MINISTERO
DELL'UNIVERSITÀ
E DELLA RICERCA **Programmi di ricerca cofinanziati - Modello D**
Rendiconto del programma di ricerca - ANNO 2005
prot. 2005015491

1. Area Scientifico Disciplinare principale	*01: Scienze matematiche e informatiche*
2. Coordinatore Scientifico del programma di ricerca	*ROSSI Francesca*
- Università	*Università degli Studi di PADOVA*
- Facoltà	*Facoltà di SCIENZE MATEMATICHE FISICHE e NATURALI*
- Dipartimento/Istituto	*Dip. MATEMATICA PURA E APPLICATA*
3. Titolo del programma di ricerca	*Vincoli e preferenze come formalismo unificante per l'analisi di sistemi informatici e la soluzione di problemi reali*
4. Settore principale del Programma di Ricerca:	*INF/01*
5. Costo originale del Programma:	*222.700 Euro*
6. Quota Cofinanziamento MIUR:	*113.000 Euro*
7. Quota Cofinanziamento Ateneo:	*48.644 Euro*
8. Finanziamento totale:	*161.644 Euro*
9. Durata:	*24 mesi*

10. Obiettivo della ricerca eseguita

L'obbiettivo di questo progetto e' studiare estensioni dei formalismi e delle tecniche esistenti per la programmazione con vincoli, con particolare riferimento ad applicazioni innovative sia a sistemi informatici (es. sicurezza, analisi di programmi) che a problemi reali (es. scheduling, bioinformatica). Utilizzeremo quindi i vincoli come formalismo unificante, e le applicazioni come spunto per le estensioni dei linguaggi e delle tecniche di risoluzione dei vincoli.

Unita' di ricerca

Per ottenere questo obbiettivo, abbiamo coinvolto alcuni tra i principali gruppi di lavoro in questo ambito di ricerca in Italia, in modo da poter sfruttare le competenze comuni per una facile comunicazione, ma anche le competenze complementari per una fruttuosa collaborazione che porti a nuovi risultati sia teorici che pratici. Tali gruppi sono presenti anche in un ambito di ricerca internazionale, e producono regolarmente risultati sia teorici che applicativi che vengono ben accolti dalla comunita' internazionale e hanno dato luogo a nuove linee di ricerca all'interno della programmazione con vincoli. In particolare:
-- l'unita' 1 (Padova), che coordina questo progetto, ha forti competenze nell'ambito dei vincoli soft e delle preferenze, e anche nell'applicazione di tecniche di vincoli a problemi di scheduling;
-- l'unita' 2 (Udine) ha esperienza nella definizione e sviluppo di nuovi linguaggi di programmazione logica con vincoli su insiemi, e anche nell'applicazione di tecniche di vincoli al problemi della bioinformatica e all'analisi di sistemi ibridi;
-- l'unita' 3 (Genova) contribuisce a questo progetto con le sue competeneze nell'ambito dell'analisi di sistemi informatici tramite tecniche basate sui vincoli;
-- l'unita' 4 (Pescara) ha competenze sia nello studio dei linguaggi logici e concorrenti con vincoli, che nell'applicazione di vincoli a problemi legati alla sicurezza.

Valore aggiunto del consorzio

Tutte le unita' hanno una profonda conoscenza delle tecniche di vincoli, e hanno rivolto la loro attenzione a diverse applicazioni utilizzando idee e tecniche correlate tra loro. Il valore aggiunto del consorzio e' rappresentato quindi dalla possibilita', attraverso una piu' stretta collaborazione e ad incontri organizzati durante lo svolgimento del progetto, di unire competenze anche complementari con lo scopo di consolidare e migliorare i risultati delle singole unita' e aprire nuove prospettive per le tecniche sviluppate nei rispettivi campi applicativi.

Linee di lavoro

Abbiamo percio' individuato delle linee di lavoro che permettano di fare cio', e che siano anche collegate tra loro in modo da favorire la tracimazione di risultati da una linea ad un'altra. In particolare, studieremo:

-- L'estensione di formalismi per poter modellare preferenze positive e negative, condizionate e non, qualitative e quantitative. In questo momento esistono molti formalismi per descrivere questi vari tipi di preferenze, ma nessuno che permetta di gestirne vari tipi allo stesso tempo.
Unita' coinvolte: Padova, Pescara.

