Apunte de Inducción Estructural

Algoritmos y Estructuras de Datos 2

1. Introducción

El siguiente es un apunte donde se presenta la resolución de 4 ejercicios de inducción estructural. El apunte pretende ser un apunte práctico basado en la ejemplificación, no un apunte completo sobre el tema en general.

Si bien este apunte se hizo con buena fe, podría contener errores involuntarios; por esta razón, en caso de encontrar alguna falla, o algo que no cierre, avisen para poder corregirlo.

2. Ejercicio 1: Duplicar una secuencia

2.1. Enunciado

Considerando la siguiente especificación:

Long : secu(α) $\longrightarrow$ nat

l_1)	Long(<>)	$\equiv$ 0
l_2)	Long(a $\bullet$ s)	$\equiv$ Long(s) + 1

Duplicar : secu(α) $\longrightarrow$ secu(α)

d_1)	Duplicar(<>)	$\equiv$ <>
d_2)	Duplicar(a $\bullet$ s)	$\equiv$ a $\bullet$ a $\bullet$ Duplicar(s)

Demuestre que ($\forall s$: secu(α))(Long(Duplicar(s)) = 2 $\times$ Long(s)).

2.2. Resolución

2.2.1. Convencernos de que lo que queremos probar es cierto

Veamos un ejemplito para ver cómo funciona la función duplicar:

Duplicar(1 $\bullet$ 2 $\bullet$ <>)	por d_2
1 $\bullet$ 1 $\bullet$ Duplicar(2 $\bullet$ <>)	nuevamente usando d_2
1 $\bullet$ 1 $\bullet$ 2 $\bullet$ 2 $\bullet$ Duplicar(<>)	y ahora por d_1
1 $\bullet$ 1 $\bullet$ 2 $\bullet$ 2 $\bullet$ <>	

En este caso vemos que la propiedad parece tener sentido, ya que efectivamente la longitud de la secuencia resultante es el doble de la original.

OJO! esto es sólo un ejemplo, para tratar de convencernos, claramente no probamos nada; sin embargo está bueno creernos que lo que queremos demostrar es verdadero.

2.2.2. Plantear la propiedad como predicado unario

Básicamente plantear el predicado unario consiste en quitar el cuantificador que liga a la variable sobre la que vamos a hacer inducción.

En este caso la propiedad era:

($\forall s$: secu(α))(Long(Duplicar(s)) = 2 $\times$ Long(s))

De modo que el predicado resultante es:

$P(s)$ $\equiv$ (Long(Duplicar(s)) = 2 $\times$ Long(s))

Notar que con esta definición de P, la expresión ($\forall s$: secu(α)) $P(s)$ resulta equivalente a lo que queremos demostrar. Ahora podemos usar el esquema como lo aprendimos.

2.2.3. Plantear el esquema de inducción

El esquema de inducción consiste en plantear los casos base que debemos probar así como los pasos inductivos. Este esquema es propio del tipo, ya que se deriva de su conjunto de generadores, por lo tanto para cualquier propiedad que quieran probar sobre un TAD dado, el esquema de inducción es el mismo.

En este caso tenemos un único generador básico (<>), es decir, que no toma instancias de secuencias, y un único recursivo (•), que toma una instancia de secuencia.

Por lo tanto el único caso base es $P(<>)$, y el único paso inductivo es:

$$(\forall s : \text{secu}(\alpha))(\underbrace{P(s)}_{HI} \Rightarrow \underbrace{(\forall a : \alpha)P(a \bullet s)}_{TI})$$

En el paso inductivo $P(s)$ es la **hipótesis inductiva** y $P(a \bullet s)$ es la **tesis inductiva**.

El esquema es entonces:

$$P(<>) \wedge (\forall s : \text{secu}(\alpha))(P(s) \Rightarrow (\forall a : \alpha)P(a \cdot s))$$

Si demostramos esto último, por el principio de inducción estructural habremos demostrado ($\forall s$: secu(α)) $P(s)$.

2.2.4. Probar el caso base

Nuestro caso base era $P(<>)$. Usando la definición que dimos de P, tenemos:

$$P(<>) = [\ \text{Long}(\text{Duplicar}(<>)) \equiv 2 \times \text{Long}(<>)\ ]$$

Entonces tenemos que probar:

$$\text{Long}(\text{Duplicar}(<>)) \equiv 2 \times \text{Long}(<>)$$

La idea es ir viendo que axiomas podemos ir aplicando para ir reduciendo la expresión que tenemos. Notar que los axiomas nos brindan equivalencias, por lo cual son "reversibles" es decir, se pueden aplicar de izquierda a derecha o de derecha a izquierda.

$$\text{Long}(\text{Duplicar}(<>)) \equiv 2 \times \text{Long}(<>)$$

Usando el axioma l_1, reemplazamos Long(<>) por 0,

$$\text{Long}(\text{Duplicar}(<>)) \equiv 2 \times 0$$

Sabemos que 2×0 da 0, entonces podemos reemplazarlo. En general los conocimientos de aritmética sobre los naturales se pueden utilizar sin demostrar, salvo que justamente el ejercicio sea demostrarlo.

$$\text{Long}(\text{Duplicar}(<>)) \equiv 0$$

Mirando el lado izquierdo tenemos Long(Duplicar(<>)). Ninguno de los axiomas de Long aplican, ya que si bien sabemos que Duplicar(<>) es una secuencia, no sabemos como se expresa en función de sus generadores, que es como está axiomatizada Long. Entonces buscamos algún axioma de Duplicar que nos permita seguir. Podemos aplicar d_1.

$$\text{Long}(<>) \equiv 0$$

Ahora sí podemos aplicar un axioma de Long, l_1.

$$0 \equiv 0$$

Y efectivamente 0 es equivalente a 0, por lo cual probamos el caso base.

Hay que tener cuidado de que todos los pasos de la deducción hayan sido "si y sólo si", ya que formalmente la deducción lógica es la que resulta de leer las expresiones desde abajo hacia arriba (partiendo de que sabemos $0 \equiv 0$, deducimos lo que queríamos probar).

2.2.5. Probar el paso inductivo

Nuestro paso inductivo era:

$$(\forall s : \text{secu}(\alpha))(P(s) \Rightarrow (\forall a : \alpha)P(a \bullet s))$$

$P(s)$ va a ser nuestra hipótesis inductiva, es lo que vamos a asumir que es verdadero, ya que si fuese falsa, y como el paso inductivo es una implicación con $P(s)$ como antecedente, sería trivialmente verdadero.

En el paso inductivo aparece una variable a, de tipo α. Es importante notar que la variable está ligada a un cuantificador universal, por lo tanto no se puede asumir nada de ese a, es decir, no se puede suponer que sea un natural mayor que 5, una secuencia de string, nada; sólo sabemos que es de tipo α y nada más.

Entonces, suponiendo que $P(s) \equiv True$, veamos que pasa con $P(a \bullet s)$ para un a cualquiera.

$$P(a \bullet s) = [\ \text{Long}(\text{Duplicar}(a \bullet s)) \equiv 2 \times \text{Long}(a \bullet s)\ ]$$

$$\text{Long}(\text{Duplicar}(a \bullet s)) \equiv 2 \times \text{Long}(a \bullet s)$$

por d_2

$$\text{Long}(a \bullet a \bullet \text{Duplicar}(s)) \equiv 2 \times \text{Long}(a \bullet s)$$

por l_2

$$1 + \text{Long}(a \bullet \text{Duplicar}(s)) \equiv 2 \times \text{Long}(a \bullet s)$$

por l_2 de nuevo

$$1 + 1 + \text{Long}(\text{Duplicar}(s)) \equiv 2 \times \text{Long}(a \bullet s)$$

$$2 + \text{Long}(\text{Duplicar}(s)) \equiv 2 \times \text{Long}(a \bullet s)$$

aplicando l_2 en el lado derecho

$$2 + \text{Long}(\text{Duplicar}(s)) \equiv 2 \times (1 + \text{Long}(s))$$

por propiedad distributiva de los naturales

$$2 + \text{Long}(\text{Duplicar}(s)) \equiv 2 + 2 \times \text{Long}(s)$$

Usando la HI, sabemos que $\text{Long}(\text{Duplicar}(s)) \equiv 2 \times \text{Long}(s)$

$$2 + 2 \times \text{Long}(s) \equiv 2 + 2 \times \text{Long}(s)$$

Aquí, como ambos lados son sintácticamente iguales, termina la demostración. Con esto probamos el paso inductivo.

Luego, como probamos antes el caso base, sabemos que la propiedad es válida para cualquier secuencia

3. Ejercicio 2: Tomar y sacar

3.1. Enunciado

Considerando la siguiente especificación:

$\bullet$ & $\bullet$: secu(α) $\times$ secu(α) $\longrightarrow$ secu(α)

$\&_1$) $<> \ \& \ t \equiv t$

$\&_2$) $(a \bullet s) \ \& \ t \equiv \text{a} \bullet (s \ \& \ t)$

Tomar : secu(α) $\times$ nat $\longrightarrow$ secu(α)

t_1) Tomar($<>, n$) $\equiv <>$

t_2) Tomar($a \bullet s, n$) $\equiv$ **if** $n = 0$ **then** $<>$ **else** a $\bullet$ Tomar($s, n-1$) **fi**

Sacar : secu(α) $\times$ nat $\longrightarrow$ secu(α)

s_1) Sacar($<>, n$) $\equiv <>$

s_2) Sacar(a $\bullet$ s, n) $\equiv$ **if** $n = 0$ **then** a $\bullet$ s **else** Sacar($s, n-1$) **fi**

demuestre que:

$$\forall s : \text{secu}(\alpha))(\forall n : \text{nat})(\text{Tomar}(s, n) \ \& \ \text{Sacar}(s, n) \equiv s)$$

3.2. Resolución

3.2.1. Convencernos de que lo que queremos probar es cierto

No lo haremos en el apunte. Hagan los casos de ejemplo que consideren necesarios.

