#	LS

HKUST – Department of Computer Science

COMP170: Discrete Math Tools for CS – FALL 2005

Midterm Examination 2

Solution Key

Date: Tue, Nov 8, 2005   Time: 19:00–20:30   Venues: LTD, LTC, LTB

Name: ____________________ Student ID: ____________________

Email: ____________________ Lecture and Tutorial: __________

Instructions

- This is a closed book exam. It consists of 20 pages and 10 questions.
- Please write your name, student ID, Email, lecture section and tutorial on this page.
- For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap paper and may also be used for rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- Only use notation given in class. Do not use notation that you have learnt outside of this class that is nonstandard.
- Calculators may be used for the exam.
- In questions 8, 9 and 10 you are asked for a solution to a recurrence. A *solution* means a formula given in closed form. Formulas using the summation symbol ($\sum$) or ellipses ($\ldots$) will not be accepted as answers.

Questions	1	2	3	4	5	6	7	8	9	10	Total
Points	10	10	10	6	11	8	12	9	12	12	100
Score											

As part of HKUST's introduction of an honor code, the HKUST senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: ______________________

Student's Signature: ____________________

Definitions and Formulas: This page contains some definitions used in this exam and a list of formulas (theorems) that you may use in the exam (without having to provide a proof). Note that you might not need all of these formulas on this exam.

Definitions

1. $N = \{0, 1, 2, 3, \ldots\}$, the set of non-negative integers.
2. $Z^+ = \{1, 2, 3, \ldots\}$, the set of positive integers.
3. R is the set of *real numbers.*
4. R^+ is the set of positive *real numbers.*

Formulas:

1. $\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$
2. If $0 < i < n$ then $\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$.
3. $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$.
4. $\neg(p \vee q)$ is equivalent to $\neg p \wedge \neg q$.
5. $\neg \forall x \in U\, (p(x))$ is equivalent to $\exists x \in U\, (\neg p(x))$
6. $\sum_{i=1}^{n-1} i = n(n-1)/2$.
7. $\sum_{i=1}^{n-1} i^2 = \frac{2n^3-3n^2+n}{6}$.
8. If $r \neq 1$ then $\sum_{i=0}^{n-1} r^i = \frac{1-r^n}{1-r}$
9. If $r \neq 1$ then $\sum_{i=0}^{n} i r^i = \frac{nr^{n+2}-(n+1)r^{n+1}+r}{(1-r)^2}$
10. If $r \neq 1$ then $\sum_{i=0}^{n} i^2 r^i = \frac{r+r^2-(n+1)^2r^{n+1}+(2n^2+2n-1)r^{n+2}-n^2r^{n+3}}{(1-r)^3}$

Problem 1: (10 points) Bob is constructing an RSA key-pair. He first chooses $p = 17$, $q = 11$ and then chooses $e = 7$. His public key is then the pair (n, e) where $n = pq = 187$.

(a) Bob then calculates his private key d.
What is the value of d?
Show how you derived this.

(b) Alice wants to send Bob the message $M = 75$.
She encrypts the message using the public key pair $(n, e) = (187, 7)$.
What is the value of the encrypted message that Alice sends Bob?

Solution: *(a)* $T = (p-1)(q-1) = 16 \cdot 10 = 160$. *Use the extended GCD:*

$$\begin{aligned} 160 &= 22 \cdot 7 + 1 \cdot 6 \\ 7 &= 1 \cdot 6 + 1 \cdot 1 \end{aligned}$$

We want to know, what are x and y in the equation $7x + 160y = 1$? x is the inverse of $7 \bmod 160$*, so x is our d.*

Iterating "backwards" (we could also use the formal algorithm given in class) yields

$$\begin{aligned} 1 &= 1 \cdot 7 - 1 \cdot 6 \\ &= 1 \cdot 7 - 1 \cdot (1 \cdot 160 - 22 \cdot 7) \\ &= 1 \cdot 7 - 1 \cdot 160 + 22 \cdot 7 \\ &= 23 \cdot 7 - 1 \cdot 160 \end{aligned}$$

So, y is -1, and $x = d = e^{-1} = 23$.