-- La modellazione e soluzione di situazioni con piu' agenti, e lo studio delle loro proprieta' fondamentali. Questa sara' un'attivita' multi-disciplinare che usera' sia tecniche di intelligenza artificiale che di teoria delle decisioni.
Unita' coinvolte: Padova.

-- Lo sviluppo di tecniche per gestire situazioni con piu' criteri di ottimizzazione. Qui si useranno anche tecniche di ricerca operativa che sono molto utili in problemi di ottimizzazione.
Unita' coinvolte: Padova, Udine.

-- La gestione di vincoli su intervalli e su (multi)insiemi. Questa linea di lavoro estendera' l'applicabilita' della programmazione con vincoli in quegli ambiti dove e' naturale specificare vincoli su intervalli o su insiemi.
Unita' coinvolte: Udine, Genova.

I campi applicativi che considereremo sono:

-- Problemi di scheduling.
Si vuole poter gestire anche problemi con preferenze sulle attivita', e dove la soluzione ottenuta sia robusta alle modifiche del contesto.
Unita' coinvolte: Padova.

-- Verifica di proprieta' di sistemi concorrenti a stati infiniti.
Si vuole estendere lo stato dell'arte in questo campo tramite tecniche di vincoli e nozioni di composizionalita'.
Unita' coinvolte: Genova, Udine, Pescara.

-- Analisi di protocolli di sicurezza multilivello.
Si vuole usare i vincoli soft per poter modellare piu' fedelmente, e quindi risolvere in modo piu' soddisfacente, problemi tipici della sicurezza dei sistemi informatici.
Unita' coinvolte: Pescara, Genova.

-- Bioinformatica.
Si vuole sviluppare risolutori di vincoli ad hoc per alcuni problemi di bioinformatica, quali la predizione della struttura tridimensionale di una proteina.
Unita' coinvolte: Udine.

---

11. Descrizione della Ricerca eseguita e dei risultati ottenuti

Il progetto ha prodotto molti risultati interessanti, che seguono le linee di lavoro individuate all'inizio e che rispettano le tempistiche iniziali del programma di lavoro. Di seguito descriviamo in dettaglio i risultati del progetto, divisi per task.

Task 1: Estensione di formalismi esistenti

1.1: Formalismi per modellare le preferenze

Abbiamo studiato la coesistenza di vari tipi di preferenze in uno stesso scenario, e abbiamo proposto come gestire tale situazione nel caso di preferenze sia qualitative e condizionali (a la CP-net) che quantitative (come i soft constraints).

Abbiamo definito un formalismo per modellare problemi con preferenze e incertezza, dove ad ogni evento incerto e' associato un grado di possibilita', e abbiamo definito un risolutore per questi problemi. Tale risolutore prima rimuove la parte incerta del problema e poi risolve il problema ottenuto sfruttando tecniche di branch and bound. La procedura adottata per rimuovere la parte incerta e' stata definita in modo tale che alcune proprieta' desiderabili relative all'ordinamento delle soluzioni e alla robustezza delle soluzioni, cioe' alla compatibilita' delle soluzioni rispetto agli eventi incerti, venissero soddisfatte.

Abbiamo anche considerato problemi con preferenze e incertezza, dove l'incertezza viene espressa tramite preferenze mancanti. Per tali problemi abbiamo definito varie nozioni di ottimalita' delle soluzioni, e abbiamo implementato un risolutore in grado di restituire i vari tipi di soluzioni ottime attraverso un processo parziale di elicitazione delle preferenze mancanti.

Abbiamo anche studiato la presenza di incertezza in problemi con preferenze sulle durate di eventi, sviluppando algoritmi che testino la controllabilita' di tali problemi. Abbiamo inoltre considerato problemi temporali in cui sia la presenza di eventi che le preferenze associate a tali eventi possono essere condizionali. Per tali problemi sono state studiate varie nozioni di consistenza e per ciascuna sono stati sviluppati algoritmi per testarne la soddisfazione.

