La Completud de Paramodulación con RFP-Resolución

Favio Ezequiel Miranda Perea
fmiranda@mealy.fciencias.unam.mx
Facultad de Ciencias
Universidad Nacional Autónoma de México
Circuito Exterior S/N, Ciudad Universitaria
04510 México D.F.
México.

Resumen

Se presenta una prueba de completud refutacional de la combinación de la regla de paramodulación con RFP-resolución para la lógica clausular con igualdad.

1 Introducción

El manejo de la igualdad dentro del razonamiento automático ha sido y continua siendo un gran reto, actualmente una de las reglas más poderosas para manejar la igualdad es la *paramodulación*, que en combinación con la regla de *resolución* de Alan Robinson, o alguno de sus refinamientos, proporciona completud refutacional para la lógica clausular con igualdad.

En 1969 Larry Wos y George Robinson presentaron la paramodulación ([Wos y Robinson, 1969]) y un año después probaron la completud de paramodulación con resolución ([Wos y Robinson, 1970]), sin embargo dicha prueba está condicionada a tener que agregar al conjunto original de cláusulas, aquellas llamadas *axiomas funcionales reflexivos*, que son las cláusulas de la forma $f(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)$ para cada símbolo de función n-ario f, del lenguaje en uso.

En 1975, Brand eliminó esta condición ([Brand, 1975]) mediante el llamado *método de modificación*, sin embargo su manera de probar la completud incluye ciertas restricciones en la manera de aplicar la resolución, restricciones que resultan artificiales en el sentido de que utilizan el concepto particular de *socio*, el cual se explicará más adelante. Lo que se hace en este trabajo es utilizar, en lugar de dichas reglas particulares, la regla de *RFP-resolución* que sirve de base para la regla de hiperresolución que resulta ser una macroinferencia de gran utilidad en programas de razonamiento automático.

2 ¿Por qué otra prueba de completud?

Desde la prueba de completud presentada en [Brand, 1975] han aparecido otras pruebas de completud de resolución y paramodulación, una breve historia puede hallarse en [Plaisted, 1994]. La prueba que presento en este artículo resulta ser un caso particular de la prueba de [Bachmair *et al.*, 1995]. La pregunta que surge de inmediato es ¿por qué tiene interés esta prueba de completud? si bien esta prueba no es novedosa para el ámbito de la investigación, la importancia y valor que le doy es la de simplicidad, respecto al nivel de conocimientos necesarios para entenderla. El lector sólo necesita conocer, a parte de la lógica básica involucrada, la regla de resolución.

La importancia de la paramodulación dentro del razonamiento automático obliga a comprender correctamente, desde las primeras etapas de estudio, su funcionamiento y la completud refutacional que proporciona al combinarse con resolución. Considero que este artículo es un buen punto de partida para lograr tal objetivo.

Las pruebas más recientes, aunque utilizan métodos más eficientes, también se sirven de un nivel más avanzado de conocimientos para su desarrollo. Por ejemplo, las pruebas de [Bachmair *et al.*, 1995; Peterson, 1983], utilizan el concepto de *orden de terminación* y *árboles semánticos*, en contraste la prueba que presento es esencialmente sintáctica. Otras pruebas necesitan conceptos más complicados como la de [Hsiang y Rusinowitch, 1991] que se desarrolla mediante *árboles semánticos transfinitos*.

Para una visión general de demostración automática basada en paramodulación véase [Nieuwenhuis y Rubio, 1999].

3 Preliminares

Se supone un conocimiento de la lógica clausular con igualdad, en particular se deben conocer la regla de resolución con factorización, los conceptos de variante, factor, unificador más general (*umg*), el concepto de equisatisfacibilidad ($\sim_{sat}$), las nociones de cláusula positiva, negativa, el conjunto $V(C)$ de variables de una cláusula C y el conjunto de instancias cerradas de un conjunto de cláusulas $\mathcal{S}$, denotado $IC(\mathcal{S})$.