(b) Encrypted message $C = M^e \bmod n = 75^7 \bmod 187 = 114$. *(Bob decrypts by doing* $M = C^d \bmod n = 114^{23} \bmod 187 = 75$, *but this is not asked in the question.)*

Problem 2: (10 pts)
(a) Efficiently calculate the value of $3^{134} \bmod 100$.
What is the value of the answer?
Describe how you got the answer and show the results of *all* of the multiplications that you performed while deriving the answer.
Note: It is *not* necessary to justify each step of your derivation.

(b) How many multiplications did you use?

Solution: *(a) Use Repeated Squaring* $3^{134} \bmod 100 = 3^{128} \cdot 3^4 \cdot 3^2 \bmod 100$.

$$\begin{aligned}
I_1 &= (a \cdot a) \bmod 100 = 3^2 \bmod 100 = 9 \bmod 100 = 9\\
I_2 &= (I_1 \cdot I_1) \bmod 100 = 9^2 \bmod 100 = 81 \bmod 100 = 81\\
I_3 &= (I_2 \cdot I_2) \bmod 100 = 81^2 \bmod 100 = 6561 \bmod 100 = 61\\
I_4 &= (I_3 \cdot I_3) \bmod 100 = 61^2 \bmod 100 = 3721 \bmod 100 = 21\\
I_5 &= (I_4 \cdot I_4) \bmod 100 = 21^2 \bmod 100 = 441 \bmod 100 = 41\\
I_6 &= (I_5 \cdot I_5) \bmod 100 = 41^2 \bmod 100 = 1681 \bmod 100 = 81\\
I_7 &= (I_6 \cdot I_6) \bmod 100 = 81^2 \bmod 100 = 6561 \bmod 100 = 61
\end{aligned}$$

$3^{134} \bmod 100 = (I_7(I_2 \cdot I_1) \bmod 100) \bmod 100 = (61(81 \cdot 9) \bmod 100) \bmod 100 = (61 \cdot 29) \bmod 100 = 69.$

(b) 9 multiplications. 7 to calculate the I_i and 2 more to actually calculate the solution from the I_i.

Problem 3: (10 pts) How many solutions x with $0 \le x < 264$ are there that satisfy

$$\begin{aligned} x \bmod 11 &= 5, \\ x \bmod 24 &= 7? \end{aligned}$$

Give all of the solutions.

Solution: *Since* 11 *and* 24 *are relatively prime the Chinese Remainder Theorem tells us that there is exactly one solution.*
Calculation shows that $24 \cdot_{11} 6 = 1$ *and* $11 \cdot_{24} 11 = 1$. *Setting* $y = 5 \cdot 6 \cdot 24 + 7 \cdot 11 \cdot 11 = 1567$ *gives*

$$\begin{aligned} y \bmod 11 &= 5, \\ y \bmod 24 &= 7. \end{aligned}$$

Setting $x = y \bmod 264 = 247$ *gives the solution.*

Problem 4: (6 pts) For each of the three statements below, state whether they are True or False and prove your answer.

For problem (c), $D(x, y)$ will denote that "x divides y", e.g., $D(3, 9)$ is True while $D(3, 10)$ is False. Also, xy will denote the normal product $x \cdot y$.

(a) $\forall x \in R \left(\forall y \in R \; (x^2 + y^2 \geq 2xy) \right)$

(b) $\forall x \in R \left(\exists y \in R^+ \; ((y - 3) \geq (x - 2)) \right)$

(c) $\forall x \in Z^+ \left(\forall y \in Z^+ \; (\forall z \in Z^+ \;\; ([D(x, z) \wedge D(y, z)] \Rightarrow D(xy, z))) \right)$

Solution: *(a) True.* $x^2 + y^2 \geq 2xy \Leftrightarrow x^2 - 2xy + y^2 \geq 0 \Leftrightarrow (x - y)^2 \geq 0$. *Since* $(x - y)^2 \geq 0$, *the statement is true for all* x *and* y.

(b) True. Choose $y = \max\{x + 1, 1\}$.

