

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



Trabajo fin de máster del
Máster en Investigación en Ingeniería del Software
de la Universidad Nacional de Educación a Distancia

Alumno: Diego J. Romero López

Directora: Prof. Dra. Dña. Elena Ruiz-Larrocha

Septiembre del 2014

Índice

1. Introducción
2. Motivación
3. Árboles Binarios de Decisión
4. Aplicaciones: Verificación de software
5. Reducción de Árboles Binarios de Decisión
6. Problemas abiertos
7. Conclusiones
8. Bibliografía fundamental

1. Introducción

La complejidad del software llega a niveles en los que es imposible abarcar los estados del sistema.

Hay sistemas críticos que no deben fallar.

Si fallan, es una catástrofe.

El coste de comprobar manualmente todos los estados de un sistema software es demasiado elevado.

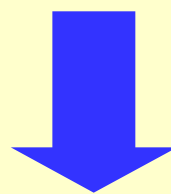
¿Puede el sistema recuperarse si detecta un fallo?

Ejemplos de sistemas críticos:

- Aviónica.
- Transportes: vehículos, trenes...
- Sistemas médicos.
- Sistemas militares
- Banca
- Sistemas de posicionamiento geográfico

Podemos definir una serie de reglas lógicas que modelen el sistema.

Si el estado del sistema no puede ser expresado por ninguna de esas reglas, hay un estado inconsistente.



Sea i cada uno de los estados posibles del sistema y p_i la proposición lógica que se evalúa como *True* si el estado actual del sistema es p_i y *False* en otro caso.

El sistema es consistente si y solamente si la siguiente disyunción es cierta:

$$p_1 \vee p_2 \vee \dots \vee p_n$$

Para evaluar la expresión en un momento determinado vamos a construir un Árbol Binario de Decisión (BDD) que contendrá esta fórmula y nos permitirá evaluarlo de forma rápida.

2. Motivación

Verificación Simbólica de Modelos:

- Método Formal
- Basada en la expresión:

$$M, s \models p$$

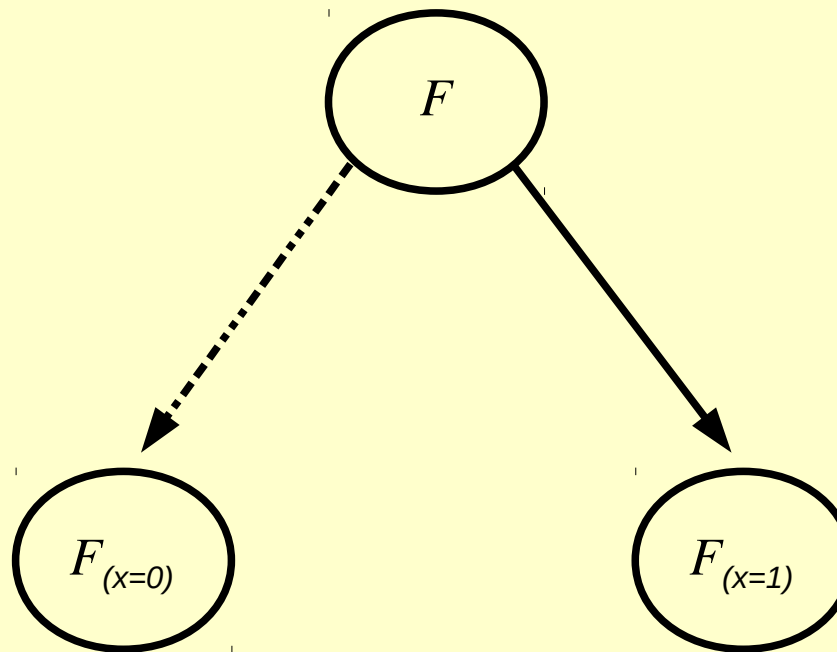
Los BDDs son excelentes a la hora de representar los estados y las relaciones de transición.

Ejemplos: SMV (NuSMV), JavaPathfinder (ext. BDD), Moped, etc.

