Fondamenti di Informatica A

Compito 1 – 4/7/2019

Cognome e Nome _____ matr. _____

Domanda 1. Si consideri la seguente dichiarazione di variabili:

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

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:

- F: vale 1, in quanto per l'operatore di and logico entrambe le variabili hanno valore "vero"
- V: l'operatore & esegue l'*and* bit-a-bit
- F: vale 1
- F: l'operatore | esegue l'*or* bit-a-bit, quindi il risultato vale 2

Domanda 2. Descrivere sinteticamente le componenti dell'architettura di Von Neumann.

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

- [V] [F] Il numero 10010110_{2C} rappresenta un valore positivo
- [V] [F] La somma di 10010110_{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 -312

Risposte:

- F: inizia con '1' quindi rappresenta un valore negativo
- F: la somma di un valore positivo e uno negativo non genera mai overflow in complemento a due
- V
- F: il minimo valore rappresentabile in complemento a due con 8 bit è -128

Domanda 4. Un disco Blu-Ray contenente 20'000'000'000 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 2'000'000 Byte/secondo

[V] [F] La banda del canale di comunicazione è di 20'000'000'000 Byte/secondo

Risposte:
- V
- F
- V
- F

Domanda 5. Sapendo che inizialmente vale l'asserzione n ≥ 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 + 3;
      { ____________________________________ }
      i = i + 1;
      { ____________________________________ }
}
{ ____________________________________ }
```

Risposta: Il programma calcola $x = 3n$; una invariante del ciclo è $I = \{x = 3i$ **and** $i \leq n\}$

```
{ n ≥ 0 }
i = 0;
x = 0;
```
{ x = 0 and i = 0 } si noti che questa asserzione, unita a n ≥ 0, implica l'invariante
```
while (i < n) {
```
{ $x = 3i$ **and** i < n }
```
      x = x + 3;
```
{ $x = 3(i + 1)$ **and** $i < n$ }
```
      i = i + 1;
```
{ $x = 3i$ **and** $i \leq n$ }
```
}
```
{ $x = 3i$ **and** $i \leq n$ **and** $i \geq n$ } che implica $x = 3n$

Domanda 6. 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 *KB*-. 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 *KB*-. 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 non conosce *KA*-, che è necessaria per eliminare lo "strato" di cifratura più esterno
- F: Trudy è in grado di eliminare lo strato esterno di cifratura, perché conosce (come tutti) la chiave pubblica *KB*+, ma non è in grado di eliminare quello più interno perché non conosce *KA*-
- F: Trudy è in grado di eliminare lo strato esterno di cifratura, perché conosce la chiave privata *KB*-, ma non è in grado di eliminare quello più interno perché non conosce *KA*-
- V: Trudy conosce la chiave pubblica *KA*+ con la quale può eliminare lo strato di cifratura più esterno, e conosce *KB*- con la quale può eliminare lo strato di cifratura interno.