(c) False. Counter example: if $x = 3, y = 6, z = 12$, *then* $xy = 18$.

Problem 5: (11 pts) In each part below, you are asked whether one statment is equivalent to another. In each case, if yes, prove your answer. If no, give a counterexample, In (a)-(d) a counterexample would be some universe U, statement $p(x)$ and value $x \in U$; in (e), a counterexample would be a truth setting of the variables.

If you are using formulas and/or theorems proven in class, state explicitly what the formulas or theorems you are using are.

(a) Is $\neg(\forall x \in R^+ \; (p(x)) \;)$ equivalent to $\exists x \in R \; (\; (x > 0) \wedge \neg p(x) \;)$?

(b) Is $\neg(\exists x \in R^+ \; (p(x)) \;)$ equivalent to $\forall x \in R \; (\; \neg(x > 0) \vee \neg p(x) \;)$?

(c) Is $\Big(\exists x \in U \; (p(x))\Big) \vee \Big(\exists y \in U \; (q(y))\Big)$ equivalent to

$\exists z \in U \; (\; p(z) \vee q(z) \;)$?

(d) Is $\Big(\exists x \in U \; (p(x))\Big) \wedge \Big(\exists y \in U \; (q(y))\Big)$ equivalent to

$\exists z \in U \; (\; p(z) \wedge q(z) \;)$?

(e) Is $\Big(p \wedge \neg q\Big) \;\Rightarrow\; \Big(\,(r \vee s) \wedge \neg t\Big)$ equivalent to

$\Big((\neg r \vee t) \wedge (\neg s \vee t)\Big) \;\Rightarrow\; (\neg p \vee q)$?

Solution: *(a) Yes. From Lecture 8 Theorem 3.2 we know we can rewrite* $\neg(\forall x \in R^+ \; (p(x)) \;)$ *as* $\neg(\forall x \in R \; ((x > 0) \Rightarrow p(x)) \;)$.
We then apply Theorem 3.3 (formula 5 on page 3 of this exam) to get the equivalent statement $(\exists x \in R \; \neg((x > 0) \Rightarrow p(x)) \;)$.
$\neg s \vee t$ *is equivalent to* $s \Rightarrow t$*, so we get:* $(\exists x \in R \; \neg(\neg(x > 0) \vee p(x)) \;)$.
Applying DeMorgan's Law yields $(\exists x \in R \; ((x > 0) \wedge \neg p(x)) \;)$.

(b) Yes. We can rewrite $\neg(\exists x \in R^+ \; (p(x)) \;)$ *as* $\neg(\exists x \in R \; ((x > 0) \wedge p(x)) \;)$ *(Theorem 3.2 in Lecture 8).*
This is equivalent (Theorem 3.3) to $(\forall x \in R \; \neg((x > 0) \wedge p(x)) \;)$.
Applying DeMorgan's Law yields $(\forall x \in R \; (\neg(x > 0) \vee \neg p(x)) \;)$.

(c) Yes. If there exists an $x \in U$ *that makes* $p(x)$ *true, then that same* x *also makes* $p(x) \vee q(x)$ *true. The same holds for a* $y \in U$ *and* $q(y)$ *respectively.*

On the other hand if we find a $z \in U$ *that makes* $p(z) \vee q(z)$ *true, this will make either* $p(z)$ *or* $q(z)$ *true and therefore the first statement.*

So, we have just shown that the first statement is true if and only if the second statment is true. They are therefore equivalent.

(d) No. $U = Z$*.* $p(x) = x$ *is even.* $q(x) = x$ *is odd. There exist even and odd integers in* Z *but none of them are* both *even and odd.*

(e) Yes. Use Lecture 9, Priciple 3.6: The statements $u \Rightarrow v$ *and* $\neg v \Rightarrow \neg u$ *are equivalent. Note that* $\big(p \wedge \neg q\big)$ *is* u*, so* $\neg u$ *is* $(\neg p \vee q)$*, and* v *is* $\big((r \vee s) \wedge \neg t\big)$*, so* $\neg v$ *is* $\big((\neg r \vee t) \wedge (\neg s \vee t)\big)$*, because*
$\neg\big((r \vee s) \wedge \neg t\big)$
$= \neg(r \vee s) \vee t$ *(DeMorgan's Law)*
$= (\neg r \wedge \neg s) \vee t$ *(DeMorgan's Law)*
$= (\neg r \vee t) \wedge (\neg s \vee t)$ *(Distributive Law).*

Problem 6: (8 pts)
Find *all* values $n \in N$ such that $3^n > n^2 - 10n + 50$.
Prove the correctness of your answer.