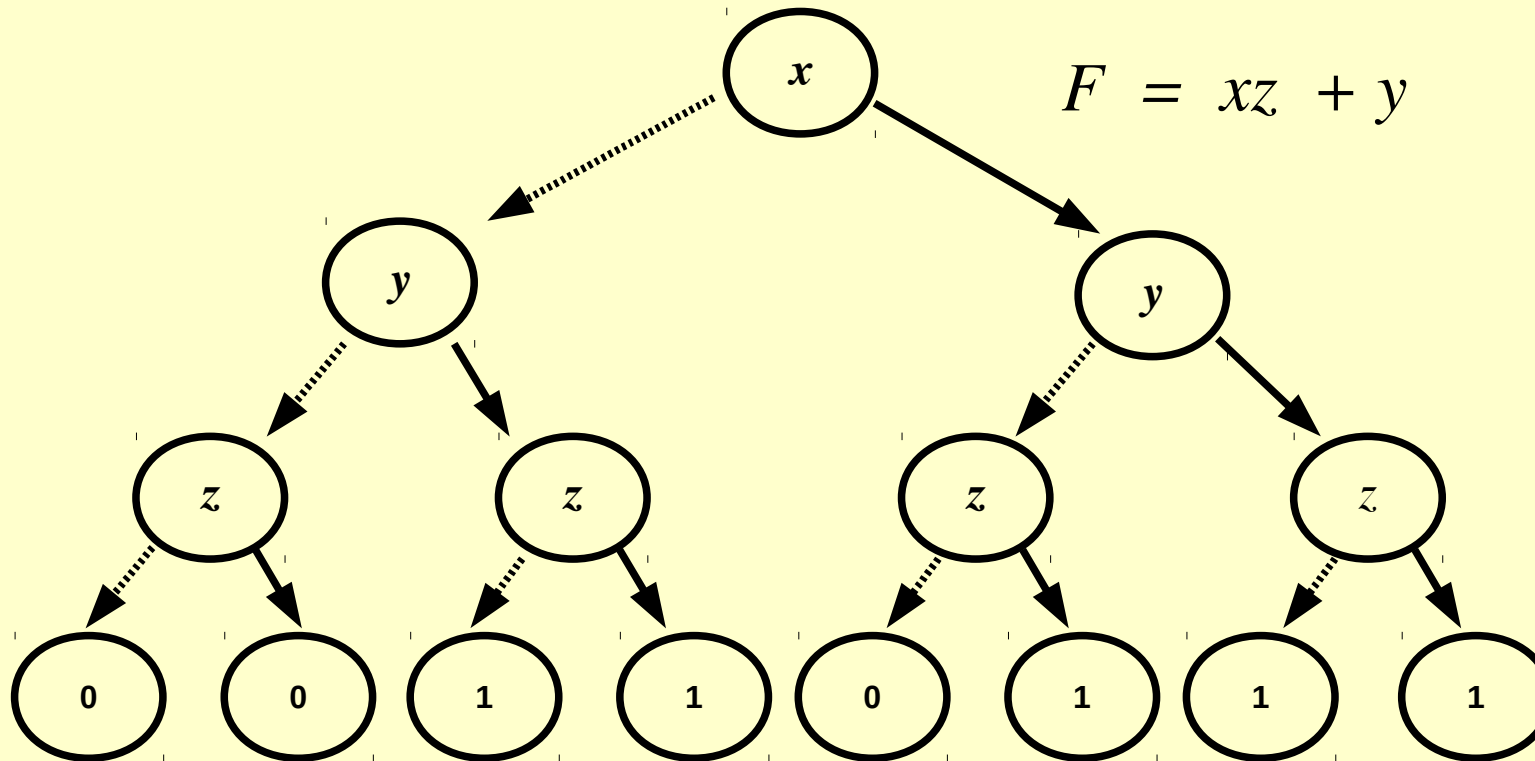
3. Árboles Binarios de Decisión

Estructura de datos basada en la expansión de Boole-Shannon:

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



Los Árboles Binarios de Decisión (BDD) son una forma de expresar una Tabla de Verdad:

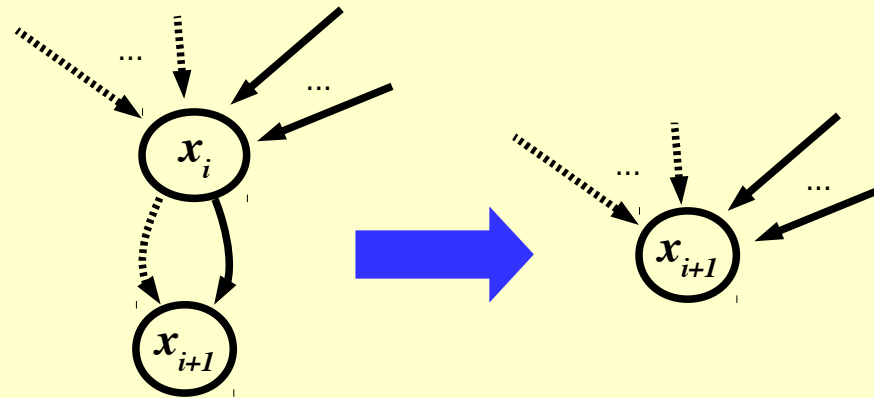


Problema: crecimiento de número de nodos con orden 2^n donde n es el número de variables.

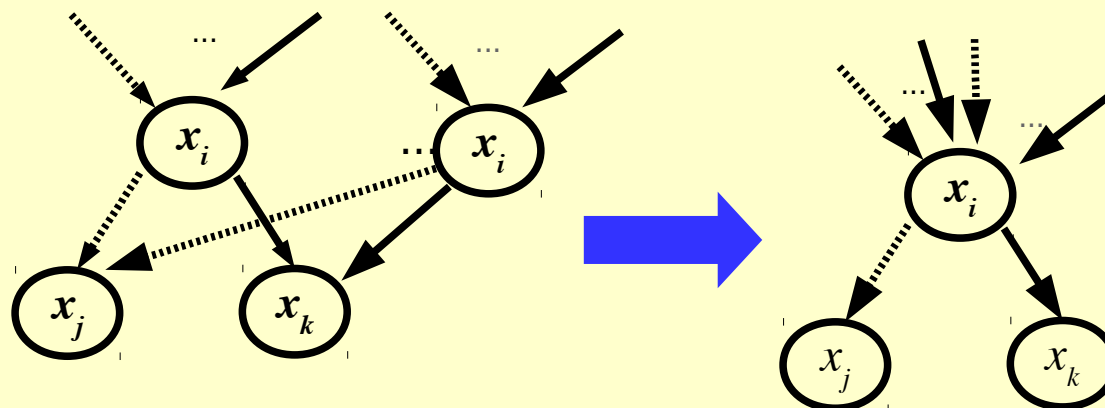
Solución: convertir el árbol en un grafo dirigido acíclico.

