Logica per la programmazione: applicazioni

Appunti ad uso degli studenti del I anno
Corso di Laurea in Informatica
Università di Pisa

a.a. 2008/09

Autori: P. Mancarella, S.Martini
Editore: F.Turini

1. Introduzione

In questa seconda parte introduciamo specializzazioni del calcolo del primo ordine finalizzate a trattare specifiche utili per la progreammazione.

Con lo scopo di semplificare alcune formule, o di utilizzare notazioni mutuate da altri settori della matematica, introdurremo in questo breve paragrafo della notazione accessoria, definita talvolta in termini degli altri concetti che abbiamo discusso sin qui.

1.1 Insiemi

Dato un predicato unario[1] P, scriveremo

$$\{x \mid P(x)\}$$

per "l'insieme di tutti gli elementi v per i quali vale P(v)" (l'universo dal quale provengono gli elementi v è in genere chiaro dal contesto; per noi, si tratta di solito dell'insieme dei naturali, o degli interi); la variabile x è legata in $\{x \mid P(x)\}$. Useremo abbastanza liberamente le usuali operazioni su insiemi (appartenenza, unione, intersezione, ecc.); il simbolo $\varnothing$ denota l'insieme vuoto, ovvero l'insieme $\{x \mid \mathbf{F}\}$. Assumiamo anche per gli insiemi la regola di ridenominazione, e la legge

$y \in \{ x \mid P(x)\} \equiv P(y)$	def-$\in$

in cui $x \in I$ denota l'appartenenza di x all'insieme I. Si noti che, se l'insieme in questione è $\varnothing$, abbiamo $y \in \varnothing \equiv \mathbf{F}$. Infatti:

$y \in \varnothing$

$\equiv$ {definizione di $\varnothing$}

$y \in \{x \mid \mathbf{F}\}$

$\equiv$ {def-$\in$}

$\mathbf{F}$.

Le leggi viste nelle sezioni precedenti per la manipolazione di formule

[1] Cioè dipendente da una sola variabile.

del calcolo dei predicati possono essere utilizzate per manipolare formule che riguardano insiemi (e, più in generale, formule che coinvolgono i quantificatori che introdurremo nel seguito). Valgono ad esempio le seguenti leggi:

(Ins:≡)
$(\forall x.\ P \equiv Q) \Rightarrow \{x \mid P\} = \{x \mid Q\}$
(Ins:⇒)
$(\forall x.\ P \Rightarrow Q) \Rightarrow \{x \mid P\} \subseteq \{x \mid Q\}$

Vediamo come esempio la dimostrazione della seconda legge, ricordando che, dati due insiemi I e J, $I \subseteq J$ se e solo se ogni elemento di I è anche un elemento di J. Dobbiamo allora dimostrare che un generico elemento dell'insieme $\{x \mid P\}$ è anche elemento dell'insieme $\{x \mid Q\}$.

$z \in \{x \mid P\}$
$\equiv$ {def-∈}
P^z_x
$\Rightarrow$ {**Ip**: $(\forall x.\ P \Rightarrow Q)$, Elim-∀}
Q^z_x
$\equiv$ {def-∈}
$z \in \{x \mid Q\}$.

Si noti come il passo di dimostrazione che introduce il connettivo ⇒ utilizzi una conseguenza dell'ipotesi fatta (l'ipotesi $\forall x.\ P \Rightarrow Q$), e cioè $P^z_x \Rightarrow Q^z_x$ che si ottiene dall'ipotesi stessa applicando la legge Elim-∀.

1.2 Intervalli

Tra gli insiemi, particolare rilevanza per i nostri scopi rivestono gli *intervalli* di naturali (o interi). Se a e b sono numeri naturali (o interi), introduciamo per gli intervalli la notazione

$[a, b] \cong \{x \mid a \leq x \leq b\}$
$[a, b) \cong \{x \mid a \leq x < b\}$
$(a, b] \cong \{x \mid a < x \leq b\}$
$(a, b) \cong \{x \mid a < x < b\}$

Si noti che [a,b) è l'intervallo vuoto se e soltanto se $a \geq b$ (ed analogamente per gli intervalli degli altri tipi).

1.3 Predicati di base

Assumiamo che il linguaggio dei predicati contenga sempre, oltre l'uguaglianza (=) (che, lo ricordiamo, assumiamo essere riflessiva, simmetrica e transitiva), i predicati $\leq$ e $\geq$ (riflessivi, antisimmetrici e transitivi). Introduciamo poi le abbreviazioni

$x \neq y \cong \sim(x=y)$
$x < y \cong x \leq y \wedge x \neq y$
$x > y \cong x \geq y \wedge x \neq y$

e la legge:

$\sim(x \leq y) \equiv x > y$ $\quad (\sim:\leq)$
$\sim(x \geq y) \equiv x < y$

Esercizio Si dimostri che $\sim(x<y) \equiv x>y \vee x=y$ e che $\sim(x>y) \equiv x<y \vee x=y$.

1.4 Dominî

Formule molto comuni nella specifica di programmi sono quelle che formalizzano asserti del tipo "per tutti gli x tali che P(x), vale Q(x)" e "esiste un x tale che P(x) per cui vale Q(x)", ovvero, rispettivamente

$(\forall x.P(x) \Rightarrow Q(x))$
$(\exists x.P(x) \wedge Q(x))$

Il ruolo svolto dal predicato P, in entrambe le formule, è quello di restringere il dominio su cui varia la variabile legata x (non l'intero universo, ma solo gli elementi per cui vale P). Introduciamo una notazione apposita per casi come questi, al fine di evitare il proliferare

dei connettivi. Introduciamo dunque le seguenti *abbreviazioni*:

$(\forall x{:}P.Q) \cong (\forall x.P \Rightarrow Q)$
$(\exists x{:}P.Q) \cong (\exists x.P \wedge Q)$

Ci riferiremo alla formula P come al *dominio* del quantificatore. Il dominio è *vuoto* se, per tutti i v, $P^{v}_{x} \equiv \mathbf{F}$ (cioè non ci sono elementi che soddisfano la formula P). Detto altrimenti, P è vuoto se $\sim(\exists x.\ P) \equiv \mathbf{T}$ o equivalentemente $(\forall x.\ \sim P) \equiv \mathbf{T}$. Se il dominio di una formula è vuoto, possiamo immediatamente determinarne il valore di verità; dimostriamolo per assurdo, ovvero dimostriamo l'implicazione $\sim(\forall x{:}P.Q) \Rightarrow \mathbf{F}$. Abbiamo allora

$\sim(\forall x{:}P.Q)$
$\equiv$ {definizione}
$\sim(\forall x.P \Rightarrow Q)$
$\equiv$ {De Morgan}
$(\exists x.\ \sim(P \Rightarrow Q))$
$\equiv$ {Elim-$\Rightarrow$}
$(\exists x.\ \sim(\sim P \vee Q)$
$\equiv$ {De Morgan}
$(\exists x.\ P \wedge \sim Q)$
$\Rightarrow$ {$(\exists x.\ P \wedge Q) \Rightarrow (\exists x.\ P) \wedge (\exists x.\ Q)$}
$(\exists x.\ P) \wedge (\exists x.\ \sim Q)$
$\equiv$ {**Ip**: P vuoto}
$\mathbf{F} \wedge (\exists x.\ \sim Q)$
$\equiv$ {Zero}
$\mathbf{F}$

Abbiamo così dimostrato la legge

$(\forall x{:}P.Q) \equiv \mathbf{T}$	se P è vuoto	(Vuoto)

La dimostrazione dell'analoga legge per il quantificatore esistenziale è lasciata per esercizio.

$(\exists x{:}P.Q) \equiv \mathbf{F}$	se P è vuoto	(Vuoto)

Molte delle leggi precedentemente viste per i quantificatori possono essere generalizzate a formule con domini; ci accontenteremo di notare quelle che seguono.

