

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 testuale, 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 teorie 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

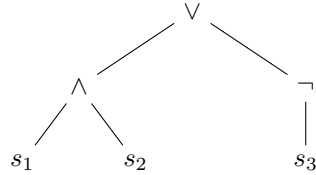
Sia $\Sigma_s = \{s_1, s_2, \dots\}$ un insieme di simboli di proposizioni atomiche, $\Sigma = \{\wedge, \vee, \neg, (,), \top, \perp\} \cup \Sigma_s$ è detto alfabeto della logica proposizionale. Con queste premesse si può definire come formule della logica proposizionale il linguaggio F generato dalla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

$$\varphi := \top \mid \perp \mid s \in \Sigma_s \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi)$$

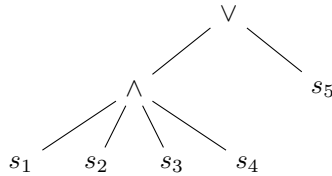
Con la funzione $ap(\gamma) \rightarrow 2^{\Sigma_s}$ si indica la funzione che associa a ogni formula γ l'insieme delle sue proposizioni atomiche. Viene chiamato *Letterale*, ogni proposizione atomica s o la sua negazione $\neg s$. Vengono inoltre introdotti i seguenti simboli come abbreviazioni:

- $(\gamma \rightarrow \kappa)$ 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 sintattico*. 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 dell'albero più veloci e algoritmi di manipolazione più semplici. Si consideri ad esempio di voler ricercare la foglia più a sinistra (s_1) nell'albero di sintattico della seguente formula $((\dots((s_1 \wedge s_2) \wedge s_3) \wedge s_4) \wedge \dots) \wedge s_n$. 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 $\{True, False\}$).

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

Un assegnamento α è detto *appropriato* per una formula $\varphi \in F$ se e solo se $ap(\varphi) \subseteq dom(\alpha)$, dove per $dom(\alpha)$ si intende il dominio (S) della funzione α . Per convenzione si assume che $\alpha(\top) = 1$ e $\alpha(\perp) = 0$ per ogni assegnamento α .

Si definisce la relazione binaria $\models \subseteq \{1, 0\}^S \times F$, detta relazione di *Soddisfacibilità*.

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) se e solo se si verifica una delle seguenti condizioni:

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

Una *Tautologia* è una formula φ tale che per ogni assegnamento α appropriato a φ , $\alpha \models \varphi$ (in notazione $\models \varphi$). Una formula è detta soddisfacibile se esiste un assegnamento appropriato che la soddisfa altrimenti è detta insoddisfacibile. Dato un insieme di formule Γ e una formula φ si dice che φ è una *conseguenza logica* di Γ (in notazione $\Gamma \models \varphi$), se e solo se ogni assegnamento α di Γ (nel senso che α è un assegnamento per ogni formula di Γ) è un assegnamento di φ . Cioè se $\alpha \models \Gamma$ allora $\alpha \models \varphi$. Due formule sono dette *equivalenti* sse $\varphi \models \psi$ e $\psi \models \varphi$ (in simboli $\varphi \equiv \psi$). Un'importante proprietà è che se $\varphi_1, \dots, \varphi_n \models \psi$ allora la formula $(\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \psi$ è una tautologia ($\models (\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \psi$). Un concetto molto simile a quello di equivalenza è l'*equisoddisfacibilità*. Due formule sono equisoddisfacibili se e solo se per ogni assegnamento della prima formula esiste un assegnamento della seconda formula e viceversa.

Un'*inferenza* è una qualunque relazione da $2^F \times F$. Un'inferenza è detta *corretta* se conserva la verità, ovvero 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 (Negation Normal Form) e CNF (Conjunctive Normal Form) sono le più famose e utilizzate, mentre la seconda, la ENNF (Equivalence Negation Normal Form), 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*. 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:

$$\eta := \top \mid \perp \mid S \in \Sigma_s \mid \neg S \in \Sigma_s \mid (\eta \wedge \eta) \mid (\eta \vee \eta)$$

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*. 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:

$$\bar{\eta} := \top \mid \perp \mid S \in \Sigma_s \mid \neg S \in \Sigma_s \mid (\bar{\eta} \wedge \bar{\eta}) \mid (\bar{\eta} \vee \bar{\eta}) \mid (\bar{\eta} \leftrightarrow \bar{\eta}) \mid (\bar{\eta} \oplus \bar{\eta})$$

