4 Specifiche logico-formali: errata corrige ed integrazioni

Le seguenti parti delle note su "Specifiche Logico-Formali" di E.Astesiano e G.Reggio (versione 3.2 - A.A. 1995-96) vanno ignorate, poiche' sono sbagliate:

- sezione 1.4
- proposizione 1.39
- teorema 2.16 asserto iii)
- teorema 2.18 asserto ii) [in ogni caso i risultati sulle algebre finali non sono inclusi nel programma]
- pagina 35-36 a partire dalla definizione 2.40.

4.1 Nozioni categoriali

Molte definizioni attinenti a strutture matematiche possono essere date in modo unificato, vedendole come casi particolari di *nozioni categoriali*. Il primo passo per questa unificazione concettuale e' l'osservazione che strutture matematiche omogenee (p.e. i gruppi) possono essere visti come oggetti di una *categoria*.

Definition 4.1 (Categoria) *Una categoria $\mathcal{C}$ e' data da:*

- *un insieme/classe $|\mathcal{C}|$, i cui elementi sono detti oggetti, con un abuso di notazione scriveremo $A \in \mathcal{C}$ per indicare che A e' un oggetto di $\mathcal{C}$*
- *per ogni coppia di oggetti $A, B \in \mathcal{C}$ un insieme $\mathcal{C}(A, B)$, i cui elementi sono detti frecce/morfismi da A a B in $\mathcal{C}$, useremo la notazione $f: A \to B$ o $A \xrightarrow{f} B$ per indicare che $f \in \mathcal{C}(A, B)$, quando $\mathcal{C}$ e' ovvia dal contesto*
- *per ogni oggetto $A \in \mathcal{C}$ una freccia $\mathrm{id}_A: A \to A$, detta l'identita' su A*
- *per ogni terna di oggetti $A, B, C \in \mathcal{C}$ una operazione di $\circ: \mathcal{C}(B, C) \times \mathcal{C}(A, B) \to \mathcal{C}(A, C)$, detta composizione, che scriveremo con l'usuale notazione infissa, cioe' se $f: A \to B$ e $g: B \to C$ allora $g \circ f: A \to C$*

Infine la composizione deve soddisfare la proprieta' associativa, cioe' se $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ allora $h \circ (g \circ f) = (h \circ g) \circ f: A \to D$, ed le opportune identita' devono comportarsi come unita' per la composizione, cioe' se $f: A \to B$ allora $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$.

E' spesso conveniente descrivere un insieme di equazioni tra espressioni che denotato frecce in una categoria mediante *diagrammi commutativi*. Un diagramma commutativo e' un (iper)grafo diretto i cui nodi sono etichettati da oggetti e i cui archi sono etichettati da frecce, in modo consistente, cioe' se si ha un arco etichettato $A \xrightarrow{f} B$, allora $f \in \mathcal{C}(A, B)$. Un diagramma commutativo G corrisponde all'insieme di equazioni

$$\{comp(p) = comp(q): A \to B \mid A, B \text{ nodi e } p, q \text{ cammini da } A \text{ a } B \text{ in } G\}$$

dove $comp(p)$ e' la composizione delle etichette (cioe' frecce di $\mathcal{C}$) che si incontrano percorrendo il cammino (poiche' la composizione e' associativa, basta dare l'ordine di composizione per definire univocamente $comp(p)$). Per esempio idiagrammi commutativi che esprimono la proprieta' associativa e le unita' per la composizione sono:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g \circ f"'] & B \arrow[d, "h \circ g"] \\
C \arrow[r, "h"'] & D
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "\mathrm{id}_A"] \arrow[d, "f"'] \arrow[dr, "f"] & A \arrow[d, "f"] \\
B \arrow[r, "\mathrm{id}_B"'] & B
\end{tikzcd}$$

Example 4.2 Vediamo alcuni esempi di categorie che usano strutture matematiche gia' familiari:

- la categoria **Set** degli insiemi (come oggetti) e delle funzioni (come frecce), dove la composizione e' l'usuale composizione funzionale

