Module Title: dmmr
Exam Diet (Dec/April/Aug): Sample 2014
Brief notes on answers:
PART A

1. (a) A relation R over A is reflexive if for all $a \in A$ aRa.

   (b) A relation R over A is transitive if for all $a, b, c \in A$, if aRb and bRc then aRc.

   (c) A relation R over A is symmetric if for all $a, b \in A$, if aRb then bRa.

   (d) ($\Rightarrow$) An equivalence relation is a relation that is reflexive, symmetric, and transitive. Thus we just need to prove that R is symmetric and transitive.

   Symmetry Let $a, b \in A$ such that aRb. By reflexivity of R we have that aRa. But then by circularity of R, because aRa and aRb, we also have that bRa. Thus R is symmetric.

   Transitivity Let $a, b, c \in A$ such that aRb and bRc. By circularity we have that cRa. But we just proved that R is symmetric, so we can conclude that aRc, and thus that R is transitive.

   ($\Leftarrow$) We just need to prove that R is circular. Let $a, b, c \in A$ such that aRb and bRc. By transitivity of equivalence relations we have that aRc. But then by symmetry of equivalence relations we have that cRa. Thus R is circular.

2. Let x be a string in $\{0,1\}^*$. We will denote $|x|_0$ the number of 0's in x, and $|x|_1$ the number of 1's in x. We prove this by induction on the length ℓ of x.

   Base case ($\ell = 0$). In that case, x is the empty string. If we let $y = z = \varepsilon$, then we do have that $x = \varepsilon = \varepsilon \cdot \varepsilon = y \cdot z$, and $|y|_0 = 0 = |z|_1$.

   Inductive hypothesis. Let $k \in \mathbb{N}$. We assume that for all $x \in \{0,1\}^*$, if $|x| \leq k$ then there exist $y, z \in \{0,1\}^*$ such that $x = y \cdot z$, and $|y|_0 = |z|_1$.

   Inductive step ($\ell = k+1$). In that case $x = x' \cdot b$ with $b \in \{0,1\}$, and $x' \in \{0,1\}^*$ such that $|x'| = k$. By inductive hypothesis we know there exist $y', z' \in \{0,1\}^*$ such that $x' = y' \cdot z'$, and $|y'|_0 = |z'|_1$. We distinguish 2 cases:

   Case $b = 0$. In that case $|z' \cdot b|_1 = |z' \cdot 0|_1 = |z'|_1$, and thus $|y'|_0 = |z' \cdot b|_1$. So if we let $y = y'$ and $z = z' \cdot b$, we do have that $x = x' \cdot b = y' \cdot z' \cdot b = y \cdot z$, and $|y|_0 = |y'|_0 = |z' \cdot b|_1 = |z|_1$.

   Case $b = 1$. We distinguish three cases

   Case $z' = \varepsilon$. In that case $|y'|_0 = 0 = |z'|_1$ and $x = y' \cdot 1$. Let $y = y' \cdot 1$ and $z = \varepsilon$. Then we do have that $x = y' \cdot 1 = y' \cdot 1 \cdot \varepsilon = y \cdot z$. Furthermore, $|y|_0 = |y' \cdot 1|_0 = |y'|_0 = 0 = |\varepsilon|_1 = |z|_1$.

   Case $z' = 0 \cdot z''$. In that case $|y'|_0 = |z'|_1 = |0 \cdot z''|_1 = |z''|_1$. Thus $|y' \cdot 0|_0 = 1 + |y'|_0 = 1 + |z'|_1 = 1 + |z''|_1 = |z'' \cdot 1|_1 = |z'' \cdot b|_1$. So if we let $y = y' \cdot 0$ and $z = z'' \cdot 1$, we do have $x = y' \cdot z' \cdot b = y' \cdot 0 \cdot z'' \cdot 1 = y \cdot z$, and $|y|_0 = |y' \cdot 0|_0 = |y'|_0 + 1 = |z'|_1 + 1 = |z''|_1 + 1 = |z'' \cdot 1|_1 = |z|_1$.

