

Desarrollo de un sistema dinámico de verificación de software basado en un comprobador de satisfacibilidad lógica



Trabajo Fin de Máster del Máster Universitario de Investigación en
Ingeniería de Software y Sistemas Informáticos
de la Universidad Nacional de Educación a Distancia

Alumno: Diego J. Romero López
Directora: Prof. Dra. Dña. Elena Ruiz Larrocha

Curso: 2013/2014
Convocatoria de defensa: Septiembre

Trabajo de Fin de Máster

Asignatura: Trabajo Fin de Máster del Máster Universitario de Investigación en Ingeniería de Software y Sistemas Informáticos de la Universidad Nacional de Educación a Distancia.

Código: 31105128.

Itinerario: Ingeniería del Software.

Título: Desarrollo de un sistema dinámico de verificación de software basado en un comprobador de satisfacibilidad lógica.

Alumno: Diego J. Romero López

Directora: Prof. Dra. Dña. Elena Ruiz Larrocha

Calificaciones

Autorización

Autorizo a la Universidad Nacional de Educación a Distancia a difundir y utilizar, con fines académicos, no comerciales y mencionando expresamente a sus autores, tanto la memoria de este Trabajo Fin de Máster, como el código, la documentación y/o el prototipo desarrollado.

Firmado:

Diego Jesús Romero López

Resumen

Este trabajo presenta una herramienta original para la especificación y prueba de sistemas software complejos basada en la evaluación de expresiones lógicas usando Árboles Binarios de Decisión (BDDs). Además, se presenta un nuevo algoritmo de reducción de BDDs que obtiene mejoras sobre el estado del arte en este campo.

Palabras clave

Árbol Binario de Decisión, Algoritmos de reducción de BDDs, Especificación de Sistemas Software, Lógica Computacional, Representación de funciones booleanas, Verificación de Modelos.

Agradecimientos

Agradezco a la Prof. Dra. Dña. Elena Ruiz Larrocha el haberme dado la oportunidad de trabajar en este trabajo fin de máster.

También agradezco a mi familia el haberme apoyado de multitud de formas a lo largo de todo el máster y en especial, este trabajo que supone el colofón del mismo.

1 Índice

1. Índice.....	8
2. Lista de figuras y tablas.....	12
2.1. Figuras.....	12
2.1.1. Capítulo 5.....	12
2.1.2. Capítulo 7.....	13
2.1.3. Capítulo 8.....	13
2.1.4. Capítulo 9.....	13
2.1.5. Capítulo 10.....	13
2.2. Tablas.....	13
2.2.1. Capítulo 4.....	13
2.2.2. Capítulo 5.....	13
2.2.3. Capítulo 8.....	13
2.2.4. Capítulo 9.....	13
3. Introducción.....	15
4. Lógica proposicional.....	21
4.1. Definición.....	21
4.2. Constantes.....	22
4.3. Operadores.....	22
4.3.1. Operador de negación.....	22
4.3.2. Operador de conjunción.....	22
4.3.3. Operador de disyunción inclusiva.....	22
4.3.4. Resto de operadores.....	23
4.4. Precedencia.....	23
4.4.1. Propiedades.....	24
4.4.1.1. Propiedad asociativa.....	24
4.4.1.2. Propiedad distributiva.....	24
4.4.2. Leyes de De Morgan.....	24

5. Árboles Binarios de Decisión.....	25
5.1. Introducción.....	25
5.2. Árboles reducidos.....	27
5.2.1. No-redundancia.....	28
5.2.2. Unicidad de cada vértice.....	29
5.3. Orden de las variables.....	30
5.4. Definición.....	32
5.5. Operaciones.....	33
5.5.1. Creación.....	33
5.5.2. Apply.....	36
5.5.3. Not.....	38
5.5.4. Restrict.....	38
5.5.5. Swap.....	40
5.6. Algoritmos.....	44
5.6.1. Window Permutation.....	44
5.6.2. Sifting de Rudell.....	44
5.6.3. Algoritmo de intercambios aleatorios.....	45
5.6.4. Algoritmo genético.....	45
5.6.4.1. Estructuras de datos.....	45
5.6.4.2. Población inicial.....	45
5.6.4.3. Selección.....	46
5.6.4.4. Cruce.....	46
5.6.4.5. Mutación.....	46
5.6.4.6. Actualización de la población.....	46
5.6.5. Algoritmo memético.....	46
6. Un nuevo algoritmo de reducción: Iterative Sifting.....	48
7. Aplicaciones de los BDDs a la Ingeniería del Software.....	51
7.1. Introducción.....	51
7.2. Métodos Formales.....	51
7.3. Estado de los métodos formales en la industria.....	53
7.4. Métodos Formales basados en los BDDs.....	54
8. Software.....	56
8.1. Herramientas usadas.....	56
8.1.1. antlr3.....	56
8.1.2. Javaluator.....	58
8.2. Diseño.....	58
8.2.1. Paquete raíz: djbdd.....	58
8.2.1.1. core.....	58
8.2.1.1.1. VariableList.....	59
8.2.1.1.2. Vertex.....	59
8.2.1.1.3. TableT.....	60
8.2.1.1.4. BooleanEvaluator.....	64
8.2.1.1.5. BDD.....	64
8.2.1.1.6. BDDApply.....	64
8.2.1.1.7. GCThread.....	65
8.2.1.2. io.....	65
8.2.1.3. logic.....	66

8.2.1.4. main.....	66
8.2.1.5. reductors.....	67
8.2.1.6. test.....	67
8.2.2. timemeasurer.....	68
8.2.3. graphvizjava.....	68
8.2.4. logger.....	68
8.3. Implementación.....	68
8.4. Manual de uso de los binarios.....	68
8.4.1. Mostrar BDDs.....	68
8.4.2. Realizar un benchmark.....	69
8.5. Ejemplos de uso de la API.....	70
9. Experimentos y resultados.....	72
9.1. Problemas no satisfacibles.....	72
9.2. Problemas satisfacibles.....	73
9.3. Datos de prueba.....	73
9.3.1. AIM.....	73
9.3.2. AIS.....	73
9.3.3. Anomaly.....	73
9.3.4. BW.....	74
9.3.5. Dubois.....	74
9.3.6. Hanoi.....	74
9.3.7. Hole.....	74
9.3.8. Nemesis.....	74
9.3.9. Parity problem.....	74
9.3.10. Quinn.....	74
9.3.11. Simple.....	74
9.4. Resultados por algoritmo.....	75
9.4.1. Sifting.....	76
9.4.1.1. Orden de variables en número de vértices descendente.....	76
9.4.1.2. Orden de variables inicial.....	77
9.4.1.3. Orden de variables aleatorio.....	78
9.4.2. Window permutation.....	79
9.4.2.1. Tamaño de ventana de 2.....	79
9.4.2.2. Tamaño de ventana de 3.....	80
9.4.2.3. Tamaño de ventana de 4.....	81
9.4.2.4. Tamaño de ventana de 5.....	82
9.4.3. Intercambios aleatorios.....	83
9.4.4. Algoritmo genético.....	84
9.4.5. Algoritmo memético.....	85
9.4.6. Algoritmo Iterative Sifting.....	86
9.5. Discusión de los resultados.....	87
10. Arquitectura de la solución software.....	93
10.1. Objetivo.....	93
10.2. Entidades.....	93
10.2.1.1. BDD.....	93
10.2.1.2. Asserter.....	93
10.2.1.3. Sistema.....	93

10.2.1.4. Motor lógico.....	94
10.3. Relaciones.....	94
10.4. Funcionamiento.....	95
10.5. Ejemplos.....	95
10.5.1. Ascensor.....	95
10.5.1.1. Introducción.....	95
10.5.1.2. Magnitudes.....	95
10.5.1.3. Expresión lógica.....	96
10.5.1.4. Funcionamiento.....	96
10.5.2. Control glucémico.....	97
10.5.2.1. Introducción.....	97
10.5.2.2. Magnitudes.....	98
10.5.2.3. Expresión lógica.....	99
10.5.2.4. Funcionamiento.....	99
11. Problemas abiertos.....	102
12. Conclusiones.....	104
12.1. DJBDD: una nueva biblioteca para tratar con BDDs.....	104
12.2. Iterative Sifting: un nuevo algoritmo reductor de BDDs.....	104
12.3. Un comprobador de consistencia lógica.....	105
13. Glosario de términos.....	106
14. Bibliografía.....	108

2 Lista de figuras y tablas

2.1 Figuras

2.1.1 Capítulo 5

Fig. 1	Expansión de Boole-Shannon de una expresión lógica F	25
Fig. 2	Expresión lógica de dos variables	26
Fig. 3	Árbol Binario de Decisión (sin reducir) para $F = xy$	26
Fig. 4	Árbol Binario de Decisión (sin reducir) para $F = xz + y$	27
Fig. 5	Árbol Binario de Decisión (reducido) para $F = xy$	28
Fig. 6	Propiedad de no redundancia de los BDDs	29
Fig. 7	Propiedad de unicidad del vértice	29
Fig. 8	Árbol Binario de Decisión (reducido) para $F = xz + y$	30
Fig. 9	BDD de la función $F = xz + y$ con orden (x, y, z)	31
Fig. 10	BDD de la función $F = xz + y$ con orden (x, z, y)	31
Fig. 11	BDD del $F = x_1x_3 + x_2x_4$ con orden (x_1, x_2, x_3, x_4)	32
Fig. 12	BDD del $F = x_1x_3 + x_2x_4$ con orden (x_1, x_3, x_2, x_4)	32
Fig. 13	BDD para la expresión $F = x_1x_3 + x_2$	34
Fig. 14	BDD de la expresión $F = x + yz$	39
Fig. 15	BDD de la expresión $F = x + yz$ haciendo $y = 1$	39
Fig. 16	Casos en la operación de intercambio de vértices en el BDD	41
Fig. 17	Operación de cruce en algoritmos evolutivos reductores de BDDs	46

2.1.2 Capítulo 7

Fig. 18	Clasificación de distintos Métodos Formales	53
---------	---	----

2.1.3 Capítulo 8

Fig. 19	BDD para la expresión $F = x_0x_2 + x_1x_3 + x_4$	61
---------	---	----

Fig. 20	Ejemplo de BDD generado con GraphVizJava	66
---------	--	----

2.1.4 Capítulo 9

Fig. 21	Reducción media por algoritmo obtenida con los datos de prueba	89
---------	--	----

Fig. 22	Comparación de los mejores algoritmos en reducción obtenida	90
---------	---	----

Fig. 23	Todos los tamaños obtenidos al reducir por cada método	92
---------	--	----

2.1.5 Capítulo 10

Fig. 24	Arquitectura del sistema de evaluación de expresiones lógicas	94
---------	---	----

Fig. 25	BDD que contiene el comportamiento del sistema de ejemplo 1	96
---------	---	----

Fig. 26	BDD reducido por el <i>Iterative Sifting</i> para el sistema de ejemplo 1	97
---------	---	----

Fig. 27	BDD que contiene el comportamiento del sistema de ejemplo 2	99
---------	---	----

Fig. 28	BDD reducido por el <i>Iterative Sifting</i> para el sistema de ejemplo 2	100
---------	---	-----

2.2 Tablas**2.2.1 Capítulo 4**

Tabla 1	Tabla de verdad del operador de negación	22
---------	--	----

Tabla 2	Tabla de verdad del operador de conjunción	22
---------	--	----

Tabla 3	Tabla de verdad del operador de disyunción	23
---------	--	----

Tabla 4	Tabla de verdad del operador de implicación	23
---------	---	----

Tabla 5	Tabla de verdad del operador de equivalencia	23
---------	--	----

2.2.2 Capítulo 5

Tabla 6	Orden de variables para $F = x_1x_2 + x_3$	33
---------	--	----

Tabla 7	Tabla T que contiene el BDD $F = x_1x_2 + x_3$	34
---------	--	----

2.2.3 Capítulo 8

Tabla 8	Tabla T para $F = x_0x_2 + x_1x_3 + x_4$	62
---------	--	----

Tabla 9	Tabla U que contiene el BDD $F = x_1x_2 + x_3$	62
---------	--	----

Tabla 10	Tabla V que contiene el BDD $F = x_1x_2 + x_3$	62
----------	--	----

2.2.4 Capítulo 9

Tabla 11	Parámetros de la JVM en los experimentos	72
----------	--	----

Tabla 12	Semillas aleatorias para los algoritmos evolutivos y aleatorios	75
----------	---	----

Tabla 13	Reducción obtenida mediante el algoritmo <i>Sifting</i> (orden desc.)	76
----------	---	----

Tabla 14	Reducción obtenida mediante el algoritmo <i>Sifting</i> (mismo orden)	77
Tabla 15	Reducción obtenida mediante el algoritmo <i>Sifting</i> (orden aleatorio)	78
Tabla 16	Reducción obtenida mediante <i>Window Permutation</i> ($k = 2$)	79
Tabla 17	Reducción obtenida mediante <i>Window Permutation</i> ($k = 3$)	80
Tabla 18	Reducción obtenida mediante <i>Window Permutation</i> ($k = 4$)	81
Tabla 19	Reducción obtenida mediante <i>Window Permutation</i> ($k = 5$)	82
Tabla 20	Reducción obtenida mediante el algoritmo <i>RandomSwapper</i>	83
Tabla 21	Reducción obtenida mediante el algoritmo genético	84
Tabla 22	Reducción obtenida mediante el algoritmo memético	85
Tabla 23	Reducción obtenida mediante el algoritmo original <i>Iterative Sifting</i>	86
Tabla 24	Tamaños obtenidos en cada proceso de reducción de BDDs	87
Tabla 25	Porcentaje de reducción para cada proceso de reducción de BDDs	88
Tabla 26	Media y desviación típica de los resultados de los algoritmos (1/2)	90
Tabla 27	Media y desviación típica de los resultados de los algoritmos (2/2)	91

3 Introducción

Desde la aparición de la lógica proposicional, formalizada por Gottfried Leibniz [LEI03], y sobre todo desde la revolución de la lógica digital, se han intentado traducir las fórmulas de la lógica de primer orden a una forma eficiente que permita su tratamiento automático. Además, cualquier posible solución se encontraba frente a la dificultad de que esa solución tenía que ser implementada con unos recursos limitados propios de los sistemas informáticos.

En el año 1986, Randal E. Bryant publicó un artículo [BRY86] en el que daba una definición formal de los Árboles Binarios de Decisión (Binary Decision Diagram, BDD en inglés). En este trabajo describía todos los algoritmos necesarios para trabajar con una estructura de datos que tenía unas características que la hacían muy atractiva para su uso en los campos de diseño de la lógica digital, la inteligencia artificial y las pruebas de software.

Otros autores habían definido la notación e incluso el término BDD [LEE59] [AKE78], pero Bryant fue más allá, añadiendo unas restricciones y fijando el orden de las variables para todas las ramas de éste, consiguió una estructura más eficiente que las que hasta entonces se habían desarrollado. Formas como las tablas de verdad o la forma en suma de productos canónica tenían un tamaño de representación muy alto, de manera que para una función de n argumentos, su tamaño era del orden de 2^n . A partir de un valor de n , no muy grande, no era práctico trabajar con estas herramientas.

Además, esta nueva estructura de datos definida por Bryant tenía una particularidad que la hacía especialmente útil frente a otras alternativas. Todos los árboles BDD para una misma fórmula lógica eran isomorfos, es decir, tenían la misma estructura y por tanto, eran computacionalmente el mismo. Exactamente con el mismo número de vértices y arcos.

Más tarde, otros autores han publicado trabajos en los que se discutían aspectos de la implementación de estos árboles. En primer lugar, se definieron cómo debían ser las estructuras de datos debían contener el árbol. En segundo lugar, la canonicidad de los BDD permitía el hacer uso de una única malla de vértices donde cada árbol era simplemente un vértice raíz de esa malla [BRA91]. Por último, se definieron los arcos complementados

[MIN90], que, aunque rompen con la unicidad de un árbol BDD por fórmula, podían tener su interés a la hora de implementarlo en sistemas digitales, donde cada puerta lógica implica un coste.

Mientras tanto, surgió el problema del orden de variables. Estos árboles se veían fuertemente influenciados por el orden de variables, pudiendo tener una diferencia entre tamaños muy sustancial dependiendo de los órdenes de variables. Pero era un problema de gran complejidad puesto que es NP-duro [BOL05]. Richard Rudell definió la operación de intercambio entre variables y presentó un algoritmo de reducción de vértices del BDD usando esta operación [RUD93]. Desde ese momento, varios autores han ido proponiendo diversos algoritmos que ofrecen mecanismos de reducción de árboles BDD con mayor o menor grado de éxito [LEN08] [ALO01] [ALO03].

Por supuesto, surgió una alternativa al ordenamiento dinámico de variables, generando un orden antes de construir el árbol, es decir, un orden estático [RIC08], pero esta alternativa no era suficiente para problemas en los que se iba a ir operando un BDD con otros de forma dinámica e impredecible.

A día de hoy, siguen surgiendo ideas y se sigue trabajando en la mejora en eficiencia de estos árboles BDD, estando muy presente mediante el diseño de algoritmos paralelos, por ejemplo, [MIL98] y [VAN12].

Una de las aplicaciones más importantes de esta estructura de datos es su uso como almacén del estado lógico de un sistema software [BEY13]. Los árboles binarios de decisión tienen un gran potencial como almacenes de restricciones y estados. En este trabajo hemos desarrollado una librería completamente nueva y un sistema que permite almacenar el estado de un sistema en un árbol BDD. A partir del cual podremos realizar operaciones sobre él y lo que es más importante, podremos comprobar si para un estado de ese sistema, la fórmula lógica contenida en el BDD, es consistente.

En general, cuando se piensa en un sistema tolerante a fallos, se suele pensar en sistemas software que tienen vidas a su cargo, como software para aviónica o para centrales nucleares, pero, supongamos por un momento un sistema web que gestione ocupaciones de reserva de plazas para un lavadero de coches. Desde el momento que el cliente inicia su compra, está reservando un intervalo de tiempo. Este intervalo de tiempo se almacena en un estado que podríamos calificar como “pendiente”, puesto que todavía no se ha pagado, y bloquea la selección de esa misma ranura de tiempo para el resto de clientes. Obviamente, en este sistema, hay condiciones de carrera puesto que los clientes entran en la web de forma paralela.

Ahora, supongamos además que hay varios servicios (lavado, encerado, control de presión, limpieza interior del vehículo...) que son seleccionables y que cada uno de ellos se realiza en una ubicación distinta en distintos “boxes”. Así, internamente el sistema deberá llevar el control de la ocupación de cada “box”.

Cuando se realice un pago por internet, con todo el protocolo de comunicación que ha de ser implementado, deberá marcar la venta como pagada y reservar efectivamente la ocupación para el cliente. Es obvio que éste se ha introducido en una máquina de estados implementada en el sitio web. Cuando el pago sea efectivo, deberá generar un ticket para que el encargado pueda leer de forma automática qué servicios ha comprado el cliente. Por supuesto, en este ticket deberá indicar quién ha realizado la compra.

Este tipo de problemas de restricciones de competencia entre instancias de un sistema pueden modelarse bien con bloqueos o pueden modelarse con árboles binarios de decisión de forma que el sistema sea capaz de detectar inconsistencias y por ende, verificar que el proceso se encuentra con unos datos incorrectos, cancelando el procedimiento actual y volviendo a un estado seguro. En el caso de una detección de un estado inconsistente, el software podrá detener el proceso y volver al estado correcto más cercano. En nuestro ejemplo, cancelar la compra.

Otro ejemplo más lejano a un usuario normal puede ser el de desarrollo de software para sistemas de control. Se modelan los estados como proposiciones lógicas y se estructura un BDD con todas las restricciones. Este árbol se mantiene en memoria y refleja el estado real del sistema. De forma que cuando el sistema entre en un estado inconsistente, puede reiniciarlo o volver a un estado seguro. Un caso posible de este tipo de sistemas puede ser cualquier software que compruebe que una máquina industrial está funcionando correctamente.

En definitiva, sea cual sea el uso que se le dé, utilizar un BDD como software de control adicional permite que se detecten errores en el software y que el sistema vuelva al estado estable más cercano. Además, el BDD reflejará en cada momento el estado real del sistema.

Así, hemos desarrollado esta *piedra angular*. Una librería eficiente para BDDs que implementa todas las herramientas para que un equipo de ingenieros de software la puedan usar para construir sistemas tolerantes a fallos. Esta librería se llama DJBDD y se encuentra disponible en un repositorio de código público, <https://github.com/diegojromerolopez/djbdd>.

El **objetivo** de este trabajo fin de máster es realizar un método de verificación de software. Decidimos usar los Árboles Binarios de Decisión, en primer lugar porque ya había trabajado con ellos con anterioridad y el tema no me era del todo desconocido y en segundo lugar, porque era uno de los temas más explotados en cuanto a verificación de software y hardware, lo que me permitiría encontrar abundante información y ejemplos de uso en el mundo real. El método de comprobación de la consistencia estaría basado en los BDD como mecanismo de almacenaje y razonamiento lógico.

Una vez fijado el tema, se desarrollaron una serie de experimentos que mostrasen cómo optimizar árboles binarios de decisión de forma sencilla. Esto no es fácil y en sucesivos trabajos he visto que los algoritmos exactos tienen órdenes de eficiencia muy grandes. Hasta que el trabajo de R. Rudell [RUD93], en el que, mediante una operación constante, el autor diseña dos algoritmos de optimización de BDDs.

Una característica destacable de los BDDs es que combinan ingeniería y ciencia a partes iguales. Por un lado, el diseñar algoritmos para reducir el árbol para enfrentarnos contra la complejidad computacional de encontrar el mejor orden de variables es un problema de Computación. Por otro, el usar estructuras de datos eficientes y consumir la menor cantidad de memoria posible son problemas de Ingeniería de Software. Esta dualidad nos pareció muy interesante.

Una vez clara la dirección del trabajo, pensamos en la implementación. Inicialmente no estaba claro si tomar una implementación referencia o realizar una propia. Es cierto que hay mucho software sobre este tema y ha sido ampliamente usado. Por ejemplo, las librerías BuDDy [BUD] y CUDD [SOM] son de las librerías más usadas y eficientes. Ahora bien, la calidad del software de estos proyectos es escasa. La legibilidad del código es pequeña y la la

documentación se refiere a su uso, pero no a su diseño. Estos paquetes tienen como objetivo el ser los más rápidos en cuanto a tiempo de ejecución, pero no logran tener ser un software de calidad ni muchos menos.

Estando en un máster de Ingeniería del Software, es natural hacer una implementación que respetase algo más los estándares y buenas prácticas [MAR08] [MCC04] y que, además, permitiese realizar experimentos de forma sencilla y sabiendo exactamente qué estaba ocurriendo. De esta manera, se puede continuar su desarrollo de forma sencilla por cualquier estudiante de máster o doctorado, al contrario de como ocurre con las otras implementaciones. Bien por estar basadas en lenguajes menos modernos, o bien por tener un gran nivel de ofuscación y falta de diseño estructurado, éstas librerías no facilitan la comprensión de su funcionamiento. Nosotros queríamos eliminar ese nivel de “oscuridad” presentando un software claro, pero sin sacrificar eficiencia.

En determinados trabajos en los que se hacía uso de paquetes con BDDs, los autores no mostraban suficiente nivel de comprensión de cómo funcionaban éstos, y eso nos parece un grave error. Si no se conoce exactamente como está desarrollado, ¿cómo se pueden extraer conclusiones científicas?

De esta forma, decidimos realizar una implementación desde cero de una librería de BDDs. Dado que la eficiencia y el competir con otras implementaciones más asentadas no era nuestro objetivo, decidimos usar un lenguaje de programación que ofreciese lo mejor de los dos mundos. Por un lado, que estuviese cercano a la máquina en cuanto a eficiencia y por otro quería que proporcionara herramientas para facilitar algunos aspectos del desarrollo, como es la gestión de memoria dinámica. Por todo eso, escogimos el lenguaje estrella de la plataforma JVM, Java.

Efectivamente era muy costosa la creación de árboles simplemente mediante un generador recursivo y se necesitaba una funcionalidad más elaborada para alcanzar un orden de eficiencia que no fuera exponencial. El objetivo era tener un paquete no que pudiera competir en tiempo con BuDDy o el CUDD, sino que permitiera trabajar con distintos algoritmos y con el que pudiera realizar experimentos.

Además, los paquetes de software existentes usaban aristas complementadas, de lo que yo no era muy partidario, ya que se pierde la unicidad del BDD ante una fórmula lógica determinada.

En este trabajo se incluye una librería de uso de BDD basada en Java que puede integrarse en sistemas de verificación formal o en sistemas de control. También se han implementado una serie de algoritmos de reducción del tamaño del árbol.

La parte más importante, es la del comprobador de consistencia muestra cómo, definiendo una serie de reglas se puede razonar si éstas son consistentes o no con un estado del software. Este tema nos parece muy interesante debido a que conocemos de fallos de sistemas software y de las catastróficas consecuencias que éstos pueden llegar a tener.

Comenzaremos esta memoria indicando, en la **Introducción**, cuál es nuestro objetivo principal y por qué hemos decidido implementar una librería de BDDs y usarla como comprobador de consistencia cuando ya hay otras disponibles públicamente.

Seguiremos con una somera explicación de **Lógica proposicional**, definiendo conceptos que luego servirán como fundamentos de los siguientes capítulos. Ese contenido puede hojearse

para recordar conceptos que la mayoría de los lectores ya conocen.

Después explicaremos los fundamentos de los **Árboles Binarios de Decisión**, sus algoritmos y las estructuras de datos que contiene el árbol. Todas las operaciones, incluyendo la creación, las operaciones lógicas AND, OR y NOT. También se indicarán los problemas que se encontraron, las soluciones que se han aportado y los algoritmos que se han usado. Es destacable que el algoritmo de intercambio de variables se detalla hasta un nivel que, hasta donde sabemos, no aparece en la bibliografía. Por último, los algoritmos de reducción se detallan de forma extensa. Hay que destacar que, en el apartado de optimización del número de vértices de los BDDs, se muestra un algoritmo completamente original, cuyo trabajo está pendiente de publicación y que logra mejoras con respecto a los algoritmos heurísticos que del estado del arte actualmente.

Una vez que hemos presentado la lógica proposicional y los BDDs como una representación de la tabla de verdad, hemos de encuadrar estos elementos en la Ingeniería del Software. Por tanto, este capítulo, **Aplicaciones de los BDDs a la Ingeniería del Software**, tratará de mostrarnos el valor de esta técnica para dar una base formal al desarrollo de software. En especial, veremos la aplicación de los BDDs a la Verificación Simbólica de Modelos.

En el siguiente capítulo, **Software**, se mostrará cómo se ha implementado la librería de BDDs. Además, se detallarán las dependencias entre los paquetes y las clases. También se incluye un pequeño manual de uso de los binarios y cómo usar la API de la librería desarrollada DJBDD.

Sigue a continuación el capítulo de **Experimentos y resultados**. Los experimentos se han centrado en la optimización de BDDs. Se han probado varios algoritmos que tratan, mediante el intercambio de variables de reducir el número de nodos de un árbol de este tipo. Las fórmulas a reducir son instancias de problemas SAT en formato CNF, en ficheros DIMACS [BUR]. No podremos construir las fórmulas completas debido a las limitaciones propias en memoria de los equipos en los que hemos realizado las pruebas. Eso sí, serán los suficientemente grandes como para comprobar si estos algoritmos de reducción funcionan correctamente o no.

El siguiente capítulo, **Arquitectura de la solución software**, se presenta nuestra librería que hace uso de este motor de satisfacibilidad basado en BDDs que tiene como objetivo permitir utilizar los BDDs como comprobadores de consistencia. Por esto, se mostrarán dos ejemplos de sistemas en los que estos sistemas logran mejorar la calidad del software de forma sustancial. El primer ejemplo se presenta a modo ilustrativo de cómo se ha de usar el software. En cambio, el segundo es un ejemplo médico real en el que un experto nos indica una serie de reglas y el sistema es el encargado de indicarnos si una decisión que toma un paciente es la correcta o no. Evidentemente, con el propósito de no sobrecargar al lector, no se incluyen todas las reglas lógicas ni todas las variables, salvo las más representativas.

Procederemos después, en el capítulo de **Problemas abiertos** a mostrar algunos interrogantes que han surgido a lo largo de este trabajo y que son una muestra de las nuevas vías de investigación en este mismo área.

Terminamos este trabajo con las **Conclusiones**. En este capítulo hacemos un compendio de lo más importante, resumiendo y recordando los puntos clave tratados en este trabajo.

Por último, queremos destacar el hecho de que **todo lo contenido en este trabajo fin de**

máster es completamente original, desde las tablas, figuras y diagramas incluidos en este documento. Además del software que ha sido desarrollado por el autor, sólo se han usado referencias bibliográficas, pero no otras herramientas externas.

4 Lógica proposicional

La lógica proposicional es un sistema formal en el que las fórmulas de un lenguaje formal se interpretan como proposiciones. Se usa un conjunto de reglas de inferencia y axiomas para derivar fórmulas. A estas fórmulas derivadas se les llama teoremas.

En la lógica proposicional, podemos interpretar las fórmulas de manera sintáctica, realizando derivaciones unas de otras y obteniendo resultados, o por el contrario podemos dar valores a cada proposición y aplicando los operadores lógicos obtener una interpretación de la fórmula. Ambas formas de proceder son equivalentes [HUT04], así que para los propósitos de este trabajo supondremos que ambos tipos de demostración son válidos e iguales.