Con $\mathcal{A}$ denotamos a la siguiente forma débil del axioma de transitividad: $x \neq y \vee x \neq z \vee y = z$, $\Box$ es la cláusula vacía mientras que $\equiv$ denota a la igualdad en la metateoría.

El fin de una demostración se denota con "$\dashv$".

Cualquier duda puede aclararse en [Amor y Miranda, 1998; Miranda, 1999].

Definición 3.1 Si C es una cláusula de la forma $C_1 \vee C_2$ tal que C_1 es positiva y C_2 es negativa, (alguna o ambas podrían ser $\square$) entonces decimos que C está en *PN-forma.* C_1 (C_2) se llama la parte positiva (negativa) de C.

3.1 RFP-Resolución

La regla de RFP-resolución es una forma especial de resolución que condiciona la forma en que ésta puede operar.

Definición 3.2 Sean C, D dos PN-cláusulas tal que D es positiva y C es de la forma $C' \vee \neg Q$ donde Q es un átomo. Sea D' una variante de un factor de D tal que $V(D') \cap V(C) = \emptyset$ y $D' = D_1 \vee P \vee D_2$ donde P es un átomo. Supongase que $\{P, Q\}$ es unificable mediante el umg σ. Entonces $(D_1 \vee D_2 \vee C')\sigma$ es un *RFP-resolvente* (Restricción a Factores Positivos) de C y D.

Obsérvese que cada RFP-resolvente es también un resolvente ordinario en PN-forma (resolviendo D desde la izquierda). La factorización esta restringida a cláusulas positivas y la regla de resolución solo puede aplicarse a la literal que está más a la derecha en la cláusula no positiva.

Ejemplo 3.1 Sea $S = \{C_1, C_2, C_3, C_4\}$ donde $C_1 = P(x) \vee P(y), C_2 = P(x) \vee \neg R(x), C_3 = \neg R(x) \vee \neg R(y) \vee \neg P(x), C_4 = R(b)$.
Los resolventes $\neg R(x) \vee \neg R(y)$ y $P(v) \vee \neg R(x) \vee \neg R(y)$ son RFP-resolventes de C_1 y C_3.
$\neg R(x) \vee \neg R(u) \vee \neg R(v)$ es un resolvente de C_2 y C_3 pero no es un RFP-resolvente, puesto que ni C_2 ni C_3 son positivas.
$\neg R(x)$ es un resolvente de C_1 y C_3, pero no es un RFP-resolvente, pues se ha aplicado la factorización a una cláusula no positiva.
$\neg P(b)$ es un resolvente de C_3 y C_4 pero no es un RFP-resolvente puesto que la literal eliminada en la cláusula no positiva no es la que está más a la derecha. Obsérvese que no hay RFP-resolventes de C_3 y C_4.

Teorema 3.1 (Completud de la RFP-Resolución)
Si $\mathcal{S}$ es un conjunto no satisfacible de cláusulas entonces existe una refutación de $\mathcal{S}$ mediante RFP-resolución.

Demostración:
La prueba se basa en técnicas de levantamiento (*lifting*) y es consecuencia de diversos resultados de [Miranda, 1999] $\dashv$

3.2 Paramodulación

Paramodulación es una generalización de la regla de sustitución de iguales en el sentido de que combina en un solo paso la búsqueda de una sustitución que permite un reemplazo de igualdad con el reemplazo en si mismo. Mientras otras reglas de inferencia tienen como principal actor a las literales, la paramodulación es una regla orientada hacia los términos.
La regla de paramodulación es la siguiente:

$$\frac{u = v \vee C \quad D[s]}{(C \vee D[v])\sigma}$$

donde la notación $D[s]$ distingue una presencia del término s en la cláusula D y σ es un umg de $\{s, u\}$. Dentro de las premisas la cláusula con la igualdad se llama *cláusula origen* o "desde" y la otra se llama *cláusula destino* o "hacia"; la conclusión se llama *paramodulante.* Veamos algunos ejemplos:

Ejemplo 3.2

$$\frac{a = b \vee R(b) \quad P(a) \vee Q(b)}{R(b) \vee P(b) \vee Q(b)}$$

en este caso el término distinguido es a y el unificador es $\sigma = \emptyset$.

