Mini-Quiz 3

1. Write your name:

2. **Velleman 2.3, Ex. 5:** Let $I = \{2, 3\}$, and for each $i \in I$ let $A_i = \{i, 2i\}$ and $B_i = \{i, i+1\}$.

   (a) List the elements of the sets A_i and B_i for all $i \in I$.

   Solution:
   For $i = 2$, $A_i = \{2,4\}$ and $B_i = \{2,3\}$.
   For $i = 3$, $A_i = \{3,6\}$ and $B_i = \{3,4\}$.

   (b) Find $\cap_{i \in I}(A_i \cup B_i)$ and $(\cap_{i \in I} A_i) \cup (\cap_{i \in I} B_i)$. Are they the same?

   Solution:

$$\begin{aligned}\cap_{i \in I}(A_i \cup B_i) &= (A_2 \cup B_2) \cap (A_3 \cup B_3)\\ &= \{2,3,4\} \cap \{3,4,6\}\\ &= \{3,4\}\end{aligned}$$

$$\begin{aligned}(\cap_{i \in I} A_i) \cup (\cap_{i \in I} B_i) &= (A_2 \cap A_3) \cup (B_2 \cap B_3)\\ &= \emptyset \cup \{3\}\\ &= \{3\}\end{aligned}$$

   Therefore, the two sets are not equal.

Tutorial 3 Problems

Problem 1 Well ordering

Rosen 3.2, Ex. 58: The well-ordering property can be used to show that there is a unique greatest common divisor of two positive integers. Let a and b be positive integers, and let S be the set of positive integers of the form $as + bt$, where s and t are integers.
a) Show that S is nonempty.
b) Use the well-ordering property to show that S has a smallest element c.
c) Show that if d is a common divisor of a and b, then d is a divisor of c.
d) Show that $c|a$ and $c|b$. (Hint: First, assume that $c \not| a$. Then $a = qc + r$, where $0 < r < c$. Show that $r \in S$, contradicting the choice of c.)
e) Conclude from (c) and (d) that the greatest common divisor of a and b exists. Finish the proof by showing that this greatest common divisor of two positive integers is unique.

Solutions:

a For example, just set $s = 1$, and $t = 1$. Then $as + bt = a + b$, which is a positive integer by our definitions of a and b.

b The Well Ordering Property states that every non-empty set of non-negative integers has a smallest member. Since we just showed in part a that the set S is non-empty, it must have a smallest member, which we may call c.

c If d divides a and b, then d divides as and bt for any positive integers a and b. Therefore, d also divides the sum $as + bt$. Since $c \in S$, c must be such a sum, by our definition of membership in S. Therefore, d can divide c.

d We will just show $c|a$, as the argument is identical to show $c|b$.
Proof by Contradiction.
Assume for the purpose of contradiction that $c \not| a$.
If c does not evenly divide into a, then we can write the expression $a = qc + r$, for some postive integer r, where $0 < r < c$.
We can rewrite this in terms of r: $r = a - qc$.
Now, since $c \in S$, we know that c is of the form $c = as + bt$, for some integral values of s and t. Rewriting our expression for r again, we get:
$r = a - qc = a - q(as + bt) = a - aqs - qbt = a(1 - qs) + b(-qt)$. But now we are done, because we have expressed the positive integer r as a linear combination with integer coefficients of a and b. This means that $r \in S$, which we know is not possible since $r < c$. Thus, we have a contradiction, and our assumption that $c \not| a$ must be wrong, so we can conclude that $c|a$.

e Finally, by part (d), c is a divisor of both a and b. Furthermore, from part (c) we know that any divisor of both a and b is also a divisor of c. This means that every common divisor of a and b is no greater than c, and so c is the greatest common divisor of a and b. To see that the greatest common divisor of a number is unique, one just needs to note that it makes no sense to have two numbers, each of which is greater than the other.

Problem 2 Induction and Recursive Algorithms

Procedure *binary search*(x, i, j)
$m := \lfloor (i+j)/2 \rfloor$
if $x = a_m$ **then**
  $location := m$
else if ($x < a_m$ and $i < m$) **then**
  binary search$(x, i, m-1)$
else if ($x > a_m$ and $j > m$) **then**
  binary search$(x, m+1, j)$
else $location := 0$

The above procedure searches x in a sequence $a_1, a_2, \ldots, a_n$ (when called with $i = 1$, $j = n$). Prove by (strong) induction that the binary search procedure sets *location* to an index i such that $a_i = x$, if there is such an index, and otherwise sets *location* to 0.

