



UNIVERSIDAD NACIONAL AUTÓNOMA DE  
MÉXICO

---

---

FACULTAD DE CIENCIAS

VERIFICACIÓN FORMAL DE ÁRBOLES  
ROJINEGROS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:  
LICENCIADO EN CIENCIAS DE LA COMPUTACIÓN

PRESENTA:

DAVID FELIPE HERNÁNDEZ CHIAPA

TUTORA:

DRA. LOURDES DEL CARMEN GONZÁLEZ  
HUESCA

Ciudad Universitaria, Ciudad de México, 2021





Universidad Nacional  
Autónoma de México

Dirección General de Bibliotecas de la UNAM

**Biblioteca Central**



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



*Tesis realizada bajo el proyecto PAPIME 102117 “Tópicos en Ciencia de la Computación Teórica”.*



# Agradecimientos

A mi padre y a mi madre por ser la mas grande motivación en mi vida.

A mi hermana por siempre escucharme y abrazarme cuando estaba perdiendo ánimos.

A Lourdes por no desesperarse de mi aparente falta de habilidad al redactar.

A todo Ññ por siempre ayudarnos en todo lo que podíamos.

A Dan y Diego por ser los mejores amigos y la mas grata compañía.

A Gilberto por ayudarme con todos los temas que no entendía. A Clau por sacarse los ojos con este trabajo y ayudarme a mejorarlo.

A Daniel por aguantarme y escucharme hablar de cosas sin sentido.



# Índice general

<b>Agradecimientos</b>	<b>III</b>
<b>1. Introducción</b>	<b>1</b>
1.1. Motivación . . . . .	1
1.2. Árboles rojinegros . . . . .	3
1.3. Pruebas unitarias . . . . .	4
1.4. Traducción de Haskell a <i>Coq</i> . . . . .	6
1.4.1. Ventajas . . . . .	6
1.4.2. Desventajas . . . . .	7
1.5. Sobre este trabajo . . . . .	7
<b>2. Implementación en <i>Coq</i></b>	<b>9</b>
2.1. Traducción de implementaciones . . . . .	9
2.1.1. Traducción directa de implementaciones de Haskell a <i>Coq</i> . . . . .	9
2.2. Definición en <i>Coq</i> de los árboles rojinegros . . . . .	11
2.3. Inserción de elementos en un árbol rojinegro . . . . .	12
2.3.1. Operaciones de balanceo . . . . .	12
2.3.2. Función de inserción . . . . .	14
2.4. Eliminación de elementos en un árbol rojinegro . . . . .	16
2.4.1. Función de eliminación . . . . .	16
2.4.2. Función de concatenación . . . . .	18
2.4.3. Extensión de funciones de balanceo . . . . .	20
<b>3. Verificación en <i>Coq</i></b>	<b>23</b>
3.1. Verificación Formal en <i>Coq</i> . . . . .	23
3.1.1. Capturando invariantes de los árboles rojinegros . . . . .	24
3.1.2. Verificación de la operación de inserción . . . . .	28
3.1.3. Verificación de la operación de eliminación . . . . .	32
<b>A. Conceptos básicos de <i>Coq</i></b>	<b>55</b>



# Índice de figuras

1.1. Árbol rojinegro . . . . .	4
2.1. Árbol rojinegro antes de insertar nodo 7. . . . .	12
2.2. Árbol rojinegro después de insertar nodo 7. . . . .	12
2.3. Casos antes de balanceo, <i>lbal</i> arriba, <i>rbal</i> abajo. . . . .	13
2.4. Después de balanceo. . . . .	14
2.5. Árbol rojinegro antes de eliminar nodo 6. . . . .	17
2.6. Árbol rojinegro roto, después de eliminar nodo 6. . . . .	18
2.7. Árbol rojinegro después de aplicar función de concatenación. . . . .	18
2.8. Caso $T R a x b \Rightarrow T R (T B a x b) k r$ . . . . .	21
2.9. Caso $T B a y b \Rightarrow rbal' l k (T R a y b)$ . . . . .	21
2.10. Caso $T R (T B a y b) z c \Rightarrow T R (T B l k a) y (rbal' b z (makeRed c))$ . . . . .	22
3.1. Lema <i>ins_rr_rb</i> . . . . .	29
3.2. Lema <i>ins_arb</i> . . . . .	30
3.3. Lema <i>makeBlack_rb</i> . . . . .	31
3.4. Instancia de inserción de la clase <i>redblack</i> . . . . .	31
3.5. Lema <i>append_arb_rb</i> . . . . .	33
3.6. Casos del lema <i>append_arb_rb</i> . . . . .	33
3.7. Lema <i>lbalS_rb</i> . . . . .	41
3.8. Lema <i>del_arb</i> . . . . .	43
3.9. Instancia de eliminación de la clase <i>redblack</i> . . . . .	47
3.10. Lema <i>makeBlack_rb</i> . . . . .	47



# Índice de listados

1.	Función factorial, Haskell. . . . .	2
2.	Función factorial. . . . .	2
3.	Prueba unitaria escrita en Java[Pelález, 2019]. . . . .	5
4.	Ejemplo de ‘totalización’ de función. . . . .	10
5.	Árboles rojinegros en Coq. . . . .	11
6.	Funciones de balanceo. . . . .	13
7.	Función de inserción. . . . .	14
8.	Definiciones para pintar la raíz de negro. . . . .	15
9.	Función de eliminación. . . . .	17
10.	Función de concatenación. . . . .	19
11.	Función de balanceo de lado izquierdo extendida. . . . .	21
12.	Funciones de balanceo de lado derecho extendida. . . . .	22
13.	Función de balanceo de lado derecho alternativa. . . . .	22
14.	Función inductiva <i>isRB</i> . . . . .	25
15.	Función inductiva <i>nearRB</i> . . . . .	25
16.	Función inductiva <i>is_redblack</i> . . . . .	26
17.	Funciones inductivas <i>redred_tree</i> y <i>nearly_redblack</i> . . . . .	27
18.	Clase de árboles <i>redblack</i> . . . . .	28
19.	Tipo Inductivo. . . . .	55
20.	Función <i>Fixpoint</i> . . . . .	56
21.	Sustitución textual con <i>Definition</i> . . . . .	56
22.	Ejemplo del uso de tácticas y lemas. . . . .	56
23.	Ejemplo de una <i>meta</i> . . . . .	57



# Capítulo 1

## Introducción

### 1.1. Motivación

Hoy en día en el desarrollo de software existe un conjunto de normas a las cuales se les denomina *buenas prácticas de programación*. Algunos ejemplos de estas practicas serían: elegir si usaremos espacios o tabuladores para realizar la indentación, la documentación del código, respetar las convenciones del lenguaje que estamos usando y verificar que nuestro programa se comporta de la manera deseada. En específico, se pueden realizar pruebas unitarias.

Las *pruebas unitarias* nos ayudan a saber si un código tiene el comportamiento que buscamos, pero esto sólo nos sirve hasta cierto punto; por ejemplo, si tenemos una función que recibe un par de números naturales, para poder verificar que la función es correcta<sup>1</sup> se tendrían que probar todos los casos de entradas, es decir, todas las combinaciones de pares de números naturales que existan, sin embargo, estas combinaciones son infinitas y se necesitaría la misma cantidad de memoria y de tiempo para poder ejecutar una prueba unitaria exhaustiva. Teóricamente esto es posible, pero en la práctica simplemente no contamos con los recursos suficientes.

Siendo así, escribir una prueba unitaria exhaustiva no es factible, en tal caso ¿que podríamos hacer para verificar una implementación? Escribir una prueba unitaria que itere sobre un conjunto representativo de los datos que la función puede recibir como argumentos es una opción. Sin embargo, ¿qué se puede esperar si la prueba unitaria misma es errónea? No hay una respuesta clara para esto y la industria hoy en día utiliza métodos como el expuesto anteriormente para probar código pero, ciertamente, esto no es suficiente para decidir si el programa es correcto respecto a una especificación.

La única manera en que se puede demostrar que una función o programa es correcto respecto a una especificación es mediante una prueba matemática formal. El problema con este método es que es muy complejo, enredoso y a veces

---

<sup>1</sup>Podemos decir que una función es correcta si para toda entrada, la función regresa la salida esperada respecto a una especificación.

tardado para usarse en la industria o en el día a día. A lo largo del tiempo se ha buscado la manera de hacer este proceso mas amigable para el programador. Un ejemplo de esto son los lenguajes de programación funcionales, como lo sería Haskell. Este paradigma lleva a los programas a un contexto donde la notación es muy parecida a lo que se usaría en las matemáticas tradicionales, es decir, funciones que van de un conjunto de datos a otro. Damos como ejemplo la función que calcula el factorial de un número natural. Esta la escribiremos tanto en Haskell como en la notación que suele usarse en cursos de matemáticas tradicionales (ver figuras 1 y 2). Podemos apreciar cómo las definiciones son casi idénticas, ya que ambas cumplen los siguientes puntos:

- Ambas definen el tipo de sus variables, o en otras palabras, el conjunto al que las variables pertenecen.
- Ambas definiciones establecen de que tipo de dato toman sus argumentos, es decir, la entrada de la función es un número natural al igual que el resultado.
- Podemos intercambiar ‘f’ por ‘fac’ en cualquiera de las dos definiciones y el significado no cambiaría.

```
fac :: (Integral n) => n -> n
fac 0 = 1
fac n = n * fac (n - 1)
```

Listado 1: Función factorial, Haskell.

Sea  $n \in \mathbb{N}$  y  $f(n)$  la función factorial definida como sigue:

$$\begin{aligned} f : \mathbb{N} &\rightarrow \mathbb{N} \\ f(0) &= 1 \\ f(n) &= n \times f(n - 1) \end{aligned}$$

Listado 2: Función factorial.

La gran similitud entre estas definiciones facilita la demostración formal de los programas escritos en estos tipos de lenguajes, sin embargo, estas demostraciones son realizadas de manera tradicional usando lápiz y papel. No obstante, la única manera en que estemos seguros acerca de la corrección de la demostración es que otra persona lea, entienda y valide la misma. Todos estos procesos así como la creación y revisión de la demostración, están hechos por humanos, por lo tanto son susceptibles a errores.

En los últimos años han comenzado su desarrollando diversos programas que nos ayudan a solucionar este tipo de problemas, como son los *demostradores automáticos* y los *asistentes de prueba*. Estas herramientas son sistemas o programas que realizan o gestionan demostraciones. Nosotros nos enfocaremos

en el segundo uso; en particular en este trabajo usaremos el asistente interactivo de pruebas llamado *Coq*<sup>2</sup>. Este nos guiará por la prueba, llevando un control de los casos que nos falten por demostrar y las hipótesis disponibles para cada caso, todo esto sobre programas escritos en el lenguaje funcional del mismo asistente.

Sin embargo, el uso de este asistente genera otro problema: no podemos probar cualquier programa escrito en un lenguaje funcional, primero tenemos que traducir este programa al lenguaje de *Coq* para poder comenzar con las demostraciones. Aquí tenemos tres opciones: traducir a mano, o adaptar una implementación al lenguaje de *Coq*, o utilizar una herramienta que nos ayude a traducir. En este trabajo usaremos la segunda opción, una herramienta llamada *hs-to-coq* [Spector-Zabusky et al., 2017], para probar formalmente la corrección<sup>3</sup> de una estructura de datos como lo son los árboles rojinegros<sup>4</sup>.

Tomando como referencia el trabajo [López Campos, 2015], en donde se realizaron diversas implementaciones de árboles rojinegros usando el lenguaje de programación Haskell, por ejemplo, se desarrollaron implementaciones usando constructores inteligentes y otra implementación mas compleja usando tipos anidados. La principal motivación de elegir esta estructura de datos no trivial para este trabajo fue realizar una verificación formal de la implementación de constructores inteligentes. Sin embargo, por motivos que se tocaran en secciones posteriores, realizar una traducción del código de dicha tesis resulto no factible. Lo cual nos obligo a tomar otro camino: tomar la implementación de *Coq* de árboles rojinegros con pequeñas adecuaciones sacadas del código de la tesis antes mencionada, entre otras cosas que se explicaran mas adelante.

## 1.2. Árboles rojinegros

Los árboles rojinegros son una estructura de datos donde sus operaciones de inserción, eliminación y búsqueda se efectúan en tiempo logarítmico, es decir, la complejidad de estas operaciones es  $O(\log(n))$ . Los árboles rojinegros son una subclase de los árboles binarios de búsqueda, en los cuales la complejidad de dichas operaciones crece hasta  $O(n)$ , como si estos fueran una lista simple o doblemente ligada. Esta mejora se obtiene gracias a la introducción de colores a los nodos del árbol (rojo y negro, de ahí rojinegros) y a invariantes relacionados con estos, los cuales describiremos en la siguiente definición.

**Definición 1.2.1.** (Árboles rojinegros) Un árbol binario de búsqueda es un árbol rojinegro [Peláez Valdés, 2018] si satisface lo siguiente:

1. Todos sus nodos son rojos o negros.
2. La raíz es negra
3. Las siguientes invariantes se tienen que cumplir:

<sup>2</sup>Como en este trabajo no se profundizara sobre el funcionamiento de la herramienta, presentamos la pagina de referencia del mismo: <https://coq.inria.fr/>.

<sup>3</sup>Del inglés *correctness*.

<sup>4</sup>Más adelante se definirá esta clase de árboles.

- Un nodo rojo debe tener hijos negros.
- Todos los caminos de la raíz a las hojas deben tener la misma cantidad de nodos negros.
- Todas las hojas del árbol son vacías y de color negro.

Decimos que un árbol es negro o rojo si la raíz es de ese color. También podemos decir que la altura negra de un nodo es el número de nodos negros que aparecen en el camino de ese nodo a la raíz.

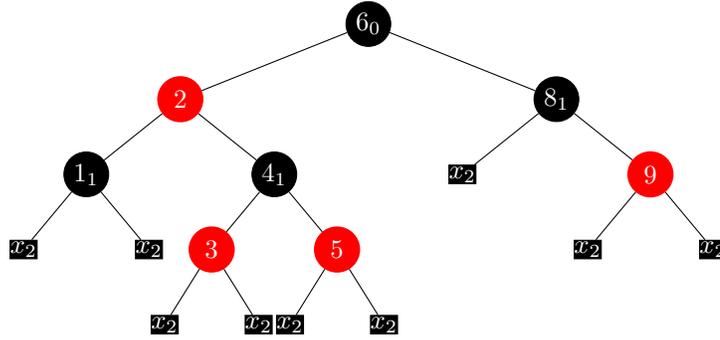


Figura 1.1: Árbol rojinegro

En la figura 1.1 podemos ver un ejemplo de un árbol rojinegro que respeta la definición que acabamos de presentar: las etiquetas de los nodos representan la información que se puede almacenar en ellos, siendo en este caso números naturales, las etiquetas  $x$  en las hojas representan los nodos vacíos y estos son negros, y los subíndices que aparecen en los nodos negros representan la altura negra del subárbol. Con este ejemplo se ilustra cómo la cantidad de nodos negros de la raíz a cualquier hoja es siempre la misma.

Nos interesa estudiar este tipo no trivial de *árboles binarios de búsqueda* para poder demostrar la corrección de la implementación funcional en [López Campos, 2015] usando el asistente de pruebas *Coq*. De esta manera mostraremos las ventajas y desventajas del proceso de verificación de una estructura de datos, el cual comienza escribiendo de cero una estructura o traduciendo la misma del lenguaje Haskell a *Coq*, y de igual manera las demostraciones que se realizarán con el asistente de pruebas. En este trabajo se nos enfocaremos en código ya traducido.

### 1.3. Pruebas unitarias

Las *pruebas unitarias* [Osherove, 2014] son bloques de código, funciones o métodos, que invocan a otros bloques para poder verificar ciertas suposiciones sobre el programa a probar. Estas pruebas en principio deben de ser fáciles de escribir, entender, extender, deben ejecutarse en poco tiempo y sobre todo ser

fidedignas. De nada nos servirían pruebas unitarias que estén mal escritas o que estas mismas sean demasiado complejas y puedan contener errores.