- la categoria **Rel** degli insiemi e delle relazioni, dove la composizione e' l'usuale composizione di relazioni
- la categoria **Sig** delle segnature (con predicati) e morfismi di segnatura
- la categoria $\mathbf{Alg}_\Sigma$ delle Σ-algebre e Σ-omomorfismi
- la categoria $\mathbf{Alg}^s_\Sigma$ delle Σ-algebre e **Σ-omomorfismi forti**, dove un Σ-omomorfismo $h: A \to B$ e' **forte** $\stackrel{\Delta}{\iff}$ per ogni arieta' w, simbolo di predicato $pr \in PR_w$ ed elemento $a \in A_w$ si ha $pr^A(a) \leftrightarrow pr^B(h_w(a))$.
  Quindi $\mathbf{Alg}^s_\Sigma$ e' una *sotto-categoria* di $\mathbf{Alg}_\Sigma$.
- dato un (pre)ordine parziale $(X, \leq)$ lo possiamo vedere come una categoria $\mathbf{X}$, i cui oggetti sono gli $x \in X$, mentre le frecce sono coppie di oggetti (x, y) t.c. $x \leq y$, piu' precisamente $(x,y): x \to y \stackrel{\Delta}{\iff} x \leq y$.
- data una segnatura Σ (senza predicati) e fissato un insieme (infinito) X di variabili possiamo definire una categoria $\mathbf{T}_\Sigma(X)$ i cui oggetti sono sottoinsiemi (finiti) $A \subseteq X$, mentre una freccia $\sigma: A \to B$ e' data da una funzione $\sigma: A \to T_\Sigma(B)$, cioe' una sostituzione. Per definire la composizione si fa' uso della estenzione omomorfa $\sigma^*: T_\Sigma(A) \to T_\Sigma(B)$ di σ a $T_\Sigma(A)$.
- data una categoria $\mathcal{C}$ si puo' definire una nuova categoria $\mathcal{C}^{op}$, detta **categoria opposta o duale**, con gli spessi oggetti ma dove le frecce sono *rovesciate*, cioe' $\mathcal{C}^{op}(A, B) = \mathcal{C}(B, A)$.

Vediamo adesso dei semplici esempi di nozioni categoriali, cioe' che hanno senso in qualunque categoria, e a cosa corrispondono negli esempi di categorie dati sopra.

Definition 4.3 *Data una freccia $f: A \to B$ in $\mathcal{C}$ si dice che*

- *f e'* **mono** $\stackrel{\Delta}{\iff} \forall X \in \mathcal{C}.\forall g, h: X \to A.(f \circ g = f \circ h) \implies g = h$
- *f e'* **epi** $\stackrel{\Delta}{\iff} \forall X \in \mathcal{C}.\forall g, h: B \to X.(g \circ f = h \circ f) \implies g = h$
  Epi e' la proprieta' duale *di mono, poiche' f e' un epi in $\mathcal{C}$ sse f e' un mono in $\mathcal{C}^{op}$*
- *f e' un* **iso** $\stackrel{\Delta}{\iff} \exists g: B \to A.(f \circ g = \mathrm{id}_B) \land (g \circ f = \mathrm{id}_A)$
  g e' detta **inversa** *di f. La proprieta' di essere un iso e'* auto-duale*, cioe' e' il duale di se stessa. Scriviamo $A \cong B$ se esiste (non necessariamente unico) un isomorfismo da A a B.*

Proposition 4.4 *Se f e' un iso, allora la sua inversa e' unica (ed e' a sua volta un iso). Se f e' un iso allora e' sia mono che epi (ma in generale non vale l'inverso). Le identita' sono iso (e quindi anche mono ed epi). La classe dei mono/epi/iso e' chiusa per composizione. Se $g \circ f$ e' mono allora f e' mono (e dualmente se $g \circ f$ e' epi allora g e' epi).*

Example 4.5 Vediamo cosa sono in concreto i mono, gli epi e gli iso in alcuni degli esempi di categorie:

- in **Set** una funzione $f: A \to B$ e' mono sse e' iniettiva, e' epi sse e' surgettiva, ed e' iso sse e' bigettiva
- in **Rel** una relazione $R: A \to B$ (cioe' $R \subseteq A \times B$) e' mono $R^c irc \circ R$ e' l'identita' su A ($R^c irc$ e' la relazione inversa, cioe' $R^\circ(b, a) \leftrightarrow R(a, b)$), e' epi sse $R \circ R^\circ$ e' l'identita' su B, ed ' iso sse e' mono ed epi
- in $\mathbf{X}$ (la categoria corrispondente ad un preordine parziale) tutte le frecce sono sia mono che epi, mentre (x, y) e' iso sse $x \leq y \leq x$.
- in $\mathbf{Alg}_\Sigma$ un Σ-omomorfismo $h: A \to B$ e' mono sse le sue componenti sono funzioni iniettive, epi sse le sue componenti sono surgettive, ed iso sse e' **forte** le sue componenti sono bigettive.

