

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 Binding-Fragments in Vampire

Relatore

Prof. Massimo Benerecetti

Correlatore

Prof. Fabio Mogavero

Candidato

Matteo Richard Gaudino

Matricola

N86003226

Anno Accademico 2022 - 2023

Indice

Introduzione	5
1 Logica e automazione dei problemi di Decisione	6
1.1 Logica Proposizionale	6
1.1.1 Formule	6
1.1.2 Assegnamenti	7
1.1.3 Forme Normali	9
1.1.4 Naming	9
1.2 Logica del primo ordine	9
1.2.1 Termini	9
1.2.2 Formule	9
1.2.3 Semantica	9
1.2.4 Forme Normali	9
1.2.5 Skolemizzazione	9
1.2.6 Unificazione	9
1.3 Soddisfacibilità e Validità	9
1.4 Resolution	9
1.5 Il formato TPTP	9
2 Algoritmo di decisione di Frammenti Binding	10
2.1 Classificazione	10
2.2 Algoritmo Astratto	10
3 Il Theorem prover Vampire	11
3.1 I Termini	11
3.2 Formule e Clausole	11
3.3 Unificazione e Substitution Trees	11
3.4 Preprocessing	11
3.5 Saturazione e Refutazione	11
3.6 Il SAT-Solver	11
3.7 Misurazione dei Tempi	11

3.8	Opzioni	11
4	Implementazione di procedure di decisione per frammenti Binding in Vampire	12
4.1	Algoritmo di Classificazione	12
4.2	Preprocessing	12
4.2.1	Boolean Top Formula	12
4.2.2	Forall-And	12
4.2.3	SAT-Clausification	12
4.3	Procedura di Decisione	12
4.3.1	Implicants Sorting	12
4.3.2	Maximal Unifiable Subsets	12
4.3.3	Algoritmo Finale	12
5	Analisi Sperimentale	13
5.1	La libreria TPTP	13
5.2	Analisi dei risultati	13
5.3	Ottimizzazioni	13
5.4	Conclusioni e Possibili Sviluppi futuri	13

Introduzione

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

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 particolare, verranno introdotti i concetti di logica proposizionale e del primo ordine, definita come estensione della prima. 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 quello di accennare la teoria logica utilizzata nell'implementazione di vampire e della procedura di decisione per i Binding-Fragments. Perciò, verranno date per scontate nozioni di teoria degli insiemi, algebra booleana e teoria dei linguaggi formali.

1.1 Logica Proposizionale

1.1.1 Formule

Sia $\Sigma_c = \{c_1, c_2, \dots\}$ un insieme di simboli di costante, $\Sigma = \{\wedge, \vee, \neg, (,), \top, \perp\} \cup \Sigma_c$ è detto alfabeto della logica proposizionale. Con queste premesse possiamo definire come formule della logica proposizionale il linguaggio $F \subseteq \Sigma_c$ generato dalla grammatica Context Free seguente:

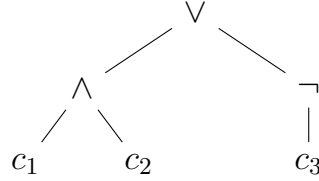
$$\varphi := \top \mid \perp \mid C \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi)$$

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

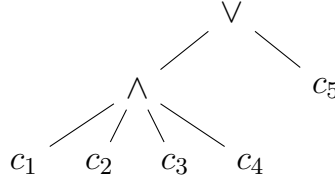
- $(\gamma \Rightarrow \kappa)$ per $(\neg\gamma \vee \kappa)$

- $(\gamma \Leftrightarrow \kappa)$ 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 $(c_1 \wedge c_2) \vee \neg c_3$ 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. $(c_1 \wedge (c_2 \wedge (c_3 \wedge c_4))) \vee c_5$ può essere scritto come $(c_1 \wedge c_2 \wedge c_3 \wedge c_4) \vee c_5$. 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 $((\dots(((c_1 \wedge c_2) \wedge c_3) \wedge c_4) \wedge \dots) \wedge c_n)$. 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 $C \subseteq \Sigma_c$ nell'insieme $\{1, 0\}$ (o $\{True, False\}$).

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

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*:

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

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 variabile c_x allora $\alpha \models \varphi$ sse $\alpha(c_x) = 1$
- 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 $\alpha \models \chi$

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 $\varphi = c_1$ e $\psi = \neg c_1$. 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 $\beta(c_1) = 1 - \alpha(c_1)$ e viceversa.

Un'*inferenza* è una qualunque funzione da F in F . Un'inferenza è detta *corretta* se conserva la soddisfacibilità, ovvero se non può generare una formula insoddisfacibile a partire da una formula soddisfacibile (soundness).

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 serie d'inferenze (corrette) in una forma normale. In questo paragrafo verranno descritte le forme normali che sono state utilizzate per il preprocessing dell'algoritmo.

ennf nnf cnf

1.1.4 Naming

1.2 Logica del primo ordine

1.2.1 Termini

1.2.2 Formule

1.2.3 Semantica

1.2.4 Forme Normali

1.2.5 Skolemizzazione

1.2.6 Unificazione

1.3 Soddisfacibilità e Validità

1.4 Resolution

1.5 Il formato TPTP

Capitolo 2

Algoritmo di decisione di Frammenti Binding

2.1 Classificazione

2.2 Algoritmo Astratto

Capitolo 3

Il Theorem prover Vampire

3.1 I Termini

3.2 Formule e Clausole

3.3 Unificazione e Substitution Trees

3.4 Preprocessing

3.5 Saturazione e Refutazione

3.6 Il SAT-Solver

3.7 Misurazione dei Tempi

3.8 Opzioni

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