Abbiamo poi definito un formalismo che modella problemi con preferenze bipolari. Tale formalismo generalizza quello gia' esistente dei vincoli soft che riesce a modellare solo le preferenze negative, permettendo di rappresentare anche le preferenze positive e l'indifferenza, cioe' l'assenza sia di una preferenza positiva che di una preferenza negativa. Inoltre, permette anche di compensare le preferenze positive e negative. Abbiamo inoltre definito un risolutore basato su tecniche di branch and bound per trovare le soluzioni ottime di problemi bipolari. Abbiamo anche considerato la presenza dell'incertezza anche in problemi bipolari, definendo un formalismo per modellare questi problemi e una procedura per rimuovere l'incertezza che garantisce che valgano alcune proprieta' desiderabili sulla robustezza del problema.

1.2: Scenari multi-agente.

Abbiamo considerato come aggregare le preferenze parzialmente ordinate di piu' agenti per ottenere un insieme di alternative

ottime. Abbiamo poi definito in questo contesto la nozione di strategy-proofness, cioe' la nozione di non-manipolabilita'. Abbiamo quindi esteso al caso di preferenze parzialmente ordinate il classico teorema di Gibbard-Satterthwaite noto per preferenze totalmente ordinate, che afferma che se non c'e' un dittatore, allora gli agenti possono manipolare il risultato esprimendo in maniera strategica le loro preferenze.

Abbiamo inoltre analizzato la presenza dell'incertezza nel contesto multiagente. In particolare abbiamo considerato scenari in cui alcuni agenti decidono di non rivelare tutte le loro preferenze. In questo contesto abbiamo dimostrato che e' NP-hard determinare i vincitori possibili e necessari, ed abbiamo individuato delle condizioni sufficienti sulla regola di aggregazione delle preferenze che permettono di determinare questi vincitori in tempo polinomiale.

Inoltre, abbiamo analizzato la complessita' computazionale di calcolare i vincitori in una specifica regola di aggregazione di preferenze: sequential majority voting. Abbiamo dimostrato che determinare i vincitori possibili e necessari per questa regola e' polinomiale, mentre calcolare i vincitori possibili diventa NP-hard se si richiede che l'albero di voto sia bilanciato. Abbiamo inoltre studiato la complessita' computazionale di determinare i vincitori quando alcune delle preferenze non sono ancora state rivelate e l'albero di voto non e' ancora stato deciso, dimostrando che e' polinomiale sia stabilire se un candidato vince in tutti gli alberi di voto, sia decidere se c'e' un albero dove il candidato vince indipendentemente dalle preferenze incomplete, mentre e' un problema NP-completo decidere se c'e' un candidato che non puo' vincere in nessuna sequenza per nessun completamento delle preferenze. Abbiamo inoltre provato che quest'ultimo risultato vale anche quando richiediamo che l'albero di voto sia bilanciato.

Abbiamo inoltre considerato la complessita' computazionale di determinare i vincitori quando alcune delle preferenze non sono ancora state rivelate, ma l'albero di voto e' gia' stato deciso. In questo caso abbiamo provato che e' polinomiale determinare se un candidato vince nell'albero di voto fissato in almeno uno o in tutti i modi possibili di completare le preferenze mancanti.

1.3: Ottimizzazione multi-obbiettivo.

Abbiamo studiato nuovi algoritmi di integrazione di tecniche di programmazione a vincoli con tecniche di ricerca operativa per l'ottimizzazione multi-obiettivo. Sono stati studiati metodi per applicare il pruning sui costi ridotti, molto usato nell'ottimizzazione mono-obiettivo, per integrare un risolutore lineare con la programmazione a vincoli. Questo ha portato a sviluppare un nuovo vincolo per il linguaggio di programmazione logica a vincoli ECLiPSe che utilizza i costi ridotti nella ricerca della frontiera Pareto-ottima. Tale metodo e` stato sperimentato su alcuni problemi accademici, mostrando di ottenere risultati migliori sia di quelli di un risolutore multi-obiettivo basato esclusivamente sulla programmazione a vincoli, sia di quelli di un risolutore basato sui costi ridotti ma su una singola funzione obiettivo. Un'euristica basata sui costi ridotti acquisiti da piu` funzioni obiettivo (che quindi non e` applicabile quando si usano i costi ridotti relativi solo ad una funzione obiettivo) ha mostrato di migliorare ulteriormente l'efficienza dell'algoritmo.

1.4: Vincoli e intervalli.

