<u>*Sistemi di riscrittura*</u>

- Preliminare all'utilizzo di linguaggi algebrici come linguaggi di programmazione.
- Di interesse assoluto in varie aree.
  - Implementazione di prototipi nella fase di specifica
  - (una specifica può essere implementata dando origine a un prototipo su cui studiare il comportamento del sistema specificato)
  - tecniche di intelligenza artificiale come parti di sistemi di deduzione automatica
- di interesse culturale
  - "calcolo delle espressioni" cos'è ?
  - cosa sono i numeri come entità manipolabili
    in che senso, data una specifica algebrica degli interi con 0, pred e succ, si può dire che i numeri hanno la forma 0, $pred^n(0)$, $succ^n(0)$?

N. B. pred succ 0 non c'è più !!
si vuole ottenere :
- uno e uno solo rappresentante per classe di congruenza
- rappresentante "canonico" nel senso che sia il più semplice possibile da un certo punto di vista
- da un termine deve essere ottenibile (calcolabile) il rappresentante canonico della sua classe in modo effettivo

Soluzione: si cercano, data una specifica, dei <u>sistemi di riscrittura</u> tali che * può essere riscritto via via nel suo rappresentante canonico (se esiste).

<u>Relazione con OBJ 3</u>

in obj 3
- un programma è un termine
- il risultato (valore del programma) è il rappresentante canonico per il termine
  (eventualmente modulo certe equivalenze elementari)

relazione estendibile a un qualunque prototipo si specifiche algebriche.

<u>Term rewriting</u>

(sistemi di riscrittura dei termini)

Σ: segnatura (senza predicati ⇒specifiche equazionali)

- una <u>coppia</u> $(t,t') \in T_\Sigma(X)_S \times T_\Sigma(X)_S$ con X S−famiglia di variabili è <u>usabile</u> (ovvero è una regola di riduzione) se $Var(t') \subseteq Var(t)$

  Nota: poichè spesso si parte da coppia (t,t') vista come eguagliare

$t = t'$ si dice anche che (t, t') è un'eguaglianza usabile; però occhio al fatto che la coppia è ordinata, quindi con parte sinistra e destra. Si usa perciò anche assegnare le regole di riduzione $t \to t'$.

- Una riscrittura (generata da (t, t') è una coppia $(\alpha(t), \alpha(t'))$ dove α è una sostituzione , cioè α è l'omomorfismo $T_\Sigma(X) \to T_\Sigma(X)$ generato da una valutazione in $T_\Sigma(X)$ delle variabili in t e t'.
- un passo di riscrittura è una coppia di termini della forma $(C[\alpha(t)], C[\alpha(t')])$ dove $C[\,]$ è un contesto ad un solo buco e $(\alpha(t), \alpha(t'))$ è una riscrittura.

Dato E insieme di coppie (o eguaglianze orientate) si definisce la relazione di riscrittura a un passo $\to_E$ ponendo $t_1 \to_E t_2$ sse (t_1, t_2) è un passo di riscrittura per E, cioè se $\exists\, C[\,], (t, t') \in E, \alpha$ sostituzione t.c. $t_1 = C[\alpha(t)]$ $t_2 = C[\alpha(t')]$.

Indichiamo con $\to_E^+$, $\to_E^*$ rispettivamente la chiusura transitiva, transitiva e riflessiva di $\to_E$ con $\longleftrightarrow_E$ la chiusura per simmetria, con $\longleftrightarrow_E^*$ la chiusura per equivalenza.

Formulazioni diverse di un sistema di riscrittura
es. Scoprire coincidenze e differenze

- $\to_{IE}$ definita induttivamente da

$$\frac{}{\alpha(t) \to_{IE} \alpha(t')} (t, t') \in E \quad \text{con } \alpha \text{ sostituzione}$$

$$\frac{t \to_{IE} t'}{C[t] \to_{IE} C[t']} C[\,] \text{ contesto per } t \text{ e } t'$$

- $\to_{2E}$

$$\frac{}{t \to_{2E} t'} (t, t') \in E$$

$$\frac{t \to_{2E} t'}{\alpha(t) \to_{2E} \alpha(t')} \quad \alpha \text{ sostituzione}$$

$$\frac{t \rightarrow_{2E} t'}{\sigma(t_{1,} ..., t, ..., t_n) \rightarrow_{2E} \sigma(t_{1,} ..., t', ..., t_n)} \sigma \in$$

- $\rightarrow_{3E}$ come in $\rightarrow_{2E}$, ma con la terza regola sostituita dalla chiusura per contesti come in $\rightarrow_{1E}$.