3.2.2. Plantear la propiedad como predicado unario

$$P(s) = (\forall n : \text{nat})(\text{Tomar}(s, n) \ \& \ \text{Sacar}(s, n) \equiv s)$$

3.2.3. Plantear el esquema de inducción

Es el mismo que para el ejercicio anterior:

$$P(<>) \wedge (\forall s : \text{secu}(\alpha))(P(s) \ \Rightarrow \ (\forall a : \alpha)P(a \bullet s))$$

3.2.4. Probar el caso base

$$P(<>)$$
$$(\forall n : \text{nat})(\text{Tomar}(<>, n) \ \& \ \text{Sacar}(<>, n) \equiv <>)$$

sacamos el cuantificador n, pero teniendo en cuenta que no podemos suponer nada de n, que es un nat arbitrario

$$\text{Tomar}(<>, n) \ \ \& \ \ \text{Sacar}(<>, n) \equiv <>$$

usamos t_1

$$<> \ \& \ Sacar(<>, n) \equiv <>$$

usamos s_1

$$<> \ \ \& \ \ <> \equiv <>$$

usamos $\&_1$

$$<> \equiv <>$$

3.2.5. Probar el paso inductivo

$$P(a \bullet s)$$
$$(\forall n : nat)(\text{Tomar}(a \bullet s, n) \ \& \ \text{Sacar}(a \bullet s, n) \equiv a \bullet s)$$
$$\text{Tomar}(a \bullet s, n) \ \& \ \text{Sacar}(a \bullet s, n) \equiv a \bullet s$$

por t_2

$$(\textbf{if } n = 0 \textbf{ then } <> \textbf{ else } a \bullet \text{Tomar}(s, n - 1) \textbf{ fi}) \ \& \ \text{Sacar}(a \bullet s, n) \equiv a \bullet s$$

podemos meter el & dentro de cada rama del if (ver Anexo):

$$\textbf{if } n = 0 \textbf{ then } (<> \ \& \ \text{Sacar}(a \bullet s, n)) \textbf{ else } (a \bullet \text{Tomar}(s, n - 1)) \ \& \ \text{Sacar}(a \bullet s, n) \textbf{ fi} \equiv a \bullet s$$

aplicando s_2

```
a • s  ≡ if n = 0 then
           (<> & if n = 0 then (a • s) else Sacar(s, n-1) fi)
         else
           ((a • Tomar(s, n - 1)) & if n = 0 then <> else Sacar(s, n-1) fi)
         fi
```

aquí podemos ver que en la rama del **then** en el **if** principal, no tiene sentido preguntar nuevamente si $n = 0$, ya que si llegamos ahí era porque efectivamente valía la guarda, por lo cual, nos podemos quedar sólo con la parte **then** en el **if** interno (ver propiedad en el Anexo)

```
a • s  ≡ if n = 0 then
           (<> & (a • s))
         else
           ((a • Tomar(s, n - 1)) & if n = 0 then <> else Sacar(s, n-1) fi)
         fi
```

por $\&_1$:

a • s $\equiv$ **if** n = 0 **then**
(a • s)
else
((a • Tomar(s, n - 1)) & **if** n = 0 **then** <> **else** Sacar(s, n-1) **fi**)
fi

al contrario de lo que pasaba antes, ahora miramos la rama del **else**, y por lo tanto sabemos que vale $n \neq 0$, por lo cual del segundo **if** nos podemos quedar sólo con la parte del **else** (esto también se obtiene componiendo propiedades que aparecen en el Anexo):

a • s $\equiv$ **if** n = 0 **then** (a • s) **else** ((a • Tomar(s, n - 1)) & Sacar(s, n-1)) **fi**

aplicando ahora $\&_2$

a • s $\equiv$ **if** n = 0 **then** (a • s) **else** (a • (Tomar(s, n - 1) & Sacar(s, n-1))) **fi**

recordemos que la hipótesis inductiva es $P(s)$, y por lo tanto vale para todo posible segundo parámetro, inclusive $n - 1$,

a • s $\equiv$ **if** n = 0 **then** (a • s) **else** (a • s) **fi**

como ambas ramas del **if** desembocan en lo mismo, tenemos una vez más una propiedad que nos permite reducir simplemente

a • s $\equiv$ a • s

Es importante notar de este ejercicio lo útil que es tener las propiedades del **if** probadas previamente, ya que si no habría que hacer toda la consideración de casos dentro de esta demostración, ensuciando la misma.

4. Ejercicio 3: Diccionarios múltiples

4.1. Enunciado

Considerando la siguiente especificación:

TAD DICCIONARIO MÚLTIPLE

parámetros formales
géneros *clave*,*sig*

géneros diccmul(clave,sig)

exporta diccmul(clave,sig), generadores, observadores

igualdad observacional

$$(\forall d, d' : \text{diccmul}(clave, significado)) \left(d =_{\text{obs}} d' \iff \begin{pmatrix} (\forall c : clave)\ \text{sigsActuales}(c, d) =_{\text{obs}} \\ \text{sisActuales}(c, d') \wedge \\ \text{sisArcaicos}(c, d) =_{\text{obs}} \\ \text{sigsArcaicos}(c, d') \end{pmatrix} \right)$$

observadores básicos
sigsActuales : clave × diccmul(clave, significado) $\longrightarrow$ conj(sig)
sisArcaicos : clave × diccmul(clave, significado) $\longrightarrow$ conj(sig)

generadores
vacio : $\longrightarrow$ diccmul(clave, sig)
definir : clave c × sig s × diccmul(clave × significado) d $\longrightarrow$ diccmul(clave, sig) {s∉sisArcaicos(c,d)}
enDesuso : clave c × sig s × diccmul(clave × significado) d $\longrightarrow$ diccmul(clave, sig) {s∈sigsActuales(c,d)}

axiomas $\forall d$: diccmul(clave,sig), $\forall c, k$: clave, $\forall s, t$: sig
s_1) sigsActuales(c,vacio) $\equiv$ $\emptyset$
s_2) sigsActuales(c,definir(k,s,d)) $\equiv$ **if** c=k **then** Ag(s,sigsActuales(c,d)) **else** sigsActuales(c,d) **fi**
s_3) sigsActuales(c,enDesuso(k,s,d)) $\equiv$ **if** c=k **then** sigsActuales(c,d)-{s} **else** sigsActuales(c,d) **fi**
sa_1) sigsArcaicos(c,vacio) $\equiv$ $\emptyset$
sa_2) sigsArcaicos(c,definir(k,s,d)) $\equiv$ sigsActuales(c,d)

sa_3) sigsArcaicos(c,enDesuso(k,s,d)) $\equiv$ **if** c=k **then** Ag(s,sigsArcaicos(c,d)) **else** sigsArcaicos(c,d) **fi**

Fin TAD

Demuestre:

$$\forall c : \text{clave}, \forall d : \text{diccmul(clave, sig)}\ \text{sigsActuales}(c, d) \cap \text{sigsArcaicos}(c, d) \equiv \emptyset$$

4.1.1. Convencernos de que lo que queremos probar es cierto

Queda como ejercicio.

4.1.2. Plantear la propiedad como predicado unario

En este caso la propiedad era:
$\forall c : \text{clave}, \forall d : \text{diccmul(clave, sig)}\ \text{sigsActuales}(c, d) \cap \text{sigsArcaicos}(c, d) \equiv \emptyset$
De modo que el predicado resultante es:

$$P(d) = (\forall c : \text{clave})(\text{sigsActuales}(c, d) \cap \text{sigsArcaicos}(c, d) \equiv \emptyset)$$

4.1.3. Plantear el esquema de inducción

Tenemos un constructor base y dos constructores recursivos. Notemos que los generadores recursivos tienen restricciones, que hay que tener en cuenta. Es decir, cuando aplicamos definir no podemos dar cualquier significado, sino que tiene que ser un significado que no este en los arcaicos. Algo similar ocurre para enDesuso.

$$P(\text{vacio}) \wedge$$
$$\forall d : \text{diccmul(clave, sig)}(\underbrace{P(d)}_{HI} \Rightarrow \underbrace{(\forall k : \text{clave}, s : \text{sig}(s \notin \text{sigsArcaicos}(k, d) \Rightarrow P(\text{definir}(k, s, d))))}_{TI}) \wedge$$
$$\forall d : \text{diccmul(clave, sig)}(\underbrace{P(d)}_{HI} \Rightarrow \underbrace{(\forall k : \text{clave}, s : \text{sig}(s \in \text{sigsActuales}(k, d) \Rightarrow P(\text{enDesuso}(k, s, d))))}_{TI})$$

4.1.4. Probar el caso base

$$P(\text{vacio})$$
$$(\forall c : \text{clave})(\text{sigsActuales}(c, \text{vacio}) \cap \text{sigsArcaicos}(c, \text{vacio}) \equiv \emptyset)$$

Sacamos el cuantificador, pero no lo olvidamos, es decir no vamos a pedir nada sobre c

$$\text{sigsActuales}(c, \text{vacio}) \cap \text{sigsArcaicos}(c, \text{vacio}) \equiv \emptyset$$

por s_1

$$\emptyset \equiv \emptyset \cap \text{sigsArcaicos}(c, \text{vacio})$$

por sa_1

$$\emptyset \equiv \emptyset \cap \emptyset$$

por el axioma de intersección

$$\emptyset \equiv \emptyset$$

De esta forma probamos el caso base.

