NATIONAL UNIVERSITY OF SINGAPORE

CS1231 - DISCRETE STRUCTURES

(Semester 1: AY2016/17)

SOLUTIONS

Time Allowed: 90 minutes

Part A
(20 marks) Multiple choice questions. Answer on the OCR form.

Use **2B pencil** for this section. **Shade** and **write** your student number completely and correctly (please check!) on the OCR form. You do not need to fill in any other particulars on the OCR form.

For each multiple choice question, choose the best answer and **shade** the corresponding choice on the OCR form. Each multiple choice question is worth 2 marks. No mark is deducted for wrong answers.

Q1. On the fabled Island of Knights and Knaves, you meet three persons Aiken, Dueet, and Kenyu. One of them is a knight, one a knave, and one a spy. The knight always tells the truth, the knave always lies, and the spy can either lie or tell the truth. Given the following conversation, who is the knight, who the knave, and who the spy?

Aiken: I am a knight.

Dueet: I am not a spy.

Kenyu: I am a knave.

A. Aiken is the knight, Kenyu the knave, and Dueet the spy.
B. Dueet is the knight, Kenyu the knave, and Aiken the spy.
C. Kenyu is the knight, Aiken the knave, and Dueet the spy.
D. Aiken is the knight, Dueet the knave, and Kenyu the spy.
E. Dueet is the knight, Aiken the knave, and Kenyu the spy.

Q2. For ease of reference, we call a positive integer with at least 9 digits (duplicates allowed) a 'long integer'. Which of the following statements are true?

(I) The digits in any long integer that is divisible by 9 can be rearranged such that the newly formed long integer is divisible by all n, where $1 < n < 9$.

(II) The digits in any long integer that is divisible by 9 can be rearranged such that the newly formed long integer is divisible by some n, where $1 < n < 9$.

(III) If all the digits (0 to 9) appear in a long integer, and they appear in equal number, then the long integer is divisible by 9.

(IV) If all the digits (0 to 9) appear in a long integer, not necessarily in equal number, then the digits can be rearranged such that the newly formed long integer is divisible by at least 2 prime numbers.

A. (I) and (III) only.
B. (II) and (III) only.
C. (III) and (IV) only.
D. (II), (III) and (IV) only.
E. None of (A), (B), (C) or (D) is correct.

Q3. Given the following premises, what is the valid conclusion?

1. No reindeer is a clown.
2. Every child loves Santa.
3. Scrooge does not love anything which is weird.
4. Anything which has a red nose is weird or is a clown.
5. Rudolph is a reindeer, and Rudolph has a red nose.
6. Everyone who loves Santa loves any reindeer.

A. Everyone who does not love Santa does not loves any reindeer.
B. There exists another reindeer with a red nose.
C. A child loves anything that is weird or is a clown.
D. Scrooge is not a child.
E. None of the above.

Q4. Which of the following statements is/are logically equivalent to $p \leftrightarrow q$?

(I) $(\sim p \vee q) \wedge (p \vee \sim q)$
(II) $(\sim p \wedge \sim q) \vee (p \wedge q)$
(III) $(\sim p \vee \sim q) \wedge (p \vee q)$
(IV) $(\sim p \wedge q) \vee (p \wedge \sim q)$

A. (I) only.
B. (I) and (II) only.
C. (I) and (III) only.
D. (II) and (III) only.
E. (II) and (IV) only.

Q5. What is/are the missing premise(s) to make the following argument valid?

$p \rightarrow r$
$q \rightarrow s$
(Some missing premise(s))
$\bullet\ (p \vee q) \rightarrow (r \wedge s)$

(I) $p \vee q$
(II) $(p \wedge q) \rightarrow (r \wedge s)$
(III) $p \rightarrow s$
(IV) $q \rightarrow r$

A. (I) only.
B. (II) only.
C. (I) and (II) only.
D. (III) and (IV) only.
E. None of (A), (B), (C) or (D) would make the argument valid.

Q6. Integer x satisfies $x^2 \equiv 24 \pmod 5$. Then x could be

A. 1

B. 3

C. 19

D. $\sqrt{24}$

E. There is no solution.

Q7. All of the following are equal to $(\mathrm{C3})_{16}$, EXCEPT

A. $(195)_{10}$

B. $(11000011)_2$

C. $(1240)_5$

D. $(168)_{11}$

E. $(123)_{12}$

The next three questions, Q8 — Q10, refer to the following definitions.

