# Logica per la Programmazione

## Lezione 11

- Logica del Primo Ordine con Quantificatori Funzionali

# Estensione del Primo Ordine con Quantificatori Funzionali

- Abbiamo esteso il linguaggio del primo ordine con
  - notazione intensionale per insiemi
  - simboli di disuguaglianza
  - notazione per intervalli
  - abbiamo introdotto le relative leggi e alcune leggi per le formule con dominio
- Ora aggiungiamo alcuni **"quantificatori funzionali"**
  - minimo/massimo di un insieme di valori
  - sommatoria di un insieme di valori
  - cardinalità di un insieme
  - sono quantificatori funzionali perché restituiscono un valore, non un booleano
  - anche questi concetti saranno utili per la verifica di programmi con Triple di Hoare

# Quantificatore Sommatoria

$$(\Sigma\ x : P(x) \,.\, E(x))$$

- denota "la somma di tutti gli $E(v)$ per i valori $v$ per cui vale $P(v)$"
- quindi, $P(x)$ è una formula (**"dominio della sommatoria"**), $E(x)$ è un termine (un'espressione)
- Esempi:
  - $(\Sigma x : x > 0 \wedge x \leq 3 \,.\, x^2) = 1 + 4 + 9 = 14$
  - $(\Sigma x : x \in [3, 5) \,.\, 2x + 1) =?? = 7 + 9 = 16$
  - $(\Sigma x : x \in [0, 10) \wedge pari(x) \,.\, x) =?? = 0 + 2 + 4 + 6 + 8 = 20$
  - $(\Sigma x : x > 7 \wedge x \in [0, 10) \,.\, 5) =?? = 5 + 5 = 10$
  - $(\Sigma x : \mathbf{F} \,.\, 2x + 5) =?? = 0$

# Quantificatore Cardinalità

$$\#\{x : P(x) \mid Q(x)\}$$

- denota il numero dei valori v per cui valgono sia $P(v)$ che $Q(v)$
- in questo caso sia $P(x)$ e $Q(x)$ sono formule, in particolare $P(x)$ è il dominio
- quindi $\mid$ ha il significato di "$\wedge$"
- Esempi:
  - $\#\{x : x \in [0,10) \mid pari(x)\} = 5$
  - $\#\{x : x \in [0,10) \mid (\exists .y \in \mathbb{N} \wedge y^2 = x)\} = ?? = 4$
  - $\#\{x : \mathbf{T} \mid x^2 \leq x\} = ?? = 2$
  - $\#\{x : \mathbf{F} \mid x \in [3,5) \wedge pari(x)\} = ?? = 0$
- Nota: $\#$ può essere definita mediante $\Sigma$:

$$\#\{x : P \mid Q\} = (\Sigma x : P \wedge Q \,.\, 1) \qquad \text{(Elim-\#)}$$

# Quantificatori per Minimo e Massimo

- Ricordiamo l'ovvia definizione degli operatori binari di massimo e minimo:

$$a \;\mathbf{max}\; b = \begin{cases} a & \text{se } a \geq b \\ b & \text{altrimenti} \end{cases} \qquad a \;\mathbf{min}\; b = \begin{cases} a & \text{se } a \leq b \\ b & \text{altrimenti} \end{cases}$$

- Introduciamo ora i due quantificatori corrispondenti, che denotiamo sempre con **min** e **max**:

$$(\mathbf{max}\; x : P(x) \,.\, E(x))$$

denota il massimo dei valori $E(v)$ per tutti i $v$ per cui vale $P(v)$

$$(\mathbf{min}\; x : P(x) \,.\, E(x))$$

denota denota il minimo dei valori $E(v)$ per tutti i $v$ per cui vale $P(v)$

- $P(x)$ è una formula (il **dominio**), $E(x)$ è un'espressione

# Minimo e Massimo: Esempi

- $(\mathbf{max}\ x : x \in [3, 10) \wedge primo(x) \,.\, x^2) = 7^2 = 49$

*Array a*

| | | | | |
|---|---|---|---|---|
| 45 | 23 | 10 | 16 | 13 |

- $(\mathbf{min}\ i : i \in [0, 5) \,.\, a[i]) = ?? = 10$
- $(\mathbf{max}\ i : i \in [0, 5) \wedge primo(a[i]) \,.\, a[i]) = ?? = 23$
- $(\mathbf{min}\ i : i \in [0, 5) \wedge primo(a[i]) \,.\, i) = ?? = 1$

