Relazione conclusiva del Progetto GNCS-2013 *"Specifica e verifica di algoritmi tramite strumenti basati sulla teoria degli insiemi"*

Responsabile: Eugenio G. Omodeo
Dipartimento di Matematica e Geoscienze
Università degli Studi di Trieste
eomodeo@units.it

1 Attività svolta e risultati ottenuti

Le attività del progetto svolto sono state guidate dall'obiettivo di approfondire lo studio delle potenzialità dell'utilizzo dei linguaggi logico-insiemistici per la codifica (dichiarativa) e la risoluzione (efficiente) di problemi in diversi contesti applicativi.

Come previsto nella proposta di progetto, questi obiettivi sono stati perseguiti a diversi livelli:

- a un livello più teorico, con lo studio di adeguati algoritmi di decisione operanti su formule insiemistiche;
- a livello degli strumenti di supporto alla programmazione, con lo sviluppo e messa a punto della libreria Java denominata JSetL;
- a livello degli scenari d'uso, con l'applicazione della sillogistica quantificata alla logica modale, con la specifica e verifica di correttezza in Referee di algoritmi operanti su grafi, ed infine con l'utilizzo del linguaggio di programmazione logica a vincoli insiemistici {log} per la generazione di "test-cases" a partire da specifiche in linguaggio Z.

Analizziamo qui di seguito più in dettaglio i risultati ottenuti, articolati in questi tre diversi livelli di intervento.

1.1 Metodi logici, algoritmi d'inferenza

Eliminazione di quantificatori dalla logica del I ordine. La tecnica di Skolemizzazione globale presentata in [5] ottimizza il metodo per l'eliminazione dei quantificatori nella logica del primo ordine implicitamente introdotto da Davis-Fechter nel 1991, ove i quantificatori sono rappresentati da opportuni

termini di Skolem.[1] L'estensione in [5] ammette l'eliminazione in un sol passo di gruppi di quantificatori dello stesso tipo, dando così luogo a termini di Skolem meno complessi e, conseguentemente, a dimostrazioni più brevi e chiare.

Rispetto a una versione preliminare di questo lavoro pesentata in precedenza al CILC 2012[2] è stata ottenuta una tecnica di de-skolemizzazione che consente l'intertraducibilità tra il formalismo di Davis-Fechter ed il nostro.

Procedure di decisione. In tale ambito sono stati studiati frammenti della teoria degli insiemi e della logica relazionale.

Teoria degli insiemi. Lo studio presentato a GandALf 2012[3] è stato approfondito ed esteso nella versione invitata [4] per la pubblicazione su un numero speciale di *Theoretical Computer Science*. Esso tratta il sottolinguaggio quantificato della teoria degli insiemi, denominato $\forall^{\pi}_{\mathbf{0},\mathbf{2}}$, in cui sono presenti due distinte sorte di variabili, rispettivamente per insiemi generici e per mappe (intese come insiemi di coppie ordinate), nonché costrutti che permettono la manipolazione esplicita di coppie ordinate. Per il problema della soddisfacibilità di formule di $\forall^{\pi}_{\mathbf{0},\mathbf{2}}$, viene descritta una procedura di decisione che richiede tempo esponenziale non-deterministico nel caso pessimo. Tuttavia tale procedura, se ristretta a formule di $\forall^{\pi}_{\mathbf{0},\mathbf{2}}$ con un numero *a priori* limitato di quantificatori, richiede soltanto tempo polinomiale non-deterministico. Tale frammento trova applicazioni nel campo della rappresentazione della conoscenza. Viene infatti presentata una nuova logica descrittiva, denominata $\mathcal{DL}\langle\forall^{\pi}_{\mathbf{0},\mathbf{2}}\rangle$, che estende con alcune caratteristiche di meta-modellizzazione la logica $\mathcal{DL}\langle\forall^{\pi}_{\mathbf{0}}\rangle$ studiata in un lavoro del 2011 da Cantone-Longo-Nicolosi.[4] In particolare, la distinzione tra *concetti* ed *individui* risulta essere rilassata in $\mathcal{DL}\langle\forall^{\pi}_{\mathbf{0},\mathbf{2}}\rangle$ in modo tale da consentire ai concetti sia di partecipare a relazioni che essere istanze di altri concetti, come accade per gli individui. Nonostante ciò, il problema della consistenza per $\mathcal{DL}\langle\forall^{\pi}_{\mathbf{0},\mathbf{2}}\rangle$ rimane NP-completo. Viene, infine, dimostrata l'indecidibilità di alcune estensioni del linguaggio $\forall^{\pi}_{\mathbf{0},\mathbf{2}}$.

