Lezione 17 MSC
Assiomatizzazioni

Roberto Gorrieri

Ragionamento equazionale

- Definizione di teorie equazionali (dette assiomatizzazioni) che caratterizzano le congruenze.
- Fino ad ora, due sistemi potevano essere dimostrati congruenti attraverso una opportuna ispezione del loro spazio degli stati (equivalence-checking)
- Ma ora, dato che i due LTS sono in realtà termini di un linguaggio, la loro congruenza può essere dimostrata sintatticamente, mostrando che il primo termine può essere eguagliato al secondo per mezzo di una dimostrazione di deduzione equazionale.

Ragionamento equazionale (2)

- Una assiomatizzazione E che caratterizza una congruenza comportamentale R offre una tecnica di prova alternativa, puramente sintattica, per dimostrare che due processi sono congruenti secondo R
- Allora, E può esistere solo per i sottocalcoli di CCS per cui R è decidibile.
- Per semplicità, ci limitiamo a considerare solo CCS finito, ma assiomatizzazioni esistono anche per finite-state CCS e per regular CCS.

Sintassi “Open” di CCS Finito

- Ci limitiamo a considerare Finite CCS, ovvero CCS dove le costanti non possono essere usate, con questa sintassi per termini aperti:

  $P ::= 0 \mid x \mid \mu.P \mid P+P \mid P|P \mid (\nu a)P$

- Sintassi più generale (ammetto scelta non guardata), ma considera un insieme finito di azioni Act.
- Termini aperti (con occorrenze di variabili) e termini chiusi (processi “veri”)

Teoria equazionale /Assiomatizzazione

- Una teoria equazionale (o assiomatizzazione) per CCS Finito è data da un insieme E di equazioni del tipo $t_1 = t_2$, dove t_1 e t_2 sono termini possibilmente aperti di CCS Finito.
- A partire dalle equazioni in E è possibile derivare delle uguaglianze tra termini di CCS Finito, usando un insieme di assiomi e di regole d'inferenza (deduzione equazionale)

Deduzione Equazionale (1)

1. Reflexivity $$\frac{}{t = t}$$
2. Symmetry $$\frac{t_1 = t_2}{t_2 = t_1}$$
3. Transitivity $$\frac{t_1 = t_2 \quad t_2 = t_3}{t_1 = t_3}$$
4. Substitutivity $$\frac{t_i = t_i'}{f(t_1, \ldots t_i, \ldots t_k) = f(t_1, \ldots t_i', \ldots t_k)}$$ for any operator f
5. Instantiation $$\frac{t_1 = t_2}{t_1[\rho] = t_2[\rho]}$$ for any substitution ρ
6. Axioms $$\frac{}{t_1 = t_2}$$ for all axioms $t_1 = t_2$ in E

Deduzione Equazionale (2)

- Una prova è una sequenza finita di uguaglianze

  $t_1 = t'_1 \;\; t_2 = t'_2 \;\; t_3 = t'_3 \; .... \; t_k = t'_k$

  tale che ogni $t_j = t'_j$ o è un assioma (regole 1 e 6), oppure è ottenuta usando una regola (2-5) con premesse alcune delle uguaglianze precedenti nella sequenza.
- Scriviamo $E \vdash t_1 = t_2$ per indicare che esiste una prova, usando gli assiomi in E, che termina con l'uguaglianza $t_1 = t_2$.
- Questo determina una congruenza:

$$t_1 =_E t_2 \text{ sse } E \vdash t_1 = t_2$$

Assiomi per l'operatore +

Gli assiomi usano, di solito, termini aperti

A1	Associativity	$x + (y + z) = (x + y) + z$
A2	Commutativity	$x + y = y + x$
A3	Identity	$x + \mathbf{0} = x$
A4	Idempotence	$x + x = x$

Esempio di prova (1)