Abbiamo sviluppato procedure di decisione, basate su metodi a tableau, per diverse logiche temporali intervallari. In particolare, una procedura di decisione per il frammento della Propositional Neighborhood Logic (PNL) contenente i soli operatori futuri, interpretato sul dominio dei naturali, per l'intera logica PNL, interpretata sul dominio degli interi, e per una logica temporale ramificata ottenuta combinando PNL e CTL. In tutte le procedure la gestione dei vincoli introdotti dagli operatori temporali occupa un ruolo centrale. Abbiamo, inoltre, studiato in modo sistematico le proprietà di decidibilità ed espressività della logica PNL rispetto a diverse classi di strutture e trattato il caso delle logiche D dei sottointervalli interpretate su ordini lineari densi, prendendo in esame ogni possibile relazione di sottointervallo. Abbiamo introdotto opportuni pseudo modelli sui quali abbiamo dimostrato la decidibilità delle logiche tramite small model theorems. Anche per le logiche D, abbiamo introdotto delle procedure di decisione tableau-based di complessità ottimale. Si sono anche applicate tecniche di constraint programming su intervalli al problema della ricostruzione di una scena 3D.

1.5: Vincoli su (multi)insiemi.

Nell'ambito dei vincoli su (multi) insiemi, e' stato proposto un nuovo algoritmo di unificazione insiemistica che generalizza tutte le proposte esistenti, e' stato sviluppato un constraint solver parametrico per domini di liste, multi-insiemi, liste compatte ed insiemi, e sono stati studiati risultati di decidibilità per teorie di tipo insiemistico con atomi. Lo studio e lo sviluppo dell'integrazione tra solver su insiemi e domini finiti ha dato luogo a un solver combinato inglobato sia in un linguaggio logico (SICStus Prolog) che in Java. E' stata analizzata e realizzata l'integrazione tra il risolutore di vincoli insiemistici di JSetL ed un nuovo risolutore di vincoli su domini finiti, denominato JFD, sfruttando i meccanismi di multitasking e comunicazione tra processi offerti da Java, secondo un'architettura master-slave. Si sono confrontati il formalismo dell'answer set programming e le tecniche di programmazione con vincoli su domini finiti su un insieme di problemi di benchmark. Si sono inoltre studiati linguaggi per la descrizione di problemi di planning basati su vincoli, fornendo anche un tool per la loro esecuzione basato sia su answer set programming che su CLP(FD).

Abbiamo definito un linguaggio di specifica, chiamato CMRS, che combina riscrittura di multi-insiemi di predicati con una sottoclasse di vincoli aritmetici lineari chiamati "gap-order constraints". Il linguaggio risultante permette di specificare una classe interessante di sistemi concorrenti. Ad esempio si possono modellare diversi tipi di comunicazione con passaggio di valori e generazione e manipolazione di nomi (ad es. identificatori di processi). Per questo linguaggio abbiamo definito una procedura di analisi simbolica che risolve il problema chiamato "control state reachability", cioe' la raggiungibilita' di configurazioni che contengono un numero fissato a priori di un certo insieme di simboli di predicato. La procedura utilizza operazioni su gap-order constraint quali test di soddisfacibilita' ed eliminazione di variabili ed e' basata su un algoritmo di ricerca backward. La decidibilita' del problema di control reachability vale per una versione ristretta del linguaggio nel quale i predicati non possono avere arieta' maggiore di uno.

Task 2: Applicazione delle tecniche di vincoli.

2.1: Problemi di scheduling.

Abbiamo proposto algoritmi innovativi per la gestione delle esecuzioni di schedulazioni in presenza di eventi disturbanti. Sono stati proposti sia approcci off-line che approcci on-line basati su vincoli. Un contributo ulteriore e' la definizione di un ambiente sperimentale per la comparazione dei diversi approcci risolutivi rispetto a diversi pattern di eventi disturbanti. Utilizzando tale ambiente, sono stati proposti alcuni studio empirici sia su strategie off-line che su strategie on-line.

Abbiamo inoltre proposto varie estensioni del metodo di ottimizzazione Iterative Flattening, una strategia per minimizzare la durata complessiva di uno schedule. Sono state proposte diverse varianti che potenziano l'algoritmo originale, modificando lo schema iniziale con nuove procedure di rilassamento e di risoluzione, o analizzando varianti che integrano tecniche di tabu-search.

