Dott.ssa Roberta Gori

ATTIVITÀ DI RICERCA:

in questi anni ha riguardato diversi aspetti della dimostrazione di proprieta' e verifica di programmi appartenenti al paradigma logico, funzionale e ultimamente anche al paradigma del BioAmbient calculus.
Questi diversi filoni di ricerca sono caratterizzati dalla comune metodologia: l'uso della teoria dell'interpretazione astratta introdotta da Cousot e Cousot nel 1977.
La teoria dell'interpretazione astratta e' una teoria ricca e complessa che permette di formalizzare il concetto intuitivo di astrazione.
Questa metodologia si e' dimostrata uno strumento potente e flessibile sia nel campo dell'analisi statica di programmi che nel campo della semantica.
L'analisi di programmi consiste nel derivare automaticamente a tempo di compilazione informazione sul comportamento run-time di un programma.
Nell'ambito della semantica l'interpretazione astratta e'stata usata sia per mettere in relazione semantiche definite indipendentemente per modellare proprieta' diverse, sia per definire sistematicamente nuove semantiche che modellino proprieta' di interesse o approssimazioni di tali semantiche.
L'approccio basato sull'interpretazione astratta infatti e' molto generale e ci permette di trattare uniformemente sia il caso in cui la semantica astratta modelli la proprieta' di interesse in modo preciso e non vi sia perdita di informazione rispetto a tale proprieta', sia il caso in cui la semantica astratta descriva solo in maniera approssimata le proprieta'. In questo ultimo caso l'interesse e' di ottenere semantiche che approssimino solo la proprieta' ma che siano effettivamente calcolabili. Tali semantiche vengono comunemente chiamate semantiche non-standard.Algoritmi di analisi possono essere definiti partendo da semantiche astratte non-standard definite su un dominio di descrizioni di proprieta' approssimate.
L'algoritmo di analisi in questo caso consiste nel calcolo della semantica astratta, calcolo che termina avendo imposto opportune condizioni sul dominio astratto.
La sua attivita' di ricerca si e' inserita in questo contesto. Si sono definite nuove analisi statiche per il linguaggio Prolog, capaci di catturare informazioni sulla finitezza delle variabili, cioe' quali siano le variabili che sicuramente in un dato punto del programma saranno legate a termini non infiniti. La teoria dell'interpretazione astratta e' stata inoltre utilizzata per derivare un framework nel quale poter definire semantiche capaci di modellare comportamenti operazionali dei programmi logici che non erano ancora stati modellati, come il fallimento finito e le computazioni infinite. A partire da tali semantiche si sono derivate delle opportune approssimazioni che ci hanno permesso di definire nuove analisi statiche (calcolabili) capaci di approssimare la proprieta' di interesse. A partire da questa approssimazioni si e' derivato un nuovo metodo di verifica capace di provare che un dato programma e' parzialmente corretto rispetto al fallimento finito.
L'approccio basato sull'interpretazione astratta e' stato anche utilizzato nella definizione di un framework di verifica per i programmi logici, parametrico rispetto alla proprieta' astratta che si intende verificare.
Data una proprieta', le condizioni di verifica corrispondenti sono sistematicamente derivate dal framework e sono garantite essere condizioni sufficienti per la correttezza parziale. Questo framework e' stato utilizzato per ricostruire i metodi di verifica noti per la programmazione logica, per confrontare tra loro i diversi metodi e per definirne

di nuovi. L'interpretazione astratta e' stata anche utilizzata nell'ambito del paradigma funzionale per ricostruire metodi di inferenza noti e per definirne di nuovi.
Malgrado l'approccio basato sull'interpretazione astratta e i sistemi di tipi appaiano due approcci molto diversi tra loro essi sono invece strettamente correlati.
Alcuni recenti lavori di Monsuez e Cousot 97 hanno mostrato come sia possibile derivare sistematicamente una gerarchia di sistemi di tipo con i relativi algoritmi di type checking e/o inference mediante tecniche di interpretazione astratta.
Sviluppando quest'idea, abbiamo definito un nuovo operatore di punto fisso su un dominio di tipi monomorfi, rappresentati come termini di Herbrand con variabili.
L'operatore da noi introdotto generalizza l'algoritmo di inferenza di tipi di Hindley (quello usato nel sistema di inferenza di tipi di ML). In questo modo \`e stato possibile ricostruire l'algoritmo di inferenza di tipi di ML e, utilizzando questa costruzione, definire un nuovo algoritmo di inferenza di tipi che realizza una forma di ricorsione intermedia tra la ricorsione monomorfa e quella polimorfa.

Ultimamente si e' utilizzata la teoria dell'interpretazione astratta per esplorare una nuova area di ricerca, cioe' quella legata all'applicazione dei metodi formali per descrivere e analizzare sistemi biologici. I risultati ottenuti appaiono essere molto promettenti.