   Case $z' = 1 \cdot z''$. In that case $|y'|_0 = |z'|_1 = |1 \cdot z''|_1 = |z'' \cdot 1|_1$. Furthermore, $|y'|_0 = |y' \cdot 1|_0$. So if we let $y = y' \cdot 1$ and $z = z'' \cdot 1$, we do have $x = y' \cdot z' \cdot b = y' \cdot 1 \cdot z'' \cdot 1 = y \cdot z$, and $|y|_0 = |y' \cdot 1|_0 = |y'|_0 = |z'|_1 = |1 \cdot z''|_1 = |z'' \cdot 1|_1 = |z|_1$.

3. (a) The procedure `ex3` applied to $\bar{a}$ returns 1

   The procedure `ex3` applied to $\bar{c}$ returns -1

   (b) The procedure `ex3` looks for the first element in the sequence given as argument that occurs twice in that sequence

   (c) On an input sequence of sice n, the outer `while` loop is executed at most $n-1$ times. At the i^{th} iteration of the outer `while` loop, the inner `while` loop will be executed at most $n-i$ times (in the case where no element occurs twice in the input sequence). So the inner `while` loop will be executed at most $\sum_{k=1}^{n-1} k$ times, and at each of these iterations 2 comparisons are performed (the test that controls the `while` loop and the test in the `if`). Thus, in total the maximum number of comparisons that can be performed is:

$$
\begin{array}{rcll}
A_n & = & n-1 & \text{one comparison at each iteration of the outer } \texttt{while} \text{ loop} \\
 & + & 1 & \text{the comparison that makes the outer } \texttt{while} \text{ loop break} \\
 & + & \sum_{k=1}^{n-1} 2k & \text{2 comparisons at each iteration of the inner } \texttt{while} \text{ loop} \\
 & + & n-1 & \text{the comparisons that makes the inner } \texttt{while} \text{ loop break} \\
 & & & \\
 & = & 2n-1+2\sum_{k=1}^{n-1} k & \\
 & & & \\
 & = & n^2+n-1 &
\end{array}
$$

   (d) (i). Let $k=1$ and $C=2$. In that case, we have

$$\forall n \geq k.\ n \leq n^2$$

But this implies that

$$\forall n \geq k.\ n^2+n \leq n^2+n^2 = Cn^2$$

Furthermore, we trivially have that

$$\forall n \geq k.\ n^2+n-1 \leq n^2+n$$

Combining all these we can conclude that

$$\forall n \geq k.\ A_n = n^2+n-1 \leq Cn^2$$

which proves that $k=1$ and $C=2$ are witnesses that $A_n \in \mathcal{O}(n^2)$.

(ii). Let $k=1$ and $C=1$. In that case, we have

$$\forall n \geq k.\ n-1 \geq 0$$

But this implies that

$$\forall n \geq k.\ A_n = n^2+n-1 \geq n^2 = Cn^2$$

which proves that $k=1$ and $C=1$ are witnesses that $A_n \in \Omega(n^2)$.

We can finally conclude by definition that $A_n \in \Theta(n^2)$.

4. (a) Bookwork. Suppose no box has more than $\lceil \frac{N}{k} \rceil - 1$ objects. Sum up the number of objects in the k boxes. It is at most $k \cdot (\lceil \frac{N}{k} \rceil - 1) < k \cdot ((\frac{N}{k} + 1) - 1) = N$. Thus, there must be fewer than N. Contradiction. Full marks for full answer. They could do it inductively too.

   (b) Let a_j be the number of games played on or before the jth day of the three weeks, $1 \leq j \leq 21$. So, $a_1, \ldots, a_{21}$ is a strictly increasing sequence with $a_{21} = 30$. Consider the second sequence $a_1 + 11, \ldots, a_{21} + 11$ which is also strictly increasing with $a_{21} + 11 = 41$; we now have 42 elements and 41 pigeonholes; so $a_i = a_j + 11$ for some different i and j. Full marks for a full answer.

5. (a) With in the first 10 positive integers we identify the following pairs that have sum 11: $(1, 10), (2, 9), (3, 8), (4, 7), (5, 6)$. By the pigeon-hole principle, we can select at most 5 integers, that are in pairwise distinct pairs. Therefore choosing the 6th and the 7th number we have to have chosen 2 integers each from the same set.

   (b) No: We can chose the numbers $1, 2, 3, 4, 5, 6$. By the list of pairs we have specified in a) we get that only the pair $(5, 6)$ has sum 11.