4.1.5. Probar los pasos inductivos

Probemos primero el paso inductivo de definir.
Tenemos:

$$P(d) \Rightarrow ((\forall k : \text{clave}, s : \text{sig})(s \notin \text{sigsArcaicos}(k, d) \Rightarrow P(\text{definir}(k, s, d))))$$

$P(d)$ la vamos a suponer como verdadera, es nuestra hipótesis inductiva, nos queda ver entonces que:

$$P((\forall k : \text{clave}, s : \text{sig}(s \notin \text{sigsArcaicos}(k, d) \Rightarrow P(\text{definir}(k, s, d))))$$

Por simplicidad sacamos los cuantificadores:

$$s \notin \text{sigsArcaicos}(k, d) \Rightarrow P(\text{definir}(k, s, d))$$

Si no se cumple el antecedente, y s está en los significados arcaicos, no hay nada que probar. Por eso vamos a considerar el caso donde vale $s \notin \text{sigsArcaicos}(k, d)$
Expandiendo $P(\text{definir}(k, s, d))$

$$(\forall c : \text{clave})(\text{sigsActuales}(c, \text{definir}(k, s, d)) \cap \text{sigsArcaicos}(c, \text{definir}(k, s, d)) \equiv \emptyset)$$

Sacanos el cuantificador por comodidad
$\emptyset \equiv \text{sigsActuales}(c, \text{definir}(k, s, d)) \cap \text{sigsArcaicos}(c, \text{definir}(k, s, d))$
por s_2,
$\emptyset \equiv$ (**if** $c = k$ **then** $\text{Ag}(s, \text{sigsActuales}(c, d))$ **else** $\text{sigsActuales}(c, d)$ **fi**) $\cap \text{sigsArcaicos}(c, \text{definir}(k, s, d))$
por sa_2,
$\emptyset \equiv$ (**if** $c = k$ **then** $\text{Ag}(s, \text{sigsActuales}(c, d))$ **else** $\text{sigsActuales}(c, d)$ **fi**) $\cap \text{sigsArcaicos}(c, d)$
Ahora vamos a separar en casos, o bien $c = k$ o bien son distintas. Es muy importante prestar atención cuando se separa en casos, hay que recordar que caso se está considerando y asegurarse que se consideren todos, es decir que no nos olvidemos de probar ninguno. Si hay un if sólo, esto es relativamente fácil, pero cuando empiezan a aparecer mas y la cantidad de casos aumenta hay que ser mas cuidadoso.
Supongamos primero que son distintos, entonces entramos por la rama del else:
$\emptyset \equiv$ (**if** c = k **then** Ag(s, sigsActuales(c, d)) **else** sigsActuales(c, d) **fi**) $\cap$ sigsArcaicos(c,d)
$\emptyset \equiv$ sigsActuales(c, d) $\cap$ sigsArcaicos(c,d)
Y esto sabemos que es verdadero, por hipótesis inductiva!
¿Qué pasa si eran iguales las claves? Entramos por la rama del then:
$\emptyset \equiv$ (**if** c = k **then** Ag(s, sigsActuales(c, d)) **else** sigsActuales(c, d) **fi**) $\cap$ sigsArcaicos(c,d)
$\emptyset \equiv$ Ag(s, sigsActuales(c, d))$\cap$ sigsArcaicos(c,d)
Podemos aplicar el axioma de la intersección:
$\emptyset \equiv$ **if** s $\in$ sigsArcaicos(c,d) **then**
Ag(s,sigsActuales(c, d) $\cap$ sigsArcaicos(c,d))
else
sigsActuales(c, d)$\cap$ sigsArcaicos(c,d)
fi
Para que se cumpla la restricción de definir, tiene que valer $s \notin \text{sigsArcaicos}(k, d)$ (lo vimos antes) y como $c = k$, vale $s \notin \text{sigsArcaicos}(c, d)$. Por esta razón, entramos por la rama del else:
$\emptyset \equiv$ sigsActuales(c, d) $\cap$ sigsArcaicos(c,d)
Y nuevamente, esto es cierto por HI.

Probemos ahora el paso inductivo para enDesuso:
$P(d) \Rightarrow (\forall k : \text{clave})(\forall s : \text{sig})(s \in \text{sigsActuales}(k, d) \Rightarrow P(\text{enDesuso}(k, s, d)))$
Nuevamente P(d) va a ser nuestra hipótesis inductiva, y nuevamente también tenemos una restricción sobre s. Vamos a suponer que la restricción sobre s vale, porque si no, no tenemos nada que probar.
Concentrémonos entonces en $P(\text{enDesuso}(k, s, d)))$

$$P(\text{enDesuso}(k, s, d))$$

$$(\forall c : \text{clave})\text{sigsActuales}(c, \text{enDesuso}(k, s, d)) \cap \text{sigsArcaicos}(c, \text{enDesuso}(k, s, d)) \equiv \emptyset$$

$\emptyset \equiv \text{sigsActuales}(c, \text{enDesuso}(k, s, d)) \cap \text{sigsArcaicos}(c, \text{enDesuso}(k, s, d))$
por s_3
$\emptyset \equiv$ (**if** $c = k$ **then** $\text{sigsActuales}(c, d) - \{s\}$ **else** $\text{sigsActuales}(c, d)$ **fi**) $\cap \text{sigsArcaicos}(c, \text{enDesuso}(k, s, d))$

Otra vez podemos separar en casos, según si $c = k$ o si no.

Si consideramos que $c \neq k$, entramos por la rama del else:

$\emptyset \equiv \text{sigsActuales}(c, d) \cap \text{sigsArcaicos}(c, \text{enDesuso}(k, s, d))$

Aplicamos sa_3

$\emptyset \equiv \text{sigsActuales}(c, d) \cap (\textbf{if } c = k \textbf{ then } \text{Ag}(s, \text{sigsArcaicos}(c, d)) \textbf{ else } \text{sigsArcaicos}(c, d) \textbf{ fi})$

Recordemos que estamos suponiendo que c es distinta a k, por lo tanto acá también nos vamos a la rama del else:

$\emptyset \equiv \text{sigsActuales}(c, d) \cap (\textbf{if } c = k \textbf{ then } \text{Ag}(s, \text{sigsArcaicos}(c, d)) \textbf{ else } \text{sigsArcaicos}(c, d) \textbf{ fi})$

$\emptyset \equiv \text{sigsActuales}(c, d) \cap \text{sigsArcaicos}(c, d)$

Y esto es cierto, por hipótesis inductiva

Ahora hagamos el caso en el que vale que $c = k$:

En este caso entramos por la rama del then:

$\emptyset \equiv (\textbf{if } c = k \textbf{ then } \text{sigsActuales}(c, d) - \{s\} \textbf{ else } \text{sigsActuales}(c, d) \textbf{ fi}) \cap \text{sigsArcaicos}(c, \text{enDesuso}(k, s, d))$

$\emptyset \equiv \text{sigsActuales}(c, d) - \{s\} \cap \text{sigsArcaicos}(c, \text{enDesuso}(k, s, d))$

por sa_3:

$\emptyset \equiv \text{sigsActuales}(c, d) - \{s\} \cap (\textbf{if } c = k \textbf{ then } \text{Ag}(s, \text{sigsArcaicos}(c, d)) \textbf{ else } \text{sigsArcaicos}(c, d) \textbf{ fi})$

Como suponemos que $c = k$:

$\emptyset \equiv \text{sigsActuales}(c, d) - \{s\} \cap \text{Ag}(s, \text{sigsArcaicos}(c, d))$

No tenemos ningún axioma para seguir, entonces hay que pensar. Mirando la expresión que nos quedo vemos que tiene sentido: Sabemos que $\text{sigsActuales}(c, d) \cap \text{sigsArcaicos}(c, d) \equiv \emptyset$ por HI, ademas s está en $\text{sigsActuales}(c, d)$, ya que $c = k$ y $s \in \text{sigsActuales}(k, d)$ era una restricción que le pedimos a s. Si bien s se agrega a $\text{sigsArcaicos}(c, d)$, se la quita de $\text{sigsActuales}(c, d)$ por lo cual la intersección no debería cambiar.

Lo que vamos a hacer es plantear un lema, o sea un resultado auxiliar que nos permita continuar con nuestra demostración. Luego probaremos que el lema es cierto, si no lo fuera nuestra demostración no tendría validez.

El lema que queremos es:

$$(\forall a, b : \text{conj}(\alpha), \forall e : \alpha)(a \cap b \equiv \emptyset \ \Rightarrow \ (a - \{e\} \cap \text{Ag}(e, b) \equiv \emptyset))$$

Aplicando el lema, ya tenemos probado el segundo paso inductivo.

Sólo falta probar el lema. Los pasos son los mismos, y ya nos convencimos de que anda, entonces pasemos a plantear el predicado unario. Hasta ahora siempre las propiedades tenían una única variable del tipo sobre el que hacíamos inducción. En este lema hay dos variables de tipo conjunto. ¿Sobre cuál trabajamos?