Predicates $P(x, y)$ and $Q(x, y, z)$ are defined as follows:

$$\begin{aligned} P(x,y) = &\ (\ \forall z \in \mathbb{Z}^+,\ (z \mid x \wedge z \mid y) \rightarrow z = 1\ ),\ \forall x, y \in \mathbb{N}. \\ Q(x,y,z) = &\ (\ z \mid x - y\ ),\ \forall x, y, z \in \mathbb{Z}^+. \end{aligned}$$

Q8. Which of the following is true?

(I) $P(5, 13)$ (II) $P(3^{50}, 6^{21})$ (III) $P(0, 0)$ (IV) $P(8, 27)$

A. (I) only.

B. (IV) only.

C. (I) and (IV) only.

D. (II) and (III) only.

E. All of (I),(II), (III) and (IV).

Q9. Which pair of x, y makes **false** the statement: $Q(x, y, 1) \rightarrow P(x, y)$?

(I) $x = 0, y = 0$ (II) $x = 13, y = 17$ (III) $x = 10^{20}, y = 7^7$ (IV) $x = 11!, y = 7!$

A. (I) only.

B. (II) only.

C. (IV) only.

D. (I), (III) and (IV) only.

E. All of (I),(II), (III) and (IV).

Q10. Which statement is true?

A. $\forall a, b \in \mathbb{Z}^+,\ Q(a,\ b,\ \frac{ab}{\mathbf{lcm}(a,b)})$.

B. $\forall$ primes $p, q,\ Q(p^2q,\ pq^2,\ p+q)$.

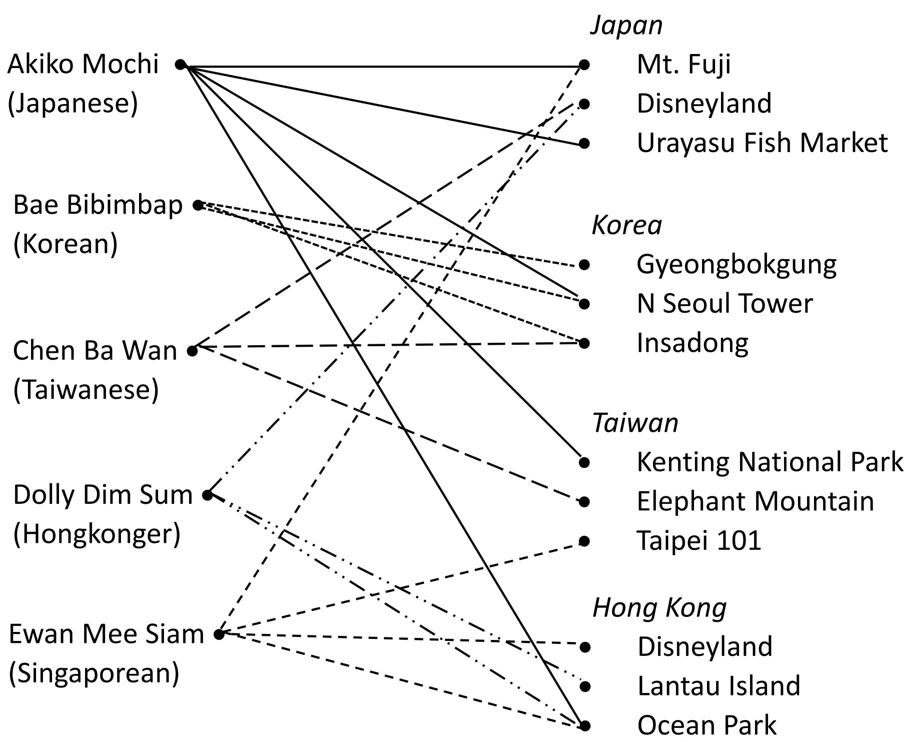
C. $\forall a, b \in \mathbb{Z}^+,\ Q(\text{lcm}(a,b),\ \text{gcd}(a,b),\ ab)$.

D. $Q(2^{12}-1,\ 3^{15}-1,\ 6)$.

E. None of the above.

Part B
(30 marks) Structured questions. Write your answer in the space provided in the Answer sheet.

Q11. (4 marks) The diagram below shows the places of interest five visitors visited. Each country has three places of interest. Every person is resident in the country of their nationality. A line joining a person to a place of interest indicates that the person visited that place of interest. Answer the following questions below with either "true" or "false".



(a) (1 mark) Every visitor visited at least two places of interest in some country.

> **Solution: False**. Chen Ba Wan did not visit at least two places of interst in any country.

(b) (1 mark) Some of the places of interest in every country were visited only by non-residents of that country.

> **Solution: False**. None of Korea's places of interest were visited solely by non-residents.

(c) (1 mark) Every visitor visited some places of interest that was also visited by another visitor.