Este tipo de pruebas son usadas para verificar que cada componente de un programa funcione de la manera esperada. En el caso de los árboles rojinegros este tipo de pruebas nos ayudan a verificar los invariantes de un determinado árbol. La figura 3 es una prueba unitaria escrita en el lenguaje de programación Java, la cual verifica la altura negra de un árbol rojinegro [Peláez, 2019].

```

/* Valida que los caminos del vértice a sus hojas tengan todos
    el mismo número de vértices negros. */
private static <T extends Comparable<T>> int
validaCaminos(ArbolRojinegro<T> arbol,
              VerticeArbolBinario<T> v) {
    int ni = -1, nd = -1;
    if (v.hayIzquierdo()) {
        VerticeArbolBinario<T> i = v.izquierdo();
        ni = validaCaminos(arbol, i);
    } else {
        ni = 1;
    }
    if (v.hayDerecho()) {
        VerticeArbolBinario<T> d = v.derecho();
        nd = validaCaminos(arbol, d);
    } else {
        nd = 1;
    }
    Assert.assertTrue(ni == nd);
    switch (arbol.getColor(v)) {
    case NEGRO:
        return 1 + ni;
    case ROJO:
        return ni;
    default:
        Assert.fail();
    }
    // Inalcanzable.
    return -1;
}

```

Listado 3: Prueba unitaria escrita en Java [Peláez, 2019].

Sin embargo, como se menciona en la motivación, el hecho de que las pruebas unitarias puedan verificar las invariantes de un árbol dado no nos asegura que todos los árboles creados por nuestras operaciones de inserción y eliminación las respeten. La única manera de que esta prueba podría verificar esto sería realizando todas las combinaciones de operaciones y entradas posibles y aplicar la

prueba a todos los resultados de estas entradas. Esto es una prueba exhaustiva y en este caso<sup>5</sup> las posibilidades son infinitas, es decir, no existe modo de realizar todas estas pruebas en un tiempo razonable. Más aún, no existe memoria suficiente para almacenar los infinitos valores que se necesitarían para realizar dichas pruebas.

Finalmente, como las pruebas unitarias no nos permiten cubrir todos los casos necesarios para poder probar en su totalidad un programa, es que se requiere utilizar algún otro tipo de herramienta para realizar una verificación, en este trabajo usaremos *Coq*.

## 1.4. Traducción de Haskell a *Coq*

El enfoque que hemos decidido darle a este trabajo consiste en considerar una implementación de la estructura descrita en la sección 1.1 y solamente realizar la verificación formal de la misma. Para este trabajo decidimos usar *Coq*. Este asistente nos guía a través de la prueba recordando cuáles son las *metas*<sup>6</sup> que debemos demostrar y también nos ofrece *tácticas* para poder resolver dichas metas. Sin embargo, ésta también nos presenta nuevos desafíos.

Al comenzar a utilizar el asistente nos encontramos con la problemática de decidir si vamos a escribir el programa directamente en el lenguaje de *Coq* o si lo que buscamos es traducir un programa ya existente al lenguaje del asistente de pruebas. Lo que se busca es poder verificar un programa antes escrito, es decir, para el caso de los árboles rojinegros queremos traducir este código de Haskell a *Coq*.

En el artículo ‘Total Haskell is Reasonable Coq’ [Spector-Zabusky et al., 2017] se describen las principales ventajas y desventajas de traducir de Haskell a *Coq*, los cuales expondremos a continuación.

### 1.4.1. Ventajas

- Haskell es un excelente lenguaje para escribir programas funcionales puros.
- La gran comunidad de programadores que usan y mantienen Haskell.
- El compilador GHC de Haskell, el cual es muy usado e incluso a nivel industrial.
- El ambiente de *Coq* es “amigable” para desarrollar demostraciones formales.
- *Coq* permite razonar acerca de programas funcionales totales.

---

<sup>5</sup>De hecho en la mayoría.

<sup>6</sup>Una meta consiste de dos cosas: la conclusión y un contexto. El segundo contiene las hipótesis, definiciones y variables que podemos usar para demostrar la conclusión. [The Coq Team and contributors, 2011c].

### 1.4.2. Desventajas

- Haskell utiliza el razonamiento ecuacional, por lo que en general no se usa un lenguaje formal para realizar las demostraciones.
- Los programadores de Haskell razonan acerca de su código informalmente, si se llegan a realizar pruebas de éste, generalmente está hecho a mano “en papel”, lo cual es tedioso y susceptible a errores.
- *Coq* no tiene la extensa biblioteca de funciones ni la misma cantidad de programadores que lo usen y mantengan como lo tiene Haskell.
- El hecho de que los programadores de Haskell sólo razonen acerca de su código informalmente puede que resulte en que se generen funciones parciales, es decir, que no se cubran todas las combinaciones de parámetros posibles para una función.
- La traducción de Haskell a *Coq* sólo es posible si todas las funciones a traducir son totales.

El artículo propone el uso de una herramienta llamada *hs-to-coq*, la cual actualmente se encuentra en etapa de desarrollo y está siendo usada para traducir código de Haskell a *Coq*. Por las razones expuestas al comienzo de esta sección es que decidimos usar esta herramienta de traducción y enfocarnos únicamente en la verificación de los árboles rojinegros.

## 1.5. Sobre este trabajo

El contenido y demostraciones que se describen en este trabajo se encuentran almacenados en: <https://github.com/DavidFHCh/Tesis-FTW>. Aquí presentamos definiciones, lemas y clases sin incluir las demostraciones en *Coq*, en otras palabras, los *scripts* de prueba. En su lugar se describen de manera informal las demostraciones para poder entender en alto nivel la estructura de la verificación formal realizada.

La herramienta *hs-to-coq* fue utilizada para obtener las traducciones de las bibliotecas de Haskell; éstas fueron usadas para poder verificar la implementación, comenzando con el trabajo de [López Campos, 2015] y adecuándolo a la implementación de [The Coq Team and contributors, 2011b] que se usó en el trabajo.

En los siguientes capítulos se describe el procedimiento usado para la verificación de la estructura de datos, la cual está enfocada a las invariantes de los cuatro puntos de la definición 1.2.1 dejando de lado la verificación de ser un árbol de búsqueda<sup>7</sup>.

---

<sup>7</sup>El lector interesado puede revisar [Appel, 2018].



## Capítulo 2

# Implementación en *Coq*

### 2.1. Traducción de implementaciones

Se tomaron un par de implementaciones funcionales de árboles rojinegros para verificarlas. La primera contiene las implementaciones de [López Campos, 2015] en Haskell que fueron utilizadas como entrada para la herramienta *hs-to-coq*, es decir, una traducción directa<sup>1</sup>. La segunda implementación y la que se usó para este trabajo, fue obtener de [The Coq Team and contributors, 2011b] la implementación de los árboles rojinegros que se usan en la biblioteca estándar de *Coq*, los cuales son una versión de los árboles rojinegros de [Okasaki, 1998]. En el segundo caso, se usaron las bibliotecas traducidas de Haskell a *Coq*, las cuales contienen los tipos y operaciones sobre ellos de Haskell. Esta traducción se obtuvo con la ayuda del traductor *hs-to-coq* y sustituyen a los tipos y operaciones de *Coq*. A continuación profundizaremos de estos dos casos.

#### 2.1.1. Traducción directa de implementaciones de Haskell a *Coq*

De la tesis [López Campos, 2015] se obtuvieron diversas implementaciones de árboles rojinegros. Debido a que la operación de borrado es compleja (eliminación de un nodo interno) ya que se deben cumplir las invariantes del árbol resultante, dicha operación es significativamente más compleja que su contraparte, es decir, la operación de inserción. Las diferentes implementaciones de la tesis [López Campos, 2015], las cuales buscan una solución más eficiente, son: la implementación de Okasaki (siendo esta la más simple) los constructores inteligentes (implementación anterior con optimizaciones) y los tipos anidados (una implementación totalmente diferente a las anteriores y más elegante).

Por la compleja naturaleza de estas implementaciones, el intento de realizar la traducción manual del código de Haskell resultó ser muy problemática y no se llevó a cabo, esto porque en las implementaciones escritas en Haskell se

---

<sup>1</sup>Por motivos de como se escribieron las implementaciones, la traducción no pudo realizarse.

tomó ventaja del hecho de que en este lenguaje se pueden declarar funciones parciales, lo cual representa un reto al momento de intentar traducir a *Coq*, ya que este lenguaje únicamente acepta funciones totales. Se buscaron soluciones para ‘totalizar’ estas funciones. Sin embargo, sólo traerían problemas al intentar realizar las demostraciones, ya que al totalizar se generarían casos inalcanzables en la ejecución, pero tendrían que ser demostrados para poder completar la verificación.

A pesar de ello, se intentó totalizar las funciones de Haskell y así poder usar la herramienta *hs-to-coq* y de esta manera facilitar la traducción pero, por las mismas razones antes descritas, la herramienta caía en alguna de estas dos situaciones:

- El tiempo de ejecución de la herramienta era muy alto y eventualmente los recursos de la maquina virtual, donde esta herramienta se ejecutó, se quedaba sin recursos (en especial memoria). Esto probablemente se deba a la falta de totalidad en alguna función.
- La herramienta generaba código en *Coq* pero con elementos de Haskell cuyas bibliotecas todavía no habían sido traducidas del todo. Esto porque las implementaciones en Haskell podían llegar a ser muy complejas y utilizar módulos de GHC, a los cuales todavía no se les había traducido con la herramienta.

Por ejemplo el listado 4, se presenta una función de una de las implementaciones que propone [López Campos, 2015], árboles rojinegros con aritmética de colores para controlar la invariante. Podemos notar que el último caso de la caza de patrones devuelve un error, esto no estaba en el código de Haskell original, pero al querer realizar la traducción con la herramienta *hs-to-coq* era necesario agregar ese caso. El problema en este caso es que *error* no estaba en la biblioteca de traducciones de *hs-to-coq*, por lo cual no podíamos verificar. Se penso en usar tipos *Option* y regresar *None* en lugar de errores, pero la verificación habría aumentado considerablemente su complejidad.

```
sucBlack :: Color -> Color
sucBlack NB = R
sucBlack R = B
sucBlack B = BB
sucBlack BB = error "no hay sucesor para BB"
```

Listado 4: Ejemplo de ‘totalización’ de función.

Por estas razones se buscó otro acercamiento para poder verificar esta estructura. Sabemos que el equipo de desarrollo de la herramienta *hs-to-coq* ha traducido exitosamente una fracción de las bibliotecas de Haskell a *Coq*<sup>2</sup>, por

---

<sup>2</sup>El nombre de esta es *GHC.Base*, nos referiremos a las funciones de la biblioteca con ese mismo prefijo.

esta razón, se optó por el uso de la implementación de árboles rojinegros de las bibliotecas de *Coq*, [The Coq Team and contributors, 2011b], pero usando los tipos y operaciones obtenidos de las traducciones con la herramienta.

## 2.2. Definición en Coq de los árboles rojinegros

La biblioteca de *Coq* contiene una gran variedad de funciones y estructuras de datos, implementadas y verificadas con los tipos nativos del lenguaje de Coq. En este trabajo tomaremos la implementación de los árboles rojinegros de la biblioteca antes mencionada, sustituiremos los tipos de Coq por los tipos que la herramienta *hs-to-coq* obtuvo de realizar la traducción de las bibliotecas de Haskell al lenguaje de Coq.

```

Inductive Color : Type := R : Color | B : Color.

Inductive RB a : Type := E : RB a |
  T : Color -> (RB a) -> a -> (RB a) -> RB a.

Arguments E {_}.
Arguments T {_} _ _ _ _ .

```

Listado 5: Árboles rojinegros en Coq.

En el listado 5 definimos los colores y la forma de los árboles rojinegros, podemos notar que un árbol está definido de la siguiente manera:

- Se define un tipo inductivo con dos colores:  $R$  y  $B^3$ .
- Se define un segundo tipo inductivo con las dos formas de un árbol rojinegro:
  - $E$ , el cual es el árbol vacío.
  - Un árbol  $T$ ; el cual contiene un  $Color$ , un árbol rojinegro, un tipo  $a$  y otro árbol rojinegro.

El tipo  $a$  que se usa en la definición de los árboles se refiere a un tipo ordenado, más específicamente que pertenezca a la definición de tipo ordenado de la biblioteca de Haskell [HaskellDoc, 2005]. A lo largo de este trabajo se podrá encontrar que las funciones de inserción, eliminación y sus respectivas funciones auxiliares, tendrán la siguiente anotación:  $\{GHC.Base.Ord\ a\}$ . La cual indica que la función solo acepta tipos que respeten dicha anotación.

<sup>3</sup>Se refieren a los nombres en inglés del color rojo y negro, i.e. *Red* y *Black*.

### 2.3. Inserción de elementos en un árbol rojinegro

La inserción de elementos a un árbol rojinegro es la operación más sencilla de las dos que se verificarán en este trabajo. La idea principal detrás de este algoritmo es que únicamente se agreguen hojas al árbol binario y se efectúen “giros” o funciones de balanceo para mantener las invariantes de la estructura (ver figura 2.1 y 2.2).

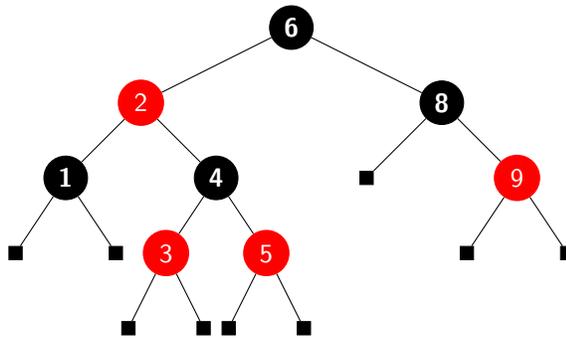


Figura 2.1: Árbol rojinegro antes de insertar nodo 7.

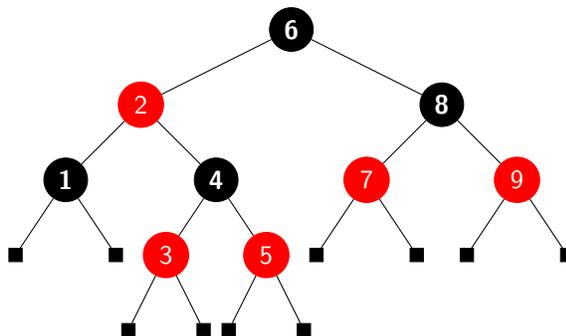


Figura 2.2: Árbol rojinegro después de insertar nodo 7.

#### 2.3.1. Operaciones de balanceo

Los giros antes mencionados están definidos en las operaciones de balanceo, las cuales son dos: una para los subárboles izquierdos y otra para los derechos. Estas funciones (ver figura 6) se encargan de solucionar los casos en los que inmediatamente después de agregar una hoja alguna de las invariantes sean violadas, por ejemplo, dos nodos rojos que resultan contiguos en algún lugar de la estructura del árbol.

El balanceo elimina el doble nodo rojo al crear un único nodo rojo con dos hijos negros (ver figuras 2.3 y 2.4, obtenidas de [López Campos, 2015]). De igual

```

Definition lbal {a} `GHC.Base.Ord a} (l:RB a) (k:a) (r:RB a) :=
  match l with
  | T R (T R a x b) y c => T R (T B a x b) y (T B c k r)
  | T R a x (T R b y c) => T R (T B a x b) y (T B c k r)
  | _ => T B l k r
end.