Sempre nell'ambito della decidibilità in teoria degli insiemi, è stato ultimato un lavoro su una procedura di decisione per il problema della soddisfacibilità per l'estensione MLSSPF del linguaggio MLSS (Multi-Level Syllogistic with

[1] M. Davis and R. Fechter: A Free Variable Version of the First-Order Predicate Calculus. *J. Log. Comput.* 1(4): 431-451, 1991.

[2] In F. Lisi, editor, *Proceedings of the 9th Italian Convention on Computational Logic (CILC 2012), Rome, Italy, June 6-7, 2012*, volume 857, pages 17–31. CEUR Workshop Proceedings, ISSN 1613-0073, 2012.

[3] D. Cantone and C. Longo. A decidable quantified fragment of set theory with ordered pairs and some undecidable extensions. In M. Faella and A. Murano, editors, Proc. Third International Symposium on *Games, Automata, Logics and Formal Verification,* Napoli, Italy, 6-8th June 2012, volume 96 of *Electronic Proceedings in Theoretical Computer Science*, pages 224–237. Open Publishing Association, 2012.

[4] D. Cantone, C. Longo, and M. Nicolosi Asmundo. A decidable quantified fragment of set theory involving ordered pairs with applications to description logics. In M. Bezem, editor, Computer Science Logic (CSL11), 25th International Workshop/20th Annual Conference of the EACSL, volume 12 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 129–143, Dagstuhl, Germany, April 2011.

Singletons) con l'operatore *powerset* e il predicato di finitezza *Finite* (si veda [7]).

Logica relazionale. Sono state disegnate delle procedure di decisione basate sul metodo dei tableaux duali relazionali per alcuni frammenti della logica RL delle relazioni binarie (si veda [6]). Alcune procedure sono state definite modificando la regola di decomposizione per formule del tipo $x(R;S)y$, rendendola meno liberale, e forzando un ordine nella decomposizione delle formule occorrenti sui rami del tableau. Le logiche a cui tali procedure sono state applicate sono caratterizzate da alcuni vincoli imposti nella costruzione di termini $R;S$ il cui operatore principale è la composizione relazionale. Il primo frammento ammette che la parte sinistra R di tali termini possa essere una variabile relazionale soltanto; il secondo ammette che, all'interno di R, occorrano anche l'unione e l'intersezione di relazioni; il terzo ammette che R sia la costante $\mathbf{1}$, rappresentante la relazione universale. La procedura di decisione per l'ultimo frammento contiene anche una condizione di *blocking* che ne garantisce la terminazione. Tutte le procedure di cui sopra mantengono un certo grado di non-determinismo che potrà essere ridotto oppure eliminato al momento dell'implementazione.

È stata anche disegnata una procedura di decisione deterministica basata sui tableaux duali per una classe di frammenti relazionali che ammettono un numero infinito di costanti relazionali che possono godere delle proprietà di riflessività, di transitività, e di ereditarietà (cf. [3]). Al posto delle regole di decomposizione per formule del tipo $x(R;S)y$ e $x(-(R;Q))y$, nella procedura è stata introdotta un'unica regola che permette di decomporre in un sol passo tutte le formule di entrambi i tipi (composizionale e composizionale negativo) che soddisfino il vincolo di condividere la stessa variabile sinistra. I frammenti relazionali considerati permettono di esprimere diverse logiche non-classiche fra cui logiche multimodali e logiche descrittive.

1.2 Strumenti per la programmazione

Messa a punto e testing di JSetL. Come previsto nella proposta di progetto, è stato portato avanti lo sviluppo di JSetL, una libreria Java che offre un linguaggio di vincoli insiemistici all'interno di un ambiente di programmazione convenzionale object-oriented.

In particolare si è **** completata l'integrazione in JSetL di un risolutore di vincoli su domini finiti di interi e su domini finiti di insiemi di interi e aggiunta la possibilità di trattare intervalli di interi e di insiemi e multi-intervalli di interi. La nuova versione aggiornata di JSetL è disponibile all'indirizzo `http://cmt.math.unipr.it/jsetl.html`.

