si } A = (e, AI, AD) \end{cases}$$

Observe que $Aplan$ es una función de los árboles binarios a las listas.

Lema 1. *Sea L una lista tal que $L = L_1 + +L_2$ para un par de listas no vacías L_1, L_2. $x \in L$ si y solo si $x \in L_1$ o $x \in L_2$.*

Demostración. Dado que $L = L_1 + +L_2$, los elementos de L son distribuidos entre L_1 y L_2 por lo que un elemento aparece en L si y solo si aparece en L_1 o en L_2. $\square$

Definición 5. Se llama altura de un árbol a la longitud de la trayectoria más larga en el árbol desde la raíz.

Teorema 1. *Dado un árbol A, $x \in A$ si y solo si $x \in Aplan(A)$.*

Demostración. Se procede a demostrar la afirmación por inducción sobre la altura del árbol. Para el caso en que la altura es cero, entonces $A = NA$ y se sigue la afirmación por vacuidad.

Suponga que para todos los árboles con altura menor a n se cumple la afirmación y sea $A = (e, AI, AD)$ un árbol con altura n. Luego hay dos casos a considerar:

- Si $x = e$ entonces por la definición de aplanamiento se sigue el resultado, pues en este caso x es la cabeza de $Aplan(A)$.
- Si $x \neq e$ entonces de la estructura del árbol y la hipótesis de inducción, se da alguno de los siguientes casos,
    - $x \in AI$ si y solo si $x \in Aplan(AI)$
    - $x \in AD$ si y solo si $x \in Aplan(AD)$

  y del lema 1 se sigue el resultado. □

2. Ordenes 1 y 2.

Definición 6. Se define la relación binaria $\leq_1$ sobre $\mathbb{N}$ de la siguiente manera:

$$\begin{aligned}
U_0 &= \{(n,m) \in \mathbb{N} \times \mathbb{N} : n = m\} \\
U_1 &= \{(n,m+1) \in \mathbb{N} \times \mathbb{N} : (n,m) \in U_0\} \\
&\vdots \\
U_{n+1} &= \{(n,m+1) \in \mathbb{N} \times \mathbb{N} : (n,m) \in U_n\} \\
&\vdots \\
\leq_1 &= \bigcup_{n \in \mathbb{N}} U_n
\end{aligned}$$

Además se notará $n \leq_1 m$ si y solo si existe $k \in \mathbb{N}$ tal que $(n,m) \in U_k$, sin pérdida de generalidad siempre se puede tomar k mínimo. También se dirá que $n <_1 m$ si y solo si $n + 1 \leq_1 m$.

Definición 7. Se define la relación binaria $<_2$ sobre $\mathbb{N}$ de la siguiente manera:

$$\begin{aligned}
V_0 &= \{(n,m) \in \mathbb{N} \times \mathbb{N} : n = 0 \text{ y } m \neq 0\} \\
V_1 &= \{(n+1,m+1) \in \mathbb{N} \times \mathbb{N} : (n,m) \in V_0\} \\
&\vdots \\
V_{n+1} &= \{(n+1,m+1) \in \mathbb{N} \times \mathbb{N} : (n,m) \in V_n\} \\
&\vdots \\
<_2 &= \bigcup_{n \in \mathbb{N}} V_n
\end{aligned}$$

Se dirá que $n <_2 m$ si y solo si existe $l \in \mathbb{N}$ tal que $(n,m) \in V_l$, sin pérdida de generalidad siempre se puede tomar l mínimo. Además se notara $n \leq_2 m$ si y solo si $n = m$ o $n <_2 m$.

Observe que las definiciones dadas son equivalentes a las definiciones por reglas, para el caso del orden 1 se cumple que $n \leq_1 m$ hay dos posibles casos dados por las reglas:

- $n \leq_1 n$ por la regla $o1refl$, en este caso $(n,n) \in U_0$.
- Inductivamente, si $n \leq_1 m + 1$ por la regla $o1s$, entonces $(n, m+1) \in U_{k+1}$ con $k \in \mathbb{N}$ que está dada por la hipótesis $n \leq_1 m$.

Observar que el orden 2 corresponde con las reglas, es análogo.

Teorema 2. *Dados $n, m \in \mathbb{N}$ tales que $(n, m) \in U_k$, existen $k', s \in \mathbb{N}$ y una sucesión $(n, n), ..., (n, n+s)$ tales que:*

- $k = k' + s$.
- $m = n + s$
- $(n, n) \in U_{k'}$, $(n, n+1) \in U_{k'+1}$, ..., $(n, m) \in U_k$.

Demostración. La prueba se realiza por inducción sobre k. En el caso que $(n, m) \in U_0$ entonces se tiene que $n = m$ y se puede tomar entonces $k' = k$ y $s = 0$.