E' stata sviluppata un'applicazione reale nel campo dello scheduling che riguarda la costruzione di un orario delle lezioni, che e` stato utilizzato nella produzione dell'orario delle lezioni di un corso di laurea presso la Facolta` di Ingegneria di Ferrara. Questo software tiene in considerazione i vincoli dei singoli docenti e quelli imposti dal consiglio del corso di laurea. La funzione obiettivo cerca di rendere il piu` compatto possibile l'orario per gli studenti.

La Programmazione Logica a Vincoli e` stata anche applicata, in congiunzione con l'abduzione, alla programmazione di software ad agenti, in particolare per il ragionamento associato alle scadenze temporali (deadline).

Un'ulteriore applicazione reale e` stata lo sviluppo di un software per lo scheduling degli appuntamenti nello screening per il tumore dell'utero. Si tratta di un problema con vincoli con due obiettivi sono da perseguire: invitare per prime le pazienti in ritardo rispetto alla visita precedente, e invitare per prime le pazienti ad alto rischio. L'algoritmo sviluppato utilizza la programmazione a vincoli e permette un bilanciamento, tramite pesi, dei due criteri.

2.2. Analisi di sistemi concorrenti.

Abbiamo esplorato in modo approfondito l'utilizzo di particolari classi di automi per la specifica e verifica di sistemi complessi. In particolare, abbiamo mostrato come gli automi single-string, estesi con contatori, possano essere impiegati per rappresentare e manipolare granuarità temporali multiple e come gli automi temporizzati permettano di specificare e validare schemi di workflow con vincoli temporali. Abbiamo inoltre indagato le potenzialità di un approccio basato sugli automi rispetto al problema della modellazione e verifica di sistemi a stati infiniti, confrontandolo con altri approcci proposti in letteratura. Per studiare la rappresentazione delle strutture temporali, sono state studiate a fondo alcune problematiche cruciali nei formalismi per la rappresentazione e la manipolazione delle granularità. In particolare, è stata proposta una sottoclasse degli automi di Büchi chiusa per unione, proiezione e complementazione che cattura i linguaggi regolari di sole parole definitivamente periodiche e per la quale il problema di equivalenza è risolto in spazio lineare. E' stata considerata la classe degli automi ibridi che possono essere ottenuti componendo automi o-minimali semi-algebrici. Abbiamo mostrato che gli automi di tale classe hanno un potere espressivo maggiore rispetto agli automi o-minimali semi-algebrici e consentono di modellare in maniera naturale fenomeni (p.es., biologici) in cui vi è un'interazione tra più sistemi semplici modellabili attraverso automi o-minimali. Il problema della raggiungibilità su tale classe di automi non si presta ad essere analizzato attraverso le tecniche standard di quoziente attraverso (bi)simulazione in quanto abbiamo mostrato l'esistenza di automi della classe aventi un quoziente per simulazione infinito. Abbiamo applicato quindi la tecnica di traduzione in vincoli sui reali, combinata con risultati di teoria dei numeri computazionale, allo studio di questa classe dimostrando la decidibilità del problema di raggiungibilità.

Abbiamo utilizzato il linguaggio CMRS e una tecnica di verifica basata su ricerca simbolica backward con gap-order constraint ad una vasta gamma di di protocolli parametrici di mutua esclusione (cioe' definiti per N-processi con N generico) nei quali le guardie per le transizioni dei singoli processi possono essere definite tramite formule quantificate universalmente (cioe' devono essere soddisfatte da tutti i processi). Un classico esempio di questo tipo di sistema e' l'algoritmo di mutua esclusione per N-processi di Szymanski. Per poter trattare condizioni globali e' stata applicata un'approssimazione conservativa basata sulla trasformazione di una condizione global di tipo universale in una post-condizione. Questa approssimazione permette l'uso di vincoli booleani e/o interi per l'analisi simbolica di questa classe di sistemi. L'approssimazione si e' rivelata molto efficace. Infatti ha permesso di verificare tutti gli esempi di sistemi parametrici con condizioni globali dove i processi individuali hanno un numero finito di stati trattati in letteratura. Inoltre e' stata applicata con successo all'analisi di protocolli molto complessi dove i singoli processi hanno un insieme infinito di stati (a causa di variabili locali su domini infiniti) e le loro transizioni sono definite tramite condizioni globali. Esempi di questi protocolli sono: il caso generico dell'algoritmo Bakery di Lamport o il protocollo con time-stamp di Ricart e Agrawala. La tecnica e' stata implementata utilizzando risolutori di vincoli su Booleani, interi (Omega library) e reali (libreria clp(Q,R)).

