Università degli Studi di Napoli Federico II
Scuola Politecnica e delle Scienze di Base
Dipartimento di Ingegneria Elettrica e Tecnologie dell'Informazione

Corso di Laurea in Informatica

Implementazione di una procedura di decisione per frammenti Binding in Vampire

Relatori
Prof. Massimo Benerecetti
Prof. Fabio Mogavero

Candidato
Matteo Richard Gaudino

Matricola
N86003226

Anno Accademico 2022 - 2023

Indice

Introduzione

Capitolo 1

Logica e automazione dei problemi di Decisione

In questo capitolo verranno descritte le nozioni di base necessarie per comprendere il lavoro svolto in questa tesi. In particolare, verranno introdotti i concetti di logica proposizionale e del primo ordine, definita come estensione della prima. Verrà anche introdotto il problema della decisione, ovvero il problema di stabilire se una data formula è soddisfacibile o meno e le principali tecniche ad alto livello che vengono utilizzate dai theorem prover moderni per risolvere questo problema. Nell'ultimo paragrafo del capitolo verrà descritto in che modo le formule di logica del primo ordine possono essere rappresentate in un formato di file, per poi essere processate come input da un theorem prover. Lo scopo di questo capitolo è quindi quello di accennare la teoria logica utilizzata nell'implementazione di vampire e della procedura di decisione per i Binding-Fragments. Non è tra gli obbiettivi dare una trattazione esaustiva sulla logica o in generale sulle varie teoria matematiche coinvolte, perciò verranno date per scontate nozioni di teoria degli insiemi, algebra, teoria della computazione e teoria dei linguaggi.

1.1 Logica Proposizionale

La logica proposizionale è un ramo della logica formale che si occupa dello studio e della manipolazione delle proposizioni, ovvero dichiarazioni che possono essere classificate come vere o false, ma non entrambe contemporaneamente (Principio di bivalenza). Essa fornisce un quadro formale per analizzare il ragionamento deduttivo basato su connettivi logici, come "e", "o", e "non". Questo strumento anche se incluso nella logica del primo ordine, rimane un pilastro fondamentale per lo studio svolto in questa tesi e quindi è necessario farne un'introduzione indipendente.

1.1.1 Formule

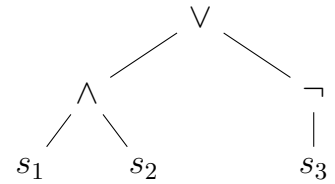
Sia $\Sigma_s = \{s_1, s_2, ...\}$ un insieme di simboli di costante, $\Sigma = \{\wedge, \vee, \neg, (,), \top, \bot\} \cup \Sigma_s$ è detto alfabeto della logica proposizionale. Con queste premesse si può definire come formule della logica proposizionale il linguaggio F generato dalla grammatica Context Free seguente:

$$\varphi := \top \mid \bot \mid S \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi)$$

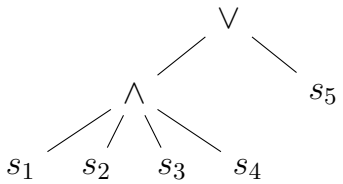
Dove $S \in \Sigma_s$ è un simbolo di costante. Con la funzione $const(\gamma) \to 2^{\Sigma_s}$ si indica la funzione che associa a ogni formula γ l'insieme dei suoi simboli di costante. Viene chiamato *Letterale*, ogni simbolo di costante s o la sua negazione $\neg s$. Vengono inoltre introdotti i seguenti simboli come abbreviazioni:

- $(\gamma \Rightarrow \kappa)$ per $(\neg\gamma \vee \kappa)$
- $(\gamma \Leftrightarrow \kappa)$ per $((\gamma \Rightarrow \kappa) \wedge (\kappa \Rightarrow \gamma))$
- $(\gamma \oplus \kappa)$ per $\neg(\gamma \Leftrightarrow \kappa)$

È possibile rappresentare una qualunque formula attraverso il proprio albero di derivazione. Questo albero verrà chiamato in seguito anche *albero sintattico* della formula. Ad esempio, la formula $(s_1 \wedge s_2) \vee \neg s_3$ può essere rappresentata dal seguente albero sintattico:



La radice dell'albero è detta *connettivo principale* e i sotto alberi della formula vengono dette *sottoformule*. Per compattezza, grazie alla proprietà associativa di $\wedge$ e $\vee$, è possibile omettere le parentesi, es. $(s_1 \wedge (s_2 \wedge (s_3 \wedge s_4))) \vee s_5$ può essere scritto come $(s_1 \wedge s_2 \wedge s_3 \wedge s_4) \vee s_5$. Allo stesso modo, nell'albero sintattico della formula è possibile compattare le catene di $\wedge$ e $\vee$ come figli di un unico nodo:



Questa è una caratteristica molto importante, in quanto non solo permette di risparmiare inchiostro, ma consente di vedere $\wedge$ e $\vee$ non più come operatori binari ma come operatori n-ari. A livello implementativo, ciò si traduce in un minor impatto in memoria, visite all'albero più veloci e algoritmi di manipolazione

più semplici. Si consideri ad esempio di voler ricercare la foglia più a sinistra nell'albero di derivazione della seguente formula $((...(((s_1 \wedge s_2) \wedge s_3) \wedge s_4) \wedge ...) \wedge s_n)$. Senza compattazione, l'algoritmo di ricerca impiegherebbe $O(n)$ operazioni, mentre con la compattazione $O(1)$.

1.1.2 Assegnamenti

Un *assegnamento* è una qualunque funzione α da un insieme $S \subseteq \Sigma_s$ nell'insieme $\{1, 0\}$ (o $\{True, False\}$).

$$\alpha : S \to \{1, 0\}$$

Un assegnamento α è detto *appropriato* per una formula $\varphi \in F$ se e solo se $const(\varphi) \subseteq dom(\alpha)$.

Si definisce la relazione binaria di *Soddisfacibilità*:

$$\models \subseteq \{1, 0\}^S \times F$$

In modo tale che dato un assegnamento α appropriato a una formula φ, si dice che $\alpha \models \varphi$ (α soddisfa φ) o anche α è un assegnamento per φ o se e solo se:

- Se φ è una costante s allora $\alpha \models \varphi$ sse $\alpha(s) = 1$
- Se φ è $\top$ allora $\alpha \models \varphi$
- Se φ è $\bot$ allora $\alpha \not\models \varphi$
- Se φ è della forma $\neg\psi$ (dove ψ è una formula) allora $\alpha \models \varphi$ sse $\alpha \not\models \psi$
- Se φ è della forma $(\psi \wedge \chi)$ (con ψ e χ formule) allora $\alpha \models \varphi$ sse $\alpha \models \psi$ e $\alpha \models \chi$
- Se φ è della forma $(\psi \vee \chi)$ (con ψ e χ formule) allora $\alpha \models \varphi$ sse $\alpha \models \psi$ o $\alpha \models \chi$

Per convenzione si assume che $\alpha(\top) = 1$ e $\alpha(\bot) = 0$ per ogni assegnamento α. Una *Tautologia* è una formula φ tale che per ogni assegnamento α appropriato a φ, $\alpha \models \varphi$ (in simboli $\models \varphi$). Una formula è detta soddisfacibile se esiste un assegnamento appropriato che la soddisfa altrimenti è detta insoddisfacibile. Date due formule φ e ψ, si dice che ψ è *conseguenza logica* di φ (in simboli $\varphi \models \psi$) se e solo se per ogni assegnamento α appropriato a entrambe le formule, se $\alpha \models \varphi$ allora $\alpha \models \psi$. Due formule sono dette *equivalenti* sse $\varphi \models \psi$ e $\psi \models \varphi$ (in simboli $\varphi \equiv \psi$). Un'importante proprietà è che se $\varphi \models \psi$ allora la formula $\varphi \Rightarrow \psi$ è una tautologia ($\models \varphi \Rightarrow \psi$).

Due concetti molto simili a quello di equivalenza e conseguenza logica sono l'*equisoddisfacibilità* e la *soundness*. In pratica, due formule sono sound se e solo se, se la prima formula è soddisfacibile allora lo è anche la seconda. Due formule sono equisoddisfacibili se e solo se sono sound in entrambe le direzioni.

Quindi la conseguenza logica implica la soundness ma non il viceversa. Allo stesso modo l'equivalenza logica implica l'equisoddisfacibilità ma non il viceversa. Si consideri ad esempio le due formule $\varphi = s_1$ e $\psi = \neg s_1$. Ovviamente non può esserci conseguenza logica tra le due formule, ma sono equisoddisfacibili, infatti se α è un assegnamento per φ allora è possibile costruire un assegnamento β per ψ tale che $\beta(s_1) = 1 - \alpha(s_1)$ e viceversa.

Un'*inferenza* è una qualunque relazione da $F^n \times F$. Un'inferenza è detta *corretta* se conserva la soddisfacibilità, ovvero se a a partire da formule soddisfacibili non associa formule insoddisfacibili (soundness). Un esempio di inferenza è la regola del *Modus Ponens*. Date le premesse $\varphi, (\varphi \Rightarrow \psi)$ si può inferire ψ. Viene utilizzato il simbolo $P \vdash C$ per indicare l'applicazione di un'inferenza alla *Premessa* P per ottenere una *Conclusione* C. In notazione la regola del modus ponens viene espressa così: $[\varphi, \varphi \Rightarrow \psi] \vdash \psi$ oppure $\frac{\varphi, \varphi \Rightarrow \psi}{\psi}$.

Infine, si definisce *Implicante* di una formula φ un insieme I di letterali di φ che rendono vera φ. Cioè, costruendo una assegnazione α tale che $\alpha \models c$ per ogni letterale $c \in I$, si ha che $\alpha \models \varphi$. In altre parole la formula costruita dalla congiunzione di tutti i letterali di I implica logicamente φ. Spesso con abuso di terminologia gli elementi di I vengono chiamati anch'essi implicanti, di solito è facile intuire dal contesto se si sta parlando dell'insieme o dei letterali. È possibile anche costruire un Implicante a partire da una assegnazione. È sufficiente prendere l'insieme dei letterali della formula soddisfatti dall'assegnamento e si ottiene così un implicante.

1.1.3 Forme Normali

Una delle strategie più utilizzate dai dimostratori di teoremi automatici è la *normalizzazione* delle formule. Una *forma normale* è essenzialmente un sottoinsieme di F che rispetta determinate proprietà. Una *normalizzazione* invece è il processo di trasformazione di una formula tramite una successione d'inferenze (corrette) in una forma normale. In questo paragrafo verranno descritte le tre forme normali che sono state utilizzate per il preprocessing dell'algoritmo. In questo caso, tutte e tre le forme presentate preservano la relazione di equivalenza logica, quindi è sempre possibile trasformare una formula in un'altra equivalente in uno di questi tre formati. La prima e l'ultima ossia le forme NNF e CNF sono le più famose e utilizzate, mentre la seconda, la ENNF, non è abbastanza conosciuta da essere definita standard e viene utilizzata per bypassare alcuni problemi di efficienza causati dalla CNF grazie all'utilizzo di tecniche di Naming, che però verranno discusse nella prossima sezione.

La prima tra queste è la *NNF* ossia *Negated Normal Form* (Forma normale negata). Una formula è in formato NNF sse non contiene connettivi semplificati

$(\Rightarrow, \Leftrightarrow, \oplus)$ e la negazione è applicata solo a letterali. La classe di formule NNF è generata dalla seguente grammatica:

$$\eta := \top \mid \bot \mid S \mid \neg S \mid (\eta \wedge \eta) \mid (\eta \vee \eta)$$

Dove $S \in \Sigma_s$ è un simbolo di costante. La normalizzazione di una formula in NNF è un processo semplice che consiste nell'applicare opportunamente le regole di De Morgan e le regole di semplificazione dei connettivi.