# Sintassi del Primo Ordine con Quantificatori Funzionali

- Estendiamo le categorie sintattiche di termini, costanti ed espressioni con la sintassi vista:

$$
\begin{array}{lcl}
\mathit{Term} & ::= & \ldots \mid (\Sigma\ \mathit{Var} : \mathit{Fbf} \,.\, \mathit{Term}) \mid \#\{\mathit{Var} : \mathit{Fbf} \mid \mathit{Fbf}\} \mid \\
 & & (\mathbf{max}\ \mathit{Var} : \mathit{Fbf} \,.\, \mathit{Term}) \mid (\mathbf{min}\ \mathit{Var} : \mathit{Fbf} \,.\, \mathit{Term}) \mid \mathit{Exp} \\
\mathit{Const} & ::= & 0 \mid 1 \mid 2 \mid \ldots \mid +\infty \mid -\infty \\
\mathit{Exp} & ::= & \text{ordinarie espressioni aritmetiche}
\end{array}
$$

- $x$ occorre **legata** in

$$(\Sigma x : P \,.\, E), \quad \#\{x : P \mid Q\}, \quad (\mathbf{max}\ x : P \,.\, E), \quad (\mathbf{min}\ x : P \,.\, E)$$

# Leggi per i Quantificatori Funzionali

- I quantificatori funzionali, introdotti come estensione della Logica dei Predicati, possono essere definiti nella logica estesa con i naturali.
- Nella dispensa [LP2] "Logica per la Programmazione: Applicazioni" sono riportate numerose leggi che descrivono loro proprietà.
- Molte di queste descrivono proprietà abbastanza ovvie: ne vediamo velocemente alcune.
- Altre sono molto importanti per la parte del corso su Triple di Hoare, e le vediamo in dettaglio.
- Come al solito, le leggi sono dimostrabili usando le definizioni e/o altre leggi.

# Leggi Generali (come per le normali Quantificazioni)

- **Legge di ridenominazione**
  ad esempio
  $$(\Sigma x : P \,.\, E) = (\Sigma y : P[y/x] \,.\, E[y/x])$$
  se $y$ non occorre né in $P$ né in $E$
- **Legge di annidamento**
  ad esempio
  $$(\Sigma y : R \,.\, (\Sigma x : S \,.\, P)) = (\Sigma x : S \,.\, (\Sigma y : R \,.\, P))$$
  se $y$ non è libero in $S$ e $x$ non è libero in $R$

# Leggi Specifiche

- **(min:max)**
  - $(\mathbf{min}\ x : P . -E) = -(\mathbf{max}\ x : P . E)$
- Dominio equivalente (analogamente per gli altri quantificatori):
  - $(\forall x . P \equiv Q) \Rightarrow \#\{x : P \mid R\} = \#\{x : Q \mid R\}$ $(\# :\equiv)$
- Inclusione di Dominio:
  - $(\forall x . P \Rightarrow Q) \Rightarrow (\mathbf{min}\ x : P . E) \geq (\mathbf{min}\ x : Q E)$ $(min :\Rightarrow)$
  - $(\forall x . P \Rightarrow Q) \Rightarrow (\mathbf{max}\ x : P . E) \leq (\mathbf{max}\ x : Q . E)$ $(max :\Rightarrow)$
  - $(\forall x . P \Rightarrow Q) \Rightarrow \#\{x : P \mid R\} \leq \#\{x : Q \mid R\}$ $(\# :\Rightarrow)$
  - $(\forall x . (E \geq 0) \wedge (P \Rightarrow Q)) \Rightarrow (\Sigma x : P . E) \leq (\Sigma x : Q . E)$ $(\Sigma :\Rightarrow)$
  - $(\forall x . (E \leq 0) \wedge (P \Rightarrow Q)) \Rightarrow (\Sigma x : P . E) \geq (\Sigma x : Q . E)$ $(\Sigma :\Rightarrow)$

# Leggi di Distributività

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

# Costante

- $(\Sigma x : P \,.\, c) = c \times (\Sigma x : P \,.\, 1)$ 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
  dove $\mathbf{m} \in \{\mathbf{min}, \mathbf{max}\}$
- $(\Sigma x : P \,.\, c \times E) = c \times (\Sigma x : P \,.\, E)$ 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