Nozione di forma normale

("il più semplice rappresentante")

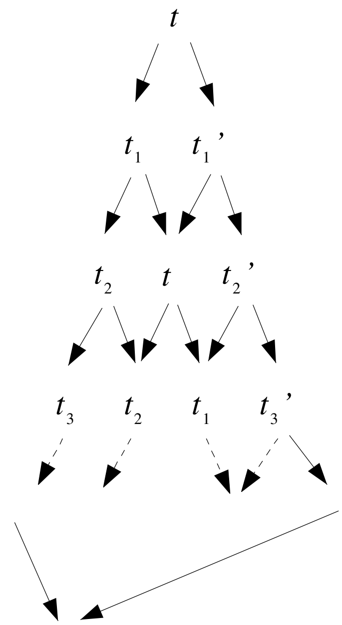
Definizione

- t è in <u>forma normale</u> (rispetto a E) sse $\neg \ \exists\, t'$ t. c. $t \rightarrow_E t'$
- t ha <u>forma normale</u> sse $t \rightarrow_E^* t'$ e t' è in forma normale
- $\rightarrow_E$ (o anche E) è <u>*terminante*</u> sse $\neg \ \exists \{t_i\}_{i \in \mathbb{N}}$ t. c. $t_i \rightarrow_E t_{i+1}$
- $\rightarrow_E$ (o anche E) è <u>*confluente*</u> (o Church – Rosser) sse $t \rightarrow_E^* t_1, t \rightarrow_E^* t_2 \Rightarrow \exists\, t'$ tale che $t_1 \rightarrow_E^* t', t_2 \rightarrow_E^* t'$.

Graficamente

$$\begin{tikzcd}
 & t \arrow[dl, "*"'] \arrow[dr, "*"] & \\
t_1 \arrow[dr, "*"'] & & t_2 \arrow[dl, "*"] \\
 & t' &
\end{tikzcd}$$

<u>Commenti</u>
La confluenza (CR) produce l'effetto **diamante** (diamond filling)



Teorema (fondamentale) della forma normale

<u>Teorema FN</u>
Sia E (usabile) confluente e terminante su Σ. Allora

1. ogni $t \in T_\Sigma(X)$ ha una e una sola forma normale (indicata con $nf(t)$):
2. le famiglie $N = \{N_s\}_{s\in S}$ definita da $N_s =$ insieme delle forme normali degli elementi di $(T_\Sigma(X))_S$ con le operazioni σ^N definite da $\sigma^N(nf_{1,} ..., nf_n) = nf(\sigma(nf_{1,} ..., nf_n))$ è una $\Sigma -$algebra (detta algebra delle forme normali).
3. $N \simeq T_\Sigma/_{\equiv E}$ $\quad (\simeq T_\Sigma/_{\equiv Mod(\Sigma,E)})$

Corollario
(nelle ipotesi precedenti)

1. per $X = \emptyset$ N è iniziale in $Mod(\Sigma, E)$
2. se Σ e E sono finiti (basta che la riscrittura sie effettiva), allora il problema della parola $t \equiv_E t'$ per $t, t' \in T_\Sigma$ è decidibile.

Illustriamo ora alcune proprietà importanti della riscrittura che, oltre a far comprendere meglio la tecnica e il suo significato, permettono di provare facilmente il teorema FN delle forme normali.
Innanzitutto chiariamo il collegamento fra riscrittura e sistema deduttivo di Birkhoff.

Teorema A

$E \mid -^{B} t = t'$ sse $t \longleftrightarrow_{E}^{*} t'$ (cioè $\equiv_{E} \;\; = \longleftrightarrow_{E}^{*}$)

$\mid -^{B}$ nel caso si specifiche equazionali E e' un insieme di equazioni $t = t$ con $t, t' \in T_{\Sigma}(X)$

B1 $\dfrac{}{t = t}$ B2 $\dfrac{t = t'}{t' = t}$ B3 $\dfrac{t = t', \quad t' = t''}{t = t''}$ equivalenza

B4 $\dfrac{t_i = t'_i, \quad i = 1, \dots, n}{op(t_{1,} \dots, t_n) = op(t'_{1,} \dots t'_n)}$ congruenza

B5 $\dfrac{}{\alpha(t)' = \alpha(t')}$ con $t = t' \in E$ e α sostituzion

$E \mid -^{B}$

Definizione

$t \overset{*}{\downarrow} t'$ sse $\exists \bar{t}$ t.c. $t \overset{*}{\rightarrow} \bar{t}$ e $t' \overset{*}{\rightarrow} \bar{t}$

Lemma B

i. $t \overset{*}{\downarrow} t' \Rightarrow t \longleftrightarrow_{E}^{*} t'$

ii. $t \overset{+}{\overset{*}{\downarrow}} t' \Leftrightarrow t \longleftrightarrow_{E}^{*} t'$ ($t \overset{+}{\overset{*}{\downarrow}} t'$ sse $\exists t_{1,} \dots, t_n$ t.c. $t_i \overset{*}{\downarrow} t_{i+1}$ con $t_1 = t$ e $t_n = t'$)

