Un Vistazo a la Construcción Automática de Modelos

José Alfredo Amor Montaño y
Favio Ezequiel Miranda Perea

Departamento de Matemáticas

Facultad de Ciencias UNAM

Circuito Exterior, Ciudad Universitaria

04510, México D.F., México

jaam@hp.fciencias.unam.mx

favio@abulafia.fciencias.unam.mx

Resumen

Encontrar modelos de teorías es parte importante de la actividad matemática. Con la incorporación de las computadoras a las matemáticas, se han empezado a estudiar métodos algorítmicos para la construcción de modelos, como los basados en la regla de resolución.Un proceso R basado en la regla de resolución es completo si y sólo si al aplicarlo a un conjunto no satisfacible $\mathbb{S}$ de cláusulas, se obtiene entre los elementos del conjunto de salida la cláusula vacía $\square$, que representa contradicción. Si dado un conjunto de cláusulas $\mathbb{S}$ como entrada en un proceso completo éste termina, es decir, la salida es finita, y en $R(\mathbb{S})$ no figura $\square$, entonces necesariamente el conjunto original tiene modelo. Este hecho es la base de la rama de la lógica llamada construcción automática de modelos. Se presenta un proceso particular de construcción automática de modelos para cierta clase de conjuntos de cláusulas. La idea consiste en construir a partir de $R(\mathbb{S})$ un modelo para $\mathbb{S}$ del tipo de los modelos de Herbrand del lenguaje de $\mathbb{S}$.

[0] *Clasificación AMS:* 03C13,03C07,03C15,03C68

1 Introducción

Encontrar e investigar modelos de teorías, es parte importante de la actividad matemática, pero aunque la lógica matemática ha desarrollado un campo extraordinario de conocimiento acerca de los modelos de teorías en lenguajes de primer orden, es muy poco lo que se sabe acerca de métodos algorítmicos para construir modelos.

En tiempos recientes se ha investigado la construcción algorítmica de modelos basados en métodos de demostración de teoremas como son los procedimientos basados en la regla de resolución y refinamientos de ella ([6], [1], [3]). Cada uno de estos autores ha trabajado con diferentes clases decidibles de fórmulas de la lógica de predicados.

Muchas teorías matemáticas se formulan o se pueden formular con lenguajes de predicados con igualdad por medio de conjuntos de enunciados de dichos lenguajes. Por ejemplo la teoría de grupos, la teoría de campos o la teoría de álgebras de Boole son, respectivamente los conjuntos de enunciados formados por sus axiomas y por todos los enunciados que se pueden probar a partir de ellos. Un *modelo* para una teoría es una estructura abstracta, digamos un conjunto con relaciones y/o operaciones y/o objetos distinguidos, respecto a los cuales son verdaderos los enunciados de la teoría. Por ejemplo, dar un modelo (finito) para la teoría de grupos consiste en dar un conjunto (finito), la tabla de la operación y la tabla de los inversos, de modo que se cumplan los axiomas. Veamos ahora por qué es importante la construcción de modelos.

Si T es una teoría (conjunto de enunciados) y φ es un enunciado del mismo lenguaje de T, y que no sabemos si es cierto en la teoría en cuestión, entonces cabe hacerse las siguientes preguntas: ¿se prueba φ a partir de T? o ¿se prueba $\neg\varphi$ a partir de T?. Nótese que es posible que φ no se pruebe a partir de T y que $\neg\varphi$ tampoco se pruebe a partir de T.

Proposición 1 *Si T es una teoría y φ es un enunciado entonces:*

*φ se prueba a partir de T si y sólo si $T \cup \{\neg\varphi\}$ **no** tiene modelo.*

Equivalentemente: φ **no** se prueba a partir de T si y sólo si $T \cup \{\neg\varphi\}$ **sí** tiene modelo.

De lo anterior se sigue que para demostrar que un enunciado φ **no** se puede demostrar a partir de un conjunto de enunciados T es suficiente mostrar un modelo del conjunto $T \cup \{\neg\varphi\}$.

Una literal es una fórmula atómica o una negación de atómica, por ejemplo: $Q(y, a)$, $P(c)$, $\neg P(x)$, son literales. Una *cláusula* es una disyunción finita de literales, por ejemplo: $P(x) \vee \neg Q(y, c) \vee P(a)$, $\neg P(f(a)) \vee Q(x, y)$, son cláusulas; $\square$ denota la cláusula **sin** literales o *cláusula vacía*.