Inoltre abbiamo esteso queste tecniche in modo da gestire sistemi con condizioni globali valutate in modo non atomico. Infine abbiamo studiato tecniche per l'analisi di modelli astratti di software basate su risolutori per vincoli lineari e tecniche di raffinamento dell'astrazione basate su interpretazione astratta.

I vincoli e l'abduzione sono anche applicati alla verifica formale di Web Services. Le interazioni corrette fra web service sono definite formalmente tramite una coreografia, che viene espressa in un opportuno linguaggio logico a vincoli. Sia la specifica del web service, sia quella della coreografia, vengono definite tramite un linguaggio logico che combina programmazione a vincoli ed abduzione. L'uso dei vincoli risulta fondamentale per tagliare rami dell'albero di ricerca e rendere accettabili i tempi di elaborazione. L'abduzione con vincoli e` stata applicata anche al ragionamento su contratti di business.

Abbiamo suggerito un modello formale per rappresentare e risolvere il problema di instradamento di pacchetti in reti multicast con QoS (quality of service). Nella rappresentazione usiamo grafi and-or per modellare la rete, e programmi in SCLP sui tali grafi per calcolare l'albero migliore, in accordo ai criteri di QoS. Dato un gruppo multicast di nodi riceventi e un insieme di funzioni obiettivo da ottimizzare, il problema di instradamento multicast corrisponde al processo di costruzione dell'albero multicast in grado di ottimizzare queste funzioni, in modo da minimizzare quindi il costo totale dell'albero. I costi dei collegamenti, in termini di metriche QoS, sono tradotti in costi per archi e connettori (archi multicast).

2.3. Sicurezza.

La sicurezza di una rete è basata non solo sulla sicurezza delle sue componenti e delle interconnessione dirette tra loro, ma anche sulla potenziale possibilità che i sistemi possono avere di interoperare indirettamente attraverso le connessioni di rete. Tale possibilità può infatti potenzialmente creare dei "cascading path" che violano la sicurezza dei sistemi attraverso le connessioni di rete. In particolare, abbiamo studiato come l'uso dei vincoli in un sistema possa aiutare nella gestione della rete, arrivando fino a quello che e' detto "autonomic network management". In questo caso, la rete è autogestita, auto configurata, auto protetta, in accordo con gli obiettivi della impresa o degli utenti. La proposta formulata utilizza vincoli per rappresentare la rete e la situazione da mantenere (tramite eventuali riconfigurazioni automatiche). Inoltre abbiamo descritto e risolto i "cascade" problem in reti autoconfiguranti di questo tipo. Abbiamo anche affrontato il problema della sicurezza delle applicazioni web, in particolare di quelle applicazioni in cui entità multiple (ad esempio differenti web service) comunicano tra di loro. Come caso applicativo, si pensi ad un sito web che, per le vendite on-line, si appoggia ad un servizio bancario che convalida l'acquisto. Viene proposta una politica basata su differenti livelli di integrità e su oggetti che possono cambiare il loro livello attuale allo scopo di cooperare in maniera sicura. La politica viene formalizzata in un'algebra dei processi, e varie sue proprietà verificate con un model checker. Stiamo lavorando sulla definizione di un metodo per la specifica e la verifica automatica di proprietà temporali di sistemi reattivi a stati infiniti ed alla sua applicazione a problemi di integrità e di controllo dell'accesso in protocolli di mutua esclusione e di coerenza della memoria. I sistemi reattivi sono specificati per mezzo di programmi logici con vincoli con negazione localmente stratificata, le proprietà temporali prese in considerazione sono espresse nella logica CTL (Computation Tree Logic), mentre la verifica delle proprietà avviene applicando una tecnica automatica di specializzazione di programmi basata su regole e strategie di trasformazione. Abbiamo effettuato uno studio sulla gestione del rischio relativo agli attacchi di sicurezza, considerando come base iniziale la nozione di "attack tree". Un attack tree è una struttura ad albero dove la radice rappresenta il bene oggetto dell'attacco e le foglie rappresentano le differenti vulnerabilità del sistema (e i relativi percorsi di attacco). Utilizzando questa struttura abbiamo definito una nozione quantitativa della pericolosita' dell'attacco e utilizzato vari formalismi per rappresentare le diverse possibilità offerte ad attaccante e difensore. Da una parte abbiamo studiato come l'attacco e la difesa di un sistema poteva venire rappresentato come un gioco e come gli equilibri del gioco stesso rappresentassero le strategie ottimali per attaccante e difensore. Dall'altra abbiamo usato il formalismo delle CP-net per rappresentare l'ordine di preferenza che il difensore deve adottare nella scelta delle contromisure agli attacchi. In parallelo con lo studio di protocolli di comunicazione e' stato avviato uno studio esplorativo per verificare la possibilita' di applicazione di tecniche simboliche di analisi basate su vincoli e riscrittura nel campo della sicurezza. Nel corso del primo anno abbiamo ottenuto risultati preliminari sulla decidibilita' del problema di "control state reachability" per un modello di protocolli crittografici con definizioni ricorsive e scambio di messaggi "ping-pong" (cioe' definito tramite prefix rewrite rules). L'algoritmo utilizza vincoli che rappresentano in modo finito insiemi di stringhe (di lunghezza arbitraria) utilizzati per modellare i messaggio scambiati nei protocolli ping-pong.