La seconda forma normale è la *ENNF* ossia *Extended Negated Normal Form* (Forma normale negata estesa). Il formato ENNF è essenzialmente una classe più permissiva della NNF, in quanto conserva il vincolo sulla negazione ma vieta esclusivamente l'uso di '$\Rightarrow$'. La classe di formule ENNF è generata dalla seguente grammatica:

$$\overline{\eta} := \top \mid \bot \mid S \mid \neg S \mid (\overline{\eta} \wedge \overline{\eta}) \mid (\overline{\eta} \vee \overline{\eta}) \mid (\overline{\eta} \Leftrightarrow \overline{\eta}) \mid (\overline{\eta} \oplus \overline{\eta})$$

La terza e ultima forma normale è la *CNF* ossia *Conjunctive Normal Form* (Forma normale congiuntiva). Una formula è in formato CNF sse è una congiunzione di disgiunzioni di letterali. La classe di formule CNF è generata dalla seguente grammatica:

$$\zeta := \xi \mid (\xi \wedge \zeta)$$
$$\xi := \top \mid \bot \mid S \mid \neg S \mid (\xi \vee \xi)$$

La classe CNF è storicamente la più famosa e utilizzata, in quanto è la più semplice da implementare e da manipolare. È possibile vedere le clausole come insiemi di letterali mentre la formula principale è vista come un insieme di clausole. Ad esempio, la CNF $(s_1 \vee \neg s_2) \wedge (s_3)$ può essere rappresentata in termini insiemistici come $\{\{s_1, \neg s_2\}, \{s_3\}\}$. La clausola vuota $\{\}$ è una clausola speciale che rappresenta la formula $\bot$, viene spesso raffigurata dal simbolo $\square$. La normalizzazione di una formula in CNF è un processo più complesso rispetto alle altre due forme normali. Non esiste un unica tecnica di normalizzazione, ma una strategia comune è questa:

1. Si trasforma la formula in NNF.
2. Se la formula è del tipo $\varphi_1 \wedge ... \wedge \varphi_n$ allora la struttura principale è già una congiunzione di formule, quindi si procede applicando l'algoritmo sulle sottoformule $\varphi_1, ..., \varphi_n$.
3. Se la formula è del tipo $(\varphi_1 \wedge \varphi_2) \vee \psi_1$ si applica la proprietà distributiva di $\vee$ su $\wedge$ in modo da spingere i connettivi $\vee$ il più possibile in profondità.

Si ottiene così una formula del tipo $(\varphi_1 \vee \psi_1) \wedge (\varphi_2 \vee \psi_1)$ si procede poi ricorsivamente con il punto 2.

Il processo di generazione delle clausole prende il nome di *clausificazione*. Questa tecnica di clausificazione nella peggiore delle ipotesi porta a una generazione di un numero di clausole esponenziale rispetto alla dimensione della formula originale. Ad esempio la formula $(s_1 \wedge s_2) \vee (s_3 \wedge s_4) \vee ... \vee (s_{n-1} \wedge s_n)$ genera esattamente 2^n clausole diverse tutte da n letterali.

1.1.4 Naming

Come già accennato il processo di normalizzazione di una formula può portare a una crescita esponenziale del numero di clausole generate. Si assuma ad esempio di voler clausificare una formula del tipo:

$$\varphi \vee \psi$$

E che φ e ψ generino rispettivamente n e m clausole. Continuando a clausificare con l'algoritmo descritto nel paragrafo 1.1.3, si ottengono $n \cdot m$ clausole. Questo perché la continua applicazione della proprietà distributiva porta a una duplicazione considerevole delle sottoformule. Una possibile tecnica di ottimizzazione è quella del *Naming* [7] anche detto *Renamig*. In generale per *Naming* si intende una qualunque tecnica di rinomina di letterali o sottoformule. In questo caso, per *Naming* si intende la rinomina di sottoformule tramite l'aggiunta di un nuovo simbolo di costante. Per l'esempio precedente si assuma che s_n sia un simbolo di costante non presente nella formula originale. Applicando il *Naming* si ottiene la seguente formula:

$$(\varphi \vee s_n) \wedge (s_n \vee \psi)$$

In questo modo, la clausificazione della formula genera solo $n + m$ clausole al costo dell'aggiunta di un nuovo simbolo di costante. Un discorso simile vale per formule con la doppia implicazione e lo xor, solo che in questo caso anche solo la normalizzazione in NNF può portare a una crescita esponenziale del numero di sottoformule. La trasformazione in NNF e poi in CNF della formula:

$$((...((s_1 \Leftrightarrow s_2) \Leftrightarrow s_3) \Leftrightarrow ...) \Leftrightarrow s_n)$$

Porta alla generazione di 2^{n-1} clausole. Nell'esempio particolare in cui $n = 6$ si ottengono 32 clausole ma con l'introduzione di due nuovi nomie s_7 e s_8 è possibile ottenere la seguente formula:

$$(s_7 \Leftrightarrow (((s_1 \Leftrightarrow s_2) \Leftrightarrow s_3) \Leftrightarrow s_4))$$
$$\wedge$$
$$(s_8 \Leftrightarrow (s_7 \Leftrightarrow s_5))$$
$$\wedge$$
$$(s_8 \Leftrightarrow s_6)$$

Che genera solo 22 clausole. Il processo per stabilire quale sottoformula rinominare è un problema complesso. Solitamente stabilisce un numero detto *Threshold* (Soglia) che rappresenta il numero massimo di clausole che si è disposti a generare. Se una sottoformula genera un numero di clausole maggiore del Threshold, allora viene rinominata. Ma anche questo è un discorso non banale e non verrà approfondito oltremodo in questo documento. In generale la nuova formula generata dal namig è equisoddisfacibile all'originale.

1.2 Logica del primo ordine

La logica dei predicati rappresenta un'estensione della logica proposizionale, ampliando il suo ambito per trattare in maniera più ricca e dettagliata le relazioni tra gli oggetti e le proprietà delle entità coinvolte. Mentre la logica proposizionale si occupa di proposizioni atomiche, la logica dei predicati introduce i predicati, che sono relazioni che sono vere o false a seconda dell'interpretazione e dalle variabili che contengono. Vengono generalizzati anche i connettivi logici $\wedge$ e $\vee$ tramite i quantificatori universali ed esistenziali $\forall$ e $\exists$ in modo da poter parlare di anche di insiemi di oggetti non finiti.

1.2.1 Termini e Formule

Si introducono tre nuovi insiemi di simboli:

- $\Sigma_f = \{f_1, f_2, ...\}$ insieme di simboli di funzione
- $\Sigma_p = \{p_1, p_2, ...\}$ insieme di simboli di predicato (o relazione)
- $\Sigma_x = \{x_1, x_2, ...\}$ insieme di simboli di variabile

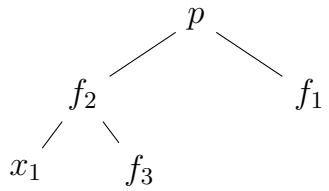
Si definisce la funzione *arity* : $\Sigma_f \cup \Sigma_p \to \mathbb{N}$ che associa ad ogni simbolo di funzione o predicato la sua arità. Funzioni e predicati di arità 0 sono detti rispettivamente *Funzioni costanti* e *Predicati costanti*. I simboli contenuti in $\Sigma_f \cup \Sigma_p$ sono detti *simboli non logici* e ogni suo sottoinsieme è detto *tipo*. Un *termine* è una stringa generata dalla seguente grammatica:

$$\tau := X \mid f(\tau_1, ..., \tau_n)$$

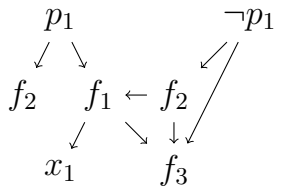
Dove X è un simbolo di variabile e f è un simbolo di funzione tale che $arity(f) = n$. In altre parole:

- Ogni variabile è un termine
- Ogni funzione costante è un termine
- Se $\tau_1, ..., \tau_n$ sono termini e f è un simbolo di funzione di arità n allora $f(\tau_1, ..., \tau_n)$ è un termine

Si indica con T l'insieme di tutti i termini generati dalla grammatica precedente. Verranno chiamati *Atomo* tutte le stringhe del tipo $p(\tau_1, ..., \tau_n)$ dove p è un simbolo di relazione di arità n e $\tau_1, ..., \tau_n$ sono termini. Vengono chiamati *Letterali* tutti gli atomi e la loro negazione. Termini e Letterali sono detti *ground* se non contengono variabili. Come già visto per le formule proposizionali, è possibile rappresentare un termine o un letterale attraverso il proprio albero di derivazione. Ad esempio, il letterale $p_1(f_2(x_1, f_3), f_1)$ può essere rappresentato dal seguente albero sintattico:



Come intuibile i sottoalberi di un termine sono detti *sottotermini*. Si assuma di avere due letterali $p_1(f_2, f_1(x_1, f_3))$ e $\neg p_1(f_2(f_1(x_1, f_3), f_3), f_3)$ di volerli rappresentare in un unico grafo. Al posto di creare una foresta con due alberi indipendenti, è possibile creare un unica struttura condividendo i sottotermini comuni:



Una struttura del genere è detta *Prfectly Shared* (Perfettamente condivisa). Nella pratica questa tecnica di condivisione di sottotermini è indispensabile dato che, anche se a un costo per la creazione e la gestione non indifferente, permette un risparmio di memoria e di tempo considerevole. Per effettuare ad esempio un controllo di uguaglianza tra due sottotermini è sufficiente controllare che le due frecce che partono dai termini padre puntino allo stesso sottotermine, senza dover visitare l'intera sotto struttura, rendendo così tale operazione a tempo costante.

A questo punto si definisce finalmente le formule della logica del primo ordine. Prendendo come punto di partenza le formule proposizionali, si definisce alfabeto

delle formule del primo ordine l'insieme: $\Sigma' = (\Sigma \setminus \Sigma_s) \cup \Sigma_f \cup \Sigma_p \cup \Sigma_x \cup \{\forall, \exists\}$ e Si definisce come formule del primo ordine il linguaggio F' generato dalla seguente grammatica:

$$\phi := \top \mid \bot \mid A \mid \neg\phi \mid (\phi \wedge \phi) \mid (\phi \vee \phi) \mid \forall x(\phi) \mid \exists x(\phi)$$

Dove A è un atomo e x è un simbolo di variabile. I simboli $\forall$ e $\exists$ sono detti quantificatori universali ed esistenziali. Una variabile x è detta *vincolata* se è contenuta in una formula del tipo $\forall x(\varphi')$ o $\exists x(\varphi')$ altrimenti è detta *libera*. Una formula è detta *enunciato* se non contiene variabili libere. Una formula è detta *ground* se tutti i suoi letterali sono ground.

Per comodità di scrittura è possibile raggruppare catene di quantificatori dello stesso tipo. Ad esempio, la formula $\forall x_1 \forall x_2 \forall x_3 \exists x_4 \exists x_5 \forall x_6 \forall x_7(\phi)$ può essere scritta come $\forall x_1 x_2 x_3 \exists x_4 x_5 \forall x_6 x_7(\phi)$. In modo simile a come visto per $\vee$ e $\wedge$ è possibile vedere $\forall$ e $\exists$ come operatori n-ari che prendono in input n-1 variabili e una formula.