La respuesta a esa pregunta depende del conjunto de axiomas que tengamos, en este caso los de conjunto, suelen hacer inducción sobre el primer parámetro, por lo cual nos conviene plantear el predicado unario como función de a y no como función de b (Ejercicio: probar plantearlo como $P(b)$).

De acuerdo con esto, el predicado es:

$$P(a) = (\forall b : \text{conj}(\alpha), \forall e : \alpha)(a \cap b \equiv \emptyset \ \Rightarrow \ (a - \{e\} \cap \text{Ag}(e, b) \equiv \emptyset))$$

Planteamos el esquema de inducción:

$$P(\emptyset) \wedge (P(a) \ \Rightarrow \ (\forall e : \alpha) P(\text{Ag}(e, a)))$$

El caso base:

$$P(\emptyset)$$

$$(\forall b : \text{conj}(\alpha), \forall e : \alpha)(\emptyset \cap b \equiv \emptyset \ \Rightarrow \ (\emptyset - \{e\} \cap \text{Ag}(e, b) \equiv \emptyset))$$

El predicado es una implicación. Veamos que el antecedente es verdadero:

$$\emptyset \cap b \equiv \emptyset$$

Por el axioma $\cap_1$

$$\emptyset \equiv \emptyset$$

Vemos que el antecedente es siempre verdadero, por lo cual no aporta información.

Concentrémonos entonces en el consecuente:

$\emptyset \equiv \emptyset - \{e\} \cap \text{Ag}(e, b)$

Por el axioma $-\{\cdot\}_1$
$\emptyset \equiv \emptyset \cap \text{Ag}(e, b)$
Por $\cap_1$
$\emptyset \equiv \emptyset$
Ya tenemos el caso base.
Probemos ahora el paso inductivo

$$P(a) \Rightarrow (\forall k : \alpha) P(\text{Ag}(k, a))$$

$$P(\text{Ag}(k, a))$$
$$\text{Ag}(k, a) \cap b \equiv \emptyset \Rightarrow (\forall e : \alpha)(\text{Ag}(k, a) - \{e\} \cap \text{Ag}(e, b) \equiv \emptyset)$$

Estudiemos el antecedente, recordemos que nos va a interesar sólo el caso en el que es verdadero:
$\emptyset \equiv \text{Ag}(k, a) \cap b$
Por el axioma $\cap_2$
$\emptyset \equiv$ **if** $k \in b$ **then** $\text{Ag}(k, a \cap b)$ **else** $a \cap b$ **fi**
Si la guarda del if es verdadera, nunca puede ocurrir que $\text{Ag}(k, a) \cap b \equiv \emptyset$, ya que el resultado de la intersección tiene por lo menos un elemento (tiene a k). Entonces la guarda tiene que ser falsa. De acá vemos que tiene que ocurrir que $\neg k \in b$. Por otro lado como la guarda es falsa, vemos que $a \cap b \equiv \emptyset$
Vayamos ahora al consecuente:
$\emptyset \equiv \text{Ag}(k, a) - \{e\} \cap \text{Ag}(e, b)$
Por el axioma $-\{\cdot\}_2$
$\emptyset \equiv$ (**if** $k = e$ **then** $a - \{e\}$ **else** $\text{Ag}(k, a - \{e\})$ **fi**) $\cap \text{Ag}(e, b) \equiv \emptyset$
Separemos en casos:
Caso 1: $k = e$
Entramos por la rama del then:
$\emptyset \equiv$ (**if** $k = e$ **then** $a - \{e\}$ **else** $\text{Ag}(k, a - \{e\})$ **fi**) $\cap \text{Ag}(e, b)$
$\emptyset \equiv a - \{e\} \cap \text{Ag}(e, b)$
Por lo que vimos en el antecedente, $a \cap b \equiv \emptyset$, entonces por HI concluimos que esto es cierto.
Caso 2: $k \neq e$
Vamos a la rama del else:
$\emptyset \equiv \text{Ag}(k, a - \{e\}) \cap \text{Ag}(e, b)$
Por $\cap_2$
$\emptyset \equiv$ **if** $k \in \text{Ag}(e, b)$ **then** $\text{Ag}(k, a - \{e\} \cap \text{Ag}(e, b))$ **else** $a - \{e\} \cap \text{Ag}(e, b)$ **fi**
Por el axioma $\in_2$
$\emptyset \equiv$ **if** $k = e \vee k \in b$ **then** $\text{Ag}(k, a - \{e\} \cap \text{Ag}(e, b))$ **else** $a - \{e\} \cap \text{Ag}(e, b)$ **fi**
Ahora bien, estamos suponiendo que $k = e$ no vale, y vimos, cuando analizamos el antecedente, que $k \in b$ es falso. Entonces entramos por la rama del else:
$\emptyset \equiv a - \{e\} \cap \text{Ag}(e, b)$
Como vimos antes $a \cap b \equiv \emptyset$, aplicamos la HI y terminamos. Con esto probamos el lema. Al probarlo, terminamos la demostración de la propiedad.
Como ejercitación adicional, prueben de rehacer la demostración utilizando las propiedades de **if** que aparecen en el anexo en lugar de dividir por casos.

5. Ejercicio 4: polinomios

5.1. Enunciado

Dadas las siguientes operaciones sobre el TAD POLINOMIO de la práctica 1:

EsPolin0? : pol $\longrightarrow$ bool

e_1)	EsPolin0?(Cte(k))	$\equiv k = 0$
e_2)	EsPolin0?(X)	$\equiv$ false
e_3)	EsPolin0?($p_1 + p_2$)	$\equiv$ EsPolin0?(p_1) $\wedge$ EsPolin0?(p_2)
e_4)	EsPolin0?($p_1 \cdot p_2$)	$\equiv$ EsPolin0?(p_1) $\vee$ EsPolin0?(p_2)

derivado : pol $\longrightarrow$ pol

d_1)	derivado(Cte(k))	$\equiv$ cte(0)

$d_2)$ derivado(X) $\equiv$ cte(1)
$d_3)$ derivado($p_1 + p_2$) $\equiv$ derivado(p_1) + derivado(p_2)
$d_4)$ derivado($p_1 \cdot p_2$) $\equiv$ derivado(p_1) $\cdot$ p_2 + derivado(p_2) $\cdot$ p_1

grado : pol $\longrightarrow$ nat
$g_1)$ grado(Cte(k)) $\equiv$ 0
$g_2)$ grado(X) $\equiv$ 1
$g_3)$ grado($p_1 + p_2$) $\equiv$ máx (grado(p_1),grado(p_2))
$g_4)$ grado($p_1 \cdot p_2$) $\equiv$ **if** EsPolin0?(p_1) $\vee$ EsPolin0?(p_2) **then**
0
else
grado(p_1) + grado(p_2)
fi

Demostrar:

$$(\forall q : \text{pol})(\text{grado}(q) > 0) \Rightarrow (\text{grado}(\text{derivado}(q)) + 1 \equiv \text{grado}(q)))$$

5.2. Resolución

5.2.1. Convencernos de que lo que queremos probar es cierto

La propiedad que tenemos que probar nos dice que cuando derivamos un polinomio, si este no tenia grado 0, se obtiene un polinomio con un grado uno menor. Sabemos que esto es cierto de álgebra 1, y si miramos con cuidado los axiomas nos podemos convencer de que representan correctamente las reglas de derivación, cálculo de grado, etc. Adicionalmente, podríamos hacer algunos ejemplos concretos sobre el TAD, pero no lo haremos en este apunte.

5.2.2. Plantear la propiedad como predicado unario

$$P(q) = (\text{grado}(q) > 0) \Rightarrow (\text{grado}(\text{derivado}(q)) + 1 \equiv \text{grado}(q)))$$

5.2.3. Plantear el esquema de inducción

A diferencia de anteriormente, en este caso hay dos generadores no recursivos, por lo tanto hay dos casos base:

$$(\forall k : \text{nat})P(\text{cte}(k)) \text{ y } P(\text{X})$$

También son dos los generadores recursivos, por lo cual tenemos dos pasos inductivos

$$(\forall q_1, q_2 : \text{pol}) \underbrace{(P(q_1) \wedge P(q_2))}_{HI} \Rightarrow \underbrace{P(q_1 + q_2)}_{TI}$$

$$(\forall q_1, q_2 : \text{pol}) \underbrace{(P(q_1) \wedge P(q_2))}_{HI} \Rightarrow \underbrace{P(q_1 \cdot q_2)}_{TI}$$

Notemos como la hipótesis inductiva en este caso aplica para dos polinomios q_1 y q_2. El esquema queda entonces:

$$((\forall k : \text{nat})P(\text{cte}(k))) \wedge P(\text{X}) \wedge$$
$$((\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \Rightarrow P(q_1 + q_2)) \wedge ((\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \Rightarrow P(q_1 \cdot q_2))$$

5.2.4. Probar los casos base

Tenemos que probar la propiedad tanto para los polinomios constantes como para el polinomio X. Notemos que la propiedad es una implicación, por lo cual hay que prestar atención a que el antecedente sea verdadero, porque en el caso en el que el antecedente sea falso, no hay nada que probar.

