Fondamenti di Informatica A

Compito 2 – 4/7/2019

Cognome e Nome _____ matr. _____

Domanda 1. Sapendo che inizialmente vale l'asserzione $n \geq 0$, scrivere negli appositi spazi le asserzioni più specifiche che valgano in quel punto, assumendo che tutte le variabili siano di tipo `int` (poiché l'asserzione $n \geq 0$ vale sempre, è possibile ometterla)

```
{ n ≥ 0 }
i = 0;
x = 0;
{ ____________________________________ }
while (i < n) {
      { ____________________________________ }
      x = x + 5;
      { ____________________________________ }
      i = i + 1;
      { ____________________________________ }
}
{ ____________________________________ }
```

Risposta: Il programma calcola $x = 5n$; una invariante del ciclo è $I = \{x = 5i$ **and** $i \leq n\}$

```
{ n ≥ 0 }
i = 0;
x = 0;
```
{ $x = 0$ **and** $i = 0$ } si noti che questa asserzione, unita a $n \geq 0$, implica l'invariante
```
while (i < n) {
      { x = 5i and i < n }
      x = x + 5;
      { x = 5(i + 1) and i < n }
      i = i + 1;
      { x = 5i and i ≤ n }
}
```
{ $x = 5i$ **and** $i \leq n$ **and** $i \geq n$ } che implica $x = 5n$

Domanda 2. Si consideri la seguente dichiarazione di variabili:

```
int a = 1;
int b = 0;
int c = 2;
```

Supponiamo che i valori di tipo int siano rappresentati in complemento a due con $N = 32$ bit. Allora, subito dopo le dichiarazioni precedenti:

- [V] [F] L'espressione `(a && b)` vale zero
- [V] [F] L'espressione `(a & b)` vale zero
- [V] [F] L'espressione `(b || c)` vale zero
- [V] [F] L'espressione `(b | c)` vale zero

Risposte:

- V
- V
- F: vale 1

- F: l'operatore | esegue l'*or* bit-a-bit, quindi il risultato vale 2

Domanda 3. Considerando la rappresentazione in complemento a due di valori interi utilizzando $N = 8$ bit. Allora:

[V] [F] Il numero 01010110_{2C} rappresenta un valore maggiore o uguale a zero

[V] [F] La somma di 01110110_{2C} e 00101101_{2C} genera overflow

[V] [F] 01100011_{2C} rappresenta un valore maggiore di 00110101_{2C}

[V] [F] È possibile rappresentare il valore decimale -103

Risposte:
- V: inizia con '0' quindi rappresenta un valore non negativo
- V: sono due valori positivi, ma la somma con 8 bit risulta 10100011_{2C} che rappresenta un valore negativo.
- V
- V: il minimo valore rappresentabile in complemento a due con 8 bit è -128, quindi -103 è rappresentabile

Domanda 4. Descrivere a parole che cosa è una Macchina di Turing

Domanda 5. Si consideri un sistema di crittografia a chiave pubblica in cui *KA*+ e *KA*- indichino, rispettivamente, le chiavi pubblica e privata di Alice, e *KB*+, *KB*- le chiavi pubblica e privata di Bob. Supponiamo che un intruso (Trudy) conosca, oltre a tutte le chiavi pubbliche, anche la chiave privata *KA*-. Indichiamo con E(*K*, *M*) il messaggio che si ottiene cifrando *M* con la chiave *K*. Nelle domande seguenti con "decifrare il messaggio" si intende la possibilità di individuare *M* conoscendo il messaggio cifrato *M*', le chiavi pubbliche, e la chiave privata *KA*-. Allora:

[V] [F] Trudy è in grado di decifrare il messaggio *M*' = E(*KA*+, E(*KB*+, *M*))

[V] [F] Trudy è in grado di decifrare il messaggio *M*' = E(*KB*-, E(*KA*+, *M*))

[V] [F] Trudy è in grado di decifrare il messaggio *M*' = E(*KB*+, E(*KA*+, *M*))

[V] [F] Trudy è in grado di decifrare il messaggio *M*' = E(*KA*-, E(*KB*+, *M*))

Risposte:
- F: Trudy conosce *KA*-, per cui è in grado di derivare E(*KB*+, *M*). Non conosce però *KB*-, che è richiesto per derivare i.
- V: Trudy è in grado di eliminare lo strato esterno di cifratura, perché conosce (come tutti) la chiave pubblica *KB*+, e in più conosce anche *KA*- che è necessario per ottenere *M*.
- F: Trudy non è in grado di eliminare lo strato esterno di cifratura, perché non conosce la chiave privata *KB*-.
- F: Trudy conosce la chiave pubblica *KA*+ con la quale può eliminare lo strato di cifratura più esterno, ma non conosce *KB*- che è necessario per rimuovere lo strato interno di cifratura.

Domanda 6. Un CD-ROM contenente 600'000'000 Byte di dati viene spedito usando un corriere espresso. Il corriere impiega 10'000 secondi per percorrere una distanza di 100 Km (100'000 m) che separa il mittente e il destinatario. Allora:

[V] [F] La latenza del canale di comunicazione è di 10'000 secondi

[V] [F] La latenza del canale di comunicazione è di 10 metri/secondo

[V] [F] La banda del canale di comunicazione è di 60'000 Byte/secondo

[V] [F] La banda del canale di comunicazione è di 600'000'000 Byte/secondo

Risposte:

- V
- F
- V
- F