1.2.2 Unificazione

Dato un termine τ (o un letterale), con la scrittura $\tau[x_k/t]$ si indica il termine (o il letterale) ottenuto sostituendo tutte le occorrenze della variabile x_k con il termine t in τ. Ad esempio se $\tau = f_1(x_1, x_2)$ allora $\tau[x_1/f_2] = f_1(f_2, x_2)$. Si può estendere questa notazione in modo da poter sostituire più variabili contemporaneamente. Si definisce come *sostituzione* una qualunque funzione da un insieme di variabili a termini. Dato un termine τ e una sostituzione $\sigma = \{(x_1, t_1), ..., (x_n, t_n)\}$, con la scrittura $\tau[x_1/t_1, ..., x_n/t_n]$ oppure τ^σ si indica il termine ottenuto sostituendo *contemporaneamente* tutte le occorrenze delle variabili $x_1, ..., x_n$ con i termini $t_1, ..., t_n$ in τ. Con contemporaneamente si intende che ogni singola sostituzione viene effettuata sul termine originale, senza essere influenzata dalle sostituzioni precedenti o successive. Ad esempio, se $\tau = f(x_1, x_2)$ allora $\tau[x_1/x_2, x_2/x_1] = f(x_2, x_1)$ e non $f(x_1, x_1)$ che è invece il risultato dell'applicazione sequenziale delle due regole $\tau[x_1/x_2][x_2/x_1]$.

Dati due termini τ_1 e τ_2 si dice che τ_1 è *più generico* di τ_2 o che τ_2 è *più specifico* di τ_1 se e solo se esiste una sostituzione σ tale che $\tau_1^\sigma = \tau_2$. Se esiste una sostituzione σ tale che $\tau_1^\sigma = \tau_2^\sigma$ allora i due termini sono detti *unificabili* e la sostituzione σ è detta *unificatore* dei due termini.

Date due sostituzioni σ_1 e σ_2 si dice che σ_1 è *più generica* di σ_2 o che σ_2 è *più specifica* di σ_1 se e solo se per ogni termine θ, σ_2 è sussunta da σ_1, ossia sse esiste una sostituzione θ tale che $\tau^{\sigma_2} = (\tau^{\sigma_1})^\theta$. Dati due termini unificabili τ_1 e τ_2 si dice che σ_1 è un MGU (Most General Unifier) di τ_1 e τ_2 se è la sostituzione più generica tra tutti gli unificatori dei due termini.

È possibile generalizzare il concetto di unificazione per insiemi di termini, letterali e insiemi di letterali. Dato un insieme di termini T, si dice che T è unificabile se esiste una sostituzione σ tale che $\tau_1^\sigma = \tau_2^\sigma$ per ogni coppia di termini $\tau_1, \tau_2 \in T$. In questo caso σ è detto unificatore di T. Due letterali della stessa arità $L_1 = p_1(\tau_1, ..., \tau_n)$ e $L_2 = p_2(\tau'_1, ..., \tau'_n)$ sono unificabili se e solo se esiste una sostituzione che li eguaglia ignorando il simbolo di predicato. In altre parole sia f una funzione di arità n allora L_1 e L_2 sono unificabili se e solo se sono unificabili i termini $f(\tau_1, ..., \tau_n)$ e $f(\tau'_1, ..., \tau'_n)$. Letterali di diversa arità non sono mai unificabili. Un insieme di letterali è unificabile se e solo se esiste una sostituzione che unifica a due a due tutti i letterali dell'insieme.

Un importante risultato è questo:

Proposizione 1. *Se due termini non sono unificabili allora vale una delle seguenti affermazioni:*

1. *I due termini hanno arità diverse*
2. *I due termini presentano una function obstruction*
3. *I due termini presentano una variable obstruction*

Una function obstruction è una situazione in cui visitando allo stesso modo l'albero sintattico dei termini si incontrano due simboli di funzione diversi. Ad esempio, i termini $f_1(x_1, f_2(x_2))$ e $f_1(x_1, f_3(x_2))$ non sono unificabili in quanto presentano una function obstruction, $f_2 \neq f_3$. Una variable obstruction invece è una situazione in cui visitando allo stesso modo l'albero sintattico dei termini si incontra una variabile x nel primo termine e si incontra un sottotermine t ($\neq x$) che contiene x nel secondo termine. Ad esempio i termini $f_1(x_1, f_2(x_2))$ e $f_1(f_2(x_1), x_1)$ non sono unificabili in quanto presentano una variable obstruction, x_1 è contenuta in $f_2(x_1)$.

Un noto algoritmo per la ricerca di un MGU di due termini è l'algoritmo di unificazione di *Robinson*. Il collo di bottiglia di questo algoritmo è la occurrence-check, ovvero la ricerca di una variable obstruction. Se si assume che i termini in input non contengono variabili in comune è possibile ignorare questa situazione. Di seguito viene riportato l'algoritmo di Robinson senza occurrence-check:

Algorithm 1: Algoritmo di unificazione di Robinson senza occurrence-check

Firma: unify(τ_1, τ_2)
Input: τ_1, τ_2 due termini
Output: σ un MGU di τ_1 e τ_2 o $\perp$ se non esiste
$S :=$ Empty Stack of pair of terms;
$\sigma :=$ Empty Substitution;

$S.push(\tau_1, \tau_2)$;
while *S is not Empty* **do**
  $(\tau_1, \tau_2) := S.pop()$;
  while τ_1 *is a variable* $\wedge\ \tau_1 \neq \tau_1^\sigma$ **do**
    $\tau_1 := \tau_1^\sigma$;
  end
  while τ_2 *is a variable* $\wedge\ \tau_2 \neq \tau_2^\sigma$ **do**
    $\tau_2 := \tau_2^\sigma$;
  end

  if $\tau_1 \neq \tau_2$ **then**
    switch $\tau_1\tau_2$ **do**
      case τ_1 is a variable x and τ_2 is a variabile $y \Rightarrow \sigma := \sigma \cup \{x/y\}$;
      case τ_1 is a variable $x \Rightarrow \sigma := \sigma \cup \{x/\tau_2\}$;
      case τ_2 is a variable $y \Rightarrow \sigma := \sigma \cup \{y/\tau_1\}$;
      case $\tau_1 = f(s_1, ..., s_n)$ and $\tau_2 = f(t_1, ..., t_n) \Rightarrow$
       $S.push(s_1, t_1), ..., S.push(s_n, t_n)$;
      case $\tau_1 = f(s_1, ..., s_n)$ and $\tau_2 = g(t_1, ..., t_m) \Rightarrow$ **return** $\perp$;
    end
  end
end
return σ;

1.2.3 Semantica

Si indica con *tipo* di φ, l'insieme di tutti i simboli non logici presenti nella formula (costanti, funzioni e predicati). Si definisce *Modello* di un tipo Γ una coppia $\mathcal{M} = (D, I)$ dove D è un insieme non vuoto detto *Dominio* e I è una funzione: $I : \Gamma \to D$ detta d'*Interpretazione* che associa ogni simbolo non logico del tipo a un elemento del dominio in modo tale che per ogni simbolo non logico s:

- Se s è un simbolo di funzione n-aria allora $I(s)$ è una funzione n-aria su D: $I(s) : D^n \to D$.

- Se s è un simbolo di predicato n-ario allora $I(s)$ è una relazione n-aria su D: $I(s) \subseteq D^n$.

Per l'interpretazioni delle costanti si assume che nel dominio siano presenti almeno due oggetti distinti $\{0, 1\} \in D$:

- Se s è un simbolo di funzione costante allora $I(s) \in D$ è un oggetto del dominio.
- Se s è un simbolo di predicato costante allora $I(s) \in \{0, 1\}$.
- Se s è $\top$ allora $I(s) = 1$
- Se s è $\bot$ allora $I(s) = 0$

Per semplicità di lettura, d'ora in poi l'applicazione della funzione I ad un simbolo s verrà indicata con s^I. Si definisce *Contesto*, una qualunque mappatura $\gamma : \Sigma_x \to D$ che associa variabili a un elemento del dominio. Con la scrittura $\gamma[x/t]$ si indica il contesto ottenuto sostituendo il valore della variabile x con l'elemento t. Ad esempio se $\gamma = \{x_1 \to a, x_2 \to b\}$ allora $\gamma[x_1/b] = \{x_1 \to b, x_2 \to b\}$. Per l'applicazione di un contesto a una variabile si utilizza la stessa notazione usata per le funzioni, ovvero $\gamma(x)$. Per l'esempio precedente $\gamma(x_1) = a$, $\gamma(x_2) = b$ e $\gamma[x_1/b](x_1) = b$. Se una variabile x non è presente nel contesto allora si assume che $\gamma(x) = x$. Si definisce l'interpretazione di un termine o predicato τ nel contesto γ secondo l'interpretazione I:

- Se τ è una variabile x allora $\tau_\gamma^I = \gamma(x)$
- Se τ è una funzione $f(\tau_1, ..., \tau_n)$ allora $\tau_\gamma^I = f^I({\tau_1}_\gamma^I, ..., {\tau_n}_\gamma^I)$
- se τ è un predicato $p(\tau_1, ..., \tau_n)$ allora $\tau_\gamma^I = p^I({\tau_1}_\gamma^I, ..., {\tau_n}_\gamma^I)$

Data una formula del primo ordine φ si dice che il modello $\mathcal{M}$ è appropriato per la formula φ se e solo se il tipo della formula è contenuto nel tipo del modello. Un modello appropriato $\mathcal{M}$ soddisfa una formula φ nel contesto γ se e solo se:

- Se φ è un predicato costante p (o $\top/\bot$) allora $\mathcal{M}, \gamma \models p$ se e solo se $p^I = 1$
- Se φ è della forma $\neg\psi$ (dove ψ è una formula) allora $\mathcal{M}, \gamma \models \varphi$ se e solo se $\mathcal{M}, \gamma \not\models \psi$
- Se φ è della forma $(\psi \wedge \chi)$ (con ψ e χ formule) allora $\mathcal{M}, \gamma \models \varphi$ se e solo se $\mathcal{M}, \gamma \models \psi$ e $\mathcal{M}, \gamma \models \chi$
- Se φ è della forma $(\psi \vee \chi)$ (con ψ e χ formule) allora $\mathcal{M}, \gamma \models \varphi$ se e solo se $\mathcal{M}, \gamma \models \psi$ o $\mathcal{M}, \gamma \models \chi$
- Se φ è della forma $\forall x(\psi)$ (dove ψ è una formula) allora $\mathcal{M}, \gamma \models \varphi$ se e solo se per ogni elemento $m \in D$ vale $\mathcal{M}, \gamma[x/m] \models \psi$

- Se φ è della forma $\exists x(\psi)$ (dove ψ è una formula) allora $\mathcal{M}, \gamma \models \varphi$ se e solo se esiste un elemento $m \in D$ tale che $\mathcal{M}, \gamma[x/m] \models \psi$
- Infine se φ è un letterale $p(\tau_1, ..., \tau_n)$ allora $\mathcal{M}, \gamma \models \varphi$ se e solo se $p^I({\tau_1}^I_\gamma, ..., {\tau_n}^I_\gamma)$

Data una formula φ si dice che un modello $\mathcal{M}$ soddisfa φ o anche che $\mathcal{M}$ è un modello di φ se e solo se $\mathcal{M}$ è appropriato per φ e $\mathcal{M}, \gamma \models \varphi$ per ogni contesto γ, in notazione $\mathcal{M} \models \varphi$. Una formula è detta *soddisfacibile* se esiste un modello che la soddisfa. Una formula è detta *valida* se ogni modello la soddisfa. La relazione di conseguenza logica, equivalenza, equisoddisfacibilità e soundness sono definite in modo analogo alla logica proposizionale cambiando la parola 'assegnamento' con 'modello'.

