Estratto da

R. Ferro e A. Zanardo (a cura di), *Atti degli incontri di logica matematica* Volume 3, Siena 8-11 gennaio 1985, Padova 24-27 ottobre 1985, Siena 2-5 aprile 1986.

Disponibile in rete su http://www.ailalogica.it

UN SISTEMA DI ASSEGNAZIONE DI TIPI PARZIALI

M. DEZANI – CIANCAGLINI, B. VENNERI
Dipartimento di Informatica, Università di Torino

Introduzione.

Scopo di questo lavoro e' presentare un sistema di assegnazione di *tipi parziali* a termini del λ-calcolo puro, seguendo la nozione di tipo parziale introdotta con motivazioni semantiche in [Cartwright '84].
Il modo piu' naturale di definire la semantica di tipi e termini del λ-calcolo e' quello di interpretarli in un dominio **D** in modo che l'interpretazione di un termine sia contenuta nell'interpretazione di ogni tipo assegnabile a quel termine. Ma l'interpretazione di tipi come insiemi qualsiasi di **D** presenta alcune difficolta' per i tipi polimorfi, poiche' si possono dedurre tipi (costruiti con il quantificatore ∀) la cui interpretazione in ogni modello risulta essere l'insieme vuoto. La soluzione proposta in [MacQueen,Plotkin e Sethi '84] e' quella di interpretare i tipi come *ideali* , ossia insiemi chiusi per approssimazioni e limiti di catene crescenti.
Tuttavia anche la teoria degli ideali non e' del tutto soddisfacente quando si considerano tipi definiti ricorsivamente, perche' manca un meccanismo generale di risoluzione delle equazioni di tipo ricorsive. La proposta di Cartwright, cioe' l'interpretazione dei tipi come *intervalli*, non solo risolve i problemi suddetti ma, soprattutto, introduce un nuovo modo di intendere un tipo non piu' come un insieme di valori ma come un

----

(*) Ricerca parzialmente finanziata dal M.P.I. 40% Comitato per la Ingegneria.
(**) Centro Linceo Interdisciplinare di Scienze Matematiche e loro applicazioni (per gli anni accademici 85-86, 86-87 e 87-88).

insieme (intervallo) di insiemi di valori. In conseguenza, la nozione di appartenenza a un tipo assume un duplice significato: un valore *appartiene necessariamente* o *possibilmente* all'intervallo **A** a seconda che si sia provata la sua appartenenza, rispettivamente, a *tutti* o a *qualche* insieme di **A**. Si introduce cosi' la possibilita' di caratterizzare un termine mediante un tipo anche in modo parziale, quindi in generale una tipizzazione piu' fine. Cartwright [Cartwright '84] considera che gli insiemi di valori siano ideali ed ottiene, quindi, un insieme di intervalli che include quello degli ideali.
In questo lavoro gli autori presentano un sistema di regole di assegnazione di tipi parziali, di cui hanno dimostrato la *correttezza* e la *completezza* rispetto ad una semantica degli intervalli che e' una generalizzazione di quella di Cartwright.

Regole di assegnazione di tipi.

I tipi sono costruiti, come e' usuale, usando il connettivo $\rightarrow$ e gli operatori $\forall$, μ . Se φ, ϕ... sono variabili di tipo e ρ, σ, τ... denotano tipi, la grammatica che definisce i tipi e'

$\tau ::= \varphi \mid \sigma \rightarrow \tau \mid \forall\varphi.\sigma \mid \mu\varphi.\sigma$.