$(\forall y{:}R.(\forall x{:}S.P)) \equiv (\forall x{:}S.(\forall y{:}R.P))$	(Annid)
se y non è libera in S e x non è libera in R	
$(\exists y{:}R.(\exists x{:}S.P)) \equiv (\exists x{:}S.(\exists y{:}R.P))$	
se y non è libera in S e x non è libera in R	

$(\forall x{:}R.P \wedge Q) \equiv (\forall x{:}R.P) \wedge (\forall x{:}R.Q)$	$(\forall{:}\wedge)$
$(\exists x{:}R.P \vee Q) \equiv (\exists x{:}R.P) \vee (\exists x{:}R.Q)$	$(\exists{:}\vee)$

$(\forall x{:}P \vee Q.R) \equiv (\forall x{:}P.R) \wedge (\forall x{:}Q.R)$	(Dominio)[2]
$(\exists x{:}P \vee Q.R) \equiv (\exists x{:}P.R) \vee (\exists x{:}Q.R)$	

$(\forall x{:}R.Z) \equiv Z$	se x non è libera in Z e R non è vuoto	(Costante)
$(\exists x{:}R.Z) \equiv Z$	se x non è libera in Z e R non è vuoto	
$(\forall x{:}R.P) \vee Z \equiv (\forall x{:}R.P \vee Z)$	se x non è libera in Z	(Distrib)
$(\exists x{:}R.P) \wedge Z \equiv (\exists x{:}R.P \wedge Z)$	se x non è libera in Z	

$(\forall x{:}R.P) \wedge Z \equiv (\forall x{:}R.P \wedge Z)$	se x non è libera in Z e R non è vuoto
$(\exists x{:}R.P) \vee Z \equiv (\exists x{:}R.P \vee Z)$	se x non è libera in Z e R non è vuoto

$\sim(\forall x{:}R.P) \equiv (\exists x{:}R.\sim P)$	(De Morgan)
$\sim(\exists x{:}R.P) \equiv (\forall x{:}R.\sim P)$	

[2] Si osservi che si tratta soltanto di una riscrittura della legge (Dominio) utilizzando la nuova notazione, che motiva anche il nome dato alla legge.

$(\forall x{:}x{=}i.P) \equiv P^{i}_{x}$	(Singoletto)
$(\exists x{:}x{=}i.P) \equiv P^{i}_{x}$	

Esercizio: Si dimostrino le leggi appena enunciate, riconducendole alla loro forma estesa ed utilizzando poi le altre leggi.

Riserviamo una notazione particolare a quelle formule il cui dominio è costituito da un intervallo. Dato un intervallo I, introduciamo le abbreviazioni

$(\forall x \in I.Q) \cong (\forall x{:}x \in I.Q)$
$(\exists x \in I.Q(x)) \cong (\exists x{:}x \in I.Q)$

Utilizzeremo inoltre le ulteriori abbreviazioni

$(\forall x, y \in I.\ Q) \cong (\forall x \in I.\ (\forall y \in I.\ Q))$
$(\exists x, y \in I.\ Q) \cong (\exists x \in I.\ (\exists y \in I.\ Q))$

analoghe a quelle già introdotte per i quantificatori universale ed esistenziale. Anche queste abbreviazioni si possono generalizzare come segue:

$(\forall x_1,\ldots,x_n, y \in I.\ Q) \cong (\forall x_1,\ldots,x_n \in I.\ (\forall y \in I.\ Q))$	$n \geq 1$
$(\exists x_1,\ldots,x_n, y \in I.\ Q) \cong (\exists x_1,\ldots,x_n \in I.\ (\exists y \in I.\ Q))$	$n \geq 1$

Si osservi che, in virtù di (Vuoto), $(\forall x \in \varnothing.Q) \equiv \mathbf{T}$, mentre $(\exists x \in \varnothing.Q) \equiv \mathbf{F}$.

Concludiamo questo paragrafo con alcune leggi interessanti e molto utili nei calcoli.

$(\forall x{:}P.\ Q) \equiv (\forall x{:}P \wedge x \neq k.\ Q) \wedge Q^{k}_{x}$	se P^{k}_{x}
$(\forall x{:}P.\ Q) \equiv (\forall x{:}P \wedge x \neq k.\ Q)$	se $\sim P^{k}_{x}$
$(\exists x{:}P.\ Q) \equiv (\exists x{:}P \wedge x \neq k.\ Q) \vee Q^{k}_{x}$	se P^{k}_{x}
$(\exists x{:}P.\ Q) \equiv (\exists x{:}P \wedge x \neq k.\ Q)$	se $\sim P^{k}_{x}$

Una scrittura equivalente di tali leggi, che useremo anche in seguito, è:

$$(\forall x{:}P.\ Q) \equiv \begin{cases} (\forall x : P \wedge x \neq k.\, Q) \wedge Q_x^k & \text{se } P_x^k \\ (\forall x : P \wedge x \neq k.\, Q) & \text{se} \sim P_x^k \end{cases}$$

$$(\exists x{:}P.\ Q) \equiv \begin{cases} (\exists x : P \wedge x \neq k.\, Q) \vee Q_x^k & \text{se } P_x^k \\ (\exists x : P \wedge x \neq k.\, Q) & \text{se} \sim P_x^k \end{cases}$$

Dimostriamo la prima, lasciando le altre per **esercizio**. Osserviamo innanzitutto che dobbiamo dimostrare la seguente implicazione:

$P_x^k \Rightarrow ((\forall x{:}P.\ Q) \equiv (\forall x{:}P \wedge x{\neq}k.\ Q) \wedge Q_x^k)$

$(\forall x{:}P.\ Q)$
$\equiv$ {Terzo escluso, Unità}
$(\forall x{:}P \wedge (x{=}k \vee x{\neq}k).\ Q)$
$\equiv$ {Distributività}
$(\forall x{:}\ (P \wedge x{=}k) \vee (P \wedge x{\neq}k).\ Q)$
$\equiv$ {Dominio}
$(\forall x{:}\ P \wedge x{=}k.\ Q) \wedge (\forall x{:}\ P \wedge x{\neq}k.\ Q)$
$\equiv$ {Leibniz}
$(\forall x{:}\ P_x^k \wedge x{=}k.\ Q) \wedge (\forall x{:}\ P \wedge x{\neq}k.\ Q)$
$\equiv$ {**Ip**: P_x^k, Unità}
$(\forall x{:}x{=}k.\ Q) \wedge (\forall x{:}\ P \wedge x{\neq}k.\ Q)$
$\equiv$ {Singoletto}
$Q_x^k \wedge (\forall x{:}\ P \wedge x{\neq}k.\ Q)$

Nel caso particolare in cui il dominio in questione sia un intervallo, le leggi precedenti si possono riscrivere nel seguente modo:

(Interv)

$$(\forall x \in [a,b).\ Q) \equiv \begin{cases} (\forall x : x \in [a,b) \wedge x \neq k.\ Q) \wedge Q_x^k & \text{se } k \in [a,b) \\ (\forall x : x \in [a,b) \wedge x \neq k.\ Q) & \text{se } k \notin [a,b) \end{cases}$$

$$(\exists x \in [a,b).\ Q) \equiv \begin{cases} (\exists x : x \in [a,b) \wedge x \neq k.\ Q) \vee Q_x^k & \text{se } k \in [a,b) \\ (\exists x : x \in [a,b) \wedge x \neq k.\ Q) & \text{se } k \notin [a,b) \end{cases}$$

Le leggi seguenti si possono derivare facilmente dalle precedenti (la loro dimostrazione è lasciata per **esercizio**).

(Interv)

$(\forall x \in [a,b].P) \equiv (\forall x \in [a,b).P) \wedge P_x^b$ se [a,b] non è vuoto

$(\forall x \in [a,b).P) \equiv (\forall x \in (a,b].P) \wedge P_x^a$ se [a,b] non è vuoto

$(\exists x \in [a,b].P) \equiv (\exists x \in [a,b).P) \vee P_x^b$ se [a,b] non è vuoto

$(\exists x \in [a,b].P) \equiv (\exists x \in (a,b].P) \vee P_x^a$ se [a,b] non è vuoto

2. Altri quantificatori

Lo scopo del calcolo che stiamo introducendo è quello, lo ricordiamo, di descrivere, specificare e "calcolare" programmi e loro risultati. A questo scopo è opportuno estendere il linguaggio dei termini a disposizione, per poter esprimere valori quali "la somma di tutti quegli x per cui vale P(x)", o "il numero degli x per cui vale P(x)". Vedremo che questi costrutti sintattici introducono, come i quantificatori, delle variabili legate. Modifichiamo per prima cosa la produzione relativa ai termini (della sintassi del calcolo dei predicati[3]) ed alcune definizioni accessorie per tener conto di queste modifiche.

```
Term ::= Const | Var | FIde (Term {, Term} ) |
         (Σ Var: Fbf.Term) | #{Var:Fbf | Fbf}|
         (max Var:Fbf.Term) |
         (min Var:Fbf.Term)
```

La variabile x occorre legata in (**Σ**x:P.E), #{x:P | Q}, (**max** x:P.E) e (**min** x:P.E). Anche per queste nuove forme quantificate introduciamo delle forme abbreviate per il caso in cui il dominio sia un intervallo (ad esempio (**Σ**x□I.E) ≅ (**Σ**x:x□I.E), ed analogamente per gli altri).