Randall E. Bryant define una serie de restricciones para construir el grafo a partir de un árbol binario de decisión:

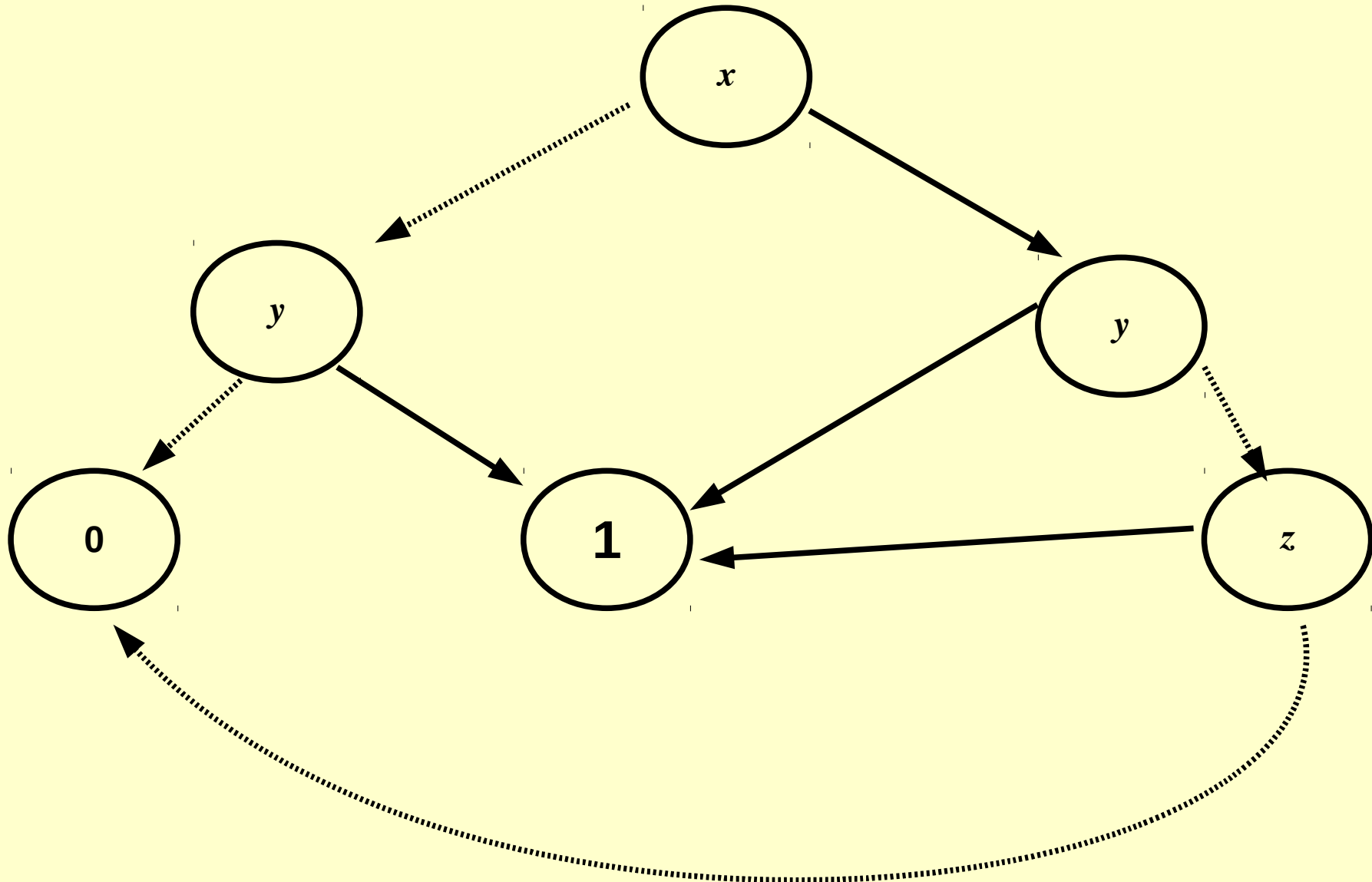
Unicidad:



No-redundancia:



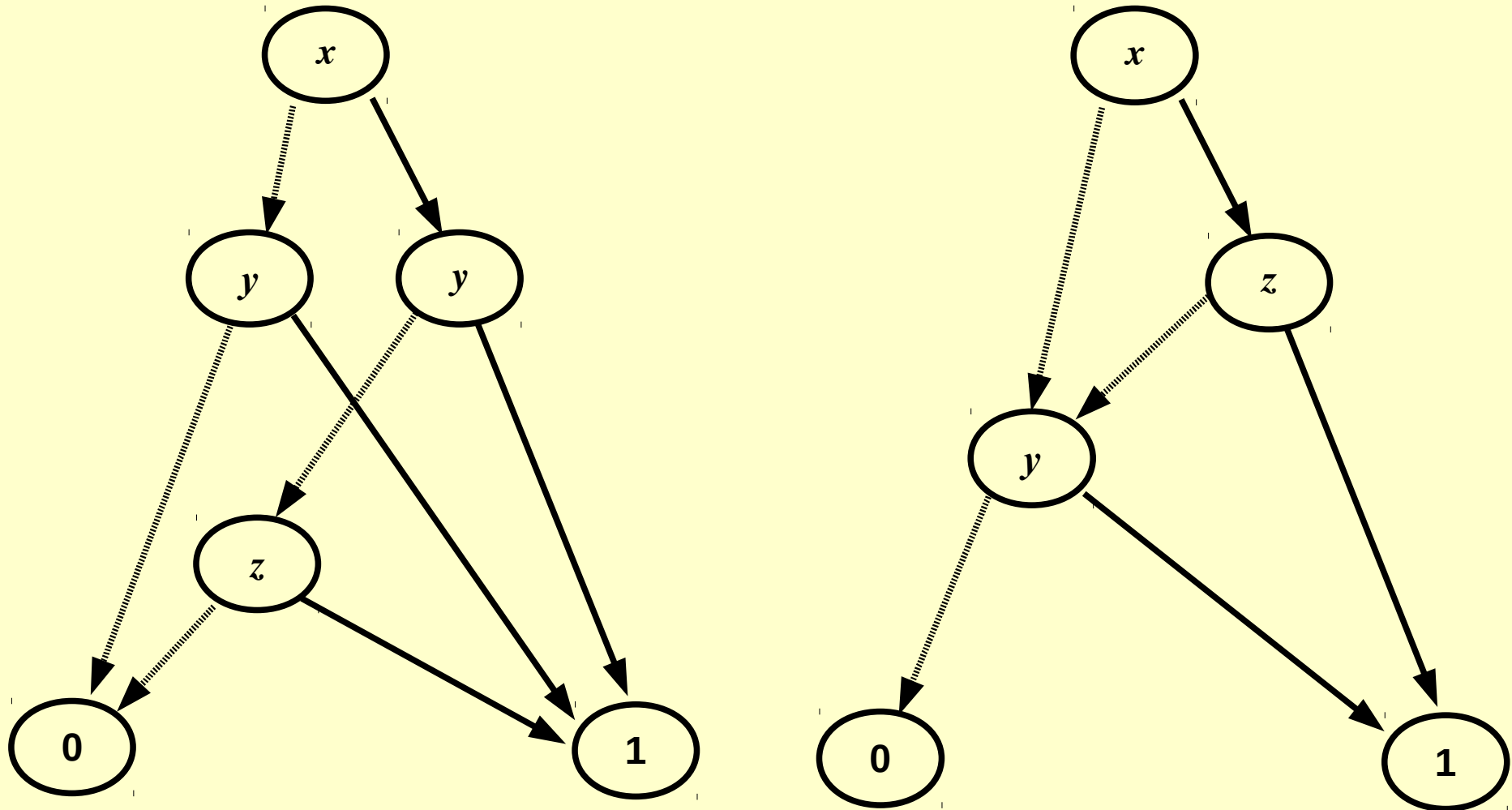
Aplicando esas restricciones a nuestro ejemplo:



Propiedades

- Se pueden aplicar operaciones lógicas sobre árboles:
 - **AND**
 - **OR**
 - **NOT**
 - **Restrict**: evalúa la función lógica que contiene.
- Los BDDs proporcionan un mecanismo de **minimización** de expresiones lógicas.
- Los árboles son **únicos** para un orden de variables.
- La **implantación en hardware** de un BDD es *sencilla*.¹²

El tamaño de los BDDs depende del orden de variables:



Encontrar el orden que hace el BDD óptimo en tamaño es un problema NP-duro.

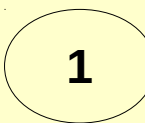
4. Verificación de software

Los BDDs pueden usarse como evaluadores de expresiones lógicas, de las restricciones del sistema.