2.4. Bioinformatica

Nell'ambito vincoli e bioinformatica, alcuni membri dell'unità di Udine sono stati program co-chair del secondo e terzo workshop su constraints e bioinformatica, tenutosi a Nantes e a Porto. Hanno anche curato un numero speciale della rivista constraints su tali argomenti. Diversi sono i lavori relativi al problema della determinazione della struttura tridimensionale delle proteine. Su astrazioni discrete (lattice models) è stato sviluppato il nuovo solver dedicato (COLA) che migliora notevolmente le prestazioni rispetto alla codifica del problema su solver standard CLP(FD) ed è in grado di sfruttare architetture parallele. Abbiamo affrontato lo studio di vincoli globali su reticolo con anche l'utilizzo di informazioni provenienti da mappe di densità elettronica. In tale ambito abbiamo inoltre mostrato come sfruttare tecniche e algoritmi di model checking. Il problema è stato anche studiato off-lattice, sviluppando nuove tecniche di simulazione basate su multi-level agent based programming (MASPF) e nuovi potenziali di energia. Abbiamo sviluppato una variante stocastica del linguaggio CCP (Concurrent Constraint Programming) e studiato la sua applicabilità nel campo della modellizzazione biologica. Lo strumento è molto flessibile, sia grazie al potere espressivo dei vincoli che grazie a un meccanismo di definizione dei rate stocastici che è context-dependent, e permette di descrivere agevolmente e composizionalmente sistemi biologici a diversi gradi di complessità. È stato anche realizzato un prototipo di interprete/simulatore del linguaggio. E' stato affrontato uno studio sul rapporto tra modelli stocastici definiti mediante questo linguaggio e sistemi di equazioni differenziali ed automi ibridi.

Lo studio esplorativo per verificare la possibilita' di applicazione di tecniche simboliche di analisi basate su vincoli e riscrittura e' stato esteso anche al campo della bio-informatica. In questo ambito abbiamo studiato la decidibilita' dei problemi di reachability e spatial reachability (assimilabile al problema di control state reachability descritto in 1.5) per modelli utilizzati per specificare sistemi mobili e biologici. Tali sistemi sono accomunati dall'uso di processi strutturati in modo gerarchico. Gli algoritmi proposti utilizzano vincoli che rappresentano in modo finito il numero di processi (non limitato a priori) contenuto in ogni livello della struttura ad albero che modella una componente biologica o un sistema ad ambienti.

12. Problemi riscontrati nel corso della ricerca

Non sono stati riscontrati problemi che possano aver condizionato l'esecuzione del programma previsto.

Nell'unita' di Udine, alcuni membri (Dal Palu' e Bortolussi) hanno vinto un posto da ricercatore e si sono spostati in altre sedi, ma hanno continuato e continueranno a collaborare con i loro colleghi di questo progetto, portando avanti le linee di lavoro previste.