Ejemplo 3.3

$$\frac{f(g(b)) = a \vee R(g(c)) \quad P(g(f(x))) \vee Q(x)}{R(g(c)) \vee P(g(a)) \vee Q(g(b))}$$

aquí el término distinguido es $f(x)$ y el unificador es $\sigma = \{x/g(b)\}$.

Ejemplo 3.4 Mediante el umg $\sigma = \{z/g(y), x/h(g(y))\}$ se tiene la siguiente instancia de paramodulación

$$Q(g(a)) \vee f(h(z), z) = g(z)$$

$$\frac{\neg P(f(x, g(y))) \vee k(x, g(y)) = h(y)}{Q(g(a)) \vee \neg P(g(g(y))) \vee k(h(g(y)), g(y)) = h(y)}$$

La razón por la que se necesitan los axiomas funcionales reflexivos en la prueba de completud de [Wos y Robinson, 1970] es su importancia en las técnicas de levantamiento (*lifting*) involucradas en ella. Como ejemplo consideremos la siguiente instancia de paramodulación:

$$\frac{a = b \quad f(f(a)) = c}{f(f(b)) = c}$$

aquí la segunda premisa es instancia de la cláusula $f(x) = c$ mediante la sustitución $\{x/f(a)\}$. No obstante, no se pueden generar paramodulantes a partir de $a = b$ y $f(x) = c$, de manera que el paramodulante $f(f(b)) = c$ pueda levantarse, es decir, pueda obtenerse mediante una sustitución. El problema radica en que se reemplazó un subtérmino de la cláusula instanciada, a saber, el término $f(a)$.
Los axiomas funcionales reflexivos permiten instanciar más cláusulas, por ejemplo, paramodulando hacia x, con $\{x/a\}$, tenemos:

$$\frac{a = b \quad f(x) = f(x)}{f(b) = f(a)}$$

Enseguida se toma éste paramodulante como premisa y con el umg $\{x/f(b)\}$ se obtiene

$$\frac{f(b) = f(a) \quad f(x) = c}{f(f(a)) = c}$$

Finalmente, paramodulando hacia la a de la segunda premisa obtenemos

$$\frac{a = b \quad f(f(a)) = c}{f(f(b)) = c}$$

Lo cual muestra que el levantamiento es posible.

3.3 El Método de Modificación

Aquí presentamos las nociones y resultados indispensables para la prueba del teorema de completud, no se presenta el método de modificación en su totalidad. Lo que debe quedar claro es que la base de todas las pruebas es la lógica sin igualdad, el predicado "=" es sólo un predicado binario sin ninguna propiedad particular, si bien se construyen interpretaciones que simulan las propiedades de la igualdad.
La noción fundamental para el método de modificación es la de *socio*. La idea es la siguiente: "sacar" un término t de una literal $P(t)$ y hacerlo su socio mediante una variable. Por ejemplo, la literal $P(f(a))$ se reemplaza por $f(a) \neq w \vee P(w)$, donde w es una variable nueva. A $f(a) \neq w$ se le llama *socio* de $P(w)$. A cada literal se le asocia un número natural llamado el *nivel*, en el ejemplo anterior el nivel de $P(w)$ es 0 y el nivel de $f(a) \neq w$ es 1. La literal $f(a) \neq w$ se sigue procesando sacando el término a, obteniéndose la cláusula $a \neq u \vee f(u) \neq w$ donde $a \neq u$ es socio de $f(u) \neq w$ y su nivel es 2. Una literal se puede ver como un árbol, donde los nodos son los socios y en la raíz figura el predicado original, con esto en mente damos la siguiente definición.

Definición 3.3 Una *cláusula aplanada* C es un bosque de literales tal que cada literal L que no es raíz tiene la forma $s \neq w$, donde la variable w tiene exactamente otra presencia en C en el predecesor inmediato K de L. En tal situación L es *socio* de K.

Obsérvese que los socios son cláusulas negativas.

Definición 3.4 A toda literal de una cláusula aplanada se le asocia un *nivel* como sigue: las raices tienen nivel 0 y los socios de K tienen el nivel de K más uno.