Vediamo innanzitutto come interpretiamo intuitivamente questi nuovi termini, insieme a delle utili varianti notazionali. In ciò che segue, assumeremo, se non specificato altrimenti, che il dominio di interpretazione sia $\mathbb{Z}$, l'insieme dei numeri interi.

2.1 Sommatoria

La stringa (**Σ**x:P(x).E(x))[4] denota "la somma di tutti gli E(v) per tutti i v per cui vale P(v)". Particolarmente frequente è il caso in cui il

---

3 In appendice è riportata la sintassi che risulta dalle varie aggiunte che abbiamo fatto nel corso di queste note.

4 Abbiamo evidenziato in questo termine il fatto che sia P che E, in genere, dipendono dalla variabile legata x.

dominio P(x) sia un intervallo; scriveremo allora (**Σ**x∈[a,b].E), od anche, secondo l'usuale notazione,

$$\sum_{x=a}^{b} E$$

per (**Σ**x:x∈[a,b].E).

2.2 Cardinalità

La stringa #{x:P(x)|Q(x)} denota "il numero dei Q(v) veri per tutti i v per cui vale P(v)"; si osservi che Q(x) è in questo caso una formula, e non un termine. Quando non si hanno restrizioni sul dominio, cioè P≡**T**, potremo scrivere #{x|Q(x)} — cioè l'usuale modo di scrivere la cardinalità dell'insieme di tutti gli x per i quali vale Q(x) — al posto di #{x:**T**|Q(x)}. Il lettore attento non avrà difficoltà a convincersi che la cardinalità può essere definita in termini della sommatoria, un fatto che costituisce la prima legge che menzioniamo

#{x:P|Q} = (**Σ**x:P ∧ Q.1) (Elim-#)

Utilizzando questa legge è facile dimostrare le seguenti uguaglianze:

#{x:P|Q} = #{x | P ∧ Q} = #{x: P ∧ Q | **T**}

2.3 Minimizzazione e Massimizzazione

La stringa (**max** x:P(x).E(x)) denota "il massimo dei valori E(v) per tutti i v per cui vale P(v)"; dualmente, (**min** x:P(x).E(x)) denota "il minimo dei valori E(v) per tutti i v per cui vale P(v)". La legge seguente collega, alla maniera delle leggi di De Morgan, **min** e **max**.

(**min** x:P.–E) = – (**max** x:P.E) (**min**:**max**)

Come per la cardinalità, è conveniente utilizzare anche per il massimo ed il minimo una notazione insiemistica, scrivendo[5] **m** {x | P} per (**m** x:P.x). Se poi il dominio è una congiunzione del tipo x∈I ∧ P, dove

[5] **m** sta sia per **max** che per **min**.

I è un intervallo, scriveremo **m** $\{x \in I \mid P\}$ per (**m** x: $x \in I \wedge P.x$).

2.4 Leggi

Quali altre leggi possiamo assumere per questi quantificatori *non standard*? Un attimo di riflessione mostra che, per ciascuno di essi, possiamo assumere leggi *analoghe* a quelle già introdotte per il quantificatore universale e quello esistenziale. In particolare, per ciascuno di essi avremo una *legge di ridenominazione* (ad esempio $(\mathbf{\Sigma}x{:}P.E) \equiv (\mathbf{\Sigma}y{:}P{}^{y}_{x}.E{}^{y}_{x}.)$, se y non occorre né in P né in E) ed una *legge di annidamento* (ad esempio $(\mathbf{\Sigma}y{:}R.(\mathbf{\Sigma}x{:}S.P)) = (\mathbf{\Sigma}x{:}S.(\mathbf{\Sigma}y{:}R.P))$, se y non è libero in S e x non è libero in R).

Le leggi che seguono consnetono di "ragionare" sui domini delle formule che coinvolgono i quantificatori appena introdotti.

(**min**:⇒)
$(\forall x.\ P \Rightarrow Q) \Rightarrow (\mathbf{min}\ x{:}P.\ E) \geq (\mathbf{min}\ x{:}Q.\ E)$

(**max**:⇒)
$(\forall x.\ P \Rightarrow Q) \Rightarrow (\mathbf{max}\ x{:}P.\ E) \leq (\mathbf{max}\ x{:}Q.\ E)$

(**m**:≡)
$(\forall x.\ P \equiv Q) \Rightarrow (\mathbf{m}\ x{:}P.\ E) = (\mathbf{m}\ x{:}Q.\ E)$

(#:≡)
$(\forall x.\ P \equiv Q) \Rightarrow (\#\{\ x{:}P \mid R) = (\#\{\ x{:}Q \mid R)$

(#:⇒)
$(\forall x.\ P \Rightarrow Q) \Rightarrow (\#\{\ x{:}P \mid R) \leq (\#\{\ x{:}Q \mid R)$
$(\forall x.\ R \Rightarrow S) \Rightarrow (\#\{\ x{:}P \mid R) \leq (\#\{\ x{:}P \mid S)$

(**Σ**:≡)
$(\forall x.\ P \equiv Q) \Rightarrow (\mathbf{\Sigma}x{:}P.\ E) = (\mathbf{\Sigma}x{:}Q.\ E)$

Per quanto riguarda il quantificatore **Σ**, non possiamo stabilire una legge del tipo (**Σ**:⇒), a meno di non fare ipotesi sull'espressione in questione. Valgono ad esempio le leggi:

$$(\forall x.\ E \geq 0 \wedge P \Rightarrow Q) \Rightarrow (\mathbf{\Sigma} x{:}P.E) \leq (\mathbf{\Sigma} x{:}Q.E) \qquad (\mathbf{\Sigma}{:}\Rightarrow)$$
$$(\forall x.\ E \leq 0 \wedge P \Rightarrow Q) \Rightarrow (\mathbf{\Sigma} x{:}P.E) \geq (\mathbf{\Sigma} x{:}Q.E)$$

La corrispondenza tra un predicato P e l'insieme $\{x \mid P\}$ e le leggi (Ins:≡) e (Ins:⇒) dovrebbe aiutare il lettore a convincersi della validità delle leggi precedenti.

Allo stesso modo dei quantificatori logici, poi, avremo le leggi seguenti[6]

$$(\mathbf{\Sigma} x{:}P.E+F) = (\mathbf{\Sigma} x{:}P.E) + (\mathbf{\Sigma} x{:}P.F) \qquad (\mathbf{\Sigma}{:}+)$$
$$(\mathbf{max}\ x{:}P.E\ \mathit{max}\ F) = (\mathbf{max}\ x{:}P.E)\ \mathit{max}\ (\mathbf{max}\ x{:}P.F) \qquad (\mathbf{max}{:}\mathit{max})$$
$$(\mathbf{min}\ x{:}P.E\ \mathit{min}\ F) = (\mathbf{min}\ x{:}P.E)\ \mathit{min}\ (\mathbf{min}\ x{:}P.F) \qquad (\mathbf{min}{:}\mathit{min})$$

(Dominio)

$$(\mathbf{\Sigma} x{:}P \vee Q.E) = (\mathbf{\Sigma} x{:}P.E) + (\mathbf{\Sigma} x{:}Q.E) - (\mathbf{\Sigma} x{:}P \wedge Q.E)$$
$$\#\{x{:}P \vee Q \mid R\} = \#\{x{:}P \mid R\} + \#\{x{:}Q \mid R\} - \#\{x{:}P \wedge Q \mid R\}$$
$$(\mathbf{max}\ x{:}P \vee Q.E) = (\mathbf{max}\ x{:}P.E)\ \mathit{max}\ (\mathbf{max}\ x{:}Q.E)$$
$$(\mathbf{min}\ x{:}P \vee Q.E) = (\mathbf{min}\ x{:}P.E)\ \mathit{min}\ (\mathbf{min}\ x{:}Q.E)$$

(Costante)

$(\mathbf{\Sigma} x{:}P.c) = c*(\mathbf{\Sigma} x{:}P.1)$ se x non è libera in c

$(\mathbf{m}\ x{:}P.c) = c$ se x non è libera in c e P non è vuoto

6 Le leggi relative alla cardinalità si ottengono utilizzando la legge (Elim-#), ma assumono spesso una forma abbastanza complessa. Ci limiteremo ad annotare quelle più semplici, e più utili.