Così come è stata posta questa semantica la soddisfacibilità per formule con variabili libere non è ben definita. Per ovviare a questa cosa si potrebbe estende la definizione di soddisfacibilità per formule con variabili libere. Dato un modello $\mathcal{M}$ appropriato ad una formula φ si dice che $\mathcal{M}$ soddisfa φ se e solo se

- Se la formula non contiene variabili libere allora la definizione di soddisfacibilità rimane invariata.
- Se φ contiene variabili libere allora $\mathcal{M} \models \varphi$ se e solo se per ogni contesto γ che contiene almeno ogni variabile libera di φ vale $\mathcal{M}, \gamma \models \varphi$.

In questo modo fomule con variabili libere divengono uguali in termini di semantica alle stesse formule con le variabili libere quantificate universalmente. Da questo momento in poi ogni variabile libera presente in una formula verrà considerata come vincolata da un quantificatore universale posto all'inizio della formula.

Un'altra osservazione interessante è che se nella formula sono presenti esclusivamente predicati costanti e simboli logici allora il modello si comporta esattamente come un'assegnazione proposizionale. In questo caso è sufficiente rimuovere eventuali quantificatori e cambiare i simboli di predicato da p a s mantenendo l'indice e si ottiene una formula proposizionale che, ha una assegnazione se e solo se la formula originale ha un modello. È possibile estendere questa considerazione anche alle formule ground, ovvero formule senza variabili. Infatti se ogni predicato ground viene sostituito da un nuovo simbolo di costante proposizionale allora la formula proposizionale risultante si comporterà, in termini di soddisfacibilità, esattamente come la formula originale. Ad esempio la formula ground $(p_1(f_2) \vee p_2(f_3, f_1(f_2))) \wedge \neg p_1(f_2) \wedge p_3$ è esattamente equivalente alla formula proposizionale $(s_2 \vee s_3) \wedge \neg s_2 \wedge s_1$, nel senso che per ogni assegnamento per la seconda formula esiste un modello per la prima e viceversa.

1.2.4 Skolemizzazione e Forme Normali

In questo paragrafo verrà descritta una procedura fondamentale per la dimostrazione automatica di teoremi, la *Skolemizzazione*. Varrà inoltre introdotta una nuova forma normale chiamata *PNF* e verranno estese le forme normali descritte nel paragrafo della logica proposizionale per adattarle alla logica del primo ordine.

La definizione per le forme ENNF e NNF per la logica del primo ordine è pressoché identica a quella della logica proposizionale. Come per la logica proposizionale, la trasformazione di una formula in ENNF/NNF preserva la relazione di conseguenza logica ed è sempre possibile trasformare una formula in una equivalente in ENNF/NNF. Il calcolo per la normalizzazione viene effettuato allo stesso modo ma con l'aggiunta di due regole per la negazione dei quantificatori:

$$\neg\forall x(\varphi) \vdash \exists x(\neg\varphi)$$
$$\neg\exists x(\varphi) \vdash \forall x(\neg\varphi)$$

Chiameremo *prefisso di quantificatori* una lista di quantificatori (es. $\forall x_1 \forall x_2 \exists x_3$). Un prefisso viene detto *universale* se è composto esclusivamente da quantificatori universali e viene detto *esistenziali* se è composto esclusivamente da quantificatori esistenziali. Una formula è in formato PNF (Prenex Normal Form) se tutti e soli i quantificatori si trovano all'inizio della formula. La classe di formule PNF è generata dalla seguente grammatica:

$$P_0 := \rho(P)$$
$$P := \top \mid \bot \mid A \mid \neg P \mid (P \wedge P) \mid (P \vee P)$$

Dove ρ è un prefisso di quantificatori e A è un atomo. La parte della formula generata dalla seconda regola viene spesso chiamata *matrice*. È sempre possibile normalizzare una formula in PNF, è un processo sound, ma non è sempre possibile mantenere la relazione di conseguenza logica.

La skolemizzazione è una procedura che permette di eliminare i quantificatori esistenziali da una formula. Sia ρ un prefisso di quantificatori qualunque, la funzione $sk : F' \to F'$ può essere descritta in questo modo:

- Se la formula è del tipo $\exists x(\rho\phi)$ allora sk rimuove il primo quantificatore esistenziale e sostituisce la variabile x all'interno della formula con una nuova costante f_{n+1}, dove n è il massimo indice di costante presente nella formula.
- Se la formula è del tipo $\forall x_k ... x_{k+m-1} \exists x_{k+m}(\rho\phi)$ allora sk rimuove il primo quantificatore esistenziale in ordine lessicografico e si sostituisce la variabile

x_{k+m} all'interno della formula con una nuova funzione $f_{n+1}(x_k, ..., x_{k+m-1})$ $m-1$-aria, dove n è il massimo indice di funzione presente nella formula.

Applicando la funzione sk tante volte quanto il numero di quantificatori esistenziali presenti nella formula si ottiene una formula senza quantificatori esistenziali. Anche la skolemizzazione è un processo sound, ma non è detto che preservi la conseguenza logica.

Combinando le tecniche apprese finora è possibile definire una procedura di normalizzazione che permette di trasformare una formula del primo ordine in formato CNF. Le formule CNF per il primo ordine sono definite come segue:

$$\zeta_0 := \rho(\zeta_1)$$
$$\zeta_1 := \xi \mid (\xi \wedge \zeta_1)$$
$$\xi := \top \mid \bot \mid L \mid (\xi \vee \xi)$$

Dove ρ è un prefisso di quantificatori universale e L un letterale. Per ottenere una formula CNF è sufficiente:

1. Normalizzare la formula in NNF
2. Normalizzare la formula in PNF
3. Skolemizzare la formula
4. Applicare lo stesso algoritmo di clausificazione descritto per la logica proposizionale sulla matrice della formula

Visto le tecniche applicate il processo di clausificazione per la logica del primo ordine è sound ma non preserva la conseguenza logica. Dato che in una formula CNF tutte le variabili sono universalmente quantificate per brevità è possibile omettere il prefisso di quantificatori. Ad esempio, la formula CNF $\forall x_1 x_2 x_3 x_4(\neg p_1(x_1) \vee p_2(x_2) \vee p_3(x_3)) \wedge (\neg p_4(x_4))$ può essere scritta come $(\neg p_1(x_1) \vee p_2(x_2) \vee p_3(x_3)) \wedge (\neg p_4(x_4))$ e quindi rappresentata in forma insiemistica come $\{\{\neg p_1(x_1), p_2(x_2), p_3(x_3)\}, \{\neg p_4(x_4)\}\}$. Un'osservazione interessante è che visto che tutte le variabili sono universalmente quantificate, è possibile rinominare le variabili di clausole diverse senza cambiare il significato della formula. È quindi possibile normalizzare le clausole in modo tale che ogni coppia di clausole contenga variabili diverse. Un caso d'uso tipico è quello di voler unificare due letterali di due clausole diverse. Con l'assunzione che le variabili siano tutte diverse è possibile applicare l'algoritmo di unificazione senza occurrence-check visto nel capitolo sull'Unificazione.

1.3 Soddisfacibilità e Validità

Nei precedenti capitoli si è data la definizione di soddisfacibilità e validità per formule proposizionali e del primo ordine. In questa sezione verrà approfondito il discorso e verranno introdotte alcune nozioni fondamentali per capire il funzionamento di un *ATP system* (Automatic Theorem Prover), nonché per capire le motivazioni che hanno spinto la creazione di sistemi ATP e i vincoli teorici con cui si devono confrontare. Questa non vuole essere una trattazione esaustiva dei teoremi di incompletezza di Gödel o della teoria della computazione, ma una panoramica generale discorsiva e informale. Il contesto storico è stato estrapolato dai famosi best-seller di *Douglas Hofstadter 'Gödel, Escher, Bach: un'Eterna Ghirlanda Brillante'* [4] e *Martin Davis 'Il calcolatore universale'* [3] mentre i dettagli tecnici sono stati presi dal libro di *Dirk van Dalen 'Logic and Structure'* [10].

Il problema della soddisfacibilità/validità è il problema di determinare se una formula è soddisfacibile/valida o meno (Una tautologia nel caso della logica proposizionale). Sorge spontanea la domanda: *È possibile creare una procedura di decisione che risolva questo problema?*

In primo luogo è bene specificare che il problema della validità è riducibile al problema della soddisfacibilità. Si immagini di voler dimostrare che una formula $\varphi = (A_1 \wedge ... \wedge A_n) \Rightarrow C$ è valida. Nel caso fosse valida allora la sua negazione $A_1 \wedge ... \wedge A_n \wedge \neg C$ sarebbe insoddisfacibile. Nel caso $\neg\varphi$ fosse soddisfacibile allora esisterebbe un modello $\mathcal{M}$ tale che $\mathcal{M} \models \neg\varphi$ che quindi per definizione $\mathcal{M} \not\models \varphi$. In tal caso φ non è valida. In altre parole se un'implicazione è vera allora non è possibile che le premesse siano vere e la conclusione falsa. Tecniche dimostrative del genere sono dette di *Refutazione* o prove per *Assurdo*. Esistono anche altre tecniche dimostrative ma la quasi totalità degli ATP si basano sulla refutazione.

Nel caso della logica proposizionale la risposta alla domanda precedente è affermativa, anche se il problema equivalente *Circuit-SAT* è stato dimostrato essere *NP-completo* dal noto teorema *Cook-Levin*. Data una formula proposizionale di n costanti esistono al massimo 2^n possibili assegnazioni quindi un approccio naive per risolvere il problema della soddisfacibilità potrebbe essere quello di creare un algoritmo brute-force che prova tutte le possibili assegnazioni di verità. Altri metodi verranno discussi nel capitolo 1.4. Nel contesto della logica del primo ordine, la risposta è intricata e la sua soluzione è considerata uno dei risultati più significativi del secolo scorso, rilevante nel campo della matematica, della logica e della filosofia.

Agli inizi del 900' il matematico David Hilbert pubblicò un articolo in cui elencava 23 problemi matematici, all'epoca aperti, che avrebbero dovuto guidare la ricerca matematica del secolo successivo. Il secondo problema di Hilbert era il seguente:

È possibile dimostrare la coerenza dell'insieme degli assiomi dell'aritmica?

La domanda di Hilbert si riferisce al sistema di assiomi dell'aritmetica basati sulla logica del primo ordine proposti nei tre volumi di *Principia Mathematica* (PM) di Bertrand Russell e Alfred North Whitehead. L'indagine del problema portò il suo risolutore, il logico Kurt Gödel, alla scoperta di due importanti risultati.

Il primo risultato, detto *Primo teorema di incompletezza* afferma che:

In ogni sistema formale consistente che contiene un'aritmetica elementare, esiste una formula che non è dimostrabile in quel sistema.

Il secondo risultato, detto *Secondo teorema di incompletezza* afferma che:

Se un sistema formale consistente contiene un'aritmetica elementare, allora non può dimostrare la propria coerenza.

Per capire il senso dei due teoremi è necessario introdurre, i concetti di *Teoria*, *Teorema* e *Sistema formale*. Un sistema formale è un insieme di questi quattro elementi:

- Un alfabeto di simboli.
- Delle regole per la generazione di stringhe dette formule.
- Un insieme di formule dette assiomi.
- Un insieme di regole sintattiche dette d'inferenza che associano formule ad altre formule.