- Vogliamo dimostrare che

$$\{A1,A2,A4\} \vdash a.0 + (b.w + a.0) = a.0 + b.w$$

1.	$x+y=y+x$	Axiom **A2**
2.	$b.w+a.\mathbf{0}=a.\mathbf{0}+b.w$	Rule 5: Instantiation of line 1
3.	$a.\mathbf{0}+(b.w+a.\mathbf{0})=a.\mathbf{0}+(a.\mathbf{0}+b.w)$	Rule 4: Substitutivity on line 2
4.	$x+(y+z)=(x+y)+z$	Axiom **A1**
5.	$a.\mathbf{0}+(a.\mathbf{0}+b.w)=(a.\mathbf{0}+a.\mathbf{0})+b.w$	Rule 5: Instantiation of line 4
6.	$x+x=x$	Axiom **A4**
7.	$a.\mathbf{0}+a.\mathbf{0}=a.\mathbf{0}$	Rule 5: Instantiation of line 6
8.	$(a.\mathbf{0}+a.\mathbf{0})+b.w=a.\mathbf{0}+b.w$	Rule 4: Substitutivity on line 7
9.	$a.\mathbf{0}+(b.w+a.\mathbf{0})=(a.\mathbf{0}+a.\mathbf{0})+b.w$	Rule 3: Transitivity on lines 3 and 5
10.	$a.\mathbf{0}+(b.w+a.\mathbf{0})=a.\mathbf{0}+b.w$	Rule 3: Transitivity on lines 9 and 8

Esempio di prova (2)

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{\dfrac{x+y=y+x}{b.w+a.\mathbf{0}=a.\mathbf{0}+b.w}}
}{a.\mathbf{0}+(b.w+a.\mathbf{0})=a.\mathbf{0}+(a.\mathbf{0}+b.w)}
\qquad
\dfrac{\dfrac{}{x+(y+z)=(x+y)+z}}{a.\mathbf{0}+(a.\mathbf{0}+b.w)=(a.\mathbf{0}+a.\mathbf{0})+b.w}
}{a.\mathbf{0}+(b.w+a.\mathbf{0})=(a.\mathbf{0}+a.\mathbf{0})+b.w}
\qquad
\dfrac{\dfrac{\dfrac{}{x+x=x}}{a.\mathbf{0}+a.\mathbf{0}=a.\mathbf{0}}}{(a.\mathbf{0}+a.\mathbf{0})+b.w=a.\mathbf{0}+b.w}
}{a.\mathbf{0}+(b.w+a.\mathbf{0})=a.\mathbf{0}+b.w}
$$

Assiomatizzazioni (ground) sound & (ground) complete

- Sia R una relazione su processi di CCS Finito (closed). L'assiomatizzazione E è detta (ground) sound per R se

$$E \vdash t_1 = t_2 \quad \text{implies} \quad (t_1, t_2) \in R$$

- L'assiomatizzazione E è detta (ground) complete per R se

$$(t_1, t_2) \in R \quad \text{implies} \quad E \vdash t_1 = t_2$$

Quindi E è sound & complete per R sse R è una congruenza e R coincide con $=_E$ (su termini chiusi)

Assiomatizzazione SB (non finita) di ~ per Finite CCS

- Oltre agli assiomi A1,A2,A3,A4 visti per il +, dobbiamo anche considerare i seguenti:

$$
\begin{array}{lll}
\mathbf{R1} & & (\nu a)\mathbf{0} = \mathbf{0} \\
\mathbf{R2} & \text{if } \mu \notin \{a, \bar{a}\} & (\nu a)\mu.x = \mu.(\nu a)x \\
\mathbf{R3} & \text{if } \mu \in \{a, \bar{a}\} & (\nu a)\mu.x = \mathbf{0} \\
\mathbf{R4} & & (\nu a)(x+y) = (\nu a)x + (\nu a)y
\end{array}
$$

$$
\begin{array}{ll}
\mathbf{Exp} & \text{if } x = \Sigma_{i=1}^{n} \mu_i.x_i \text{ and } y = \Sigma_{j=1}^{m} \mu'_j.y_j \\
& x \,|\, y \;=\; \Sigma_i \mu_i.(x_i \,|\, y) \;+\; \Sigma_j \mu'_j.(x \,|\, y_j) \;+\; \Sigma_{i,j:\overline{\mu_i}=\mu'_j} \tau.(x_i \,|\, y_j)
\end{array}
$$

- R1-R4 sono schemi di assioma (uno diverso per ogni scelta delle azioni a e μ che sono finite)
- Exp è pure uno schema, ma non finito! (uno per ogni n, m)