Suponga ahora que el resultado se cumple para $k \neq 0$ y sea $(n, m) \in U_{k+1}$, luego por la definición de U_{k+1} se sigue que $(n, m-1) \in U_k$ y por lo tanto existen k'_0, s_0 y la sucesión $(n, n), ..., (n, n+s)$ que cumplen las condiciones. Es así que si $k' = k'_0$, $s = s_0 + 1$ y la sucesión $(n, n), ..., (n, n+s), (n, n+s+1)$ se cumple que:

- $k + 1 = k' + s = k'_0 + s_0 + 1 = k + 1$.
- $m = n + s = n + s_0 + 1 = m - 1 + 1$.
- $(n, n) \in U_{k'}$, $(n, n+1) \in U_{k'+1}$, ..., $(n, m-1) \in U_k$, $(n, m) \in U_{k+1}$.

Concluyendo que la afirmación es cierta para todo k por inducción y en consecuencia para toda pareja $n \leq_1 m$. □

Lema 2. *Para $n, m, p \in \mathbb{N}$, si $n \leq_1 m$ y $m \leq_1 p$, entonces $n \leq_1 p$.*

Demostración. Sea $k_m, k_p \in \mathbb{N}$ dados por el teorema 2 para $n \leq_1 m$ y $m \leq_1 p$ respectivamente. Luego $(n, p) \in U_{k_m + k_p}$. □

Lema 3. *No existe $n \in \mathbb{N}$ tal que $n <_2 n$.*

Demostración. Suponga que existe un $n \in \mathbb{N}$ (se puede suponer mínimo) tal que $n <_2 n$, luego existe un $l \in \mathbb{N}$ tal que $(n, n) \in V_l$, luego hay dos casos según sea l:

- $l = 0$, en este caso necesariamente $n = 0$ y $n \neq 0$ lo cual es contradictorio.
- $l \neq 0$ en este caso $(n-1, n-1) \in V_{l-1}$. Lo cual contradice que n era mínimo.

En ambos casos se contradice que existe l, por contradicción se sigue el resultado. □

Teorema 3. *Para todos $n, m \in \mathbb{N}$, $n \leq_1 m$ si y solo si $n \leq_2 m$.*

Demostración. Sean $n, m \in \mathbb{N}$ y suponga que $n \leq_1 m$, luego existe un $k \in \mathbb{N}$ tal que $(n, m) \in U_k$. Si $k = 0$ entonces $n = m$ y por lo tanto $n \leq_2 m$ por definición del orden 2. En el caso que $k \neq 0$ entonces del teorema 2 existe $s \in \mathbb{N}$ tal que $m = n + s$, además como $m \neq n$ entonces $s \neq 0$ y por lo tanto $(0, s) \in V_0$ y en consecuencia $(n, m) \in V_n$.

En la otra dirección, suponga que $n \leq_2 m$. Entonces hay dos casos, si $n = m$ entonces se tiene que $(n, m) \in U_0$ y por lo tanto $n \leq_1 m$. En el segundo caso $n <_2 m$ y por lo tanto existe $l \in \mathbb{N}$ tal que $(n, m) \in V_l$, si $l = 0$ entonces se cumple que $(n, m) = (0, l) \in U_l$ y por lo tanto $n \leq_1 m$. En el caso que $l \neq 0$ entonces se puede suponer que $l = n$ y por lo tanto tomando $k = m - l$ entonces se tiene que $(n, m) \in U_k$ pues $(n, n) \in U_0$. □

Teorema 4. *Dados $n, m \in \mathbb{N}$, $n <_1 m$ si y solo si $n <_2 m$.*

Demostración. Suponga que $n <_1 m$, luego la definición indica que $n + 1 \leq_1 m$, por el teorema anterior existe un $l \in \mathbb{N}$ tal que $(n+1, m) \in V_l$ además se cumple que $l \neq 0$ ya que $n + 1 \neq 0$, por lo que entonces $(n, m) \in V_{l-1}$, i.e. $n <_2 m$.

En la otra dirección suponga que $n <_2 m$, luego existe $l \in \mathbb{N}$ tal que $(n, m) \in V_l$ y hay dos casos:

- Si $l = 0$, entonces $(n, m) \in U_m$ ya que $(0, 0) \in U_0$.
- Si $l \neq 0$, entonces se puede suponer sin perdida de generalidad que $l = n$ y que existe $p \neq 0$ tal que $(0, p) \in V_0$ y $p + l = m$. Entonces $(n, m) \in U_p$, ya que $n + p = l + p = m$ y $(n, n) \in U_0$. □

3. Propiedades del orden.

Para esta parte se ha preferido el orden uno en las pruebas.