In particolare in [11] viene mostrato come sfruttare il non-determinismo insito nelle operazioni insiemistiche e nel risolutore di vincoli JSetL per fornire una semplice soluzione a problemi naturalmente esprimibili in termini non-deterministici, come ad esempio problemi su grafi o realizzazione di semplici analizzatori sintattici (DCG). Questo è ottenuto sfruttando diverse possibilità offerte da JSetL—come variabili logiche, strutture dati parzialmente specificate,

unificazione—combinate con un risolutore di vincoli che permette di risolvere vincoli in modo non-deterministico e all'utente di definire nuovi vincoli propri. L'utente può così definire le proprie procedure non-deterministiche come nuovi vincoli, lasciando che sia il risolutore di vincoli a gestirle in modo opportuno.

Avvio della realizzazione di un nuovo interprete per SETL. Questa attività s'intreccia con la storia del proof-checker ÆtnaNova/Referee menzionato altrove[5]: in effetti, dato che il verificatore è stato scritto in SETL, disporre di un nuovo interprete SETL serve a proteggerlo da una rapida obsolescenza.

Abbiamo intrapreso lo sviluppo di un interprete SETL che, pur mantenendo tutte le peculiarità del linguaggio originale, le integrasse con istruzioni di supporto per la verifica. Allo stato attuale, l'interprete implementa:

1. tutti i tipi primitivi di SETL
2. la valutazione di espressioni logiche e aritmetiche
3. l'assegnazione
4. i costrutti if-then, if-then-else, while e for
5. la stampa a video

Con l'intento di minimizare i tempo di computazione e le risorse di memoria necessarie alla valutazione di un programma SETL, l'interprete supporta il copy-on-write e ad ogni richiesta di copia di un valore si limita ad effettuare una copia del riferimento a quel valore, posticipando una eventuale duplicazione alla richiesta di modifica.

1.3 Illustrazioni d'uso

{log} come generatore di "test case" per il "Test Template Framework" (TTF). Il problema che è stato affrontato è quello della generazione dei "casi di test" per un programma nell'ambito di un approccio di "model-based testing", in base al quale i "casi di test" sono generati a partire dalla specifica del programma (non dal codice sorgente).

TTF è un metodo di model-based testing per specifiche scritte in Z (linguaggio di specifica basato sulla logica del I ordine arricchita con la teoria degli insiemi). Data una specifica Z, TTF partiziona il suo spazio di input e genera delle "specifiche di test", ovvero delle congiunzioni di predicati atomici scritti in Z. Una qualsiasi soluzione di questa formula rappresenta un "caso di test" per il programma originario

In [12] e [13] viene mostrato come le "specifiche di test" scritte in Z possano essere trasformate in formule {log} e quindi risolte tramite il constraint solver di {log}. Per ottenere questo è stato realizzato un traduttore automatico in grado di tradurre formule Z in goal {log} e, viceversa, risposte generate da

[5] Ideazione e specifica di dettaglio del linguaggio di programmazione SETL devono molto all'illustre matematico e informatico Jacob T. Schwartz (1930–2009).

{log} in formule Z. Si è inoltre modificato un ambiente per la generazione di casi di test preesistente, denominato FasTest, per renderlo in grado di invocare, in modo del tutto automatico e trasparente all'utente, il traduttore {log}-Z e quindi il risolutore {log}, sia per individuare le specifiche di test insoddisfacibili, sia per calcolare una soluzione possibile (e cioe' un caso di test) per quelle soddisfacibili. Infine, l'efficienza e l'efficacia di tale approccio è stata valutata applicando questo ambiente ad oltre 2000 formule Z.

Questo lavoro e' stato svolto in stretta collaborazione con Maximiliano Cristiá dell'Università di Rosario (Argentina).

Sperimentazione con il proof-checker ÆtnaNova/Referee. Già in un precedente progetto GNCS era stata avviata una linea di sperimentazione riguardante i "*claw-free graph*", di cui Milanič–Tomescu hanno recentemente dimostrato (ma al di fuori di questo progetto) la rappresentabilità come grafi aventi per vertici degli insiemi e per archi le coppie non orientate di nodi dei quali uno appartenga (in quanto insieme) all'altro.

Sfruttando questo risultato di rappresentazione, è stata sviluppata formalmente e verificata con il proof-checker ÆtnaNova/Referee la dimostrazione che ogni grafo *claw-free* ammette un matching quasi-perfetto (perfetto quando il numero dei vertici è pari) nonché un cammino hamiltoniano.