```

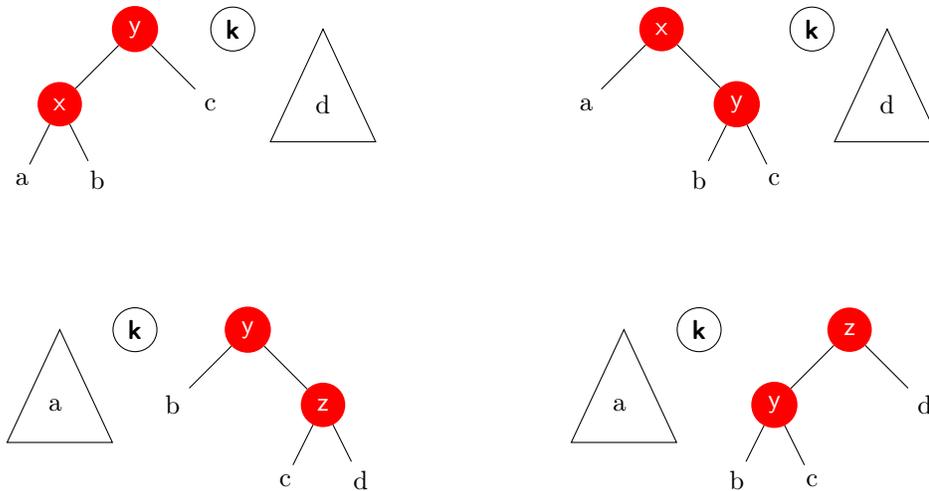
```

Definition rbal {a} `GHC.Base.Ord a} (l:RB a) (k:a) (r:RB a) :=
  match r with
  | T R (T R b y c) z d => T R (T B l k b) y (T B c z d)
  | T R b y (T R c z d) => T R (T B l k b) y (T B c z d)
  | _ => T B l k r
end.

```

Listado 6: Funciones de balanceo.

manera esto nos asegura que el árbol crece de forma controlada en número de nodos negros, es decir, mantiene la invariante de la altura negra, lo cual se debe a que en ningún momento se están agregando dos nodos negros contiguos<sup>4</sup>. Cabe mencionar que esta es la única operación en donde se agregan nodos negros, con la excepción de *makeBlack*, la cual describiremos más adelante.

Figura 2.3: Casos antes de balanceo, *lbal* arriba, *rbal* abajo.

En puntos posteriores se explicarán los casos de uso de esta función, se desarrollará el porqué los únicos casos a los que se les da un trato especial es a los de nodos rojos contiguos y en el resto sólo se regresa un árbol con raíz negra

<sup>4</sup>Nodos padre e hijo negros después de balancear.

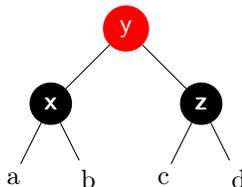


Figura 2.4: Después de balanceo.

sin hacer mayor acomodo.

### 2.3.2. Función de inserción

Esta función es donde se presenta por primera vez el uso de las bibliotecas traducidas de Haskell, podemos apreciar como los tipos<sup>5</sup> de los elementos que se están agregando al árbol son tipos ordenados de la biblioteca *Base* del compilador de GHC y por esa misma razón estamos usando las operaciones (comparaciones) de esa biblioteca.

```

Fixpoint ins {a} `{GHC.Base.Ord a} (x:a) (s:RB a) :=
  match s with
  | E => T R E x E
  | T c l y r =>
    if x GHC.Base.< y : bool then
      match c with
      | R => T R (ins x l) y r
      | B => lbal (ins x l) y r
      end
    else
      if x GHC.Base.> y : bool then
        match c with
        | R => T R l y (ins x r)
        | B => rbal l y (ins x r)
        end
      else s
    end.
  
```

Listado 7: Función de inserción.

Analizando más detenidamente la función (listado 7) se puede observar que las operaciones de balanceo sólo se efectúan cuando el nodo por el que se está pasando es negro, esto sucede porque los nodos de este color son los que se toman en cuenta para decidir si un árbol cumple con el balanceo adecuado. Al aplicar el balanceo en estos nodos, podemos garantizar que no quedarán con

<sup>5</sup>El tipo que se usa en los árboles rojinegros es representado con la letra *a*.

nodos negros extras alguno de los hijos de este nodo, es decir, que ninguno de los caminos de la raíz a las hojas tenga mas nodos negros que los demás. Esto se puede apreciar si recordamos lo que se mencionó en las definiciones de las operaciones de balanceo, tomemos *rbal* (listado 6)<sup>6</sup>, tenemos dos casos:

- Sean  $x$ ,  $y$  y  $z$  nodos del árbol y sea  $t$  un subárbol,  $x$  es el nodo al que se le aplica la operación de balanceo y éste es de color negro,  $t$  es el subárbol izquierdo,  $y$  es el nodo derecho de  $x$  y  $z$  es hijo de  $y$  (es irrelevante si es derecho o izquierdo, el resultado es el mismo.) Suponiendo que  $y$  y  $z$  son rojos<sup>7</sup>, se cae en cualquiera de los dos casos de *rbal* que no sean el caso general. En este momento es donde se efectúa el *balanceo* del árbol y resulta lo siguiente:  $x$  se vuelve el hijo izquierdo de  $y$  y  $z$  se pinta de negro<sup>8</sup>, todas las demás estructuras del árbol permanecen igual.

En el momento en que  $x$  se convierte en hijo izquierdo de  $y$  el árbol se desbalancea, es por esto que se pinta de negro a  $z$ , así los dos nodos negros son hijos de  $y$  y la invariante se conserva.

- En cualquier otro caso el árbol no sufre modificación alguna.

Este balanceo es necesario en esta función ya que todos los elementos nuevos que se agregan al árbol son hojas rojas. Esto puede traer consigo violaciones a los invariantes, en especial al de que existan dos nodos rojos contiguos y esta operación ayuda a mitigar este problema.

A pesar de que las operaciones de balanceo cuidan la mayoría de invariantes en el cuerpo del árbol, la función *ins* no necesariamente cumple con uno de los invariantes, específicamente en el que la raíz del árbol es negra. Es por ello que se introducen las definiciones de la figura 8.

```
Definition makeBlack {a} ` {GHC.Base.Ord a} (t:RB a) :=
  match t with
  | E => E
  | T _ a x b => T B a x b
end.
```

```
Definition insert {a} ` {GHC.Base.Ord a} (x:a) (s:RB a) :=
  makeBlack (ins x s).
```

Listado 8: Definiciones para pintar la raíz de negro.

La definición *makeBlack* únicamente colorea un nodo de color negro y la definición *insert* es una envoltura de *ins*, con la cual nos aseguramos de que la raíz de los árboles siempre sea de color negro, esto se logra con ayuda de *makeBlack*.

<sup>6</sup>Con *lbal* la idea es análoga.

<sup>7</sup>Se viola una invariante, dos nodos rojos contiguos.

<sup>8</sup>El hijo se vuelve padre y el padre se vuelve hijo.

Estas funciones y definiciones son suficientes para poder construir árboles rojinegros que respeten las invariantes que planteamos en la definición 1.2.1.

## 2.4. Eliminación de elementos en un árbol rojinegro

Como se mencionó en la sección anterior, la operación de eliminación es significativamente más compleja que su contraparte. Esto se debe al hecho de que cualquier nodo puede ser eliminado en un árbol rojinegro, mientras que en la inserción sólo se agrega el elemento como una hoja de color rojo, es decir, la altura únicamente se modifica en la inserción cuando se aplica el balanceo.

La acción de eliminar un nodo de cualquier parte de un árbol rojinegro presenta una problemática muy grande para mantener las invariantes de los árboles rojinegros. Esto se suscita al eliminar un nodo interno del árbol derivando en dos subárboles que tienen que ser concatenados de alguna forma.

### 2.4.1. Función de eliminación

Para poder comprender la lógica de las funciones que conforman a la operación de eliminación es necesario comenzar por la función que retira el nodo del árbol (ver el listado 9). La idea central de esta operación es bastante simple: como los árboles rojinegros son árboles de búsqueda, lo primero que hacemos es buscar el nodo a eliminar. Si se encuentra se elimina y se concatenan los subárboles restantes de esta operación (ver figuras 2.5, 2.6 y 2.7). A continuación se describen más a fondo los casos de la misma:

- Si se recibe un árbol vacío como argumento de la función, se regresa este mismo pues al eliminar un elemento del árbol vacío se obtiene el vacío. También este caso sirve para cuando un elemento no es encontrado en el árbol, es el caso base de la recursión de búsqueda del nodo a eliminar.
- En otro caso, se realiza recursivamente la búsqueda del elemento a eliminar. Si el nodo actual no contiene el elemento que buscamos, se compara si es menor o mayor para seguir buscando en el árbol izquierdo o derecho respectivamente, describimos los casos:
  - Si el nodo es menor y el nodo del árbol izquierdo es negro, entonces aplicamos la función *lbalS*<sup>9</sup> al árbol resultante de seguir buscando el nodo a eliminar por el subárbol izquierdo. En otro caso sólo seguimos buscando por el subárbol izquierdo.
  - Si el nodo es mayor y el nodo del árbol derecho es negro, entonces aplicamos la función *rbalS*<sup>10</sup> al árbol resultante de seguir buscando el nodo a eliminar por el subárbol derecho. En otro caso sólo seguimos buscando por el subárbol derecho.

<sup>9</sup>Función de balanceo extendida para subárboles izquierdos.

<sup>10</sup>Función de balanceo extendida para subárboles derechos.

- Si el elemento en el que estamos no es ni mayor ni menor al que buscamos, en ese caso eliminamos el elemento y concatenamos los subárboles restantes usando la función *append*<sup>11</sup>.

```

Fixpoint del {a} ` {GHC.Base.Ord a} (x:a) (t:RB a) :=
  match t with
  | E => E
  | T _ a y b =>
    if x GHC.Base.< y : bool then
      match a with
      | T B _ _ => lbalS (del x a) y b
      | _ => TR (del x a) y b
    end
    else
      if x GHC.Base.> y : bool then
        match b with
        | T B _ _ => rbalS a y (del x b)
        | _ => TR a y (del x b)
      end
      else append a b
    end
end.

```

Definition remove x t := makeBlack (del x t).

Listado 9: Función de eliminación.

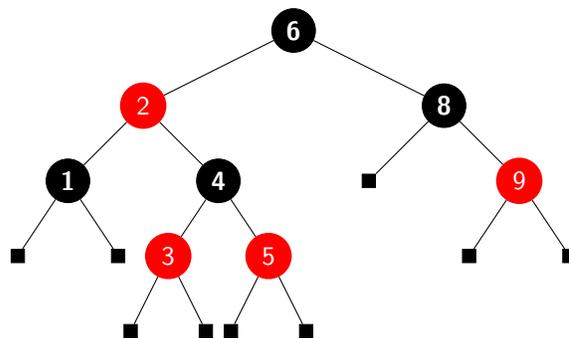


Figura 2.5: Árbol rojinegro antes de eliminar nodo 6.

Podemos ver que las funciones de balanceo *lbalS* y *rbalS* se aplican cuando el nodo en el que estamos parados, llamémoslo *n*, es negro. Esto evita que después de eliminar un nodo y aplicar la función *append* se acabe con dos nodos rojos seguidos, es decir, que el hijo y alguno de los nietos del nodo *n* sean rojos.

<sup>11</sup>Función donde se juntan lo arboles restantes de esta operación.

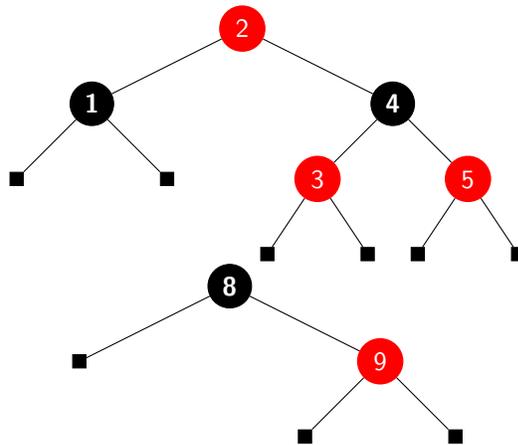


Figura 2.6: Árbol rojinegro roto, después de eliminar nodo 6.

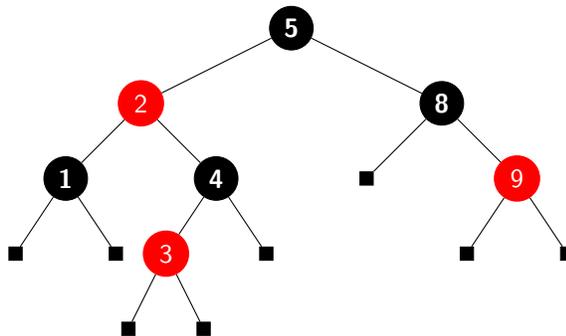


Figura 2.7: Árbol rojinegro después de aplicar función de concatenación.

### 2.4.2. Función de concatenación

La función de concatenación (listado 10) es usada cuando se ha encontrado el elemento a eliminar en un árbol rojinegro, resultando en dos árboles que tienen que ser concatenados, los cuales deben de respetar los invariantes de los árboles rojinegros. Esta función recibe como parámetros los dos árboles<sup>12</sup> que estamos buscando unir. Esta operación se describe con mayor detalle enseguida.

Sean  $a$  y  $b$  los dos subárboles a los que se les aplicará la función *append*, es decir, *append a b*, tenemos los siguientes casos que están definidos dentro de la función auxiliar local (*append\_l*):

- Si  $a$  es el árbol vacío, entonces se regresa  $b$ .
- Si  $b$  es el árbol vacío, entonces regresamos  $a$ .

<sup>12</sup>Estos arboles pueden no cumplir con todas las invariantes de los árboles rojinegros.

```

Fixpoint append {a} `{GHC.Base.Ord a} (l:RB a) : RB a -> RB a :=
  match l with
  | E => fun r => r
  | T lc ll lx lr =>
    fix append_l (r:RB a) : RB a :=
      match r with
      | E => l
      | T rc rl rx rr =>
        match lc, rc with
        | R, R =>
          let lrl := append lr rl in
          match lrl with
          | T R lr' x rl' => T R (T R ll lx lr') x (T R rl' rx rr)
          | _ => T R ll lx (T R lrl rx rr)
          end
        | B, B =>
          let lrl := append lr rl in
          match lrl with
          | T R lr' x rl' => T R (T B ll lx lr') x (T B rl' rx rr)
          | _ => lbalS ll lx (T B lrl rx rr)
          end
        | B, R => T R (append_l rl) rx rr
        | R, B => T R ll lx (append lr r)
        end
      end
    end
  end.

```

Listado 10: Función de concatenación.

- Si  $a$  y  $b$  son árboles con raíces rojas, entonces se aplica *append* al subárbol derecho de  $a$ , siendo este  $ar$ , junto con el subárbol izquierdo de  $b$ , digamos  $bl$ , es decir, *append ar bl*. Tenemos dos subcasos:
  - Si el resultado de esta operación es un árbol con raíz roja, llamémosle  $arbl$ , los árboles  $a$  y  $b$  se pintan de rojo y se concatenan con la raíz de  $arbl$ , igual de color rojo;  $ar$  se reemplaza por el subárbol izquierdo de  $arbl$  y  $bl$  se reemplaza por el subárbol derecho de  $arbl$ .
  - En otro caso, si el árbol resultante de *append ar bl* no es rojo, tomamos  $a$  y  $b$ , los pintamos de rojo, el subárbol derecho de  $a$  se reemplaza por  $b$  y el subárbol izquierdo de  $b$  se reemplaza por el resultado de *append ar bl*.
- Si  $a$  y  $b$  son árboles con raíces negras, entonces se aplica *append* al subárbol derecho de  $a$ , llamémosle  $ar$ , con el subárbol izquierdo de  $b$ , digamos  $bl$ , es decir, *append ar bl*. Tenemos los siguientes casos:

- Sea *arbl* el resultado de esta operación, si éste es un árbol con raíz roja, los árboles *a* y *b* se pintan de negro y se concatenan con la raíz de *arbl*, está de color rojo; *ar* se reemplaza por el subárbol izquierdo de *arbl* y *bl* se reemplaza por el subárbol derecho de *arbl*.
  - En otro caso, si el árbol resultante de *append ar bl* no es rojo, tomamos *a* y *b*, el subárbol derecho de *a* se reemplaza por *b* y el subárbol izquierdo de *b* se reemplaza por el resultado de *append ar bl* y a este resultado le aplicamos una función de balanceo, *lbalS*.
- Si *a* es un árbol de color negro y *b* de color rojo, entonces se toma *b* rojo pero en lugar de su subárbol izquierdo, se aplica una llamada recursiva con *bl* (subárbol izquierdo de *b*) a la función embebida en *append*, llamada *append\_l*, es decir: *append\_l bl*, esta llamada también carga al árbol *a* gracias al *currying*[HaskellWiki, 2020].
  - Si *a* es un árbol de color rojo y *b* de color negro, entonces se toma *a*, se pinta de rojo pero en lugar de su subárbol derecho, digamos *ar*, se hace una llamada recursiva con *append(ar, b)*.