4.1 Definición

La lógica proposicional es aquella determinada por enunciados que pueden ser o bien ciertos, o bien falsos. A estos enunciados se les conoce como **proposiciones lógicas**. Éstas pueden tener dos valores constantes:

- TRUE: si la proposición es cierta.
- FALSE: si la proposición es falsa.

Estas proposiciones lógicas se pueden combinar mediante operadores. De manera formal, decimos que una expresión lógica es:

- p , donde p es una proposición lógica.
- $\neg \psi$, donde ψ es una expresión lógica y \neg el operador de negación
- Dadas ψ y φ expresiones lógicas y Θ un operador lógico binario, $\psi \Theta \varphi$ es otra proposición lógica.

A continuación explicamos cada uno de estos conceptos.

4.2 Constantes

La lógica proposicional se basa en dos proposiciones atómicas constantes que representan la verdad y la falsedad (TRUE y FALSE, respectivamente):

- TRUE: proposición cierta. Se representa como TRUE, *true*, 1 o T.
- FALSE: proposición falsa. Se representa con FALSE, *false*, 0 o F.

4.3 Operadores

Los operadores en la lógica proposicional se definen mediante tablas de verdad. Recordemos lo dicho anteriormente, que la demostración sintáctica y semántica son equivalentes.

En este apartado supondremos que ψ , φ y τ son expresiones lógicas, de manera que cuando hablemos de la interpretación de una de ellas, nos referiremos al valor de verdad que tomará una vez resuelto el cálculo de este valor entre sus proposiciones.

4.3.1 Operador de negación

Este operador invierte el valor de verdad de la expresión sobre la que esté actuando:

ψ	$\neg \psi$
0	1
1	0

Tabla 1

4.3.2 Operador de conjunción

Este operador se interpreta como TRUE siempre y cuando sus operandos sean interpretados con el valor TRUE también:

ψ	φ	$\psi \wedge \varphi$
0	0	0
0	1	0
1	0	0
1	1	1

Tabla 2

Muchas veces este operador se identifica con los símbolos \cdot , AND. También suele escribirse yuxtaponiendo directamente sus operandos, de forma que se escribirían una detrás de otra, por lo que si vemos $F = xy$, nos referiremos a $F = x \text{ AND } y$.

4.3.3 Operador de disyunción inclusiva

Este operador proporciona una proposición cierta siempre y cuando al menos uno de sus operandos, lo sea:

ψ	φ	$\psi \vee \varphi$
0	0	0
0	1	1
1	0	1
1	1	1

Tabla 3

Este operador también se identifica con los símbolos OR, V, +.

4.3.4 Resto de operadores

El resto de operadores posibles puede definirse en función de los ya indicados. Por ejemplo, el operador de implicación obedece la siguiente tabla de verdad:

ψ	q	$p \Rightarrow q$	$\neg p \vee q$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Tabla 4

Para el operador de equivalencia tendríamos:

ψ	φ	$\psi \Leftrightarrow \varphi$	$(\neg \psi \vee \varphi) \wedge (\psi \vee \neg \varphi)$
0	0	1	1
0	1	0	0
1	0	0	0
1	1	1	1

Tabla 5

No es nuestro objetivo mostrar todos los posibles operadores binarios lógicos, por lo que, ante un operador no incluido aquí, supondremos que la fórmula puede convertirse sin problemas a cualquier combinación de los operadores incluidos anteriormente.

En este trabajo no vamos a detallar todos los operadores posibles como XOR, NAND, NOR, etc. Para más información se puede consultar [HUT04].

4.4 Precedencia

De aquí en adelante, vamos a suponer que la precedencia de operadores sigue el siguiente orden:

- NOT
- AND
- OR

- \Rightarrow

De todas formas, salvo en el caso de NOT, que tiene siempre la mayor precedencia, vamos a incluir paréntesis para evitar confusiones.

4.4.1 Propiedades

En este apartado se muestran las propiedades que permitirán la construcción de los Árboles Binarios de Decisión. Se puede consultar [HUT04] para obtener una descripción más detallada de las mismas.

4.4.1.1 Propiedad asociativa

Los operadores OR y AND son asociativos, esto quiere decir que se cumplen estas equivalencias:

- Asociatividad del operador OR

$$\psi \vee (\varphi \vee \tau) \Leftrightarrow (\psi \vee \varphi) \vee \tau$$

- Asociatividad del operador AND

$$\psi \wedge (\varphi \wedge \tau) \Leftrightarrow (\psi \wedge \varphi) \wedge \tau$$

4.4.1.2 Propiedad distributiva

- Distribución de la conjunción con respecto a la disyunción

$$\psi \wedge (\varphi \vee \tau) \Leftrightarrow (\psi \wedge \varphi) \vee (\psi \wedge \tau)$$

- Distribución de la disyunción con respecto a la conjunción

$$\psi \vee (\varphi \wedge \tau) \Leftrightarrow (\psi \vee \varphi) \wedge (\psi \vee \tau)$$

4.4.2 Leyes de De Morgan

Las leyes de De Morgan relacionan los operadores AND y OR mediante el de negación según las siguientes expresiones:

$$\neg(\psi \wedge \varphi) \Leftrightarrow \neg\psi \vee \neg\varphi$$

$$\neg(\psi \vee \varphi) \Leftrightarrow \neg\psi \wedge \neg\varphi$$

Estas propiedades son interesantes debido a que las usaremos en la negación de los subárboles de decisión. Estas leyes son las que se usan cuando se construye una expresión en la que la negación afecta a una subexpresión compleja, como por ejemplo: $\neg((\psi \wedge \varphi) \vee \tau)$.

5 Árboles Binarios de Decisión

5.1 Introducción

Un árbol binario de decisión [BRY86] es una forma de representar una tabla de verdad basada en la expansión de Boole¹, en la que se enuncia que cualquier fórmula lógica puede descomponerse en la expresión:

$$F = xF_{(x=1)} + \neg xF_{(x=0)},$$

donde $F_{(x=0)}$ es la expresión F asignando a la variable x el valor *false* y $F_{(x=1)}$ es la expresión F sustituyendo la variable x por el valor *true*.

Si representamos esta expresión de forma gráfica tendremos un nodo con la expresión F (que depende de la variable x), de forma que si se le da a la x el valor 0 se obtiene $F_{(x=0)}$ y se le da el valor 1 se obtiene $F_{(x=1)}$. La asignación de $x=0$ la marcamos con una flecha discontinua, y la asignación de $x=1$ la marcamos con una flecha continua. En la siguiente figura² podemos ver una representación gráfica de esta *expansión* de la fórmula lógica:

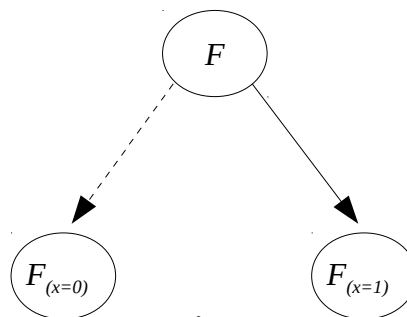


Fig. 1

-
- 1 También se le suele llamar expansión de Shannon, aunque su creador fue George Boole, matemático, lógico y filósofo inglés del siglo XIX. Nosotros usaremos indistintamente cualquiera de estos dos nombres.
 - 2 Tal y como se ha indicado en la introducción, salvo que se indique lo contrario, todas las figuras, diagramas y tablas son originales, producidas por el autor de este trabajo fin de máster.

Si F depende además de otra variable, y , podremos repetir este mismo proceso de bifurcación de asignaciones con $F_{(x=0)}$ y con $F_{(x=1)}$. Es decir, si suponemos que la siguiente variables es y , tendríamos el siguiente árbol de decisión:

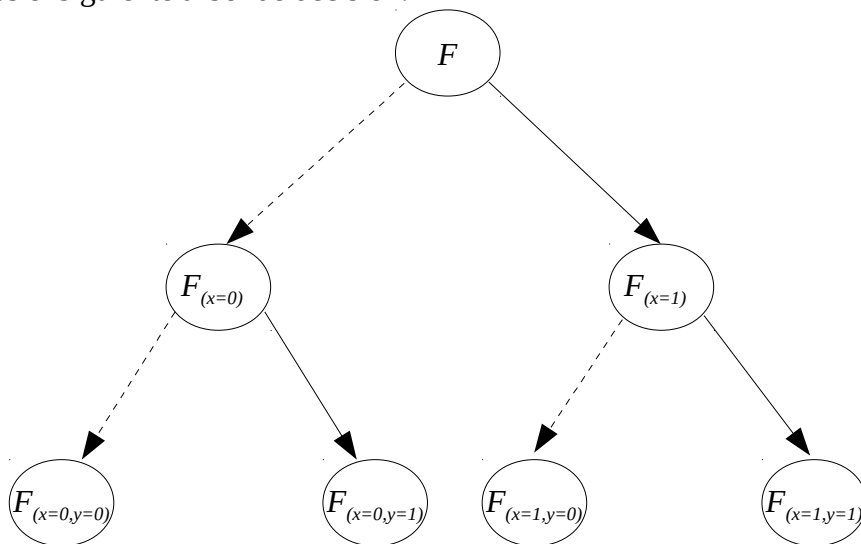


Fig. 2

Por tanto, hablamos de árboles binarios de decisión porque cada nodo tiene exactamente dos nodos como descendientes.

Puede ocurrir que alguno de los nodos no dependa de ninguna variable y tenga un valor constante (**0** ó **1**). En este caso, ese nodo será un nodo hoja, dado que no tendrá descendientes, y sólo podrá tomar el valor *true* o *false*.

Vamos a ver un ejemplo de fórmula lógica real $F = xy$, donde tomamos el orden de las variables como primero x , y en segundo lugar y . También, para facilitar la visibilidad del diagrama, suponemos que $F_{(a,b)} = F_{(x=a, y=b)}$.

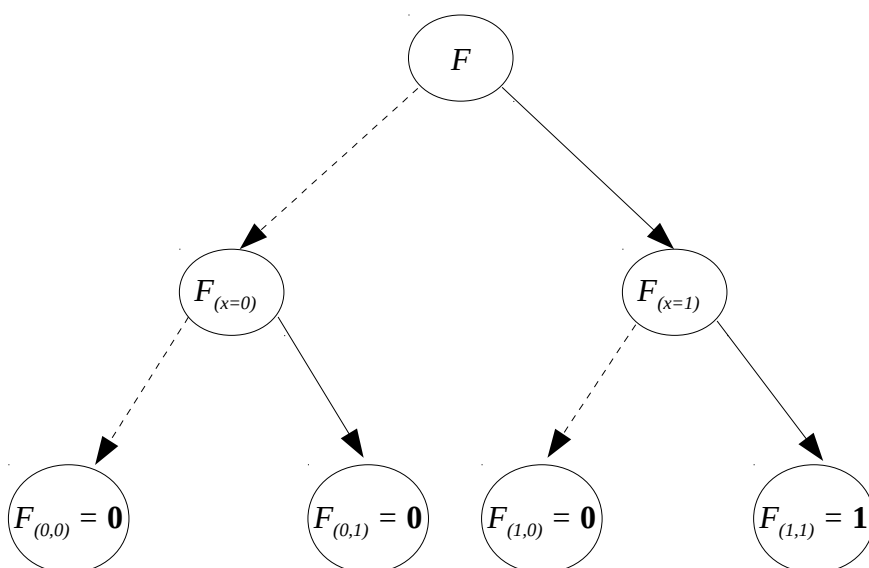


Fig. 3

Notemos que al nodo que viene de una arista punteada se le suele llamar, *low*, y al de la línea llena *high*, debido a que son producto de la asignación de **0** y **1** a su vértice padre, respectivamente. Explicaremos con más detalles estos conceptos en la página 22.

Otro ejemplo en el que podemos ver varios niveles es el siguiente: $F = xz + y$, con el orden x, y, z .

En los árboles binarios de decisión, cada vértice representa una decisión, de manera que cada vértice tiene una variable asociada (que aparece dibujada en su interior). Así, el primer vértice de la **Fig. 4** tiene la variable x , indicando que habrá dos subárboles descendientes en los que, para el subárbol de su izquierda se tomará $x=0$ y para el subárbol de su derecha se tomará $x=1$. De igual forma para cada uno de los vértices hasta llegar a los vértices hoja, con las constantes **1** (valor verdadero) y **0** (valor falso).

Por otro lado, como se puede ver en este ejemplo, hay ramas completas repetidas. En la siguiente sección vamos a mostrar cómo se pueden reducir los BDD haciendo que pasen de ser árboles binarios a grafos dirigidos acíclicos.

5.2 Árboles reducidos

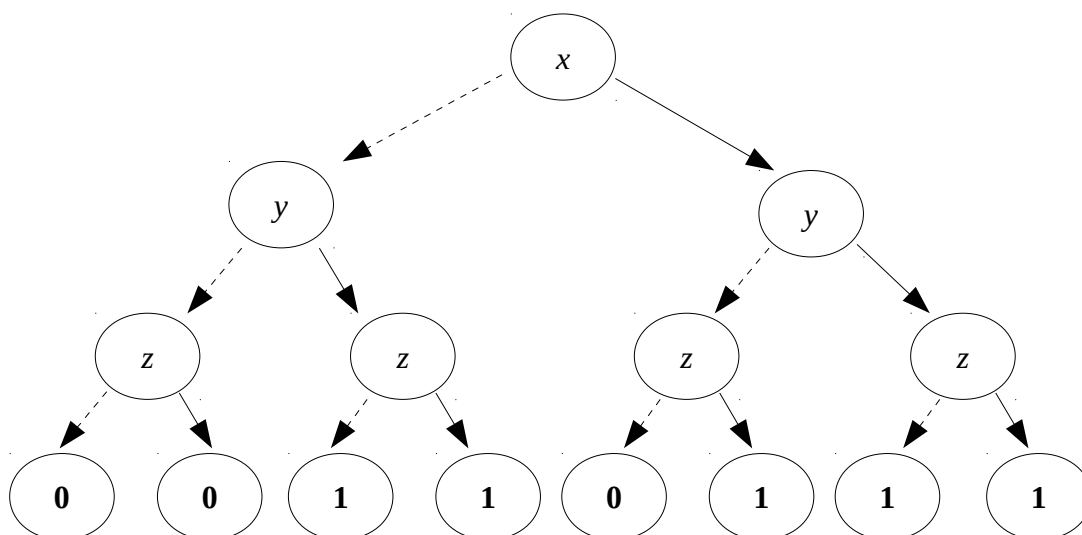
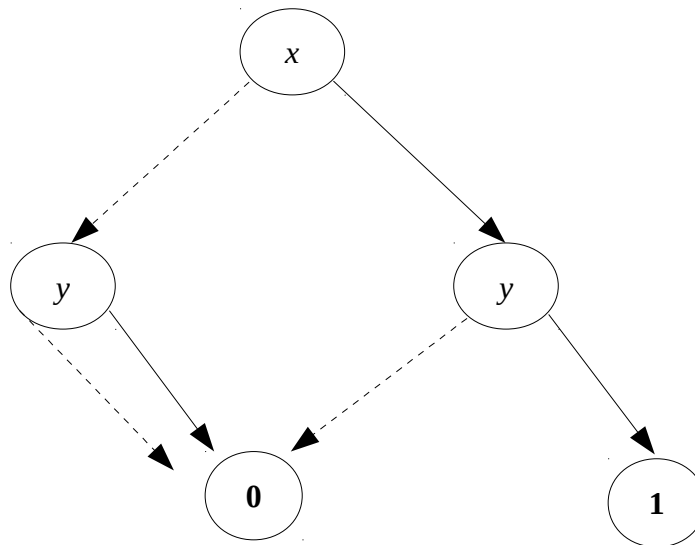


Fig. 4

Dado el árbol de la **Fig. 3** (función $F = xy$), un detalle importante que podemos apreciar es la repetición de nodos. Es decir, podemos ver cómo se repiten los nodos hoja y tenemos tres nodos con el valor **0** y sólo uno con el valor **1**. Si eliminamos los nodos con el mismo valor, obtenemos el siguiente árbol binario reducido:

**Fig. 5**

Hemos reducido, por tanto, el árbol en 2 nodos sobre un total de 7. Esto no puede parecer mucho, pero pensemos a gran escala, en fórmulas de miles de variables, conseguir una reducción de un tercio de su tamaño es muy deseable.

También vemos como, en el nodo y de la izquierda, independientemente del valor que tome y , se obtiene el valor **0**. ¿Se podría disponer de unas normas para reducir aún más el árbol evitando repeticiones innecesarias?

Randal Bryant en la Universidad Carnegie Mellon introdujo el concepto de Diagrama de Decisión Binario Ordenado Reducido Compartido en [BRY86], indicando las restricciones que debía tener un BDD para que fuera mínimo y único dado el mismo orden de variables. Para ello, el diagrama ha de cumplir dos propiedades que explicamos a continuación: ser no-redundante y que cada uno de sus vértices sea único.

5.2.1 No-redundancia

En primer lugar, no debe haber vértices redundantes, esto es, no puede haber un vértice cuyos descendientes (ambos) sean un único vértice. En el caso de que en el proceso de construcción esta casuística se dé, se sustituirá el nodo de descendientes iguales por el nodo descendiente.

Dado un vértice v , si su vértice *low* y su vértice *high* son iguales, esto es, $low(v) = high(v)$, entonces se produce la siguiente sustitución:

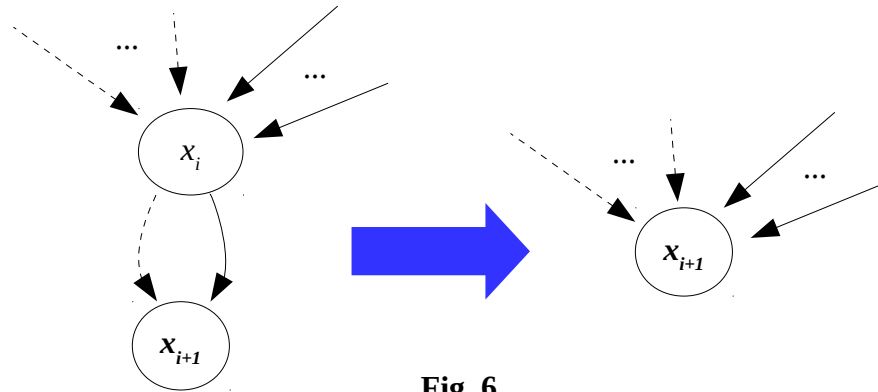


Fig. 6

5.2.2 Unicidad de cada vértice

Si un vértice tiene los mismos descendientes que otro y la misma variable, entonces ha de ser sustituido por éste. Es decir, supongamos que tenemos un árbol que tiene dos vértices distintos u y v que cumplen que ambos tienen la misma variable y que tienen los mismos descendientes *low* y *high*. Entonces, ambos han de ser considerados el mismo vértice.

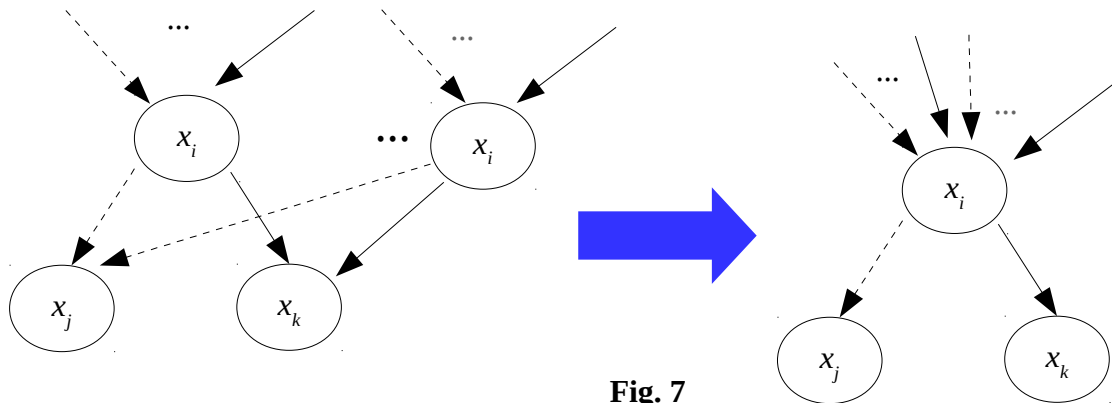
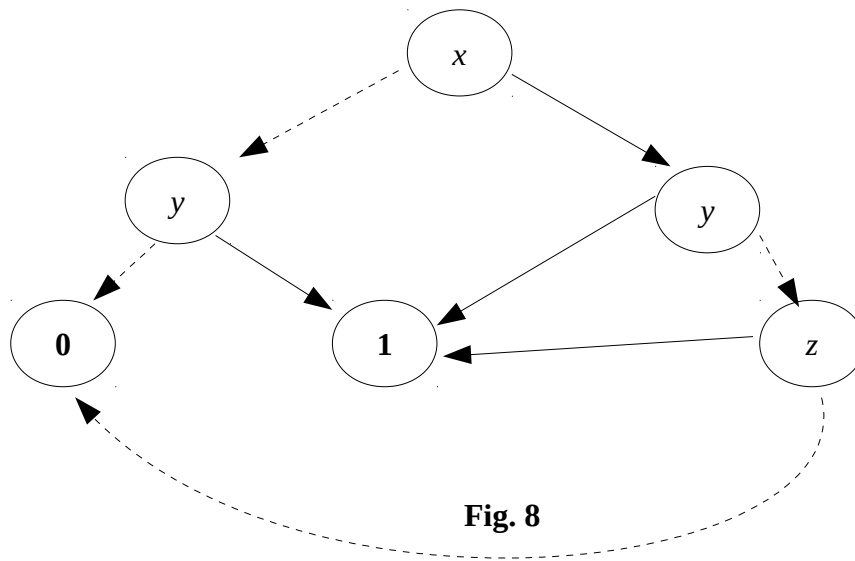


Fig. 7

Por ejemplo, si tenemos en el árbol de la Fig. 4 ($F = xz + y$), hay varios vértices repetidos y redundantes. Si los eliminamos, obtendremos el siguiente árbol reducido:

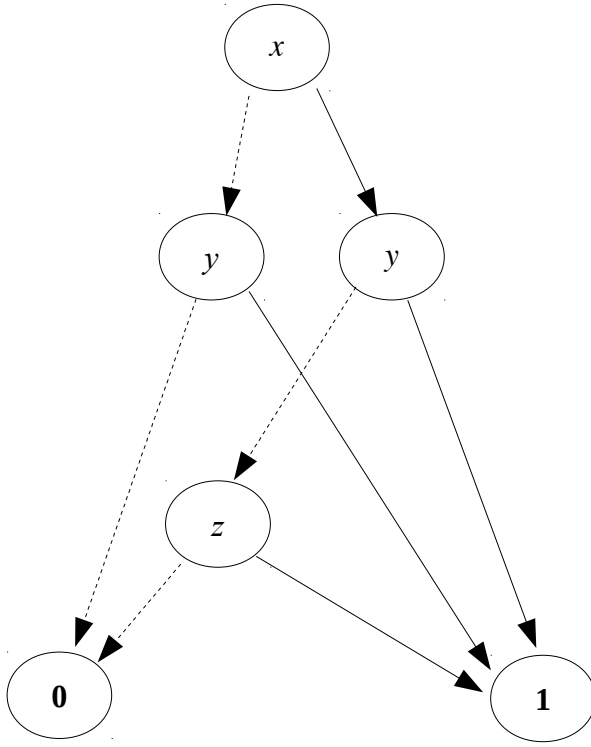
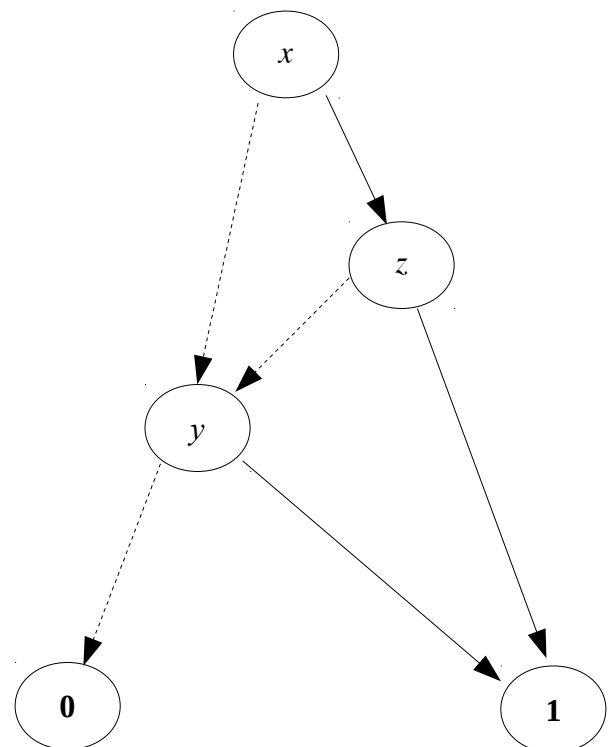


5.3 Orden de las variables

Las variables tienen un orden entre ellas que nos sirve para evitar tener niveles repetidos. Tengamos en cuenta que cada camino que sale del vértice raíz representa una asignación de valores de verdad a variables, lo que sería equivalente a una fila de una tabla de verdad, y por tanto, no se pueden repetir asignaciones.

De igual forma, hemos de respetar este orden en todas las ramas del árbol, o en otro caso, podríamos encontrarnos con problemas a la hora de evaluar funciones o de reducir el árbol.

Por ejemplo, supongamos la función $F=xz+y$, mostramos a continuación dos órdenes de los posibles, (x, y, z) en la imagen de la izquierda y (x, z, y) en la imagen de la derecha:

**Fig. 9****Fig. 10**

El BDD de la **Fig. 9**, que es el que tiene el orden (x, y, z) tiene un nodo más que el árbol de la **Fig. 10**, que es el que tiene el orden (x, z, y) . De esta forma, el orden es determinante en cuanto al tamaño del árbol.

Aunque, en este sencillo ejemplo sólo se incrementa de tamaño el BDD en un vértice, lo que no es mucho. Ahora bien, pensemos en el árbol para la fórmula lógica $F = x_1x_3 + x_2x_4$. Si suponemos que el subíndice de cada variable indica su orden en el árbol, obtendríamos un BDD de 8 vértices. En cambio, si le dotamos de un orden algo más inteligente, siendo éste (x_1, x_3, x_2, x_4) , el BDD es de un tamaño de 6 vértices.

A continuación se muestran los correspondientes árboles:

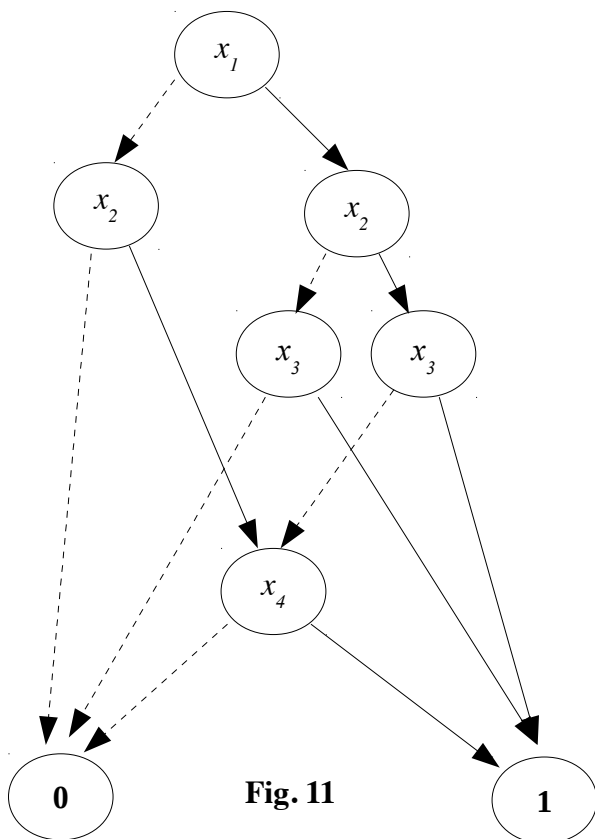


Fig. 11

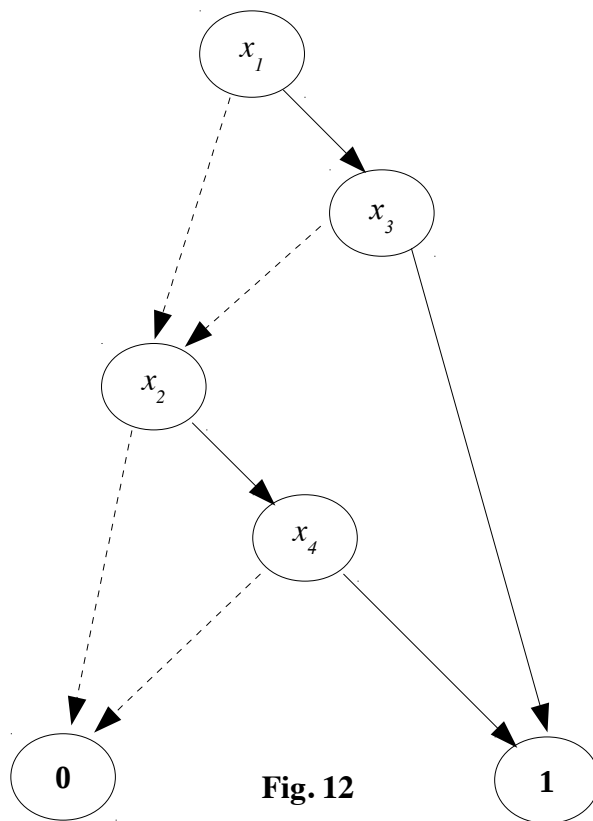


Fig. 12

Este ejemplo muestra cómo, en algunos casos, se puede pasar de un número de nodos exponencial a uno lineal simplemente cambiando el orden a las variables.