Se si considerano ad esempio le regole sintattiche definite in 1.1.1, la regola d'inferenza del modus ponens della sezione 1.1.2 e come insieme di assiomi le formule proposizionali $\{s_1, s_1 \Rightarrow s_2\}$ si ottiene a tutti gli effetti un sistema formale basato sulla logica proposizionale. Un *Teorema* è un assioma o una qualunque formula che può essere ottenuta applicando un numero finito di volte le regole d'inferenza agli assiomi. Nell'esempio precedente s_2 è un teorema del sistema formale $(s_1, (s_1 \Rightarrow s_2) \vdash s_2)$. Una derivazione sintattica di questo tipo è detta *Dimostrazione*. Per coerenza si intende la proprietà che il sistema non possa dimostrare una contraddizione, come una formula del tipo $\psi \wedge \neg\psi$. Una *Teoria* è un insieme T di formule che rispetta le seguenti proprietà:

1. $\mathcal{A} \subseteq T$ contiene gli assiomi.
2. Per ogni $P \in T^n$ se $P \vdash C$ per qualche regola d'inferenza del sistema formale allora $C \in T$ (Chiusura rispetto la derivazione).

Rispetto l'esempio precedente l'insieme $\{s_1, s_1 \Rightarrow s_2\, s_2\}$ è una teoria. In notazione si scrive $\vdash_T \varphi$ per indicare che la formula φ è dimostrabile nella teoria T.

Tornando alla tesi di Gödel, essa si basa sulla costruzione di una codifica delle formule e delle dimostrazioni di PM nello stesso linguaggio formale PM. Ogni formula (e regola di inferenza) φ viene mappata in un numero naturale $\ulcorner\varphi\urcorner$. In particolare grazie a questa codifica riesce a formalizzare i seguenti predicati all'interno di PM stesso:

- $Proof(x, y)$ che è vero se e solo se x è la codifica di una dimostrazione di una formula codificata in y.
- $Thm(x)$ che è vero se e solo se esiste $y \in \mathbb{N} : Proof(y, x)$
- $Cons$ che è vero se e solo se il sistema è consistente. Si può anche dire che $Cons$ è vero sse $\neg Thm(\ulcorner 0 = 1\urcorner)$

Un lemma fondamentale per la dimostrazione dei teoremi di Gödel è il *Teorema del punto fisso*:

> Per ogni formula φ con un unica variabile libera x allora esiste una formula γ tale che: $\vdash_{PM} \gamma \Leftrightarrow \varphi[x/\ulcorner\gamma\urcorner]$

Se si applica il teorema del punto fisso alla formula $\neg Thm(x)$ si ottiene:

> Esiste una formula γ tale che $\vdash_{PM} \gamma \Leftrightarrow \neg Thm(\ulcorner\gamma\urcorner)$

γ è chiamato *enunciato gödeliano* e in pratica afferma "sono vero se e solo se non sono dimostrabile". Spesso il predicato gödeliano viene associato al *paradosso del mentitore* che è oggetto di studi e dibattiti nell'ambito della filosofia da oltre 2000 anni. Il primo teorema di incompletezza si può quindi riformulare in questo modo:

1. Se PM (o un sistema simile) è coerente allora $\nvdash_{PM} \gamma$ e $\nvdash_{PM} \neg\gamma$

Mentre secondo si può riformulare in questo modo:

2. Se PM (o un sistema simile) è coerente allora $\nvdash_{PM} Cons$

Si potrebbe fare un discorso molto lungo su cosa significhi *'un sistema simile a PM'* ma ciò richiederebbe una dettagliata esplorazione delle dimostrazioni dei teoremi di Gödel e un approfondimento nella Teoria della *Computabilità*. Tuttavia, eviteremo di approfondire ulteriormente su questi argomenti.

In sintesi i teoremi di Gödel evidenziano i limiti di metodi sintattici per la dimostrazione di teoremi all'interno di un sistema formale. Erroneamente si potrebbe pensare che i teoremi provino l'esistenza di formule indimostrabili con ogni metodo, ma in realtà non mostrano nessuna limitazione sul fatto che una formula sia dimostrabile ad esempio in un altro sistema formale o con metodi semantici.

A chiudere il cerchio tra sistemi formali, aritmetica e logica arriva in aiuto il teorema di Church sull'indecidibilità della logica del primo ordine:

Teorema di Church 1. *La logica del primo ordine è indecidibile.*

Il teorema di Church afferma che non esiste un algoritmo che, dato un qualunque enunciato φ di una qualunque teoria T, determini se φ è dimostrabile in T. La prova si basa sull'applicazione del primo teorema di incompletezza di Gödel al sistema formale Q creato dal logico Raphael Robinson. Q è un sistema formale che contiene un'aritmetica elementare descritta da un numero finito di assiomi (al contrario di PM che ne contiene infiniti), Si assuma che $\{q_1, ..., q_n\}$ siano gli assiomi di Q e φ una qualunque formula. Se esistesse una procedura di decisione per la logica allora varrebbe:

$$q_1, ..., q_n \vdash \varphi \text{ se e solo se } \vdash (q_1 \wedge ... \wedge q_n) \Rightarrow \varphi$$

Quindi esisterebbe una procedura di decisione anche per Q, ma in Q vale il primo teorema di Gödel e quindi si giunge a una contraddizione visto che si potrebbe provare il predicato godeliano, $\vdash_Q \gamma$ o $\vdash_Q \neg\gamma$. Ciò discende anche dal fatto che il predicato Thm è *parzialmente calcolabile* ma non *calcolabile*, di conseguenza l'insieme che ha come funzione caratteristica Thm è *ricorsivamente enumerabile* ma non *ricorsivo*. Quindi si può concludere dicendo che la logica del primo ordine è semidecidibile ma non decidibile.

Il teorema di Church ha delle importanti conseguenze sui sistemi di dimostrazione automatica. Un ATP infatti può essere visto come un algoritmo di manipolazione sintattica che cerca di dimostrare la validità di una formula tramite un sistema di inferenze, ma il teorema di Church afferma che, per quanto sofisticato, esisteranno sempre degli input per cui l'algoritmo non terminerà. Questa limitazione rappresenta una barriera fondamentale nell'ambito della dimostrazione automatica.

1.4 Resolution e Dimostrazione Automatica

Resolution o *Risoluzione* è una regola d'inferenza per logica proposizionale e del primo ordine. La regola per la logica proposizionale è la seguente:

$$\frac{\{L\} \cup C_1, \{\neg L\} \cup C_1}{C_1 \cup C_2}$$

Dove C_1 e C_2 sono clausole in notazione insiemistica e L è un letterale. La regola afferma che se si hanno due clausole dove una contiene un letterale e l'altra la sua negazione allora è possibile ottenere una nuova clausola che è l'unione delle due clausole senza il letterale e la sua negazione. Resolution preserva la conseguenza. Con il nome Resolution spesso ci si riferisce anche ad una classe di algoritmi che

sfrutta questa regola come inferenza principale per risolvere il problema della soddisfacibilità. Un famoso esempio di algoritmo per la logica proposizionale basato su Resolution è l'algoritmo di Davis-Putnam anche chiamato *DPP* (Davis-Putnam-Procedure). La DPP in sintesi procede in questo modo:

1. Si trasforma la formula una CNF equivalente
2. Si eliminano le clausole tautologiche (Quelle che contengono sia un letterale che la sua negazione $l \vee \neg l$).
3. Si sceglie un qualunque letterale L da una qualunque clausola nella formula ϕ ottenuta nel punto precedente.
4. Si calcolano gli insiemi $S = \{C \in \phi \mid l \notin C \text{ e } \neg l \notin C\}$ e $T = \phi \setminus S$.
5. Si calcola l'insieme $R = \{(C_1 \setminus \{L\}) \cup (C_2 \setminus \{\neg L\}) \mid C_1, C_2 \in T \text{ e } L \in C_1 \text{ e } \neg L \in C_2\}$, detto dei risolventi, applicando la regola di Resolution.
6. Si riapplica la procedura dal punto 2. con la nuova formula $\phi' = S \cup R$ finchè o $\phi' = \{\}$ o ϕ' contiene una clausola vuota.

Se l'algoritmo termina con una clausola vuota vuol dire che nel passo precedente la formula conteneva due clausole del tipo $L \wedge \neg L$, quindi la formula originale è insoddisfacibile. Se l'algoritmo termina con $\phi' = \{\}$ allora la formula originale è soddisfacibile. L'algoritmo seppur corretto è molto inefficiente e non viene utilizzato nella pratica, ma è stato il primo basato su Resolution per il problema della soddisfacibilità. I SAT solver (programmi che risolvono il problema della soddisfacibilità) si basano su tecniche più raffinate e spesso non sono bassati su Resolution. Un esempio è l'algoritmo *DPLL* (Davis-Putnam-Logemann-Loveland) che si basa sulle tecniche di *unit propagation* e *pure literal elimination*.

Per la logica del primo ordine, come al solito, il discorso è più complesso. I primi tentativi di creare un algoritmo per determinare la soddisfacibilità di una formula del primo ordine si devono ai risultati teorici dei logici Skolem, J. Herbrand e R. Robinson. I risultati di Herbrand permettono di 'ridurre' il problema della soddisfacibilità di formule universalmente quantificate al problema della soddisfacibilità di una formula proposizionale. La strategia si basa sulla creazione di un modello il quale dominio, detto universo di Herbrand, è generato da tutti i termini ground ottenibili galla combinazione dei termini della formula originale. L'universo di Herbrand è un insieme finito (se la formula non contiene funzioni) o infinito numerabile. Il secondo passo è chiamato istanziazione ground e consiste nel sostituire tutte le variabili con un sottoinsieme finito di elementi dell'universo di Herbrand. Si ottiene così una formula ground che, come descritto in 1.2.3, può essere trasformata in una formula proposizionale e risolta da un Sat Solver. Se il Sat solver trova un'assegnazione che soddisfa la formula allora si sceglie un altro sottoinsieme finito diverso dal precedente dell'universo di Herbrand e si ripete il

procedimento. Se il Sat solver non trova un'assegnazione allora la formula originale è insoddisfacibile. Se si verificano tutti i sottoinsiemi finiti dell'universo di Herbrand senza trovare formule insoddisfacibili allora la formula originale è soddisfacibile.

È chiaro che la strategia di Herbrand è più un risultato teorico che un metodo pratico. L'unico caso in cui è garantita la terminazione è quando la formula non contiene funzioni e quindi l'universo di Herbrand è finito, così come il numero di tutti i sui sottoinsiemi. I primi algoritmi utilizzabili nella pratica iniziarono a nascere dopo che Robinson introdusse la regola di risoluzione per la logica del primo ordine:

$$\frac{\{L(\tau_1, ..., \tau_n)\} \cup C_1, \{\neg L(\omega_1, ..., \omega_n)\} \cup C_1}{(C_1 \cup C_2)^\sigma}$$

Dove σ è un unificatore dei due letterali $L(\tau_1, ..., \tau_n)$ e $L(\omega_1, ..., \omega_n)$ e C_1, C_2 sono clausole. Anche per la logica del primo ordine la regola di risoluzione è corretta e preserva la conseguenza logica. Da qui vi è un punto di svolta nello sviluppo degli ATP. Il primo ATP ad alte prestazioni basato su Resolution per la logica del primo ordine fu *Otter* sviluppato da William McCune. Otter fa parte di una classe di theorem prover basati sulla *Saturazione*. La saturazione è una tecnica concettualmente molto semplice che consiste nel generare tutte le clausole possibili a partire da un insieme di clausole iniziali. Se la formula è insoddisfacibile allora prima o poi verrà generata una clausola vuota. Se la formula è soddisfacibile allora vi sono due casi possibili. Nel primo caso l'algoritmo genera tutte le clausole generabili (satura il sistema) e l'algoritmo termina. Nel secondo caso il numero di clausole generabili dal sistema iniziale non è un numero finito. In tal caso o l'algoritmo capisce che alcune aree di ricerca non porteranno mai alla generazione di una clausola vuota e quindi termina, oppure, nell'ipotesi peggiore, l'algoritmo non termina mai rimanendo in un loop infinito. Quest'ultima è una conseguenza inevitabile dei teoremi di Church e Gödel. Una descrizione più dettagliata di Otter verrà data nel capitolo 3 sull'implementazione di Vampire.