La terza e ultima forma normale è la *CNF*. Una formula è in formato CNF sse è una congiunzione di disgiunzioni di letterali. La classe di formule CNF è generata dalla seguente grammatica:

$$\begin{aligned}\zeta &:= \xi \mid (\xi \wedge \zeta) \\ \xi &:= \top \mid \perp \mid S \in \Sigma_s \mid \neg S \in \Sigma_s \mid (\xi \vee \xi)\end{aligned}$$

La classe CNF è storicamente la più famosa e utilizzata, in quanto la sua rappresentazione è molto semplice. È infatti 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 \perp , 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 $\varphi_1 \wedge \dots \wedge \varphi_n$ allora la struttura principale è già una congiunzione di formule, quindi si procede applicando l'algoritmo sulle sottoformule $\varphi_1, \dots, \varphi_n$.
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 $(s_1 \wedge s_2) \vee (s_3 \wedge s_4) \vee \dots \vee (s_{n-1} \wedge s_n)$ 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* [?] 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 proposizionale. Per l'esempio precedente si assuma che s_n sia un simbolo proposizionale non presente nella formula originale. Applicando il *Naming* si ottiene la seguente formula:

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

In questo modo, la clausificazione della formula genera solo $n + m$ clausole al costo dell'aggiunta di un nuovo simbolo. 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 nomi s_7 e s_8 è possibile ottenere la seguente formula:

$$\begin{aligned} & (s_7 \leftrightarrow (((s_1 \leftrightarrow s_2) \leftrightarrow s_3) \leftrightarrow s_4)) \\ & \quad \wedge \\ & (s_8 \leftrightarrow (s_7 \leftrightarrow s_5)) \\ & \quad \wedge \\ & (s_8 \leftrightarrow s_6) \end{aligned}$$

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 introdotti anche due nuovi connettivi logici, \forall e \exists , che permettono di esprimere concetti come "per ogni" e "esiste", ampliando notevolmente il potere espressivo della logica, permettendo di parlare anche di insiemi non finiti.

1.2.1 Termini e Formule

Si introducono tre nuovi insiemi di simboli:

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

Si definisce la funzione *arity* : $\Sigma_f \cup \Sigma_p \rightarrow \mathbb{N}$ 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:

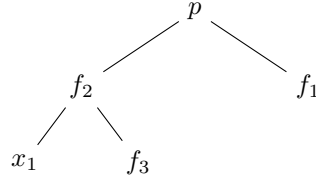
$$\tau := X \in \Sigma_x \mid f(\tau_1, \dots, \tau_n)$$

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

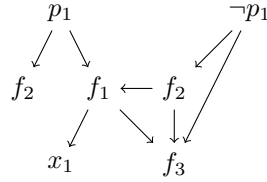
- Ogni variabile è un termine

- Ogni funzione costante è un termine
- Se τ_1, \dots, τ_n sono termini e f è un simbolo di funzione di arità n allora $f(\tau_1, \dots, \tau_n)$ 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 $p(\tau_1, \dots, \tau_n)$ dove p è un simbolo di relazione di arità n e τ_1, \dots, τ_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 sintattico. 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 una unica struttura condividendo i sottotermini comuni:



Una struttura del genere è detta *Perfectly Shared* (Perfettamente condivisa). Nella pratica questa tecnica di condivisione di sottotermini è indispensabile dato che, anche se ha 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 sottoterminale, 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:

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

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 ogni sua occorrenza è contenuta in una formula del tipo $\forall x(\phi')$ o $\exists x(\phi')$ 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 $\sigma = \{(x_1, t_1), \dots, (x_n, t_n)\}$, con la scrittura $\tau[x_1/t_1, \dots, x_n/t_n]$ oppure τ^σ si indica il termine ottenuto sostituendo *contemporaneamente* tutte le occorrenze delle variabili x_1, \dots, x_n con i termini t_1, \dots, 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 generale* 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.

Dati due sostituzioni σ_1 e σ_2 si dice che σ_1 è *più generale* 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 se esiste una sostituzione θ tale che $\sigma_2 = (\sigma_1)^\theta$. 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 generale 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 $L_1 = p_1(\tau_1, \dots, \tau_n)$ e $L_2 = p_2(\tau'_1, \dots, \tau'_n)$ 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 $f(\tau_1, \dots, \tau_n)$ e $f(\tau'_1, \dots, \tau'_n)$. 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.

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 sottoterminale 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 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*

Un noto algoritmo per la ricerca di un MGU di due termini è l'algoritmo di unificazione di *Robinson* riportato nell'algoritmo 1. Il vero collo di bottiglia di questo algoritmo è la ricerca delle *variable obstruction* che lo portano ad avere una complessità esponenziale. Vi sono vari modi per ottimizzare l'algoritmo, ad esempio utilizzando strutture di indicizzazione dei termini e variabili o utilizzando tecniche di programmazione dinamica. In alcuni casi è anche possibile evitare totalmente la ricerca delle *variable obstruction*, ad esempio se si hanno due termini senza variabili in comune e senza ripetizioni di variabili.