Solution: *We try the first few values to find:*

when $n = 1$, $3 < 1 - 10 + 50 = 41$;
when $n = 2$, $9 < 4 - 20 + 50 = 34$;
when $n = 3$, $27 < 9 - 30 + 50 = 29$;
when $n = 4$, $81 > 16 - 40 + 50 = 26$;
when $n = 5$, $243 > 25 - 50 + 50 = 25$;
when $n = 6$, $729 > 36 - 60 + 50 = 26$;
...

The statement is false when $n \leq 3$ *and it seems that it is correct for* $n \geq 4$. *We prove this by induction. We will start our induction at* $n = 4$.

Basis: We already saw that it is true for $n = 4$.

Hypothesis:

Assume that for $k \geq 4$, *when* $n = k$, $3^k > k^2 - 10k + 50$.

Step :

Consider when $n = k+1$, *what we need to prove is* $3^{k+1} - ((k+1)^2 - 10(k+1) + 50) > 0$.

$$\begin{aligned} & 3^{k+1} - ((k+1)^2 - 10(k+1) + 50) \\ > \; & 3(k^2 - 10k + 50) - (k^2 - 8k + 41) \\ = \; & 2k^2 - 22k + 109 \\ = \; & 2(k - 5.5)^2 + 48.5 \\ > \; & 0 \end{aligned}$$

So by the principle of mathematical induction, we see the inequality holds for all integers $n \geq 4$.

We could also derive the induction step from $k - 1$ to k $(k \geq 5)$ as follows.

Assume $3^{k-1} > ((k-1)^2 - 10(k-1) + 50)$.

$$\begin{aligned} 3^k = 3 \cdot 3^{k-1} \; & > \; 3((k-1)^2 - 10(k-1) + 50) \\ & = \; k^2 - 10k + 50 + (2k^2 - 26k + 133) \\ & = \; k^2 - 10k + 50 + 2(k - 6.5)^2 + 48.5 \qquad (2(k - 6.5)^2 + 48.5 > 0) \\ & > \; k^2 - 10k + 50 \end{aligned}$$

Student ID: ____________

Problem 7: (12 pts)

Prove by induction on n that $\forall n \in Z^+,\ \sum_{i=0}^{n} \binom{n}{i}(-1)^i = 0$.

Solution: *Base Case $n = 1$:* $\sum_{i=0}^{1} \binom{1}{i}(-1)^i = \binom{1}{0} \cdot 1 + \binom{1}{1} \cdot (-1) = 0.$

Inductive Hypothesis: Assume $n > 1$ and that formula holds for $n-1$, i.e., $\sum_{i=0}^{n-1} \binom{n-1}{i}(-1)^i = 0.$

Then

$$\begin{aligned}
\sum_{i=0}^{n} \binom{n}{i}(-1)^i &= 1 + (-1)^n + \sum_{i=1}^{n-1} \binom{n}{i}(-1)^i \\
&= 1 + (-1)^n + \sum_{i=1}^{n-1} \left(\binom{n-1}{i} + \binom{n-1}{i-1} \right)(-1)^i \\
&= (-1)^0 + \sum_{i=1}^{n-1} \binom{n-1}{i}(-1)^i \\
&\quad +(-1)^{((n-1)+1)} + \sum_{i=0}^{n-2} \binom{n-1}{i}(-1)^{i+1} \\
&= \binom{n-1}{0}(-1)^0 + \sum_{i=1}^{n-1} \binom{n-1}{i}(-1)^i \\
&\quad +\binom{n-1}{n-1}(-1)^{(n-1)+1)} + \sum_{i=0}^{n-2} \binom{n-1}{i}(-1)^{i+1} \\
&= \sum_{i=0}^{n-1} \binom{n-1}{i}(-1)^i + \sum_{i=0}^{n-1} \binom{n-1}{i}(-1)^{i+1} \\
&= 0 - \sum_{i=0}^{n-1} \binom{n-1}{i}(-1)^i \\
&= 0 - 0 = 0.
\end{aligned}$$

where the last two '0's come from the inductive hypothesis.