Un tipo e' chiuso se non contiene variabili libere di tipo.
Un'*asserzione* di tipo e' un'espressione della forma $\xi M:\sigma$, di cui M e' il soggetto, σ e' il predicato e ξ denota il predicato modale (scriveremo anche $\bar{\xi}$ per denotare il predicato ! se ξ=? e viceversa).
Scriviamo $!M:\sigma$ e $?M:\sigma$ per intendere, rispettivamente, che il termine M ha *necessariamente* il tipo σ e che M ha *possibilmente* il tipo σ.
Una *base* B e' un insieme , eventualmente vuoto, di asserzioni i cui soggetti sono variabili e tale che ci sia una sola asserzione per ogni soggetto.
Le regole di assegnazione di tipi sono definite in uno stile di deduzione naturale e consentono di inferire sequenti della forma $B \vdash \xi M:\sigma$:

(Ax) $B \vdash \xi x:\sigma$ se $\xi x:\sigma \in B$

$$(!\Rightarrow?)\ \frac{B \vdash !M:\sigma}{B \vdash ?M:\sigma} \qquad (?\Rightarrow!)\ \frac{B \vdash ?M:\sigma \quad \sigma \text{ e' chiuso}}{B \vdash !M:\sigma}$$

$$(\rightarrow I)\ \frac{B \cup \{\xi x:\sigma\} \vdash \bar{\xi} M:\tau}{B \vdash \xi\, \lambda x.M:\sigma\rightarrow\tau} \text{ (B non contiene asserzioni su x)}$$

$$(\rightarrow E)\ \frac{B \vdash \xi M:\sigma\rightarrow\tau \qquad B \vdash \bar{\xi} N:\sigma}{B \vdash \xi\, MN:\tau}$$

$$(\forall I)\ \frac{B \vdash \xi M:\sigma}{B \vdash \xi M:\forall\varphi.\sigma} \text{ (φ non occorre libera in alcun predicato di B il cui soggetto e' una variabile libera in M)}$$

$$(\forall I\ c.r)\ \frac{B \vdash \xi M:\sigma[\tau/\varphi] \text{ per ogni } \tau \text{ chiuso}}{B \vdash \xi M:\forall\varphi.\sigma}$$

$$(\forall E)\ \frac{B \vdash \xi M:\forall\varphi.\sigma}{B \vdash ?M:\sigma[\tau/\varphi]} \qquad (\forall E\ c.r)\ \frac{B \vdash !M:\forall\varphi.\sigma}{B \vdash !M:\sigma[\tau/\varphi]} \text{ (τ e' chiuso)}$$

$$(\mu I)\ \frac{B \vdash \xi M:\sigma[\mu\varphi.\sigma/\varphi]}{B \vdash \xi M:\mu\varphi.\sigma} \qquad (\mu E)\ \frac{B \vdash \xi M:\mu\varphi.\sigma}{B \vdash \xi M:\sigma[\mu\varphi.\sigma/\varphi]}$$

$$(EQ)\ \frac{B \vdash \xi M:\sigma \qquad M =_\beta N}{B \vdash \xi N:\sigma}$$

La regola (!⇒?) esprime il fatto che le asserzioni necessarie includono quelle possibili, come in logica modale. Le regole $(\rightarrow I)$ e $(\rightarrow E)$ corrispondono alle regole di introduzione e di eliminazione dell'implicazione adeguate per la semantica a 3 valori nel caso deterministico (modelli a 3 valori in [Girard '76]). La regola $(\forall E)$, invece, tratta diversamente le asserzioni possibili da quelle necessarie, il che non avviene nei modelli a 3 valori. Questa scelta, che e' stata fatta per definire regole corrette rispetto alla semantica degli intervalli, costituisce un indebolimento del sistema che e' parzialmente compensato dalla regola $(\forall E c.r)$. Le regole $(? \Rightarrow !)$ e $(\forall I c.r)$ sono giustificate dalla interpretazione del quantificatore universale nella semantica degli intervalli. Le regole (μI) e (μE) sono usali e la regola (EQ) e' introdotta solo per ottenere il teorema di completezza.

Semantica.