SB è sound

- Teorema: Per ogni p, q in Finite CCS (closed)

  $SB \vdash p = q$ implica $p \sim q$

  Dimostrazione per induzione sulla prova (finita) per $SB \vdash p = q$. Gli assiomi sono 1 (riflessività) e 6 (assiomi in SB). Riflessività ovviamente vale per ~, così come ogni istanziazione ground degli assiomi in SB (proprietà algebriche!). Le altre regole valgono, assumendo che la tesi valga sulla premessa, perché ~ è una equivalenza ed anche una congruenza.

SB è completa (1)

- Forma normale: p è in forma normale se è costruito solo con 0, prefisso e somma (cioè un albero!), rappresentato con una sommatoria. Ovvero p è del tipo $\sum_{i \in I} \mu_i.p_i$ dove i p_i sono a loro volta forme normali.
- Misura di una forma normale: massimo numero di prefissi annidati (si assume $\max(\varnothing) = 0$)

$$depth(\Sigma_{i \in I} \mu_i.p_i) = max\{depth(\mu_i.p_i) \mid i \in I\}$$
$$depth(\mu.p) = 1 + depth(p)$$

Proposition 4.13. *For any normal form p, if* $p \xrightarrow{\mu} p'$, *then* $\mu.p'$ *is a summand of p,* p' *is a normal form and* $depth(p') < depth(p)$. $\square$

SB è completa (2)

Proposition 4.14. (Completeness for normal forms) *If p and q are normal forms such that $p \sim q$, then $\mathscr{S}\mathscr{B} \vdash p = q$.*

Proof. By induction on the sum of depths of p and q. If the sum is 0, then $p = q = \mathbf{0}$ and the thesis follows by rule 1 (reflexivity) in Table 4.1.

Otherwise, suppose $\mu.p'$ is a summand of p, hence $p \xrightarrow{\mu} p'$. As $p \sim q$, then also $q \xrightarrow{\mu} q'$ with $p' \sim q'$. Since q is a normal form, $\mu.q'$ must be a summand of q. Observe that the sum of depths of p' and q' is strictly decreased, hence induction can be applied in order to get $\mathscr{S}\mathscr{B} \vdash p' = q'$. By rule 4 (substitutivity) of Table 4.1, then also $\mathscr{S}\mathscr{B} \vdash \mu.p' = \mu.q'$ is derivable. Hence for any summand $\mu.p'$ of p, we have found a summand $\mu.q'$ of q so that the two are equated by the axioms. Symmetrically, we can prove that for any summand $\mu.q'$ of q, there exists a summand $\mu.p'$ of p such that $\mathscr{S}\mathscr{B} \vdash \mu.p' = \mu.q'$ is derivable.

Hence, putting all the summands together (via substitutivity w.r.t. $+$), we have $\mathscr{S}\mathscr{B} \vdash p = q$ modulo the axioms **A4** (for removing possible duplicates) and **A1**-**A2** (for rearranging the remaining summands). $\square$

SB è completa (3)

- Riduzione a forma normale: per ogni processo CCS finito p, esiste una forma normale q tale che SB $\vdash$ p = q.

  Si dimostra per induzione strutturale sulla struttura di p, usando i seguenti lemmi ausiliari (dimostrati per induzione sul depth):
  - "se p e q sono forme normali, allora esiste r forma normale tale che SB $\vdash$ p|q = r."
  - "se p è una forma normale, allora esiste r forma normale tale che SB $\vdash$ (va)p = r."

  Dettagli sulle dimostrazioni sul libro.

SB è completa (4)

- Teorema: $p \sim q$ implica $SB \vdash p = q$
- Dimostrazione: per lemma di riduzione a forma normale, esistono forme normali s e t tali che

  $SB \vdash p = s$ e $SB \vdash q = t$.

  Per Teorema di soundness, allora anche $p \sim s$ e $q \sim t$.

  Dato che $p \sim q$, per transitività anche $s \sim t$.

  Per Teorema di completezza per forme normali, abbiamo $SB \vdash s = t$. Quindi la tesi $SB \vdash p = q$ segue per transitività.