De hecho, la mayoría de las estrategias de optimización tratan de encontrar órdenes que reduzcan el tamaño del árbol.

5.4 Definición

Ahora estamos en condiciones de dar la noción de árbol binario de decisión (ROBDD).

Un árbol binario de decisión es un grafo dirigido acíclico con un vértice como raíz.

Cada vértice tiene los siguientes atributos $v = \{id: Int, var: Variable, low: Vertex, high: Vertex\}$.

- *id*: identificador del vértice. Número entero mayor que cero. Nos servirá para identificar cada vértice y distinguirlo del resto.
- *var*: variable que está asociada con el vértice. Como hemos visto antes, cada nivel de vértices tiene asociada una variable. Las variables se numeran como enteros mayores que cero indicando de esta forma el orden que tienen en el árbol, esto es var_i precede a var_j si y solamente si $var_i < var_j$.
- *low*: referencia al vértice que se toma cuando se asigna el valor 0 a la variable del vértice actual.

- *high*: referencia al vértice que se toma cuando se asigna el valor 1 a la variable del vértice actual.

No se permiten ciclos en el árbol, esto es, para todo vértice v , se cumple

$$v.low = u \Leftrightarrow v.var < u.var^3$$

A *low* y *high* se le llama los descendientes de cada vértice y cumplen las siguientes propiedades:

Sean v y u vértices del árbol.

- $v.low \neq v.high$
- $v.low = u.low \text{ AND } v.high = u.high \text{ AND } v.var = u.var \Leftrightarrow v = u$

Existen unos vértices especiales constantes:

- **1**: $\{id=1, low=null, high=null\}$
- **0**: $\{id=0, low=null, high=null\}$

Estos vértices constantes no tienen descendientes, de ahí que sus atributos *low* y *high* tomen el valor *null*.

5.5 Operaciones

Los árboles de decisión tienen una serie de operaciones propias [BRY92], [SOM99]. Nosotros hemos implementado las que nos parecían más importantes. Obviamente la creación, *Apply* y la restricción. Si se desea otra operación, dada la naturaleza abierta de la librería animo al lector a estudiar la implementación de otras operaciones.

5.5.1 Creación

Normalmente los autores tal y como ocurre en [BRY92] y [AND99] hacen uso de dos estructuras de datos:

La tabla de vértices en la que un índice nos da la tripleta: *variable*, *low* y *high*. Normalmente a esta tabla se la suele llamar *T*.

Por ejemplo, para el árbol $F = x_1x_3 + x_2$

Tendríamos las variables en orden:

Variable	x_1	x_2	x_3
Índice	1	2	3

Tabla 6

³ En este documento usaremos la notación orientada a objetos para indicar que la propiedad pertenece al objeto, de manera que $v.var$ indica la variable del vértice v .

Y el siguiente árbol su tabla T:

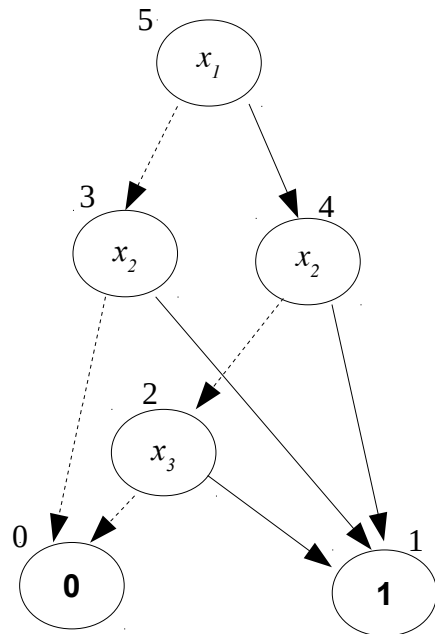


Fig. 13

id vértice	Variable	id vértice low	id vértice high
0			
1			
2	3	0	1
3	2	0	1
4	2	2	1
5	1	3	4

Tabla 7

En la tabla T , podemos ver como a los nodos hoja *true* y *false* le asignamos de forma arbitraria los identificadores 0 y 1 y obviamente sin variable ni descendientes. El resto de nodos se va asignando de abajo a arriba (veremos más adelante cómo se genera un árbol con la operación *Apply*), aunque en realidad, el identificador da igual, lo que nos tiene que interesar es que esa tabla contiene la estructura arbórea y la asociación entre vértices y variables.

De esta forma, gracias a esta tabla T podemos extraer de forma eficiente qué variable tiene el nodo y sus descendientes. Ahora bien, tal y como hemos visto antes, hablamos mucho de unicidad de nodo en cuanto a que sólo existe un nodo con la misma variable, *low* y *high*. Por tanto usaremos una tabla inversa para poder obtener y comprobar que efectivamente sólo hay un único vértice con una variable y unos valores de *low* y *high* determinados. A esta tabla inversa la podemos llamar H .

La tabla H es una tabla que dada la variable, y valores *low* y *high* obtiene el vértice o nos informa de que no existe en tiempo constante.

A partir de este momento, la construcción sigue un proceso recursivo basado en la expansión de Shannon [AND99]. Mostramos su pseudocódigo a continuación:

Obtiene un nuevo vértice

mk(variable, low, high):

Si ambos descendientes son iguales, no creamos un nuevo vértices

```

    # devolvemos uno de ellos
    if low == high:
        return low

    # Si existe el vértice con la misma variable y descendientes
    # Lo devolvemos
    if H[variable, low, high] != null:
        return H[variable, low, high]

    # Es un nuevo vértice
    v = Vertex(variable, low, high)
    H[variable, low, high] = v
    # Añadimos el vértice v a la tabla T con un id único
    T[T.getNewKey()] = v
    return v

# Construye cada uno de los niveles del árbol
# Nótese que cada nivel es en realidad una variable
build(formula, level):
    if level > n:
        if t == False
            return 0
        return 1
    else:
        # Obtiene el vértice low del nuevo vértice
        low = build(formula(x[level]=0), level+1)
        # Obtiene el vértice high del nuevo vértice
        high = build(formula(x[level]=1), level+1)
        # Nuevo vértice
        return mk(level, low, high)

# Llamada inicial
buildBDD(formula):
    return build(formula, 1)

```

Nótese que en la construcción en el paquete software este es uno de los métodos de construcción de árboles, siendo el otro el uso del algoritmo *Apply*, que se detalla a continuación.

5.5.2 Apply

El algoritmo *Apply* que permite ejecutar una operación binaria lógica entre dos árboles BDD fue detallada en [BRY86].

En este algoritmo se va construyendo de forma recursiva gracias a la siguiente propiedad de la expansión de Shannon:

Si definimos un operador que podemos llamar *if-then-else* con una forma similar al operador ternario de cualquier lenguaje de programación:

$$x \rightarrow y_0, y_1 = (x \wedge y_0) \vee (\neg x \wedge y_1)$$

Entonces la expansión de Shanon puede definirse de la siguiente forma:

$$t = x \rightarrow t_{(x=1)}, t_{(x=0)}$$

Pues bien, la siguiente propiedad se cumple para todos los operadores booleanos binarios:

$$(x \rightarrow t_1, t_2) op (x \rightarrow t'_1, t'_2) = x \rightarrow (t_1 opt'_1), (t_2 opt'_2)$$

Una vez dicho esto, podemos mostrar el pseudocódigo del algoritmo definido por Bryant:

Construye una nueva clave para cada vértice

makeUniqueKey(var_index, low, high):

 if(low==null && high==null):

 return var_index+"-"+ "NULL"+"-"+ "NULL";

 return var_index+"-"+low.index+"-"+high.index

Añade un vértice único a la tabla hash

addNewVertex(var_index, low, high):

 # Obtiene la siguiente clave e incrementa el contador global

 index = getNextKey()

 v = new Vertex(index, var_index, low, high)

 T[index] = v

 U[makeUniqueKey(var_index, low, high)] = v

 V[var_index].add(v)

 return v

Añade un vértice no-redundante a la tabla hash

addVertex(var, low, high):

 vertexUniqueKey = makeUniqueKey(var_index, low, high)

 if(uniqueKey in U):

 return U[uniqueKey]

 return addNewVertex(var, low, high)

```
# Aplica el algoritmo Apply a dos vértices
applyVertices(Vertex v1, Vertex v2):
    # Clave hash del subárbol de estos dos vértices
    String key = "1-" + v1.index + "+2-" + v2.index
    if( key in G ):
        return G[key]

    if(v1.isLeaf() && v2.isLeaf()):
        # op es la operación boolean entre dos vértices hoja
        # (que pueden ser true o false)
        if(op(v1,v2)):
            return True # Vértice con el valor true
        return False # Vértice con el valor false

    var = -1
    low = null
    high = null
    # v1.index < v2.index
    if (!v1.isLeaf() and (v2.isLeaf() or v1.variable < v2.variable)):
        var = v1.variable;
        low = applyVertex(v1.low, v2)
        high = applyVertex(v1.high, v2)
    else if (v1.isLeaf() or v1.variable > v2.variable):
        var = v2.variable
        low = applyVertex(v1, v2.low)
        high = applyVertex(v1, v2.high)
    else:
        var = v1.variable
        low = applyVertex(v1.low, v2.low)
        high = applyVertex(v1.high, v2.high)

    # Respeta la propiedad de no-redundancia:
    # "Ningún vértice ha de tener como low y high a un único vértice."
    if(low.index == high.index):
        return low

    # Respeta la propiedad de unicidad:
```

```
# "Ningún vértice ha de tener la misma variable y vértices
# low y high que otro."
Vertex u = addVertex(var, low, high)
G[key] = u
return u;
```

Llamada al algoritmo de apply

apply(operation, bdd1, bdd2):

```
# Caché para evitar cálculos repetidos
G = {}
String function = bdd1.function + " "+operation+" "+bdd2.function
# Llenar la tabla hash T que contiene el nuevo árbol
# con vértices de bdd1 y bdd2
root = applyVertex(bdd1.root, bdd2.root)
# Construcción del nuevo BDD
return new BDD(function, root)
```

5.5.3 Not

Aunque el NO lógico es definible con base en otras operaciones, nosotros preferimos mostrarlo de forma separada por facilitar la comprensión de este software.

También hay que destacar que esta librería no hace uso de arcos negados, por lo que requiere una operación específica que cicle del nodo raíz hacia los nodos hoja aplicando las Leyes de De Morgan.

Para aplicar el operador de NO lógico, simplemente hacemos uso del motor de construcción de BDDs, de manera que crea un nuevo BDD basándose en la fórmula original del BDD que la llame y aplicándole el operador NO. Como el algoritmo de creación está bien construido y es capaz de aplicar las Leyes de De Morgan, no se ha de realizar una operación específica.

5.5.4 Restrict

En [BRY92], Randal Bryant define esta operación de manipulación de árboles binarios de decisión que asigna valores booleanos a algunas variables, de esta forma restringiendo la ruta desde la raíz del árbol y obteniendo un nuevo árbol de menor tamaño.

De forma gráfica podríamos verlo más fácilmente:

Supongamos el árbol $F = x + yz$

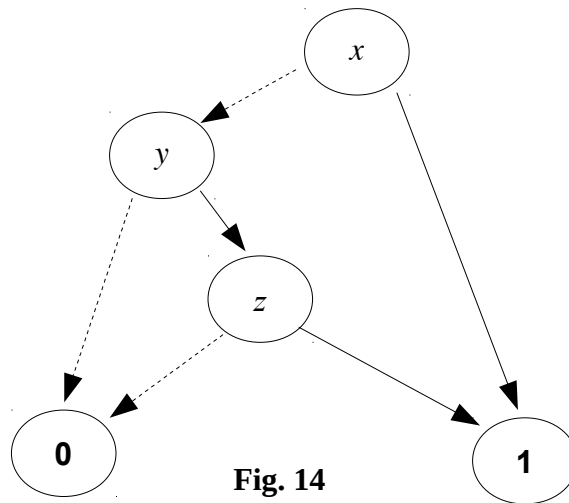


Fig. 14

Si asignamos a la variable y el valor **1**, el BDD perderá todos los vértices con esa variable y se sustituirán por los de su rama *high*. En nuestro caso, sólo hay un vértice, de forma que el *low* del vértice x llegaría directamente al vértice z , es decir:

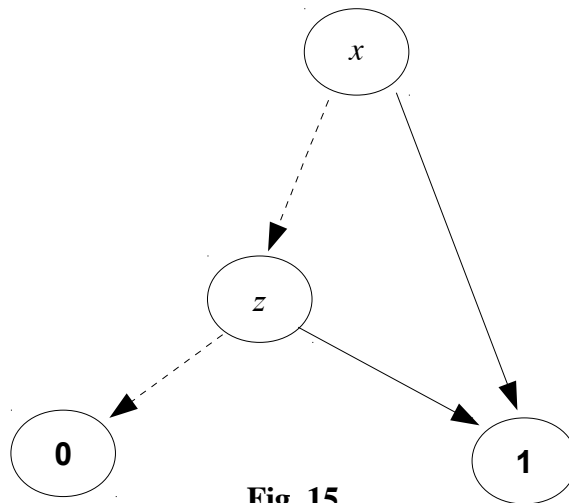


Fig. 15

Como se puede ver a simple vista, este árbol restringido, obedece a la expresión lógica $F_{y=1} = x + z$.

Además de obtener un árbol restringido, esta operación puede usarse para realizar una evaluación lógica de la expresión contenido en el BDD. De esta forma, si se asigna un valor lógico a cada variable, al final se obtendrá un árbol de sólo un vértice, el vértice **1** o **0**. Obviamente el vértice resultante será el que indique el valor de verdad de la expresión lógica contenida en el árbol, dada esa asignación de valores de verdad para las variables.

Obtiene una nueva raíz de un BDD basándose en el BDD con raíz v
 # y con una asignación de valores booleanos en algunas variables

```

restrictFromVertex(v, assignement):
    if(v.isLeaf()):
        # Hay un único vértice 1 ó 0
        return T[v.index]
    if(v.variable in assignement):
        boolean value = assignement[v.variable]
        if(value):
            return restrictFromVertex(v.high, assignement)
        else:
            return restrictFromVertex(v.low, assignement)
    else:
        low = restrictFromVertex(v.low, assignement)
        high = restrictFromVertex(v.high, assignement)
        if(low.index == high.index)
            return low
        return addVertex(v.variable, low, high)

```

Obtiene un nuevo BDD basándose en este BDD junto con una
asignación booleana a algunas variables.

```

restrict(bdd, assignement):
    restrictedBDD = restrictFromVertex(bdd.root, assignement);
    rfunction = bdd.function
    for(pair : assignement.pairs()):
        variable = VARIABLES[pair.key]
        value = pair.value
        rfunction = rfunction.replace(variable, value)
    return new BDD(rfunction, restrictedBDD)

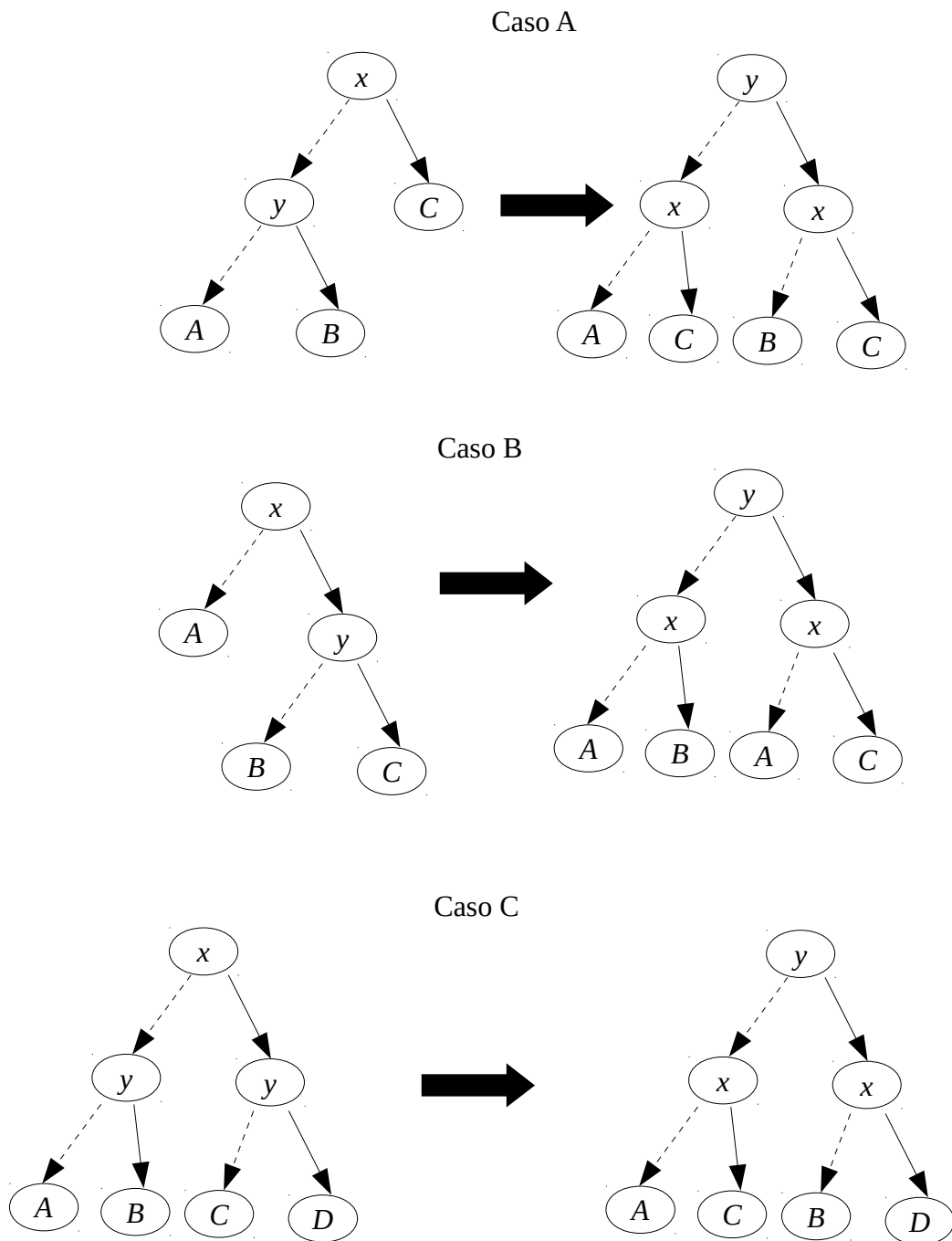
```

5.5.5 Swap

Esta operación intercambia dos niveles del árbol. El objetivo es tener una operación que permita obtener algunos vértices huérfanos, de forma que se puedan eliminar y por tanto reduciendo el tamaño del árbol.

La implementación es ignorada en la mayoría de los trabajos de la bibliografía y en ellos se indica [RUD93] como referencia. Para comprender mejor esta operación se pueden ver las notas del mismo autor en el taller [RUD].

En [JAC91], los autores indican de forma gráfica cada uno de los posibles cambios escenarios en los que se puede encontrar un vértice que ha de intercambiarse con el del siguiente nivel. Los reproducimos a continuación:

**Fig. 16**

Supongamos que en el nivel actual se encuentra la variable x y en el siguiente la variable y . El resto de vértices que no tengan ninguna de estas dos variables se les pondrá como nombre A , B , C o D .

En el resto de escenarios de intercambios de variables, el vértice x no tiene vértices descendientes con la variable y , por lo tanto, no se produce ningún intercambio.

A continuación incluimos el pseudocódigo de los distintos casos de intercambio, indicando en cada uno de ellos a qué caso se refiere.

El método `addWithoutRedundant(varI, A, C)` añade un vértice con esos valores de variable y y con los descendientes `low` y `high`, comprobando que no existe ya un vértice con esos atributos. Si no existe, devuelve un nuevo vértice con esos valores, si existe, lo obtiene y de igual forma lo devuelve.

```
# Reemplaza el vértice v (si tiene la variable varJ)
```

```
# con el vértice del siguiente nivel
```

```
swapVertex(Vertex v, int varJ):
```

```
    swapWasMade = false
```

```
    varI = v.variable
```

```
    low = v.low
```

```
    high = v.high
```

```
    A = null
```

```
    B = null
```

```
    if (!low.isLeaf()):
```

```
        A = low.low
```

```
        B = low.high
```

```
    else:
```

```
        A = low
```

```
        B = low
```

```
    C = null
```

```
    D = null
```

```
    if (!high.isLeaf()) :
```

```
        C = high.low()
```

```
        D = high.high()
```

```
    else:
```

```
        C = high
```

```
D = high

newLow = null
newHigh = null

# Caso a:
if (low != null && low.variable == varJ &&
    (high == null || high.variable != varJ)):
    newLow = addWithoutRedundant(varI, A, C)
    newHigh = addWithoutRedundant(varI, B, C)
    setVertex(v, varJ, newLow, newHigh)
    swapWasMade = true

# Caso b:
else if ((low == null || low.variable != varJ) &&
    (high != null && high.variable == varJ)):
    newLow = addWithoutRedundant(varI, A, B)
    newHigh = addWithoutRedundant(varI, A, C)
    setVertex(v, varJ, newLow, newHigh)
    swapWasMade = true

# Caso c:
else if ((low != null && low.variable == varJ) &&
    (high != null && high.variable == varJ)):
    newLow = addWithoutRedundant(varI, A, C)
    newHigh = addWithoutRedundant(varI, B, D)
    this.setVertex(v, varJ, newLow, newHigh)
    swapWasMade = true

# Caso d:
else if ((low == null || low.variable != varJ) &&
    (high == null || high.variable != varJ)):
    swapWasMade = false

# Caso e:
else if ((low == null || low.variable != varJ) && high == null):
    swapWasMade = false

return swapWasMade

# Intercambia un nivel con el siguiente
```

```
swap(int level):

    # Si es el último nivel, ignorar
    if(level == variables.size()-1)
        return false

    variableI = variables.getVariableInPosition(level)
    variableJ = variables.getVariableInPosition(level+1)

    boolean swapWasMade = false

    verticesOfThisLevel = V[variableI]
    for(Vertex v : verticesOfThisLevel):
        swapWasMade = swapWasMade || swapVertex(v, variableJ)

    variables.swap(variableI, variableJ);
    return swapWasMade
```

5.6 Algoritmos

Con el objetivo de reducir el número de vértices, hemos desarrollado una serie de algoritmos que hacen uso del intercambio de variables.

5.6.1 Window Permutation

Este algoritmo está basado en los trabajos [FUJ91] y [ISH91]. Consiste en definir una ventana móvil de un determinado tamaño sobre las variables ordenadas y obtener el mejor orden posible en cada posición. En cada iteración en la que se mueve la ventana se almacena la mejor solución y al final, se devuelve ésta.

Es decir, se obtiene para cada posición de la ventana la permutación que genera un orden cuyo tamaño de árbol es mínimo.

Rudell, en [RUD93] indica que este algoritmo es eficiente para tamaños de ventana 3, 4 ó 5, pero sus resultados indican que su algoritmo es mejor.

5.6.2 Sifting de Rudell

Richard Rudell en el año 1993 desarrolló un algoritmo de reducción del número de vértices en árboles BDD, [RUD93]. El algoritmo consiste en encontrar la posición óptima de una variable en el árbol, suponiendo que las demás variables están fijas.

Así, comenzamos con una variable determinada y movemos sus vértices hacia el fondo del árbol y luego de vuelta hacia la primera posición. En cada paso vamos calculando el número de vértices que tiene el árbol, de forma, que cuando se termine el proceso se sepa exactamente cuál es la posición que genera un tamaño de árbol menor.

Como ya sabemos la mejor posición, sólo tendremos que subir o bajar los vértices de esa variable hasta encontrar la posición antes encontrada.

Como se puede ver, este algoritmo heurístico es sencillo y da unos resultados muy buenos para problemas con pocas variables.

Un aspecto importante a tener en cuenta es el de cómo ir escogiendo las variables para ir realizando los intercambios. Nosotros hemos optado por tener varias estrategias: ir escogiendo las variables según su número de vértices, tal y como se recomendaba en [RUD] o tomar la variable que más ocurrencias tenga en la fórmula o tomar una variable al azar.

5.6.3 Algoritmo de intercambios aleatorios

Mostramos los resultados de un algoritmo aleatorio que consiste en realizar una serie de iteraciones y en cada iteración hacer un intercambio de una variable escogida de forma aleatoria con la que ocupe la posición siguiente.

En cada iteración comprobamos si el grafo resultante es de menor tamaño que el inicial, y si es así, almacenamos ese nuevo orden como mejor solución.

Por último, devolvemos el mejor orden encontrado.

Obviamente, no esperamos grandes resultados de este algoritmo, sino simplemente una base de la que partir y poder comparar con el resto de algoritmos.

5.6.4 Algoritmo genético

El algoritmo genético fue desarrollado después de leer el trabajo [LEN08] pensé que sería una buena idea implementarlo y compararlo a las heurísticas ya comentadas.

Estos algoritmos se basan en la metáfora biológica de que una población irá mejorando poco a poco si vamos realizando cruces entre ellos y mutaciones esporádicas. De esta forma, después de un número de iteraciones

En nuestra implementación, hemos optado por un algoritmo genético clásico, que no contuviera hibridación. De forma que contiene las operaciones clásicas de este tipo de algoritmos.

Antes de comenzar a describir sus partes, hemos de destacar un detalle sobre el motor de números aleatorios. Este generador usa la misma semilla para todas las operaciones aleatorias, de forma que sean reproducibles los experimentos. Es decir, que si ejecutamos con las mismas semillas los experimentos, devolverán siempre los mismos resultados.

5.6.4.1 Estructuras de datos

Hemos optado porque cada cromosoma sea un orden de variables. Cada cromosoma tendrá el orden y el número de vértices que se obtienen aplicando ese orden al BDD. Así podremos usar este número de vértices como medida de la bondad del cromosoma, evidentemente, cuanto menor sea este valor, mejor orden será.

5.6.4.2 Población inicial

De esta forma, cuando generamos inicialmente una población de cromosomas, lo que hacemos es generar órdenes aleatorios de variables y reordenar nuestro árbol para calcular el tamaño de éste. Es obvio que este proceso es costoso, y su tiempo dependerá en gran medida del número de cromosomas que vayamos a usar, dado que para aplicar al árbol el orden de cada uno de ellos, habrá que realizar como mucho para cada variable $n-1$ intercambios, por lo que tendremos un orden de eficiencia cuadrático.

5.6.4.3 Selección

Después, en la selección, se toman aleatoriamente un número determinado de padres. No se optimizan usando el algoritmo de Rudell como en [LEN08], porque pensamos que aplicar una heurística aquí podía hacer que se llegase a un máximo local y sobre todo porque queríamos tener un algoritmo genético puro, dejando el tema de las hibridaciones para otra implementación distinta.

5.6.4.4 Cruce

Estos cromosomas seleccionados se emparejan dos a dos para generar, mediante cruces, los cromosomas hijos. Este cruce sí ha sido tomado de [LEN08] y se basa en intercalar las posiciones de cada una de las variables de los padres, sin repetir variables, claro. Por ejemplo, si tenemos los siguientes órdenes, para generar su descendiente iríamos intercalando cada una de las variables:

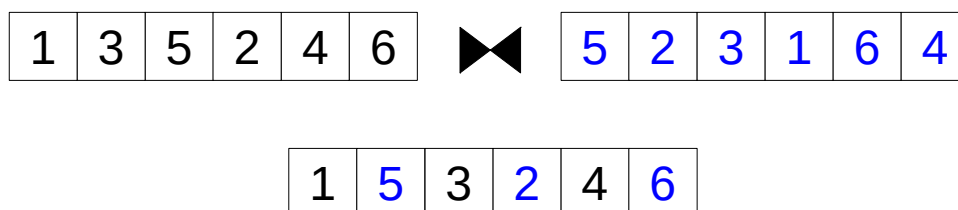


Fig. 17

Nótese que cuando se va a escoger la variable 5 del cromosoma de la izquierda, ya se le ha asignado una posición a esta variable, debido a que se encontraba en el frente del cromosoma de la derecha. Ante este problema, hemos de continuar buscando una variable del mismo padre que no se encuentre ya en el cromosoma hijo. En ese caso concreto, le asignamos la variable 4, dado que es la primera del cromosoma padre que todavía no tiene el hijo.

5.6.4.5 Mutación

La operación de mutación se ejecuta sólo con una determinada probabilidad y consiste en intercambiar las posiciones de dos variables. Obviamente, puede que en un caso concreto no se cambie ninguna variable de sitio, pero si se produce algún cambio habrá que recalcular el tamaño de grafo que genera.

5.6.4.6 Actualización de la población

Para terminar la iteración, se actualiza la población. Primero se añaden a la población los hijos anteriormente generados. Luego eliminamos de la población los peores cromosomas hasta que al final, la población permanezca con el mismo número de cromosomas que tenía inicialmente.

Hemos optado por no reiniciar la población cuando se estanque el algoritmo para no caer en mínimos locales, dado que desde un orden “malo”, es decir, un orden que genere un árbol de un tamaño enorme, se puede obtener mediante mutaciones y cruces un orden mucho mejor.

5.6.5 Algoritmo memético

El algoritmo memético es una optimización del algoritmo genético. Este algoritmo se basa en aplicar una búsqueda local a los cromosomas obtenidos en el proceso de selección.

Cuando ejecutamos el algoritmo genético, vimos cómo se expandía tanto la búsqueda, que

debido a que teníamos cromosomas que representaban órdenes que hacían que el árbol no cupiese en memoria principal. Por eso, pensamos en aplicar un método de optimización rápido que permitiese explorar más en profundidad el espacio de búsqueda, aun perdiendo algunas posibles soluciones que hicieran que el proceso se detuviese debido a falta de memoria.

