Midterm 1 Solutions

November 20, 2012

1

Let us use the following notation:

D: Dweezle can play
C: I will buy the compact disc
J: Jill can sing
P: I will buy the compact disc player

Now, the given propositions are:

(1) $(J \vee D) \rightarrow C$
(2) J
(3) P

Using **Addition** on (2), we get (4) $J \vee D$. Using **Modus ponens** on (1) and (4), we get (5) C. Using **Conjunction** on (5) and (3), we get $C \wedge P$ as a conclusion. Namely, we conclude "I will buy the compact disc and the compact disc player."

2

In resolution refutation, the given propositions and the negation of the conclusion can be represented in clauses as follows:

(1) $\sim J \vee C$

(1') $\sim D \vee C$
(2) J
(3) P
(4) $\sim C \vee \sim P$

Now we should draw a conflict, which can be done in many ways. One example is: from (1) and (2), we get (5) C. From (5) and (4), we get (6) $\sim P$. From (6) and (3) we get contradiction. Therefore the original conclusion $C \wedge P$ is true.

3

We have

$$\begin{aligned} \lambda \in L &\Rightarrow a\lambda b = ab \in L \text{ from(1)} \\ &\Rightarrow aabb \in L \text{ from(1)} \end{aligned}$$

Similarly, $ba \in L$. Now,

$$ba \in L \wedge aabb \in L \Rightarrow baaabb \in L \text{ from(2)}$$

4

(basis) $n = 1$: 3+7-2=8 is divided by 8.
(induction hypothesis) Assume that the proposition holds for $n = k$.
(induction step) Let $n = k + 1$. Then,

$$3^{k+1} + 7^{k+1} - 2 = 3(3^k + 7^k - 2) + 4(7^k + 1)$$

From the induction hypothesis, $3(3^k + 7^k - 2)$ is divisible by 8. Now, we should show $4(7^n + 1)$ is divisible by 2, so it is divisible by 8. Let us use another induction to prove it.

(basis) $n = 1$: $7 + 1 = 32$ is divisible by 8
(induction hypothesis) We assume that the given proposition holds for $n = k$.
(induction step) $n = k + 1$. Then $7^{k+1} + 1 = 7(7^k + 1) - 6$. Since both $7^k + 1$ and 6 are divisible by 2, the conclusion follows.

5

A.
$n = 513$, $\phi = 468$. Since d is inverse modulo of e, we have $ed = 1(mod\phi) \Rightarrow ed + \phi y = 1$. Since e and ϕ are mutually prime, $GCD(e, \phi) = 1$. Namely, we get the GCD of 1 in the Euclid algorithm as follows:

$$GCD(468, 7) = GCD(7, 6) = GCD(6, 1) = 1$$

From the inverse Euclid algorithm, we compute

$$1 = 7 - 1 \cdot 6 = 7 - 1 \cdot (468 - 7 \cdot 66) = 7 \cdot 67 + (-1) \cdot 468$$

Therefore, $d = 67$.
B.

$$c = m^e (mod\ n) = 13^7 (mod\ 513) = 409$$

C.

$$m = c^d (mod\ n) = 17^{67} (mod\ 513)$$

Note that $17^2\ mod\ 513 = 289$, $17^4\ mod\ 513 = (17^2\ mod\ 513)^2\ mod\ 513 = 162$, $17^8\ mod\ 513 = (17^4\ mod\ 513)^2\ mod\ 513 = 81$, $17^{16}\ mod\ 513 = (17^8\ mod\ 513)^2\ mod\ 513 = 405$, $17^{32}\ mod\ 513 = (17^{16}\ mod\ 513)^2\ mod\ 513 = 378$, and $16^{64}\ mod\ 513 = (16^{32}\ mod\ 513)^2\ mod\ 513 = 270$. Therefore,

$m = 17^{67} (mod\, 513) = ((17^{64}\ mod 513)(17^2\ mod\, 513)(17\ mod\, 513))\ mod\, 513 = 405$

6

A. Yes. All main diagonal entries are 1.
B. No. $R_{41} \neq R_{14}$.
C. Yes. $\forall_{i \neq j} R_{ij} \neq R_{ji}$.
D. Yes. All non-zero entries in R^2, have 1 in the corresponding positions in R.
E. Yes. From A, C, D.
F. No. There are incomparable elements, e.g. neither $5R1$ nor $1R5$.
G. No. Because it is not symmetric.