   (c) Proof by induction over n: As Base case ($n = 1$) we have the original pigeon hole principle. Assume now the statement is true for n and look at the statement for $n + 1$. Choose $k + n$ elements from S first. We have already chosen at least n pairs. If we have chosen $n + 1$ pairs then we are done. If we have not chosen $n + 1$ pairs, then we have chosen $2 * n$ numbers in pairs and the remaining $k - n$ as singles. As there are only k pairs that means each pair has been chosen either as single or as pair. By choosing one number more we need to choose a number from a pair that has already been chosen before. Therefore creating a new pair in the chosen numbers.

   By Induction principle the induction hold therefore for all $n \geq 1$

PART B

6. (a) Since p is a prime number, any integer $x \in (\mathbb{Z}_p)^*$ is coprime with p, *i.e.* $\gcd(x, p) = 1$. Thus, according to the theorem seen in lectures x admits an inverse mod p.

   (b) It is easy to see that $21 \cdot 3 \equiv 63 \equiv 1 + 31 \cdot 2 \equiv 1 \pmod{31}$.

   (c) Let $x \in (\mathbb{Z}_p)^*$ that is its own iverse in mod p arithmetic, *i.e.* $x^2 \equiv 1 \pmod{p}$. Then $x^2 - 1 \equiv 0 \pmod{p}$, but this is equivalent to $(x-1)(x+1) \equiv 0 \pmod{p}$ which in turn is equivalent to $p|(x - 1)(x + 1)$. Since p is prime, it must be that either $p|(x - 1)$ or $p|(x + 1)$. In other words, it must be that either $x - 1 \equiv 0 \pmod{p}$ or $x + 1 \equiv 0 \pmod{p}$. Hence, either $x \equiv -1 \pmod{p}$ or $x \equiv 1 \pmod{p}$. Because $x \in (\mathbb{Z})^*$, only $x = p - 1$ satisfies the first possibility, and only $x = 1$ satisfies the second. Which concludes our proof.

   (d) Assume there exist two distinct integers $x, y \in (\mathbb{Z})^*$ such that $x^{-1} = y^{-1}$. Let z be x^{-1}. That is we assume that $x \cdot z \equiv 1 \pmod{p}$ and $y \cdot z \equiv 1 \pmod{p}$. We further assume without loss of generality that $x > y$.

   It must thus be that $z \cdot (x - y) \equiv 0 \pmod{p}$, or equivalently that $p|z \cdot (x - y)$. Now, since z and p are coprime, we know that $p \not| z$. Thus, since p is prime, it must be that $p|(x - y)$. But $x, y \in (\mathbb{Z}_p)^*$ and $x > y$ imply that $1 \leq x - y \leq p - 2$. Then the only way to have $p|(x - y)$ is to have $x - y = 0$, and thus $x = y$ which contradicts our hypothesis. We can hence conclude that all integers in $(\mathbb{Z}_p)^*$ have a different inverst in mod p arithmetic.

(e) We distinguish two cases:

Case $p = 2$. In that case $(p-1) = (p-1)!$ thus $(p-1) \equiv (p-1)! \pmod{p}$.

Case $p > 2$. In that case there is an even number of intergers in $\{2, \ldots, p-2\}$. According to what we showed in items **??** **??** and **??**, each integer in $\{2, \ldots, p-2\}$ has a distinct inverse mod p in $\{2, \ldots, p-2\}$. Thus each term in the product $2 \ldots (p-2)$ will pair up with its inverse, that is $2 \ldots (p-2) \equiv 1 \ldots 1 \pmod{p}$. Thus $(p-1)! \equiv (p-1) \cdot 1 \ldots 1 \equiv (p-1) \pmod{p}$ which concludes our proof.

7. (a) The graph G is connected, if for every pair of vertices $v, v' \in V$ there is a path $v \to v'$. A path is a sequence of edges $(v, v_1), (v_1, v_2), ..., (v_n, v')$ with $(v, v_1) \in E$, $(v_i, v_{i+1}) \in E$ and $(v_n, v') \in E$.

(b) Inserting an edge can only connect two connected components at a time. Assume a new edge (v, v') connects 3 components H_1, H_2 and H_3. Take the vertices $v_1 \in H_1, v_2 \in H_2$ and $v_3 \in H_3$. Then there exist two paths that use the edge (v, v') in the same direction. Let without loose of generality $v_1 \to v \to v' \to v_2$ and $v_3 \to v \to v' \to v_2$. Then the path $v_1 \to v \to v_2$ is a path that does not use the new edge. Therefore H_1 and H_2 where connected before.