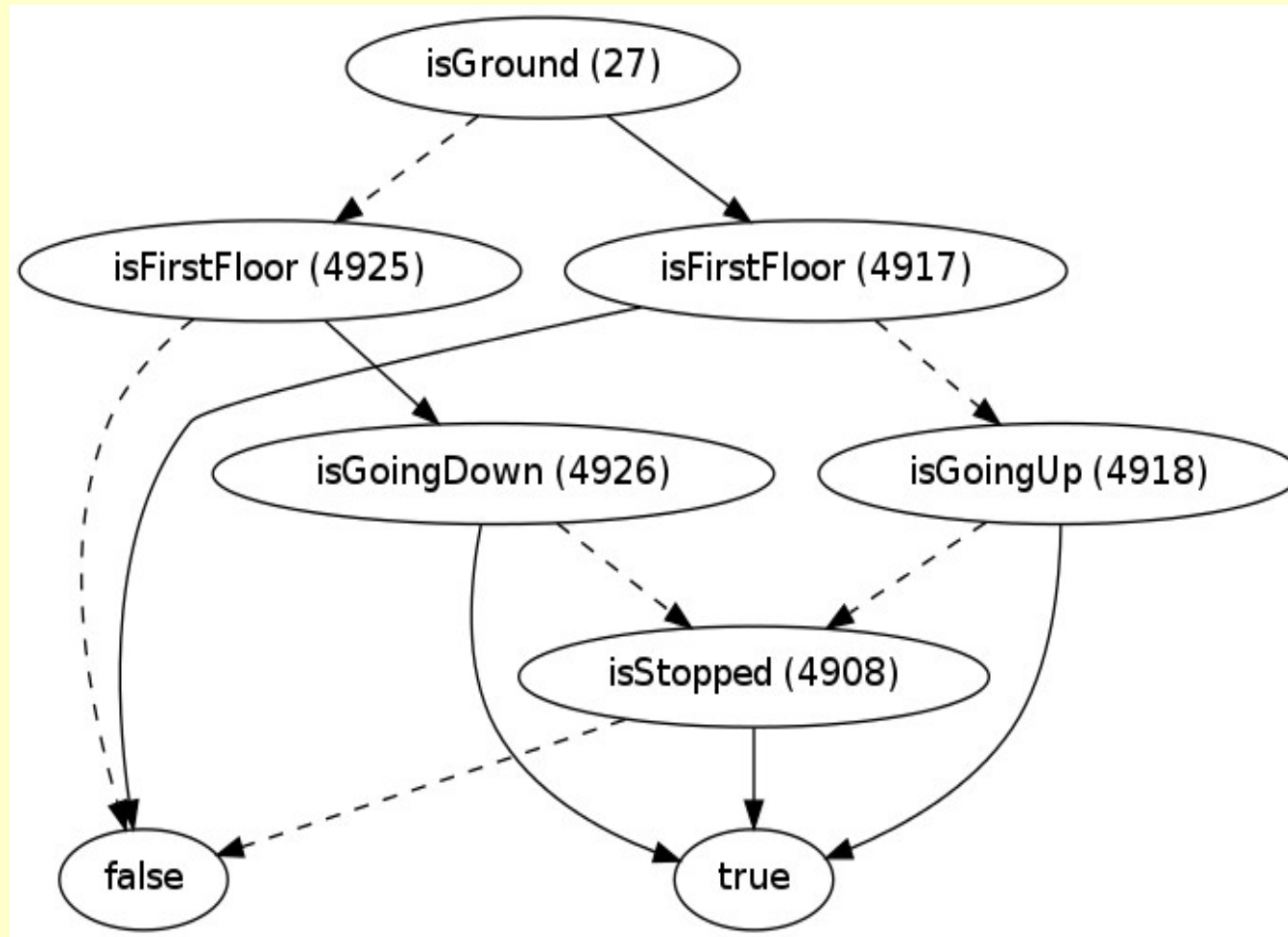
Operación **restrict**: asigna a una serie de variables unos valores de verdad y por tanto *restringe* el árbol.

Si se asignan valores de verdad a todas las variables, el BDD se comporta como un evaluador completo de la expresión, pudiendo devolver:

Árbol *false*: 

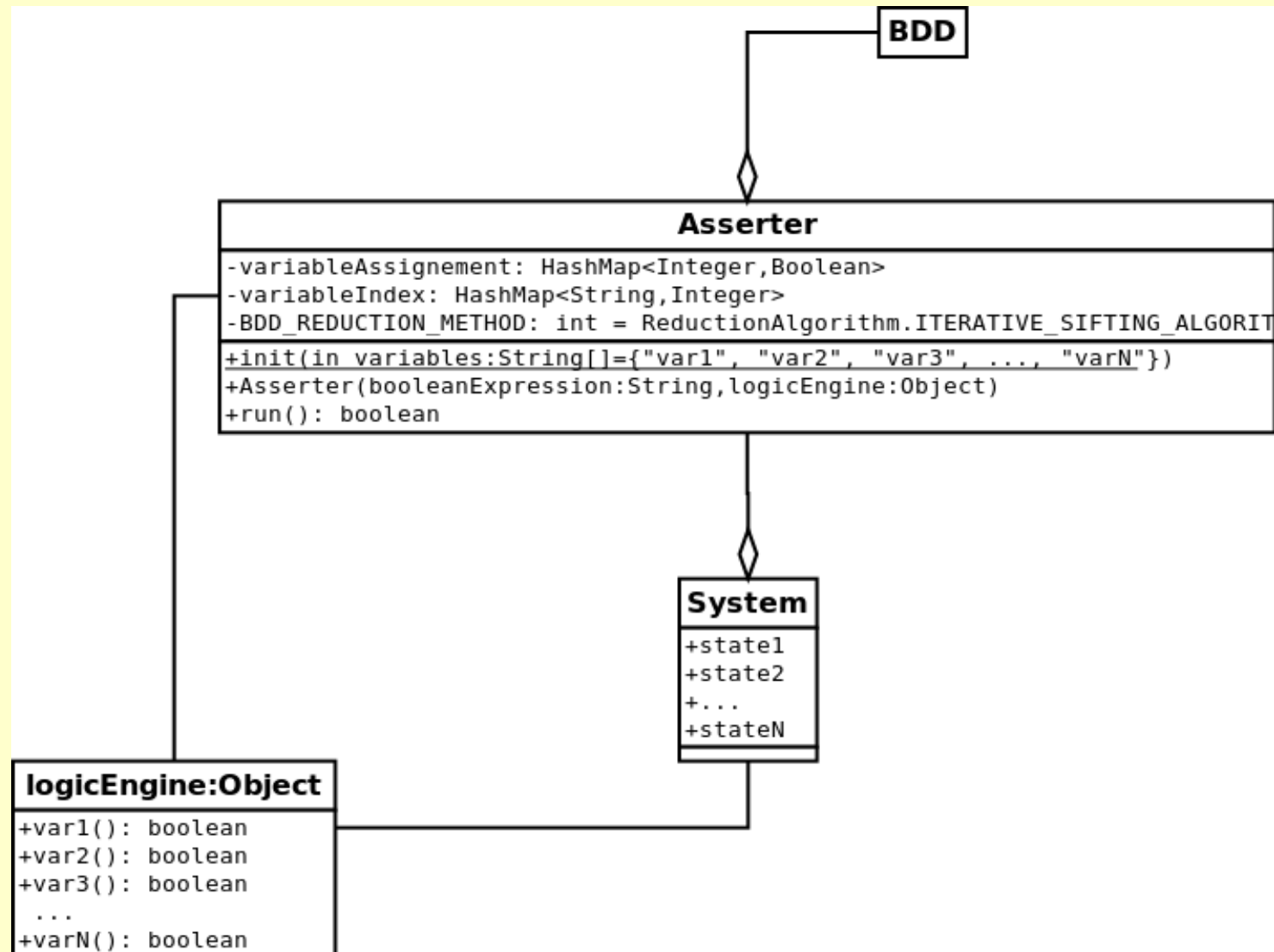
Árbol *true*: 