Lema 4. *Dados $n, m \in \mathbb{N}$ tales que $n, m \neq 0$ y $n \leq_1 m$ entonces $n - 1 \leq_1 m - 1$.*

Demostración. Del hecho que $n \leq_1 m$ y la definición de $\leq_1$ se tiene que existe un $k \in \mathbb{N}$ tal que $(n, m) \in U_k$, luego hay dos casos:

- $k = 0$, en este caso como $n, m \neq 0$, entonces $n - 1 = m - 1$ y por lo tanto $(n - 1, m - 1) \in U_0$, es decir que $n - 1 \leq_1 m - 1$.
- $k \neq 0$, en este caso usando el teorema 2 que $(n - 1, n - 1) \in U_{k'}$ y por lo tanto por la definición de $\leq_1$ $(n - 1, m - 1) \in U_k$. Concluyendo que $n - 1 \leq_1 m - 1$. □

Lema 5. *No existe $n \in \mathbb{N}$ tal que $n + 1 \leq_1 0$.*

Demostración. Suponga que existe $n \in \mathbb{N}$ tal que $n + 1 \leq_1 0$. Por la definición de $\leq_1$ existe un $k \in \mathbb{N}$ tal que $(n + 1, 0) \in U_k$. Pero, para $k \neq 0$ se cumple que los elementos de U_k tiene segunda componente no cero, y como $1 \neq 0$ tampoco se da el caso que $k = 0$, lo cual contradice que $(n + 1, 0)$ está en algún U_k. Por reducción al absurdo se sigue el resultado. □

Teorema 5. *Para todos $n, m \in \mathbb{N}$, si $n \leq_1 m$ entonces $min(n, m) = n$.*

Demostración. Se procede por inducción sobre n, en el caso que $n = 0$ entonces $min(n, m) = n = 0$ y entonces se sigue la afirmación para cualquier m. Suponga ahora cierta la afirmación para n y tome $m \in \mathbb{N}$ tal que $n + 1 \leq_1 m$. Así de la definición de $\leq_1$ existe $k \in \mathbb{N}$ tal que $(n + 1, m) \in U_k$ y hay dos casos:

- $k = 0$, por lo que entonces $n + 1 = m = min(n, m)$ y en este caso se cumple la afirmación.
- $k \neq 0$, en este caso se tiene que necesariamente $m \neq 0$ y por lo tanto $min(n+1, m) = 1 + min(n, m - 1) = 1 + n = n + 1$, ya que $n \leq_1 m - 1$ por el lema 4.

Así, por inducción matemática se sigue la afirmación. □

Teorema 6. *Para todos $n, m \in \mathbb{N}$, si $m \leq_1 n$ entonces $min(n, m) = m$.*

Demostración. La prueba es análoga al teorema anterior, al aplicar la conmutatividad en el mínimo[1]. □

Teorema 7. *Para todos $n, m \in \mathbb{N}$ se tiene que $n \leq_1 n + m$.*

Demostración. Se procede por inducción sobre m. Para el caso que $m = 0$ entonces se cumple que $n+0 = n$ y por lo tanto $n \leq_1 n + m$ ya que $(n, n) \in U_0$. Suponga ahora que $m \neq 0$ y que para m se cumple la afirmación, por lo tanto existe $k \in \mathbb{N}$ tal que $(n, n + m) \in U_k$, pero entonces $(n, n + m + 1) \in U_{k+1}$ y por lo tanto se puede concluir que $n \leq_1 n + m + 1$. Por el principio de inducción se sigue el teorema. □

Teorema 8. *Para todos $n, m \in \mathbb{N}$, se cumple que $n \leq_1 m + n$.*

Demostración. La prueba es análoga a la del teorema anterior, dado que la suma es conmutativa. □

Teorema 9. *Para $n, m, p \in \mathbb{N}$, si $n \leq_1 m$ entonces $n + p \leq_1 m + p$.*

Demostración. Se hace la demostración por inducción sobre p. Para el caso $p = 0$ por hipótesis $n \leq_1 m$. Suponga ahora que el resultado se cumple para p, por lo que entonces existe un $k \in \mathbb{N}$ tal que $(n + p, m + p) \in U_k$ y por lo tanto son dos los casos a considerar:

- $k = 0$, se cumple que $n + p = m + p$ y por lo tanto $n + p + 1 = m + p + 1$. Concluyendo entones que $n + p + 1 \leq_1 m + p + 1$.

[1] No sucede lo mismo en Coq, ya que el sistema no sabe que el mínimo conmuta.