13. Elenco unità di ricerca che hanno partecipato al programma di ricerca

nº	Università	Facoltà	Responsabile	Quota Ateneo	Cofinanziamento assegnato	Finanziamento totale	Pagato	Residuo da saldare (già fatturato)	Cifra impegnata	Spese globali sostenute	Nota

1.	*Università degli Studi "G. d'Annunzio" CHIETI-PESCARA*	*Facoltà di ECONOMIA*	*BISTARELLI Stefano*	*11.600*	*26.910*	*38.510*	*26.116*	*8.535*	*3.859*	*38.510*	
2.	*Università degli Studi di GENOVA*	*Facoltà di SCIENZE MATEMATICHE FISICHE e NATURALI*	*DELZANNO Giorgio*	*10.444*	*24.370*	*34.814*	*34.771*	*0*	*0*	*34.814*	
3.	*Università degli Studi di UDINE*	*Facoltà di SCIENZE MATEMATICHE FISICHE e NATURALI*	*DOVIER Agostino*	*15.300*	*35.540*	*50.840*	*50.840*	*0*	*0*	*50.840*	
4.	*Università degli Studi di PADOVA*	*Facoltà di SCIENZE MATEMATICHE FISICHE e NATURALI*	*ROSSI Francesca*	*11.300*	*26.180*	*37.480*	*30.584*	*0*	*6.896*	*37.480*	
	TOTALE			**48.644**	**113.000**	**161.644**	**142.311**	**8.535**	**10.755**	**161.644**	

14. Risorse umane complessivamente ed effettivamente impegnate

	(mesi uomo)		
	I anno	II anno	TOTALE
personale universitario	*63*	*62*	*125*
altro personale	*77*	*85*	*162*
Personale a contratto a carico del PRIN 2005 (escluse le borse di dottorato)	*12*	*13*	*25*
Borse di dottorato	*0*	*0*	*0*

15. Modalità di svolgimento (dati complessivi)

	(numero)
partecipazioni a convegni pertinenti:	
in Italia	*22*
all'estero	*72*
articoli pertinenti pubblicati:	
su riviste italiane con referee	*0*
su riviste straniere con referee	*33*
su altre riviste italiane	*0*
su altre riviste straniere	*0*
comunicazioni a convegni/congressi internazionali pertinenti	*106*
comunicazioni a convegni/congressi nazionali pertinenti	*9*
rapporti interni	*5*
brevetti depositati	*0*

16. Tabella delle spese sostenute

nº	Responsabile (Cognome e Nome)	Università	Materiale inventariabile	Grandi Attrezzature	Materiale di consumo	Quota forfetaria certificata	Spese per calcolo ed elaborazione dati	Personale a contratto a carico del PRIN 2005	Dottorati di ricerca a carico del PRIN 2005	Servizi esterni	Missioni	Pubblicazioni	Partecipazione / Organizzazione convegni	Altro	Cifra impegnata	TOTALE
1.	*BISTARELLI Stefano*	*Università degli Studi "G. d'Annunzio" CHIETI-PESCARA*	*11.882*	*0*	*539*	*2.550*	*0*	*0*	*0*	*0*	*6.708*	*0*	*12.972*	*0*	*3.859*	34.651
2.	*DELZANNO Giorgio*	*Università degli Studi di GENOVA*	*3.199*	*0*	*514*	*2.785*	*0*	*19.615*	*0*	*0*	*7.486*	*0*	*1.172*	*0*	*0*	34.771
3.	*DOVIER Agostino*	*Università degli Studi di UDINE*	*10.867*	*0*	*0*	*4.067*	*0*	*13.905*	*0*	*0*	*17.001*	*0*	*5.000*	*0*	*0*	50.840
4.	*ROSSI Francesca*	*Università degli Studi di PADOVA*	*5.144*	*0*	*0*	*2.998*	*0*	*5.040*	*0*	*0*	*14.715*	*0*	*2.687*	*0*	*6.896*	30.584
	TOTALE		**31.092**	**0**	**1.053**	**12.400**	**0**	**38.560**	**0**	**0**	**45.910**	**0**	**21.831**	**0**		**150.846**

(Per la copia da depositare presso l'Ateneo e per l'assenso alla elaborazione e diffusione delle informazioni riguardanti i programmi di ricerca presentati; D.lgs. 196/2003 del 30/06/2003 sulla "Tutela dei dati personali")

Data ..... (inserita dal sistema alla chiusura del consuntivo) Firma .....