Para su proceso de optimización hemos escogido el algoritmo de Rudell porque es muy eficiente y no enlentece el algoritmo demasiado. Aunque, como hemos añadido para cada cromosoma un proceso de optimización, este algoritmo será más lento. Esperamos con esta técnica reducir el consumo de memoria.

La optimización se realiza en dos lugares. En primer lugar, toda la población es generada de forma aleatoria, pero cada cromosoma es mejorado con el algoritmo de *Sifting*. Luego, los cromosomas hijos son optimizados también mediante este proceso.

6 Un nuevo algoritmo de reducción: Iterative Sifting

Como hemos visto anteriormente en el capítulo 3, el algoritmo *Sifting* de Rudell está basado en buscar la mejor posición para el nivel de variable que tenga mayor número de vértices en el árbol. Es una heurística sencilla y que da buenos resultados rápidamente.

Nosotros hemos desarrollado un algoritmo inspirado en el *Sifting* que no sólo moverá las variables a su mejor posición, sino que tratará de explotar la mejora repitiendo el proceso hasta que no se produzca ninguna mejora. Así, este algoritmo está basado en realizar de forma iterativa el movimiento de variables hasta la mejor posición y actualizar el orden si es mejor que el mejor encontrado. En cada iteración se establece el orden de variables en función del número de vértices de cada variable. De esta forma, nos aseguramos que este algoritmo heurístico tratará de mover primero las variables que tienen asociadas mayor número de vértices en el árbol, y por tanto, generando mayor optimización en el árbol, y las va moviendo hasta que cada una se encuentra en la mejor posición.

La búsqueda de la solución vuelve a comenzar en cuanto haya una mejora, ya que el proceso de optimización trata de optimizar todavía más el orden elegido, al contrario que el algoritmo de Rudell que se conforma y termina el proceso. Es decir, se explota una solución con el objetivo de encontrar un posible camino que lleve a una solución mejor.

Así pues, se basa en el algoritmo de Rudell en el sentido de que usa el mismo proceso de mover una variable dejando fijas las demás, pero lo novedoso de este algoritmo es la continuación de la búsqueda cada vez que haya una mejora. Un enfoque sencillo, pero que mejora el algoritmo de *Sifting*, tal y como se mostrará en la sección de experimentos.

Mostramos a continuación el pseudocódigo de este algoritmo:


```
IterativeSiftingReduction(bdd)
    # El orden inicial es el orden que tenga el bdd
    bestOrder bdd.variables()

    # y el mejor tamaño es el tamaño inicial
    bestSize = bdd.size()

    # Contador de iteraciones,
    i = 0;

    # ¿Hay una mejora en el proceso?
    thereIsAnImprovement = false;
    do
        i = 0
        thereIsAnImprovement = false;

        # Hay un límite de iteraciones del algoritmo en cada proceso de
mejora        while(i < iterations)
            # Ordenamos las variables de forma descendiente en función del
            # número de vértices de cada variable en el árbol bdd
            variableOrder = initVariableOrderDesc(bdd)

            foreach int vari in variableOrder
                # Para cada variable vari, la desplazamos a la posición
                # que hace el número de vértices del bdd mínimo
                findBestPositionForVariable(bdd, vari)

                # Tamaño total del BDD obtenido al
                # desplazar esta variable a su mejor posición
                currentOrderSize = bdd.size()

                # Si el tamaño es menor que el mejor tamaño,
                # almacenamos el orden
                if(bestSize > currentOrderSize)
                    bestOrder = bdd.variables()
```

```
        bestSize = currentOrderSize
        thereIsAnImprovement = true

        i++
    while(thereIsAnImprovement)

        # Se aplica el mejor orden al BDD para reducirlo
        # para cada variable, se intercambia con la siguiente o anterior
        # hasta encontrar la posición dada por bestOrder
        bestOrder.applyOrderToBDD(bdd)
```

Es importante destacar que este algoritmo es de nuevo desarrollo y su publicación está pendiente en una revista científica.

7 Aplicaciones de los BDDs a la Ingeniería del Software

7.1 Introducción

La Ingeniería del Software es una disciplina joven, de hecho, este término comenzó en usarse en la NATO Software Engineering Conference⁴ de 1986 [RAN96]. Desde entonces ha ido madurando y creciendo durante el siglo XX y XXI [BOE06]. Aun así, hay quien considera que la Ingeniería del Software no tiene las características de las ingenierías tradicionales, [DEM09] [DIJ88].

Actualmente, asociaciones como el Software Engineering Institute (SEI) tienen como objetivo estandarizar los procesos de ingeniería y dar una serie de pautas y consejos sobre cómo ha de trabajar un ingeniero de software. El SEI ha publicado un estándar en el que está contenido todo el conocimiento que ha de tener un ingeniero de software [SEI04].

Por otro lado, la Ingeniería del Software es una profesión con reconocimiento internacional. En el año 2013 el Consejo Nacional de Examinadores para Ingeniería e Inspección (*National Council of Examiners for Engineering and Surveying, NCEES*) de los EE. UU. ofreció un examen de Ingeniería del Software que permitía a los examinandos adquirir el título de Ingeniero de Software Profesional. Los licenciados con este título pueden realizar proyectos críticos en los que la salud o personas estén en riesgo. Así, países como Canadá y EE. UU. licencian a sus ingenieros, regulando esta profesión.

Una de las partes que confiere a la Ingeniería del Software la condición de ingeniería son los Métodos Formales. Estos métodos dan un rigor matemático a la disciplina, distinguiéndola de un oficio artesanal, y permitiendo desarrollar software en sistemas críticos [BUR95].

7.2 Métodos Formales

Los Métodos Formales (*Formal Methods* en inglés) son un conjunto de técnicas matemáticas

4 Congreso de Ingeniería del Software de la Organización del Tratado del Atlántico Norte

para desarrollar sistemas software y hardware. El objetivo de estas técnicas es el de dar una base científica a una ingeniería de forma similar a cómo lo hace la Física sobre el resto de ingenierías tradicionales.

Los Métodos Formales no surgieron a partir de un conjunto reducido de investigadores, sino a partir del trabajo en paralelo de multitud de investigadores, por lo que es difícil hablar de trabajos seminales en este área sin dejarse algún autor o trabajo sin nombrar. Como trabajos destacables están los de John MacCarthy [MAC83] y [MAC93] en los que daba sentido matemático a algunos aspectos de la computación. También están los trabajos de Peter Landin sobre la evaluación de expresiones [LAN64] y correspondencia entre lenguajes de programación y el λ -cálculo de Church [LAN65]. Debemos nombrar a Robert Floyd, en el que su trabajo [FLO67] tenía como objetivo, darle una semántica correcta a los programas. Por supuesto, hemos de nombrar el *An axiomatic basis for computer programming* [HOA69] de C. A. R. Hoare en el que da fundamento lógico a la programación de computadores y *Proof of Correctness of Data Representations* [HOA02]. Otros autores trataron este tema en libros, así tenemos el *A Discipline of Programming* de Edsger W. Dijkstra [DIJ76] y *The Art of Programming* de Donald Knuth [KNU68].

Todos estos autores, cada uno por un camino distinto, trataron de dar fundamentos matemáticos a la computación y por tanto, a buena parte de la Ingeniería del Software.

Viendo el nacimiento y evolución de los Métodos Formales, es fácil entender que haya muchas técnicas de este tipo. Los trabajos [WOD09] y [BJO14] proporcionan una taxonomía de los distintos métodos formales. En particular, tomando el trabajo más moderno, [BJO14], los autores realizan la siguiente clasificación basada en la distinción entre métodos de especificación y métodos de análisis y referencian una serie de herramientas basadas en Métodos Formales que indicamos a continuación como ejemplos de cada tipo.

Los **Métodos de Especificación** son los métodos más antiguos y tienen como objetivo definir un lenguaje de especificación normal. Estos lenguajes permitirán, a su vez, definir especificaciones para sistemas software de forma completa y sencilla. Hay dos subclases de métodos de especificación: los orientados a modelos y los métodos algebraicos.

- Los **Métodos de Especificación Orientados a Modelos** trasladan el comportamiento de un sistema software construyendo un modelo basado en objetos matemáticos. Ejemplos de este tipo de método es SCR, VDM, Z y las Redes de Petri.
- En cambio, los **Métodos de Especificación Algebraicos** (o métodos orientados a propiedades) definen de manera formal los tipos de datos (junto con sus operaciones), se abstraen de los detalles de implementación y definen una serie de restricciones al comportamiento de los tipos de datos. Ejemplos de estos métodos de especificación son CafeOBJ, CASL y Maude.

Los **Métodos de Análisis** se centran en el estudio de la ejecución del software. Pueden clasificarse en:

- **Interpretación Abstracta** (Astrée)
- **Demostración de Teoremas** (Coq, PVS, Z3)
- **Comprobación de Modelos** (SMV y SPIN/Promela).

Es importante notar que los Métodos de Especificación Algebraicos pueden también

considerarse métodos de análisis, debido a que al definir un álgebra para las operaciones, la lógica de su especificación se puede analizar de forma sencilla.

[BJO14] proporciona un buen resumen de los métodos existentes hasta el año 2014 que puede resumirse con el siguiente gráfico:

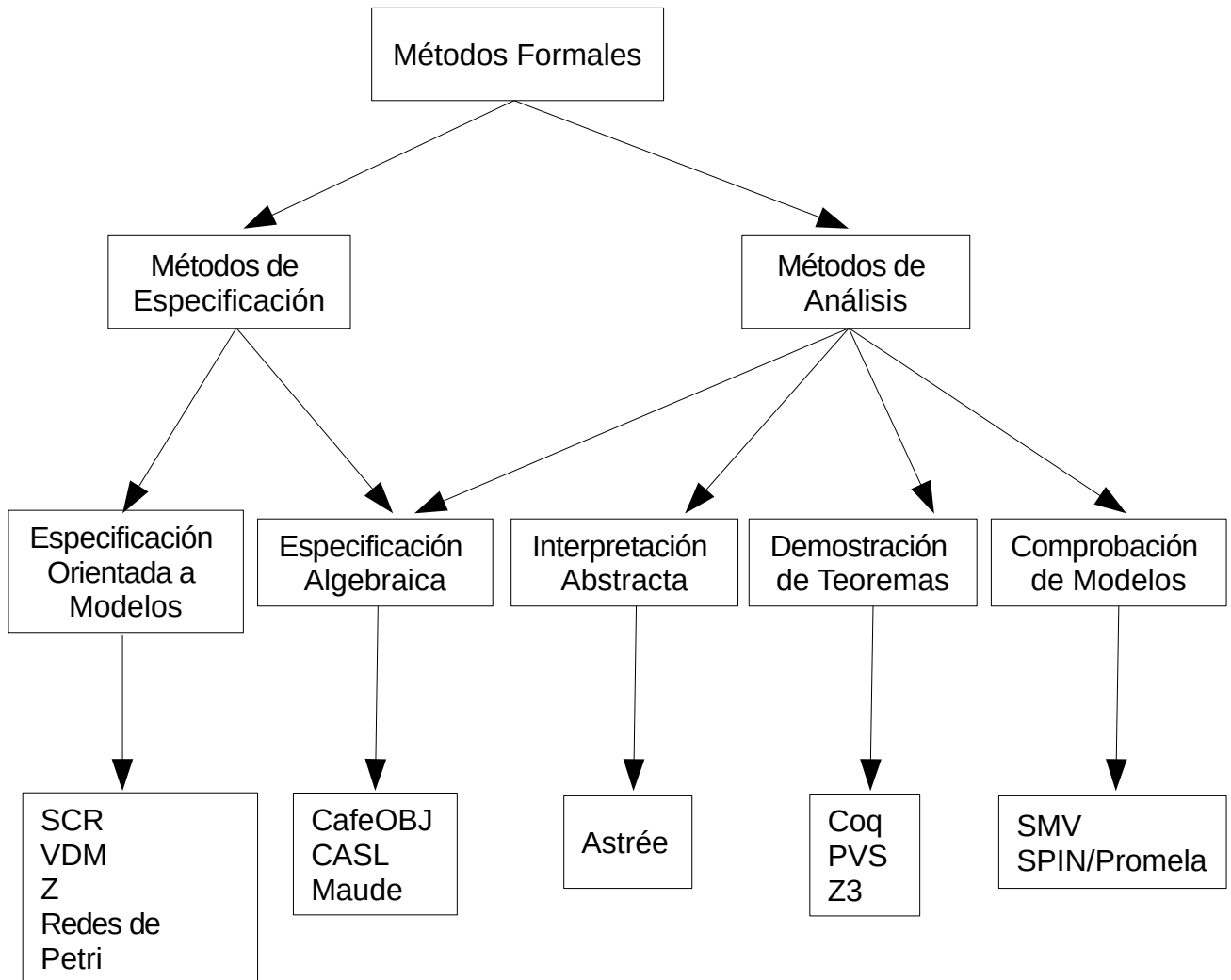


Fig. 18

7.3 Estado de los métodos formales en la industria

En [HAL90], Anthony Hall hacía una revisión de los mitos más comunes de los Métodos Formales, haciendo una crítica de la visión de los ingenieros de software sobre estos métodos. En general, Hall, descubría una serie de ideas que pueden resumirse de la siguiente forma:

- Los Métodos Formales no pueden garantizar que un software es perfecto.
- Los Métodos Formales pueden aplicarse a multitud de sistemas, no sólo a los sistemas críticos.

- Los Métodos Formales no requieren un gran componente matemático.

También en este trabajo, Hall, indicaba que estas técnicas eran muy diversas, factibles y que no tenían por qué encarecer el proceso de desarrollo. Es decir, la motivación del artículo era quitar ideas preconcebidas a los ingenieros.

Veinte años más tarde, David L. Parnas escribió un polémico artículo [PAR10] en el que se preguntaba el motivo por el que no se habían popularizado. Este autor indica cómo se publican artículos de historias de éxito de uso de Métodos Formales en la Ingeniería del Software, lo que paradójicamente, indica que éstos son ampliamente ignorados por la industria. Parnas identifica tres problemas que dificultan la adopción de los Métodos Formales entre los ingenieros de software:

- Las técnicas se centran en el aspecto matemático de la herramienta, pero no ofrecen ayudas para su uso en sistemas reales complejos.
- Los ingenieros de software no son como otros ingenieros, la calidad de su grado no es la deseada y se centran en enseñar tecnologías y matemáticas abstractas que los estudiantes no saben aplicar.
- Los científicos de la computación no usan las matemáticas de la misma forma que los propios matemáticos.

Parnas también critica la complejidad de los modelos usados y cómo los problemas reales se simplifican demasiado, de manera que se adapta el problema al modelo y no a la inversa. La librería DJBDD busca efectivamente lo contrario, de manera que implementando una serie de conectores, el desarrollador pueda evitarse desarrollar las aserciones de cada estado. De hecho, nuestro modelo podría usarse también para comprobar si los estados del sistema software son correctos, para luego eliminarse. En la sección de Arquitectura Software hablaremos de esto.

7.4 *Métodos Formales basados en los BDDs*

Los Árboles Binarios de Decisión actúan fundamentalmente como una tabla de verdad, como un evaluador de expresiones lógicas que permite:

- Evaluar una expresión lógica obteniendo un valor booleano.
- Comprobar la satisfacibilidad de una fórmula lógica.
- Comprobar si dos expresiones lógicas son equivalentes.

En este trabajo nos hemos centrado en estos dos aspectos, aunque hay otros como la capacidad de servir herramienta en el cálculo proposicional [HOL00] que no se han desarrollado, aunque se ha comprobado que la solución software puede de ser de ayuda también en ese ámbito.

Principalmente, se ha usado los BDDs como herramienta en la Comprobación de Modelos. Conocido como *Model Checking* en inglés, la **Verificación de Modelos** ([CLA81] y [QUI81]) es una técnica en la que los sistemas se modelan como máquinas de estados finitos, las propiedades se escriben en lógica temporal proposicional y se usa un procedimiento de verificación.

Dado un Modelo M , un estado inicial s y una propiedad p (expresada como una fórmula de lógica temporal), la Comprobación de Modelos se basa en la siguiente expresión:

$$M, s \models p$$

Esta expresión se puede ver como la búsqueda de todos los estados s tales que el grafo de estados y transiciones M pruebe la proposición p .

Cuando la búsqueda en el espacio de estados se basa en la representación de conjuntos de estados y las relaciones de transición se consideran fórmulas, se habla de **Verificación Simbólica de Modelos** y se pueden usar los BDDs como representación de las fórmulas lógicas. Kenneth L. McMillan fue el primero en usarlos en su tesis, [MCM92].

El objetivo de McMillan era tener una representación canónica de las expresiones lógicas y sobre todo, dado el hecho de que podía haber una explosión de estados en estos verificadores, los BDDs se plantean como una solución idónea dada la posibilidad de reducirse el número de vértices del árbol de forma dinámica gracias a los algoritmos de reducción comentados en la sección anterior.

En la actualidad, hay multitud de sistemas de verificación de modelos que usan internamente BDDs. Por nombrar a algunos, SMV [MCM93] fue el primer comprobador de modelos en usar los BDDs como método de verificación. Bepop [BALL00] es otro comprobador de modelos basado en los BDDs usado por Microsoft Research como herramienta de su analizador estático de código [BALL04].

En estos últimos años, se ha seguido aplicando los BDDs a la Verificación de Modelos, de manera que, por ejemplo, el Comprobador de Modelos CPAChecker usa los Árboles Binarios de Decisión como base para su mecanismo de análisis de programas [BEY13]. Otro ejemplo es `jpf-bdd`, una extensión del comprobador de estados *Java Pathfinder*, desarrollada por Alexander von Rhein, Sven Apel y Franco Raimondi [RHE11]. En esta extensión, usan un BDD como representador de estados, obteniendo una mejora sobre el métodos estándar, debido a las características de reducción del espacio que tienen los BDDs.

8 Software

8.1 Herramientas usadas

Para ejecutar el software proporcionado se necesita una máquina virtual de Java con la versión 7. Concretamente este paquete se ha desarrollado usando OpenJDK7 [OpenJDK].

Dada la naturaleza multiplataforma de Java, no se requiere de ningún sistema operativo específico, ni enlazado con librería externa para su uso, dado que están integradas en el paquete jar *store/DJBDD.jar*.

El proyecto se encuentra en el siguiente repositorio público del sistema de control de versiones GIT:

<https://github.com/diegojromerolopez/djbdd>

A continuación, vamos a detallar las librerías usadas, dando un fundamento al motivo que nos ha llevado a hacerlas parte integral de nuestro proyecto:

8.1.1 antlr3

Antlr proporciona la posibilidad de crear reconocedores para gramáticas. En nuestro caso lo hemos usado para proporcionar a nuestra librería de la capacidad de construir árboles a partir de una expresión lógica con la misma sintaxis que una expresión lógica en el lenguaje de programación Java.

Recordemos que la construcción del BDD se realizaba de forma recursiva realizando *Apply* entre sucesivos árboles generados a partir de la expresión lógica. Pues bien, el proceso es el siguiente, tomamos la expresión lógica, la convertimos en un árbol sintáctico abstracto usando antlr3 y vamos recorriendo ese árbol, generando BDDs y vamos operándolos entre ellos hasta obtener uno que contenga toda la expresión completa.

Este paquete contiene herramientas muy sencillas que permiten la creación de un reconocedor sintáctico a partir de una gramática como la que hemos usado:

```
grammar Logic;
```



```

options {
    output=AST;
}
parse
    : expression EOF!    // omitir token EOF
    ;
expression
    : dimplication
    ;
dimplication
    : isdifferent ('<->'^ isdifferent)*    // '<->' es equivalencia o doble
imp.
    ;
isdifferent
    : implication ('!='^ implication)*    // '!=' es lo contrario de <->
    ;

implication
    : notimplication ('->'^ notimplication)*    // '->' es la implicación
    ;
notimplication
    : or ('!->'^ or)*    // '!->' es la implicación negada
    ;
or
    : and ('||'^ and)*    // '||' es el 0 lógico
    ;
and
    : not ('&&'^ not)*    // '&&' es el Y lógico
    ;
not
    : '!'^ atom    // '!` es el operador de negación
    | atom
    ;
atom
    : ID
    | TRUE

```

```

| FALSE
| '(! expression )'!    // los paréntesis no tienen valor sintáctico
;

TRUE  : 'true';    // True y False los tomamos como palabras reservadas
FALSE : 'false'; //

ID    : ('a'..'z' | 'A'..'Z' | '0'..'9' | '_' | '{' | '}')+; // Variable
lógica

Space : (' ' | '\t' | '\r' | '\n')+ {$channel=HIDDEN;}; // Caracteres
vacíos

```

Para facilitarnos las cosas, se puede ver como hemos incluido cada operador y su negación. Esto permitirá poder negar un árbol completo de forma sencilla sin usar aristas etiquetadas. En siguientes secciones se profundizará en este detalle.

Con respecto a la versión, conocemos que existe una versión nueva de *antlr* (la versión 4), pero dado que nuestra gramática es sencilla y generativa por la derecha, no veíamos la necesidad de usar la nueva versión porque entre otras cosas, éramos familiares a la 3.

8.1.2 Javaluator

Tal y como hemos visto con el apartado de construcción y el anterior, la generación se realiza de forma recursiva generando un árbol sintáctico y generando BDDs y operando sobre ellos hasta obtener el BDD de la raíz, que es el que representa el árbol binario de toda la expresión.

Ahora bien, para dotar de mayor flexibilidad al desarrollador, permitimos que el proceso recursivo de creación del árbol no requiera de un análisis sintáctico, ni del uso de la operación *Apply*, sino simplemente de la creación implícita de la tabla de verdad, evaluando la expresión lógica con todas las posibles combinaciones de asignaciones de valores de verdad para las variables.

Obviamente esta opción no es deseable y es ineficiente, por lo que está desactivada por defecto y sólo debería usarse para expresiones lógicas triviales o cuando tengan un número lo suficientemente pequeño de variables como para ser eficiente, dado que probar todas las combinaciones de n variables implica realizar 2^n evaluaciones.

8.2 Diseño

A nivel de diseño software, a continuación se muestran los paquetes ordenados de forma alfabética y desarrollamos en cada uno de ellos la funcionalidad que contiene.

8.2.1 Paquete raíz: djbdd

Paquete raíz que contiene a todos los de la librería djbdd.

8.2.1.1 core

Este es el módulo principal, contiene todas las clases básicas de la librería. Sin estas clases, no habría sistema. Inicialmente se introdujeron estas clases en el paquete predeterminado, pero debido a que se vio que era una mala práctica, se creó un paquete por defecto en el que estuvieran todas. Este es ese paquete.

A continuación, describimos cada una de ellas de la forma más detallada posible en el orden lógico de uso:

8.2.1.1.1 VariableList

Lista de variables. Inicialmente se pensó en hacer que la lista de variables no fuera una clase sino simplemente una colección de objetos `String`. Eso se vio que no era propicio debido a que queríamos tener por un lado las variables, cada una con su índice y por otro el orden que se le había dotado en función a los intercambios realizados.

Por tanto, esta clase tiene dos estructuras principales (y una para facilitarnos el desarrollo, pero que no es vital):

- `variables`: lista de variables donde el índice indica el identificador de la variable. Este atributo no cambia nunca en el transcurso de la vida del sistema.
- `orderedVariables`: lista de variables de acuerdo al orden. Se usa para depuración, ya permite tener las variables en el orden natural. Cuando se intercambien dos variables, esta lista tomará el orden natural de las variables.
- `order`: indica el orden de cada variable, de forma que el valor en la posición i indica el orden de la variable i -ésima. Inicialmente, cada valor contiene la posición en la que se encuentra. En cuanto se empiecen a realizar intercambios de variables, los valores cambiarán a la posición donde se encuentre realmente.

8.2.1.1.2 Vertex

Esta clase contiene la estructura de cada uno de los vértices del

Tiene los siguientes atributos:

- `index`: clave única en la tabla T .
- `variable`: identificador de la variable que contiene en la lista de variables. Los vértices hoja la tienen asignada a un valor fijo que no representa a ninguna variable.
- `low`: referencia al descendiente *low*. Para los vértices hoja es *null*.
- `high`: referencia al descendiente *high*. Para los vértices hoja es *null*.
- `num_parents`: contador de vértices que apuntan a este vértice. Dado que usamos una misma red de vértices para todos los BDDs, tenemos que llevar la cuenta de cuándo un vértice no es apuntado por ningún otro.
- `num_rooted_bdds`: indica para cuántos BDDs es este vértice la raíz. De forma similar a `num_parents`, este atributo guarda la cuenta de cuántos BDDs lo usan como raíz, debido a que se comparte toda la malla de vértices.

Además de estos atributos, el vértice tiene las siguientes operaciones destacadas:

- `isLeaf`: informa si el vértice es un vértice hoja.
- `isRedundant`: informa si sus atributos *low* y *high* son iguales.
- `isDuplicate`: informa si dos vértices son duplicados, es decir, si comparten los mismos atributos *variable*, *low* y *high*.
- `isOrphan`: informa si el vértice es huérfano, es decir, si no hay ningún BDD que lo tenga como raíz y si no hay ningún vértice que apunte a él. En ese caso, este vértice puede eliminarse.

- `isChildOf/isParentOf`: comprobación de descendencia/paternidad (respectivamente). Estos métodos permiten saber si un vértice que se pasa como parámetro es hijo/padre (respectivamente) del vértice actual.

Por supuesto hay operaciones de conversión a cadena y de establecimiento de variable, *low* y *high* del vértice. Con respecto a esta última operación, hemos de notar que no es pública (al contrario del resto) sino que es propia del paquete puesto que se hace uso en la operación de intercambio de variables, implementada en la clase `TableT`.

8.2.1.1.3 `TableT`

Esta clase contiene las estructuras que definen el grafo global en el que están basados todos los BDDs.

En primer lugar, hay una tabla *T*, que contiene cada vértice dado su índice. Es decir, es una tabla hash en la que para cada vértice, se guarda una entrada en la que la clave es su atributo *index* y el valor es el propio vértice.

En segundo lugar, hay una tabla *hash* que almacena de forma única todos los vértices, de manera que nunca haya dos vértices con el mismo trío de valores variable, *low* y *high* que sea igual. Así, la clave es la concatenación sigue estas reglas:

- Si es el vértice hoja **1**: "-1-N-N"
- Si es el vértice hoja **0**: "-2-N-N"
- Si es otro tipo de vértice: `variable+"-"+low.index+"-"+high.index`

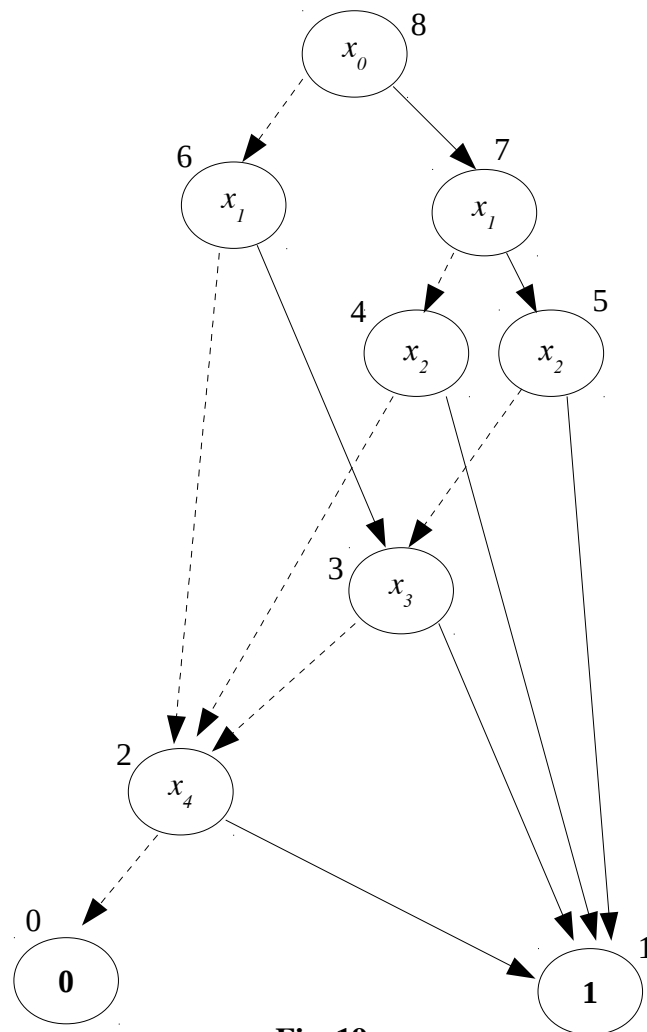
A esta tabla *hash* la llamamos *U* (de tabla de unicidad de vértices).

En tercer lugar, hay una estructura que agrupa todos los vértices en conjuntos según la variable que contiene cada uno. Implementamos esta estructura de grupos de vértices por variables como una tabla *hash* en la que la clave es la variable y el valor es una lista con todas las variables.

Como veremos en cuando expliquemos las distintas alternativas del algoritmo de intercambio de variables de Rudell, necesitamos tener un acceso rápido a los vértices de cada nivel. Obviamente, en cada intercambio, tendremos que cambiar a los vértices del conjunto que hayamos adelantado un nivel, y por tanto, cambiarles también su variable.

Esta estructura la llamaremos *V*, porque agrupa a los vértices por variables.

