

Introduzione

L'informatica e la logica condividono origini comuni poiché entrambe si sono sviluppate inizialmente con l'obiettivo di descrivere e/o emulare le capacità cognitive umane, tra cui il ragionamento. Sebbene attualmente lo studio dell'intelligenza artificiale si basi principalmente su metodi di apprendimento piuttosto che sulla deduzione, la logica rimane comunque uno strumento estremamente utile, in grado di descrivere in modo preciso il linguaggio matematico. La dimostrazione automatica di teoremi è un'importante branca dell'informatica e della logica, trovando largo utilizzo nell'ambito della verifica formale di software e hardware. I sistemi ATP (Automated Theorem Prover) sono utilizzati come strumento di supporto nella ricerca matematica, per affinare o verificare dimostrazioni formali.

I primi tentativi di realizzare un sistema di dimostrazione automatica risalgono agli anni '50, quando i ricercatori Allen Newell, Herbert A. Simon e Cliff Shaw progettarono il primo dimostratore automatico: il *Logic Theorist* che, tramite varie euristiche, tentava di dimostrare teoremi simulando il ragionamento umano. Da quel momento la ricerca si è spostata su metodi più formali e rigorosi, meno ispirati ai ragionamenti umani e più adatti ad essere eseguiti da un calcolatore. Gli studi moderni si basano principalmente sulla tecnica chiamata *Resolution*.

Vampire è un moderno ATP, basato su Resolution, creato da Andrei Voronkov e Alexandre Riazanov presso l'Università di Manchester. Uno dei suoi punti di forza è l'efficienza. Il team di sviluppo infatti partecipa annualmente al CASC (una competizione tra sistemi ATP), vincendo in almeno una categoria ogni anno. La sua implementazione è open-source ed è sviluppato in C++.

Il problema di dimostrare se una formula è un teorema o meno è riconducibile al problema di determinare se una formula è soddisfacibile. Una formula è soddisfacibile se esiste un'interpretazione che la rende vera. Il problema è decidibile per la logica proposizionale, nel senso che esiste un algoritmo che, dato in input una formula, restituisce una risposta positiva o negativa, ma diventa indecidibile per la logica del primo ordine. Per queste ragioni, la ricerca si è concentrata sull'individuazione di frammenti sintattici della logica del primo ordine decidibili rispetto al problema della soddisfacibilità. Tra questi, vi sono i frammenti Binding che sono oggetto di studio di questa tesi. L'algoritmo di decisione per i frammenti Binding non è basato su Resolution, ma risolve il problema utilizzando la teoria dell'unificazione, in combinazione ad un algoritmo di decisione per la logica proposizionale.

Le formule dei frammenti Binding sono, essenzialmente, combinazioni booleane di formule in Prenex Normal Form (PNF). La struttura della matrice delle formule PNF ne stabilisce il sotto frammento Binding di appartenenza. Il sotto frammento meno espressivo è chiamato *One Binding*. Le formule di questo sotto frammento sono costituite da combinazioni booleane di letterali che condividono la stessa lista di termini. Tale combinazione booleana è chiamata τ -Binding. Gli altri due sotto frammenti sono chiamati *Conjunctive Binding* e *Disjunctive Binding*. Le formule del sotto frammento Conjunctive Binding sono costituite da una congiunzione di formule τ -Binding, mentre le formule del sotto frammento Disjunctive Binding sono costituite da una disgiunzione di formule τ -Binding. I primi due sotto frammenti sono decidibili per il problema della soddisfacibilità, mentre il terzo è indecidibile. Questo perché se fosse decidibile, sarebbe possibile creare un algoritmo di decisione per l'intera logica del primo ordine. La particolare struttura delle formule *One Binding* consente di stabilire che una

formula è soddisfacibile se e solo se esiste un implicante booleano che, per ogni suo sottoinsieme unificabile, la conversione booleana del sottoinsieme è soddisfacibile. Da questo risultato si può costruire un algoritmo di decisione per i frammenti *One Binding* e *Conjunctive Binding*.

Questa tesi si propone di implementare l'algoritmo di decisione per i frammenti Binding all'interno del sistema di dimostrazione automatica Vampire e di valutarne le prestazioni, in confronto ad un metodo di decisione generale basato su Resolution per l'intera logica del primo ordine. Per fare ciò, è stato necessario studiare il funzionamento di Vampire e le sue componenti principali, in modo da poterle modificare e/o estendere per supportare l'algoritmo di decisione per i frammenti Binding. Per valutarne le prestazioni, sono stati classificati i problemi della libreria TPTP (Thousands of Problems for Theorem Provers) in base al frammento Binding di appartenenza e sono stati eseguiti dei test sperimentali sui problemi appartenenti ai frammenti *One Binding* e *Conjunctive Binding*.

La tesi è strutturata come segue:

- Nel capitolo 1 verrà data un'introduzione alla logica proposizionale, alla logica del primo ordine, al problema della soddisfacibilità, ai teoremi di incompletezza di Gödel e al problema della dimostrazione automatica.
- Nel capitolo 2 verranno presentati i frammenti Binding e l'algoritmo di decisione.
- Nel capitolo 3 verranno descritte le componenti principali di Vampire, con particolare attenzione a quelle necessarie per l'implementazione dell'algoritmo di decisione per i frammenti Binding.
- Nel capitolo 4 verrà descritto in che modo le componenti studiate nel capitolo precedente sono state utilizzate per implementare l'algoritmo di decisione.
- Nel capitolo 5 verranno presentati i risultati sperimentali ottenuti dall'esecuzione dell'algoritmo e verrà fatto un confronto con l'algoritmo di decisione generale basato su Resolution.