Un BDD puede mantener las reglas de un sistema:



Permitiendo evaluar si su estado es *consistente* o *inconsistente*.

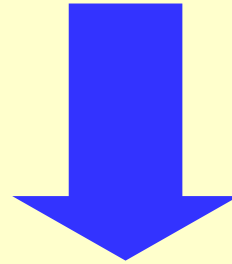
Arquitectura software del comprobador:



¿Cuántos proposiciones lógicas (variables) hacen falta para poder expresar las restricciones sobre un sistema software?

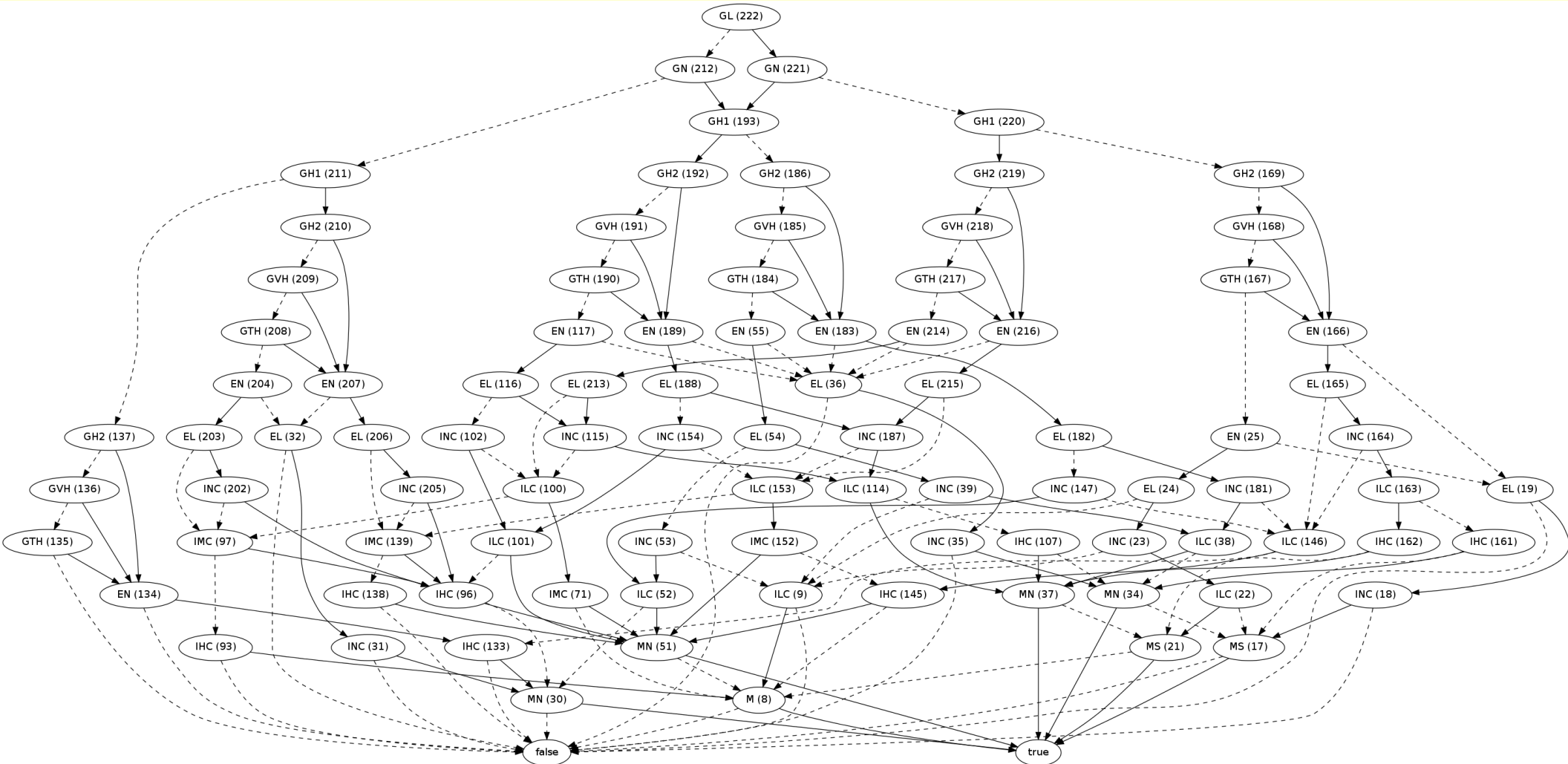
¿Cuál es la estructura de la fórmula?

