HKUST – Department of Computer Science and Engineering
COMP 2711: Discrete Math Tools for Computer Science

Spring 2022 Midterm Examination

Date: Friday, 25 March 2022 Time: 19:00–20:50

Problem 1: (a) [6 pts] Given $\neg a \vee (b \to \neg c)$, express its equivalent statements using only:

(i) NOT ($\neg$) and Implication ($\to$).
(ii) NOT ($\neg$) and OR ($\vee$).
(iii) NOT ($\neg$) and AND ($\wedge$).

(b) (3 pts) Given the statement $(a \vee b) \wedge (\neg b \vee c)$, express its equivalent statement using only NOT ($\neg$) and Implication ($\to$).

Solution: (a) (i) $a \to (b \to \neg c)$
(ii) $\neg a \vee \neg b \vee \neg c$
(iii) $\neg(a \wedge b \wedge c)$

(b)

$$\begin{aligned} & (a \vee b) \wedge (\neg b \vee c) \\ \equiv\ & (\neg a \to b) \wedge (b \to c) \\ \equiv\ & \neg(\neg(\neg a \to b) \vee \neg(b \to c)) \\ \equiv\ & \neg((\neg a \to b) \to \neg(b \to c)) \end{aligned}$$

Problem 2: [9 pts] Let $W(x, y)$ denote the predicate that x has visited website y, where the domain for x consists of people in the world and the domain for y consists of all websites. Express each of the following statements using predicate logic.

(a) There is a website that both Alice and Bob have visited.
(b) There is a person other than David who has visited all the websites David has visited.
(c) There are two distinct people who have visited exactly the same sites.

Solution: (a) $\exists y\ (W(Alice, y) \wedge W(Bob, y))$
(b) $\exists y \forall z\ (y \neq David \wedge (W(David, z) \to W(y, z)))$
(c) $\exists x \exists y \forall z\ (((x \neq y) \wedge (W(x, z) \leftrightarrow W(y, z))))$
Grading Scheme: (a) $\exists$ goes with $\wedge$ 2 pts, (b) $\exists$ goes with $\wedge$ 1 pt, $\forall$ goes with $\to$ 1 pt (c) $\exists x \exists y (x \neq y)$ 1 pt

Problem 3: [10 pts] Let $P(x), Q(x), R(x), S(x)$ be the following predicates:

$P(x)$: "x is a hummingbird."
$Q(x)$: "x is large."
$R(x)$: "x lives on honey."
$S(x)$: "x is richly colored."

Let the domain be all the birds. First translate the following statements into predicate logic (you may assume that "small" is the same as "not large" and that "dull in color" is the same as "not richly colored"):

(1) "All hummingbirds are richly colored."

(2) "No large birds live on honey."

(3) "Birds that do not live on honey are dull in color."

(4) "Hummingbirds are small."

Let the first three statements be premises and the fourth be the conclusion. Show a step-by-step proof using inference rules. You don't have to write down the name of the rule used; instead, you can just write down from which statement(s) a new statement is derived. For example, instead of writing "(3): statement (Modus tollens using (1) and (2))", you can just write "(3): statement (from (1) and (2))".

Solution: (1) $\forall x\ (P(x) \to S(x))$.

(2) $\neg\exists x\ (Q(x) \wedge R(x))$.

(3) $\forall x\ (\neg R(x) \to \neg S(x))$.

(4) $\forall x\ (P(x) \to \neg Q(x))$.

Step	**Reason**
(5) $\forall x\ (\neg Q(x) \vee \neg R(x))$	(2) equivalence
(6) $\forall x\ (\neg P(x) \vee S(x))$	(1) equivalence
(7) $\forall x\ (R(x) \vee \neg S(x))$	(3) equivalence
(8) $R(a) \vee \neg S(a)$ for arbitrary a	Universal instantiation using (7)
(9) $\neg P(a) \vee S(a)$	Universal instantiation using (6)
(10) $\neg P(a) \vee R(a)$	Resolution using (8) and (9)
(11) $\neg Q(a) \vee \neg R(a)$	Universal instantiation using (5)
(12) $\neg P(a) \vee \neg Q(a)$	Resolution using (10) and (11)
(13) $P(a) \to \neg Q(a)$	(12) equivalence
(14) $\forall x\ (P(x) \to \neg Q(x))$	Universal generalization using (13)

Grading Scheme: 4 pts for translation. Deduct 3 pts if no statement numbers given under reason.