Veamos el caso constante:

$$P(\text{cte}(k)) = (\text{grado}(\text{cte}(k)) > 0) \Rightarrow (\text{grado}(\text{derivado}(\text{cte}(k))) + 1 \equiv \text{grado}(\text{cte}(k))))$$

$$(grado(cte(k)) > 0) \Rightarrow (grado(derivado(cte(k))) + 1 \equiv grado(cte(k))))$$

Pero grado(cte(k)) $\equiv 0$ por g_1 y $0 \not> 0$, por lo tanto el antecedente es falso, luego toda la implicación es verdadera, no nos queda nada por probar $\ddot\smile$.

Ahora el caso polinomio X:

$$P(\text{X}) = (\text{grado(X)} > 0) \Rightarrow (\text{grado(derivado(X))} + 1 \equiv \text{grado(X)}))$$

En este caso por g_2, grado(X) $\equiv 1$ y $1 > 0$, por lo tanto el antecedente es verdadero, podemos olvidarnos de él y trabajar con el consecuente, así

$$(\text{grado}(X) > 0) \Rightarrow (\text{grado(derivado}(X)) + 1 \equiv \text{grado}(X)))$$

Por g_2,

$$(1 > 0) \Rightarrow (\text{grado(derivado}(X)) + 1 \equiv \text{grado}(X)))$$

$$\text{true} \Rightarrow (\text{grado(derivado}(X)) + 1 \equiv \text{grado}(X)))$$

$$\text{grado(derivado}(X)) + 1 \equiv \text{grado}(X)$$

Por d_2,

$$\text{grado(cte(1))} + 1 \equiv \text{grado}(X)$$

Por g_1,

$$0 + 1 \equiv \text{grado}(X)$$

$$1 \equiv \text{grado}(X)$$

Por g_2,

$$1 \equiv 1$$

Y esto es verdadero, por lo tanto probamos el caso base para el polinomio X.

5.2.5. Probar los pasos inductivos

Vamos a probar primero la propiedad para el caso de suma de polinomios.

El predicado nos queda:

$$P(q_1 + q_2) = (\text{grado}(q_1 + q_2) > 0) \Rightarrow (\text{grado(derivado}(q_1 + q_2)) + 1 \equiv \text{grado}(q_1 + q_2))$$

A diferencia de los casos anteriores, el antecedente de la implicación puede ser verdadero o falso, según que polinomios se sumen, por ejemplo si sumamos cte(3) + cte(4) vemos que el grado de la suma es 0 y por lo tanto el antecedente es falso, pero si sumamos dos polinomios X, el grado es uno y por lo tanto el antecedente es verdadero.

Como vimos antes, cuando el antecedente es falso no tenemos nada que hacer, así que podemos suponer que el antecedente es verdadero y seguir la demostración. Al suponer que el antecedente es verdadero, estamos suponiendo que q_1 y q_2 son polinomios tales que grado($q_1 + q_2$) > 0 que según el axioma g_3 es lo mismo que decir que máx(grado(q_1), grado(q_2)) > 0, es decir que por lo menos uno de los dos tiene un grado mayor que 0. Esto nos agrega información para continuar con la demostración.

OJO!, sabemos que vale por hipótesis inductiva $P(q_1)$ y $P(q_2)$, pero ambos predicados son implicaciones, así que no podemos asumir que vale el antecedente para ellos, es decir que no podemos asumir que ambos tienen grado mayor a 0. Si queremos usar el consecuente de $P(q_1)$, tendremos que demostrar su antecedente.

Centrándonos entonces en el consecuente, tenemos que probar que:

$$\text{grado(derivado}(q_1 + q_2)) + 1 \equiv \text{grado}(q_1 + q_2)$$

Por d_3,

$$\text{grado(derivado}(q_1) + \text{derivado}(q_2)) + 1 \equiv \text{grado}(q_1 + q_2)$$

por g_3,

$$\text{máx(grado(derivado}(q_1)), \text{grado(derivado}(q_2))) + 1 \equiv \text{grado}(q_1 + q_2)$$

por g_3, pero en el lado derecho,

$$\text{máx(grado(derivado}(q_1)), \text{grado(derivado}(q_2))) + 1 \equiv \text{máx(grado}(q_1), \text{grado}(q_2))$$

Ahora podemos continuar suponiendo que máx(grado(q_1), grado(q_2)) ≡ grado(q_1) y luego lo mismo pero suponiendo que máx(grado(q_1), grado(q_2)) ≡ grado(q_2). Dado que ambas suposiciones tienen como consecuencia enunciados equivalentes (tarea: corroborarlo), continuamos con uno sólo de los caminos y el otro se demuestra analogámente. Entonces, suponemos que máx(grado(q_1), grado(q_2)) ≡ grado(q_1).

$$\text{máx}(\text{grado}(\text{derivado}(q_1)), \text{grado}(\text{derivado}(q_2))) + 1 \equiv \text{máx}(\text{grado}(q_1), \text{grado}(q_2))$$

$$\text{máx}(\text{grado}(\text{derivado}(q_1)), \text{grado}(\text{derivado}(q_2))) + 1 \equiv \text{grado}(q_1)$$

Por lo que vimos cuando analizamos el antecedente, sabemos que máx(grado(q_1), grado(q_2)) > 0, por lo tanto grado(q_1) > 0. Entonces, usando la HI para q_1, resulta que grado(q_1) ≡ grado(derivado(q_1)) + 1.

Usando eso,

$$\text{máx}(\text{grado}(\text{derivado}(q_1)), \text{grado}(\text{derivado}(q_2))) + 1 \equiv \text{grado}(\text{derivado}(q_1)) + 1$$

$$\text{máx}(\text{grado}(\text{derivado}(q_1)), \text{grado}(\text{derivado}(q_2))) \equiv \text{grado}(\text{derivado}(q_1))$$

Acá nos trabamos un poco, porque no podemos saber nada de grado(derivado(q_2))

¿Podría ser que grado(derivado(q_2)) > grado(derivado(q_1)? Si bien intuitivamente nos parece que no, no lo podemos asumir. Lo conveniente en este caso es plantear un lema auxiliar y continuar con la demostración.

¿Qué lema? Bueno, hay varios lemas que se pueden pedir en este caso y que nos ayudarían a seguir. Propongo uno, pero hay otros. La idea es la siguiente, intuitivamente nos parece que grado(derivado(q_2)) > grado(derivado(q_1)) no puede pasar porque sino grado(q_2) > grado(q_1) y eso es contrario a lo que suponíamos. Entonces un lema que nos alcanza es el siguiente:

Lema 1

$$(\forall q : \text{pol})\text{grado}(q) \geq \text{grado}(\text{derivado}(q))$$

Este lema nos alcanza por lo siguiente: Si grado(derivado(q_2)) > grado(derivado(q_1)),
vale que grado(derivado(q_2)) > 0,
pero si grado(derivado(q_2)) > 0,
por el lema grado(q_2) > 0,
pero entonces por nuestra HI, grado(q_2) ≡ grado(derivado(q_2)) + 1.

Por otro lado, estábamos suponiendo que máx(grado(q_1), grado(q_2)) ≡ grado(q_1),
por lo cual, grado(q_1) ≥ grado(q_2),
o lo que es lo mismo usando las HI, grado(derivado(q_1)) + 1 ≥ grado(derivado(q_2)) + 1.

Pero esto es contradictorio con grado(derivado(q_2)) > grado(derivado(q_1))

Entonces podemos continuar con la demostración,

$$\text{máx}(\text{grado}(\text{derivado}(q_1)), \text{grado}(\text{derivado}(q_2))) \equiv \text{grado}(\text{derivado}(q_1))$$

$$\text{grado}(\text{derivado}(q_1)) \equiv \text{grado}(\text{derivado}(q_1))$$

Dejemos la prueba del lema para mas adelante, y sigamos con el paso inductivo para la multiplicación de polinomios.

La propiedad en este caso es:

$$P(q_1 \cdot q_2) = (\text{grado}(q_1 \cdot q_2) > 0) \;\Rightarrow\; (\text{grado}(\text{derivado}(q_1 \cdot q_2)) + 1 \equiv \text{grado}(q_1 \cdot q_2))$$

Al igual que en el caso anterior, ahora también tenemos que el antecedente puede ser verdadero en algunos casos, y falso en otros. Nuevamente vamos a suponer que el antecedente es verdadero, ver que información obtenemos de eso y continuar la demostración.

$$\text{grado}(q_1 \cdot q_2) > 0$$

Por g_4,

(**if** EsPolin0?(q_1) ∨ EsPolin0?(q_2) **then** 0 **else** grado(q_1) + grado(q_2) **fi**)> 0

La comparación se puede "meter" adentro del if, por lo cual tenemos:

if EsPolin0?(q_1) ∨ EsPolin0?(q_2) **then** 0 > 0 **else** grado(q_1) + grado(q_2)> 0 **fi**

if EsPolin0?(q_1) ∨ EsPolin0?(q_2) **then** false **else** grado(q_1) + grado(q_2)> 0 **fi**

Si queremos que esto sea verdadero, necesitamos que el **if** entre por el lado del **else**, es decir, que la guarda sea falsa. De esto podemos deducir que vale:

$$\neg\text{EsPolin0?}(q_1) \wedge \neg\text{EsPolin0?}(q_2) \wedge \text{grado}(q_1) + \text{grado}(q_2) > 0$$

Del hecho de que

$$\text{grado}(q_1) + \text{grado}(q_2) > 0$$

podemos ver que alguno de los dos grados es mayor que 0. Notar que sólo hicimos razonamientos no tan formales sobre aritmética de naturales y de expresiones booleanas, nunca sobre lo que estamos intentando demostrar sobre polinomios.