(Distrib)

$(\mathbf{\Sigma}x{:}P.c*E) = c*(\mathbf{\Sigma}x{:}P.E)$ se x non è libera in c

$(\mathbf{m}\ x{:}P.c+E) = c+(\mathbf{m}\ x{:}P.E)$ se x non è libera in c e P non è vuoto

(Singoletto)

$$(\mathbf{\Sigma}x{:}x{=}y.E) = E^{y}_{x}.$$

$$\#\{x{:}x{=}y \mid R\} = \begin{cases} 1 & \text{se } R^{y}_{x} \\ 0 & \text{se } \sim R^{y}_{x} \end{cases}$$

$$(\mathbf{m}\ x{:}x{=}y.E) = E^{y}_{x}.$$

Per enunciare le leggi relative al dominio vuoto occorre supporre l'esistenza, tra i termini, di due costanti, che chiameremo $+\infty$ e $-\infty$, per le quali postuliamo $(\forall x.x \leq +\infty)$ e $(\forall x.-\infty \leq x)$.

(Vuoto)

$(\mathbf{\Sigma}x{:}P.E) = 0$ se P è vuoto

$\#\{x{:}P \mid P\} = 0$ "

$(\mathbf{min}\ x{:}P.E) = +\infty$ "

$(\mathbf{max}\ x{:}P.E) = -\infty$ "

Ricordiamo che P vuoto significa $\sim(\exists x.P)$. L'ipotesi di avere a disposizione $+\infty$ e $-\infty$ non è così strana come può sembrare a prima vista. Tutto dipende, infatti, dall'universo su cui le formule sono interpretate. Se tale universo è quello dei numeri naturali, allora $-\infty \cong 0$. Se, poi, l'universo di interpretazione è un tipo di dato di un linguaggio di programmazione, come **nat** o **integer**, allora è plausibile assumere anche l'esistenza di un massimo numero naturale (o intero) rappresentabile.

Il trattamento di formule che coinvolgono i quantificatori che abbiamo appena introdotto richiede una certa cautela. Che significato dobbiamo attribuire ad esempio alle seguenti espressioni?

$(\mathbf{\Sigma}x: x \geq 0.\ x)$
max $\{x \mid x \geq 1\}$ (*)
$\#\{x \mid x \geq 2\}$.

Si noti come in tutti questi casi, i valori che soddisfano la proprietà relativa al dominio delle espressioni sono infiniti. Ciò non toglie che, in alcune situazioni, il valore di tali espressioni sia comunque determinabile: ad esempio, la legge Costante ci consente di stabilire che

$(\mathbf{max}\ x: x \geq 1.\ c) = c$

se x non è libera in c, nonostante siano infiniti i numeri naturali maggiori o uguali a 1. Non è nostro interesse addentrarci nella discussione del significato di espressioni come le (*): nella pratica, infatti, raramente ci si trova a dover manipolare espressioni di questo tipo, e, se ciò dovesse succedere, consentiremo di addurre giustificazioni informali alle nostre dimostrazioni.

Elenchiamo qui di seguito altre leggi interessanti, che sono poi quelle più utili in pratica.

(Interv)

Sia [a,b] un intervallo non vuoto di naturali e sia $k \in [a,b]$.

$$(\mathbf{\Sigma}x: x \in [a,b] \wedge P.E) = \begin{cases} (\Sigma x : x \in [a,b) \wedge x \neq k \wedge P.E) + E_x^k & \text{se } P_x^k \\ (\Sigma x : x \in [a,b) \wedge x \neq k \wedge P.E) & \text{se} \sim P_x^k \end{cases}$$

$$\#\{x \in [a,b] \mid P\} = \begin{cases} \#\{x \in [a,b) \mid x \neq k \wedge P\} + 1 & \text{se } P_x^k \\ \#\{x \in [a,b) \mid x \neq k \wedge P\} & \text{se} \sim P_x^k \end{cases}$$

$$(\mathbf{m}\ x{:}x\in[a,b]\wedge P.E)=\begin{cases}(\mathbf{m}\ x : x\in[a,b)\wedge x\neq k\wedge P.E)\ m\ E_x^k & \text{se } P_x^k\\ (\mathbf{m}\ x : x\in[a,b)\wedge x\neq k\wedge P.E) & \text{se} \sim P_x^k\end{cases}$$

Dimostriamo, a titolo d'esempio, la prima legge, ovvero:

$P_x^k \Rightarrow ((\mathbf{\Sigma}x: x\in[a,b]\wedge P.E) = ((\mathbf{\Sigma}x: x\in[a,b]\wedge x\neq k\wedge P.E) + E_x^k))$

utilizzando le ipotesi date ([a,b] non vuoto e $k\in[a,b]$). Abbiamo allora:

$(\mathbf{\Sigma}x: x\in[a,b]\wedge P.E)$

$=$ {Terzo escluso, Zero}

$(\mathbf{\Sigma}x: x\in[a,b]\wedge (x=k\vee x\neq k)\wedge P.E)$

$=$ {Distributività}

$\mathbf{\Sigma}x: (x\in[a,b]\wedge x=k\wedge P)\vee(x\in[a,b]\wedge x\neq k\wedge P).E$

$=$ {Dominio}

$(\mathbf{\Sigma}x: x\in[a,b]\wedge x=k\wedge P.E) +$

$(\mathbf{\Sigma}x: x\in[a,b]\wedge x\neq k\wedge P.E) -$

$(\mathbf{\Sigma}x: x\in[a,b)\wedge x=k\wedge x\neq k\wedge P.E)$

$=$ {Contraddizione, Vuoto}

$(\mathbf{\Sigma}x: x\in[a,b]\wedge x=k\wedge P.E) +$

$(\mathbf{\Sigma}x: x\in[a,b]\wedge x\neq k\wedge P.E)$

$=$ {Leibniz}

$(\mathbf{\Sigma}x: k\in[a,b]\wedge x=k\wedge P_x^k.E) +$

$(\mathbf{\Sigma}x: x\in[a,b]\wedge x\neq k\wedge P.E)$

$=$ {**Ip**: $k\in[a,b]\wedge P_x^k$}

$(\mathbf{\Sigma}x: x=k.E) + (\mathbf{\Sigma}x: x\in[a,b]\wedge x\neq k\wedge P.E)$

$=$ {Singoletto}

$(\mathbf{\Sigma}x: x\in[a,b]\wedge x\neq k\wedge P.E) + E_x^k$

Le leggi precedenti si riducono ad una forma semplificata nel caso in cui k sia uno dei due estremi dell'intervallo: vediamo tali leggi semplificate quando k=b (leggi analoghe, che lasciamo per **esercizio**, si ottengono per k=a).

Sia [a,b] un intervallo non vuoto di naturali. (Interv)

$$(\mathbf{\Sigma}x{:}x\in[a,b] \wedge P.\ E) = \begin{cases} (\Sigma x : x \in [a,b) \wedge x \neq k \wedge P.E) + E_x^b & \text{se } P_x^b \\ (\Sigma x : x \in [a,b) \wedge x \neq k \wedge P.E) & \text{se} \sim P_x^b \end{cases}$$

$$\#\{x\in[a,b] \mid P\} = \begin{cases} \#\{x \in [a,b) \mid P\} + 1 & \text{se } P_x^b \\ \#\{x \in [a,b) \mid P.E\} & \text{se} \sim P_x^b \end{cases}$$

$$(\mathbf{m}\ x{:}x\in[a,b]\wedge P.E) = \begin{cases} (\mathbf{m}\ x : x \in [a,b) \wedge x \neq k \wedge P.E)\ m\ E_x^b & \text{se } P_x^b \\ (\mathbf{m}\ x : x \in [a,b) \wedge x \neq k \wedge P.E) & \text{se} \sim P_x^b \end{cases}$$

Le leggi (Interv) si riducono alla forma seguente nel caso in cui P sia equivalente a **T**.

(Interv)

Sia [a,b] un intervallo non vuoto di naturali e sia $k\in[a,b]$.