Problem 4: [6 pts] Give an example of two uncountable sets A, B such that $A - B$ is:

(a) Finite

(b) Countable infinite

(c) Uncountable

No Justification is needed.

Solution: There are several solutions. One solution is:

(a) $A = [1, 2), B = (1, 2) \implies A - B = \{1\}$

(b) $A = (-\infty, -1) \cup \mathbb{N}$, $B = (-\infty, -1) \implies A - B = \mathbb{N}$

(c) $A = [1, 3], B = [1, 2) \implies A - B = [2, 3]$

Problem 5: [8 pts] For each of the following sets, determine if it is countable or uncountable. No justification is needed.

(a) $\{x \in \mathbb{R} \mid x^2 \in \mathbb{Z}\}$

(b) $\{x \in \mathbb{R} \mid$ there is a decimal expansion of x with only even digits$\}$

(c) The union of countably many countable sets.

(d) The set of circles in the plane.

Solution: (a) Countable

(b) Uncountable

(c) Countable

(d) Uncountable

Problem 6: Assume p is a prime and n is a positive integer such that $p \mid (4n^2+1)$.

(a) [8 pts] Show that $p \nmid n$.

(b) [10 pts] Show that $p \equiv 1 \pmod 4$. (Hint: Analyze $(2n)^{p-1}$ using Fermat's Little Theorem and part (a))

(c) [Bonus 10 pts] Show that there are infinitely many primes of the form $4k+1$.

Solution: (a) We use proof by contradiction. Suppose $n = kp$ for some integer k. Then $4n^2+1 = 4(kp)^2+1 = 4k^2p^2+1 = pk'$ for some integer k', i.e., $p(k'-4k^2p) = 1$, which is impossible for prime p.

(b) $4n^2+1$ is an odd number so we know that p has to be odd. So either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. Assume $p \equiv 3 \pmod 4$ which means $p = 4k+3$. Since $p \nmid n$ and p is an odd prime, so $p \nmid 2n$. By Fermat's Little Theorem, we have $(2n)^{p-1} \equiv (2n)^{4k+2} \equiv (4n^2)^{2k+1} \equiv 1 \pmod p$. Recall that $p \mid 4n^2+1 \implies 4n^2 \equiv -1 \pmod p$. So $(4n^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod p$. Now we have $1 \equiv -1 \pmod p$, which is impossible since $p \neq 2$. This proves that $p \equiv 1 \pmod 4$.

(c) Assume we have finitely many primes of form $4k+1$, say $p_1, p_2, \cdots, p_t$. Consider $N = 4(p_1p_2...p_t)^2+1$. Let p be any prime factor of N (p may be N itself if N is prime). Based on part (b), $p = 4k+1$ for some k. Also note that p must be different from $p_1, \ldots, p_t$, since none of them divides N. Then we have found a new prime p in the form of $4k+1$, which is a contradiction.

Grading Scheme:

Problem 7: Calculate the following quantities. Show your steps.

(a) [5 pts] $2^{542} \bmod 109$.

(b) [5 pts] $3^{3^{2022}} \bmod 10$.

Solution: (a) 109 is a prime number. By using Fermat's Little Theorem: $2^{108} \equiv 1 \pmod{109} \implies (2^{108})^5 \equiv 1^5 \implies 2^{540} \equiv 1 \pmod{109}$. So $2^{542} = 2^2 \cdot 2^{540} \equiv 2^2 \equiv 4 \pmod{109}$.

(b) We use a similar idea but can't use Fermat's Little Theorem since 10 is not a prime. But observe that $3^4 \equiv 81 \equiv 1 \pmod{10} \implies 3^{4t} \equiv 1 \pmod{10}$ for any integer t. So it suffices to find $3^{2022} \bmod 4$. Since $3^2 \equiv 1 \pmod 4$, $3^{3022} \equiv 1 \pmod 4$. Then $3^{3^{2022}} = 3^{4t+1} \equiv 3 \pmod{10}$.

Problem 8: Consider RSA encryption with $p = 7, q = 19$ and $e = 29$.

(a) [5 pts] What is the encrypted message for plaintext $m = 12$?