Ahora, vamos a mostrar un ejemplo de la estructura que se tendría en memoria para el árbol de la función $F = x_0x_2 + x_1x_3 + x_4$ siendo el orden de las variables el indicado por el subíndice de cada una de ellas. Así, tenemos el BDD representado gráficamente a continuación:

**Fig. 19**

Nótese que las variables ahora comienzan en 0, dado que en nuestra implementación, las variables son el índice de posición en la `VariableList`, comenzando en 0 y terminando en $n-1$, siendo n el número de variables.

Mostramos a continuación los valores de cada una de las tablas para el BDD con la expresión lógica $F = x_0x_2 + x_1x_3 + x_4$:

Tabla T

Índice	Variable	Low	High
0	-1	<i>null</i>	<i>null</i>
1	-2	<i>null</i>	<i>null</i>
2	4	0	1
3	3	2	1
4	2	2	1
5	2	3	1
6	1	2	3
7	1	4	5
8	0	6	7

Tabla 8**Tabla U**

Clave	Vértice
-2-N-N	0
-1-N-N	1
4-0-1	2
3-2-1	3
2-2-1	4
2-3-1	5
1-2-3	6
1-4-5	7
0-6-7	8

Tabla 9**Tabla V**

Variable	Vértices
0	{8}
1	{6, 7}
2	{4, 5}
3	{3}
4	{2}

Tabla 10

Una vez mostrado el ejemplo, queda un aspecto importante que tratar sobre la

implementación de estas tablas. Dado que en las operaciones sobre los BDDs, hay que liberar vértices, estas tablas deben reflejar esas eliminaciones.

La forma de realizar esta eliminación es la de mantener dos contadores de referencias en cada vértice. Hay un contador que indica cuántos vértices tienen al vértice como descendiente (atributo `num_parents`) y un atributo que indica para cuántos BDDs es la raíz, `num_rooted_bdds`.

Estos dos contadores se van modificando conforme se va construyendo el árbol de forma automática, y cuando tanto el contador de padres como el de número de BDDs para los que es raíz son 0, el vértice decimos que es huérfano y puede ser eliminado de las tablas.

Todo vértice huérfano no cumple ninguna función y puede ser eliminado en cuanto se pueda. Así, existe un método de recolección de basura que elimina de forma explícita los vértices. Este método de recolección de basura implementado para solventar este problema se llama `gc`.

Este método de resolución del problema de los vértices huérfanos puede parecer tosco, y de hecho, antes habíamos pensado una solución automática que permitía que el desarrollador se olvidase de tener que ir llamando periódicamente a la recolección de basura, aunque como se vio más adelante, no era lo suficiente eficiente para nuestros propósitos.

Antes de tener una malla de vértices común para todos los árboles, desarrollamos una arquitectura distinta que separaba completamente los vértices de un árbol de los de otro. Es decir, cada árbol tenía sus propias tablas *T* y *U*. Esta arquitectura tenía la ventaja de que al ser la estructura distinta era fácilmente paralelizable y permitía la carga en paralelo, obviamente.

Además, de esta característica, las tablas *T* y *U* de cada árbol no tenían referencias a vértices, sino referencias débiles a objetos de la clase `Vertex`, vértices en definitiva, [ORA] [NIC]. El objetivo de esta decisión era que si el vértice no era referenciado por nadie más que por estas tablas, o lo que es igual, no era descendiente de ningún otro, el recolector de basura lo podía eliminar. O dicho de otra forma, estas referencias no tienen poder como para indicar al recolector de basura que no han de eliminar a los vértices a los que apuntan.

Con esta arquitectura no hacían falta contadores de referencias y de hecho, la recolección de basura era totalmente transparente al desarrollador. Dado que, en cuanto un vértice dejaba de estar apuntado por otro, el recolector de basura de la JVM tenía la capacidad para eliminar el objeto, y por tanto, liberar la memoria usada.

Pero este enfoque tenía un gran problema: la gran redundancia de vértices entre distintos árboles. Ante cualquier operación lógica nos quedábamos sin memoria, porque repetíamos de forma insistente vértices en distintos árboles.

Además, otro problema era el liberar de forma periódica las referencias débiles que no apuntan a nada. Cuando se libera el objeto apuntado por una referencia débil, esta se convierte en una referencia nula que se ha de eliminar. Al final, había que implementar un método específico de liberación de referencias débiles nulas, o lo que es igual, un método de compactación de tablas para cada BDD.

En definitiva, no merecía la pena el esfuerzo para perder el control de la liberación de memoria y sobre todo, para no ahorrar nada, puesto que había igualmente que desarrollar un recolector de basura.

Continuando con los métodos destacados de este clase, está el método de recolección de basura antes comentado, métodos de comprobación de existencia dado un vértice, métodos de adición de vértices a las tres tablas y por supuesto, métodos de eliminación de vértices.

Tenemos que notar, también, el método de intercambio de un nivel con el siguiente, dado que este método se usa en los algoritmos de reducción por intercambio de variables que hemos implementado. Además, esta clase, llevará la cuenta de cuántas veces se ha realizado la operación de intercambio, dado que usaremos ese dato para comprobar la efectividad de cada método.

Por último, notamos que hay métodos que imprimen en un archivo de texto en formato DJBDD y en PNG el grafo completo.

8.2.1.1.4 BooleanEvaluator

Esta clase encapsula la llamada a *Javaluator* y permite que se pueda evaluar una expresión lógica de forma sencilla. Esta clase hereda de *AbstractEvaluator* que es una clase abstracta de *Javaluator*. Por supuesto, define todos los operadores lógicos posibles, su precedencia y su asociatividad. Por último, sobrescribe el método *evaluate*, para que devuelva la semántica correcta de cada operación lógica.

Cabe destacar, que el método de evaluación es un método estático llamado *evaluateFunction* que prepara la expresión sustituyendo cada variable por su valor de verdad y realizando la llamada a *evaluate*. Así, ocultaremos todo lo relacionado con *Javaluator* al resto de componentes de este software, logrando una buena separación entre niveles de abstracción.

8.2.1.1.5 BDD

Esta clase representa a un BDD concreto. Es decir, a un expresión lógica en forma de árbol binario de decisión.

Como atributos, cada árbol está determinado por un vértice raíz, un subconjunto de variables de las definidas como posibles variables de la expresión y su tamaño.

Estas variables permiten optimizar las operaciones lógicas con otros BDDs, además del propio proceso de construcción. El motivo de esto son las expresiones lógicas que no tienen todas las variables. Por ejemplo, en determinadas fórmulas, se usaban sólo una decena de variables, pero como habíamos definido más de 4000, el proceso de construcción era muy lento sin razón de serlo. Cuando aplicamos esta optimización, el proceso de construcción fue mucho más rápido.

El tamaño de un BDD ha de consultarse visitando todos los vértices que cuelgan del vértice raíz. Este proceso es costoso, de manera que una vez calculado, se guarda para futuras consultas.

Por último, la última optimización que le introduje fue la de almacenar si era un árbol tautológico o contradictorio, es decir, si el árbol devolvía siempre verdad o siempre falso, respectivamente.

8.2.1.1.6 BDDApply

Esta clase contiene la implementación del algoritmo *Apply* para ejecutar operaciones entre dos BDDs.

Cabe destacar que se usa una tabla de caché para no volver a computar las operaciones varias

veces sobre los mismos vértices, pero podemos decir que es una implementación muy fiel al algoritmo antes mostrado.

8.2.1.1.7 GCThread

Esta clase contiene la implementación de una hebra que permite la ejecución de forma concurrente de un recolector de basura.

Actualmente, la implementación de BDDs se basa en referencias débiles, tal y como hemos visto anteriormente. Pero esas referencias débiles han de ser eliminadas puesto que a fin de cuentas, ocupan espacio. Pues bien, esta clase permite al desarrollador olvidarse de la tarea de ir llamando al recolector de basura del sistema de BDDs, pudiendo configurar además la frecuencia de llamada de éste de forma dinámica.

Además, se ha desarrollado esta funcionalidad con una estructura orientada a objetos, para poder tratar con ella de la forma más correcta desde el punto de vista de la Ingeniería del Software.

8.2.1.2 io

Siguiendo la convención de Java, este módulo contiene utilidades de entrada y salida. Este módulo contiene clases para tratar con cada uno de los tipos de fichero desde los que se puede cargar un BDD.

Así, tenemos los siguientes tipos de cargadores:

- `CstyleFormulaFileLoader`: carga un BDD a partir de una expresión en estilo C.
- `DimacsFileLoader`: carga un BDD a partir de un archivo de cláusulas en formato DIMACS.
- `SheFileLoader`: carga un archivo a partir de un archivo en formato de Stephen She.

Además de estos cargadores de BDDs desde archivos, existe una clase que permite generar un archivo PNG usando la librería `GraphVizJava`. Esta clase es `Printer`. Por ejemplo, el siguiente gráfico ha sido generado usando esta funcionalidad:

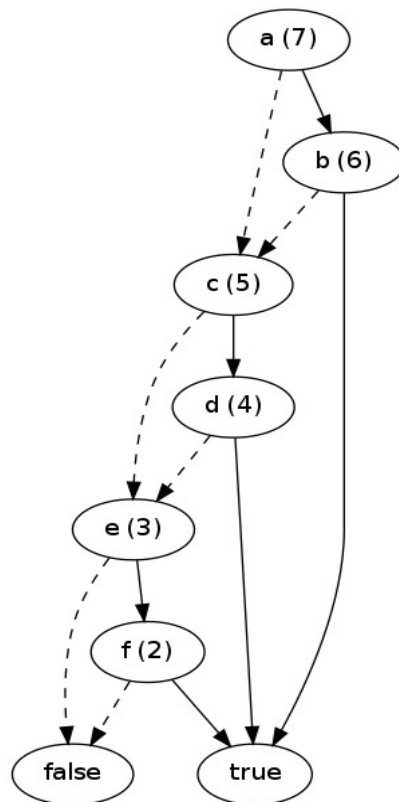


Fig. 20

Nótese que en el diagrama generado a los vértices hoja se les llama *false* y *true* para representar el vértice **0** y el **1** (respectivamente). Y que el resto de vértices contiene la variable y el identificador único de cada vértice entre paréntesis.

El resto de clases son ayudantes internos que permiten descargar de funcionalidad a las clases principales y que no tienen mucha más relevancia.

8.2.1.3 *logic*

Paquete que contiene métodos con el analizador sintáctico de fórmulas basado en antlr3. Contiene las clases generadas por antlr3, *LogicLexer* y *LogicParser* y un analizador desarrollado por mí que hace uso de éstas, *FormulaParser*. También hay una clase con ejemplos de uso que puede ignorarse completamente.

FormulaParser devuelve un árbol de sintaxis con los símbolos terminales y operadores de la fórmula. Este árbol lo usaremos en la construcción del BDD que hace uso de *Apply*.

8.2.1.4 *main*

Módulo principal, contiene el controlador que procesa los argumentos pasados desde línea de órdenes y realiza las llamadas a cada uno de los módulos según las órdenes que le pase el usuario.

Si se ejecuta sin argumentos, se muestra un pequeño manual de uso con todas las opciones que puede usar.

8.2.1.5 *reductors*

Este paquete contiene cada uno de los algoritmos de reducción del tamaño del BDD.

Cada método de reducción ha de heredar de la clase `ReductionAlgorithm`, que tiene el método `execute` que ha de ser sobrescrito por el desarrollador que quiera implementar un método de reducción.

Además esta clase contiene varias referencias a objetos globales para hacer la vida más sencilla al desarrollador, guarda una referencia de la tabla global `T` y de las variables. Por ende, la reducción se aplica al grafo total con todos los vértices. Esto es muy útil en el sentido de que podemos generar varios árboles BDD y mientras estén en memoria, si no los destruimos, si aplicamos algún método de reducción podremos comprobar cómo se reduce el tamaño de todos.

Cada método se implementa junto con sus clases necesarias en un subpaquete, de forma que sus requisitos más inmediatos estén ahí contenidos.

Los métodos de reducción implementados son los siguientes:

- `WindowPermutationReductor`: reduce el tamaño de los BDDs usando el algoritmo [FUJ91]. Lo llamamos con el nombre que le dio R. Rudell: Algoritmo de Permutación en una ventana.
- `SiftingReductor`: aplica el método de reducción de Rudell [Rudell93] sobre todos los BDDs que existan en el sistema.
- `RandomSwapperReductor`: método de reducción que consiste en ir realizando un intercambio sobre una variable escogidas de forma aleatoria en cada iteración. Este algoritmo lo usamos como base para compararlo con los algoritmos genético y memético.
- `GeneticReductor`: esta clase contiene la implementación del algoritmo genético de Lenders y Baier [LEN08].
- `MemeticReductor`: esta clase contiene una mejora del algoritmo genético de Lenders y Baier [LEN08]. Estos autores hablan de la posibilidad de desarrollar este algoritmo, aunque no muestran unos resultados sobre el mismo.
- `IterativeSifting`: esta clase contiene la implementación de nuestro algoritmo original que soluciona algunos problemas del algoritmo de Rudell, que como veremos en la sección de resultados, logra una mejora sobre sus porcentajes de reducción del tamaño del BDD. Está pendiente de publicación un trabajo sobre este método.

8.2.1.6 *test*

Pruebas de funcionamiento del paquete de BDD. Consta de 18 pruebas que pueden ejecutarse con la opción `--runtest` seguida del número de test que deseemos.

Cada test es estático e independiente. No produce resultados especiales, sino que el desarrollador ha de saber de antemano qué test está ejecutando para poder interpretar correctamente la salida que éste genera. Normalmente se tratan de impresiones de un BDD o de mensajes que indican por sí mismos si el tests es correcto o ha fallado.

Usamos este paquete como método rápido de probar fórmulas lógicas convenientes durante el proceso de desarrollo del software.

Nos habría gustado que el mismo test indicase si es válido o no e implementar tests unitarios, pero nuestro conocimiento en ese particular es limitado y el tiempo era limitado, por lo que no se ha hecho.

8.2.2 timemeasurer

En Java no existe un método canónico de medición de tiempos y queríamos encapsularlo en algún tipo de unidad funcional. Por tanto, hemos creado una clase, `TimeMeasurer`. Esta clase empieza a contar el tiempo desde que se construye una instancia de ella y termina, al ejecutar el método `end`. Como se puede ver, el nivel de encapsulación llega hasta las mediciones de tiempo.

8.2.3 graphvizjava

Este paquete contiene una clase realizada por Laszlo Szathamary, que permite tratar con GraphViz [GRA] de forma sencilla desde Java. Usamos esta utilidad, porque permite de forma sencilla convertir un archivo PNG a partir de un archivo `dot` [GRA2]. Usamos el formato `dot` como formato intermedio para mostrar los BDDs.

Para ver más información sobre este software, vea [SZ], donde se incluye todo el paquete de software original, los créditos completos y más información adicional.

8.2.4 logger

Contiene un sistema de registro de mensajes centralizado que permite activar y desactivarlo en tiempo de compilación. Si se desactiva antes de compilar este módulo, no se ejecutarán las condiciones de comprobación puesto que Java comprobará que la condición para mostrar los mensajes es falsa de forma constante, por lo que no se producirá una pérdida de rendimiento. Eso sí, este módulo no se puede activar y desactivar en tiempo de ejecución, por lo que sugiero realizar todas las pruebas primero, desactivarlo y finalmente generar el `.jar`.

Sólo contiene una clase, la clase `Log` que contiene varios métodos de impresión de mensajes con nombres exactamente iguales a los de `System.out`, como son `print`, `println`, etc.

8.3 Implementación

La mayoría de las implementaciones actuales están realizadas en código C o C++ de baja calidad. De hecho, en la mayoría de los trabajos encontrados, no se preocupan de detalles de cómo está implementada la operación `swap`, de manera que a la hora de mostrar resultados, simplemente se desarrolla un algoritmo basado en esta operación y se toman tiempos.

He optado por realizar una implementación libre y gratuita que pudiera usarse como laboratorio por parte de investigadores.

La implementación se encuentra disponible para descargar bajo licencia libre GPL3 con excepción de uso de clases en <https://github.com/diegojromerolopez/djbdd>.

8.4 Manual de uso de los binarios

8.4.1 Mostrar BDDs

Imprimir el BDD como imagen:

```
java -jar DJBDD.jar --image --<format> <file>
```

Imprimir el BDD a un archivo:

```
java -jar DJBDD.jar --print --<format> <file>
```

Formatos soportados (parámetro <format>)

- **dimacs:** formato de cláusulas en forma normal conjuntiva. Por ejemplo:

```
c simple_v3_c2.cnf
c
p cnf 3 2
1 3 0
-2 3 -1 0
```

Equivale a la fórmula $(x1 \text{ OR } x3) \text{ AND } (\text{NOT } x2 \text{ OR } x3 \text{ OR NOT } x1)$.

- **cstyle:** expresiones booleanas al estilo de C, usando como operadores lógicos el &&, ||, ->, <-> y el !, para el AND, OR, implicación y doble implicación, respectivamente. Deben estar precedidas por una línea con todas las variables separadas por comas, dadas en el orden el que han de tomarse. Ejemplos de expresiones válidas son los siguientes:
 - $a \ \&\& \ !b$
 - $a \ -> \ (!b \ \&\& \ (c \ || \ d))$
 - $a \ <-> \ (b \ \&\& \ !c)$
 - $a \ != \ (b \ \&\& \ !c)$
 - $x0 \ \&\& \ x1 \ \&\& \ !x2$
- **djbdd:** archivo DJBDD. Formato de texto en el que se pueden guardar los árboles BDD en este paquete. Este formato no se soporta para la llamada al procedimiento de reducción.

8.4.2 Realizar un benchmark

```
java -jar --memory-optimization-benchmark --dimacs <ruta del fichero>\
    <algorithm> [alg_params]
```

Donde <algorithm> es uno de los siguientes algoritmos:

- **sifting:** usa el algoritmo de Rudell tomando las variables con un orden basado en la ocurrencia de vértices.
- **sifting_sameorder:** usa el algoritmo de Rudell tomando las variables con el orden dado por el fichero.
- **sifting_randomorder:** usa el algoritmo de Rudell tomando las variables con un orden aleatorio. Tiene como parámetro una semilla aleatoria (parámetro `random_seed`).
- **window_permutation**, que tiene el parámetro `window_size` que ha de ser un entero y representa el tamaño de la ventana de este algoritmo.
- **random_swapper**, que además de la semilla aleatoria (parámetro `random_order`) tiene como parámetro el número de iteraciones (`iterations`) en las que ciclará el algoritmo.
- **genetic:** ejecución del algoritmo genético con los siguientes parámetros:

- `random_seed`: semilla aleatoria.
- `population`: número de cromosomas que usará el algoritmo genético.
- `generations`: número de ciclos del algoritmo genético.
- `selection_percentage`: porcentaje de cromosomas seleccionados en cada iteración.
- `mutation_probability`: probabilidad de que un gen de un cromosoma sufra una mutación.
- `memetic`: tiene los mismos parámetros del algoritmo genético.
- `isifting`: ejecución del algoritmo Iterative Sifting. Tiene los siguientes parámetros:
 - `iterations`: número de iteraciones del proceso.

Por ejemplo, una ejecución de todos los *benchmarks* que tenemos en nuestro paquete software usando un algoritmo genético, es la siguiente:

```
java -jar DJBDD.jar --memory-optimization-benchmark --dimacs \  
    ./data/benchmarks genetic random_seed=121481 population=20\  
    generations=1000 selection_percentage=0.2 mutation_probability=0.1
```

Nótese que los parámetros del algoritmo requieren el uso del signo igual para darles un valor concreto.

8.5 Ejemplos de uso de la API

```
// Variables booleanas
```

```
String[] variables={"a", "b", "c", "d", "e", "f"};
```

```
// Siempre ha de iniciar el sistema BDD antes de crear
```

```
// cualquier objeto BDD. Si no, el sistema dará error
```

```
BDD.init(variables);
```

```
// Las funciones se especifican con la sintaxis de operadores lógicos de  
Java,
```

```
// añadiendo además los operadores -> (operador de implicación)
```

```
// y <-> (operador de doble implicación)
```

```
String function = "(a && b) || (c && d)";
```

```
// Con la implementación actual, el orden de las variables
```

```
// es global a todos los BDDs, por lo tanto, si queremos cambiarlo
```

```
// hemos de usar la operación de intercambio de niveles,
```

```
// que intercambiará dos niveles para todos los BDDs
```

```
// Construcción de un nuevo BDD
```

```
BDD bdd = new BDD(function);

// Mostrar el BDD bdd en la salida estándar
bdd.print();

// Puede imprimir el BDD como una imagen PNG
Printer.printBDD(bdd1, "bdd_"+bdd1.size());

// Otro BDD
String function2 = "(a && e) || f"
BDD bdd2 = new BDD(function2);

// Muestra el BDD en el terminal
bdd2.print();

// Operaciones entre BDDs

// Este BDD es el AND lógico entre bdd y bdd2
BDD bdd3 = bdd.apply("and", bdd2);

// Este BDD es el OR lógico entre bdd y bdd2
BDD bdd4 = bdd.apply("or", bdd2);

// Construye el árbol con la negación
BDD not_bdd3 = bdd.not();

// Destruye explícitamente bdd2
bdd2.delete();

// Se puede liberar memoria de nodos "huérfanos" llamando
// a esta función de recolección de basura
BDD.gc();
```

9 Experimentos y resultados

Hemos realizado diversos experimentos con los algoritmos de reducción. Hemos tratado de usar datos lo más representativos del mundo real para mostrar el funcionamiento de cada uno de los métodos de reducción.

Los experimentos se han realizado sobre una máquina con un procesador Intel(R) Core(TM) i7-3770 CPU a 3.40GHz. En cuanto al software sobre el que se han realizado las pruebas, el sistema operativo es Ubuntu 12.04 con Java 1.7.0_25 con los siguientes parámetros

AdaptivePermSizeWeight	20
ErgoHeapSizeLimit	0
HeapSizePerGCThread	87241520
InitialHeapSize	196186624
LargePageHeapSizeThreshold	134217728
MaxHeapSize	3139436544
MaxPermSize	174063616
PermSize	21757952

Tabla 11

9.1 Problemas no satisfacibles

La librería se comporta muy bien, y es capaz de comprobar la satisfacibilidad de un problema concreto. Evidentemente, no buscábamos eso cuando la desarrollábamos, pero es una muestra más de que el trabajo es correcto.

Una fórmula no satisfacible es una contradicción, por lo que al construir el árbol, dado que

nos ha de devolver una representación de los caminos posibles según los valores de las variables, ha de darnos el único camino que hay: el vértice *false*. Este vértice indica que independientemente de los valores que se asignen a las variables de esa fórmula, se va a obtener un resultado negativo siempre.

9.2 Problemas satisfacibles

Todas las fórmulas que construimos y optimizamos son satisfacibles por los motivos anteriormente comentados.

Hemos tomado las 50 primeras cláusulas lógicas de los distintos archivos DIMACS y hemos trabajado sobre ellas, debido a que no buscábamos un software eficiente a nivel de poder competir con los paquetes que hay en la red, sino proporcionar un entorno con las más avanzadas características de software de ingeniería y que además, nos permitiera estudiar el proceso de construcción y optimización de un árbol BDD.

9.3 Datos de prueba

Se han tomado los datos de *benchmarks* de resolución de cláusulas lógicas de [HOO]. En esa web hay una serie de fórmulas lógicas expresadas en el formato DIMACS, que se usan para comprobar la eficiencia de determinados algoritmos de comprobación de satisfacibilidad.

Debido a la complejidad de los problemas, no se toman enteros, y sólo se consideran las primeras 50 cláusulas lógicas de cada fichero. Estos ficheros provienen de los distintos paquetes que se indican a continuación:

9.3.1 AIM

Fórmulas de 3 cláusulas generadas de forma aleatoria. Consta de los siguientes ficheros:

- aim-50-1_6-yes1-1.cnf
- aim-50-1_6-yes1-4.cnf
- aim-50-2_0-yes1-3.cnf
- aim-100-1_6-yes1-3.cnf
- aim-200-2_0-yes1-1.cnf

9.3.2 AIS

Instancias de un problema aritmético de búsqueda estocástica definido por Holger H. Hoos. Obtenidos de [AIS]. Tenemos 4 ficheros que son los siguientes:

- ais6.cnf
- ais8.cnf
- ais10.cnf
- ais12.cnf

9.3.3 Anomaly

Fórmula que contiene cláusulas lógicas derivadas del problema de la anomalía de Sussman en la planificación de acciones en un mundo de bloques. Consta sólo de un único fichero:

- anomaly.cnf

9.3.4 BW

Más problemas para el mundo de bloques. Distintas planificaciones con diferente estructura y tamaño.

- `bw_large.a.cnf`
- `bw_large.b.cnf`
- `bw_large.c.cnf`
- `bw_large.d.cnf`
- `huge.cnf`
- `medium.cnf`

9.3.5 Dubois

Instancias de fórmulas generadas por Olivier Dubois mediante `gensathard.c`. A priori no son satisfacibles, pero debido a que tomamos sólo las 50 primeras cláusulas, sí que lo son:

- `dubois21.cnf`
- `dubois22.cnf`

9.3.6 Hanoi

El problema de las torres de Hanoi con un número determinados de torres codificado como cláusulas lógicas.

- `hanoi4.conf`: el problema para 4 torres de Hanoi.
- `hanoi5.conf`: el problema para 5 torres de Hanoi.

9.3.7 Hole

Problema de situar palomas n palomas en $n+1$ agujeros sin que haya 2 palomas en el mismo agujero.

- `hole6.conf`

9.3.8 Nemesis

Cláusulas lógicas obtenidas del programa de patrones Nemesis. Para más información, visite [HOO2]:

- `bf0432-007.cnf`

9.3.9 Parity problem

Las instancias en este fichero provienen del problema de aprendizaje de la función de paridad:

- `par8-1.cnf`

9.3.10 Quinn

Un ejemplo descrito en el libro [Quinn] de Michael Quinn.

- `quinn.cnf`

9.3.11 Simple

Ejemplo de 6 variables trivial. Usado para comprobar para ejemplos triviales cuánto tarda en procesar cada algoritmo un ejemplo inmediato.

- `simple_v3_c2.cnf`

9.4 Resultados por algoritmo

En esta sección, mostramos los resultados por cada algoritmo. Mostramos los resultados en tablas, indicando no sólo la reducción en número de vértices y el tiempo de ejecución en segundos, sino también el número de intercambios entre variables realizado.