> **Solution: True**.

(d) (1 mark) The place of interest visited by the most visitors is located in the country visited by the most visitors.

Solution: False. The place of interest visited by the most visitors is Hong Kong's Ocean Park. However, the country visited by the most visitors is Japan.

Q12. (5 marks) Theorem 2.1.1 is given below. Given any statement variables p, q and r, the following logical equivalences hold.

1. *Commutative laws:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2. *Associative laws:*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3. *Distributive laws:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4. *Identity laws:*	$p \wedge \textbf{true} \equiv p$	$p \vee \textbf{false} \equiv p$
5. *Negation laws:*	$p \vee \sim p \equiv \textbf{true}$	$p \wedge \sim p \equiv \textbf{false}$
6. *Double negative law:*	$\sim(\sim p) \equiv p$	
7. *Idempotent laws:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8. *Universal bound laws:*	$p \vee \textbf{true} \equiv \textbf{true}$	$p \wedge \textbf{false} \equiv \textbf{false}$
9. *De Morgan's laws:*	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10. *Absorption laws:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11. *Negations of* **true**/**false**:	$\sim\textbf{true} \equiv \textbf{false}$	$\sim\textbf{false} \equiv \textbf{true}$

In addition to the above, for simplicity, you may use the commutative form of the equivalances wherever appropriate without citing the commutative law. For example, you may write $\sim p \vee p \equiv \textbf{true}$ instead of adding an additional step such as $\sim p \vee p \equiv p \vee \sim p \equiv \textbf{true}$.

Using these rules, derive a simpler statement that is logically equivalent to $p \vee (\sim p \wedge q)$. Justify every step in your derivation by citing the rule used. Do not use Truth Tables.

Solution:

$p \vee (\sim p \wedge q)$	
$\equiv (p \vee \sim p) \wedge (p \vee q)$	(distributive law)
$\equiv \textbf{true} \wedge (p \vee q)$	(negation law)
$\equiv (p \vee q) \wedge \textbf{true}$	(commutative law) (optional)
$\equiv p \vee q$	(identity law)

Q13. (6 marks) Translate the following English sentences into mathematical statements using only the three predicates defined below. Do not define any new predicates. You may assume that the domain is the set of humans, and thus you may omit it in your statements.

$$\text{love}(x, y) = (x \text{ loves } y).$$
$$\text{man}(x) = (x \text{ is a man}).$$
$$\text{hate}(x, y) = (x \text{ hates } y).$$

(a) (2 marks) "Everyone loves everyone else." (In other words: "everyone loves everyone except himself".)

> **Solution:** $\forall x \forall y\, (x \neq y \leftrightarrow \text{love}(x, y))$
> Note that the following is wrong as it means that loving oneself is allowed. $\forall x \forall y\, (x \neq y \rightarrow \text{love}(x, y))$

(b) (2 marks) "Everyone loves someone." Show that this is ambiguous by writing two quantified statements for it and explaining what each means.

> **Solution:**
> i $\forall x \exists y$ love(x, y)
> "For every person x, there is someone x loves."
> ii $\exists y \forall x$ love(x, y)
> "There is a person y whom everybody loves."

(c) (2 marks) "Every man who loves Judy hates every man whom Judy loves."

> **Solution:** $\forall x\ (\text{man}(x) \land \text{love}(x, \text{Judy})) \rightarrow \forall y\ ((\text{man}(y) \land \text{love}(\text{Judy}, y)) \rightarrow \text{hate}(x, y))$
> (Note that interestingly this means if a man loves Judy and Judy loves him, then the man hates himself.)
> Alternative solution (which is logically equivalent to the above):
> $\forall x\ \forall y\ ((\text{man}(x) \land \text{love}(x, \text{Judy}) \land \text{man}(y) \land \text{love}(\text{Judy}, y)) \rightarrow \text{hate}(x, y))$

Q14. (4 marks) A Pythagorean triple is a triple of integers a, b, c such that $a^2 + b^2 = c^2$.

(a) (1 mark) Find a Pythagorean triple.

Solution: $a = 3, b = 4, c = 5$, since $3^2 + 4^2 = 5^2$.

(b) (3 marks) In a Pythagorean triple, is it possible that both a and b are odd? If so, give an example; otherwise prove that a, b cannot both be odd.

Solution: Both cannot be odd.