We have just proven the inductive step.

So by the principle of mathematical induction, we see the formula holds for all $n \in Z^+$.

Problem 8: (9 pts)

(a) Consider the recurrence below defined on $n \geq 2$.

$$T(n) = \begin{cases} 5 & \text{if } n = 2 \\ 4T(n-1) + 3 & \text{if } n > 2 \end{cases}$$

Give a closed-form, exact solution to the recurrence.
You only have to give the solution. You do not need to show how you derived it.
(b) Now, prove the correctness of your solution by induction.

Solution: *(a) Using Theorem 4.14, or by iterating the recurrence or by using recursion trees we get* $T(n) = 6 \cdot 4^{n-2} - 1$.

(b) Base Case $n = 2$*:* $T(2) = 6 \cdot 4^{2-2} - 1 = 5$.

Inductive Hypothesis: Assume $n > 2$ *and that formula holds for* $n - 1$*, i.e.,* $T(n-1) = 6 \cdot 4^{n-3} - 1$.

Then

$$\begin{aligned} T(n) &= 4T(n-1) + 3 \\ &= 4(6 \cdot 4^{n-3} - 1) + 3 \\ &= 6 \cdot 4^{n-2} - 4 + 3 \\ &= 6 \cdot 4^{n-2} - 1 \end{aligned}$$

We have just proven the inductive step.

So by the principle of mathematical induction, we see the formula holds for all integers $n > 1$.

Problem 9: (12 pts)
(a) Consider the recurrence below defined on $n \geq 0$.

$$T(n) = \begin{cases} 5 & \text{if } n = 0 \\ 3T(n-1) + n^2 3^n & \text{if } n > 0 \end{cases}$$

Give a closed-form, exact solution to the recurrence.
You only have to give the solution. You do not need to show how you derived it.
(b) Now, prove the correctness of your solution by induction.

Solution: *(a) Using Theorem 4.14, or by iterating the recurrence or by using recursion trees, we get*

$$T(n) = 3^n(5 + (2n^3 + 3n^2 + n)/6) = \frac{3^n}{6}\left(2n^3 + 3n^2 + n + 30\right).$$

(b) Base Case $n = 0$:
$T(0) = \frac{3^0}{6}(30) = 5.$

Inductive Hypothesis: Assume $n > 0$ and that formula holds for $n - 1$, i.e.,

$$T(n-1) = \frac{3^{n-1}}{6}\left(2(n-1)^3 + 3(n-1)^2 + (n-1) + 30\right).$$

Then

$$\begin{aligned} T(n) &= 3T(n-1) + n^2 3^n \\ &= 3\frac{3^{n-1}}{6}\left(2(n-1)^3 + 3(n-1)^2 + (n-1) + 30\right) + n^2 3^n \\ &= \frac{3^n}{6}\left(2(n-1)^3 + 3(n-1)^2 + (n-1) + 30 + 6n^2\right) \\ &= \frac{3^n}{6}\left(2(n-1)^3 + 3(n-1)^2 + (n-1) + 30 + 6n^2\right) \\ &= \frac{3^n}{6}\left((2n^3 - 6n^2 + 6n - 2) + (3n^2 - 6n + 3) + (n-1) + 30 + 6n^2\right) \\ &= \frac{3^n}{6}\left(2n^3 + 3n^2 + n + 30\right) \end{aligned}$$

We have just proven the inductive step.

So by the principle of mathematical induction, we see that the formula holds for all integers $n \geq 0$.