- $k \neq 0$, usando el teorema 2 se cumple que existe $k' \in \mathbb{N}$ tal que $(n+p+1, n+p+1) \in U_{k'}$ y por lo tanto $(n+p+1, m+p+1) \in U_k$

Por inducción sobre p se sigue el resultado. □

Teorema 10. *Para todos $n, m \in \mathbb{N}$, se tiene que $n \leq_1 m$ o $m \leq_1 n$.*

Demostración. La prueba se hace por inducción sobre n. Para el caso que $n = 0$ entonces se cumple que $(0,0) \in U_0$ y para cualquier otro m no cero, $(0, m) \in U_m$. Por lo que entonces $0 \leq_1 m$ para cualquier $m \in \mathbb{N}$. Suponga que la afirmación es cierta para n, por lo que entonces dado cualquier $m \in \mathbb{N}$ se cumple que $n \leq_1 m$ o $m \leq_1 n$ y hay dos casos:

- En el primer caso, suponga que $(n, m) \in U_k$ para cierto $k \in \mathbb{N}$. Entonces si $k = 0$ se tiene que $(m, n+1) \in U_1$ y en el caso que $k \neq 0$ entonces por el teorema 2 se cumple que existe $k' \in \mathbb{N}$ tal que $(n+1, n+1) \in U_{k'}$ y $(n+1, m) \in U_{k-1}$. Por lo que se da que $n \leq_1 m$ o $m \leq_1 n$.

- En el segundo caso se tiene que $(m, n) \in U_k$ para algún $k \in \mathbb{N}$ y por lo tanto $(m, n+1) \in U_{k+1}$.

Por lo que se concluye para $n+1$ que se tiene alguno de los dos casos y por inducción se sigue el resultado. □

Teorema 11. *Para todos $n, m \in \mathbb{N}$, $n \leq_1 m$ si y solo si existe $p \in \mathbb{N}$ tal que $m = n + p$.*

Demostración. La suficiencia es consecuencia inmediata del teorema 2. Para la necesidad, basta con observar que si existe $p \in \mathbb{N}$ tal que $m = n + p$, entonces $(n, m) \in U_p$ pues $(n, n) \in U_0$. □

4. Función take.

Definición 8. Sea L una lista, se define la función longitud φ de la siguiente manera:

$$\varphi(L) = \begin{cases} 0 & \text{Si } L = NL \\ 1 + \varphi(L_0) & \text{Si } L = [x, L_0] \end{cases}$$

Definición 9. take Sea L una lista y $n \in \mathbb{N}$, luego:

$$take(n, L) = \begin{cases} L & \text{Si } \varphi(L) \leq n \\ [x_1, ..., x_n] & \text{Si } n < \varphi(L) \text{ y } L = [x_1, ..., x_n, ...] \end{cases}$$

es decir, *take* toma los primeros n elementos de L.

Lema 6. *Sea $n \in \mathbb{N}$ y $L = [x, L_0]$ una lista no vacía. Luego $take(n+1, L) = [x] + +take(n, L_0)$.*

Demostración. Por la definición de la función *take* se cumple que al tomar $n+1$ elementos siempre se tomará la cabeza de la lista, por lo que tomar $n+1$ elementos de L es lo mismo que tomar la cabeza y n elementos de L_0. □

Teorema 12. *Para toda lista L y $n, m \in \mathbb{N}$, $take(n, take(m, L)) = take(min(n, m), L)$.*

Demostración. La prueba se realiza por doble inducción sobre n y m. Para comenzar considere el caso en que n = 0 o m = 0. En este caso $take(m, L) = NL$ o $take(n, take(m, L)) = NL$, a su vez en cualquiera de los dos casos se cumple que $min(n, m) = 0$ y $take(min(n, m), L) = NL$, por lo que se cumple el caso base.

Suponga ahora que la afirmación es cierta para los naturales menores a $n > 0$ y los naturales menores a $m > 0$. Se tienen dos casos según sea L:

- En caso que $L = NL$, entonces $take(m, L) = NL$ y $take(n, take(m, L)) = NL = take(min(n, m), L)$ por la definición de *take*.

- Suponga ahora que $L = [x, L_0]$, por el lema 6 se cumple que $take(m, L) = [x] + +take(m-1, L_0)$ y por lo tanto $take(n, take(m, L)) = [x] + +take(n-1, take(m-1, L_0))$. Por otro lado como $min(n, m) > 0$ pues $n, m > 0$, $min(n-1, m-1)+1 = min(n, m)$ y es así que $take(min(n, m), L) = take(min(n-1, m-1)+1, L) = [x] + +take(min(n-1, m-1), L_0)$. Por la hipótesis de inducción se cumple que $take(min(n-1, m-1), L_0) = take(m-1, take(n-1, L_0))$. Concluyendo la igualdad para este caso.

Concluyendo a la afirmación para n, m y por lo tanto por inducción matemática para todos $n, m \in \mathbb{N}$. $\square$