(b) [8 pts] Compute the private key d. Show your steps.

Your solution should be numbers.

Solution: (a) $c = 12^e \bmod pq$, which is $12^{29} \bmod 133$. This can be solved by repeated squaring. Set $I_i \equiv 12^{2^i} \pmod{133}$.

$I_0 = 12$
$I_1 = I_0 \cdot I_0 \bmod 133 = 11$
$I_2 = I_1 \cdot I_1 \bmod 133 = 121$
$I_3 = I_2 \cdot I_2 \bmod 133 = 11$
$I_4 = I_3 \cdot I_3 \bmod 133 = 121$

Note that $12^{29} = 12^{16} \cdot 12^8 \cdot 12^4 \cdot 12 = 12^{2^4} \cdot 12^{2^3} \cdot 12^{2^2} \cdot 12^{2^0}$.

Thus, $12^{29} \equiv (I_4I_3I_2I_0) \pmod{133} \equiv (12 \cdot 11 \cdot 121^2) \pmod{133} \equiv 122 \pmod{133}$.
So the encrypted message is 122.

(b) The private key d is the multiplicative inverse of e modulo $(p-1)(q-1) = 108$. First find $\gcd(108, 29)$:

$$\begin{aligned} 108 &= 29 \cdot 3 + 21 \\ 29 &= 21 \cdot 1 + 8 \\ 21 &= 8 \cdot 2 + 5 \\ 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

So, $\gcd(108, 29) = 1$.

Rewriting and substituting:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= -5 + 2 \cdot 3 \\ &= -5 + 2 \cdot (8 - 5) \\ &= 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3 \cdot (21 - 2 \cdot 8) \\ &= -3 \cdot 21 + 8 \cdot 8 \\ &= -3 \cdot 21 + 8 \cdot (29 - 21) \\ &= 8 \cdot 29 - 11 \cdot 21 \\ &= 8 \cdot 29 - 11 \cdot (108 - 3 \cdot 29) \\ &= -11 \cdot 108 + 41 \cdot 29 \end{aligned}$$

Multiplicative inverse of 29 modulo 108 is 41, so $d = 41$.

Grading Scheme: (a) Computing I_i 2 pts (b) Steps of computing gcd 3 pts, linear combination 3 pt, inverse 2 pts

Problem 9: [6pts] Arrange the following running times in order of increasing asymptotic complexity. Just give the answer; no explanation is needed.

$$2^n, \sqrt{2n}, n^2 + 20, \log(n^3), \log(2^n), n^{1/3} \log n$$

Note that you must write function $f(n)$ before function $g(n)$ if $f(n) = O(g(n))$.

Solution:

$$\log(n^3), n^{1/3} \log n, \sqrt{2n}, \log(2^n), n^2 + 20, 2^n$$

Problem 10: Determine the best-case and worst-case running time of the following algorithms using the Θ notation. No justification is needed.

(a) [3 pts] The following algorithm finds the maximum of a sequence $\{a_1, a_2, \ldots, a_n\}$ of n integers:

```
max ← a_1
for i ← 2 to n
    if max < a_i then max ← a_i
return max
```

(b) [4 pts] The following algorithm finds an element x in a list of n integers:

```
for i ← 1 to n
    if x = a_i then return i
return "not found".
```

(c) [4 pts] The following algorithm finds x in an sorted list of n integers (note that instead of comparing with the median, this algorithm compares with the 25%-quantile in each iteration):

```
i ← 1
j ← n
while i ≤ j
    m ← ⌊(3/4)i + (1/4)j⌋
    if x = a_m then return m
    if x > a_m then i ← m + 1
    else j ← m − 1
return "not found"
```

Solution: (a) The number of comparisons does not depend on the values of a_1 through a_n. Exactly $n-1$ comparisons are used. Therefore, the best and worst case performance are both $\Theta(n)$.

(b) In the best case $x = a_1$. Thus, the best-case running time is $\Theta(1)$. In the worst case $x = a_n$. The worst-case running time is $\Theta(n)$.

(c) The best-case running time is $\Theta(1)$. Since each iteration reduces $j - i$ by $1/4$, the worst-case running time is $\Theta(\log_{3/4} \frac{1}{n}) = \Theta(\log n)$.