Proposición 2 *Toda fórmula φ se puede transformar a un conjunto de cláusulas $CL(\varphi)$ mediante un procedimiento algorítmico. $CL(\varphi)$ denota la forma clausular de φ.*

Lo anterior se generaliza obviamente a un procedimiento algorítmico para obtener $CL(T)$ a partir de un conjunto de fórmulas T. En razonamiento automático es mucho más conveniente teórica y prácticamente manejar las transformaciones de fórmulas llamadas forma clausular o cláusulas en vez de las fórmulas mismas, con lo cual no se pierde generalidad pues los resultados respecto a tener modelo resultan ser equivalentes.

Teorema 1 *Un conjunto M tiene modelo si y sólo si su forma clausular $CL(M)$ correspondiente a M, tiene modelo.*

De todo lo anterior se sigue como corolario que: si T es una teoría o conjunto de enunciados y φ es un enunciado, entonces

φ **no** se prueba a partir de T si y sólo si $CL(T \cup \{\neg\varphi\})$ **sí** tiene modelo.

Así pues, de lo antes dicho se tiene que como procedimiento para probar que un enunciado φ **no** se puede demostrar a partir de un conjunto de enunciados T, es suficiente mostrar o construir un modelo del conjunto de cláusulas $CL(T \cup \{\neg\varphi\})$.

De aquí en adelante hablaremos siempre de cláusulas y nuestro interés será decidir si un conjunto de cláusulas tiene modelo, es decir, si es satisfacible y la construcción de modelos para conjuntos satisfacibles de cláusulas. Esto se puede asegurar para ciertas clases de cláusulas como las llamadas BS (Bernays-Schonfinkel), de Horn, PVD (Variable Positiva Dominada), entre otras. Nosotros trabajaremos sólo con la clase PVD.

2 Hiperresolución

Si L es una literal entonces L^c denota la literal "de signo contrario"; es decir, si $L = P$ entonces $L^c = \neg P$ y si $L = \neg P$ entonces $L^c = P$.

Definición 1 (Robinson) Si C y D son cláusulas con variables ajenas, L y M son literales de C y D respectivamente tales que $\{L^c, M\}$ es unificable por el unificador más general μ, entonces $E = (C-L)\mu \vee (D-M)\mu$ es un *resolvente* de C y D. Esquemáticamente:

$$\frac{C \quad D}{(C-L)\mu \vee (D-M)\mu} \quad (\mu \text{ es el umg de } \{L^c,\ M\})$$

Ejemplo 1 Si $C = Q(x,b) \vee P(z,a)$ y $D = \neg Q(a,w) \vee R(w,b)$ entonces $E = P(z,a) \vee R(b,b)$ es un resolvente de C, D, el umg es $\mu = \{x/a, w/b\}$. Esquemáticamente:

$$\frac{Q(x,b) \vee P(z,a) \quad \neg Q(a,w) \vee R(w,b)}{P(z,a) \vee R(b,b)} \quad \mu = \{x/a, w/b\} \text{ es el umg de } \{Q(x,b)^c,\ \neg Q(a,w)\}.$$

Ejemplo 2 Si $C = P(b) \vee R(f(a))$ y $D = \neg P(y) \vee \neg Q(g(y))$ entonces el resolvente bajo $\mu = \{y/b\}$ es $E = R(f(a)) \vee \neg Q(g(b))$. Esquemáticamente:

$$\frac{P(b) \vee R(f(a)) \quad \neg P(y) \vee \neg Q(g(y))}{R(f(a)) \vee \neg Q(g(b))} \quad \mu = \{y/b\} \text{ es el umg de } \{P(b)^c,\ \neg P(y)\}.$$

La regla de *hiperresolución* es una macroinferencia basada en la regla de resolución, cuyo objetivo es producir una cláusula positiva (llamada hiperresolvente) a partir de una sucesión Γ de varias cláusulas, una de ellas negativa[1] o mixta (llamada núcleo) y todas las demás positivas (llamadas satélites o electrones). En la cláusula núcleo (negativa o mixta) se resuelve primero la literal negativa de la extrema derecha.

Ejemplo 3 Núcleo: $Padre(y,z) \vee \neg Madre(x,z) \vee \neg Casado(x,y)$
Satélite1: $Casado(Tere, Pedro) \vee Masviejo(Tere, Pedro)$
Satélite2: $Madre(Tere, Sergio)$
Hiperresolvente: $Padre(Pedro, Sergio) \vee Masviejo(Tere, Pedro)$

[1]Una cláusula es negativa si todas sus literales son negativas, es positiva si todas sus literales son positivas. Es mixta en otro caso.