Assiomatizzazione per simulation equivalence e per trace equivalence

- Si può dimostrare che se ad SB aggiungiamo S

  $$\mathbf{S} \quad \mu.(x+y) = \mu.(x+y) + \mu.y$$

  otteniamo una assiomatizzazione sound e completa di simulation equivalence.
- Si può dimostrare che se ad SB aggiungiamo T

  $$\mathbf{T} \quad \text{Distributivity} \quad \mu.(x+y) = \mu.x + \mu.y$$

  otteniamo una assiomatizzazione sound e completa di trace equivalence.

Assiomatizzazione finita per trace equivalence

- L'assiomatizzazione per trace equivalence del lucido precedente non è finita perché usa lo schema infinitario di assioma EXP. Possiamo al suo posto mettere i seguenti assiomi (o schemi finitari):

P1	$\mathbf{0} \mid x = x$	
P2	$x \mid y = y \mid x$	
P3	$(x+y) \mid z = x \mid z + y \mid z$	
P4	$\mu.x \mid \mu'.y = \mu.(x \mid \mu'.y) + \mu'.(\mu.x \mid y)$	if $\mu' \neq \overline{\mu}$
P5	$\alpha.x \mid \overline{\alpha}.y = \alpha.(x \mid \overline{\alpha}.y) + \overline{\alpha}.(\alpha.x \mid y) + \tau.(x \mid y)$	

- N.B: P3 non è sound per bisimulation e neanche per simulation.

Assiomatizzazione WB per $\approx^c$

- WB = SB U {W1,W2,W3} corrispondenti alle tre tau-laws

$$\begin{array}{ll} \textbf{W1} & \mu.\tau.x = \mu.x \\ \textbf{W2} & x + \tau.x = \tau.x \\ \textbf{W3} & \mu.(x+\tau.y) = \mu.(x+\tau.y) + \mu.y \end{array}$$

- Teorema di soundness: per p e q processi Finite CCS (closed), WB $\vdash$ p = q implica p $\approx^c$ q
- Dim. per induzione sulla prova di WB $\vdash$ p = q. La soundness degli assiomi W1-W2-W3 è una nota proprietà algebrica.

Completezza di WB

- Forma normale saturata: una forma normale $p = \sum_i \mu_i.p_i$ è saturata se ogni volta che $p=\mu=>p'$ allora $\mu.p'$ è un addendo di p (e p' è a sua volta saturato).

1. Ogni forma normale può essere saturata (Saturation Lemma + Proposizione)
2. Ogni processo può essere ridotto in forma normale saturata.
3. Completezza per forme normali saturate.

Saturation Lemma

Lemma 4.5. (Saturation Lemma)

Given a normal form p, if $p \stackrel{\mu}{\Longrightarrow} p'$, *then* $\mathscr{W}\mathscr{B} \vdash p = p + \mu.p'$.

Proof. By induction on the length of $p \stackrel{\varepsilon}{\Longrightarrow} \stackrel{\mu}{\longrightarrow} \stackrel{\varepsilon}{\Longrightarrow} p'$. The base case is when $p \stackrel{\mu}{\longrightarrow} p'$; this means that $\mu.p'$ is a summand of p. Then, by axiom **A4** the thesis follows.

Inductively, we have two cases: either $p \stackrel{\mu}{\longrightarrow} q \stackrel{\tau}{\Longrightarrow} p'$ or $p \stackrel{\tau}{\longrightarrow} q \stackrel{\mu}{\Longrightarrow} p'$. In the former case, we have that $\mu.q$ is a summand of p. Moreover, by induction (as the computation is shorter) we know that $\mathscr{W}\mathscr{B} \vdash q = q + \tau.p'$. Hence, we conclude that

$\mathscr{W}\mathscr{B} \vdash p = p + \mu.q$	axiom **A4**
$= p + \mu.(q + \tau.p')$	by induction and substitutivity
$= p + \mu.(q + \tau.p') + \mu.p'$	axioms **W3**
$= p + \mu.p'$	by previous steps reversed

In the latter case, we have that $\tau.q$ is a summand of p. Moreover, by induction, we know that $\mathscr{W}\mathscr{B} \vdash q = q + \mu.p'$. Hence, we conclude that