Definición 3.5 Una cláusula C está en *E-forma* si y sólo si todo término constante o compuesto que figura en C lo hace únicamente como argumento de $=$ ó de $\neq$.

Ejemplo 3.5 La cláusula $C \equiv f(c) = x \vee g(x, y) = w \vee y = z$ no está en E-forma pues el término constante c no figura como argumento de igualdad sino como argumento de un símbolo de función.

La siguiente modificación es de gran importancia al demostrar la completud.

Definición 3.6 La *E-modificación*, $EMod(C)$, de una cláusula C se define recursivamente como sigue:

- Si C está en E-forma entonces $EMod(C) \equiv C$.
- Sea s un término constante o compuesto que figura en C pero no como argumento de $=$ y sea C' obtenida a partir de C reemplazando $L[s]$ por $s \neq w \vee L[w]$ donde w es una variable nueva. Entonces $EMod(C) \equiv EMod(C')$.

Es fácil comprobar que toda E-modificación está en E-forma y que $C \sim_{sat} EMod(C)$. Además obsérvese que es posible recuperar la cláusula C, al resolver todos los socios de $EMod(C)$ con $x = x$.

Ejemplo 3.6 Si $C \equiv Pf(a, gx) \vee f(x, y) = g(a)$ y $D \equiv Q(ha, gb, x) \vee ga = hb$, entonces
$EMod(C) \equiv a \neq u \vee gx \neq v \vee f(u, v) \neq w \vee Pw \vee a \neq z \vee f(x, y) = gz$ y
$EMod(D) \equiv a \neq v \vee\ hv \neq u \vee\ b \neq y \vee\ gy \neq w \vee Q(u, w, x) \vee\ a \neq z \vee\ b \neq x_1 \vee\ gz = hx_1$.

Ahora presentamos algunos conceptos semánticos necesarios para la prueba de completud.

Definición 3.7 Una *S-interpretación* es una asignación de valores (verdadero o falso) a cada literal cerrada, la cual interpreta a la igualdad de manera simétrica, es decir, $s = t$ y $t = s$ tienen el mismo valor de verdad.

Definición 3.8 Una S-interpretación M es un *S-modelo* para un conjunto de cláusulas $\mathcal{S}$ si y sólo si M es un modelo de $IC(\mathcal{S})$.

Resulta adecuado observar que $\mathcal{S}$ tiene un S-modelo si y sólo si $\mathcal{S} \cup \{x \neq y \vee y = x\}$ tiene un modelo.

Definición 3.9 Sea M una S-interpretación. Una *E-inconsistencia c.r.a.*[1] $s = t$ en M es un par de literales $(L[s], \neg L[t])$ que son verdaderas en M. Una *E-inconsistencia* en M es una terna $(s = t, L[s], \neg L[t])$ tal que $s = t$ es verdadera en M y $(L[s], \neg L[t])$ es una E-inconsistencia c.r.a. $s = t$. M es *E-consistente c.r.a.* $s = t$ si no contiene E-inconsistencias c.r.a. $s = t$. M es *E-consistente* si no tiene E-inconsistencias.

Definición 3.10 Una S-interpretación M es un *E-modelo* para $\mathcal{S}$ si y sólo si M es un S-modelo para $\mathcal{S} \cup \{x = x\}$ y M es E-consistente.

Recuérdese el axioma $\mathcal{A}$, definido al inicio de la sección 3.

Teorema 3.2 *Si $\mathcal{S}$ es un conjunto satisfacible de cláusulas en E-forma tal que $\mathcal{A}, x = x \in \mathcal{S}$, entonces $\mathcal{S}$ tiene un E-modelo.*

Demostración:
Véase [Miranda, 1999]. $\dashv$

El uso del axioma $\mathcal{A}$ es de gran importancia en la prueba

[1]c.r.a. abrevia "con respecto a".

del teorema anterior, sin embargo es posible eliminar su uso mediante cierta transformación, como lo garantiza la proposición 3.1 que se enuncia más adelante.