Algorithm 1: Algoritmo di unificazione di Robinson

Firma: $\text{unify}(\tau_1, \tau_2)$

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;

$S.\text{push}(\tau_1, \tau_2);$

while S is not Empty **do**

$(\tau_1, \tau_2) := S.\text{pop}();$

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 variable y **do**
 $\sigma := \sigma \cup \{x/y\}$

end

case τ_1 is a variable x **do**

if x in τ_2^σ **then**

return \perp

end

else

$\sigma := \sigma \cup \{x/\tau_2\}$

end

end

case τ_2 is a variable x **do**

if x in τ_1^σ **then**

return \perp

end

else

$\sigma := \sigma \cup \{x/\tau_1\}$

end

end

case $\tau_1 = f(u_1, \dots, u_n)$ and $\tau_2 = f(t_1, \dots, t_n)$ **do**

$S.\text{push}(u_1, t_1), \dots, S.\text{push}(u_n, t_n)$

end

case $\tau_1 = f(u_1, \dots, u_n)$ and $\tau_2 = g(t_1, \dots, t_m)$ **do**

return \perp

end

end

end

end

return $\sigma;$

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 $\mathcal{M} = (D, \mathfrak{I})$ dove D è un insieme non vuoto detto *Dominio* ($1 \in D$) e \mathfrak{I} è una funzione: $\mathfrak{I} : \Gamma \rightarrow D$ 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 $\mathcal{I}(s)$ è una funzione n -aria su D : $\mathcal{I}(s) : D^n \rightarrow D$.
- Se s è un simbolo di predicato n -ario allora $\mathcal{I}(s)$ è una relazione n -aria su D : $\mathcal{I}(s) \subseteq D^n$.
- Se s è un simbolo di funzione o predicato costante allora $\mathcal{I}(s) \in D$ è un oggetto del dominio.

Per semplicità di lettura, d'ora in poi l'applicazione della funzione \mathcal{I} ad un simbolo s verrà indicata con $s^{\mathcal{I}}$. Si definisce *Contesto*, una qualunque funzione $\gamma : \Sigma_x \rightarrow D$ 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 $\gamma = \{x_1 \rightarrow a, x_2 \rightarrow b\}$ allora $\gamma[x_1/b] = \{x_1 \rightarrow b, x_2 \rightarrow b\}$. 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 nella definizione di un contesto allora si assume che $\gamma(x) = x$. Si definisce l'interpretazione di un termine o predicato τ nel contesto γ secondo l'interpretazione \mathcal{I} :

- Se τ è una variabile x allora $\tau_\gamma^{\mathcal{I}} = \gamma(x)$
- Se τ è una funzione $f(\tau_1, \dots, \tau_n)$ allora $\tau_\gamma^{\mathcal{I}} = f^{\mathcal{I}}(\tau_{1\gamma}^{\mathcal{I}}, \dots, \tau_{n\gamma}^{\mathcal{I}})$
- se τ è un predicato $p(\tau_1, \dots, \tau_n)$ allora $\tau_\gamma^{\mathcal{I}} = p^{\mathcal{I}}(\tau_{1\gamma}^{\mathcal{I}}, \dots, \tau_{n\gamma}^{\mathcal{I}})$

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 , in notazione $\mathcal{M}, \gamma \models \varphi$, se e solo se si verifica una delle seguenti condizioni:

- Se φ è un predicato costante p allora $p^{\mathcal{I}} = 1$ oppure φ è \top
- Se φ è della forma $\neg\psi$ (dove ψ è una formula) allora $\mathcal{M}, \gamma \not\models \psi$
- Se φ è della forma $(\psi \wedge \chi)$ (con ψ e χ formule) allora $\mathcal{M}, \gamma \models \psi$ e $\mathcal{M}, \gamma \models \chi$
- Se φ è della forma $(\psi \vee \chi)$ (con ψ e χ formule) allora $\mathcal{M}, \gamma \models \psi$ o $\mathcal{M}, \gamma \models \chi$
- Se φ è della forma $\forall x(\psi)$ (dove ψ è una formula) allora 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 esiste un elemento $m \in D$ tale che $\mathcal{M}, \gamma[x/m] \models \psi$
- Infine se φ è un predicato $p(\tau_1, \dots, \tau_n)$ allora $p^{\mathcal{I}}(\tau_{1\gamma}^{\mathcal{I}}, \dots, \tau_{n\gamma}^{\mathcal{I}})$

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 e equisoddisfacibilità 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 ciò si potrebbe estendere 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, formule con variabili libere divengono equivalenti 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 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 equisoddisfacibile 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 adattare 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 l'equivalenza 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:

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

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

Viene chiamato *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:

$$P_0 := \wp(P)$$

$$P := \top \mid \perp \mid A \mid \neg P \mid (P \wedge P) \mid (P \vee P)$$

Dove \wp 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 e anche in questo caso la normalizzazione preserva l'equivalenza.