7

A.
The worst case input for the given algorithm is where the the list s is in the non-increasing order.
B.

$$f(n) = 1 + 2 + 3 + \cdots + (n-1) = \frac{n(n-1)}{2}$$

C.
$f(n) = O(n^2)$.
Proof:
$f(n) = 1 + 2 + 3 + \cdots + (n-1) \leq n + n + n + \cdots + n = n(n-1) \leq n^2$
D.
$f(n) = \Omega(n^2)$.
Proof:

$$\begin{aligned}
f(n) &= 1 + 2 + 3 + \cdots + (n-1) \\
&\geq \left\lceil \frac{n-1}{2} \right\rceil + (\left\lceil \frac{n-1}{2} \right\rceil + 1) + (\left\lceil \frac{n-1}{2} \right\rceil + 2) + \cdots + (n-1) \\
&\geq \left\lceil \frac{n-1}{2} \right\rceil + \cdots + \left\lceil \frac{n-1}{2} \right\rceil \\
&= \left(\left\lceil \frac{n-1}{2} \right\rceil \right)^2 \\
&\geq \left(\frac{n-1}{2} \right)^2 \\
&\geq \left(\frac{n^2}{16} \right) \quad \forall n \geq 2
\end{aligned}$$

8

A. No. $P(A \cap B) = 0 \neq 0.09 = P(A)P(B)$.
B. Yes. $P(B \cap C) = 0.06 = P(B)P(C)$.

9

No. $\lceil 0.5 + 0.5 \rceil = 1 \neq \lceil 0.5 \rceil + \lceil 0.5 \rceil = 2$.

10

$GCD(68718952447, 1095) = GCD(1095, 217) = GCD(217, 10) = GCD(10, 7) = GCD(7, 3) = 1$

11

A.
Given $P(V) = 0.1$, $P(+|V) = 0.95$, $P(+| \sim V) = 0.02$,

$$\begin{aligned} P(V|+) &= \frac{P(V,+)}{P(+)} \\ &= \frac{P(V|+)P(V)}{P(+)} \\ &= \frac{P(V|+)P(V)}{P(+|V)P(V) + P(+| \sim V)P(\sim V)} \\ &= \frac{0.95 \times 0.1}{0.95 \times 0.1 + 0.02 \times 0.9} \\ &\approx 0.84 \end{aligned}$$

B.

$$\begin{aligned} P(V|+) &= \frac{0.95 \times 0.0001}{0.95 \times 0.0001 + 0.02 \times 0.9999} \\ &\approx 0.0047 \end{aligned}$$

The probability of a person tested positive actually having the virus is extremely low. The test result is utterly unreliable.

12

Let the item numbers for the 60 in-stock items be $k_1,\ k_2,\ \ldots, k_{60}$. Now, make a list of item numbers as $k_1 + 4,\ k_2 + 4, \ldots, k_{60} + 4$. Since these 120 numbers range from 1 to 119, there is at least one item number K that come from both lists. Namely, both K and $K - 4$ were in the original list. The conclusion follows.

13

A.
$\forall x\ Q(x) \rightarrow P(x)$, $\exists x\ Q(x) \wedge \sim P(x)$
B.
$\exists x\ Q(x) \wedge P(x)$, $\forall x\ \ \sim Q(x) \vee \sim P(x)$

14

A.
False. Counter example: $x = -3$ and $y = -2$
B.
True. Example: $x = 1$ and $y = 2$