Definición 3.11 Una cláusula C está en *T-forma* si sucede lo siguiente: cada igualdad que figura en C es de la forma $s = w$ donde w es una variable, C contiene también una literal $t \neq w$ y éstas son las únicas presencias de w en C.

Obsérvese que una cláusula se transforma en T-forma si cada una de sus igualdades $s = t$ se sustituye por $s = w \vee t \neq w$, donde w es una variable que no figuraba en la cláusula.

Ejemplo 3.7 Sean C, D las cláusulas del ejemplo 3.6, las T-formas de C y D son respectivamente: $Pf(a, gx) \vee f(x, y) = w \vee ga \neq w$ y $Q(ha, gb, x) \vee ga = v \vee hb \neq v$.

Definición 3.12 Un conjunto de cláusulas $\mathcal{S}$ está en *ST-forma* si cada cláusula de $\mathcal{S}$ está en T-forma y si $(t \neq w \vee s = w) \vee C') \in \mathcal{S}$ implica que $(s \neq w \vee t = w) \vee C') \in \mathcal{S}$.

Obsérvese que para obtener un conjunto en ST-forma cada igualdad $s = t$ se sustituye por su T-forma $s = w \vee t \neq w$ y se agrega la T-forma de la cláusula correspondiente a la igualdad invertida $t = s$.

Ejemplo 3.8 Sea $\mathcal{S} = \{C, D\}$, el conjunto de cláusulas del ejemplo 3.6. La ST-forma de $\mathcal{S}$ es:

$$\{ \; Pf(a, gx) \vee ga \neq w \vee f(x, y) = w,$$

$$Pf(a, gx) \vee f(x, y) \neq w \vee ga = w,$$

$$Q(ha, gb, x) \vee hb \neq v \vee ga = v,$$

$$Q(ha, gb, x) \vee ga \neq v \vee hb = v \; \}$$

La importancia de los conjuntos en ST-forma se halla en la siguiente proposición.

Proposición 3.1 *Si $\mathcal{S}$ es un conjunto de cláusulas en ST-forma, entonces*

$$\mathcal{S} \cup \{x = x\} \sim_{sat} \mathcal{S} \cup \{\mathcal{A}, x = x\}.$$

Demostración:
Véase [Brand, 1975]. ⊣

4 El Teorema de Completud

En esta sección demostraremos el teorema de completud para la paramodulación con RFP-resolución sin los axiomas funcionales reflexivos, si bien nos seguiremos basando en [Brand, 1975], la incorporación de la RFP-resolución es una aportación nuestra que proporciona mayor claridad que el tratamiento original.
La idea es transformar una refutación del conjunto $\mathcal{S} \cup \{x = x\}$, obtenida con RFP-resolución, en una refutación que sustituye en ciertos casos una aplicación de RFP-resolución por una aplicación de paramodulación.

Lema 4.1 (Miranda 1998)
Sea $\mathcal{S}$ un conjunto de cláusulas aplanadas. Si E es un RFP-resolvente de cláusulas de $\mathcal{S}$ entonces E es aplanada.

Demostración:
Sean $C \equiv C' \vee \neg Q$ y $D' \equiv D_1 \vee P \vee D_2$ tales que Q, P son átomos unificables mediante el umg σ, D' es variante de un factor de la cláusula positiva D y $C, D \in \mathcal{S}$, además, como C debe estar en PN-forma, suponemos sin perder generalidad que los socios de una literal figuran a su derecha.
Queremos demostrar que el RFP-resolvente $E \equiv (D_1 \vee D_2 \vee C')\sigma$ está aplanado. Puesto que D es positiva y aplanada, su factor D' no puede producir socios así que D' permanece aplanada. Analicemos ahora al RFP-resolvente E. Cada socio en E se obtiene aplicando σ a un socio de C' (D no tiene socios pues es positiva); un socio en C' es por hipótesis de la forma $s \neq w$ y para que σ mueva a w ésta tendría que figurar en una de las literales sobre las que se resolvió pero esto no puede ser pues tales literales no tienen socios, ya que la resolución sólo se aplica a la cláusula más a la derecha en C. Por lo tanto E es aplanada. ⊣

La siguiente definición nos proporciona una correspondencia unívoca que asigna a cada literal de una cláusula aplanada cierta expresión mediante la cual podremos transformar una derivación dada.