Nótese que para los algoritmos con componente aleatorio como son los siguientes:

- La variante del algoritmo de Rudell seleccionando las variables de forma aleatoria
- El algoritmo de los intercambios aleatorios
- El algoritmo genético
- El algoritmo memético.
- El algoritmo Iterative Sifting

Se han realizado 3 ejecuciones con las siguientes semillas aleatorias:

Semillas aleatorias

10

327489

121481

Tabla 12

En la siguiente página se muestran todos los resultados obtenidos:

9.4.1 Sifting

9.4.1.1 Orden de variables en número de vértices descendente

Benchmark using Sifting algorithm					
<i>File</i>	<i>Nvars</i>	<i>InitSize</i>	<i>ReducSize</i>	<i>Nswaps</i>	<i>Time (s)</i>
huge.cnf	32	1099	444	1918	0.3487
anomaly.cnf	17	84	54	539	0.0190
quinn.cnf	16	18	18	480	0.0065
ais12.cnf	12	29	25	250	0.0068
ais8.cnf	16	34	32	485	0.0112
hanoi4.cnf	44	31519	9152	3568	13.1421
aim-200-2_0-yes1-1.cnf	46	80	35	2188	0.0340
aim-50-2_0-yes1-3.cnf	38	34	34	1984	0.0164
par8-1-c.cnf	19	46	37	685	0.0069
dubois21.cnf	27	40957	97	1385	2.0657
bw_large.c.cnf	36	311	68	2139	0.0420
ais10.cnf	20	34	32	757	0.0066
aim-100-1_6-yes1-3.cnf	47	40	39	2665	0.0250
medium.cnf	20	203	78	707	0.0273
hole6.cnf	21	144	43	843	0.0136
dubois20.cnf	27	40957	97	1385	2.0087
bf0432-007.cnf	30	128	60	1797	0.0203
simple_v3_c2.cnf	3	6	6	12	0.0001
aim-50-1_6-yes1-1.cnf	43	43	43	3280	0.0257
bw_large.d.cnf	30	1195	47	1326	0.1016
bw_large.a.cnf	24	157	47	819	0.0114
ais6.cnf	24	42	42	1104	0.0106
bw_large.b.cnf	25	1409	53	1064	0.0581
aim-50-1_6-yes1-4.cnf	42	42	42	3120	0.0179
dubois22.cnf	27	40957	97	1385	1.9840

Tabla 13

9.4.1.2 Orden de variables inicial

Benchmark using sifting_sameorder algorithm					
File	Nvars	InitSize	ReducSize	Nswaps	Time (s)
huge.cnf	32	1099	321	1903	0.2792
anomaly.cnf	17	84	47	495	0.0137
quinn.cnf	16	18	18	480	0.0043
ais12.cnf	12	29	25	258	0.0035
ais8.cnf	16	34	32	484	0.0069
hanoi4.cnf	44	31519	6589	3536	16.6437
aim-200-2_0-yes1-1.cnf	46	80	35	2084	0.0260
aim-50-2_0-yes1-3.cnf	38	34	34	1984	0.0167
par8-1-c.cnf	19	46	37	683	0.0064
dubois21.cnf	27	40957	101	1025	3.5016
bw_large.c.cnf	36	311	68	2054	0.0334
ais10.cnf	20	34	32	757	0.0065
aim-100-1_6-yes1-3.cnf	47	40	39	2665	0.0202
medium.cnf	20	203	78	674	0.0170
hole6.cnf	21	144	46	753	0.0117
dubois20.cnf	27	40957	101	1025	3.4641
bf0432-007.cnf	30	128	62	1780	0.0209
simple_v3_c2.cnf	3	6	6	12	0.0001
aim-50-1_6-yes1-1.cnf	43	43	43	3280	0.0253
bw_large.d.cnf	30	1195	46	1441	0.1231
bw_large.a.cnf	24	157	44	763	0.0093
ais6.cnf	24	42	42	1104	0.0105
bw_large.b.cnf	25	1409	40	1026	0.0492
aim-50-1_6-yes1-4.cnf	42	42	42	3120	0.1185
dubois22.cnf	27	40957	101	1025	3.3841

Tabla 14

9.4.1.3 Orden de variables aleatorio

Media de 3 ejecuciones con las semillas aleatorias anteriormente indicadas:

Sifting with random variable order (Average)					
File	Nvars	initSize	reducSize	Nswaps	Time
huge.cnf	32	1099	249.00	1847.67	0.2741
anomaly.cnf	17	84	50.33	510.67	0.0135
quinn.cnf	16	18	18.00	480.00	0.0045
ais12.cnf	12	29	25.67	262.33	0.0034
ais8.cnf	16	34	32.00	484.33	0.0071
hanoi4.cnf	44	31519	8096.67	3554.00	13.5872
aim-200-2_0-yes1-1.cnf	46	80	35.00	2123.00	0.0264
aim-50-2_0-yes1-3.cnf	38	34	34.00	1984.00	0.0142
par8-1-c.cnf	19	46	37.00	680.33	0.0064
dubois21.cnf	27	40957	206.33	1230.33	1.4411
bw_large.c.cnf	36	311	90.33	2170.00	0.0406
ais10.cnf	20	34	32.00	757.00	0.0063
aim-100-1_6-yes1-3.cnf	47	40	39.00	2663.67	0.0214
medium.cnf	20	203	77.33	705.33	0.0187
hole6.cnf	21	144	45.67	808.67	0.0121
dubois20.cnf	27	40957	206.33	1230.33	1.4960
bf0432-007.cnf	30	128	62.00	1818.00	0.0224
simple_v3_c2.cnf	3	6	6.00	12.00	0.0001
aim-50-1_6-yes1-1.cnf	43	43	43.00	3280.00	0.0267
bw_large.d.cnf	30	1195	52.67	1143.33	0.0830
bw_large.a.cnf	24	157	49.00	844.67	0.0124
ais6.cnf	24	42	42.00	1104.00	0.0106
bw_large.b.cnf	25	1409	55.33	1053.67	0.0418
aim-50-1_6-yes1-4.cnf	42	42	42.00	3120.00	0.0177
dubois22.cnf	27	40957	206.33	1230.33	1.4670

Tabla 15

9.4.2 Window permutation

9.4.2.1 Tamaño de ventana de 2

File	Window Permutation $k=2$				
	Nvars	InitSize	ReducSize	Nswaps	Time (s)
huge.cnf	32	1099	1079	61	0.0273
anomaly.cnf	17	84	82	31	0.0024
quinn.cnf	16	18	18	28	0.0008
ais12.cnf	12	29	29	20	0.0010
ais8.cnf	16	34	34	28	0.0010
hanoi4.cnf	44	31519	30985	85	0.4897
aim-200-2_0-yes1-1.cnf	46	80	76	41	0.0012
aim-50-2_0-yes1-3.cnf	38	34	34	52	0.0009
par8-1-c.cnf	19	46	45	35	0.0006
dubois21.cnf	27	40957	40957	50	0.4618
bw_large.c.cnf	36	311	307	69	0.0031
ais10.cnf	20	34	34	36	0.0005
aim-100-1_6-yes1-3.cnf	47	40	40	56	0.0011
medium.cnf	20	203	197	37	0.0019
hole6.cnf	21	144	140	39	0.0013
dubois20.cnf	27	40957	40957	50	0.5192
bf0432-007.cnf	30	128	124	57	0.0013
simple_v3_c2.cnf	3	6	6	2	0.0000
aim-50-1_6-yes1-1.cnf	43	43	43	76	0.0013
bw_large.d.cnf	30	1195	1131	57	0.0117
bw_large.a.cnf	24	157	147	37	0.0015
ais6.cnf	24	42	42	44	0.0007
bw_large.b.cnf	25	1409	1361	47	0.0115
aim-50-1_6-yes1-4.cnf	42	42	42	72	0.0010
dubois22.cnf	27	40957	40957	50	0.4618

Tabla 16

9.4.2.2 Tamaño de ventana de 3

<i>File</i>	<i>Window Permutation k=3</i>				
	<i>Nvars</i>	<i>InitSize</i>	<i>ReducSize</i>	<i>Nswaps</i>	<i>Time (s)</i>
huge.cnf	32	1099	1071	176	0.0736
anomaly.cnf	17	84	79	87	0.0053
quinn.cnf	16	18	18	78	0.0019
ais12.cnf	12	29	28	56	0.0018
ais8.cnf	16	34	33	80	0.0024
hanoi4.cnf	44	31519	30467	249	1.3132
aim-200-2_0-yes1-1.cnf	46	80	72	125	0.0027
aim-50-2_0-yes1-3.cnf	38	34	34	154	0.0017
par8-1-c.cnf	19	46	45	100	0.0014
dubois21.cnf	27	40957	32765	146	1.5634
bw_large.c.cnf	36	311	303	200	0.0083
ais10.cnf	20	34	33	104	0.0012
aim-100-1_6-yes1-3.cnf	47	40	39	172	0.0024
medium.cnf	20	203	191	105	0.0049
hole6.cnf	21	144	136	110	0.0030
dubois20.cnf	27	40957	32765	146	1.4369
bf0432-007.cnf	30	128	120	164	0.0034
simple_v3_c2.cnf	3	6	6	0	0.0017
aim-50-1_6-yes1-1.cnf	43	43	43	224	0.0029
bw_large.d.cnf	30	1195	1095	164	0.0316
bw_large.a.cnf	24	157	139	109	0.0041
ais6.cnf	24	42	42	126	0.0017
bw_large.b.cnf	25	1409	1313	134	0.0318
aim-50-1_6-yes1-4.cnf	42	42	42	214	0.0022
dubois22.cnf	27	40957	32765	146	1.4540

Tabla 17

9.4.2.3 Tamaño de ventana de 4

<i>File</i>	<i>Window Permutation k=4</i>				
	<i>Nvars</i>	<i>InitSize</i>	<i>ReducSize</i>	<i>Nswaps</i>	<i>Time (s)</i>
huge.cnf	32	1099	1027	341	0.1169
anomaly.cnf	17	84	78	162	0.0063
quinn.cnf	16	18	18	144	0.0021
ais12.cnf	12	29	27	99	0.0017
ais8.cnf	16	34	33	146	0.0025
hanoi4.cnf	44	31519	29535	485	2.7877
aim-200-2_0-yes1-1.cnf	46	80	68	252	0.0055
aim-50-2_0-yes1-3.cnf	38	34	34	302	0.0037
par8-1-c.cnf	19	46	45	181	0.0045
dubois21.cnf	27	40957	26621	281	2.7812
bw_large.c.cnf	36	311	299	392	0.0177
ais10.cnf	20	34	32	195	0.0027
aim-100-1_6-yes1-3.cnf	47	40	39	339	0.0045
medium.cnf	20	203	188	198	0.0098
hole6.cnf	21	144	134	210	0.0059
dubois20.cnf	27	40957	26621	281	2.7080
bf0432-007.cnf	30	128	116	317	0.0064
simple_v3_c2.cnf	3	6	6	0	0.0017
aim-50-1_6-yes1-1.cnf	43	43	43	438	0.0017
bw_large.d.cnf	30	1195	1059	315	0.0650
bw_large.a.cnf	24	157	123	213	0.0072
ais6.cnf	24	42	42	240	0.0033
bw_large.b.cnf	25	1409	1249	255	0.0651
aim-50-1_6-yes1-4.cnf	42	42	42	420	0.0045
dubois22.cnf	27	40957	26621	281	2.5959

Tabla 18

9.4.2.4 Tamaño de ventana de 5

<i>File</i>	<i>Window Permutation k=5</i>				
	<i>Nvars</i>	<i>InitSize</i>	<i>ReducSize</i>	<i>Nswaps</i>	<i>Time (s)</i>
huge.cnf	32	1099	1025	552	0.1762
anomaly.cnf	17	84	77	250	0.0094
quinn.cnf	16	18	18	220	0.0028
ais12.cnf	12	29	26	144	0.0025
ais8.cnf	16	34	34	220	0.0040
hanoi4.cnf	44	31519	28527	787	5.1653
aim-200-2_0-yes1-1.cnf	46	80	62	411	0.0095
aim-50-2_0-yes1-3.cnf	38	34	34	492	0.0062
par8-1-c.cnf	19	46	45	281	0.0047
dubois21.cnf	27	40957	19453	447	3.9210
bw_large.c.cnf	36	311	291	631	0.0276
ais10.cnf	20	34	32	303	0.0037
aim-100-1_6-yes1-3.cnf	47	40	39	549	0.0072
medium.cnf	20	203	184	312	0.0151
hole6.cnf	21	144	132	324	0.0095
dubois20.cnf	27	40957	19453	447	4.2917
bf0432-007.cnf	30	128	110	508	0.0112
simple_v3_c2.cnf	3	6	6	0	0.0018
aim-50-1_6-yes1-1.cnf	43	43	43	712	0.0096
bw_large.d.cnf	30	1195	1021	511	0.1055
bw_large.a.cnf	24	157	115	350	0.0113
ais6.cnf	24	42	42	380	0.0052
bw_large.b.cnf	25	1409	1169	407	0.0995
aim-50-1_6-yes1-4.cnf	42	42	42	684	0.0063
dubois22.cnf	27	40957	19453	447	4.5412

Tabla 19

9.4.3 Intercambios aleatorios

A continuación se presenta la media de las 3 ejecuciones de 100 iteraciones en las que se intercambian variables de orden de forma aleatoria:

<i>File</i>	<i>Random Swapper (Average)</i>				<i>Time</i>
	<i>Nvars</i>	<i>initSize</i>	<i>reducSize</i>	<i>Nswaps</i>	
huge.cnf	32	1099	1057.67	122.67	0.074
anomaly.cnf	17	84	80.00	115.00	0.009
quinn.cnf	16	18	18.00	119.33	0.003
ais12.cnf	12	29	26.33	104.33	0.004
ais8.cnf	16	34	33.67	121.00	0.006
hanoi4.cnf	44	31519	31165.00	135.33	0.836
aim-200-2_0-yes1-1.cnf	46	80	72.00	54.33	0.001
aim-50-2_0-yes1-3.cnf	38	34	34.00	94.67	0.001
par8-1-c.cnf	19	46	43.33	127.33	0.002
dubois21.cnf	27	40957	33782.33	125.67	1.184
bw_large.c.cnf	36	311	301.33	118.00	0.005
ais10.cnf	20	34	34.00	120.67	0.001
aim-100-1_6-yes1-3.cnf	47	40	39.67	92.67	0.001
medium.cnf	20	203	166.33	108.67	0.005
hole6.cnf	21	144	126.00	109.00	0.003
dubois20.cnf	27	40957	33782.33	125.67	1.164
bf0432-007.cnf	30	128	113.33	122.33	0.002
simple_v3_c2.cnf	3	6	6.00	69.33	0.001
aim-50-1_6-yes1-1.cnf	43	43	43.00	126.67	0.001
bw_large.d.cnf	30	1195	1061.33	116.33	0.022
bw_large.a.cnf	24	157	132.00	96.00	0.003
ais6.cnf	24	42	42.00	124.67	0.002
bw_large.b.cnf	25	1409	945.67	101.00	0.021
aim-50-1_6-yes1-4.cnf	42	42	42.00	120.00	0.001
dubois22.cnf	27	40957	33782.33	125.67	1.202

Tabla 20

9.4.4 Algoritmo genético

Media de tres ejecuciones de 10 iteraciones, con una población de 8 cromosomas, un porcentaje de selección del 20% y una probabilidad de mutación de 0,1:

<i>File</i>	<i>Genetic Algorithm (Avg.)</i>				
	<i>Nvars</i>	<i>InitSize</i>	<i>ReducSize</i>	<i>Nswaps</i>	<i>Time (s)</i>
huge.cnf	32	1099	950.33	6067.00	35.7175
anomaly.cnf	17	84	70.67	1551.00	0.1124
quinn.cnf	16	18	18.00	1387.33	0.0233
ais12.cnf	12	29	28.00	761.33	0.0134
ais8.cnf	16	34	34.00	0.00	0.0009
hanoi4.cnf	44	31519	31519.00	0.00	0.0000
aim-200-2_0-yes1-1.cnf	46	80	70.33	6251.00	1.9144
aim-50-2_0-yes1-3.cnf	38	34	34.00	6038.67	1.2038
par8-1-c.cnf	19	46	46.00	1917.33	0.1238
dubois21.cnf	27	40957	40957.00	0.00	0.0000
bw_large.c.cnf	36	311	159.00	7260.33	1.8114
ais10.cnf	20	34	34.00	2082.00	0.0753
aim-100-1_6-yes1-3.cnf	47	40	40.00	7436.67	7.0141
medium.cnf	20	203	203.00	0.00	0.0000
hole6.cnf	21	144	103.00	2435.33	0.2585
dubois20.cnf	27	40957	16241.00	0.00	0.0001
bf0432-007.cnf	30	128	128.00	5384.67	4.0595
simple_v3_c2.cnf	3	6	6.00	10.67	0.0003
aim-50-1_6-yes1-1.cnf	43	43	43.00	9574.00	4.5974
bw_large.d.cnf	30	1195	1195.00	0.00	0.0001
bw_large.a.cnf	24	157	96.00	2805.67	0.1379
ais6.cnf	24	42	42.00	239.00	0.3381
bw_large.b.cnf	25	1409	170.00	3537.00	1.5405
aim-50-1_6-yes1-4.cnf	42	42	42.00	9074.00	6.7386
dubois22.cnf	27	40957	40957.00	0.00	0.0001

Tabla 21

En primer lugar, hemos de notar que varios ficheros de datos no han podido ser completados. Estos ficheros son los que tienen un fondo gris, de ahí que marquen un número de intercambios y un tiempo de ejecución igual a 0 y que indiquen un tamaño de reducción igual al tamaño inicial del árbol.

Este fenómeno de no poder reducir algunos ejemplos se debe a que como en distintas operaciones del algoritmo genético obtenemos órdenes muy diversos, puede que el árbol asociado sea tan grande que no nos quepa en memoria principal.

9.4.5 Algoritmo memético

Media de tres ejecuciones de 10 iteraciones, con una población de 8 cromosomas, un porcentaje de selección del 20% y una probabilidad de mutación de 0.1. Se usa como proceso heurístico de mejora el algoritmo *Sifting*:

File	Memetic Algorithm (Avg.)				
	Nvars	InitSize	ReducSize	Nswaps	Time (s)
huge.cnf	32	1099	187.67	20936.67	23.8565
anomaly.cnf	17	84	47.33	5723.33	0.1303
quinn.cnf	16	18	18.00	5284.00	0.0560
ais12.cnf	12	29	20.00	2884.00	0.0297
ais8.cnf	16	34	29.00	5207.00	0.2096
hanoi4.cnf	44	31519	31519.00	0.00	0.0000
aim-200-2_0-yes1-1.cnf	46	80	35.00	23502.00	4.3155
aim-50-2_0-yes1-3.cnf	38	34	34.00	21910.67	8.9621
par8-1-c.cnf	19	46	37.00	7141.67	0.2512
dubois21.cnf	27	40957	40957.00	0.00	0.0000
bw_large,c.cnf	36	311	51.00	24416.00	1.0941
ais10.cnf	20	34	32.00	7766.33	0.1990
aim-100-1_6-yes1-3.cnf	47	40	39.00	29257.00	52.7974
medium.cnf	20	203	67.67	7961.33	0.3423
hole6.cnf	21	144	34.00	9032.33	0.2694
dubois20.cnf	27	40957	93.67	14802.33	58.5887
bf0432-007.cnf	30	128	48.33	19639.00	3.8528
simple_v3_c2.cnf	3	6	6.00	108.00	0.0011
aim-50-1_6-yes1-1.cnf	43	43	43.00	36090.00	44.5990
bw_large,d.cnf	30	1195	47.00	13591.67	0.6144
bw_large,a.cnf	24	157	45.67	9295.00	0.1923
ais6.cnf	24	42	42.00	11730.00	2.4013
bw_large,b.cnf	25	1409	47.00	12696.00	0.8040
aim-50-1_6-yes1-4.cnf	42	42	42.00	34034.00	48.2101
dubois22.cnf	27	40957	93.67	12547.67	26.8965

Tabla 22

Al igual que ocurre en el algoritmo genético, en estos resultados vemos como los ficheros de datos hanoi4.cnf, y el fichero dubois21.cnf no dan solución. Esto se debe a las restricciones de memoria a las que hemos sometido el algoritmo, evitando que pueda consumir toda la memoria del sistema.

9.4.6 Algoritmo Iterative Sifting

El algoritmo desarrollado por nosotros basado en el de Ruddell, se comporta de forma extraordinaria, mejorando los resultados obtenidos por éste. Establecemos un número pequeño de iteraciones 10:

Benchmark using Iterative Sifting algorithm (iterations = 10)					
<i>File</i>	<i>Nvars</i>	<i>InitSize</i>	<i>ReducSize</i>	<i>Nswaps</i>	<i>Time (s)</i>
huge.cnf	32	1099	191	39571	2.4820
anomaly.cnf	17	84	46	10852	0.1616
quinn.cnf	16	18	18	4800	0.0252
ais12.cnf	12	29	25	5266	0.0422
ais8.cnf	16	34	32	9605	0.0932
hanoi4.cnf	44	31519	558	75264	51.5871
aim-200-2_0-yes1-1.cnf	46	80	35	42316	0.3340
aim-50-2_0-yes1-3.cnf	38	34	34	19840	0.1305
par8-1-c.cnf	19	46	37	13681	0.1236
dubois21.cnf	27	40957	55	41829	12.5471
bw_large.c.cnf	36	311	68	44471	0.5104
ais10.cnf	20	34	32	15197	0.1207
aim-100-1_6-yes1-3.cnf	47	40	39	53281	0.3763
medium.cnf	20	203	66	15142	0.3164
hole6.cnf	21	144	34	16812	0.1345
dubois20.cnf	27	40957	55	41829	12.4465
bf0432-007.cnf	30	128	60	34781	0.3255
simple_v3_c2.cnf	3	6	6	120	0.0009
aim-50-1_6-yes1-1.cnf	43	43	43	32800	0.2591
bw_large.d.cnf	30	1195	47	25266	1.1519
bw_large.a.cnf	24	157	44	16770	0.2249
ais6.cnf	24	42	42	11040	0.1117
bw_large.b.cnf	25	1409	52	23403	0.4155
aim-50-1_6-yes1-4.cnf	42	42	42	31200	0.1933
dubois22.cnf	27	40957	55	41829	12.6035

Tabla 23

9.5 Discusión de los resultados

Si comparamos todos los algoritmos para cada fichero, obtenemos las siguientes reducciones⁵:

File	Size obtained in each reduction process										RandSwapper	Genetic	Memetic	Isifting
	Nvars	InitSize	Sifting	Sifting (s. o.)	Sifting (r. o.)	WP _{K=2}	WP _{K=3}	WP _{K=4}	WP _{K=5}					
huge.cnf	32	1099	444	321	249.00	1079	1071	1027	1025	1057.67	950.33	187.67	191	
anomaly.cnf	17	84	54	47	50.33	82	79	78	77	80.00	70.67	47.33	46	
quinn.cnf	16	18	18	18	18.00	18	18	18	18	18.00	18.00	18.00	18	
ais12.cnf	12	29	25	25	25.67	29	28	27	26	26.33	28.00	20.00	25	
ais8.cnf	16	34	32	32	32.00	34	33	33	34	33.67	34.00	29.00	32	
hanoi4.cnf	44	31519	9152	6589	8096.67	30985	30467	29535	28527	31165.00	31519.00	31519.00	558	
aim-200-2_0-yes1-1.cnf	46	80	35	35	35.00	76	72	68	62	72.00	70.33	35.00	35	
aim-50-2_0-yes1-3.cnf	38	34	34	34	34.00	34	34	34	34	34.00	34.00	34.00	34	
par8-1-c.cnf	19	46	37	37	37.00	45	45	45	45	43.33	46.00	37.00	37	
dubois21.cnf	27	40957	97	101	206.33	40957	32765	26621	19453	33782.33	40957.00	40957.00	55	
bw_large.c.cnf	36	311	68	68	90.33	307	303	299	291	301.33	159.00	51.00	68	
ais10.cnf	20	34	32	32	32.00	34	33	32	32	34.00	34.00	32.00	32	
aim-100-1_6-yes1-3.cnf	47	40	39	39	39.00	40	39	39	39	39.67	40.00	39.00	39	
medium.cnf	20	203	78	78	77.33	197	191	188	184	166.33	203.00	67.67	66	
hole6.cnf	21	144	43	46	45.67	140	136	134	132	126.00	103.00	34.00	34	
dubois20.cnf	27	40957	97	101	206.33	40957	32765	26621	19453	33782.33	16241.00	93.67	55	
bf0432-007.cnf	30	128	60	62	62.00	124	120	116	110	113.33	128.00	48.33	60	
simple_v3_c2.cnf	3	6	6	6	6.00	6	6	6	6	6.00	6.00	6.00	6	
aim-50-1_6-yes1-1.cnf	43	43	43	43	43.00	43	43	43	43	43.00	43.00	43.00	43	
bw_large.d.cnf	30	1195	47	46	52.67	1131	1095	1059	1021	1061.33	1195.00	47.00	47	
bw_large.a.cnf	24	157	47	44	49.00	147	139	123	115	132.00	96.00	45.67	44	
ais6.cnf	24	42	42	42	42.00	42	42	42	42	42.00	42.00	42.00	42	
bw_large.b.cnf	25	1409	53	40	55.33	1361	1313	1249	1169	945.67	170.00	47.00	52	
aim-50-1_6-yes1-4.cnf	42	42	42	42	42.00	42	42	42	42	42.00	42.00	42.00	42	
dubois22.cnf	27	40957	97	101	206.33	40957	32765	26621	19453	33782.33	40957.00	93.67	55	
Avg	27.44	6382.72	428.88	321.16	393.32	6354.68	5345.76	###	3657.32	5477.19	5327.45	2944.64	68.64	

Tabla 24

La media nos puede servir para ver cuáles son los algoritmos que mejor se comportan en todos los casos de forma global. Viendo la tendencia de ciertos algoritmos a no reducir mucho el árbol independientemente del conjunto de datos tomado.

Para poder verlo más claro, hemos calculado los porcentajes de reducción del árbol para cada fichero de prueba:

⁵ (s.o.) indica que es el algoritmo de *Sifting* con las variables en el orden dado por el fichero y (r. o.) indica que es el algoritmo *Sifting* en el que se toman las variables de forma aleatoria. WP $K=X$ es el algoritmo de la permutación en ventana con un tamaño de ventana igual a X . *RandSwapper* es el algoritmo de intercambio de variables de forma aleatoria.

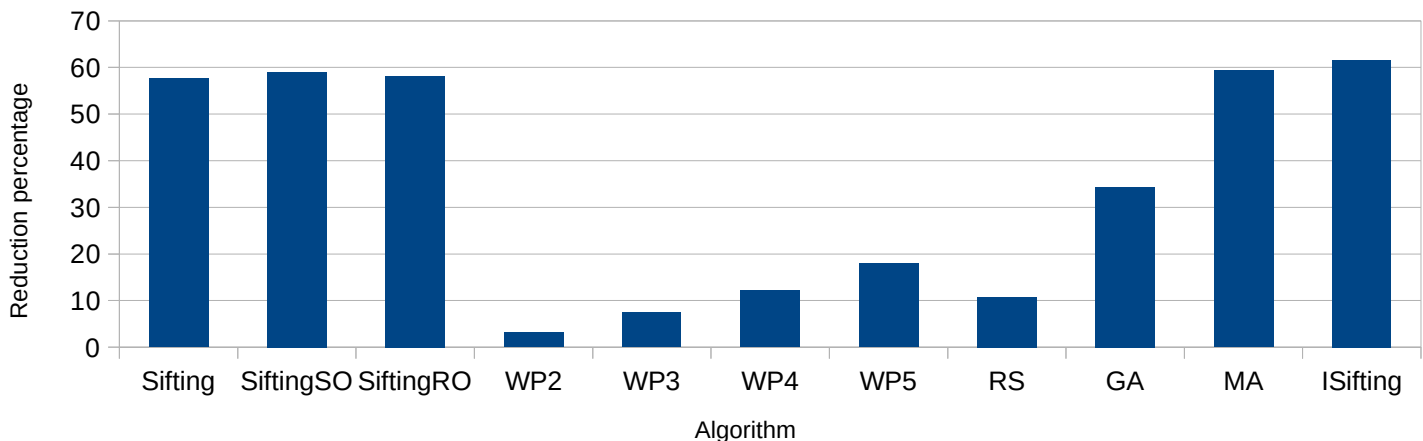
File	Percentage of reduction obtained in each reduction process												
	Nvars	InitSize	Sifting	Sifting (s. o.)	Sifting (r. o.)	WP _{K=2}	WP _{K=3}	WP _{K=4}	WP _{K=5}	RandSwapper	Genetic	Memetic	Isifting
huge.cnf	32	1099	59.60	70.79	77.34	1.82	2.55	6.55	6.73	3.76	13.53	82.92	82.62
anomaly.cnf	17	84	35.71	44.05	40.08	2.38	5.95	7.14	8.33	4.76	15.87	43.65	45.24
quinn.cnf	16	18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ais12.cnf	12	29	13.79	13.79	11.49	0.00	3.45	6.90	10.34	9.20	3.45	31.03	13.79
ais8.cnf	16	34	5.88	5.88	5.88	0.00	2.94	2.94	0.00	0.98	0.00	14.71	5.88
hanoi4.cnf	44	31519	70.96	79.10	74.31	1.69	3.34	6.29	9.49	1.12	0.00	0.00	98.23
aim-200-2_0-yes1-1.cnf	46	80	56.25	56.25	56.25	5.00	10.00	15.00	22.50	10.00	12.08	56.25	56.25
aim-50-2_0-yes1-3.cnf	38	34	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
par8-1-c.cnf	19	46	19.57	19.57	19.57	2.17	2.17	2.17	2.17	5.80	0.00	19.57	19.57
dubois21.cnf	27	40957	99.76	99.75	99.50	0.00	20.00	35.00	52.50	17.52	0.00	0.00	99.87
bw_large.c.cnf	36	311	78.14	78.14	70.95	1.29	2.57	3.86	6.43	3.11	48.87	83.60	78.14
ais10.cnf	20	34	5.88	5.88	5.88	0.00	2.94	5.88	5.88	0.00	0.00	5.88	5.88
aim-100-1_6-yes1-3.cnf	47	40	2.50	2.50	2.50	0.00	2.50	2.50	2.50	0.83	0.00	2.50	2.50
medium.cnf	20	203	61.58	61.58	61.90	2.96	5.91	7.39	9.36	18.06	0.00	66.67	67.49
hole6.cnf	21	144	70.14	68.06	68.29	2.78	5.56	6.94	8.33	12.50	28.47	76.39	76.39
dubois20.cnf	27	40957	99.76	99.75	99.50	0.00	20.00	35.00	52.50	17.52	60.35	99.77	99.87
bf0432-007.cnf	30	128	53.13	51.56	51.56	3.13	6.25	9.38	14.06	11.46	0.00	62.24	53.13
simple_v3_c2.cnf	3	6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
aim-50-1_6-yes1-1.cnf	43	43	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
bw_large.d.cnf	30	1195	96.07	96.15	95.59	5.36	8.37	11.38	14.56	11.19	0.00	96.07	96.07
bw_large.a.cnf	24	157	70.06	71.97	68.79	6.37	11.46	21.66	26.75	15.92	38.85	70.91	71.97
ais6.cnf	24	42	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
bw_large.b.cnf	25	1409	96.24	97.16	96.07	3.41	6.81	11.36	17.03	32.88	87.93	96.66	96.31
aim-50-1_6-yes1-4.cnf	42	42	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
dubois22.cnf	27	40957	99.76	99.75	99.50	0.00	20.00	35.00	52.50	17.52	0.00	99.77	99.87
Avg	27.44	6382.72	43.79	44.87	44.20	1.53	5.71	9.29	12.88	7.77	12.38	40.34	46.76
Avg _{val(xi) > 0}	27.44	6382.72	57.62	59.04	58.16	3.20	7.51	12.23	17.89	10.78	34.38	59.33	61.53
s			38.28	38.78	38.48	1.91	6.12	10.79	16.25	8.38	22.67	38.74	40.29
s _{val(xi) > 0}			34.55	34.73	34.63	1.59	6.15	11.12	17.13	8.29	27.47	33.88	36.00

Tabla 25

A continuación, incluimos un gráfico a modo de resumen de los porcentajes de reducción:

Average Reduction

For reduction percentages greater than zero

**Fig. 21**

Cada barra del gráfico es cada uno de los algoritmos desarrollados para esta memoria, incluyendo el algoritmo *Iterative Sifting* original por nuestra parte.

El algoritmo de Rudell se comporta relativamente bien, logrando porcentajes de reducción superiores al 50%. Es importante notar que no hay gran diferencia entre tomar un orden inicial de variables determinado u otro. Básicamente, las tres versiones del algoritmo superan ampliamente los porcentajes de reducción del 50%. Esto es consecuente con lo indicado por el autor en [RUD93].