Proof. (by Contradiction)

1. Suppose a, b are both odd:
   - 1.1. Then $a = 2m + 1$, and $b = 2n + 1$ for some integers m, n, by definition of odd.
   - 1.2. Then $(2m + 1)^2 + (2n + 1)^2 = c^2$, by subtitution.
   - 1.3. Thus, $2(2m^2 + 2m + 2n^2 + 2n + 1) = c^2$, by basic algebra.
   - 1.4. Note that $2m^2 + 2m + 2n^2 + 2n + 1$ is an integer, by the closure property.
   - 1.5. So c^2 is even, by definition of even.
   - 1.6. So c is even, by Proposition 4.6.4 (Epp).
   - 1.7. Let $c = 2k$, for some integer k, by definition of even.
   - 1.8. Then, $2(2m^2 + 2m + 2n^2 + 2n + 1) = 4k^2$, by basic algebra.
   - 1.9. Which means, $2(m^2 + m + n^2 + n) + 1 = 2k^2$, by basic algebra.
   - 1.10. Both $m^2 + m + n^2 + n$, and k^2 are integers, by the closure property.
   - 1.11. The left hand side of the equation in Line 1.9. is odd, by definition of odd, while the right hand side is even, by the definition of even. This contradicts Theorem 4.6.2 (Epp), which says that a number cannot be both odd and even.
2. Thus, a and b cannot both be odd, by the Contradiction rule.

■

Q15. (7 marks) Recall the definition of *floor* from Tutorial 4:

> Definition: Given any real number x, the *floor of* x, denoted $\lfloor x \rfloor$, is the unique integer n such that $n \le x < n+1$.
> Symbolically, if x is a real number and n is an integer, then:
>
> $$\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \le x < n+1.$$
>
> Examples: $\lfloor 1.999 \rfloor = 1 = \lfloor 1 \rfloor$, and $\lfloor -2.01 \rfloor = -3$.

(a) (1 mark) Calculate: $\lfloor \sqrt{1} \rfloor + \lfloor \sqrt{2} \rfloor + \lfloor \sqrt{3} \rfloor + \lfloor \sqrt{4} \rfloor + \lfloor \sqrt{5} \rfloor + \lfloor \sqrt{6} \rfloor$.

> **Solution:** $\lfloor \sqrt{1} \rfloor + \lfloor \sqrt{2} \rfloor + \lfloor \sqrt{3} \rfloor + \lfloor \sqrt{4} \rfloor + \lfloor \sqrt{5} \rfloor + \lfloor \sqrt{6} \rfloor = 1+1+1+2+2+2 = 9$.

(b) (6 marks) Prove by Mathematical Induction:

$$\forall n \in \mathbb{Z}^+, \sum_{i=1}^{n-1} \lfloor \sqrt{i} \, \rfloor \;=\; na - \frac{a^3}{3} - \frac{a^2}{2} - \frac{a}{6}, \text{ where } a = \lfloor \sqrt{n} \rfloor.$$

Hint: You may use, without proving, the fact that $\lfloor \sqrt{m+1} \rfloor - \lfloor \sqrt{m} \rfloor = 0$ or 1, for any $m \in \mathbb{Z}^+$.

> **Solution:**
>
> *Proof.* (by Mathematical Induction)
>
> 1. Let $P(n) = (\ \sum_{k=1}^{n-1} \lfloor \sqrt{k} \rfloor \;=\; na - \frac{a^3}{3} - \frac{a^2}{2} - \frac{a}{6}\ )$, $\forall n \in \mathbb{Z}^+$, and $a = \lfloor \sqrt{n} \rfloor$
> 2. Base case: $n = 1$
>   - 2.1. $\sum_{k=1}^{n-1} \lfloor \sqrt{k} \rfloor \; = 0$, since the sum is empty.
>   - 2.2. Right hand side $= 1 \cdot 1 - \frac{1}{3} - \frac{1}{2} - \frac{1}{6} = 0$, by basic algebra.
>   - 2.3. Thus $P(1)$ is true.
> 3. Inductive step: For any $m \in \mathbb{Z}^+$:
>   - 3.1. Assume $P(m)$ is true, ie. $\sum_{k=1}^{m-1} \lfloor \sqrt{k} \rfloor = ma - \frac{a^3}{3} - \frac{a^2}{2} - \frac{a}{6}$, where $a = \lfloor \sqrt{m} \rfloor$.
>   - 3.1.1. Consider $m+1$:
>   - 3.1.2. $\sum_{k=1}^{m} \lfloor \sqrt{k} \rfloor = \sum_{k=1}^{m-1} \lfloor \sqrt{k} \rfloor + \lfloor \sqrt{m} \rfloor$ by basic algebra.
>   - 3.1.3. $= (m+1)a - \frac{a^3}{3} - \frac{a^2}{2} - \frac{a}{6}$, where $a = \lfloor \sqrt{m} \rfloor$, by basic algebra.
>   - 3.1.4. If $\lfloor \sqrt{m+1} \rfloor = \lfloor \sqrt{m} \rfloor$:
>   - 3.1.4.1. Then Line 3.1.3. is exactly the right hand side.
>   - 3.1.4.2. Thus, $P(m+1)$ is true.
>   - 3.1.5. Else $\lfloor \sqrt{m+1} \rfloor = \lfloor \sqrt{m} \rfloor + 1$:
>   - 3.1.5.1. (Claim: $m = a^2 + 2a$.)
>   - 3.1.5.2. By definition of floor, $a \le \sqrt{m} < a+1$.
>   - 3.1.5.3. Thus, $a^2 \le m < (a+1)^2$, by basic algebra.
>   - 3.1.5.4. $\Rightarrow\ m < a^2 + 2a + 1$, or $m - (a^2 + 2a) < 1$ by basic algebra.
>   - 3.1.5.5. Also, by assumption, $\lfloor \sqrt{m+1} \rfloor = a + 1$.
>   - 3.1.5.6. Thus, $a + 1 \le \sqrt{m+1} < a+2$, by definition of floor.