1.5 Il formato TPTP

In questa sezione verrà descritto il formato TPTP [9] (Thousands of Problems for Theorem Provers) per la rappresentazione di problemi di logica del primo ordine. TPTP è una nota libreria di problemi utilizzata per testare e valutare diversi ATP systems (Automatic Theorem Prover). TPTP fornisce diversi formati per la rappresentazione dei problemi, in questa sezione ci si soffermerà sui formati *CNF* (Clausal Normal Form) e *FOF* (First Order Formula).

La traduzione dei predicati, termini e variabili è la stessa sia per il formato CNF che per il formato FOF. Ogni variabile è rappresentata da una stringa alfanumerica Maiuscola. Simboli di funzione, predicato e costanti sono tutti rappresentati senza distinzione da stringhe alfanumeriche minuscole. Le regole della grammatica della generazione dei termini è esattamente la stessa vista nel paragrafo 1.2.1. Per esempio il predicato $p_1(f_1(x_1), x_2, p_2)$ può essere rappresentato come `p1(f1(X1), X2, p2)` o anche `pred(fun(VAR_A), VAR_B, costante)`.

Per la traduzione dei simboli logici si utilizza la seguente mappatura:

Simbolo	Traduzione
$\top$	`$true`
$\bot$	`$false`
$\neg$	`~`
$\wedge$	`&`
$\vee$	`|`
$\Rightarrow$	`=>`
$\Leftrightarrow$	`<=>`
$\oplus$	`<~>`
$\forall$	`!`
$\exists$	`?`

Tabella 1.1: Traduzione dei simboli logici

Anche le regole per la generazione delle formule sono le stesse viste nella sezione 1.2.1, con l'unica differenza che i simboli logici vengono tradotti secondo la tabella 1.1. Le parentesi '(' e ')' possono essere omesse e in tal caso si segue il seguente ordine di valutazione dei simboli: `!`, `?`, `~`, `&`, `|`, `<=>`, `=>`, `<~>`. Dopo un quantificatore (`!`/`?`) è necessaria la lista delle variabili quantificate racchiuse tra parentesi quadre '[' e ']' seguite da ':' e la formula quantificata. Per esempio la formula $\forall x_1 x_2 \exists x_3 (p_1(x_1) \vee p_2(x_2) \vee p_3(x_3))$ viene rappresentata come `![X1, X2] : (?[X3] : (p1(X1) | p2(X2) | p3(X3)))`. Se non presenti quantificatori nella formula le variabili libere vengono considerate quantificate universalmente.

Il formato FOF prevede una lista di assiomi seguiti da una congettura. Il formato cambia a seconda della domanda che si vuole porre all'ATP. Data una lista di assiomi $A_1, ..., A_n$ e una congettura C:

- Se si da in input la lista di assiomi $A_1, ..., A_n$ l'ATP cerca di determinare la Soddisfacibilità della formula $A_1 \wedge ... \wedge A_n$.
- Se vengono dati sia gli assiomi che la congettura l'ATP cerca di determinare se $A_1 \wedge ... \wedge A_n \Rightarrow C$ è valida.
- Se invece viene data solo la congettura l'ATP cerca di determinare se C è valida.

Il formato per inserire un assioma o la congettura è il seguente:

```
fof(<nome>, <tipo>, <formula>).
```

'Nome' è una stringa alfanumerica che identifica la formula, 'tipo' può essere `axiom` per gli assiomi e `conjecture` per la congettura. 'Formula' è una formula del primo ordine in formato FOF. Ad esempio con il file di input:

```
fof(ax1, axiom, p(X)).
fof(ax2, axiom, p(X) => q(X)).
fof(conj, conjecture, q(X)).
```

L'ATP cercherà di determinare se la formula $(p(X) \wedge (p(X) \Rightarrow q(X))) \Rightarrow q(X)$ è valida. Per le formula CNF invece il formato è il seguente:

```
cnf(<nome>, axiom, <clausola>).
```

Dove 'nome' è definito come per il formato FOF e 'clausola' è una clausola del primo ordine. L'unico tipo consentito è `axiom` e non è possibile inserire una congettura. In questo formato ogni clausola deve essere scritta in un'annotazione separata. Ad esempio lo stesso problema dell'esempio precedente può essere posto all'ATP in questo modo:

```
cnf(ax1, axiom, p(X)).
cnf(ax2, axiom, ~p(X) | q(X)).
cnf(conj, axiom, ~q(X)).
```

Capitolo 2

Algoritmo di decisione di Frammenti Binding

Nella sezione 1.3, sono stati esaminati i teoremi di Gödel e Church, mentre nella sezione 1.4 sono state viste alcune delle loro conseguenze. La logica del primo ordine è intrinsecamente indecidibile; tuttavia, è possibile identificare alcune sue componenti che risultano decidibili. Queste componenti sono dette *Frammenti* della logica del primo ordine. Si pensi ad esempio ai risultati di Herbrand citati nella sezione 1.4. Se una formula non contiene funzioni ed è universalmente quantificata allora l'universo di Herbrand è finito e vi sono un numero finito di possibili instanziazioni ground. In questo caso determinare la soddisfacibilità di una formula di questo tipo è riducibie al problema della soddisfacibilità proposizionale che è notoriamente decidibile. In letteratura questo frammento è noto come *Bernays–Schönfinkel Fragment*. Altre esempi di frammenti decidibili sono il *Monadic Fragment*, il *Two-variable Fragment*, *Unary negation fragment* e il *Guarded Fragment*. In questo capitolo verrà descritta una famiglia di frammenti relativamente recente chiamata *Binding Fragments* [6] [2].

2.1 Tassonomia dei Frammenti Binding

Si dice che una formula del primo ordine appartiene alla classe *Boolean Binding* (BB) se generata dalla seguente grammatica:

$$\varphi := \top \mid \bot \mid (\varphi \vee \varphi) \mid (\varphi \wedge \varphi) \mid \mathcal{P}(\psi)$$
$$\psi := \rho \mid (\psi \vee \psi) \mid (\psi \wedge \psi)$$

Dove $\mathcal{P}$ è un prefisso di quantificatori e ρ è una combinazione booleana di letterali che hanno come argomento tutti la stessa lista di termini. Una formula

di questo tipo verrà chiamata con il nome τ-Binding, dove τ indica la lista di termini comune. Ad esempio sono $(f_1(x_1), f_2)$-Binding le formule: $p_1(f_1(x_1), f_2)$, $p_1(f_1(x_1), f_2) \vee \neg p_3(f_1(x_1), f_2)$. Per semplicità di scrittura è possibile omettere la lista di termini comune e posizionarla in notazione postfissa:

$$p_1(f_1(x_1), f_2) \vee \neg p_3(f_1(x_1), f_2) \text{ diventa } (p_1 \vee \neg p_3)(f_1(x_1), f_2)$$

Con $\mathcal{B}^\tau$ verrà indicato l'insieme di tutte le formule τ-Binding. Si definisce la funzione $term : \mathcal{B}^\tau \to T^n$ che associa ogni τ-Binding alla sua lista di termini comune τ. Ad esempio $term((p_1 \vee \neg p_3)(f_1(x_1), f_2)) = (f_1(x_1), f_2)$. Verranno chiamati impropriamente τ-Binding anche formule universalmente quantificate la cui matrice è un τ-Binding. In questo caso ci si riferisce esclusivamente alla matrice della formula eliminando i quantificatori.

I frammenti Binding possono essere ottenuti restringendo le regole di ψ:

- Il frammento *One Binding* (1B) viene ottenuto restringendo la seconda formula a $\psi := \rho$
- Il frammento *Conjunctive Binding* (CB o $\wedge$B) viene ottenuto restringendo la seconda formula a $\psi := \rho \mid (\psi \wedge \psi)$
- Il frammento *Disjunctive Binding* (DB o $\vee$B) viene ottenuto restringendo la seconda formula a $\psi := \rho \mid (\psi \vee \psi)$

Un'istanza particolare del frammento 1B è quando la formula non contiene quantificatori esistenziali. Una formula 1B con soli prefissi universali viene detta del frammento *Universal One Binding* ($\forall 1B$).

2.2 Soddisfacibilità dei frammenti Binding

In questa sezione verrà analizzato il problema della soddisfacibilità dei frammenti binding. In particolare verrà descritto l'algoritmo di decisione per i frammenti 1B e CB che è il soggetto principale dello studio di questa tesi.

Data una formula del frammento 1B è facile osservare che il processo di skolemizzazione converte la formula in formato $\forall 1B$. Se si applica la stessa procedura ad una formula CB, le sottoformule generate dalla regola ψ saranno del tipo: $\mathcal{P}(\rho_1 \wedge ... \wedge \rho_n)$ con $\mathcal{P}$ un prefisso universale e $(\rho_1 \wedge ... \wedge \rho_n)$ τ-Binding. In questo caso è possibile distribuire il '$\forall$' sui vari τ-Binding e si ottiene così una formula equisoddisfacibile in formato $\forall$1B.

Teorema: Decidibilità dei frammenti 1B e CB 2.2.1. *I frammenti 1B e CB sono frammenti decidibili del primo ordine.*

Una dimostrazione dettagliata di questo teorema può essere trovata nell'articolo [2]. Si può osservare che il processo di clausificazione del primo ordine porta alla generazione di una formula equisoddisfacibile che rispetta il formato DB. Ne consegue immediatamente per il teorema di Church:

Teorema: Indecidibilità del frammento Disjunctive Binding 2.2.2. *Il frammento DB è un frammento indecidibile del primo ordine.*

Dimostrazione. Per assurdo Esiste un algoritmo di decisione totale S per formule del frammento DB. Data una qualunque formula φ è possibile trasformarla in una equisoddisfacibile in formato CNF. Se si distribuisce il quantificatore universale sulle clausole si ottiene una formula φ' che rispetta i requisiti sintattici del frammento DB. S è quindi una procedura di decisione totale per tutta la logica del primo ordine ma ciò è in contraddizione con il teorema di Church. □

Il processo di skolemizzazione consente di concentrarsi sullo studio del frammento $\forall$1B per la risoluzione del problema della soddisfacibilità. Prima di descrivere l'algoritmo bisogna introdurre tre nuovi concetti: L'Unificazione per τ-Binding, Implicante di una formula del primo ordine e la conversione booleana di un τ-Binding. Data una formula del primo ordine φ per Implicante di φ si intende la conversione del primo ordine di un implicante della 'struttura proposizionale esterna'. ad esempio la formula $\forall x_1(p_1(x_1) \vee p_2(x_1)) \wedge (p_1(f_1) \vee \exists x_2(p_3(x_2))) \wedge \neg p_1(f_1) \wedge \exists x_2(p_3(x_2))$ ha la seguente struttura booleana $s_1 \wedge (s_2 \vee s_3) \wedge \neg s_2 \wedge s_3$. Un implicante (e anche il solo) di questa formula è l'insieme $\{s_1, s_3\}$ che ri-convertito nel primo ordine diventa l'insieme $\{\forall x_1(p_1(x_1) \vee p_2(x_1)), \exists x_2(p_3(x_2))\}$. In questo caso è stata creata implicitamente un bi-mappa tra costanti proposizionali e formule del primo ordine:

- $s_1 \rightleftarrows \forall x_1(p_1(x_1) \vee p_2(x_1))$
- $s_2 \rightleftarrows p_1(f_1)$
- $s_3 \rightleftarrows \exists x_2(p_3(x_2))$

Un τ_1-Biding e un τ_2-Biding sono detti unificabili se e solo se l'insieme congiunto di tutti i loro letterali è unificabile. Si può anche dire che sono unificabili sse le due liste τ_1 e τ_2 hanno la stessa lunghezza n e dato un qualunque predicato p n-ario $p(\tau_1)$ e $p(\tau_2)$ sono unificabili. Una insieme di τ-Biding è unificabile sse esiste una sostituzione che unifica a due a due tutti gli elementi dell'insieme. Dato un τ-Binding ϕ la sua conversione booleana $bool(\phi)$ è una formula proposizionale che si ottiene da ϕ mantenendo la sua struttura proposizionale, eliminando gli argomenti dai letterali e convertendo i simboli di predicato in simboli di costante con lo stesso indice. Ad esempio il τ-Binding $((p_1 \wedge p_4) \vee p_2 \vee \neg p_4)(\tau)$ viene convertito nella seguente formula proposizionale $(s_1 \wedge s_4) \vee s_2 \vee \neg s_4$

A questo punto è possibile enunciare il teorema di caratterizzazione della soddisfacibilità del frammento ∀1B.