Definición 4.1 Sean $\tilde{C}$ una cláusula aplanada y $\tilde{L}$ una literal de $\tilde{C}$, definimos recursivamente $\Psi(\tilde{L})$ y L como sigue:
Sean $\tilde{L_1}, \ldots, \tilde{L_n}$ todos los socios de $\tilde{L}$, digamos que $\tilde{L_i} \equiv s_i \neq w_i$ y $\tilde{L} \equiv \tilde{L}[w_1, \ldots, w_n]$. Suponiendo definida L_i a partir de $\tilde{L_i}$ definimos L a partir de $\tilde{L}$ como $L \equiv \tilde{L}[\Psi(L_1), \ldots, \Psi(L_n)]$. Finalmente, si $\tilde{L}$ tiene nivel cero entonces definimos $\Psi(\tilde{L}) \equiv L$ y si $\tilde{L}$ tiene nivel mayor que cero entonces L es de la forma $s \neq w$ y definimos $\Psi(\tilde{L}) \equiv s$.
En el caso que $\tilde{L}$ no tenga socios entonces $\tilde{L} \equiv s \neq w$ y definimos $\Psi(\tilde{L}) \equiv s, \; L \equiv \tilde{L}$.
Por último extendemos Ψ a cláusulas aplanadas como:

$$\Psi(\tilde{C}) \equiv \bigvee \{\Psi(\tilde{L}) \mid \; \tilde{L} \text{ figura en } \tilde{C} \text{ y } \tilde{L} \text{ tiene nivel cero}\}$$

Veamos algunos ejemplos.

Ejemplo 4.1 Sea $\tilde{C} \equiv a \neq u \vee gx \neq v \vee f(u, v) \neq w \vee Pw \vee a \neq z \vee f(x, y) = gz$. Obtenemos $\Psi(\tilde{L})$ para todas las literales de $\tilde{C}$:

1. $\Psi(a \neq u) \equiv a$ pues $a \neq u$ no tiene socios.
2. $\Psi(gx \neq v) \equiv gx$ pues $gx \neq v$ no tiene socios.

3. $\tilde{L} \equiv f(u,v) \neq w$ tiene como socios a $a \neq u, gx \neq v$ y tiene nivel mayor que cero, pues es socio de Pw. Así que $L \equiv (f(u,v) \neq w)[\Psi(a \neq u), \Psi(gx \neq v] \equiv (f(u,v) \neq w)[a, gx] \equiv f(a,gx) \neq w$. Por lo tanto $\Psi(f(u,v) \neq w) \equiv f(a,gx)$.

4. $\tilde{L} \equiv \Psi(Pw)$ tiene nivel cero, así que $\Psi(\tilde{L}) = L$, donde $L \equiv Pw[\Psi(f(u,v) \neq w)] \equiv Pw[f(a,gx)] \equiv Pf(a,gx)$. Por lo tanto $\Psi(Pw) \equiv Pf(a,gx)$.

5. $\Psi(a \neq z) \equiv a$ pues $a \neq z$ no tiene socios.

6. $\tilde{L} \equiv f(x,y) = gz$ tiene nivel cero. En este caso $L \equiv (f(x,y) = gz)[\Psi(a \neq z] \equiv (f(x,y) = gz)[a] \equiv f(x,y) = ga$. Por lo tanto $\Psi(f(x,y) = gz) \equiv f(x,y) = ga$.

La idea para la prueba de completud es reemplazar cada aplicación de RFP-resolución, donde se resolvió un socio de una cláusula aplanada, por una aplicación de paramodulación cuyo paramodulante es el RFP-resolvente.

Teorema 4.1 (Brand 1975, Completud de la Paramodulación).
Si $\mathcal{S}$ es un conjunto de cláusulas que no tiene E-modelo entonces existe una refutación de $\mathcal{S} \cup \{x = x\}$ que sólo utiliza las reglas de RFP-resolución y Paramodulación.