La nozione di iso e' particolamente importante, infatti in teoria delle categorie due oggetti isomorfi sono a tutti gli effetti indistinguibili, fornendo quindi un livello di astrazione (rispetto a dettagli "implementatitivi") non ottenibile con la uguaglianza insiemistica.

Definition 4.6 *Un oggetto $I \in \mathcal{C}$ e' detto* **iniziale** $\stackrel{\Delta}{\iff} \forall A \in \mathcal{C}.\exists! f: I \to A$ *(dove $\exists!$ vuoel dire esiste ed e' unico).*

La proprieta' di inizialita' e' un esempio particolarmente semplice di *proprieta' universale*, cioe' una proprieta' che identifica un oggetto (con struttura associata) in modo univoco a meno di isomorfismi.

Proposition 4.7 *Se I e I' sone entrambi iniziali allora l'unico $f: I \to I'$ e' un isomorfismo (con inversa data da l'unico $f': I' \to I$). Se $I \cong I'$ e I e' iniziale, allora anche I' e' iniziale.*

La nozione duale di oggetto iniziale e' quella di oggetto terminale, cioe' T e' terminale $\stackrel{\Delta}{\iff} \forall A \in \mathcal{C}.\exists! f: A \to T$.

Example 4.8 Vediamo esempi di oggetti iniziali e terminali in varie categorie:

- in **Set** l'unico oggetto iniziale e' l'insieme vuoto, mentre gli oggetti terminali sono quelli che hanno esattamente un elemento.
- In **Rel** l'unico oggetto iniziale (che e' anche l'unico oggetto terminale) e' l'insieme vuoto. Questo fa' vedere che i morfismi giocano un ruolo fondamentale (in teoria delle categorie), anche perche' senza precisare quali sono i morfismi non si puo' definire quando due oggetti sono isomorfi.
- In **X** l'oggetto iniziale e' un elemento minimo di $(X, \leq)$ (in un preordine vi possono essere piu' elementi minimi, tutti equivalenti tra loro), mentre l'oggetto iniziale e' un elemento massimo.
- In $\mathbf{T}_\Sigma(X)$ l'unico oggetto iniziale e' l'insieme vuoto, mentre in generale non esistono oggetti terminali.
- In $\mathbf{Alg}_\Sigma$ un esempio di oggetto iniziale e' la Σ-algebra T_Σ dei termini chiusi, mentre gli oggetti terminali sono le Σ-algebre dove ogni sort ha esattamento un elemento ed i predicati atomici sono sempre veri.
- In $\mathbf{Alg}^s_\Sigma$ non esistono ne' oggetti iniziali ne' terminali.

4.2 Categorie di algebre

In questa sezione focalizzeremo l'attenzione su sotto-categorie $\mathcal{C}$ di $\mathbf{Alg}_\Sigma$ con le seguenti proprieta':

- chiusura per isomorfismo, cioe' se $A \in \mathcal{C}$ e $A \cong B$ in $\mathbf{Alg}_\Sigma$ allora $B \in \mathcal{C}$
- pienezza, cioe' $\mathcal{C}(A, B) = \mathbf{Alg}_\Sigma(A, B)$ per ogni $A, B \in \mathcal{C}$

Si osservi che la sotto-categoria $\mathbf{Alg}^s_\Sigma$ e' chiusa per isomorfismo (banalmente, poiche' ha gli stessi oggetti di $\mathbf{Alg}_\Sigma$), ma non e' piena.
Le categorie di questa forma includono tutte le categorie indotte dalle classi $Mod(SP)$ dei modelli di una specifica SP. Infatti, e' ragionevole aspettarsi che qualunque formalismo di specifica non sia in grado di distinguere tra Σ-algebre isomorfe (questo e' certamente vero per le specifiche del primo ordine, ma vale anche per la *logica del secondo ordine*).