Teorema: Caratterizzazione della soddisfacibilità per il frammento ∀1B 2.2.3. *Data una formula φ del frammento ∀1B, φ è soddisfacibile se e solo se:*
Esiste un implicante I dove: per ogni sottoinsieme $U \subseteq I$ di τ-Binding, se $U = \{\gamma_1, ..., \gamma_n\}$ è unificabile allora la formula proposizionale $bool(\gamma_1) \wedge ... \wedge bool(\gamma_n)$ è soddisfacibile.

Dal teorema appena descritto si estrapola intuitivamente l'algoritmo per la soddisfacibilità delle formule del frammento:

Algorithm 2: Algoritmo per la soddisfacibilità del frammento ∀1B

Firma: oneBindingAlgorithm(φ)
Input: φ una formula ∀1B
Output: $\top$ o $\bot$
foreach *I Implicant of φ* **do**
  $res := \top$;
  foreach $(U := \{\gamma_1, ..., \gamma_n\}) \subseteq I$ **do**
    if *U is unifiable* **then**
      if *$bool(\gamma_1) \wedge ... \wedge bool(\gamma_n)$ is not satisfiable* **then**
        $res := \bot$;
        Break;
      end
    end
  end
  if $res = \top$ **then**
    return $\top$
  end
end
return $\bot$

I prossimi capitoli si concentreranno sullo studio dei dettagli tecnici per l'implementazione di questo algoritmo, con annesse osservazioni sulle sfide implementative e una analisi dei risultati sperimentali ottenuti.

Capitolo 3

Il Theorem prover Vampire

Vampire [8] [5] [1] è un dimostratore di teoremi automatico per la logica del primo ordine basato sulle regole di *Resolution* e *Paramodulation*. Nasce nel 1998 come progetto di ricerca degli autori Andrei Voronkov e Alexandre Riazanov, adesso è correntemente mantenuto e sviluppato da un team più ampio presso il dipartimento di Computer Science dell'Università di Manchester. Il software è open-source, sviluppato in C++ e al momento della scrittura di questa tesi è giunto alla versione 4.8 con licenza BSD-3. Vampire incorpora un complesso sistema strutture dati, algoritmi per la manipolazione di formule e termini e un vasto sistema di inferenze. Uno dei suoi punti di forza è l'efficienza, Il team di sviluppo infatti partecipa annualmente al *CASC* (The CADE ATP System Competition), una competizione tra sistemi ATP, e fino ad ora ha sempre vinto almeno in una categoria ogni anno. Questa ambizione per l'efficienza ha influenzato molto la struttura di Vampire e la sua implementazione. Questo è sia un lato positivo che negativo, infatti se da un lato ci si ritrova con funzioni efficienti e ben ottimizzate, dall'altro lato ci si ritrova spesso con un codice complesso e difficile da comprendere che predilige la velocità alla pulizia. Ogni suo componente è riconducibile ad un articolo che ne spiega il funzionamento ad alto livello ma spesso alcune scelte implementative sono poco o per nulla documentate. Spesso lo stesso nome di una funzione o di una classe fa intuire il suo scopo e funzionamento ma non sempre è così e altrettanto spesso si è costretti a fare 'Reverse Engineering' del codice sorgente per capire come è stato utilizzato in altri contesti. Questo è un problema di cui il team di sviluppo è consapevole e negli ultimi anni sta cercando di migliorare. In questo capitolo si cercherà di dare una panoramica generale di Vampire, spiegando le sue componenti principali e come queste interagiscono tra di loro, con un focus particolare su quelle che sono state utilizzate per la realizzazione della procedura di decisione per frammenti Binding. Nella figura 3.1 è mostrata la disposizione delle cartelle di Vampire. La struttura è molto piatta ma assolutamente organizzata. Nella cartella *Kernel*

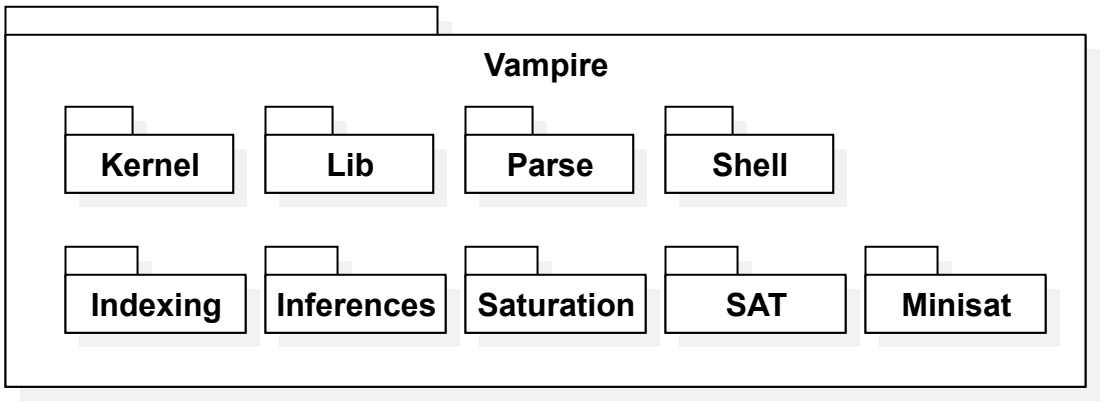


Figura 3.1: Struttura delle cartelle di Vampire.

sono presenti le componenti principali del sistema come ad esempio le strutture per le formule e i termini, e il 'Main Loop' del programma che si occupa di gestire il processso di dimostrazione. La struttura delle formule verrà trattata nella sezione 3.1. Nella cartella *Lib* sono presenti le strutture dati e le funzioni di utilità come Array, Mappe, Liste, Stack, ecc. Nella cartella *Parse* sono presenti le classi che decodificano i file TPTP. Nella cartella *Shell* sono presenti le classi per la gestione dell'input/output da riga di comando e tutte le funzioni necessarie per il Preprocessing. Gli step del preprocessing verranno approfonditi nella sezione 3.4. Nella cartella *Indexing* sono presenti i componenti per l'indicizzazione dei termini. Le particolari strutture per l'unificazione verranno trattate nella sezione 3.3. Nelle cartelle *Inferences* e *Saturation* sono presenti le classi che contengono le regole di inferenza e gli algoritmi di saturazione. Questi verranno trattati nelle sezioni 3.5 e 3.6. Nelle cartelle *SAT* e *Minisat* sono presenti le interfacce per utilizzare i SAT-Solver e il codice di Minisat, un SAT-Solver open-source. Il funzionamento dei sat solver verrà discusso nella sezione 3.6.

3.1 I Termini

I termini, insieme a clausole e formule, sono la struttura dati più importante in un dimostratore di teoremi ed è quindi fondamentale che siano rappresentati nel modo più efficiente possibile. Nella figura 3.2 è mostrata una rappresentazione ad alto livello e molto semplificata della struttura dei termini implementata in Vampire. Un termine come inteso nella sezione 1.2.1 è rappresentata dalla classe *TermList*. TermList è composto da tre elementi principali: *term*, *content* e *info*. I tre componenti sono definiti all'interno di una **union** per risparmiare memoria.

- *term* è un puntatore ad un oggetto della classe *Term*
- content è un intero di 64 bit

- info è una struttura BitField di esattamente 64 bit

Essendo definiti all'interno di una union, ogni TermList dovrebbe occupare esattamente 64 bit di memoria. In vampire ogni variabile è rappresentata da un numero intero senza segno mentre i termini complessi composti da funzioni sono rappresentati dalla classe Term. Se TermList rappresenta una variabile allora content shiftato di 2 bit a destra rappresenta l'indice di quella variabile ($content/4$), nel caso rappresenti una funzione allora term punta ad un oggetto di tipo Term che contiene l'effettiva struttura della funzione. Nella classe Term il nome della funzione è rappresentata da un intero senza segno globalmente univoco definito nella classe *Signature*. La classe Signature contiene le informazioni relative all'indice, arità e nome di funzioni e predicati. Term inoltre contiene un Array di TermList di lunghezza pari ad $arity + 1$ che rappresenta gli argomenti della funzione listati da destra verso sinistra. L'elemento in posizione 0 contiene un Termlist fittizio che contiene le info dello stesso termine.

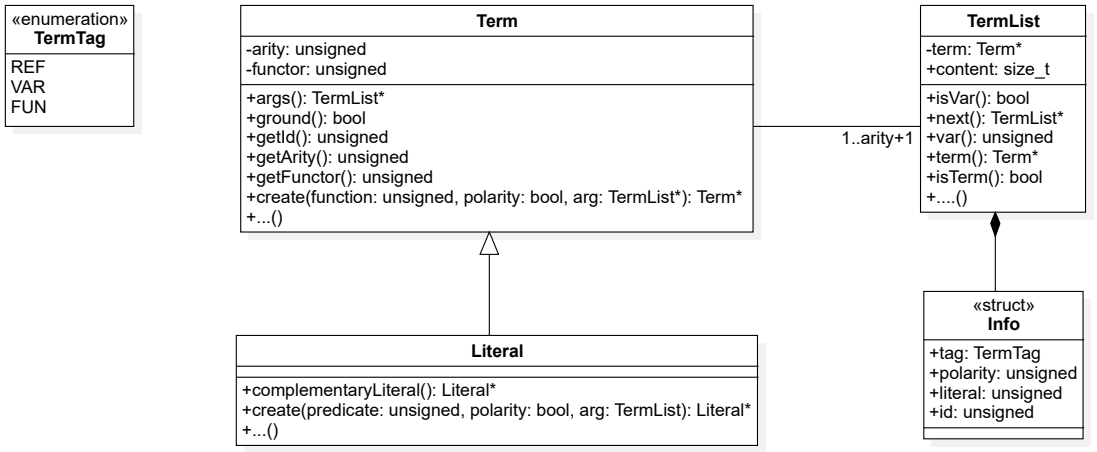


Figura 3.2: Struttura dei termini

Tutti i termini di default sono rappresentati da una struttura Perfectly Shared (come descritto in 1.2.1) per risparmiare memoria e velocizzare le operazioni di confronto. I letterali sono rappresentati dalla classe *Literal* che è una specializzazione della classe *Term*. Nell'implementazione Vampire non fa nessuna distinzione tra nomi di funzione funzioni o predicati essi sono infatti rappresentati entrambi nella Signature come funzioni. Termini e Letterali sono salvati nella Signature in strutture di indicizzazione (SubstitutionTree) per permettere un accesso veloce. Un accenno a queste strutture verrà fatto nella sezione 3.3. Literal in contiene inoltre funzioni specifiche per la manipolazione dei letterali come *complementaryLiteral* che restituisce lo stesso letterale negato (dalla struttura di indicizzazione se presente altrimenti ne crea uno nuovo). Le funzioni

Term::create e Literal::create sono le funzioni utilizzate per creare nuovi termini e letterali e inserirli nella struttura di indicizzazione.