Demostración:
(*Miranda 1998*) Sea $\tilde{\mathcal{S}} \equiv EMod(\mathcal{S})$. Por el teorema 3.2 el conjunto $\tilde{\mathcal{S}} \cup \{\mathcal{A}, x = x\}$ es no satisfacible. Así que, por la proposición 3.1, dado que cualquier cláusula es satisfaciblemente equivalente a su ST-forma, el conjunto $\tilde{\mathcal{S}} \cup \{x = x\}$ es no satisfacible, por lo tanto el teorema 3.1 garantiza que $\tilde{\mathcal{S}} \cup \{x = x\}$ tiene una refutación mediante RFP-resolución. Sea $\tilde{\Delta}$ una refutación de $\tilde{\mathcal{S}} \cup \{x = x\}$ que utiliza únicamente RFP-resolución. Puesto que $\tilde{\mathcal{S}} \cup \{x = x\}$ consiste de cláusulas aplanadas, el lema 4.1 garantiza que $\tilde{\Delta}$ consta de cláusulas aplanadas.
A partir de $\tilde{\Delta}$ vamos a definir una refutación Δ que utiliza paramodulación. Sea $\tilde{\Delta} \equiv (\tilde{C_1}, \ldots, \tilde{C_m})$, donde $\tilde{C_m} = \Box$. Definimos $\Delta \equiv (\Psi(\tilde{C_1}), \ldots, \Psi(\tilde{C_m}))$. Ahora falta definir las justificaciones de cada paso en la derivación Δ.
De la observación que sigue a la definición 3.6, se sigue que si $\tilde{C} \in EMod(\mathcal{S})$ entonces $\Psi(\tilde{C}) \equiv C$. Así que si $\tilde{C_i}$ se justificaba como elemento de $\tilde{\mathcal{S}}$ en la refutación $\tilde{\Delta}$ entonces $\Psi(\tilde{C_i})$ se justifica como elemento de $\mathcal{S}$ en Δ.
Si $\tilde{C_i}$ se obtuvo mediante RFP-resolución de $\tilde{C_j}, \tilde{C_k}$ entonces hay dos casos:

1. Se resolvió un socio. Este caso corresponde a la paramodulación. La situación es como sigue: $\tilde{C_j} \equiv \tilde{C_j}' \vee \tilde{L}[w] \vee s' \neq w$, $\tilde{C_k} \equiv s = t \vee \tilde{C_k}'$ y entonces $\tilde{C_i} \equiv (\tilde{C_j}' \ \vee \tilde{L}[w] \ \vee \tilde{C_k})\sigma$,donde σ es umg de $\{s' = w, s = t\}$. Es decir, se aplicó RFP-resolución de la siguiente manera:

$$\frac{\tilde{C_j}' \vee \tilde{L}[w] \vee s' \neq w \qquad s = t \vee \tilde{C_k}'}{(\tilde{C_j}' \ \vee \tilde{L}[w] \ \vee \tilde{C_k})\sigma}$$

Las imagenes respectivas de $\tilde{C_j}, \tilde{C_k}, \tilde{C_i}$ son $C_j \equiv C_j' \vee L[s'], C_k \equiv \ s = t \vee C_k',\ C_i \equiv (C_j' \vee L[w] \vee C_k')\sigma$ de manera que el RFP-resolvente $\tilde{C_i}$ se mapea en un paramodulante desde C_k hacia C_j. Como $s'\sigma = s\sigma,\ w\sigma = t\sigma$ la paramodulación queda como sigue:

$$\frac{s = t \vee C_k' \quad C_j' \vee L[s']}{(C_k' \vee C_j' \vee L[t])\sigma}$$

Supongamos que este caso se ha realizado exhaustivamente y pasemos al siguiente caso.

2. Se resolvió una literal $\tilde{L}$ de nivel cero. Como ya no hay socios tenemos $\Psi(\tilde{L}) \equiv \tilde{L}$ y todo se justifica de igual forma en Δ.