El unificador es $\mu = \{x/Tere,\ y/Pedro,\ z/Sergio\}$.

Un operador de refinamiento de resolución R_x puede pensarse como una máquina que recibe como entrada un conjunto de cláusulas y da como salida toda la información que se pueda obtener de él mediante alguna inferencia basada en resolución.

Definición 2 Un operador de refinamiento de resolución R_x es *completo* si para cualquier conjunto de cláusulas $\mathbb{S}$, $\mathbb{S}$ es satisfacible si y sólo si $\Box \notin R(\mathbb{S})$.

La idea para la construcción de modelos, basada en refinamientos de resolución (como hiperresolución), es la siguiente: dado un conjunto de cláusulas $\mathbb{S}$ y un operador de refinamiento de resolución R_x que sea completo, calcular $R_x(\mathbb{S})$; si la cláusula vacía pertenece a $R_x(\mathbb{S})$, es decir, $\Box \in R_x(\mathbb{S})$, entonces $\mathbb{S}$ no puede tener modelo (es **no** satisfacible). Este tipo de resultados así como su decidibilidad efectiva ha sido estudiado con gran detalle dentro del razonamiento automático, véase por ejemplo [5]. Por otra parte, si $\Box \notin R_x(\mathbb{S})$ por la completud se sigue que $\mathbb{S}$ sí tiene modelo (es satisfacible). La construcción automática de modelos parte de este hecho y tiene como meta principal obtener a partir de $R_x(\mathbb{S})$ un modelo de $\mathbb{S}$.

Con $\rho_H(\mathbb{S})$ denotamos al conjunto de todos los hiperresolventes posibles del conjunto de cláusulas $\mathbb{S}$.

Ejemplo 4 *Sea* $\mathbb{S} = \{Pa \vee Sa,\ Qa \vee Ra,\ Px \vee Qx \vee \neg Rx \vee \neg Sx,\ \neg Pa \vee \neg Qa\}$

$\Gamma_1 = (Px \vee Qx \vee \neg Rx \vee \neg Sx;\ Pa \vee Sa,\ Qa \vee Ra)$
El hiperresolvente de Γ_1 es $Pa \vee Qa$.
$\Gamma_2 = (\neg Pa \vee \neg Qa;\ Qa \vee Ra,\ Pa \vee Sa)$
El hiperresolvente de Γ_2 es $Ra \vee Sa$.
Dado que no hay más hiperresolventes, entonces $\rho_H(\mathbb{S}) = \{Pa \vee Qa,\ Ra \vee Sa\}$.

Definición 3 El *operador de hiperresolución* R_H se define por recursión usando iteradamente la operación ρ_H.

$$R_H^0(\mathbb{S}) = \mathbb{S} \qquad R_H^{n+1}(\mathbb{S}) = R_H^n(\mathbb{S}) \cup \rho_H(R_H^n(\mathbb{S}))$$

$R_H(\mathbb{S}) = \cup_{n\in\mathbb{N}} R_H^n(\mathbb{S})$

Decimos que una cláusula C se deriva de $\mathbb{S}$ con hiperresolución si $C \in R_H(\mathbb{S})$. El operador de hiperresolución R_H es *completo* en el sentido ya dicho de que para cualquier conjunto $\mathbb{S}$ de cláusulas, $\mathbb{S}$ es satisfacible si y sólo si $\square \notin R_H(\mathbb{S})$. Véase [5].

Para definir el operador de *hiperresolución con reemplazo* necesitamos antes definir la relación de *subsunción* entre cláusulas.

Definición 4 Sean C, D cláusulas, decimos que C *subsume a* D si hay una sustitución σ tal que $Lit(C)\sigma \subseteq Lit(D)$. Es decir, si todas las literales de C bajo σ se convierten en literales de D.

Ejemplo 5 $Q(x)$ subsume a $Q(c) \vee R(y)$
$Q(a) \vee R(y)$ subsume a $P(x) \vee Q(a) \vee R(c)$
$P(x) \vee P(f(x))$ subsume a $P(f(y)) \vee P(f(f(y)))$

Intuitivamente una cláusula subsume a otra cuando contiene ya toda la información de una parte de la otra por lo que, siendo disyunciones las cláusulas, la implica lógicamente. Obsérvese también que la subsunción es una relación transitiva. Así, la relación de subsunción permite eliminar cláusulas redundantes que son las cláusulas subsumidas por otra. Esto permite tener un *operador de subsunción Sub* para conjuntos de cláusulas, de modo que si $\mathbb{S}$ es un conjunto de cláusulas, $Sub(\mathbb{S})$ es un subconjunto de $\mathbb{S}$ en el que se eliminaron todas las cláusulas subsumidas por otras. Obsérvese que todo modelo de $\mathbb{S}$ es también modelo de $Sub(\mathbb{S})$ e inversamente.