Problem 10: (12 pts)
(a) Consider the recurrence below defined on $n \geq 1$?.

$$T(n) = \begin{cases} 2 & \text{if } n = 1 \\ 2T\left(\frac{n}{4}\right) + 3n & \text{if } n > 1 \end{cases}$$

Give a closed-form, exact solution to the recurrence.
Your solution should assume that n is always a power of 4. You only have to give the solution. You do not need to show how you derived it.
(b) Now, prove the correctness of your solution by induction.

(a) Use recursion tree or iterate the recurrence:

$$\begin{aligned} T(n) &= 2T(n/4) + 3n \\ &= 2(2T(n/16) + 3n/4) + 3n \\ &= 2^2T(n/4^2) + 3n/2^1 + 3n \\ &= 2^2(2T(n/4^3) + 3n/4^2) + 3n/2^1 + 3n \\ &= 2^3T(n/4^3) + 3n/2^2 + 3n/2^1 + 3n \\ &\vdots \\ &= 2^{\log_4 n}T(n/4^{\log_4 n}) + 3n/2^{\log_4(n)-1} + \ldots + 3n/2^2 + 3n/2^1 + 3n \\ &= 2^{\log_4 n}T(1) + 3n\sum_{i=0}^{\log_4(n)-1}(1/2)^i \\ &= 2^{\log_4 n} \cdot +3n\frac{1-(1/2)^{\log_4 n}}{1-(1/2)} \\ &= 2^{1+\log_4 n} + 3n \cdot 2(1-(1/2)^{\log_4 n}) \\ &= 2^{1+\log_4 n} + 6n(1-(1/2)^{\log_4 n}) \end{aligned}$$

Now, noting that $2^{\log_4 n} = \sqrt{n}$ this gives

$$T(n) = 2\sqrt{n} + 6n\left(1 - \frac{1}{\sqrt{n}}\right) = 6n - 4\sqrt{n}.$$

(b) Base Case $n = 1$: $T(1) = 6 - 4\sqrt{1} = 2$.
Inductive Hypothesis: If $m = 4^j$ with $1 \leq j < i$, then $T(m) = 6m - 4\sqrt{m}$.
Now suppose $n = 4^i$.
By the i.h., $T(n/4) = 6\frac{n}{4} - 4\sqrt{\frac{n}{4}} = 3\frac{n}{2} - 2\sqrt{n}$, so

$$\begin{aligned} T(n) &= 2T(n/4) + 3n \\ &= 2\left(3\frac{n}{2} - 2\sqrt{n}\right) + 3n \\ &= 6n - 4\sqrt{n} \end{aligned}$$

and we have just proven the inductive step. So by the principle of mathematical induction, we see the formula holds for all integers $n \geq 1$ *that are multiples of* 4.

Alternatively, we can use induction on the longer form of the solution.

Base Case $n = 1$*:* $T(1) = 2^{1+\log_4 1} + 6 \cdot 1(1 - (1/2)^{\log_4 1}) = 2 + 0 = 2.$

Inductive Hypothesis: If $m = 4^j$ *with* $1 \leq j < i$*, then* $T(m) = 2^{1+\log_4 m} + 6m(1 - (1/2)^{\log_4 m})$.

Now suppose $n = 4^i$.

By the i.h., $T(n/4) = 2^{1+\log_4 n/4} + 6n/4(1 - (1/2)^{\log_4 n/4})$*, so*

$$\begin{aligned}
T(n) &= 2T(n/4) + 3n \\
&= 2(2^{1+\log_4 n/4} + 6n/4(1 - (1/2)^{\log_4 n/4})) + 3n \\
&= 2^{1+\log_4 n} + 3n - 3n(1/2)^{\log_4 n/4} + 3n \\
&= 2^{1+\log_4 n} + 6n - 6n(1/2)(1/2)^{\log_4 (n)-1} \\
&= 2^{1+\log_4 n} + 6n - 6n(1/2)^{\log_4 n} \\
&= 2^{1+\log_4 n} + 6n(1 - (1/2)^{\log_4 n})
\end{aligned}$$

We have just proven the inductive step.

So by the principle of mathematical induction, we see the formula holds for all integers $n \geq 1$ *that are multiples of* 4.