Debemos mencionar que el árbol resultante de aplicar esta función no necesariamente cumple con todas las invariantes de un árbol rojinegro, estas invariantes se logran conservar ya que en la función *del* se realizan llamadas a las funciones extendidas de balanceo, las cuales desarrollaremos en la siguiente sección.

### 2.4.3. Extensión de funciones de balanceo

En la sección 2.3 de este trabajo se trató la inserción de elementos a un árbol rojinegro, en donde se describen un par de funciones llamadas ‘de balanceo’, tratadas en las subsección 2.3.1; estas funciones a su vez toman los nombres *rbal* y *lbal* (listado 6). Estas operaciones resultan insuficientes para balancear un árbol al momento de eliminar un nodo y concatenar los dos árboles restantes con la función *append*, es por esto que se implementan las extensiones de estas funciones, llamadas *lbalS* y *rbalS* (códigos 11 y 12 respectivamente) las cuales a su vez llaman a las funciones *rbal'*<sup>13</sup> (código 13) y *lbal*. Estas extensiones agregan mas casos de manejo de subárboles negros, esto sucede porque existen casos en los que se puede llegar a eliminar un nodo negro intermedio del árbol o inclusive la misma raíz y se debe poder asegurar que las invariantes no se violen después de concatenar los subárboles restantes.

Las funciones *rbalS* y *lbalS* son usadas en la función *del* (listado 9) cuando la llamada recursiva busca el nodo a eliminar en un subárbol con raíz negra, al aplicar la función de balanceo en estos nodos podemos asegurar que los dos subárboles de este nodo no se van a desequilibrar, es decir, que un subárbol tenga mayor altura negra que el otro. Estas funciones básicamente hacen un

<sup>13</sup>La función *rbal'* es una variación de la función *rbal*, sólo cambia el orden de la caza de patrones.

```

Definition lbalS {a} `{-}{GHC.Base.Ord a} (l:RB a) (k:a) (r:RB a) :=
  match l with
  | T R a x b => T R (T B a x b) k r
  | _ =>
    match r with
    | T B a y b => rbal' l k (T R a y b)
    | T R (T B a y b) z c => T R (T B l k a) y (rbal' b z (makeRed c))
    | _ => T R l k r
  end
end.

```

Listado 11: Función de balanceo de lado izquierdo extendida.

reacomodo de los nodos de los subárboles para después llamar a las funciones *rbal'* y *lbal*, es por eso que decimos que son extensiones de éstas. Las figuras 2.8, 2.9 y 2.9 representan gráficamente estos casos mas complejos (Ilustraciones obtenidas de [López Campos, 2015]). A pesar de que las ilustraciones fueron concebidas para código de Haskell podemos notar como corresponden uno a uno con los casos.

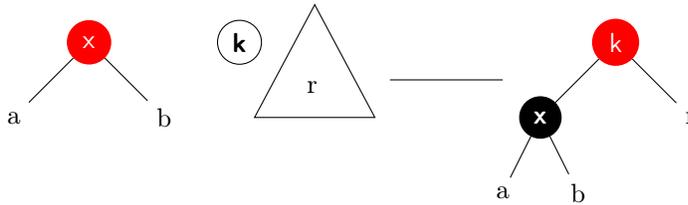


Figura 2.8: Caso  $T R a x b \Rightarrow T R (T B a x b) k r$

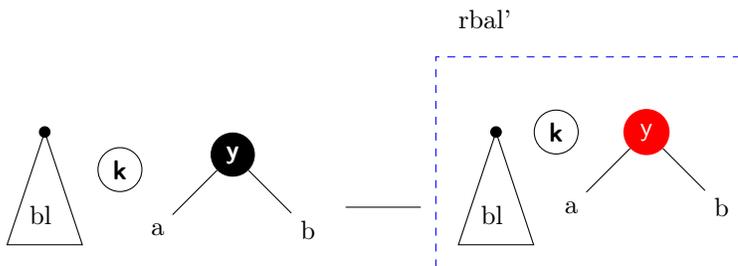


Figura 2.9: Caso  $T B a y b \Rightarrow rbal' l k (T R a y b)$

Existe otra función donde se utiliza una de estas operaciones de balanceo, específicamente *lbalS*, esta función es *append*. Esto sucede en el caso en que los árboles que son argumentos de *append* sean negros, es decir, la misma razón

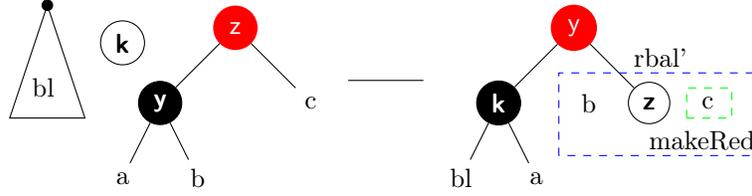


Figura 2.10: Caso  $TR (TB a y b) z c \Rightarrow TR (TB l k a) y (rbal' b z (makeRed c))$

```

Definition rbalS {a} `{GHC.Base.Ord a} (l:RB a) (k:a) (r:RB a) :=
  match r with
  | TR b y c => TR l k (TB b y c)
  | _ =>
    match l with
    | TB a x b => lbal (TR a x b) k r
    | TR a x (TB b y c) => TR (lbal (makeRed a) x b) y (TB c k r)
    | _ => TR l k r
  end
end.

```

Listado 12: Funciones de balanceo de lado derecho extendida.

por la que se aplican las funciones de balanceo en *del* sobre los nodos de color negro: para que sus subárboles no se desbalancen.

```

Definition rbal' {a} `{GHC.Base.Ord a} (l:RB a) (k:a) (r:RB a) :=
  match r with
  | TR b y (TR c z d) => TR (TB l k b) y (TB c z d)
  | TR (TR b y c) z d => TR (TB l k b) y (TB c z d)
  | _ => TB l k r
  end.

```

Listado 13: Función de balanceo de lado derecho alternativa.

Las definiciones y funciones presentadas son suficientes para poder eliminar cualquier nodo de un árbol rojinegro y que el resultado no viole los invariantes de éstos. En esta etapa del trabajo nos agradaría llegar a esta conclusión, sin embargo, esta sentencia tiene que ser demostrada, es decir, tenemos que probar que nuestros árboles rojinegros cumplen con la definición de los mismos. Esto es lo que veremos en el siguiente capítulo.

## Capítulo 3

# Verificación en *Coq*

En el primer capítulo de este trabajo se mencionó que los árboles rojinegros son una estructura de datos que mejora el tiempo de acceso, de inserción y eliminación de elementos con respecto a otras estructuras de datos como las listas simples, las listas doblemente ligadas y los árboles de búsqueda. En el segundo capítulo se muestran las implementaciones funcionales de los algoritmos de esta estructura de datos y podemos notar como estas implementaciones no son triviales, es decir, son rebuscadas por los tipos usados en un lenguaje que utiliza el estilo de programación funcional como lo hace *Coq*, e incluso son diferentes y alejadas de una implementación en un lenguaje con un paradigma imperativo como *Java* o *C*. Por esta razón es que nos preocupa que las implementaciones que realicemos sean correctas, en otras palabras, se desea verificar que las implementaciones de las operaciones descritas en el capítulo anterior respeten en todos los casos los invariantes de los árboles rojinegros.

### 3.1. Verificación Formal en *Coq*

Es claro que las pruebas unitarias no nos son suficientes para poder verificar formalmente un programa, es por esto que se requieren realizar demostraciones matemáticas para poder obtener los resultados que buscamos pero de igual manera no queremos escribir a mano estas demostraciones ya que al igual que las pruebas unitarias estas son susceptibles al error humano. Por esta razón es que es mejor que un sistema como *Coq* guíe la demostración para verificar cada paso, ya que a su vez esta herramienta esta verificada para asegurar que no se incluyan errores y también para garantizar la consistencia de las pruebas[Geuvers, 2009].

La verificación formal de un programa usando *Coq* esta compuesto de las siguientes etapas:

- Capturar los invariantes o propiedades de un programa usando definiciones inductivas en *Coq*, de esta manera podemos saber si las operaciones que se implementaron las respetan. Las operaciones pueden o no estar programadas en *Coq*.

- Enunciar lemas, corolarios y teoremas que describan los comportamientos de las operaciones que queremos verificar y escribirlos en *Coq*, usando las definiciones inductivas descritas en el punto anterior.
- Por último, demostrar todos los enunciados del punto anterior utilizando las tácticas que el asistente de pruebas nos provee.

### 3.1.1. Capturando invariantes de los árboles rojinegros

Una de las etapas más importantes al realizar la verificación formal en *Coq* de cualquier estructura de datos, inclusive de cualquier programa, es capturar sus invariantes de manera correcta, es decir, poder escribir una o varias definiciones inductivas que describan a la estructura de datos y sus invariantes. Después, con estas mismas es que se enuncian los lemas, clases y posteriormente instancias de las clases.

A continuación se describen dos conjuntos de definiciones inductivas, muy similares entre ellas<sup>1</sup>, los cuales nos ayudaran a verificar formalmente los árboles rojinegros. La primera es un primer intento que es insuficiente ya que los tipos inductivos y los principios de demostración no son los óptimos, es decir, describen correctamente lo que es un árbol rojinegro pero nos dificultan demasiado la demostración. El segundo intento es un conjunto de definiciones inductivas que tienen mas detalle para describir los invariantes. Estas definiciones están relacionadas con las propiedades de las operaciones de inserción y eliminación.

Es importante mencionar que estas definiciones aprovechan la expresividad de la lógica o de los tipos de *Coq* ya que se están usando a su vez otros tipos inductivos para describir las invariantes.

#### Primer conjunto de definiciones inductivas

Los dos conjuntos de definiciones inductivas comparten la misma idea: una definición que describe estrictamente lo que es un árbol rojinegro y otra definición más laxa de la misma. Utilizar una definición mas restrictiva que otra es una implementación, hasta cierto punto, de la técnica *divide y vencerás*<sup>2</sup>, la cual es una manera de resolver problemas mas complejos dividiéndolo en partes mas pequeñas. En este caso la división se realiza en las invariantes.

La primera definición llamada *isRB*<sup>3</sup> (listado 14) tiene tres casos, los cuales describiremos a continuación:

- **IsRB\_Leaf**: el árbol vacío con altura negra 0 es rojinegro. En este caso se tiene un sólo nodo, es decir, una hoja<sup>4</sup>.

<sup>1</sup>Obtenidas de los trabajos [López Campos, 2015] y [The Coq Team and contributors, 2011b] respectivamente.

<sup>2</sup>*Divide and conquer* en inglés.

<sup>3</sup>Las variables *n* y *c* se refieren a la altura negra y al color del nodo anterior, respectivamente.

<sup>4</sup>Recordemos que las hojas son vacías y de color negro.

```

Inductive isRB : Tree -> color -> nat -> Prop :=
| IsRB_leaf: forall c, isRB E c 0
| IsRB_r: forall t1 k tr n,
    isRB t1 Red n ->
    isRB tr Red n ->
    isRB (T Red t1 k tr) Black n
| IsRB_b: forall c t1 k tr n,
    isRB t1 Black n ->
    isRB tr Black n ->
    isRB (T Black t1 k tr) c (S n).

```

Listado 14: Función inductiva *isRB*.

- **IsRB\_r**: Para cualesquiera árboles *tl* y *tr* que cumplan con la definición *isRB* con color rojo y altura *n*, se cumple que un árbol de color rojo con *tl* y *tr* como subárboles, llamémosle *t*, cumple con *isRB* con color negro y altura *n*. El color se refiere al color del padre, en este caso, en la llamada de *isRB* a *tl* y *tr* se le pasa el color rojo porque *t* es rojo. La altura *n* se refiere a que hay *n* nodos negros en cualquier camino del nodo actual a alguna hoja, aquí no crece *n* porque tanto *tl* y *tr* son rojos.
- **IsRB\_b**: Para cualesquiera árboles *tl* y *tr* que cumplan con la definición *isRB* con color negro y altura *n*, se cumple que un árbol de color negro con *tl* y *tr* como subárboles, llamémosle *t*, cumple con *isRB* con cualquier color y altura *S(n)*. En este caso, en la llamada de *isRB* a *tl* y *tr* se le pasa el color negro porque *t* es negro y aquí se le suma uno a *n* porque tanto *tl* y *tr* son negros.

Con estos tres casos podemos asegurar que las invariantes se respetan, pero esta función inductiva es demasiado restrictiva y esto dificulta poder demostrar las propiedades de los árboles rojinegros, por esto pasamos a la segunda definición inductiva, *nearRB*, ésta permite mas flexibilidad en el árbol, se muestra y describe en el listado 15.

```

Inductive nearRB : Tree -> nat -> Prop :=
| nrRB_r: forall t1 k tr n,
    isRB t1 Black n ->
    isRB tr Black n ->
    nearRB (T Red t1 k tr) n
| nrRB_b: forall t1 k tr n,
    isRB t1 Black n ->
    isRB tr Black n ->
    nearRB (T Black t1 k tr) (S n).

```

Listado 15: Función inductiva *nearRB*.

Podemos apreciar que sólo se tienen dos casos y no se tiene un argumento para un color, sin embargo, a diferencia de *isRB* ésta no se llama recursivamente, en lugar de eso se llama a *isRB* inmediatamente, además podemos ver que ambas definiciones comparten el contador de nodos negros. Con estas modificaciones se permite una cosa, que en la raíz del árbol puedan haber a lo más dos nodos rojos contiguos.

**Intento de verificación** Utilizando las definiciones inductivas descritas en esta sección se realizó un intento fallido de verificación de la operación de inserción, como se muestra en [Appel, 2018]. Sin embargo, al estar desarrollando la demostración se encontró un problema: la falta de un conjunto de hipótesis para poder probar una meta. Esto se debe probablemente a una mala elección de estilo de demostración, implementación o de las definiciones inductivas mostradas anteriormente. Se notó que el hecho de que toda la información referente a los invariantes estuviera codificada en las dos funciones inductivas, sin uso de “funciones auxiliares” complica la verificación. Se llegó a esta conclusión ya que el caso “sencillo” de la verificación de árboles rojinegros es la inserción y con este conjunto de funciones inductivas las demostraciones se volvían muy largas y complicadas de seguir.

### Segundo conjunto de definiciones inductivas

Con el conocimiento que se obtuvo del conjunto de definiciones anterior, nos realizamos la siguiente pregunta: ¿cómo capturar las invariantes de los árboles rojinegros, y al mismo tiempo facilitar la verificación de éstos?

Utilizamos una definición inductiva, llamada *is\_redblack* para poder capturar los invariantes, la cual lleva como parámetros un contador y un árbol. El contador lleva el control de la cantidad de nodos negros, es decir, la altura negra del nodo, mientras que el árbol es aquel que estamos buscando verificar que cumpla con las invariantes de un árbol rojinegro. Se presenta esta definición en el listado 16.

```

Inductive is_redblack {a} `{GHC.Base.Ord a} : nat -> RB a -> Prop :=
| RB_Leaf : is_redblack 0 E
| RB_R n l k r : notred l -> notred r ->
    is_redblack n l -> is_redblack n r ->
    is_redblack n (T R l k r)
| RB_B n l k r : is_redblack n l -> is_redblack n r ->
    is_redblack (S n) (T B l k r).

```

Listado 16: Función inductiva *is\_redblack*.