Dato un λ-modello $\langle \mathbf{D}, \cdot, \epsilon \rangle$ diciamo che un sottoinsieme Z di $\mathbf{D}$ e' un insieme-zero se per ogni $z \in Z$, $d \in \mathbf{D}$ anche $z \cdot d \in Z$.

Un *intervallo* $|X,Y|$ su $\mathbf{D}$, dove $Z \subseteq X \subseteq Y \subseteq \mathbf{D}$, e' definito come

$|X,Y| = \{U \subseteq \mathbf{D} \mid X \subseteq U \subseteq Y\}$ (si noti che questa definizione comprende quella di Cartwright come caso particolare).

Interpretiamo i tipi nell'insieme $Type_{\mathbf{D}}$ degli intervalli su $\mathbf{D}$: una interpretazione dei tipi e' una funzione $\mathcal{V}$:Tipi $\rightarrow Type_{\mathbf{D}}$ tale che

i) $\mathcal{V}(\sigma \rightarrow \tau) = \mathcal{V}(\sigma) \rightarrow \mathcal{V}(\tau)$

ii) $\mathcal{V}(\forall \varphi.\sigma) = \bigcap_{\tau \text{ chiuso}} \mathcal{V}(\sigma[\tau/\varphi])$

iii) $\mathcal{V}(\mu\varphi.\sigma) = \mathcal{V}(\sigma[\mu\varphi.\sigma/\varphi])$

dove $\rightarrow$ e $\bigcap$ fra intervalli sono definiti da

$|X,Y| \rightarrow |V,T| = |Y \rightarrow V, X \rightarrow T|$ e $|X,Y| \cap |V,T| = |X \cap V, Y \cap T|$.

Conveniamo che, se $\mathcal{V}(\sigma) = |X,Y|$, allora $\mathcal{V}^!(\sigma) = X$ e $\mathcal{V}^?(\sigma) = Y$.

La nozione di soddisfacibilita' semantica $(\models)$ e' definita in modo ovvio.

$B \models \xi M{:}\sigma$ sse, per ogni λ-modello $\mathcal{M}$ e per ogni ρ e $\mathcal{V}$:

$[\![x]\!]^{\mathcal{M}}_{\rho} \in \mathcal{V}^{\xi'}(\tau)$ per ogni $\xi' x{:}\tau \in B \Rightarrow [\![M]\!]^{\mathcal{M}}_{\rho} \in \mathcal{V}^{\xi}(\sigma)$.

Gli autori hanno provato che le regole di assegnazione di tipi sopra definite sono semanticamente *corrette* e *complete*, ossia che

$$B \vdash \xi M{:}\sigma \quad \Leftrightarrow \quad B \models \xi M{:}\sigma$$

La dimostrazione della correttezza e' per induzione sulla dimostrazione, mentre la prova della completezza usa il "term-model" dell'uguaglianza β. Inoltre si dimostra che, se $\mathbf{D}$ e' un c.p.o. algebrico, anche $Type_{\mathbf{D}}$ e' un c.p.o algebrico e che tutti i costruttori di tipo sono funzioni continue e preservano gli elementi totali (ossia gli intervalli che contengono un solo insieme).

Per tutte le dimostrazioni citate gli autori rimandano ad un loro lavoro di prossima pubblicazione.

Riferimenti

CARTWRIGHT R. *Types as Intervals.* Conference Record of the 12-th Annual ACM Symposium on Principles of Programming Languages (1985), pp.22-36.

GIRARD J.Y. *Three-valued Logic and Cut-elimination: The Actual Meaning of Takeuti's Conjecture.* Dissertationes Mathematicae , Warszawa (1976), pp.1-31.

MACQUEEN D., G.PLOTKIN e R.SETHI. *An Ideal Model for Recursive Polimorphic Types.* Conference Record of the 11-th Annual ACM Symposium on Principles of Programming Languages (1984), pp.165-174.

MITCHELL J.C., *Polymorphic Type Inference and Containment.* Accettato per la pubblicazione su Information and Control.