Definición 5 Si $\mathbb{S}$ es un conjunto de cláusulas, la *sucesión de reemplazo* a partir de $\mathbb{S}$ está definida así:

$$S^0_{H_r}(\mathbb{S}) = Sub(\mathbb{S}) \qquad\qquad S^{n+1}_{H_r}(\mathbb{S}) = Sub[S^n_{H_r}(\mathbb{S}) \cup \rho_H(S^n_{H_r}(\mathbb{S}))]$$

Obsérvese que para todo n, todo modelo de $\mathbb{S}$ es también modelo de $S^n_{H_r}(\mathbb{S})$ e inversamente. También hay que observar que como el operador de subsunción, en general "reduce" y el de hiperresolución, en general "aumenta" cláusulas, y la sucesión $< S^n_{H_r}(\mathbb{S}) >_{n\in\mathbb{N}}$ de hiperresolución con reemplazo es una mezcla de ambos, entonces no es monótona creciente ni decreciente, sin embargo en ciertos casos que nos interesan, converge.

Definición 6 Una sucesión de reemplazo $< S^n_{H_r}(\mathbb{S}) >_{n\in\mathbb{N}}$ *converge* si hay $k \in \mathbb{N}$ tal que $S^{k+1}_{H_r}(\mathbb{S}) = S^k_{H_r}(\mathbb{S})$. En tal caso el límite es $S^k_{H_r}(\mathbb{S})$ y se denota con $R_{H_r}(\mathbb{S})$. En otro caso, la sucesión es *divergente*.

El operador de resolución con reemplazo es completo en el siguiente sentido:

Teorema 2 *Si $\mathbb{S}$ es un conjunto no satisfacible de cláusulas entonces su sucesión de reemplazo converge y el límite $R_{H_r}(\mathbb{S}) = \{\Box\}$.*

Sin embargo en el caso de que $\mathbb{S}$ sea satisfacible, la sucesión de reemplazo puede converger o no como lo muestran los siguientes ejemplos:

Ejemplo 6 *Si $\mathbb{S} = \{Px \vee Qx,\ Px \vee \neg Qx,\ Qx \vee \neg Px\}$ entonces $\mathbb{S}$ es satisfacible y su sucesión de reemplazo es:*

$$\mathbb{S},\ \{Px,\ Qx\},\ \{Px,\ Qx\},\ \ldots\ .$$

que es convergente.

Ejemplo 7 *Si $\mathbb{S} = \{Pa,\ Pfx \vee \neg Px\}$ entonces $\mathbb{S}$ es satisfacible y su sucesión de reemplazo es:*

$$\mathbb{S},\ \mathbb{S} \cup \{Pfa\},\ \mathbb{S} \cup \{Pfa,\ Pf^2a\},\ \ldots\ .$$

que es divergente pues $Pf^ka \in S^k_{H_r}(\mathbb{S}) - S^{k-1}_{H_r}(\mathbb{S})$ para $k > 0$.

3 La clase PVD

Definición 7 Un conjunto de cláusulas $\mathbb{S}$ *pertenece a la clase PVD (Variable Positiva Dominada)* si y sólo si para toda cláusula C en $\mathbb{S}$ se cumple lo siguiente:

PVD1) $Var(C^+) \subseteq Var(C^-)$

PVD2) Para toda x en $Var(C^+)$: $\tau_{\max}(x, C^+) \leq \tau_{\max}(x, C^-)$. Esto significa que la complejidad de la parte positiva es menor que la de la parte negativa en toda cláusula de $\mathbb{S}$.

Ejemplo 8 *El conjunto* $\mathbb{S} = \{E(a) \vee S(a),\ Q(a) \vee R(a),\ P(x) \vee Q(x) \vee \neg R(x) \vee \neg S(x),\ \neg P(a) \vee \neg Q(a)\}$ *pertenece a* PVD*.*

El conjunto $\mathbb{S} = \{P(z) \vee Q(g(z), z),\ R(f(z, w)),\ P(a),\ R(x, y) \vee \neg Q(y)\}$ *no pertenece a* PVD *pues hay cláusulas positivas con variables y la cláusula* $R(x, y) \vee \neg Q(y)$ *viola la condición* $PVD1$*).*

Obsérvese que toda cláusula positiva en un conjunto PVD, es cerrada pues no puede tener variables ya que no hay parte negativa.