¿Cuál es el mejor orden para construir el BDD?



¿Cuántos nodos harán falta para construir el BDD asociado?

Ejemplo: Asesor de control glucémico para diabéticos T1



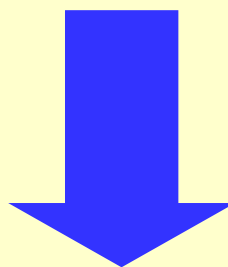
- 17 variables.
- 10 reglas.
- 94 vértices.

5. Reducción de BDDs

El BDD depende fuertemente del orden de variables.

Podemos reordenar las variables del BDD hasta obtener un orden de variables *suficientemente pequeño* como para que sea *fácil* trabajar con él.

Nos centraremos en la reordenación dinámica.



Es más versátil y se puede usar una vez construido el BDD (o durante su construcción).

Hay diversas estrategias:

- Algoritmos de Búsqueda Local:
 - Sifting.
 - Window Permutation
- Algoritmos Evolutivos
 - Algoritmos Genéticos.
 - Algoritmos Meméticos.
- Algoritmos Exactos:
 - Búsqueda Exhaustiva.

Mi solución (Iterative Sifting) **vence en la mayoría de las pruebas** realizadas debido a su forma de explotar la búsqueda de soluciones.

Algorithm 1 Iterative Sifting

Require: *numIterations*: Number of iterations.

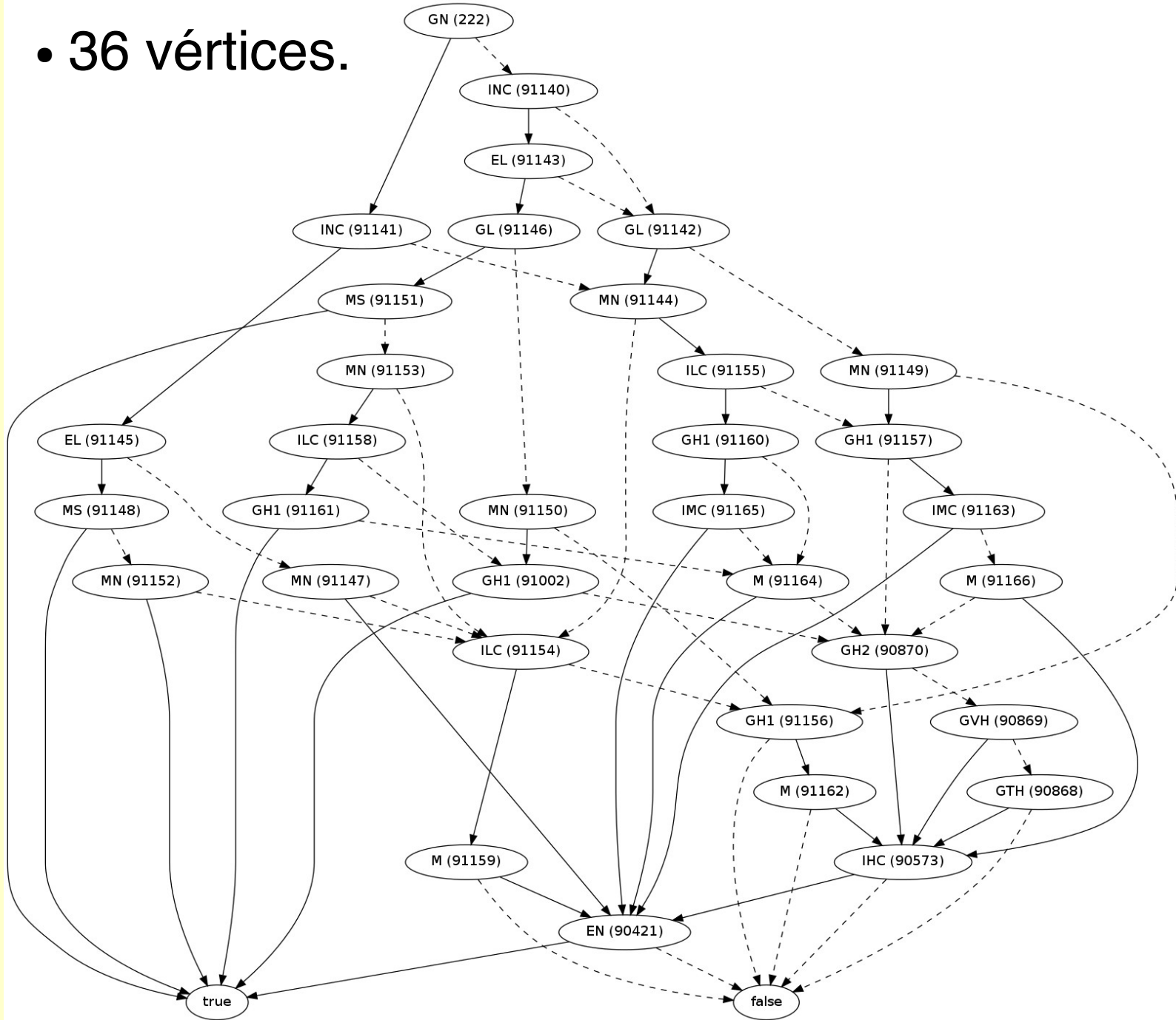
Require: *BDD* A Binary Decision Diagram.