Proposition 4.9 *La Σ-algebra T_Σ (vedi [AR96, Def. 1.12]) e' un oggetto iniziale in $\mathbf{Alg}_\Sigma$.*

Diamo adesso delle definizioni categoriali che in $\mathbf{Alg}_\Sigma$ risultano equivalenti a nozioni definite in modo piu' concreto in [AR96] (e quindi non direttamente applicabili ad altre categorie).

Proposition 4.10 (sotto-algebra) *Una sotto-algebra B di A (vedi [AR96, Def. 1.20]) corrisponde ad un Σ-omomorfismo forte e mono $m: B \to A$. Piu' precisamente, l'immagine di m e' una sotto-algebra, ogni sotto-algebra la si ottiene in questo modo prendendo come $m: B \to A$ l'inclusione.*

In effetti, la nozione categoriale di **strong mono** puo' essere data in modo del tutto generale: $m: A \to B$ e' uno **strong mono** $\stackrel{\Delta}{\iff}$ m e' un mono t.c. $(\forall f, g, e.(m \circ f = g \circ e) \wedge$ e epi $) \implies \exists h.(f = h \circ e) \wedge (g = m \circ h)$.

Proposition 4.11 (algebra term-generated) *Le seguenti definizioni sono equilaventi*

- *A e' term-generated (vedi [AR96, Def. 1.24]), cioe' ogni elemento di A e' l'interpretazione di un termine chiuso*
- *l'unica sotto-algebra di A e' A stessa (vedi [AR96, Prop 1.25])*
- *l'unico morfismo $T_\Sigma \to A$ dall'algebra iniziale ad A e' epi (vedi [AR96, Prop 1.25]).*

La terza caratterizzazione e' particolarmente semplice, e permette di dedurre immediatamente che la sotto-categoria piena $\mathbf{Gen}_\Sigma$ delle algebre term-generated e' chiusa per isomorfismo (e soddisfa le altra proprieta' enunciate in [AR96, Prop. 1.27]).

Definition 4.12 *Fissata una qualsiasi sotto-categoria piena $\mathcal{C}$ di $\mathbf{Alg}_\Sigma$ chiusa per isomorfismi, esiste unica (a meno di isomorfismi) $I_C \in \mathbf{Gen}_\Sigma$ t.c. $I_C \models F \iff \mathcal{C} \models F$ per ogni formula atomica ground $F \in A_\Sigma$.*

Theorem 4.13 *Data una qualunque sotto-categoria piena $\mathcal{C}$ di $\mathbf{Alg}_\Sigma$ chiusa per isomorfismi, $I_C \in \mathcal{C}$ sse $\mathcal{C}$ ha un oggetto iniziale I che appartiene a $\mathbf{Gen}_\Sigma$.*

Usando la (soundness e) conpleteness del sistema di Birkhoff ristretto alle formule atomiche (vedi [AR96, Def. 2.44]) si dimostra facilmente che la categoria $\mathbf{Mod}(SP)$ di una specifica condizionale, ha un modello iniziale term-generated (sotto delle ipotesi aggiuntive che garantiscono la soundness, cioe' l'assenza di carrier vuoti), vedi [AR96, Thm 2.46] per dettagli.

5 Sistemi di riscrittura

Nonostante le ottime proprieta' delle specifiche condizionali, quali l'esistenza di un modello minimo (che in programmazione logica va' sotto il nome di modello di Herbrand), stabilire se una formula (atomica) e' derivabile dagli assiomi e' in generale non decidibile. Vi sono ulteriori restrizione che si possono imporre su una specifica, per garantire la decidibilita' (o comunque ridurre il grado di non-determinismo nella ricerca automatica di una dimostrazione). Da questo punto di vista i sistemi di riscrittura vanno considerati come uno strumento tecnico per studiare teorie equazionali.

Per semplicita' ci limiteremo a considerare teorie single-sorted (con una sola sort), ma i risultati si estendeno in modo ovvio al caso many-sorted (vedi [AstTR]).