Un'esposizione ragionata di questi risultati è stata finalmente pubblicata—proprio questo mese—sul Journal of Automated Reasoning,[6]; mancava, invece, una formalizzazione del risultato di rappresentazione di Milanič–Tomescu da cui esso scaturiva. Ora anche il risultato in questione è stato dimostrato formalmente, assieme ad altri ad esso affini, grazie al nostro verificatore di correttezza di dimostrazioni. Alla URL `http://www2.units.it/eomodeo/GraphsViaMembership.html` si trova documentazione al riguardo, in particolare l'articolo [16], che è in fase di ultimazione per la sottomissione a una rivista scientifica. Una comunicazione su questa attività, [1], è stata portata al CILC 2013, a Catania. Un'altra comunicazione di taglio piú ampio, [14], è stata invitata allo stesso convegno.

Teoria delle decisioni. Prendendo spunto da un lavoro di Eliaz-Ok del 2006,[7] è stata introdotta in [2] una nuova nozione di *indiscernibilità* per una funzione di scelta, dimostrando varie proprietà in presenza di assiomi molto deboli. Tale nozione è in stretta relazione con la nozione analoga relativa alle NaP-preferences. L'obiettivo finale è di formulare una teoria assiomatica della scelta in *teoria delle decisioni* che è alternativa rispetto a quella classica, legandola strettamente alla nozione di NaP-preferences mediante la teoria delle preferenze rivelate.

[6] E. G. Omodeo, A. I. Tomescu. Set Graphs. III. Proof Pearl: Claw-free Graphs Mirrored into Transitive Hereditarily Finite Sets. (DOI: 10.1007/s10817-012-9272-3). Journal of Automated Reasoning, **52**(1), 1–29, Springer (2014).

[7] K. Eliaz and E.A. Ok. Indifference or indecisiveness? Choice-theoretic foundations of incomplete preferences. *Games and Economic Behavior*. Vol. 56, pp. 6186, 2006.

Specifica di sistemi ibridi tramite formule al primo ordine sui reali. Questa linea di ricerca si è occupata di individuare tecniche per modellare sistemi ibridi, cioè sistemi che evolvono sia in modo continuo che discreto, tramite formule al primo ordine sui reali. Inoltre, l'attività di ricerca ci ha portato ad investigare la possibilità di calcolare delle approssimazioni degli insiemi di raggiungibilità di tali modelli interpretando delle formule, appartenenti alla teoria di specifica del modello stesso, in opportune semantiche non standard [**?**, **?**].

2 Rendiconto spese

Tutti i partecipanti al progetto previsti nella domanda iniziale hanno effettivamente partecipato e contribuito allo sviluppo del progetto stesso. Il finanziamento erogato (5000 Euro) è stato in larga misura utilizzato per il rimborso di spese di missione per partecipazione dei componenti del progetto a convegni e ad incontri di lavoro; inoltre in occasione dell'incontro conclusivo del progetto è stato invitato in qualità di relatore esterno Alfio Giarlotta.

Le spese sono state ripartite indicativamente come segue:

- Casagrande, missione a Taormina (31 agosto 2013–04 settembre 2013) per workshop HSB 2013: iscrizione 195 Euro.
- Omodeo, missione a Palermo (8–11 settembre 2013) per partecipazione a Convegno annuale ICTCS, ove ha presentato anche un contributo scientifico: 597 Euro.
- Rossi, missione a Catania (24–27 settembre 2013) per partecipazione a Convegno CILC 2013, ove ha presentato anche due contributi scientifici: 678 Euro.
- Bergenti, missione a Torino (1 dicembre 2013–7 dicembre 2012) per partecipazione a conferenza AI*IA ed workshop WOA 2013: 400 Euro.
- Cantone (27 novembre 2013–1 dicembre 2013), missione a Trieste per coordinamento attività di ricerca relative al progetto: 400 Euro.
- Cantone, Casagrande, Nicolosi Asmundo, Omodeo, Rossi, missione a Udine per incontro di lavoro relativo al progetto (20 gennaio 2014); esteso, nel caso di Cantone e Nicolosi, in permanenze di collaborazione a Trieste (18–25 gennaio 2014): 1480 Euro.
- Giarlotta (relatore), missione a Udine e Trieste (19–22 gennaio 2014), per due conferenze: 850 Euro.

N.B. Le cifre indicate sopra si riferiscono, per le missioni piú recenti, agli impegni di spesa assunti e non alle cifre effettivamente rimborsate.