Volvamos entonces al consecuente:

$$\text{grado}(\text{derivado}(q_1 \cdot q_2)) + 1 \equiv \text{grado}(q_1 \cdot q_2)$$

Usando d_4,

$$\text{grado}(\text{derivado}(q_1) \cdot q_2 + \text{derivado}(q_2) \cdot q_1) + 1 \equiv \text{grado}(q_1 \cdot q_2)$$

usando g_3,

$$\text{máx}(\text{grado}(\text{derivado}(q_1) \cdot q_2), \text{grado}(\text{derivado}(q_2) \cdot q_1)) + 1 \equiv \text{grado}(q_1 \cdot q_2)$$

usando g_4 en el lado derecho,

máx(grado(derivado(q_1) · q_2),grado(derivado(q_2) · q_1))+1 ≡ **if** EsPolin0?(q_1) ∨ EsPolin0?(q_2) **then**
0
else
grado(q_1) + grado(q_2)
fi

Como asumimos que ¬EsPolin0?(q_1) ∧ ¬EsPolin0?(q_2)

$$\text{máx}(\text{grado}(\text{derivado}(q_1) \cdot q_2), \text{grado}(\text{derivado}(q_2) \cdot q_1)) + 1 \equiv \text{grado}(q_1) + \text{grado}(q_2)$$

Vimos antes también que uno de los polinomios q_1 y $q_2$tiene grado mayor a 0. Sin perder generalidad (como hicimos antes con los casos análogos) supongamos que es q_1.

De q_2, sólo sabemos que no es el polinomio 0, pero nada mas. Acá podríamos volver a usar un lema, o podemos separar en casos, ¿En qué casos? Bueno, lo que nos molesta es que no sabemos que pasa con el grado de q_2, entonces pensemos que pasa si su grado es 0 y que pasa si su grado es mayor que 0.

¿Qué pasa si grado(q_2) ≡ 0?

Por el lema que vimos antes, sabemos que grado(derivado(q_2)) ≤ grado(q_2), entonces no queda otra que grado(derivado(q_2)) ≡ 0

Lo que tenemos que probar era:

$$\text{máx}(\text{grado}(\text{derivado}(q_1) \cdot q_2), \text{grado}(\text{derivado}(q_2) \cdot q_1)) + 1 \equiv \text{grado}(q_1) + \text{grado}(q_2)$$

Estudiemos grado(derivado(q_1) · q_2), por g_4

if EsPolin0?(derivado(q_1)) ∨ EsPolin0?(q_2) **then** 0 **else** (grado(derivado(q_1)) + grado(q_2)) **fi**

pero el grado de q_2 es 0, entonces queda

if EsPolin0?(derivado(q_1)) ∨ EsPolin0?(q_2) **then** 0 **else** grado(derivado(q_1)) **fi**

Por otro lado, estudiemos grado(derivado(q_2) · q_1)

if EsPolin0?(derivado(q_2)) ∨ EsPolin0?(q_1) **then** 0 **else** (grado(derivado(q_2)) + grado(q_1)) **fi**

Pero grado(derivado(q_2)) ≡ 0, asi que queda

if EsPolin0?(derivado(q_2)) ∨ EsPolin0?(q_1) **then** 0 **else** grado(q_1) **fi**

Por otro lado, propongo el siguiente lema:

Lema 2

$$(\forall q : \text{pol})\text{grado}(q) \equiv 0 \;\Rightarrow\; \text{EsPolin0?}(\text{derivado}(q))$$

De alguna forma este lema nos está diciendo que todos los polinomios de grado 0, al derivarse dan como resultado el polinomio 0, esto tiene sentido porque todos los polinomios de grado 0 en verdad son constantes.

Aceptando el nuevo lema, que demostraremos luego, resulta que:

if EsPolin0?(derivado(q_2)) ∨ EsPolin0?(q_1) **then** 0 **else** grado(q_1) **fi**

if true **then** 0 **else** grado(q_1) **fi** ≡ 0

Por otra parte teníamos, **if** EsPolin0?(derivado(q_1)) ∨ EsPolin0?(q_2) **then** 0 **else** grado(derivado(q_1)) **fi**

Volvemos a estar trabados, por eso propongo un nuevo lema:

Lema 3

$$(\forall q : \text{pol})\text{grado}(q) > 0 \;\Rightarrow\; \neg\text{EsPolin0?}(\text{derivado}(q))$$

Este lema nos está diciendo que si tenemos un polinomio de grado mayor a 0, al derivarlo no vamos a obtener el polinomio nulo.

Podemos utilizar el nuevo lema,
if EsPolin0?(derivado(q_1)) $\vee$ EsPolin0?(q_2) **then** 0 **else** grado(derivado(q_1)) **fi**
if false $\vee$ EsPolin0?(q_2) **then** 0 **else** grado(derivado(q_1)) **fi**
if EsPolin0?(q_2) **then** 0 **else** grado(derivado(q_1)) **fi**
Cuando analizamos el antecedente, vimos que EsPolin0?(q_2) era falso, entonces,
if EsPolin0?(q_2) **then** 0 **else** grado(derivado(q_1)) **fi**
if false **then** 0 **else** grado(derivado(q_1)) **fi** $\equiv$ derivado(q_1))
reemplacemos las definiciones de grado de la derivada que vimos por separado en lo que queríamos demostrar:

$$\text{máx}(\text{grado}(\text{derivado}(q_1) \cdot q_2), \text{grado}(\text{derivado}(q_2) \cdot q_1)) + 1 \equiv \text{grado}(q_1) + \text{grado}(q_2)$$

$$\text{máx}(\text{derivado}(q_1), 0) + 1 \equiv \text{grado}(q_1) + \text{grado}(q_2)$$

recordemos que grado(q_2) $\equiv 0$

$$\text{máx}(\text{derivado}(q_1), 0) + 1 \equiv \text{grado}(q_1)$$

$$\text{derivado}(q_1) + 1 \equiv \text{grado}(q_1)$$

Y esto vale por la HI aplicada a q_1.
¿Qué pasa si grado(q_2) > 0?
Lo que tenemos que probar era:

$$\text{máx}(\text{grado}(\text{derivado}(q_1) \cdot q_2), \text{grado}(\text{derivado}(q_2) \cdot q_1)) + 1 \equiv \text{grado}(q_1) + \text{grado}(q_2)$$

Estudiemos grado(derivado(q_1) $\cdot$ q_2), por g_4,
if EsPolin0?(derivado(q_1)) $\vee$ EsPolin0?(q_2) **then** 0 **else** (grado(derivado(q_1)) + grado(q_2)) **fi**
Usando el lema 3, tenemos que EsPolin0?(derivado(q_1)) $\equiv$ false, además, por lo que vimos del antecedente, resulta que EsPolin0?(q_2) $\equiv$ false, por lo tanto:
if EsPolin0?(derivado(q_1)) $\vee$ EsPolin0?(q_2) **then** 0 **else** (grado(derivado(q_1)) + grado(q_2)) **fi**
if false $\vee$ false **then** 0 **else** (grado(derivado(q_1)) + grado(q_2)) **fi**

$$\text{grado}(\text{derivado}(q_1)) + \text{grado}(q_2)$$

Si estudiamos grado(derivado(q_2) $\cdot$ q_1), llegamos de forma análoga a grado(derivado(q_2)) + grado(q_1)
Entonces,

$$\text{máx}(\text{grado}(\text{derivado}(q_1) \cdot q_2), \text{grado}(\text{derivado}(q_2) \cdot q_1)) + 1 \equiv \text{grado}(q_1) + \text{grado}(q_2))$$

$$\text{máx}(\text{grado}(\text{derivado}(q_1)) + \text{grado}(q_2)), \text{grado}(\text{derivado}(q_2)) + \text{grado}(q_1))) + 1 \equiv \text{grado}(q_1) + \text{grado}(q_2)$$

Sin perder generalidad, podemos suponer que grado(derivado(q_1)) + grado(q_2)) es el máximo. Entonces,

$$\text{grado}(\text{derivado}(q_1)) + \text{grado}(q_2) + 1 \equiv \text{grado}(q_1) + \text{grado}(q_2)$$

$$\text{grado}(\text{derivado}(q_1)) + 1 \equiv \text{grado}(q_1)$$

Y esto es cierto por HI.

5.2.6. Lemas

Aclaración: Para la demostración de los lemas se va a omitir el planteo del esquema de inducción
Lema 1

$$(\forall q : \text{pol})\text{grado}(q) \geq \text{grado}(\text{derivado}(q))$$

Predicado unario:

$$P(q) = \text{grado}(q) \geq \text{grado}(\text{derivado}(q))$$

Casos Base:

- $P(\text{cte}(k)) = \text{grado}(\text{cte}(k)) \geq \text{grado}(\text{derivado}(\text{cte}(k)))$.