Definition 5.1 *Dato un insieme $E \subseteq T_\Sigma(X) \times T_\Sigma(X)$ di coppie (usabili) di Σ-termini aperti definiamo la* **relazione di riscrittura** $\xrightarrow[E]{} \subseteq T_\Sigma(X) \times T_\Sigma(X)$ *induttivamente, tramite le seguenti regole*

$$E\ \frac{}{\sigma(t) \xrightarrow[E]{} \sigma(t')}\ (t,t') \in E \text{ e } \sigma: X \longrightarrow T_\Sigma(X) \qquad op\ \frac{t \xrightarrow[E]{} t'}{op(\bar{t}_1, t, \bar{t}_2) \xrightarrow[E]{} op(\bar{t}_1, t', \bar{t}_2)}\ op \in \Sigma_n \text{ e } |\bar{t}_1| + 1 + |\bar{t}_2| = n$$

Quando E e' chiaro dal contesto, scriveremo $\longrightarrow$ invece di $\xrightarrow[E]{}$.

Una definizione piu' concisa di $\xrightarrow[E]{}$, che pero' richiede di introdurre i contesti con un solo buco, e' data in [AstTR]:

> $t_1 \xrightarrow[E]{} t_2 \overset{\Delta}{\iff} t_1 \equiv C[\sigma(t)]$ e $t_1 \equiv C[\sigma(t')]$ per qualche $(t,t') \in E$, contesto $C[\_]$ con un solo buco e sostituzione $\sigma: X \to T_\Sigma(X)$.

Definition 5.2 *Definiamo le seguenti relazioni derivate da $\xrightarrow[E]{}$:*

- $\xleftrightarrow[E]{}$ *e' la chiusura simmetrica di $\xrightarrow[E]{}$, cioe' $t \xleftrightarrow[E]{} t'$ sse $t \xrightarrow[E]{} t'$ oppure $t' \xrightarrow[E]{} t$*
- $\xrightarrow[E]{+}$ *e' la chiusura transitiva di $\xrightarrow[E]{}$*
- $\xrightarrow[E]{*}$ *e' la chiusura riflessiva e transitiva di $\xrightarrow[E]{}$*
- $t_1 \downarrow_E^* t_2 \overset{\Delta}{\iff}$ *esiste t t.c. $t_1 \xrightarrow[E]{*} t$ e $t_2 \xrightarrow[E]{*} t$.*

Analogamente si definiscono le relazioni $\xleftrightarrow[E]{+}$ e $\xleftrightarrow[E]{*}$.

Diciamo che t e' in **forma normale** $\overset{\Delta}{\iff}$ *non esiste t' t.c. $t \xrightarrow[E]{} t'$. Diciamo che t' e' una forma normale di t $\overset{\Delta}{\iff}$ $t \xrightarrow[E]{*} t'$ e t' e' in forma normale.*

Proposition 5.3 *$t_1 \xleftrightarrow[E]{*} t_2$ sse $t_1 = t_2$ e' derivabile dall'insieme di assiomi equazionali E.*

Proof Si usi la completezza (e sensatezza) relativa alle formule atomiche del sistema di Birkhoff per dare una definizione induttiva delle equazioni derivabili. Quindi si dimostra (per induzione sulla derivazione) che i due sistemi induttivi: quello di Birkhoff e quello che definisce $\xleftrightarrow[E]{*}$ generano la stessa relazione. ∎

Definition 5.4 *Diciamo che una relazione di riscrittura* $\xrightarrow[E]{}$ *e'*

- **confluente** *(Church-Rosser)* $\stackrel{\Delta}{\iff} \forall t, t_1, t_2.(t \xrightarrow[E]{*} t_1 \wedge t \xrightarrow[E]{*} t_2) \Longrightarrow \exists t_3.t_1 \xrightarrow[E]{*} t_3 \wedge t_2 \xrightarrow[E]{*} t_3$
- **debolmente confluente** *(weak Church-Rosser)* $\stackrel{\Delta}{\iff} \forall t, t_1, t_2.(t \xrightarrow[E]{} t_1 \wedge t \xrightarrow[E]{} t_2) \Longrightarrow \exists t_3.t_1 \xrightarrow[E]{*} t_3 \wedge t_2 \xrightarrow[E]{*} t_3$
- **terminante** *(Strongly Normalizing)* $\stackrel{\Delta}{\iff}$ *non esiste una sequenza infinita di termini* t_n *t.c.* $\forall n.t_n \xrightarrow[E]{} t_{n+1}$
- **debolmente terminante** *(Weakly Normalizing)* $\stackrel{\Delta}{\iff}$ *ogni termine* t *ha una forma normale* t'.