$(\mathbf{\Sigma}x\in[a,b].\ E) = (\mathbf{\Sigma}x{:}\ x\in[a,b] \wedge x\neq k.\ E) + E_x^k$
$\#\{x \mid x\in[a,b]\} = \#\{x \mid x\in[a,b] \wedge x\neq k\} + 1$
$(\mathbf{m}\ x{:}x\in[a,b].\ E) = (\mathbf{m}\ x{:}\ x\in[a,b] \wedge x\neq k.\ E)\ m\ \ E_x^k$

Vediamo un semplice esempio di dimostrazione che coinvolge le leggi appena viste. Sia pari(x) un predicato che vale se e soltanto se x è un numero pari. Dimostriamo allora:

$s = (\mathbf{\Sigma}x{:}\ x\in[1,\ 3] \wedge \text{pari}(x)\ .\ x^2) \equiv s = 4$

$s = (\mathbf{\Sigma}x{:}\ x\in\ [1,\ 3] \wedge \text{pari}(x)\ .\ x^2)$
$\equiv$ {Interv, $1\in[1,3]$, ~pari(1), def. di intervallo}
$s = (\mathbf{\Sigma}x{:}\ x\in[2,\ 3] \wedge \text{pari}(x)\ .\ x^2)$

$\equiv$ {Interv, $3 \in [2,3]$, $\sim$pari(3), def. di intervallo}

$s = (\mathbf{\Sigma} x: x \in [2, 2] \wedge \text{pari}(x) \,.\, x^2)$

$\equiv$ {Interv, $2 \in [2, 2]$, pari(2), def. di intervallo}

$s = (\mathbf{\Sigma} x: x \in (2, 2] \wedge \text{pari}(x) \,.\, x^2) + 4$

$\equiv$ {(2,2] vuoto, Vuoto}

$s = 0 + 4$

$\equiv$ {calcolo}

$s = 4$

Come il lettore avrà certamente intuito, gli intervalli di numeri naturali rivestono per noi un'importanza particolare. Per questo, elenchiamo altre leggi che consentono di manipolare agevolmente formule i cui domini coinvolgono appunto intervalli.

Sia [a,b) un intervallo non vuoto di naturali.

(#:$\forall$)

$\#\{x \in [a, b) \mid P\} = 0 \equiv (\forall x \in [a,b).\ \sim P)$

(#:$\exists$)

$\#\{x \in [a, b) \mid P\} > 0 \equiv (\exists x \in [a,b).\ P)$

(**max**:$\forall$)

$(\forall x \in [a,b).\ \sim P) \Rightarrow (\mathbf{max}\{x \in [a,b) \mid P\} = -\infty)$

(**max**:$\exists$)

$(\exists x \in [a,b).\ P) \Rightarrow \mathbf{max}\{x \in [a,b) \mid P\} \in [a,b)$

$(\exists x \in [a,b).\ P) \Rightarrow (\ m = \mathbf{max}\{x \in [a,b) \mid P\} \equiv$
$(m \in [a,b) \wedge P^{\,m}_{x} \wedge (\forall x \in (m,b).\ \sim P))\ )$

(**min**:$\forall$)

$(\forall x \in [a,b).\ \sim P) \Rightarrow (\mathbf{min}\{x \in [a,b) \mid P\} = +\infty)$

(**min**:$\exists$)

$(\exists x \in [a,b).\ P) \Rightarrow \mathbf{min}\{x \in [a,b) \mid P\} \in [a,b)$

$(\exists x \in [a,b).\ P) \Rightarrow (\ m = \mathbf{min}\{x \in [a,b) \mid P\} \equiv$
$(m \in [a,b) \wedge P^{\,m}_{x} \wedge (\forall x \in [a,\ m).\ \sim P))\ )$

Concludiamo riportando due esempi di dimostrazioni che coinvolgono

i quantificatori introdotti.

Esempi

1. Sia [a, b) un intervallo non vuoto di naturali. Dimostriamo allora:

$(\exists x \in [a,b).\ P) \Rightarrow (b\ max\ \mathbf{min}\{x \in [a,b) \mid P\}) = b.$

Per convenienza di notazione, assumiamo $m = \mathbf{min}\{x \in [a,b) \mid P\}$.
Abbiamo allora:

$(\exists x \in [a,b).\ P)$
$\Rightarrow$ {**min**:$\exists$}
$m \in [a,b)$
$\equiv$ {def. di intervallo}
$a \leq m \wedge m < b$
$\Rightarrow$ {Sempl.-$\wedge$}
$m < b$
$\Rightarrow$ {def. di *max*}
$(b\ max\ m) = b$
$\equiv$ {$m = \mathbf{min}\{x \in [a,b) \mid P\}$}
$(b\ max\ \mathbf{min}\{x \in [a,b) \mid P\}) = b$

2. Supponendo:

$x = (\mathbf{max}\ j : j < N+1.\ (\mathbf{max}\ i : R(i, j).\ i*j))$ (Ip1)
$y = (\mathbf{max}\ i : R(i, N+1).\ i*(N+1))$ (Ip2)

dove N è un numero naturale e R un predicato binario, si vuole calcolare un'espressione priva di quantificatori ed equivalente a:

$(\mathbf{max}\ j : j \leq N+1.\ (\mathbf{max}\ i : R(i, j).\ i*j)).$
$(\mathbf{max}\ j : j \leq N+1.\ (\mathbf{max}\ i : R(i, j).\ i*j))$
$=$ {definizione di $\leq$}
$(\mathbf{max}\ j : j<N+1 \vee j=N+1.\ (\mathbf{max}\ i : R(i, j).\ i*j))$
$=$ {Dominio}
$(\mathbf{max}\ j : j<N+1.\ (\mathbf{max}\ i : R(i, j).\ i*j))\ max$
$(\mathbf{max}\ j : j=N+1.\ (\mathbf{max}\ i : R(i, j).\ i*j))$
$=$ {**Ip**: Ip1}
$x\ max\ (\mathbf{max}\ j : j=N+1.\ (\mathbf{max}\ i : R(i, j).\ i*j))$

= {Singoletto}
x *max* (**max** i: R(i, N+1). i*(N+1))
= {**Ip**: Ip2}
x *max* y

Esercizi

1. Si dimostri la seguente legge, dove I è un intervallo e k un numero naturale: $\sim(k \in I) \Rightarrow (x \in I \wedge x \neq k \equiv x \in I)$
2. Si enuncino le leggi (Interv) relative agli altri tipi di intervallo.
3. Si dimostrino le leggi (Interv).
4. Dimostrare che

   $k = \mathbf{min}\{x \in [a,b) \mid P\} \wedge k \in [a,b) \Rightarrow (\forall x \in [a, k).\ \sim P)$

   assumendo [a, b) non vuoto.
4. Dimostrare che

   $((\mathbf{min}\{x \in [0,N) \mid P\}\ \mathit{min}\ N) \neq N) \equiv (\exists x \in [0,N).\ P)$

   dove N è un numero naturale.

3. Specifiche

Siamo finalmente arrivati al termine della nostra fatica: il calcolo formale per la specifica e la derivazione di programmi che volevamo introdurre può dirsi completo. In quest'ultimo paragrafo mostreremo, per via d'esempi, come varie situazioni di stati e programmi possono essere formalizzate con il bagaglio di notazioni viste sin qui. Su queste formule non si effettueranno ancora calcoli, lo scopo di questo paragrafo essendo di guidare ad esprimere con scioltezza, in modo formale, stati e specifiche di programmi. Lo studente è invitato a cercare da solo la formalizzazione di ogni asserto, confrontando solo successivamente quello che ha determinato con la nostra proposta (quasi mai l'unica possibile, per altro). In tutto questo paragrafo supporremo che l'universo in cui i termini assumono significato sia l'insieme dei numeri naturali (che designeremo con $\mathbb{N}$)[7].

• x divide y.

$$(\exists z.y=z*x)$$

È utile introdurre un predicato Divide che corrisponda a questa formula, in modo da poterlo usare in seguito.

$$\text{Divide}(x,y) \equiv (\exists z.y=z*x)$$

Si noti che il predicato è binario (a due argomenti), essendo due le variabili libere in $(\exists z.y=z*x)$.

• x è pari.

$$\text{Pari}(x) \equiv \text{Divide}(2,x)$$

• x è il massimo comun divisore tra y e z (x è il massimo comun divisore tra y e z se x è un divisore sia di y che di z ed inoltre è il massimo naturale che divide entrambi).

$$\text{MCD}(x,y,z) \equiv \text{Divide}(x,y) \wedge \text{Divide}(x,z) \wedge (\forall w.\text{Divide}(w,y) \wedge \text{Divide}(w,z) \Rightarrow w \leq x)$$

Si osservi come la sottoformula quantificata esprima la proprietà che x

[7] Per noi $0 \in \mathbb{N}$.