Podemos notar ciertas similitudes con la definición inductiva de la sección pasada. Sin embargo, el principal cambio que presenta esta definición, es el hecho de que se dejan de controlar los colores de los subárboles en los parámetros de la definición y se crea la función *notred* la cual, como su nombre dice, verifica que

el árbol que se este pasando no tenga raíz roja. La definición *is\_redblack* tiene tres casos, *RB\_Leaf*, *RB\_R* y *RB\_B*. Desarrollando la idea de cada caso:

- **RB\_Leaf**: el árbol vacío es rojinegro. Este caso nos dice que el árbol vacío es un árbol rojinegro.
- **RB\_R**: un árbol rojo donde se lleven contabilizados  $n$  nodos negros, donde sus hijos sean árboles rojinegros y no sean rojos. Este caso nos dice explícitamente que los subárboles del árbol que esta recibiendo la función no pueden ser rojos, esto porque el árbol que se esta analizando tiene raíz roja. Como no se esta analizando algún nodo negro, la altura negra se mantiene en  $n$ .
- **RB\_B**: un árbol negro donde se lleven contabilizados  $n + 1$  nodos negros, incluido el actual, y sus hijos sean árboles rojinegros. En este último caso se tiene la libertad de que los subárboles sean de cualquier color, pero la altura del árbol de regreso es  $S(n)$  porque el nodo que se esta analizando es de color negro, los antecedentes al no tomar en cuenta a su nodo padre tienen altura  $n$ .

Esta definición captura los invariantes que estamos buscando, sin embargo, no es suficiente para poder probar la corrección de los árboles rojinegros. La definición es demasiado restrictiva y costaría mucho trabajo proceder con las demostraciones solamente con ella. Por esta razón se agregan dos definiciones inductivas auxiliares; *redred\_tree* y *nearly\_redblack* (listado 17).

```

Inductive redred_tree {a}
  `{GHC.Base.Ord a} (n:nat) : RB a -> Prop :=
| RR_Rd l k r : is_redblack n l -> is_redblack n r
               -> redred_tree n (T R l k r).

Inductive nearly_redblack {a}
  `{GHC.Base.Ord a} (n:nat)(t:RB a) : Prop :=
| ARB_RB : is_redblack n t -> nearly_redblack n t
| ARB_RR : redred_tree n t -> nearly_redblack n t.

```

Listado 17: Funciones inductivas *redred\_tree* y *nearly\_redblack*.

Podemos notar que estas definiciones son versiones menos restrictivas de *is\_redblack*. La definición *nearly\_redblack* permite que existan dos nodos rojos en la raíz del árbol, aprovechándose de *redred\_tree*, pues esta definición es exactamente el caso *RB\_R* de *is\_redblack* pero sin las restricciones de que los subárboles sean rojos, lo cual nos permite que hayan dos nodos rojos exactamente en la raíz. Entonces un *nearly\_redblack* es un árbol rojinegro con la excepción de que la raíz puede ser roja. Esto sucede porque si analizamos nuestras funciones de balanceo, no tenemos manera de pintar la raíz de negro mas que al utilizar la función *makeBlack* al final de las operaciones que se realicen.

Estas definiciones, a diferencia del conjunto anterior, utilizan mas acentuadamente la técnica de *divide y vencerás*. Es decir, se buscan demostrar definiciones mas laxas<sup>5</sup> para al final utilizar estos resultados para realizar la demostración de la definición más estricta.

Finalmente, lo que se busca demostrar es que los árboles rojinegros con las operaciones de inserción y eliminación estén dentro de la clase de árboles *redblack* (listado 18).

```
Class redblack {a} ` {GHC.Base.Ord a} (t:RB a) :=
  RedBlack : exists d, is_redblack d t.
```

Listado 18: Clase de árboles *redblack*.

Lo que estamos describiendo con el enunciado del listado 18 es que dado un árbol rojinegro ( $t: RB\ a$ ), existe una altura negra  $d$  que cumple con las invariantes establecidas por la definición *is\_redblack*. Esta clase<sup>6</sup> representa un refinamiento en los tipos inductivos para describir las invariantes de las estructuras de datos y es mas expresivo que los tipos de datos usados en la implementación de *Haskell*.

**Segundo intento de verificación** En contraste con el conjunto de definiciones de la sección pasada, la definición de *nearly\_redblack* se reescribe, dejando de codificar las invariantes en las llamadas recursivas de la definición, creando funciones auxiliares para capturar las invariantes de manera mas sencilla, como *redred\_tree* y *notred*. Además se crea la clase de árboles rojinegros, lo cual afina mas la definición de los mismos. Tomando en cuenta todas estas modificaciones a las definiciones fue que se eligió este conjunto para verificar formalmente la estructura de datos<sup>7</sup>. Estas definiciones inductivas fueron obtenidas de [The Coq Team and contributors, 2011b].

### 3.1.2. Verificación de la operación de inserción

Para poder realizar la verificación de la operación de inserción es necesario escribir enunciados, ya sean lemas, proposiciones, etc. Estos enunciados los escribiremos usando las definiciones inductivas presentadas en la sección pasada, es decir, *is\_redblack*, *nearly\_redblack* y *redred\_tree*.

A continuación mostraremos los lemas *ins\_rr\_rb*, *ins\_arb* y una instancia [Castéran and Sozeau, 2016] de la clase *redblack*, *add\_rb*. Estos lemas y la instancia fueron obtenidos de [The Coq Team and contributors, 2011b], la

<sup>5</sup>Sin todas las invariantes.

<sup>6</sup>Las clases en este contexto funcional se pueden ver, desde un alto nivel, como equivalencias a las clases del paradigma orientado a objetos.

<sup>7</sup>La elección de este conjunto fue correcta ya que facilitó la demostración de las propiedades y probó ser suficiente para verificar la estructura.

idea principal de estos enunciados es explicarnos que ciertos árboles de búsqueda que respeten las definiciones mas generales, es decir, *nearly\_redblack* y *redred\_tree*, también como consecuencia respetarán *is\_redblack*.

### Primer lema

```
Lemma ins_rr_rb {a} `{GHC.Base.Ord a} (x:a) (s: RB a) (n : nat) :
is_redblack n s ->
  ifred s (redred_tree n (ins x s)) (is_redblack n (ins x s)).
```

Figura 3.1: Lema *ins\_rr\_rb*.

En este primer lema (figura 3.1) enunciamos lo siguiente: sea  $s$  un árbol rojinegro bajo la definición de *is\_redblack*, entonces si  $s$  es un árbol con raíz roja, insertar un elemento  $x$  en  $s$  resulta en un árbol que cumple la definición de *redred\_tree*, en otro caso cumple con la definición de *is\_redblack*.

En otras palabras, lo que esta enunciado es que si tenemos un árbol rojinegro e insertamos un elemento a ese árbol, el resultado puede tener raíz roja, e incluso puede tener dos nodos rojos, uno en la raíz y otro en cualquiera de los dos, o incluso en los dos nodos siguientes.

La demostración de este lema comienza con una inducción sobre el antecedente del enunciado, lo cual resulta en tres casos:

```
-----(1/3)
ifred E (redred_tree 0 (ins x E)) (is_redblack 0 (ins x E))
-----
-----
ifred (T R l k r) (redred_tree n (ins x (T R l k r)))
                (is_redblack n (ins x (T R l k r)))
-----
-----
ifred (T B l k r) (redred_tree (S n) (ins x (T B l k r)))
                (is_redblack (S n) (ins x (T B l k r)))
```

La función *ifred* que se usa en este lema, es una función auxiliar que nos ayuda a decidir si un árbol es rojo o no.

En el primero de estos casos notamos que su solución se da simplificando las funciones y resulta en uno de los casos de *is\_redblack*, específicamente en el caso *RB\_R*, ya que el árbol vacío no es rojo y la simplificación de  $(ins(x, E))$  resulta en un árbol rojo con un elemento, esto por definición de *ins*.

Los dos casos sobrantes están relacionados con los colores de las raíces del árbol, en el segundo el árbol es rojo y en el tercero es negro.

Analicemos el segundo caso; como el árbol es rojo entramos al primer caso de *if\_red*, es decir, al caso donde se aplica la definición *redred\_tree*, lo cual significa que al insertar un elemento al árbol rojo, sin tener conocimiento de cómo son los subárboles de éste, puede resultar en un árbol con uno o dos nodos rojos consecutivos en la raíz del mismo. Ya que la operación de balanceo se fija

en los nodos hijos y nietos del nodo al que se le aplica la operación, y como los nodos hijos de la raíz no tienen nodo abuelo, el balanceo no se efectúa en los nodos de la raíz, dando lugar a árboles con uno o más nodos rojos consecutivos en la raíz<sup>8</sup>.

El caso sobrante, es decir, el caso del árbol con raíz negra se complica un poco más que el anterior ya que este es el caso en el que la altura negra del árbol se ve modificada, en otras palabras, puede aumentar en uno. Este caso se verifica con las dos funciones de balanceo, *lbal* y *rbal*:

```
H1_ : is_redblack n l
H1_0 : is_redblack n r
IHis_redblack1 :
  ifred l (redred_tree n (ins x l)) (is_redblack n (ins x l))
IHis_redblack2 :
  ifred r (redred_tree n (ins x r)) (is_redblack n (ins x r))
----- (1/2)
is_redblack (S n) (lbal (ins x l) k r)
----- (2/2)
is_redblack (S n) (rbal l k (ins x r))
```

Estos casos son análogos y los dos se resuelven simplificando las funciones de balanceo, en otros términos, simplificando las expresiones y aplicando las definiciones inductivas<sup>9</sup>.

### Segundo lema

```
Lemma ins_arb {a} `GHC.Base.Ord a} (x:a) (s:RB a) (n:nat) :
is_redblack n s -> nearly_redblack n (ins x s).
```

Figura 3.2: Lema *ins\_arb*

Este segundo lema (figura 3.2) enuncia lo que en el capítulo anterior se mencionó acerca de la función *ins*: la función *ins* no garantiza que el árbol resultante sea un árbol rojinegro, ya que es posible que se termine la ejecución de la función con un nodo rojo como raíz. La demostración comienza introduciendo los antecedentes a las hipótesis y aplicando el lema anterior, *ins\_rr\_rb*, a una de las hipótesis:

```
H1 : ifred s (redred_tree n (ins x s)) (is_redblack n (ins x s))
----- (1/1)
nearly_redblack n (ins x s)
```

Aplicamos el lema *ins\_rr\_rb* a la hipótesis porque éste nos genera dos casos, uno con la función *redred\_tree* y otro con *is\_redblack*. Lo que hace necesario

<sup>8</sup>Hasta 3, la raíz y sus hijos.

<sup>9</sup>*is\_redblack*, *nearly\_redblack*.

que se aplique este lema, es que con ayuda de las definiciones que introduce son con las que *nearly\_redblack* fue definido.

Como no se sabe si el árbol *s* tiene raíz roja o negra, se tienen que probar los dos casos: uno con la hipótesis de que el árbol resultante sea *is\_redblack* y otro con *redred\_tree*. Estos casos se resuelven sencillamente con la aplicación de alguno de los dos casos de la definición inductiva de *nearly\_redblack*, respectivamente.

### Instancia de la función de inserción

Para poder probar que el resultado de la inserción es una instancia de la clase *redblack*, es decir, que se cumplen con las propiedades descritas por la clase, vamos a necesitar el lema auxiliar que se encuentra en la figura 3.3:

```
Lemma makeBlack_rb {a} `{GHC.Base.Ord a} n t :
nearly_redblack n t -> redblack (makeBlack t).
```

Figura 3.3: Lema *makeBlack\_rb*

Este lema auxiliar se resuelve siguiendo la idea de que la definición inductiva *nearly\_redblack* únicamente viola las invariantes al poder tener dos nodos rojos consecutivos en su raíz, entonces, si se colorea la raíz de negro con la función *makeBlack*, el árbol resultante es un árbol rojinegro el cual respeta la definición de la clase *redblack*.

La figura 3.4 enuncia la instancia de inserción de la clase *redblack*, la cual también nos generará una demostración:

```
Instance add_rb {a} `{GHC.Base.Ord a} (x:a) (s: RB a) :
redblack s -> redblack (insert x s).
```

Figura 3.4: Instancia de inserción de la clase *redblack*.

Para poder crear la instancia de la clase *redblack* es necesario usar la definición *insert*, la cual es una envoltura para la función *ins*. Esta función lo que hace es colorear la raíz del árbol resultante de la función *ins* de color negro. De esta manera podemos asegurar que el árbol resultante ya no entra en la definición de *redred\_tree*.

```
H1 : is_redblack n s
-----(1/1)
redblack (makeBlack (ins x s))
```

En este momento se utiliza el lema auxiliar *makeBlack\_rb* el cual nos devuelve lo siguiente:

```
H1 : is_redblack n s
----- (1/1)
nearly_redblack n (ins x s)
```

Esta última meta se resuelve aplicando el segundo lema que enunciamos, *ins\_arb*, lo cual nos deja con una meta idéntica a la hipótesis H1 y con esto terminamos la verificación de la operación de inserción.

Se puede decir que esta implementación de la función de inserción es correcta respecto a las invariantes establecidas en la definición inductiva *is\_redblack*. La operación ha sido verificada formalmente, ahora continuaremos con la función de eliminación.

### 3.1.3. Verificación de la operación de eliminación

Al igual que en la función de inserción se enuncian lemas para ayudarnos a llegar al resultado de verificar la operación de eliminación. Estos lemas giran en torno a las funciones auxiliares que se usaron para poder demostrar la operación, como *append* y *del*.

A continuación se describe el razonamiento usado para poder verificar dichas funciones.

#### Primer lema

La función más importante para la operación de eliminación es *append*, la cual concatena dos subárboles. Estos dos subárboles son el resultado de buscar, encontrar y eliminar un nodo. En este primer lema se enuncia lo antes descrito: que para cualesquiera dos árboles si estos cumplen con la definición inductiva de *is\_redblack*, ambos con altura *n*, el resultado de concatenar es casi un árbol rojinegro, en otras palabras, la concatenación cumple con la definición de *nearly\_redblack*. Pero si los árboles que se van a concatenar además de cumplir con *is\_redblack*, también cumplen con *notred*, es decir, las raíces de dichos árboles no son rojas, el resultado de concatenar respeta también la definición *is\_redblack*. La demostración de este lema en *Coq* se describe en seguida:

```
----- (1/1)
Forall (r : RB a) (n : nat),
  is_redblack n l
-> is_redblack n r
  /\ (notred l -> notred r -> is_redblack n (append l r))
```

En esta primera etapa de la demostración podemos ver lo que se describió en el párrafo anterior. Se decidió proseguir con esta demostración usando inducción, primero sobre el árbol *l* y posteriormente sobre *r*. Los casos base de estas inducciones consisten en simplificación de las expresiones y fácilmente se llega a una hipótesis o a una contradicción. Estos casos no se tratarán más a fondo en este trabajo, pasaremos directamente a los casos más interesantes.

```

Lemma append_arb_rb {a} `GHC.Base.Ord a (n:nat) (l r: RB a) :
  is_redblack n l -> is_redblack n r ->
  (nearly_redblack n (append l r)) /\
  (notred l -> notred r -> is_redblack n (append l r)).

```

Figura 3.5: Lema *append\_arb\_rb*.

```

----- (1/4)
forall n : nat,
is_redblack n (T R ll lx lr)
-> is_redblack n (T R rl rx rr)
-> nearly_redblack n (append (T R ll lx lr) (T R rl rx rr))
/\ (notred (T R ll lx lr)
-> notred (T R rl rx rr)
-> is_redblack n (append (T R ll lx lr) (T R rl rx rr)))
----- (2/4)
forall n : nat,
is_redblack n (T R ll lx lr)
-> is_redblack n (T B rl rx rr)
-> nearly_redblack n (append (T R ll lx lr) (T B rl rx rr))
/\ (notred (T R ll lx lr)
-> notred (T B rl rx rr)
-> is_redblack n (append (T R ll lx lr) (T B rl rx rr)))
----- (3/4)
forall n : nat,
is_redblack n (T B ll lx lr)
-> is_redblack n (T R rl rx rr)
-> nearly_redblack n (append (T B ll lx lr) (T R rl rx rr))
/\ (notred (T B ll lx lr)
-> notred (T R rl rx rr)
-> is_redblack n (append (T B ll lx lr) (T R rl rx rr)))
----- (4/4)
forall n : nat,
is_redblack n (T B ll lx lr)
-> is_redblack n (T B rl rx rr)
-> nearly_redblack n (append (T B ll lx lr) (T B rl rx rr))
/\ (notred (T B ll lx lr)
-> notred (T B rl rx rr)
-> is_redblack n (append (T B ll lx lr) (T B rl rx rr)))

```

Figura 3.6: Casos del lema *append\_arb\_rb*.