$\mathscr{W}\mathscr{B} \vdash p = p + \tau.q$	axiom **A4**
$= p + \tau.q + q$	axioms **W2**
$= p + \tau.q + q + \mu.p'$	by induction and substitutivity
$= p + \mu.p'$	by previous steps reversed

and this concludes the proof. □

Saturazione di forme normali

Proposition 4.17. (Saturation of normal forms) *For any normal form p, there exists a saturated normal form q of equal depth such that $\mathscr{W}\mathscr{B} \vdash p = q$.*

Proof. By induction on the depth of p. If it is 0, then $p = \mathbf{0}$, which is a saturated normal form. Otherwise, assume by induction that for any summand $\mu_i.p_i$ of p, $\mathscr{W}\mathscr{B} \vdash p_i = q_i$ where q_i is a saturated normal form such that $depth(p_i) = depth(q_i)$. By substitutivity, we have $\mathscr{W}\mathscr{B} \vdash \mu_i.p_i = \mu_i.q_i$. Let $q' = \Sigma_i \mu_i.q_i$. Then, by substitutivity, $\mathscr{W}\mathscr{B} \vdash p = q'$. Process q' is a normal form of equal depth but not saturated yet because for some i, μ_i can be τ. Now we consider the set $I = \{(\mu'_k, p'_k) \mid q' \stackrel{\mu'_k}{\Longrightarrow} p'_k$ but not $q' \xrightarrow{\mu'_k} p'_k\}$. Then, by Lemma 4.5, if $|I| = m$, $\mathscr{W}\mathscr{B} \vdash q' = q' + \mu'_1.p'_1 + \ldots + \mu'_m.p'_m$ which is a saturated normal form. Note that this saturated normal form has the same depth as q' because any summand $\mu'_k.p'_k$ has smaller depth (the maximal paths are shorter). $\square$

- Allora ogni processo può essere prima ridotto in forma normale (già visto), e poi in forma normale saturata.

Completezza di WB
per forme normali saturate

Proposition 4.17. (Completeness for saturated normal forms) *If p and q are saturated normal forms such that $p \approx^c q$, then $\mathscr{W}\mathscr{B} \vdash p = q$.*

Proof. By induction on the sum of the depths of p and q. If the sum is 0, then $p = q = \mathbf{0}$ and the thesis follows by rule 1 (reflexivity) in Table 4.1.

Otherwise, suppose $\mu.p'$ is a summand of p, hence $p \xrightarrow{\mu} p'$. As $p \approx^c q$, we have that $q \stackrel{\mu}{\Longrightarrow} q'$ with $p' \approx q'$. Since q is a saturated normal form, we have $q \xrightarrow{\mu} q'$, i.e., $\mu.q'$ is a summand of q. Summing up, for each summand $\mu.p'$ of p, we have a summand $\mu.q'$ of q such that $p' \approx q'$. Now, by Lemma 4.1 (Hennessy Lemma), we know that

$$p' \approx q' \text{ iff } (p' \approx^c q' \text{ or } p' \approx^c \tau.q' \text{ or } \tau.p' \approx^c q').$$

We have three cases.

(1) If $p' \approx^c q'$ then, as p' and q' are saturated normal forms, by induction (the sum of the depths is strictly decreased), $\mathscr{W}\mathscr{B} \vdash p' = q'$, hence $\mathscr{W}\mathscr{B} \vdash \mu.p' = \mu.q'$ by substitutivity.

Completezza di WB per forme normali saturate (2)

(2) If $p' \approx^c \tau.q'$, we have first of all to reduce $\tau.q'$ to a saturated normal form. By Proposition 4.16 we have that there exists a saturated normal form q'' of equal depth such that $\mathscr{W}\mathscr{B} \vdash \tau.q' = q''$. By Theorem 4.8, we have that $\tau.q' \approx^c q''$, hence $p' \approx^c q''$ by transitivity. Since $p' \approx^c q''$ and the sum of depth of p' and q'' is one less than that of p and q, we can apply induction and derive that $\mathscr{W}\mathscr{B} \vdash p' = q''$, hence $\mathscr{W}\mathscr{B} \vdash p' = \tau.q'$ by transitivity, and $\mathscr{W}\mathscr{B} \vdash \mu.p' = \mu.\tau.q'$ by substitutivity, and $\mathscr{W}\mathscr{B} \vdash \mu.p' = \mu.q'$ by axiom **W1** *and transitivity.*

(3) If $\tau.p' \approx^c q'$, then we can proceed as for case (2) above.