è "il massimo che divide sia y che z". Alternativamente, potevamo usare il quantificatore **max** ed un'uguaglianza:

$$MCD(x,y,z) \equiv$$
$$x = \mathbf{max}\ \{w \mid Divide(w,y) \wedge Divide(w,z)\}$$ [8]

• x è un numero primo.

$$Primo(x) \equiv (\forall w.Divide(w,x) \Rightarrow w=x \vee w=1)$$

• Tutti i numeri primi maggiori di 2 sono dispari.

$$(\forall w.Primo(w) \wedge w>2 \Rightarrow \sim Pari(w))$$

Si osservi come la frase "tutti i primi maggiori di due sono…" sia stata resa con una quantificazione ed un'implicazione ($\forall w.Primo(w) \wedge w>2 \Rightarrow \ldots$). Facendo uso dei dominî (paragrafo 8.3), possiamo scrivere, equivalentemente

$$(\forall w{:}Primo(w) \wedge w>2\ .\ \sim Pari(x)) \qquad (*)$$

Osserviamo, infine, come in quest'esempio si ottenga una formula chiusa, mentre nei precedenti i predicati definiti dipendevano tutti da variabili libere; così, mentre la verità di Primo(x) o di Divide(x,y) dipende da specifici valori associati ad x ed y nello stato corrente, la verità o la falsità di (*) dipende esclusivamente dalla struttura del nostro universo (nel nostro universo $\mathbb{N}$ (*) è una formula vera).

• Esiste un numero primo compreso tra 20 e 30.

$$(\exists x.Primo(x) \wedge x \in [20,30])$$

Anche qui, come nell'esempio precedente ma con il quantificatore esistenziale, abbiamo un asserto del tipo "esiste un numero primo tale che…" che viene resa con "$\exists x.Primo(x) \wedge \ldots$). Utilizzando i domini, possiamo alternativamente scrivere:

$$(\exists x{:}x \in [20,30].Primo(x)) \quad \text{oppure} \quad (\exists x{:}Primo(x).x \in [20,30]).$$

• Non esiste un numero maggiore di tutti gli altri.

---

[8] Si ricordi che, per definizione:
max {w | Divide(w,y)∧Divide(w,z)} ≅ (**max** w : Divide(w,y)∧Divide(w,z).w).

Ancora un esempio di formula chiusa:

$\sim(\exists x.(\forall y.\ x>y))$

• p è **T** se x è pari; **F** altrimenti.

$p \equiv Pari(x)$.

• Se x è pari, allora y è 91, altrimenti y è 100.

Questo è un caso abbastanza importante che viene formalizzato come

$(Pari(x) \Rightarrow y=91) \wedge (\sim Pari(x) \Rightarrow y=100)$

od anche come

$(Pari(x) \wedge y=91) \vee (\sim Pari(x) \wedge y=100)$

grazie alla tautologia $(p \Rightarrow q) \wedge (\sim p \Rightarrow r) \equiv (p \wedge q) \vee (\sim p \wedge r)$.

Ma osserviamo che le seguenti formalizzazioni sono scorrette:

$(Pari(x) \wedge y=91) \vee\ y=100$ NO!

$(Pari(x) \Rightarrow y=91) \wedge y=100$ NO!

$(Pari(x) \Rightarrow y=91) \vee (\sim Pari(x) \Rightarrow y=100)$ NO!

La prima formula, infatti, è vera anche quando x è pari e y è 100; la seconda è falsa quando x è pari e y è 91; la terza è vera quando x è pari e y è 100.

• Se x è uguale a b allora per tutti gli elementi compresi tra a e b (b escluso) il predicato P è falso (dando per scontato che a<b).

$x=b \Rightarrow (\forall w \in [a,b).\ \sim P(w))$

od anche, sfruttando una delle abbreviazioni introdotte,

$x=b \Rightarrow (\forall w \in [a,b).\sim P(w))$.

• Se x è uguale a b allora per tutti gli elementi compresi tra a e b (b escluso) il predicato P è falso; altrimenti, esiste un valore compreso tra a e b (b escluso) per cui il predicato P è vero (dando per scontato che a<b).

$x=b \equiv (\forall w.w \in [a,b) \Rightarrow \sim P(w))$.

• z è uguale al più piccolo tra x ed y.

$z = x \mathit{min} y$

Se non volessimo usare l'operatore *min*, potremmo scrivere

$(x \leq y \Rightarrow z=x) \wedge (y \leq x \Rightarrow z=y)$.

• b è uguale a 1, 2 o 3 a seconda che il minimo tra x, y e z sia rispettivamente x, y o z.

$(x \mathit{min} y \ \mathit{min} z)$[9]$=x \Rightarrow b=1) \wedge (x \mathit{min} y \ \mathit{min} z)=y \Rightarrow b=2)$

$\wedge (x \mathit{min} y \ \mathit{min} z)=z \Rightarrow b=3)$.

• x è uguale alla somma di tutti i numeri primi minori di 100.

$x = (\sum y:\text{Primo}(y) \wedge y<100.y)$.

• x è un numero perfetto (un numero naturale si dice *perfetto* se è uguale alla somma dei suoi divisori, eccetto se stesso).

$x = (\sum y:\text{Divide}(y,x) \wedge y \neq x.y)$.

• x è uguale alla somma dei quadrati dei naturali minori di 10.

$x = (\sum y:y<10.y^2)$

od anche, con una variante di notazione,

$x = (\sum y \in [0,10).y^2)$

o ancora

$$x = \sum_{y=0}^{9} y^2 .$$

• x è il numero dei primi minori di 100.

Le seguenti sono tutte formulazioni equivalenti (perché?)

$x = \#\{y \mid \text{Primo}(y) \wedge y<100\}$

$x = \#\{y:\text{Primo}(y) \mid y<100\}$

$x = \#\{y:y<100 \mid \text{Primo}(y)\}$

• x è il numero dei divisori di y.

$x = \#\{z \mid \text{Divide}(z,y)\}$.

---

9 Si ricordi che *min* è associativo.

• x è un numero primo (variante).

$\#\{ z \mid Divide(z,x) \} = 2$.

• x è il più piccolo dei divisori di y che sia maggiore di 10.

$x = (\mathbf{min}\ z : Divide(z,y) \wedge z>10.z)$

od anche

$x = \mathbf{min}\ \{z \mid Divide(z,y) \wedge z>10\}$.

• x è il massimo tra tutti i quadrati dei numeri minori di 100.

$x = (\mathbf{max}\ y : y<100.\ y^2)$

od anche

$x = \mathbf{max}\ \{y^2 \mid y<100\}$

(ovviamente, sapendo che il quadrato è una funzione monotona crescente, potevamo direttamente esprimere l'asserto come $x = 99^2$).

Esercizi

1. Tutti i multipli di 4 sono pari.
2. k è la minima potenza di 2 che supera n.
3. Il doppio di ogni numero è pari.
4. x è uguale alla somma di due numeri primi.
5. z è minore del minimo tra x e y.
6. A è il massimo numero il cui quadrato è minore o uguale a n.
7. La somma dei primi n interi è maggiore di n.
8. x divide la somma dei naturali minori di 20.
9. y è uguale al massimo dei divisori di x, eccettuato x.
10. Se x è perfetto, y è il massimo dei suoi divisori (eccettuato x); altrimenti y è zero.
11. Se a è maggiore di b, x è il numero dei primi compresi tra a e b; altrimenti è il numero dei primi compresi tra b e a.

10.1 Sequenze

Particolare importanza per i nostri scopi assumono asserti che coinvolgono *sequenze* di valori, cioè valori che si ottengono al variare

di un opportuno *indice*. Seguendo l'usuale notazione introdotta a questo scopo dai linguaggi di programmazione, indichiamo una sequenza di nome a di n naturali con indici da 0 a n-1 con

a : **array** [0,n) **of nat**

(l'usuale modo di scriverla in matematica sarebbe stato $\underline{a} = (a_0, a_1,\ldots,a_{n-1})$). Un elemento di questa sequenza, ad esempio quello di indice i, sarà denotato con a[i]. L'intervallo [0,n) è detto *dominio* di a (notazione: *dom* a = [0,n)). Gli esempi seguenti formalizzano asserti relativi a sequenze; in essi assumiamo sempre a,b : **array** [0,n) **of nat**.

• Le sequenze a e b sono uguali.

$(\forall i \in [0,n).a[i]=b[i]))$.

• La sequenza a è crescente.

$(\forall i \in [0,n).(\forall j \in [i+1,n).a[i]<a[j]))$

od anche, in virtù delle abbreviazioni introdotte,

$(\forall i,j \in [0,n).\ i<j \Rightarrow a[i]<a[j])$

• x è uguale al minimo valore della sequenza a.

x = (**min** i:i∈[0,n).a[i])

Utilizzando le abbreviazioni introdotte per gli intervalli, scriveremo, in modo più compatto,

x = (**min** i∈[0,n).a[i])

• v è uguale alla minima differenza, in valore assoluto, tra due elementi successivi della sequenza a.

v = (**min** i∈[0,n-1) . | a[i] - a[i+1] |)

Si osservi che il dominio del quantificatore è [0,n-1), in modo da garantire che l'espressione | a[i]–a[i+1] | sia sempre definita (se, infatti, i potesse variare in [0,n), per i uguale a n-1, a[i+1] non sarebbe definito, in quanto *dom* a = [0,n)).