  Por g_1

  $$0 \geq \text{grado}(\text{derivado}(\text{cte}(k)))$$

  por d_1

  $$0 \geq \text{grado}(\text{cte}(0))$$

  por g_1

  $$0 \geq 0$$

- $P(X) = \text{grado}(X) \geq \text{grado}(\text{derivado}(X))$

  Por g_2

  $$1 \geq \text{grado}(\text{derivado}(X))$$

  por d_2

  $$1 \geq \text{grado}(\text{cte}(1))$$

  por g_1

  $$1 \geq 0$$

Pasos inductivos

- $(\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \Rightarrow P(q_1 + q_2) = \text{grado}(q_1 + q_2) \geq \text{grado}(\text{derivado}(q_1 + q_2))$

  Por g_3,

  $$\text{máx}(\text{grado}(q_1) + \text{grado}(q_2)) \geq \text{grado}(\text{derivado}(q_1 + q_2))$$

  por d_3,

  $$\text{máx}(\text{grado}(q_1), \text{grado}(q_2)) \geq \text{grado}(\text{derivado}(q_1) + \text{derivado}(q_2))$$

  por g_3,

  $$\text{máx}(\text{grado}(q_1), \text{grado}(q_2)) \geq \text{máx}(\text{grado}(\text{derivado}(q_1)), \text{grado}(\text{derivado}(q_2)))$$

  por HI y monotonicidad de máx respecto de $\geq$,

  $$\text{máx}(\text{grado}(\text{derivado}(q_1)), \text{grado}(\text{derivado}(q_2))) \geq \text{máx}(\text{grado}(\text{derivado}(q_1)), \text{grado}(\text{derivado}(q_2)))$$

- $(\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \Rightarrow P(q_1 \cdot q_2) = \text{grado}(q_2 \cdot q_2) \geq \text{grado}(\text{derivado}(q_2 \cdot q_2))$

  Por g_4,

  if EsPolin0?$(q_1) \vee$ EsPolin0?(q_2) **then** 0 **else** grado(q_1) + grado(q_2) **fi** $\geq$ grado(derivado$(q_2 \cdot q_2)$)

  por d_4,

  if EsPolin0?$(q_1) \vee$ EsPolin0?(q_2) **then** 0 **else** grado(q_1) + grado(q_2) **fi** $\geq$ grado(derivado$(q_1)\cdot q_2$+derivado$(q_2)\cdot q_1$))

  por g_3,

  if EsPolin0?$(q_1) \vee$ EsPolin0?(q_2) **then** 0 **else**
  grado(q_1) + grado(q_2) **fi** $\geq$ máx(grado(derivado$(q_1) \cdot q_2$), grado(derivado$(q_2) \cdot q_1$))

  Vamos a partir en casos:

  caso 1: EsPolin0?$(q_1) \vee$ EsPolin0?$(q_2) \equiv$ true

  Sin perdida de generalidad, podemos suponer que EsPolin0?$(q_1) \equiv$ true

  if EsPolin0?$(q_1) \vee$ EsPolin0?(q_2) **then** 0 **else**
  grado(q_1) + grado(q_2) **fi** $\geq$ máx(grado(derivado$(q_1) \cdot q_2$), grado(derivado$(q_2) \cdot q_1$))

  0 $\geq$ máx(grado(derivado$(q_1) \cdot q_2$), grado(derivado$(q_2) \cdot q_1$))

  Para poder seguir voy a plantear un nuevo lema:

  Lema 4

  $$(\forall q : \text{pol})\text{EsPolin0?}(q) \Rightarrow \text{grado}(q) \equiv 0$$

  Usando el lema 4, vemos que grado$(q_1) \equiv 0$, usando esto mas el lema 2, resulta que vale EsPolin0?(derivado$(q_1)) \equiv$ true.

  Luego operando resulta que,

  $$0 \geq \text{máx}(\text{grado}(\text{derivado}(q_1) \cdot q_2), \text{grado}(\text{derivado}(q_2) \cdot q_1))$$

  Como q_1 y derivado(q_1) son el polinomio nulo, por d_4,

  $$0 \geq \text{máx}(0, 0)$$

  $$0 \geq 0$$

  caso 2: EsPolin0?$(q_1) \vee$ EsPolin0?$(q_2) \equiv$ false

Esto quiere decir que EsPolin0?$(q_1) \equiv$ false y EsPolin0?$(q_2) \equiv$ false.

Entonces, de lo que teníamos,

if EsPolin0?$(q_1) \vee$ EsPolin0?(q_2) **then** 0 **else**
grado(q_1) + grado(q_2) **fi** $\geq$ máx(grado(derivado$(q_1) \cdot q_2$), grado(derivado$(q_2) \cdot q_1$))

Nos queda,

$$\text{grado}(q_1) + \text{grado}(q_2) \geq \text{máx}(\text{grado}(\text{derivado}(q_1) \cdot q_2), \text{grado}(\text{derivado}(q_2) \cdot q_1))$$

Ahora, si aplicamos g_4 nos quedan 2 posibilidades. Si ninguno de los derivados es nulo obtendremos

$$\text{grado}(q_1) + \text{grado}(q_2) \geq \text{máx}(\text{derivado}(q_1) + \text{grado}(q_2), \text{grado}(\text{derivado}(q_2)) + \text{grado}(q_1)))$$

y podemos terminarlo por HI, ya que el lado izquierda resulta mayor o igual a ambos parámetros del máx.

Si algun derivado es nulo, sin pérdida de generalidad supongamos que derivado(q_1) lo es, y obtenemos, también con g_4

$$\text{grado}(q_1) + \text{grado}(q_2) \geq \text{máx}(0, \text{grado}(\text{derivado}(q_2)) + \text{grado}(q_1)))$$

que también podemos terminarlo por HI.

Lema 2

$$(\forall q : \text{pol})\text{grado}(q) \equiv 0 \ \Rightarrow \ \text{EsPolin0?}(\text{derivado}(q))$$

Predicado unario:

$$P(q) = \text{grado}(q) \equiv 0 \ \Rightarrow \ \text{EsPolin0?}(\text{derivado}(q))$$

Casos Base:

- $P(\text{cte}(k)) = \text{grado}(\text{cte}(k)) \equiv 0 \ \Rightarrow \ \text{EsPolin0?}(\text{derivado}(\text{cte}(k)))$

  Por g_1,

  $$0 \equiv 0 \ \Rightarrow \ \text{EsPolin0?}(\text{derivado}(\text{cte}(k)))$$
  $$\text{EsPolin0?}(\text{derivado}(\text{cte}(k)))$$

  por d_1,

  $$\text{EsPolin0?}(\text{cte}(0))$$

  por e_1

  $$0 = 0$$

- $P(X) = \text{grado}(X) \equiv 0 \ \Rightarrow \ \text{EsPolin0?}(\text{derivado}(X))$

  Por g_2,

  $$1 \equiv 0 \ \Rightarrow \ \text{EsPolin0?}(\text{derivado}(X))$$

  Queda probado, porque el antecedente es siempre falso.

Pasos inductivos

- $(\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \ \Rightarrow \ P(q_1 + q_2) \ = \ \text{grado}(q_1 + q_2) \equiv 0 \ \Rightarrow \ \text{EsPolin0?}(\text{derivado}(q_1 + q_2))$

  Por g_3,

  $$\text{máx}(\text{grado}(q_1), \text{grado}(q_2)) \equiv 0 \ \Rightarrow \ \text{EsPolin0?}(\text{derivado}(q_1 + q_2))$$

  Si nos centramos en el caso que nos importa (cuando vale el antecedente) vemos que tiene que valer que: grado$(q_1) =$ grado$(q_2) = 0$.

  $$\text{EsPolin0?}(\text{derivado}(q_1 + q_2))$$

  Por d_3

  $$\text{EsPolin0?}(\text{derivado}(q_1) + \text{derivado}(q_2))$$

  Por e_3

  $$\text{EsPolin0?}(\text{derivado}(q_1)) \wedge \text{EsPolin0?}(\text{derivado}(q_2))$$

  Y como vimos que grado$(q_1) =$ grado$(q_2) = 0$, por HI, esto es verdadero.

- $(\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \Rightarrow P(q_1 \cdot q_2) = \text{grado}(q_1 \cdot q_2) \equiv 0 \Rightarrow \text{EsPolin0?}(\text{derivado}(q_1 \cdot q_2))$

  Mirando el antecedente, por g_4,

  if EsPolin0?$(q_1) \vee$ EsPolin0?(q_2) **then** 0 **else** grado(q_1) + grado(q_2) **fi** $\equiv 0$

  Esto puede ser verdadero de dos formas: o bien alguno de los dos polinomios es el polinomio 0, o ninguno de los dos es el polinomio 0, pero ambos tienen grado 0.

  caso 1: Un polinomio es nulo. Sin pérdida de generalidad, EsPolin0?$(q_1) \equiv$ true

  El consecuente era:

  $$\text{EsPolin0?}(\text{derivado}(q_1 \cdot q_2))$$

  por d_4,

  $$\text{EsPolin0?}(\text{derivado}(q_1) \cdot q_2 + \text{derivado}(q_2) \cdot q_1)$$

  por e_3,

  $$\text{EsPolin0?}(\text{derivado}(q_1) \cdot q_2) \wedge \text{EsPolin0?}(\text{derivado}(q_2) \cdot q_1)$$

  por e_4,

  $$(\text{EsPolin0?}(\text{derivado}(q_1)) \vee \text{EsPolin0?}(q_2)) \wedge \text{EsPolin0?}(\text{derivado}(q_2) \cdot q_1)$$

  Estamos suponiendo que vale EsPolin0?$(q_1) \equiv$ true, entonces por el lema 4, vemos que el grado de q_1 es 0, luego por HI vale que EsPolin0?$(\text{derivado}(q_1)) \equiv true$, luego

  $$\text{true} \wedge \text{EsPolin0?}(\text{derivado}(q_2) \cdot q_1)$$

  por e_4,

  $$\text{EsPolin0?}(\text{derivado}(q_2)) \vee \text{EsPolin0?}(q_1)$$

  Y como estabamos suponiendo que EsPolin0?$(q_1) \equiv$ true, probamos este caso.