Ensure: A BDD with a new variable order that reduces its previous size.

```
1: thereWasAnImprovement = False
2: i = 0
3: bestVariableOrder = BDD.variables()
4: bestBDDSize = BDD.size()
5: repeat
6:   thereWasAnImprovement = False
7:   i = 0
8:   while i < numIterations do
9:     # Order variables in descending order according to
10:    # the number of vertices of each one in the BDD.
11:    variableOrder = orderVariables(BDD.variables())
12:    for all varj ∈ variableOrder do
13:      # Move the variable varj to the best position
14:      # That is, the position that makes the BDD minimal.
15:      # Described in [7]
16:      moveVariableBestPosition(varj, BDD)
17:      bddSize = BDD.size()
18:      if bddSize < bestBDDSize then
19:        bestVariableOrder = BDD.variables()
20:        bestBDDSize = bddSize
21:        thereWasAnImprovement = True
22:      end if
23:    end for
24:    i = i + 1
25:  end while
26: until not thereWasAnImprovement
27: applyOrderToBDD(BDD, bestVariableOrder)
28: return BDD
```

Ejemplo: Asesor de Diabéticos T1 (reducido)

- 36 vértices.



Enviado a IEEE Transactions on Computers

 https://mc.manuscriptcentral.com/tc-cs?PARAMS=xik_aQX5w1jrK6NZxR2mbMfAb2XQj7hPKHNsGM45UKe59fommCewQLfrTsaSuiHg4f62v561ipRDohCT2Riif1LMse852FLEWKwvGtcR...

Transactions on Computers

Preview

From: n.cicero@ieee.org

To: diegojromerolopez@gmail.com, elena@issi.uned.es

CC: diegojromerolopez@gmail.com, elena@issi.uned.es

Subject: Submission Received & Confirmation TC-2014-05-0392

Body: Subject: RE: TC-2014-05-0392, "Iterative Sifting: A New Approach to Reduce BDD Size"
Manuscript Type: Regular
Authors: Romero-López, Diego; Ruiz-Larrocha, Elena

Dear Mr. Diego Romero-López:

Please consider this notification as confirmation that your manuscript has been received.

We will contact you if we have any concerns or questions regarding your paper's compliance with our submission guidelines. If your paper is compliant, we will simply process your submission and forward it to the Editor-in-Chief for consideration.

As an author, you are responsible for understanding our requirements. For more information, please refer to <http://www2.computer.org/portal/web/peerreviewjournals/author>.

If you find that you have made an error in the submission of your manuscript (eg. Downloaded the wrong file or left out one or more files, etc.), or would like to take advantage of the opportunity to gain further exposure to your paper by submitting supplemental material, relevant to your paper and to the research community, in the form of audio or video multimedia, which is strongly encouraged, please contact me VIA E-Mail at n.cicero@ieee.org. Please do NOT attempt to delete and/or resubmit it into ScholarOne Manuscripts, as this will only produce duplicate entries of the paper.

Please mention the above manuscript ID in all future correspondence or when calling the office for questions. If there are any changes in your street address or e-mail address, please log in to ScholarOne Manuscripts at <https://mc.manuscriptcentral.com/tc-cs> and edit your user information as appropriate.

You can also view the status of your manuscript at any time by checking your Author Center after logging in to <https://mc.manuscriptcentral.com/tc-cs>.

Thank you for submitting your manuscript to IEEE Transactions on Computers.

Sincerely,

Natalie Cicero
IEEE Transactions on Computers
n.cicero@ieee.org

Date Sent: 16-May-2014

6. Problemas abiertos relacionados

- ¿Paralelización de estos árboles? ¿Cómo?
- ¿Es la descomposición de fórmulas lógicas de Boole-Shannon la mejor?
- Técnicas de reducción:
 - Compresión.
 - Uso de propiedades geométricas.
- ¿Qué hacer frente a la *explosión* de estados?

7. Conclusiones

- **DJBDD** es una biblioteca nueva para trabajar con Árboles Binarios de Decisión.
- He desarrollado una herramienta para el uso de BDDs como comprobadores de consistencia.
- Hay dos ejemplos de uso de comprobación de consistencia, uno de ellos real.
- He desarrollado un nuevo algoritmo de reducción de BDDs: Iterative Sifting, cuya publicación está siendo evaluada en el IEEE Transactions on Computers.

8. Bibliografía fundamental

R. E. Bryant. *Symbolic Boolean Manipulation with Ordered Binary Decision Diagrams*, ACM Computing Surveys, 1992.

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.

B. Bollig, I. Wegener. *Improving the Variable Ordering of OBDDs is NP-Complete*, IEEE Transactions on Computers, vol 45, 993-1002. 2005.

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.

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.

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.