Proposition 5.5 *Se* $\xrightarrow[E]{}$ *e' confluente, allora un termine* t *ha al piu' una forma normale, che indicheremo con* $nf(t)$.

Theorem 5.6 *Se* $\xrightarrow[E]{}$ *e' confluente, allora* $t_1 \xleftrightarrow[E]{*} t_2$ *sse* $t_1 \downarrow_E^* t_2$.

Theorem 5.7 *Se* $\xrightarrow[E]{}$ *e' confluente e debolmente terminante, allora* $t_1 \xleftrightarrow[E]{*} t_2$ *sse* $nf(t_1) \equiv nf(t_2)$.

Il precedente teorema ci permette di dare una costruzione alternativa del modello iniziale, detto modello N delle forme normali. Gli elementi sono i termini ground (cioe' senza variabili libere) in forma normale. In questo caso e' importante supporre che E consista di coppie usabili, poiche' cio' garantisce che se t e' ground e $t \xrightarrow[E]{} t'$, allora anche t' e' ground. L'interpretazione delle operazioni in N e' dato da $op^N(t_i|i \in m) \stackrel{\Delta}{=} nf(op(t_i|i \in m))$. Un'altra consequenza importante e' che la teoria equazionale e' decidibile.

Corollary 5.8 *Se* E *e' un sottoinsieme decidibile di* $T_\Sigma(X) \times T_\Sigma(X)$, *ed inoltre* $\xrightarrow[E]{}$ *e' confluente e debolmente terminante, allora anche* $\xleftrightarrow[E]{*}$ *e' un sottoinsieme decidibile.*

Proof Per il teorema precedente e' sufficiente dimostrare che la funzione totale nf sui termini e' calcolabile. Dato un termine t per trovare $nf(t)$ si genera in modo incrementale l'albero (infinito) dei termini in cui t e' riscrivibile in un numero finito di passi, e ci si ferma appena si e' trovato un termine in forma normale. ∎

Remark 5.9 In generale, se E e' decidibile l'unica cosa che si puo' dedurre e' che $\xleftrightarrow[E]{*}$ e' semi-decidibile.

Dai precedenti risultati si e' visto che e' importante sapere se una relazione di riscrittura e' confluente e/o terminante. Diamo adesso alcuni risultati che ci permettono di stabilire tali proprieta' a partire da proprieta' *piu' semplici.*

Definition 5.10 (coppia critica) *Dato un insieme di equazioni* E, *si dice che* (t, t') *e' una coppia critica per* E *sse*

- *esistono due regole di riscrittura distinte di* E, $t_1 \to t_1'$ *e* $t_2 \to t_2'$ *(che supporremo non avere variabili a comune), un termine* $\underline{t}$ *che non e' una variabile, un contesto con un solo buco* $C[\_]$ *ed una sostituzione* σ *t.c.* $t_1 \equiv C[\underline{t}]$, $\sigma = mgu(\underline{t}, t_2)$, $t \equiv \sigma(C[t_2'])$ *e* $t' \equiv \sigma(t_1')$
- *oppure esiste una regola di riscrittura* $t_1 \to t_1'$ *di* E, *una sua ridenominazione* $t_2 \to t_2'$ *con variabili non usate, t.c. valga quanto detto sopra ed in piu'* $C[\_] \not\equiv \_$.

Quindi t *e* t' *sono due* modi diversi *di riscrivere* $\sigma(t_1) \equiv \sigma(C[t_2])$.

Theorem 5.11 (Newman) *Se* $\xrightarrow[E]{}$ *e' terminante e debolmente confluente, allora e' confluente.*

Theorem 5.12 (Knuth-Bendix) *Se ogni coppia critica* (t_1, t_2) *per* E *e' confluente (cioe'* $t_1 \downarrow_E^* t_2$*), allora* $\xrightarrow[E]{}$ *e' debolmente confluente.*

In genere non e' banale dimostrare che una relazione di riscrittura e' terminante. Il seguente risultato ci permette di dimostrare la confluenza a prescindere dalla terminazione.