Solution:
Proof by Strong Induction:

P(n): The binary search procedure correctly searches a list of length n such that the *location* variable is set to i, where $a_i = x$, if such an index exists, and otherwise *location* is set to 0.

Base Case: P(1) - Calling binary search on an array consisting of one element. If that element is equal to x, then, according to the first *if statement*, *location* will be set equal to $\lfloor (i+2)/2 \rfloor = \lfloor (1+1)/2 \rfloor = 1$, as desired. If, however, $a_1 \neq 1$, then since i is not less than m and j is not greater than m $(i = 1, j = 1, m = 1)$, the program would go to the final *else statement*, where *location* gets set to 0, as desired.

P(n+1): To see that this procedure correctly searches a list of length $(n+1)$, we need only to check that the two *else if statements* do the correct thing, because they each call binary search on a smaller array, which, we know by our strong inductive hypothesis, will get searched correctly. Now, if the element we are looking for (x), is less than a_m and $i < m$ (meaning that there are more indices to search through), then the procedure gets called again on a smaller array, that consisting of indices i up to $m-1$. We already know the procedure searches this correctly by our strong inductive hypothesis. The second *else if statement* does the same thing if x is bigger than our current element $(x > a_m)$, and there is more of the array to search through $(j > m)$. Therefore, the procedure correctly calls itself on a smaller array, which by P(n) we know does the correct search. Therefore, we have show that $P(1) \vee P(2) \vee P(3) \vee \ldots \vee P(n) \implies P(n+1)$, and our proof by strong induction is complete.

Problem 3 Relations

(a) Consider the following putative theorem and the accompanying proof.

Theorem. *For any sets* A*,* B*,* C*, and* D*, if* $A \times B \subseteq C \times D$ *then* $A \subseteq C$ *and* $B \subseteq D$*.*

Proof. Suppose $A \times B \subseteq C \times D$. Let a be an arbitrary element of A, b be an arbitrary element of B, and $(a, b) \in A \times B$. Since $A \times B \subseteq C \times D$, it follows that $(a, b) \in C \times D$. Therefore, $a \in C$ and $b \in D$. Since a and b were arbitrary elements of A and B, respectively, this shows that $A \subseteq C$ and $B \subseteq D$. ■

Is the proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct?

Solution:
The problem lies in the statement *"let a be an arbitrary element of A"* (and without loss of generality, b an arbitrary element in B). Namely, if $A = \emptyset$, $B = \{1, 2, 3\}$, $C = \{1, 2\}$, and $D = \{3, 4\}$, then $A \times B \subseteq C \times D$ ($\emptyset \subseteq E$ for any set E), but $B \not\subseteq D$. This is an example of the proof failing at a boundary case.

(b) Let A be the adjacency matrix for a digraph G with n vertices. Note that A is a zero-one valued $n \times n$ matrix. In this problem we use the Boolean "OR" operation, $\vee$, instead of "+" when multiplying zero-one valued matrices (this is called "boolean" matrix product).

(i) For $k \in \mathbb{N}$, let A^k be the kth *Boolean* power of A. Prove that ${A^k}_{ij} = 1$ iff there is a directed path of length k from the ith to the jth vertex of G.

Solution:
Let $P(n)$ be the predicate that $A^n_{ij} = 1$ iff there is a directed path of length n from the ith to the jth vertex of G. We prove that $P(n)$ holds for all $n \geq 1$ by induction on n.

Inductive Hypothesis: $P(k) : A^k_{ij} = 1$ iff there is a directed path of length k from the ith to the jth vertex of G.

Base Case: $k = 1$. By the definition of an adjacency matrix A, $A_{ij} = 1$ iff there is a directed edge (directed path of length $k = 1$) from the ith to the jth vertex of G.

Inductive Step: Assume $P(k)$ to prove $P(k + 1)$.

$$A^k_{ij} = \bigvee_{l \in G} (A^k_{il} \wedge A_{lj})$$

Now we consider both directions for the iff.

Case 1:

There is a directed path of length $k + 1$ from the ith to the jth vertex of G. This path looks like $i, i_1, i_2, \ldots i_k, j$. Then consider $l = i_k$. $A^k_{il} = 1$ (inductive hypothesis). $A_{lj} = 1$ (there is an edge from i_k to j), under the Case 1 assumption. Therefore,

$$({A^k}_{il} \wedge A_{lj}) = 1$$

$$A^{k+1}{}_{ij} = 1$$

Case 2: $A^{k+1}_{ij} = 1$.