Teorema 3 *Hiperresolución decide la clase* PVD*. Es decir, si* $\mathbb{S} \in PVD$ *entonces el conjunto* $R_H(\mathbb{S})$ *es finito. Esto último significa que el operador termina y se puede decidir si tiene a la cláusula vacía o no, y por lo tanto si* $\mathbb{S}$ *tiene modelo o no.*

Lema 1 *Para cualquier* $\mathbb{S} \in PVD$*, la sucesión* $\langle S^n_{H_r}(\mathbb{S})\rangle_{n \in \mathbb{N}}$ *converge.*

4 Modelos de Herbrand

Si $\mathbb{S}$ es un conjunto de cláusulas, una *interpretación de Herbrand para* $\mathbb{S}$ es un subconjunto cualquiera H del conjunto de todas las instancias cerradas de los átomos que figuran en las cláusulas de $\mathbb{S}$, con el lenguaje de $\mathbb{S}$. El significado intuitivo intencional es de que las instancias atómicas que pertenecen a H son verdaderas y las del complemento de H son falsas. Esta interpretación se extiende de modo natural para las literales y las cláusulas.

Definición 8 Un *modelo de Herbrand para* $\mathbb{S}$ es una interpretación de Herbrand para $\mathbb{S}$, respecto a la cual todas las cláusulas de $\mathbb{S}$ son verdaderas.

Un resultado básico es el que afirma que para cláusulas, tener un modelo y tener un modelo de Herbrand resulta equivalente.

Teorema 4 *Para cualquier conjunto $\mathbb{S}$ de cláusulas, $\mathbb{S}$ tiene un modelo si y sólo $\mathbb{S}$ si tiene un modelo de Herbrand.*

Así los modelos que se construyen son modelos de Herbrand que además son fáciles de manejar sintácticamente, por lo que de aquí en adelante sólo hablaremos de este tipo de modelos.

5 Representaciones Atómicas de modelos de Herbrand

Lo que se quiere hacer es dar un procedimiento que construya modelos de conjuntos de cláusulas, pero esto en realidad es un abuso de lenguaje; lo que se hace realmente es dar un procedimiento que proporciona una descripción formal o representación de un modelo de Herbrand del conjunto de cláusulas. Para ello veremos primero lo que es una *representacion atómica* de un modelo de Herbrand.

Definición 9 Un conjunto cualquiera de átomos A es una *representación atómica* del conjunto $IC(A)$ de todas las instancias cerradas de A.

Este conjunto $IC(A)$ de instancias cerradas de A, es claramente un modelo de Herbrand.

Ejemplo 9 Sea el conjunto de cláusulas $\mathbb{S} = \{P(f(a)),\ P(x) \vee P(f(x)),\ \neg P(a)\}$. Entonces $H = \{P(f(t)) \ / \ t \in H(\mathbb{S})$[2]$\}$ es un modelo de Herbrand de $\mathbb{S}$. El conjunto $A = \{P(f(x))\}$ es claramente una representacion atómica del modelo H.

Hay modelos de Herbrand que son únicos, por ejemplo si $\mathbb{S}' = \{P(f(a)),\ P(x) \vee P(f(x)),\ \neg P(a),\ \neg P(x) \vee \neg P(f(x))\}$ entonces

$$H' = \{P(f^{2n+1}(a)) \ / \ n \geq 0\}$$

es el único modelo de Herbrand de $\mathbb{S}'$.

[2] $H(\mathbb{S})$ denota al conjunto de todos los términos sin variables del lenguaje de $\mathbb{S}$, conocido como Universo de Herbrand de $\mathbb{S}$.

6 Un caso sencillo: cláusulas de Horn

Las cláusulas de Horn son las cláusulas en las que figura a lo más una literal positiva. Ejemplos de cláusulas de Horn son todas las cláusulas negativas y todas las cláusulas positivas unitarias. Otras cláusulas de Horn son $Pa \vee \neg Qx$, $Qy \vee \neg Pz \vee \neg Rc$.