Ad esempio, il predicato $\neg p_1(f_2, f_3(x_5), x_5, f_3(x_5))$ viene rappresentato in memoria:

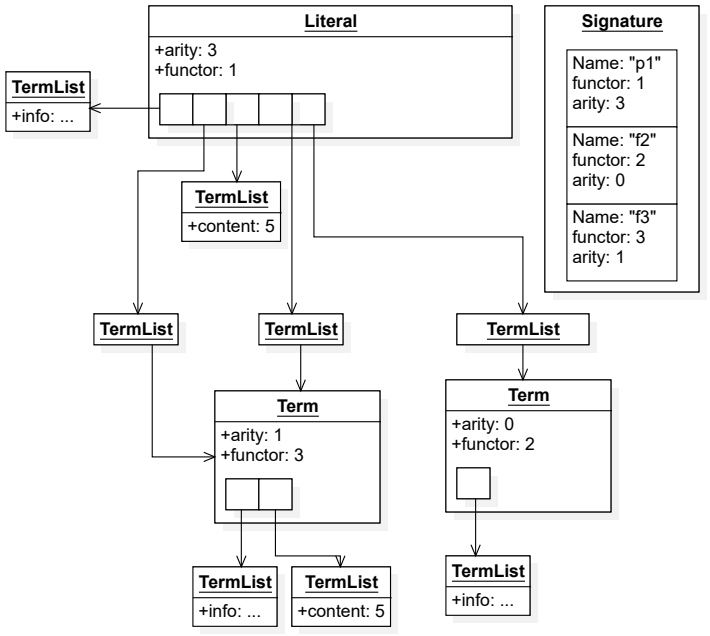


Figura 3.3: Esempio di rappresentazione di un termine

3.2 Unità, Formule e Clausole

Vampire prende in input formule del tipo $A_1 \wedge A_2 \wedge ... \wedge A_n \wedge \neg C$, dove $A_1, A_2, ..., A_n$ sono assiomi e C è la congettura, e cerca di dimostrarne l'insoddisfacibilità. Per fare ciò il problema principale viene scomposto in una lista di elementi chiamati *Unità*. Un unità è una formula o una clausola affiancata da una regola di inferenza che lo ha generata. In sostanza vi sono due tipi di inferenze, quelle che rappresentano unità date in input come *Axiom* per indicare che l'unità è un assioma in input o *Negated Conjecture* per indicare che l'unità è la negazione della congetture e quelle che rappresentano altre formule/clausole generate all'interno del processo dimostrativo. Le inferenze di questo tipo includono anche una reference alle formule che hanno generato la nuova unità, rendendo quindi possibile risalire alla dimostrazione al termine dell'esecuzione.

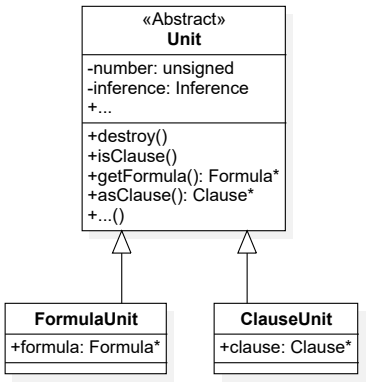


Figura 3.4: Struttura delle unità

Le unità come mostrato in figura 3.4 sono rappresentate dalla classe astratta *Unit*, che si specializza nelle classi *FormulaUnit* e *ClauseUnit* che contengono rispettivamente un puntatore ad un oggetto di tipo *Formula* e *Clause*. Le formule sono rappresentate da una struttura ad albero esattamente come quelle vista in 1.1.1 e 1.2.1. La classe *Formula* 3.5 è una classe astratta che si specializza nelle classi:

- *AtomicFormula* che rappresenta una formula composta da un solo letterale.
- *BinaryFormula* rappresenta le formule binarie $A \Rightarrow B$, $A \Leftrightarrow B$ e $A \oplus B$.
- *NegatedFormula* rappresenta le formule negate del tipo $\neg A$.
- *QuantifiedFormula* rappresenta le formule quantificate del tipo $\forall/\exists x1, x2, ..., xn : A$.
- *JunctionFormula* rappresenta le formule composte dalla concatenazione di $\wedge$ e $\vee$.

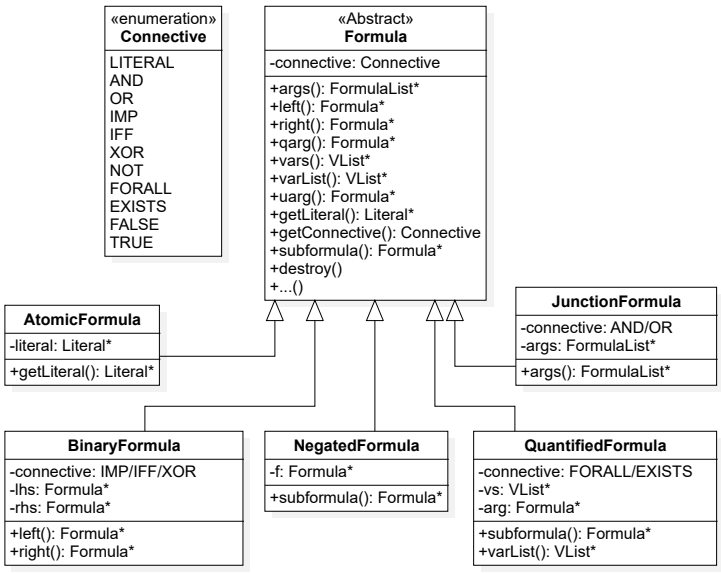


Figura 3.5: Struttura delle formule

Le clausole sono rappresentate dalla classe *Clause* 3.6 che è una specializza della classe *Unit*. Ogni clausola contiene un Array di letterali e sono quindi rappresentate in maniera molto simile alla notazione insiemistica vista in 1.1.3.

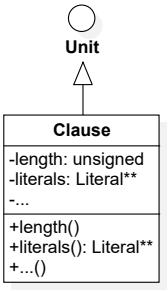


Figura 3.6: Struttura delle Clausole

3.3 Unificazione e Substitution Trees

3.4 Preprocessing

3.5 Algoritmo di Saturazione

3.6 Il SAT-Solver

Vampire non implementa un SAT-Solver ma ha un vasto sistema di interfacce per utilizzare al meglio SAT-Solver esterni. Al momento gli unici SAT-Solver

supportati sono MiniSat e Z3, anche se l'inclusione di Z3 è ancora in fase sperimentale. Per utilizzare un SAT-Solver è necessario creare Clausole e letterali appositi per la rappresentazione delle costanti proposizionali. Nella figura 3.7 è mostrata la struttura delle classi e delle interfacce per il SAT-Solver. La classe *SATLiteral* rappresenta una costante proposizionale ed è costituita da una coppia intero-booleano che rappresenta l'indice della costante e la sua polarità. La classe *SATClause* come la classe *Clause* è costituita da un Array, in questo caso di *SATLiteral*. Uno dei componenti Built-in di Vampire è la classe *SAT2FO* che si occupa di convertire letterali e clausole del primo ordine (FO) in oggetti di tipo *SATLiteral* e *SATClause* (SAT) e viceversa. La chiamata della funzione *SAT2FO*

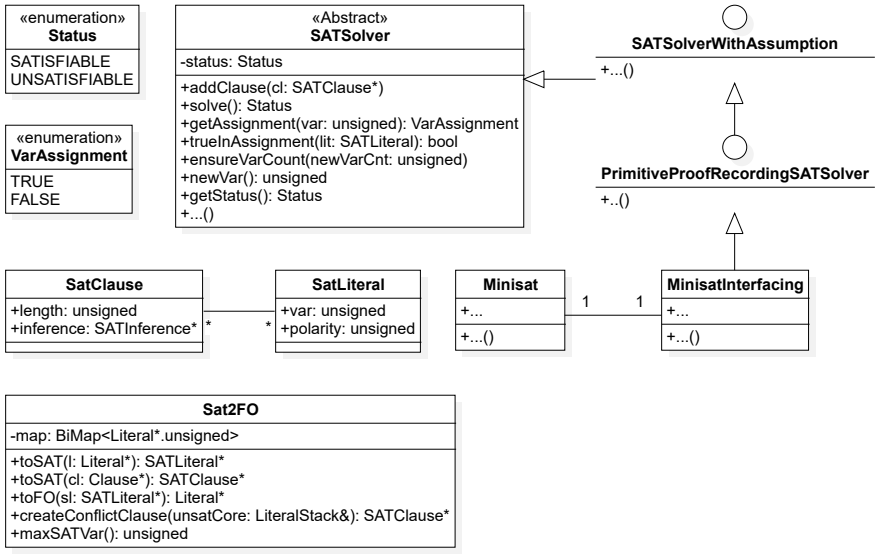


Figura 3.7: Classi e interfacce per il SAT-Solver

3.7 Misurazione dei Tempi

Capitolo 4

Implementazione di procedure di decisione per frammenti Binding in Vampire

L'algoritmo di decisione, la classificazione, Il preprocessing

4.1 Algoritmo di Classificazione

4.2 Preprocessing

4.2.1 Boolean Top Formula

4.2.2 Forall-And

4.2.3 SAT-Clausification

4.3 Procedura di Decisione

4.3.1 Implicants Sorting

4.3.2 Maximal Unifiable Subsets

4.3.3 Algoritmo Finale

Capitolo 5

Analisi Sperimentale

5.1 La libreria TPTP

5.2 Analisi dei risultati

5.3 Ottimizzazioni

5.4 Conclusioni e Possibili Sviluppi futuri

Bibliografia

[1] vampire website. `https://vprover.github.io/`.

[2] Simone Bova and Fabio Mogavero. Herbrand property, finite quasi-herbrand models, and a chandra-merlin theorem for quantified conjunctive queries. In *2017 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–12, 2017.

[3] M. Davis. *Il calcolatore universale. Da Leibniz a Turing*. Biblioteca scientifica. Adelphi, 2003.

[4] D.R. Hofstadter. *Gödel, Escher, Bach: un'eterna ghirlanda brillante ; una fuga metaforica su menti e macchine nello spirito di Lewis Carroll*. Biblioteca scientifica / Adelphi. Adelphi, 2009.

[5] Laura Kovács and Andrei Voronkov. First-order theorem proving and vampire. In Natasha Sharygina and Helmut Veith, editors, *Computer Aided Verification*, pages 1–35, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[6] Fabio Mogavero and Giuseppe Perelli. Binding Forms in First-Order Logic. In Stephan Kreutzer, editor, *24th EACSL Annual Conference on Computer Science Logic (CSL 2015)*, volume 41 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 648–665, Dagstuhl, Germany, 2015. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[7] Nonnengart, Andreas and Rock, Georg and Weidenbach, Christoph. On Generating Small Clause Normal Forms. 2000.

[8] Alexandre Riazanov and Andrei Voronkov. The design and implementation of vampire. *AI Commun.*, 15:91–110, 01 2002.

[9] G. Sutcliffe. The Logic Languages of the TPTP World. *Logic Journal of the IGPL*, 2022.

[10] Dirk van Dalen. *Logic and Structure*. Universitext. Springer London, 2012.