Prove:

- /* schema a zig–zag sugli appunti */

Lemma C

Se E è confluente allora $t \overset{*}{\downarrow} t' \Leftrightarrow t \longleftrightarrow^{*} t'$

Lemma D

i. E terminante $\Rightarrow$ t ha forma normale per ogni t

ii. E confluente $\Rightarrow$ se t ha forma normale , è unica per ogni t

iii. E terminante e confluente $\Rightarrow$ t ha una e una sola forma normale per ogni t

Prova

i. per assurdo, se esistesse t senza forma normale, allora $t \to t_1 \to \ldots \to t_n \to t_{n+1} \to \ldots$ cioè esiste una catena di riscrittura infinita, contro l'ipotesi.

ii. Supponiamo che $t \to^* t_1$, $t \to^* t_2$ con t_1 e t_2 in forma normale, cioè ?????? per l'ipotesi di confluenza, $\exists\, \bar{t}$ t. c. $t_1 \to^* \bar{t}$, $t_2 \to^* \bar{t}$, ma essendo t_1, t_2 in forma nomale deve essere $t_1 = \bar{t} = t_2$.

iii. Immediata da i) e ii).

Lemma E

Sia E confluente, inoltre t_1 e t_2 abbiano forma normale $nf(t_1), nf(t_2)$.

Allora $t_1 \longleftrightarrow_E^* t_2$ sse $nf(t_1) = nf(t_2)$.

Prova

$\Leftarrow$ si ha

$$t_1 \xrightarrow{*} nf(t_1) = nf(t_2) \xleftarrow{*} t_2$$

da cui $t_1 \longleftrightarrow_E^* t_2$ (per chiusura transitiva)

$\Rightarrow$ per il lemma C $\quad t_1 \overset{*}{\downarrow} t_2$, quindi $\quad \exists\, \bar{t}$ t. c.

$$
\begin{tikzcd}
 & t_1 \arrow[dl, "*"'] \arrow[dr, "*"] & & t_2 \arrow[dl, "*"'] \arrow[dr, "*"] & \\
nf(t_1) \arrow[drr, dashed] & & \bar{t} \arrow[ll, dashed, "*"'] \arrow[rr, dashed, "*"] & & nf(t_2) \arrow[dll, dashed] \\
 & & t' & &
\end{tikzcd}
$$

Teorema F
Se E è confluente, sono fatti equivalenti:

1. $t \overset{*}{\longleftrightarrow}_E t'$
2. $t \equiv_E t'$
3. $t \overset{*}{\downarrow} t'$
4. $t \equiv_{Mod(\Sigma,E)} t'$

inoltre, se t e t' hanno forma normale, allora $\quad nf(t_1) \equiv nf(t_2)$

Conseguenza del teorema della forma normale
Sia E terminante, confluente, finito: allora $\equiv_E$ su T_Σ è decidibile. Si dice che il problema della parola è decidibile.

Prova: per ogni termine si può ottenere effettivamente la sua forma normale. Infatti, per l'unicità, basta riscrivere un termine fino a ottenere la sua unica forma normale. Perciò tutto si riduce a poter esibire algoritmicamente i termini t' in cui t si può riscrivere. Essendo finito E e l'insieme dei sottotermini di t esiste un algoritmo per ottenere i t' in cui t si riscrive. Allora presi t_1 e t_2 per decidere se $t_1 \equiv_E t_2$, per il teorema della forma normale, basta verificare Se $nf(t_1) \equiv nf(t_2)$.

Osservazione: in generale i problemi legati alla riscrittura sono indecidibili.
<u>*Es:*</u>

$t \equiv_E t'$

t ha forma normale
t ha una riscrittura infinita

<u>*Spiegazione (dimostrazione)*</u>
consideriamo E costituito da

- Σ omogenea
- S, K operatori zerari
- (_ _) operazione binaria (applicazione o combinazione)
- $\left(\left(KX\right)Y\right)\to X$
- $\left(\left(\left(SX\right)Y\right)Z\right)\to\left(\left(XZ\right)\left(YZ\right)\right)$

1. E risulta confluente,ma non terminante.
2. Vedendo E come eguaglianze, si ha una specifica con modello iniziale (e libera per ogni insieme di variabili X).
3. Posso interpretare E come definente un linguaggio con semantica, quella di inizialità con questa semantica questo sistema viene detto <u>calcolo combinatorio di Curry</u> (N. B. solo due simboli S e K, nessuna variabile nel linguaggio!!!).
4. Questo linguaggio è <u>universale</u>, cioè equivalente alle macchine di Turing e dunque al Pascal.
5. Alcuni problemi dell'esempio si riconducono all'indecidibilità dei problemi relativi alle macchien di Turing.