Teorema 5 *Sea $\mathbb{S}$ un conjunto satisfacible de cláusulas de Horn. Entonces $R_H^+(\mathbb{S})$ es una representación atómica de un modelo de Herbrand de $\mathbb{S}$.*

Ejemplo: $\mathbb{S} = \{Pa, Qb, Rb, Pd, \neg Qd, \neg Rd, Px \vee \neg Rx\}$
$\rho_H(\mathbb{S}) = \{Pb\}$
$R_H^1(\mathbb{S}) = \mathbb{S} \cup \rho_H(\mathbb{S})$ y como $\mathbb{S} \cup \rho_H(\mathbb{S})$ no produce hiperresolventes nuevos, entonces
$R_H(\mathbb{S}) = \{Pa, Qb, Rb, Pd, Pb, \neg Qd, \neg Rd, Px \vee \neg Rx\}$
y entonces $R_H^+(\mathbb{S}) = \{Pa, Qb, Rb, Pd, Pb\}$ es un modelo de Herbrand para $\mathbb{S}$.

7 Conjuntos estables

Definición 10 Sea $\mathbb{S}$ un conjunto de cláusulas. Se dice que $\mathbb{S}$ es *estable* si y sólo si $\mathbb{S} = Sub[\mathbb{S} \cup \rho_H(\mathbb{S})]$

Intuitivamente un conjunto estable es aquel que ya no genera información, puesto que los hiperresolventes que genera o bien ya le pertenecían o bien se subsumen por cláusulas que ya figuraban en él.

¿Cómo generar conjuntos estables?, una respuesta la proporciona el siguiente lema:

Lema 2 *Sea $\mathbb{S}$ un conjunto de cláusulas. Si $\langle S_{H_r}^n(\mathbb{S})\rangle_{n\in\mathbb{N}}$ converge, entonces el límite $R_{Hr}(\mathbb{S})$ es un conjunto estable.*

Obsérvese que las definiciones de límite de una sucesión de reemplazo y de conjunto estable, son suficientes para la afirmación de este lema.

8 Construcción de Representaciones Atómicas

Para explicar el proceso de construcción de modelos que nos interesa presentar, daremos dos operadores más usando los operadores anteriores, así como una serie de lemas que determinan sus propiedades.

Lema 3 *Sean $\mathbb{S}$ un conjunto finito de cláusulas* ***no*** *positivas y $\mathbb{A}$ un conjunto finito de átomos, tales que $\mathbb{S} \cup \mathbb{A}$ es satisfacible y estable. Entonces $\mathbb{A}$ es una representación atómica de un modelo de Herbrand de $\mathbb{S} \cup \mathbb{A}$.*

Este lema sugiere el siguiente proceso de construcción de modelos: dado un conjunto finito y satisfacible de cláusulas $\mathbb{S}$, obtener $R_{Hr}(\mathbb{S})$ que es estable. Luego construir un conjunto finito de átomos $\mathbb{A}$ tal que[3] $NP(R_{Hr}(\mathbb{S})) \cup \mathbb{A}$ sea finito, satisfacible, estable y además implique lógicamente a $R_{Hr}(\mathbb{S})$. En tal caso, $\mathbb{A}$ es una representación atómica de un modelo de Herbrand de $\mathbb{S}$.

La transformación de un conjunto $\mathbb{S}$ hacia un conjunto cuyas cláusulas positivas son todas unitarias, se sirve de un operador α que selecciona, de manera determinista una cláusula positiva no unitaria $D \in \mathbb{S}$, una literal P en D y reemplaza a $\mathbb{S}$ con $(\mathbb{S} - \{D\}) \cup \{P\}$. Esto es:

$$\alpha(\mathbb{S}) = (\mathbb{S} - \{D\}) \cup \{P\}$$
$$\alpha(\mathbb{S}) = \mathbb{S} \text{ si todas las cláusulas positivas de } \mathbb{S} \text{ ya son unitarias.}$$

El siguiente lema es de gran importancia para transformar un conjunto estable en un conjunto equivalente que también es estable y donde las cláusulas positivas son unitarias.

Lema 4 *Sea $\mathbb{S} \in PVD$ un conjunto satisfacible y estable. Entonces*

a) $\alpha(\mathbb{S})$ *es satisfacible.*

b) Todo modelo de $\alpha(\mathbb{S})$ *es modelo de* $\mathbb{S}$.

[3] NP abrevia "la parte *N*o *P*ositiva de ..."

Para a) es necesaria la estabilidad de $\mathbb{S}$, pues por ejemplo $\mathbb{S} = \{P(a) \vee P(b),\ \neg P(b)\}$ es satisfacible pero no estable y $\alpha(\{P(a) \vee P(b), \neg P(b)\}) = \{P(b),\ \neg P(b)\}$ que no es satisfacible. El inciso b) es inmediato.