In all the three cases above, for each summand $\mu.p'$ of p, we have a summand $\mu.q'$ of q such that $\mathscr{W}\mathscr{B} \vdash \mu.p' = \mu.q'$. Symmetrically, it can be proved that for each summand $\mu.q'$ of q, we have a summand $\mu.p'$ of p such that $\mathscr{W}\mathscr{B} \vdash \mu.p' = \mu.q'$.

Therefore, $\mathscr{W}\mathscr{B} \vdash p = q$ by substitutivity and possible applications of axioms **A4** *(for removing possible duplicates) and* **A1**-**A2** *(for rearranging the remaining summands).* $\square$

WB è completa in generale

- Teorema: $p \approx^c q$ implica $WB \vdash p = q$
- Dimostrazione: per lemma di riduzione a forma normale saturata, esistono forme normali saturate s e t tali che $WB \vdash p = s$ e $WB \vdash q = t$.

  Per Teorema di soundness, allora $p \approx^c s$ e $q \approx^c t$.

  Dato che $p \approx^c q$, per transitività anche $s \approx^c t$.

  Per Teorema di completezza per forme normali saturate, abbiamo $WB \vdash s = t$. Quindi la tesi

  $WB \vdash p = q$ segue per transitività.

Assiomatizzazione Finita di ~ via operatori ausiliari per Finite CCS

- Left merge:

$$(\text{Left})\ \frac{p \xrightarrow{\mu} p'}{p \lfloor q \xrightarrow{\mu} p' \mid q}$$

- Synchronization merge:

$$(\text{Merge})\ \frac{p \xrightarrow{\alpha} p' \qquad q \xrightarrow{\overline{\alpha}} q'}{p \| q \xrightarrow{\tau} p' \mid q'}$$

- Si può dimostrare che ~ è una congruenza per questi operatori ausiliari.

ASB – assiomatizzazione finita

- Oltre agli assiomi A1-A2-A3-A4 per il + e gli assiomi R1-R2-R3-R4 per la restrizione, ASB aggiunge i seguenti (al posto di EXP):

$$\textbf{Par} \quad x|y = x\lfloor y + y\lfloor x + x\|y$$

$$\begin{array}{ll}
\textbf{L1} & \mathbf{0}\lfloor y = \mathbf{0} \\
\textbf{L2} & (\mu.x)\lfloor y = \mu.(x|y) \\
\textbf{L3} & (x+y)\lfloor z = x\lfloor z + y\lfloor z
\end{array}$$

$$\begin{array}{lll}
\textbf{C1} & & x\|y = y\|x \\
\textbf{C2} & & \mathbf{0}\|y = \mathbf{0} \\
\textbf{C3} & \text{if } \mu_1 = \overline{\mu_2} & (\mu_1.x)\|(\mu_2.y) = \tau.(x|y) \\
\textbf{C4} & \text{if } \mu_1 \neq \overline{\mu_2} & (\mu_1.x)\|(\mu_2.y) = \mathbf{0} \\
\textbf{C5} & & (x+y)\|z = x\|z + y\|z
\end{array}$$

ASB è sound & complete per ~

- Teorema (soundness): ASB $\vdash$ p = q implica p ~ q

  (si possono dimostrare sound tutti gli assiomi per gli operatori ausiliari)
- Riduzione a forma normale: per ogni processo p (che anche usa gli operatori ausiliari) esiste una forma normale q tale che ASB $\vdash$ p = q.
- Completezza per forma normale (come per SB)
- Completezza in generale, usando la riduzione a forma normale e la soundness (come fatto per SB).

Assiomatizzazioni finite per rooted weak bisimilarity

- Le cose sono più complicate per rooted weak bisimilarity $\approx^c$, ma si può comunque ottenere una assiomatizzazione finita. (Vedi libro)