Esta doble inducción nos deja con los siguientes cuatro casos, expuestos en la figura 3.6:

- Los árboles a concatenar son rojos.
- El árbol que se concatenará a la izquierda es rojo y el derecho es negro.
- El árbol que se concatenará a la izquierda es negro y el derecho es rojo.
- Los árboles a concatenar son negros.

En estos cuatro casos se cuida el hecho de no desbalancear el árbol, en otras palabras, que la altura negra sea la misma al terminar de la concatenación. Por eso es que se tiene cuidado especial en los casos donde se manejan nodos negros, ya que éstos son los únicos nodos considerados para el balanceo.

En las siguientes subsecciones explicamos mas a fondo los pasos usados para probar estos casos.

**Concatenación de dos árboles rojos.** Este primer caso es la concatenación de dos árboles con raíces rojas, en el siguiente fragmento de la salida del asistente de pruebas se observa cómo la meta es una conjunción.

```
IHlr : forall (r : RB a) (n : nat),
  is_redblack n lr
  -> is_redblack n r
    -> nearly_redblack n (append lr r)
      /\ (notred lr -> notred r -> is_redblack n (append lr r))
IHrl : forall n : nat,
  is_redblack n (T R ll lx lr)
  -> is_redblack n rl
    -> nearly_redblack n (append (T R ll lx lr) rl)
      /\ (notred (T R ll lx lr)
        -> notred rl -> is_redblack n (append (T R ll lx lr) rl))
-----(1/1)
forall n : nat,
  is_redblack n (T R ll lx lr)
  -> is_redblack n (T R rl rx rr)
    -> nearly_redblack n (append (T R ll lx lr) (T R rl rx rr))
      /\ (notred (T R ll lx lr)
        -> notred (T R rl rx rr)
          -> is_redblack n (append (T R ll lx lr) (T R rl rx rr)))
```

Podemos observar que la segunda parte de la conjunción es una contradicción, ya que al introducir los antecedentes de la meta tendríamos lo siguiente:

```
H21 : notred (T R ll lx lr)
H22 : notred (T R rl rx rr)
-----(1/1)
is_redblack n (append (T R ll lx lr) (T R rl rx rr))
```

Evidentemente las dos funciones *notred* de las hipótesis *H21* y *H22* se evalúan a falso y por esto es una contradicción.

Nos queda por demostrar la primera parte de la conjunción. La meta de este caso, como se ve en seguida, es que al ser concatenados un par de árboles rojos el árbol resultante cumple con la definición de ser de *nearly\_redblack*, es decir, que la raíz del árbol puede tener dos nodos rojos consecutivos.

```
----- (1/2)
nearly_redblack n (append (T R ll lx lr) (T R rl rx rr))
```

El siguiente paso sería simplificar esta expresión, la cual cae en el caso de dos nodos rojos de la función *append* y nos resulta en la siguiente meta:

```
----- (1/1)
redred_tree n
  match append lr rl with
  | T R lr' x rl' => T R (T R ll lx lr') x (T R rl' rx rr)
  | _ => T R ll lx (T R (append lr rl) rx rr)
  end
```

Podemos ver que la caza de patrones depende de la evaluación de la expresión *append(lr, rl)*, digamos *rbt*, esto nos daría dos casos:

- El primer caso, como se ve en seguida, se puede resolver usando las definiciones inductivas de *redred\_tree* e *is\_redblack*, y las metas resultantes son resultados directos de aplicar las hipótesis que se muestran.

```
H8 : notred lr
H9 : is_redblack n ll
H14 : notred rl
H16 : notred rr
H18 : is_redblack n rr
H19 : nearly_redblack n E
H20 : notred lr -> notred rl -> is_redblack n E
H21 : redred_tree n E
----- (1/2)
redred_tree n (T R ll lx (T R E rx rr))
```

- El segundo caso es un poco más complejo, pues se tienen que ver los casos en que *rbt*, resulta en un árbol con raíz roja y negra:

- En caso de que el árbol sea rojo, se aplica de igual manera las definiciones inductivas mencionadas en el caso anterior y las metas resultantes son implicaciones directas de las hipótesis que se muestran.

```
H6 : notred ll
H9 : is_redblack n ll
H14 : notred rl
```

```

H16 : notred rr
H20 : notred lr ->
      notred rl -> is_redblack n (T R r1_1 a0 r1_2)
----- (1/1)
redred_tree n (T R (T R ll lx r1_1) a0 (T R r1_2 rx rr))

```

- El caso donde el árbol es negro, al igual que en el caso pasado se hacen uso de las definiciones inductivas ya mencionadas y se siguen directamente de las siguientes hipótesis.

```

H6 : notred ll
H8 : notred lr
H9 : is_redblack n ll
H10 : is_redblack n lr
H14 : notred rl
H16 : notred rr
H17 : is_redblack n rl
H18 : is_redblack n rr
H19 : nearly_redblack n (T B r1_1 a0 r1_2)
H20 : notred lr ->
      notred rl -> is_redblack n (T B r1_1 a0 r1_2)
----- (1/1)
redred_tree n (T R ll lx (T R (T B r1_1 a0 r1_2) rx rr))

```

Con este procedimiento queda demostrado este caso de concatenar/unir dos árboles rojos con la función *append*. Se puede apreciar como los pasos de la demostración tienden a repetirse, esto puede significar que existan una serie de comandos y/o tácticas del asistente de pruebas que nos ayuden a acortar esta prueba. Sin embargo, en éste trabajo se está tomando el camino más extenso para mostrar la simplificación de la línea de pensamiento al demostrar estructuras complejas.

**Concatenación de un árbol rojo y uno negro.** Ahora es turno de analizar la demostración del caso donde se concatena un árbol rojo y uno negro, es decir,  $append(r, b)$ , donde  $r$  es un árbol rojo y  $b$  es uno negro.

```

IHlr : forall (r : RB a) (n : nat),
  is_redblack n lr
-> is_redblack n r
  -> nearly_redblack n (append lr r)
  /\ (notred lr -> notred r -> is_redblack n (append lr r))
----- (1/1)
forall n : nat,
  is_redblack n (T R ll lx lr)
-> is_redblack n (T B rl rx rr)
-> nearly_redblack n (append (T R ll lx lr) (T B rl rx rr))
  /\ (notred (T R ll lx lr)

```

```

-> notred (T B rl rx rr)
-> is_redblack n (append (T R ll lx lr) (T B rl rx rr))

```

En este segundo caso la conjunción también contiene una contradicción en la mitad derecha de ésta, ya que se tiene *notred* ( $T R ll lx lr$ ), entonces al igual que el caso pasado sólo resolveremos la primera mitad de la conjunción. Para esta demostración tenemos que guiar al asistente de pruebas un poco más de lo normal, pues le tenemos que decirle que  $r$  y el árbol ( $T B rl rx rr$ ) son el mismo.

```

r := T B rl rx rr : RB a
IHlr : forall n : nat,
  is_redblack n lr
-> is_redblack n r
  -> nearly_redblack n (append lr r)
    /\ (notred lr -> notred r -> is_redblack n (append lr r))
n : nat
H1 : is_redblack n (T R ll lx lr)
H2 : is_redblack n r
----- (1/1)
nearly_redblack n (T R ll lx (append lr r))

```

Podemos observar que se realizó una simplificación de la meta, donde se desarrolló lo mas posible la función `append` y se introdujeron los antecedentes a las hipótesis. Para poder demostrar esta nueva meta tenemos que destruir la hipótesis ‘IHlr’, lo cual nos introduciría los dos antecedentes de la misma como metas. Se destruye esta hipótesis para poder obtener su consecuente como hipótesis.

```

r := T B rl rx rr : RB a
IHlr : forall n : nat,
  is_redblack n lr
-> is_redblack n r
  -> nearly_redblack n (append lr r)
    /\ (notred lr -> notred r -> is_redblack n (append lr r))
IHrl : forall n : nat,
  is_redblack n (T R ll lx lr)
-> is_redblack n rl
  -> nearly_redblack n (append (T R ll lx lr) rl)
    /\ (notred (T R ll lx lr)
      -> notred rl -> is_redblack n (append (T R ll lx lr) rl))
n : nat
H1 : is_redblack n (T R ll lx lr)
H2 : is_redblack n r
----- (1/3)
is_redblack n lr
----- (2/3)
is_redblack n r

```

```

----- (3/3)
nearly_redblack n (T R ll lx (append lr r))

```

Para poder demostrar los dos primeros casos basta con aplicar la definición inductiva *is\_redblack*, lo cual nos introduce las hipótesis necesarias para poder cumplir las metas. Para el último caso nos basta de igual manera con aplicar la misma definición inductiva a H1 y a la meta aplicar las definiciones de *nearly\_redblack* y *redred\_tree* y esto nos da metas, que gracias a las nuevas hipótesis integradas por H1, se pueden probar sin mayor problema.

Con esto demostrado este caso está completo.

**Concatenación de un árbol negro y uno rojo.** En este caso se invierten los colores con respecto al caso anterior; el árbol derecho es rojo y el izquierdo es negro. Este caso, al igual que el pasado, requiere de una pequeña ayuda al asistente de pruebas, la cual explicaremos más adelante.

```

IHlr : forall (r : RB a) (n : nat),
  is_redblack n lr
-> is_redblack n r
  -> nearly_redblack n (append lr r)
    /\ (notred lr -> notred r -> is_redblack n (append lr r))
IHrl : forall n : nat,
  is_redblack n (T B ll lx lr)
-> is_redblack n rl
  -> nearly_redblack n (append (T B ll lx lr) rl)
    /\ (notred (T B ll lx lr)
      -> notred rl -> is_redblack n (append (T B ll lx lr) rl))
----- (1/1)
forall n : nat,
  is_redblack n (T B ll lx lr)
-> is_redblack n (T R rl rx rr)
  -> nearly_redblack n (append (T B ll lx lr) (T R rl rx rr))
    /\ (notred (T B ll lx lr)
      -> notred (T R rl rx rr)
      -> is_redblack n (append (T B ll lx lr) (T R rl rx rr)))

```

En este caso al igual que los dos pasados, como uno<sup>10</sup> de los arboles es de color rojo, la segunda parte de la conjunción vuelve a ser una contradicción, por la expresión *notred*.

Entonces sólo nos quedamos con la primera mitad de la conjunción:

```

l := T B ll lx lr : RB a
IHrl : forall n : nat,
  is_redblack n l
-> is_redblack n rl

```

---

<sup>10</sup>O los dos.

```

      -> nearly_redblack n (append l rl)
      /\ (notred l -> notred rl -> is_redblack n (append l rl))
n : nat
H1 : is_redblack n l
H2 : is_redblack n (T R rl rx rr)
----- (1/2)
nearly_redblack n (T R (append l rl) rx rr)

```

Podemos apreciar que este caso es el caso espejo del caso pasado, entonces el procedimiento a usar para demostrar esta meta es el mismo, lo único que cambia es cuáles hipótesis se usan para lograr esto. En el caso pasado se destruyó la hipótesis IHlr, en este caso se usa su contraparte IHrl y el resto de la demostración se sigue directamente de las nuevas metas introducidas y del uso de las definiciones inductivas mencionadas en el caso pasado.

**Concatenación de dos árboles negros.** Este último caso es el único que no incluye una contradicción ya que ésta se daba al tener un árbol rojo como uno de los dos árboles que se pasan a la función *append*, pero en este caso los dos árboles a concatenar son negros, entonces la conjunción completa será probada.

```

IHlr : forall (r : RB a) (n : nat),
  is_redblack n lr
  -> is_redblack n r
  -> nearly_redblack n (append lr r)
  /\ (notred lr -> notred r -> is_redblack n (append lr r))
IHrl : forall n : nat,
  is_redblack n (T B ll lx lr)
  -> is_redblack n rl
  -> nearly_redblack n (append (T B ll lx lr) rl)
  /\ (notred (T B ll lx lr)
      -> notred rl -> is_redblack n (append (T B ll lx lr) rl))
----- (1/1)
forall n : nat,
  is_redblack n (T B ll lx lr)
  -> is_redblack n (T B rl rx rr)
  -> nearly_redblack n (append (T B ll lx lr) (T B rl rx rr))
  /\ (notred (T B ll lx lr)
      -> notred (T B rl rx rr)
      -> is_redblack n (append (T B ll lx lr) (T B rl rx rr)))

```

Esta demostración se inicia con una inducción sobre la altura negra, es decir, una inducción sobre  $n$ . Esto porque hacer la inducción sobre esta propiedad nos garantiza que el resultado de la concatenación no estará desbalanceado.

Esta inducción nos da el caso base con  $n = 0$ , seguido de la separación de la conjunción y esto nos da 2 casos base, como se muestra en seguida:

```

IHlr : forall n : nat,
  is_redblack n lr
  -> is_redblack n rl
      -> nearly_redblack n (append lr rl)
          /\ (notred lr -> notred rl -> is_redblack n (append lr rl))
IHrl : forall n : nat,
  is_redblack n (T B ll lx lr)
  -> is_redblack n rl
      -> nearly_redblack n (append (T B ll lx lr) rl)
          /\ (notred (T B ll lx lr)
              -> notred rl -> is_redblack n (append (T B ll lx lr) rl))
H1 : is_redblack 0 (T B ll lx lr)
H2 : is_redblack 0 (T B rl rx rr)
----- (1/2)
nearly_redblack 0 (append (T B ll lx lr) (T B rl rx rr))
----- (2/2)
notred (T B ll lx lr)
-> notred (T B rl rx rr)
-> is_redblack 0 (append (T B ll lx lr) (T B rl rx rr))

```

Estos casos base se resuelven aplicando las definiciones inductivas correspondientes tanto a las metas como a las hipótesis H1 y H2, esto nos da las hipótesis necesarias para probar estos dos casos.

Nos queda por probar el paso inductivo, en seguida podemos ver que la hipótesis de inducción ‘IH’ es parte de IHlr, la cual se obtuvo de destruir esa hipótesis, en el siguiente paso se explica por qué se decidió destruir esta hipótesis y no su contraparte IHrl.

```

IHlr : forall n : nat,
  is_redblack n lr
  -> is_redblack n rl
      -> nearly_redblack n (append lr rl)
          /\ (notred lr -> notred rl -> is_redblack n (append lr rl))
IHrl : forall n : nat,
  is_redblack n (T B ll lx lr)
  -> is_redblack n rl
      -> nearly_redblack n (append (T B ll lx lr) rl)
          /\ (notred (T B ll lx lr)
              -> notred rl -> is_redblack n (append (T B ll lx lr) rl))
n : nat
H1 : is_redblack (S n) (T B ll lx lr)
H2 : is_redblack (S n) (T B rl rx rr)
IH : nearly_redblack n (append lr rl)
----- (1/1)
nearly_redblack (S n) (append (T B ll lx lr) (T B rl rx rr))
/\ (notred (T B ll lx lr)

```

```
-> notred (T B rl rx rr)
  -> is_redblack (S n) (append (T B ll lx lr) (T B rl rx rr)))
```

Proseguimos con la separación de la conjunción, lo cual nos da dos casos que trabajaremos por separado:

### Primera mitad de conjunción

```
----- (1/1)
nearly_redblack (S n) (append (T B ll lx lr) (T B rl rx rr))
```

Después de simplificar la meta de este caso, nos queda una meta que depende del resultado de una llamada recursiva a *append* de los subárboles *lr* y *rl*, lo cual nos genera otros dos casos:

```
----- (1/2)
is_redblack (S n) (lbalS ll lx (T B E rx rr))
----- (2/2)
is_redblack (S n)
  match c with
  | R => T R (T B ll lx r1) a0 (T B r2 rx rr)
  | B => lbalS ll lx (T B (T c r1 a0 r2) rx rr)
  end
```

Como podemos ver en ambas metas, tenemos una función nueva, *lbalS*. Esta es una función de balanceo, la cual extiende a las funciones que ya se habían usado con anterioridad en la función de inserción, como lo son *rba'*, *rba* y *lba*.