• Ogni elemento a[j] della sequenza a è uguale alla somma degli

elementi della sequenza b con indice minore o uguale a j.

$$(\forall j \in [0, n) \,.\, a[j] = \sum_{i=0}^{j} b[j]\,).$$

• x è uguale alla somma degli elementi di a con indice pari e minore di k (supposto $k \in [0,n]$).

$$x = (\sum i.\ i \in [0,k) \wedge \text{Pari}(i) \,.\, a[i])$$

• v è **T** se e solo se la sequenza a è simmetrica rispetto al suo punto centrale, cioè il suo primo elemento è uguale all'ultimo, il secondo uguale al penultimo e così via.

$$v \equiv (\forall j \in [0, n \textbf{ div } 2) \,.\, a[j]=a[n-j-1])$$[10].

Si osservi attentamente come la formula proposta comprenda sia il caso in cui n è pari, sia quello in cui n è dispari.

• Il valore di ogni elemento, b[i], di b è il numero degli elementi di a il cui valore è i.

$$(\forall i \in [0,n).\ b[i] = \#\{j \in [0,n) \mid a[j]=i\})$$

• x è uguale alla maggioranza di a (che esiste per ipotesi) (un valore v si dice la *maggioranza* di una sequenza a con dominio [0,n) se almeno (n **div** 2) elementi di a sono uguali a v; si osservi che la maggioranza non esiste per ogni sequenza, ma quando esiste è unica).

$$\#\{i \in [0,n) \mid a[i]=x\} \geq (n \textbf{ div } 2).$$

Vediamo ora un esempio di dimostrazione che coinvolge le sequenze. Dimostriamo la seguente proprietà:

$$(\forall x: x \in [0,N) \wedge x \neq k.\ a[x]=2) \Rightarrow (\quad (\forall x: x \in [0,N).\ a[x]=2) \vee (k \in [0, N) \wedge a[k] \neq 2)\ ).$$

La dimostrazione è fatta per casi: detta R la formula precedente, dimostriamo cioè separatamente $S \Rightarrow R$ e $\sim S \Rightarrow R$, dove S è la formula

---

10 L'operatore **div** denota la divisione intera; una notazione alternativa per (x **div** y) è $\lfloor x/y \rfloor$.

$(k \in [0, N) \wedge a[k] = 2)$.

$(\forall x: x \in [0, N).\ a[x]=2)$

$\equiv$ {**Ip**: $(k \in [0, N)$
$P^{k,x} \Rightarrow (\forall x:P.\ Q) \equiv (\forall x:P \wedge x \neq k.\ Q)$ }

$(\forall x: x \in [0,N) \wedge x \neq k.\ a[x]=2) \wedge a[k]=2$

$\equiv$ {**Ip**: $a[k] = 2$}

$(\forall x: x \in [0,N) \wedge x \neq k.\ a[x]=2)$

Vediamo ora il secondo caso: osserviamo innanzitutto che ci troviamo a dover dimostrare una formula del tipo

$\sim(k \in [0,N) \vee a[k] \neq 2) \Rightarrow \ldots\ldots$

che, per una delle leggi di complemento, è equivalente a

$\sim(k \in [0,N) \vee (k \in [0,N) \wedge a[k] \neq 2) \Rightarrow \ldots\ldots$

Ora, facendo appello a una delle leggi Sempl.Sinistra-$\Rightarrow$, possiamo dimostrare separatamente

$\sim(k \in [0,N)) \Rightarrow \ldots\ldots$ e $(k \in [0,N) \wedge a[k] \neq 2) \Rightarrow \ldots\ldots$

$(\forall x: x \in [0,N) \wedge x \neq k.\ a[x]=2)$

$\equiv$ {**Ip**: $\sim(k \in [0,N)$,
$\sim P^{k,x} \Rightarrow (\forall x:P.\ Q) \equiv (\forall x:P \wedge x \neq k.\ Q)$ }

$(\forall x: x \in [0,N).\ a[x]=2)$

$\Rightarrow$ {Intro-$\vee$}

$(\forall x: x \in [0,N).\ a[x]=2) \vee (k \in [0, N) \wedge a[k] \neq 2)$

Abbiamo infine:

$(\forall x: x \in [0,N).\ a[x]=2) \vee (k \in [0, N) \wedge a[k] \neq 2)$

$\Leftarrow$ {Intro-$\vee$ }

$(k \in [0, N) \wedge a[k] \neq 2)$

$\Leftarrow$ {Sempl-$\wedge$}

$(\forall x: x \in [0,N) \wedge x \neq k.\ a[x]=2) \wedge (k \in [0, N) \wedge a[k] \neq 2)$

$\equiv$ {**Ip**: $(k \in [0, N) \wedge a[k] \neq 2)$}

$(\forall x: x \in [0,N) \wedge x \neq k.\ a[x]=2)$

Esercizi

1. v è uguale al massimo della differenza in valore assoluto tra due qualsiasi elementi distinti della sequenza a.
2. La sequenza b è la sequenza a "rovesciata".
3. Gli elementi di indice pari della sequenza a sono dispari.
4. Gli elementi di indice pari della sequenza a sono uguali agli elementi con lo stesso indice della sequenza b (nulla è detto sugli elementi ad indice dispari di a).
5. La sequenza a non contiene elementi nulli.
6. Nella sequenza a, se c'e' un valore pari, esso compare con indice dispari.
7. p è **T** se e solo se tutti gli elementi di a sono minori di k.
8. x è il numero di elementi della sequenza a che sono maggiori della somma di quelli che lo precedono (ossia, che hanno indice minore).
9. Si esprima a parole il senso della seguente formula concernente due sequenze a e b:

   $(\forall i \in [0,n): a[i] = b[i - \#\{j \in [1,i] \mid a[j]=a[j-1]\}])$.

10. La sequenza b si ottiene dalla sequenza a ponendo b[i] uguale all'elemento di a con indice i-1 (quando questo esiste) e ponendo l'elemento di b con indice minimo uguale a quello di indice massimo di a (b è lo "*shift* destro" di a).

Appendice

A.1 Sintassi

La seguente grammatica, non ambigua, genera il linguaggio dei predicati con tutte le aggiunte e modifiche che si sono apportate nel corso di queste note. Essa introduce implicitamente, inoltre, le precedenze tra connettivi definite nel paragrafo 3 e l'associatività per $\equiv$, $\wedge$ e $\vee$.

Linguaggio dei Predicati

Fbf ::= Prop | FbfQuant
Prop ::= Impl | Prop ≡ Prop
Impl ::= Giunz | Giunz ⇒ Impl
Giunz ::= And | Or
And ::= Andprim { ∧ Andprim}
Or ::= Orprim { ∨ Orprim}
Andprim ::= Prim | (Or)
Orprim ::= Prim | (And)
Prim ::= Atom | ~Atom
Atom ::= **T** | **F** | Ide | (Prop) | Pred
Term = Term | FbfQuant
Ide ::= p | q | ……
FbfQuant ::= (∀Var:Fbf) | (∃Var:Fbf)
Pred ::= PIde (Term {, Term})
Term ::= Const | Var| FIde (Term {, Term}) |
(ΣVar:Fbf.Term) | #{Var:Fbf|Fbf} |
(**max** Var:Fbf.Term) |
(**min** Var:Fbf.Term) | Exp
Exp::= …
Const ::= 0 | 1 | 2 | …
| +∞ | –∞ | …

Exp è un nonterminale da cui si possono dedurre (almeno) le ordinarie espressioni aritmetiche; Ide, FIde, PIde e Var sono categorie sintattiche disgiunte di identificatori.