Desafortunadamente, dado un conjunto estable, la transformación $\alpha(\mathbb{S})$ no necesariamente nos da un conjunto estable, de manera que tenemos que hacer una reducción para obtener el siguiente conjunto estable, esto se hace con la ayuda del operador T.

El operador T se define sobre conjuntos estables de cláusulas de PVD como sigue:

$$T(\mathbb{S}) = R_{Hr}(\alpha(\mathbb{S}))$$

La iteración de T se define de la manera usual:

$$T^0(\mathbb{S}) = \mathbb{S}$$
$$T^{n+1}(\mathbb{S}) = T(T^n(\mathbb{S}))$$

Lema 5 *Sea $\mathbb{S}$ en PVD. La iteración de T tiene las siguientes propiedades:*

a) $T^n(\mathbb{S})$ es estable.

b) $T^n(\mathbb{S}) \in PVD$.

c) $T^n(\mathbb{S})$ es satisfacible.

d) Todo modelo de $T^n(\mathbb{S})$ es un modelo de $\mathbb{S}$.

Teorema 6 *Sea $\mathbb{S} \in PVD$ un conjunto estable y satisfacible de cláusulas. La sucesión $\langle T^n(\mathbb{S})\rangle_{n\in\mathbb{N}}$ converge a un conjunto de cláusulas D tal que D^+ es una representación atómica de un modelo de Herbrand de $\mathbb{S}$.*

9 Un ejemplo final

Sea $\mathbb{S} = \{E(a) \vee S(a),\ Q(a) \vee R(a),\ P(x) \vee Q(x) \vee \neg R(x) \vee \neg S(x),\ \neg P(a) \vee \neg Q(a)\}$.

Tenemos que $\Gamma = (\ P(x) \vee Q(x) \vee \neg R(x) \vee \neg S(x);\ E(a) \vee S(a),\ Q(a) \vee R(a))$ produce el hiperresolvente $Ea \vee Pa \vee Qa$.

De hecho se tiene que $\rho_H(\mathbb{S}) = \{Ea \vee Pa \vee Qa\}$ y como esta cláusula no es subsumida por ninguna otra de $\mathbb{S}$ entonces $\mathbb{S}$ no es estable. Calculamos la sucesión de reemplazo:

$S^0_{H_r}(\mathbb{S}) = \mathbb{S}$

$S^1_{H_r}(\mathbb{S}) = sub(\mathbb{S} \cup \rho_H(\mathbb{S})) = \mathbb{S} \cup \{Ea \vee Pa \vee Qa\}$.

$(\neg Pa \vee \neg Qa;\, Qa \vee Ra,\, Ea \vee Pa \vee Qa)$ produce el único hiperresolvente nuevo que es $Ea \vee Qa \vee Ra$.

Por lo tanto $\rho_H(S^1_{H_r}(\mathbb{S})) = \{Ea \vee Pa \vee Qa,\, Ea \vee Qa \vee Ra\}$ y como $Qa \vee Ra$ subsume a $Ea \vee Qa \vee Ra$ entonces tenemos que:

$S^2_{H_r}(\mathbb{S}) = sub(S^1_{H_r}(\mathbb{S}) \cup \rho_H(S^1_{H_r}(\mathbb{S}))) = \mathbb{S} \cup \{Ea \vee Pa \vee Qa\}$. Por lo tanto $R_{H_r}(\mathbb{S}) = \mathbb{S} \cup \{Ea \vee Pa \vee Qa\}$.

Así que el conjunto $\mathbb{S}_1 = R_{H_r}(\mathbb{S})$ es estable y satisfacible. Además cualquier modelo de $\mathbb{S}_1$ es modelo de $\mathbb{S}$, por lo que nos dedicamos a buscar un modelo de $\mathbb{S}_1$ mediante la iteración del operador T.

$\alpha(\mathbb{S}_1) = (\mathbb{S}_1 - \{Ea \vee Sa\}) \cup \{Sa\} = \{Sa,\, Qa \vee Ra,\, Ea \vee Pa \vee Qa,\, Px \vee Qx \vee \neg Rx \vee \neg Sx,\, \neg P(a) \vee \neg Q(a)\}$

$\rho_H(\alpha(\mathbb{S}_1)) = \{Pa \vee Qa,\, Ea \vee Qa \vee Ra\}$.