Siguiendo con el gráfico, los algoritmos de permutación en ventana comienzan a comportarse medianamente bien a partir de valores elevados del tamaño de ventana, pero tal y como indica Rudell en su trabajo [RUD93], son superados ampliamente por su algoritmo.

Por otro lado, en el campo de los algoritmos evolutivos, si bien ofrecen resultados admisibles, nos llevamos una decepción debido a los limitados resultados obtenidos. Esto se debe a, sobre todo, a su tendencia a consumir demasiada memoria, es decir, si se generan durante el proceso evolutivo cromosomas que representa a órdenes muy malos, al intentar evaluar el tamaño, nos quedaremos sin memoria. Si hubiéramos podido tener algún tipo de heurística sobre los órdenes que nos indicase que un orden es mejor que otro sin generar el árbol, podríamos haber obtenido mejores resultados. En nuestros experimentos nos hemos visto muy limitados por este detalle y no hemos podido ejecutar más que unas pocas iteraciones estos algoritmos, y aun así, algunos ficheros han hecho fracasar este método al producirse un desbordamiento de memoria principal.

Además, para estos algoritmos el hecho de tener que construir el árbol cada vez que quisiéramos evaluar un orden ha hecho que fueran mucho más lentos, que los puramente heurísticos. Intentamos solventar este hecho usando una caché de evaluaciones, de forma que nunca un orden se calculase dos veces, pero para fórmulas con valores altos de fórmulas, esto era insuficiente.

Por último, destaca nuestra propuesta de solución, el algoritmo *Iterative Sifting* que, da una mejora sobre el algoritmo de Rudell considerable. Esto se debe a que el proceso en cada iteración vuelve a rehacer el orden, por lo que no es un algoritmo voraz simplemente, ya que puede volver a tomar varias veces la misma variable en distintas iteraciones.

Si comparamos nuestra propuesta con el algoritmo de Rudell:

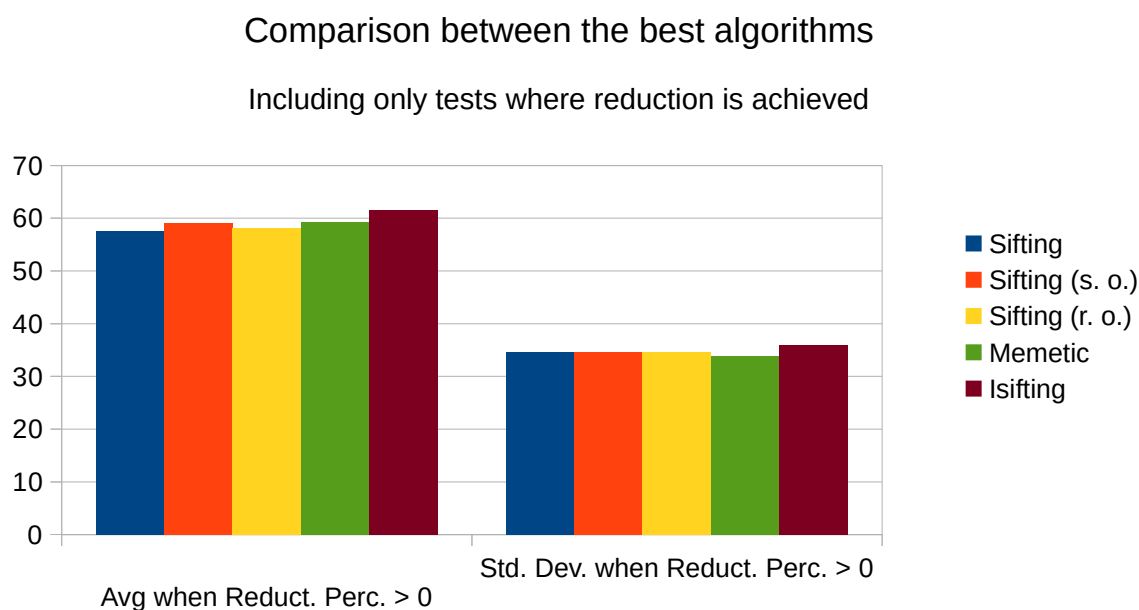


Fig. 22

Vemos como nuestro algoritmo sobrepasa por poco el 60% de reducción, logrando una mejora de casi un 5% sobre el algoritmo de Rudell.

Notemos que para estas gráficas sólo hemos considerado la media (y desviación) de aquellos ficheros en los que se generaban reducción. Algunos de nuestros ejemplos no generaban reducción, bien por ser ejemplos demasiado sencillos y servir sólo a modo de demostración o por carencias de los algoritmos. En esta tabla se resumen la media de las reducciones del *Sifting*, del algoritmo memético y de nuestro algoritmo.

Algorithm	<i>Sifting</i>	<i>Sifting (s. o.)</i>	<i>Sifting (r. o.)</i>	<i>Memetic</i>	<i>Isifting</i>
Avg	43.79	44.87	44.20	40.34	46.76
Avg when Reduct. Perc. > 0	57.62	59.04	58.16	59.33	61.53
Std. Dev	38.28	38.78	38.48	38.74	40.29
Std. Dev. when Reduct. Perc. > 0	34.55	34.73	34.63	33.88	36.00

Tabla 26

El algoritmo memético tiene unos buenos resultados, pero no debido a que explore el espacio de búsqueda mucho, sino a que usa el algoritmo de Rudell como heurística, y eso le da una buena base. Estamos seguros de que una exploración mayor del espacio de búsqueda hubiera dado lugar a mayor número de soluciones que hubieran generado órdenes de variables tan ineficientes que se hubiera desbordado la memoria.

El resto de algoritmos no genera reducciones significativas, salvo el algoritmo genético, pero

muy lejos de los valores obtenidos por el resto por los motivos antes comentados, si explora demasiado se queda sin memoria, y si explora poco, obtiene soluciones muy limitadas.

Algorithm	$WP_{K=2}$	$WP_{K=3}$	$WP_{K=4}$	$WP_{K=5}$	<i>RandSwapper</i>	<i>Genetic</i>
Avg	1.53	5.71	9.29	12.88	7.77	12.38
Avg when Reduct. Perc. > 0	3.20	7.51	12.23	17.89	10.78	34.38
Std. Dev	1.91	6.12	10.79	16.25	8.38	22.67
Std. Dev. when Reduct. Perc. > 0	1.59	6.15	11.12	17.13	8.29	27.47

Tabla 27

En definitiva, el algoritmo *Iterative Sifting* soluciona los problemas tanto del algoritmo *Sifting* como los de los genéticos. En primer lugar, carece del gran problema del desbordamiento de la memoria principal que era un problema que plagaba cualquier que explore el espacio de búsqueda sin un control, como son los algoritmos evolutivos clásicos implementados para este problema de optimización de tamaños del árbol BDD. En segundo lugar es capaz de explotar más las soluciones, ofreciendo una mejora de un 5% en los experimentos ejecutados.

Por último, mostramos todos los resultados de reducciones de tamaños de árboles en la siguiente página:

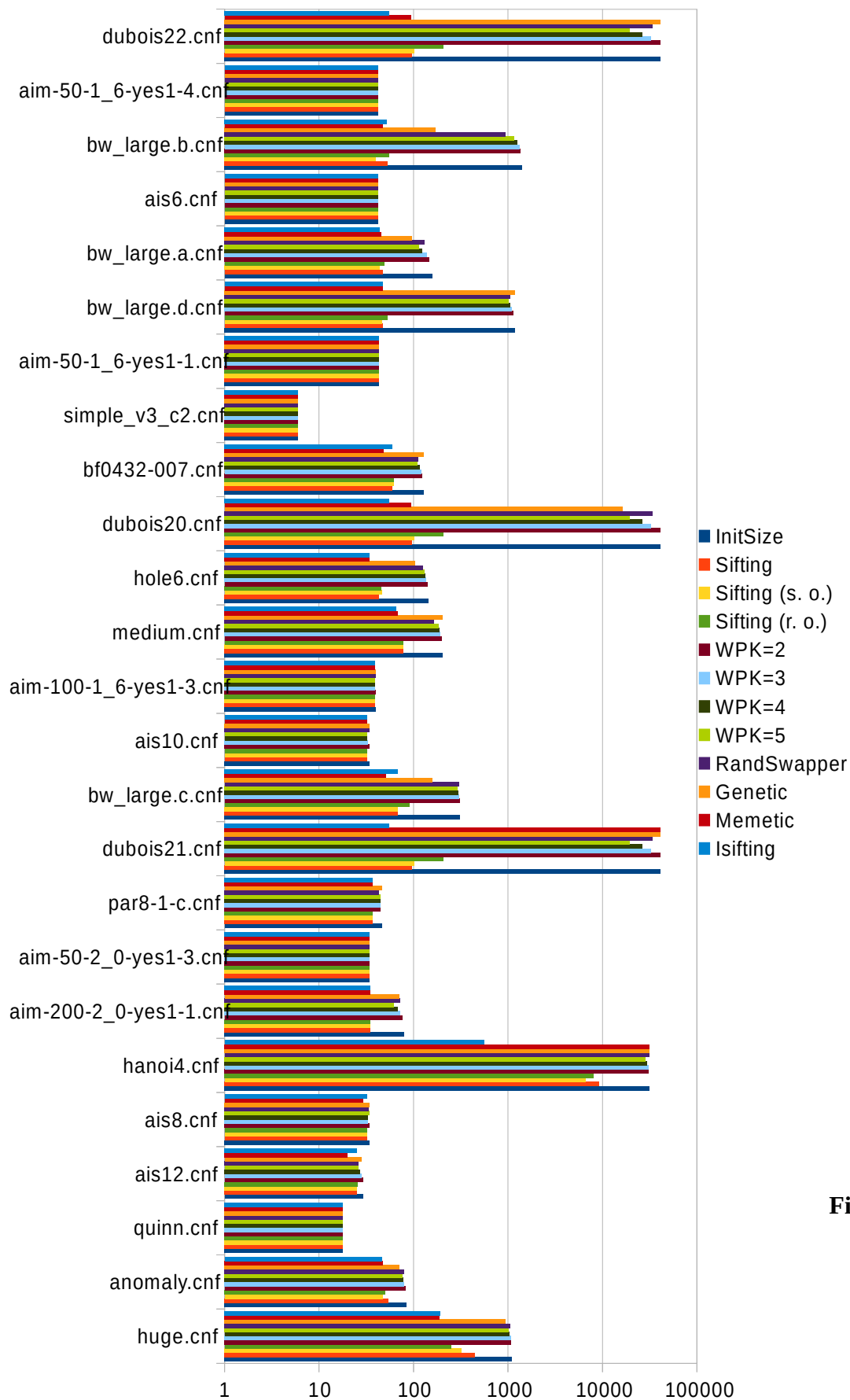


Fig. 23

10 Arquitectura de la solución software

En esta sección se muestra la arquitectura de la solución software que permite controlar si un software externo está en un estado consistente o no.

10.1 Objetivo

Recordemos que el objetivo de este sistema es el de permitir comprobar de forma sencilla y eficiente si un estado de un sistema es consistente. Es decir, si el estado en el que se encuentra ahora mismo el sistema es legal dentro de los sistemas definidos por el ingeniero, cada uno con sus estados bien diferenciados.

10.2 Entidades

Las entidades que tiene este sistema son las siguientes:

10.2.1.1 BDD

Árbol binario de decisión que contendrá la expresión lógica que recoja los estados posibles del sistema. Además de sólo almacenar la fórmula lógica, optimizará la evaluación de la expresión, usando el mejor método de reducción, desarrollado de forma original aquí y mostrado anteriormente en esta misma memoria.

10.2.1.2 Asserter

Es la clase que contiene la lógica de comprobación de la consistencia. Por eso, contiene las definiciones de las variables lógicas que describen al sistema.

Obviamente, esta clase es la encargada de gestionar el árbol binario de decisión y realizar las llamadas al objeto que pueda obtener una instantánea con los valores de verdad del sistema.

10.2.1.3 Sistema

El sistema cuya consistencia vamos a comprobar. Aquí lo mostraremos implementado como una clase, pero obviamente se tratará de una fachada, ya que el sistema puede ser tan complejo como se necesite.

10.2.1.4 Motor lógico

Puede ser el mismo sistema, pero según la complejidad de éste, nos interesará tener un observador que sea capaz de obtener la información de en qué estado se encuentra el sistema. La forma de comunicarla al Asserter es implementando métodos públicos que devuelvan valores booleanos cuyo nombre sea igual a las variables definidas

10.3 Relaciones

En el siguiente gráfico se puede ver un diagrama somero de clases en las que se muestran las relaciones entre las distintas clases.

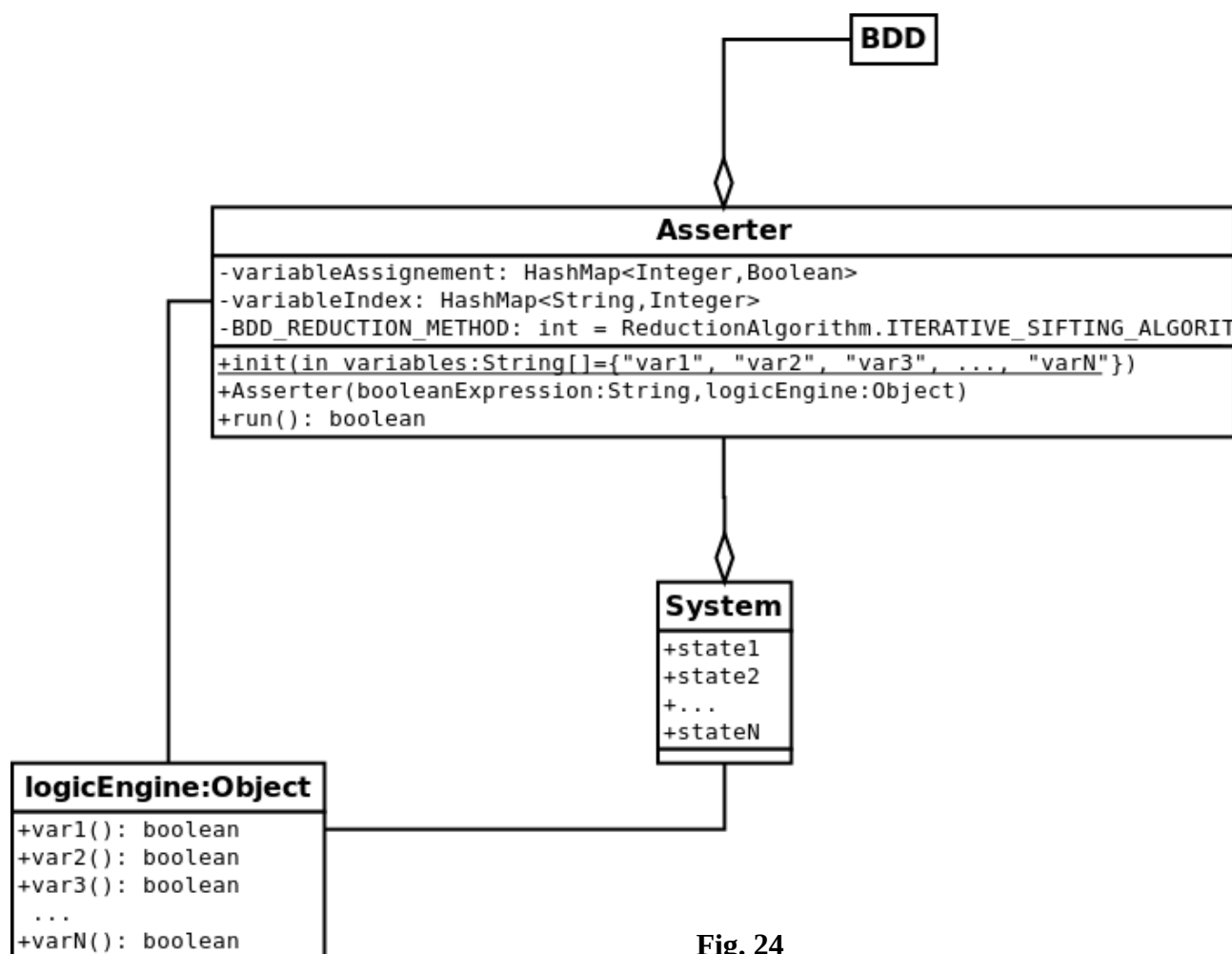


Fig. 24

Se puede ver como la clase **Asserter** es el núcleo de nuestro sistema, conteniendo el árbol binario de decisión y teniendo acceso al consultor de estados del sistema.

Por otro lado, el sistema se muestra como una máquina de estados, a la que puede acceder el motor lógico. El consultor lógico deberá convertir los estados del sistema a proposiciones lógicas que pueda comprender el comprobador de consistencia.

10.4 Funcionamiento

Inicialmente se ha de construir el comprobador de consistencia a partir de una expresión lógica y del objeto que tenga como responsabilidad ofrecer los valores de verdad de cada una de las variables que aparezcan en dicha expresión.

El motor deberá tener cada variable implementada como un método público. Suponemos que este motor lógico deberá acceder a estados internos del sistema, realizar comprobaciones y lo más importante, traducir de forma fidedigna los estados de la máquina de estados que es el sistema en variables lógicas.

Por último, se deberá introducir la llamada al método `run` protegiendo las zonas de código que deban cumplir las restricciones propias determinadas por el sistema. Este método llamará a la operación `restrict` del BDD con la asignación de valores de verdad obtenida en el instante de la llamada. Una vez que se haya restringido con la asignación realizada, sólo quedará ver si el árbol resultante es el vértice `TRUE` o el vértice `FALSE`. Si es el primero, eso indicará que la asignación de valores de verdad es consistente, por lo que el estado es correcto y se podrá seguir con la ejecución normal en el sistema. En cambio, si el BDD se convierte en el vértice constante `FALSE`, tendremos que recuperar el sistema a un estado consistente para poder proseguir la ejecución del mismo.

10.5 Ejemplos

En la librería `DJBDD` se han incluido varios ejemplos. Hay un ejemplo de un ascensor, y otro un segundo de un recomendador de cuándo realizar ejercicio para pacientes diabéticos tipo 1. El primero es muy sencillo y sirve como estudio y aprendizaje, en cambio, en el segundo se puede comprobar la gran funcionalidad de este sistema.

10.5.1 Ascensor

10.5.1.1 Introducción

Este primer ejemplo es un caso sencillo de un ascensor en un bloque de pisos con dos plantas. El comprobador de consistencia tiene como objetivo que el ascensor no pueda realizar una acción ilegal como intentar de bajar estando ya en la planta baja, o intentar subir estando en la primera planta.

10.5.1.2 Magnitudes

Supongamos un ascensor en un edificio de dos plantas con los siguientes posibles estados:

- Planta: planta baja, primera planta.
- Estado: parado, subiendo o bajando.

Que transformaremos en las siguientes variables en el motor de consulta:

- `isGround`: está en planta baja.
- `isFirstFloor`: está en la primera planta.
- `isStopped`: el ascensor está parado.
- `isGoingUp`: el ascensor está subiendo (de la planta baja a la primera planta).
- `isGoingDown`: el ascensor está bajando (de la primera planta a la planta baja).

10.5.1.3 Expresión lógica

Se pueden ver algunas relaciones claras entre ellas, pero nosotros vamos a usar la siguiente expresión lógica que será la que deberá mantenerse constantemente para que el sistema funcione correctamente:

```
((isGoingUp AND isGround) OR (isGoingDown AND isFirstFloor) OR (isGround AND isStopped) OR (isFirstFloor AND isStopped)) AND ((isGround AND !isFirstFloor) OR (!isGround AND isFirstFloor))
```

10.5.1.4 Funcionamiento

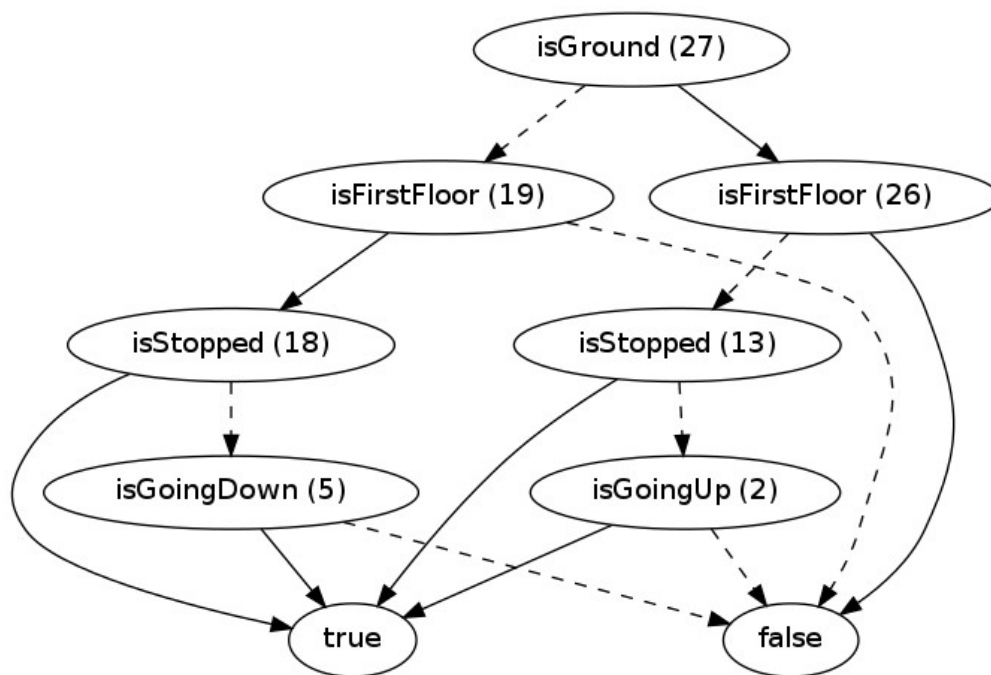


Fig. 25

El sistema de comprobación de la consistencia construye un árbol BDD con esa expresión, e inmediatamente le aplica un algoritmo de reducción para tratar de mantener en memoria la estructura de menor tamaño posible, obteniendo el siguiente árbol:

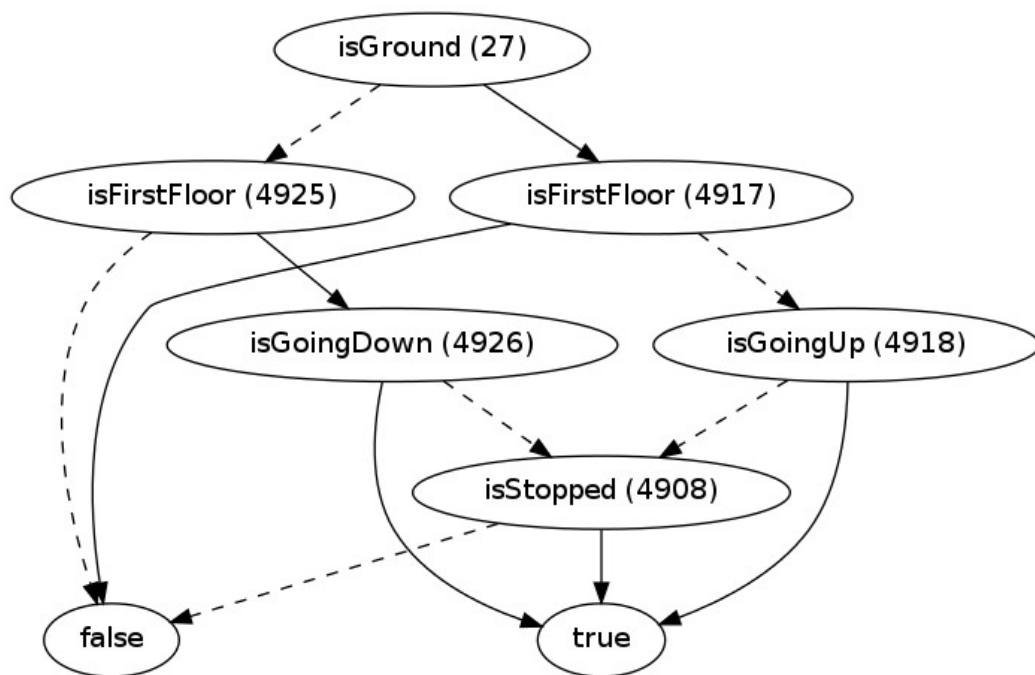


Fig. 26

A partir de este momento, en cada transición del sistema, que en nuestro caso será movimiento de subida o bajada del ascensor, las variables cambiarán pero siempre se deberá respetar la consistencia. Para ello, definimos dos operaciones up y down que estarán protegidas por una ejecución del comprobador de consistencia.

Nótese que las variables se implementan como métodos en la misma clase Elevator, que será, además del propio sistema, la clase observador que nos permita obtener los valores de cada una de las variables.

10.5.2 Control glucémico

10.5.2.1 Introducción

Un medidor continuo de glucosa es un aparato que recoge los datos de un sensor subcutáneo que realiza mediciones de la glucosa en sangre. La glucosa en sangre ha de encontrarse entre 80 mg/dl y 180 mg/dl. Valores superiores a 180mg/dl de forma continuada dañan los tejidos y los órganos provocando neuropatías y otras dolencias. En cambio, valores inferiores a 80 mg/dl causan hipoglucemia, y si persiste ese valor bajo o baja más el paciente puede llegar a perder el conocimiento.

En enfermedades como la diabetes tipo I un buen control de los niveles de glucosa puede suponer la diferencia entre múltiples complicaciones (neuropatías, nefropatías, etc...) y evitar las hipoglucemias, que de forma fulminante pueden provocar la muerte.

Para controlar los niveles de glucosa en sangre, los pacientes diabéticos (tipo 1) se inyectan insulina en su cuerpo. La insulina es una hormona que permite a las células captar glucosa del torrente sanguíneo.

El ejercicio actúan favoreciendo la acción de la insulina. Es importante destacar sólo se ha de hacer ejercicio con niveles suficientemente altos de glucosa (para evitar la hipoglucemia), pero tampoco muy altos porque entonces el paciente podría entrar en cetoacidosis.

El objetivo de este sistema es comprobar si la acción que va a realizar el usuario se ajusta a lo realmente ha de hacer desde el punto de vista médico. Nótese que este es un sistema de ejemplo y las reglas que se han incluido son sólo algunas de las que han de seguir los pacientes y no se aconseja ni se aprueba el uso de este ejemplo como asistente de pacientes.

10.5.2.2 Magnitudes

Hay muchas magnitudes que interactúan con el nivel de la glucosa, nosotros nos centraremos en dos: el propio nivel de glucosa y el ejercicio.

- Nivel de glucosa
 - Nivel de glucosa < 70: hipoglucemia. El paciente ha de comer para elevar su nivel de glucosa en sangre. Variable: GL (GlucoseLow).
 - [70, 180]: nivel correcto. El paciente no ha de realizar una acción de corrección. Variable: GN (GlucoseNormal).
 - (180, 250]: nivel elevado pero sin poliuria. El paciente ha de realizar una pequeña acción de corrección (inyectarse unas pocas unidades de insulina). Variable: GH1 (GlucoseHigh1).
 - [250, 350]: nivel elevado. El paciente ha de realizar una acción correctora media. Variable: GH2 (GlucoseHigh2).
 - (350, 400]: nivel muy elevado. Aumenta la resistencia a la insulina. El paciente ha de realizar una acción correctora alta. Variable: GVH (GlucoseVeryHigh).
 - (400, 600]: nivel peligroso. El paciente ha de inyectarse cuanto antes una cantidad de insulina. El paciente ha de realizar una gran acción correctora. Variable: GTH (GlucoseTooHigh).
- Ejercicio
 - Sin ejercicio: el paciente no hace ejercicio. Variable: EN (ExerciseNone).
 - Leve: 30 minutos andando. Variable: EL (ExerciseLight).
 - Moderado: 30 minutos corriendo. Variable: EM (ExerciseMedium).
 - Duro: 1 hora corriendo. Variable: EH (ExerciseHard).
- Insulina
 - Sin corrección. Variable: INC (InsulinNoCorrection).
 - Corrección leve: (1-3) unidades. Variable: ILC (InsulinLightCorrection).
 - Corrección media: (4-7) unidades. Variable: IMC (InsulinMediumCorrection).
 - Corrección alta > 12. Variable: IHC (InsulinHighCorrection).
- Comer: indica si el paciente ha de suplementar su dieta con un alimento extra en ese momento.

- No Comer: indica que el paciente no come. Variable MN (MealNo).
- Comer un suplemento alimenticio: indica que el paciente come un suplemento. Variable MS (MealSupplement).
- Comida principal del día: indica que el paciente toma el desayuno, almuerzo o cena. Variable M (Meal).