Finalmente, como $\tilde{\Delta}$ es una refutación de $\tilde{\mathcal{S}} \cup \{x = x\}$ mediante RFP-resolución y claramente $\Psi(\Box) \equiv \Box$, entonces Δ es una refutación de $\mathcal{S}$ mediante RFP-resolución y Paramodulación. $\dashv$

5 Consecuencias Computacionales

La completud de paramodulación con RFP-resolución tiene diversas consecuencias en el campo computacional, en particular puedo mencionar la completud de diversas combinaciones y restricciones de paramodulación con hiperresolución implementadas en el programa de razonamiento automático OTTER. Mas recientemente, en 1996, con ayuda de diversas estrategias de paramodulación (véase [McCune, 1997a]) se resolvió, por medio del programa de razonamiento automático EQP, el problema de Robbins que habia permanecido abierto desde los años treinta (véase [McCune, 1997b]). Ambos programas se encuentran disponibles en `http://www-unix.mcs.anl.gov/AR/`.

Agradecimientos

Agradezco a los árbitros anónimos por las correcciones y sugerencias que me permitieron mejorar el contenido y ampliar la bibliografía de este artículo.

Referencias

[Amor y Miranda, 1998] José A. Amor M., Favio E. Miranda P. Demostración Automática de Teoremas y la Nutria. En *Memorias del XXX Congreso Nacional de la SMM*, Aportaciones Matemáticas 22:159-179, Sociedad Matemática Mexicana. México 1998.

[Bachmair *et al.*, 1995] L. Bachmair, H. Ganzinger, C. Lynch, W. Snyder. Basic Paramodulation. En *Information and Computation* 121(2):171–192. 1995.

[Brand, 1975] D. Brand. Proving Theorems with the Modification Method. En *SIAM Journal on Computing*, 4(4):412–430. Diciembre 1975.

[Hsiang y Rusinowitch, 1991] J. Hsiang, M. Rusinowitch. Proving Refutational Completeness of Theorem Proving Strategies: The Transfinite Semantic Tree Method. En *Journal of the A.C.M.*, 38(3):559–587. Julio 1991.

[McCune, 1997a] William McCune. 33 Basic Test Problems: A Practical Evaluation of Some Paramodulation Strategies. En *Automated Reasoning and Its Applications: Essays in Honor of Larry Wos*, 71-114. Editado por R. Veroff y G. Pieper. MIT Press. 1997

[McCune, 1997b] William McCune. Solution of the Robbins Problem. En *Journal of Automated Reasoning* 19(3):263-276. 1997.

[Miranda, 1999] Favio E. Miranda P. *Fundamentos Lógicos del Programa de Razonamiento Automático OTTER*. Tesis de Maestria, Facultad de Ciencias, UNAM. 1999.

[Nieuwenhuis y Rubio, 1999] R. Nieuwenhuis, A. Rubio. Paramodulation–based Theorem Proving. En *Handbook of Automated Reasoning*. Editado por Alan Robinson y Andrei Voronkov. Por Aparecer, Elsevier Science. 1999.

[Peterson, 1983] G.E. Peterson. A Technique for establishing Completeness Results in Theorem Proving with Equality. En *SIAM Journal on Computing* 12(1):82–100. Febrero 1983.

[Plaisted, 1994] D. A. Plaisted. Equational Reasoning and Term Rewriting Systems. En *Handbook of Logic In Artificial Intelligence and Logic Programming*, Vol 1. Logical Foundations, 273–364. Editado por D.M. Gabbay, C.J. Hogger y J.A. Robinson. Oxford Science Publications. 1994.

[Wos y Robinson, 1969] Larry Wos, George A. Robinson. Paramodulation and Theorem Proving in First Order Theories with Equality. En *Machine Intelligence* 4:135-150. Editado por B. Meltzer, D. Michie. American Elsevier, New York. 1969.

[Wos y Robinson, 1970] Larry Wos, George A. Robinson. Paramodulation and set of support. En *Proceedings of the Symposium in Automatic Demonstration*, LNM 125. Springer Verlag. 1970.