$S^1_{H_r}(\alpha(\mathbb{S}_1)) = sub(\alpha(\mathbb{S}_1) \cup \rho_H(\alpha(\mathbb{S}_1))) = sub(\{Sa,\, Qa \vee Ra,\, Ea \vee Pa \vee Qa,\, Px \vee Qx \vee \neg Rx \vee \neg Sx,\, \neg P(a) \vee \neg Q(a)\} \cup \{Pa \vee Qa,\, Ea \vee Qa \vee Ra\}$

$= \{Sa,\, Qa \vee Ra,\, Pa \vee Qa,\, P(x) \vee Q(x) \vee \neg R(x) \vee \neg S(x),\, \neg P(a) \vee \neg Q(a)\}$

$\rho_H(S^1_{H_r}(\alpha(\mathbb{S}_1))) = \{Qa \vee Ra,\, Qa \vee Pa\}$ entonces $S^2_{H_r}(\alpha(\mathbb{S}_1)) = S^1_{H_r}(\alpha(\mathbb{S}_1))$.

Así que $R_{H_r}(\alpha(\mathbb{S}_1)) = S^1_{H_r}(\alpha(\mathbb{S}_1))$ y

$\mathbb{S}_2 = T(\mathbb{S}_1) = R_{H_r}(\alpha(\mathbb{S}_1)) = \{Sa,\, Qa \vee Ra,\, Pa \vee Qa,\, P(x) \vee Q(x) \vee \neg R(x) \vee \neg S(x),\, \neg P(a) \vee \neg Q(a)\}$.

Ahora calculamos $T(\mathbb{S}_2)$

$\alpha(\mathbb{S}_2) = (\mathbb{S}_2 - \{Pa \vee Qa\}) \cup \{Qa\}$.

$\rho_H(\alpha(\mathbb{S}_2)) = \{Pa \vee Qa\}$.

$S^1_{H_r}(\alpha(\mathbb{S}_2)) = sub(\{Sa,\, Qa \vee Ra,\, Qa,\, P(x) \vee Q(x) \vee \neg R(x) \vee \neg S(x),\, \neg P(a) \vee \neg Q(a)\} \cup \{Pa \vee Qa\})$

$= \{Sa,\, Qa,\, P(x) \vee Q(x) \vee \neg R(x) \vee \neg S(x),\, \neg P(a) \vee \neg Q(a)\}$

$\rho_H(S^1_{H_r}(\alpha(\mathbb{S}_2))) = \phi$ entonces $S^2_{H_r}(\alpha(\mathbb{S}_2)) = S^1_{H_r}(\alpha(\mathbb{S}_2))$.

Así que $R_{H_r}(\alpha(\mathbb{S}_2)) = S^1_{H_r}(\alpha(\mathbb{S}_2))$ y

$\mathbb{S}_3 = T(\mathbb{S}_2) = T^2(\mathbb{S}_1) = R_{H_r}(\alpha(\mathbb{S}_2)) = \{Sa,\, Qa,\, P(x) \vee Q(x) \vee \neg R(x) \vee \neg S(x),\, \neg P(a) \vee \neg Q(a)\}$.

Claramente se tiene que $\alpha(\mathbb{S}_3) = \mathbb{S}_3$ y como $\mathbb{S}_3$ es estable entonces $T(\mathbb{S}_3) = \mathbb{S}_3$.

Por lo tanto la sucesión $< T^n(\mathbb{S}_1) >$ converge a $\mathbb{S}_3$ y el modelo deseado es la parte positiva de $\mathbb{S}_3$, $\mathbb{S}_3^+ = \{Sa, Qa\}$.

Bibliografía

[1] R. Caferra, N. Zabel, A Method for Simultaneous Search for Refutations and Models by Equational Constraint Solving. Journal of Symbolic Computation **13**, 613-641. 1992.

[2] A. Leitsch, The Resolution Calculus, Springer Verlag, 1997.

[3] C. G. Fermüller and A. Leitsch, Hyperresolution and Automated Model Building. Journal of Logic and Computation **6**(2), 173-203. 1996

[4] C. G. Fermüller and A. Leitsch, Resolution Decision Procedures. En Handbook of Automated Reasoning, Ed. A. Robinson y A. Voronkov, 1999.

[5] F. E. Miranda P., Fundamentos Lógicos del Programa de Razonamiento Automático OTTER, Tesis de Maestría, UNAM, 1999.

[6] T. Tammet, Using resolution for deciding solvable classes and building finite models. Lecture Notes in Computer Science **502** 33-64. Springer Verlag 1991.