Importanza fondamentale della canonicità.

Problema: garantire / conoscere la canonicità.

Supponiamo E, Σ finiti

terminazione:

indecidibile (oppure semidecidibile, anche con card(E) = 2)
decidibile se E è ground (senza variabili)

confluenza:

indecidibile
decidibile se E è ground

Decidibilità della confluenza

Nozione di confluenza locale

E equazioni usabili. Il sistema è localmente confluente sse $\forall t, t', t''$ tali che

$$\begin{tikzcd}[column sep=small] & t \arrow[dl] \arrow[dr] & \\ t' & & t'' \end{tikzcd}$$

$\exists\, t'''$ tale che

$$\begin{tikzcd}[column sep=small] t' \arrow[dr, "*"'] & & t'' \arrow[dl, "*"] \\ & t''' & \end{tikzcd}$$

<u>Teorema di Newman</u>. Se E è terminante allora E è confluente sse è localmente confluente.

Nozione di unificatore minimo

- dato un insieme E di equazioni e due termini t, t' una sostituzione σ si dice E–unificatore di t e t' (σ E–unifica t e t') se $\sigma(t) \equiv_E \sigma(t')$. Nel caso $E = \emptyset$ si dice semplicemente <u>unificatore</u>. Si osservi che E–unificare t e t' equivale a trovare una ?soluzione? Di t = t' modulo $\equiv_E$. In particolare, per $E = \emptyset$, unificare t e t' equivale a trovare una soluzione di t = t' in $T_\Sigma(X)$ (cioè come pura eguaglianza di termini).
- Date due sostituzioni σ e σ' , si pone $\sigma < \sigma'$ sse esiste una sostituzione σ'' t. c. $\sigma' = \sigma'' \circ \sigma$. In sostanza $\sigma < \sigma'$ sse σ' è una sostituzione non meno semplice di σ .
- In generale, fissati t e t', l'insieme degli unificatori può essere vuoto e inoltre ci possono essere più unificatori minimali. Però per $E = \emptyset$, se t e t' sono unificabili, allora esiste l'unificatore minimo, detto anche unificatore più generale e indicato con mgu(t, t'). sempre per $E = \emptyset$, esistono algoritmi ?????? per la ricerca dell'mgu; il più celebre è quello di Martelli–Montanari [82].

Nozione di coppia critica

Siano $t_1 \to t_2$ e $t'_1 \to t'_2$ due regole di E con t_1 e t'_1 senza variabili comuni. Sia E

un sottotermine di t_1 della stessa sort di t'_1 e σ unificatore minimo di $\bar{t}$ e t'_1 .
Allora $\left\langle \sigma\left(t_1\left[t'_2/\bar{t}\right], \sigma\left(t_2\right)\right)\right\rangle$ si dice coppia critica per E.

Teorema di Kluth−Bendix (generalizzato da Huet)
E è localmente confluente sse ogni coppia critica confluisce (converge).

Corollario / teorema
Se E è terminante , con Σ , E finito, allora la confluenza è decidibile.
Prova: per Kluth−Bendix la confluenza locale è decidibile, in quanto le coppie critiche sono in numero finito e la loro confluenza, in ipotesi di terminazione, si riduce al confronto delle forme normali. Per il teorema di Newman, allora è decidibile la confluenza.

Terminazione per ordinamento
Un ordinamento parziale > in $T_\Sigma(X)$ è un ordinamento di riduzione (reduction ordering) sse

- $t > t' \Rightarrow \sigma(t) > \sigma(t')$
- $t_i > t'_i \Rightarrow op(t_{1,} ..., t_n) > op(t'_{1,} ..., t'_n) \qquad \forall\, op \in \Sigma$
- > è terminante

Teorema
Sia E usabile. Allora E è terminante sse $\exists >$ ordine di riduzione tale che $\rightarrow_E \subseteq >$.

Metodi di prova della terminazione spesso si riducono a definire un ordinamento di riduzione.

Conclusione
1. Occorre ricondursi a sistemi terminanti e confluenti. Questi sistemi sono detti completi o canonici.
2. Un sistema E può non essere completo e tuttavia essere equivalente ad un sistema completo è.
3. $\exists$ un algoritmo (piuttosto furbo) di Knuth−Bendix (78) che tenta di completare un sistema E, producendo un sistema è equivalente ad E, però può :
   - terminare con un insuccesso (anche se esiste è)
   - non terminare (però con ciclo controllabile).

Questo algoritmo (che usa il teorema di Kluth Bendix e testa la terminazione) è implementato in certe ?????? avanzate di implementazione di sistemi di riscrittura.