# Leggi di Dominio

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

# Singoletto e Dominio Vuoto

- $$(\Sigma x : x = y \,.\, E) = E[y/x]$$
- $$\#\{x : x = y \mid R\} = \begin{cases} 1 & \text{se } R[y/x] \\ 0 & \text{se } \neg R[y/x] \end{cases}$$
- se $P$ è vuoto
$$(\Sigma x : P \,.\, E) = 0$$
- se $P$ è vuoto
$$\#\{x : P \mid Q\} = 0$$
- se $P$ è vuoto
$$(\mathbf{min}\ x : P \,.\, E) = +\infty$$
- se $P$ è vuoto
$$(\mathbf{max}\ x : P \,.\, E) = -\infty$$

# Leggi dell'Intervallo

Sia $[a, b]$ un intervallo non vuoto di naturali

$$(\Sigma x : x \in [a, b] \wedge P \,.\, E) = \begin{cases} (\Sigma x : x \in [a, b) \wedge P \,.\, E) + E[b/x] & \text{se } P[b/x] \\ (\Sigma x : x \in [a, b) \wedge P \,.\, E) & \text{se } \neg P[b/x] \end{cases}$$

$$\#\{x : x \in [a, b] \mid P\} = \begin{cases} \#\{x : x \in [a, b) \wedge P\} + 1 & \text{se } P[b/x] \\ \#\{x : x \in [a, b) \wedge P\} & \text{se } \neg P[b/x] \end{cases}$$

$$(\mathbf{m}\ x : x \in [a, b] \wedge P \,.\, E) = \begin{cases} (\mathbf{m}\ x : x \in [a, b) \wedge P \,.\, E)\ m\ E[b/x] & \text{se } P[b/x] \\ (\mathbf{m}\ x : x \in [a, b) \wedge P \,.\, E) & \text{se } \neg P[b/x] \end{cases}$$

**Attenzione**: queste leggi sono errate nella dispensa

# Uso di Leggi dell'Intervallo: Esempio

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

$$
\begin{array}{ll}
 & s = (\Sigma x : x \in [1,3] \wedge pari(x) \,.\, x^2) \\
\equiv & \quad \{(\text{Intervallo-}\Sigma),\ \neg pari(3)\} \\
 & s = (\Sigma x : x \in [1,2] \wedge pari(x) \,.\, x^2) \\
\equiv & \quad \{(\text{Intervallo-}\Sigma),\ pari(2)\} \\
 & s = (\Sigma x : x \in [1,1] \wedge pari(x) \,.\, x^2) + 2^2 \\
\equiv & \quad \{(\text{Intervallo-}\Sigma),\ \neg pari(1)\} \\
 & s = (\Sigma x : x \in \emptyset \wedge pari(x) \,.\, x^2) + 2^2 \\
\equiv & \quad \{(\Sigma\text{-vuoto})\} \\
 & s = 0 + 2^2 \\
\equiv & \quad \{\text{calcolo}\} \\
 & s = 4
\end{array}
$$

# Esercizi

Utilizzando le leggi dei quantificatori funzionali, dimostrare le seguenti formule:

- $k = (\mathbf{min}\ x : x \in [a, b) \wedge P\,.\,x) \wedge k \in [a, b) \Rightarrow (\forall x \in [a, k)\,.\,\neg P)$ con $[a, b)$ non vuoto
- $(((\mathbf{min}\ x : x \in [0, N) \wedge P\,.\,x)\ \mathrm{min}\ N) \neq N) \equiv (\exists x \in [0, N)\,.\,P)$ con $N$ numero naturale

# Formalizzazione di Enunciati con Quantificatori Funzionali

Si assuma che le sequenze siano array con dominio $[0, n)$

- $x$ è il Massimo Comun Divisore di y e z (usando il predicato $Divide(x, y) \equiv (\exists z \,.\, y = x * z)$)
- $x$ è un numero **perfetto** (cioè è la somma dei suoi divisori eccetto se stesso)
- la sequenza **a** contiene più numeri pari che numeri dispari
- $x$ è il numero di elementi della sequenza **a** che sono maggiori della somma degli elementi che lo precedono
- $x$ è uguale alla somma dei quadrati degli elementi di **a** con indice pari

# Altri esercizi di Formalizzazione

Si assuma che le sequenze siano array con dominio $[0, n)$

- Nella sequenza $\mathbf{a}$ c'è un solo elemento uguale alla sua posizione
- Gli elementi di indice pari della sequenza $\mathbf{a}$ sono dispari
- Definire il predicato $Palindroma(\mathbf{a})$, che vale $\mathbf{T}$ se e solo la sequenza $\mathbf{a}$ è simmetrica rispetto al suo punto centrale