Si noti anche che una missione di Marianna Nicolosi Asmundo che era stata programmata per il periodo 15–18 dicembre 2013 non ha potuto aver luogo per via della chiusura dell'aeroporto di Catania causata dall'attività dell'Etna.

3 Prodotti della ricerca

Software

- JSetL. Home page:
  `http://cmt.math.unipr.it/jsetl.html`
- {log}. Home page:
  `http://people.math.unipr.it/gianfranco.rossi/setlog.Home.html`

Proofware

- Scenario sulla rappresentazione di grafi tramite la relazione di appartenenza e relativa documentazione:
  `http://www2.units.it/eomodeo/GraphsViaMembership.html`.

Pubblicazioni e Comunicazioni a convegni

[1] P. Calligaris, E. G. Omodeo, A. I. Tomescu. A proof-checking experiment on representing graphs as membership digraphs. Proc. CILC 2013, v. `http://www.dmi.unict.it/~cilc2013/submissions/cilc20130_submission_21.pdf`.

[2] D. Cantone and A. Giarlotta. *Individual choice and revealed NaP-preference: the relation of indiscernibility.* Work in progress, 2014.

[3] D. Cantone, J. Golińska-Pilarek, and M. Nicolosi Asmundo. *A relational dual tableau decision procedure for multimodal and description logics.* Work in progress, 2014.

[4] D. Cantone and C. Longo. A decidable quantified fragment of set theory with ordered pairs and some undecidable extensions. Submitted to *Theoretical Computer Science* (Special issue on GandALF 2012), 2013.

[5] D. Cantone, M. Nicolosi Asmundo, and E. G. Omodeo. *On the elimination of quantifiers through descriptors in predicate logic.* Work in progress, 2014.

[6] D. Cantone, M. Nicolosi Asmundo, and E. Orłowska. *A dual tableau decision procedure for an expressive relational logic with restricted composition.* Work in progress, 2013.

[7] D. Cantone and P. Ursino. Formative processes with applications to the decision problem in set theory: II. Powerset and singleton operators, finiteness predicate. Submitted to *Information and Computation*, 2013.

[8] A. Casagrande, T. Dreossi, C. Piazza. Approximated Symbolic Computations over Hybrid Automata. HAS 2013: 43–57.

[9] A. Casagrande, T. Dreossi. pyHybrid Analysis: A Package for Semantics Analysis of Hybrid Systems. DSD 2013: 815–818.

[10] A. Casagrande, J. Jarmolowska, M. Turconi, F. Fabris, P. P. Battaglini. PolyMorph: A P300 Polymorphic Speller. Brain and Health Informatics 2013: 297–306.

[11] G. Rossi, F. Bergenti. Nondeterministic Programming in Java with JSetL. In D.Cantone and M.Nicolosi Asmundo, eds, CILC 2013: Italian Conference on Computational Logic, CEUR Workshop Proceedings, Vol. 1068 (http://ceur-ws.org/Vol-1068/), ISSN 1630-0073, Sept. 2013, 211-226.

[12] M. Cristiá, G. Rossi. Using {log} as a Test Case Generator for Z Specifications. Proc. CILC 2013 - 28-esimo Convegno Italiano di Logica Computazionale, Sept. 2013, v. `http://www.dmi.unict.it/~cilc2013/submissions/cilc20130_submission_18.pdf`.

[13] M. Cristiá, G. Rossi, C. Frydman. {log} as a Test Case Generator for the Test Template Framework. In R.M.Hierons, M.G.Merayo, and M.Bravetti, eds, Software Engineering and Formal Methods - 11th International Conference, SEFM 2013, Lecture Notes in Computer Science, Vol. 8137, Springer, ISBN: 978-3-642-40560-0, 2013, 229243.

[14] E. G. Omodeo. Proof verification within set theory. CILC 2013, conferenza invitata, v. `http://www.dmi.unict.it/~cilc2013/invitati_ita.html`.

[15] E. Omodeo, A. Policriti, A. I. Tomescu. Bridging syllogistics with combinatorics. Comunicazione ad ICTCS 2013, v. `http://www.unipa.it/ictcs13/accepted.html`.

[16] E. G. Omodeo, A. I. Tomescu. Set Graphs. V. Proof Pearl: On representing graphs as membership digraphs. (Pronto per la sottomissione, v. `http://www2.units.it/eomodeo/GraphsViaMembershipPAPER.pdf`).