Then $\exists\ l \in G : (A^k_{il} \wedge A_{lj}) = 1$. Thus there is an edge from l to j and there is path of length k from i to l(by the inductive hypothesis) which looks like $i, i_1, i_2, \ldots i_{k-1}, l$. Thus, there is a path of length $k+1$ from i to j which hits l on the kth step and then has the $k+1$st edge from l to j. This path follows the vertices: $i, i_1, i_2, \ldots i_{k-1}, l, j$.

Q.E.D.

(ii) Let $B = A \vee I$ where I is the $n \times n$ identity matrix. Prove that $B^k_{ij} = 1$ iff there is a directed path of length $\leq k$ from the ith to the jth vertex of G.

Solution:
From part a, it can be seen that $B^k_{ij} = 1$ iff there is a directed path of length k from the ith to the jth vertex of G', where G' is the graph described by the adjacency matrix B. Since G' is just G with self loops, a path exists between i and j in G' iff a path exists between i and j in G (all vertices have paths of length 0 to themselves).

For any such path between i and j in G', either it uses a self-loop edge or it does not. If it does not, then the equivalent path in G will have the same length. If it does, then there is a shorter path in G which can be obtained by not using the self loop. So if there is a path of length k between i and j in G' then there is a path of length $\leq k$ between i and j in G.

If there is a path of length $\leq k$ between i and j in G, then it can be made to be of length k by using self loops to lengthen the path. Thus there is a path in G' of length k iff there is a path in G of length $\leq k$. Since $B^k_{ij} = 1$ iff there is a path of length k between i and j in G' then $B^k_{ij} = 1$ iff there is a path of length $\leq k$ between i and j in G.

(iii) Conclude that $B^n_{ij} = 1$ iff there is a directed path from the ith to the jth vertex.

Solution:
If $B^n_{ij} = 1$ then there is a directed path from the ith to the jth vertex. If $B^n_{ij} = 0$ then there is no path of length less than or equal to n from the ith to the jth vertex. There must also be no path of length greater than n from the ith to the jth vertex. If there were, then the path must cross through some vertices twice, since the length of the path is greater than n. For those vertices through which the path passes twice, eliminate the loops so that the path uses no vertex more than once. This means the path must be of length less than or equal to n, which reaches a contradiction, since we know that there are no paths from i to j of length less than or equal to n. Therefore, if ${B^n}_{ij} = 0$ there is no path from i to j at all.

Problem 4 Equivalence Relations Let $(a, b) \sim (c, d)$ if $a + d = b + c$. We claim that $\sim$ is an equivalence relation.

(a) Partition the set $\{0,1,2\} \times \{0,1,2\}$ into the distinct equivalence classes under $\sim$.

We can rewrite $(a,b) \sim (c,d)$ if $a+d=b+c$ as $(a,b) \sim (c,d)$ if $a-b=c-d$. This shows that with any equivalence class $\mathcal{C}$ we can associate a *difference* d such that $(a,b) \in \mathcal{C} \Rightarrow a-b=d$. This gives us an easy way to list the equivalence classes of $\{0,1,2\} \times \{0,1,2\}$.

- $d=-2:\ \{(0,2)\}$.
- $d=-1:\ \{(0,1),(1,2)\}$.
- $d=0:\ \{(0,0),(1,1),(2,2)\}$.
- $d=1:\ \{(1,0),(2,1)\}$.
- $d=2:\ \{(2,0)\}$.

(b) Prove that $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}$.

- *Reflexivity* $(a,b) \sim (a,b)$ since $a+b=b+a$.
- *Symmetry* $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$ since $a+d=b+c \Rightarrow c+b=d+a$.
- *Transitivity* Assume $(a,b) \sim (c,d)$, i.e. $a+d=b+c$. And, $(c,d) \sim (e,f)$, i.e. $c+f=d+e$. Adding we get $a+d+c+f=b+c+d+e$ or $a+f=b+e$, i.e. $(a,b) \sim (e,f)$. Hence $(a,b) \sim (c,d) \wedge (c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$.

Since $\sim$ is reflexive, symmetric and transitive it is an equivalence relation.

(c) How many distinct equivalence classes under $\sim$ are there on the set $\{0,1,\ldots,n\} \times \{0,1,\ldots,n\}$. You do not need to prove your answer.

$2n+1$ since the difference can be any value in $\{-n,\ldots,n\}$.