Università degli Studi di Bologna

Corso di Laurea in Informatica
Esame scritto di LOGICA PER L'INFORMATICA (9/6 CFU)
13/09/2022

Scrivere **nome, cognome, numero di CFU e numero di matricola in alto a destra** in tutti i fogli protocollo. Gli esercizi con un doppio punteggio riportano prima il punteggio nel caso dell'esame da 9 CFU e poi quello nel caso di esame da 6 CFU. Fare attenzione all'esercizio 10 che è diverso a seconda del numero di CFU.

1 (1 punto). Dare la sintassi per le formule della logica proposizionale.

2 (4 punti/6 punti). Considerare le seguenti grammatiche per liste di elementi generati da un non-terminale X, dove ":" è associativo a destra:

$$L \quad ::= \quad [] \mid X : L$$

Data una lista L di numeri, **scrivere** per ricorsione strutturale su L e **testare** sull'esempio qui sotto una funzione $f(L)$ che restituisca la lista di liste $L_1 : \ldots : L_n : []$ t.c.

(a) $L_1 @ \ldots @ L_n = L$ dove "@" è la concatenazione di liste

(b) ogni L_i sia una sequenza non decrescente di lunghezza massima

Esempio: $f(2 : 2 : 1 : 3 : 5 : 2 : []) = (2 : 2 : []) : (1 : 3 : 5 : []) : (2 : []) : []$

È possibile utilizzare funzioni ausiliare definite per ricorsione strutturale e/o passare parametri ausiliari. Nel caso di uso di parametri ausiliari per la funzione principale f, specificare il valore iniziale da passare per risolvere il problema.
Dettagliare la specifica di tutte le funzioni ausiliarie introdotta. Testare ogni funzione ausiliaria su un input di esempio.

3 (5 punti). Dimostrare in teoria assiomatica degli insiemi che

$$\forall A \forall B (A \times B \subseteq B \times A \quad \wedge \quad A \neq \emptyset \quad \wedge \quad B \neq \emptyset \quad \Rightarrow \quad A = B)$$

Prima della dimostrazione riportare l'**enunciato di tutti gli assiomi di teoria degli insiemi che usate nella dimostrazione**.

La dimostrazione deve essere una dimostrazione valida in logica del prim'ordine, ovvero ogni passaggio deve corrispondere a uno o più passaggi di deduzione naturale classica o intuizionista. Preferire una prova intuizionista ove possibile.

4 (1 punto). Dare la definizione di relazione d'ordine.

5 (1 punto). Mostrare il paradosso di Russell per la teoria degli insiemi naive.

6 (1 punto). Dare la definizione di regola localmente corretta per la deduzione naturale.

7 (5 punti). Considerare la seguente implementazione del Crivello di Eratostene:

```
erat L [] = L
erat L (x:l) = IF divl L x THEN erat L l ELSE erat (x:L) l
```

dove

```
divl [] x = ff
divl (n:L) x = n|x || divl L x
```

e $n|x$ se e soltanto se n divide x.

(a) Calcolare `erat [] (2:3:4:5:6:7:[])` mostrando un numero sufficiente di passaggi intermedi

(b) Dimostrare, per induzione strutturale su l, che per ogni L,
se esistono k, n e u t.c.

- $l = [] \vee l = k : (k+1) : \ldots : (k+u) : []$ e
- $L = [] \vee L = p_n : p_{n-1} : \ldots : p_1 : []$ dove p_i indica l'i-esimo numero primo (es. $p_1 = 2, p_2 = 3, p_3 = 5$) e
- se $l \neq []$ e $L \neq []$ allora $p_n < k$ e $\forall j.(p_n < j < k \Rightarrow \exists p \in L.p|j)$

allora esiste un h t.c. `erat L l`$= p_h : p_{h-1} : \ldots : p_1 : []$

Nella prova è possibile utilizzare i seguenti lemmi, oltre alle usuali proprietà aritmetiche:

(a) $\forall L, x. divl\ L\ x\ =\ tt \iff \exists p \in L.p|j$

(b) $$\begin{array}{l} \forall n, j.n = p_j \iff \\ \quad \nexists p \in p_{j-1} : \ldots : p_1 : [].p|p_j \wedge \\ \quad\quad (\forall l.p_{j-1} < l < n \Rightarrow \exists h < j.p_h|l) \end{array}$$

8 (6 punti). Si consideri il seguente ragionamento:

La Francia avrà dei blackout e la Germania l'aiuterà se: 1) l'inverno sarà rigido o 2) non ci saranno blackout in Francia. Se il Nord Stream non riaprirà e l'inverno sarà rigido, allora la Germania non aiuterà la Francia. Quindi Il Nord Stream riaprirà o ci sarà un blackout con un inverno mite.

Verificare la correttezza del ragionamento utilizzando la deduzione naturale per la logica proposizionale. Preferire una prova intuizionista se possibile.

9 (1 punto/2 punti). Considerare il seguente frammento di codice:

```
int x;
int f(int y, int z) {
   int w = z + x;
   return y*w*a;
}
```

Specializzare il codice della funzione `f` ottenendo una funzione `g` dove al parametro formale `y` viene sostituita l'espressione `x+a+w` **mantenendo la semantica del codice**, ovvero, per ogni espression `E`, l'output di `g(E)` e di `f(x+a+w,E)` deve essere lo stesso. Svolgere l'esercizio **minimizzando il numero di ridenominazioni di variabili legate**.

10 (2 punti). **PER CHI SOSTIENE L'ESAME DA 6 CFU**
Dimostrare il seguente teorema usando la deduzione naturale al prim'ordine, preferendo una prova intuizionista a una classica ove possibile. Considerare la somma associativa a destra.

$$\forall x.\forall y.(f(s(x), y) \Rightarrow \exists z.f(x, s(z))) \vdash f(s(s(y)), y) \Rightarrow \exists x.f(y, s(x))$$

10 (5 punti). **PER CHI SOSTIENE L'ESAME DA 9 CFU**
Chiamiamo **premod** una struttura algebrica $(B, A, *, +, 0)$ t.c.

(a) $+ \in A^{A\times A}$, $0 \in A$, $* \in A^{B\times A}$

(b) $b * 0 = 0$ per ogni $b \in B$

(c) $b * (a_1 + a_2) = b * a_1 + b * a_2$ per ogni $b \in B$, $a_1, a_2 \in A$

(d) $a + 0 = 0 + a = a$ per ogni $a \in A$

(e) $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$ per ogni $a_1, a_2, a_3 \in A$

Rispondere alle seguenti domande fornendo risposte ben giustificate (es. con da una dimostrazione o da un controesempio), assumendo che $(B, A, *, +, 0)$ si aun premod:

(1) Che tipo di struttura algebrica è $(A, +, 0)$? È abeliana?

(2) Siano $B' \subseteq B$ e $A' \subseteq A$. $(B', A, *, +, 0)$ è un premod? E $(B, A', *, +, 0)$ lo è?

(3) Quale delle seguenti strutture sono premod?

   i. $(\mathbb{N}, \mathbb{L}, *, @, [])$ dove $\mathbb{L}$ sono liste di numeri naturali, @ è la concatenazione di liste, [] la lista vuota e $n * L = L@ \ldots @L$ dove la concatenazione avviene n volte

   ii. $(\mathbb{N}, \mathbb{L}, \circ, @, [])$ dove $n \circ [m_1, \ldots, m_k] = [n * m_1, \ldots, n * m_k]$

   iii. $(\mathbb{N}, \mathbb{L}, \ddagger, @, [])$ dove $n \ddagger L$ è la lista ottenuta da L cancellando tutte le occorrenze di n

(4) Per un $b \in B$ sia bA definito come $\{b * a \mid a \in A\}$. bA è una sottostruttura di $(A, +, 0)$?

(5) Sia $(A, +, 0)$ un monoide. Un monoide si dice **idempotente** quando per ogni $a \in A$ si ha $a + a = a$. $(A, A, +, +, 0)$ è un premod? Lo è quando $(A, +, 0)$ è idempotente? E quando è idempotente e abeliano?