Para poder resolver esta parte de la demostración nos apoyaremos de otro lema (figura 3.7), el cual ilustra una propiedad de la operación *lbalS*.

```
Lemma lbalS_rb {a} `{GHC.Base.Ord a}
(n : nat) (l : RB a) (x : a) (r : RB a) :
nearly_redblack n l -> is_redblack (S n) r ->
  notred r -> is_redblack (S n) (lbalS l x r).
```

Figura 3.7: Lema *lbalS\_rb*.

Lo que el lema, arriba escrito en sintaxis de *Coq*, quiere decir es que si tenemos un par de árboles, sean *l* y *r*, un número natural *n* y un elemento *x*, si el árbol *l* cumple con la definición inductiva *nearly\_redblack* y *r* no es de color rojo y cumple con la definición inductiva *is\_redblack*, entonces balancear estos dos árboles con *lbalS* resulta en un árbol rojinegro que cumple con la definición *is\_redblack*.

La demostración de este lema se convierte en un análisis de casos en el cual solamente es necesario simplificar, aplicar las definiciones inductivas y las metas que se generan son consecuencias directas de las hipótesis generadas, la inducción no es necesaria.

Regresando a las dos metas generadas por destruir la función *append*, si nos fijamos en la primera, podemos ver que se puede aplicar directamente el lema *lbalS<sub>r</sub>b*, lo cual nos genera 3 nuevas metas:

```
H1 : is_redblack (S n) (T B ll lx lr)
H2 : is_redblack (S n) (T B rl rx rr)
IH : nearly_redblack n E
----- (1/3)
nearly_redblack n ll
----- (2/3)
is_redblack (S n) (T B E rx rr)
----- (3/3)
notred (T B E rx rr)
```

Estas metas de nuevo caen en el caso de simplificar y aplicar las respectivas definiciones inductivas para obtener las metas deseadas, de esta manera el primer caso queda resuelto.

Ahora nos vamos al segundo caso generado al destruir la función *append* el cual nos dice que tenemos que hacer un análisis de casos sobre el color del nodo:

```
H1 : is_redblack (S n) (T B ll lx lr)
H2 : is_redblack (S n) (T B rl rx rr)
IH : nearly_redblack n (T R r1 a0 r2)
----- (1/2)
is_redblack (S n) (T R (T B ll lx r1) a0 (T B r2 rx rr))
----- (2/2)
is_redblack (S n) (lbalS ll lx (T B (T B r1 a0 r2) rx rr))
```

Ese análisis de casos nos da dos metas nuevas, una por color. El primer caso solamente requiere simplificación y aplicación de definiciones inductivas para obtener las metas deseadas. El segundo caso sigue los mismos pasos con la única diferencia de volver a aplicar el lema *lbalS*.

De esta manera queda demostrada la primera mitad de la conjunción.

### Segunda mitad de conjunción

```
----- (1/1)
notred (T B ll lx lr)
-> notred (T B rl rx rr)
  -> is_redblack (S n) (append (T B ll lx lr) (T B rl rx rr))
```

Esta segunda mitad sigue exactamente el mismo procedimiento antes descrito con la única diferencia de que se agregan hipótesis nuevas:

```
H1 : is_redblack (S n) (T B ll lx lr)
H2 : is_redblack (S n) (T B rl rx rr)
IH : nearly_redblack n (append lr rl)
```

```

H3 : notred (T B ll lx lr)
H4 : notred (T B rl rx rr)
----- (1/1)
is_redblack (S n)
  match append lr rl with
  | T R lr' x rl' => T R (T B ll lx lr') x (T B rl' rx rr)
  | _ => lbalS ll lx (T B (append lr rl) rx rr)
  end

```

Al hacer el análisis de casos destruyendo la función *append* con los parámetros *lr* y *rl*, obtenemos exactamente las mismas metas que en la primera parte de la conjunción y al tener mas hipótesis la demostración se acorta por un par de pasos pero el procedimiento es el mismo.

De esta manera queda demostrado el primer lema. A pesar de ser larga y tediosa, se puede observar el poder del asistente de pruebas, ya que las demostraciones se reducen a álgebra ecuacional, es decir, tratar de igualar la meta con lo que se tiene como hipótesis. Esto se seguirá viendo en las siguientes pruebas.

```

Lemma del_arb {a} `{GHC.Base.Ord a} (s:RB a) (x:a) (n:nat) :
  is_redblack (S n) s ->
  isblack s -> nearly_redblack n (del x s)
with del_rb {a} `{GHC.Base.Ord a} (s:RB a) (x:a) (n:nat) :
  is_redblack n s ->
  notblack s -> is_redblack n (del x s).

```

Figura 3.8: Lema *del\_arb*

## Segundo lema

Este siguiente lema utiliza una palabra especial en el lenguaje de *Coq*, *with*. Esta palabra es un truco para demostrar dos lemas simultáneamente, el cual es el caso como se ve en la figura 3.8.

Como podemos ver, el lema en sí define dos lemas. Esto se hace de esta manera porque la demostración de uno de estos lemas depende del otro. De esta manera podemos definir ambos lemas y sólo usar una sola prueba.

```

del_arb : forall (a : Type) (H : Base.Eq_ a) (HO : Base.Ord a)
  (s : RB a) (x : a) (n : nat),
  is_redblack (S n) s ->
  isblack s -> nearly_redblack n (del x s)
del_rb : forall (a : Type) (H : Base.Eq_ a) (HO : Base.Ord a)
  (s : RB a) (x : a) (n : nat),
  is_redblack n s ->
  notblack s -> is_redblack n (del x s)
----- (1/2)

```

```

is_redblack (S n) s -> isblack s -> nearly_redblack n (del x s)
----- (2/2)
is_redblack n s -> notblack s -> is_redblack n (del x s)

```

Lo que el asistente de pruebas está haciendo es que nos está integrando al ambiente de hipótesis los dos lemas. De esta manera podemos realizar suposiciones con éstos y así ayudarnos a demostrar los lemas. Realizaremos las pruebas de estos lemas por separado.

### Prueba de *del\_arb*

```

----- (1/1)
is_redblack (S n) s -> isblack s -> nearly_redblack n (del x s)

```

Este lema enuncia lo siguiente: sea un árbol  $s$ , un elemento  $x$  y un número natural  $n$ , si  $s$  cumple con la definición inductiva *is\_redblack* y  $s$  es negro, entonces  $s$  cumple con la definición de *nearly\_redblack* después de eliminar el elemento  $x$ . En otras palabras, si tenemos un árbol con la raíz de color negro, el resultado de eliminar un elemento será un árbol casi rojinegro.

La prueba empieza con una inducción sobre  $s$  lo cual nos da las dos metas siguientes:

```

----- (1/2)
forall n : nat, is_redblack (S n) E ->
  isblack E -> nearly_redblack n (del x E)
----- (2/2)
forall n : nat,
  is_redblack (S n) (T c s1 a0 s2) ->
  isblack (T c s1 a0 s2) ->
  nearly_redblack n (del x (T c s1 a0 s2))

```

A primera vista podemos apreciar que la primera meta contiene un antecedente falso ya que el árbol vacío  $E$  no puede ser negro, entonces esta meta es una contradicción. La segunda meta podemos ver que si analizamos los dos casos del color del árbol, el caso rojo es igualmente una contradicción por el mismo antecedente *isblack*. Esto sólo nos deja con el caso negro de la segunda meta.

```

IHs1 : forall n : nat, is_redblack (S n) s1 ->
  isblack s1 -> nearly_redblack n (del x s1)
IHs2 : forall n : nat, is_redblack (S n) s2 ->
  isblack s2 -> nearly_redblack n (del x s2)
----- (1/1)
forall n : nat,
  is_redblack (S n) (T B s1 a0 s2)
-> isblack (T B s1 a0 s2) ->
  nearly_redblack n (del x (T B s1 a0 s2))

```

Después de introducir los antecedentes y simplificar la meta, se hace un análisis de casos sobre la operación *del*, primero se ve el caso si el nodo a eliminar está en el subárbol derecho y después en el izquierdo.

```

IHs1 : forall n : nat, is_redblack (S n) s1 ->
      isblack s1 -> nearly_redblack n (del x s1)
IHs2 : forall n : nat, is_redblack (S n) s2 ->
      isblack s2 -> nearly_redblack n (del x s2)
H1 : is_redblack (S n) (T B s1 a0 s2)
H2 : isblack (T B s1 a0 s2)
H6 : is_redblack n s1
H8 : is_redblack n s2
----- (1/2)
nearly_redblack n
match s1 with
| T B _ _ _ => lbalS (del x s1) a0 s2
| _ => T R (del x s1) a0 s2
end
----- (2/2)
nearly_redblack n
(if _GHC.Base.>_ x a0
 then
  match s2 with
  | T B _ _ _ => rbalS s1 a0 (del x s2)
  | _ => T R s1 a0 (del x s2)
  end
 else append s1 s2)

```

Seguimos con el análisis de los dos casos:

- En el primer caso seguimos con la destrucción del árbol *s1* para tener un análisis de casos, si simplificamos con las definiciones inductivas estas metas, eventualmente encontramos metas de las siguientes formas:

```
is_redblack n (del x E)
```

```
is_redblack n (del x (T R s1_1 a1 s1_2))
```

Estos casos son particulares del lema *del\_rb*, para solucionar esto usamos una táctica de *Coq* llamada *assert*, la cual nos deja agregar hipótesis, las cuales después tendremos que demostrar, en este caso ésta quedaría demostrada al terminar de demostrar todo este lema. Entonces como en este caso estamos destruyendo *s1*, la hipótesis a agregar sería:

```

IH1' : forall n : nat, is_redblack n s1 ->
      notblack s1 -> is_redblack n (del x s1)

```

Al agregarla al inicio de la prueba podemos solamente aplicarla cuando lleguemos a los casos arriba mencionados.

- El segundo caso se divide en dos, la primera parte es el caso espejo al pasado, se realiza lo mismo pero para el árbol  $s_2$ , lo cual nos da la siguiente hipótesis a agregar:

```
IHr' : forall n : nat, is_redblack n s2 ->
      notblack s2 -> is_redblack n (del x s2)
```

Se aplica de la misma manera y llegamos a la segunda parte donde nos resulta la siguiente meta:

```
----- (1/1)
nearly_redblack n (append s1 s2)
```

La cual es un caso particular del lema antes demostrado *append\_arb\_rb*.

### Prueba de *del\_rb*

```
----- (1/1)
is_redblack n s -> notblack s -> is_redblack n (del x s)
```

Este segundo lema enuncia lo siguiente: sea un árbol  $s$ , un elemento  $x$  y un número natural  $n$ , si  $s$  cumple con la definición inductiva *is\_redblack* y  $s$  no es negro, entonces  $s$  cumple con la definición de *is\_redblack* después de eliminar el elemento  $x$ . En otras palabras, si tenemos un árbol con la raíz de color rojo, el resultado de eliminar un elemento será un árbol casi rojinegro.

El enunciado con respecto al anterior busca que el resultado sea mas específico, pues la propiedad de ser *is\_redblack* es la que buscamos que las operaciones cumplan. Sin embargo, la demostración en términos de *Coq* no es muy distinta; iniciamos con inducción sobre  $s$ .

```
----- (1/2)
forall n : nat, is_redblack n E ->
  notblack E ->
  is_redblack n (del x E)
----- (2/2)
forall n : nat, is_redblack n (T c s1 a0 s2) ->
  notblack (T c s1 a0 s2) ->
  is_redblack n (del x (T c s1 a0 s2))
```

La primera meta se soluciona simplificando hasta obtener la meta deseada, mientras que la segunda meta se le hace un análisis sobre el color  $c$ , el cual arroja dos casos, rojo y negro. El caso de que  $c$  sea negro es una contradicción porque no cumple con la meta de ser *notblack*, solamente nos enfocaremos en el caso en que  $c$  es rojo.

```
IHs1 : forall n : nat,
  is_redblack n s1 ->
  notblack s1 -> is_redblack n (del x s1)
```

```

IHs2 : forall n : nat,
      is_redblack n s2 ->
      notblack s2 -> is_redblack n (del x s2)
H1 : is_redblack n (T R s1 a0 s2)
H2 : notblack (T R s1 a0 s2)
----- (1/1)
is_redblack n (del x (T R s1 a0 s2))

```

Al igual que en *del\_arb* se hacen los casos de si el elemento a eliminar está en el subárbol derecho o izquierdo. Otra similitud que esta prueba tiene con respecto con la pasada es que también tenemos que agregar una hipótesis extra, en este caso de *del\_arb*. De aquí en adelante la prueba es muy similar a la anterior, simplificar, aplicar definiciones inductivas hasta llegar a contradicciones o a las metas deseadas.

En este lema se usan lemas auxiliares muy similares a *lbalS\_rb*<sup>11</sup>, como su espejo *rbalS\_rb* o sus contrapartes *rbalS\_arb* y *lbalS\_arb*. Estos son lemas de balanceo sencillos de demostrar pero muy largos, tediosos y repetitivos, por lo tanto no se incluirán en este trabajo<sup>12</sup>.

Hasta este momento sólo se han demostrado partes de la operación total de eliminación, como unir dos subárboles después de eliminar su raíz, qué sucede si eliminamos de un árbol con raíz roja o de uno con raíz negra. En seguida uniremos todos estos lemas en uno.

### Instancia de la función de eliminación

```

Instance remove_rb s x : redblack s -> redblack (remove x s).

```

Figura 3.9: Instancia de eliminación de la clase *redblack*.

Al igual que en la función de inserción, terminamos la operación de eliminación generando una instancia de la clase *redblack* (figura 3.9). Al igual que en la operación opuesta, requerimos de un lema auxiliar con respecto a la clase *redblack* (figura 3.10).

```

Lemma makeBlack_rb {a} `{GHC.Base.Ord a} n t :
nearly_redblack n t -> redblack (makeBlack t).

```

Figura 3.10: Lema *makeBlack\_rb*.

Lo que este enunciado describe es la propiedad de que si un árbol *t* cumple con la definición inductiva de ser *nearly\_redblack*, pintar su raíz de color negro lo convierte en una instancia de la clase *redblack*. La demostración de este lema

<sup>11</sup>Descrito en la prueba de la función *append*.

<sup>12</sup>Se pueden consultar en: <https://github.com/DavidFHCh/Tesis-FTW>.

es muy simple gracias al asistente de pruebas, ya que sólo basta con hacer un análisis de casos sobre el árbol  $t$ :

- El árbol vacío  $E$ , la meta a demostrar para este caso es:

```
nearly_redblack n E -> redblack (makeBlack E)
```

Como la clase *redblack* esconde un existencial en su definición, para poder demostrar este caso basta con decir que existe  $n$  con valor 0, esto nos da un caso trivial al ser la misma definición inductiva de *is\_redblack*.

- El segundo caso se reduce a los dos casos en los que puede caer la definición inductiva de *nearly\_redblack*.

```
H1 : nearly_redblack n (T c t1 a0 t2)
H2 : is_redblack n (T c t1 a0 t2)
----- (1/2)
redblack (makeBlack (T c t1 a0 t2))
```

Este primer caso se reduce a hacer un análisis de casos sobre el color  $c$ , la solución de ambos colores consiste en, decir que existe  $n'$  tal que su valor es  $S(n)$ , después de esto se simplifican las expresiones hasta obtener que las metas cumplan con las hipótesis.

```
H1 : nearly_redblack n (T c t1 a0 t2)
H2 : redred_tree n (T c t1 a0 t2)
----- (2/2)
redblack (makeBlack (T c t1 a0 t2))
```

El segundo caso es más corto que el primero, ya que al hacer el análisis de los colores, podemos ver que la definición de *redred\_tree* no está definida para árboles negros, entonces sólo nos queda demostrar para árboles rojos. Sin embargo, los pasos a seguir para este caso son los mismos que para el color rojo del caso anterior.