3.1.5.7. So $(a+1)^2 \leq m+1 < (a+2)^2$, by basic algebra.
3.1.5.8. Thus, $0 \leq m - (a^2+2a)$, by basic algebra.
3.1.5.9. With Line 3.1.5.4., this means $m - (a^2+2a) = 0$ as claimed.
3.1.5.10. Re-write Line 3.1.3.:
$(m+1)a - \frac{a^3}{3} - \frac{a^2}{2} - \frac{a}{6} + 1 - 1 + m - (a^2+2a)$, by basic algebra.
3.1.5.11. $= (m+1)(a+1) - \frac{1}{6}[2a^3 + 3a^2 + a] - 1 - (a^2+2a)$, by basic algebra.
3.1.5.12. $= (m+1)(a+1) - \frac{(a+1)^3}{3} - \frac{(a+1)^2}{2} - \frac{a+1}{6}$, by basic algebra.
3.1.5.13. $= (m+1)b - \frac{b^3}{3} - \frac{b^2}{2} - \frac{b}{6}$, where $b = a+1 = \lfloor\sqrt{m+1}\rfloor$.
3.1.5.14. Which equals the right hand side.
3.1.5.15. Thus, $P(m+1)$ is true.

4. Thus, by Mathematical Induction, the statement is true. ■

Q16. (4 marks) So Dueet is happily married to Aiken, after passing the test given by Aiken's father. Six months later, Aiken's mother approaches Dueet for help.

For years, she and her farmer neighbor have been settling their debts using farm animals instead of cash. A cow is worth \$180, a chicken is worth \$75, and a goat is worth \$120. Thus, if Aiken's mother owes \$30, she would give one cow to the neighbor and get back two chickens.

Aiken's mother currently owes her neighbor \$70. She cannot quite figure out how many of each type of animal to give, and what to receive in return. Dueet is stumped too.

Help Dueet solve the problem by determining the number and type of animal to be exchanged. If a solution is not possible, explain with a proof why not.

Solution: There is no solution.

The problem to be solved is: find $x, y, z \in \mathbb{Z}$ such that $180x + 75y + 120z = 70$.

However, an equation $ax + by + cz = m$ has a solution if, and only if, $\gcd(a, b, c) \mid m$ (proof below). In this case $\gcd(180, 75, 120) = 15$, because $180 = 2^2 \cdot 3^2 \cdot 5$, $75 = 3 \cdot 5^2$, $120 = 2^3 \cdot 3 \cdot 5$. And $15 \nmid 70$. So there is no solution.

Proof. (Direct proof)

1. (Forward direction):
2. If $ax + by + cz = m$ has a solution:
   2.1. Then, since $\gcd(a, b, c)$ divides a, b, c, it also divides m, by Theorem 4.1.1 (Linear combination)
3. (Backward direction):
4. If $\gcd(a, b, c) \mid m$:

4.1. Let $m = k \times \gcd(a, b, c)$, for some integer k, by definition of divisibility.

4.2. Then, by Bézout's Identity, $\exists r, s, t \in \mathbb{Z}$ such that $ar + bs + ct = \gcd(a, b, c)$.

4.3. (Comment: Bézout's Identity can be extended to 3 integers using the fact that $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$, which was proven in Q3(b) of Tutorial 4.)

4.4. Thus, $a(kr) + b(ks) + c(kt) = k \gcd(a, b, c) = m$, by basic algebra.

4.5. Thus, a solution is $x = kr, y = ks, z = kt$. ■

END OF PAPER