After inserting one edge we have reduced G to a graph with $k-1$ connected components and we can apply the same argument again. Therefore the insertion of each edge reduces the number of connected components by at most 1. Inserting $k-1$ edges reduces the components by $k-1$. Since 1 connected component is left the graph must have had k connected components. further inserted edge can connect one further connected component. Therefore if we insert $k-1$ edges we can connect at most k connected components.

(c) In $G - x$ there is ate least one connected component and at most $\deg(x)$ components. As example the star graph $V = \{v_1, ..., v_n\}$ with $E = \{(v_1, v_i \mid i \in \{2, ..., n\}\}$. If we choose $x = v_1$ then $G - x$ does not have any edges and thus we get $n-1$ connected components, which is $\deg(x)$. If we choose x to be v_2, then we only remove one edge (v_1, v_2). v_1 is still connected to each other vertex and thus we still have a path from v_i to v_1 and further to v_j for $i, j \in \{3, ..., n\}$. The lower bound does not need to be proved as every graph has at least one connected component.

The upper bound can be proved in the following way: Assume the vertex x has degree l. That means the neighbours of x can be written as $x_1, ..., x_l$. We now insert the $l-1$ edges $(x_1, x_2), (x_2, x_3), ..., (x_{l-1}, x_l)$. Consider a path $v \to v'$ in G: if the path does not use x it is still a path in $G - x$. If the path did use the edges $(x_i, x), (x, x_j)$ (without loss of generality $i > j$, then we can replace these two edges by the path $(x_i, x_{i+1}), (x_{i+1}, x_{i+2}), ..., (x_{j+1}, xj)$. Since all pairs of vertices were connected by a path in G we now have a path between each pair in the modified graph and therefore the Graph is connected. As we have only inserted $l-1$ edges compared to $G-x$ we get that $G-x$ has at most l connected components

(d) We proceed by induction on $|V(G)|$. As a base case, observe that if G is a connected graph with $|V(G)| = 2$, then both vertices of G satisfy the required conclusion. For the inductive step, let G be a connected graph with $|V(G)| \geq 2$ and assume that the theorem holds for every graph with $< |V(G)|$ vertices. If $G - x$ is connected for every vertex $x \in V(G)$, then we are done, so we may assume this is not so, and choose $x \in V(G)$ so that $G - x$ has components $H_1, H_2, ..., H_m$ where $m \geq 2$. For every $1 \leq i \leq m$ let H_i' be the graph obtained from H_i by adding back the vertex x and all edges with one end x and the other end in $V(H_i)$. So every H_i' is a connected graph with at least two vertices. Furthermore,$|V(H_i')| < |V(G)|$, so by induction, H_i' must have at least one vertex $x_i \neq x$ so that $H_i' - x_i$ is connected. It then follows that $G - x_i$ is connected. Since we have such an x_i for every component (and at least two components), this completes the proof.

8. (a) This is the values for $1, \ldots, 8$

$$1/8 + 2/8 + 3/8 + 4/8 + 5/8 + 6/8 + 7/8 + 8/8$$

which is 9/2. Full marks for doing the calculation.

(b) Just a question of calculations:

$$E(\sum_{i=1}^{n} X_i) = \sum_{s \in S} P(s) \sum_{i=1}^{n} X_i(s) = \sum_{i=1}^{n} \sum_{s \in S} P(s) X_i(s) = \sum_{i=1}^{n} E(X_i).$$

$$E(aX + b) = \sum_{s \in S} P(s)(aX(s) + b) = (a \sum_{s \in S} P(s)X(s)) + b \sum_{s \in S} P(s)$$

. Full marks accordingly.

(c) Use linearity to calculate result for five octal dice to get 45/2 (five times 9/2). Full marks for doing this.

(d) A straightforward calculation does this.

$$\begin{aligned} V(X) &= E((X - E(X))^2) \\ &= E(X^2 - 2XE(X) + E(X)^2) \\ &= E(X^2) - 2E(X)E(X) + E(X)^2 \\ &= E(X^2) - E(X)^2. \end{aligned}$$

Full marks again for full answer.