Definition 5.13 (sistema ortogonale) *Si dice che E e' ortogonale sse non ha coppie critiche ed e' left-linear, cioe' vi e' al piu' una occorrenza di x in t, se $(t \to t') \in E$ e x e' una variabile.*

Theorem 5.14 *Se E e' ortogonale, allora $\xrightarrow[E]{}$ e' confluente.*

Proof La dimostrazione usa una relazione ausiliaria $\xrightarrow[E]{p}$, detta parallel one-step reduction, per cui e' facile dimostrare la proprieta' diamante (da cui discende banalmente la confluenza)

$$\text{refl}\ \frac{}{t \xrightarrow[E]{p} t} \qquad E\ \frac{\{t_x \xrightarrow[E]{p} t'_x | x \in \mathrm{FV}(t)\}}{t[x := t_x|x] \xrightarrow[E]{p} t'[x := t'_x|x]}\ (t,t') \in E \qquad op\ \frac{\{t_i \xrightarrow[E]{p} t'_i | i \in m\}}{op(\overline{t}) \xrightarrow[E]{p} op(\overline{t}')}\ op \in \Sigma_n \text{ e } |\overline{t}| = |\overline{t}'| = m$$

$\xrightarrow[E]{p}$ soddisfa le seguenti proprieta':

- subst $\dfrac{t_1 \xrightarrow[E]{p} t'_1 \qquad t_2 \xrightarrow[E]{p} t'_2}{t_1[x := t_2] \xrightarrow[E]{p} t'_1[x := t'_2]}$
- $\xrightarrow[E]{} \subset \xrightarrow[R]{p} \subset \xrightarrow[E]{*} = \xrightarrow[E]{p*}$

Se E e' ortogonale, allora $\xrightarrow[E]{p}$ soddisfa la proprieta' diamante (che si ottiene dalla def. di confluenza sostituendo $\xrightarrow[E]{p}$ a $\xrightarrow[E]{*}$), ed anche la proprieta' $\forall t.\exists t''.\forall t'.t \xrightarrow[E]{p} t' \Longrightarrow t' \xrightarrow[E]{p} t''$ (che implica la proprieta' diamante). ∎

5.1 Tecniche per dimostrare la terminazione

Sia E un insieme di coppie usabili (equazioni) sulla segnatura Σ, indichiamo con T_Σ l'insieme dei Σ-termini (non ci interessa specificare se sono chiusi o possono avere variabili libere). Si osservi che la terminazione di $\xrightarrow[E]{}$ equivale a dire che la relazione su T_Σ data da $t_1 < t_2 \overset{\Delta}{\Longleftrightarrow} t_2 \xrightarrow[E]{} t_1$ e' ben-fondata.

Proposition 5.15 *Se esiste una $f: T_\Sigma \to N$ t.c. $t_2 \xrightarrow[E]{} t_1 \Longrightarrow f(t_2) > f(t_1)$, allora $\xrightarrow[E]{}$ e' terminante.*

Infatti una sequenza di riscritture che inizia con t potra' avere al piu' lunghezza $f(t)$. Nella proposizione si puo' rimpiazzare $(N, <)$ con una qualsiasi relazione ben-fondata $(W, <)$. Sotto certe ipotesi aggiuntive sulla funzione f possiamo limitarci a considerare solo istanze di coppie usabili.

Corollary 5.16 *Se esiste una $f: T_\Sigma \to N$ t.c. $f(t_2) > f(t_1) \Longrightarrow f(C[t_2]) > f(C[t_1])$ e $(t_2, t_1) \in E \Longrightarrow f(v(t_2)) > f(v(t_1))$, allora $\xrightarrow[E]{}$ e' terminante.*

Quando $f: T_\Sigma \to N$ e' definita per induzione sulla struttura dei termini, cioe' $f(op(t_i | i \in m)) = f_{op}(f(t_i) | i \in m)$ dove $f_{op}: N^m \to N$, allora la proprieta' $f(t_2) > f(t_1) \Longrightarrow f(C[t_2]) > f(C[t_1])$ vale sse e solo se ogni f_{op} e' strettamente monotona in ciascuno dei suoi argomenti.