A.2 Rassegna delle leggi di base e derivate

A.2.1 Minimo e Massimo

a *m* b = b *m* a	(Commutatività)
a *m* (b *m* c) = (a *m* b) *m* c	(Associatività)
a *m* a = a	(Idempotenza)
a + (b *m* c) = (a+b) *m* (a+c)	(Distributività di + su *m*)
a *max* b ≥ a	(*max*:≥)
a *min* b ≤ a	(*min*:≤)
-a *min* -b = -(a *max* b)	(*min*:*max*)

-a *max* -b = - (a *min* b)	(*max*:*min*)

A.2.2 Calcolo proposizionale

Leggi di Base

$p \equiv p$	(Riflessività)
$(p \equiv q) \equiv (q \equiv p)$	(Simmetria)
$(p \equiv q) \wedge (q \equiv r) \Rightarrow (p \equiv r)$	(Transitività)
$p \vee q \equiv q \vee p$	(Commutatività)
$p \wedge q \equiv q \wedge p$	
$((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$	(Associatività)
$p \vee (q \vee r) \equiv (p \vee q) \vee r$	
$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	
$p \vee p \equiv p$	(Idempotenza)
$p \wedge p \equiv p$	
$(p \equiv \mathbf{T}) \equiv p$	(Unità)
$p \wedge \mathbf{T} \equiv p$	
$p \vee \mathbf{F} \equiv p$	
$p \wedge \mathbf{F} \equiv \mathbf{F}$	(Zero)
$p \vee \mathbf{T} \equiv \mathbf{T}$	
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	(Distributività)
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	
$\sim(\sim p) \equiv p$	(Doppia negazione)
$p \vee \sim p \equiv \mathbf{T}$	(Terzo escluso)
$p \wedge \sim p \equiv \mathbf{F}$	(Contraddizione)
$\sim p \vee \sim q \equiv \sim(p \wedge q)$	(De Morgan)
$\sim p \wedge \sim q \equiv \sim(p \vee q)$	
$\sim\mathbf{T} \equiv \mathbf{F}$	(**T**:**F**)
$\sim\mathbf{F} \equiv \mathbf{T}$	
$(p \Rightarrow q) \equiv (\sim p \vee q)$	(Elim-$\Rightarrow$)
$(p \equiv q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$	(Elim-$\equiv$)
$(p \Leftarrow q) \equiv (q \Rightarrow p)$	(Elim-$\Leftarrow$)

Leggi derivate

$p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$	
$p \wedge (p \vee q) \equiv p$	(Assorbimento)
$p \vee (p \wedge q) \equiv p$	
$p \vee (\sim p \wedge q) \equiv p \vee q$	(Complemento)
$p \wedge (\sim p \vee q) \equiv p \wedge q$	
$(p \wedge (p \Rightarrow q)) \Rightarrow q$	(Modus ponens)
$p \wedge q \Rightarrow p$	(Sempl.-$\wedge$)
$(p \Rightarrow \sim p) \equiv \sim p$	(Riduzione ad assurdo)
$(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p)$	(Controposizione)
$p \wedge q \Rightarrow r \equiv p \wedge \sim r \Rightarrow \sim q$	(Scambio)
$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$	(Transitività-$\Rightarrow$)
$(p \equiv q) \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$	(Elim-$\equiv$-bis)
$p \Rightarrow p \vee q$	(Intro-$\vee$)
$(p \vee q) \wedge \sim p \Rightarrow q$	(Tollendo Ponens)
$((p \Rightarrow q) \wedge \sim q) \Rightarrow \sim p$	(Tollendo Tollens)
$(p \Rightarrow q) \wedge (p \Rightarrow r) \equiv (p \Rightarrow q \wedge r)$	(Sempl.Destra-$\Rightarrow$)
$(p \Rightarrow q) \vee (p \Rightarrow r) \equiv (p \Rightarrow q \vee r)$	
$(p \Rightarrow r) \vee (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r)$	(Sempl.Sinistra-$\Rightarrow$)
$(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q \Rightarrow r)$	
$p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r)$	
$(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow (p \wedge r \Rightarrow q \wedge s)$	(Sempl.-$\Rightarrow$)
$(p \vee q) \wedge (\sim p \vee r) \Rightarrow (q \vee r)$	(Risoluzione)
$(p \vee q) \wedge (p \Rightarrow r) \wedge (q \Rightarrow s) \Rightarrow (r \vee s)$	(Sillogismo disgiuntivo)

A.2.3 Calcolo dei predicati

Leggi di Base

$(\forall x.P) \equiv (\forall y.P^{y,x})$	se y non occorre in P	(Ridenom)
$(\exists x.P) \equiv (\exists y.P^{y,x})$	se y non occorre in P	
$(\forall y.\forall x.P) \equiv (\forall x.\forall y.P)$		(Annidamento)
$(\exists y.\exists x.P) \equiv (\exists x.\exists y.P)$		
$(\forall x.P \wedge Q) \equiv (\forall x.P) \wedge (\forall x.Q)$		$(\forall:\wedge)$
$(\exists x.P \vee Q) \equiv (\exists x.P) \vee (\exists x.Q)$		$(\exists:\vee)$
$(\forall x.Z) \equiv Z$	se x non è libera in Z	(Costante)
$(\exists x.Z) \equiv Z$	se x non è libera in Z	
$(\forall x.P) \vee Z \equiv (\forall x.P \vee Z)$	se x non è libera in Z	(Distrib)
$(\exists x.P) \wedge Z \equiv (\exists x.P \wedge Z)$	se x non è libera in Z	
$(\forall x.P) \Rightarrow P_x^t$	per un generico termine t	(Elim-$\forall$)
$P_x^t \Rightarrow (\exists x.P)$	per un generico termine t	(Intro-$\exists$)
$\sim(\exists x.P) \equiv (\forall x.\sim P)$		(De Morgan)
$\sim(\forall x.P) \equiv (\exists x.\sim P)$		
$x=y \Rightarrow (P \equiv P^{y,x})$		(Leibniz)
$x=y \wedge P \equiv x=y \wedge P^{y,x}$		

Leggi derivate

$(\forall x.\ P \vee Q \Rightarrow R) \equiv (\forall x.P \Rightarrow R) \wedge (\forall x.Q \Rightarrow R)$		(Dominio)
$(\exists x.\ (P \vee Q) \wedge R) \equiv (\exists x.P \wedge R) \vee (\exists x.Q \wedge R)$		
$(\forall x.P) \wedge Z \equiv (\forall x.P \wedge Z)$	se x non è libera in Z	(Distrib)
$(\exists x.P) \vee Z \equiv (\exists x.P \vee Z)$	se x non è libera in Z	
$(\forall x.x=y \Rightarrow P) \equiv P^{y,x}$		(Singoletto)
$(\exists x.x=y \wedge P) \equiv P^{y,x}$		
$(\forall x.\mathbf{T})$		
$\sim(\exists x.\mathbf{F})$		
$(\forall x.P) \vee (\forall x.Q) \Rightarrow (\forall x.P \vee Q)$		
$(\exists x.P \wedge Q) \Rightarrow (\exists x.P) \wedge (\exists x.Q)$		
$(\forall x.P) \Rightarrow (\forall x.P \vee Q)$		(Indebolimento:$\vee$)
$(\exists x.P) \Rightarrow (\exists x.P \vee Q)$		
$(\exists x.P \wedge Q) \Rightarrow (\exists x.P)$		(Indebolimento:$\wedge$)
$(\forall x.P \wedge Q) \Rightarrow (\forall x.P)$		

Abbreviazioni

$(\forall x, y.\ P) \cong (\forall x.\ (\forall y.\ P))$
$(\exists x, y.\ P) \cong (\exists x.\ (\exists y.\ P))$
$(\forall x_1,\ldots,x_n, y.\ P) \cong (\forall x_1,\ldots,x_n.\ (\forall y.\ P))$ $n\geq 1$
$(\exists x_1,\ldots,x_n, y.\ P) \cong (\exists x_1,\ldots,x_n.\ (\exists y.\ P))$ $n\geq 1$

$[a, b] \cong \{x \mid a\leq x\leq b\}$ (Intervalli)
$[a, b) \cong \{x \mid a\leq x<b\}$
$(a, b] \cong \{x \mid a<x\leq b\}$
$(a, b) \cong \{x \mid a<x<b\}$

$(\forall x{:}P.Q) \cong (\forall x.P \Rightarrow Q)$ (Dominî)
$(\exists x{:}P.Q) \cong (\exists x.P \wedge Q)$

$(\forall x\in I.Q(x)) \cong (\forall x{:}x\in I.Q(x))$
$(\exists x\in I.Q(x)) \cong (\exists x{:}x\in I.Q(x))$

$(\forall x, y\in I.\ Q) \cong (\forall x\in I.\ (\forall y\in I.\ Q))$
$(\exists x, y\in I.\ Q) \cong (\exists x\in I.\ (\exists y\in I.\ Q))$
$(\forall x_1,\ldots,x_n, y\in I.\ P) \cong (\forall x_1,\ldots,x_n\in I.\ (\forall y\in I.\ P))$ $n\geq 1$
$(\exists x_1,\ldots,x_n, y\in I.\ P) \cong (\exists x_1,\ldots,x_n\in I.\ (\exists y\in I.\ P))$ $n\geq 1$