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

- Se la formula è del tipo $\exists x(\wp\phi)$ 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 $\forall x_k \dots x_{k+m-1} \exists x_{k+m}(\wp\phi)$ 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 $f_{n+1}(x_k, \dots, x_{k+m-1})$ $m-1$ -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. La skolemizzazione è un processo sound, ma non è detto che preservi l'equivalenza. Questo per colpa del fatto che vengono introdotti nuovi simboli non presenti nella formula originale. Ad esempio si prenda il modello $\mathcal{M} = (\{1, 2\}, \mathcal{I})$ con $p_1^{\mathcal{I}} = \{(1, 2), (2, 1)\}$ e le formule $\varphi = \forall x_1 \exists x_2 (p_1(x_1, x_2))$ e la sua skolemizzazione $sk(\varphi) = \forall x_1 (p_1(x_1, f_1(x_1)))$. \mathcal{M} è un modello per φ ma non è un modello per $sk(\varphi)$ in quanto f_1 non è definita in \mathcal{I} . È possibile però creare un nuovo modello \mathcal{M}' come \mathcal{M} ma aggiungendo $f_1^{\mathcal{I}'} = \{(1, 2), (2, 1)\}$. \mathcal{M}' è un modello sia per $sk(\varphi)$ che per φ . Per queste ragioni le formule skolemizzate sono equisoddisfacibili alle formule originali ma non equivalenti.

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:

$$\begin{aligned}\zeta_0 &:= \wp(\zeta_1) \\ \zeta_1 &:= \xi \mid (\xi \wedge \zeta_1) \\ \xi &:= \top \mid \perp \mid L \mid (\xi \vee \xi)\end{aligned}$$

Dove \wp 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.

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 sistema *ATP* (Automated 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' [?]* e *Martin Davis 'Il calcolatore universale' [?]* mentre i dettagli tecnici sono stati presi dal libro di *Dirk van Dalen 'Logic and Structure' [?]*.

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 $\varphi = (A_1 \wedge \dots \wedge A_n) \rightarrow C$ è valida. Nel caso fosse valida allora la sua negazione $A_1 \wedge \dots \wedge A_n \wedge \neg C$ 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'aritmetica?

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 $P \subseteq T$ 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 al teorema 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 codificata 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 $\not\vdash_{PM} \gamma$ e $\not\vdash_{PM} \neg \gamma$

Mentre il secondo teorema si può riformulare in questo modo:

2. Se PM (o un sistema simile) è consistente allora $\not\vdash_{PM} Cons$

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'indcidibilità 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 $\{q_1, \dots, q_n\}$ siano gli assiomi di Q e φ una qualunque formula. Se esistesse una procedura di decisione per la logica allora varrebbe:

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

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:

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

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 in 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 $\phi' = S \cup R$ finché 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 basati 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 cui dominio, detto universo di Herbrand, è generato da tutti i termini ground ottenibili dalla 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 suoi sottoinsiemi. I primi algoritmi utilizzabili nella pratica iniziarono a nascere dopo che Robinson introdusse la regola di risoluzione per la logica del primo ordine:

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

Dove σ è un unificatore dei due letterali $L(\tau_1, \dots, \tau_n)$ e $L(\omega_1, \dots, \omega_n)$ 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 ?? sull'implementazione di Vampire.

1.5 Il formato TPTP

In questa sezione verrà descritto il formato TPTP [?] (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 sistemi ATP. 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 tabella:

Simbolo	Traduzione
\top	<code>\$true</code>
\perp	<code>\$false</code>
\neg	<code>~</code>
\wedge	<code>&</code>
\vee	<code> </code>
\rightarrow	<code>=></code>
\leftrightarrow	<code><=></code>
\oplus	<code><~></code>
\forall	<code>!</code>
\exists	<code>?</code>

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, \dots, A_n e una congettura C :

- Se si da in input la lista di assiomi A_1, \dots, A_n l'ATP cerca di determinare la Soddisfacibilità della formula $A_1 \wedge \dots \wedge A_n$.
- Se vengono dati sia gli assiomi che la congettura l'ATP cerca di determinare se $A_1 \wedge \dots \wedge A_n \rightarrow C$ 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)).
```