  Caso 2: EsPolin0?$(q_1) \equiv$ EsPolin0?$(q_2) \equiv false \wedge \text{grado}(q_1) = \text{grado}(q_2) = 0$

  $$\text{EsPolin0?}(\text{derivado}(q_1 \cdot q_2))$$

  por d_4, e_3 y e_4,

  $$(\text{EsPolin0?}(\text{derivado}(q_1)) \vee \text{EsPolin0?}(q_2)) \wedge (\text{EsPolin0?}(\text{derivado}(q_2)) \vee \text{EsPolin0?}(q_1))$$

  Como grado$(q_1) \equiv$ grado$(q_2) \equiv 0$, por HI EsPolin0?$(\text{derivado}(q_2)) \equiv$ EsPolin0?$(\text{derivado}(q_2)) \equiv true$, luego probamos este caso también. Por lo tanto probamos el lema 2.

Lema 3

$$(\forall q : \text{pol})\text{grado}(q) > 0 \Rightarrow \neg\text{EsPolin0?}(\text{derivado}(q))$$

Predicado unario:

$$P(q) = \text{grado}(q) > 0 \Rightarrow \neg\text{EsPolin0?}(\text{derivado}(q))$$

Casos Base:

- $P(\text{cte}(k)) = \text{grado}(\text{cte}(k)) > 0 \Rightarrow \neg\text{EsPolin0?}(\text{derivado}(\text{cte}(k)))$

  por g_1,

  $$0 > 0 \Rightarrow \neg\text{EsPolin0?}(\text{derivado}(\text{cte}(k)))$$

  Luego, la implicación es verdadera por ser falso el antecedente

- $P(X) = \text{grado}(X) > 0 \Rightarrow \neg\text{EsPolin0?}(\text{derivado}(X))$

  Por g_1 vemos que el antecedente es siempre verdadero. Debemos entonces ver entonces que el consecuente es verdadero

  $$\neg\text{EsPolin0?}(\text{derivado}(X))$$

  por d_2,

  $$\neg\text{EsPolin0?}(\text{cte}(1))$$

  por e_1,

  $$\neg 1 = 0?$$

  $$\text{true}$$

Pasos inductivos

- $(\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \Rightarrow P(q_1 + q_2) = \text{grado}(q_1 + q_2) > 0 \Rightarrow \neg\text{EsPolin0?}(\text{derivado}(q_1 + q_2))$

  Vamos a considerar el caso donde el antecedente es verdadero. Como ya vimos antes, si $\text{grado}(q_1 + q_2) > 0$ vale que alguno de los dos tiene grado mayor a 0, sin perdida de generalidad podemos decir que es q_1

  $$\neg\text{EsPolin0?}(\text{derivado}(q_1 + q_2))$$

  por d_3,

  $$\neg\text{EsPolin0?}(\text{derivado}(q_1) + \text{derivado}(q_2))$$

  por e_3,

  $$\neg(\text{EsPolin0?}(\text{derivado}(q_1)) \wedge \text{EsPolin0?}(\text{derivado}(q_2)))$$

  Como dijimos que $\text{grado}(q_1) > 0$, aplicamos la HI y vemos que $\text{EsPolin0?}(\text{derivado}(q_1)) \equiv \text{false}$.

  Por lo tanto,

  $$\neg(\text{EsPolin0?}(\text{derivado}(q_1)) \wedge \text{EsPolin0?}(\text{derivado}(q_2)))$$

  $$\neg(\text{false} \wedge \text{EsPolin0?}(\text{derivado}(q_2)))$$

  $$\neg\text{false}$$

  $$\text{true}$$

- $(\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \Rightarrow P(q_2 \cdot q_2)\text{grado}(q_1 \cdot q_2) > 0 \Rightarrow \neg\text{EsPolin0?}(\text{derivado}(q_2 \cdot q_2))$

  Nuevamente, nos interesa el caso donde el antecedente es verdadero, por lo cual $\text{grado}(q_1 \cdot q_2) > 0$, entonces vimos antes que se puede deducir que

  $$\neg\text{EsPolin0?}(q_1) \wedge \neg\text{EsPolin0?}(q_2) \wedge \text{grado}(q_1) + \text{grado}(q_2) > 0$$

  sin pérdida de generalidad podemos considerar que $\text{grado}(q_1) > 0$

  $$\neg\text{EsPolin0?}(\text{derivado}(q_2 \cdot q_2))$$

  por d_4,

  $$\neg\text{EsPolin0?}(\text{derivado}(q_1) \cdot q_2 + \text{derivado}(q_2) \cdot q_1)$$

  por e_3,

  $$\neg(\text{EsPolin0?}(\text{derivado}(q_1) \cdot q_2) \wedge \text{EsPolin0?}(\text{derivado}(q_2) \cdot q_1))$$

  por e_4,

  $$\neg((\text{EsPolin0?}(\text{derivado}(q_1)) \vee \text{EsPolin0?}(q_2)) \wedge \text{EsPolin0?}(\text{derivado}(q_2) \cdot q_1))$$

  Por el antecedente sabemos que $\text{EsPolin0?}(q_2) \equiv false$, y por hipótesis inductiva sobre q_1, sabemos que vale $\neg\text{EsPolin0?}(\text{derivado}(q_1))$, por lo cual tenemos

  $$\neg(((\text{EsPolin0?}(\text{derivado}(q_1)) \vee \text{EsPolin0?}(q_2)) \wedge \text{EsPolin0?}(\text{derivado}(q_2) \cdot q_1))$$

  $$\neg((\text{false} \vee \text{false}) \wedge \text{EsPolin0?}(\text{derivado}(q_2) \cdot q_1))$$

  $$\neg(\text{false} \wedge \text{EsPolin0?}(\text{derivado}(q_2) \cdot q_1))$$

  $$\neg\text{false}$$

  $$\text{true}$$

  Con esto probamos el lema 3. Notar que ademas el contrareciproco del lema, nos dice que si el derivado de un polinomio es el polinomio 0, entonces el polinomio original tiene grado 0.

Lema 4

$$(\forall q : \text{pol})\text{EsPolin0?}(q) \Rightarrow \text{grado}(q) \equiv 0$$

Predicado unario:

$$P(q) = \text{EsPolin0?}(q) \Rightarrow \text{grado}(q) \equiv 0$$

Casos base

- $P(\text{cte}(k)) = \text{EsPolin0?}(\text{cte}(k)) \Rightarrow \text{grado}(\text{cte}(k)) \equiv 0$

  Por g_1, el consecuente es siempre verdadero, con lo cual la implicación es verdadera.

- $P(X) = \text{EsPolin0?}(X) \Rightarrow \text{grado}(X) \equiv 0$

  Por e_2, que el antecedente es siempre falso, con lo cual la implicación es veradera.

Pasos inductivos

- $(\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \Rightarrow P(q_1 + q_2) = \text{EsPolin0?}(q_1 + q_2) \Rightarrow \text{grado}(q_1 + q_2) \equiv 0$

  Si vale $\text{EsPolin0?}(q_1 + q_2)$, resulta por e_3

  $$\text{EsPolin0?}(q_1) \wedge \text{EsPolin0?}(q_2)$$

  mirando el consecuente,

  $$\text{grado}(q_1 + q_2) \equiv 0$$

  por g_3,

  $$\text{máx}(\text{grado}(q_1), \text{grado}(q_2)) \equiv 0$$

  usando HI, vemos que esto vale.

- $(\forall q_1, q_2 : \text{pol})(P(q_1) \wedge P(q_2)) \Rightarrow P(q_1 \cdot q_2) = \text{EsPolin0?}(q_1 \cdot q_2) \Rightarrow \text{grado}(q_1 \cdot q_2) \equiv 0$

  Si vale $\text{EsPolin0?}(q_1 \cdot q_2)$, por e_4 resulta $\text{EsPolin0?}(q_1) \vee \text{EsPolin0?}(q_2)$.

  Ahora en el consecuente, $\text{grado}(q_1 \cdot q_2) \equiv 0$, por g_4,

  if $\text{EsPolin0}(q_1) \vee \text{EsPolin0?}(q_2)$ **then** 0 **else** ... **fi** $\equiv 0$

  Vemos por el antecedente que entramos por la rama del **then** en el **if**, y se concluye que la tesis inductiva es verdadera directamente.

Es importante notar, al demostrar con lemas, que no haya un ciclo de uso de lemas, ya que la demostración resutlaría inválida. En este caso, se nota que para demostrar cada lema solo citamos lemas con números superiores. La demostración principal también debe entrar en consideración como si fuera un lema más.

6. Anexo: Propiedades válidas sobre el if

Estas son algunas de las propiedades relacionadas con **if** que se pueden utilizar sin demostrar. Pueden demostrarlas como ejercicio si quieren, es fácil.

- **if** p **then** q **else** q **fi** $\equiv q$
- función(**if** p **then** q **else** r **fi**) $\equiv$ **if** p **then** función(q) **else** función(r) **fi** [1]
- **if** $\neg p$ **then** q **else** r **fi** $\equiv$ **if** p **then** r **else** q **fi**
- **if** p **then** (**if** p **then** q **else** r **fi**) **else** t **fi** $\equiv$ **if** p **then** q **else** t **fi**

[1] Vale también si función toma mas parámetros