10.5.2.3 Expresión lógica

La expresión lógica que gobierna el sistema es la siguiente de recomendación de ajuste de insulina es la siguiente conjunción de expresiones:

(GL AND EN AND ILC AND M) OR
 (GL AND EL AND INC AND MS) OR
 (GN AND EL AND INC AND MN) OR
 (GN AND EN AND INC AND MN) OR
 (GN AND EN AND ILC AND M) OR
 (GH1 AND EN AND IMC AND MN) OR
 (GH1 AND EN AND IHC AND M) OR
 ((GH2 OR GVH OR GTH) AND EN AND IHC AND MN) OR
 (GN AND EL AND INC AND MS) OR
 (GH1 AND EL AND INC AND MN)

10.5.2.4 Funcionamiento

Esta expresión lógica da un árbol binario de decisión de 94 vértices:

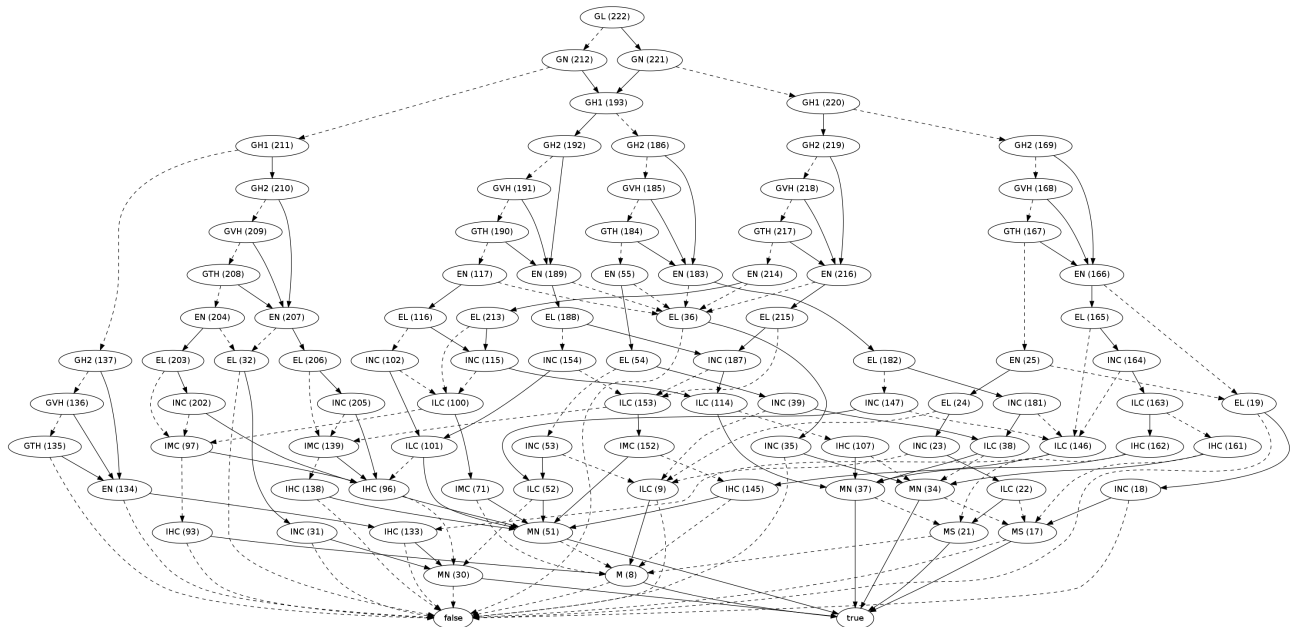
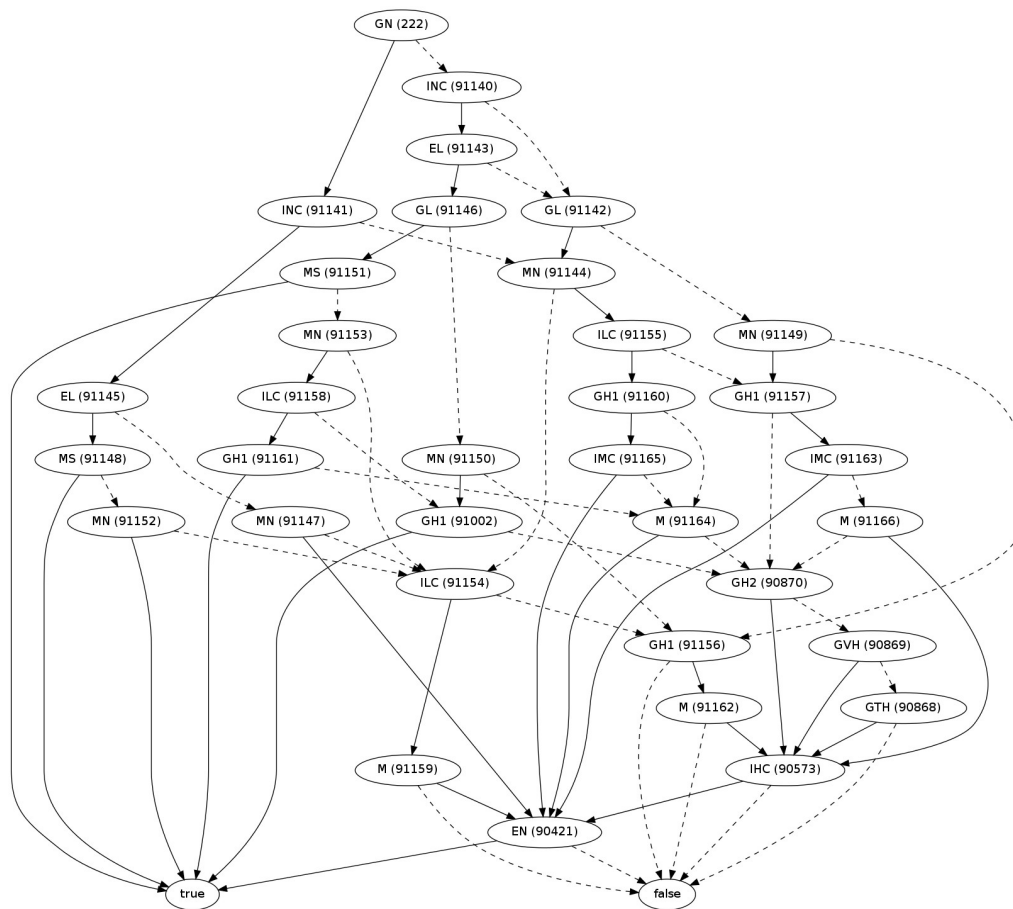


Fig. 27

Usando nuestro método de reducción, casi se logra una disminución a un tercio de su tamaño:

**Fig. 28**

A partir de ese momento, podemos ejecutar la simulación, que consiste en la llamada a varios métodos de la clase Human que simulan acciones de un paciente diabético tipo 1 en el mundo real. La clase padre es DiabetesT1Assistant, que será la que tenga las referencias a Human y a Asserter y contenga una simulación de un sistema software que ha de comprobar la consistencia a partir de unos datos reales.

La simulación está diseñada de forma que para cada decisión que tome el paciente, el sistema le indicará con un mensaje de texto si la decisión que ha tomado era mala o buena para su salud.

Este ciclo se prolonga a lo largo de 7 días, simulando una semana de decisiones de un paciente. Notemos que estas decisiones parten de datos aleatorios, como el valor de la glucosa al comenzar al día, justo antes de tomar el desayuno.

Para cada acción, se imprime si fue una decisión del paciente acertada o no y a continuación, los datos fuente que se usaron para comprobar si la acción era buena o no. Por ejemplo, en la siguiente acción tenemos que el paciente toma una comida normal con la glucosa alta, sin haber hecho ejercicio y se pone una cantidad pequeña de insulina. Como debería haberse puesto una cantidad del intervalo “medio” (según las reglas presentadas anteriormente), se informa al usuario de que la decisión era incorrecta:

EAT standard meal

BAD DECISION

BloodGlucose: GH1

Exercise: EN

Insulin: ILC

Meal: M

En este otro ejemplo, en cambio, el paciente tenía la glucosa normal, hizo un ejercicio ligero y no se puso insulina ni comió. Esto es una buena decisión según las reglas definidas para el sistema.

WALK

GOOD DECISION

BloodGlucose: GN

Exercise: EL

Insulin: INC

Meal: MN

Por otro lado, hemos de notar que hay muchas variables que se nos escapan como si el paciente está enfermo, el nivel de estrés del paciente, o incluso la época del año. Eso sí, hemos podido comprobar como, a medida que se van añadiendo variables, se va incrementando el tamaño del árbol, por eso es tan importante el tener un mecanismo de reducción del árbol BDD y por eso es importante, no tanto que sea muy rápido, sino que el resultado que dé sea un árbol BDD lo más mínimo posible.

11 Problemas abiertos

En primer lugar, está el problema de la naturaleza misma de los árboles binarios de decisión. Algunos autores han definido otro tipo de árboles de decisión como los KFDD [DRE94], FDD [KEB94], ZDD [MIS01], etc. Estos árboles se basan en distintas descomposiciones de las expresiones lógicas. Según la naturaleza de la fórmula lógica algunos tipos de árboles tendrán un tamaño menor a otros, y por tanto, se comportarán de forma más eficiente. El cálculo de cuál es el mejor tipo de árbol para una fórmula lógica determinada es un problema que ha sido estudiado por algunos autores como en [BEC95], pero no hemos encontrado estudios que indiquen cuál es el tipo de diagrama de decisión con el que se comporta mejor una expresión lógica de una determinada estructura.

Centrándonos en los árboles binarios de decisión, hay varios problemas que se están estudiando en la actualidad que comentamos a continuación.

Para comenzar, la paralelización del algoritmo *Apply*. Como hemos visto anteriormente, este algoritmo permite la construcción de un árbol a partir de una operación lógica y dos árboles binarios de decisión. Algunos trabajos como [KIM90] y [VAN12] han implementado esta operación de forma paralela, reduciendo su orden de eficiencia y permitiendo la construcción de árboles en menor tiempo.

Seguimos con el problema de la memoria principal limitada. Cuando comenzamos a trabajar con los ficheros DIMACS, intentamos cargar algunos de las fórmulas que usaban en las competiciones de cálculo de la satisfacibilidad. Esto se tornó imposible debido a su gran número de variables, y sobre todo, de su complejidad computacional. No se puede depender tanto del orden de las variables que si se escoge un orden que no es el óptimo, la estructura no quepa en memoria principal. Ante este problema, tenemos dos soluciones: minimizar el tamaño del árbol o tratar de estimar el tamaño a partir del orden, o lo que es igual, tener algún tipo de heurística que nos indique si un orden determinado generará un BDD inabarcable en nuestra memoria.

Por otro lado, pensamos que se podrían usar heurísticas avanzadas para implementar las

funciones de *fitness* de los algoritmos evolutivos que eviten la generación completa. Por ejemplo, realizando estimaciones con los cromosomas ya generados, o estimando, hasta cierto nivel, el tamaño del árbol y evitando tener que construir el árbol BDD completo para contar el número de vértices que tiene asociado un orde de variables.

Por último, es importante destacar que, inicialmente, estos árboles se usan como reductores de expresiones lógicas a la hora de implementar circuitos, pero en la actualidad tienen muchos otros más campos que se están descubriendo en los campos más diversos [STE10]. En concreto, en la Ingeniería del Software, con mucho éxito como se puede ver en [BEY13] y [ALU13]. Creemos que cualquier campo de la ciencia o ingeniería en el que se puedan modelar restricciones con expresiones de lógica booleana puede ser un buen candidato para usar este tipo de árboles.

12 Conclusiones

12.1 DJBDD: una nueva biblioteca para tratar con BDDs

Actualmente las bibliotecas que se usan para realizar experimentos con árboles binarios de decisión tienen carencias en cuanto a calidad de código y facilidad de comprensión.

Se ha desarrollado una nueva biblioteca en Java para la representación de árboles binarios de decisión con énfasis en la calidad y claridad de código. Esta biblioteca contiene los métodos necesarios para trabajar con árboles, incluyendo las operaciones de creación como las de operaciones entre dos árboles.

Por otro lado, esta biblioteca contiene varias técnicas avanzadas como el uso de una única malla de vértices o un contador de referencias. Además contiene utilidades para mostrar el árbol de forma gráfica o crear árboles a partir de expresiones lógicas escritas en distintos formatos.

Con el objetivo de completar esta biblioteca, también se han desarrollado una serie de algoritmos de reordenación dinámica de variables para poder reducir el tamaño de un árbol de forma dinámica, y no sólo poder hacerlo conociendo la estructura de la expresión lógica a reducir.

La biblioteca se llama DJBDD y está disponible de forma pública en un repositorio de github en <https://github.com/diegojromerolopez/djbdd>. Puede integrarse en cualquier proyecto para proporcionar labores de almacenamiento de restricciones, comprobación de consistencia lógica o reducción de expresiones lógicas booleanas.

12.2 Iterative Sifting: un nuevo algoritmo reductor de BDDs

Hemos mostrado cómo un algoritmo basado en el intercambio de variables se comporte mejor que el algoritmo *Sifting* de Rudell y varios algoritmos evolutivos. Este nuevo algoritmo funciona mejor que otros algoritmos bien conocidos en el conjunto de pruebas para el que los hemos comparado. Nuestro algoritmo consigue una mayor reducción que los algoritmos evolutivos y no depende de un generador aleatorio, lo que lo hace más sólido que estos

métodos. Esto es, nuestro algoritmo se convierte en un buen candidato usarlo como método de optimización en técnicas híbridas de reducción.

Para lograr estos resultados, se han hecho unas pruebas con expresiones lógicas provenientes de instancias de problemas de satisfacibilidad lógica (SAT).

Además, estas pruebas han descubierto un problema grave de los algoritmos evolutivos, ya que al explorar sin ninguna restricción el espacio de búsqueda, pueden tratar de construir el árbol binario de decisión para un orden *malo*, en el sentido de que el árbol generado tenga tal tamaño que no quepa en memoria principal.

12.3 Un comprobador de consistencia lógica

También se ha presentado un sistema que permite la integración de un comprobador de consistencia lógica en otros paquetes software. La integración no es complicada, donde reside la complejidad es en la definición de las variables lógicas en función de las magnitudes que se vayan a medir y en hacer que nuestro sistema de comprobación pueda acceder a sus valores en un momento determinado.

Para facilitar la labor de comprensión de la herramienta, se exponen dos ejemplos de implementación. El primero es un caso que sirve como modelo a futuros desarrolladores al modelar un sistema limitado del mundo real. En cambio, en el segundo ejemplo se puede ver cómo se construye un árbol BDD para un caso real y se puede comprobar como si una serie de decisiones de pacientes son conformes a las reglas definidas por un médico.

En ambos ejemplos se muestran los árboles binarios de decisión generados, y cómo se puede reducir el tamaño árbol mediante nuestro algoritmo *Iterative Sifting*, obteniendo un BDD optimizado.

13 Glosario de términos

Algoritmo Genético	Algoritmo Evolutivo que se basa en procesos y representaciones biológicas para obtener un mejor resultado en problemas que se pueden modelar con una serie de operaciones [LEN08].
Algoritmo Memético	Algoritmo Evolutivo que aplica un proceso de búsqueda local sobre el cromosoma en cada iteración.
Árbol Binario de Decisión	Representación compacta de una expresión lógica basada en un diagrama de decisión binario [BRY86] [BRY92].
BDD	Ver Árbol Binario de Decisión.
BuDDy	Librería de BDDs de dominio público [BUD].
CNF	Forma Normal Conjuntiva. Tipo de estructura para expresiones lógicas compuesta por la conjunción de cláusulas disyuntivas [AND97].
CUDD	Librería de BDDs desarrollada por Fabio Somenzi [SOM].
Consistencia Lógica	Una expresión lógica se dice consistente si no es una contradicción [AND97].
DIMACS	Formato de fichero para almacenamiento de fórmulas lógicas en formato CNF [BUR].
DJBDD	Librería de BDDs desarrollada por Diego J. Romero López que implementa una gran cantidad de algoritmos y

aplicaciones.

Expansión de Boole-Shannon	Descomposición de una fórmula lógica como disyunción de otras dos fórmulas asignando a una variable en una de ellas el valor cierto y a otra el valor falso. [AND99]
Iterative Sifting	Algoritmo original que explota la búsqueda de la mejor posición para cada variable en el BDD.
Satisfacibilidad	Una expresión lógica es satisfacible si y solamente si hay una asignación de valores de verdad para sus proposiciones que la hace cierta [AND97].
Sifting	Algoritmo heurístico de reducción del tamaño de BDDs basado en el intercambio de variables, que busca la mejor posición para cada variable en el árbol binario de decisión [RUD93].
Verificación de Modelos	Model Checking en inglés. Disciplina que tiene como objetivo dar un modelo matemático para sistemas cambiantes en el tiempo [AND97].
Window Permutation	Algoritmo heurístico de reducción del tamaño de BDDs basado en el intercambio de variables, que genera intercambios por ventanas [RUD93].

14 Bibliografía

- [AND99] H. R. Andersen. An Introduction to Binary Decision Diagrams. Lecture notes for Efficient Algorithms and Programs. IT Universidad de Copenhagen, 1999.
- [AKE78] S. B. Akers. *Binary Decision Diagrams*. IEEE Transactions on Computers, Vol. C-27, No. 6, pp. 509-516, 1978.
- [AND97] H. R. Andersen y H. Hulgaard. *Boolean expression diagrams*. Logic in Computer Science. LICS'97. Proceedings., 12th Annual IEEE Symposium on (pp. 88-98). IEEE, 1997.
- [ALU13] R. Alur, T. A. Henzinger, M. Y. Vardi. Theory in Practice for System Design and Verification. 2013
- [ALO03] F. A. Aloul, I. L. Markov y K. A. Sakallah. *FORCE: A Fast and Easy-To-Implement Variable-Ordering Heuristic*, GLSVLSI, 2003.
- [ALO01] F. A. Aloul, I. L. Markov, y K. A. Sakallah. *Faster SAT and Smaller BDDs via Common Function Structure*. ICCAD, 443-448, 2001.
- [BALL00] T. Ball y S. K. Rajamani. *Bebop: A symbolic model checker for Boolean programs*. En SPIN 00: SPIN Workshop, LNCS 1885, pages 113–130. Springer-Verlag, 2000.
- [BALL04] T. Ball, B. Cook, V. Levin y S. K. Rajamani. SLAM and Static Driver Verifier: Technology Transfer of Formal Methods inside Microsoft. Technical Report. MSR-TR-2004-08. Microsoft Research, 2004.
- [BEC95] B. Becker y R. Drechsler. How many Decomposition Types do we need? IEEE

European Design & Test Conference, pp. 438-443, 1995.

- [BEY13] D. Beyer y A. Stahlbauer. *BDD-based software model checking with CPACHECKER*. En *Mathematical and Engineering Methods in Computer Science*. Springer Berlin Heidelberg, 2013. p. 1-11.
- [BJO14] D. Bjørner, K. Havelund. *40 Years of Formal Methods*. FM 2014: Formal Methods. Springer International Publishing, 2014. p. 42-61.
- [BRY86] R. E. Bryant. *Graph-Based Algorithms for Boolean Function Manipulation*. Computers, IEEE Transactions on, 100(8), 677-691, 1986.
- [BRY92] R. E. Bryant. *Symbolic Boolean Manipulation with Ordered Binary Decision Diagrams*, ACM Computing Surveys, 1992.
- [BUD] BuDDy: A BDD package, <http://buddy.sourceforge.net/manual/main.html>
- [BUR] J. Burkardtl, [Formato DIMACS CNF](#).
- [BUR95] C. J. Burgess. *The Role of Formal Methods in Software Engineering Education and Industry*. 1995.
- [BRA91] K. S. Brace, R. L. Rudell, R. E. Bryant. *Efficient implementation of a BDD package*, Proceedings of the 27th ACM/IEEE design automation conference (pp. 40-45), ACM, 1991.
- [BEY13] D. Beyer y A. Stahlbauer. *BDD-Based Software Model Checking with CPACHECKER*. *Mathematical and Engineering Methods in Computer Science* (pp. 1-11), Springer Berlin Heidelberg, 2013.
- [BOE06] B. Boehm. *A view of 20th and 21st century software engineering*. En *Proceedings of the 28th international conference on Software engineering*. ACM, 2006. p. 12-29.
- [BOL05] B. Bollig, I. Wegener. *Improving the Variable Ordering of OBDDs is NP-Complete*, IEEE Transactions on Computers, vol 45, 993-1002. 2005.
- [CLA81] E. M. Clarke y E. A. Emerson, *Design and Synthesis of Synchronization Skeletons Using Branching-Time Temporal Logic*, D. Kozen (Ed.) *Logic of Programs*. Volumen 131 de LNCS, p. 52-71, 1981. Springer.
- [DEM09] T. De Marco. *Software engineering: an idea whose time has come and gone?*. IEEE Software, 2009, vol. 26, n. 4, p. 96-95.
- [DIJ76] E. W. Dijkstra, y otros. *A discipline of programming*. Englewood Cliffs: Prentice-hall, 1976.
- [DIJ88] E. W. Dijkstra. *On the cruelty of really teaching computing science*. No publicado, EWD, 1988, vol. 1036.

- [DRE01] R. Drechsler. *Binary Decision Diagrams: Theory and Implementation*. Vol. 4. SIAM, Springer, 2001.
- [DRE94] R. Drechsler, A. Sarabi, M. Theobald, B. Becker y M. A. Perkowski. Efficient representation and manipulation of switching functions based on ordered kronecker functional decision diagrams, Design Automation, Conference on, pp. 43-47. IEEE, 1994.
- [FLO67] R. W. Floyd. *Assigning meanings to programs*. Mathematical aspects of computer science, 1967, vol. 19, no 19-32, p. 1.
- [GRA] Equipo de desarrollo de Graphviz. Graph Visualization Software. [Enlace](#).
- [GRA2] Equipo de desarrollo de Graphviz . Formato del lenguaje DOT. [Enlace](#).
- [HOA69] C. A. R. Hoare. *An axiomatic basis for computer programming*. Communications of the ACM, 1969, vol. 12, no 10, p. 576-580.
- [HOA02] C. A. R. Hoare. *Proof of correctness of data representations*. Springer Berlin Heidelberg, 2002.
- [HOL00] S. Hölldobler, S. Störr, Hans-Peter. *BDD-based reasoning in the fluent calculus-first results*. arXiv preprint cs/0003047, 2000.
- [JAV] Equipo de desarrollo de Javaluator, <http://javaluator.sourceforge.net/en/home/>
- [EBE05] R. Ebdnt, F. Görschwin y R. Drechsler. Advanced BDD Optimization. Heidelberg: Springer, 2005.
- [FUJ91] M. Fujita, Y. Matsunaga, y T. Kakuda. *On variable ordering of binary decision diagrams for the application of multi-level logic synthesis*. Proceedings of the conference on European design automation (pp. 50-54). IEEE Computer Society Press, 1991.
- [HOO98] H. H. Hoos Stochastic Local Search - Methods, Models, Applications. Tesis doctoral, TU Darmstadt, 1998 [Problemas codificados para SAT, All Interval Series](#).
- [HOO] H. H. Hoos. [SATLIB benchmark problems](#).
- [HOO2] H. H. Hoos. [Instances for Circuit Fault Analysis](#).
- [HUT04] M. Huth y M. Ryan. Logic in Computer Science. Cambridge University Press, 2004.
- [HAL90] A. Hall. *Seven myths of formal methods*. Software, IEEE, 1990, vol. 7, nº 5, p. 11-19.
- [HAS02] S. Hassoun y T. Sasao. Logic Synthesis and Verification. Springer, 2002.

- [ISH91] N. Ishiura, H. Sawada y S. Yajima. *Minimization of Binary Decision Diagrams Based on Exchanges of Variables*, Proceedings International Conference on Computer-Aided Design, 1991.
- [JAC91] R. Jacobi, N. Calazans y C. Trullemans. *Incremental Reduction of Binary Decision Diagrams*, Circuits and Systems, IEEE International Symposium on, (pp. 3174-3177). IEEE, 1991.
- [KIM90] S. Kimura y E. M. Clarke. *A parallel algorithm for constructing binary decision diagrams*, *Computer Design: VLSI in Computers and Processors*, ICCD'90. Proceedings, IEEE International Conference on (pp. 220-223). IEEE, 1990.
- [KEB94] U. Kebschull, E. Schubert y W. Rosenstiel. Multilevel logic synthesis based on functional decision diagrams. European Design Automation Conf., pp 8-13, 1994.
- [KNU68] D. Knuth. The Art of Computer Programming. Volúmenes 1-4. Addison-Wesley, Reading, Mass., EE. UU.
- [LAN64] P. J. Landin. *The mechanical evaluation of expressions*. The Computer Journal, 1964, vol. 6, no 4, p. 308-320.
- [LAN65] P. J. Landin. *Correspondence between ALGOL 60 and Church's Lambda-notation: part I*. Communications of the ACM, 1965, vol. 8, no 2, p. 89-101.
- [LEI03] G. W. Leibniz. *Generales inquisitiones de analysi notionum et veritatum*. Opusculs et fragments inédits, 1ª Ed. París, 1903.
- [LEE59] C. Y. Lee. Representation of Switching Circuits by Binary-Decision Programs, Bell System Technical Journal, Vol. 38, pp. 985-999, 1959.
- [LEN08] W. Lenders y C. Baier. *Genetic Algorithms for the Variable Ordering Problem of Binary Decision Diagrams*, Foundations of Genetic Algorithms (pp. 1-20). Springer Berlin Heidelberg, 2008.
- [MIL98] K. Milvang-Jensen. BDDNOW: a parallel BDD package. *Formal Methods in Computer-Aided Design* (pp. 501-507). Springer Berlin Heidelberg, 1998.
- [MAC83] J. McCarthy. Recursive functions of symbolic expressions. Springer Berlin Heidelberg, 1983.
- [MAC93] J. McCarthy. *Towards a mathematical science of computation*. Program Verification. Springer Netherlands, 1993. p. 35-56.
- [MAR08] R. C. Martin. Clean Code. Prentice Hall. 1ª Ed. Junio 2008.
- [MCC04] S. McConnell. Code Complete: A Practical Handbook of Software Construction, 2ª Ed. Microsoft Press. 2004.
- [MCM92] K. L. McMillan. Symbolic Model Checking: An approach to the state explosion

- problem. CMU-CS-92-131. Phd. Thesis, Carnegie Mellon University, 1992.
- [MCM93] K. L. McMillan. *The SMV system*. En Symbolic Model Checking. Springer US, 1993. p. 61-85.
- [MIS01] A. Mishchenko. An introduction to zero-suppressed binary decision diagrams, 2001. [Enlace](#).
- [MIN90] S. I. Minato, N. Ishiura, y S. Yajima. *Shared binary decision diagram with attributed edges for efficient Boolean function manipulation*. Design Automation Conference, 1990. Proceedings., 27th ACM/IEEE (pp. 52-57). IEEE, 1990.
- [MEI98] C. Meinel y T. Theobald. *Algorithms and Data Structures in VLSI Design: OBDD-foundations and applications*. Springer, 1998.
- [NIC] E. Nicholas. Understanding Weak References, Java.net. [Enlace](#).
- [ORA] Oracle Corp. Documentación de la API de Java 7 sobre referencias débiles. [Enlace](#).
- [ORA2] Oracle Corp. [Documentación de la API de Java 7](#).
- [ORA3] Oracle Corp. Plataforma de referencia de desarrollo Java de código abierto. [Enlace](#).
- [PAR10] D. L. Parnas. *Really rethinking 'formal methods'*. Computer, 2010, vol. 43, no 1, p. 28-34.
- [PAR13] T. Parr. The definitive ANTLR reference: building domain-specific languages. Pragmatic Bookshelf, 2013.
- [PAR] T. Parr. Analizador de lenguajes ANTLRv3. <http://www.antlr3.org/>
- [QUI81] J. P. Quielle y J. Sifakis. Specification and verification of concurrent systems in CESAR. 5th International Symposium in Programming, volume 137 de LCNS. Springer-Verlag, 1981.
- [RAN96] B. Randell. The 1968/69 nato software engineering reports. History of Software Engineering, 1996, p. 37.
- [RHE11] A. von Rhein, S. Apel y F. Raimondi. *Introducing binary decision diagrams in the explicit-state verification of Java code*. En Proc. Java Pathfinder Workshop. 2011. p. 82.
- [RUD93] R. L. Rudell. *Dynamic variable ordering for ordered binary decision diagrams*, Proceedings of the 1993 IEEE/ACM international conference on Computer-aided design (pp. 42-47). IEEE Computer Society Press, 1993.

- [RUD] R. L. Rudell. BDDs: Implementation Issues & Variable Ordering. Notas de CAD applications of BDDs: theory and practice.
- [RIC08] M. Rice y S. Kulhari. A Survey of Static Variable Ordering Heuristics for Efficient BDD/MDD Construction. University of California, Tech. Report, 2008.
- [SEI04] R. Dupuis y otros. Software Engineering Body of Knowledge. 2004.
- [SOM99] F. Somenzi. *Binary Decision Diagrams*, Computational System Design, vol. 173 of NATO Science Series F: Computer and Systems Sciences, 1999.
- [SZA] L. Szathmary, Paquete de software de uso de GraphViz desde Java. [Enlace](#).
- [SOM] F. Somenzi, CUDD: CU Decision Diagram Package. Release 2.5.0. University of Colorado at Boulder. <http://vlsi.colorado.edu/~fabio/CUDD/>
- [STO96] A. Stornetta, F. Brewer. *Implementation of an Efficient Parallel BDD Package*, Proceedings of the 33rd annual Design Automation Conference (pp. 641-644). ACM, 1996.
- [STE10] S. Stergiou y J. Jain. *Novel Applications of a Compact Binary Decision Diagram Library to Important Industrial Problems*. FUJITSU Sci. Tech. J., vol. 46, nº 1, pp. 111-119, 2010.
- [SAS96] T. Saso y M. Fujita (Ed.). Representations of Discrete Functions, Springer, 1996
- [VAN12] T. Van Dijk. The Parallelization of Binary Decision Diagram operations for model checking. Tesis de Máster. Universidad de Twente, 2012.
- [WEG00] I. Wegener. *Branching Programs and Binary Decision Diagrams: Theory and Applications*. SIAM, 2000.
- [WOD09] J. Woodcock y otros. *Formal methods: Practice and experience*. ACM Computing Surveys (CSUR), 2009, vol. 41, no 4, p. 19.