Con este lema demostrado ya contamos con todas las herramientas para poder demostrar que si tenemos a un árbol que es instancia de la clase *redblack* y eliminamos un elemento de él, el árbol resultante sigue siendo instancia de la clase, esta demostración comienza con un análisis de casos sobre el árbol  $s$ :

```
H1 : is_redblack n E
----- (1/2)
redblack (makeBlack (del x E))
----- (2/2)
redblack (makeBlack (del x (T c s1 c0 s2)))
```

Podemos ver que se hace uso de la función *makeBlack*. En la primera meta basta con aplicar el lema *makeBlack\_rb*, simplificar y ésta se soluciona. En la segunda meta se tiene que hacer otro análisis de casos, esta vez sobre el color:

```
H1 : is_redblack n (T R s1 c0 s2)
----- (1/2)
redblack (makeBlack (del x (T R s1 c0 s2)))
```

En la primera meta, color rojo, comenzamos por aplicar *makeBlack\_rb*, el cual después de simplificar con la definición inductiva nos resulta en la siguiente meta:

```
H1 : is_redblack n (T R s1 c0 s2)
----- (1/1)
is_redblack n (del x (T R s1 c0 s2))
```

La cual es un caso particular del lema *del\_rb*, nos basta con aplicarlo, simplificar y esta meta queda resuelta. La única meta que nos quedaría por demostrar sería el caso de la raíz negra:

```
H1 : is_redblack n (T B s1 c0 s2)
----- (1/1)
redblack (makeBlack (del x (T B s1 c0 s2)))
```

En este caso hacemos un análisis sobre  $n$ , los dos casos serían 0 y  $S(n)$ . Para 0 basta con simplificar y la meta se resuelve, pero para  $S(n)$ , es necesario volver a aplicar el lema *makeBlack\_rb*, una vez que hacemos esto, nos queda la siguiente meta:

```
H1 : is_redblack (S n) (T B s1 c0 s2)
----- (1/1)
nearly_redblack n (del x (T B s1 c0 s2))
```

La cual resulta ser un caso particular del lema *del\_arb*, al aplicar este lema y simplificar nuevamente, las metas resultantes quedan resueltas. Podemos ver que las demostraciones cubiertas en este trabajo, en especial en la operación de eliminación, son muy repetitivas y sólo buscamos hacer que las metas empaten con las hipótesis que tenemos.

Con esta operación demostrada podemos decir que tenemos una estructura correcta respecto a los invariantes descritos por las definiciones inductivas de *is\_redblack* con las operaciones de borrado e inserción y de la misma manera que estas dos operaciones son métodos de la clase *redblack*, por lo cual podemos hacer estas operaciones cuantas veces queramos y el resultado seguirá siendo instancia de esta clase.



# Conclusiones

Como se ha ilustrado a lo largo de este trabajo, lo que buscamos es otra manera de demostrar la corrección de una estructura de datos, en este caso de árboles rojinegros usando un asistente de pruebas como lo es *Coq*, con traducciones de una biblioteca de tipos y funciones originarios de Haskell.

Hemos mencionado en repetidas ocasiones que la opción mas tradicional para realizar una prueba de este estilo sería usar lápiz y papel, pero como se ha visto en capítulos anteriores el desarrollo de la prueba puede llegar a tener demasiados casos. Esto lo convierte en una tarea muy complicada y tediosa de escribir, y posteriormente de leer y entender por alguien más. En cambio, un asistente de pruebas como *Coq* ayuda en organizar esta tarea, también puede simplificar y logra reducirla a usar álgebra ecuacional ya que, como se vio mayoritariamente en este trabajo, lo único que se busca obtener es que las metas que queremos probar se igualen con alguna de las hipótesis que se tienen. Esto también tiene sus detrimentos ya que se deja de razonar de manera formal.

Sin embargo, el uso de una herramienta de esta naturaleza por sí sola no simplifica del todo este tipo de pruebas. Para poder llegar a un escenario donde se pueda desarrollar una demostración primero se debe tener claro qué es lo que se quiere probar y codificarlo en el lenguaje que la herramienta comprenda.

En la vida real, esto significaría tener un programa escrito en algún lenguaje de programación como Java, Python, Haskell, etc. y traducirlo al lenguaje de la herramienta. Esto requeriría la implementación de un traductor o en su defecto traducir los programas a mano, esta segunda opción siendo una solución no óptima ya que es susceptible a errores. En este trabajo se usó el traductor de Haskell a *Coq* llamado *hs-to-coq* [Spector-Zabusky et al., 2017], que aunque nos dio algunas bibliotecas de Haskell traducidas a *Coq*, sigue en estado de desarrollo. Además, aunque Haskell comparte el mismo paradigma que el lenguaje de *Coq*, lograr traducir en un 100% un lenguaje resulta muy complicado ya que éste siempre está evolucionando, en especial si es un lenguaje tan ampliamente usado como lo es Haskell.

Otra restricción que se tiene que establecer es que no todos los programas escritos en Haskell podrían ser traducidos al lenguaje de *Coq*. Este lenguaje a pesar de que entra en la categoría de lenguajes funcionales, sólo acepta funciones totales. Esto introduce otras problemáticas: la traducción un programa de un paradigma imperativo, lógico, etc. a uno funcional y después asegurar que todas las funciones de éste son totales.

Supongamos que resolvemos todos estos problemas que se han presentado hasta ahora, es decir, tenemos un programa donde todas sus funciones son totales y se logró traducir correcta y completamente. Siguiendo nuestra metodología, se tienen que generar las definiciones inductivas las cuales ayudarán a guardar invariantes del programa, y con éstas escribir los lemas que se buscan probar para poder asegurar que el programa en cuestión ha sido verificado formalmente, lo cual podría tomar el mismo tiempo que tomó traducir todo el programa al lenguaje de la herramienta.

Actualmente en la industria lo que se hace para minimizar los errores en código es hacer que este pase por una serie de filtros, es decir, que otra persona revise el código para identificar defectos y ejecutar pruebas ya existentes. Con esto se busca asegurar que el nuevo código no introduzca errores a componentes que funcionaban correctamente dentro del programa y que se escriban pruebas que confirmen el correcto funcionamiento del código a introducir. En este momento la idea de poder probar que un programa cualquiera puede ser probado formalmente usando un asistente de pruebas es muy atractiva, ya que un único desarrollador podría desarrollar la prueba y no depender de código ajeno que muestre que su programa es correcto. Sin embargo, esta idea resulta muy poco factible hoy en día ya que, además de los problemas expuestos con anterioridad (las traducciones del código implementado), se suma el hecho de que se tendrían que traducir y probar todas las bibliotecas ocupadas del lenguaje que se está usando antes de pensar en probar un programa usando una herramienta como *Coq*.

Otro acercamiento para poder probar este tipo de programas en la industria sería desarrollar la mayor parte de estos en el asistente *Coq*. Realizando esto con las herramientas que su lenguaje nos provee, de esta manera se pueden realizar las demostraciones pertinentes y utilizar la funcionalidad que éste posee para extraer código en otros lenguajes, después de haber realizado la prueba, como lo son Haskell y O'Caml. Sin embargo, esto sólo nos permitiría desarrollar programas correctos con las funcionalidades que el lenguaje de *Coq* nos ofrezca.

Retomando el punto anterior, otra solución sería desarrollar y probar partes clave de los programas a crear, es decir, módulos pequeños como lo serían las estructuras de datos (árboles rojinegros, listas doblemente ligadas, colas, pilas, u otros tipos de árboles) o partes críticas de algún sistema. Una vez implementados estos módulos se podrían usar en cualquier parte de código. El inconveniente con hacer esto es que dependiendo del lenguaje al que se extraiga el programa probado, puede ser contraproducente para el desempeño del mismo. Este degradado en el desempeño se puede dar por razones ajenas al código y por asuntos relacionados a la implementación del compilador que se usará para generar código ejecutable y la optimización del mismo. Por ejemplo, el lenguaje C es conocido por ser muy usado en programas que requieren ser muy rápidos en sus operaciones.

Otro problema es que como no todo el código estaría probado formalmente, para componentes más grandes se necesitaría caer nuevamente en hacer otro tipo de pruebas, como las unitarias y las de integración, y como ya hemos mencionado, éstas no nos aseguran que los programas sean correctos o completos. Por lo

tanto, nuestros programas sólo estarían verificados formalmente *parcialmente*.

Como podemos apreciar, demostrar programas con un asistente de pruebas no es el procedimiento más amigable hoy en día, el tiempo que se debe invertir en aprender la herramienta o el esfuerzo para obtener una verificación lo más amplia posible son desventajas claras de estos métodos. Sin embargo, si se sigue con la actual trayectoria en el desarrollo de herramientas de traducción como lo es *hs-to-coq*, eventualmente la industria podría comenzar a utilizar herramientas de este estilo para mejorar la calidad de sus productos. Mientras tanto, se tendrán que seguir desarrollando pruebas unitarias de mejor calidad y lograr generar programas que tiendan a la corrección.



## Apéndice A

# Conceptos básicos de COQ

Para una mejor comprensión de las pruebas realizadas en este trabajo, daremos una breve explicación del asistente de pruebas *Coq*. Nos enfocaremos solamente en las características de *Coq* que se usaron en este trabajo. Este apéndice está basado en el manual del asistente que el lector puede consultar en [The Coq Team and contributors, 2011a].

Lo primero que se hace al querer probar un programa en *Coq* es escribirlo en su propio lenguaje llamado Gallina. Este contiene varias palabras reservadas para el desarrollo de funciones y de tipos especiales para el uso de las mismas, en seguida explicaremos las que se usaron:

- ***Inductive*** - Esta palabra reservada se refiere a un tipo al cual se le puede aplicar inducción estructural. Al usar esta palabra para definir a un tipo, se establecen los constructores, y en algunos casos, destructores. En el listado 19 presentamos un ejemplo de uso, definiendo los números naturales.

```
Inductive nat : Set :=  
| O : nat  
| S : nat -> nat.
```

Listado 19: Tipo Inductivo.

- ***Fixpoint*** - Esta palabra reservada se refiere a la definición de una función recursiva, aplicada a, al menos, un tipo inductivo definido con la palabra reservada ***Inductive***. El listado 20 presentamos una función recursiva usando el tipo definido arriba.
- ***Definition*** - Esta palabra reservada básicamente se refiere a una sustitución textual de una expresión por otra. En el listado 21 se hace una sustitución textual para aumentar en uno el valor de  $n$ .

En los mecanismos de definición anteriores se hace uso de la coincidencia de patrones o pattern matching. Los tipos inductivos también los usamos para

```

Fixpoint add (n m:nat) {struct n} : nat :=
match n with
| 0 => m
| S p => S (add p m)
end.

```

Listado 20: Función *Fixpoint*.

```

Definition add_one (n :nat) {struct n} : nat :=
match n with
| 0 => S (0)
| S p => S (S (p))
end.

```

Listado 21: Sustitución textual con *Definition*.

definir las invariantes o especificación formal del programa que se busca verificar. En el código *isRB* definimos la especificación de los árboles rojinegros.

Una vez escrito el programa y su especificación, procedemos a escribir lemas que nos ayuden a verificar la corrección con respecto a la especificación dada. Esto lo logramos con la palabra reservada ***Lemma***<sup>1</sup> (ver *ins\_rr\_rb*). Al usar esta palabra *Coq* entra en modo prueba, con lo cual se pueden usar las *tácticas*.

Las tácticas (ver listado 22) son palabras reservadas como: *intros*, *destruct*, *apply*, *constructor*, etc. Estas tácticas son funciones que nos ayudan a transformar el estado actual de una prueba, denominado *meta*. Una sucesión de tácticas eventualmente generan una prueba completa, a cual opcionalmente empieza con la palabra *Proof* y siempre termina con *Qed*.

```

(* lema que prueba que un arbol con al menos un elemento no es vacio.
*)
Lemma T_neq_E {a} ` {GHC.Base.Ord a}:
  forall (c:Color) (l: RB a) (k: a) (r: RB a), T c l k r <> E.
Proof.
intros. intro Hx. inversion Hx.
Qed.

```

Listado 22: Ejemplo del uso de tácticas y lemas.

Las metas (ver listado 23) consisten de dos partes: la conclusión y un contexto. El segundo contiene las hipótesis, definiciones y variables que podemos usar para demostrar la conclusión con el uso de las tácticas. En este trabajo se habla en alto nivel como se usaron las tácticas para verificar los árboles rojinegros.

<sup>1</sup>Además de esta palabra también se puede usar *Theorem*, *Proposition*, *Corolary*, para indicar una proposición.

```

H1_ : is_redblack n l
H1_0 : is_redblack n r
IHis_redblack1 :
  ifred l (redred_tree n (ins x l)) (is_redblack n (ins x l))
IHis_redblack2 :
  ifred r (redred_tree n (ins x r)) (is_redblack n (ins x r))
----- (1/2)
is_redblack (S n) (lbal (ins x l) k r)
----- (2/2)
is_redblack (S n) (rbal l k (ins x r))

```

Listado 23: Ejemplo de una *meta*.



# Bibliografía

- [Appel, 2018] Appel, A. W. (2018). Software foundations, volume 3, verified functional algorithms. [En línea; Consultado el 18 de enero de 2020].
- [Castéran and Sozeau, 2016] Castéran, P. and Sozeau, M. (2016). A gentle introduction to type classes and relations in coq. [En línea; Consultado el 12 de enero de 2020].
- [Geuvers, 2009] Geuvers, H. (2009). Proof assistants: History, ideas and future. *Sadhana*, 34:3–25.
- [HaskellDoc, 2005] HaskellDoc (2005). Data.ord. [En línea; Consultado el 30 de mayo de 2021].
- [HaskellWiki, 2020] HaskellWiki (2020). Curryng — haskellwiki. [En línea; Consultado el 21 de julio de 2020].
- [López Campos, 2015] López Campos, G. (2015). *Implementaciones funcionales de árboles roji-negros*. TESIUNAM. <http://tesis.unam.mx/> [Consultado el 12 de enero de 2020].
- [Okasaki, 1998] Okasaki, C. (1998). *Purely Functional Data Structures*. Cambridge University Press, USA.
- [Osherove, 2014] Osherove, R. (2014). *The Art of Unit Testing, Second Edition*. Manning Publications. [https://piazza.com/class\\_profile/get\\_resource/j11t8bsxngk3r3/j21w6zcyt5t61u](https://piazza.com/class_profile/get_resource/j11t8bsxngk3r3/j21w6zcyt5t61u) [En línea; Consultado el 30 de septiembre de 2020].
- [Peláez, 2019] Peláez, C. (2019). Material del curso de estructuras de datos. [En línea; Consultado el 6 de octubre de 2020].
- [Peláez Valdés, 2018] Peláez Valdés, C. (2018). *Estructuras de Datos con Java Moderno, 1a edición*. Facultad de Ciencias.
- [Spector-Zabusky et al., 2017] Spector-Zabusky, A., Breitner, J., Rizkallah, C., and Weirich, S. (2017). Total haskell is reasonable coq. *CoRR*, abs/1711.09286.

- [The Coq Team and contributors, 2011a] The Coq Team, Inria, C. and contributors (2011a). Definitions. [En línea; Consultado el 30 de mayo de 2021].
- [The Coq Team and contributors, 2011b] The Coq Team, Inria, C. and contributors (2011b). Msetrbt : Implementation of msetinterface via red-black trees. [En línea; Consultado el 18 de enero de 2020].
- [The Coq Team and contributors, 2011c] The Coq Team, Inria, C. and contributors (2011c). Tactics. [En línea; Consultado el 18 de febrero de 2021].